Top 20 - I maggiori pericoli da Internet per il 2004
Il parere degli esperti

----- Vai all'indice della Top 20 -----

Introduzione

La Top 20 del SANS delle vulnerabilità per la sicurezza Internet

La grande maggioranza dei worm e degli altri attacchi che provengono da Internet sono resi possibili dalle vulnerabilità presenti in un numero molto limitato di servizi dei più diffusi sistemi operativi.
Ciò si deve al fatto che coloro che effettuano gli attacchi agiscono in modo opportunistico, ovvero scelgono la strada più semplice e comoda, sfruttando le vulnerabilità più conosciute e impiegando gli strumenti di aggressione più efficaci e diffusi. Contano sul fatto che le organizzazioni spesso non pongono rimedio ai problemi e quindi spesso si conducono attacchi indiscriminati, scegliendo gli obiettivi dai risultati di una serie di scansioni in Internet per rilevare i sistemi vulnerabili.
La facile e distruttiva diffusione di worm come Blaster, Slammer e Code Red, ad esempio, può essere direttamente addebitata allo sfruttamento di vulnerabilità per le quali non sono state tempestivamente applicate le opportune correzioni.

Quattro anni fa, Il SANS Institute e il National Infrastructure Protection Center (NIPC) dell'l'FBI pubblicarono un documento che elencava Le dieci vulnerabilità più critiche per la sicurezza in Internet. Da allora migliaia di organizzazioni hanno utilizzato quella lista, e le sua evoluzioni in Venti vulnerabilità diffuse negli anni seguenti, come guida per risolvere rapidamente i buchi di sicurezza più pericolosi. I servizi vulnerabili che hanno favorito i tre esempi riportati sopra - i worm Blaster, Slammer e Code Red, come d'altra parte anche NIMDA - sono riportati su quella liste.

Questa versione aggiornata delle "Venti Vulnerabilità più critiche" è in effetti costituita da due liste di dieci: i dieci servizi di Windows e i dieci di Unix le cui vulnerabilità sono più frequentemente sfruttate condurre un attacco.
Sebbene vi siano migliaia di episodi di violazione della sicurezza che ogni anno colpiscono questi sistemi operativi, la stragrande maggioranza degli attacchi portati a termine sono diretti verso uno o più dei venti servizi considerati più vulnerabili.

Le Venti vulnerabilità più critiche è una lista delle vulnerabilità che richiedono un intervento immediato, ed è il risultato di un processo che riunisce assieme dozzine tra i principali esperti di sicurezza provenienti da molti paesi, da ambienti governativi, accademici e industriali.
Essi provengono dalle agenzie federali statunitensi più sensibili a problemi della sicurezza, dagli enti governativi di Gran Bretagna e Singapore, dai principali produttori di software per la sicurezza e dalle più importanti società di consulenza, dai migliori progetti universitari per la sicurezza, dal SANS Institute e da molte altre organizzazioni. L'elenco dei partecipanti è

disponibile alla fine del presente documento.

L'elenco SANS/FBI delle venti vulnerabilità più critiche è un documento in continuo aggiornamento. Contiene istruzioni dettagliate e riferimenti ad informazioni supplementari utili per correggere i problemi di sicurezza. Nel momento in cui si scoprono minacce più critiche di quelle elencate o metodi di intrusione più diffusi o più comodi, vengono aggiornati l'elenco delle vulnerabilità e le istruzioni per rimediare; in questo processo il vostro contributo è sempre gradito. Questo documento si basa sul consenso di un'intera comunità: la vostra esperienza nel combattere le intrusioni e nell'eliminare le vulnerabilità può aiutare quelli che verranno dopo di voi. Inviate i vostri suggerimenti via e-mail a top20@sans.org.

Note per i lettori

Codici CVE

Ogni vulnerabilità menzionata è accompagnata dai codici della catalogazione CVE (Common Vulnerabilities and Exposures). Spesso sono riportati anche i numeri CAN, ovvero i codici delle vulnerabilità che sono candidate ad essere incluse nella lista CVE, ma non sono state ancora completamente verificate. Per ulteriori informazioni relative al progetto CVE, oggetto di numerosi riconoscimenti ufficiali, consultate l'indirizzo http://cve.mitre.org.

I codici CVE e CAN corrispondono alle vulnerabilità più importanti che devono essere verificate per ciascuna voce. Ogni vulnerabilità CVE è collegata all'elemento corrispondente del servizio ICAT di indicizzazione delle vulnerabilità del National Institute of Standards (http://icat.nist.gov). Per ciascuna vulnerabilità ICAT fornisce una breve descrizione, un elenco delle caratteristiche (ad esempio ambito dell'attacco e danno potenziale), un elenco dei nomi e delle versioni dei software vulnerabili e i collegamenti ai bollettini sulle vulnerabilità e alle informazioni sulle patch.

Porte da bloccare a livello di firewall

---- Vai all'indice delle porte da bloccare su Firewall o sul Gateway ----

Alla fine del documento troverete una sezione aggiuntiva che presenta l'elenco delle porte più comunemente esplorate attaccate. Bloccando il traffico che passa attraverso le porte a livello di firewall o di altri dispositivi di protezione del perimetro della rete, potete ottenere uno strato di difesa aggiuntivo che vi aiuterà a tutelarvi da eventuali sviste o errori di configurazione. Tenete comunque presente che, anche se utilizzate un firewall per bloccare il traffico di rete diretto a una porta, essa non è protetta da possibili azioni causate da soggetti che si trovano già all'interno del perimetro, né dall'azione di hacker penetrati utilizzando altri metodi.
Ancora più sicura è la pratica di implementare per default a livello di firewall o di router delle regole di blocco (deny) di tutto ciò che non è esplicitamente permesso, piuttosto che bloccare una per una delle porte specifiche.

torna all'inizio ^

Le maggiori vulnerabilità dei sistemi Windows

Le maggiori vulnerabilità dei sistemi UNIX

torna all'inizio ^

Le maggiori vulnerabilità dei sistemi Windows (W)

W1 Server e Servizi Web

W1.1 Descrizione

Le installazioni di default di diversi server HTTP su piattaforme Windows e dei componenti aggiuntivi dedicati a servire richieste HTTP o contenuti multimediali in streaming verso Internet si sono dimostrate nel tempo vulnerabili ad un certo numero di attacchi piuttosto gravi. Gli effetti di queste vulnerabilità possono arrivare a:

- Interrompere il servizio
- Esporre o pregiudicare file o dati sensibili
- Permettere l'esecuzione di comandi incontrollati sul server
- Compromettere completamente il server

I server HTTP come IIS, Apache e iPlanet (ora SunOne) hanno presentato numerosi problemi per i quali sono state create delle patch quando sono stati scoperti. Accertatevi di utilizzare la versione più recente del server e che le patch siano aggiornate. Nella maggior parte dei software HTTP server la configurazione di default è piuttosto aperta e lascia grandi spazi agli exploit. Controllate la configurazione e assicuratevi che questa permetta solo le funzioni strettamente necessarie a fare sì che il sito web funzioni nel modo corretto.

IIS utilizza una funzione di programmazione nota come ISAPI per associare i file che hanno determinate estensioni con delle DLL (note come filtri ISAPI). I preprocessori come ColdFusion e PHP usano tali ISAPI, e lo stesso IIS include molti filtri ISAPI per gestire funzioni come Active Server Pages (ASP), i servizi web.Net e la condivisione di stampanti via Web. Molti filtri ISAPI installati per default con IIS non sono necessari nella maggior parte delle esigenze e molti di quei filtri sono sfruttati per condurre degli attacchi. Gli esempi di programmi dannosi che usano questo meccanismo di propagazione includono i ben noti worm Code Red e Code Red 2. Abilitate quindi solo le estensioni ISAPI che il web

server avrà bisogno di utilizzare. Sin raccomanda anche di limitare le opzioni HTTP che possono essere usate con ciascuna delle estensioni ISAPI abilitate.

La maggior parte dei web server software comprendono anche applicazioni di esempio o siti web realizzati per esemplificare le funzionalità del web server. Queste applicazioni non sono state progettate per operare in modo sicuro in un ambiente di produzione. Alcune applicazioni di esempio di IIS consentono di vedere da remoto i file o di sovrascriverne il contenuto, fino a permettere l'accesso da remoto ad altre informazioni critiche del server, compresa la password di amministrazione. Eliminate quindi queste applicazioni prima di collocare il server in ambiente di produzione.

Una installazione di IIS che non venga costantemente aggiornata è soggetta inoltre alle vulnerabilità scoperte dopo la data di rilascio. Tra queste vi sono le vulnerabilità PCT e SSL, corrette dalla patch MS04-011 di Microsoft, che possono portare a una condizione di Interruzione del servizio (DOS) o permettere a un aggressore di ottenere il controllo completo del server. L'applicazione tempestiva delle patch dei web server pubblicamente accessibili è quindi importantissima.

I componenti aggiuntivi di terze parti, come ColdFusion e php, possono introdurre ulteriori vulnerabilità in una installazione IIS, sia per configurazioni non corrette sia derivanti da vulnerabilità intrinseche nel prodotto.

W1.2 Sistemi operativi interessati
Qualunque sistema Microsoft Windows con un web server installato potrebbe esserne interessato. Tra questi sono compresi, ma non sono i soli:

- Microsoft IIS: Windows NT4.0 e successivi, incluso XP Professional
- Apache HTTP server: è supportato da Windows NT 4.0 SP3 e sistemi successivi, anche se si pensa che funzioni anche su Win95 e Win98
- Sun Java System/Sun One/iPlanet Web Server: Windows NT 4.0 SP6 e successivi

Attenzione: Windows 2000 Server ha IIS installato per default, come molti amministratori hanno scoperto durante il periodo di esplosione dei famigerati Nimda e Code Red. Si aggiunga a questo che alcune applicazioni di terze parti hanno bisogno di funzionalità fornite da IIS, per cui è possibile che quest'ultimo venga installato all'insaputa degli amministratori. Non pensate quindi che una rete sia immune da attacchi verso il web server semplicemente perché tale server non è stato volontariamente installato e controllate periodicamente le reti per rilevare la presenza di qualche web server "canaglia". Leggete il paragrafo "Come stabilire se siete a rischio" qui sotto per informazioni ulteriori.

W1.3 Riferimenti CVE/CAN

a. **IIS**

   Riferimenti CVE per IIS 2.0
   Riferimenti CVE per IIS 3.0
   Riferimenti CVE per IIS 4.0
   Riferimenti CVE per IIS 5.0

b. **Apache**
   CAN-2001-0729, CAN-2002-0249, CAN-2002-0654, CAN-2002-0661, CAN-2003-0016,

CAN-2003-0017, CAN-2003-0460, CAN-2003-0844, CAN-2004-0492, CAN-2004-0493

CVE-1999-0448, CVE-2000-0505, CVE-2001-1342, CVE-2001-1342

Moduli Apache: CAN-2003-0844, CAN-2004-0492

c. **iPlanet/Sun**
CAN-2002-0686, CAN-2002-1042, CAN-2002-1315, CAN-2002-1316, CAN-2003-0411,
CAN-2003-0412, CAN-2003-0414, CAN-2003-0676

CVE-2000-1077, CVE-2001-0252, CVE-2001-0327, CVE-2002-0845

d. **Add-on**
CAN-1999-0455, CAN-1999-0477, CAN-1999-1124, CAN-2001-0535, CAN-2001-1120,
CAN-2002-1309, CAN-2003-0172

CVE-1999-0756, CVE-1999-0922, CVE-1999-0924, CVE-2000-0410, CVE-2000-0538

ColdFusion: CVE-1999-0756¸ CVE-1999-0760, CVE-1999-0922, CVE-1999-0924, CAN-2002-1309, CAN-2004-0407, CVE-2000-0189, CVE-2000-0382, CVE-2000-0410,
CVE-2000-0538, CVE-2002-0576

PHP: CAN-2002-0249, CAN-2003-0172

e. **Altri Servizi**
CAN-1999-1369, CAN-2003-0227, CAN-2003-0349, CAN-2003-0725, CAN-2003-0905

CVE-1999-0896, CVE-1999-1045, CVE-2000-0211, CVE-2000-0272, CVE-2000-0474,
CVE-2000-1181, CVE-2001-0083

eEye SecureIIS: CAN-2001-0524

Jakarta Tomcat: CAN-2003-0045

W1.4 Come stabilire se si è a rischio
Qualunque installazione di default di un web server e quelle a cui non siano state applicate tutte le patch dovranno essere considerate vulnerabili.

La maggior parte dei produttori di server e servizi forniscono abbondanti informazioni riguardo i problemi di sicurezza in corso. Tra gli esempi vi sono:

- La Pagina principale e i Security Report per il Server HTTP Apache
- Il Microsoft TechNet Security Centre
- Il Microsoft Internet Information Server (IIS) Security Centre
- Il Sun Web, Portal, & Directory Servers Download Centre
- La Macromedia Security Zone

- Il servizio Real Networks Security Issues
- La Home Page di PHP e la sezione Downloads

Controllate *regolarmente* tra le informazioni per la sicurezza offerte dal produttore e nel database CVE il livello di aggiornamento della versione e delle patch per il web server e i servizi associati, configurazioni incluse, per valutare le potenziali vulnerabilità. È importante rendersi conto che continuamente si scoprono nuovi problemi e la procedura più corretta è quella di consultare sempre l'aggiornamento del database CVE per verificare le potenziali vulnerabilità.

Esistono alcuni strumenti di verifica, locali e da remoto, che aiutano gli amministratori dei web server ad analizzare la propria rete. Tra questi vi sono:

- Nessus (Open-source)
- SARA (Open-source)
- Nikto (Open-source)
- eEye Free Utilities & Commercial Scanners
- Microsoft Baseline Security Analyzer (specifico per IIS)

Si raccomanda di utilizzare gli strumenti di verifica da remoto su tutta la rete e non solo per i server conosciuti, in modo da poter rilevare le potenziali vulnerabilità dei web server "canaglia".

W1.5 Come proteggersi

Per la maggior parte dei sistemi

1. Applicando le relative patch sia per il servizio HTTP, sia per il Sistema Operativo e per qualsiasi applicazione caricata sulla stesso host. Una volta applicate le patch più recenti, mantenetele aggiornate.
2. Istallando sull'host software anti-virus e Intrusion Detection. Assicuratevi che siano entrambi aggiornati per quanto riguarda le patch e controllate spesso i file di log.
3. Disabilitando gli interpreti di script non utilizzati ed eliminando i relativi file binari. Questi comprendono, ad esempio, perl, perlscript, vbscript, jscript, javascript e php.
4. Abilitando il logging se l'opzione e disponibile e controllando frequentemente i log, preferibilmente attraverso un processo automatizzato che riassuma gli eventi e sottolinei le anomalie e gli eventi sospetti.
5. Utilizzando un sistema tipo syslog per salvare i log del Sistema Operativo e del servizio HTTP su un sistema diverso.
6. Rimovendo o limitando gli strumenti di sistema che di solito vengono usati dagli aggressori come appoggio sia per la cattura della prima macchina, sia per espandersi verso altri sistemi come, ad esempio, tftp(.exe), ftp(.exe), cmd.exe, bash, net.exe, remote.exe e telnet(.exe).
7. Limitando le applicazioni attive sull'host al servizio HTTP e ai servizi correlati.
8. Dove possibile, evitando di gestire un dominio o altri sistemi di autenticazione sullo stesso host del web server.
9. Ponendo attenzione e riducendo al minimo qualsiasi flusso di dati delle rete interna che entri attraverso il/i web server pubblici come le condivisioni NetBIOS, le relazioni di trust e le interazioni database.
10. Utilizzando per i sistemi con affaccio pubblico delle convenzioni diverse per denominare gli account e password non abituali rispetto a quelle dei sistemi interni. Qualsiasi fuga di notizie da un sistema con affaccio pubblico non deve essere d'aiuto per un attacco verso i sistemi interni.

a. IIS

Applicare le patch al server al momento dell'installazione è un'operazione necessaria ma non sufficiente. Quando vengono scoperti nuovi difetti di IIS, applicate la patch conseguente. Per installazioni su un singolo server, potete scegliere di utilizzare Windows Update e l'Aggiornamento Automatico. HFNetChk, Network Security Hotfix Checker, assiste gli amministratori di sistema nell'analisi di sistemi locali o remoti per la verifica delle patch da aggiornare. Tale strumento funziona su Windows NT 4, Windows 2000 e Windows XP. La versione attuale può essere scaricata da Microsoft all'indirizzo http://www.microsoft.com/technet/security/tools/hfnetchk.asp.

Su questo argomento, inoltre, potete trovare nella SANS Reading Room un documento molto utile dal titolo Securing a Windows 2000 IIS Web Server – Lessons Learned, redatto da Harpal.

Utilizzate IIS Lockdown Wizard per rafforzare l'installazione

Microsoft ha rilasciato un semplice strumento, noto come IIS Lockdown Wizard, che aiuta a rendere più sicure le installazioni di IIS. La versione più recente può essere scaricata da Microsoft all'indirizzo http://www.microsoft.com/technet/security/tools/locktool.asp

Eseguendo IIS Lockdown Wizard in modalità "custom" o "expert" si potranno apportare le seguenti modifiche consigliate a qualsiasi installazione di IIS:

- Disabilitare WebDAV (a meno che l'ambiente non lo richieda inderogabilmente per la pubblicazione dei contenuti web).
- Disabilitare tutte le estensioni ISAPI non necessarie (in particolare .htr, .idq, .ism e .printer)..
- Eliminare le applicazioni di esempio.
- Impedire al web server di eseguire comandi di sistema usati comunemente per acquisirne il controllo (es. cmd.exe e tftp.exe).

La SANS Reading Room contiene anche il documento di Jeff Wichman Using Microsoft's IISlockdown tool to protect your IIS Web Server, che riguarda specificamente IISlockdown tool.

Utilizzate URLScan per filtrare le richieste HTTP

Molti exploit di IIS, incluse le famiglie di Code Blue e Code Red, utilizzano richieste HTTP articolate appositamente per operare attacchi Unicode o buffer overflow. È possibile configurare il filtro URLScan per respingere tali richieste prima che il server tenti di processarle. La versione più recente di URLScan è integrata nel IIS Lockdown Wizard, ma può essere anche scaricata separatamente da Microsoft all'indirizzo http://www.microsoft.com/technet/security/tools/urlscan.mspx.

b. Apache

I problemi nel controllo degli accessi, nella limitazione per IP e dei moduli di sicurezza di Apache sono trattati, assieme a molti altri temi, sulla pagina Apache Tutorials.

Nella SANS Reading Room è disponibile anche l'utilissimo documento di Artur Maj Securing Apache: Step-by-Step , che descrive in dettaglio i passi da compiere per rendere sicuro un server Apache.

c. iPlanet/Sun One

Edmundo Farinas spiega come rendere sicuro iPlanet nel documento Security Considerations for the iPlanet Enterprise Web Server on Solaris, disponibile nella SANS Reading Room.

Sun fornisce inoltre il documento Sun ONE Application Server Security Goals, che descrive in dettaglio i passi raccomandati per la sicurezza di un server iPlanet/Sun One.

d. Add-on

Se si usano add-on di terze parti come ColdFusion, PerlIIS o PHP, è consigliabile verificare nei siti web dei rispettivi fornitori la presenza di patch e suggerimenti per la configurazione. Per ovvie ragioni, Microsoft non include le patch di terzi in Windows Update e negli altri servizi di aggiornamento.

Per informazioni su come rendere sicuro ColdFusion, si può leggere nella SANS Reading Room il documento Web Application Security, with a Focus on ColdFusion di Joseph Higgins.

Sempre nella SANS Reading Room, Securing PHP: Step-by-step di Artur Maj illustra il processo di sicurizzazione delle applicazioni PHP.

Un'altra risorsa molto utile è il capitolo 16 del manuale PHP (PHP Manual, Chapter 16. Security) che si occupa in dettaglio della sicurezza di PHP.

e. Altri servizi

Per quanto vi siano delle operazioni generali tra quelle indicate qui sopra che sono valide per rendere più sicuri la maggior parte dei servizi web, ciascuno di questi ha di solito la sua specifica serie di aggiornamenti e patch fornita dal produttore assieme a raccomandazioni per la configurazione e funzionalità di logging.

Passate quindi in rassegna la documentazione disponibile sul sito web del produttore, non trascurando alcuna informazione, ed iscrivetevi a tutti i servizi di notifica e a tutte le newsletter del produttore. Ciò vi aiuterà a mantenervi sempre aggiornati sui relativi problemi di sicurezza e a risolverli rapidamente ed efficacemente.

back to top ^

W2 Servizio Workstation

W2.1 Descrizione

Il servizio Workstation Windows si occupa di elaborare le richieste di accesso dell'utente a risorse come file e stampanti. Il servizio determina se la risorsa risiede sul sistema locale o in una condivisione di rete e quindi indirizza la richiesta di conseguenza.

Le funzioni di gestione di rete fornite dal servizio possono essere richiamate attraverso uno qualunque dei seguenti meccanismi.

- Chiamate DCE/RPC mediante il protocollo SMB dove essersi connessi al servizio usando una pipe chiamata \\pipe\wkssvc.
- Chiamate DCE/RPC direttamente attraverso una porta UDP (> 1024)
- Chiamate DCE/RPC direttamente attraverso una porta TCP (> 1024)

  Da notare che il servizio utilizza la prima porta TCP e UDP disponibile dopo la 1024.

Il servizio Workstation presenta un buffer overflow che riguarda lo stack, attivabile attivato

con una chiamata DCE/RPC confezionata ad arte. Il problema si presenta a causa del fatto che i parametri vengono passati alla funzione di logging senza alcuna verifica dei passaggi. Questo overflow può essere sfruttato da un aggressore remoto non autenticato per eseguire codice abusivo con privilegi “SYSTEM” sulla macchina Windows vulnerabile. L’aggressore può arrivare ad ottenere il controllo completo della macchina colpita. Il codice di exploit code che sfrutta la vulnerabilità è stato pubblicato in Internet ed è stato utilizzato in alcune varianti del worm Phatbot/Gaobot, che ha infettato milioni di sistemi in tutto il mondo.

W2.2 Sistemi operativi interessati
Windows 2000 SP2, SP3 e SP4
Windows XP
Windows XP 64 Bit Edition

W2.3 Riferimenti CVE/CAN
CAN-2003-0812

W2.4 Come stabilire se si è vulnerabili
I sistemi che utilizzano Windows 2000 senza la patch MS03-049 e Windows XP senza la patch MS03-043 sono vulnerabili.

Controllate i seguenti dati nel registro di sistema:
KB828035: Sotto HKLM\Software\Microsoft\Updates\Windows XP (Windows XP)
KB828749: Sotto HKLM\Software\Microsoft\Updates\Windows 2000 (Windows 2000)
Se non trovate queste voci di registro, il sistema Windows è vulnerabile.

In alternativa, potete usare uno scanner di rete come il Microsoft Baseline Security Analyzer (MBSA) per verificare se siano stati installati gli aggiornamenti corretti. MBSA si può scaricare da http://www.microsoft.com/technet/security/tools/mbsahome.mspx

W2.5 Come proteggersi

(a) Controllando che i sistemi Windows abbiano installate tutte le ultime patch di sicurezza. In particolare controllando che i sistemi Windows 2000 abbiano istallata la MS03-049 e i sistemi Windows XP la MS03-043.
(b) Bloccando le porte 139/tcp e 445/tcp a livello perimetrale. Ciò impedisce agli aggressori remoti di sfruttare l’overflow via SMB.
(c) Aprendo solo le porte TCP necessarie dopo la 1024 a livello perimetrale. Ciò impedisce agli aggressori remoti di sfruttare l’overflow tramite chiamate DCE/RPC. Da notare che è difficile bloccare le porte UDP oltre la 1024 a livello di firewall, in quanto le porte in questo range sono utilizzate come porte provvisorie.
(d) Usando le funzioni di filtro TCP/IP disponibili sia in Windows 2000 sia in XP, oppure l’Internet Connection Firewall di Windows XP, per bloccare l’accesso verso l’interno dalle porte interessate.
(e) Per le applicazioni di terze parti che operano su piattaforme Windows 2000/XP personalizzate, controllando che sia stata applicata una patch adatta distribuita dal produttore. Cisco, ad esempio, ha pubblicato un avviso che spiega come diversi prodotti Cisco siano vulnerabili a questo overflow. Cisco fornisce anche le patch.
(f) Se il sistema è stand-alone (cioè, ad esempio, non fa parte di un ambiente di rete Windows), il servizio Workstation può essere disattivato senza conseguenze.

Informazioni aggiuntive:

Avvisi Microsoft
http://www.microsoft.com/technet/security/bulletin/MS03-049.mspx

Avvisi eEye
http://www.eeye.com/html/Research/Advisories/AD20031111.html

Avvisi CERT
http://www.cert.org/advisories/CA-2003-28.html
http://www.kb.cert.org/vuls/id/567620

Avvisi CORE Security
http://archives.neohapsis.com/archives/vulnwatch/2003-q4/0066.html

Avvisi Cisco
http://www.cisco.com/warp/public/707/cisco-sa-20040129-ms03-049.shtml

Worm Gaobot
http://securityresponse.symantec.com/avcenter/venc/data/w32.hllw.gaobot.gen.html

torna all'inizio ^

W3 Servizi Windows di accesso remoto

W3.1 Descrizione

La famiglia delle piattaforme operative Windows supporta diversi metodi e tecnologie di rete. Vi sono supporti nativi per la maggior parte dei protocolli di rete standard e funzionalità integrate per molti metodi e tecniche di networking specifiche di Microsoft. Tra queste tecnologie di rete specifiche di Microsoft, vi sono elementi notoriamente insicuri o mal configurati come le Condivisioni di rete con NETBIOS, le connessioni con Logon anonimo o NULL session, l'accesso remoto al registro e le Remote procedure call. Questi elementi costituiscono una larga fetta dei più comuni exploit a livello di rete su Windows e sono descritti nel testo seguente.

NETBIOS - Condivisioni di rete non protette in Windows
Microsoft Windows fornisce alle macchine host la possibilità di condividere attraverso la rete file o cartelle con altri host tramite le condivisioni di rete. I meccanismi che permettono questa funzione sono il protocollo Server Message Block (SMB) o il Common Internet File System (CIFS). Questi protocolli permettono agli host di operare su file remoti come se risiedessero in locale.

Per quanto questa funzione di Windows sia utile e valida, la configurazione impropria delle condivisioni di rete può mettere in pericolo i file di sistema o può favorire processi che portino utenti o programmi ostili ad ottenere il pieno controllo dell'host. Uno dei metodi tramite i quali il worm I-Worm.Klez.a-h (della famiglia Klez), il virus Sircam (vedi il CERT Advisory 2001-22) e il worm Nimda (vedi il CERT Advisory 2001-26) si sono diffusi così rapidamente nel 2001 era proprio quello di scoprire le condivisioni di rete non protette e di replicarsi in queste. Molti possessori di computer aprono inconsciamente i loro sistemi agli hacker quando vogliono favorire i colleghi o i collaboratori esterni condividendo i loro dischi in lettura e in scrittura per gli utenti della rete. Facendo attenzione quando si configura le condivisione di rete, i rischi possono essere adeguatamente mitigati.

Logon Anonimo - Una null session è una sessione stabilita senza credenziali (es. nome utente blank e password vuote). Le null session possono essere utilizzate per visualizzare

informazioni riguardo gli utenti, i gruppi, le condivisioni e le password policy. I servizi eseguiti in Microsoft Windows NT con l'account Local System sul computer locale comunicano con altri servizi attraverso la rete stabilendo delle null session. I servizi eseguiti su Windows 2000 e successivi con l'account Local System sul computer locale utilizzano l'account del computer locale per autenticarsi sugli altri server. Active Directory eseguito in modalità nativa non accetta richieste in null session. In modalità mista, però, Active Directory permette un accesso ai sistemi pre-Windows 2000, accettando richieste in null session che, di conseguenza, ereditano le vulnerabilità delle null session di Windows NT.

Accesso remoto al registro - Microsoft Windows 9x, Windows CE, Windows NT, Windows 2000, Windows 2003, Windows ME e Windows XP impiegano un database gerarchico centralizzato, meglio conosciuto come Registro, per gestire il software, la configurazione dei dispositivi e le impostazioni degli utenti.
Permessi o impostazioni di sicurezza non corretti possono permettere un accesso remoto al Registro. È possibile sfruttare questo fatto per compromettere il sistema o porre le basi per adattare l'associazione dei file e i permessi in modo da consentire l'esecuzione di codice abusivo

Remote Procedure Call **-** Molte versioni dei sistemi operativi Microsoft (Windows NT 4.0, 2000, XP e 2003) forniscono un meccanismo di intercomunicazione che permette a programmi che girano su un dato host di eseguire codice su host remoti. Sono state pubblicate tre vulnerabilità che permettono agli aggressori di eseguire codice abusivo sugli host vulnerabili con privilegi di Local System. Una di queste vulnerabilità viene sfruttata dai worm Blaster/MSblast/LovSAN e Nachi/Welchia. Vi sono inoltre delle ulteriori vulnerabilità che permetto agli aggressori di lanciare attacchi Denial of Service nei confronti di componenti RPC.

W3.2 Sistemi operativi interessati
Windows 95, Windows 98, Windows NT Workstation e Server, Windows Me, Windows 2000 Workstation e Server, Windows XP Home e Professional, Windows 2003.

W3.3 Riferimenti CVE/CAN

NETBIOS
CVE-2000-0979

CAN-1999-0518, CAN-1999-0519, CAN-1999-0621, CAN-2000-1079

Logon anonimo
CVE-2000-1200

Accesso remoto al Registro
CVE-2000-0377, CVE-2002-0049

CAN-1999-0562, CAN-2001-0045, CAN-2001-0046, CAN-2001-0047, CAN-2002-0642, CAN-2002-0649, CAN-2002-1117

Remote Procedure Call
CAN-2002-1561, CAN-2003-0003, CAN-2003-0352, CAN-2003-0528, CAN-2003-0605, CAN-2003-0715

W3.4 Come stabilire se si è vulnerabili

Come determinare se si è vulnerabili ai problemi legati a NETBIOS.

Sono a disposizione alcuni strumenti che possono aiutare a determinare se vi siano sul sistema vulnerabilità legate NETBIOS.

NbtScan - NetBIOS Name Network esplora i servizi di condivisione NETBIOS disponibili sui sistemi analizzati. NbtScan è disponibile su: http://www.inetcat.org/software/nbtscan.html.

NLtest – un tool molto efficace, incluso nei Tool di supporto per Windows 2000 e 2003 (si trova sul CD del prodotto relativo) e nel Windows NT4 Resource Kit. NLtest può scoprire moltissime informazioni su potenziali vulnerabilità di configurazione.

Gli utenti Windows 95/98/Me possono analizzare le condivisioni di rete Windows utilizzando Legion v2.11, la più recente versione del Legion File Share scanner di Rhino9.

Gli amministratori di Windows 2000 possono utilizzare Security Fridays Share Password Checker (SPC) per analizzare i loro client 95/98/Me con cui condividono file per verificare se siano vulnerabili alla vulnerabilità Share Level Password.

Per Windows NT (SP4), Windows 2000, Windows XP e Windows 2003, il Microsoft Baseline Security Analyser riporta gli host vulnerabili agli exploit SMB e può essere utilizzato anche per risolvere il problema. Le analisi possono essere eseguite in locale o su host remoti.

Gli utenti Windows NT, Windows 2000, Windows XP e Windows 2003 possono semplicemente digitare *net share* dal prompt dei comandi per vedere quali risorse siano attualmente condivide sulla macchina. Per ulteriori informazioni riguardo al comando net share, digitate *net share /?*.

Nota IMPORTANTE: Questo capitolo contiene informazioni su come modificare le risorse condivise. Prima di modificare qualsiasi condivisione, ci si accerti di sapere come riattivare la risorsa condivisa nel caso si verifichi qualche problema. Si raccomanda di sperimentare di testare in modo esauriente qualsiasi modifica prima di effettuarla in un ambiente di produzione. Per informazioni riguardo le risorse condivise, consultate gli articoli della Microsoft Knowledge Base indicati di seguito:

125996 - Saving and Restoring Existing Windows Shares

308419 - HOW TO Set, View, Change, or Remove Special Permissions for Files and Folders in Windows XP

307874 - HOW TO Disable Simplified Sharing and Password-Protect a Shared Folder in Windows XP

174273 – How to Copy Files and Maintain NTFS and Share Permissions

I permessi di default per le nuove condivisioni:

Windows NT, Windows 2000, e Windows XP (Pre Service Pack 1)

- Everyone - Full Control

Windows XP SP1 • Everyone - Read

Windows XP ha per default una cartella condivisa chiamata "Documenti condivisi". La collocazione fisica di questa condivisione è:

"C:\Documents and Settings\All Users\ Documenti condivisi"

- Everyone Full Control

La maggior parte degli scanner di rete disponibili in commercio rilevano anche le condivisioni attive. Un rapido, gratuito e sicuro test per verificare la presenza delle condivisioni di file SMB e delle vulnerabilità ad esse correlate è disponibile presso il sito web della Gibson Research Corporation. Cliccate su *ShieldsUP* per ricevere una valutazione in tempo reale sulla vulnerabilità SMB per qualsiasi sistema e istruzioni dettagliate per aiutare gli utenti Microsoft Windows ad affrontare le vulnerabilità SMB. Tenete presente che se siete connessi attraverso una rete nella quale vi siano dispositivi intermedi che bloccano SMB, il risultato prodotto da ShieldsUP sarà che non siete vulnerabili mentre, in realtà, lo potete essere. È il caso, ad esempio, di utenti collegati tramite un provider che blocca SMB all'interno della propria rete: in questo caso ShieldsUP riporterà che non siete vulnerabili, mentre in realtà siete esposti ad eventuali attacchi da parte di tutti gli utenti che utilizzano lo stesso provider.

Strumenti automatici di scansione per rilevare le vulnerabilità da condivisione:

- Nessus-- un security scanner remoto gratuito, potente, aggiornato e facile da usare
- Winfingerprint di vacuum --Win32 Host/Network Enumeration Scanner

Come determinare se siete vulnerabili ai problemi legati a Logon anonimo. Provate a stabilire una null session al vostro sistema utilizzando il seguente comando dal prompt dei comandi (*Start --> Esegui --> digitate cmd*):

```
C:\>net use \\ipaddress\ipc$ "" /user:""
```

La sintassi precedente connette tramite l'hidden interprocess communications share (IPC$) all'indirizzo IP specificato come l'anonimo utente user predefinito (/user:"") con una password nulla ().

Se il risultato è un errore di sistema, allora l'accesso è negato è il sistema non è vulnerabile.

Se il risultato è un messaggio di comando riuscito, significa che il vostro sistema è vulnerabile.

Anche i succitati strumenti *Nessus* e *Winfingerprint* possono essere utilizzati per evidenziare vulnerabilità null session.

Come determinare se siete vulnerabili ai problemi correlati all'Accesso remoto al registro. L'NT Resource Kit (NTRK) disponibile presso Microsoft contiene un file eseguibile denominato *Regdump.exe* che verifica passivamente i permessi per l'accesso remoto al registro da un host Windows NT verso altri host Windows NT/Windows 2000 o Windows XP attraverso Internet o la rete interna.

Oltre a ciò, è possibile scaricare una raccolta di shell script a linea di comando che verificano i permessi di accesso al vostro registro, oltre a una serie di altri che riguardano la sicurezza. È disponibile all'indirizzo http://www.afentis.com/top20.

Come determinare se siete vulnerabili ai problemi correlati alle Remote Procedure

Call.
Microsoft ha creato uno strumento per il controllo delle patch , degli aggiornamenti e delle configurazioni, disponibile per il download gratuito, che costituisce probabilmente il metodo migliore per determinare se gli host Windows sono soggetti a qualcuna di queste vulnerabilità. Si chiama Microsoft Baseline Security Analyzer (MBSA) e si può scaricare da http://www.microsoft.com/technet/security/tools/mbsahome.mspx

Esiste anche uno strumento di scansione stand-alone che verifica l'eventuale mancanza di patch di sicurezza solo per le vulnerabilità descritte in CAN-2003-0352, CAN-2003-0528, CAN-2003-0605 e CAN-2003-0715, disponibile presso http://support.microsoft.com/?kbid=827363. Si consiglia comunque di utilizzare MBSA, che offre una copertura maggiore. Gli utenti domestici o di aziende che gestiscono un numero molto limitato di computer troveranno probabilmente più comodo e semplice visitare il sito Windows Update all'indirizzo http://windowsupdate.microsoft.com/ e controllare l'aggiornamento del software per ciascuna singola macchina..

W3.5 Come proteggersi

Microsoft ha corretto le vulnerabilità nei Service Pack e negli aggiornamenti per la sicurezza di Sistemi operativi e applicazioni. È quindi molto importante installare sempre sui sistemi il più recente Service Pack.
Per fare un esempio, il worm *Sasser* e i suoi cloni (che sfruttano una vulnerabilità del sistema LSASS) hanno infettato in tutto il mondo moltissimi sistemi non aggiornati, mentre quelli che avevano installato la patch MS04-011 erano immuni da questa vulnerabilità assai pericolosa. Microsoft ha rilasciato la MS04-011 poche settimane prima della comparsa del worm *Sasser*.

NOTA: Windows 95 e Windows NT4 Workstation non sono più supportate da Microsoft. Il supporto per Windows NT4 Server termina il 31 Dicembre 2004.

Per i dettagli sui sistemi operativi e i prodotti supportati, si può consultare *Product Lifecycle Dates - Windows Product Family*.

Per trovare gli aggiornamenti di sicurezza importanti di ciascun sistema si può usare:

- Il servizio Windows Update (*Start – Windows Update*), che rileva automaticamente tutti gli aggiornamenti di sicurezza necessari per il sistema e li installa dopo che l'utente seleziona (*approva*) gli aggiornamenti da installare.
- Il servizio online Windows *Security Bulletin Search* all'indirizzo: http://www.microsoft.com/technet/security/current.aspx

Anche se installando i più recenti service pack e gli aggiornamenti di sicurezza si risolve molti problemi di progettazione del software (come buffer overflow, errori di progettazione nel codice ecc.), vi sono nei sistemi operativi Windows molte funzioni pericolose che, pur avendo una propria legittima e documentata utilità, in molti casi possono essere tranquillamente disabilitate per rendere il sistema più sicuro.

Come proteggersi dagli attacchi legati a NETBIOS. Per limitare il rischio determinato dalle vulnerabilità sfruttabili attraverso le Condivisioni di rete di Windows si possono intraprendere diverse azioni:

- Disabilitare i servizi *Avvisi* e *Messenger* (sono disabilitati per default su Windows 2003, ma impostati su Tipo di avvio *Automatico* su Windows 2000/XP/NT4).

Disabilitando questi servizi si riduce sensibilmente la possibilità o i risultati della system enumeration, operazione eseguita di solito prima di un attacco o di una infezione.

Per disabilitare questi servizi:

- Selezionate *Start – Programmi – Strumenti di Amministrazione – Servizi*;
- Selezionate il servizio *Avvisi* – fate doppio click – impostate *Tipo di Avvio* al valore *Disabilitato* – premete il tasto *Applica* – premete il tasto *Arresta* – quindi premete il tasto *OK.*
- Selezionate il servizio *Messenger* – fate doppio click – impostate *Tipo di Avvio* al valore *Disabilitato* – premete il tasto *Applica* – premete il tasto *Arresta* – quindi premete il tasto *OK.*

- Disabilitare le condivisioni quando non sono necessarie.
  Se il sistema non deve fornire file e servizi di stampa (la maggior parte delle workstation utilizzate sia in ufficio che a casa rientrano in questa categoria), si può disabilitare sui sistemi Windows NT4/2000/2003/XP il servizio *Serve*. Per disabilitare il servizio *Server*:

Selezionate *Start – Programmi – Strumenti di Amministrazione – Servizi* – selezionate il servizio *Server* – fate doppio click – impostate *Tipo di Avvio* al valore *Disabilitato* – premete il tasto *Applica* – premete il tasto *Arresta* – quindi premete il tasto *OK.*
Se il sistema ha bisogno di mantenere attivo il servizio *Server*, per rendere sicuri i sistemi Windows NT4/2000/2003/XP è possibile compiere le operazioni seguenti:

1. Evidenziate tutte le condivisioni nascoste di default (*C$, D$, E$ acc.*) digitando il comando

Net share

dal prompt dei comandi di sistema. Prendete nota delle condivisioni esistenti.

2. Cancellate le condivisioni nascoste di default digitando il comando

Net share C$ /delete

dal prompt dei comandi di sistema. In molti casi tutte le condivisioni *alfabetiche* (*C$, D$, E$* ecc.) e la condivisione *ADMIN$* possono essere tranquillamente eliminate. Non si consiglia ,invece, di eliminare la condivisione di default *IPC$ su alcun sistema*.

3. Per fare in modo che la cancellazione delle condivisioni di default sia permanente (si riattiverebbero automaticamente quando il sistema o il servizio *Server* viene riavviato), è necessario apportare le seguenti modifiche al Registro:

- Aprite l'Editor del Registro di Sistema;
- Andate alla chiave di Registro:
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ lanmanserver\parameters
- Create un nuovo valore di Registro sotto questa chiave:
- Nome valore: *AutoShareWks*
- Tipo: *DWord*
- Dati valore: *00000000*

- Create un nuovo valore di Registro sotto questa chiave:
- Nome valore: *AutoShareServer*
- Tipo: *DWord*
- Dati valore: *00000000*

Controllate anche se esistano sul sistema condivisioni *non di default* (ovvero create dall'utente). Si può fare usando:

- L'interfaccia grafica (*Risorse del Computer* – tasto destro – *Gestione cartelle condivise – Condivisioni*). Selezionate le condivisioni da disabilitare – tasto destro – scegliete *Termina Condivisione.*
- La riga di comando (da prompt di sistema o usando un qualsiasi script):
    - Elencate tutte le condivisioni digitando il comando:

      ```
      Net share
      ```

      Dal promp dei comandi di sistema. Prendete nota delle condivisioni esistenti.
- Eliminate quindi le condivisioni digitando il comando:

  ```
  Net share Nomedellacondivisione /delete
  ```

Questa procedura rimuoverà permanentemente solo le condivisioni *non di default* (create dall'utente). Per rimuovere permanentemente le condivisioni nascoste di default *C$, D$, ADMIN$,* seguite le procedure descritte nel paragrafo precedente.

- Per i client Windows 95/98/Me che fanno parte di un dominio Windows NT, si raccomanda di impostare i controlli di accesso alle condivisioni a livello di utente.
- Non permettete condivisioni operate tramite Internet. Controllate tramite il Pannello di Controllo di rete di Windows che tutti gli host connessi a Internet abbiano le condivisioni di rete disabilitate. Lo scambio di file con gli host connessi ad Internet deve essere permesso solo tramite SCP, FTP o HTTP.
- Non permettete le condivisioni senza autenticazione. Se è necessaria la condivisione, configuratela in modo che sia necessaria una password per accedere alla condivisione.
- Limitate la condivisione solo alle directory strettamente necessarie. Di norma è necessario condividere solo una cartella e, al limite, le relative sottocartelle.
- Restringete il più possibile i permessi di accesso alle cartelle condivise. Ponete attenzione in particolare a consentire la scrittura solo quando strettamente necessario.
- Per una maggiore sicurezza, permettete la condivisione solo ad indirizzi IP specifici, poiché i nomi DNS possono essere aggirati.

Come proteggersi dai problemi legati al Logon anonimo sui vostri sistemi. Nota IMPORTANTE: Questo capitolo contiene informazioni su come modificare il registro. Prima di modificare il registro, accertatevi di averne effettuato un backup e assicuratevi di sapere come ripristinarlo nel caso che insorgano dei problemi. Si raccomanda di sperimentare di testare in modo esauriente qualsiasi modifica prima di effettuarla in un ambiente di produzione. Per informazioni su come effettuare il backup, su come ripristinare e su come modificare il registro, consultate gli articoli seguenti della Microsoft Knowledge Base:

256986 - Description of the Microsoft Windows Registry
323170 - HOW TO Backup, Edit, and Restore the Registry in Windows NT 4.0
322755 - HOW TO Backup, Edit, and Restore the Registry in Windows 2000

322756 - HOW TO Backup, Edit, and Restore the Registry in Windows XP Windows Server 2003

I controller di dominio di Windows NT richiedono sessioni nulle per comunicare. Perciò, se state lavorando in un dominio di rete Windows NT o sotto Active Directory in modalità mista, che permette la compatibilità di accessi da macchine con sistemi precedenti a Windows 2000, potete limitare la quantità di informazioni che può cadere in mano agli aggressori, ma non fermarne del tutto la disponibilità, impostando la chiave di registro RestrictAnonymous al valore 1. GetAcct di Security Friday, ad esempio, è uno strumento che elude l'impostazione RestrictAnonymous=1 e scopre l'elenco dei SID e degli UserID. L'impostazione ideale del valore di registro RestrictAnonymous è 2 per Active Directory nativa di Windows 2000/2003.

Per limitare le informazioni disponibili tramite sessioni nulle, consultate i seguenti articoli nella Microsoft Knowledge Base:

143474 - Restricting Information Available to Anonymous Logon Users in Windows NT
246261 - How to Use the RestrictAnonymous Registry Value in Windows 2000

Per i problemi relativi al valore di registro RestrictAnonymous, consultate il seguente articolo nella Microsoft Knowledge Base:

296405 - The RestrictAnonymous Registry Value May Break the Trust to a Windows 2000 Domain

Come proteggersi dall'Accesso remoto al registro del vostri sistemi. Per far fronte a questa minaccia, l'accesso al Registro di sistema deve essere limitato e devono essere rivisti i permessi impostati per le chiavi del Registro più critiche. Prima di ottimizzare il Registro, gli utenti di Microsoft Windows NT 4.0 devono anche assicurarsi che sul loro sistema sia già installato il Service Pack 4 (SP4) o eventualmente i successivi.

Nota importante: Questo capitolo contiene informazioni su come modificare il registro. Prima di modificare il registro, bisogna accertarsi di averne effettuato un backup e assicurarsi di sapere come ripristinarlo nel caso che insorgano dei problemi. Si raccomanda di sperimentare di testare in modo esauriente qualsiasi modifica prima di effettuarla in un ambiente di produzione. Per informazioni su come effettuare il backup, su come ripristinare e su come modificare il registro, consultate gli articoli seguenti della Microsoft Knowledge Base:

256986 - Description of the Microsoft Windows Registry
323170 - HOW TO Backup, Edit, and Restore the Registry in Windows NT 4.0
322755 - HOW TO Backup, Edit, and Restore the Registry in Windows 2000
322756 - HOW TO Backup, Edit, and Restore the Registry in Windows XP Windows Server 2003

Limitare l'accesso dalla rete. Per limitare l'accesso dalla rete al registro, seguite le istruzioni indicate qui sotto per creare la seguente chiave di registro:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\ Control\ SecurePipeServers\winreg
- Tipo: REG_SZ
- Valore: Registry Server

I permessi di sicurezza impostati in questa chiave definiscono gli Utenti o i Gruppi ai quali è

permesso l'accesso remoto al Registro. L'istallazione standard di Windows definisce questa chiave e imposta l'Access Control List per fornire pieni privilegi all'Amministratore del sistema e al Gruppo degli Amministratori (e ai Backup Operator in Windows 2000).

Le modifiche al Registro di sistema richiedono un riavvio per avere effetto. Per creare la chiave di Registro che limita l'accesso al registro:

1. Avviate l'Editor del registro ("regedt32.exe" o "regedit.exe") e andate alla seguente sottochiave: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control
2. Dal menu "Modifica", selezionate "Nuovo" e quindi "Chiave"
3. Inserite i seguenti valori: Nome chiave: SecurePipeServers - Class: REG_SZ
4. Andate quindi alla nuova sottochiave: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers
5. Dal menu "Modifica", selezionate "Nuovo" e quindi "Chiave".
6. Inserite i seguenti valori: Nome chiave: winreg - Class: REG_SZ
7. Andate quindi alla nuova sottochiave: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ SecurePipeServers\winreg
8. Dal menu "Modifica", selezionate "Nuovo" e quindi "Valore stringa"
9. Inserite i seguenti valori: Nome Valore: Description -Tipo: REG_SZ - Dati valore: Server del Registro di sistema
10. Andate quindi alla seguente sottochiave: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ SecurePipeServers\winreg
11. Selezionate "winreg." Cliccate "Protezione" e quindi "Permessi." Aggiungete gli utenti o i gruppi a cui volete concedere l'accesso.
12. Uscite dall'Editor del registro e riavviate Microsoft Windows.
13. Se in un secondo tempo volete variare la lista degli utenti che possono accedere al registro, ripetete i passi 10-12.

Limitate gli accessi remoti autorizzati. Applicare limitazioni troppo ristrette sul registro può avere effetti secondari su servizi dipendenti quali il Directory Replicator e il servizio di spooling per le stampanti di rete.

È possibile aggiungere un grado di dettaglio ai permessi, aggiungendo il nome di account per il quale il servizio funziona all'access list della chiave "winreg", oppure configurando Windows in modo che ignori le restrizioni di accesso per certe chiavi elencandole nei valori Machine o User sotto la chiave AllowedPaths:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
SecurePipeServers\winreg\AllowedPaths
Nome Valore: Machine
Tipo: REG_MULTI_SZ - Multi string
Dati valore di default: System\CurrentControlSet\Control\ProductOptionsSystem\
CurrentControlSet\Control\Print\PrintersSystem\CurrentControlSet\
Services\EventlogSoftware\Microsoft\WindowsNT\CurrentVersionSystem\
CurrentControlSet\Services\Replicator
Range Valido: (Un percorso valido a una posizione del Registro)
Descrizione: Allow machines access to listed locations in the registry provided that no explicit access restrictions exist for that location.
Valore: Users
Tipo: REG_MULTI_SZ - Multi string
Dati valore di default: (nessuno)
Range Valido: (Un percorso valido a una posizione del Registro)
Descrizione: Allow users access to listed locations in the registry provided that no explicit

access restrictions exist for that location.

Nel Registro di Windows 2000 e Windows XP:
Nome Valore: Machine
Tipo Valore: REG_MULTI_SZ - Multi string
Dati valore di default: System\CurrentControlSet\Control\ProductOptionsSystem\
CurrentControlSet\Control\Print\PrintersSystem\CurrentControlSet\ control\Server
ApplicationSystem\CurrentControlSet\Services\Eventlog\ Software\Microsoft\Windows
NT\CurrentVersion
Valore: Users (non esiste per default)

Succede spesso che si verifichi un ritardo tra il momento in cui una vulnerabilità diventa di pubblico dominio e il momento in cui viene resa disponibile una patch. Oppure, per ragioni si strategia aziendale, la vulnerabilità deve essere mantenuta. Per mitigare i rischi, si può limitare gli accessi tramite i firewall o i router. Una misura aggiuntiva sarebbe quella di scrivere delle nuove regole per un IDS (Intrusion Detection System) come Snort che comporti un avviso o attivi una adeguata risposta. Alcuni esempi di regole documentate per Snort si trovano a questo indirizzo.

Come proteggersi dai problemi legati alle Remote Procedure Call.

Il modo di gran lunga migliore è quello di applicare le relative patch identificate da MBSA o Windows Update: vedi il precedente "Come determinare se siete vulnerabili ai problemi correlati alle Remote Procedure Call". In alternativa, vi sono una serie di metodi per disabilitare o limitare alcune funzionalità si Remote Procedure Call: alcune di queste si possono trovare nell'eccellente riassunto operato in
http://www.ntbugtraq.com/dcomrpc.asp.
ATTENZIONE: disabilitare o limitare funzionalità di Remote Procedure Call può comportare l'interruzione di servizi Windows utilizzati, per cui si dovrebbe sperimentare qualsiasi modifica in un ambiente non di produzione.

Se non si può applicare le patch al sistema, è certamente possibile bloccare le porte associate con le remote procedure call di Window (porte TCP 135, 139, 445 e 593; porte UDP 135, 137, 138 e 445) al di fuori del perimetro di rete. Si da per scontato che sia sempre consigliato di bloccare *tutti* i servizi non necessari al di fuori del perimetro di rete.

Per ulteriori informazioni:

Testo nella Microsoft Knowledge Base 153183. How to Restrict Access to NT Registry from a Remote Computer.

Un'altra fonte è il Microsoft Security Bulletin Search.

MSDN Library (Ricerca per Securing Registry)

Testo nella Microsoft Knowledge Base 310426: HOW TO: Use the Windows XP and Windows Server 2003 Registry Editor

Network access: Remotely accessible registry paths and subpaths

Windows Server 2003 Security Guide

torna all'inizio ^

W4 Microsoft SQL Server (MSSQL)

W4.1 Descrizione

Microsoft SQL Server (MSSQL) contiene numerose vulnerabilità gravi che permettono ad aggressori remoti di ottenere informazioni riservate, di alterare il contenuto del database, di compromettere i server SQL e, in alcune configurazioni, anche gli host.
Le vulnerabilità di MSSQL sono molto pubblicizzate e ancora sotto attacco. Due recenti worm MSSQL, diffusisi rispettivamente nel Maggio 2002 e a Gennaio 2003, sfruttavano numerose vulnerabilità note di MSSQL. Gli host compromessi da questi worm generano un traffico di rete estremamente dannoso quando analizzano la rete alla ricerca di altri host vulnerabili. Ulteriori informazioni possono essere reperite agli indirizzi:

SQLSnake/Spida Worm (Maggio 2002)

- http://isc.incidents.org/analysis.html?id=157
- http://www.eeye.com/html/Research/Advisories/AL20020522.html
- http://www.cert.org/incident_notes/IN-2002-04.html

SQL-Slammer/SQL-Hell/Sapphire Worm (Gennaio 2003)

- http://isc.incidents.org/analysis.html?id=180
- http://www.nextgenss.com/advisories/mssql-udp.txt
- http://www.eeye.com/html/Research/Flash/AL20030125.html
- http://www.cert.org/advisories/CA-2003-04.html

Le porte 1433 e 1434 (le porte di default del server e del monitor MSSQL) sono regolarmente registrate presso l'Internet Storm Centre come due delle porte più sondate in assoluto.

Il funzionamento dell'exploit di SQLSnake è legato alla presenza di un account di amministrazione, o "sa" account, che abbia una password nulla. È fondamentale per una configurazione corretta e per la sicurezza di qualsiasi sistema accertarsi sempre che tutti gli account siano protetti da password oppure completamente disabilitati, se non sono usati. Potete trovare ulteriori informazioni riguardo alle impostazioni e alla gestione delle password degli account sa nella documentazione della Microsoft Developer Network sotto Changing the SQL Server Administrator Login, oppure sotto Verify and Change the System Administrator Password by Using MSDE. Gli account sa dovrebbero avere una password piuttosto complessa e difficile da individuare, anche se non sono utilizzati per eseguire il vostro SQL/MSDE.

Il funzionamento dell'exploit di Slammer si basa su un buffer overflow nel Resolution Service di SQL Server. Questo buffer overflow ha effetto e di conseguenza la sicurezza dell'host è compromessa quando il worm invia dei particolari pacchetti di attacco verso la porta UDP 1434 dei sistemi vulnerabili. Se la macchina esegue servizi SQL che sono soggetti a buffer overflow e riceve questi pacchetti, il risultato è di solito una totale compromissione della sicurezza del server e del sistema. Le più efficaci misure di sicurezza contro questo worm sono costituite dall'applicare diligentemente tutte le patch, nell'utilizzare procedure di configurazione che prevengano il problema e il filtraggio in entrata e in uscita della porta UDP 1434 già a livello di accesso alla rete.

Il Microsoft Server 2000 Desktop Engine (MSDE 2000) può essere considerato un "SQL Server Lite". Molti non sono a conoscenza che i propri sistemi eseguono MSDE e che hanno installato una versione di SQL Server. MSDE 2000 viene istallato assieme ai seguenti prodotti Microsoft:

- SQL/MSDE Server 2000 (versione Developer, Standard e Enterprise)
- Visual Studio .NET (versione Architect, Developer e Professional)
- ASP.NET Web Matrix Tool
- Office XP
- Access 2002
- Visual Fox Pro 7.0/8.0

Oltre a quelli elencati, anche molti altri pacchetti software possono far uso di MSDE 2000. Per una lista aggiornata, controllate all'indirizzo http://www.SQLsecurity.com/forum/applicationslistgridall.aspx. Dal momento che questi software utilizzano MSDE come core database engine, presentano necessariamente le stesse vulnerabilità di SQL/MSDE Server. MSDE 2000 può essere configurato per ricevere le connessioni client in entrata in molti modi diversi. Può essere configurato in modo che i client utilizzino le named pipe attraverso una sessione NetBIOS (porte TCP 139/445) o si connettano tramite un socket alla porta 1433 TCP, o entrambi. A prescindere dal metodo utilizzato, SQL Server e MSDE saranno comunque sempre in ascolto sulla porta 1434. Questa porta è definita come porta di controllo. I client invieranno un messaggio a questa porta per scoprire dinamicamente come connettersi al server.

Il motore MSDE 2000 restituisce informazioni che lo riguardano ogni qualvolta arriva un singolo pacchetto single byte 0x02 sulla porta UDP 1434. Altri pacchetti single byte causano un buffer overflow senza doversi mai autenticare presso il server. Ciò che complica questo problema è che l'attacco è condotto attraverso il canale UDP. Quando il processo di MSDE 2000 gira in un contesto sicuro di un utente del dominio o dell'account locale SYSTEM, lo sfruttamento riuscito di questi buchi di sicurezza può comportare una totale compromissione del sistema preso di mira.

Siccome SQL Slammer riesce a causare un buffer overflow sul sistema preso di mira, rispettare la buona abitudine di applicare periodicamente le patch e di configurare correttamente il sistema aiuta a mitigare questo pericolo. Scaricando e utilizzando strumenti di difesa come il Microsoft SQL Critical Update Kit, si può verificare se i sistemi locali siano vulnerabili a questo exploit, analizzare interi domini o reti alla ricerca di sistemi vulnerabili e aggiornare automaticamente i file tramite l'SQL Critical Update.

Consulta i report e le analisi presenti su incidents.org per maggiori dettagli sul worm SQL/MSDE Slammer. Questo particolare attacco colpì per alcune ore la dorsale principale di Internet la mattina del 25 gennaio 2003.

W4.2 Sistemi operativi interessati

Qualsiasi sistema Microsoft Windows con installato Microsoft SQL/MSDE Server 7.0, Microsoft SQL/MSDE Server 2000 o Microsoft SQL/MSDE Server Desktop Engine 2000 e tutti quei sistemi che usano separatamente il motore MSDE.

W4.3 Riferimenti CVE/CAN

CVE-1999-0999, CVE-2000-0202, CVE-2000-0402, CVE-2000-0485, CVE-2000-0603, CVE-2001-0344, CVE-2001-0879

CAN-2000-0199, CAN-2000-1081, CAN-2000-1082, CAN-2000-1083, CAN-2000-1084, CAN-2000-1085, CAN-2000-1086, CAN-2000-1087, CAN-2000-1088, CAN-2000-1209, CAN-2001-0509, CAN-2001-0542, CAN-2002-0056, CAN-2002-0154, CAN-2002-0186, CAN-2002-0187, CAN-2002-0224, CAN-2002-0624, CAN-2002-0641, CAN-2002-0642,

CAN-2002-0643, CAN-2002-0644, CAN-2002-0645, CAN-2002-0649, CAN-2002-0650, CAN-2002-0695, CAN-2002-0721, CAN-2002-0729, CAN-2002-0859, CAN-2002-0982, CAN-2002-1123, CAN-2002-1137, CAN-2002-1138, CAN-2002-1145, CAN-2003-0118

W4.4 Come stabilire se si è vulnerabili

Microsoft ha pubblicato una serie di strumenti di sicurezza all'indirizzo http://www.microsoft.com/sql/downloads/securitytools.asp. Il kit denominato SQL Critical Update Kit contiene strumenti preziosi come SQL Scan, SQL Check e SQL Critical Update.

Chip Andrews di sqlsecurity.com ha rilasciato uno strumento chiamato SQLPingv2.2. Questo tool invia un pacchetto UDB single byte (valore byte di 0x02) verso la porta 1434 di un singolo host o di una intera sottorete. I Server SQL in ascolto sulla porta UDP 1434 rispondono rivelando dettagli del sistema come la versione del software, le istanze ecc. SQLPingv2.2 è considerato uno strumento di analisi e rilevazione molto simile a SQL Scan di Microsoft, e non influisce sulla sicurezza del sistema o della rete. Sul sito di Chip Andrews SQL/MSDE Security si trovano anche altri strumenti per la sicurezza di SQL.

W4.5 Come proteggersi

Sommario:

1. Disabilitate SQL/MSDE Server Monitor sulla porta 1434 UDP.
2. Applicate il più recente service pack per Microsoft SQL/MSDE server e/o MSDE 2000.
3. Applicate le patch cumulative più recenti rilasciate dopo l'ultimo service pack.
4. Applicate ciascuna singola patch rilasciata dopo la più recente patch cumulativa.
5. Abilitate l'Authentication Logging di SQL Server.
6. Rendete più sicuro il server a livello di sistema e a livello di rete.
7. Riducete al minimo i privilegi del servizio MSSQL/MSDE Server e di SQL/MSDE Server Agent.

In dettaglio:

1. Disabilitate SQL/MSDE Server Monitor sulla porta 1434 UDP.
   Questa operazione può essere facilmente portata a termine installando e utilizzando le funzionalità comprese nel SQL Server 2000 Service Pack 3a. Il database engine Microsoft MSDE 2000 presenta due vulnerabilità buffer overflow che possono essere sfruttate da un aggressore remoto senza nemmeno autenticarsi su server. Ciò che complica questo problema è che l'attacco è condotto attraverso il canale UDP. Quando il processo di MSDE 2000 gira in un contesto sicuro di un utente del dominio o dell'account locale SYSTEM, lo sfruttamento riuscito di questi buchi di sicurezza può comportare una totale compromissione del sistema preso di mira. MS-SQL/MSDE Slammer invia un pacchetto UDP di 376 byte verso la porta 1434 utilizzando indirizzi di destinazione a caso e ripetendo l'operazione con alta frequenza. Il sistema compromesso, una volta infetto, inizia immediatamente a inviare a sua volta identici pacchetti da 376. Il worm invia il traffico a indirizzi IP casuali, includendo IP multicast, causando un Denial of Service della rete presa di mira. Singole macchine colpite dal worm hanno evidenziato dopo essere state infette un aumento del traffico dell'ordine di 50 Mb/sec.

2. Applicate il più recente service pack per Microsoft SQL/MSDE server e/o MSDE 2000.

Le versioni correnti dei service pack per il servizio Microsoft SQL/MSDE sono:

- SQL/MSDE Server 7.0 Service Pack 4
- MSDE/SQL Server 2000 Service Pack 3a

Per accertarvi di essere informati sui prossimi aggiornamenti, controllate regolarmente il documento di Microsoft Technet Make Your SQL/MSDE Servers Less Vulnerable.

3. Applicate le patch cumulative più recenti rilasciate dopo l'ultimo service pack.
   Le patch cumulativa corrente per tutte le versioni di SQL/MSDE/MSDE Server è disponibile presso MS02-061 Elevation of Privilege in SQL/MSDE Server Web Tasks (Q316333/Q327068).

   Per accertarvi di essere informati sui prossimi aggiornamenti, controllate l'uscita di nuove patch cumulative per Microsoft SQL/MSDE Server agli indirizzi:

   - Microsoft SQL/MSDE Server 7.0
   - Microsoft SQL Server 2000
   - MSDE Server Desktop Engine 2000 (MSDE 2000)

4. Applicate ciascuna singola patch rilasciata dopo la più recente patch cumulativa.
   Attualmente non vi sono patch singole rilasciate dopo la MS02-061 Elevation of Privilege in SQL/MSDE Server Web Tasks (Q316333/Q327068). Per restare al passo con i prossimi aggiornamenti, verificate la presenza di nuove patch singole agli indirizzi:

   - Microsoft SQL/MSDE Server 7.0
   - Microsoft SQL Server 2000
   - MSDE Server Desktop Engine 2000 (MSDE 2000)

5. Abilitate l'Authentication Logging di SQL Server.
   L'Authentication Logging di SQL Server di solito non è abilitato. Questa operazione può essere effettuata tramite l' Enterprise Manager (Server properties; sezione Security).

6. Rendete più sicuro il server a livello di sistema e a livello di rete.
   Una delle vulnerabilità MSSQL più frequentemente attaccate riguarda il fatto che l'account di amministrazione di default (noto come "sa") viene installato con password vuota. Se il vostro account "sa" di SQL/MSDE non è protetto da password, non potete ritenervi sicuri e potete cadere vittima di worm o di altri exploit. Perciò seguite le raccomandazioni raccolte alla voce "System Administrator (SA) Login" in SQL/MSDE Server Books Online per assicurarvi che l'account "sa" installato abbia una password sufficientemente robusta, e questo anche se il vostro server SQL/MSDE non usa tale account.
   Sulla Microsoft Developer's Network è presente la documentazione su come cambiare il login di amministratore (Changing the SQL Server Administrator Login) e su come verificare e cambiare la password di amministratore usando MSDE (Verify and Change the System Administrator Password by Using MSDE)

7. Riducete al minimo i privilegi del servizio MSSQL/MSDE Server e di SQL/MSDE Server Agent.

Eseguite il servizio MSSQL/MSDE Server e l'SQL/MSDE Server Agent sotto un account valido di dominio con privilegi minimi, non come amministratore del dominio o con l'account SYSTEM (su NT) o LocalSystem (su 2000 or XP). Se il servizio compromesso viene eseguito con privilegi locali o di dominio permette all'aggressore di ottenere il controllo completo della vostra macchina e/o della vostra rete.

a. Abilitate l'Autenticazione Windows NT, abilitate la verifica dei login effettuati e falliti e quindi fermate e riavviate il servizio MSSQL/MSDE Server. Se possibile, configurate i client in modo che usino l'Autenticazione NT.
b. Si raccomanda un'azione di packet filtering effettuata a livello perimetrale in modo da bloccare le connessioni non autorizzate in entrata e in uscita agli specifici servizi MSSQL. Il filtering per l'ingresso dalle porte TCP/UDP 1433 e 1434 può prevenire l'azione di aggressori interni o esterni che attraverso queste porte possono effettuare scansioni o infettare eventuali server Microsoft SQL/MSDE vulnerabili residenti nella rete locale che non sono esplicitamente autorizzati a fornire servizi SQL/MSDE pubblici.
c. Se i vostri servizi richiedono che le porte TCP 1433 e 1434 verso Internet debbano rimanere aperte, abilitate e personalizzate il filtering in ingresso e in uscita in modo da prevenire l'uso non corretto di queste porte.

Ulteriori informazioni su come rendere più sicuro Microsoft SQL/MSDE Server possono essere reperite agli indirizzi

- Microsoft SQL Server 7.0 Security
- Microsoft SQL Server 2000 Security

torna all'inizio ^

W5 Autenticazione in Windows

W5.1 Descrizione

In quasi tutte le interazioni tra gli utenti e i sistemi informativi vengono utilizzate password, frasi identificative o codici di sicurezza. La maggior parte delle forme di autenticazione, come la maggior parte delle protezioni per file e dati, si basa su password fornite dall'utente. Dal momento che gli accessi correttamente autenticati spesso non vengono registrati, o anche se vengono registrati non lo sono in modo da fornire alcun segnale di allarme, una password compromessa rappresenta un'opportunità potenziale di esplorare un sistema dall'interno senza essere identificati. Un aggressore avrebbe accesso completo a qualsiasi risorsa disponibile per quell'utente e sarebbe molto vicino ad essere in grado di accedere ad altri account, a macchine vicine e forse anche ad ottenere privilegi di amministrazione. Nonostante questi pericoli, gli account con password deboli o addirittura senza password rimangono estremamente diffusi e le società con una buona policy sull'utilizzo delle password ancora troppo rare.

Le più comuni vulnerabilità delle password sono dovute a:

- Account utente senza password o con password deboli.
- Al fatto che, a prescindere dalla robustezza delle password, spesso gli utenti non le proteggono adeguatamente.
- Al fatto che il sistema operativo o il software applicativo creano account di amministrazione con password deboli o privi di password.

- Al fatto che gli algoritmi di hashing delle password sono noti e spesso gli hash vengono memorizzati in modo da essere accessibili a chiunque. La difesa migliore e la più corretta contro queste vulnerabilità è una solida policy che includa le istruzioni per creare delle buone password e che riassuma i comportamenti corretti per conservarne la riservatezza, unita a una verifica proattiva dell'integrità delle password.

Microsoft Windows non salva o trasmette le password in testo piano, ma utilizza un hash della password di autenticazione. Un hash è il risultato di lunghezza fissa ottenuto applicando una funzione matematica (l'algoritmo di hashing) a una quantità discrezionale di dati (nota anche come message digest). (MSDN Library) Vi sono tre algoritmi di autenticazione in Windows: LM (il meno sicuro, ma il più compatibile); NTLM e NTLMv2 (il più sicuro e il meno compatibile). Per quanto la maggior parte degli ambienti Windows attuali non necessitino del supporto LAN Manager (LM), Microsoft memorizza per default in locale gli hash delle password legati al LM (noti anche come hash LANMAN) nei sistemi Windows NT, 2000 e XP (ma non in Windows 2003). Siccome LAN Manager usa uno schema di codifica molto più debole di quelli, più aggiornati, attualmente utilizzati da Microsoft (NTLM and NTLMv2), le password del LAN Manager possono essere violate in brevissimo tempo. Anche le password che in un altro ambiente sarebbero considerate "forti" possono essere violate con sistemi "brute-force" in meno di una settimana con gli strumenti attuali.

http://msdn.miscrosoft.com/library/default.asp?url=/library/en-us/security/Security/h_gly.asp

La debolezza degli hash del Lan Manager deriva dal fatto che:

- Le password sono troncate a 14 caratteri.
- Le password utilizzano lo spazio come carattere di riempimento per raggiungere i 14 caratteri.
- I caratteri usati nelle password vengono convertiti tutti in caratteri maiuscoli.
- Le password vengono divise in due blocchi di sette caratteri.

Questo processo di hashing comporta che, per ottenere un accesso autenticato al vostro sistema, un eventuale aggressore ha bisogno solo di determinare due semplici password da sette caratteri, che per di più contengono solo caratteri maiuscoli. Siccome la difficoltà nel violare gli hash aumenta con progressione geometrica in proporzione alla lunghezza dell'hash, ciascuna stringa di sette caratteri è almeno di un ordine di grandezza più semplice da attaccare con sistemi "brute-force" rispetto a una stringa di quattordici caratteri. Dal momento che le stringhe sono tutte esattamente di sette caratteri (spazi inclusi) e tutte in caratteri maiuscoli, anche un attacco da dizionario risulta molto semplificato. Il metodo di hashing del Lan Manager rende quindi inefficace qualsiasi buona policy sull'uso delle password.

Al rischio dettato dal fatto di avere gli hash collegati a LM memorizzati nel SAM, si aggiunge quello che deriva dal processo di autenticazione del LAN Manager, che è spesso abilitato per default sui client e accettato dai server. La conseguenza è che macchine Windows, in grado di utilizzare hash più robusti, inviano hash LM deboli attraverso la rete, rendendo l'autenticazione di Windows vulnerabile all'intercettazione attraverso packet sniffing e facilitando il compito degli aggressori di recuperare e violare le password degli utenti.

W5.2 Sistemi operativi interessati

Tutti i sistemi operativi Microsoft Windows.

W5.3 Riferimenti CVE/CAN

CVE-2000-0222

CAN-1999-0504, CAN-1999-0505, CAN-1999-0506

W5.4 Come stabilire se si è vulnerabili

Per quanto vi siano alcuni sintomi osservabili di una generale debolezza delle password, come la presenza di account attivi appartenenti a utenti che non operano più all'interno dell'organizzazione o a servizi non più attivi, l'unico modo per accertarsi che ogni singola password sia sufficientemente robusta è quello di verificare tutte le password con gli stessi strumenti per la determinazione delle password utilizzati dagli aggressori.

ATTENZIONE: Non utilizzate mai un password scanner, neanche sui sistemi per i quali avete un accesso da amministratore, senza autorizzazione esplicita e preferibilmente scritta da parte del vostro datore di lavoro. È già accaduto che amministratori di sistema con le migliori intenzioni siano stati licenziati per aver utilizzato strumenti per la determinazione delle password senza autorizzazione.

Alcuni tra i migliori strumenti per la determinazione delle password sono LC4 (l0phtcrack version 4) e John the Ripper.

Riguardo il problema degli hash di LAN Manager salvati in locale:

- Se utilizzate un'installazione predefinita di NT, 2000 o XP, siete vulnerabili, perché l'impostazione predefinita prevede il salvataggio in locale degli hash del LAN Manager
- Se nel vostro ambiente avete sistemi operativi che richiedono l'autenticazione LM per comunicare con in server, allora siete vulnerabili perché tali macchine inviano gli hash del Lan Manager attraverso la rete, e questi corrono il rischio di essere intercettati.

W5.5 Come proteggersi

La difesa migliore e la più corretta contro la debolezza delle password è una solida policy che includa le istruzioni su come generare buone password e descriva i comportamenti corretti per mantenerne la sicurezza, assieme ad una verifica proattiva dell'integrità delle password.

- **Assicuratevi che le vostre password siano sufficientemente robuste**.
  Disponendo di tempi e risorse hardware adeguate, qualsiasi password può essere violata utilizzando il sistema "brute force". Ma ci sono metodi più semplici e molto più efficaci per venire a conoscenza delle password con uno sforzo minore. I password cracker utilizzano metodi conosciuti come "attacchi da dizionario". Dal momento che i metodi crittografici sono noti, gli strumenti per l'individuazione delle password non fanno altro che confrontare le password in forma cifrata con le forme cifrate di parole del dizionario (in diverse lingue), di nomi propri, e con le permutazioni di entrambi.
  Di conseguenza una password la cui radice assomigli in qualche modo a una parola è estremamente suscettibile di essere violata da un attacco da dizionario. Molte

organizzazioni insegnano ai propri utenti a generare password che includano combinazioni di caratteri alfanumerici e caratteri speciali, e gli utenti la maggior parte delle volte prendono una parola (ad esempio "password") e convertono le lettere in numeri o caratteri speciali ("pa$$w0rd"). Queste permutazioni non proteggono, però, dagli attacchi da dizionario: "pa$$w0rd" ha la stessa possibilità di essere violata di "password."

Una buona password, quindi, non deve avere come radice una parola o un nome proprio. Una solida policy sulle password dovrebbe indirizzare gli utenti verso la creazione di password derivate da qualcosa di più casuale, come una frase o il titolo di un libro o di una canzone. Concatenando una stringa più lunga (prendendo la prima lettera di ogni parola o associando alle parole un carattere speciale o togliendo le vocali, ecc.), gli utenti possono generare stringhe sufficientemente lunghe che combinano caratteri alfanumerici e caratteri speciali in modo tale da creare una grande difficoltà ai tentativi di attacco con metodi da dizionario. E in più se la frase è facile da ricordare, lo sarà anche la password.

Una volta fornite agli utenti le corrette indicazioni su come generare buone password, possono essere messe in opera le procedure per controllare che queste indicazioni vengano seguite. Il modo migliore per farlo è quello di convalidare le password ogni volta che l'utente le cambia, impiegando Passfilt (NT4).

Windows 2000, XP e 2003 posseggono validi strumenti per rafforzare le password policy. Per visualizzare la vostra attuale password policy sulla maggior parte dei sistemi Windows, seguite questi passaggi (Start - Programmi – Strumenti di Amministrazione – Criteri di protezione locale – selezionate quindi Criteri Account – Criterio password). Le Impostazioni di protezione locale hanno i seguenti parametri:

- **Le Password devono essere conformi ai requisiti di complessità.** Determina se le password debbano rispondere a requisiti di complessità. Tali requisiti di complessità sono applicati quando le password vengono create o modificate. Se questo criterio viene abilitato, le password devono rispondere a questi requisiti minimi:
    - non devono contenere in tutto o in parte il nome account dell'utente
    - devono avere una lunghezza minima di sei caratteri
    - devono contenere caratteri di tre delle seguenti quattro categorie:
        - caratteri maiuscoli dell'alfabeto inglese (dalla A alla Z)
        - caratteri minuscoli dell'alfabeto inglese (dalla a alla z)
        - caratteri numerici (da 0 a 9)
        - caratteri non alfanumerici (es. !, $, #, %)

- **Applica l'unicità della password memorizzando le ultime (intervallo: 0-24**): Determina il numero di password univoche che devono essere associate a un account utente prima che una vecchia password possa essere riutilizzata. Il valore deve essere compreso tra 0 e 24 password. Impostando il parametro a 0 si permette di riciclare le vecchie password; impostandolo a 24 password, si obbliga a 24 cambi di password prima che la password iniziale possa essere riutilizzata. Questo criterio permette agli amministratori di aumentare la sicurezza, garantendo che le vecchie password non possano essere riutilizzate continuamente. Per mantenere l'efficacia della cronologia delle password, non permettete il cambio immediato della password

quando andrete a configurare la Validità minima della password.

- **Validità massima password (intervallo: 0-999 giorni):** Determina il periodo di tempo (in giorni) durante il quale può essere utilizzata una certa password prima che il sistema richieda all'utente di modificarla. Potete impostare la scadenza delle password dopo un numero di giorni compreso tra 1 e 999, o specificare che la password non ha scadenza impostando a 0 il numero di giorni.

- **Validità minima password (intervallo: 0-999 giorni):** Determina il periodo di tempo (in giorni) durante il quale una certa password rimane valida prima che l'utente possa modificarla. Potete impostare un valore tra 1 e 999 giorni o permettere la modifica immediata della password, impostando a 0 il numero di giorni. La Validità minima password deve essere comunque inferiore alla Validità massima password. Configurate la validità minima delle password a un valore maggiore di 0 se volete che il criterio impostato con Applica l'unicità della password memorizzando le ultime sia efficace. Senza una durata minima della password, l'utente potrebbe inserire rapidamente le nuove password fino a poter riutilizzare quella vecchia. Le impostazioni predefinite non seguono questa raccomandazione, in modo che l'amministratore possa specificare una password per l'utente e quindi richiedere all'utente stesso di cambiare la password definita dall'amministratore al primo log on. Se il criterio di cronologia delle password è impostato su 0, l'utente non è obbligato a scegliere una nuova password. Per questo motivo, il criterio di cronologia delle password è impostato per default su 1.

- **Lunghezza minima password (intervallo: 0-14 caratteri):** Determina il numero minimo di caratteri che deve contenere una password di una account utente. Si può impostare un valore tra 1 e 14 caratteri o stabilire che non è richiesta una lunghezza minima della password impostando il numero di caratteri a 0. La lunghezza minima delle password deve essere conforme alla security policy aziendale (in ogni caso si raccomanda di impostare il valore a un numero di caratteri uguale o superiore a 8; La National Security Agency (NSA) raccomanda 12 caratteri).

- **Consenti archiviazione password con crittografia reversibile** per tutti gli utenti del dominio: Determina se Windows 2000, 2003 e XP Professional archivino le password usando utilizzando una crittografia reversibile. Questo criterio è utile a quelle applicazioni che utilizzano un protocollo che richiede la conoscenza della password degli utenti per effettuare l'autenticazione. Archiviare le password utilizzando una crittografia reversibile è essenzialmente la stessa cosa di archiviare le password in testo piano. Per questo motivo tale criterio non dovrebbe mai essere abilitato se non quando i requisiti delle applicazioni superano di importanza il bisogno di protezione delle informazioni relative alle password.

Un approccio che può essere utilizzato per generare automaticamente e quindi assegnare agli account degli utenti delle password complesse è quello di eseguire il seguente comando (dal prompt di esecuzione di Windows NT4, 2000, XP o 2003):

Net user username /random

L'esecuzione di questo comando assegnerà una password complessa e casuale (ma sempre di 8 caratteri di lunghezza) a un account e stamperà tale password sullo schermo della console utilizzata. Questo metodo è di solito più adatto ad assegnare le password agli account dei servizi, piuttosto che ad utenti veri e propri.

Il sistema migliore per verificare la qualità delle password è comunque sempre quello di utilizzare strumenti per la determinazione delle password in modalità stand-alone come parte di un esame sistematico.

Nota importante: Non utilizzate mai un password scanner, neanche sui sistemi per i quali avete un accesso da amministratore, senza autorizzazione esplicita e preferibilmente scritta da parte del vostro datore di lavoro. È già accaduto che amministratori di sistema con le migliori intenzioni siano stati licenziati per aver utilizzato strumenti per la determinazione delle password senza autorizzazione.

Una volta ricevuta l'autorizzazione ad utilizzare strumenti per la determinazione delle password sul vostro sistema, attivateli regolarmente su una macchina protetta. Gli utenti le cui password vengono violate devono essere avvisati in modo confidenziale e devono essere fornite loro le istruzioni su come scegliere una buona password. Gli amministratori di sistema e il management dovrebbero sviluppare assieme questo tipo di procedure, in modo tale che il management possa provvedere quando gli utenti non rispondono ai solleciti.

Un altro modo per proteggersi da password deboli o assenti è quello di utilizzare forme alternative di autenticazione come token generatori di password o sistemi di autenticazione biometrica.

1. **Proteggere le password robuste.** Anche se le password sono robuste, gli account possono essere ugualmente compromessi se gli utenti non proteggono adeguatamente la propria password. Una buona policy include sempre istruzioni che specificano come gli utenti non devono mai riferire la propria password a nessun altro, non devono mai trascrivere la password in supporti che possano essere letti da altri e devono rendere adeguatamente sicuro qualsiasi file nel quale sia conservata una password per l'autenticazione automatica (le password sono più facili da proteggere quando questa pratica è utilizzata solo quando assolutamente necessario).
   La modifica periodica della password deve essere fatta rispettare in modo che quelle password che non rispettano queste regole siano vulnerabili solo in una finestra temporale limitata, e deve essere tassativamente vietato che le vecchie password possano essere riutilizzate. Controllate che agli utenti giungano gli avvisi e sia data loro le possibilità di modificare la propria password prima della scadenza. Quando si trovano di fronte a frasi come: "la vostra password è scaduta e deve essere cambiata," gli utenti tendono a scegliere una cattiva password.

2. **Controllare rigorosamente gli account.**
   - Qualsiasi account per l'accesso a un servizio e qualsiasi account di amministrazione che non sia più in uso deve essere disabilitato o eliminato. Qualsiasi account per l'accesso a un servizio e qualsiasi account di amministrazione che siano in uso deve essere forniti di una password solida e recente.
   - Verificate gli account presenti sul vostro sistema e create una master list. Non dimenticate di verificare le password su dispositivi come router e stampanti digitali, fotocopiatrici e controller connessi ad Internet.
   - Sviluppate procedure per aggiungere account autorizzati alla lista e per rimuove dalla lista gli account che non sono più in uso.
   - Verificate periodicamente la lista per controllare che non siano stati aggiunti nuovi account e che gli account non più in uso siano stati rimossi.
   - Adottate rigide procedure per la rimozione degli account quando i dipendenti o i collaboratori della società non lavorano più lì o quando gli account non sono più

necessari.

3. **Adottare una solida policy aziendale per le password.** In aggiunta ai controlli a livello di sistema operativo o a livello di rete, esistono degli strumenti completi che aiutano a gestire una buona policy per le password. Potete trovare molti modelli di esempio per la definizione delle policy, guide per la stesura delle policy stesse, raccomandazioni fondamentali riguardo alle password e collegamenti a numerosi siti web che trattano di security policy (che include la password policy) al sito del SANS Security Policy Project.

4. **Disabilitare l'autenticazione LM attraverso la rete**. Il modo migliore per sostituire l'autenticazione LAN Manager in Windows è quello di utilizzare NT Lan Manager versione 2 (NTLMv2). I metodi di verifica/risposta di NTLMv2 eliminano la maggior parte dei difetti del Lan Manager utilizzando crittografia più avanzata e meccanismi di autenticazione e per la sicurezza delle sessioni decisamente migliori. La chiave del registro che controlla questa proprietà per Windows NT e 2000 è:

   Hive: HKEY_LOCAL_MACHINE
   Chiave: System\CurrentControlSet\Control\LSA
   Valore: LMCompatibilityLevel
   Tipo Valore: REG_DWORD - Number
   Intervallo Valido: 0-5
   Default: 0

   D: Questo parametro specifica il tipo di autenticazione da utilizzare.

   0 - Spedisce le risposte LM e le risposte NTLM; non usa mai il meccanismo di sicurezza delle sessioni NTLMv2;
   1 - Usa il meccanismo di sicurezza delle sessioni NTLMv2 se richiesto;
   2 - Invia solo l'autenticazione NTLM;
   3 - Invia solo l'autenticazione NTLMv2;
   4 - DC rifiuta l'autenticazione LM;
   5 - DC rifiuta l'autenticazione LM e NTLM (accetta solo NTLMv2).

   Su Windows 2000, 2003 e XP la stessa funzionalità può essere implementata configurando le impostazioni del Livello di autenticazione di LAN Manager (Windows 2000) o Sicurezza di rete: Livello di autenticazione di LAN Manager (Windows XP, 2003) (Start - Programmi – Strumenti di Amministrazione – Criteri di protezione locali – Criteri locali – Opzioni di protezione).

   Se tutti i vostri sistemi sono Windows NT SP4 o successivi, potete impostare il valore a 3 su tutti i client e a 5 su tutti i controller di dominio, in modo da evitare qualsiasi trasmissione di hash LM in rete. I sistemi di vecchio tipo (come Windows 95/98) non usano NTLMv2 con il Client di rete Microsoft predefinito. Per implementare le funzionalità NTLMv2, installate il Directory Services Client. Una volta installato, la chiave del registro corrispondente è "LMCompatibility," e i valori consentiti sono 0 o 3.

   Se non potete obbligare i vostri client più vecchi ad usare NTLMv2, potete ottenere comunque un certo miglioramento nel sistema di hashing LM forzando NTLM (NT Lan Manager, versione 1) sul controller di dominio (impostate "LMCompatibilityLevel" a 4 o se usate lo strumento Criteri di protezione locali impostate il Livello di autenticazione di Lan Manager al valore: Invia solo risposte NTLMv2\Rifiuta LM). Ma l'opzione più sicura riguardo a questi sistemi è quella di passare a sistemi più recenti, dal momento che i

sistemi operativi più vecchi non permettono neanche questo minimo livello di sicurezza.

5. **Evitare l'archiviazione degli Hash LM**. Un altro problema che si presenta anche qualora si eviti che gli hash LM vengano inviati attraverso la rete è che gli hash vengono comunque creati e memorizzati nella SAM o Active Directory. Microsoft rende disponibile un meccanismo per evitare la creazione degli hash LM, ma solo in Windows 2000, 2003 e XP. Sui sistemi Windows 2000 (SP2 o successivi), la funzione è controllata da questa chiave del registro:

   Hive: HKEY_LOCAL_MACHINE
   Chiave: System\CurrentControlSet\Control\LSA\NoLMHash

   Se questa chiave viene creata in un Controller di Dominio di Windows 2000, gli hash LanMan non saranno più creati e memorizzati nella Active Directory.

   Su Windows XP e 2003, la stessa funzionalità può essere implementata abilitando l'impostazione su Protezione di rete: Non archiviare il valore hash di Lan Manager al prossimo cambio di password (Start - Programmi - Strumenti di Amministrazione - Criteri di protezione locali - Criteri locali - Opzioni di protezione).

   Dopo aver effettuato queste modifiche, il sistema deve essere riavviato perché queste abbiano effetto.

   > **Nota importante**: Questa operazione evita solo che vengano generati nuovi hash LM. Gli hash LM esistenti vengono rimossi singolarmente solo quando l'utente modifica la propria password.

6. **Evitare che gli hash delle password e il database SAM vengano copiati.** Gli strumenti per l'individuazione delle password, più volte menzionati in questa sezione, ottengono gli hash delle password:

   - Intercettando le password dalla rete. Contromisure: 1. L'uso di reti packet-swiching; 2. La ricerca e la rimozione delle schede di rete in modalità promiscua (si possono trovare utilizzando la maggior parte degli strumenti di security assessment in commercio, o con strumenti gratuiti come ethereal).
   - Copiando il file SAM file (situato nella cartella %SystemRoot%\System32\Config\ ovvero, di solito, C:\Winnt\System32\Config\ - su Windows NT4 e 2000 o C:\Windows\System32\Config\ - su Windows XP e 2003). Questo file è normalmente bloccato dal sistema operativo Windows OS e può essere copiato solo quando il sistema è stato avviato con un diverso sistema operativo. Il file SAM si può ottenere però anche ripristinando il backup del file SAM o System (Windows 2000, 2003, XP). Il file SAM si trova anche nel Disco di ripristino di NT4

   Contromisure: Limitate e controllate l'accesso fisico ai sistemi informatici (in particolare ai controller di dominio), ai dispositivi di backup e al Disco di ripristino.

   I seguenti testi Microsoft forniscono utili indicazioni in proposito:

   - How to Disable LM Authentication on Windows NT [Q147706] elenca le modifiche necessarie da apportare al registro per Windows 9x e Windows NT/2000.
   - MS03-034 : Flaw in NetBIOS Could Lead to Information Disclosure (824105)
   - LMCompatibilityLevel and Its Effects [Q175641] espone i problemi di

interoperabilità con riguardanti questi parametri.

- How to Enable NTLMv2 Authentication for Windows 95/98/2000/NT [Q239869] spiega come utilizzare il Directory Services Client di Windows 2000 per Windows 95/98 per superare le limitazioni di compatibilità di NTLMv2.
- New Registry Key to Remove LM Hashes from Active Directory and Security Account Manager

torna all'inizio ^

W6 Browser Web

W6.1 Descrizione

Il Browser è il mezzo con il quale sui sistemi Microsoft Windows gli utenti del computer accedono al Web. Il web browser più diffuso è Internet Explorer (IE) di Microsoft, che è il web browser installato per default sulle piattaforme Microsoft Windows. Vi sono altri browser Web come Mozilla, Firefox, Netscape e Opera. La versione più recente di IE è la 6, e sarà la versione trattata in questo capitolo. Le vulnerabilità discusse qui riguardano anche Mozilla versioni 1.4 - 1.7.1, Firefox versioni 0.9.x, Netscape versioni 7.x ed Opera versioni 7.x.

I problemi riguardo IE si possono suddividere in sei categorie:

1. Un enorme numero di vulnerabilità di IE durante gli ultimi anni, in confronto agli altri browser –secondo il Security Focus Archive, si sono rilevate 153 vulnerabilità di IE da Aprile 2001 ad oggi.
2. Tempi più lunghi per le patch delle vulnerabilità note di IE – Gli utenti devono aspettare anche più di sei mesi dal momento della scoperta della vulnerabilità all'uscita della patch.
3. Active X e Active Scripting di IE – Le vulnerabilità di IE, in particolare l'utilizzo della tecnologia ActiveX, hanno consentito in passato di aggirare le barriere di sicurezza del Sistema operativo per arrivare a conquistare le macchine.
4. Un gran numero di vulnerabilità mai corrette – 34, secondo http://umbrella.name/originalvuln/msie/
5. Vulnerabilità da Spyware/Adware – Queste riguardano tutti i browser, ma IE ne è soggetto maggiormente rispetto agli altri.
6. L'integrazione del browser IE nel kernel del Sistema operativo, cosa che rende il Sistema operativo stesso più vulnerabile agli attacchi.

Anche gli altri browser presentano dei problemi, ma nessuno al livello di IE. Un web designer maligno può creare delle pagine web che sfruttano alcune vulnerabilità di Internet Explorer semplicemente leggendo le pagine da web. Un esempio importante di questa caratteristica è quello della vulnerabilità "Download.Ject", che utilizzava alcuni bachi di ActiveX ed è stata presente per molti mesi. Anche dopo che l'8 Giugno 2004 fu pubblicato un exploit, si è dovuto aspettare fino a Luglio per avere una patch per IE. La combinazione tra ActiveX, scripting e la sua integrazione con il sistema operativo Windows, rendono quindi Internet Explorer più vulnerabile agli attacchi rispetto a molti altri browser. Le conseguenze possono variare dalla divulgazione del contenuto di cookie, di file o dati locali fino all'esecuzione di programmi locali, il download e l'esecuzione di codice abusivo per arrivare al controllo completo del sistema vulnerabile.

W6.2 Sistemi operativi interessati

Queste vulnerabilità riguardano sistemi Microsoft Windows che utilizzano qualsiasi versione di tali browser. È importante sottolineare che IE viene installato assieme ad una grande

varietà di software Microsoft ed è quindi di solito presente su qualsiasi sistema Windows, anche se l'utente non ha voluto installarlo o utilizzarlo. Tutti gli altri browser sono invece installati a discrezione dell'utente, che decide se questo debba essere usato da altre applicazioni.

W6.3 Vulnerabilità dei browser, cortesemente fornite da Secunia

A. Internet Explorer:

2004 - 15 Security Advisories (Alla data del 30 Luglio 2004)

1. Microsoft Internet Explorer Multiple Vulnerabilities
2. Internet Explorer Frame Injection Vulnerability
3. Internet Explorer File Download Error Message Denial of Service Weakness
4. Internet Explorer Security Zone Bypass and Address Bar Spoofing Vulnerability
5. Internet Explorer Local Resource Access and Cross-Zone Scripting Vulnerabilities
6. Microsoft Internet Explorer and Outlook URL Obfuscation Issue
7. Windows Explorer / Internet Explorer Long Share Name Buffer Overflow
8. Microsoft Outlook Express MHTML URL Processing Vulnerability
9. Internet Explorer/Outlook Express Restricted Zone Status Bar Spoofing
10. Multiple Browser Cookie Path Directory Traversal Vulnerability
11. Internet Explorer Cross Frame Scripting Restriction Bypass
12. Internet Explorer File Identification Variant
13. Internet Explorer Travel Log Arbitrary Script Execution Vulnerability
14. Internet Explorer File Download Extension Spoofing
15. Internet Explorer showHelp() Restriction Bypass Vulnerability

B. Vulnerabilità di Mozilla

2004 - 7 Secunia Advisories

1. Mozilla Fails to Restrict Access to "shell:"
2. Mozilla XPInstall Dialog Box Security Issue
3. Multiple Browsers Frame Injection Vulnerability
4. Mozilla Browser Address Bar Spoofing Weakness
5. Mozilla / NSS S/MIME Implementation Vulnerability
6. Multiple Browser Cookie Path Directory Traversal Vulnerability
7. Mozilla Cross-Site Scripting Vulnerability

C. Vulnerabilità di Netscape

2004 - 2 Secunia Security Advisories

1. Mozilla Fails to Restrict Access to "shell:"
2. Multiple Browsers Frame Injection Vulnerability

D. Vulnerabilità di Opera

2004 - 8 Secunia Security Advisories

1. Opera Browser Address Bar Spoofing Vulnerability
2. Multiple Browsers Frame Injection Vulnerability
3. Opera Address Bar Spoofing Security Issue
4. Opera Browser Favicon Displaying Address Bar Spoofing Vulnerability
5. Multiple Browsers Telnet URI Handler File Manipulation Vulnerability
6. Opera Browser Address Bar Spoofing Vulnerability
7. Multiple Browser Cookie Path Directory Traversal Vulnerability
8. Opera Browser File Download Extension Spoofing

W6.5 Come verificare e neutralizzare le vulnerabilità dei browser

Se sul vostro sistema usate Internet, non vi è attualmente modo di sapere se siete

vulnerabili, a causa delle vulnerabilità mai corrette che continuano ad esserci. **In** ogni caso si consiglia di visitare regolarmente il Sito di Windows Update per accertarsi che IE sia protetto dalle vulnerabilità per le quali sono disponibili le patch**.** Gli utenti che desiderano una protezione maggiore dalle vulnerabilità dei browser dovrebbero prendere in considerazione una delle seguenti alternative:

a. Prendere in considerazione browser alternativi che non usino ActiveX. La maggior parte dei siti Internet non usa ActiveX; siccome il sito di Windows Update, invece, gli ActiveX li usa, la qual cosa potrebbe rendere sconsigliabile questo approccio, provate ad usare in alternativa a questo le funzioni di "Aggiornamento Automatico". Altre possibilità di aggiornamento si hanno usando Shavlik's HFNetChkPro™ o il Microsoft Baseline Security Analyzer (MBSA). Oltre a questi, anche uno strumento di analisi online di Internet Explorer, come il Qualys Browser Check, può essere prezioso per valutare lo stato della sicurezza di IE sui vostri sistemi.
b. Se l'opzione a. si dimostra difficile da adottare in ambienti corporate nei quali si utilizza funzioni ActiveX in ambito Intranet, considerate la possibilità di usare Internet Explorer per le attività Intranet e un diverso browser per l'accesso a Internet.
c. Se non c'è la possibilità di usare un diverso browser, considerate la possibilità di disabilitare ActiveX, lasciando attivi solo gli applet ActiveX che possono essere preinstallati sulla macchina. Microsoft permette di impostare le opzioni del browser in modo da bloccare i controlli ActiveX in Internet Explorer.

Per gli altri browser non ci sono gli strumenti automatici di rilevazione disponibili per Internet Explorer. Se si usa Mozilla/Firefox, Netscape o Opera, bisogna controllare i rispettivi siti web (http://www.mozilla.org, http://www.netscape.com, http://www.opera.com) o http://umbrella.name/index.html) per venire a conoscenza delle vulnerabilità e dei relativi aggiornamenti.

W6.5 Come rendere sicuro Internet Explorer
Per configurare le impostazioni di sicurezza di Internet Explorer:

1. Scegliere *Opzioni Internet* dal menu *Strumenti*.
2. Scegliere l'opzione *Protezione* e quindi impostare *Livello personalizzato* nell'area *Internet*.

La maggior parte delle imperfezioni di IE sono sfruttare attraverso Active Scripting o i Controlli ActiveX.

3. Nella sezione *Esecuzione script*, scegliete *Disattiva* per la voce "*Consenti operazioni di copia tramite script*" per evitare che sia possibile vedere i contenuti della vostra clipboard (appunti).

   Nota: Disabilitando Active Scripting è possibile che alcuni siti web n funzionino più correttamente.

I Controlli ActiveX sono meno conosciuti, ma sono potenzialmente molto più pericolosi in quanto permettono un maggiore accesso al sistema.

4. Scegliete *Disattiva* per la voce "*Scarica controlli ActiveX con firma elettronica*".
5. Scegliete *Disattiva* per la voce "*Scarica controlli ActiveX senza firma elettronica*".

6. Scegliete *Disattiva* anche per la voce "*Inizializza e esegui script controlli ActiveX non contrassegnati come sicuri*".

Gli applet Java hanno di solito potenzialità maggiori rispetto agli script.

7. Sotto *Microsoft VM*, scegliete *Protezione Alta* per le *Autorizzazioni Java*, in modo da mantenere sotto controllo gli applet Java ed evitare un accesso con privilegi al vostro sistema.
8. Sotto *Varie*,selezionate *Disattiva* alla voce *Accesso all'origine dati a livello di dominio*, per evitare gli attacchi Cross-site scripting.

Controllate anche che nell'area *Siti attendibili* non vi sia alcun sito sospetto e nell'*Intranet Locale*, in quanto per queste aree le impostazioni di sicurezza sono inferiori.

torna all'inizio ^

W7 Applicazioni per il File-Sharing

W7.1 Descrizione

I programmi per la condivisione di file Peer to Peer (P2P) sono utilizzati da una base di utenti in rapida crescita. Queste applicazioni vengono utilizzate per scaricare e distribuire dati di diverso tipo (es. musica, video, immagini, testi, codice sorgente e informazioni, solo per nominarne alcuni). Le applicazioni P2P hanno una serie di usi legittimi che comprendono la distribuzione di sorgenti OpenSource/GPL, immagini ISO di distribzioni Linux inizializzabili, creazioni di artisti indipendenti ed anche contenuti multimediali commerciali come trailer di film e anteprime di giochi. In altri casi i dati sono coperti da diritti d'autore o sono di natura discutibile. A causa dei problemi legali subiti da Napster, la maggior parte di questi programmi P2P ora opera attraverso una rete distribuita di client, che condividono cartelle o file e intere unità disco di dati. Gli utenti possono inserire dei parametri di ricerca attraverso il software client, e quindi vengono aperti uno o più canali di comunicazione tra i diversi utenti quando il software contatta gli altri partecipanti della rete per localizzare i file richiesti. I client sono coinvolti per scaricare file dagli altri utenti, nel rendere disponibili agli altri i propri dati e, in alcuni modelli, fungendo da supernodi che possono coordinare le ricerche dei diversi utenti.

La comunicazione Peer to Peer consiste nella gestione delle richieste, delle risposte e del trasferimento dei file. Un utente delle reti Peer to Peer può contemporaneamente effettuare diversi download e anche servire diversi upload. Le ricerche di contenuti possono comprendere quasi qualsiasi stringa di testo che l'utente possa immaginare. Di solito la maggior parte di questi programmi utilizza porte di default, ma alcuni possono essere automaticamente o manualmente impostati per utilizzare se necessario porte diverse per evitare di essere scoperti o per aggirare la firewall o filtri in uscita. La tendenza sembra essere quella di usare degli http wrapper per aggirare più facilmente le restrizioni aziendali. La contemporaneità di operazioni di ricerca e di trasferimento può generare su reti densamente popolate un traffico significativo e in alcuni casi saturare completamente i collegamenti WAN.

Usando il software P2P si va incontro a un certo numero di vulnerabilità. Queste possono essere raggruppate in tre tipologie: vulnerabilità tecniche, quelle che possono essere sfruttate da remoto; vulnerabilità di condivisione, che possono essere sfruttate alterando o mascherando i contenuti binari che altri richiedono; vulnerabilità legali, che possono derivare da violazioni delle leggi sui diritti d'autore o quelle che non permettono la diffusione di materiale di contenuto deplorevole.

Come detto più sopra, le vulnerabilità tecniche sono quelle che possono essere sfruttate da remoto e vi si può incappare semplicemente scaricando, installando ed eseguendo i programmi. I riferimenti CVE e CAN indicati qui sotto si riferiscono tutti a vulnerabilità tecniche. Queste vanno dal Denial of Service all'accesso non autorizzato ai file, e devono essere prese molto seriamente. Anche se non sono presi in considerazione dal database CVE, i problemi di privacy e di confidenzialità che le applicazioni P2P possono generare sono questioni piuttosto preoccupanti. Molte di queste applicazioni, infatti, includono componenti "spyware" o "adware" che, oltre a consumare una rilevante quantità di banda, inviano a coloro che li hanno realizzati diverse informazioni sulle abitudini dell'utente nella navigazione web. Una configurazione poco attenta dei client P2P può inoltre fornire un accesso non autenticato a tutta la vostra rete, condividendo le unità di rete mappate attraverso l'applicazione P2P. Non vi è quasi alcuna restrizione nel tipo di file che possono essere condivisi, per cui è possibile che si verifichino anche dei pericoli per la segretezza di informazioni riservate, proprietà intellettuale o altri dati sensibili.

Le vulnerabilità di condivisione sussistono quando un utente con intenti dolosi o semplicemente precedentemente infettato crea o altera un file per farlo assomigliare a ciò che viene richiesto da un altro utente. In questo modo si possono diffondere virus, programmi trojan horse, worm ed altro codice dannoso. Le vittime di questi attacchi sono di solito gli utenti con minori conoscenze tecniche, quelli che fanno "doppio-click " su un file senza accorgersi che l'estensione o l'icona associata non è quella consueta per il tal genere di dati, o che possono essere facilmente convinti a lanciare un eseguibile. A prescindere dalla natura dei contenuti scaricati, gli utenti dovrebbero sempre utilizzare un software anti-virus aggiornato per analizzare i download. Quando possibile, bisognerebbe inoltre controllare i checksum per essere sicuri che ciò che è stato scaricato è quello che realmente l'utente desiderava e quello che il creatore intendeva distribuire. Il meccanismo P2P può essere usato anche per propagare codice dannoso, visto che diversi virus si diffondono mascherandosi da contenuti P2P desiderabili, inserendosi nelle cartelle condivise degli utenti infetti. Il traffico P2P può anche veicolare comandi e controllare il traffico verso macchine già compromesse (zombie)

I problemi di tipo legale devono essere presi molto sul serio sia dagli utenti aziendali, sia dagli utenti domestici. Spesso i contenuti disponibili attraverso le applicazioni P2P comprendono file di musica, video e software coperti da copyright. Alcune organizzazioni come MPAA, RIAA e BSA sono attivamente impegnate per cercare di porre fine ai fenomeni di violazione dei diritti d'autore che si verificano correntemente attraverso le reti P2P. Negli Stati Uniti sono state inviate molteplici citazioni in giudizio, ordini di comparizione e cause civili, ed anche in Europa sono allo studio diversi provvedimenti giudiziari contro questo tipo di reato. Il successo di questi sforzi, o anche il loro fallimento, e la moralità o l'immoralità della pratica di scaricare questo tipo di materiale, possono anche essere messi in secondo piano rispetto ai costi che un'azienda potrebbe dover sostenere per difendersi di qualche accusa di violazione delle leggi sull'argomento. Sulle reti P2P è molto diffuso anche materiale pornografico. Il fatto che secondo la legge locale tale materiale più sia o meno legale è di secondaria importanza di fronte a possibili problemi legali che possono essere sollevati da qualche dipendente che ritiene offensivo il materiale che un altro dipendente ha scaricato usando i sistemi aziendali.

W7.2 Sistemi operativi interessati

Vi sono versioni dei software P2P disponibili per i sistemi operativi Windows attualmente in circolazione, assieme a versioni per sistemi UNIX e Linux.

W7.3 Riferimenti CVE/CAN

CVE-2002-0967, CVE-2001-0368

CAN-2000-0412, CAN-2002-0314, CAN-2002-0315, CAN-2003-0397

W7.4 Come stabilire se si è vulnerabili

Scoprire l'attività P2P sulla rete può rivelarsi arduo. Si può trovare un software P2P attivo sulla vostra rete monitorando i traffico nelle più comuni porte utilizzate dal software or cercando il traffico per alcune *application layer string* comunemente usate dai software P2P. Alla fine di questo capitolo è riportata una lista delle porte più comunemente utilizzate dalle applicazioni P2P.

Ci sono molte applicazioni o servizi che possono aiutare a scoprire o a prevenire il traffico P2P. Qualche software per host di prevenzione dalle intrusioni può impedire l'installazione o l'esecuzione di applicazioni P2P. La Cisco Network Based Application Recognition (NBAR) ed altri prodotti di rete possono impedire al traffico P2P di entrare o di uscire dalla rete oppure monitorare il traffico P2P. Anche il monitoraggio della delle connessioni WAN con applicazioni come NTOP può rivelare l'eventuale traffico P2P. Si potrebbe anche ricercare nei percorsi di archiviazione in rete i file più comunemente scaricati dagli utenti, che di solito hanno estensione *.mp3, *.wma, *.avi, *.mpg, *.mpeg, *.jpg, *.gif, *.zip, *.torrent e *.exe. Può essere utile anche monitorare i rapidi cali di spazio disponibile nei dischi. Anche Nessus ha un plug-in che scopre le applicazioni P2P attive e, limitatamente alle macchine Microsoft Windows, si può usare SMS per verificare gli eseguibili installati sulle workstation.

W7.5 Come proteggersi

Policy aziendale:

1. La vostra azienda dovrebbe adottare e far rispettare una policy contro il download di materiale protetto da copyright.
2. La vostra azienda dovrebbe adottare e far rispettare una policy per il corretto utilizzo delle risorse informatiche, e in particolare della connessione aziendale ad Internet.
3. Dovreste verificare regolarmente i supporti di archiviazione in rete e le workstation per controllare che non venga salvato materiale non autorizzato.

Restrizioni di rete:

1. I normali utenti non dovrebbero avere la possibilità di installare alcun software, in particolare le applicazioni peer to peer.
2. Prendete in considerazione la possibilità di utilizzare un server proxy server per controllare l'accesso a Internet.
3. I filtri in uscita dovrebbero limitare l'accesso a qualsiasi porta che non sia necessaria all'attività aziendale, per quanto il fatto che molte applicazioni P2P stiano andando verso l'http renderà questo provvedimento meno efficace.
4. Monitorate il traffico P2P della vostra rete ed indirizzate le violazioni della policy attraverso i canali appropriati.
5. Utilizzate software antivirus in tutta l'azienda ed assicuratevi che siano sempre aggiornati quotidianamente.

Porte comunemente utilizzate dalle applicazioni peer to peer

Napster	eDonkey	Gnutella	KaZaa
tcp 8888	tcp 4661	tcp/udp 6345	tcp 80 (WWW)

tcp 8888	tcp 4661	tcp/udp 6345	tcp 80 (WWW)
tcp 8875	tcp 4662	tcp/udp 6346	tcp/udp 1214
tcp 6699	udp 4665	tcp/udp 6347	
		tcp/udp 6348	

Riferimenti nel database delle definizioni Snort all'indirizzo http://www.snort.org/cgi-bin/sigs-search.cgi?sid=p2p

549 P2P napster login
550 P2P napster new user login
551 P2P napster download attempt
552 P2P napster upload request
556 P2P Outbound GNUTella client request
557 P2P GNUTella client request
559 P2P Inbound GNUTella client request
561 P2P Napster Client Data
562 P2P Napster Client Data
563 P2P Napster Client Data
564 P2P Napster Client Data
565 P2P Napster Server Login
1383 P2P Fastrack (kazaa/morpheus) GET request
1432 P2P GNUTella GET
1699 P2P Fastrack (kazaa/morpheus) traffic
2180 P2P BitTorrent announce request
2181 P2P BitTorrent transfer

torna all'inizio ^

W8 LSASS

W8.1 Descrizione

Il Windows Local Security Authority Subsystem Service sulle edizioni Windows 2000, Server 2003 e Server 2003 64 Bit, XP e XP 64 Bit contiene un pericoloso buffer overflow che, se sfruttato, può portare alla compromissione completa del sistema. Questo overflow è sottolineato nel Microsoft Security Bulletin MS04-011. Questo attacco può essere portato a termine da remoto e in forma anonima attraverso RPC su sistemi Windows 2000 e XP, ma richiede privilegi locali per essere eseguito su Server 2003 o Windows XP 64 Bit edition.

Il Local Security Authority Subsystem Service (LSASS) svolge un ruolo importante nell'autenticazione al sistema e nelle funzionalità di Active Directory. È proprio nel processo di connessione con Active Directory che la funzione di logging della DLL LSASRV.dll può causare un overflow con una stringa particolarmente lunga. Potenzialmente questa vulnerabilità può comportare una completa compromissione del sistema.

La gravità del fatto che questa vulnerabilità possa essere facilmente sfruttata da remoto è dimostrata dalla recente propagazione dei worm Sasser and Korgo (noti anche come W32.Sasser (http://www.cert.org/current/archive/2004/07/12/archive.html#sasser,

http://www.microsoft.com/security/incident/sasser.mspx) e W32.Korgo (http://www.cert.org/current/archive/2004/07/12/archive.html#korgo), che si basano proprio su LSASS. Anche molti "bot" worm recenti e particolarmente dannosi utilizzano questa vulnerabilità: la loro importanza come problema di sicurezza in pieno sviluppo è in costante crescita, anche se viene spesso sottovalutata.

A questa vulnerabilità è assegnato il codice CVE CAN-2003-0533. Si raccomanda gli amministratori di rete di non limitarsi ad applicare sui propri sistemi le patch che riguardano questa vulnerabilità, ma di implementare anche tutti i necessari controlli di accesso ai punti di ingresso della rete per bloccare l'uso non autorizzato di Windows RPC ed impedire l'ingresso in ambienti vulnerabili.

W8.2 Sistemi operativi interessati
Windows 2000, Windows XP e XP Professional, Windows XP 64-Bit Edition, Windows 2003

W8.3 Riferimenti CVE/CAN

CVE-1999-0227

CAN-1999-1234, CAN-2001-1122, CAN-2003-0507, CAN-2003-0533, CAN-2003-0663, CAN-2003-0818

W8.4 Come stabilire se si è vulnerabili
Questa vulnerabilità si può scoprire sia in rete, sia in locale sul singolo sistema. Una verifica di rete risponde meglio alle esigenze di amministratori di rete e della sicurezza che hanno bisogno di scoprire macchine vulnerabili all'interno di una rete o di un intervallo di IP. Una verifica locale si adatta meglio a utenti finali che devono scoprire se il loro sistema è vulnerabile.

Per le verifiche di rete, i tre strumenti seguenti sono in grado di rilevare questa vulnerabilità:

1. Nessus, uno strumento di analisi delle reti, ha un plug-in smb_kb835732.nasl (id 12209) che verifica l'esistenza della patch KB835732. Per i dettagli e per il download si veda http://cgi.nessus.org/plugins/dump.php3?id=12209

2. DSScan della Foundstone permette di scandagliare intere reti e fornisce uno strumento per inviare avvisi verso i sistemi vulnerabili. Per i dettagli e per il download si veda http://www.foundstone.com/resources/proddesc/dsscan.htm

3. Il Sasser Worm Scanner della eEye determina se il sistema è vulnerabile all'exploit LSASS e al worm Sasser. Per i dettagli e per il download si veda http://www.eeye.com/html/resources/downloads/audits/index.html

Per la verifica in locale ci si può affidare ai seguenti strumenti Microsoft.

Il Microsoft Baseline Security Analyzer (MBSA) permette di stabilire se la macchina è vulnerabile all'exploit. Per i dettagli e per il download si veda at http://www.microsoft.com/technet/security/tools/mbsahome.mspx

Windows Update verifica il computer e fornisce una serie di aggiornamenti personalizzati. Se tra gli aggiornamenti non ancora installati sulla macchina risulta anche l'MS04-011 (KB835732), allora la macchina è vulnerabile. Si può

leggere le istruzioni passo-passo all'indirizzo
http://windowsupdate.microsoft.com

W8.5 Come proteggersi

Sommario:

1. Bloccando le porte sul Firewall
2. Applicando le patch più recenti di Microsoft
3. Abilitando sui sistemi il filtro avanzato TCP/IP

Dettagli:

1. Bloccare le porte sul Firewall.

   Se avete un Firewall, potete proteggere le reti e i sistemi all'interno del firewall dagli attacchi originati all'esterno bloccando le seguenti porte:

   - UDP/135, UDP/137, UDP/138, UDP/445
   - TCP/135, TCP/139, TCP/445, TCP/593

   Si consiglia di usare anche un personal firewall sull'host e di bloccare il traffico in entrata non richiesto. La funzione Internet Connection Firewall (ICF), che può essere usata come supporto alla protezione dei vostri host connessi ad Internet in Windows XP o in Windows Server 2003, blocca il traffico in entrata non richiesto per default. Per abilitare la funzione Internet Connection Firewall usando *L'Installazione guidata rete*, seguite queste istruzioni:

   a. Cliccate **Start** e quindi **Pannello di Controllo**

   b. Tra le icone scegliete **Connessioni di rete** e quindi cliccate tra le *Operazioni di rete* su **Installa una rete domestica o una piccole rete aziendale.** La funzione Internet Connection Firewall viene abilitata quando scegliete una configurazione nell'*Installazione guidata rete* che indica che il vostro sistema è connesso direttamente ad Internet.

   Per configurare manualmente l'Internet Connection Firewall per una determinata connessione, seguite queste istruzioni:

   a. Cliccate **Start** e quindi **Pannello di Controllo**
   b. Tra le icone scegliete **Connessioni di rete**.
   c. Selezionate con il tasto destro del mouse le connessioni per le quali volete abilitare l'Internet Connection Firewall, e quindi cliccate **Proprietà**
   d. Scegliete la voce **Avanzate**
   e. Selezionate l'opzione per **Proteggere il computer e la rete limitando o impedendo l'accesso al computer da Internet** e quindi cliccate **OK.**

Nota: Se volete permettere l'utilizzo di alcuni programmi e servizi attraverso il firewall, quando siete alla voce **Avanzate** cliccate su **Impostazioni**, e quindi scegliete i programmi,

e protocolli e i servizi da abilitare.

2. Applicare le patch per LSASS più recenti relative al vostro sistema operativo Windows.

   La patch per la vulnerabilità LSASS è disponibile al seguente indirizzo http://www.microsoft.com/technet/security/bulletin/MS04-011.mspx

3. Abilitare il filtro avanzato TCP/IP per bloccare tutto il traffico in entrata. Per configurare il Filtro TCP/IP, seguite queste istruzioni.

   A. Cliccate **Start**, andate al **Pannello di controllo**, andate con il tasto destro del mouse su **Connessioni di rete** e quindi scegliete **Apri**.
   B. Selezionate con il tasto destro la connessione di rete per la quale volete configurare il controllo di accesso in ingresso e quindi cliccate **Proprietà.**
   C. Sotto *La connessione utilizza i componenti seguenti* della voce **Generale**, cliccate su **Protocollo Internet (TCP/IP)** e quindi sul tasto **Proprietà**.
   D. Nella finestra **Proprietà-Protocollo Internet (TCP/IP)**, cliccate sul tasto **Avanzate**.
   E. Cliccate sulla voce **Opzioni**.
   F. Cliccate su **Filtro TCP/IP**, e quindi **Proprietà**.
   G. Selezionate la casella di opzione **Attiva filtro TCP/IP (su tutte le schede)**.
   H. In questa finestra vi sono anche tre colonne con le seguenti diciture:
      - **Porte TCP**
      - **Porte UDP**
      - **Protocolli IP**

      In ciascuna colonna, potete scegliere una delle seguenti opzioni:

      A) **Autorizza tutti**. Selezionate questa opzione se volete permettere a tutto il traffico TCP o UDP.

      B) **Autorizza solo.** Selezionate questa opzione se volete permettere solo un certo traffico TCP o UDP. Cliccate **Aggiungi** e quindi il corrispondente numero di porta o di protocollo nella finestrella **Aggiungi filtro**. Non è possibile bloccare traffico UDP o TCP scegliendo **Autorizza solo** nella colonna **Protocolli IP** e aggiungendo i Protocolli IP 6 e 17.

Nota: Quando configurate il filtro TCP/IP, ricordate quali porte volete bloccare. Per la vulnerabilità LSASS dovete bloccare la porta in ingresso TCP/445.

torna all'inizio ^

W9 Client di posta

W9.1 Descrizione

Microsoft Outlook è un gestore personale di informazioni e un client e-mail per Microsoft

Windows. È principalmente una applicazione e-mail, anche se include anche un gestore di attività, di contatti e di appuntamenti. Se usato in abbinamento a Microsoft Exchange Server, Outlook può fornire ulteriori funzionalità di gruppo, come il supporto per utenti multipli, il coordinamento delle tempistiche per le riunioni, calendari e caselle di posta condivise.

Outlook Express (OE) è una versione meno versatile ma gratuita di Outlook che presenta sevizi base per la gestione delle e-mail e dei contatti. Viene fornita assieme ad Internet Explorer sin dalla versione 1.0, ed è parte integrante di tutte le versioni di Microsoft Windows a partire da Windows 95. La versione più recente di Outlook Express, la 6.0 con il SP1 applicato, è disponibile gratuitamente per il download. Integrando prodotti quali Internet Explorer con Outlook Express in ulteriori linee di prodotto, incluso Office, BackOffice e lo stesso sistema operativo Windows, Microsoft ha consentito di usare tecnologie e codici comuni in piattaforme diverse. Sfortunatamente, questa prassi introduce anche delle debolezze specifiche e aumenta l'impatto che ciascuna specifica vulnerabilità può comportare.

Uno degli obiettivi di Microsoft è stato quello di sviluppare una soluzione per la gestione delle e-mail e delle informazioni che fosse pratica ed intuitiva. Sfortunatamente, le funzioni di automazione integrate sono in contrasto con le funzioni di controllo della sicurezza (spesso trascurate dagli utenti finali). Questa situazione ha portato a un continuo aumento dei virus per e-mail, di worm e codici pericolosi e di altre numerose forme di attacco dirette a colpire i sistemi.

Le potenziali minacce per la sicurezza dei client e-mail comprendono:

- Infezione del computer da parte di virus o worm – codice dannoso che viene diffuso negli allegati o come script incapsulato nel corpo del messaggio;
- Spam – e-mail commerciali non richieste;
- Web beaconing – conferma di indirizzi e-mail che viene attivata all'apertura di un messaggio da parte del destinatario.

Le versioni attuali di Outlook e Outlook Express, quando correttamente configurati, possono proteggere efficacemente gli utenti dalle minacce citate.

W9.2 Sistemi operativi interessati

In tutte le versioni di Microsoft Windows Outlook Express è distribuito assieme ad Internet Explorer, e quindi tutte sono potenzialmente vulnerabili.

Per identificare la versione di OE presente, avviate Internet Explorer e quindi scegliete Informazioni su Internet Explorer dal menu di aiuto (?).Le versioni antecedenti la 6 devono essere immediatamente aggiornate e corrette con tutti gli aggiornamenti di sicurezza corrispondenti.

Outlook è presente su una macchina solo se l'utente lo ha volontariamente installato, come applicazione singola o come parte della suite di Microsoft Office. Le versioni di Outlook per Microsoft Windows comprendono:

- Outlook 95
- Outlook 97
- Outlook 98
- Outlook 2000, conosciuto anche come Outlook 9
- Outlook XP, conosciuto anche come Outlook 10 o Outlook 2002

- Outlook 2003, conosciuto anche come Outlook 11

Le versioni precedenti ad Outlook 2000 non sono più supportate da Microsoft ed è quindi caldamente raccomandato il loro aggiornamento ad una versione supportata del prodotto (Outlook 2003, 2002 o 2000).

Tutte le versioni di Outlook dovrebbero avere installato l'ultimo service pack corrispondente.

Le attuali versioni del service pack per Outlook sono:
- Outlook 2000 – Service Pack 3
- Outlook XP (Outlook 2002) – Service Pack 3
- Outlook 2003 attualmente non ha un service pack.

Per identificare la versione corrente di Outlook, avviate il programma e selezionate "Informazioni su Microsoft Outlook" dal menu di aiuto.

Riferimenti:
Outlook Express http://www.microsoft.com/windows/oe/
Outlook http://www.microsoft.com/office/outlook/
Scadenze del supporto http://support.microsoft.com/default.aspx?id=fh;[ln];lifeprodo
Download per Office http://office.microsoft.com/OfficeUpdate

CVE-1999-0967, CVE-2000-0036, CVE-2000-0567, CVE-2000-0621, CVE-2000-0662, CVE-2000-0753, CVE-2000-0788, CVE-2001-0149, CVE-2001-0340, CVE-2001-0538, CVE-2001-0660, CVE-2001-0666, CVE-2001-0726, CVE-2001-1088, CVE-2002-0152, CVE-2002-0685, CVE-2002-1056

CAN-1999-0004, CAN-1999-0354, CAN-1999-1016, CAN-1999-1033, CAN-1999-1164, CAN-2000-0105, CAN-2000-0216, CAN-2000-0415, CAN-2000-0524, CAN-2000-0653, CAN-2000-0756, CAN-2001-0145, CAN-2001-0945, CAN-2001-0999, CAN-2001-1325, CAN-2002-0285, CAN-2002-0481, CAN-2002-0507, CAN-2002-0637, CAN-2002-1121, CAN-2002-1179, CAN-2002-1255, CAN-2003-0007, CAN-2003-0301, CAN-2004-0121, CAN-2004-0215, CAN-2004-0284, CAN-2004-0380, CAN-2004-0501, CAN-2004-0502, CAN-2004-0503, CAN-2004-0526

W9.3 Come stabilire se si è vulnerabili
Tutti i computer che hanno installato Internet Explorer contengono anche Outlook Express. L'installazione manuale delle applicazioni della suite Microsoft Office può comprendere Outlook assieme ai più comuni pacchetti quali Word, Excel, PowerPoint e Access.

Un sistema può essere vulnerabili se presenta una di queste de caratteristiche:

a. non è completamente aggiornato, la qual cosa può essere verificata visitando il sito di aggiornamento Microsoft, oppure
b. le impostazioni di sicurezza non sono correttamente configurate

W9.4 How to Determine if you are Vulnerable
Vi sono una serie di cose che si può fare per configurare Outlook e/o Outlook Express per ridurre al minimo i rischi.

Rendere sicuro Outlook / Outlook Express
Per default Outlook e Outlook Express hanno delle impostazioni di configurazione e di

sicurezza piuttosto disinvolte. È importante renderle più stringenti e controllare che il core software sia aggiornato. Alcune operazioni attuabili sono:

1. Visitare periodicamente il sito Microsoft Update, http://windowsupdate.microsoft.com, e applicare tutti gli Aggiornamenti importanti.
2. Disabilitare l'Anteprima dei messaggi disabilitando l'opzione "Riquadro di anteprima" al menu Visualizza.
3. Rendere più stringenti le impostazioni relative alle Aree di Sicurezza associate alla posta in arrivo.
   Selezionate Strumenti > Opzioni e quindi cliccate sulla voce Protezione. Cliccate su Impostazione Aree e quindi su "Siti con restrizioni" e quindi impostate le opzioni di protezioni in Alta. Cliccate Applica e quindi OK per salvare le impostazioni.

Protezione dagli allegati con codice potenzialmente dannoso

Le versioni di Outlook 2000 (SP3), Outlook 2002 (SP1 e successivi) e Outlook 2003 (tutte le versioni) includono una efficace protezione contro gli allegati che possono potenzialmente contenere codice dannoso. Tutti gli allegati con estensioni come .exe, .com, .vbs ecc. Vengono bloccati per default. Per questo si raccomanda di usare uno strumenti di compressione come WinZip o un diverso canale di trasferimento del file (FTP, SCP) se si rende necessario l'invio di file in eseguibili.

Una lista completa delle estensioni bloccate da Outlook è disponibile nel testo:

http://www.microsoft.com/office/ork/2003/three/ch12/OutG07.htm

Per estendere la lista predefinita delle tipologie di file da bloccare è necessario modificare il Registro nel modo seguente:

1. Cliccate Start, Esegui, digitate regedit e quindi cliccate OK.
2. Cercate e quindi selezionate la seguente chiave di registro:

Per Outlook 2003:

HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Outlook\Security

Per Outlook XP/2002:

HKEY_CURRENT_USER\Software\Microsoft\Office\10.0\Outlook\Security

Per Outlook 2000:

HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Outlook\Security

3. Dal menu modifica, andate su Nuovo e quindi cliccate Valore Stringa.
4. Nel Nome scrivete Level1Add, e quindi premete INVIO.
5. Dal menu Modifica, cliccate Modifica.
6. Scrivete nel Valore le <estensioni_file>, e quindi cliccate OK.

Nota: *estensioni_file* è una lista delle estensioni di file allegati. Ciascuna estensione va

separata da un punto e virgola. Ad esempio, scrivete ".zip; .gif" se volete bloccare tutti i file .zip e .gif che arrivano come allegato in un messaggio e-mail.

L'articolo di Microsoft Technet KB837388 *How to configure Outlook to block additional attachment file name extensions* fornisce una descrizione dettagliata di questo processo:

http://support.microsoft.com/?kbid=837388

Protezione dallo SPAM (e-mail commerciali non richieste)

Outlook 2003 include una efficace protezione dallo Spam. Per configurarla, aprite Outlook – selezionate *Azioni – Posta indesiderata – Opzioni posta elettronica indesiderata.*
La voce *Opzioni* di questa finestra di dialogo ha quattro pulsanti di scelta che controllano la configurazione e la soglia del motore anti-spam:

- Disattiva filtro automatico – lo spam non verrà filtrato;
- Basso (impostazione predefinita) – impostazione abbastanza efficace; sposta la maggior parte dello spam nella cartella Posta indesiderata e nella pratica presenta pochissimi falsi positivi;
- Alto – filtro spam piuttosto aggressivo. Filtra praticamente tutta la posta indesiderata (la invia alla cartella *Posta indesiderata*), ma può potenzialmente etichettare come spam alcune e-mail legittime. Se impostate questo livello, quindi, controllate periodicamente la cartella *Posta indesiderata* per controllare che non vi siano e-mail legittime identificate erroneamente come spam;
- Solo elenchi indirizzi attendibili – saranno consegnate solo mail da mittenti o domini presenti nell'elenco dei *Mittenti attendibili* o dei *Destinatari attendibili*. Questa è l'impostazione più a prova di spam, ma richiede un certo lavoro per popolare la lista dei Mittenti attendibili e dei Destinatari attendibili inserendo il corretto indirizzo di posta e il dominio corrispondente.

Outlook Express e le versioni precedenti di Outlook non possiedono funzionalità anti-spam efficaci, ma comunque hanno un Elenco dei Mittenti bloccati. Per impostarlo in Outlook Express, andate su *Strumenti* > *Regole Messaggi* e quindi selezionate *Elenco Mittenti bloccati*.

Protezione dal codice dannoso contenuto nel testo delle e-mail

I messaggi e-mail in formato rich-text (HTML, RTF) possono contenere nel testo codice dannoso, a differenza delle e-mail in formato testo normale, che non possono includere codice. Il modo più semplice ed efficace di proteggersi da tale codice dannoso è quello di visualizzare tutti i messaggi e-mail in testo normale. Per configurare queste preferenze in Outlook 2003, andate su *Strumenti* > *Opzioni, e* quindi selezionate la voce *Preferenze,* quindi il tasto *Opzioni di Posta elettronica*, e attivate la casella *Visualizza tutti i messaggi standard in formato testo normale* e poi *Visualizza tutti i messaggi con firma digitale in formato testo normale.* Premete quindi due volte *OK*.

Protezione dal Web Beaconing

Il Web Beaconing è un metodo che consente di verificare quando un messaggio e-mail viene visualizzato, includendo delle piccole immagini (di solito della dimensione di 1x1 pixel) nel corpo di un messaggio HTML, e di confermare di conseguenza che l'indirizzo del destinatario è valido e utilizzabile per un futuro spam. Questa tecnica viene largamente utilizzata dagli spammer e dai pubblicitari. Oltre a fornire una conferma dell'apertura del messaggio e-mail,

il Web Beaconing permette di ottenere alcune informazioni (indirizzo IP, lingua, versione del browser) che riguardano l'utente e il sistema. Per prevenire il Web Beaconing su Outlook 2003, aprite Outlook – Selezionate *Strumenti* > *Opzioni*, e quindi andate alla voce *Protezione*. Andate alla voce *Cambia impostazioni download automatico* e selezionate le caselle *Non scaricare automaticamente immagini o altro contenuto dei messaggi HTML* e *Avvisa prima di scaricare contenuto durante la modifica, l'inoltro o la risposta a messaggi* – premete quindi due volte *OK*.

Comportamento degli utenti

Siccome spesso è il fattore umano l'anello più debole della catena in un processo di sicurezza, quando si ha a che fare con la posta elettronica è importante seguire alcuni consigli.

Quando si riceve un allegato, anche se proviene da una fonte fidata, è importante sincerarsi che sia stato controllato per verificare la presenza di virus o di altri codici maligni, come descritto nella seguente sezione Anti-Virus.

Quando ricevete un allegato, salvatelo in una cartella diversa da Documenti, perché questa è proprio la cartella che molti virus usano come punto di partenza. Selezionate una cartella diversa o addirittura una diversa partizione del disco, per separare gli allegati in arrivo dai resto dei vostri file.

Non aprite mai allegati inattesi, anche se provengono da amici. Anche i file DOC e XLS possono contenere dei programmi in Basic che possono causare danni al vostro sistema. Se dovete aprire documenti con un diverso prodotto di Microsoft, quale ad esempio Word, accertatevi di andare sotto Strumenti > Opzioni > Protezione e selezionare l'opzione Alta per disabilitare le macro, a meno che queste non siano firmate.

Controllare sempre che tutte le firme digitali associate a file eseguibili garantiscano l'integrità del file e verifichino che siano originate da una fonte fidata.

Anti-Virus

Il software antivirus può contribuire a proteggere i computer nei confronti di molti virus, worm, trojan ed altro codice dannoso. Da questo punto di vista è necessario che il database delle definizioni dell'antivirus sia aggiornato almeno una volta a settimana (e meglio ancora quotidianamente e in modo automatico) per aiutare a proteggersi dalle minacce più recenti. Molte soluzioni di antivirus attuali hanno completamente automatizzato questo compito. È comunque sempre prudente sincerarsi che vengano esaminati tutti file, indifferentemente dal tipo di file e dalla loro origine.

Le moderne soluzioni antivirus hanno la capacità di esaminare tutti i file in ingresso ed in uscita per garantire che i file e gli script di tipo dannoso vengano bloccati prima di poter causare danni al sistema locale.

Si raccomanda vivamente di installare strumenti di protezione anti-virus prima di usare l'e-mail o altri servizi Internet, poiché molti virus si diffondono tramite i client e-mail in forma di allegati o di codice scritto con finalità dolose, che vengono attivati anche in fase di anteprima o di lettura del messaggio.

Riferimenti:
Riferimenti Microsoft per l'Antivirus
http://www.microsoft.com/security/protect/antivirus.asp

Aggiornare Outlook ed Outlook Express

Outlook Express stato aggiornato diverse volte nel corso di questi anni, diventando migliore in stabilità e sicurezza. La versione più recente è disponibile gratuitamente presso

http://www.microsoft.com/windows/oe/

Per assicurarsi che Outlook e tutti gli altri programmi Office siano aggiornati, visitate la Pagina degli aggiornamenti dei prodotti Office. Questo sito rileva automaticamente gli aggiornamenti importanti e indicati come necessari.

Per informazioni dettagliate inerenti le altre funzioni ed impostazioni di sicurezza in Office 2003, leggete l'Office 2003 Security white paper.
Nota: è opportuno contattare l'amministratore di sistema prima di operare cambiamenti su qualsiasi computer che faccia parte di una organizzazione che ne ha uno. L'amministratore può ottenere informazioni tecniche dettagliate sulla sicurezza per Outlook nell'Office Resource Kit.

Disinstallare Outlook ed Outlook Express
Se si utilizza un diverso client per l'e-mail o per la gestione delle informazioni, si può tranquillamente disinstallare Outlook ed Outlook Express.

Outlook su tutte le versioni di Windows
Si può rimuovere Outlook cliccando Start > Impostazioni > Pannello di controllo e facendo doppio click sull'icona Installazione applicazioni. Quando si apre la relativa finestra, si seleziona la voce Outlook e quindi il tasto Rimuovi.

Outlook Express su Windows 98/ME
Si può rimuovere Outlook dal computer cliccando Start > Impostazioni > Pannello di controllo e facendo doppio click sull'icona Installazione applicazioni. Quando si apre la relativa finestra di dialogo, si seleziona la voce Installazione di Windows e si scende nell'elenco dei componenti fino ad incontrare la voce Microsoft Outlook Express. A questo punto deselezionate la casella a fianco.
Cliccando infine i tasti Applica e quindi OK, salverete questa scelta e procederete alla disinstallazione di Outlook Express.

Outlook Express su Windows 2000/XP o per le versioni aggiornate di Internet Explorer
I passi necessari per la rimozione di Outlook Express sotto Windows 2000/XP o per gli utenti che vogliano utilizzare un browser di versione diversa da quella presente nella installazione standard sono molto più complessi:

Utenti di Windows 2000 che impiegano Microsoft Outlook Express versioni 5.x/6.0
http://support.microsoft.com/default.aspx?scid=kb;EN-US;q263837

Windows 98/Me aggiornati a Microsoft Outlook Express versioni 5.x/6.0
http://support.microsoft.com/default.aspx?scid=kb;EN-US;q256219

Note: Outlook Express può essere re-installato senza che lo sappiate se si installa un service pack o un aggiornamento del sistema operativo.

torna all'inizio ^

W10 Instant Messaging

W10.1 Descrizione

La tecnologia di Instant Messaging è diventata matura negli ultimi anni da una nuova applicazione aggiunta alle funzioni principali dei sistemi operativi Windows che permette agli utenti mantenere un rapido contatto con amici e parenti, ma che è spesso utilizzata per comunicazioni d'affari, le collaborazioni e le operazioni di supporto. Anche se le applicazioni

di Instant Messaging (IM) di terze parti mantengono ancora una grossa fetta delle istallazioni IM, vi è una tendenza crescente ad integrare funzionalità di messaggistica negli stessi sistemi operativi che possono comportare minacce dirette alla sicurezza alle organizzazioni che non hanno delle policy di utilizzo delle risorse o strutture tecniche operative che impediscono l'utilizzo di questa tecnologia. La scoperta di vulnerabilità in questi programmi mette a grave rischio anche le organizzazioni che mancano di contromisure tecnologiche, personale dedicato alla sicurezza o possibilità di ridurre in qualche modo questa crescente minaccia interna.

La stragrande maggioranza di applicazioni IM che si trovano su sistemi Windows appartengono a una lista che annovera Yahoo! Messenger (YM), AOL Instant Messenger (AIM), MSN Messenger (MSN) e Windows Messenger (WM), che ora è pienamente integrato in Windows XP nelle edizioni Professional e Home. Le funzionalità che questi programmi apportano al desktop sono di ampio raggio e possono fornire agli utenti la possibilità, assieme e al di là di una semplice chat testuale, di verificare web mail remote, instaurare delle chat vocali, realizzare comunicazioni video ed inviare e condividere file di dati. C'è anche una crescita dei programmi di messaging "multi network" che offrono all'utente un'interfaccia centralizzata per i più disparati sistemi di messaggistica e i protocollo più vari, come Trillian e l'alleanza recentemente stretta tra AOL, Yahoo! E MSN chat, che permette a tutti e tre questi client di interagire da un'unica postazione.

Le vulnerabilità sfruttabili da presenti in questi programmi e nelle risorse a questi collegate sono un problema crescente per l'integrità e la sicurezza delle reti, direttamente proporzionale alla loro rapida integrazione e diffusione sui sistemi Windows. Gli scenari di attacco alle vulnerabilità di Instant Messaging sono estremamente variegati e possono concretizzarsi nella forma di buffer overflow eseguiti da remoto (basati su RPC o su pacchetti malformati), attacchi basati sul link URI pericolosi, su vulnerabilità di trasferimento file e su exploit Active X.

Le vulnerabilità in questi programmi di solito derivano dalle seguenti categorie:

- **Controlli ActiveX obsoleti** – es. Buffer Overflow della "ResDLL" di MSN Messenger CAN-2002-0155, Yahoo! Voice Chat ActiveX Control Buffer Overflow Vulnerability (http://www.securityfocus.com/bid/7561), Yahoo! Webcam ActiveX Control Buffer Overrun Vulnerability (http://www.securityfocus.com/bid/8634).
- **Problemi di implementazione URI** – es. Esecuzione di script dannosi su Yahoo! Messenger CAN-2002-0032, URI handler buffer overflow di Yahoo! Messenger CAN-2002-0031.
- **Vari Buffer Overflow, come quelli derivati dal trasferimento di file.** – es. file validation failure in MSN Messenger CAN-2004-0122, buffer overflow "Imvironment" e del campo "message" in Yahoo! Messenger, rispettivamente CAN-2002-0320 e CAN-2002-0320, TLV 0x2711 packet parsing buffer overflow in AOL Instant Messenger CAN-2002-0005, VU#912659, YAuto.DLL Open Buffer Overflow in Yahoo! Messenger (http://www.securityfocus.com/bid/9145), Vulnerabilità Getfile Screenname Buffer Overrun i AOL Instant Messenger (http://www.securityfocus.com/bid/8825).

Queste applicazioni non solo introducono vulnerabilità di rete nei singolo sistemi, ma portano anche un rischio di perdita della proprietà intellettuale, un potenziale rischio di perdita della riservatezza e pericoli di calo della produttività da parte dei dipendenti. Per quanto la riduzione delle debolezze sfruttabili da remoto in questi programmi sia di primaria importanza, una indispensabile policy di utilizzo delle risorse e la sicurizzazione del traffico

in entrata e in uscita assumono parimenti una enorme importanza per risolvere o, meglio, evitare i problemi che l'Instant Messaging può introdurre in una rete.

W10.2 Sistemi operativi interessati:

Windows 98, Windows ME, Widows 2000 e Professional, Windows XP e Windows 2003 supportano Microsoft Instant Messenger. Tutte le versioni di Microsoft Windows XP presentano Instant Messenger integrato nel sistema operativo.

W10.3 Riferimenti CVE/CAN:

CVE-2002-0005, CVE-2002-0032, CVE-2002-0155, CVE-2002-0785,

CAN-2002-0031, CAN-2002-0228, CAN-2002-0320, CAN-2002-0362, CAN-2003-0717, CAN-2004-0043, CAN-2002-1486

W10.4 Come stabilire se si è vulnerabili:
Per identificare la versione installata di Microsoft Instant Messenger, avviate l'applicazione e quindi selezionate la voce Informazioni su Instant Messenger dal menu di aiuto. Le verioni precedenti la 6.2 devono essere sostitite con la più recente e aggiornate con le patch e gli aggiornamenti di sicurezza appropriati.

W10.5 Come proteggersi:

(a) Controllate che qualsiasi software di messaggistica installato come Yahoo, MSN, AOL, Trillian ecc. Sia aggirnato con tutte le patch fornite dal produttore.

(b) Configurate un Intrusion Prevention/Detection system per avvisare quando avviene un trasferimento di file attraverso qualche programma di messaging.

(c) Se la policy di sicurezza del luogo lo permette, bloccate la seguenti porte sul firewall. Tenete presente che ciò non offre una protezione completa, in quanto alcune di queste applicazioni possono anche aggirare le regole del firewall.

1863/tcp: Microsoft .NET Messenger, MSN Messenger
5050/tcp: Yahoo Messenger
6891/tcp: Trasferimenti di file con MSN Messenger
5190-5193/tcp: AOL Instant Messenger

(d) Bloccate l'accesso alle pagine web che contengono link con URL come "aim:" o "ymsgr:". Questo può prevenire lo sfruttamento delle vulnerabilità negli handler URI. Un'altra via è quella di rimuovere accuratamente queste chiavi di registro nella "HKEY_CLASSES_ROOT".

(e) Bloccate l'accesso alle pagine web che chiamano i controlli ActiveX associati con qualche problema del messenger. Ciò può prevenire lo sfruttamento di vulnerabilità dei controlli ActiveX associati ai programmi di messaggistica.

torna all'inizio ^

Le maggiori vulnerabilità dei sistemi Unix (U)

U1 BIND Domain Name System

U1.1 Descrizione

Il pacchetto Berkeley Internet Name Domain (BIND) è diventato il software di gran lunga più utilizzato al mondo per il Domain Name Service (DNS). DNS è il fondamentale sistema che facilita la conversione degli hostname (ad esempio www.sans.org) nell'indirizzo IP registrato corrispondente. A causa della sua onnipresenza e del suo ruolo cruciale, BIND è diventato il bersaglio privilegiato di frequenti attacchi. In particolare gli attacchi Denial of Service (DoS), che di solito comportano ai siti Internet la completa interruzione dei servizi di naming, sono stati per lungo tempo una piaga per BIND. In BIND sono state scoperte nel tempo anche molte altre possibilità di attacco come fenomeni di buffer overflow e cache poisoning. Per quanto il team che sviluppa BIND sia storicamente molto rapido nel rispondere e nel correggerne le vulnerabilità, un numero eccessivo di server non aggiornati o mal configurati rimane esposto agli attacchi.

A questa condizione contribuiscono un certo numero di fattori. I più importanti sono costituiti dal fatto che gli amministratori che non si informano degli aggiornamenti di sicurezza, dal fatto che molti sistemi utilizzano il daemon BIND (chiamato "named") senza averne bisogno e dal fatto che spesso i file di configurazione non sono corretti. Ciascuno di questi sistemi può subire un denial of service, un buffer overflow o un DNS cache poisoning. Tra le più recenti debolezze scoperte in BIND, vi è quella del Denial of Service discusso nel CERT Advisory CA-2002-15. In questo caso un aggressore potrebbe inviare particolari pacchetti DNS per forzare un controllo interno che è in sé vulnerabile, causando la disattivazione del daemon BIND Un'altra vulnerabilità scoperta permette un attacco buffer overflow, trattato nel CERT Advisory CA-2002-19, nel quale gli aggressori utilizzano le versioni vulnerabili delle librerie del DNS resolver. Inviando risposte DNS confezionate ad arte, l'aggressore può sfruttare questa vulnerabilità ed eseguire codice abusivo o anche causare un'interruzione del servizio.

Un rischio ulteriore è costituito dal fatto che un server BIND vulnerabile può essere compromesso e utilizzato come deposito di materiale illecito senza che l'amministratore lo sappia oppure essere coinvolto in attacchi nei quali può costituire una piattaforma per attività dannose che hanno come obiettivo altre macchine su Internet.

U1.2 Sistemi operativi interessati

Praticamente tutti i sistemi UNIX e Linux vengono distribuiti con una qualche versione di BIND. Le installazioni di BIND possono essere intenzionali per utilizzare il server DNS o involontarie durante una installazione generale. Esiste anche una versione binaria di BIND per piattaforme Windows.

U1.3 Riferimenti CVE/CAN

CVE-1999-0009, CVE-1999-0024, CVE-1999-0184, CVE-1999-0833, CVE-1999-0837, CVE-1999-0835, CVE-1999-0848, CVE-1999-0849, CVE-1999-0851, CVE-2000-0887, CVE-2000-0888, CVE-2001-0010, CVE-2001-0011, CVE-2001-0012, CVE-2001-0013,

CAN-2002-0029, CAN-2002-0400, CAN-2002-0651, CAN-2002-0684, CAN-2002-1219, CAN-2002-1220, CAN-2002-1221, CAN-2003-0914

U1.4 Come stabilire se si è vulnerabili

Qualsiasi server DNS che utilizza una versione di BIND integrate nel sistema operativo dovrebbe essere controllata per verificare se adotta le patch più recenti distribuite dal produttore del sistema operativo. Se la versione adottata di BIND è stata compilata dal sorgente dell'Internet Software Consortium (ISC), bisognerebbe verificare che si tratti della versione più recente. Le versioni obsolete o non aggiornate di BIND hanno maggiori

probabilità di essere vulnerabili.

Nella maggior parte dei sistemi, il comando "named -v" mostra la versione di BIND installata, numerata come X.Y.Z, dove X è la versione principale, Y è la versione secondaria e Z è il livello di patch. Attualmente le tre versioni principali di BIND sono la 4, la 8 e la 9. Se si utilizza BIND installato dal codice sorgente, si dovrebbe evitare la versione 4 ed optare, invece, per la versione 9. Potete recuperare il codice aggiornato, la versione 9.3.0rc2, dal sito ISC.

Un approccio preventivo per mantenere la sicurezza di BIND è costituito dal sottoscrivere un servizio di alerting e di report delle vulnerabilità personalizzato, del tipo di quelli disponibili presso SANS o recuperando gli avvisi pubblicati su OSVDB. In aggiunta agli avvisi di sicurezza, anche l'utilizzo di uno strumento per la verifica delle vulnerabilità può essere molto efficace per controllare tutte le potenziali vulnerabilità del sistema DNS.

U1.5 Come proteggersi

- **Come proteggersi dalle vulnerabilità di BIND in genere:**

    1. Disabilitando il daemon BIND (chiamato "named") su tutti i sistemi che non sono specificatamente demandati e autorizzati ad essere server DNS.
    2. Applicando tutte le patch del produttore o aggiornando i server DNS alla versione più recente. Per maggiori informazioni su come rafforzare un'istallazione di BIND, consultate gli articoli su come rendere sicuri i servizi di naming riportati nella UNIX Security Checklist del CERT.
    3. Per rendere più difficili gli attacchi o le scansioni automatiche al sistema, si può nascondere il banner "Version String" di BIND sostituendo la reale versione di BIND con un numero di versione falso nel file "named.conf".
    4. Permettendo i trasferimenti di zona solo verso DNS server secondari in domini affidabili. Disabilitate i trasferimenti di zona verso domini padri o figli, utilizzando al loro posto le opzioni di delegation e forwarding.
    5. Jail: Per evitare che "named" compromessi mettano a rischio il vostro intero sistema, fate in modo che BIND venga eseguito come utente senza privilegi in una directory in chroot(). Per BIND 9, consultate http://www.losurs.org/docs/howto/Chroot-BIND.html.
    6. Disabilitando la recursion e il glue fetching, per difendersi dalla DNS cache poisoning.

- **Come proteggersi dalle vulnerabilità di BIND scoperte recentemente:**

    1. Per la vulnerabilità Denial of Service su ISC BIND 9: http//www.cert.org/advisories/CA-2002-15.html
    2. Per le molte vulnerabilità Denial of Service su ISC BIND 8: http://www.isc.org/products/BIND/bind-security.html
    3. Per il Cache poisoning tramite risposte negative: http://www.kb.cert.org/vuls/id/734644

Esistono molte guide eccellenti per l'hardening di BIND. Un'ottima guida per rafforzare BIND sui sistemi Solaris, con altri riferimenti per ottenere documentazione su BIND, può essere consultata presso Running the BIND9 DNS Server Securely, assieme agli archivi dei documenti sulla sicurezza di Bind disponibili presso Afentis. Potete anche consultare la documentazione che riguarda le tecniche generali per la sicurezza di BIND presso

http://www.linuxsecurity.com/resource_files/server_security/securing_an_internet_name_server.pdf.
Gli amministratori possono anche dare un'occhiata ad alternative a BIND come DJBDNS, disponibile all'indirizzo http://cr.yp.to/djbdns.html.

torna all'inizio ^

U2 Web server

U2.1 Descrizione

Il traffico HTTP è di gran lunga la risorsa più utilizzata dell'Internet pubblica. I Web server Unix come Apache e Sun Java System Web Server (già iPlanet) gestiscono la maggior parte di tale traffico e in conseguenza di ciò meritano un esame accurato dei relativi problemi di sicurezza. Questi problemi riguardano vulnerabilità proprie del server ed altre dei moduli aggiuntivi, di script di default/esempio/test, di bug PHP e di diversi altri vettori di attacchi.

Per quanto esista una tale varietà di strade, la principale e la più diffusa causa di danno a un web server Unix è la non corretta configurazione al momento dell'installazione o la mancanza di un regolare aggiornamento. Il risultato degli attacchi che ne approfittano può andare dal Denial of Service al defacement del sito web, fino alla possibilità di un completo accesso al server con privilegi di root da parte dell'aggressore, passando per tutte le gradazioni intermedie di danneggiamento.

Molti produttori e progetti open-source offrono dei consigli per la configurazione e continui aggiornamenti di sicurezza per i loro prodotti, ed è fondamentale che qualsiasi amministratore di un sito web ne tanga conto e ne sia costantemente aggiornato. È importante capire che la maggior parte dei web server sono compromessi a causa di exploit pubblici e ben conosciuti che approfittano di vulnerabilità per le quali da tempo esiste una patch o qualche altro sistema di correzione fornito dal produttore.

U2.2 Sistemi operativi interessati

Tutti i sistemi UNIX hanno la funzionalità di server HTTP. Molte varianti di Linux e UNIX hanno Apache installato ed abilitato per default. Apache ed iPlanet/Java System sono in grado di funzionare anche su host con altri sistemi operativi, compreso Windows, e sono verosimilmente soggetti alle stesse vulnerabilità.

U2.3 Riferimenti CVE/CAN

NOTA: Come già ricordato, Apache e iPlanet/Java System sono utilizzabili su varie piattaforme. Gli utenti di questi server dovrebbero quindi consultare i corrispondenti "Riferimenti CVE/CAN " seguenti assieme a quelli del capitolo W1.3 su Windows per avere un quadro completo delle possibili vulnerabilità.

Apache
CVE-1999-0021, CVE-1999-0066, CVE-1999-0067, CVE-1999-0070, CVE-1999-0146, CVE-1999-0172, CVE-1999-0174, CVE-1999-0237, CVE-1999-0260, CVE-1999-0262, CVE-1999-0264, CVE-1999-0266, CVE-2000-0010, CVE-2000-0208, CVE-2000-0287, CVE-2000-0941, CVE-2002-0061, CVE-2002-0082, CVE-2002-0392,

CAN-2002-0513, CAN-2002-0655, CAN-2002-0656, CAN-1999-0509, CAN-2000-0832, CAN-2002-0657, CAN-2002-0682, CAN-2003-0132, CAN-2003-0189, CAN-2003-0192, CAN-2003-0254 ,CAN-2004-0488, CAN-2004-0492

iPlanet/Sun Java System Web Server
CVE-2000-1077, CVE-2002-0845

CAN-2001-0419, CAN-2001-0746, CAN-2001-0747, CAN-2002-0686, CAN-2002-1315, CAN-2002-1316

OpenSSL
CAN-2003-0543, CAN-2003-0544, CAN-2003-0545

PHP
CVE-2002-0081,

CAN-2003-0097, CAN-2004-0594

Altri
CAN-2004-0529, CAN-2004-0734

U2.4 Come stabilire se si è vulnerabili
Qualsiasi istallazione di default o non aggiornata di un web server deve essere considerata vulnerabile.

Il modo migliore di mantenersi aggiornati sui problemi di sicurezza di un determinato prodotto è quello di consultare la pagina di informazione del rispettivo produttore. Alcune di queste pagine sono:

- La Pagina principale e i Security Report dell'HTTP Server Apache (ci si trovano anche i collegamenti ad ApacheWeek)
- Sun Web, Portal, & Directory Servers Download Center e il BigAdmin Portal
- L'Home Page e la sezione Downloads di PHP
- OpenSSL

Ciascuna delle vulnerabilità elencate devono essere affrontate *più rapidamente possibile*. La finestra di tempo tra il momento in cui la vulnerabilità viene resa nota e la pubblicazione di un exploit, ovvero di un sistema per sfruttarla, e quindi del momento in cui un worm che si avvale di tale exploit viene diffuso nel mondo sta diventando sempre più ristretta.

Per agevolare il processo di analisi delle vulnerabilità ci si può avvalere dei diversi strumenti di analisi disponibili, come Nessus e SARA (entrambi open-source), o di qualcuno degli Strumenti gratuiti o degli Scanner commerciali presenti presso eEYE. Questa scansioni dovrebbero essere eseguite su tutta la rete per permettere agli amministratori di valutare il rischio sia dei server noti che di quelli sconosciuti.

U2.5 Come proteggersi

1. Controllando che tutti i web server utilizzino il più recente livello di patch; si guardi al paragrafo "Come stabilire se si è vulnerabili " per i collegamenti al sito del produttore corrispondente.
2. Disabilitando nel server qualunque funzione non strettamente necessaria. Ciò riguarda in particolare l'accesso CGI, il supporto php, mod_ssl e mod_proxy (per Apache). Disabilitateli per default e abilitateli solo quando il servizio li richiede!
    - Se sono necessari PHP, CGI, SSI o altri linguaggi di scripting, considerate l'utilizzo di suEXEC. suEXEC permette di eseguire gli script su Apache con un user id diverso da quello di Apache.
    - **ATTENZIONE:** è necessario capire bene il funzionamento di suEXEC. Se

utilizzato in modo non corretto, può creare nuovi problemi di sicurezza.
    1. Per Apache 1.3.x consultate http://httpd.apache.org/docs/suexec.html
    2. Per Apache 2.0.x consultate http://httpd.apache.org/docs-2.0/suexec.html
3. Rendendo sicure il contenuti di cgi-bin e delle altre cartelle di script. Tutti gli script di default e di esempio devono essere eliminati.
4. Rendendo sicuro PHP:
   Questo è un argomento molto ampio che potrebbe essere trattato separatamente. Quelli che seguono sono alcuni solidi punti di partenza nel processo di sicurizzazione di PHP.
    - Disabilitate i parametri per cui PHP svela alcune informazioni negli header HTTP.
    - Controllate che PHP funzioni in safe mode.

      Le informazioni dettagliate si possono trovare qui:
      http://www.securityfocus.com/printable/infocus/1706

5. Vi sono moduli aggiuntivi che aiutano la sicurezza di Apache. Il modulo mod_security (www.modsecurity.org) può aiutare a proteggersi da Cross Site Scripting (XSS) e SQL injection. Sul sito indicato sono si possono trovare tutte le istruzioni per l'implementazione.
6. È importante anche verificare che gli script non presentino vulnerabilità come XSS e SQL injection. Esistono alcuni strumenti open source preposti a questo compito. Nikto (disponibile all'indirizzo http://www.cirt.net/code/nikto.shtml) è uno degli strumenti di analisi CGI più completi.
7. Considerando la possibilità di eseguire il server HTTP in un ambiente chroot().One. Se il server HTTP viene eseguito in chroot non può accedere ad alcuna parte della struttura delle directory del sistema operativo al di fuori dell'area chroot definita. Ciò può spesso aiutare a prevenire gli attacchi. Ad esempio, un exploit può richiamare una shell e siccome /bin/sh verosimilmente non risiede (e non deve risiedere) nella chroot, l'operazione sarebbe inefficace.
   ATTENZIONE: l'esecuzione in chroot potrebbe aver effetti negativi su CGI, PHP, database ed altri moduli o comunicazioni che possono aver bisogno dell'accesso a librerie o binari in ambiente server.
   Vi sono numerosi metodi di chrooting, e quindi è necessario consultare la documentazione del software specifico per le istruzioni. Ulteriori informazioni si possono trovare su.
    - http://www.w3.org/Security/Faq/wwwsf3.html#SVR-Q5
    - http://www.modsecurity.org/documentation/apache-internal-chroot.html
    - http://wwws.sun.com/software/whitepapers/webserver/wp_ws_security.pdf
8. Evitando di eseguire il web server come root. Sarebbe corretto creare a questo scopo un utente e un gruppo specifico con privilegi ristretti e fare in modo che nessun altro processo del sistema venga eseguito sotto tale utente o gruppo (ad esempio, eseguite Apache con l'utente "apache" invece che con l'utente "nobody").
9. Limitando la diffusione di informazioni sul server.
   Per quanto questo suggerimento tende ad incontrare l'opposizione di coloro che sostengono che la "security by obscurity" non sia un metodo accettabile di riduzione del rischio e malgrado un certo numero di tentativi di exploit realizzati sulla rete pubblica siano fatti alla cieca (prova ne sia il fatto che si notano nei log di Apache numerosi tentativi di exploit per IIS), vi sono anche molti exploit che vengono lanciati basandosi sulle informazioni dell'header.
    - Per modificare il messaggio predefinito di risposta HTTP in Apache.

1. Per Apache 1.3.x consultate http://httpd.apache.org/docs/mod/core.html#servertokens http://httpd.apache.org/docs/mod/core.html#serversignature.
2. Per Apache 2.0.x consultate http://httpd.apache.org/docs-2.0/en/mod/core.html#servertokens.

- Controllate che mod_info non sia accessibile da Internet.
- Disabilitate l'indicizzazione delle directory.

10. Un logging efficiente e completo è essenziale per tracciare correttamente ogni possibile problema di sicurezza o qualche comportamento poco chiaro del web server. Un buon metodo è quello di avvicendare periodicamente i log e di archiviare i vecchi log. Ciò farà in modo che la dimensione del file di log sia più gestibile e sia più semplice analizzarlo se si rendesse necessario.
    Varie informazioni riguardo i formati e la rotazione dei log si trovano su:
    - Per Apache 1.3.x consultate: http://httpd.apache.org/docs/logs.html
    - Per Apache 2.0.x consultate: http://httpd.apache.org/docs-2.0/logs.html

    In molti scenari il contenuto di questi log può non essere sufficiente. In particolare se si utilizza PHP, CGI o altri sistemi di scripting, una buona idea è quella di registrare le operazioni GET e POST. Questa procedura può fornire dati e prove importanti nel caso di una compromissione della sicurezza. Il log delle operazioni GET e POST può essere implementato attraverso mod_security (in Apache).

    - http://www.modsecurity.org
    - http://www.securityfocus.com/infocus/1706

torna all'inizio ^

U3 Autenticazione

U3.1 Descrizione

In quasi tutte le interazioni tra gli utenti e i sistemi informativi vengono utilizzate password, frasi identificative o codici di sicurezza. La maggior parte delle forme di autenticazione, come la maggior parte delle protezioni per file e dati, si basa su password fornite dall'utente o dal produttore. Dal momento che gli accessi correttamente autenticati spesso non vengono registrati, o anche se vengono registrati non lo sono in modo da fornire alcun segnale di allarme, una password compromessa rappresenta un'opportunità di esplorare un sistema dall'interno senza essere identificati. Un aggressore avrebbe accesso completo a qualsiasi risorsa disponibile per quell'utente e sarebbe molto vicino ad essere in grado di accedere ad altri account, a macchine vicine e forse anche ad ottenere privilegi di amministrazione. Nonostante questi pericoli, gli account con password deboli o addirittura senza password rimangono estremamente diffusi e le società con una buona policy sull'utilizzo delle password sono ancora troppo rare.

Le più comuni vulnerabilità delle password sono dovute (a) ad account senza password o con password deboli, (b) ad account utente con password conosciute da molti e spesso apertamente visibili, (c) al fatto che il sistema operativo o il software applicativo creano account di amministrazione con password deboli o privi di password (d) al fatto che gli algoritmi di hashing delle password sono deboli o comunque noti e/o gli hash delle password degli utenti vengono memorizzati in modo non sicuro e sono accessibili a chiunque.

La migliore difesa contro tutte queste vulnerabilità è una password policy ben strutturata che comprenda: descrizioni dettagliate su come gli utenti possano creare delle password robuste; regole esplicite che indichino agli utenti come accertarsi che la propria password

rimanga sicura e di modificarla periodicamente; una procedura adeguata diretta allo staff IT per sostituire rapidamente password di default/deboli/insicure/conosciute da troppi e per bloccare prontamente account non utilizzati; una procedura proattiva e periodica di verifica della robustezza e della complessità delle password; la rimozione degli account predefiniti di amministratore e di utente n necessari; la verifica regolare dei file di log del sistema di accesso/autenticazione. La Guida generale alla configurazione di Unix è disponibile presso http://www.cert.org/tech_tips/unix_configuration_guidelines.html

U3.2 Sistemi operativi interessati
Qualsiasi sistema operativo e applicazione su qualsiasi piattaforma nella quale gli utenti si autentichino tramite user ID e password.

U3.3 Riferimenti CVE/CAN
CVE-1999-0502, CVE-2001-0259, CVE-2001-0553, CVE-2001-0978, CVE-2001-1017, CVE-2001-1147, CVE-2001-1175,

CAN-2004-0243, CAN-2004-0653, CAN-1999-0501, CAN-1999-1029,

U3.4 Come stabilire se si è vulnerabili

1. Verifica per account generici

- Se vi sono account utente diffusamente noti e utilizzati da più persone o da personale temporaneo e/o password mostrate apertamente, scritte su bigliettini attaccati sulla scrivania o sul monitor, queste costituiscono delle manifeste aperture verso la rete da parte di chiunque abbia accesso fisico a tali sistemi.

2. Verifica delle password deboli o dell'inefficacia della strategia di gestione delle password.

- La pratica di configurare i nuovi account utente con la stessa password iniziale o con una password iniziale facilmente intuibile (anche se la password iniziale sarà cambiata dopo il primo login) può aprire agli aggressori una finestra di opportunità per ottenere l'accesso ai sistemi.

- Determinate su ciascun sistema locale se gli hash delle password sono salvati in /etc/passwd o in /etc/shadow. Il file /etc/passwd ha bisogno di essere leggibile da tutti gli utenti della rete per poter permettere il processo di autenticazione. Se tale file include anche gli hash delle password, allora ogni utente con accesso al sistema può leggere gli hash e provare a violarli con un password cracker. Il file /etc/shadow è nato per essere leggibile solo da root e quando possibile dovrebbe essere utilizzato per custodire gli hash delle password. Se gli account locali non sono protetti da /etc/shadow, il rischio per le password è estremamente alto. La maggior parte dei nuovi sistemi operativi usano per default /etc/shadow per archiviare gli hash delle password, a meno che questa opzione non venga ignorata da colui che li installa. C'è anche la possibilità di creare gli hash delle password utilizzando l'algoritmo MD5, molto più sicuro del precedente algoritmo crittografico.

3. Ambienti NIS

- NIS è un set di servizi che funziona come un database che fornisce informazioni di localizzazione, chiamate Map, ad altri servizi di rete come Network File System

(NFS). Per la sua stessa natura progettuale, i file di configurazione di NIS contengono gli hash delle password NIS, per cui gli hash sono leggibili da qualsiasi utente e quindi le password sono a rischio. Questo evento può verificarsi anche con alcune implementazioni di LDAP, usato come servizio di autenticazione di rete. Le versioni più recenti di NIS, come NIS+ o LDAP, hanno generalmente opzioni più rigorose nella protezione degli hash delle password, a meno che queste non siano ignorate da colui che li installa. Queste nuove versioni, però, potrebbero risultare più difficili da installare e configurare e ciò potrebbe essere un deterrente alla loro adozione.

4. Considerazioni generali

- Anche se gli hash delle password sono protetti da /etc/shadow o da altro, le password possono essere indovinate in altri modi. Vi sono altre aree di debolezza delle password abbastanza comuni, come la presenza di account attivi appartenenti ad utenti che non operano più all'interno dell'organizzazione. Le diverse organizzazioni sono di solito poco diligenti nel chiudere i vecchi account utente, a meno che non siano in uso procedure specifiche o che l'amministratore stesso non sia particolarmente diligente.

- Le installazioni di default (originate dal fabbricante o da un amministratore) di sistemi operativi o applicazioni di rete possono introdurre una vasta area di servizi non necessari e non utilizzati. In molti casi, se il fabbricante o l'amministratore sono in dubbio sulla necessità di un sistema operativo o una specifica applicazione, spesso sono spinti ad installare tutto il software possibile, nel caso sia necessario in futuro. Ciò semplifica significativamente il processo di installazione, ma introduce anche un'ampia serie di servizi inutili e di account con password deboli, di default o comunque note.

- Anche le password inviate in chiaro attraverso la rete, come ad esempio via telnet, FTP o HTTP, corrono il rischio di essere intercettate da malintenzionati. Si può usare una connessione crittata, come quelle con OpenSSH o SSL, per nascondere le password a coloro che spiano le connessioni di rete.

U3.5 Come proteggersi

La difesa migliore e la più corretta contro la debolezza delle password è una solida policy che includa le istruzioni su come generare buone password e descriva i comportamenti corretti per mantenerne la sicurezza, assieme ad una verifica proattiva dell'integrità delle password:

1. **Assicuratevi che le password siano sufficientemente robuste.** Disponendo di tempi e risorse hardware adeguate, qualsiasi password può essere violata utilizzando il sistema "brute force". Ma ci sono metodi più semplici e molto più efficaci per venire a conoscenza delle password con uno sforzo minore. I password cracker utilizzano metodi conosciuti come "attacchi da dizionario". Dal momento che i metodi crittografici sono noti, gli strumenti per l'individuazione delle password non fanno altro che confrontare le password in forma cifrata con le forme cifrate di parole del dizionario (in diverse lingue), di nomi propri, e con le permutazioni di entrambi. Di conseguenza una password la cui radice assomigli in qualche modo a una parola è estremamente suscettibile di essere violata da un attacco da dizionario. Molte organizzazioni insegnano ai propri utenti a generare password che includano combinazioni di caratteri alfanumerici e caratteri speciali, e gli utenti la maggior parte delle volte prendono una parola (ad esempio password) e convertono le lettere

in numeri o caratteri speciali (pa$$w0rd). Queste permutazioni non proteggono, però, dagli attacchi da dizionario: pa$$w0rd ha la stessa possibilità di essere violata di password.

Una buona password, quindi, non deve avere come radice una parola o un nome proprio. Una solida policy sulle password dovrebbe indirizzare gli utenti verso la creazione di password derivate da qualcosa di più casuale, come una frase o il titolo di un libro o di una canzone. Concatenando una stringa più lunga (prendendo la prima lettera di ogni parola o associando alle parole un carattere speciale o togliendo le vocali, ecc.), gli utenti possono generare stringhe sufficientemente lunghe che combinano caratteri alfanumerici e caratteri speciali in modo tale da creare una grande difficoltà ai tentativi di attacco con metodi da dizionario. E in più se la frase è facile da ricordare, lo sarà anche la password.

Una volta fornite agli utenti le corrette indicazioni su come generare buone password, possono essere messe in opera le procedure di dettaglio per controllare che queste indicazioni vengano seguite. Il modo migliore per farlo è quello di convalidare le password ogni volta che l'utente le cambia. La maggior parte dei tipi di UNIX/LINUX può usare Npasswd come front-end per verificare le password inserite alla luce della vostra policy. I sistemi abilitati PAM possono anche includere cracklib (le librerie del tool "Crack") per verificare le password una volta generate. La maggior parte dei sistemi più recenti abilitati PAM possono anche essere configurati per non accettare le password che non rispondono a determinati requisiti.

In ogni caso, se non è possibile verificare le password al momento dell'inserimento attraverso librerie a dizionario usando strumenti come Npasswd o librerie compatibili PAM, l'amministratore di sistema dovrebbe attivare delle procedure di prevenzione periodiche che prevedano l'utilizzo di strumenti di cracking in modalità stand-alone. Gli strumenti utilizzati dai potenziali aggressori sono di solito quelli più adatti. Su una piattaforma UNIX/LINUX, tra questi vi sono Crack e John the Ripper.

Attenzione*:* Non utilizzate mai un password scanner, neanche sui sistemi per i quali avete un accesso da amministratore, senza autorizzazione esplicita e preferibilmente scritta da parte del datore di lavoro. È già accaduto che amministratori di sistema con le migliori intenzioni siano stati licenziati per aver utilizzato strumenti per la determinazione delle password senza autorizzazione. Questa autorizzazione dovrebbe avere la forma di una lettera scritta che faccia parte della policy che l'organizzazione adotta per rafforzare le password e dovrebbe permettere l'effettuazione di analisi programmate periodicamente.

Una volta ricevuta l'autorizzazione ad utilizzare strumenti per la determinazione delle password sul vostro sistema, attivateli regolarmente su una macchina protetta e sicura. Gli strumenti residenti sulla macchina non dovrebbero essere apertamente accessibili a nessuno, se non l'amministratore di sistema autorizzato.Gli utenti le cui password vengono violate devono essere avvisati in modo confidenziale e devono essere fornite loro le istruzioni su come scegliere una buona password. Come parte della password policy dell'organizzazione, gli amministratori e il management dovrebbero sviluppare assieme queste procedure di notifica, in modo che il management possa fornire indicazioni e/o assistenza quando gli utenti non rispondono a tali avvisi.

Altri metodi per proteggersi da password deboli o assenti e/o di supportare le

procedure della password policy sono (a) quello di utilizzare forme alternative di autenticazione come token generatori di password o sistemi di autenticazione biometrica. Questi sono strumenti efficaci per risolvere i problemi costituiti dalle password deboli e possono essere usati come metodo alternativo di autenticazione degli utenti. È necessario sottolineare che alcuni token generatori di password richiedono la messa in opera di procedure che garantiscano la non accessibilità agli utenti non autorizzati e che neghino prontamente l'accesso al sistema se questi vengono rubati. La biometria è un settore in pieno sviluppo e dipende dal tipo di autenticazione (es. impronte digitali o riconoscimento facciale), alcune delle tecnologie non sono ancora del tutto perfezionate e sono comune gli errori di autenticazione. (b) Esistono molti strumenti molto completi di terze parti (gratuiti e commerciali) che possono aiutare a gestire meglio le password policy.

2. **Proteggete le password robuste.** Se custodite gli hash delle password in /etc/passwd, aggiornate i vostri sistemi per usare /etc/shadow. Se sul vostro sistema utilizzate NIS or LDAP in un modo per cui gli hash non possono essere protetti, chiunque (anche un utente non autenticato) può leggere gli hash delle vostre password e tentare di violarli. Dovreste cercare alternative più sicure rispetto alle versioni di NIS e LDAP che state utilizzando. Fino a quando queste applicazioni non saranno sostituite o rese sicure, dovreste rendere sicuri i permessi e compiere regolarmente delle verifiche di violabilità anche nei confronti di queste applicazioni. Considerate anche l'opzione di sostituire l'attuale crittografia per l'hash delle password con algoritmo MD5.

   Anche se le password sono robuste, gli account possono essere ugualmente compromessi se gli utenti non proteggono adeguatamente la propria password. Una buona policy include sempre istruzioni che specificano come gli utenti non devono mai riferire la propria password a nessun'altro, non devono mai trascrivere la password in supporti che possano essere letti da altri, devono rendere adeguatamente sicuro qualsiasi file nel quale sia conservata una password per l'autenticazione automatica e se si accorge che la password gli è stata rubata da altri, deve prontamente avvisare l'amministratore di sistema. La modifica periodica della password deve essere fatta rispettare in modo che quelle password che non rispettano queste regole siano vulnerabili solo in una finestra temporale limitata, e deve essere tassativamente vietato che le vecchie password possano essere riutilizzate. Controllate che agli utenti giungano gli avvisi e sia data loro le possibilità di modificare la propria password prima della scadenza. Quando si trovano di fronte a frasi come: "la vostra password è scaduta e deve essere cambiata," gli utenti tendono a scegliere una cattiva password.

3. Controllate rigorosamente gli account

Quelle che seguono sono una serie di precauzioni che garantiscono un controllo più rigoroso degli account:

- Qualsiasi account che non sia utilizzato tra quelli per l'accesso a un servizio, quelli di amministrazione e quelli predefiniti delle diverse applicazioni, deve essere disabilitato e se possibile eliminato completamente.
- Qualsiasi account in uso tra quelli per l'accesso a un servizio, quelli di amministrazione e quelli predefiniti delle diverse applicazioni, deve essere dotato di una nuova e solida password nel momento in cui il servizio o l'account sono installati o attivati.
- Configurate i nuovi account utente con password iniziali generate in modo casuale ed obbligate gli utenti a cambiarle al primo log in.

- Programmate periodiche verifiche preventive degli account sui vostri sistemi e conservate una master list di tutti questi account, specificando il servizio che richiede l'account e il fine a cui è destinato.
- Controllate periodicamente se gli account sono ancora necessari
- Sviluppate rigorose procedure per l'aggiunta e la rimozione degli account autorizzati dalla lista.
- Adottate rigide procedure anche per la rimozione degli account quando i dipendenti o i collaboratori lasciano la società o quando non sono più necessari.
- Create un contatto con la struttura di gestione del personale della vostra organizzazione in modo da essere costantemente informati su chi lascia l'organizzazione.
- Controllare periodicamente la master list facendo attenzione che non sia stato aggiunto alcun nuovo account e che gli account non utilizzati siano stati rimossi.

Non dimenticate inoltre di verificare account e password anche su sistemi di supporto come router, switch e stampanti digitali, fotocopiatrici e controller di stampanti collegati ad Internet. Se questi hanno una gestione inefficace delle password e qualche utente usa su queste la stessa password che utilizza anche su un sistema Unix, possono offrire ai malintenzionati una comoda opportunità di ingresso.

Potete trovare una lista delle password di default dei diversi produttori in:
http://www.cirt.net/cgi-bin/passwd.pl

4. Login cifrati

L'uso di password più robuste può risultare inutile se le password vengono inviate in chiaro attraverso la rete. Quando questo succede, chiunque acceda al traffico di rete può vedere le password quando vengono inviate. Alcuni programmi e protocolli che spediscono le password in chiaro sono telnet, FTP, HTTP e i Berkeley r-services.

Per prevenire questa evenienza si dovrebbero utilizzare programmi e protocolli cifrati. Usando la crittografia, le password non vengono inviate in chiaro attraverso la rete ed è molto più difficile scoprirle con uno sniffing tradizionale.

Vi sono diversi alternative ai programmi elencati sopra: OpenSSH può sostituire telnet, FTP e i Berkeley r-services, mentre per fornire un canale crittato al protocollo HTTP si può usare SSL.

5. Account superuser

L'account *root* è quello con maggiori privilegi in un sistema Unix. Non ha restrizioni di sicurezza, il che significa che può essere utilizzato per eseguire qualunque operazione sul sistema. Questo è L'ACCOUNT al quale un utente malintenzionato vuole accedere!

- Non permettete il login da remoto come root. Per ottenere un accesso root, l'utente deve usare il comando *su*. *Su* modifica l'effettivo uid dell'account in quello di un altro account, in questo caso in quello dell'account root.
- Se l'utente ha bisogno dei privilegi per alcuni comandi, si usa *sudo*. *Sudo* (superuser do) permette all'amministratore di sistema di assegnare a determinati utenti (o gruppi di utenti) la possibilità di eseguire alcuni (o tutti) comandi come root invece di consentire tutti i comandi ed opzioni. In questo caso, l'utente non deve inserire la password di root.
- L'uso dell'account root dovrebbe essere limitato alla configurazione del sistema, alle

applicazioni per l'installazione, a configurazioni specifiche o a situazioni di emergenza.
- Limitate l'accesso alle password di root. Queste dovrebbero essere conosciute solo a coloro che hanno compiti di amministratore del sistema.

Ulteriori informazioni su *Sudo* sono disponibili presso http://www.courtesan.com/sudo/, mentre le informazioni su *Su* si possono ottenere digitando *man su* al prompt dei comandi.

6. Account generici

Gli account generici sono spesso usati in fase di sviluppo per permettere ad un'applicazione di comunicare con un'altra o con un database. Un'altra situazione in cui sono usati degli account generici è quando si da accesso a fornitori. È importante fare molta attenzione nella gestione di questi account perché sia mantenuta la responsabilità di ciascuna operazione effettuata.

In generale

- Per prima cosa, usate account generici come ultima risorsa. Se un utente ha bisogno di un accesso frequente o prolungato, dovrebbe essergli assegnato un account specifico.
- Laddove fossero necessari account generici (molti individui diversi che hanno bisogno di un accesso come fornitori, applicazioni che necessitano di un accesso autenticato, ecc.), una persona autorizzata deve essere responsabile per tutte le azioni eseguite con tale account.

Account applicativi

Non scrivete le password nel codice delle applicazioni.
Garantite un'adeguata protezione delle informazioni riguardanti l'account e la password (file cifrati, permessi di lettura, ecc.)

Accesso a fornitori

- Richiedete una accettazione firmata di un support account agreement quando il fornitore accetta la responsabilità delle azioni effettuate con l'account.
- Nominate un responsabile della custodia delle password dei fornitori che gestisca questa categoria di password
- Conservate in una busta la password degli account di supporto e richiedi che il fornitore telefoni prima di aprirgli l'accesso.
- Usate, quando possibile, una autenticazione a due fattori.
- Fate in modo che il custode delle password dei fornitori modifichi le password degli account di supporto dopo il loro utilizzo, quando possibile o necessario. Questa fase non è strettamente necessaria se si sa una autenticazione a due fattori.
- Controllate che le buste che custodiscono le password non siano state manomesse.
- Effettuate controlli periodici dell'attività.

7. Traccia di controllo

Tenere una traccia di controllo dell'attività dell'utente è una parte essenziale della sicurezza di un sistema. Fare il log di tutti i tentativi di autenticazione e se hanno avuto o meno successo aiuta a capire cosa sta succedendo sul sistema. È essenziale anche il log specifico dell'attività *su* e *sudo*, poiché mostra chi ha cercato di effettuare operazione

con permessi diversi da quelli propri.

La verifica frequente delle tracce di controllo può portare alla scoperta di potenziali abusi di privilegi o di attività anomala di altro genere sul sistema.

Per maggiori informazioni su tutti gli aspetti del logging, potete andare su http://www.loganalysis.org/

torna all'inizio ^

U4 Sistemi di controllo delle versioni

U4.1 Descrizione

I sistemi di controllo delle versioni forniscono strumenti per la gestione di diverse versioni di documenti o codice sorgente e permettono a persone diverse di lavorare contemporaneamente sullo stesso gruppo di file. Questi sistemi sono indispensabili nella gestione di qualsiasi progetto di sviluppo software o di documenti legali e aziendali, in quanto forniscono non solo una soluzione di archiviazione centralizzata, ma di risalire con facilità alle differenti versioni.

Concurrent Versions System (CVS) è il più popolare sistema di controllo del codice sorgente tra quelli attualmente utilizzati in ambienti Linux/Unix. Molti progetto open-source permettono un accesso "anonimo" agli archivi CVS. Un archivio CVS può essere configurato per l'accesso remoto tramite il protocollo "pserver", che per default opera sulla porta 2401/tcp. Un server configurato in questo modo presenta le seguenti vulnerabilità:

A) Un buffer overflow nell'area di memoria *heap* che può essere attivato da "Entry-Lines" opportunamente configurate. Un aggressore può sfruttare il buffer overflow per eseguire codice abusivo sul server CVS. Il codice dell'exploit per i server CVS con piattaforme Linux, FreeBSD e Solaris è stato spedito alle mailing list di sicurezza. È importante quindi rendersi conto che qualsiasi archivio configurati per l'"accesso anonimo" è potenzialmente vulnerabile.
B) Un aggressore autenticato può sfruttare le vulnerabilità insite nell'esecuzione di altri comandi e funzioni per provocare una interruzione del servizio al server CVS o per eseguire codice abusivo sul server CVS. Alcune di queste falle possono essere anche sfruttate con utente "anonimi".

Un altro sistema di controllo delle versioni per Linux che sta guadagnando popolarità è Subversion. Il progetto era iniziato con l'intento di creare un sistema migliore rispetto a CVS. Si può accedere ad un archivio di Subversion tramite il protocollo "svn", se l'archivio esegue "svnserve". Il server svn opera per default sulla porta 3690/tcp. Questo server presenta le seguenti vulnerabilità:

- Un buffer overflow nell'area di memoria *heap* che se sfruttato da un aggressore può permettere l'esecuzione di codice abusivo.
- Un overflow dello stack che può essere attivato da uno speciale comando svn "get-dated-rev". Se il server è configurato per l'accesso anonimo, un aggressore non autenticato può sfruttarlo per eseguire codice abusivo sul server. Diversi exploit di questa falla sono stati pubblicati su Internet.

Se un aggressore ottiene l'accesso, potrebbe non solo infettare i file sorgenti con backdoor o bug che, quando il software è stato sviluppato, comporterebbero un alto numero di sistemi compromesso, ma potrebbe anche far incriminare un leale impiegato per attività illecite tramite un furto di identità.

U4.2 Sistemi operativi interessati
Linux, FreeBSD, AIX, HP-UX, Solaris, SGI e potenzialmente qualsiasi sistema che supporti CVS e/o Subversion.

U4.3 Riferimenti CVE/CAN
CAN-2004-0396, CAN-2004-0414, CAN-2004-0416, CAN-2004-0417, CAN-2004-0418, CAN-2004-0397, CAN-2004-0413

U4.4 Come stabilire se si è vulnerabili
Se il server CVS è configurato per l'accesso remoto tramite il protocollo "pserver" e si utilizza una delle seguenti versioni del software CVS, allora il server CVS è vulnerabile -
CVS stable release versione 1.11.16 e precedenti
CVS feature release versione 1.12.8 e precedenti.
La versione di CVS può essere verificata eseguendo il comando "cvs ver".

Se il server Subversion è configurato per l'accesso remoto tramite il protocollo "svn" e si utilizza una versione precedente alla 1.0.5, il server è vulnerabile.

U4.5 Come proteggersi

Per server CVS:
- Controllando che il software CVS sia aggiornato al più recente livello di patch. Il codice sorgente per il software più recente può essere scaricato da: https://www.cvshome.org/ .
- Configurando il server CVS perchè utilizzi il protocollo SSH per l'accesso remoto invece di pserver. Inoltre, eseguendo il server CVS server in un ambiente "chroot". Instruzioni dettagliate sono disponibili all'indirizzo: http://www.netsys.com/library/papers/chrooted-ssh-cvs-server.txt
- Se l'archivio CVS è utilizzato solo all'interno della rete aziendale, bloccando la porta 2401/tcp al perimetro di rete.
- Controllando che gli exploits pubblicati non siano efficaci sul server CVS. Gli exploits pubblici si possono trovare presso: http://www.k-otik.com/exploits/05212004.CVS_Linux.c.php http://www.k-otik.com/exploits/05212004.CVS_Solaris.c.php.
- Ospitando il server CVS per l'accesso annimo in sola lettura su un sistema stand-alone, come ad esempio nella DMZ.

Per server Subversion:
- Controllando che il server Subversion sia aggiornato alla più recente versione del software. L'ultima versione si può scaricare da: http://subversion.tigris.org
- Configurando gli archivi Subversion per l'accesso via webDAV invece che usando il protocollo "svn".
- Se l'archivio Subversion è utilizzato solo all'interno della rete aziendale, bloccando la porta 3690/tcp al perimetro di rete.
- Controllando che gli exploits pubblicati non siano efficaci sul server Subversion. Gli exploits pubblici si possono trovare presso: http://www.metasploit.com/projects/Framework/modules/exploits/svnserve_date.pm http://www.k-otik.com/exploits/06112004.subexp.c.php.
- Ospitando il server Subversion per l'accesso annimo in sola lettura su un sistema

stand-alone, come ad esempio nella DMZ.

U4.6 Riferimenti

CERT Advisory
http://www.kb.cert.org/vuls/id/192038

BID SecurityFocus
http://www.securityfocus.com/bid/10384
http://www.securityfocus.com/bid/10499
http://www.securityfocus.com/bid/10386
http://www.securityfocus.com/bid/10519

Homepage CVS
http://www.cvshome.org

Homepage Subversion
http://subversion.tigris.org

Messaggi nelle Security List
http://www.securityfocus.com/archive/1/363775/2004-05-17/2004-05-23/0
http://www.securityfocus.com/archive/1/365541/2004-06-07/2004-06-13/0
http://www.securityfocus.com/archive/1/363781/2004-05-17/2004-05-23/0
http://archives.neohapsis.com/archives/bugtraq/2004-06/0180.html

torna all'inizio ^

U5 Servizi di posta

U5.1 Descrizione

L'e-mail è una tra le applicazioni usate più diffusamente in Internet, così come SMTP è uno dei protocolli più vecchi. I Mail Transport Agent (MTA) sono i server delegati a consegnare la posta dal mittente verso il destinatario o i destinatari previsti, di solito tramite il protocollo SMTP, che può esser crittato con SSL verso porte considerate insicure mediante TSL, se entrambe le parti lo supportano. Sendmail è l'MTA più comunemente usato in ambito Unix, anche se negli anni la raffica di problemi legati alla sicurezza e la complessità nel configurare questo venerabile pezzo di software ha lasciato spazio a svariate e popolari alternative quali Qmail, Courier-MTA, Postfix ed Exim.

Non sorprende dunque che, dato l'ampio uso della posta elettronica, questi sistemi siano costantemente soggetti ad attacchi da parte di virus, worm e aggressori umani. Se molti di questi attacchi si concentrano sui client di posta più comunemente usati, è da rilevare anche come spesso anche gli MTA siano vettori d'attacco. La maggior parte delle vulnerabilità su cui si fa leva per agire contro questi server possono essere raccolte nelle seguenti categorie:

- Attacchi portati contro sistemi non corretti, come buffer overrun, heap overflow, ecc
- Abuso di open relay, lo strumento preferito degli spammer
- Sfruttamento di altre carenze nelle configurazioni al di là del discorso relay, come database degli account degli utenti, per propiziare spam o attacchi di social engineering (o anche attacchi verso i client e-mail).

Si può esser certi che se una qualche vulnerabilità legata agli MTA è presente in rete, verrà

rilevata e sfruttata quasi immediatamente. Fortunatamente si possono drasticamente ridurre questi rischi al solo sistema di e-mail adottando dei semplici accorgimenti in fase d'installazione e seguendo delle regole base per le attività di manutenzione. Quegli MTA che seguono in modo rigido le disposizioni contenute nei relativi RFC sono predisposti in modo migliore, e la maggior parte del software usato dallo spam non lo fa.

U5.2 Sistemi operativi interessati

Quasi tutte le principali distribuzioni di Unix vengono fornite con uno degli MTA indicati in precedenza, integrato nel sistema. Se da un lato molti fornitori di Unix hanno certamente migliorato negli anni recenti le caratteristiche di sicurezza delle installazioni di default, si dovrebbe comunque assumere che qualunque sistema avente un MTA che non sia stato aggiornato o soggetto a manutenzione o che operi con una configurazione preimpostata sia vulnerabile.

U5.3 Riferimenti CVE/CAN

Sendmail

CVE-1999-0047, CVE-1999-0095, CVE-1999-0096, CVE-1999-0129, CVE-1999-0131, CVE-1999-0203, CVE-1999-0204, CVE-1999-0206, CVE-1999-1109, CVE-2000-0319, CVE-2001-0653, CVE-2001-1349, CVE-2002-0906

CAN-1999-0098, CAN-1999-0163, CAN-2001-0713, CAN-2001-0714, CAN-2001-0715, CAN-2002-1165, CAN-2002-1278, CAN-2002-1337, CAN-2003-0161, CAN-2003-0285, CAN-2003-0694

Qmail

CVE-2000-0990,

CAN-2003-0654

Courier-MTA

CVE-2002-0914, CVE-2002-1311, CVE-2003-0040, CVE-2004-0224, CVE-2004-0777

Exim

CVE-2001-0889

CAN-2003-0743,CAN-2004-0399, CAN-2004-0400

Postfix

CAN-2003-0468

U5.4 Come stabilire se si è vulnerabili

Controllando il livello di patch

Per determinare se il sistema sia vulnerabile la prima cosa da fare è verificare il livello di patch applicate all'MTA e verificare se esistano o meno vulnerabilità per la revisione in uso. Si può verificare se vi siano vulnerabilità associate al proprio MTA controllando nel CVE (http://cve.mitre.org/).

Sendmail

Per Sendmail sono state riscontrate in passato un gran numero di vulnerabilità. Queste vulnerabilità sono spesso dovute alla sua complessità. Esse hanno reso Sendmail uno dei

servizi maggiormente violati in Internet.

Qualunque versione del software non aggiornata o non corretta è potenzialmente vulnerabile.

Per determinare qual è la versione in uso di Sendmail, utilizzate il seguente comando:
echo \$Z | sendmail –bt –d.

Non fidatevi della version string che si ottiene in risposta dal daemon, poiché essa viene soltanto letta da un file di testo presente sul sistema che potrebbe non essere stato aggiornato adeguatamente.

Per determinare se la versione in uso è quella corrente, controllate all'indirizzo:
http://www.sendmail.org/current-release.html

Exim

Exim è un altro MTA d'uso comune dotato di molte funzioni. Ha avuto in passato alcune vulnerabilità.

Per determinare la versione in uso di Exim il comando è:
exim –bV

Per determinare se la versione in uso è quella corrente, controllate all'indirizzo:
http://www.exim.org/version.html

Qmail

Qmail è un MTA sicuro che ha avuto alcune vulnerabilità in passato. È anche uno tra gli MTA più popolari, dopo Sendmail.

Non c'è un modo semplice ed efficace per determinare quale versione di Qmail sia in uso se non quella di verificare nelle pagine di man usando il comando GNU grep:

```
grep -A1 version /var/qmail/man/man7/qmail.7
```

Qmail dispone di molte migliori apportate dagli utenti che possono rendere l'identificazione di potenziali vulnerabilità un compito piuttosto complesso.

Si possono rintracciare le patch raccomandate presso:
http://www.qmail.org/top.html#patches e si può trovare un package (chiamato netqmail) contenente qmail e le patch raccomandate, a questo indirizzo: http://qmail.org/netqmail/

Courier-MTA

Courier-MTA è un sistema mail server che aderisce in modo rigido agli RFC e che supporta Maildir+, maildrop e MySQL, Postgresql e LDAP per l'archiviazione degli account degli utenti e degli alias.

Per identificarne la versione, usate il comando "showmodules".

Per informazioni relative alla sicurezza e per scoprire l'ultima versione l'indirizzo è
http://www.courier-mta.org

Postfix

Al pari di Qmail, Postfix è un MTA sicuro ed ha avuto in passato un numero ancora inferiore di vulnerabilità. Le versioni recenti hanno migliorato le funzioni per il controllo d'accesso, l'ispezione dei contenuti e il rate limiting, tanto che l'aggiornamento alla versione più recente rappresenta sempre una buona idea anche se si dispone di una versione considerata non vulnerabile.

Per determinare la versione di Postifx in uso, il comando è:
postconf –d mail_version

Per verificare se la versione in uso è quella corrente, si veda qual è l'ultima rilasciata al sito:
ftp://ftp.porcupine.org/mirrors/postfix-release/index.html

- **Controllate il relay status**

Cos'è un open relay
Il relaying della posta è una funzione base di un MTA, ma configurazioni non corrette possono far diventare il proprio MTA un open relay. Ciò avviene quando un MTA ritrasmette un messaggio di posta nei casi in cui né il destinatario né il mittente sono utenti locali. In altri termini, il destinatario ed il mittente non fanno parte del dominio e l'MTA non ha alcuna relazione con la comunicazione. In circostanze normali, l'e-mail non avrebbe alcun motivo per passare tramite tale MTA.

Come verificare se il proprio MTA è un open relay
Verificare che il proprio MTA non sia un open relay è una delle cose più importanti dopo che si sono applicate le opportune correzioni alla versione installata. Ciò darà modo di determinare se sia possibile che qualcuno usi l'MTA per inviare della posta indesiderata (SPAM). Gli strumenti seguenti aiutano a compiere questa operazione:
http://www.abuse.net/relay.html
http://www.cymru.com/Documents/auditing-with-expect.html

Cos'è una Realtime Blackhole List?
Una Real-time Blackhole List (RBL) è una lista di indirizzi IP di server i cui responsabili rifiutano di bloccare la proliferazione di spam in Internet. Queste liste sono utilizzate dagli amministratori di mail al fine di rifiutare connessioni al proprio MTA provenienti da qualcuno di questi spammer noti.

Come verificare che il proprio server non sia inserito in una RBL
Se ci si accorge che il proprio server è incluso in una di queste liste, vi sono possibilità ragionevoli che questo sia un open relay, a meno che non si abbia modificato di recente la configurazione. Può anche accadere che uno degli utenti abilitati abusi del server per inviare spam o newsletter. Ciò può comportare che il server finisca in una RBL. Potete controllare a questi indirizzi se l'IP del vostro server è compreso nelle liste:
http://www.mail-abuse.com/support/lookup.html
http://www.ordb.org/

Si tenga conto che vi sono molte RBL e quindi tale ricerca va estesa almeno a quelle più popolari.

- **Esaminare il mail server**

Esaminare il mail server vi permetterà di identificare vulnerabilità che potrebbero essere sfruttate da malintenzionati per eseguire azioni non autorizzate sul/con il mail server.

Nessus
Nessus è un vulnerability scanner remoto potente e gratuito che include uno specifico plugin per server SMTP. Permette di identificare eventuali vulnerabilità dell'MTA in modo rapido ed efficace.

Si può trovare Nessus e i suoi plugin all'indirizzo http://www.nessus.org

SARA
Sara è l'acronimo di Security Auditor's Research Assistant. Si tratta di uno strumento di analisi della sicurezza che include le vulnerabilità elencate nella Top 20 SANS tra quelle ricercate.

SARA è disponibile presso http://www-arc.com/sara/

U5.5 Come proteggersi
Le istruzioni che seguono sono quelle da tener presenti per la protezione dei mail server e sono suddivise in due sezioni: raccomandazioni generali, valide a prescindere dalla tipologia di server, e raccomandazioni specifiche per i mail server Sendmail, Qmail e Postfix:

1.Raccomandazioni generali

- Decidete se avete realmente bisogno di utilizzare un MTA e se questo debba avere un affaccio pubblico.
- Disabilitate il Mail Server su qualsiasi sistema non specificamente dedicato e autorizzato ad essere un server di posta. Si dovrebbe anche adottare delle procedure per prevenire la possibilità che I mail server vengano anche erroneamente ri-abilitati. Agite sulle policy del firewall per rafforzare tali disposizioni.
- Applicate tutte le patch fornite dal produttore o aggiornate il vostro Mail Server alla versione più recente.
- Adottate un MTA interno separato per gestire il traffico di posta interna.
- Limitate il livello di privilegi con i quali viene eseguito l'MTA o, se possibile, farlo funzionare in una jail chrooted.
- Leggete tutta la documentazione relativa ai mail server ed iscrivetevi alle corrispondenti mailing list, se disponibili.

Proteggersi dal mail relaying

Per evitare che il Mail Server venga usato indebitamente dagli spammer, questo deve essere configurato per non permettere il relay della posta di reti o domini non riconosciuti come affidabili:

Sendmail
Se dovete utilizzare Sendmail in modalità daemon, assicuratevi che la vostra configurazione sia progettata per inviare correttamente la posta e solo per i sistemi sotto il vostro controllo. Consultate http://www.sendmail.org/tips/relaying.html e http://www.sendmail.org/m4/anti_spam.html per i consigli su come effettuare una corretta configurazione del vostro server. A partire dalla versione 8.9.0 di Sendmail, la funzione di open relay è disabilitata per default. Molti produttori di sistemi operativi, però, la ri-abilitano nelle loro configurazioni di default. Se state utilizzando la versione di Sendmail che vi è

arrivata con il vostro sistema operativo, controllate con molta attenzione che il vostro server non sia utilizzabile come relay.

Qmail
Qmail offre una buona documentazione riguardo il relaying selettivo e su come disabilitare il relaying nel sistema. Consultate http://www.lifewithqmail.org/lwq.html#relaying

Courier-MTA
Closed-relay per sua natura, Courier fornisce istruzioni su come abilitare il relay per determinate reti o indirizzi Ip. In più, Courier usa l'autenticazione SMTP Authentication per fornire il relaying.
Http://www.courier-mta.org – sezione FAQ.

Exim
Anche Exim ha istruzioni dettagliate su come prevenire il relaying.
http://www.exim.org/howto/relay.html

Postfix
Per quanto riguarda Postfix, vi sono alcune operazioni che aiutano a limitare l'accesso e a controllare il relay. Solo gli host e le reti elencate nel parametro 'mynetworks' saranno abilitate al relay. Consultate http://www.postfix.org/SMTPD_ACCESS_README.html

2. Altri dettagli specifici delle singole applicazioni

A) Informazioni aggiuntive su come configurare ed eseguire Sendmail in modo più sicuro sono disponibili su:
http://www.sendmail.org/secure-install.html
http://www.sendmail.org/m4/security_notes.html
http://www.sendmail.org/~gshapiro/security.pdf

B) Per evitare che un sistema Postfix compromesso metta in pericolo l'intero sistema, limitatelo in modo che venga eseguito con un utente con privilegi limitati in una directory chroot()ed. Per la configurazione di Postfix, si veda
http://www.linuxjournal.com/article.php?sid=4241
C) Il seguente collegamento porta a un esempio su come configurare l'MTA per usare il blackholing http://www.ordb.org/faq/#usage
D) Courier-MTA supporto nativamente le liste RBL e fornisce una lista iniziale di rbl-server nel file di configurazione esmtpd.
E) Postfix contiene molte funzioni per limitare l'UCE, su cui si possono trovare informazioni all'indirizzo:
http://www.securitysage.com/antispam/intro.html

torna all'inizio ^

U6 Simple Network Management Protocol (SNMP)

U6.1 Descrizione

Il Simple Network Management Protocol (SNMP) è largamente utilizzato per controllare e configurare da remoto quasi tutti i tipi di dispositivi TCP/IP moderni. Anche se SNMP è supportato nelle sue varie distribuzioni da quasi tutte le piattaforme di rete, è usato più di frequente come metodo per configurare e gestire dispositivi quali stampanti, router e switch e per inviare input a servizi di monitoraggio della rete.

La comunicazione Simple Network Management consiste in diversi tipi di messaggi scambiati tra le stazioni di gestione SNMP e i dispositivi di rete che eseguono quello che comunemente è definito come agent software. Sia metodologia con la quale questi messaggi sono trattati, sia il meccanismo di autenticazione che sottende a tale trattamento, presentano significative vulnerabilità.

Le vulnerabilità che stanno dietro il metodo attraverso il quale la versione 1 di SNMP tratta e cattura i messaggi è descritta in dettaglio nel CERT Advisory CA-2002-03. Esistono una serie di vulnerabilità nel modo in cui i messaggi di richiesta e cattura sono gestiti e decodificati dalle stazioni di gestione e dagli agenti.

Queste vulnerabilità non sono limitate a una specifica implementazione di SNMP, ma affliggono una varietà di distribuzioni di SNMP di diversi produttori. Sfruttando queste vulnerabilità gli aggressori possono arrivare a risultati che variano dal denial of service alla modifica della configurazione e del sistema di gestione delle macchine abilitate all'SNMP.

Il meccanismo interno di autenticazione dei protocolli SNMP meno recenti presenta anche un'altra importante vulnerabilità. Le versioni 1 e 2 di SNMP utilizzano un meccanismo di autenticazione "community string" non crittata. La mancanza di crittografia è già abbastanza grave, ma in più la community string usata per default nella grande maggioranza dei dispositivi SNMP è "public," e solo pochi produttori più accorti di apparati di rete la modificano in "private" per il trattamento delle informazioni più sensibili. Gli aggressori possono sfruttare la vulnerabilità di SNMP per riconfigurare o per spegnere i dispositivi da remoto. Lo sniffing del traffico SNMP può rivelare molti dettagli relativi alla struttura della vostra rete e ai dispositivi ad essa collegati Gli intrusi utilizzano queste informazioni per scegliere gli obiettivi e per pianificare gli attacchi.

Molti produttori abilitano per default la versione 1 di SNMP e molti non offrono prodotti in grado di utilizzare SNMP versione 3, che possono essere configurati per utilizzare metodi di autenticazione migliori. In ogni caso esistono dei sostituti gratuiti che provvedono a fornire il supporto SNMPv3 con licenza GPL o BSD.

SNMP non è un'esclusiva di UNIX e viene usato diffusamente anche in Windows, access point e ponti wireless, stampanti e altri servizi interni. La maggior parte degli attacchi che si appoggiano a SNMP finora riscontrati si è presentata però su sistemi UNIX con configurazioni non corrette. Il traffico SNMP viene trasmesso in chiaro, per cui bisogna fare attenzione al suo utilizzo nei casi in cui il traffico può essere intercettato.

Per far capire meglio le problematiche delle vulnerabilità SNMP, il CERT CC ha sviluppato una serie esaustiva di FAQ su SNMP, disponibili all'indirizzo http://www.cert.org/tech_tips/snmp_faq.html.

U6.2 Sistemi operativi interessati

Quasi tutti i sistemi UNIX e Linux sono distribuiti con l'SNMP installato e spesso abilitato per default. Anche la maggior parte degli altri sistemi operativi e dispositivi compatibili con SNMP sono vulnerabili.

U6.3 Riferimenti CVE/CAN

CVE-1999-0294, CVE-1999-0472, CVE-1999-0815, CVE-1999-1335, CVE-2000-0221, CVE-2000-0379, CVE-2000-0515, CVE-2000-1058, CVE-2001-0236, CVE-2001-0487, CVE-2001-0514, CVE-2001-0564, CVE-2001-0888, CVE-2002-0017, CVE-2002-0069,

CVE-2002-0302,

CAN-1999-0186, CAN-1999-0254, CAN-1999-0499, CAN-1999-0516, CAN-1999-0517, CAN-1999-0615, CAN-1999-0792, CAN-1999-1042, CAN-1999-1126, CAN-1999-1245, CAN-1999-1460, CAN-1999-1513, CAN-2000-0147, CAN-2000-0885, CAN-2000-0955, CAN-2000-1157, CAN-2000-1192, CAN-2001-0046, CAN-2001-0352, CAN-2001-0380, CAN-2001-0470, CAN-2001-0552, CAN-2001-0566, CAN-2001-0711, CAN-2001-0840, CAN-2001-1210, CAN-2001-1220, CAN-2001-1221, CAN-2001-1262, CAN-2002-0012, CAN-2002-0013, CAN-2002-0053, CAN-2002-0109, CAN-2002-0305, CAN-2002-0478, CAN-2002-0540, CAN-2002-0812, CAN-2002-1048, CAN-2002-1170, CAN-2002-1408, CAN-2002-1426, CAN-2002-1448, CAN-2002-1555, CAN-2003-0137, CAN-2003-0935, CAN-2003-1002, CAN-2004-0311, CAN-2004-0312, CAN-2004-0576, CAN-2004-0616, CAN-2004-0635, CAN-2004-0714

U6.4 Come stabilire se si è vulnerabili

Potete verificare se SNMP è attivo sui dispositivi connessi alla vostra rete adoperando uno scanner o effettuando un controllo manuale.

- SNMPing – Recuperate lo strumento di scanning gratuito SNMPing dal SANS Institute all'indirizzo http://www.sans.org/alerts/snmp/.
- Foundstone ha creato un altro strumento per lo scanning SNMP di semplice uso chiamato SNScan, che può essere scaricato da http://www.foundstone.com/knowledge/free_tools.html.
- Nessus – Uno scanner open source per il security assessment, recuperabile da http://www.nessus.org

Se non potete utilizzare uno degli strumenti sopra citati, avete la possibilità di verificare manualmente se SNMP è attivo sui vostro sistemi. Consultate la documentazione del vostro sistema operativo per le indicazioni su come identificare l'implementazione specifica di SNMP, di solito il daemon di base può essere identificato ricercando "snmp" nella process list o cercando tra i servizi che girano sulle porte 161 o 162. (Lo strumento lsof può rivelarsi utile per stabilire le porte da trattare).

Una istanza SNMP attiva è probabilmente una prova sufficiente che siete vulnerabili alla cattura estesa o a errori nella gestione delle richieste. Consultate il CERT Advisory CA-2002-03 per ulteriori informazioni.

Se SNMP è attivo e riscontrate una delle seguenti variabili, potreste soffrire di una vulnerabilità legata a una stringa di default o comunque troppo facile da indovinare:
1. Community name SNMP vuoti o di default.
2. Community name SNMP facili da indovinare.
3. Community string SNMP nascoste.

Leggete http://www.sans.org/resources/idfaq/snmp.php per informazioni su come identificare la presenza di queste condizioni.

U6.5 Come proteggersi

Vulnerabilità di cattura e gestione della richiesta:
1. Se non avete necessità assoluta di utilizzare l'SNMP, disabilitatelo.
2. Quando possibile, utilizzate il modello di sicurezza basato sull'utente SNMPv3 con messaggio di autenticazione e possibilmente con la crittografia del protocol data unit.
3. Se dovete usare SNMPv1 o v2, controllate di aver installato la patch più recente rilasciata dal vostro produttore. Un buon punto di partenza per ottenere le informazioni specifiche per ciascun produttore è consultare l'Appendice A del CERT Advisory CA-2002-03.

4. Filtrate SNMP (porte 161 TCP/UDP e 162 TCP/UDP) ai punti di ingresso delle vostre reti, a meno che non sia assolutamente necessario effettuare il polling o gestire i dispositivi dall'esterno della rete locale.
5. Sui sistemi con gli agenti SNMP effettuate un controllo degli accessi basato sugli host. Anche se questa possibilità dipende dalle funzionalità del sistema che ospita gli agenti SNMP, è possibile effettuare comunque un controllo per verificare da quali sistemi i vostri agenti accettano richieste. Sulla maggior parte dei sistemi UNIX è possibile effettuare questo controllo configurando TCP-Wrappers o Xinetd. Potete anche usare un firewall che effettui il packet filtering sugli agenti per bloccare le richieste SNMP indesiderate.

Vulnerabilità correlate alle stringhe di default o troppo semplici da indovinare:
1. Se non avete necessità assoluta di utilizzare l'SNMP, disabilitatelo.
2. Quando possibile, utilizzate il modello di sicurezza basato sull'utente SNMPv3 con messaggio di autenticazione e possibilmente con la crittografia del protocol data unit.
3. Se dovete usare SNMPv1 o v2, utilizzate per i community name la stessa policy che usate per le password. Assicuratevi che siano difficili da indovinare o da violare e che siamo periodicamente modificati.
4. Controllate e convalidate i community name utilizzando snmpwalk. Potete trovare maggiori informazioni su http://www.zend.com/manual/function.snmpwalk.php. Una buona guida per questo strumento è reperibile all'indirizzo http://www.sans.org/resources/idfaq/snmp.php.
5. Filtrate SNMP (porte 161 TCP/UDP e 162 TCP/UDP) ai punti di ingresso delle vostre reti, a meno che non sia assolutamente necessario effettuare il polling o gestire i dispositivi dall'esterno della rete locale. In questo caso, se possibile, configurate il filtering in modo da permettere il traffico SNMP solo tra sottoreti affidabili.
6. Dove possibile, impostate le MIB in sola lettura. Potete trovare maggiori informazioni sull'argomento all'indirizzo http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/snmp.htm#xtocid210315

torna all'inizio ^

U7 Open Secure Sockets Layer (SSL)

U7.1 Descrizione

La libreria open-source OpenSSL fornisce supporto crittografico alle applicazioni che comunicano attraverso la rete. Si tratta di un'implementazione del protocollo SSL/TLS molto diffusa ed utilizzata da un gran numero di produttori. L'esempio meglio conosciuto di applicazione che usa questa libreria è il web server Apache (per supportare le connessioni http sicure). Anche molti dei server POP3, IMAP, SMTP e LDAP tra quelli più utilizzati possiedono un componente basato su OpenSSL.

Siccome la libreria OpenSSL è integrata con diverse applicazioni, qualsiasi vulnerabilità della libreria può essere sfruttata tramite queste applicazioni. Vi sono ad esempio molti exploit pubblicamente disponibili che possono colpire I server Apache compilati con certe versioni della libreria. Gli stessi exploit possono essere facilmente adattati per colpire sendmail, openLDAP, CUPS o alter applicazioni che integrano OpenSSL.

Nella libreria OpenSSL sono state scoperte molte vulnerabilità. Le più gravi sono costituite da una serie di 5 vulnerabilità elencate in CAN-2002-0655, CAN-2002-0656, CAN-2002-0557, CAN-2002-0659 e CAN-2003-0545. Queste vulnerabilità possono essere sfruttate da remoto per eseguire codice abusivo con il livello di privilegi delle applicazioni che usano la libreria OpenSSL. In alcuni casi, come per 'sendmail', un attacco riuscito può conferire privilegi di "root".

U7.2 Sistemi operative interessati
Qualsiasi sistema UNIX o LINUX che presenta le versioni di OpenSSL (a) 0.9.7c o precedenti (b) 0.9.6l o precedenti, è vulnerabile. Questo problema può riguardare pacchetti Linux come Apache, CUPS, Curl, OpenLDAP, Stunnel, Sendmail e qualsiasi altra applicazione che integra OpenSSL.

U7.3 Riferimenti CVE/CAN
CVE-1999-0428, CVE-2001-1141,

CAN-2000-0535, CAN-2002-0655, CAN-2002-0656, CAN-2002-0557, CAN-2002-0659, CAN-2003-0078, CAN-2003-0131, CAN-2003-0147, CAN-2003-0543, CAN-2003-0544, CAN-2003-0545, CAN-2003-0851, CAN-2004-0079, CAN-2004-0081, CAN-2004-0112, CAN-2004-0607

U7.4 Come stabilire se è vulnerabili
Verificate il risultato del commando 'openssl version'. Se la versione non è 0.9.7d o 0.9.6m, il sistema è vulnerabile.

U7.5 Come proteggersi

1. Aggiornate il sistema alla versione più recente di OpenSSL. Se OpenSSL è preinstallato nel sistema operativo, applicate le patch più recenti fornite dal produttore. Notate che in alcuni casi l'aggiornamento delle librerie comporta una ri-compilazione e/o un ri-collegamento delle applicazioni.

2. Se possibile, usate ipfilter / netfilter o altri strumenti firewall per limitare I sistemi che si connettono ad un server abilitato OpenSSL. Tenete presente che uno degli utilizzi più comuni di OpenSSL è quello di rendere sicuro il traffico HTTP sulla Internet pubblica nel commercio elettronico, nel qual caso limitare l'acceso ad alcuni host probabilmente non è un'operazione attuabile.

torna all'inizio ^

U8 Configurazioni non corrette dei servizi NIS/NFS
U8.1 Descrizione
Il Network File System (NFS) e il Network Information Service (NIS) sono due importanti servizi frequentemente attivati su server / reti UNIX. NFS è un servizio creato originariamente da Sun Microsystems, progettato per condividere ("esportare") file system / directory e file attraverso una rete tra sistemi UNIX. Parallelamente, Anche NIS è un set di servizi che lavora come un database che fornisce informazioni di localizzazione, chiamate map, ad altri servizi di rete come NFS. Le map più comuni sono collegate i file passwd e group usati, da quel momento, per l'autenticazione centralizzata. NIS ha a che fare spesso anche con il file host.

I problemi di sicurezza di entrambi i servizi, rappresentati dalle continue vulnerabilità scoperte nel corso degli anni (buffer overflow, DoS e autenticazione debole), fanno in modo che questi servizi siano obiettivo di frequenti attacchi.

Oltre al fatto che persistono molti servizi a cui non sono state applicate tutte le patch, il rischio più alto è rappresentato da configurazioni non corrette di NFS e NIS che aprono falle di sicurezza che possono essere sfruttate e attaccate da utenti locali o remoti.

L'autenticazione debole offerta da NIS nell'interrogazione delle map NIS permette agli utenti di usare applicazioni come ypcat o getent che possono visualizzare i valori del database NIS database, o le map, e permettere di entrare in possesso del file della password. Lo stesso tipo di problemi si verificano con NFS che implicitamente accredita gli UID (user ID) e i GID (group ID) che il client NFS presenta al server e, a seconda della configurazione del server, può permettere all'utente il mount e l'esplorazione del file system remoto.

U8.2 Sistemi operativi interessati
Quasi tutti i sistemi Unix e Linux sono distribuiti con una versione di NFS e NIS installata e spesso abilitata per default. Nel caso di NFS, benché questo possa essere abilitato per default, il file exports è di solito vuoto (il file exports specifica quali directory sono condivise e come effettuano la condivisione).

U8.3 Riferimenti CVE/CAN

NFS
CVE-1999-0002, CVE-1999-0166, CVE-1999-0167, CVE-1999-0170, CVE-1999-0211, CVE-1999-0832, CVE-1999-1021, CVE-2000-0344, CVE-2002-0830

CAN-1999-0165, CAN-1999-0169, CAN-2000-0800, CAN-2002-0830, CAN-2002-1228, CAN-2003-0252, CAN-2003-0379, CAN-2003-0576, CAN-2003-0680, CAN-2003-0683, CAN-2003-0976, CAN-2004-0154

NIS
CVE-1999-0008, CVE-1999-0208, CVE-1999-0245, CVE-2000-1040

CAN-1999-0795, CAN-2002-1232, CAN-2003-0176, CAN-2003-0251

U8.4 Come stabilire se si è vulnerabili
I seguenti punti si riferiscono alle vulnerabilità del software NIS/NFS:

1. Verificate di essere al passo con le patch rilasciate dal vostro produttore. Nella maggior parte dei sistemi operativi il comando rpc.mountd -version per NFS e ypserv -version per NIS mostrerà la versione del software. Qualsiasi versione obsoleta o non aggiornata è da considerarsi vulnerabile.
2. Per quanto riguarda le vulnerabilità software, un approccio più completo sarebbe quello di utilizzare un vulnerability scanner aggiornato per verificare periodicamente che i vostri sistemi non contengano nuove vulnerabilità.

I seguenti punti si riferiscono alla configurazione di NIS:

1. Assicuratevi che la password di root non sia conservata in una map NIS.
2. Controllate che le password degli utenti siano in accordo con i criteri di sicurezza. Per portare a termine questo compito potete utilizzare un password cracker.
3. Se possibile, usate Blowfish o MD5 per l'hashing delle password invece di DES.

Nota importante: Non utilizzate mai un password cracker, neanche sui sistemi per i quali avete un accesso root, senza autorizzazione esplicita e preferibilmente scritta da parte del

vostro datore di lavoro. È già accaduto che amministratori di sistema con le migliori intenzioni siano stati licenziati per aver utilizzato strumenti per la determinazione delle password senza autorizzazione.

I seguenti punti si riferiscono alla configurazione di NFS:

1. Verificate se gli host, i gruppi di rete e i permessi di accesso nel file /etc/exports siano aggiornati.
2. Eseguite il comando *showmount -e IP_DEL-SERVER* per vedere cosa è stato esportato. Controllate se i vostri mount sono in accordo con la vostra security policy.

U8.5 Come proteggersi

I seguenti punti si riferiscono alla configurazione di NIS:

1. Potete specificare in ciascun client una lista dei server NIS a cui possono collegarsi, evitando così che altri sistemi si mascherino da server NIS.
2. Se fate file DBM, attivate la funzione YP_SECURE per assicurarvi che il server risponda ai client solo sulle porte che hanno i corretti privilegi. Ciò può essere realizzato usando lo switch “s” con il comando makedbm.
3. Inserite gli host e le reti affidabili in /var/yp/securenets usato dai processi ypserv e ypxfrd, e ricordatevi di riavviare i daemon perché le modifiche abbiano effetto.
4. Controllate sui vostri client NIS che nel password file ci sia il valore +:*:0:0:::.
5. Considerate la possibilità di usare NIS attraverso un protocollo sicuro come SSH. Un buon punto di partenza è http://www.math.ualberta.ca/imaging/snfs/.

Nota: Il Lightweight Directory Access Protocol (LDAP) sostituisce NIS in alcune configurazioni e tutte le versioni di Linux supportano LDAP come sorgente di diversi elementi dei name service come passwd, group, e host. Un buon manuale sull’amministrazione del sistema LDAP si rivelerà molto utile a questo scopo. Tenete presente che LDAP supporta naturalmente la cifratura SSL e la replicazione.

I seguenti punti si riferiscono alla configurazione di NFS:

1. Quando assegnate i client nel file /etc/exports file usate indirizzi IP numerici o domi a dominio completi invece di alias (dal file hosts o da una map hosts NIS).
2. Usate il file /etc/exports per limitare l’accesso al file system NFS aggiungendo i seguenti parametri:
    - Per evitare che i normali utenti possano eseguire mount su un file system NFS si aggiunge un parametro secure dopo l’indirizzo IP o il nome a dominio del vostro client NFS. (es.: /home 10.20.1.25(secure))
    - Esportare il file system NFS con i permessi appropriati. Per fare ciò aggiungete i permessi appropriati (ro per Read-only o rw for Read-Write) dopo l’indirizzo IP o il nome a dominio del vostro client NFS nel file /etc/exports (es. /home 10.20.1.25(ro))
    - Se possibile, usate il parametro root_squash dopo l’indirizzo IP o il nome a dominio del vostro client NFS. Se questo parametro è abilitato, il superuser ID root sul client NFS sarà sostituito nel server NFScon lo user ID nobody e con il group ID nogroup (possono essere modificati se ce n’è bisogno con i parametri "anonuid" e "anongid"). Ciò significa che l’utente root sul client non può più accedere o modificare file che solo root del server può accedere o modificare, evitando che il primo ottenga privilegi superuser sul server. (es: /home 10.20.1.25(root_squash)).
    - Se volete esportare una directory con permessi tipo-anonymous, usate il

parametro "all_squash", che mappa tutti gli user id e i group id negli ID anonuid e anongid.
- Una gamma completa di parametri è disponibile sulla pagina principale di /etc/exports "man exports". Oppure online all'indirizzo http://www.netadmintools.com/html/5exports.man.html

3. Per testare la configurazione potete usare uno strumento chiamato NFSBug. I test comprendono la ricerca dei file system esportati, la determinazione di come funzionano le restrizioni di esportazione, la verifica se si possa eseguire il mount dei file system attraverso il portmapper, il tentativo di indovinare i file handle e la verifica di diversi bug che possono comportare l'accesso ai file system. http://ftp.cerias.purdue.edu/pub/tools/unix/sysutils/nfsbug/

4. Su sistema operativo Solaris attivate la funzione di Port Monitoring, aggiungendo la linea set nfssrv:nfs_portmon = 1 sul file /etc/system.
I sistemi Linux negano per default la connessione a client NFS che usano porte che non hanno i corretti privilegi. (quelli oltre la 1024).

Considerazioni generali su NIS e NFS:

1. Controllate le policy del vostro firewall e assicuratevi che siano bloccate le porte non necessarie, come anche la porta 111 (Portmap) e la porta 2049 (Rpc.nfsd). Permettete l'accesso ai server NIS e NFS solo ai client autorizzati.. Un'altra possibile misura è quella di restringere l'accesso attraverso tcp_wrappers, disponibili su http://sunsite.cnlab-switch.ch/ftp/software/security/security-porcupine.org/.

   Nel vostro file /etc/hosts.allow indicate il servizio e gli IP autorizzati ad accedere al servizio (es. portmap: 10.20.0.0/16 per permettere alla rete privata di Classe-B 10.20.0.0 di accedere al servizio portmap). Dovreste inoltre includere nel file /etc/hosts.deny il servizio e gli IP che NON sono autorizzati ad accedere al servizio (es: portmap: ALL negherà l'accesso a tutti gli indirizzi IP non inclusi in /etc/hosts.allow). Portmap è un servizio per cui è importante bloccare gli accessi non necessari, poiché è uno dei servizi che opera tramite NFS.

2. Considerate la possibilità di usare NFS su un protocollo sicuro come SSH. Un buon punto di partenza è http://www.math.ualberta.ca/imaging/snfs/.

3. Applicate tutte le patch o gli aggiornamenti forniti dal vostro produttore per i server NIS e NFS. Per maggiori informazioni sull'hardening della vostra installazione UNIX, consultate la UNIX Security Checklist del CERT.

4. Disabilitate i daemon NFS e NIS su tutti i sistemi che non sono specificatamente designati ed autorizzati ad essere server NFS e/o NIS. Per fare in modo che questa modifica non sia capovolta, potrebbe essere saggio rimuovere del tutto dal sistema il software NFS e/o NIS.

torna all'inizio ^

U9 Database

U9.1 Descrizione

I Database sono una risorsa fondamentale dei sistemi di Commercio elettronico, dei sistemi

finanziari, bancari e di Enterprise Resource Planning (ERP) e contengono informazioni critiche di partner, clienti e dipendenti. Anche se altrettanto importanti per l'integrità e la riservatezza dei dati, i database management system (DBMS) di solito non sono soggetti allo stesso livello di attenzione per la sicurezza dei sistemi operativi e delle reti. I Database management system sono raccolte di programmi che permettono l'archiviazione, la modifica e l'estrazione di informazioni dai database.

L'integrità e la riservatezza dei dati possono essere minate da molti fattori, compresi la complessità di implementazione, l'uso insicuro delle password, errate configurazioni, codici applicativi scritti male, password inserite nel codice e backdoor dei sistemi non ravvisate. La maggior parte delle organizzazioni pubbliche e private usa dei database per salvare dati personali quali quelli delle buste paga e dei dati medici dei dipendenti, verso i quali hanno la responsabilità legale di mantenerne la privacy e la riservatezza. I database contengono anche dati finanziari critici, passati e futuri, come riferimenti di scambi commerciali, transazioni economiche e finanziarie o dati di accounting. I database contengono anche informazioni dettagliate sui clienti, quali conti finanziari, numeri di carta di credito e dati sull'affidabilità di business partner.

I database sono applicazioni estremamente complesse e, spesso, difficili da configurare in modo corretto e sicuro. Le applicazioni database quali MySQL, PostgreSQL e ORACLE comprendono molte delle seguenti funzioni: sistemi di verifica di account utente e password, modelli di autorizzazione e permessi specifici per il controllo di oggetti del database, comandi integrati, linguaggi di scripting e di programmazione specifici, protocolli di rete, patch e service pack, nonché potenti utility per la gestione del database e strumenti di sviluppo. Molti amministratori si occupano dell'amministrazione dei database solo part-time e spesso non hanno una conoscenza profonda della complessità di queste applicazioni. Il risultato di tutto ciò è che gravi vulnerabilità di sicurezza e cattive configurazioni spesso restano non verificate o del tutto ignorate. Storicamente, la comunità della sicurezza ha per lo più ignorato il problema della sicurezza dei database; molti professionisti dei database non considerano la sicurezza come una delle proprie responsabilità. Molti database posseggono un'ampia gamma di funzioni e possibilità d'uso che possono essere utilizzate in modo non corretto o sfruttate per compromettere la riservatezza, la disponibilità e l'integrità dei dati.

Tutti i moderni sistemi database relazionali sono "port addressable", che significa che chiunque, con l'aiuto di strumenti di facile reperimento, può provare a connettersi direttamente al database, aggirando i meccanismi di sicurezza usati dal sistema operativo. Si può, ad esempio, accedere ad Oracle dalla porta TCP 1521, a MySQL dalla porta TCP 3306, a PostgreSQL dalla porta TCP 5432. La maggior parte delle applicazioni database hanno anche degli account e delle password di default che sono ben noti e che forniscono diversi livelli di accesso alle risorse e alle tabelle del database. Oggi la maggior parte dei database sono strettamente correlati con le applicazioni di front-end, tra le quali le più comuni sono applicazioni web-based. Se l'applicazione è scritta o configurata male, può permettere a un aggressore di condurre un attacco SQL injection o di sfruttare una delle vulnerabilità del database.

Il CERT CC ha pubblicato un advisory, CA-2003-05, per diverse vulnerabilità Oracle che possono compromettere tale database. Più recentemente, anche US-CERT ha pubblicato un advisory sulle vulnerabilità SQL Injection in Oracle E-Business Suite (TA04-160A) che possono compromettere l'applicazione database e l'integrità dei dati.

Allo stesso modo, anche MySQL è soggetto a vulnerabilità simili. Una breve descrizione di alcuni tra gli attacchi più comuni a MySQL è contenuta in un recente documento pubblicato

da Next Generation Software, http://www.nextgenss.com/papers/HackproofingMySQL.pdf.

U9.2 Sistemi operativi interessati
Quasi tutti i sistemi Linux vengono distribuiti con una versione di un DBMS open source come MySQL e PostgreSQL oppure con una soluzione DBMS commerciale come Oracle. Diverse tipologie di UNIX come Solaris, AIX e HPUX supportano ORACLE, DB2 ed altri importanti database commerciali, come la maggior parte dei DBMS open source.

U9.3 Riferimenti CVE/CAN

Oracle:
CVE-2002-0567, CVE-2002-0571

CAN-1999-0652, CAN-1999-1256, CAN-2002-0858, CAN-2002-1264, CAN-2003-0095, CAN-2003-0096, CAN-2003-0222, CAN-2003-0634, CAN-2003-0727, CAN-2003-0894

MySQL:
CVE-1999-1188, CVE-2000-0045, CVE-2000-0148, CVE-2000-0981, CVE-2001-0407

CAN-1999-0652, CAN-2001-1274, CAN-2001-1275, CAN-2002-0229, CAN-2002-0969, CAN-2002-1373, CAN-2002-1374, CAN-2002-1375, CAN-2002-1376, CAN-2003-0073, CAN-2003-0150, CAN-2003-0515, CAN-2003-0780, CAN-2004-0381, CAN-2004-0388, CAN-2004-0627, CAN-2004-0628

PostgreSQL:
CVE-2002-0802

CAN-1999-0862, CAN-2000-1199, CAN-2001-1379, CAN-2002-0972, CAN-2002-1397, CAN-2002-1398, CAN-2002-1399, CAN-2002-1400, CAN-2002-1401, CAN-2002-1402, CAN-2003-0040, CAN-2003-0500, CAN-2003-0515, CAN-2003-0901, CAN-2004-0366, CAN-2004-0547

U9.4 Come stabilire si è vulnerabili
Assicuratevi che tutti i DBMS distribuiti assieme al sistema operativo utilizzino la versione del software più recente. Le versioni di database obsolete o non corrette sono spesso vulnerabili.

Le installazioni di default dei DBMS presentano probabilmente vulnerabilità sfruttabili da un aggressore.

Eseguite una scansione delle vulnerabilità sul sistema per stabilire se il software DBMS è vulnerabile:

- MySQL Network Scanner: permette la scansione di reti intere alla ricerca di server MySQL con password di default (vuote) e può identificare anche i "rogue" server.
- Lo scanner delle vulnerabilità open source Nessus (http://www.nessus.org) comprende anche esami per rilevare i bachi comuni nei database su UNIX.
- Si possono usare anche strumenti commerciali per la rilevazione delle vulnerabilità dei database come Foundstone, Qualys, eEyE Retina.
- Oltre a questi, vi sono anche degli scanner appositi per database come AppSecInc o ISS Database Scanner.

U9.5 Come proteggersi

Per prima cosa è essenziale controllare che le applicazioni database siano aggiornate al più recente livello di patch disponibile. Verificate presso il sito del produttore la eventuali informazioni sulle patch:

- Oracle (http://otn.oracle.com/software/index.html)
- MySQL (http://www.mysql.com/products/mysql/)
- PostgreSQL (ftp://ftp.postgresql.org/pub)

Quindi controllate che il DBMS e le applicazioni siano state rese sicure:

- Usate privilegi minimi.
- Eliminate/Modificate le password di default dagli account di sistema e dagli account del database con diritti elevati, prima di collegare in rete il sistema.
- Usate dove possibile procedure archiviate.
- Eliminate/Modificate le procedure archiviate non necessarie.
- Impostate limiti di lunghezza per qualsiasi campo nei form.
- Convalidate tutti i dati sul lato server (lunghezza, formato, tipo).

Sono disponibili molte utili risorse che aiutano a rendere sicuri i DBMS:

- Oracle (http://otn.oracle.com/deploy/security/index.html)
- MySQL (http://dev.mysql.com/doc/mysql/en/Security.html)
- PostgreSQL (http://www.postgresql.org/docs/7/interactive/security.htm)

Mantenetevi aggiornati sulle vulnerabilità e gli avvisi pubblicati dai produttori:

- Oracle Security Alerts (http://otn.oracle.com/deploy/security/alerts.htm)
- MySQL (http://lists.mysql.com/)
- PostgreSQL (http://www.postgresql.org/lists.html)

Il SANS Institute ha pubblicato una esaustiva security checklist per Oracle che è molto utile per analizzare una installazione database Oracle:
http://www.sans.org/score/oraclechecklist.php

Anche il Center for Internet Security ha sviluppato un Oracle Database Benchmark Tool, utile per mettere alla prova la sicurezza del database:
http://www.cisecurity.org/bench_oracle.html

SANS Security Oracle Step-by-Step fornisce utili e pratici suggerimenti per l'hardening di Oracle (https://store.sans.org/store_item.php?item=80)

Infine, potete trovare ulteriori informazioni sulla sicurezza dei database a questi indirizzi:

- SANS Reading Room on Database Security (http://www.sans.org/rr/catindex.php?cat_id=3)
- http://www.petefinnigan.com/orasec.htm

torna all'inizio ^

U10 Kernel

U10.1 Descrizione

Il cuore di un sistema operativo è il kernel. Il kernel è responsabile di un certo numero di interazioni a basso livello tra il sistema operativo e hardware, memoria, la schedulazione dei processi, l'intercomunicazione tra i processi stessi, il file system ed altri elementi ancora. Poiché il kernel ha un accesso privilegiato a tutti gli aspetti del sistema, una compromissione a livello di kernel può essere devastante. I rischi apportati dalle vulnerabilità kernel comprendono le possibilità di Denial of service, esecuzione di codice abusivo con privilegi system, accesso illimitato al file system o accesso a livello root. Molte vulnerabilità vengono sfruttate da remoto e sono pericolose specialmente quando la via attraverso la quale arriva un attacco passa per un servizio fornito pubblicamente via Internet. In alcuni casi, inviando un pacchetto icmp malformato il kernel può bloccarsi in un loop, consumando tutte le risorse CPU e rendendo la macchina inutilizzabile, portando a un'interruzione del servizio.

Una corretta messa a punto del kernel non solo serve a proteggere il sistema dagli attacchi, ma migliora anche le performance del sistema.

U10.2 Sistemi operativi interessati

Praticamente tutte le varianti di Unix, comprese Solaris e HP-UX, le distribuzioni Linux, le versioni BSD, e le varie versioni di Windows hanno avuto esperienze di vulnerabilità kernel, sia a causa di fattori interni, sia derivanti da bachi contenuti in applicazioni che impattano negativamente sul kernel.

U10.3 Riferimenti CVE/CAN

CVE-1999-0295, CVE-1999-0367, CVE-1999-0482, CVE-1999-0727, CVE-1999-0804, CVE-1999-1214, CVE-1999-1339, CVE-1999-1341, CVE-2000-0274, CVE-2000-0375, CVE-2000-0456, CVE-2000-0506, CVE-2000-0867, CVE-2001-0062, CVE-2001-0268, CVE-2001-0316, CVE-2001-0317, CVE-2001-0859, CVE-2001-0993, CVE-2001-1166, CVE-2002-0046, CVE-2002-0766, CVE-2002-0831

CAN-1999-1166, CAN-2000-0227, CAN-2001-0907, CAN-2001-0914, CAN-2001-1133, CAN-2001-1181, CAN-2002-0279, CAN-2002-0973, CAN-2003-0127, CAN-2003-0247, CAN-2003-0248, CAN-2003-0418, CAN-2003-0465, CAN-2003-0955, CAN-2003-0984, CAN-2004-0003, CAN-2004-0010, CAN-2004-0177, CAN-2004-0482, CAN-2004-0495, CAN-2004-0496, CAN-2004-0497, CAN-2004-0554, CAN-2004-0602

U10.4 Come stabilire se si è vulnerabili

Esistono una serie di tecniche per determinare se i kernel sono vulnerabili.

- Se il produttore li fornisce, richiedete i servizi via e-mail di aggiornamento della sicurezza al momento della registrazione del software.
- La maggior parte delle mailing list sulla sicurezza riferiscono delle vulnerabilità kernel non appena vengono scoperte.
- Un controllo della versione del kernel attiva nei diversi sistemi dovrebbe far parte delle procedure standard.
- Si può usare i software di security assessment per determinare la versione del kernel attiva sui diversi sistemi. Nessus presenta una serie di plug-in per l'analisi dei sistemi alla ricerca di vulnerabilità kernel. *Attenzione:* molti di questi plug-in possono causare condizioni di interruzione del servizio ed è quindi necessario utilizzarli con cautela per la scansione della rete, al fine di prevenire dei tempi di down non previsti.

U10.5 Come proteggersi

Vi sono due classi di parametri che si può configurare sul kernel per ostacolare gli attacchi. Il primo è quello di mettere a punto le risorse di sistema in modo da limitare gli attacchi denial of service e i buffer overflow. La seconda categoria di operazioni comprende l'hardening delle impostazioni di configurazione di rete contro gli attacchi. I comandi e i parametri di configurazione dipendono dalla specifica piattaforma utilizzata. Bisogna quindi consultare la relativa documentazione per capire bene come mettere a punto il kernel.

Si raccomanda di testare bene tutte le modifiche prima di implementarle in un ambiente di produzione e di tenere sempre a disposizione dei backup aggiornati nel caso che sorgano dei problemi.

Esistono diverse utili risorse per migliorare la sicurezza ottimizzando correttamente il kernel del sistema.

Solaris Tunable Parameters Reference Manual (Solaris 8)
Solaris Tunable Parameters Reference Manual (Solaris 9)
Solaris Operating Environment Network Settings for Security
Solaris Kernel Tuning for Security or http://www.securityfocus.com/infocus/1385

Linux Kernel Hardening
The Linux Kernel Archives
Linux Kernel Hardening

AIX Kernel Tuning

HP-UX Kernel Tuning and Performance Guide

http://docs.hp.com/hpux/pdf/5185-6559.pdf
http://docs.hp.com/hpux/pdf/TKP-90203.pdf
http://docs.hp.com/cgi-bin/otsearch/hpsearch
http://docs.hp.com/

Manuale FreeBSD (contiene informazioni per l'ottimizzazione del kernel):
http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/index.html

OpenBSD:
http://www.openbsd.org/faq/index.html
http://www.openbsd.org/docum.html (for more info)

NetBSD Tuning, Kernel Tuning

torna all'inizio ^

Appendix A: Porte generalmente vulnerabili

In questa sezione, abbiamo elencato le porte che sono generalmente esaminate e attaccate. Il blocco di queste porte rappresenta il requisito minimo per la sicurezza perimetrale, non una lista esaustiva delle specifiche per il firewall. Una regola di gran lunga migliore sarebbe quella di bloccare tutte le porte inutilizzate ad esempio

negare tutto il traffico e quindi permettere a specifici protocolli (quelli per i quali la vostra attività ha esigenza specifica) di entrare nel perimetro della vostra rete. Comunque, anche se ritenete che queste porte siano bloccate, dovete sempre controllarle attivamente per scoprire eventuali tentativi d'intrusione. Un ultimo avvertimento è doveroso: il blocco di alcune delle porte elencate può disabilitare servizi necessari. Prima di implementare queste raccomandazioni, consideratene i potenziali effetti.

> **Nota**: È orai comunemente condivisa l'opinione che sia più efficace in termini di sicurezza la pratica di impostare nella configurazione del firewall un deny di default o di bloccare tutto ciò che non è esplicitamente permesso, piuttosto che ricorrere al blocco delle specifiche porte. Questo approccio semplifica anche le procedure di amministrazione di router o di firewall, in quanto le rispettive liste di controllo e di configurazione tendono ad essere più corte, più logiche e semplici da mantenere.

Tenete presente che il blocco di queste porte non rappresenta un sostituto alle security policy e ai progetti per la sicurezza. Se le porte non sono state rese sicure in maniera adeguata su ogni sistema host della vostra organizzazione, un aggressore che ha ottenuto l'accesso alla vostra rete con altri mezzi (un modem telefonico, un trojan allegato ad un'e-mail o un complice interno all'organizzazione, per esempio) può sfruttare dette porte anche se sono bloccate.

Nome	**Porta**	**Protocollo**	**Descrizione**
Small services	<20	tcp/udp	small services
FTP	21	tcp	file transfer
SSH	22	tcp	login service
TELNET	23	tcp	login service
SMTP	25	tcp	mail
TIME	37	tcp/udp	time synchronization
WINS	42	tcp/udp	WINS replication
DNS	53	udp	naming services
DNS zone transfers	53	tcp	naming services
DHCP server	67	tcp/udp	host configuration
DHCP client	68	tcp/udp	host configuration
TFTP	69	udp	miscellaneous
GOPHER	70	tcp	old WWW-like service
FINGER	79	tcp	miscellaneous
HTTP	80	tcp	web
alternate HTTP port	81	tcp	web
alternate HTTP port	88	tcp	web (sometimes Kerberos)
LINUXCONF	98	tcp	host configuration
POP2	109	tcp	mail
POP3	110	tcp	mail
PORTMAP/RPCBIND	111	tcp/udp	RPC portmapper

NNTP	119	tcp	network news service
NTP	123	udp	time synchronization
NetBIOS	135	tcp/udp	DCE-RPC endpoint mapper
NetBIOS	137	udp	NetBIOS name service
NetBIOS	138	udp	NetBIOS datagram service
NetBIOS/SAMBA	139	tcp	file sharing & login service
IMAP	143	tcp	mail
SNMP	161	tcp/udp	miscellaneous
SNMP	162	tcp/udp	miscellaneous
XDMCP	177	udp	X display manager protocol
BGP	179	tcp	miscellaneous
FW1-secureremote	256	tcp	CheckPoint FireWall-1 mgmt
FW1-secureremote	264	tcp	CheckPoint FireWall-1 mgmt
LDAP	389	tcp/udp	naming services
HTTPS	443	tcp	web
Windows 2000 NetBIOS	445	tcp/udp	SMB over IP (Microsoft-DS)
ISAKMP	500	udp	IPSEC Internet Key Exchange
REXEC	512	tcp	} the three
RLOGIN	513	tcp	} Berkeley r-services
RSHELL	514	tcp	} (used for remote login)
RWHO	513	udp	miscellaneous
SYSLOG	514	udp	miscellaneous
LPD	515	tcp	remote printing
TALK	517	udp	miscellaneous
RIP	520	udp	routing protocol
UUCP	540	tcp/udp	file transfer
HTTP RPC-EPMAP	593	tcp	HTTP DCE-RPC endpoint mapper
IPP	631	tcp	remote printing
LDAP over SSL	636	tcp	LDAP over SSL
Sun Mgmt Console	898	tcp	remote administration
SAMBA-SWAT	901	tcp	remote administration
Windows RPC programs	1025	tcp/udp	} often allocated
Windows RPC programs	to		} by DCE-RPC portmapper
Windows RPC programs	1039	tcp/udp	} on Windows hosts
SOCKS	1080	tcp	miscellaneous
LotusNotes	1352	tcp	database/groupware
MS-SQL-S	1433	tcp	database
MS-SQL-M	1434	udp	database
CITRIX	1494	tcp	remote graphical display
WINS replication	1512	tcp/udp	WINS replication
ORACLE	1521	tcp	database
NFS	2049	tcp/udp	NFS file sharing

COMPAQDIAG	2301	tcp	Compaq remote administration
COMPAQDIAG	2381	tcp	Compaq remote administration
CVS	2401	tcp	collaborative file sharing
SQUID	3128	tcp	web cache
Global catalog LDAP	3268	tcp	Global catalog LDAP
Global catalog LDAP SSL	3269	tcp	Global catalog LDAP SSL
MYSQL	3306	tcp	database
Microsoft Term. Svc.	3389	tcp	remote graphical display
LOCKD	4045	tcp/udp	NFS file sharing
Sun Mgmt Console	5987	tcp	remote administration
PCANYWHERE	5631	tcp	remote administration
PCANYWHERE	5632	tcp/udp	remote administration
VNC	5800	tcp	remote administration
VNC	5900	tcp	remote administration
X11	6000-6255	tcp	X Windows server
FONT-SERVICE	7100	tcp	X Windows font service
alternate HTTP port	8000	tcp	web
alternate HTTP port	8001	tcp	web
alternate HTTP port	8002	tcp	web
alternate HTTP port	8080	tcp	web
alternate HTTP port	8081	tcp	web
alternate HTTP port	8888	tcp	web
Unix RPC programs	32770	tcp/udp	} often allocated
Unix RPC programs	to		} by RPC portmapper
Unix RPC programs	32899	tcp/udp	} on Solaris hosts
COMPAQDIAG	49400	tcp	Compaq remote administration
COMPAQDIAG	49401	tcp	Compaq remote administration
PCANYWHERE	65301	tcp	remote administration

ICMP: bloccate le richieste echo in entrata (ping e Windows traceroute), bloccate le risposte echo in uscita, i messaggi di time exceeded e destination unreachable, con l'esclusione dei messaggi "packet too big" (type 3, code 4). (Questa operazione presuppone che si intenda rinunciare agli usi legittimi delle richieste echo ICMP al fine di bloccare alcuni utilizzi noti di questa risorsa a scopo doloso.)

Oltre alle porte elencate, bloccate gli indirizzi ingannevoli (spoofed): i pacchetti che provengono dall'esterno della vostra società con indirizzo interno, gli indirizzi privati (RFC1918) e gli indirizzi riservati IANA (per i dettagli, consultate http://www.iana.org/assignments/ipv4-address-space). Si suggerisce anche di bloccare i pacchetti destinati a indirizzi broadcast e multicast. Risulterà vantaggioso bloccare in particolare i pacchetti source routed o qualsiasi pacchetto che abbia le opzioni IP impostate.

Dovreste anche mettere in atto dei filtri in uscita sui vostri router perimetrali per bloccare i pacchetti ingannevoli (spoofed) originati dalla vostra rete. Permettete che dalla vostra organizzazione vengano instradati solo pacchetti originati dai vostri indirizzi riconosciuti.

Riconoscimento dei Marchi: Il SANS Institute riconosce l'importanza della proprietà, dei marchi, del copyright, dei marchi per i servizi e dei brevetti e ha fatti di tutto per riconoscere tali standard in questo documento. I seguenti prodotti, sistemi o applicazioni sono marchi registrati. Se vi accorgete che ci siamo lasciati sfuggire qualche marchio di prodotto, scrivete via email a top20@sans.org i vostri commenti le vostre osservazioni e vi assicuriamo che se necessario procederemo a un aggiornamento del documento.

> Microsoft, Windows, Windows Server 2003, Microsoft SQL Server, Microsoft Outlook sono marchi o marchi registrati di Microsoft Corporation negli Stati Uniti e/o in altri paesi.
>
> Sendmail è un marchio o un marchio registrato di Sendmail, Inc. negli Stati Uniti e/o in altri paesi.
>
> SSH è un marchio o un marchio registrato di SSH Communication Security negli Stati Uniti e/o in altri paesi.
>
> CERT Coordination Center è un marchio o un marchio registrato di Carnegie Mellon; Software Engineering Institute negli Stati Uniti e/o in altri paesi.
>
> UNIX è un marchio o un marchio registrato di The Open Group negli Stati Uniti e/o in altri paesi.

torna all'inizio ^

Appendice B

Gli esperti che hanno collaborato a creare la lista dei venti servizi più vulnerabili 2003

Adair Collins, US Department of Energy
Alan Paller, SANS Institute
Alex Lucas, United Kingdom National Infrastructure Security Co-ordination Center
Alexander Kotkov, CCH Legal Information Services
Anton Chuvakin, Ph.D., netForensics
BJ Bellamy, Kentucky Auditor of Public Accounts
Bradley Peterson, US Department of Energy
Cathy Booth, United Kingdom National Infrastructure Security Co-ordination Center - Incident Response CESG
Chris Benjes, National Security Agency
Christopher Misra, University of Massachusetts Amherst
Dave Dobrotka, Ernst & Young
Dominic Beecher, United Kingdom National Infrastructure Security Co-ordination
Ed Fisher, CableJiggler Consulting, LLC
Edward Skoudis, International Network Services

Edward W. Ray, MMICMAN LLC
Erik Kamerling, Pragmeta Networks/SANS Institute - Editor
Gerhard Eschelbeck, Qualys
Jeff Campione, Editor 2002
Jeff Ito, Indus Corporation
Jeni Li, Arizona State University
Kevin Thacker, United Kingdom National Infrastructure Security Co-ordination
Koon Yaw Tan, Infocomm Development Authority of Singapore (IDA)
Pedro Paulo Ferreira Bueno, MetroRED Telecom, Brazil
Pete Beck, United Kingdom National Infrastructure Security Co-ordination
Richard (Rick) Wanner, InfoSec Centre of Expertise (COE) CGI Information Systems & Management Consultants Inc.
Roland M Lascola, U.S. Dept. of Energy - Office of Independent Oversight and Performance Assurance
Ross Patel, Afentis Security
Russell Morrison, AXYS Environmental Consulting Ltd.
Scott A. Lawler, CISSP, Veridian Information Solutions
Stephen Northcutt, SANS Institute
Valdis Kletnieks, Virginia Tech
William Eckroade, U.S. Dept. of Energy

Si ringrazia anche le persone nella seguente lista per il loro eccellente lavoro di produzione, redazione e assemblaggio della lista 2003

Audrey (Dalas) Bines, SANS Institute
Brian Corcoran, SANS Institute
Cara L. Mueller, SANS Institute

Il team Top 20 vorrebbe anche ringraziare i seguenti studenti SANS che hanno donato il proprio tempo per rivedere e commentare le bozze 2003

Paul Graham, CIT at the University at Buffalo (UB)
Jerry Berkman, UC Berkeley
Neil W Rickert, Northern Illinois University
Travis Hildebrand, US Department of Veteran Affairs
Christoph Gruber, WAVE Solutions
Mark Worthington, Affiliated Computer Services (ACS), Riverside Public Library
Matthew Nehawandian, CISSP

Gli esperti che hanno collaborato alla creazione della lista dei venti servizi più vulnerabili per il 2002

Jeff Campione, Federal Reserve Board - Editor
Eric Cole, Editor, 2001 Edition
Ryan C. Barnett, Department of the Treasury/ATF
Chris Benjes, National Security Agency
Matt Bishop, University of California, Davis
Chris Brenton, SANS Institute
Pedro Paulo Ferreira Bueno, Open Communications Security, Brazil
Anton Chuvakin, Ph.D., netForensics
Rob Clyde, Symantec
Dr. Fred Cohen, Sandia National Laboratories

Gerhard Eschelbeck, Qualys
Dan Ingevaldson, Internet Security Systems
Erik Kamerling, Pragmeta Networks
Gary Kessler, Gary Kessler Associates
Valdis Kletnieks, Virginia Tech CIRT
Alexander Kotkov - CCH Legal Information Services
Jamie Lau, Internet Security Systems
Scott Lawler, Veridias Information Solutions
Jeni Li, Arizona State University
Nick Main, Cerberus IT, Australia
Jose Marquez, Alutiiq Security and Technology
Christopher Misra, University of Massachusetts
Stephen Northcutt, SANS Institute
Craig Ozancin, Symantec
Alan Paller, SANS Institute
Ross Patel, Afentis, UK
Marcus Ranum, ranum.com
Ed Ray - MMICMAN LLC
Chris Rouland, Internet Security Systems
Bruce Schneier, Counterpane Internet Security Inc.
Greg Shipley, Neohapsis
Ed Skoudis, Predictive Systems
Gene Spafford, Purdue University CERIAS
Koon Yaw Tan, Infocomm Development Authority of Singapore
Mike Torregrossa, University of Arizona
Viriya Upatising, Loxley Information Services, Thailand
Rick Wanner, CGI Information Systems and Management Consultants

Le persone che hanno collaborato nell'organizzare secondo un ordine di priorità le singole voci CVE per definire i test utilizzati negli scanner Top 20 del 2002. Per i dettagli sui procedimenti utilizzati, consultate www.sans.org/top20/testing.pdf

Charles Ajani, Standard Chartered Bank, London, UK
Steven Anderson, Computer Sciences Corporation, North Kingstown RI
John Benninghoff, RBC Dain Rauscher, Minneapolis MN
Layne Bro, BEA Systems, Denver CO
Thomas Buehlmann, Phoenix AZ
Ed Chan, NASA Ames Research Center, San Jose CA
Andrew Clarke, Computer Solutions, White Plains NY
Brian Coogan, ManageSoft, Melbourne Australia
Paul Docherty, Portcullis Computer Security Limited,UK
Arian Evans, U.S. Central Credit Union, Overland Park KS
Rich Fuchs, Research Libraries Group, Mountain View CA
Mark Gibbons, International Network Services, Minneapolis MN
Dan Goldberg, Rochester NY
Shan Hemphill, Sacramento CA
Michael Hensing, Charlotte, NC, Microsoft
Simon Horn, Brisbane Australia
Bruce Howard, Kanwal Computing Solutions, Jilliby NSW Australia
Tyler Hudak, Akron OH
Delbert Hundley, MPRI Division of L-3COM, Norfolk VA
Chyuan-Horng Jang, Oak Brook IL
Kim Kelly, The George Washington University, Washington DC

Martin Khoo, Singapore Computer Emergency Response Team (SingCERT), Singapore
Susan Koski, Pittsburgh PA
Kevin Liston, AT&T, Columbus OH
Andre Marien, Ubizen, Belgium
Fran McGowran, Deloitte & Touche, Dublin, Ireland, UK
Derek Milroy, Zurich North America, Chicago IL
Bruce Moore, Canadian Forces Network Operations Center, DND, Ottawa Canada
Castor Morales, Ft. Lauderdale FL
Luis Perez, Boston MA
Reg Quinton, University of Waterloo, Ontario Canada
Bartek Raszczyk, UWM Olsztyn, Olsztyn Poland
Teppo Rissanen, Plasec Oy, Helsinki Finland
Alan Rouse, N2 Broadband, Duluth GA
Denis Sanche, PWGSC ITSD/IPC, Hull, QC Canada
Felix Schallock, Ernst & Young, Vienna, Austria
Gaston Sloover, Fidelitas, Buenos Aires Argentina
Arthur Spencer, UMASS Medical School, Worcester MA
Rick Squires
Jeff Stehlin, HP
Koon Yaw TAN, Infocomm Development Authority of Singapore, Singapore
Steven Weil, Seitel Leeds & Associates, Seattle WA
Lance Wilson, Time Warner Cable/Broadband IS, Orlando FL
Andrew Wortman, Naval Research Laboratory, Washington DC
Carlos Zottman, Superior Tribunal de Justica, Brasilia Brazil

Ulteriori esperti di sicurezza che hanno collaborato alla stesura della Top20 del 2001 e della Top10 del 2000, che rappresentano le fondamenta sulle quali sono state costruite le successive liste

Billy Austin, Intrusion.com
Phil Benchoff, Virginia Tech CIRT
Tina Bird, Counterpane Internet Security Inc.
Lee Brotzman, NASIRC Allied Technology Group Inc.
Mary Chaddock
Steve Christey, MITRE
Scott Conti, University of Massachusetts
Kelly Cooper, Genuity
Scott Craig, KMart
Sten Drescher, Tivoli Systems
Kathy Fithen, CERT Coordination Center
Nick FitzGerald, Computer Virus Consulting Ltd.
Igor Gashinsky, NetSec Inc.
Bill Hancock, Exodus Communications
Robert Harris, EDS
Shawn Hernan, CERT Coordination Center
Bill Hill, MITRE
Ron Jarrell, Virginia Tech CIRT
Jesper Johansson, Boston University
Christopher Klaus, Internet Security Systems
Clint Kreitner, Center for Internet Security
Jimmy Kuo, Network Associates Inc.

Jim Magdych, Network Associates Inc.
Dave Mann, BindView
Randy Marchany, Virginia Tech
Mark Martinec "Jozef Stefan" Institute
William McConnell, Trend Consulting Services
Peter Mell, National Institutes of Standards and Technology
Larry Merritt, National Security Agency
Mudge, @stake
Tim Mullen, AnchorIS.com
Ron Nguyen, Ernst & Young
David Nolan, Arch Paging
Hal Pomeranz, Deer Run Associates
Chris Prosise, Foundstone Inc.
Jim Ransome
RAZOR Research - BindView Development
Martin Roesch, Snort
Vince Rowe, FBI, NIPC
Marcus Sachs, JTF-CNO US Department of Defense
Tony Sager, National Security Agency
Gene Schultz, Lawrence Berkeley Laboratory
Eric Schultze, Foundstone
Derek Simmel, Carnegie Mellon University
Ed Skoudis, Predictive Systems
Lance Spitzner, Sun Microsystems, GESS Team
Wayne Stenson, Honeywell
Jeff Stutzman
Frank Swift
Bob Todd, Advanced Research Corporation
Jeff Tricoli, FBI NIPC
Laurie Zirkle, Virginia Tech CIRT

Gli esperti che hanno collaborato alla localizzazione italiana della Top 20

Francesco Millotti, Data Security
Simone Brun, Data security
Jess Garcia, LAEFF-INTA

torna all'inizio ^