Ethical Hacking and Countermeasures

Version6

Module I

Introduction to Ethical Hacking

Scenario

Jeffery came across some books that were related to hacking. He was curious to know about hacking public and private networks. He bought a book related to it from the nearby bookstore.

Amazed to learn new techniques about hacking, Jeffrey wanted to get hands on them. He visited a local library and plugged his laptop to its network to search the database of books. Jeffrey wanted to find the vulnerability present in the library's network and then show the report to the concerned authorities.

Jeffrey launched the tools from a CD that was offered with the book and discovered lot of loopholes in the network!

What is wrong with Jeffrey's act?

Is his action justified?

PCWorld

'Hacker Safe' Seal: Web Site Shield, or Target?

More than 80,000 Web sites worldwide display a small green logo that proclaims them to be "Hacker Safe." Is it a promise or a target?

Jaikumar Vijayan, Computerworld

Tuesday, January 22, 2008 02:00 PM PST

More than 80,000 Web sites worldwide display a small green logo that proclaims them to be "Hacker Safe." The logo is provided to them by ScanAlert Inc., a vendor that scans the sites of its clients daily in search of security vulnerabilities.

ScanAlert's logo is the most widely used security seal of its kind on the Web, and it can be found on dozens of marquee-brand sites, including those of Johnson & Johnson, Sony Corp. and Warner Bros. Entertainment Inc. Such widespread use attracted the attention of security vendor McAfee Inc., which in late October agreed to acquire ScanAlert.

But Napa, Calif.-based ScanAlert was put on the defensive this month after online technology retailer Geeks.com warned an undisclosed number of customers that their personal and credit card data may have been compromised in a hacking incident. Geeks.com, whose formal name is Genica Corp., displays the Hacker Safe logo at the bottom of its home page.

A ScanAlert spokesman said "preliminary evidence" suggests that the breach likely occurred during one of several periods last year when ScanAlert had withdrawn its certification from Geeks.com after finding vulnerabilities on the Web site.

Debate Rekindled

Even so, the incident at Geeks.com has rekindled a debate about the value of security seals such as the Hacker Safe logo.

ScanAlert users say that the scanning service can sniff out at least some security problems and that the logo is a valuable marketing tool for them.

On the other hand, ScanAlert's detractors say the service can give companies and their online customers a false sense of security. Indeed, hacker groups have claimed that they have targeted and broken into numerous Web sites displaying the Hacker Safe logo.

Source : *http://www.pcworld.com/*

News

Stolen: Google employees' personal data

By Brendon Chase
http://news.cnet.com/Stolen-Google-employees-personal-data/2100-1029_3-6243093.html

Story last modified Thu Jul 03 10:09:42 PDT 2008

Google has confirmed that personal data of U.S. employees hired prior to 2006 have been stolen in a recent burglary.

Records kept at Colt Express Outsourcing Services, an external company Google and other companies use to handle human resources functions, were stolen in a burglary on May 26. An undisclosed number of employees' details and those of dependents such as names, addresses, and Social Security numbers were on the stolen computers. It is understood that Colt did not employ encryption to protect the information.

It's still unclear how many more of Colt Express' clients were affected by the breach. CBS' CNET Networks, publisher of News.com, was also affected by the burglary, with about 6,500 employees' details stolen.

Although there is no evidence of misuse of the data to date, the information obtained could be used by identity thieves to create fake accounts and identities.

It's only come to light now that Google was one of the companies affected. Google itself was not burglarized, nor were any of its internal systems compromised.

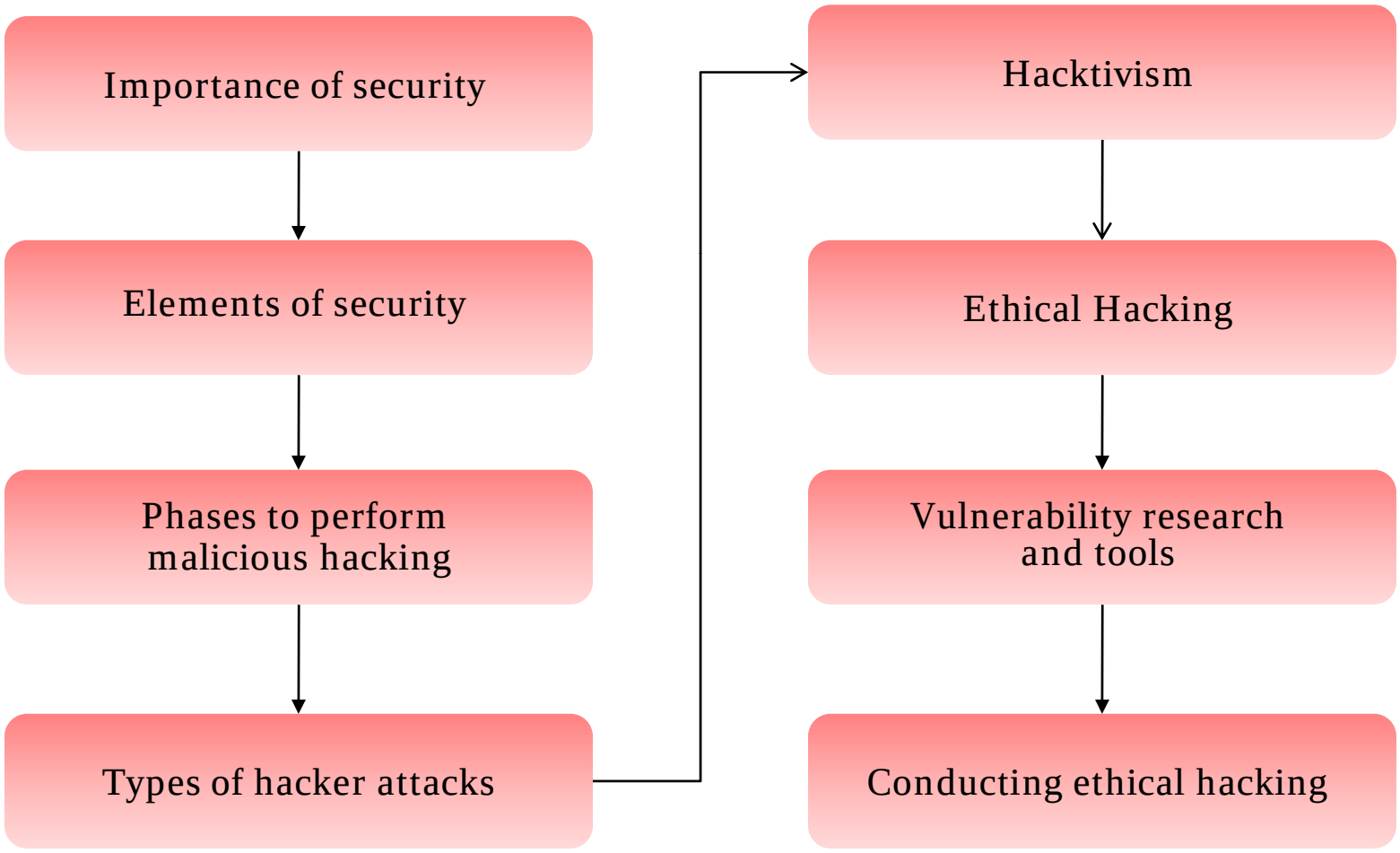
Source: *http://news.cnet.com/*

Module Objective

This module will familiarize you with:

- Importance of information security in today's world
- Elements of security
- Various phases of the Hacking Cycle
- Types of hacker attacks
- Hacktivism
- Ethical Hacking
- Vulnerability research and tools
- Steps for conducting ethical hacking
- Computer crimes and implications
- Cyber Laws prevailing in various parts around the world

Module Flow



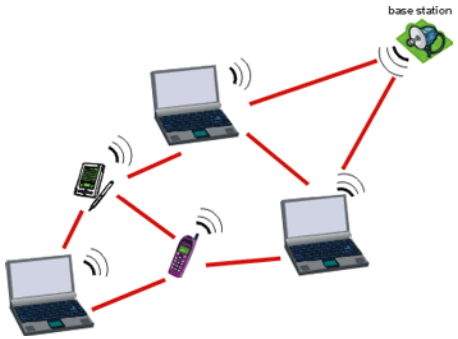
Problem Definition – Why Security?

Evolution of technology focused on ease of use

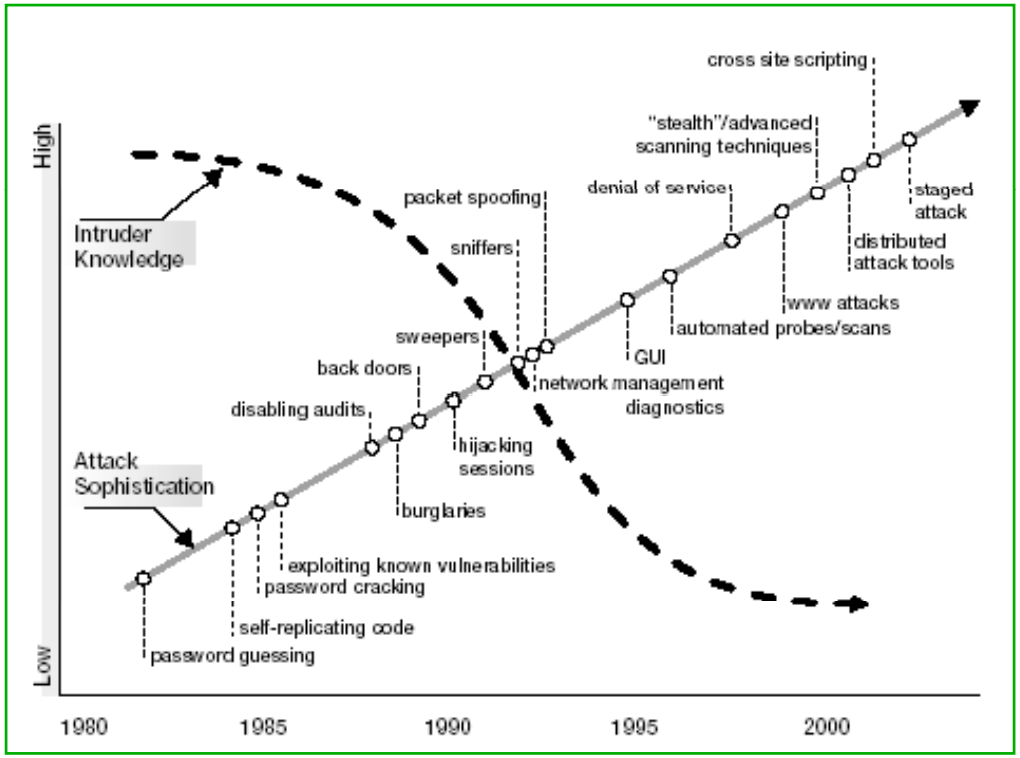
Microsoft Internet Explorer Drag and Drop Vulnerability

Secunia Advisory:	SA12321
Release Date:	2004-08-19
Last Update:	2004-10-12
Critical:	Highly critical
Impact:	System access
Where:	From remote

Increased network environment and network based applications



Decreasing skill level needed for exploits



Problem Definition – Why Security? (cont'd)

Direct impact of security breach on corporate asset base and goodwill

Bookie reveals $100,000 cost of denial-of-service extortion attacks

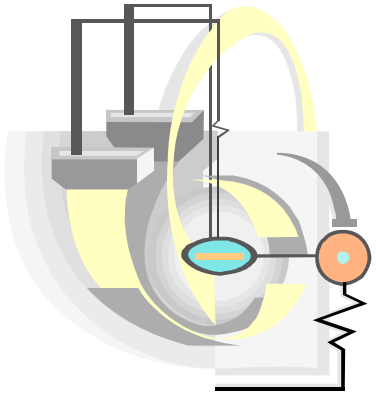
June 11 2004

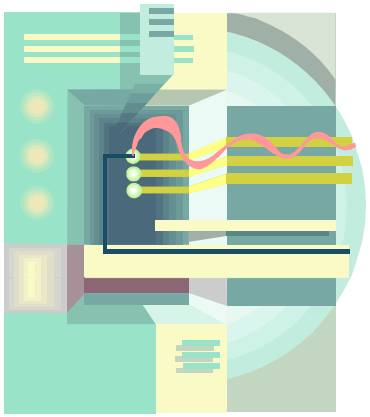
by Andy McCue

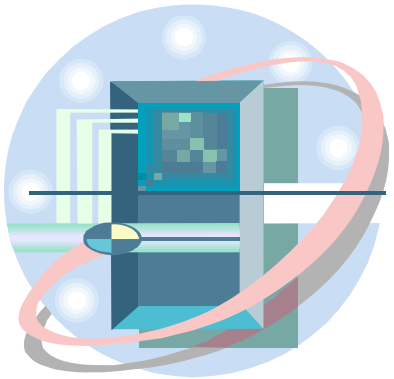
And that's just for starters – an online betting site tells all to silicon.com...

"Our first attack was in November last year. We got a demand for $50,000 from an unidentified source." These are the words of a UK-based online bookmaker who has agreed to speak to silicon.com, on condition of anonymity, to reveal the full scale of the denial of service extortion threats that betting sites have been battling against for nine months.

Increasing complexity of computer infrastructure administration and management







Essential Terminologies

Threat:

- An action or event that might compromise security. A threat is a potential violation of security

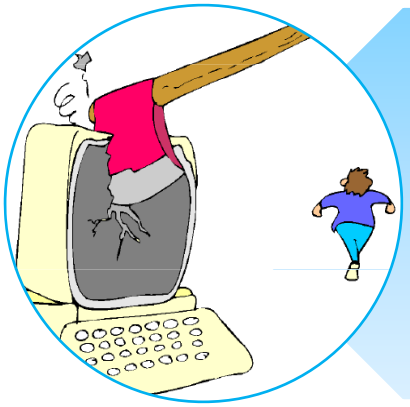
Vulnerability:

- Existence of a weakness, design, or implementation error that can lead to an unexpected and undesirable event compromising the security of the system

Target of Evaluation:

- An IT system, product, or component that is identified/subjected to require security evaluation

Essential Terminologies (cont'd)



Attack:

- An assault on the system security that is derived from an intelligent threat. An attack is any action that violates security

Exploit:

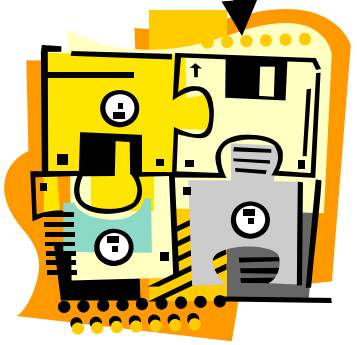
- A defined way to breach the security of an IT system through vulnerability

Elements of Security

Security

- A state of well-being of information and infrastructure in which the possibility of successful yet undetected theft, tampering, and disruption of information and services is kept low or tolerable

Any hacking event will affect any one or more of the essential security elements



Elements of Security (cont'd)

Security rests on confidentiality, authenticity, integrity, and availability

Confidentiality

- The concealment of information or resources

Authenticity

- The identification and assurance of the origin of information

Integrity

- The trustworthiness of data or resources in terms of preventing improper and unauthorized changes

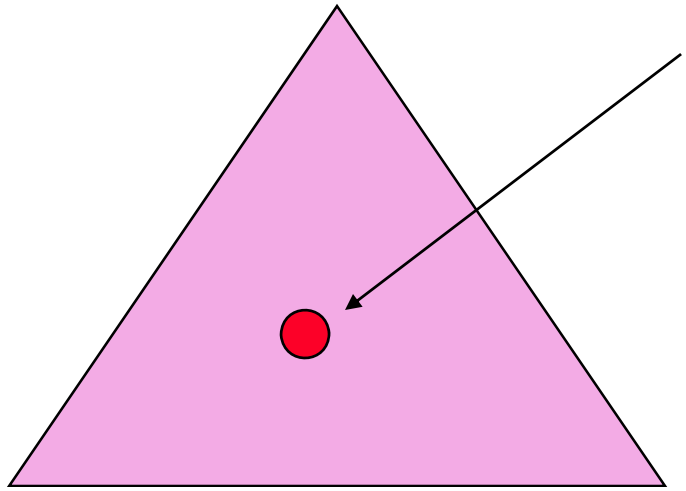
Availability

- The ability to use the desired information or resource

The Security, Functionality, and Ease of Use Triangle

The number of exploits is minimized when the number of weaknesses is reduced => greater security

Takes more effort to conduct the same task => reduced functionality



Moving the ball towards security means moving away from the functionality and ease of use

Case Study

WORM'S EFFECTS

Customers of the Canadian Imperial Bank of Commerce in Toronto were unable to withdraw money using ATMs during part of Saturday.

Korea Telecom Freetel and SK Telecom service failed, stranding millions of South Korean Internet users.

Internet congestion prevented consumers from contacting Microsoft over the Internet to unlock the anti-piracy features of its latest products, including the Windows XP and Office XP software packages.

The U.S. departments of State, Agriculture, Commerce and some units of the Defense Department appeared hardest hit among federal agencies.

Alan was stranded at Newark airport. He was to attend his friend's wedding and Continental airlines just announced the cancellation of his hop-over flight

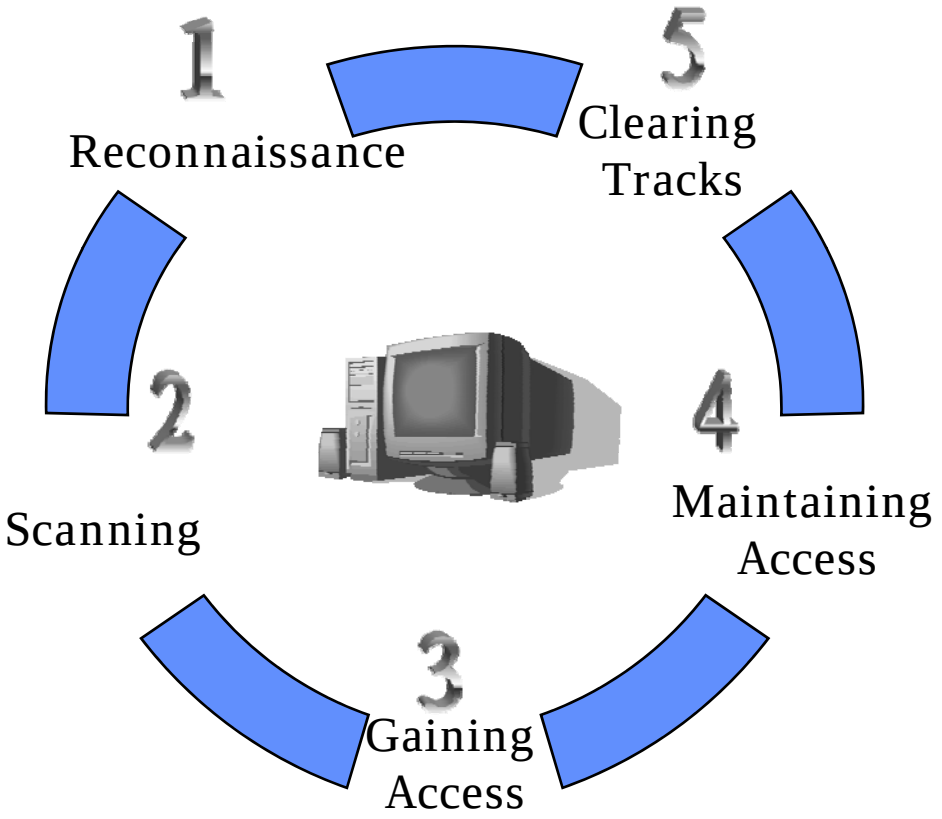
He decided to purchase a seat on another airline, but the Bank of America Corp ATM just did not work

All seemed wrong with the world as the airline staff were using pen and paper to take down new reservations. They could not even confirm the availability

Source: *http://www.cnn.com/*

What Does a Malicious Hacker Do

- **Reconnaissance**
  - Active/passive
- **Scanning**
- **Gaining access**
  - Operating system level/application level
  - Network level
  - Denial of service
- **Maintaining access**
  - Uploading/altering/ downloading programs or data
- **Clearing tracks**



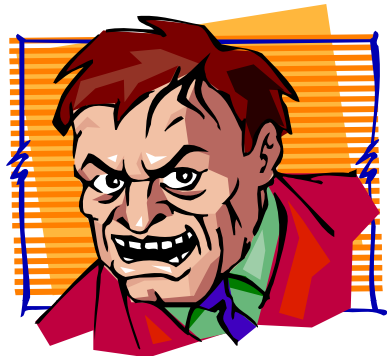
Effect on Business

"They (hackers) don't care what kind of business you are, they just want to use your computer," says Assistant U.S. Attorney Floyd Short in Seattle, head of the Western Washington Cyber Task Force, a coalition of federal, state, and local criminal justice agencies

If the data is altered or stolen, a company may risk losing credibility and the trust of their customers

There is a continued increase in malware that installs open proxies on systems, especially targeting broadband user's zombies

Businesses most at risk, experts say, are those handling online financial transactions



Hacker

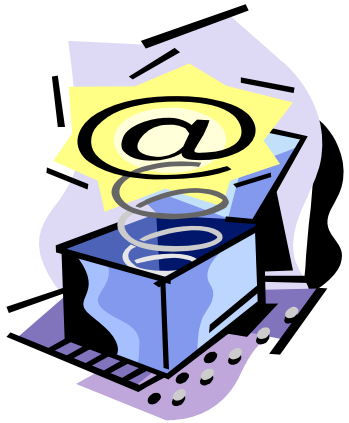
Office User

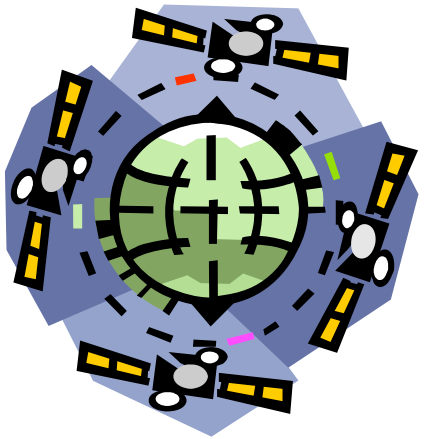
Phase 1 - Reconnaissance

Reconnaissance refers to the preparatory phase where an attacker seeks to gather as much information as possible about a target of evaluation prior to launching an attack

Business Risk: **Notable** - Generally noted as "rattling the door knobs" to see if someone is watching and responding

Could be the future point of return, noted for ease of entry for an attack when more about the target is known on a broad scale





Reconnaissance Types

Passive reconnaissance involves acquiring information without directly interacting with the target

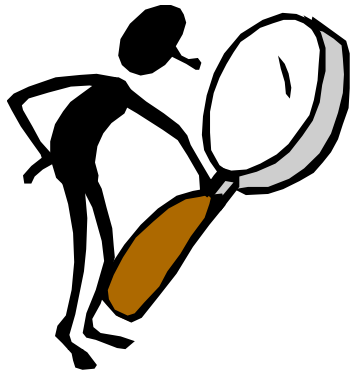
- For example, searching public records or news releases

Active reconnaissance involves interacting with the target directly by any means

- For example, telephone calls to the help desk or technical department

Phase 2 - Scanning

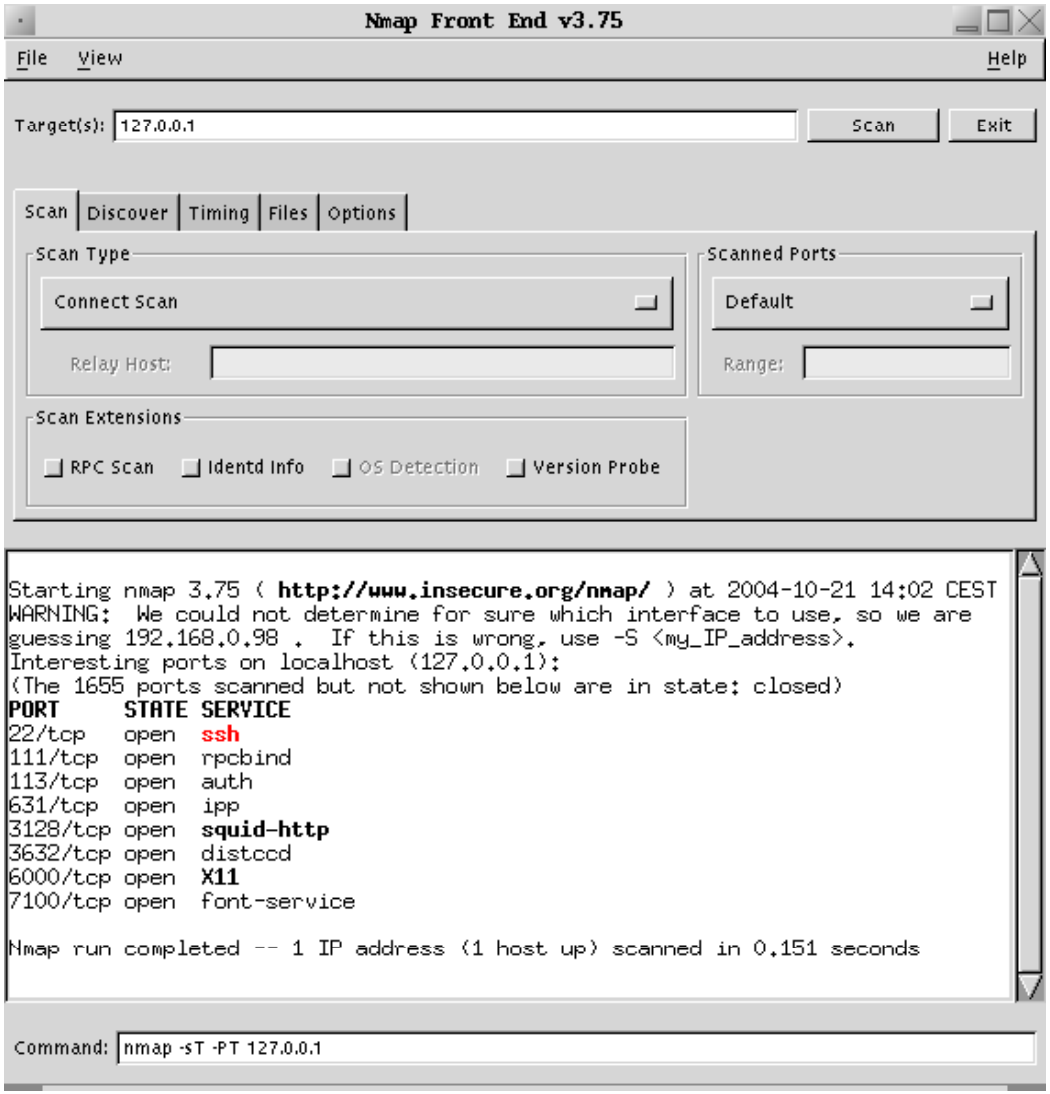
Scanning refers to the pre-attack phase when the hacker scans the network for specific information on the basis of information gathered during reconnaissance



Business Risk: **High** – Hackers have to get a single point of entry to launch an attack

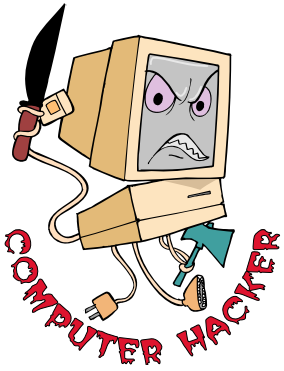
Scanning can include use of dialers, port scanners, network mapping, sweeping, vulnerability scanners, and so on

Phase 2 – Scanning (cont'd)



Phase 3 - Gaining Access

Gaining access refers to the penetration phase. The hacker exploits the vulnerability in the system



The exploit can occur over a LAN, the Internet, or as a deception, or theft. Examples include buffer overflows, denial of service, session hijacking, and password cracking

Influencing factors include architecture and configuration of the target system, the skill level of the perpetrator, and the initial level of access obtained

Business Risk: **Highest** – The hacker can gain access at the operating system level, application level, or network level

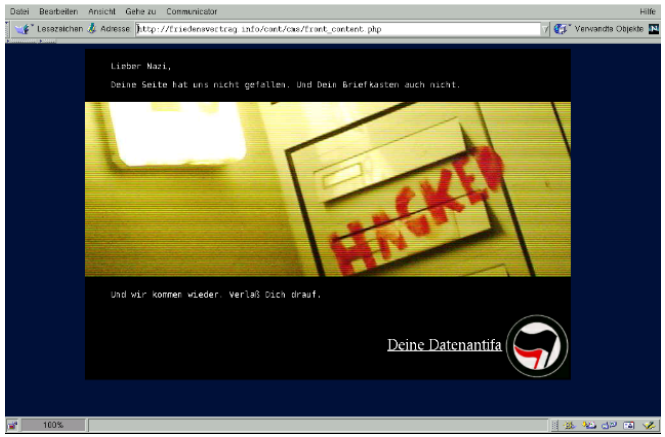
Phase 4 - Maintaining Access

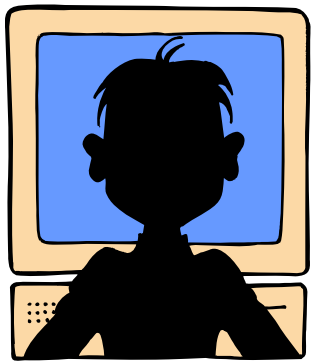
Maintaining access refers to the phase when the hacker tries to retain his/her ownership of the system

The hacker has compromised the system

Hackers may harden the system from other hackers as well (to own the system) by securing their exclusive access with Backdoors, RootKits, or Trojans

Hackers can upload, download, or manipulate data, applications, and configurations on the owned system





Phase 5 - Covering Tracks

Covering Tracks refer to the activities that the hacker does to hide his misdeeds

Reasons include the need for prolonged stay, continued use of resources, removing evidence of hacking, or avoiding legal action

Examples include Steganography, tunneling, and altering log files

Types of Hacker Attacks

There are several ways an attacker can gain access to a system

The attacker must be able to exploit a weakness or vulnerability in a system

Attack Types:

- Operating System attacks
- Application-level attacks
- Shrink Wrap code attacks
- Misconfiguration attacks

1. Operating System Attacks

Microsoft probes secret code leak

Microsoft is investigating how part of its Windows operating system source code found its way onto the net.

It is the second security worry for Bill Gates' company this week

Microsoft spokesman Tom Pilla said it was not known how the chunks of Windows 2000 and NT code had leaked out.

"We are currently investigating these postings and are working with the appropriate law enforcement authorities," he said.

More than 90% of PCs use Microsoft software, so this leak of intellectual property is a concern for the company.

"It's illegal for third parties to post Microsoft source code, and we take such activity very seriously," added Mr Pilla.

1. Operating System Attacks (cont'd)

- Today's operating systems are complex in nature
- Operating systems run many services, ports, and modes of access and require extensive tweaking to lock them down
- The default installation of most operating systems has large numbers of services running and ports open
- Applying patches and hotfixes are not easy in today's complex network
- Attackers look for OS vulnerabilities and exploit them to gain access to a network system

Security News: Default Installation

ATM passwords found online

Up to 70,000 US cash machines vulnerable

Andrew Charlesworth, vnunet.com 22 Sep 2006

The manufacturers' passwords for cash machines used widely across the US are available online in an installation manual.

New York-based security researcher Dave Goldsmith, founder and president of penetration testing outfit Matasano Security, pieced together clues from a CNN broadcast and the website of Tranax Technologies, the ATM's manufacturer.

Then he searched for the ATM's installation and maintenance manual online which he said gave him enough information to hijack a Tranax Mini-bank 1500 series ATM if the manufacturer's default passwords had been left unchanged.

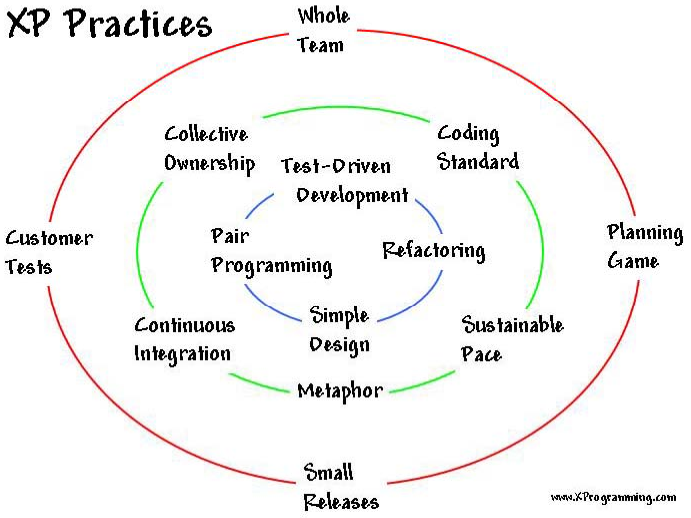
"My guess is that most of these mini-bank terminals are sitting around with default passwords untouched," Goldsmith told eWeek.

According to the Tranax website, around 70,000 1500 series ATMs are installed in the US.

Source: *http://www.vnunet.com/*

2. Application Level Attacks

- Software developers are under tight schedules to deliver products on time
- Extreme Programming is on the rise in software engineering methodology
- Software applications come with tons of functionalities and features
- Sufficient time is not there to perform complete testing before releasing products
- Security is often an afterthought and usually delivered as "add-on" component
- Poor or non-existent error checking in applications which leads to "Buffer Overflow Attacks"



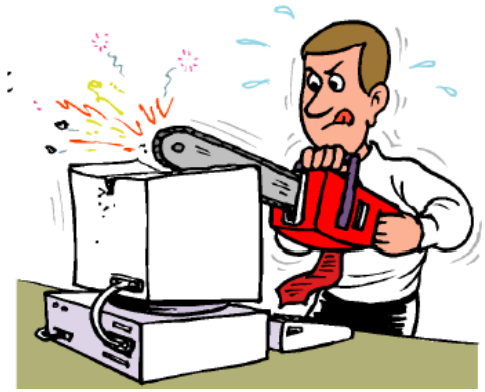
3. Shrink Wrap Code Attacks

Why reinvent the wheel when you can buy off-the-shelf "**libraries**" and code?

When you install an OS/Application, it comes with tons of sample scripts to make the life of an administrator easy

The problem is "**not fine tuning**" or customizing these scripts

This will lead to default code or shrink wrap code attack



3. Shrink Wrap Code Attacks (cont'd)

```
01522  Private Function CleanUpLine(ByVal sLine As String) As String
01523      Dim lQuoteCount As Long
01524      Dim lcount      As Long
01525      Dim sChar       As String
01526      Dim sPrevChar   As String
01527
01528      ' Starts with Rem it is a comment
01529      sLine = Trim(sLine)
01530      If Left(sLine, 3) = "Rem" Then
01531          CleanUpLine = ""
01532          Exit Function
01533      End If
01534
01535      ' Starts with ' it is a comment
01536      If Left(sLine, 1) = "'" Then
01537          CleanUpLine = ""
01538          Exit Function
01539      End If
01540
01541      ' Contains ' may end in a comment, so test if it is a comment or in the
01542      ' body of a string
01543      If InStr(sLine, " '") > 0 Then
01544          sPrevChar = " "
01545          lQuoteCount = 0
01546
01547          For lcount = 1 To Len(sLine)
01548              sChar = Mid(sLine, lcount, 1)
01549
01550              ' If we found " '" then an even number of " characters in front
01551              ' means it is the start of a comment, and odd number means it is
01552              ' part of a string
01553              If sChar = "'" And sPrevChar = " " Then
01554                  If lQuoteCount Mod 2 = 0 Then
01555                      sLine = Trim(Left(sLine, lcount - 1))
01556                      Exit For
01557                  End If
01558              ElseIf sChar = """" Then
01559                  lQuoteCount = lQuoteCount + 1
01560              End If
01561              sPrevChar = sChar
01562          Next lcount
01563      End If
01564
01565      CleanUpLine = sLine
01566  End Function
```

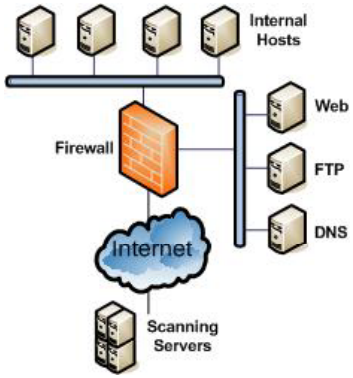
4. Misconfiguration Attacks

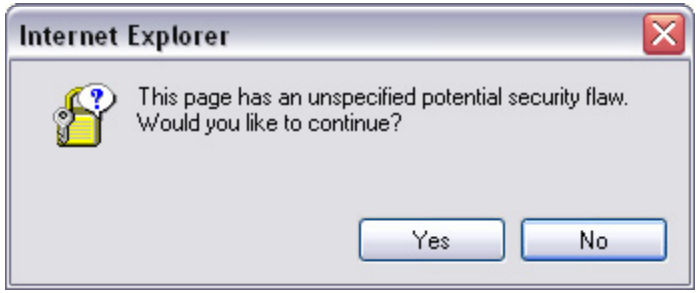
Systems that should be fairly secure are hacked because they were not configured correctly

Systems are complex and the administrator does not have the necessary skills or resources to fix the problem

Administrator will create a simple configuration that works

In order to maximize your chances of configuring a machine correctly, remove any unneeded services or software





Remember This Rule!

If a hacker wants to get inside your system, **he/she will** and there is nothing you can do about it

The only thing you can do is **make it harder** for him to get in

Hacktivism

- Refers to the idea of hacking with or for a cause
- Comprises of hackers with a social or political agenda
- Aims at sending a message through their hacking activity and gaining visibility for their cause and themselves
- Common targets include government agencies, MNCs, or any other entity perceived as bad or wrong by these groups or individuals
- It remains a fact, however, that gaining unauthorized access is a crime, no matter whatever the intention is

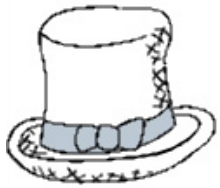
Hacker Classes

Black Hats

- Individuals with extraordinary computing skills, resorting to malicious or destructive activities. Also known as crackers

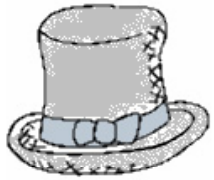
White Hats

- Individuals professing hacker skills and using them for defensive purposes. Also known as security analysts



Gray Hats

- Individuals who work both offensively and defensively at various times



Suicide Hackers

- Individuals who aim to bring down critical infrastructure for a "cause" and do not worry about facing 30 years in jail for their actions

Security News: Suicide Hacker

Army expects 'suicide hacker' attacks

Munir Kotadia, ZDNet Australia
September 28, 2006

Australia is preparing for cyber-terrorism attacks from "suicide hackers", who will aim to bring down critical infrastructure for a "cause" and not worry about facing 30 years in jail for their actions.

So far there have been no major acts of cyber-terrorism -- where hackers take down parts of the critical infrastructure by breaking into power, water, transport or even air traffic control systems -- but the subject has been discussed a great deal.

On Tuesday, Colonel Paul Straughair, the director of network centric warfare at the Australian Army and part of the Australian Department of Defence, said he saw "no logical reason" why suicide hackers would not strike in the future.

"We see suicide bombers that are prepared to die for their cause. I don't think it is too far before we start to see people who are quite prepared to conduct cyber-terrorism.

"While the risk will be high that they will be caught, they will accept that as a fact of life for 'the cause' and be prepared to go to prison for 30 years because they stopped a banking system working or a power grid taken down or took down the air traffic control system of a country for a period of time," Straughair told *ZDNet Australia*.

The suicide hacker scenario was possible but unlikely, according to Jo Stewart-Rattray, director of information security at Vectra, who said she found it hard to believe that someone would be willing to spend 30 years in prison for "a cause".

"We know hackers are getting bolder and bolder and it is possible that someone would do that ... but it sounds like an unlikely scenario," she said.

According to Stewart-Rattray, there was now a heightened awareness of cyber-terrorism, which would make it harder to cause chaos than it would have done a few years ago.

"When I was working in critical infrastructure -- even after 9/11 -- I would hear engineers say 'but it is only engineering data, who would care'. I think that attitude has greatly changed," Stewart-Rattray told *ZDNet Australia*.

However, she admitted that if a hacker was determined and patient enough and really didn't care about getting caught, it would be possible to "create havoc".

"It would have to be a really planned attack and it may well be about infiltrating the system where somebody would actually be in there as a 'trusted' member of staff.

Source: *http://www.zdnet.com.au/*

Ethical Hacker Classes

Former Black Hats

- Reformed crackers
- First-hand experience
- Lesser credibility perceived

White Hats

- Independent security consultants (may be groups as well)
- Claim to be knowledgeable about black hat activities

Consulting Firms

- Part of ICT firms
- Good credentials

What Do Ethical Hackers Do

"If you know the enemy and know yourself, you need not fear the result of a hundred battles"

– Sun Tzu, *Art of War*

Ethical hackers try to answer the following questions:

- What can the intruder see on the target system? (*Reconnaissance and Scanning phases*)
- What can an intruder do with that information? (*Gaining Access and Maintaining Access phases*)
- Does anyone at the target notice the intruders' attempts or successes? (*Reconnaissance and Covering Tracks phases*)

If hired by any organization, an ethical hacker asks the organization what it is trying to protect, against whom, and what resources it is willing to expend in order to gain protection

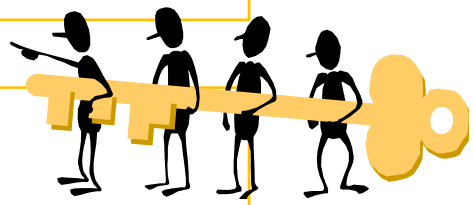
Can Hacking be Ethical

Hacker:

- Refers to a person who enjoys learning the details of computer systems and to stretch his/her capabilities

Cracker:

- Refers to a person who uses his hacking skills for offensive purposes



Hacking:

- Describes the rapid development of new programs or the reverse engineering of the already existing software to make the code better and more efficient

Ethical hacker:

- Refers to security professionals who apply their hacking skills for defensive purposes

How to Become an Ethical Hacker

To become an ethical hacker, you must meet the following requirements:

- Should be proficient with programming and computer networking skills
- Should be familiar with vulnerability research
- Should have mastery in different hacking techniques
- Should be prepared to follow a strict code of conduct

Skill Profile of an Ethical Hacker

A computer expert adept at technical domains

Has in-depth knowledge of target platforms, such as Windows, Unix, and Linux

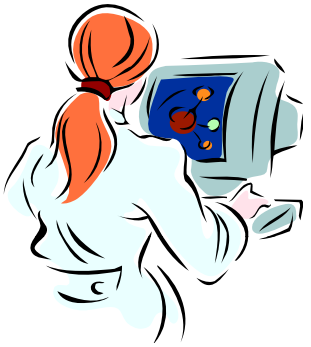
Has exemplary knowledge of networking and related hardware and software

Knowledgeable about security areas and related issues

In other words, you must be “highly technical” to launch sophisticated attacks

What is Vulnerability Research

Discovering vulnerabilities and designing weaknesses that will open an operating system and its applications to attack or misuse



Includes both dynamic study of products and technologies and ongoing assessment of the hacking underground

Relevant innovations are released in the form of alerts and are delivered within product improvements for security systems

Can be classified based on:

- Severity level (low, medium, or high)
- Exploit range (local or remote)

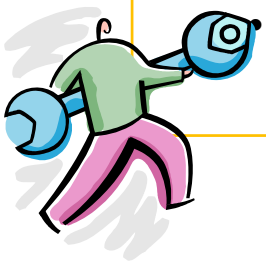
Why Hackers Need Vulnerability Research

- To identify and correct network vulnerabilities
- To protect the network from being attacked by intruders
- To get information that helps to prevent security problems
- To gather information about viruses
- To find weaknesses in the network and to alert the network administrator before a network attack
- To know how to recover from a network attack

Vulnerability Research Tools

US-CERT publishes information regarding a variety of vulnerabilities in "US-CERT Vulnerabilities Notes"

- Similar to alerts but contains less information
- Does not contain solutions for all the vulnerabilities
- Contains vulnerabilities that meet certain criteria
- Contains information that is useful for the administrator
- Vulnerability notes can be searched by several key fields: name, vulnerability ID number, and CVE-name
- Can be cross checked with the Common Vulnerabilities and Exposures (CVE) catalog



Vulnerability Research Websites

- www.securitytracker.com
- www.microsoft.com/security
- www.securiteam.com
- www.packetstormsecurity.com
- www.hackerstorm.com
- www.hackerwatch.org
- www.securityfocus.com
- www.securitymagazine.com

National Vulnerability Database (nvd.nist.gov)

Securitytracker (www.securitytracker.com)

Keep Track of the *Latest* Vulnerabilities with SecurityTracker!

Home | View Topics | Search | Contact Us | Help |

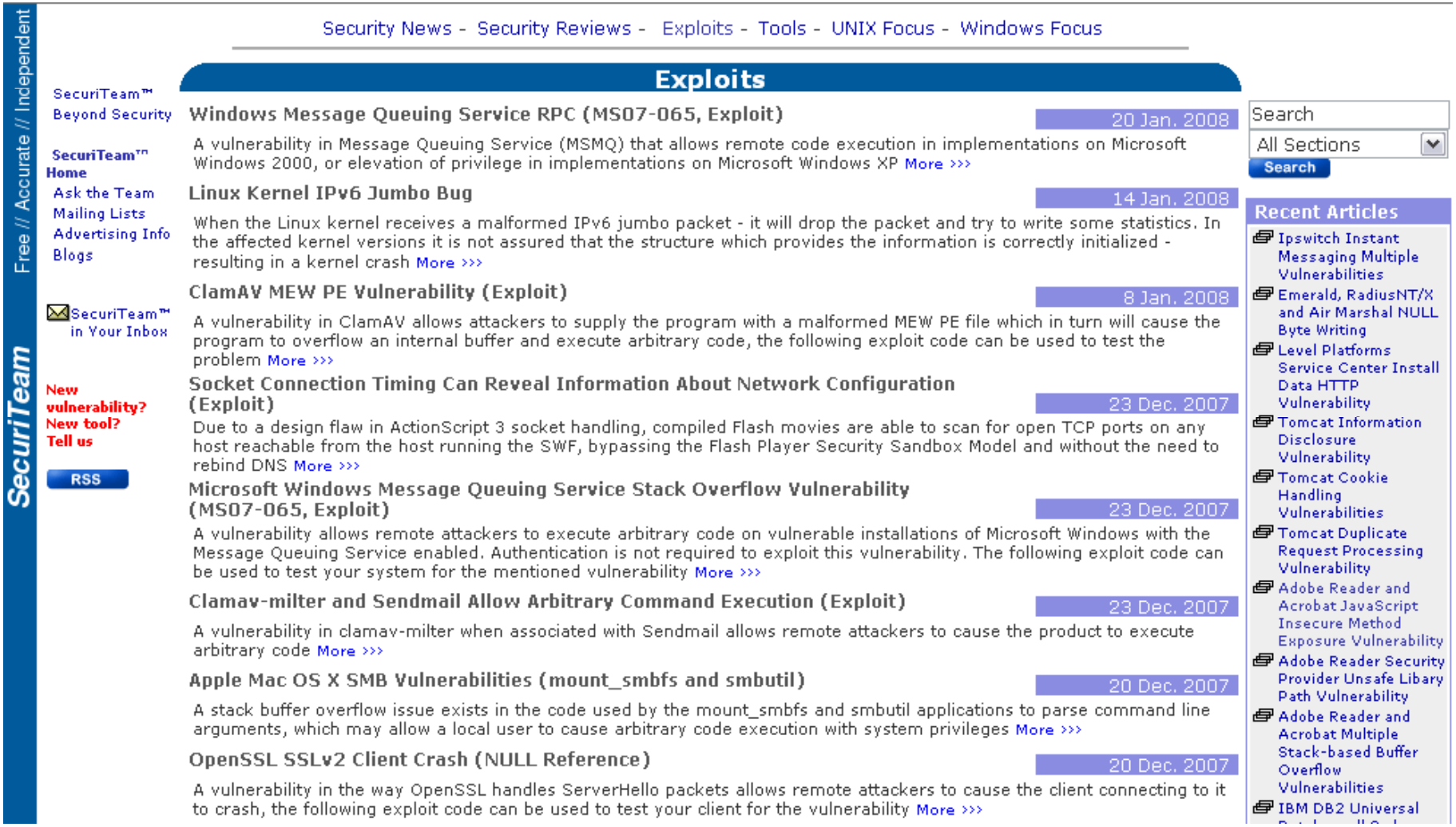
View Topics > Summary > All Primary Archived Entries

Showing Results - Page: 1 of 164

Previous Page | Next Page | First Page (1) | Last Page (164)

Feb 8 2008	Symantec Ghost Solution Suite Authentication Bug Lets Remote Users Execute Arbitrary Code
Feb 8 2008	Adobe Reader Stack Overflows, Insecure Methods, Unsafe Library Path, and Other Bugs Let Remote Users Execute Arbitrary Code
Feb 8 2008	Mozilla Firefox Lets Remote Users Obscure Web Forgery Dialog Warnings.
Feb 8 2008	Mozilla Firefox Stylesheet Processing Bug May Let Remote Users Obtain URL Parameters
Feb 8 2008	Mozilla Firefox Lets Remote Users Prevent the Browser From Opening Local Plain Text Files in Certain Cases
Feb 8 2008	Mozilla Firefox Lets Remote Users Tamper with Security Dialogs
Feb 8 2008	Mozilla Firefox Lets Remote Web Sites Corrupt the Password Store in Certain Cases
Feb 8 2008	Mozilla Firefox Lets Remote Users Steal the Focus to Obtain Keystrokes
Feb 8 2008	Mozilla Firefox chrome: URI Directory Traversal Bug Lets Remote Users Load Local Files
Feb 8 2008	Mozilla Firefox designMode Frames May Let Remote Users Obtain Information and Potentially Execute Arbitrary Code
Feb 8 2008	Mozilla Firefox JavaScript Bugs Let Remote Users Conduct Cross-Site Scripting Attacks and Execute Arbitrary Code
Feb 8 2008	HP Select Identity Lets Remote Authenticated Users Gain Access
Feb 8 2008	Mozilla Firefox Bugs in JavaScript Engine Let Remote Users Execute Arbitrary Code
Feb 8 2008	Mozilla Firefox Bugs in Browser Engine Let Remote Users Execute Arbitrary Code
Feb 8 2008	IBM DB2 Alternate Path Bug Lets Local Users Gain Root Privileges
Feb 8 2008	IBM DB2 Universal Database Administration Server Memory Corruption Error Lets Remote Users Execute Arbitrary Code
Feb 7 2008	Check Point VPN-1 SecuRemote/SecureClient Auto Local Logon Feature Lets Local Users Authenticate as Other Users
Feb 7 2008	WordPress XML-RPC Bug Lets Remote Users Edit Arbitrary Posts
Feb 7 2008	IBM WebSphere Edge Server Input Validation Hole in CGI Mapping Error Page Permits Cross-Site Scripting Attacks

Securiteam (www.securiteam.com)



Free // Accurate // Independent

SecuriTeam

Security News - Security Reviews - Exploits - Tools - UNIX Focus - Windows Focus

SecuriTeam™ Beyond Security

SecuriTeam™ Home
Ask the Team
Mailing Lists
Advertising Info
Blogs

SecuriTeam™ in Your Inbox

New vulnerability? New tool? Tell us

RSS

Exploits

Windows Message Queuing Service RPC (MS07-065, Exploit) — 20 Jan. 2008

A vulnerability in Message Queuing Service (MSMQ) that allows remote code execution in implementations on Microsoft Windows 2000, or elevation of privilege in implementations on Microsoft Windows XP More >>>

Linux Kernel IPv6 Jumbo Bug — 14 Jan. 2008

When the Linux kernel receives a malformed IPv6 jumbo packet - it will drop the packet and try to write some statistics. In the affected kernel versions it is not assured that the structure which provides the information is correctly initialized - resulting in a kernel crash More >>>

ClamAV MEW PE Vulnerability (Exploit) — 8 Jan. 2008

A vulnerability in ClamAV allows attackers to supply the program with a malformed MEW PE file which in turn will cause the program to overflow an internal buffer and execute arbitrary code, the following exploit code can be used to test the problem More >>>

Socket Connection Timing Can Reveal Information About Network Configuration (Exploit) — 23 Dec. 2007

Due to a design flaw in ActionScript 3 socket handling, compiled Flash movies are able to scan for open TCP ports on any host reachable from the host running the SWF, bypassing the Flash Player Security Sandbox Model and without the need to rebind DNS More >>>

Microsoft Windows Message Queuing Service Stack Overflow Vulnerability (MS07-065, Exploit) — 23 Dec. 2007

A vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Microsoft Windows with the Message Queuing Service enabled. Authentication is not required to exploit this vulnerability. The following exploit code can be used to test your system for the mentioned vulnerability More >>>

Clamav-milter and Sendmail Allow Arbitrary Command Execution (Exploit) — 23 Dec. 2007

A vulnerability in clamav-milter when associated with Sendmail allows remote attackers to cause the product to execute arbitrary code More >>>

Apple Mac OS X SMB Vulnerabilities (mount_smbfs and smbutil) — 20 Dec. 2007

A stack buffer overflow issue exists in the code used by the mount_smbfs and smbutil applications to parse command line arguments, which may allow a local user to cause arbitrary code execution with system privileges More >>>

OpenSSL SSLv2 Client Crash (NULL Reference) — 20 Dec. 2007

A vulnerability in the way OpenSSL handles ServerHello packets allows remote attackers to cause the client connecting to it to crash, the following exploit code can be used to test your client for the vulnerability More >>>

Search
All Sections
Search

Recent Articles

- Ipswitch Instant Messaging Multiple Vulnerabilities
- Emerald, RadiusNT/X and Air Marshal NULL Byte Writing
- Level Platforms Service Center Install Data HTTP Vulnerability
- Tomcat Information Disclosure Vulnerability
- Tomcat Cookie Handling Vulnerabilities
- Tomcat Duplicate Request Processing Vulnerability
- Adobe Reader and Acrobat JavaScript Insecure Method Exposure Vulnerability
- Adobe Reader Security Provider Unsafe Libary Path Vulnerability
- Adobe Reader and Acrobat Multiple Stack-based Buffer Overflow Vulnerabilities
- IBM DB2 Universal

Secunia (secunia.com/product/)

Secunia monitors vulnerabilities in more than 9,500 products

Secunia
Stay Secure

Verified Vulnerability Intelligence
where it matters.

Home | Corporate Website | Jobs | Mailing Lists | RSS | Blog | Advertise | Search

Solutions For
- Security Professionals
- Security Vendors

Free Solutions For
- Open Communities
- Journalists & Media

Software Inspectors
- Scan Online
- Personal (PSI) Get it
- Network (NSI)

Secunia Advisories
- Search
- Historic Advisories
- Listed By Product
- Listed By Vendor
- Statistics / Graphs
- Secunia Research
- Report Vulnerability
- About Advisories

Virus Information

Secunia Advisories by Product

Below you will find a complete index of software and operating systems currently in the Secunia database. Our database currently includes **16,976** pieces of software and operating systems.

New software and operating systems are added to our database on a daily basis, through software suggestions from customers and vulnerability reports affecting new software.

Select a letter below for a complete list of products.

Operating Systems and Hardboxes (1,119)

0-9 (24)	N (135)	
A (107)	O (26)	
B (38)	P (28)	
C (136)	Q (2)	
D (44)	R (35)	
E (31)	S (136)	
F (43)	T (28)	
G (11)	U (17)	
H (54)	V (9)	
I (40)	W (25)	
J (22)	X (6)	
K (1)	Y (2)	
L (34)	Z (9)	
M (76)		

Software (15,857)

0-9 (113)	N (680)	
A (1,335)	O (345)	
B (570)	P (1,203)	
C (1,277)	Q (153)	
D (676)	R (444)	
E (603)	S (1,667)	
F (581)	T (596)	
G (478)	U (195)	
H (497)	V (408)	
I (787)	W (646)	
J (175)	X (218)	
K (206)	Y (59)	
L (387)	Z (131)	
M (1,413)		

Secunia PSI
Scan | Patch | Track
Free Download

Secunia Poll

Have your organisation taken any extraordinary steps to remediate the Microsoft Windows URI vulnerability?

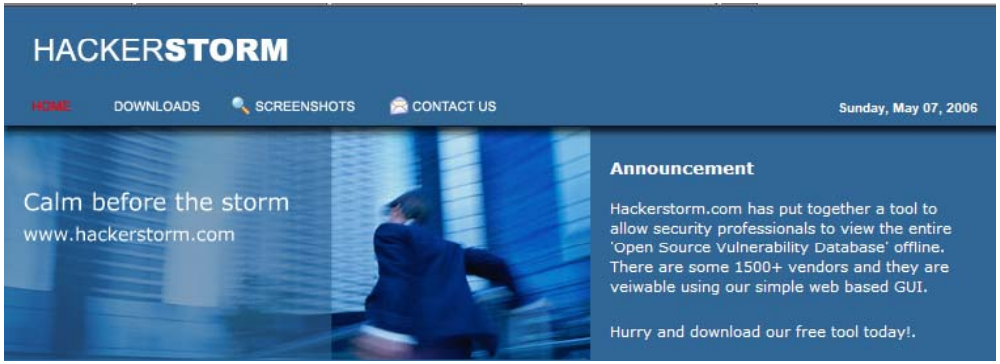
- Yes
- No
- No, we're not affected

See Results | Vote!

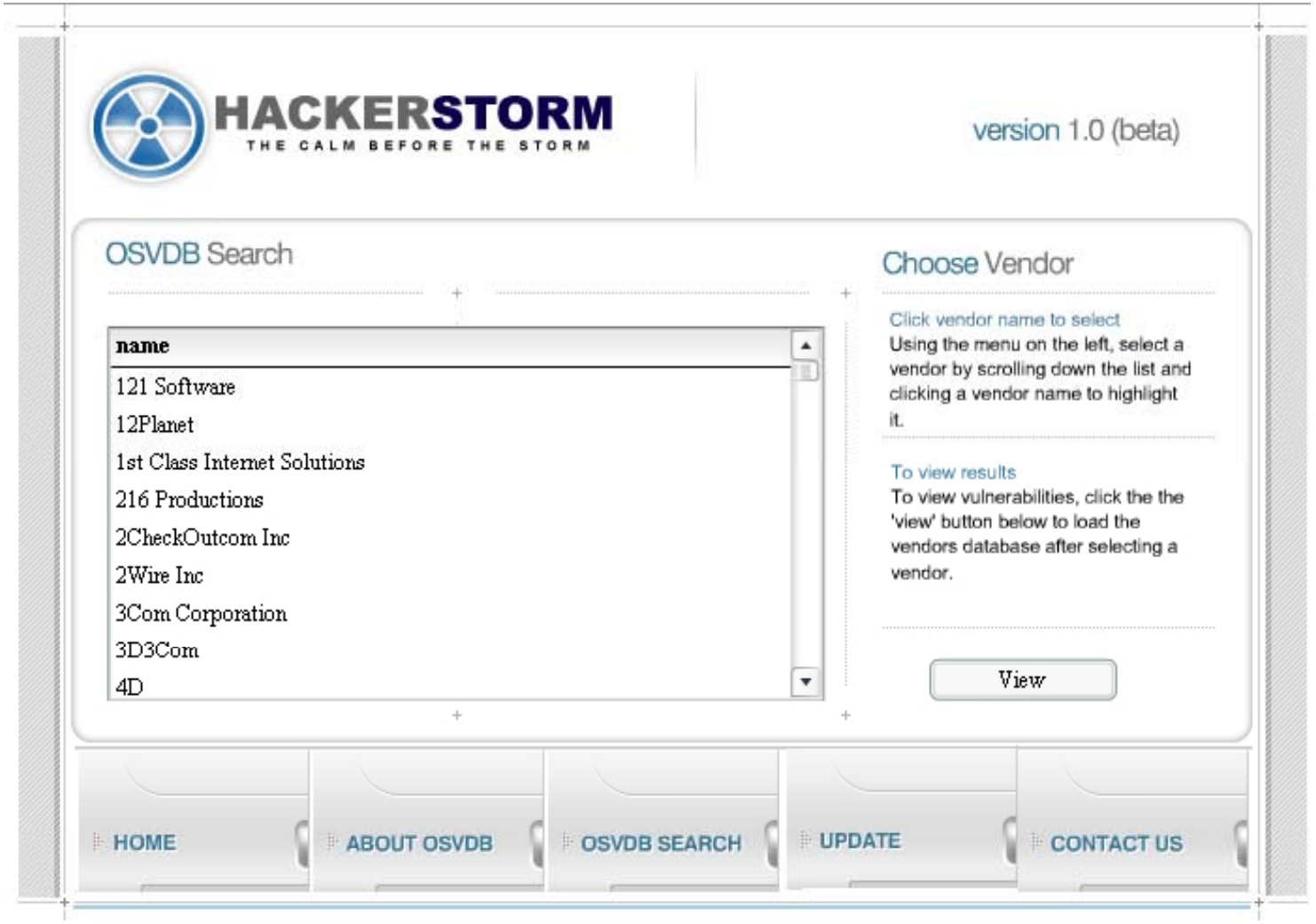
Hackerstorm Vulnerability Database Tool (www.hackerstorm.com)

You can search CVS Vulnerability database using this tool

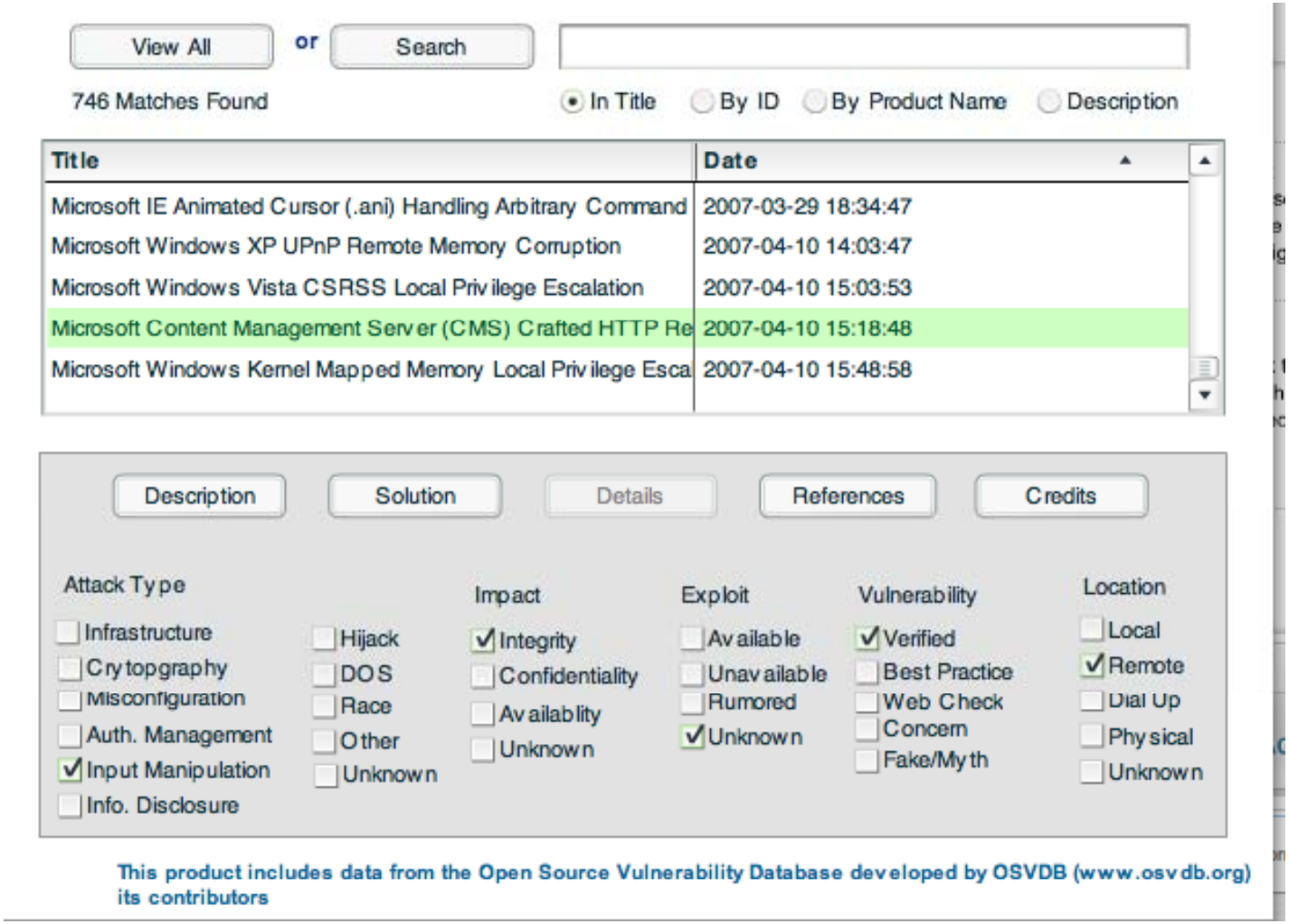
- Updates provided daily and are free
- You can view vulnerability database offline (without Internet access)
- Easy to use Web-based GUI; requires a browser with flash
- Data includes description, solution, attack type, external references, and credit
- Source is available for those who wish to contribute and enhance the tool
- Data is provided by www.osvdb.org and its contributors



Hackerstorm Vulnerability Database: Screenshot 1



Hackerstorm Vulnerability Database: Screenshot 2



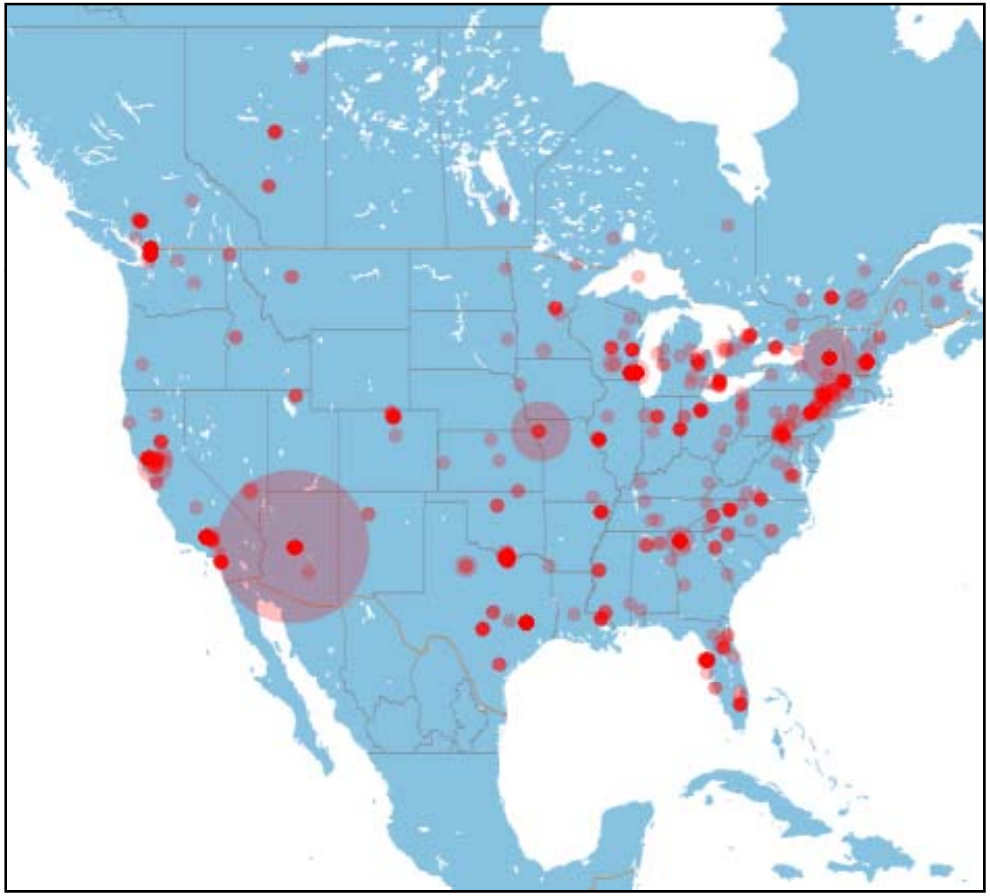
HackerWatch
(www.hackerwatch.org)

HackerWatch lets you report and share information that helps to identify, combat, and prevent the spread of Internet threats and unwanted network traffic

HackerWatch provides reports and graphical up-to-date snapshots of unwanted Internet traffic and threats

Snapshots include critical port incidents graphs, worldwide port activity statistics, and target and source maps showing unwanted traffic and potential threats to Internet security

HackerWatch



Recent Port Activity

Top event ports reported to HackerWatch during the past 5 days

Event Tracking

Significant incidents recently reported to HackerWatch.org

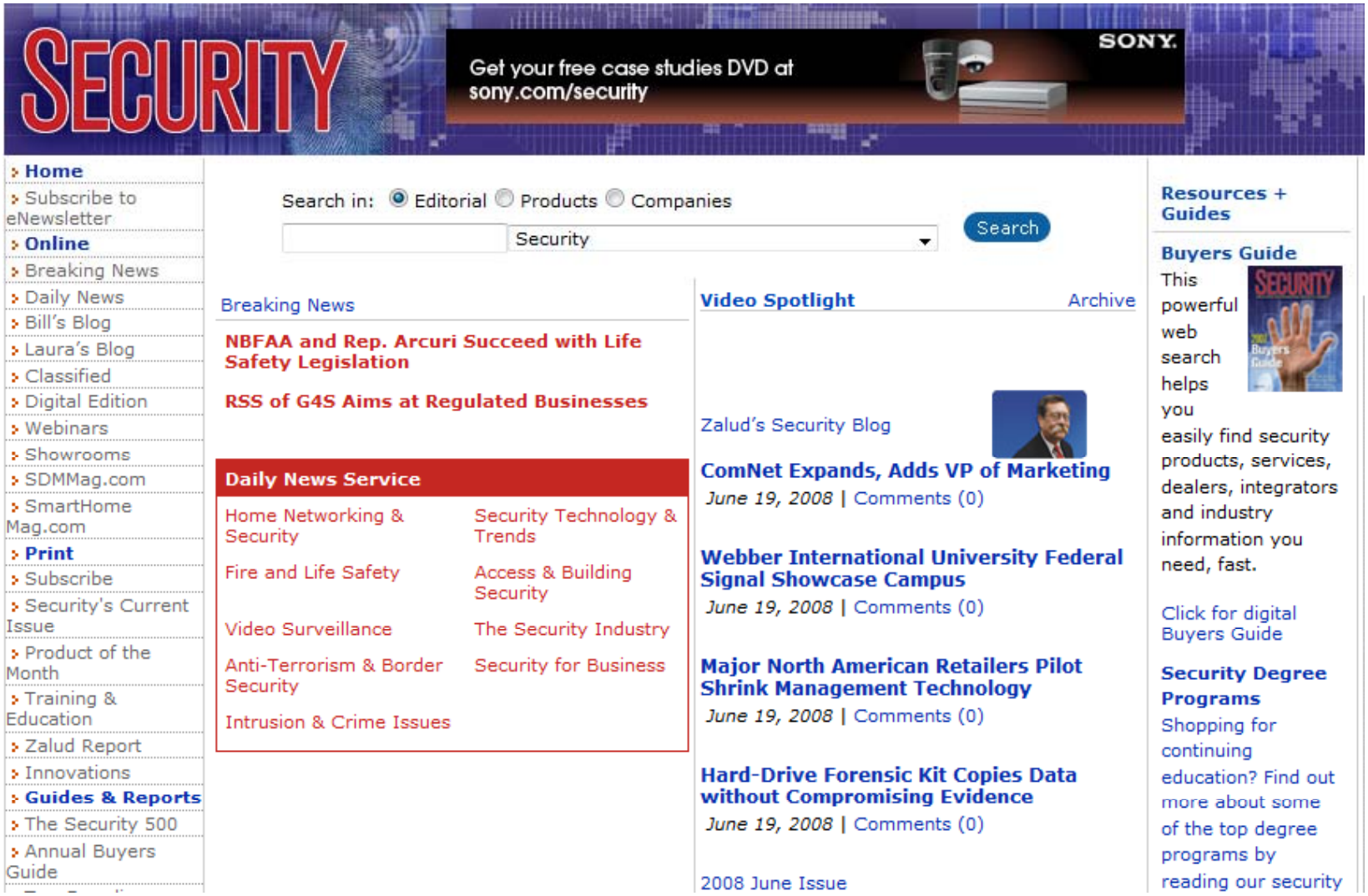
24 Hours	78,541,667
7 Days	547,791,660
30 Days	2,356,379,550

w32/Lovsan

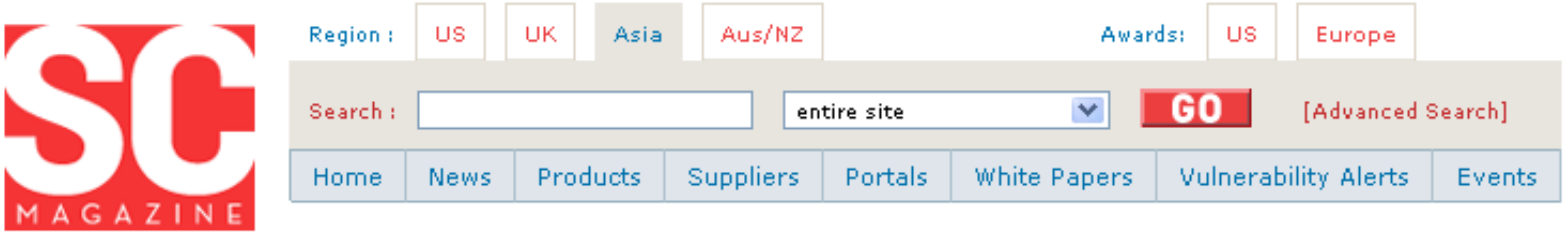
Special information on the recent Lovsan RPC-Worm outbreak

SecurityFocus
www.securityfocus.com

SecurityMagazine
www.securitymagazine.com



SC Magazine
www.scmagazine.com



You are here: SC Magazine Asia > Vulnerability Alerts

VULNERABILITY ALERTS

CERT/CC

US-CERT Cyber Security Alerts provide timely information about current security issues, vulnerabilities, and exploits. Cyber Security Alerts are released in conjunction with Technical Cyber Security Alerts when there is an issue that affects the general public. Cyber Security Alerts outline the steps and actions that non-technical home and corporate computer users can take to protect themselves from attack.

More threats from CERT/CC

- SA07-226A: Microsoft Updates for Multiple Vulnerabilities

  Microsoft Updates for Multiple Vulnerabilities.

- SA07-199A: Mozilla Updates for Multiple Vulnerabilities

  Mozilla Updates for Multiple Vulnerabilities.

- SA07-193A: Apple Releases Security Updates for QuickTime

  Apple Releases Security Updates for QuickTime.

MILWORM

[home] [contents] [platforms] [shellcode] [search] [cracker] [links] [rss] [archive]

MILWORM

[remote]

-::DATE	-::DESCRIPTION	-::HITS				-::AUTHOR
2008-02-10	ImageStation (SonyISUpload.cab 1.0.0.38) ActiveX BOF Exploit	350	R		D	X Elazar
2008-02-09	Microsoft DirectSpeechSynthesis Module Remote Buffer Overflow Exploit	1792	R		D	X rgod
2008-02-07	SapLPD 6.28 Remote Buffer Overflow Exploit (win32)	1967	R		D	BackBone
2008-02-07	Backup Exec System Recovery Manager <= 7.0.1 File Upload Exploit	1362	R		D	titon
2008-02-06	dBpowerAMP Audio Player Release 2 M3U File Buffer Overflow Exploit	1544	R		D	securfrog
2008-02-03	Yahoo! JukeBox MediaGrid ActiveX mediagrid.dll AddBitmap() BOF Exploit	2650	R		D	X Elazar

[local]

-::DATE	-::DESCRIPTION	-::HITS				-::AUTHOR
2008-02-09	Linux Kernel 2.6.23 - 2.6.24 vmsplice Local Root Exploit	9131	R		D	qaaz
2008-02-09	Linux Kernel 2.6.17 - 2.6.24.1 vmsplice Local Root Exploit	42952	R		D	qaaz
2008-02-07	Total Video Player 1.20 M3U File Local Stack Buffer Overflow Exploit	821	R		D	fl0 fl0w
2008-02-01	Total Video Player 1.03 M3U File Local Buffer Overflow Exploit	1573	R		D	fl0 fl0w
2008-01-29	Safenet IPSecDrv.sys <= 10.4.0.12 Local kernel ring0 SYSTEM Exploit	1872	R		D	mu-b
2008-01-28	IrfanView 4.10 .FPX File Memory Corruption Exploit	2010	R		D	Marsu

[web apps]

-::DATE	-::DESCRIPTION	-::HITS				-::AUTHOR
2008-02-10	Mix Systems CMS (parent/id) Remote SQL Injection Exploit	752	R		D	halkfild
2008-02-10	PacerCMS 0.6 (last_module) Remote Code Execution Vulnerability	586	R		D	GoLd_M
2008-02-10	SAPID CMF Build 87 (last_module) Remote Code Execution Vulnerability	535	R		D	GoLd_M
2008-02-10	ITechBids 6.0 (detail.php item_id) SQL Injection Vulnerability	542	R		D	SoSo H H
2008-02-10	PKs Movie Database 3.0.3 XSS / SQL Injection Vulnerabilities	603	R		D	H-T Team
2008-02-09	Mambo Component Comments <= 0.5.8.5g SQL Injection Vulnerability	1174	R		D	CheebaHawk215

How to Conduct Ethical Hacking

Step 1: Talk to your client on the needs of testing

Step 2: Prepare NDA documents and ask the client to sign them

Step 3: Prepare an ethical hacking team and draw up schedule for testing

Step 4: Conduct the test

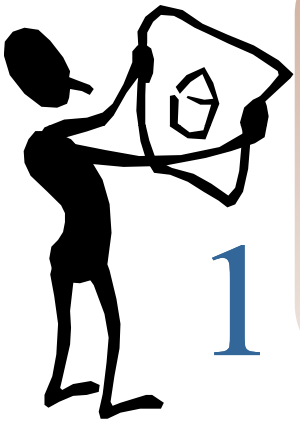
Step 5: Analyze the results and prepare a report

Step 6: Deliver the report to the client

Note: In-depth Penetration Testing methodology is covered in EC-Council's LPT program

How Do They Go About It

Any security evaluation involves three components:

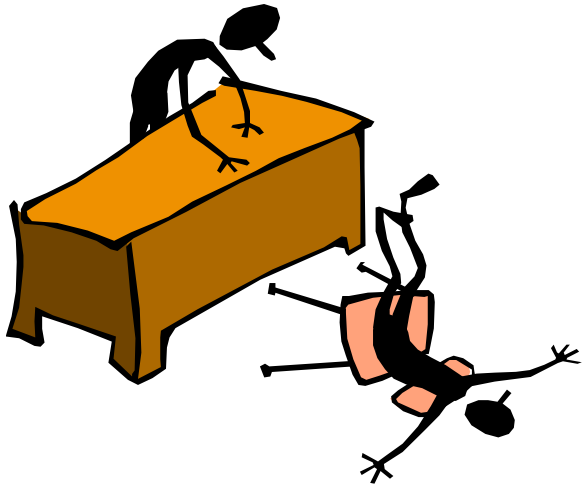


1

Preparation – In this phase, a formal contract is signed that contains a non-disclosure clause as well as a legal clause to protect the ethical hacker against any prosecution that might otherwise attract during the conduct phase. The contract also outlines infrastructure perimeter, evaluation activities, time schedules, and resources available to him

Conduct – In this phase, the evaluation technical report is prepared based on testing potential vulnerabilities

2



3

Conclusion – In this phase, the results of the evaluation are communicated to the organization or sponsors and corrective action is taken if needed

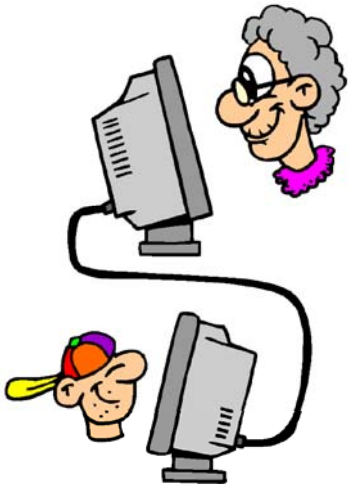
Approaches to Ethical Hacking

Remote network:

- This approach attempts to simulate an intruder launching an attack over the Internet

Remote dial-up network:

- This approach attempts to simulate an intruder launching an attack against the client's modem pools



Local network:

- This approach simulates an employee with legal access gaining unauthorized access over the local network

Approaches to Ethical Hacking (cont'd)

Stolen equipment:

- This approach simulates theft of a critical information resource, such as a laptop owned by a strategist that was taken from its owner and given to the ethical hacker

Social engineering:

- This approach attempts to check the integrity of the organization's employees

Physical entry:

- This approach attempts to physically compromise the organization's ICT infrastructure

Ethical Hacking Testing

There are different forms of security testing. Examples include vulnerability scanning, ethical hacking, and penetration testing

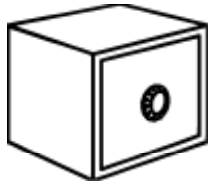
Approaches to testing are shown below:

Black box

- With no prior knowledge of the infrastructure to be tested

White box

- With a complete knowledge of the network infrastructure



Gray box

- Also known as Internal Testing. It examines the extent of the access by insiders within the network

Ethical Hacking Deliverables

An Ethical Hacking Report:

- Details the results of the hacking activity, matching it against the work schedule decided prior to the conduct phase
- Vulnerabilities are detailed and prevention measures are suggested. It is usually delivered in hard copy format for security reasons

Issues to consider:

- Team, sensitivity of information, Nondisclosure clause in the legal contract (availing the right information to the right person), integrity of the evaluation

Computer Crimes and Implications

Computer Crime & Intellectual Property Section
United States Department of Justice

Home | Computer Crime | Intellectual Property | Electronic Evidence | Other High Tech Legal Issues | About CCIPS

News | Site Index | Search

Computer Crime & Intellectual Property Section

Statement of Andrew Lourie, Acting Principal Deputy Assistant Attorney General and Chief of Staff, Criminal Division, Concerning "Privacy and Cybercrime Enforcement Act of 2007" (December 18, 2007)

Latest Press Releases

- Three Indicted and Arrested in One of the Largest Counterfeit Goods Prosecutions in U.S. History: Infringed Goods Valued at More Than $100 Million (January 17, 2008)
- Former St. Cloud Hospital Employee Pleads Guilty to Planting "Logic Bomb" on Hospital Computer (January 10, 2008)
- Foreign National Pleads Guilty in Complex Computer Fraud Scheme Victimizing Hundreds of Individuals (January 9, 2008)
- Four Minnesota Residents Charged in California with Scheme to Defraud Cisco of Computer Networking Equipment: Defendant Fraudulently Conspired to Obtain over $400,000 in Equipment From Cisco under the SMARTnet Service Contract Program (January 9, 2008)
- Former Systems Administrator Gets 30 Months in Prison for Planting

Hot Documents

- How to Report Cyber and IP Crime
  - How to Report Computer- and Internet-Related Crime
  - How to Report Intellectual Property Crime
- NPR Interview with CCIPS and FBI: Cyber Sleuths Zero In as Web Fraud Takes Toll (January 20, 2008)
- Digital Forensic Analysis Methodology Flowchart (PDF) (August 22, 2007)
- New Manual, "Prosecuting Computer Crimes" Now Available (March 2007)
- New Edition of "Prosecuting Intellectual Property Crimes" Manual Available (October 2006)

Computer Crimes and Implications (cont'd)

The Cyber Security Enhancement Act of 2002 mandates life sentences for hackers who recklessly endanger the lives of others

The CSI/FBI 2002 Computer Crime and Security Survey noted that 90 percent of respondents acknowledged security breaches, but only 34 percent reported the crimes to law enforcement agencies

The FBI computer crimes squad estimates that between 85 and 97 percent of computer intrusions are not even detected

What Happened Next

Even though Jeffrey's intention was honest, his action is considered illegitimate.

Hacking into networks without prior permission of concerned authorities and a legal clearance from the court of law, is considered a criminal offence

Summary

- Security is critical across sectors and industries
- Ethical Hacking is a methodology to simulate a malicious attack without causing damage
- Hacking involves five distinct phases
- Security evaluation includes preparation, conduct, and evaluation phases
- Cyber crime can be differentiated into two categories
- U.S. Statutes ξ 1029 and 1030 primarily address cyber crime

"First I searched for Larry in Yahoo, then Lycos, Excite and Infoseek. Eventually, I found him in the bathroom."

"I think he's ready to start using the computer. He just said 'Google'!"