Les Attaques en Réseau sous Linux

www.udivers.com

Plan
□ □ □ □ □

Introduction Partie 1: ARP Spoofing Partie 2: Outils de simulation. Partie 3: Démonstration de l'attaque. . Partie 4: Prévention et détection de

□

l'attaque. Partie 5: Pratique de l'attaque

www.udivers.com

www.udivers.com

Introduction sur les attaques
Les attaques réseaux s'appuient en général sur des vulnérabilités liées à la conception des protocoles de communication, ou liées à leur implémentation. Un pirate pourra exploiter ces vulnérabilités pour lire, modifier ou bloquer la communication entre deux systèmes en contournant les mécanismes de sécurité en place

www.udivers.com

www.udivers.com

Introduction sur les attaques
Outre la mise en place de pare-feux et de systèmes d'authentification de plus en plus sécurisés, il est nécessaire, pour compléter cette politique de sécurité, d'avoir des outils de surveillance pour auditer le système d'information et détecter d'éventuelles intrusions.

www.udivers.com

www.udivers.com

Les Différents types d'attaques
□

Une « attaque » est l'exploitation d'une faille d'un système informatique (système d'exploitation, logiciel ou bien même de l'utilisateur) à des fins non connues par l'exploitant du systèmes et généralement préjudiciables. Sur internet des attaques ont lieu en permanence, à raison de plusieurs attaques par minute sur chaque machine connectée. Ces attaques sont pour la plupart lancées automatiquement à partir de machines infectées (par des virus, chevaux de Troie, vers, etc.), à l'insu de leur propriétaire. Plus rarement il s'agit de l'action de pirates informatiques.

www.udivers.com

www.udivers.com

1) Anatomie d'une attaque :

***Probe *Penetrate *Persist *Propagate *Paralyze**

www.udivers.com

www.udivers.com

2) Les attaques réseaux :

Ce type d'attaque se base principalement sur des failles liées aux protocoles ou à leur implémentation. Les RFC1 ne sont parfois pas assez spécifiques, et un choix particulier

d’implémentation dans les différents services ou clients peut entraîner un problème de sécurité. Observons quelques attaques bien connues

www.udivers.com

Les techniques de scan

Le scan simple : aussi appelé le scan connect(), il consiste à établir une connexion TCP complète sur une suite de ports. S’il arrive à se connecter, le port est ouvert ; sinon, il est fermé. Cette méthode de scan est très facilement détectable.

www.udivers.com

Le scan furtif : aussi appelé scan SYN, il s’agit d’une amélioration du scan simple. Ce scan essaie également de se connecter sur des ports donnés, mais il n’établit pas complètement la connexion : pas de commande ACK (acquittement) après avoir reçu l’accord de se connecter. Grâce à ceci, la méthode est bien plus furtive que le scan normal.

www.udivers.com

Le scan à l’aveugle : s’effectue via une machine intermédiaire et avec du spoofing Le système attaqué pense que le scan est réalisé par la machine intermédiaire et non par le pirate.

www.udivers.com

Le scans passif : est la méthode la plus furtive. Consiste à analyser les champs d’en-tête des paquets (TTL, ToS, MSS, …) et les comparer avec une base de signatures qui pourra déterminer les applications qui ont envoyé ces paquets.

www.udivers.com

Spoofing

L'usurpation d'adresse IP (en anglais : IP address spoofing) est une technique de hacking consistant à utiliser l'adresse IP d'une machine, ou d'un équipement, afin d'en usurper l'identité. Elle permet de récupérer l'accès à des informations en se faisant passer pour la machine dont on spoofe l'adresse IP. De manière plus précise, cette technique permet la création de paquets IP avec une adresse IP source appartenant à quelqu'un d'autre.

www.udivers.com

□

Déroulement : il existe des utilitaires qui permettent de modifier les paquets IP ou de créer ses propres paquets (ex : hping2). Grâce à ces utilitaires, il est possible de spécifier une adresse IP différente de celle que l'on possède, et ainsi se faire passer pour une autre « machine »

www.udivers.com

Source routing : technique consistant à placer le chemin de routage directement dans le paquet IP. Cette technique ne fonctionne plus de nos jours, les routeurs rejetant cette option. Reroutage : cette technique consiste à envoyer des paquets RIP aux routeurs afin de modifier les tables de routage. Les paquets avec l'adresse spoofée seront ainsi envoyés aux routeurs contrôlés par le pirate et les réponses pourront être également reçues par celui-ci.

www.udivers.com

ARP Spoofing

www.udivers.com

ARP Spoofing (usurpation)
1) Protocole ARP
□

□

□

□

Une machine source qui voudra communiquer avec une autre destination sur le réseau a besoin de savoir son adresse physique. Elle diffuse donc une requête de la forme «qui a l'adresse IP X.X.X.X». chaque machine sur le réseau va examiner la requête et va voir s'elle a cette adresse IP. La machine avec l'adresse X.X.X.X va répondre avec son adresse physique. Pour minimiser le nombre de requête ARP diffusée sur le réseau, le système d'exploitation garde une cache ARP sous forme de table de correspondance entre les adresses physiques et les adresses IP et lorsque la machine reçoit une nouvelle réponse ARP, elle va mettre à jour cette table.

www.udivers.com

□

La vulnérabilité du protocole ARP vient du fait qu'il ne garde pas l'état des requêtes/réponses ARP envoyées et reçues. Et la plupart des systèmes d'exploitation (sauf Solaris) vont mettre à jour leur cache dés la réception d'une réponse ARP, mis à part si cette réponse corresponde à une requête déjà formulée ou pas.

www.udivers.com

17

2)L'attaque «Empoisonnement du cache ARP».ARP pour la redirection des paquets Cette attaque utilise la cache vers un pirate.

□ □

□

La machine de pirate pourra capturer donc tout le trafic qui passe entre une machine victime et une autre cible en utilisant un simple renifleur comme Tcpdump ou Ethereal et ceci même dans le cas d'un réseau avec commutateurs. Le pirate commence par envoyer des réponses ARP sous la forme de «l'adresse IP de cible corresponde à l'adresse physique du pirate». Ceci va forcer la mise à jour du cache de la machine victime. De cette façon le trafic envoyé à la machine cible va être redirigé vers la machine du pirate. L'objectif du pirate est capturer le trafic et pas interrompe la communication. Il va donc activer l'acheminement IP sur sa machine, et de cette façon le trafic pourra continuer son chemin vers la cible.

www.udivers.com

18

2.1 Outils de simulation.

□

□

Pour simuler l'attaque d'empoisonnement du cache ARP, nous allons utiliser le générateur de réponse ARP « arpspoof » qui est un programme de la suite des outils Dsniff. Dsniff est une collection d'outils pour auditer un réseau et effectuer des tests **d'intrusion** et pourra être téléchargé à partir du site http://naughty.monkey.org/~dugsong/dsniff/.

www.udivers.com

19

2.2 Démonstration de l'attaque.

□

Concéderons le réseau de la figure 2.2, la machine de pirate, victime et cible ont comme adresses IP, 192.168.0.200, 192.168.0.100 et 192.168.0.102 respectivement.

www.udivers.com

20

□

Le pirate voudra que le trafic transite par sa machine, il doit donc activer le réacheminement IP sur sa machine.

www.udivers.com

21

□

□

Avant de lancer l'attaque, il faut s'assurer que la communication entre les deux machine Victime et Cible est directe, et ne passe pas par la machine du pirate, ou par une autre machine. On exécute donc la commande traceroute à partir de la machine victime vers la machine Cible

www.udivers.com

Le tableau 2.1 montre la cache ARP de cette machine. Elle montre la correspondance entre l'adresse IP et l'adresse physique des deux machines, Cible et Pirate.

Machine Cible Hacker

Adresse IP 192.168.0.102 192.168.0.200

Adresse Physique 00:0C:29:9E:10: 54 00:0C:29:65:79:F 2

www.udivers.com

Pour avoir une idée sur ce que se passe au niveau de la machine Victime, on va capturer le trafic sur cette machine en utilisant la commande tcpdump. Le pirate a comme objectif la capture de la communication VictimeCible. Démarrons donc l'outil « arpspoof » sur la machine du pirate.

www.udivers.com

La figure 3.6 montre la capture sur la machine Victime. On remarque que à chaque deux secondes un message IS-AT est envoyé à la victime, qui confirme que l'adresse physique de la station Cible (192.168.0.102) est l'adresse physique de la machine du pirate (00:0C:29:65:79:F2).

www.udivers.com

Pour s'assurer que la machine Victime a accepté le message IS-AT, on affiche le contenu de sa table ARP. La figure 2.7 montre la table ARP de cette machine, on remarque bien que les deux adresses IP de la cible et du pirate correspondent à la même adresse physique. Ceci veut dire que la machine Victime va utiliser la machine (00:0C:29:21:96:7E du pirate) pour communiquer avec la machine Cible.

www.udivers.com

Pour s’assurer que le trafic destiné à la machine Cible passe bien par la machine du pirate, on va exécuter la commande traceroute vers la machine Cible.

www.udivers.com

□

□

□

On voit bien –figure 2.8- que les paquets de la commande traceroute passent via la machine (192.168.0.200) qu’est la machine du pirate. Pour apparaître le grand danger d’une attaque d’empoisonnement du cache ARP, On va capturer le nom d’utilisateur et le mot de passe d’une connexion FTP. Pour se faire nous allons démarrer la capture sur la machine du pirate avec «tcpdump –xX», puis nous allons établir une connexion FTP sur la machine Cible.

www.udivers.com

□

Les Figures 2.9 et 2.10 montre les deux paquets capturés durant la connexion. Le nom d’utilisateur est donc «med» et le mot de passe est «make».

www.udivers.com

www.udivers.com

3 Prévention et détection de l’attaque.

□ □

□

□

L’attaque “empoisonnement du cache ARP” pourra être évitée en utilisant des tables ARP statique sur chaque machine du réseau. Cette solution est efficace mais non pratique.Une autre façon de protection est d’activé la liaison IP/MAC sur le commutateur, ceci permet de lier l’adresse physique de chaque machine sur le réseau avec son adresse IP, cette configuration ne pourra être modifié que par l’administrateur du réseau. Cette attaque pourra être détectée en utilisant un système de détection **d’intrusion** comme Snort. Aussi on pourra trouver sur Internet des outils qui permettent la détection comme ARPwatch.

www.udivers.com

□

La figure 3.1 montre l’affichage de la commande «arpwatch -dN» durant une attaque

d’empoisonnement du cache.

www.udivers.com

□

détection de l’attaque l’empoisonnement du cache par arpwatch. C’est une alerte «flip flop» qui fait référence de changement d’adresse physique dans la cache ARP.

www.udivers.com

4 Pratique

□

Notre cas:dsniff 2.4b1 wget http://www.monkey.org/~dugsong/dsniff/beta/dsniff2.4b1.tar.gz tar zxf dsniff-2.4b1.tar.gz cd dsniff-2.4 ./configure && make && sudo make install

□ □

Dans le cas de package RPM sous Fedora Core 1 et Red Hat Linux 9:

rpm -Uvh http://www.brandonhutchinson.com/dsniff-2.3-1_rh9.i386.rpm

www.udivers.com

4 Installing dsniff 2.3
Note: Vérifier

□

que les RPMs suivants sont déjà installer.

libpcap db4 db4-devel openssl krb5-libs krb5-devel openssl-devel

www.udivers.com

MERCI

www.udivers.com