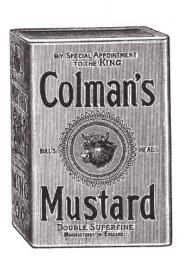
Tests de pénétration internes

Marcin Kurpiewski



Les tests de pénétration internes sont des techniques utilisées pour détecter les failles de sécurité dans les systèmes informatiques. Elles consistent à simuler les actions d'un intrus potentiel. Elles ont donc pour but de refléter des attaques réelles et doivent réunir le plus grand nombre de méthodes connues afin de pénétrer dans les divers systèmes.

es tests de pénétration internes consistent à examiner les réseaux et les systèmes informatiques à l'intérieur de leur environnement de travail. Cette forme de tests permet de simuler la résistance de votre environnement aux attaques dont la source peut provenir des employés ou encore d'autres utilisateurs d'un réseau privé.

Essayons d'effectuer un test de pénétration interne (cf. l'Encadré *Préparation des tests*). Dans notre exemple, le système testé sera FreeBSD version 5.2.1 (l'édition du février 2004). Ensuite, nous testerons le système MS Windows 2003 Server – bien qu'il ne soit pas le système principalement examiné, il est utile de connaître les différences en ce qui concerne les vulnérabilités des services fonctionnant sur les deux serveurs.

Exécution des tests

Après la sélection des outils de test (cf. l'Encadré *Outils utilisés dans les tests*), nous pouvons passer à l'examen du réseau. Dans notre cas, l'ordinateur de test est le portable HP Compaq nx9005 avec la carte réseau externe USB (3Com 3C460) et le système Linux (noyau 2.6.9-rc2) installé, connecté à un commutateur

localisé dans la zone DMZ (en anglais *demilitarized zone* – zone démilitarisée). Un schéma général du réseau examiné et la localisation du testeur sont présentés sur la Figure 1.

Phase préliminaire – recherche des hôtes

La première étape du test est la reconnaissance – il faut connaître les adresses des hôtes travaillant dans le réseau local. Pour ce faire, nous pouvons utiliser un outil interceptant les paquets qui circulent dans le réseau. Le plus pratique est d'intercepter les paquets ARP (*Address Resolution Protocol*), envoyés par les ordinateurs dont le but est de retrouver d'autres machines. Ils

Cet article explique ...

 utilisation des méthodes de tests de pénétration internes.

Ce qu'il faut savoir ...

- utiliser la ligne de commande (CLI) dans les systèmes de la famille Unix,
- les principes de fonctionnement du protocole TCP/IP.

Tests de pénétration

Préparation des tests

Le test de pénétration est une *simulation* des actions de l'intrus – la personne effectuant le test doit donc prévoir le comportement de l'intrus. C'est la raison pour laquelle les tests doivent être relativement agressifs, il est donc recommandé de faire des copies de sécurité des données.

Dans la plupart des cas, les simulations internes sont effectuées par le biais de la méthode de la boîte noire (en anglais *black box*). On admet alors que nous ne connaissons pas la structure et les programmes installés sur les serveurs :

- · officiellement, nous ne connaissons pas le réseau à étudier,
- · nous ne sommes pas administrateur des systèmes à tester,
- un accord pour effecteur les tests nous a été consenti.

Pour les tests, nous allons utiliser les outils recherchant les hôtes vulnérables dans le réseau, les scanners de failles et les programmes capturant les données envoyées via le réseau. Les principales méthodes sont :

- écoute passive sur le réseau (sniffing),
- · recherche des hôtes non protégés scannage de ports,
- · reconnaissance d'un système distant,
- reconnaissance des services réseau,
- interception de transmission des données,
- recherches des failles dans les programmes et les systèmes d'exploitation.

Dans la phase préliminaire, il faut configurer l'ordinateur permettant d'effectuer les tests de façon à ce qu'il utilise le serveur DNS du réseau local pour la résolution des noms. Pour ce faire, il faut ajouter une ligne appropriée dans le fichier /etc/resolv.conf. L'idéal serait que le serveur DNS choisi stocke les noms des hôtes et des serveurs dans ce qu'on appelle la résolution inverse (tuple PTR). La résolution d'adressage des hôtes spécifiques sous la forme canonique peut faciliter les tests du réseau – elle permet de détecter la destination de la machine à travers son nom.

seront peu nombreux mais indiqueront une grosse partie des ordinateurs (pour établir une connection, les machines doivent d'abord communiquer à l'aide d'ARP).

Pour intercepter les paquets ARP, nous utiliserons le programme tcpdump (cf. l'Encadré Outils exploités dans les tests). C'est un outil passif – il n'envoie pas de données sur le réseau, mais il attend les paquets envoyés par d'autres ordinateurs. Le résultat de son fonctionnement n'est donc pas immédiat - nous devons patienter afin d'obtenir les résultats. La liste obtenue peut être longue, cela dépend du nombre d'ordinateurs et du trafic sur le réseau. Mais il peut arriver qu'elle ne contienne pas tous les hôtes (certains d'entre eux peuvent ne pas communiquer avec les autres). Voici le résultat du travail dans un réseau LAN:

```
# tcpdump arp
18:01:25.024801
```

```
arp who-has domain-srv.example.com
tell 192.168.0.13
18:01:25.157800
```

arp reply domain-srv.example.com
is-at 00:04:76:00:D5:B8

Et voici le résultat du fonctionnent de *tcpdump* dans la zone démilitarisée (DMZ) du réseau examiné :

```
# tcpdump arp

18:05:13.157800
arp who-has router.example.com
tell 192.168.1.111

18:05:16.142648
arp who-has mail-srv.example.com
tell 192.168.1.13

18:05:31.063157
arp reply router.example.com
is-at 00:04:C1:D1:DA:46

18:05:32.071232
arp reply mail-srv.example.com
is-at 00:06:1B:DF:36:0B
```

Le résultat de l'écoute permet de supposer que le réseau contient des hôtes dont au moins deux ordinateurs (mail-srv et domain-srv) sont des serveurs, et l'un travaille comme routeur. Maintenant, il faut rechercher les dispositifs sur le réseau qui ne sont pas présents sur la liste et qui peuvent se trouver dans le même segment du réseau. Ce n'est pas difficile – si nous connaissons l'adresse du réseau, nous pouvons le scanner précisément au moyen de Nmap.

Nmap fonctionne en mode actif. Cela signifie qu'il envoie les paquets préparés aux ordinateurs scannés et identifie les hôtes à partir des

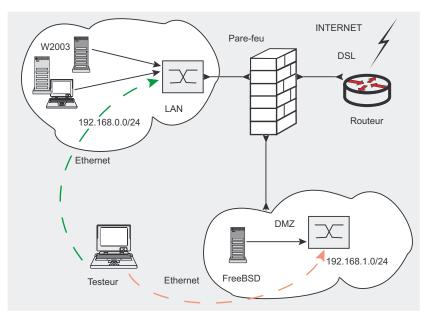


Figure 1. Schéma du réseau soumis aux tests de pénétration