

# Tutorial du workshop de Tunis 2002

## Méthodes de reconnaissance réseau : utilisation et prévention

Elie Bursztein, Julien Olivain

19, 20 septembre 2002

### Table des matières

|  |          |
|--|----------|
| <b>Introduction</b>  | <b>1</b> |
| <b>1 Méthodes de reconnaissance réseau</b>                       | <b>2</b> |
| 1.1 Détection de machines . . . . .                              | 2        |
| 1.1.1 Ping . . . . .   | 2        |
| 1.1.2 Traceroute . . . . .                                       | 2        |
| 1.1.3 DNS query . . . . .  | 3        |
| 1.2 Balayage de services . . . . .                               | 3        |
| 1.2.1 Balayage direct . . . . .                                  | 3        |
| 1.2.2 Balayage furtif . . . . .                                  | 3        |
| 1.2.3 Balayage utilisant un relais . . . . .                     | 3        |
| 1.2.4 Balayage par témoin . . . . .                              | 4        |
| 1.3 Détection de système d'exploitation et de services . . . . . | 4        |
| 1.3.1 Technique passive . . . . .                                | 4        |
| 1.3.2 Techniques actives . . . . .                               | 4        |
| <b>2 Détection et prévention</b>                                 | <b>5</b> |
| 2.1 Détection de la reconnaissance réseau . . . . .              | 5        |
| 2.1.1 Détecter les balayages de machines . . . . .               | 5        |
| 2.1.2 Détecter les balayages de services . . . . .               | 5        |
| 2.1.3 Détecter les prises d'empreintes . . . . .                 | 6        |
| 2.2 Prévention de la détection réseau . . . . .                  | 6        |
| 2.2.1 Empêcher le balayage de machines . . . . .                 | 6        |
| 2.2.2 Empêcher les balayages de services . . . . .               | 6        |
| 2.2.3 Empêcher la prise d'empreinte . . . . .                    | 7        |
| <b>Conclusion</b>  | <b>7</b> |

### Introduction

Avec l'augmentation des interconnexions réseau, la menace sur les réseaux d'entreprises n'est plus seulement locale, elle peut surgir de n'importe où. Avant toute attaque, une phase de reconnaissance est effectuée par les hackers afin de déterminer les cibles et la manière

d'exploiter leurs faiblesses. Il faut donc comprendre les mécanismes sous-jacents mis en oeuvre durant cette phase, afin de pouvoir anticiper les attaques et réduire le champ d'investigation des hackers. Ces techniques peuvent aussi servir à l'administrateur qui a besoin de faire l'état des lieux de son réseau. Ce tutorial présente les différents mécanismes de reconnaissance ainsi que les méthodes visant à rendre celle-ci aussi difficile que possible. La détection de cette activité de reconnaissance se fait au moyen d'un NIDS (Network Intrusion Detector Software).

## 1 Méthodes de reconnaissance réseau

### 1.1 Détection de machines

La première étape consiste à déterminer quelles machines sont connectées. Il s'agit du premier pas vers la connaissance du réseau. Ces informations permettent de cibler les tests sur les machines réellement présentes pour optimiser l'efficacité de la reconnaissance, aussi bien en terme de temps que de trafic. Elles permettent aussi de mettre en évidence la topologie et les différents équipements du réseau tels que les routeurs ou les firewalls.

#### 1.1.1 Ping

Le **Ping()** utilise les paquets ICMP *Echo Request (type 8)* et *Echo Reply (type 0)*. C'est la technique de base pour le diagnostic des réseaux. Il détermine si les machines répondent ou pas. Une variante du **Ping()** utilise le TCP qui permet d'effectuer cette reconnaissance même si la politique de filtrage de paquets ne permet pas le trafic ICMP. Cela permet de déterminer quelles sont les machines qui répondent sur le réseau indépendamment de la politique de filtrage du réseau.

#### 1.1.2 Traceroute

L'inconvénient du **Ping()** est que celui-ci ne permet pas de déterminer la topologie d'un réseau ni de savoir par où transitent les paquets avant d'atteindre l'hôte cible. En utilisant les paquets ICMP *time exceed in traffic*, le **Traceroute()** permet de déterminer les différents routeurs se trouvant avant la machine cible. Son principe repose sur l'existence du champ TTL (Time to Live). Ce dernier évite aux paquets de boucler indéfiniment sur le réseau : ceux-ci ne peuvent effectuer qu'un nombre maximum de sauts (hop en anglais). Lorsque le nombre maximal de sauts est atteint le paquet est abandonné et un message d'échec ICMP *Time Exceed (Type 11)* est retourné à la machine source. Le **Traceroute** consiste donc à envoyer un paquet ayant un TTL de 1 pour obtenir le premier routeur, puis de 2 et ainsi de suite jusqu'à atteindre la machine cible. Il existe différentes variantes de cette méthode pour déclencher la réponse ICMP, le **Traceroute()** peut être totalement ICMP (typiquement sous Windows), soit UDP/ICMP, (Typiquement UNIX) voire même TCP/ICMP. Le **Traceroute()** reverse permet d'identifier les machines par lesquelles transite le trafic retour et d'évaluer si le trafic est symétrique ou non (cette méthode comporte cependant quelques limites car l'enregistrement de route est limité à 9). La généralisation du concept du **Traceroute()** est le **Firewalk()** (<http://www.packetfactory.net>) qui permet de déterminer les ACL des firewalls. Dans le cas du **Firewalk()**, on teste successivement tous les ports TCP/UDP, avec pour cible une machine située derrière le firewall évalué et un TTL supérieur de 1 au nombre de sauts

nécessaires pour atteindre ce firewall. Si on a un retour ICMP, le paquet est passé, sinon le port est bloqué. Le Traceroute permet de déterminer la topologie du réseau et d'identifier les routeurs et firewalls.

### 1.1.3 DNS query

Le DNS fournit le mécanisme de traduction des adresses IP en noms humainement compréhensibles, et inversement. Les noms humainement compréhensibles sont regroupés en domaines et sous domaines, qui correspondent à des zones DNS. Une fois déterminée, la zone DNS qui regroupe le réseau cible, il est intéressant de tenter d'extraire les différents hôtes existants dans cette zone. A l'inverse, en vérifiant si une IP possède une entrée DNS valide, on obtient une indication sur l'existence de cette machine ainsi que sur sa fonction. Il est possible en outre que l'administrateur ait rajouté des informations concernant la machine dans l'enregistrement DNS.

## 1.2 Balayage de services

Après avoir déterminé l'existence d'une machine, il est utile de connaître sa fonction, c'est-à-dire de savoir quels sont les services qu'elle propose. Cette phase est appelée balayage de services (Port scanning en anglais). Avec le temps, différentes méthodes de balayage plus ou moins furtives ont fait leur apparition. Les différents balayages présentés ici sont effectués grâce au scanner bien connu **NMAP()** de Fyodor. (<http://www.insecure.org>)

### 1.2.1 Balayage direct

Le premier type de balayage mis en oeuvre est le test des ports ouverts en TCP avec la fonction **connect()** Unix. Cela reste à ce jour l'une des techniques les plus furtives. Ce balayage utilise un trafic normal et ne peut donc pas faire l'objet d'une signature de détecteur d'intrusion. Seule une analyse temporelle permet de révéler une tentative de balayage. Cependant si le balayage est distribué ou très lent, il devient extrêmement difficile, parfois impossible à voir. C'est en outre le seul à ne pas nécessiter les droits super utilisateur (root)

### 1.2.2 Balayage furtif

Les balayages furtifs sont de deux types :

- ceux faisant appel à des paquets standards, c'est-à-dire conformes à un trafic normal
- ceux utilisant des paquets anormaux, donc non conformes à un trafic normal

Les différentes méthodes présentées :

- Half-Open scan
- Null scan
- Fin scan
- Xmas scan

### 1.2.3 Balayage utilisant un relais

Afin de dissimuler la machine effectuant le balayage réseau ou pour déjouer certaines règles de Firewall, il est possible d'utiliser des machines faisant tourner certains services pour relayer le balayage. Parmi ces services :

- FTP
- IDENT
- Socks
- Proxy HTTP

Avantage : l'IP de la machine attaquante est totalement masqué.

#### 1.2.4 Balayage par témoin

Le dernier type de balayage présenté est le balayage par témoin, qui utilise comme relais une machine ayant un défaut d'implémentation du champ IP ID (Typiquement un Windows). Cela permet de masquer totalement l'IP de la machine attaquante à la machine cible. L'avantage est que cette technique ne nécessite la présence d'aucun service sur la machine utilisée comme relais.

### 1.3 Détection de système d'exploitation et de services

Une fois qu'on a déterminé les services ouverts, il faut connaître le type de machine et de services auxquels on a affaire afin d'évaluer les vulnérabilités pouvant exister sur ces services. Il existe de nombreux types d'implémentation des différents services. Par exemple, pour le FTP on dénombre plus de 10 types de serveurs différents : (**PureFTPD**, **ProFTPD**, **IIS**, **WarFTPD**, **WU-FTPD**...). Les vulnérabilités dépendent aussi du système d'exploitation de la machine car les exploits (programmes permettant d'exploiter les vulnérabilités) sont généralement écrits pour une architecture spécifique. Pour le système d'exploitation des machines on distingue deux types de techniques : la technique passive et les techniques actives. Ces techniques s'appuient toutes sur la différenciation des machines grâce à la spécificité de l'implémentation de leur pile TCP/IP.

#### 1.3.1 Technique passive

Cette technique consiste à utiliser un sniffer qui regarde le trafic passant sur le brin réseau. En examinant les en-têtes des paquets, il reconnaît le système distant. Pour connaître le type d'un hôte précis on peut être amené à générer du trafic vers cet hôte : on se retrouve donc dans le cas d'une technique active.

#### 1.3.2 Techniques actives

Les techniques actives sont plus efficaces que la technique passive. Cependant, elles requièrent la génération d'un trafic. Celui-ci peut faire l'objet d'une signature, donc être détecté.

**Récupération de bannières** La plus ancienne des méthodes consiste à se connecter sur les ports ouverts et à regarder les en-têtes des services. C'est la seule technique connue pour déterminer de manière fiable le service qui tourne. Quelques subtilités permettent de contourner certaines falsifications des bannières.

**Prise d'empreinte TCP** Cette technique se base sur 9 tests (dans la version **NMAP()** de ce type de prise d'empreinte) et permet en utilisant des paquets non standards de déterminer de manière relativement fiable le système d'exploitation de la machine cible. L'inconvénient

est que certains paquets utilisés étant non standards cette prise d’empreinte est facilement détectable.

**Prise d’empreinte ICMP** Cette technique se base sur un maximum de 5 tests ICMP, et permet de déterminer de manière plus précise que la prise d’empreinte TCP le système d’exploitation de la machine cible. Le trafic ICMP étant généralement bloqué, cette méthode peut s’avérer inefficace. N’utilisant que des paquets standards, elle est difficilement détectable.

**Temps de retransmission TCP** La plus récente des méthodes se caractérise par son extrême furtivité : un seul paquet SYN est nécessaire pour déterminer le système distant.

## 2 Détection et prévention

### 2.1 Détection de la reconnaissance réseau

Parce que la reconnaissance réseau annonce généralement une attaque, il est important de pouvoir la détecter, et d’être alerté pour pouvoir réagir avant que l’incident ne se produise. Pour la surveillance des réseaux les N.I.D.S (Network Intrusion Detection Software : Détecteurs d’intrusion réseau) sont le fer de lance de la panoplie de l’administrateur.

#### 2.1.1 Détecter les balayages de machines

Les paquets utilisés pour le balayage des machines sont très caractéristiques, donc facilement détectables. L’important est de faire des corrélations entre les alertes afin de connaître l’ampleur de l’attaque et de savoir si celle-ci est ciblée ou non. Notons que ce type de trafic peut également être légitime quand il est utilisé pour le diagnostic réseau. Ce n’est que grâce aux recoupements entre les différents tests que l’on peut déterminer si ce trafic est légitime, car ciblé sur une machine ou un groupe de machines, ou bien s’il s’agit d’une reconnaissance réseau.

#### 2.1.2 Détecter les balayages de services

Comme dit précédemment, les balayages réseaux sont de deux types : ceux qui utilisent des paquets standards et ceux qui utilisent des paquets non standards. Ceux utilisant des paquets non standards sont détectables grâce à des signatures précises dues à leur nature. Ces paquets étant non conformes aux RFC, ils ne doivent pas transiter sur les réseaux. Ce sont autant de signaux d’une activité frauduleuse pour l’administrateur. Les balayages utilisant des paquets standards posent de nombreux problèmes dus à la faiblesse temporelle des détecteurs d’intrusion. Même si certains détecteurs d’intrusion possèdent des modules pour détecter de tels balayages, ils ont leurs limites. En effet, la seule manière de détecter de tels balayages est de corréliser les différentes tentatives de connexions. Mais la mémoire de la machine est restreinte, on ne peut pas garder indéfiniment trace de toutes les tentatives de connexion. De fait, un balayage lent échappe à coup sûr aux détecteurs d’intrusion car ceux-ci ne gardent trace de toutes les tentatives de connexion que quelques minutes maximum sur les réseaux chargés.

### 2.1.3 Détecter les prises d'empreintes

La détection de prises d'empreintes, à l'instar des balayages de services, peut être classée en deux catégories : les prises d'empreintes qui utilisent des paquets standards et celles qui n'utilisent pas des paquets standards. Si les secondes sont facilement détectables en raison de leur nature non conventionnelle, les premières posent problème pour une détection fiable.

## 2.2 Prévention de la détection réseau

Pour prévenir la détection réseau, il faut généralement intervenir au niveau du firewall, ou bien de chaque machine du réseau. La première solution a l'avantage d'offrir une gestion centralisée de l'implémentation des contre-mesures mises en place.

### 2.2.1 Empêcher le balayage de machines

Comme les balayages de machine emploient des paquets caractéristiques on peut empêcher la plupart des méthodes utilisées. Cependant de telles restrictions sont nuisibles à la bonne marche du réseau, notamment en ce qui concerne le diagnostic des problèmes réseau. Il faut donc s'assurer que quelques mesures simples ont été prises. Par exemple, il est impensable de laisser les adresses de Broadcasts accessibles depuis l'extérieur, d'autant qu'elles peuvent être utilisées pour des dénis de service (Smurf). Les Traceroutes, quant à eux, sont des paquets ayant un TTL de 1, il est donc facile de les interdire, mais toujours au risque de détériorer le diagnostic réseau. Au niveau du D.N.S il faut restreindre le transfert de zones aux serveurs autorisés et ne pas mettre d'informations sur les machines dans les zones.

### 2.2.2 Empêcher les balayages de services

Quelques mesures peuvent rendre hasardeuse la détection des services présents. Ignorer tous les paquets à destination des ports fermés permet de ralentir considérablement les différents balayages, provoquant généralement l'abandon de l'attaquant au bout d'une dizaine de ports. Pour les balayages de type « Half-open », Ignorer les paquets permet que tous les ports fermés apparaissent comme filtrés, rendant l'analyse beaucoup plus difficile, voire impossible dans le cas des services réellement filtrés. Certains balayages peuvent être rendus inopérants. Ainsi les balayages de type Null scan ou Xmas scan peuvent sans problème être filtrés, car de tels paquets ne sont pas conformes aux trafics normaux et n'ont pas de raison d'être. Cependant on ne peut empêcher complètement tous les types de balayage sous peine de ne plus pouvoir fournir de services. Le balayage utilisant un simple connect() n'est pas différentiable d'une tentative réelle de connexion. La seule manière de filtrer véritablement un tel scan est d'effectuer une analyse temporelle des paquets. Ceci pose les mêmes problèmes que pour la détection. Quelques mesures au niveau des services peuvent être prises pour sécuriser d'avantage le réseau, notamment en vérifiant que les Proxys du réseau ne peuvent pas servir de relais ou ne sont accessibles que depuis les bonnes IP. Par exemple, un serveur de type Proxy HTTP ne doit pas être ouvert sur l'extérieur. De même, certains services - tel le SSH utilisé uniquement par les administrateurs - peuvent être limités à quelques IP externes afin de limiter les risques. Si cette restriction ne peut être mise en place, un système de SKEY est envisageable.

### 2.2.3 Empêcher la prise d’empreinte

Dans certains cas, la prise d’empreinte peut être rendu inopérante par des règles simples de firewall. Elle peut être falsifiée lors de la récupération des bannières ou de la prise d’empreinte TCP. La prise d’empreinte utilisant la retransmission TCP fait elle appel à un mécanisme plus complexe afin de pouvoir la déjouer.

## Conclusion

Rendre son réseau le moins ouvert possible à la reconnaissance est une nécessité fondamentale en matière de politique de sécurité. Si les attaquants ne peuvent déterminer ce qu’ils attaquent, ils sont moins efficaces. Une détection de l’attaque dès la reconnaissance permet de prendre des mesures préventives plutôt que curatives.