L'idle host scan

Ghosts In The Stack
http://www.ghostsinthestack.org

Heurs

Résumé

C'est une technique qui n'est pas toute jeune mais qui est loin d'etre démodée. Elle permet de faire un scan de ports TCP sur une machine, mais la machine ciblée croit que c'est une autre personne que vous qui la scanne. Ainsi anonymat quasiment garanti ;)

Table des matières

1 IPID et incrémentation

Pour ceux qui ne le savent pas, un paquet TCP est composé d'au moins deux protocoles : l'IP et le TCP. Ce sont deux protocoles bien distincts. Sur l'IP on peux par exemple monter un protocole de couche supérieure, par exemple ICMP, UDP, IGMP etc...

Quand votre ordinateur reçoit deux paquets de facon trés raprochée, il faut bien qu'il arrive a déterminer quel paquet à été envoyé en premier. Une chance pour nous, le protocole IP à un champ prévu pour numéroter les paquets, il s'appelle l'IPID !

L'IPID est par défaut incrémenté à chaque paquet (envoyer) de facon régulière, nous le voyons dans l'exemple ci-dessous :

```
heurs@GITS:~$ hping 192.168.0.1 -1
HPING 192.168.0.1 (eth0 192.168.0.1): icmp mode set, 28 headers + 0 data bytes
len=46 ip=192.168.0.1 ttl=128 id=62341 icmp_seq=0 rtt=0.4 ms
len=46 ip=192.168.0.1 ttl=128 id=62344 icmp_seq=1 rtt=0.3 ms
len=46 ip=192.168.0.1 ttl=128 id=62347 icmp_seq=2 rtt=0.3 ms
len=46 ip=192.168.0.1 ttl=128 id=62350 icmp_seq=3 rtt=0.3 ms
len=46 ip=192.168.0.1 ttl=128 id=62353 icmp_seq=4 rtt=0.3 ms
len=46 ip=192.168.0.1 ttl=128 id=62356 icmp_seq=5 rtt=0.3 ms
len=46 ip=192.168.0.1 ttl=128 id=62359 icmp_seq=6 rtt=0.3 ms
len=46 ip=192.168.0.1 ttl=128 id=62362 icmp_seq=7 rtt=0.2 ms
len=46 ip=192.168.0.1 ttl=128 id=62365 icmp_seq=8 rtt=0.2 ms
```

```
len=46 ip=192.168.0.1 ttl=128 id=62368 icmp_seq=9 rtt=0.3 ms

--- 192.168.0.1 hping statistic ---
10 packets transmitted, 10 packets received, 0% packet loss
round-trip min/avg/max = 0.2/0.3/0.4 ms
```

Nous pouvons voir trés clairement ici que notre IPID est incrémenté de 3 à chaque paquet. L'incrémentation est donc régulière.

2 Théorie de l'attaque

Le but de cette attaque est que la victime ne puisse jamais voir notre adresse IP, pour se faire le spoofing va etre à l'honneur.

Nous avons vu que l'IPID était incrémenté régulièrement sur cetaines machines, et même la plus part. Dans notre exemple, si nous envoyons des paquets, nous verrons une incrémentation de 3 entre chaque paquet. En revanche, si un autre PC envoie un paquet a cette machine et que celle ci répond, une incrémentation supplémentaire sera due à cette réponse. Et nous nous verrons une incrémentation de 6 au lieu de 3 à un moment.

Vous me suivez ? Alors c'est reparti !

Maintenant regardons les flags de TCP, ou tout du moins les 3 plus importants : SYN, ACK, RST

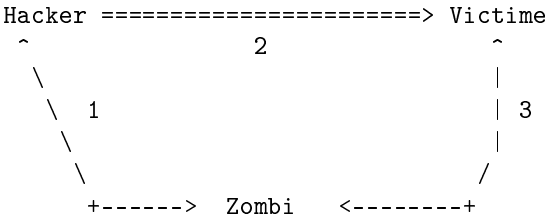
- SYN : Demande l'établissement d'une connection. Généralement le PC distant répond soit par un RST/ACK ou un SYN/ACK (si il accepte et demande donc lui aussi une connexion)
- ACK : C'est ni plus ni moins qu'un accusé de réception (parfois il sert aussi à accepter une communication), en théorie il doit suivre tout les paquets d'une transmition aprés le premier paquet envoyer.
- RST : Stoppe une connection violament. Il demande la coupure de la communication, on peut le trouver quand on essaye d'établir une communication sur un port fermé.

Voici deux exemples de communication classiques :

```
Port ouvert :
Machine A : SYN <====== Demande de connection
Machine B : SYN/ACK <====== B a bien reçu le paquet et demande lui aussi une connexion (la connexion de
Machine A : ACK <====== A à bien recut le packet et accept la connection.

Port fermé :
Machine A : SYN <====== Demande de connection
Machine B : RST/ACK <====== B a bien reçu le paquet et nous informe que le port est fermé.
Machine A : RST <====== A rompt aussi la connection.
```

Rentrons dans le vif du sujet : voici le plan de l'attaque :



Bon ok, ca doit vous paraître un peu brouillon, mais nous allons tout détailler.

Le Pc Zombi doit etre un PC sans activité, comme ca aucun trafic ne viendra perturber notre scan. L'ordre chronologique est le suivant :

- 1 : Hacker ping Zombie pour obtenir son IPID est son icrémentation.
- 2 : Hacker envoie des packets SYN avec l'IP source de Zombi à Victime.
- 3 : Si le port est fermé, Victime renverra un RST/ACK à Zombi. A ce momment là Zombi ne connait pas Victime et vien de recvoir un paquet de sa part... Comme c'est un RST, Zombi ne cherchera pas a comprendre et ne répondra rien.
- Si le port est ouvert, Victime répondra un SYN/ACK, et là Zombi ne connait pas non plus Victime... Comme il y a un SYN et que Zombi n'a jamais demandé d'établissement de connexion il répondra un RST/ACK, donc l'IPID de Zombi aura une incrémentation supplémentaire que nous n'aurons pas vu.
- 1 : Hacker ping Zombi pour obtenir son IPID.

Si entre le 1er et dernier prélevement d'IPID l'incrémentation est régulière, cela veut dire que le port de Victime est fermé. Puisque Zombi n'a pas renvoyé de paquet cela signifie qu'il a reçu un RST/ACK.

Si entre le 1er et dernier prélevement d'IPID l'incrémentation est de deux fois la normale, cela signifie que le port est ouvert. Puisque Zombi aura répondu un RST/ACK cela voudra dire qu'il a recu un SYN/ACK.

3 Mise en pratique

Pour ce faire, nous utiliseront nmap, tout simplement parce qu'il à déja cette option d'implémentée. Il faut utiliser l'option -sI (scan Idle) en mettant en premier argument l'adresse IP du zombi et en deuxième argument l'adresse IP de la victime.

Et voici le démonstration de cette technique (sous Windows, pour changer) :

```
C:\>nmap -sI 192.168.0.184 192.168.0.1
WARNING: Many people use -P0 w/Idlescan to prevent pings from their true IP.  On
 the other hand, timing info Nmap gains from pings can allow for faster, more re
liable scans.

Starting Nmap 4.01 ( http://www.insecure.org/nmap ) at 2006-07-06 18:56 Paris, M
adrid (heure d'ÚtÚ)
Idlescan using zombie 192.168.0.184 (192.168.0.184:80); Class: Incremental
Interesting ports on 192.168.0.1:
(The 1663 ports scanned but not shown below are in state: closed|filtered)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
```

```
445/tcp  open  microsoft-ds
1002/tcp open  windows-icfw
1025/tcp open  NFS-or-IIS
1720/tcp open  H.323/Q.931
3006/tcp open  deslogind
5000/tcp open  UPnP
MAC Address: 00:0E:2E:00:97:0C (Edimax Technology Co.)

Nmap finished: 1 IP address (1 host up) scanned in 147.171 seconds
```

Conclusion

Il est tout a fait possible de scanner sans qu'un pare-feu ne reconnaisse le vrai attaquant, mais les possibilités de ce scan restent trés limitées, donc pas de vrai gros risque ;)

Références

- ouah : un pdf trés pédagogique[1]
- Idle host scan avec uniquement hping, assez interessent.[2]

[1] http://www-src.lip6.fr/homepages/Fabrice.Legond-Aubry/www.ouah.org/idlehostscan.pdf
[2] http://www.ouah.org/hpin2.htm