# DIGITAL NETWORK

| | | |
|---|---|---|
| Siège : 13 chemin de Fardeloup<br>13600 La Ciotat<br>Siret : 43425494200015<br>APE : 722 Z<br>www.digital–network.org<br>www.dnsi.info | | Laboratoires : 120 Avenue du Marin Blanc, ZI Les Paluds,<br>13685 Aubagne<br>www.digital–internetwork.net<br>www.securite–reseaux.net |

## Le Idle Host Scan

**Auteur : Brain Override |Christophe Casalegno | Digital Network**
**http://www.digital–network.org | http://www.dnsi.info**
**http://www.digital–internetwork.net | UIN : 103408553**
**christophe.casalegno@digital–network.org**

**Introduction :** Quel apprenti pirate n'a jamais rêver de pouvoir **scanner** le pentagone sans que jamais son adresse apparaisse ? Quel administrateur n'a jamais angoissé que cela soit possible ? Bien sur il existe une méthode simple... les **proxies anonymes.** Cependant deux inconvénients pour l'attaquant apparaissent.

Un **proxy** est un **relais applicatif**, il ne relaye pas toujours les protocoles souhaités (exception faite pour les **proxies socks**), et de plus, il peut s'agir d'un pot de miel sous contrôle d'un gouvernement ou autre société.

Tous les accès au **proxy** se faisant au niveau applicatif, ils sont loggués dans **98%** des cas. De plus certains retransmettent l'adresse qui est derrière.

Du point de vue de la cible, il est assez facile pour elle de savoir qu'il s'agit d'un **proxy.** Un simple **scan** donnant comme ouvert un port comme 3128, 8080 ou 1080 est en effet révélateur.

L'**idle host scan** va lui beaucoup plus loin....

**Définition :**

L'**idle host scanning** est essentiellement une combinaison de trois techniques :

- L'observation de l'état de la pile TCP/IP d'un hôte.
- Le scan de port
- L'ip spoofing

La combinaison de ces 3 méthodes permet à celui qui le veux de scanner une ou un ensemble de machines, sans dévoiler à sa cible, son identité.

Le principe est en fait relativement simple : **analyser le comportement d'un hôte tiers** dans le but d'**obtenir des informations** sur une cible, sans jamais apparaître directement à la cible.

Les informations, peuvent donc être les **services** tournant sur l'hôte, les **ports ouverts** ou encore dans certains cas, le **système d'exploitation** utilisé. On peut donc obtenir approximativement les même informations que lors d'un scan de port.

Il existe un autre avantage pour le pirate à cette technique. Elle pourra par exemple être utilisée pour scanner une cible à travers un filtre par exemple, à partir d'une machine approuvée.

Avec le **relatif anonymat** qui peut être maintenu pendant l'utilisation de cette méthode, à travers l'utilisation d'une **troisième machine**, voire d'un **ensemble de machines ne se doutant de rien**, ce type de sondage de réseau est **extrêmement difficile a tracer**.

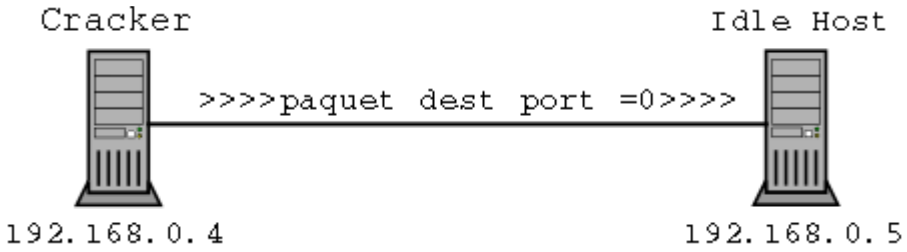
De plus comme pour l'essentiel des attaques, le **pirate** utilisera comme base de lancement de son attaque, un hôte lui même corrompu et sous on contrôle total. L'étude de cette technique par les responsables sécurité, peuvent leur permettre d'augmenter la sécurité de leurs systèmes, et également leur éviter de contacter les mauvaises personnes en cas de problèmes.

**Explications :**

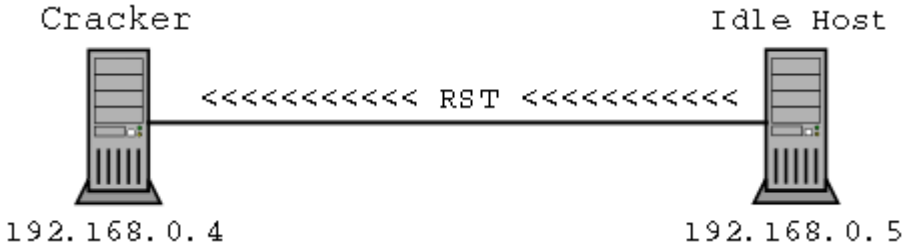
Ceci est un cas réel effectué lors d'un test d'intrusion. Pour des raisons de confidentialité, les vrais IP incriminées ont été remplacés.

| ***Machines*** | ***Cracker*** | ***Idle Host*** | ***Cible*** |
|---|---|---|---|
| ***Système d'exploitation*** | Linux | Routeur cisco | Linux |
| ***Adresse IP*** | 192.168.0.4 | 192.168.0.5 | 192.168.0.6 |

**Phase 1:** La première étape pour l'attaquant est d'envoyer à l'**idle host** des paquets **sans aucun flag** de configuré, à d**estination du port 0.**Ceci va avoir pour effet de mettre le cracker dans l'attente d'un **RST (reset)** de la part de **l'idle host.**

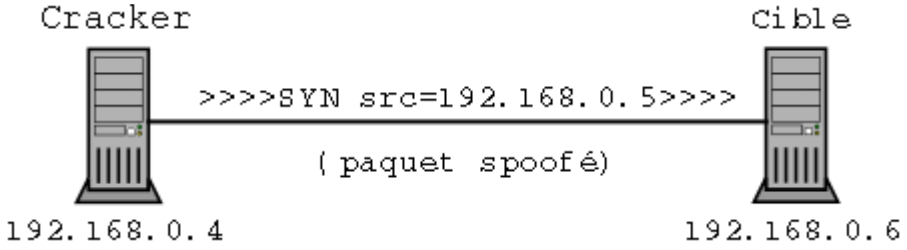



**Phase 2:** Dans la deuxième phase, l'idle host répond à l'attaquant avec un paquet **RST**.

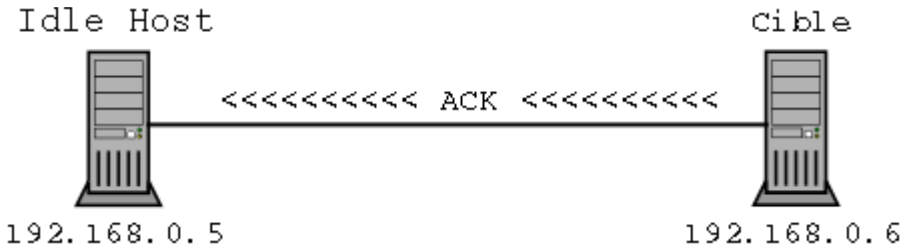



**Phase 3:** Dans la troisième partie de l'attaque, le **cracker** envoie des paquets **SYN** (demande d'ouverture de connexion) **spoofés** à la cible, avec pour adresse d'origine l' **Idle host** soit 192.168.0.5.
Concrètement cela consiste à remplacer le champs **IP source** dans le **paquet envoyé.**

L'**ip source d'origine** serait **192.168.0.4**, elle est **remplacée par 192.168.0.5.** Nous verrons ensuite comment l'on procède dans la pratique.

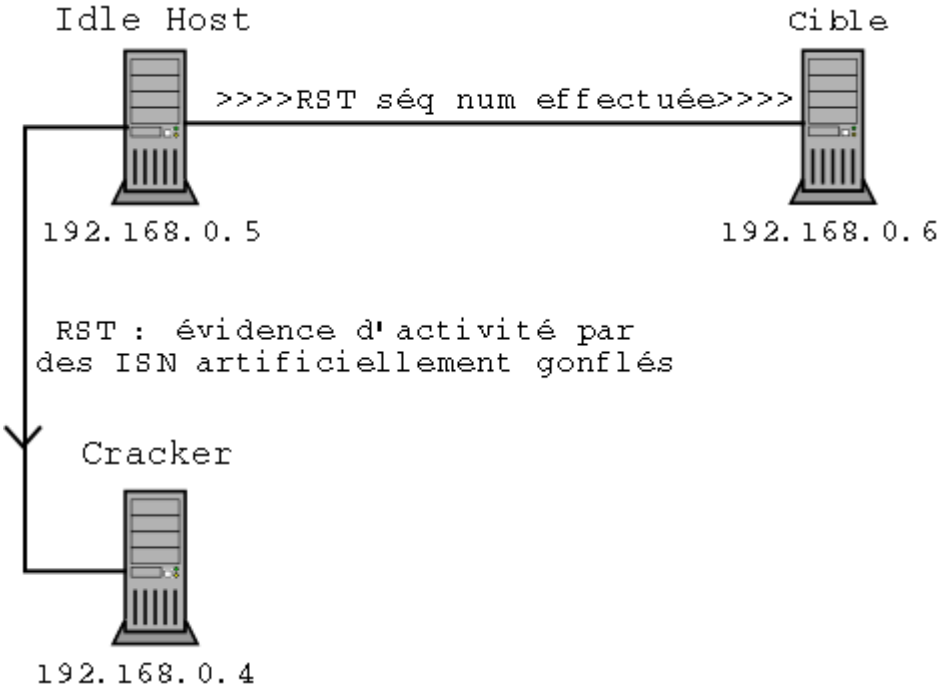


**Phase 4:** Lorsque la cible à répondu aux **paquets spoofés**, et donc, envoyé la réponse à **l'idle host,** la quatrième phase est complète.




**Phase 5:** L'attaquant observe sur une session dédiée la pile TCP/IP de l'idle host en espérant y voir le **reflet des ISN** ( initial sequence number) dans les **paquets RST** que **l'idle host** renvoie**.**

**Implication : L'idle host** envoie des paquets **RST (reset) à la cible pour un ACK (acquittement) inattendu** (il n'y a pas d'**ACK** dans des paquets **RST**)**.** Ces **paquets RST** vont donc **augmenter leurs ISN(numéro de séquence initial) et** donc **augmenter les ISN dans les paquets RST que l'idle host** envoie à l'attaquant**.**




L'attaque est ici réussie. En effet la **génération d'ISN de l'idle host** destiné à l'attaquant à bien été affectée**.** Le pirate sait donc à ce moment, que la cible répond à des **paquets SYN (demande de connexion) spoofés**, envoyés à destination d'un **port particulier**.

Comme la génération des **ISN** de l'idle host est bien affectée**,** cela signifie que le port scanné est bien en écoute sur la cible

Cette méthode de scan dépend fortement de la **prédiction des numéros de séquence générés par l'idle Host** Il existe de nombreux **OS** permettant d'exploiter cette technique (Windows, routeurs)
Pour information cette technique a été essayée avec succès sur plusieurs **routeurs cisco** à travers **Internet.**

Une machine sous un linux récent ou un bsd n'est pas un idle host valide car les **numéros de séquence aléatoires sont générés indépendamment du niveau d'activité.**

Il est étrange que des appareils très utilisés comme des routeurs n'utilisent pas une génération moins prévisible des numéros de séquence.

**Cas pratique**

Les informations suivantes sont une copie directe d'un **Hping idle host scan**, réalisée lors d'un test d'intrusion .

**Ci–dessous est présenté la première étape dans l'attaque, l'initiation d'une session Hping avec l'idle host.**

```
[root@test sbin]# ./hping 195.xxx.xxx.xxx –r –p 513
eth0 default routing interface selected (according to /proc)
HPING 195.XXX.XXX.XXX (eth0 195.xxx.xxx.xxx): NO FLAGS are set,
  40 headers + 0 data bytes
46 bytes from 195.xxx.xxx.xxx: flags=RA seq=0 ttl=243 id=4126 win=0 rtt=25.4 ms
46 bytes from 195.xxx.xxx.xxx: flags=RA seq=1 ttl=243 id=+1 win=0 rtt=24.3 ms
46 bytes from 195.xxx.xxx.xxx: flags=RA seq=2 ttl=243 id=+1 win=0 rtt=24.2 ms
46 bytes from 195.xxx.xxx.xxx: flags=RA seq=3 ttl=243 id=+1 win=0 rtt=24.2 ms
46 bytes from 195.xxx.xxx.xxx: flags=RA seq=4 ttl=243 id=+1 win=0 rtt=23.3 ms
46 bytes from 195.xxx.xxx.xxx: flags=RA seq=5 ttl=243 id=+1 win=0 rtt=22.4 ms
46 bytes from 195.xxx.xxx.xxx: flags=RA seq=6 ttl=243 id=+1 win=0 rtt=25.2 ms
--- 195.xxx.xxx.xxx hping statistic ---
7 packets transmitted, 7 packets received, 0% packet loss
round-trip min/avg/max = 22.4/23.9/25.4 ms
```

On constate que la sortie d'hping est facilement lisible. L'option **–r** sert à montrer uniquement les différences obtenus dans le **champ id**. Cela permet d'obtenir uniquement la différence dans ce champ.

En analysant le **champ id**, l'attaquant va pouvoir déterminer si l'hôte envoie des paquets vers et depuis internet. Si l'on constate que la valeur du **champ id change fréquemment**, et de manière **imprévisible**, l'attaquant pourra en déduire que que l'hôte incriminé effectue des **échanges de paquets**.

La sortie précédente, nous montre que nous avons un hôte relativement inactif. En pleine journée (ce test a été réalisé de nuit), il était un peu plus actif, et il était donc plus dur de s'en servir d'idle host.

Il faut cependant garder a l'esprit que n'importe quel dispositif relié a **Internet** avec une pile **TCP/IP** peut être utilisé de cette manière, que ce soit des stations, des routeurs, des serveurs, des imprimantes, certains appareil réseaux administrables.

A noter que si l'idle host scan est de type windows, la **valeur dans le champ id**, augmente alors d'un **standard + 256** pour chaque paquets envoyés. Dans ce cas l'option de hping **–**W permet de compenser ce comportement qui rendrait moins lisible notre sortie

Pendant que notre session hping tourne encore, nous lançons la commande suivante dans une autre session. Nous décidons de scanner le port 80 de la cible.

```
[root@test sbin]# ./hping -a 195.xxx.xxx.xxx –S –p 80 213.xxx.xxx.xxx
eth0 default routing interface selected (according to /proc)
HPING 213.xxx.xxx.xxx (eth0 213.xxx.xxx.xxx): S set, 40 headers + 0 data bytes
--- 213.xxx.xxx.xxx hping statistic ---
7 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

```
[root@test sbin]# ./hping 195.xxx.xxx.xxx -r -p 513

eth0 default routing interface selected (according to /proc)

HPING 195.xxx.xxx.xxx (eth0 195.xxx.xxx.xxx): NO FLAGS are set,

  40 headers + 0 data bytes

46 bytes from 195.xxx.xxx.xxx: flags=RA seq=0 ttl=243 id=4141 win=0 rtt=20.4 ms

46 bytes from 195.xxx.xxx.xxx: flags=RA seq=1 ttl=243 id=+1 win=0 rtt=20.3 ms

46 bytes from 195.xxx.xxx.xxx: flags=RA seq=2 ttl=243 id=+1 win=0 rtt=20.2 ms

46 bytes from 195.xxx.xxx.xxx: flags=RA seq=3 ttl=243 id=+1 win=0 rtt=20.3 ms

46 bytes from 195.xxx.xxx.xxx: flags=RA seq=4 ttl=243 id=+1 win=0 rtt=20.2 ms

46 bytes from 195.xxx.xxx.xxx: flags=RA seq=5 ttl=243 id=+1 win=0 rtt=22.2 ms

46 bytes from 195.xxx.xxx.xxx: flags=RA seq=6 ttl=243 id=+1 win=0 rtt=18.2 ms

46 bytes from 195.xxx.xxx.xxx: flags=RA seq=7 ttl=243 id=+1 win=0 rtt=20.2 ms

--- 192.168.0.5 hping statistic ---
8 packets transmitted, 8 packets received, 0% packet loss
round-trip min/avg/max = 0.2/0.3/0.4 ms
```

On constate bien que la valeur du champs id ne change pas dans cette session. On peut donc considérer que le port n'est pas ouvert.

Dans le cas ou le port est ouvert, le cheminement est le suivant :

– La cible reçoit les paquets SYN spoofés (ipsrc=idle host).

– La cible répond aux paquets à l'idle host.

– L'idle host reçoit les paquets SYN/ACK, et répond convenablement avec un RST, car il n'a pas fait de demande de connexion FTP.

Dans ce cas, la **génération des paquets RST** auraient modifiés les valeurs dans le schéma de numérotation **id de l'idle host.**

Dans le cas précédent le service questionné n'est donc pas disponible. Si un système de détection d'intrusion (IDS) est disponible sur le réseau, il montrera une tentative de connexion provenant de l'idle host scan. L'administrateur risque donc d'accuser un réseau totalement innocent.

Continuons maintenant notre idle host scan.

L'attaquant envoie des paquets SYN spoofés au port 22 de la cible.

```
[root@test sbin]# ./hping -a 195.xxx.xxx.xxx -S -p 22 213.xxx.xxx.xxx

eth0 default routing interface selected (according to /proc)

HPING 213.xxx.xxx.xxx (eth0 213.xxx.xxx.xxx): S set, 40 headers + 0 data bytes

--- 213.xxx.xxx.xxx hping statistic ---
7 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

L'attaquant surveille donc toujours sa session :

```
[root@test sbin]# ./hping 195.xxx.xxx.xxx -r -p 513

eth0 default routing interface selected (according to /proc)

HPING 195.xxx.xxx.xxx (eth0 195.xxx.xxx.xxx): NO FLAGS are set,

  40 headers + 0 data bytes
```

```
46 bytes from 195.xxx.xxx.xxx flags=RA seq=0 ttl=243 id=5173 win=0 rtt=20.3 ms
46 bytes from 195.xxx.xxx.xxx: flags=RA seq=1 ttl=243 id=+1 win=0 rtt=20.2 ms
46 bytes from 195.xxx.xxx.xxx: flags=RA seq=2 ttl=243 id=+1 win=0 rtt=22.2 ms
46 bytes from 195.xxx.xxx.xxx: flags=RA seq=3 ttl=243 id=+1 win=0 rtt=18.3 ms
46 bytes from 195.xxx.xxx.xxx: flags=RA seq=4 ttl=243 id=+2 win=0 rtt=20.2 ms
46 bytes from 195.xxx.xxx.xxx: flags=RA seq=5 ttl=243 id=+2 win=0 rtt=19.2 ms
46 bytes from 195.xxx.xxx.xxx: flags=RA seq=6 ttl=243 id=+2 win=0 rtt=21.2 ms
46 bytes from 195.xxx.xxx.xxx: flags=RA seq=7 ttl=243 id=+2 win=0 rtt=20.2 ms
46 bytes from 195.xxx.xxx.xxx: flags=RA seq=8 ttl=243 id=+2 win=0 rtt=20.2 ms
46 bytes from 195.xxx.xxx.xxx: flags=RA seq=9 ttl=243 id=+2 win=0 rtt=20.2 ms
46 bytes from 195.xxx.xxx.xxx: flags=RA seq=10 ttl=243 id=+2 win=0 rtt=20.3 ms
46 bytes from 195.xxx.xxx.xxx: flags=RA seq=11 ttl=243 id=+1 win=0 rtt=21.2 ms
46 bytes from 195.xxx.xxx.xxx: flags=RA seq=12 ttl=243 id=+1 win=0 rtt=19.2 ms
46 bytes from 195.xxx.xxx.xxx: flags=RA seq=13 ttl=243 id=+1 win=0 rtt=19.2 ms
46 bytes from 195.xxx.xxx.xxx: flags=RA seq=14 ttl=243 id=+1 win=0 rtt=20.2 ms

--- 195.xxx.xxx.xxx hping statistic ---

15 packets transmitted, 15 packets received, 0% packet loss

round-trip min/avg/max = 18.3/20.2/21.2 ms
```

**La chose la plus importante a noter au sujet des données ci–dessus, est le changement dans le champ id de l'idle host.**

Le pirate peut supposer que les x **paquets SYN spoofés** qui ont été envoyés a la cible, ont bien été reconnus avec x **paquets ACK.** Les **paquets ACK** ont donc été envoyés a **l'idle host, qui en retour renvoie à la cible 7 paquets RST.**

Ces **paquets RST** ont occupé les nombres **id**, qui sont donc reflétés dans la sortie de la session de surveillance maintenue avec l'idle host.

Avec x **paquets spoofés** envoyés, on sait que l'impact sur les valeurs id de l'idle host sont approximativement de x, les données sont fortement révélatrice d'un service offert sur la cible**.** L'attaquant peut donc en déduire que le port es ouvert**.**

Il existe une autre grande utilité à cette attaque, et particulièrement en ce qui nous concerne lors des tests d'intrusion. Admettons le réseau suivant :

Un réseau classique relié à **Internet** par l'intermédiaire d'un **routeur** et protégé par un **firewall**. Soit deux hôtes situés derrière le filtre A et B. A fournit un service public (web par ex) tandis que le **firewall** bloque les accès externes en direction de B**.**

Nous pouvons utiliser la technique de l'**idle host scan** afin de **scanner** la machine B qui est pourtant inaccessible de l'extérieur**.** Grâce à cette technique, nous pouvons scanner cette machine, sans nous soucier du filtre**.** Bien sur ceci ne sera possible que dans certains cas (quand le firewall n'est pas statefull) et dans certaines conditions**.**

Pour finir ajoutons que l'excellent scanner nmap de fyodor (www.insecure.org) incorpore dans ses dernières beta version cette option**.** Il suffit de l'utiliser de la manière suivante :

```
nmap -v -sI idlehost:port cible
```

Même si cela permet aux gens du métier de la sécurité d'utiliser plus facilement cette technique, cela la met maintenant également à la portée du premier venu...

**Christophe Casalegno | Digital Network**
**http://www.digital–network.org | http://www.dnsi.info**
**http://www.digital–internetwork.net | UIN : 103408553**
**CAMPAGNE INTERNATIONALE CONTRE LES PEDOPHILES**
**http://www.bouclier.org/campagne**