

# Étude bibliographique sur les mécanismes réseaux utilisés en cybercriminalité

Gildas Cotten



# Sommaire

- 1 Introduction
- 2 Cartographie du réseau visé par l'attaque
- 3 Écoute du réseau
- 4 Man In The Middle
- 5 Usurpation d'IP et Détournement de session TCP
- 6 Attaques Deny Of Service (DOS)
- 7 Conclusion



# Sommaire

- 1 Introduction
- 2 Cartographie du réseau visé par l'attaque
- 3 Écoute du réseau
- 4 Man In The Middle
- 5 Usurpation d'IP et Détournement de session TCP
- 6 Attaques Deny Of Service (DOS)
- 7 Conclusion

## Contexte

### Sujet

- Étude bibliographique sur les mécanismes utilisés en cybercriminalité
- On s'intéressera uniquement aux aspects réseaux avec les outils utilisés

### Sujet cybercriminalité très médiatisé en 2016-2017

- Élections présidentielle USA : possible attaque qui a permis la divulgation de mails d'Hilary Clinton.
- Objets connectés piratés et utilisés contre les serveurs DNS de DYN aux USA (Amazon, CNN, Ebay, netflix...)

### Multitude de méthodes cybercriminelles

- Cette étude porte sur les attaques réseaux mais il existe beaucoup d'autres méthodes exploitant :
- Les failles humaines, applicatives, liées aux systèmes d'exploitation .



# Sommaire

- 1 Introduction
- 2 Cartographie du réseau visé par l'attaque**
- 3 Écoute du réseau
- 4 Man In The Middle
- 5 Usurpation d'IP et Détournement de session TCP
- 6 Attaques Deny Of Service (DOS)
- 7 Conclusion

# Cartographie

## Récupérer les informations du poste de l'attaquant

- Adresse IP, DNS , DHCP
- Routes

## Découverte du réseau avec ICMP

- ping souvent accepté par les pare-feu
- traceroute

## Effectuer un scan du réseau

- Scan à destination de l'ensemble des postes du réseau.
- Scanner uniquement certains ports TCP
- Utilisation de la commande nmap, d'outils python ou de logiciels comme "look@lan" et "the dude".
- Peut être bloqué par des pare-feu ou même détectés par des Systèmes de Détection d'Intrusion.

## Port scan avec nmap

### Zenmap (nmap graphique) : exemple de ports ouverts sur une freebox

Zenmap

Scan Outils Profil Aide

Cible: 192.168.0.0/24 Profil: Intense scan Scan

Commande: nmap -T4 -A -v 192.168.0.0/24

hôtes Services

OS hôte

- 192.168.0.35
- 192.168.0.46
- 192.168.0.254

Sortie de Nmap Ports / hôtes Topologie Détails de l'hôte Scans

Port	Protocole	Etat	Service	Version
21	tcp	closed	ftp	
80	tcp	open	http	nginx
139	tcp	open	netbios-ssn	Samba smbd 3.X (workgroup: WORKGROUP)
443	tcp	open	http	nginx
445	tcp	open	netbios-ssn	Samba smbd 3.X (workgroup: WORKGROUP)
548	tcp	closed	afp	
554	tcp	open	rtsp	Freebox rtspd 1.2
1723	tcp	closed	pptp	
5000	tcp	open	upnp	
5001	tcp	closed	complex-link	
5678	tcp	open	upnp	fbxigdd 1.1 (AliceBox PM203 UPnP; UPnP 1.0)
6000	tcp	closed	X11	
8090	tcp	open	http	nginx
9091	tcp	open	http	nginx

Filtrer les hôtes

3/3 hôtes visibles Filtre:

# Sommaire

- 1 Introduction
- 2 Cartographie du réseau visé par l'attaque
- 3 Écoute du réseau**
- 4 Man In The Middle
- 5 Usurpation d'IP et Détournement de session TCP
- 6 Attaques Deny Of Service (DOS)
- 7 Conclusion



## Sniffer le réseau

### Utiliser un logiciel de capture de trames

- tcpdump, wireshark.
- "dsnif -i eth0" qui permet d'afficher les login et mot de passe qui passent en clair
- ethercap, cain-abel qui essaye de cracker les mots de passe cryptés
- Des outils spécifiques aux réseaux WIFI (aircrack ...)

### Contre mesures

- Pas de Hub, attention aux switchs manneageable (port mirroring).
- Protocoles sécurisés (SSHV2) plutôt que FTP, telnet...
- Contre les attaques Brute Force (crackage de mots de passe) , choisir mot de passe complexe et le changer régulièrement

## Traversée de routeur

- Les routeurs / pare-feu bloquent les paquets SYN du WAN
- Attaques parfois possibles avec des paquets SYN/ACK , fragmentation ou chevauchement de paquets.

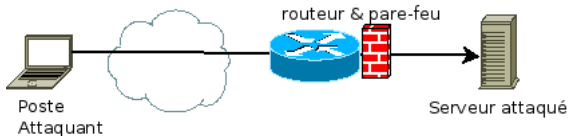


FIGURE: Traversée de routeur pare-feu

Paquet IP	
Fragment 0	Fragment 1
Aucun indicateur SYN ou ACK	Indicateur de connexion SYN sans ACK

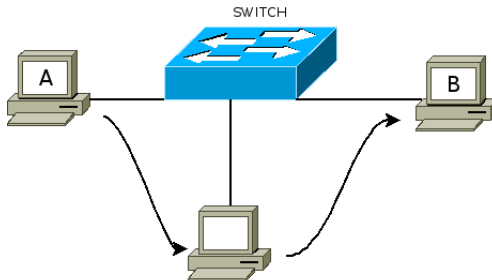
TABLE: Chevauchements de fragments

# Sommaire

- 1 Introduction
- 2 Cartographie du réseau visé par l'attaque
- 3 Écoute du réseau
- 4 Man In The Middle**
- 5 Usurpation d'IP et Détournement de session TCP
- 6 Attaques Deny Of Service (DOS)
- 7 Conclusion

## Man In The Middle

- Le trafic entre A et B est capturé par l'attaquant MITM
- B est un poste du réseau, un routeur du LAN, ou un site Internet



Le Pirate "Man In The Middle"

FIGURE: Exemple d'attaque Man In The Middle.

# Attaques MITM

## ARP POISONING

- Empoisonner le cache ARP de A avec des fausses réponses ARP
- Analyser le trafic entre A et B pour récupérer des login/mot de passe.

## Corruption DNS

- DNS ID Spoofing : se faire passer pour le serveur DNS et faire croire à la victime A qu'on est le serveur B.
- DNS Cache Poisoning : l'attaquant envoie des fausses réponses DNS pour empoisonner le serveur DNS consulté par la victime A.

## Contre-mesures

- arp statique sur les postes, utiliser IPV6 , arpwatsh (sous linux)
- Configurer les DNS locaux pour résoudre les noms dont il a autorité.
- Désactiver le cache DNS sur les postes clients.

# Exemple d'attaque MITM sous Kali Linux.

La victime 10.0.0.1 se connecte sur le serveur 10.0.0.2 sans se rendre compte de la redirection vers le MITM.

The screenshot displays a Kali Linux desktop environment. In the foreground, a terminal window shows the command `root@kali: ~/Documents/python`. Behind it, a network capture window titled "Capturing from eth0" is open, showing a list of captured packets. The packets are filtered by the expression `10.0.0.1`. The capture shows a victim (10.0.0.1) connecting to a server (10.0.0.2) via a MITM (10.0.0.3). The MITM is redirecting traffic from the victim to itself and then to the server. The victim is unaware of the redirection.

No.	Time	Source	Destination	Protocol	Length	Info
249	71.9740848298	10.0.0.1	10.0.0.3	DNS	85	Standard query 0x2468 A teredo.ipv6.microsoft.com.
250	71.974095950	10.0.0.3	10.0.0.1	ICMP	115	Destination unreachable (Port unreachable)
251	73.059937629	Cadmusco_27:06:d4	Cadmusco_4d:e1:24	ARP	42	10.0.0.2 is at 08:00:27:4d:e1:24
252	73.149649735	Cadmusco_27:06:d4	Cadmusco_fc:60:d4	ARP	42	10.0.0.1 is at 08:00:27:27:06:d4 (duplicate)
253	74.691409589	Cadmusco_27:06:d4	Cadmusco_4d:e1:24	ARP	42	10.0.0.2 is at 08:00:27:27:06:d4
254	74.739904414	Cadmusco_27:06:d4	Cadmusco_fc:60:d4	ARP	42	10.0.0.1 is at 08:00:27:27:06:d4 (duplicate)
255	75.418340362	192.168.56.1	192.168.56.255	OS-LSP	247	Droptail LSP sync Discovery Protocol
256	75.549370773	10.0.0.1	10.0.0.2	TCP	60	49197->8000 [SYN] seq=0 win=65536 len=0 MSS=
257	75.549391631	10.0.0.1	10.0.0.2	TCP	60	[TCP out-of-order] 49197->8000 [SYN] seq=0
258	75.549324461	10.0.0.2	10.0.0.1	TCP	60	8000->49197 [SYN, ACK] seq=0 ack=1 win=2920
259	75.549373053	10.0.0.3	10.0.0.2	ICMP	84	Redirect (Redirect for host)
260	75.549785251	10.0.0.2	10.0.0.1	TCP	60	[TCP out-of-order] 8000->49197 [SYN, ACK] S
261	75.550014703	10.0.0.1	10.0.0.2	TCP	60	49197->8000 [ACK] seq=1 ack=1 win=65536 len=
262	75.550038244	10.0.0.1	10.0.0.2	TCP	54	[TCP out-of-order] 49197->8000 [ACK] seq=1
263	75.550330451	10.0.0.1	10.0.0.2	HTTP	395	GET / HTTP/1.1
264	75.550239380	10.0.0.1	10.0.0.2	TCP	395	[TCP Retransmission] 49197->8000 [PSH, ACK]
265	75.550450489	10.0.0.2	10.0.0.1	TCP	60	8000->49197 [ACK] seq=1 ack=332 win=30336
266	75.550477474	10.0.0.2	10.0.0.1	TCP	54	[TCP out-of-order] 8000->49197 [ACK] seq=1
267	75.552051493	10.0.0.2	10.0.0.1	TCP	71	[TCP segment of a reassembled PDU]
268	75.552071313	10.0.0.2	10.0.0.1	TCP	71	[TCP Retransmission] 8000->49197 [PSH, ACK]
269	75.552333042	10.0.0.2	10.0.0.1	HTTP	1328	HTTP/1.0 200 OK (text/html)
270	75.552341529	10.0.0.2	10.0.0.1	TCP	1328	[TCP out-of-order] 8000->49197 [PSH, ACK]

Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0  
Ethernet II, Src: Cadmusco\_27:06:d4 (08:00:27:06:d4), Dst: Cadmusco\_4d:e1:24 (08:00:27:4d:e1:24)  
Address Resolution Protocol (reply)

0000 08 00 27 4d e1 24 08 00 27 06 d4 08 06 00 01  
0010 08 00 06 04 00 02 08 00 27 06 d4 0a 00 00 02  
0020 08 00 27 4d e1 24 0a 00 00 01

root@kali: ~/Documents/python

File Edit View Search Terminal Help

Sent 1 packets.  
Sent 1 packets.  
Sent 1 packets.  
Sent 1 packets.  
Sent 1 packets.  
Sent 1 packets.

# Sommaire

- 1 Introduction
- 2 Cartographie du réseau visé par l'attaque
- 3 Écoute du réseau
- 4 Man In The Middle
- 5 Usurpation d'IP et Détournement de session TCP**
- 6 Attaques Deny Of Service (DOS)
- 7 Conclusion

# Usurpation (spoofing) d'IP

## TCP HIJACKING

- Créer une connexion TCP sur un serveur mais en envoyant un paquet SYN avec une fausse adresse IP source (par ex avec scapy)
- Il n'est pas évident d'exploiter cette attaque puisqu'on ne reçoit pas les réponses.

## Détournement de session TCP (TCP Session Hijacking)

- Repérer et imiter les numéros de ACK et SEQ pour prendre la main sur une connexion établie.
- Injecter un paquet RST(ReSeT) avec un ACK correct pour réinitialiser un connexion TCP active et ainsi se connecter.

## Contre-mesures

- Ces méthodes ne fonctionnent pas avec SSHV2 (ne pas utiliser telnet , FTP...)



# Sommaire

- 1 Introduction
- 2 Cartographie du réseau visé par l'attaque
- 3 Écoute du réseau
- 4 Man In The Middle
- 5 Usurpation d'IP et Détournement de session TCP
- 6 Attaques Deny Of Service (DOS)**
- 7 Conclusion

# DOS

## DOS

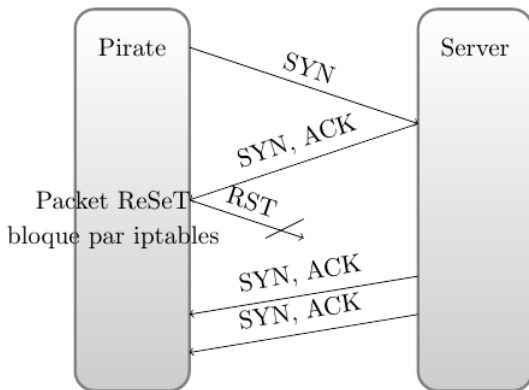
- Inondation (Flood) de paquets pour faire "tomber" un serveur.
- SYN flood ou UDP flood.
- Ping of Death (ancienne attaque peu exploitable de ping volumineux).
- Smurfing : ping en grand nombre.
- Bombes email : envoi de mails volumineux.

## Distributed DOS

- Les attaques DOS se font désormais de façon distribuée afin d'inonder encore plus de paquets le serveur visé.
- Exemple en octobre 2016 avec l'attaque de "DYN" avec des objets connectés.

## SYN flooding

Envoi massif de paquets SYN pour créer des connexion semi-ouvertes et ainsi saturer le serveur.



# Contre-mesures DOS/DDOS

## Contre-mesures

- Mises à jour des systèmes, des serveurs.
- Pare-feu.
- IDS/IPS Système de détection et de prévention d'intrusions.
- Méthodes pour ne pas garder sur le serveur les informations de connexions TCP : SYN Cookie, Syn Cache, Syn Proxy.



# Sommaire

- 1 Introduction
- 2 Cartographie du réseau visé par l'attaque
- 3 Écoute du réseau
- 4 Man In The Middle
- 5 Usurpation d'IP et Détournement de session TCP
- 6 Attaques Deny Of Service (DOS)
- 7 Conclusion

## Conclusion

### Conclusion

- Les attaques réseau en interne sont à prendre en considération. Beaucoup de réseaux ne sont pas protégés contre une attaque Man In The Middle. Il est important de privilégier des protocoles sécurisés et de ne pas installer de serveurs comme les serveurs FTP, telnet ou ssh V1 qui ne résiste pas à une attaque bien menée. Et si possible passer à IPv6 uniquement.
- Concernant les attaques à distance à grande échelle, il est difficile de trouver un système qui permet de résister à une attaques venant de milliers de postes et générant ainsi des Gigabits de données qui arrivent dans un laps de temps très court. Ex : OVH a créé ses propres IDS à base de carte FPGA.
- La sécurité des systèmes nécessite une prévention accrue avec notamment l'installation systématique des mises à jours , de systèmes de détection d'intrusion et également par des tests d'intrusions.