IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Étude bibliographique sur les mécanismes réseaux utilisés en cybercriminalité

Gildas Cotten

Sommaire

Sommaire

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 ...

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Sommaire

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

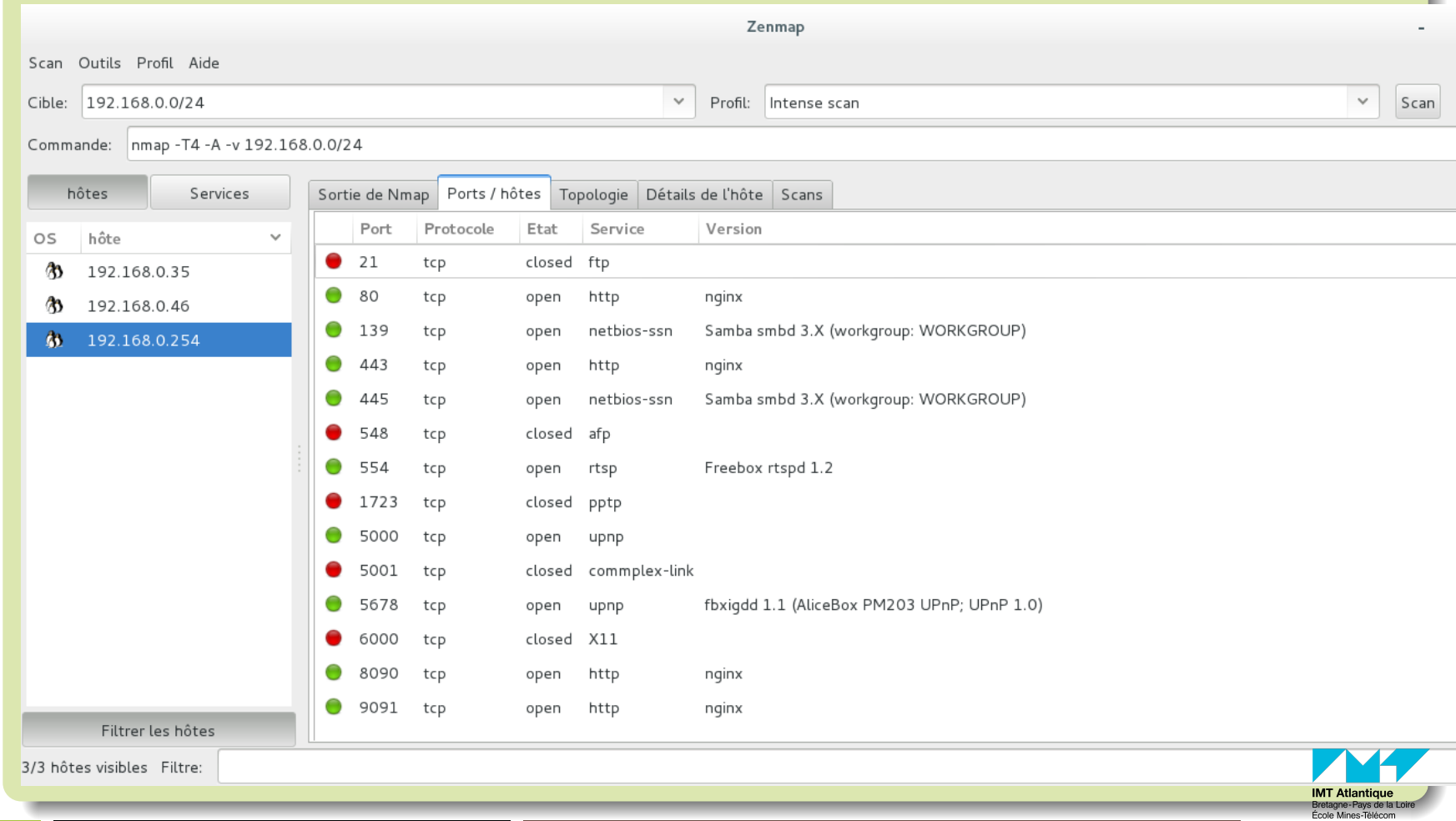
Effectuer un scan du réseau

- 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.

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Port scan avec nmap

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



Sommaire

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 ax switchs manneageable (port mirroring).
- Protocole 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

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

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.

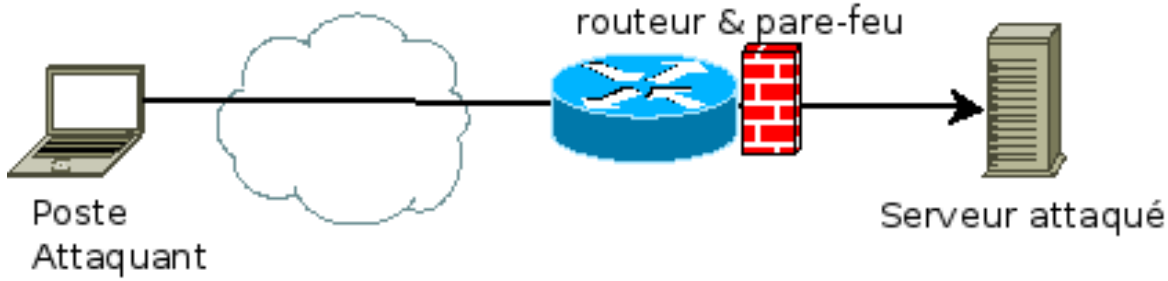


FIGURE: Traversée de routeur pare-feu

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

TABLE: Chevauchements de fragments

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Sommaire

Man In The Middle

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

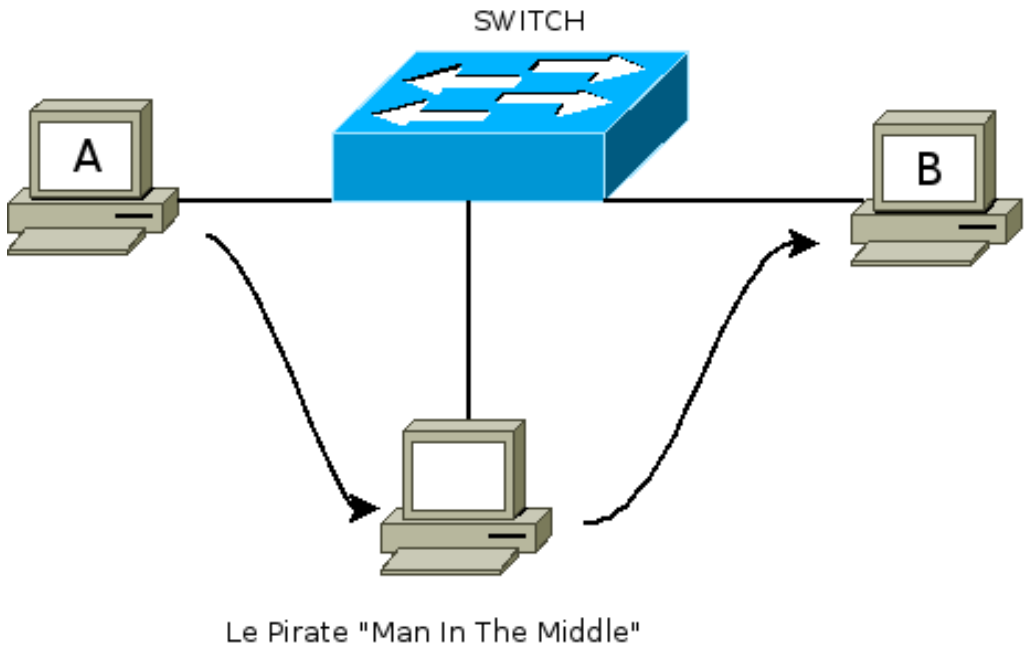


FIGURE: Exemple d'attaque Man In The Middle.

Attaques MITM

ARP POISONING

- Empoisonner le cache ARP de A avec des fausses réponses ARP
- Analyser le traffic 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.

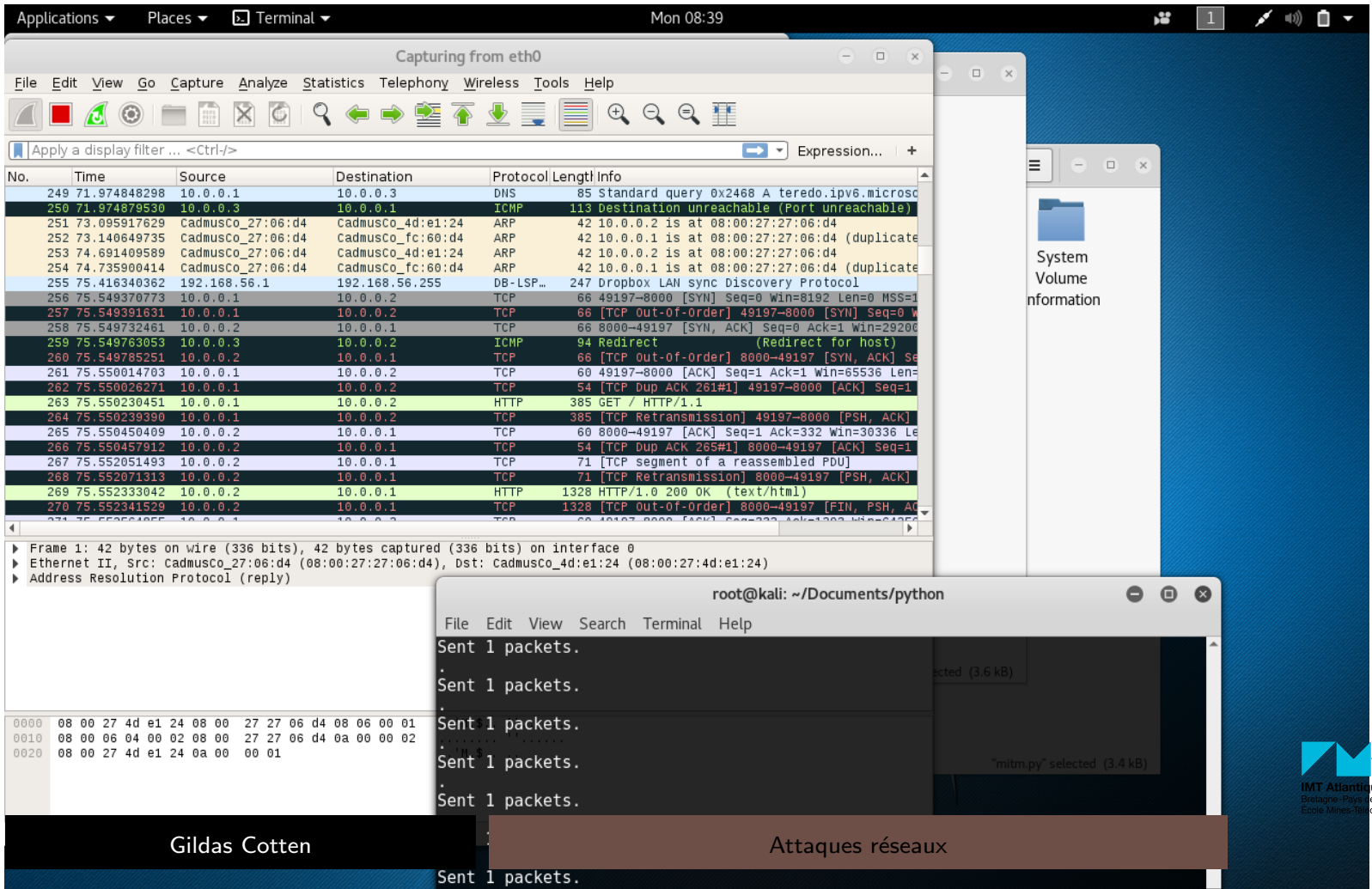
Contre-mesures

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

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

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.



Sommaire

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

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...)

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Sommaire

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.

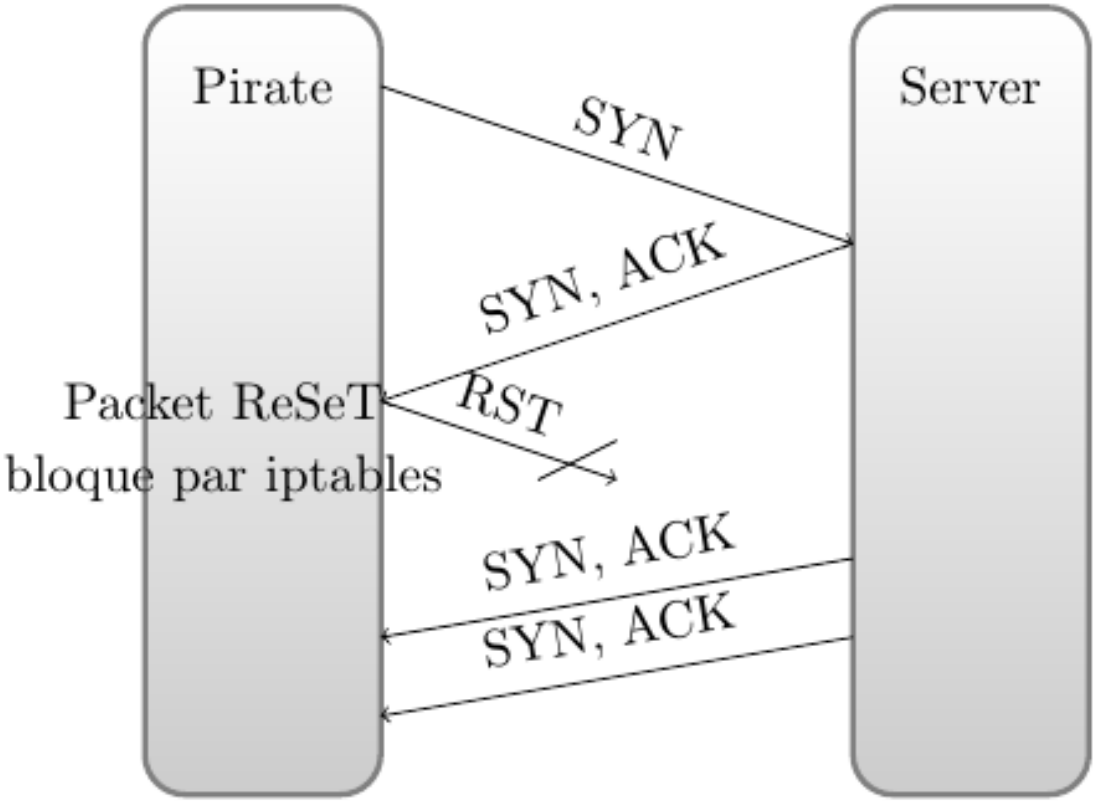
Distributed DOS

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

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

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

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.

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom