Chamberland-Dozois, Léandre (matricule : 1792798)

Rapport TP2

INF8402

Travail présenté à M. Kadi

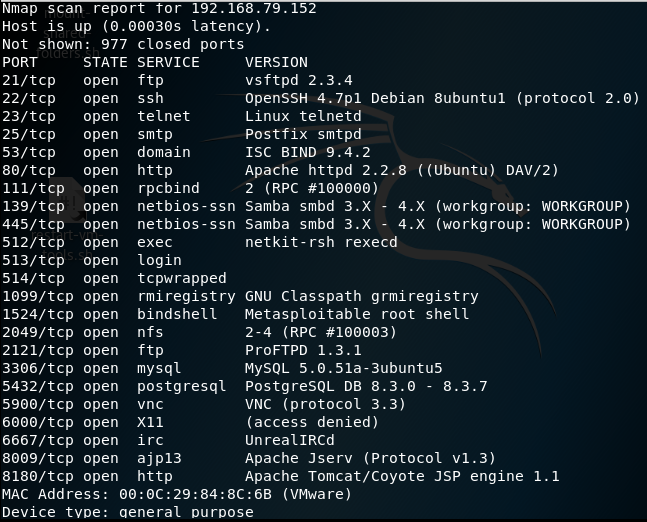
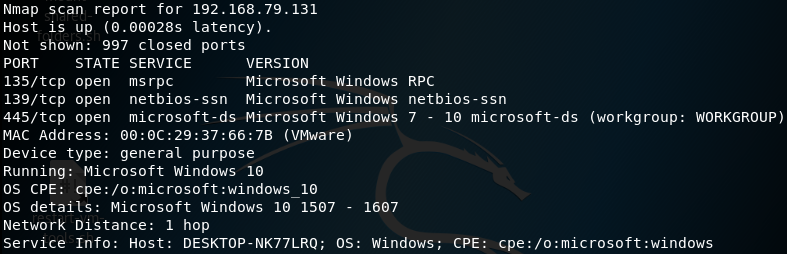
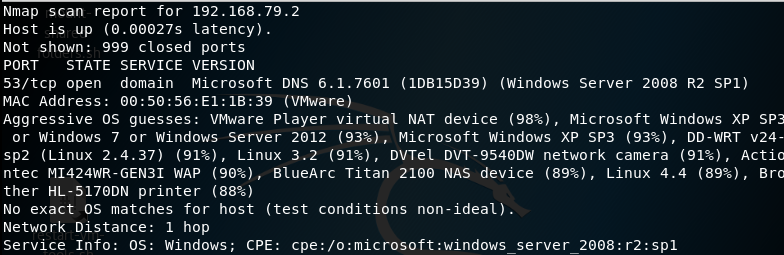
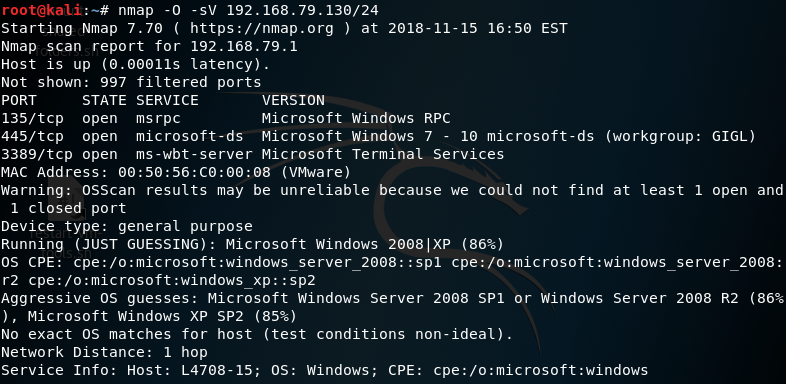
gr. 01

Machine : L4708-05

20 novembre 2018

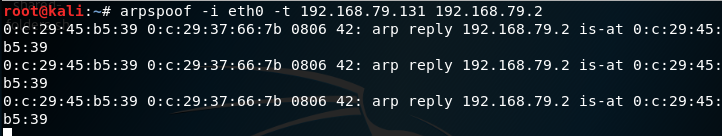
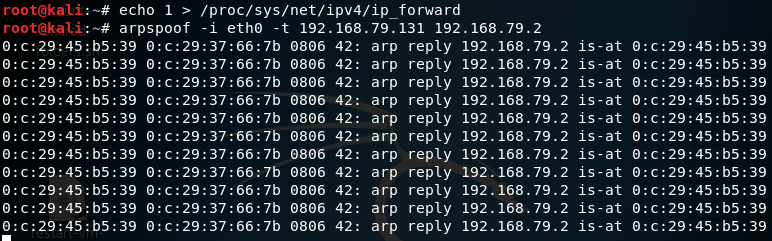
**4.1**

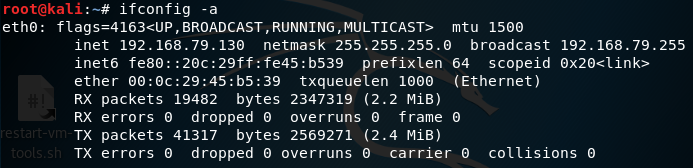
1)



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Windows 10 (192.168.79.131) | Metasploit2.0 (192.168.79.152) | 192.168.79.1 | 192.168.79.2 | 102.168.79.254 |
| Services/port ouvert | 135/tcp msrpc  139/tcp netbios-ssn  445/tcp microsoft-ds | 21/tcp ftp  22/tcp ssh  23/tcp telnet  25/tcp smtp  53/tcp domain  80/tcp http  111/tcp rpc-bind  139/tcp netbios-ssn  445/tcp netbios-ssn  512/tcp exec  513/tcp login  514/tcp tcpwrapped  1099/tcp rmiregistry  1524/tcp bindshell  2049/tcp nfs  2121/tcp ftp  3306/tcp mysql  5432/tcp postgresql  5900/tcp vnc  6000/tcp x11  6667/tcp irc  8009/tcp ajp13  8180/tcp http | 135/tcp msrpc  145/tcp Microsoft-ds  3389/tcp ms-wbt-server | 53/tcp domain | Aucun services/ports ouverts |
| Information sur l’OS | Windows 10 | Linux 2.6.9 | Microsoft windows server 2008 | Non-déterminé | Non-déterminé |
| Distance en saut | 1 hop | 1 hop | 1 hop | 1 hop | 1 hop |

**4.2**



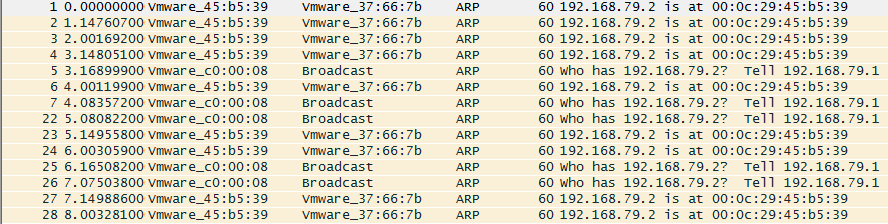


2)



En utilisant la commande suivante : ip route | grep default

3)



On peut voir que les paquets arp associe l’adresse IP de la passerelle par défaut à l’adresse MAC de kali-linux. Cela est causé par l’arp spoofing. Une fois cette association faite, tous les paquets partant de la machine windows 10 passeront par la machine kali-linux.

4)

« echo 1 > /proc/sys/net/ipv4/ip\_forward »

Cette commande active la ré-acheminassions des paquets. (Laisse passer tous les paquets)

« arpspoof -i eth0 -t <Adresse IPv4 Win10> <Adresse IPv4 passerelle par défaut>»

Cette commande spoof tous les paquets partant de la machine windows 10 et ayant comme destination la passerelle par défaut. Ce spoofing est effectué en « empoisonnant » la cache ARP de la passerelle par défaut avec l’association suivante : adresse IPv4 Win10 – adresse MAC de kKali Linux.

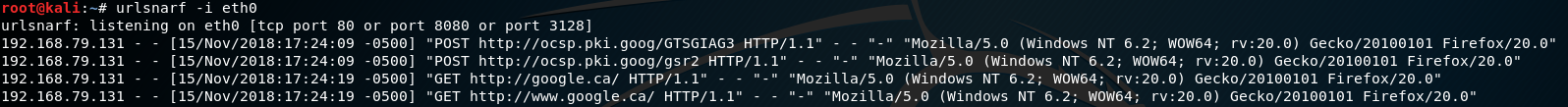
« arpspoof -i eth0 -t <Adresse IPv4 passerelle par défaut> <Adresse IPv4 Win10>»

Cette commande spoof tous les paquets partant de la passerelle par défaut et ayant comme destination la machine windows 10. Ce spoofing est effectué en « empoisonnant » la cache ARP de la machine windows 10 avec l’association suivante : adresse IPv4 Passerelle par défaut – adresse MAC de Kali Linux.

**4.3**

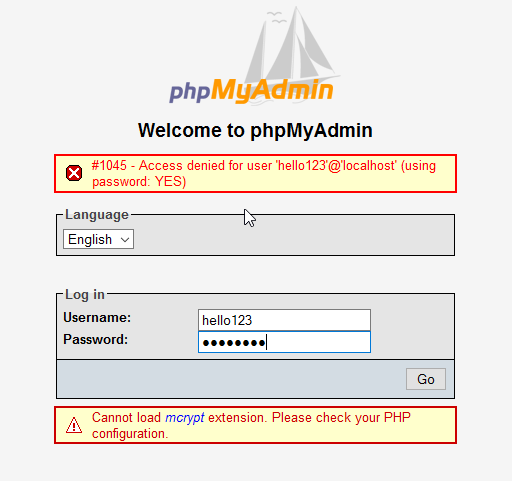
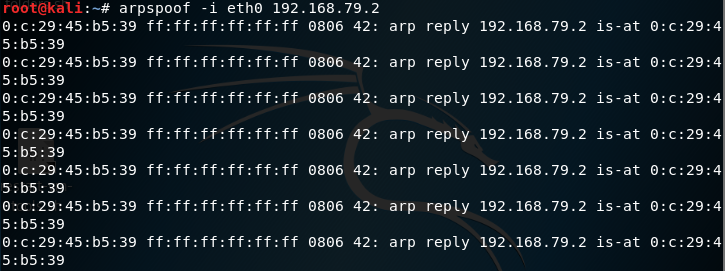


5)

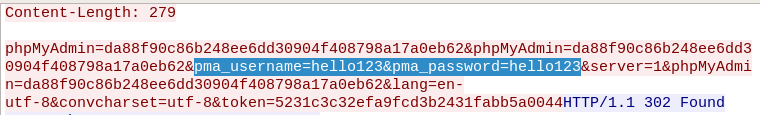


La commande urlsnarf sert à afficher les requêtes http passant par l’hôte (kali\_linux dans ce cas). On peut voir que les requêtes http de la machine windows 10 sont affichées, car les paquets de windows 10 sont acheminés vers kali-linux à cause du arp spoofing.

**4.4**



6)

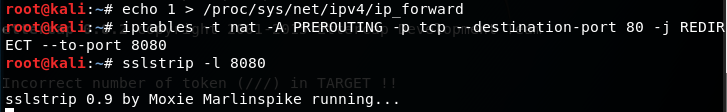


On peut voir le nom d’utilisateur et le mot de passe à découvert.

7)

La commande en 4.4 empoisonne toutes les caches arp du réseau contrairement à la commande en 4.2 qui n’infectait que la passerelle par défaut et la machine windows 10. Il pourrait être préférable d’utiliser la commande en 4.4 si on ne cible pas une victime en particulier, mais l’ensemble du réseau.

**4.5**



8)

« echo 1 > /proc/sys/net/ipv4/ip\_forward »

Cette commande à la même utilité qu’en 4.2.1.

« iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port

8080 »

Cette commande modifie les paquets avec un port de destination 80 pour des paquets avec un port de destination 8080.

« sslstrip -l 8080 »

Cette commande effectue l’attaque sslstrip en falsifiant une page https sur le port 8080.

« ettercap -TqM arp:remote /192.168.0.12// /192.168.0.1// »

Cette commande sniff le réseau pour des paquets ayant comme source 192.168.0.12 et comme destination 192.168.0.1.

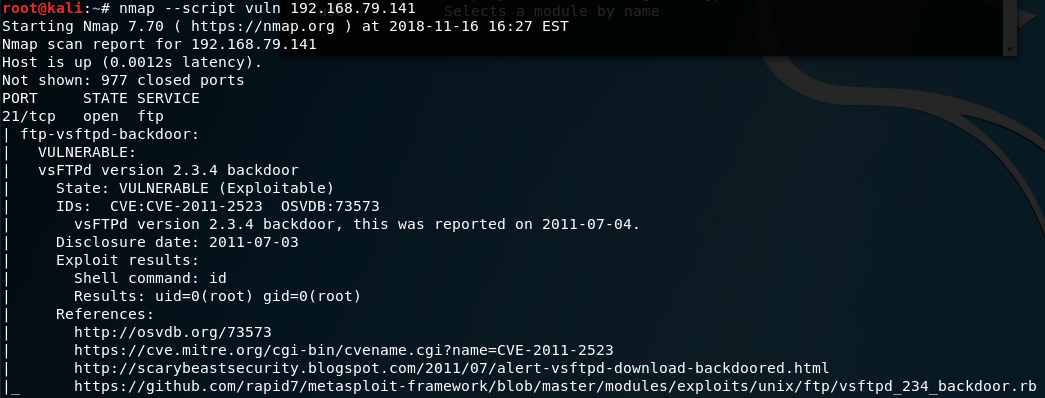
**4.6**

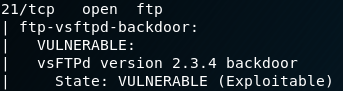
Machine utilisée : L4708-11

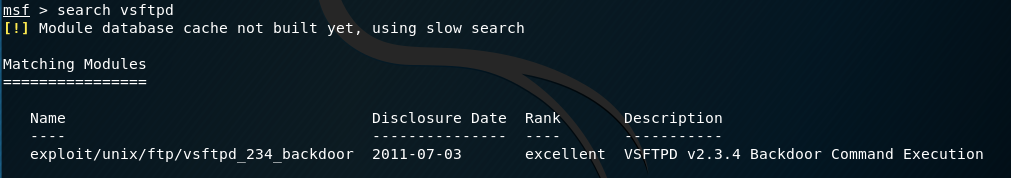
Metasploit2.0 : 192.168.79.141

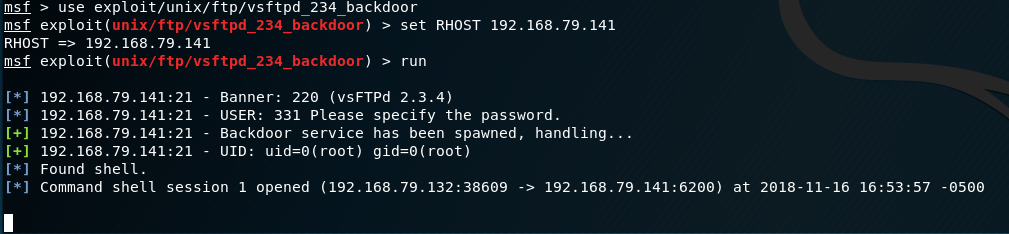
Kali Linux : 192.168.79.132

Windows : 192.168.79.139









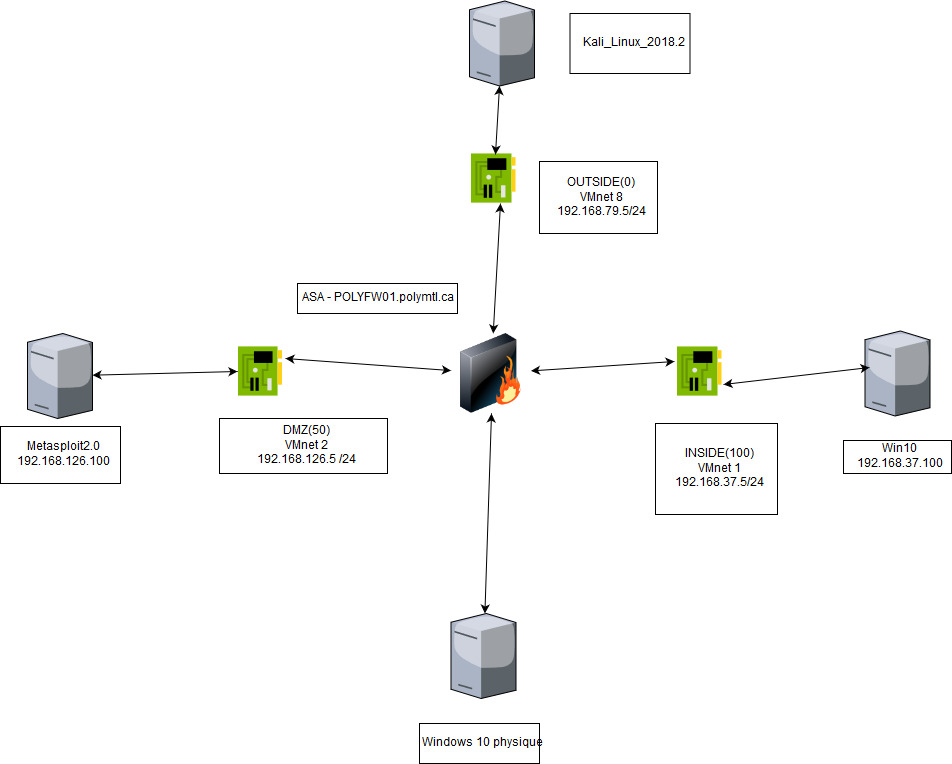
**Explication de la démarche d’attaque**

Tout d’abord, il a fallu évaluer les vulnérabilités sur la machine metasploit2.0. Il a donc fallu utiliser nmap avec –script vuln comme argument pour récupérer la liste des exploits utilisable sur la machine 192.168.79.141 (Metasploit2.0). Ensuite, en regardant le résultat de la commande nmap, j’ai constaté que le service ftp était offert par un serveur vsftpd de version 2.3.4 qui est vulnérable. Par après, pour lancer l’attaque, j’ai ouvert une console metasploit et j’ai chargé l’exploit pour vsftpd. J’ai spécifié l’adresse IP de metasploit2.0 et j’ai exécuté l’exploit. L’exploit m’a ouvert un terminal ssh sur la machine cible.

**4.7**

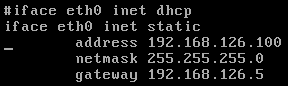
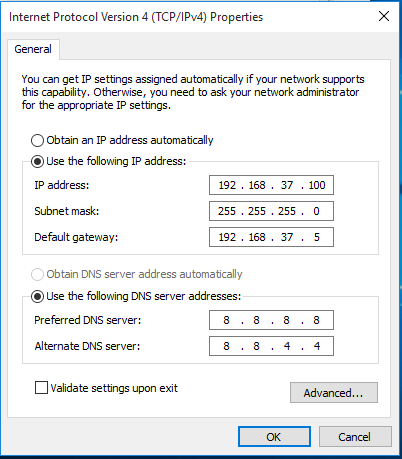
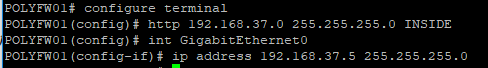
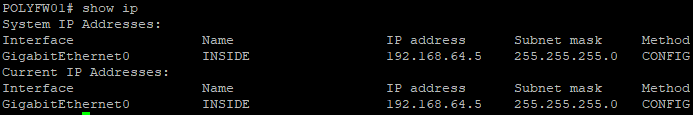
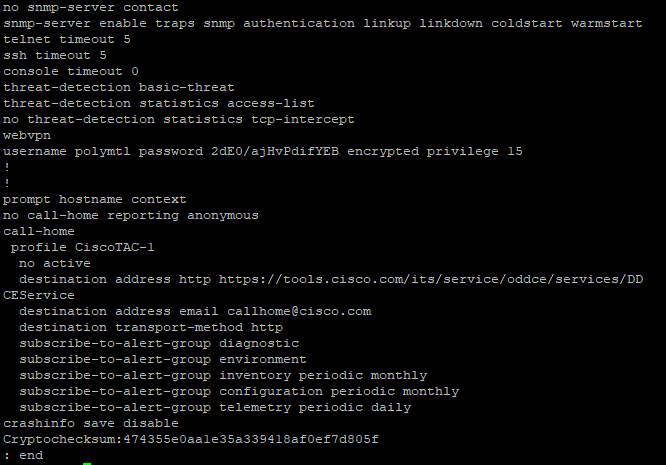
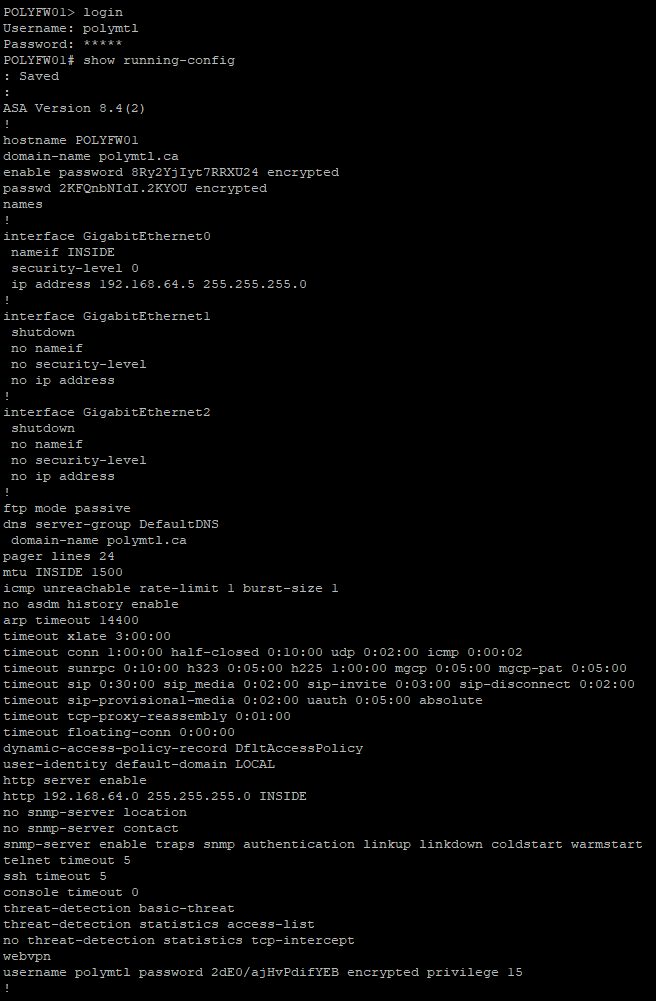
Machine utilisée : L4708-20

**Schéma de la configuration réseau**

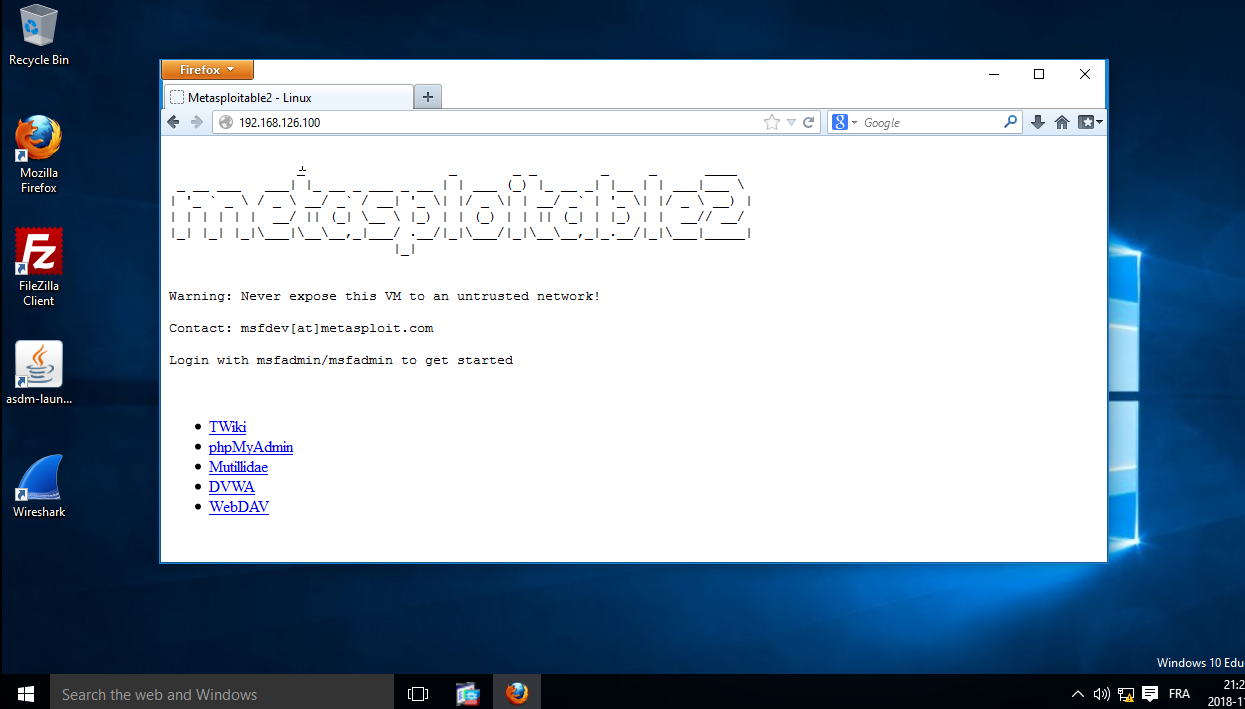
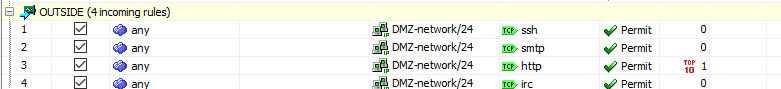
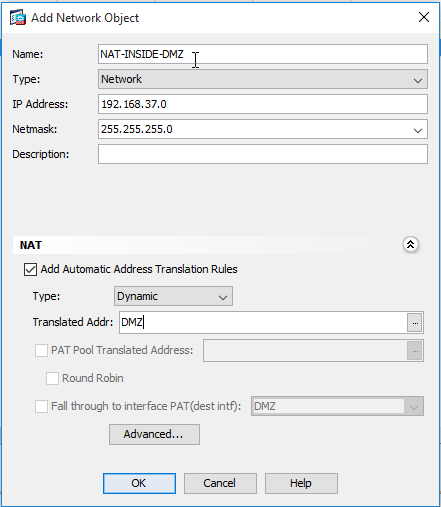
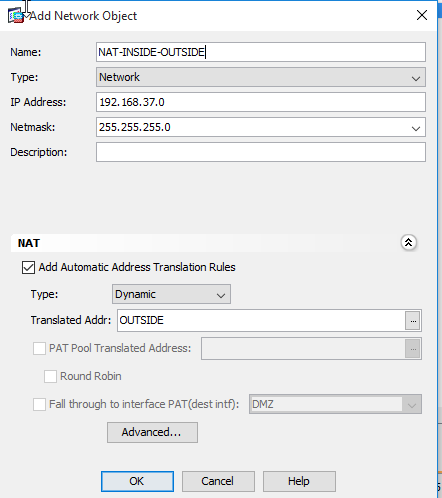
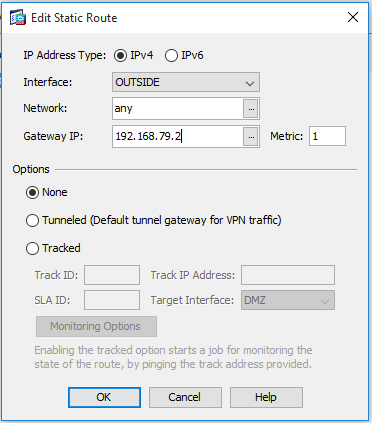
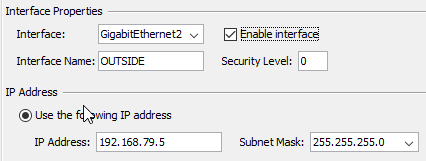
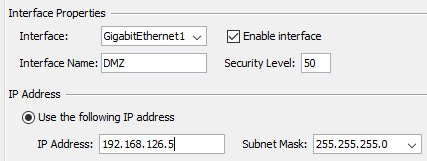
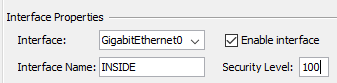


**Tableau de la configuration IP**

|  |  |
| --- | --- |
| **Machines impliquées** | Configuration IP |
| Windows 10 (virtuelle) | IP : 192.168.37.100  Networks : INSIDE, VMNet1 |
| Kali | IP : 192.168.79.100  Networks : OUTSIDE, VMNet8 |
| Metasploitable | IP : 192.168.126.100  Networks : DMZ, VMNet 2 |
| ASA | INSIDE: 192.168.37.5/24  OUTSIDE: 192.168.79.5/24  DMZ: 192.168.126.5/24 |



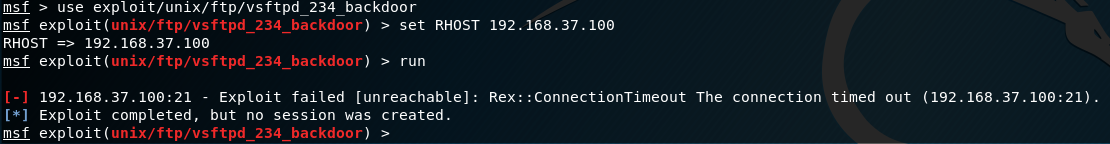




**Explication des manipulations**

Il a tout d’abord fallu configurer les adresses IP des machines du réseau de la même façon que lors du premier TP. L’interface INSIDE de la machine ASA a été configuré grâce à putty sur la machine windows 10 physique. Les trois autres machines virtuelles ont ensuite été configurés manuellement avec les bonnes adresses IP et les bonnes passerelles par défauts. De plus, pour que les machines virtuelles roulent sur les bons réseaux, leur configuration de carte réseau virtuelles ont été changés (VMNet8, VMNet2 et VMNet1). La machine Kali-linux a été placé dans le réseau VMNet8(OUTSIDE), la machine windows 10 a été placé dans le réseau VMNet1(INSIDE) et la machine metasploit2.0 a été placé dans le réseau VMNet2(DMZ). Ensuite, les interfaces ont été configurés avec le bon niveau de sécurité (100 pour INSIDE, 50 pour DMZ et 0 pour OUTSIDE). Ces niveaux de sécurités protègent la machine Metasploit2.0 de toute attaque venant de OUTSIDE(Kali-Linux) et protègent la machine windows 10 de DMZ et de OUTSIDE. Ensuite, pour ajouter une couche de protection pour INSIDE, un objet NAT a été créer pour empêcher les machines externes de connaitre les adresses IP des machines internes. Finalement, des règles de whitelisting ont été ajouté au firewall de OUTSIDE pour permettre aux machines de OUTSIDE d’utiliser certains services offerts par Metasploit2.0 (ssh, smtp, http, irc).

**Attaque plus reproductible**



On peut voir que l’attaque n’est plus fonctionnelle.