King Fahd University of Petroleum & Minerals
College of Computing and Mathematics
ICS 344: Information Security (242)
Project-P3

King Fahd University of Petroleum & Minerals

ICS 344: Information Security (242)

Term 242

Project-P3

MOHMAD ALMAHDOOD	s202034660
ALI ALABDULJABBAR	s202027280
ALI ALMATROOD	s202040180

SECTION 5

May 2, 2025

King Fahd University of Petroleum & Minerals
College of Computing and Mathematics
ICS 344: Information Security (242)
Project-P3

Contents

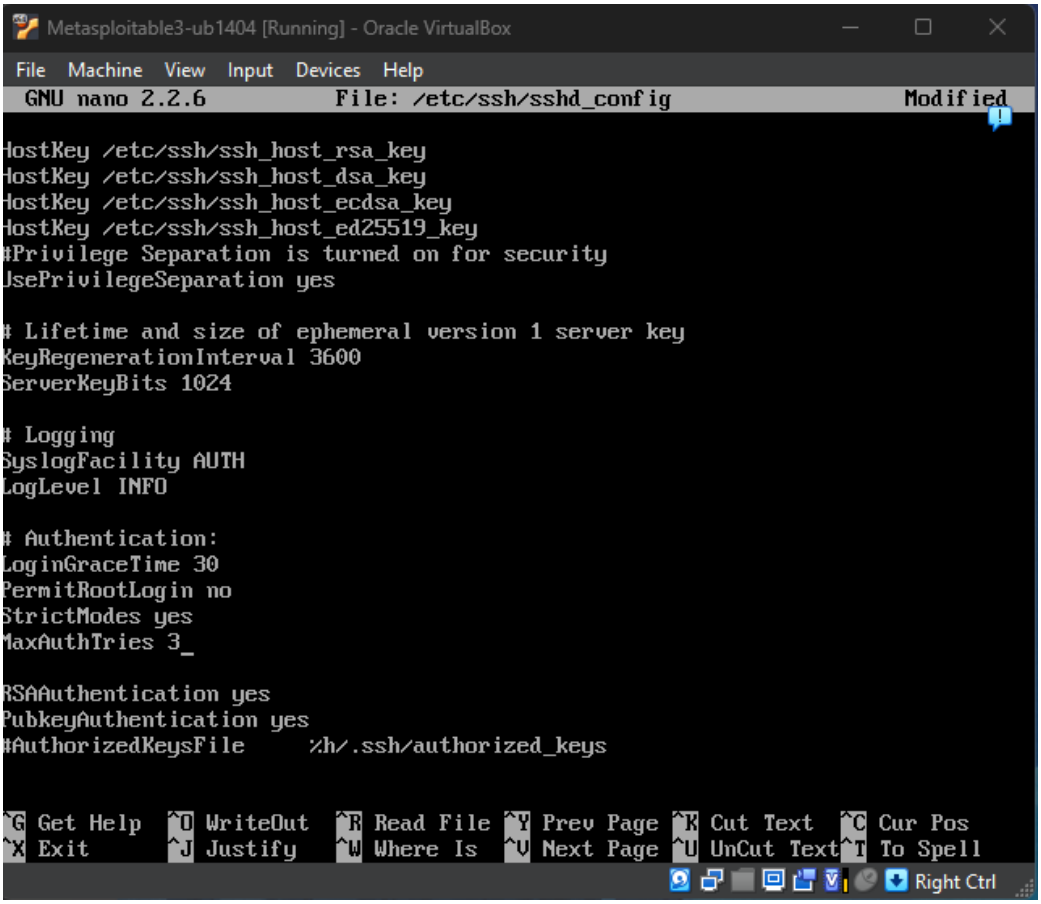
King Fahd University of Petroleum & Minerals
College of Computing and Mathematics
ICS 344: Information Security (242)
Project-P3

Phase 3: Defensive Strategy Proposal

To defense against the ssh brute force attack, we will take the ssh hardening measures.

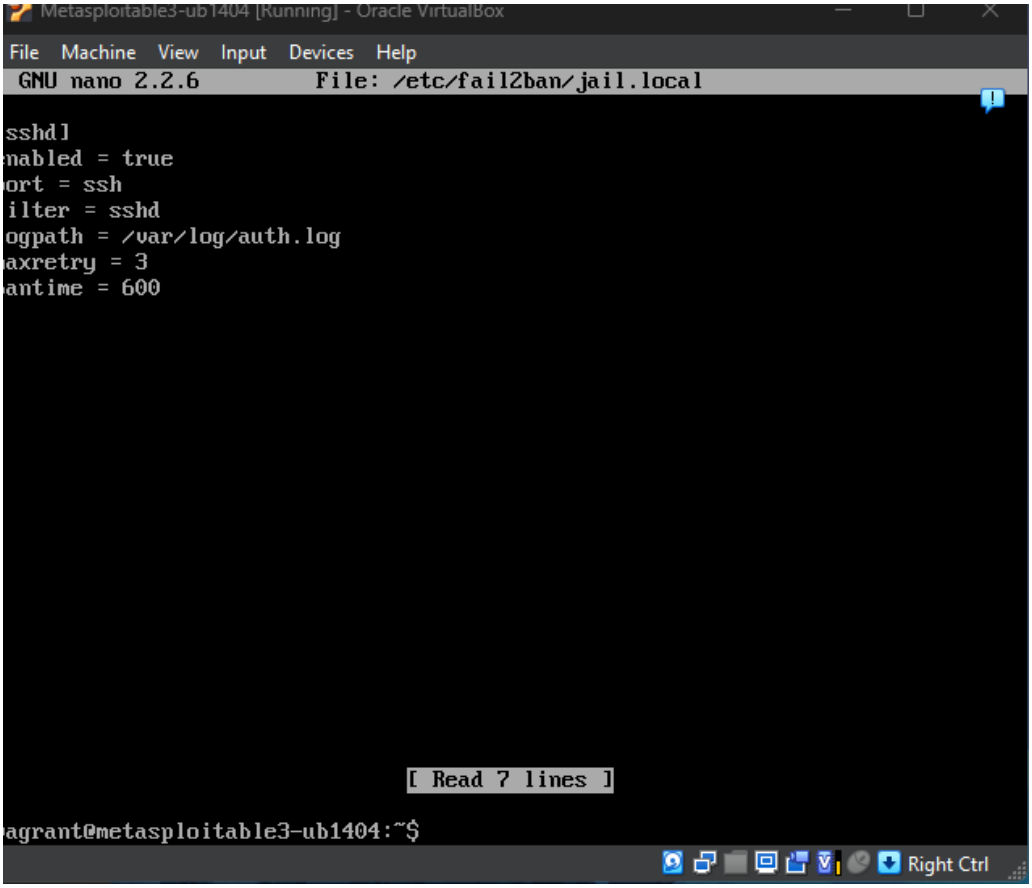
Step 1: implement the SSH hardening measures

1. Implement strong password policies



2. Install and configure Fail2Ban

Fail2Ban is an intrusion prevention tool that monitors log files for filed login and block suspicious IPS.
After downloading it, we add our configuration to enable it.



Step 2: validate the defense mechanisms applied:

1. Test 3 wrong attempts to test the password policies
2. Test the brute force to check that Fal2ban works.

```
msf6 auxiliary(scanner/ssh/ssh_login) > exploit
[*] 192.168.56.103:22 - Starting bruteforce
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) >
```

```
ss; user unknown
May  2 16:29:18 metasploitable3-ub1404 sshd[2434]: pam_unix(sshd:auth): authenti
cation failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.56.102
May  2 16:29:20 metasploitable3-ub1404 sshd[2434]: Failed password for invalid u
ser  from 192.168.56.102 port 37539 ssh2
May  2 16:29:20 metasploitable3-ub1404 sshd[2434]: Connection closed by 192.168.
56.102 [preauth]
May  2 16:29:20 metasploitable3-ub1404 sshd[2437]: Invalid user  from 192.168.56
.102
May  2 16:29:20 metasploitable3-ub1404 sshd[2437]: input_userauth_request: inval
id user  [preauth]
May  2 16:29:20 metasploitable3-ub1404 sshd[2437]: pam_unix(sshd:auth): check pa
ss; user unknown
May  2 16:29:20 metasploitable3-ub1404 sshd[2437]: pam_unix(sshd:auth): authenti
cation failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.56.102
May  2 16:29:22 metasploitable3-ub1404 sshd[2437]: Failed password for invalid u
ser  from 192.168.56.102 port 38233 ssh2
May  2 16:29:22 metasploitable3-ub1404 sshd[2437]: Connection closed by 192.168.
56.102 [preauth]
May  2 16:29:22 metasploitable3-ub1404 sshd[2439]: Invalid user  from 192.168.56
.102
May  2 16:29:22 metasploitable3-ub1404 sshd[2439]: input_userauth_request: inval
id user  [preauth]
May  2 16:29:22 metasploitable3-ub1404 sshd[2439]: pam_unix(sshd:auth): check pa
ss; user unknown
May  2 16:29:22 metasploitable3-ub1404 sshd[2439]: pam_unix(sshd:auth): authenti
cation failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.56.102
May  2 16:29:24 metasploitable3-ub1404 sshd[2439]: Failed password for invalid u
ser  from 192.168.56.102 port 41171 ssh2
```

As we can see from the logs the and the output of the brute fore attempt in Metasploit, we can see that the connection closed but Fail2Ban and the brute force stopped in the Metasploit.

Conclusion:

There are many ways to prevent ssh service exploitation such as implementing password policies and downloads IP tools like Fail2Ban. Also, there is many other ways like changing the default ssh port and configuring TCP wrappers that allows specific Ips. And finally implement key-based authentication instead of passwords.