

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

Phase 3: Defensive Strategy Proposal .....	3
Step 1: implement the SSH hardening measures .....	3
Step 2: validate the defense mechanisms applied: .....	5
Conclusion: .....	6

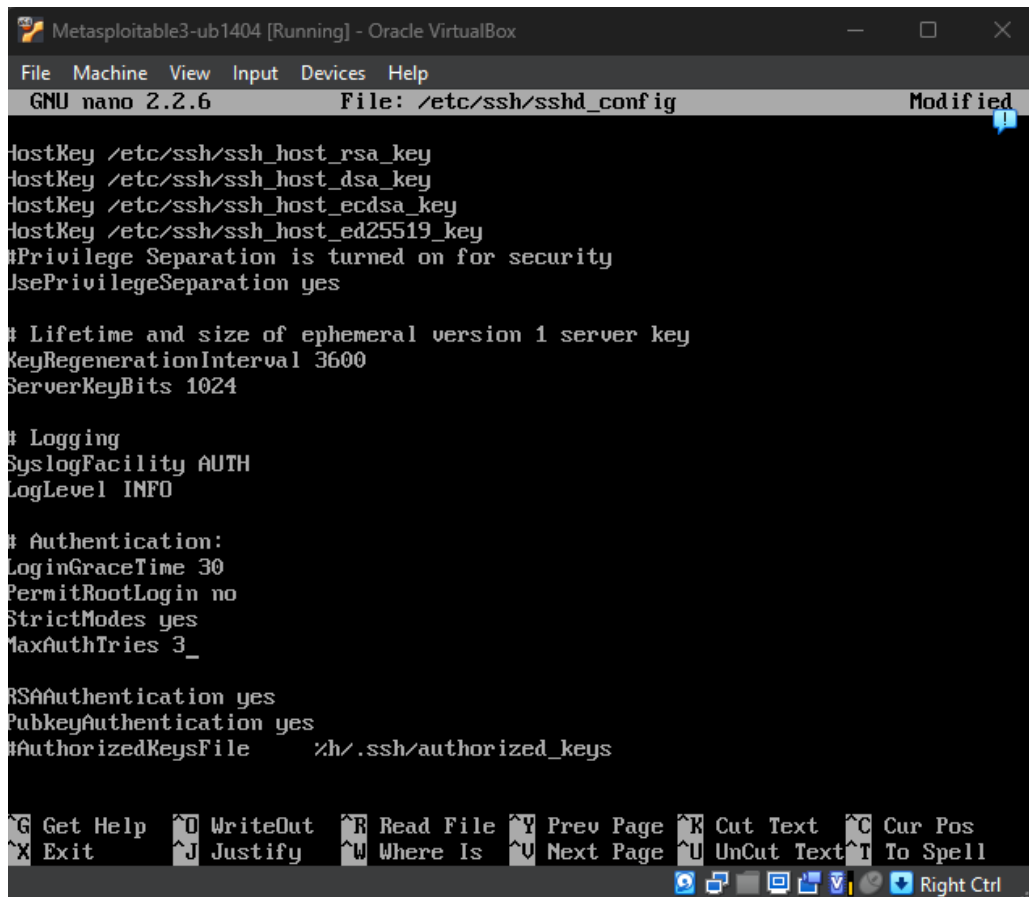
King Fahd University of Petroleum & Minerals  
College of Computing and Mathematics  
ICS 344: Information Security (242)  
Project-P3

## 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



```
Metasploitable3-ub1404 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
GNU nano 2.2.6 File: /etc/ssh/sshd_config Modified
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key
#Privilege Separation is turned on for security
UsePrivilegeSeparation yes

# Lifetime and size of ephemeral version 1 server key
KeyRegenerationInterval 3600
ServerKeyBits 1024

# Logging
SyslogFacility AUTH
LogLevel INFO

# Authentication:
LoginGraceTime 30
PermitRootLogin no
StrictModes yes
MaxAuthTries 3

RSAAuthentication yes
PubkeyAuthentication yes
#AuthorizedKeysFile      %h/.ssh/authorized_keys

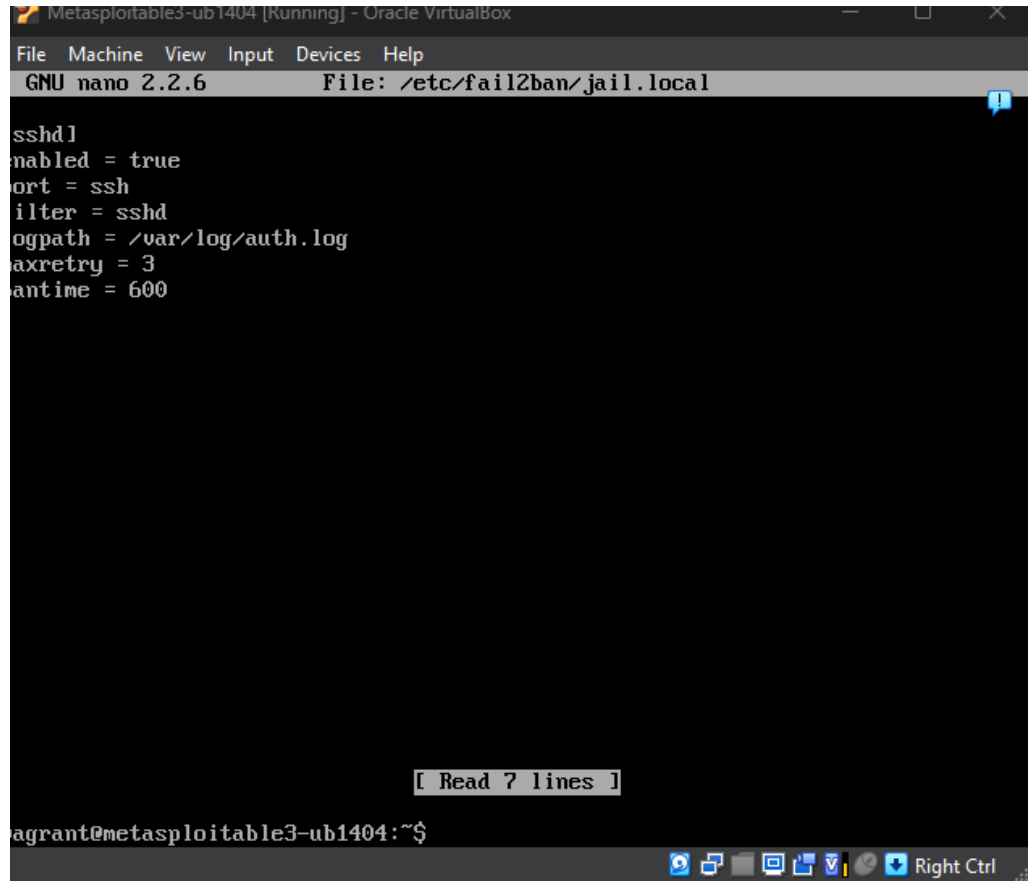
^G Get Help ^O WriteOut ^R Read File ^V Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^U Next Page ^U UnCut Text ^T To Spell
Right Ctrl
```

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

2. Install and configure Fail2Ban

Fail2Ban is an intrusion prevention tool that monitors log files for failed login and block suspicious IPS.

After downloading it, we add our configuration to enable it.



The screenshot shows a terminal window titled "Metasploitable3-ub1404 [Running] - Oracle VirtualBox". The window displays the nano text editor editing the file `/etc/fail2ban/jail.local`. The configuration for the `sshd` service is visible, with the following settings: `enabled = true`, `port = ssh`, `filter = sshd`, `logpath = /var/log/auth.log`, `maxretry = 3`, and `bantime = 600`. A status bar at the bottom of the editor indicates "[ Read 7 lines ]". The terminal prompt at the bottom shows the user is `agrant` on the machine `metasploitable3-ub1404`, with a tilde symbol indicating the home directory.

```
Metasploitable3-ub1404 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
GNU nano 2.2.6 File: /etc/fail2ban/jail.local

sshd
enabled = true
port = ssh
filter = sshd
logpath = /var/log/auth.log
maxretry = 3
bantime = 600

[ Read 7 lines ]

agrant@metasploitable3-ub1404:~$
```

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

## 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 Fail2ban 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): authentication 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 user 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: invalid user [preauth]
May 2 16:29:20 metasploitable3-ub1404 sshd[2437]: pam_unix(sshd:auth): check pass: user unknown
May 2 16:29:20 metasploitable3-ub1404 sshd[2437]: pam_unix(sshd:auth): authentication 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 user 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: invalid user [preauth]
May 2 16:29:22 metasploitable3-ub1404 sshd[2439]: pam_unix(sshd:auth): check pass: user unknown
May 2 16:29:22 metasploitable3-ub1404 sshd[2439]: pam_unix(sshd:auth): authentication 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 user 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.

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

## 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.