ICS 344

TERM 242

TEAM PROJECT

GROUP 7

Mohammed Al Lail => ID/202152850

Ali almatar => ID/202158190

Hassan Al Nasser => ID/202163950

Phase 3

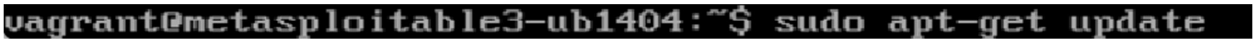
We chose to defend against SSH brute-force attacks (the same attack in phase 1) that compromise the Metasploitable VM. We used **Fail2Ban** to prevent repeated login attempts by banning attacking IPs failing 3 attempts within a 30-minute window for 30 minutes. This setup makes **automated brute-force** attacks ineffective.

Fail2Ban Setup

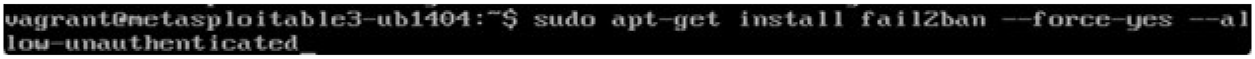
To update the system and install fail2ban, we ran:

sudo apt-get update

sudo apt-get install fail2ban --allow-unauthenticated --force-yes



```
vagrant@metasploitable3-ub1404:~$ sudo apt-get update
```



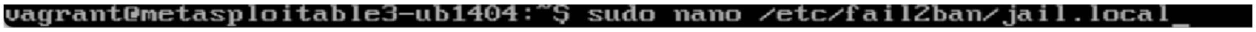
```
vagrant@metasploitable3-ub1404:~$ sudo apt-get install fail2ban --force-yes --al
low-unauthenticated_
```

We then configured **Fail2Ban** by editing **/etc/fail2ban/jail.local** file.

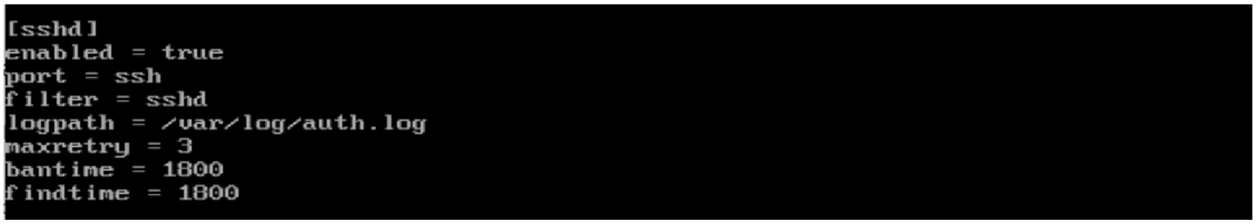
maxretry = 3 (only 3 attempts are allowed before getting banned)

bantime = 1800 (ban duration is 30 minutes)

findtime = 1800 (failure attempts counted within a 30-min window)

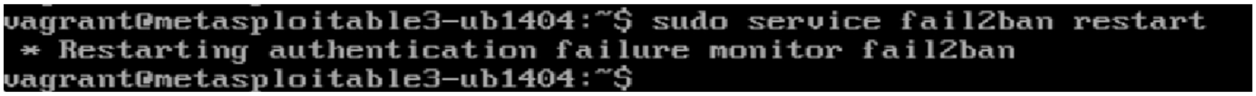


```
vagrant@metasploitable3-ub1404:~$ sudo nano /etc/fail2ban/jail.local_
```



```
[sshd]
enabled = true
port = ssh
filter = sshd
logpath = /var/log/auth.log
maxretry = 3
bantime = 1800
findtime = 1800
```

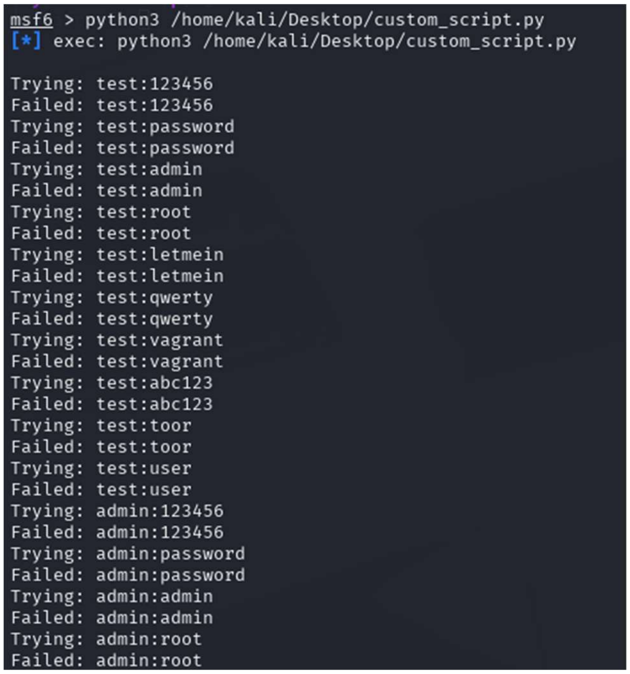
We restarted Fail2Ban to reflect the changes in **/etc/fail2ban/jail.local** file.



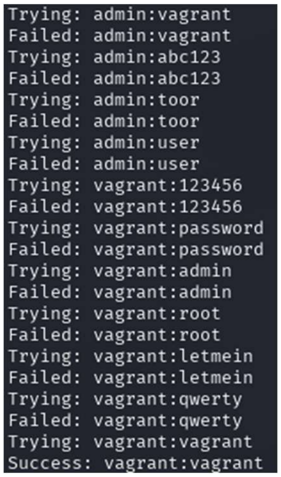
```
vagrant@metasploitable3-ub1404:~$ sudo service fail2ban restart
 * Restarting authentication failure monitor fail2ban
vagrant@metasploitable3-ub1404:~$
```

Attack

Before using Fail2Ban:



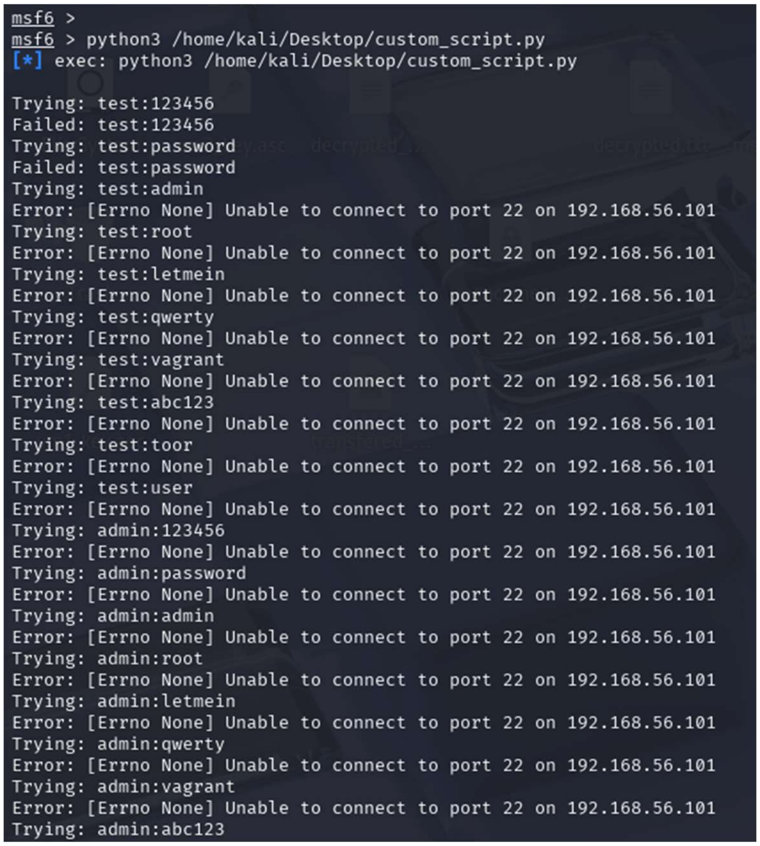
```
msf6 > python3 /home/kali/Desktop/custom_script.py
[*] exec: python3 /home/kali/Desktop/custom_script.py

Trying: test:123456
Failed: test:123456
Trying: test:password
Failed: test:password
Trying: test:admin
Failed: test:admin
Trying: test:root
Failed: test:root
Trying: test:letmein
Failed: test:letmein
Trying: test:qwerty
Failed: test:qwerty
Trying: test:vagrant
Failed: test:vagrant
Trying: test:abc123
Failed: test:abc123
Trying: test:toor
Failed: test:toor
Trying: test:user
Failed: test:user
Trying: admin:123456
Failed: admin:123456
Trying: admin:password
Failed: admin:password
Trying: admin:admin
Failed: admin:admin
Trying: admin:root
Failed: admin:root
```



```
Trying: admin:vagrant
Failed: admin:vagrant
Trying: admin:abc123
Failed: admin:abc123
Trying: admin:toor
Failed: admin:toor
Trying: admin:user
Failed: admin:user
Trying: vagrant:123456
Failed: vagrant:123456
Trying: vagrant:password
Failed: vagrant:password
Trying: vagrant:admin
Failed: vagrant:admin
Trying: vagrant:root
Failed: vagrant:root
Trying: vagrant:letmein
Failed: vagrant:letmein
Trying: vagrant:qwerty
Failed: vagrant:qwerty
Trying: vagrant:vagrant
Success: vagrant:vagrant
```

After using Fail2Ban:

This user is banned for 30 minutes because he tried to login 3 times with the wrong username and password.



```
msf6 >
msf6 > python3 /home/kali/Desktop/custom_script.py
[*] exec: python3 /home/kali/Desktop/custom_script.py

Trying: test:123456
Failed: test:123456
Trying: test:password
Failed: test:password
Trying: test:admin
Error: [Errno None] Unable to connect to port 22 on 192.168.56.101
Trying: test:root
Error: [Errno None] Unable to connect to port 22 on 192.168.56.101
Trying: test:letmein
Error: [Errno None] Unable to connect to port 22 on 192.168.56.101
Trying: test:qwerty
Error: [Errno None] Unable to connect to port 22 on 192.168.56.101
Trying: test:vagrant
Error: [Errno None] Unable to connect to port 22 on 192.168.56.101
Trying: test:abc123
Error: [Errno None] Unable to connect to port 22 on 192.168.56.101
Trying: test:toor
Error: [Errno None] Unable to connect to port 22 on 192.168.56.101
Trying: test:user
Error: [Errno None] Unable to connect to port 22 on 192.168.56.101
Trying: admin:123456
Error: [Errno None] Unable to connect to port 22 on 192.168.56.101
Trying: admin:password
Error: [Errno None] Unable to connect to port 22 on 192.168.56.101
Trying: admin:admin
Error: [Errno None] Unable to connect to port 22 on 192.168.56.101
Trying: admin:root
Error: [Errno None] Unable to connect to port 22 on 192.168.56.101
Trying: admin:letmein
Error: [Errno None] Unable to connect to port 22 on 192.168.56.101
Trying: admin:qwerty
Error: [Errno None] Unable to connect to port 22 on 192.168.56.101
Trying: admin:vagrant
Error: [Errno None] Unable to connect to port 22 on 192.168.56.101
Trying: admin:abc123
```

In conclusion, our defense mechanism **(Fail2Ban)** has successfully prevented automatic brute force attacks by banning user IPs that entered the username and password **three times** incorrectly for half an hour. This only allows **144 attempts per day** for the attacker.

For the case of distributed attacks, we can combine Fail2Ban with a slightly stronger password to make millions of attempts not sufficient to compromise the machine. Even a weak password such as **sr!Nope** can decrease the chances of attackers significantly.