

Phase 3: Setup a Suitable Defense Strategy

- Showcase the brute force attack on Metasploit trying to get through by trying multiple password combinations until manually stopped.

```
[*] 172.20.10.11:22 - Starting bruteforce
[-] 172.20.10.11:22 - Failed: 'vagrant:123456'
[!] No active DB -- Credential data will not be saved!
[-] 172.20.10.11:22 - Failed: 'vagrant:12345'
[-] 172.20.10.11:22 - Failed: 'vagrant:123456789'
[-] 172.20.10.11:22 - Failed: 'vagrant:password'
[-] 172.20.10.11:22 - Failed: 'vagrant:iloveyou'
[-] 172.20.10.11:22 - Failed: 'vagrant:princess'
[-] 172.20.10.11:22 - Failed: 'vagrant:1234567'
[-] 172.20.10.11:22 - Failed: 'vagrant:rockyou'
[-] 172.20.10.11:22 - Failed: 'vagrant:12345678'
[-] 172.20.10.11:22 - Failed: 'vagrant:abc123'
[-] 172.20.10.11:22 - Failed: 'vagrant:nicole'
^C[*] Caught interrupt from the console ...
[*] Auxiliary module execution completed
```

- Use and configure fail2ban jail.local file to ban out ip addresses with repeated tries.
- The parameters are configured such that after 5 attempts at accessing the ssh port the ip will be banned and logged to auth.log for 300 seconds.

```
[sshd]
enabled = true
port = ssh
filter = sshd
logpath = /var/log/auth.log
maxretry = 5
bantime = 300
```

- Now we can see that the brute force attack is stopped after 7 attempts
- The reason that it didn't stop exactly 7 times is because the log ins are happening quickly and fail2ban polls periodically.

```
msf6 auxiliary(scanner/ssh/ssh_login) > run
[*] 172.20.10.11:22 - Starting bruteforce 172.20.10.11 port 22: Connection refused
[-] 172.20.10.11:22 - Failed: 'vagrant:123456'
[!] No active DB -- Credential data will not be saved!
[-] 172.20.10.11:22 - Failed: 'vagrant:12345'
[-] 172.20.10.11:22 - Failed: 'vagrant:123456789'
[-] 172.20.10.11:22 - Failed: 'vagrant:password'
[-] 172.20.10.11:22 - Failed: 'vagrant:iloveyou'
[-] 172.20.10.11:22 - Failed: 'vagrant:princess'
[-] 172.20.10.11:22 - Failed: 'vagrant:1234567'
[-] Could not connect: The connection was refused by the remote host (172.20.10.11:22).
[-] Could not connect: The connection was refused by the remote host (172.20.10.11:22).
[-] Could not connect: The connection was refused by the remote host (172.20.10.11:22).
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) >
```

- We can see that the attacker device cannot ssh into the vagrant user victim device.

```
(ilka@kali)-[~]
$ ssh vagrant@172.20.10.11
ssh: connect to host 172.20.10.11 port 22: Connection refused
172.20.10.11:22 - Failed: 'vagrant:123456'
```

- We can also see the attacker's ip is blacklisted by fail2ban on the victim's device.

```
Chain fail2ban-ssh (1 references)
num target prot opt source destination
1 REJECT all -- 172.20.10.12 0.0.0.0/0 reject-with icmp-port-unreachable
2 RETURN all -- 0.0.0.0/0 0.0.0.0/0
vagrant@metasploitable3-ub1404:/etc/fail2ban$
```