ICS 344

Project Phase 3

Defence

We decided to disable SSH service to prevent attacks.

This will be done by running “sudo service ssh stop”.

```
21/tcp   open   ftp
22/tcp   closed ssh
```

Therefore, the connection wasn’t listened to by the attacker after an attempt to.

The following picture shows how it is **after** implementing the firewall:

```
msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 192.168.16.166:22 - Starting bruteforce
[-] Could not connect: The connection was refused by the remote host (192.168.16.166:22).
[!] No active DB -- Credential data will not be saved!
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

The following picture shows how it was **before** implementing the firewall:

```
msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 192.168.16.166:22 - Starting bruteforce
[+] 192.168.16.166:22 - Success: 'vagrant:vagrant' 'uid=900(vagrant) gid=900(vagrant) groups=90
0(vagrant),27(sudo) Linux metasploitable3-ub1404 3.13.0-170-generic #220-Ubuntu SMP Thu May 9 1
2:40:49 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux '
[!] No active DB -- Credential data will not be saved!
[*] SSH session 1 opened (192.168.16.167:45709 → 192.168.16.166:22) at 2025-05-07 05:36:59 -04
00
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) >
```