Scanning Networks and finding alive hosts with NMAP

1. Run Nmap and perform 3 different scans against targets.

-perform Xmas scan against Win XP machine:

nmap –sX –v <target IP>

-perform a udp scan:

nmap –sU <target IP>

-perform an ACK scan

nmap –sA –P0 <target IP>

Compare results from UDP and TCP scans that you did. Which one is more time consuming?

2. Open up a terminal on your Kali machine and type in: **fping** ,then: **man fping** for options

Run the program to perform a ping sweep.

Fping –a –g (IP network range)>hosts.txt

For example: **fping –a –g 192.168.23.100 192.168.23.254>hosts.txt**

Open up the txt file to see results with: **cat hosts.txt**

3. Packet crafter. Use HPING3 program, create different types of packets and send them to a target:

• Create an ACK packet and send it to port 80 on the victim:

Hping3 –A <target IP address> -p 80

• Create an SYN scan against different ports on a victim:

Hping3 -8 50-56 –s <target IP address> -v

• Create a packet with FIN, URG, and PSH flags set and send it to port 80 on the victim:

Hping3 –F –p -U <target IP address> -p 80

4. Using traceroute option can be used to trace the path to the specified host:

Example : nmap --traceroute scanme.nmap.org

5. Turn on the firewall on your target machine. Launch the following command:

nmap –sS –T4 –A –f –v <target IP>

Try to spoof your MAC address also:

nmap -PN --spoof-mac 0 <target IP>

6. Nmap scripting engine (NSE) – prebuilt tools to do various things. To invoke them should use: "- - script" argument (auth , brute , discovery , dos , exploit ,external ,fuzzer , intrusive , malware ,safe, version)

Try the following command:

nmap - - script banner <target IP>

The script called : "vuln" will try to find all vulnerabilities on a target:

nmap - - script vuln <target IP>

You are encouraged to try different scripts ,get used to them and see the results of each one.