**Module 3 Scanning & Enumeration**

**3.0 Scan Enumeration**

**Scanning Methodology**

1. Check for live systems
2. Check for open ports
3. Scan beyond IDS
4. Perform banner grabbing
5. Scan for vulnerabilities
6. Draw network diagrams
7. Prepare proxies

**3 Way Handshakes**

1. SYN
2. SYN/ACK
3. ACK
4. Connection established

**TCP Header Flags**

1. Synchronize (SYN) – set during initial communication establishment & indicates negotiation of parameters & sequence numbers
2. Acknowledgement (ACK) – acknowledges SYN flag
3. Reset (RST) – forces termination of communications in both directions
4. Finish (FIN) – signifies ordered close to comms
5. Push (PSH) – forces delivery of data w/o concern for buffering
6. Urgent (URG) – indicates data is being sent out of band

**TCP 3 way Handshake Process**

1. A sends SYN packet to B to establish communications
   1. Has sequence number (Eg. 100)
2. B sends back ACK packet to accept communications
   1. Has sequence number + 1 (Eg. 101)
3. B also sends SYN packet to A
   1. “I want to talk to you, do you want to talk to me?”
   2. Sequence number is 300
4. A sends back ACK packet to B
   1. Sequence number + 1 (Eg. 301)

**Performing Checks for Live Systems**

1. Use nmap & hping3 to identify live systems on target
2. Nmap type, nmap -sn 192.16.0.1/24
   1. -sn to disable port scanning (just sends ping requests)
3. Hping3 type, hping3 -1 192.168.0.1
   1. -1 is switch used for ping scans

**Scan for Open Ports with NMAP & HPING3**

1. Nmap type, nmap 192.168.0.1
   1. Scans most common ports to see if open
   2. Can use open ports as entry points & see running services
2. Hping3 type, hping3 -8 0-5000 -S 192.168.0.1
   1. -8 enables SCAN mode
   2. 0-5000 = range of ports to scan
   3. -S = set SYN flag

**Scanning Techniques**

1. For test, enable apache web service with DVWA (Damn Vulnerable Web App) on port 80 on target machine
2. Nmap half-connect scan
   1. Type, nmap -sS 192.168.0.1
   2. If don’t spcify range of ports nmap will perform SYN scan on 1000 well-known TCP ports on target
   3. -sS = TCP SYN port scan
3. Nmap full-connect scan
   1. Type, nmap – sT 192.168.0.1
      1. -sT = TCP connect port scan (Default with root privilege)
4. Nmap XMAS scan
   1. XMAS scan works against linux machines but not windows
   2. Use Zenmap (nmap with GUI)
   3. In zenmap cmd type, nmap -sX 192.168.0.3
      1. XMAS scan very noisy (not stealthy)
      2. -sX switch sets FIN, PSH, URG flags but not SYN flag
      3. Port will be marked as closed if sends RST flag
      4. Port marked as open if no response received
   4. In zenmap cmd type, nmap -sX -reason 192.168.0.3
      1. Displays reason why a port is in certain state
5. Nmap ACK scan
   1. ACK scans not used for scanning ports to see if open/not as will not show ports in open state
   2. Shld be used with other switches to gain more info abt firewalls/IDS between target
      1. Used to determine rules of a filter
      2. Helps determine if firewall is stateless (blocks incoming SYN packets) or stateful (tracks connections & blocks unsolicited ACK packets)
      3. If RST packet received in response to ACK packet, port considered “Unfiltered”
   3. In cmd type, nmap -sA -p 80 192.168.0.1
      1. -sA = ACK switch
      2. -p = specify port num to scan (80 is HTTP)
      3. In this tutorial its unfiltered
6. Nmap ACK scan & Windows Firewall
   1. Go customise settings page In firewall > Private network settings > turn on windows firewall area > check “Block all incoming connections including those in list of allowed apps”
   2. Save changes
   3. Now should show as filtered
7. Hping3 SYN scan
   1. In cmd type, hping3 -8 0-5000 -S 192.168.0.1 (See above)
8. Hping3 ACK scan
   1. In cmd type, hping3 -c 1 -V -p 80 -s 5555 -A 192.168.0.1
      1. -c = packet count
      2. -V = verbose
      3. -p = specify port
      4. -s = base port from whr packets sent (which port to send in packet)
      5. -A = ACK flag
9. Hping3 XMAS scan
   1. In cmd type, hping3 -c 1 -V -p 80 -s 5555 -M 0 -UPF 192.168.0.1
      1. -M = sets TCP sequence number
      2. -UPF = sets URG, PSH & FIN flags
   2. 100% packet loss cuz XMAS doesn’t work on windows even though port 80 is open
      1. Windows can detect XMAS scan (but work on linux)

**OS Fingerprinting**

1. Use nmap (active OS fingerprinting) & P0F (passive OS fingerprinting) to identify OS running on remote hosts
2. Type, nmap -sS -0 192.168.0.1 192.168.0.4
   1. -sS = performs TCP SYN scan
   2. -0 = enables OS detection
   3. Performs 2 scans on 2 target IPs
3. P0f
   1. Connect target and host through XAMPP apache service
   2. In kali cmd type, p0f -p -l eth0
      1. -p = put listening interface in promiscuous mode
      2. -l = listen on specified interface
   3. Go to browser & access web service of target
      1. Can see p0f captured packets from target
      2. Can see SYN/ACK packets & OS from captured packets

**Mapping Networks with ManageEngine OpManager**

1. In zenmap cmd type, nmap -sn 192.168.0.1/24
   1. Click topology tab
   2. Select fisheye tab
   3. Click & drag any host point to focus/change view
   4. Select controls tab
2. Install ManageEngine OpManager
   1. Download & install
   2. In port selection panel page in Webserver choose 8443
   3. Keep default value at NetFlow box & select Next
   4. On select server mode page select “Standalone or Primary Server”
   5. On backend database for OpManager page select “POSTGRESQL”
   6. Click ok at manageengine opmanager box
3. Config manageengine opmanager
   1. Type localhost:8443 into address bar
   2. Manageengine login page
      1. Uid – admin, pwd -admin
   3. In opmanager admin page discovery input,
      1. Start IP – 192.168.0.1
      2. End IP – 192.168.0.255
   4. Click add credential button
      1. Click windows/WMI
      2. In name box type Windows Credentials
      3. In domain name/username box type – PRACTICELABS.COM/Administrator
      4. Password – Passw0rd
   5. Save
   6. Under discover-interface keep default settings & NEXT
   7. Under discovery-schedule keep default settings
   8. Under discovery-schedule email notif keep default
   9. Under discover-summary save & execute
   10. Opmanager will now scan network to map available devices
   11. Select invent tab on left side
   12. Click dashboard to view overall network info

**Enumeration Tools**

1. Enumeration is defined as a process which establishes an active connection to the target hosts to discover potential attack vectors in the system, and the same can be used for further exploitation of the system.
2. Nslookup
   1. Type, nslookup
      1. In nslookup, server 192.168.0.1
         1. (pretend that 192.168.0.1 is DNS server)
      2. Type, set type=any
         1. Retrieve all records from server
      3. Type, ls -d practice-labs.com
3. Dig (Domain Info Groper)
   1. In kali type, dig axfr practice-labs.com 192.168.0.1
      1. Axfr = provide complete listing of domain records
      2. Server we using not vulnerable to DNS zone transfers so will not see successful outputs
4. Psinfo
   1. In cmd type, Psinfo.exe [\\192.168.0.1](file:///\\192.168.0.1) -h -d (must cd to dir with the exe first)
      1. -h = displays listing of installed hotfixes
      2. -d = displays info related to disk volume
   2. Shows windows version, CPU etc.
5. Finger
   1. In kali type, finger -s root
      1. Displays info abt all users available on system
      2. Shows logged in users, login time etc.