**Module 3 Scanning & Enumeration**

**3.2 Banner Grab**

**Fragmentation**

1. Breaking
   1. Breaking up packets into smaller chunks to get past IDS
   2. Break up packets so IDS doesn’t know what we actually want
2. Colasoft Packet Builder
   1. Use for breaking

**ICMP (Internet Control Message Protocol)**

1. ICMP Message Types & Description/important Codes
   1. 0: Echo Reply – answer to Type 8 Echo request
   2. 3: Dest unreachable – 0, 1, 6, 7, 9, 10, 13
      1. 0 – dest network unreachable
      2. 1 – dest host unreachable
      3. 6 – network unknown
      4. 7 – host unknown
      5. 9 – network administratively prohibited
      6. 10 – host administratively prohibited
      7. 13 – communication administratively prohibited
   3. 4: source Quench – congestion control msg
   4. 5: Redirect – 0 (Redirect network), 1 (redirect host)
   5. 8: Echo request – ping msg that requests echo reply
   6. 11: Time exceeded

**Port Scanning**

1. Types of port scans
   1. Full-Open – AKA TCP connect & full connect
      1. Runs 3 way handshake on all ports
      2. Easy to detect
   2. Half-Open (Stealth/SYN) – no completion of 3 way handshake
      1. No ACK to complete
   3. Inverse TCP – uses FIN, URG, PSH flags
      1. No response = port open
   4. XMAS – doesn’t work on Windows (as RFC 793)
      1. Sends all sorts of packets to get info (works on linux)
   5. ACK – ACK packet sent & header reviewed for RST packet TTL 64<
      1. If Time to Live is < 64
   6. IDLE – spoofed IP address

**NMAP**

**Banner Grabbing**

1. Find out what OS target using
   1. Eg. run Telnet on port 80 (HTTP) then it run error msg revealing server info

**DNS Zone Transfers**

1. Get info like name servers, MX records

**Source Routing**

1. Attacker forces path/route for router instead of it choosing the shortest path

**Enumeration**

1. Discovering diff hosts/devices on network
2. A lot of scanners alrdy have enumeration

**Vulnerability Tools**

1. OpenVAS
2. Nessus

**Vulnerability Scoring System**

1. Common Vulnerability Scoring System (CVSS)
2. Score – 0 to 10

**Vulnerability Management Lifecycle**

1. Discover
2. Prioritise asset
3. Assess
4. Report
5. Remediate
6. Verify
7. Back to num 1

**Vulnerability Assessment Solutions**

1. Garner
   1. analyse products and reports to give VAS

**Banner Grabbing Tutorial**

1. Enable web services
   1. Enable apache & DVWA on port 80 for test
   2. In browser go to 192.169.0.1/dvwa/login.php
      1. Apache version shown as Error 404
2. telnet
   1. use to tell apache ver & info of server
   2. in cmd type, telnet 192.168.0.1 80
      1. 80 = port 80 (HTTP)
      2. Established connection to device
   3. Type, GET /dvwa/HTTP/1.1 (This in telnet)
      1. GET = obtains data from web server
      2. HTTP – protocol to connect with
   4. Type, Host: 192.168.0.1
      1. Press enter a few times
3. Netcat
   1. In kali type, nc 192.168.0.1 80
      1. Type, GET /dvwa/HTTP/1.1
      2. Host: 192.168.0.1
      3. Press Enter a few times
4. Nmap
   1. In kali type, nmap -sS -p 80 -A 192.168.0.1
      1. -sS = SYN scan
      2. -p = port
      3. -A = aggressive mode
   2. Shows apache, windows OS, server info, running ports etc.