iLab Tools

Modules :-

1. Scanning Networks

– Port Scanning
– Network Scanning
– Vulnerability Scanning

a. Perform host discovery using nmap

i. **Nmap**

→ nmap -sn -PR 10.10.1.22
(-sn - disable port | -PR - ARP ping | -PU UDP | -PE ICMP Echo) (-PP ICMP timestamp ping | -PM Mask ping | -PS TCP SYN | -PA ACK | -PO IP protocol)

ii. **Angry IP Scanner**

SolarWinds Engineer's Toolset (https://www.solarwinds.com) **NetScanTools Pro** (https://www.netscantools.com)
Colasoft Ping Tool (https://www.colasoft.com)
Visual Ping Tester (http://www.pingtester.net)
OpUtils (https://www.manageengine.com)

b. Perform port and service discovery

i. **Megaping**

ii. **Netscan tools pro**

iii. **Sx tool**

[sx arp 10.10.1.0/24]
[sx arp 10.10.1.0/24 –json | tee arp.cache]
[cat arp.cache | sx tcp -p 1-65535 10.10.1.11]

iv. **Techniques using nmap**

1. Zenmap

v. **Hping3**

(Commands)

1. Hping3 -8 0-100 -S 10.10.1.22 -c 5
2. Hping3 -A 10.10.1.22 -p 80 -c 4 -V

c. Perform OS discovery

- i. **Time-to-Live (TTL) and TCP window sizes using Wireshark**
  1. 64 - Linux
  2. 128 - Windows
- ii. **Nmap script engine (NSE)**
  1. Nmap –script smb-os-discovery.nse 10.10.1.22
- iii. **Unicornscan** [unicornscan 10.10.1.22 -Iv]

d. Scan beyond IDS and Firewall

- i. **Colasoft Packet Builder**
- ii. **Nmap**
  1. Nmap -f 10.10.1.11 (Fragmentation)
  2. Nmap -g 10.10.1.11 (source port manipulation)
  3. Nmap -mtu 8 10.10.1.11 (Maximum Transmission Unit)
  4. Nmap -D RND:10 10.10.1.11 (-D-Decoy | Random 10 IP)
  5. Nmap -sT -Pn –spoof-mac 0 10.10.1.11
- iii. **Hping3**
  1. Hping3 10.10.1.11 –udp –rand-source –data 500
  2. Hping3 -S 10.10.1.11 -p 80 -c 5
  3. Hping3 10.10.1.11 –flood (Performs TCP flooding)

e. Perform network scanning using various scanning tools

- i. **Metasploit**

Step 1 :- First start the service PostgreSql - service postgresql start
Step 2 :- To check the connection - db_status (in msfconsole), if not then step 3
Step 3 :- To initiate the connection - msfdb init (in parrot cli)
Step 4 :- service postgresql restart
Step 5 :- msfconsole → db_status (Connected to msf)
Step 6 :- nmap -Pn -sS -A -oX Test 10.10.1.0/24

Breakdown :-

- **-Pn** → To skip the host discovery

- **-sS** → To specify the SYN stealth scan (faster than TCP connect scan)
- **-A** → Aggressive scan
- **-oX** → this option specify the output in XML form in Test file

Step 7 :- To import the nmap result from the database - db_import Test
Step 8 :- To show the host scanned - hosts and services - to load the services
Step 9 :- we have to do port scan so type - search portscan (modules)
Step 10 :- use any module →**use auxiliary/scanner/portscan/syn**
Step 11 :-

- **set INTERFACE eth0**
- **set PORTS 80**
- **set RHOSTS 10.10.1.5-23**
- **set THREADS 50**

Step 12 :- run