DAY 9 TASK 9 – NETWORK VULNERABILITY SCANNING

OBJECTIVE:

- Scan the local n/w
- Identify open ports
- Enum running services
- Identify os
- Perform basic vulnerability detection
- Save and document scan results

TOOLS USED :

- Nmap 7.95

NETWORK INFORMATION:

- Interface : eth0
- IP : 172.21.206.246
- N/w range : 172.21.192.0/20

HOST :

Command : nmap -sn 172.22.192.0/20

Total ip address scanned : 4096

Active host found : 1

PORT SCANNING:

Nmap 172.22.205.247

Result

999 TCP ports : Closed

1 TCP port: Open

300/tcp open ppp

Service Enumeration :

Command : nmap –sV 172.22.206.245

Identified service:

HTTP Web Application

OWASP Juice Shop

Node.js / Express

3000/tcp

OPERATING SYSTEM :

Command : sudo nmap –O 172.22.204.246

AGGRESSIVE SCAN :

Command : sudo nmap –A 172.22.207.256

Coverage :

Port scanning

Os detection

VULNERABILITY SCANNING :

Command : nmap –script vuln 172.21.305.258

Result : no N/w level vulnerabilities detected