Cyber Security

Class no 18

CIA 🡪 Fundamental concept

C – Confidentiality

I – Integrity

A – Accessibility

Defensive Security: Protect any system

Offensive Security: Testing security 🡪

* Penetration Testing(Ethical Hacking) : find any security gap
  + Information Gathering 🡪 BLACK BOX,WHITE BOX, Gray BOX
  + Network Scanning 🡪
    - Scanning IP address
    - Details scanning for one IP address
    - Find the open port for target IP address (0 to 65535 port)
    - Probe packet(without data packet): find response to become ensure port is open or not
    - Scanning tools:
      * Nmap/ zenmap
      * Hhping2/hpings
      * Masscan
    - Need to know 6 topic
* Red Teaming: advance and un-analogue testing.

Discovery Scan

* Nmap –sn –PR (target ip)
* 192.168.10.0/24
* From Terminal nmap –sn 192.168.10.0/24
* Find live ip : nmap –sn 192.168.10.0/24 🡪C block
* 17 hosts up mean 17 hosts are in live

┌──(root㉿kali)-[~]

└─# **nmap -sn 192.168.0.101/24**

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-04 13:32 EDT

Nmap scan report for 192.168.0.1

Host is up (0.0076s latency).

MAC Address: D8:32:14:63:32:E8 (Tenda Technology,Ltd.Dongguan branch)

Nmap scan report for 192.168.0.108

Host is up (0.00075s latency).

MAC Address: A8:41:F4:1D:81:D1 (Unknown)

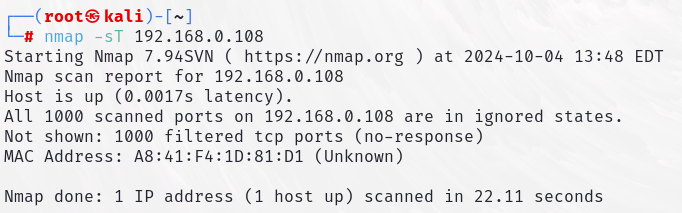
Nmap scan report for 192.168.0.101

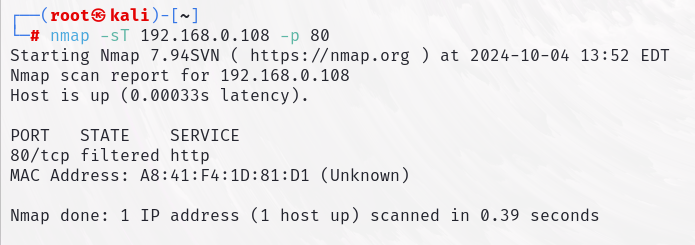
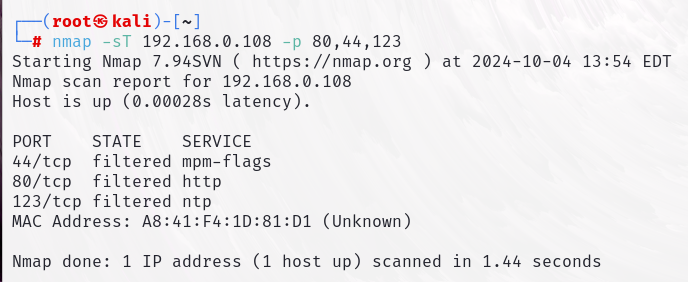
Host is up.

Nmap done: 256 IP addresses (3 hosts up) scanned in 2.13 seconds

Common scanning Techniques

* Metasploitable -2
* nmap –sT 192.168.10.100 (only 1000 port work) 🡪 It is the default TCP scan method. It completes the three-way handshake, making it easier to detect by firewalls.



* nmap –sT 192.168.10.100 –p 80 🡪for single port
* nmap –sT 192.168.10.100 –p 80,44,123
* nmap –sT 192.168.10.100 –p 80-1000
* nmap –sT 192.168.10.100 –p- 🡪for scanning all port (65535 port)
* nmap –sU 192.168.10.100 –p 80 🡪 for scanning UDP port