Bushra Akter

Class Number : 07

Date : 28 Sep 2024

**Theory Part:**

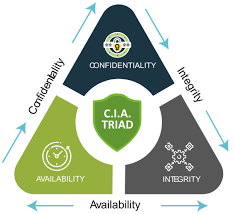
CIA:

CIA à Fundamental concept

C – Confidentiality

I – Integrity

A – Accessibility

****

Defensive Security: Protect any system

Offensive Security: Testing security à

· Penetration Testing(Ethical Hacking) : find any security gap

o Information Gathering à BLACK BOX,WHITE BOX, Gray BOX

o Network Scanning à

§ 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

·

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 àC block

· 17 hosts up mean 17 hosts are in live

Process of Scan IP:

· Information Gathering

· Network Scanning

· Enumeration

**Lab part:**

┌──(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

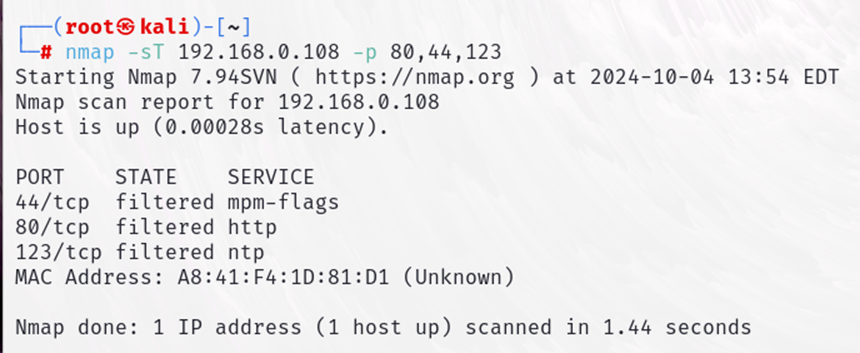
· nmap –sT 192.168.10.100 (only 1000 port work) à It is the default TCP scan method. It completes the three-way handshake, making it easier to detect by firewalls.



· nmap –sT 192.168.10.100 –p 80 àfor single port



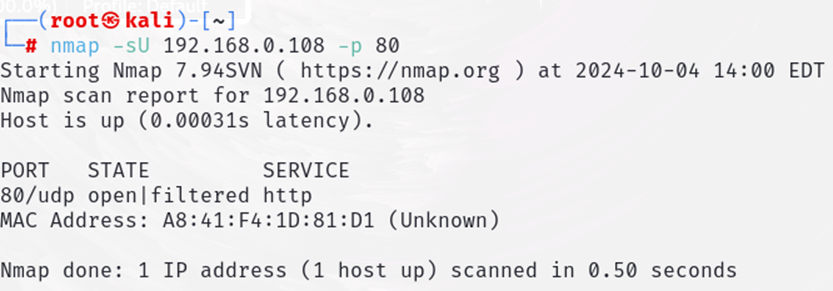
· nmap –sT 192.168.10.100 –p 80,44,123



· nmap –sT 192.168.10.100 –p 80-1000

· nmap –sT 192.168.10.100 –p- àfor scanning all port (65535 port)

· nmap –sU 192.168.10.100 –p 80 à for scanning UDP port



· nmap –sS 192.168.10.100 –p 80 à syn port à just check port is open or not,not send data



· open wireshark and run all above code in terminal

· nmap 192.168.10.100 –p 80 –sv à show service version (is it latest or old version)

· nmap 192.168.10.100 –p 80 –sv -O à for show operating system details

Nmap Scan Speed

· -T0-T5 (slow to fast search T1-T2..-T5)

· Normally use T4

· nmap 192.168.10.100 –p 80 –sv -T4

Inverse Scan (For bypass firewall)

· First send reset (allow firewall)

· If port in open, there was no any response and vice versa

· Download : Metasploitable-3 (Windows 2008)

· ping 192.168.10.100

· If ttl value 64,63 this is linux

· If ttl value 128,127 this is windows

· nmap 192.168.10.198 (showing blocking our ping probes)

· 2 technique for bypass

o –sX –xmass

o –sX –Maimon scan

· nmap 192.168.10.198 –sX –p 137,139,445 (if ip not work,create new ip on virtual box)

Scan Domain(when admin block any ip)

· nmap 192.168.10.100 –D RND:10 (open wireshark)

Enumeration (collect more details of target ip):

· SMTP Enumeration

o 25 port is open (email gateway)

o nmap –p 25 192.168.10.100

o telnet 192.168.10.100 25

o VRFY root (smpt command)

o VRFY test

o Hunter.io (collect mail ip service)

o quit for exit

o nano users.txt àctrl+Xàyàenter

o cat users.txt à show data

o smtp-user-enum –M VRFY –U users.txt –t 192.168.10.100 (M = mode U=user t=target)

o namp –p 2049 192.168.10.100 (p=port)

o showmount –e 192.168.10.100

o

Target – 192.168.10.100 à ping 192.168.10.100

If ttl value 64, 63 this is Linux

If ttl value 128, 127 this is windows

For find help menu à name –help example: namp –help

sudo passwd rootà change root password

su root à for switch to root