

Cyber Security

Class no 07

28 Sep 2024

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

Common scanning Techniques

- Metasploitable -2
- nmap –sT 192.168.10.100 (only 1000 port work)
- 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
- `nmap -sS 192.168.10.100 -p 80` → syn port → 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` → show service version (is it latest or old version)
- `nmap 192.168.10.100 -p 80 -sv -O` → 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 is 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
 - `-sX -xmass`
 - `-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
 - 25 port is open (email gateway)
 - `nmap -p 25 192.168.10.100`

- telnet 192.168.10.100 25
- VRFY root (smtp command)
- VRFY test
- Hunter.io (collect mail ip service)
- quit for exit
- nano users.txt → ctrl+X → y → enter
- cat users.txt → show data
- smtp-user-enum -M VRFY -U users.txt -t 192.168.10.100 (M = mode U=user t=target)
- namp -p 2049 192.168.10.100 (p=port)
- showmount -e 192.168.10.100
-

Target – 192.168.10.100 → 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 → name -help like: namp -help

sudo passwd root → change root password

su root → for switch to root

Process of Scan IP:

- Information Gathering
- Network Scanning
- Enumeration