Ethical Hacking Basics Course

By : Mohammad Askar
@Mohammadaskar2

Module 3
Information Gathering.

Definition of Information Gathering

Information Gathering means the proccess to collecting data and information about any of computer system components or about persons who manage the computer system.

Definition of Information Gathering

Information Gathering means the proccess to collecting data and information about any of computer system components or about persons who manage the computer system.

Types of Information Gathering

- Passive Information Gathering.
- Active Information Gathering.

Passive Information Gathering

- Collecting / Gathering data without interact with the real host (Company).
- Don’t excpect a lot of data.
- Examples :
  * Google /GHDB.
  * Whois.
  * Social Media.
  * Bing Search Engine.
  * TheHarvester.
  * Netcraft.

Google

- Use Google to collect (gather) data about the host.
- Examples :

  * site:www.example.com.
  * inurl:admin.
  * filetype:php.
  * intext:example.

Google Hacking Database

- Less targeted.
- random attack method.
- https://www.exploit-db.com/google-hacking-database/

Whois

- Great way to gather personal data such as Emails , Phone numbers , domain servers.
- Web interface.
  * http://www.who.is
- We can use it from terminal using whois command.

Social Media

- Twitter.
- Linkedin.
- Facebook.
- etc ..

Bing search engine

- Most common way to search for ip address.
- ip:127.0.0.1
- http://bing.com.

The Harvester

- Python script for gather emails.
- SHODAN support.
- Ex : python theHarvester.py -d microsoft -l 200 -b linkedin.

-d Domain.
-l Limit number of results.
-b Data source : google , linkedin , twitter ..

Netcraft

- Great source to know information about domains and servers.
- Web interface.
- Widely used by security guys.
- http://searchdns.netcraft.com.

Active Information Gathering

- Collecting / Gathering data by interacting with the real host (Company).
- Excpect a lot of data.
- Examples :
  * host.
  * ping.
  * dig.
  * nslookup.
  * netcat.
  * manual enumeration.

host command

- Performing DNS lookups.
- Mainly used to convert names to IP addresses.
- linux terminal command.
- simple type : host example.com.

host command arguments

- -4 for detecting ipv4.
- -6 for detecting ipv6.
- -t [query type] such as MX , A , CNAME etc ...

Dig command

- Tool for querying DNS nameservers for information about host addresses, mail exchanges, nameservers, and related information.

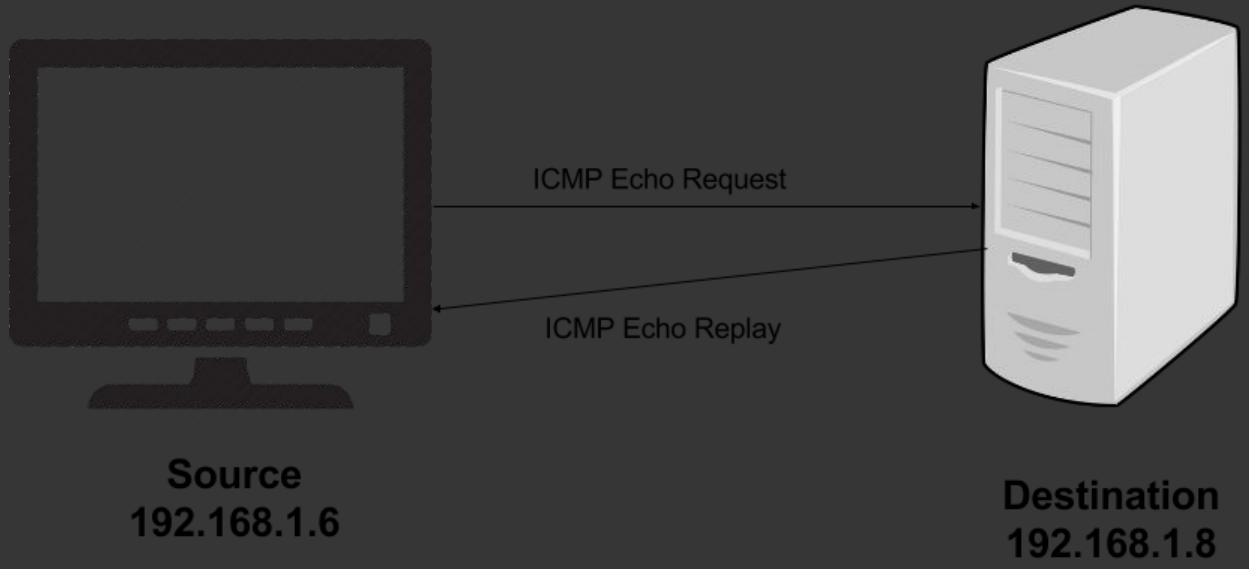
Nslookup

- Interactive mode.
- Non-interactive method.
- easy to use tool.

ping command

- Used to test the ability of the source computer to reach a specified destination computer.
- Internet Control Message Protocol (ICMP).
- Send Request (Echo Request) messages and wait for response (Echo Response).

ping command



Ping Sweep

- use this technique to detect all working (up) machines on the network.
- use the same technique that used by ping , but on multiple hosts.
- Write bash script to do that.
- Doing it using Nmap (Later).

Port Scanning

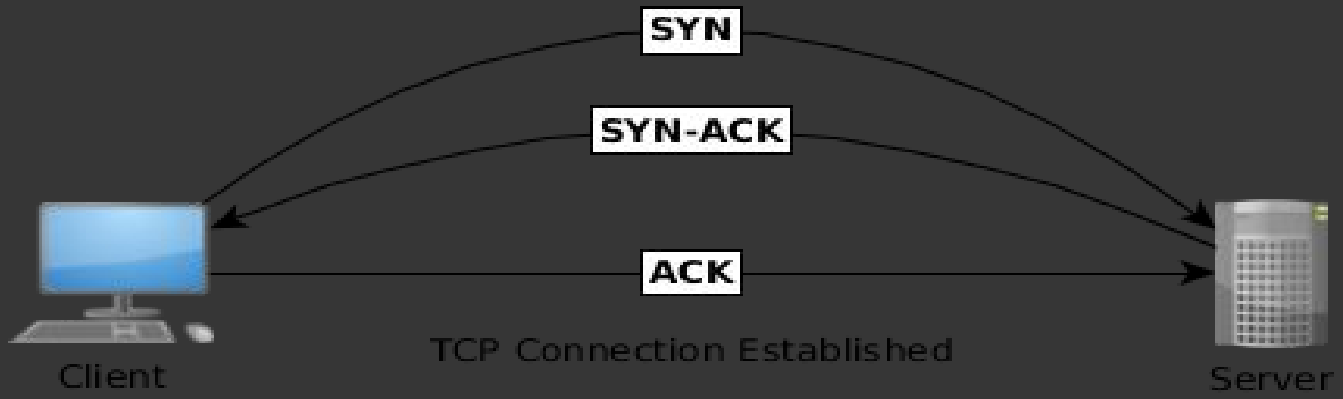
- Technique that used to detect all open ports and services on the target.
- Also we Could use Scanning technique to detect the target OS.

Transmission Control Protocol

- Known as TCP.
- The responsible protocol about data exchange on the network.
- We will have deep look on it later.

TCP - How it works

- Using Three Way handshake.



TCP segment structure

TCP Header

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Source port																Destination port															
4	32	Sequence number																															
8	64	Acknowledgment number (if ACK set)																															
12	96	Data offset				Reserved 0 0 0				N S	C W R	E C E	U R G	A C K	P S H	R S T	S Y N	F I N	Window Size															
16	128	Checksum																Urgent pointer (if URG set)															
20 ...	160 ...	Options (if *data offset* > 5. Padded at the end with "0" bytes if necessary.) ...																															

Banner Grabbing

- Technique used to gather information about a computer system on a network and the services running on it’s open ports.
- Manual Banner Grabbing using netcat.
- Using Nmap to perform Banner Grabbing.

Nmap

- Nmap - Network Mapper.
- The most popular scanning tool.
- Open Source tool.
- We can depend on it to perform port scanning , banner grabbing and much more.

Nmap

- Nmap has GUI called Znmap.
- Programmed by Lua programming Language.
- Nmap has many options and techniques to detect open ports and running services on the host.

Nmap Scan Types

- Syn Scan.
- TCP Scan.
- UDP Scan.
- TCP NULL, FIN, and Xmas scans.

Nmap Timing (-T)

- 0 = Paranoid.
- 1 = Sneaky.
- 2 = Polite.
- 3 = Normal.
- 4 = Aggressive.
- 5 = Insane.
- Example : nmap -T5 -sS 192.168.1.1

Identify Hostnames

- Do a simple DNS query for the specified ip.
- This allows you to find hostnames for all of the ip's in a subnet without having send a packet to the individual hosts themselves.
- Example : nmap -sL 192.168.1.0/24

Syn Scan

- SYN scan is the default and most popular scan option for good reasons.
- can be performed quickly, scanning thousands of ports per second on a fast network not hampered by restrictive firewalls.
- Port status could be open , filtered or closed.
- This technique is often referred to as half-open scanning, because you don't open a full TCP connection.

Syn Scan

- A SYN/ACK indicates the port is listening (open), while a RST (reset) is indicative of a non-listener.
- We can perform Syn Scan using -sS option.
- Example : nmap -sS 192.168.1.1

TCP Scan

- This scan is the default scan for nmap.
- This scan nmap will attempt a TCP SYN connection to 1000 of the most common ports.
- also will send icmp echo request to determine if a host is up.
- We can perform it using -sT option.
- Example : nmap -sT 192.168.1.1

UDP Scan

- Search for based on UDP services such as DNS:53 , DHCP:67/68 SNMP:161/162.
- very heavy and slow scan.
- Example : nmap -sU 192.168.1.1

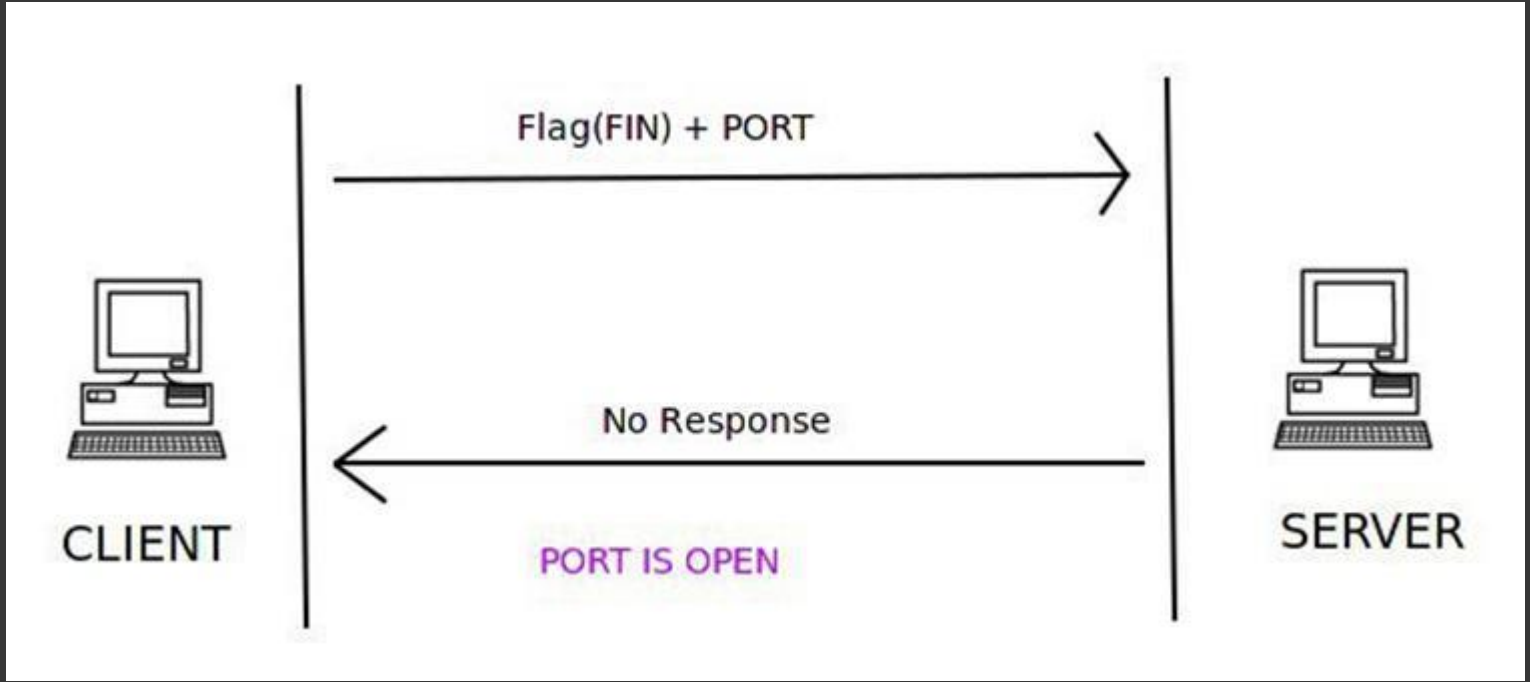
Xmas scan

- Work only with Linux OS.
- Send a packet with URG , FIN , PSH flags to the host.
- If the result was RST that means the port is closed.
- If the host ignored the connection , that means the port is open

FIN scan

- Work only with Linux OS.
- Send a packet with FIN.
- If the result was RST that means the port is closed.
- If the host ignored the connection , that means the port is open

FIN scan



Null scan

- Work only with Linux OS.
- Send a packet with 0 flags to the host.
- If the result was RST that means the port is closed.
- If the host ignored the connection , that means the port is open

Exporting Nmap Scan

- You can export nmap scan result to various types.
- -oN : export the result as normal output.
- -OX : export the result as XML file.
- -oG : export a deprecated result.

Netcat

- AKA The Swiss Army Knife.
- Great network pentesting tool.
- you can deal with both TCP and UDP protocols.
- https://www.sans.org/security-resources/sec560/netcat_cheat_sheet_v1.pdf


VICTORINOX

Nmap Scripting Engine

- Some extra Scripts that wrote especially for nmap.
- /usr/share/nmap/scripts/ - here you can find all scripts.
- https://nmap.org/nsedoc.