[Q]uantitative Project

The Road To Ethical Hacking

MercedCyber.tk

(4) TECHNICAL: INTRODUCING EVERYTHING NMAP

DETOUR

Access the deep web.

- TOR: The Onion Router
  - https://www.torproject.org/
  - Tor was United States Naval Research Laboratory employees.
  - Paul Syverson, Michael G. Reed and David Goldschlag
- Always wear protection.
  - VPN
    - https://www.betternet.co/

Never Enough

- Browse responsibly
- Safe Practices

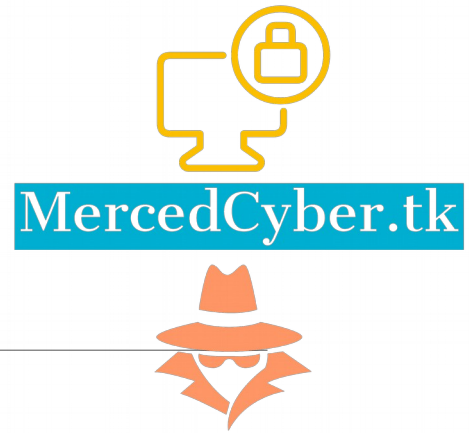
WARNING

MercedCyber.tk

Before network scanning make sure you have explicitly written permission. Or else contact your local laywer.

Tell your kids, friends, family and mistress that may not be around.

What is network mapping.



Network Mapping is an essential tool for managing networks.

- Are Systems online? Are they working properly? Is everything up to date?

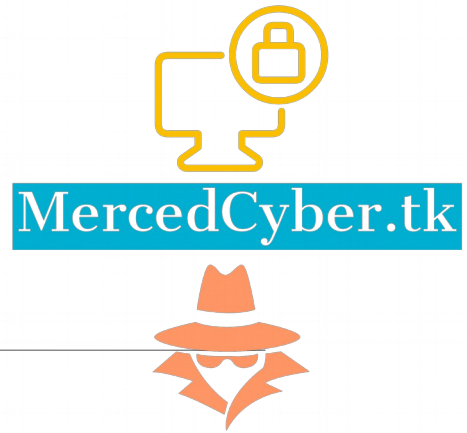
Using NMAP to determine the consequences of aggressive network traffic on systems.

- Will it network traffic crash systems? How much can a system take?

Why the Linux Command Line?

- NMAP is very powerful when it runs in the Linux Command Line.
- Many functionalities are exclusive to NMAP
- This is why we learned the Linux Command Line

Installing NMAP



The latest version of Nmap is 7.70

Use the Linux Command Line (Kali Has it preinstalled)

- Open Command Line (Install From Repositories)
- sudo apt-get update
- sudo apt-get install nmap

Windows, MacOS, Linux

- https://nmap.org/
- Windows: **nmap-7.70-setup.exe**

From the source *Optional,

wget http://nmap.org/dist/nmap-7.70.tar.bz2

tar xvf nmap-7.70.tar.bz2

-x : Extract, **-v :** Verbose , **-f :** filename

cd nmap-7.70

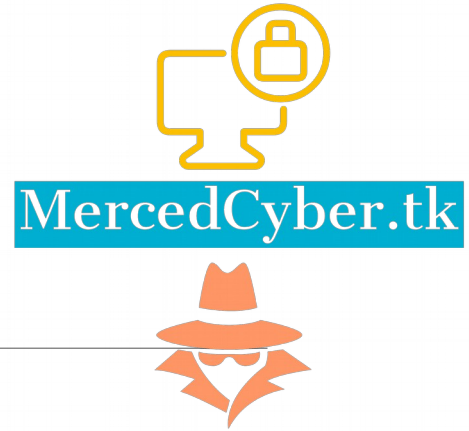
change directory

./configure

execute

sudo make install

Internet?



Local Area Network (LAN)

- Consists of many computer, but may only have one IP Address in the internet.
- Scanning inside the LAN gives you access to target machine.
- Use Ethernet and Wi-Fi
- Router with internet access.
- Router shares internet amongst devices.

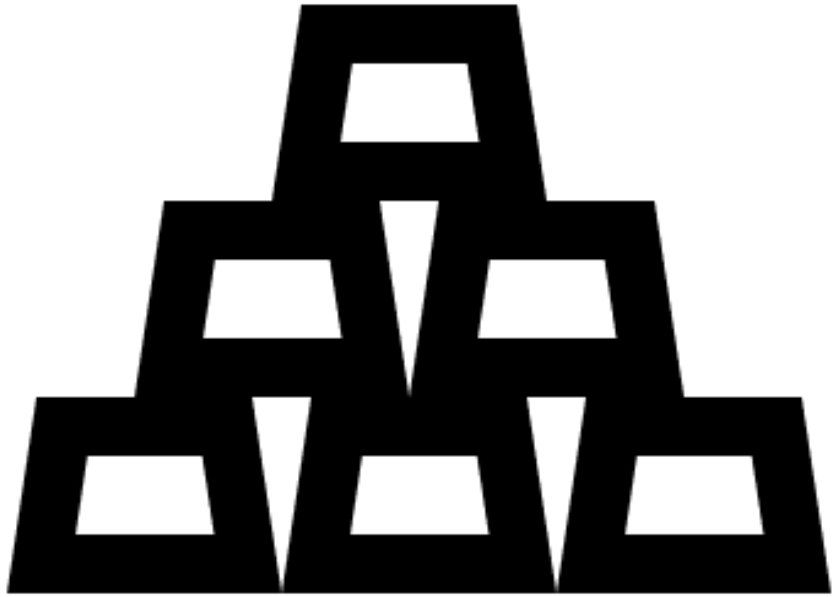
Outside LAN (Over the internet)

- Unable to see target machine.

Packets.

Information that travels from machine to another.

- Information is split into pieces, travel through the network, and assembles.
- **Transmission Control Protocol** (TCP)
  - Determines how packets of data are sent.
  - Sending an image through the internet.
    - TCP divides the image data into small pieces.

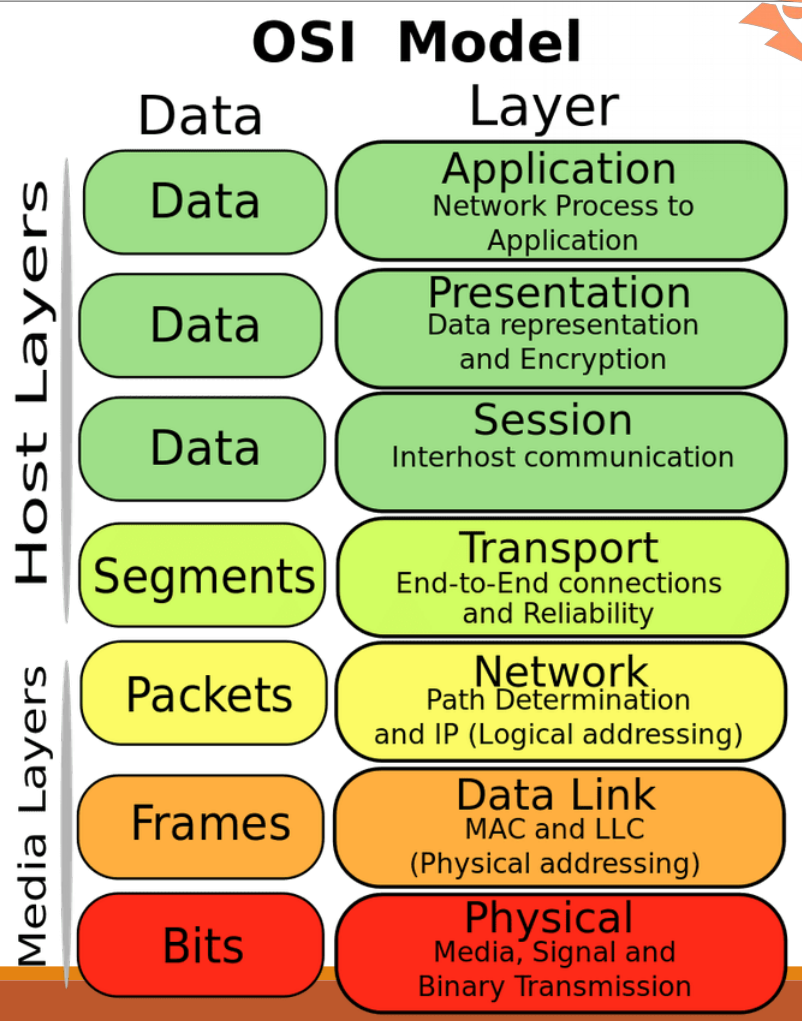


Open System Interconnection (OSI)

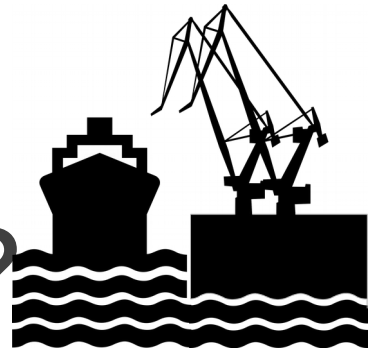
MercedCyber.tk

Information is not readily available.

- Capturing or viewing packets while they are moving is not very easy.
  - Wireshark – Can capture packets while in transit.



What is a port?



MercedCyber.tk

Accessing a network service.

- Client – Host

Computers

- Have 65,535 ports, may be open or closed

HTTP (Port 80)

- Hypertext Transfer Protocol
- From webbrowser to website.
- For webpages.

FTP (Port 21)

- File Transfer Protocol
  - Not very secure

The Gold Standard

- SSH (Port 22)
  - Secure Shell

IP ADRESS is an apartment building

Port is the apartment number (Rooms)

- 5200 Lake Rd, Merced, CA 9534
  - GLACIER (IP Address)
- GLCR 135 (Port)

Default Port Numbers

- Let’s assume GLCR only allows pizza deliveries.
- GLCR only allows sandwiches.

Example: 127.0.0.1:80

- IP Address 127.0.0.1
- Port 80, HTTP port.

[Q]uantitative Project

Thank You


RAMIRO GONZALEZ


RGONZALEZ69@UCMERCED.EDU


209-962-2524