[Q]uantitative
Project

The Road To Ethical Hacking

MercedCyber.tk

(7) TECHNICAL: THE END OF NMAP& BEGINNING APPLICATIONS

WARNING

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

!!!!!

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

Speed (Flags)

In order to not get detected or overwhelm the system, you should run scans at appropriate speed.

-T1 (Paranoid), -T1 (Sneaky), –T2 (Polite), -T3 (Normal), -T4(Aggressive), -T5 (Insane)

-T1 may take forever, but avoids detection

-T5 be careful.

NSE (Nmap Scripting Engine)

- Lua Programming language

This is an extension of Nmap. Recall Nmap just scans and nothing more. NSE however makes it possible for Nmap to interact, DoS, Exploit Vulnerabilities, do actual work.

Writing your own scripts makes Nmap more malleable.

https://nmap.org/nsedoc/

For now, just know that it exists, remember what NSE stands for, and read about it.

Go and find out more, write your own scripts.

```
sudo nmap –script-updatedb
```

updates the script database.

Internet Protocol (IP)

Public IP (Not hard to come by)

- Below I provide a tutorial of how to find other peoples public IP.

- https://bit.ly/2PGWJYc (Tutorial) Put in browser.

-Dynamic vs Static (Discuss)

Private IP (One can do damage)

- A little more work.

Discussion: What can you do with IP?

EDUCATIONAL PURPOSE ONLY: NOT FOR THE LIGHT OF HEART

Check this out: (PLEASE DO NOT CLICK ON THIS LINK OR OPEN IN BROWSER)

https://grabify.link/3FOJZA

Code: Z2JS3M

Why

By now you should have seen the commands and flag, have done some scans. Although we are limited by scanme.nmap.org, we should be familiar with what NMAP is capable of. Make sure you know IP, TCP, UDP, MAC Address…

Ending…….

We begin…….

https://ucmerced.box.com/s/ne9b3gyfgs2d3ubaxrdsurxihdc65nak

https://bit.ly/2OrPezQ

Password will be provided by discussion leader.

Vocabulary

LAN: Local Area Network (Private Internet protocol)

ISP: Internet Service Provider | (at&t, Verizon, ..)

IoT: Internet of Things | (devices)

Tools

A Linux Distribution

Do you have the following in a virtual machine? Choose one, for ubuntu you may have to download some tools. Kali Linux has tools pre installed.

1. Kali Linux
2. Ubuntu

Using Python Version 2

- Python 3 is the latest version, but since version 2 has been around for a while a lot of important libraries are in version 2.
- Open Command Line: Type✉ python2
  - exit() #to exit python
- If you do not have python version 2, install it.

Downloading libraries: (pip is a package manager)

- sudo apt-get install python-setuptools python-pip
- pip install github3.py #check it works, install trojan to be used later

Make a file in desktop and go into it.

mkdir ~/Desktop/playground

cd ~/Desktop/playground

Python 2

https://docs.python.org/2/tutorial/index.html

Task One: Using the Linux Command line and vim, create a file names welcome.py and output a message.

- “Welcome to MercedCyber”

What is a module?

“A module is a file containing Python definitions and statements”

- Basically, somebody wrote functions that are available to be used.
  - import math # here we define the function, by importing. (This is a comment)
  - Example: math.pow(4,2) #call the function

module: socket

https://docs.python.org/2/library/socket.html

Used to write TCP and UDP clients and servers.

▯ Open The Code and Run ✉

-TCP Client | Transmission Control Protocol

AF_INET : Standard IPv4 address/hostname

SOCK_STREAM : A TCP client

Task: Set up a TCP client and Server: Send messages

- https://www.keycdn.com/support/x-content-type-options

WARNING!

What you are about to learn is very dangerous, please take caution. Please don’t be evil.

What is NetCat?

http://netcat.sourceforge.net/

How do you establish a connection between systems? netcat

A client and a server. For chatting, file transferring and port scanning. (Backdoors)

- Sys admins generally make sure net cat is not installed in their systems why?

How would you find IP address.

https://www.advanced-ip-scanner.com/

using NMAP (recall) nmap –sn 192.168.1.0/24

Android

https://play.google.com/store/apps/details?id=com.myprog.netutils&hl=en_US

Kali (Linux)

netdiscover –p (To not get caught, may take a while)

----

your IP: hostname -I

Hands on

To open a port using netcat, type in the following.

- nc -l -p 666
  - -l stand for listener, p is for port. You are listening in port 666

You are listening, but for what?

The client.

- nc Local_IP 666

You may face a problem here. When binding, why would you receive “permission denied”

opening port 666 may be reserved. Ports below 1024 are called “privileged ports”

- You can send messages, and so what? why not just use Facebook?

Remote Control (Open File on GitHub)

Server:

```
nc –Lp 666 –vv –e cmd.exe
```

Client:

```
nc 192.0.0.1 666
```

[Q]uantitative Project

Thank You

RAMIRO GONZALEZ & LORENZO SCATURCHIO

RGONZALEZ69@UCMERCED.EDU

209-962-2524

MercedEnergy.com