Introduction to Pentesting

Make sure you have Kali ready :)

UMASS CYBERSEC CLUB

Women in Cybersecurity Chapter Planning

Aspiring Leaders are wanted to establish a new **Women in Cybersecurity Chapter at UMass**

- (Participation is not mutually exclusive with the UMass Cybersecurity Club)

Great Benefits!

- Scholarships
- Job Fairs & Career Workshops
- Exclusive Conferences & Competitions
- Skillbuilding
- Advocacy

Interest Form (Leadership or Members)

UMASS
CYBERSEC
CLUB

DISCLAIMER

All content covered is purely for educational/informative purposes!

Please don’t utilize anything learned here to do anything stupid.

DISCLAIMER

All content covered is purely for educational/informative purposes!
Please don’t utilize anything learned here to do anything stupid.

<u>AND ILLEGAL.</u>

UMASS CYBERSEC CLUB

What is Pentesting?

Ethical Hacking: A company hires you to simulate being an attacker, in order to find, exploit, and report vulnerabilities.

- “Pretending to be evil”.

Network

Web

Mobile

Stages of Pentesting

Open Source Intelligence (OSINT)

- Gather publicly available information on target

Enumeration

- Run various scanning tools on target, and gather information about running services, software they run, etc

Exploitation

- Use the previously gathered information to exploit a vulnerability you found to gain control over the system

Post Exploitation

- Escalate privileges and pivot to other machines in the network to gain **complete control over the entire network**

Some Essential Networking Knowledge: IP

- **IP Address:** identifies device on network or the internet so data can be routed to correct destination.
  - **IPv4**: 4 numbers (each between 0 to 255) separated by dots.
  - **localhost:** 127.0.0.1
  - ***ifconfig*****:** Linux command to get IP address

123.89.46.72

IPv4 IP Address example

Some Essential Networking Knowledge: Ports

Port: Each IP address has 65535 ports that help with sorting network traffic.

- Different network protocols happen different at port numbers (0-1023 are well defined)

Network Protocol	**Port Number(s)**
SSH	22
HTTP/HTTPS	80/443
SMB	139/445

Netcat

A powerful networking tool to send and receive information over different protocols.

- Main tool used to catch reverse shells.

> Demo Time!

UMASS CYBERSEC CLUB

Netcat Demo

Try it yourself! See if you can connect to yourself as localhost and then connect to our device on:

IP - 52.72.210.209

Port - 12345

Listener - `nc -lvp <PORT #>`

Client - `nc <IP Address> <PORT #>`

Some More Essential Knowledge: Server

A specialized device or software that provides functionality for other devices.

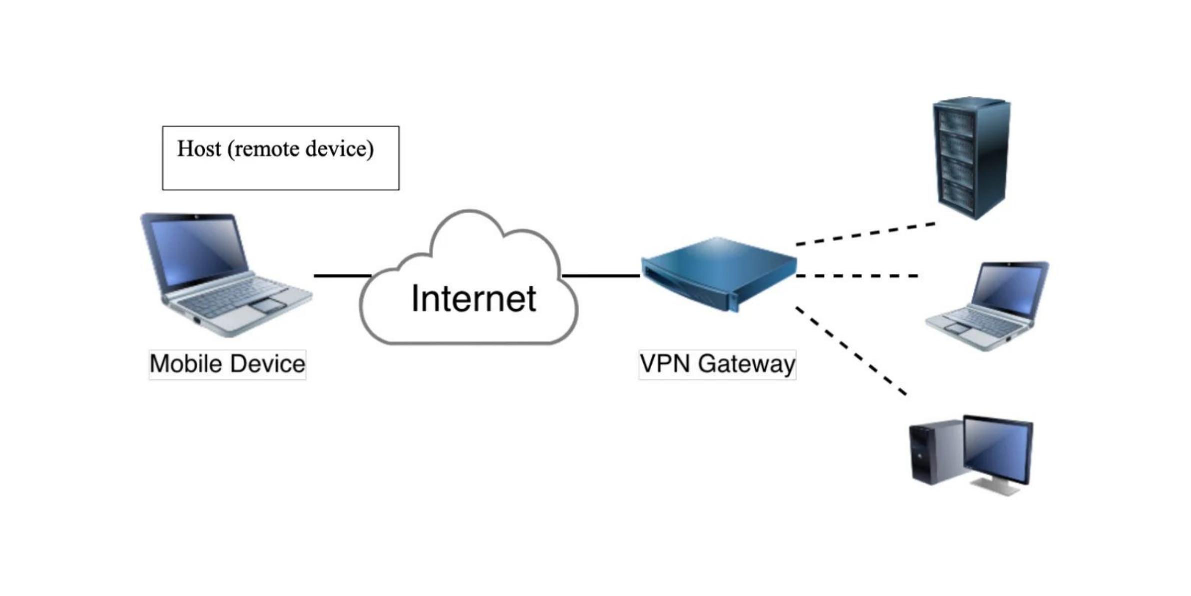
Example: web servers, email servers, Minecraft servers, etc.

Client - requests services/information from server

UMASS CYBERSEC CLUB

Virtual Private Network - VPN

Creates a tunnel between us and another network.

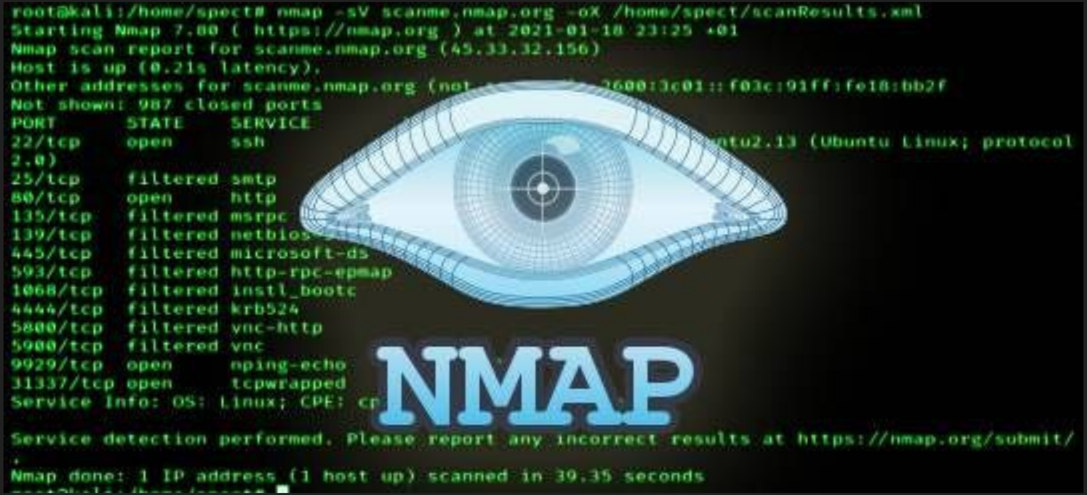


Nmap

Mostly wide used port scanner used to get information about targets

Provide an IP address and will identify ports and their service version

Includes a scripting engine for finding specific exploits



```
root@kali:/home/spect# nmap -sV scanme.nmap.org -oX /home/spect/scanResults.xml
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-18 23:25 +01
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.21s latency).
Other addresses for scanme.nmap.org (not                  2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 987 closed ports
PORT       STATE    SERVICE
22/tcp     open     ssh                                      ntu2.13 (Ubuntu Linux; protocol
2.0)
25/tcp     filtered smtp
80/tcp     open     http
135/tcp    filtered msrpc
139/tcp    filtered netbios
445/tcp    filtered microsoft-ds
593/tcp    filtered http-rpc-epmap
1068/tcp   filtered instl_bootc
4444/tcp   filtered krb524
5800/tcp   filtered vnc-http
5900/tcp   filtered vnc
9929/tcp   open     nping-echo
31337/tcp open     tcpwrapped
Service Info: OS: Linux; CPE: cp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 39.35 seconds
```

Nmap Practice

Try doing a nmap scan on **52.72.210.209** and discuss the following with the people around you:

- **Number of services open**
- **Port numbers**

Then try doing it with the -sV for service enumeration and discuss what happens:

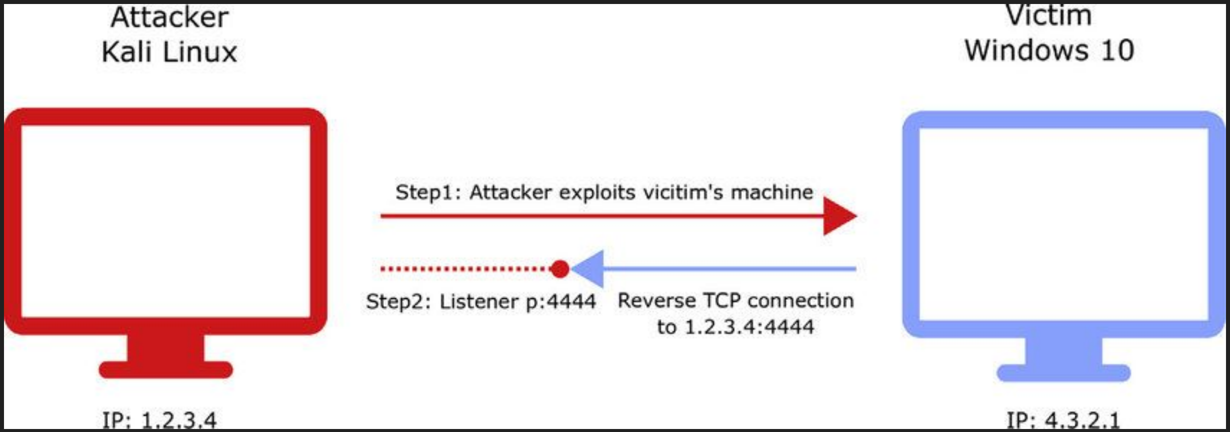
Finding Exploitable Services

- Use Google to search for versions of service and look for vulnerabilities
  - ***Example***: Apache 2.2.11 exploit
- Large public database - exploit-db.com
- **Searchsploit** - search for exploits using enumerated info
  - manual
- Online cheat sheets - Google: *hacktricks <service name>*

Shell and Reverse Shell

Shell: program that can execute commands that interact with your computer's operating system

Reverse Shell: a shell connection that allows you to make commands to a remote machine (revshells.com - DEMO on netcat)



UMASS CYBERSEC CLUB

Metasploit!

Multifunctional Pentesting tool used to automate process of running and finding exploits

> DEMO TIME!!! icecast

Open by typing in Kali terminal: **msfconsole**

Cheatsheet

Collegiate Pentesting Competition (CPTC)

- Given fictional company infrastructure to hack and team that finds the most vulnerabilities
- Defending New England Champion
- Talk to us **ASAP** (after the workshop) if interested!
  - We have a deadline of **tomorrow** to finalize the team!

UMASS
First Place
To represent this regional at the Global CPTC Finals, January 2023 in Rochester, NY

Hands on Practice

Blue Lab: https://tryhackme.com/room/blue

1. Register and login to **TryHackMe.**
2. Go to the room by visiting the link above.
3. Click "*Start Machine*".
4. **CONNECT USING THE OPENVPN CONFIG. VERY IMPORTANT!**
5. Use **Nmap** to see what services are running.
6. Run vulnerability checks with **Nmap.**
7. Exploit with ***msfconsole***.

How to Learn More?

- **Vulnerable machines to hack:** hackthebox.com
  - Write-ups for retired boxes can be found here: IppSec
- **TryHackMe**: tryhackme.com
- **Red Team/Blue Team Simulations** *(one this Friday)*.
- **COMPSCI 561**: System Defense and Test