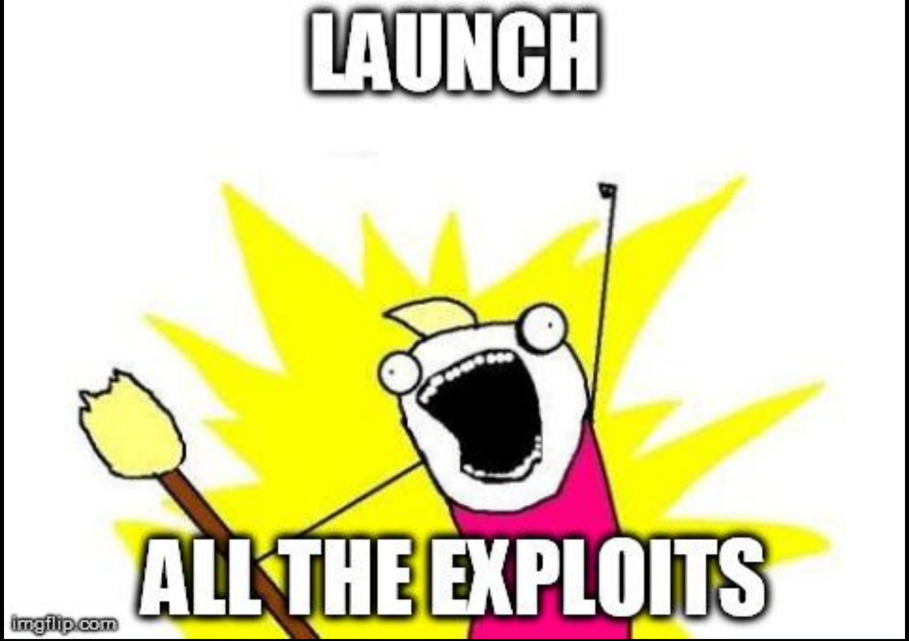
ACM Cyber

Nmap and Metasploit

https://tinyurl.com/CyberMetasploit


LAUNCH
ALL THE EXPLOITS
imgflip.com

Overview

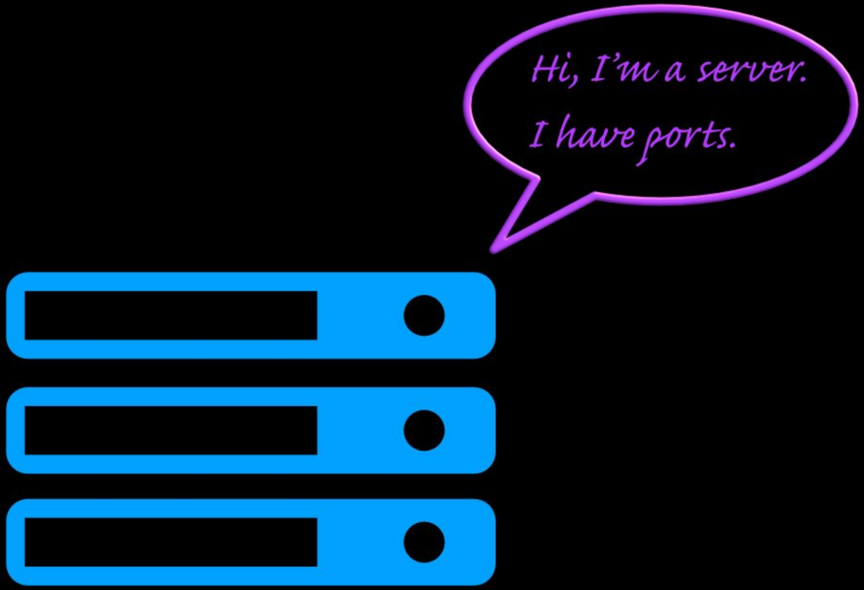
1) What’s a port?
2) Nmap
3) Demo & follow-along
4) Kahoot!
5) What’s Metasploit?
6) What are payloads?
7) Exploits
8) Demo
9) Kahoot

Nmap

Port scanning at your fingertips

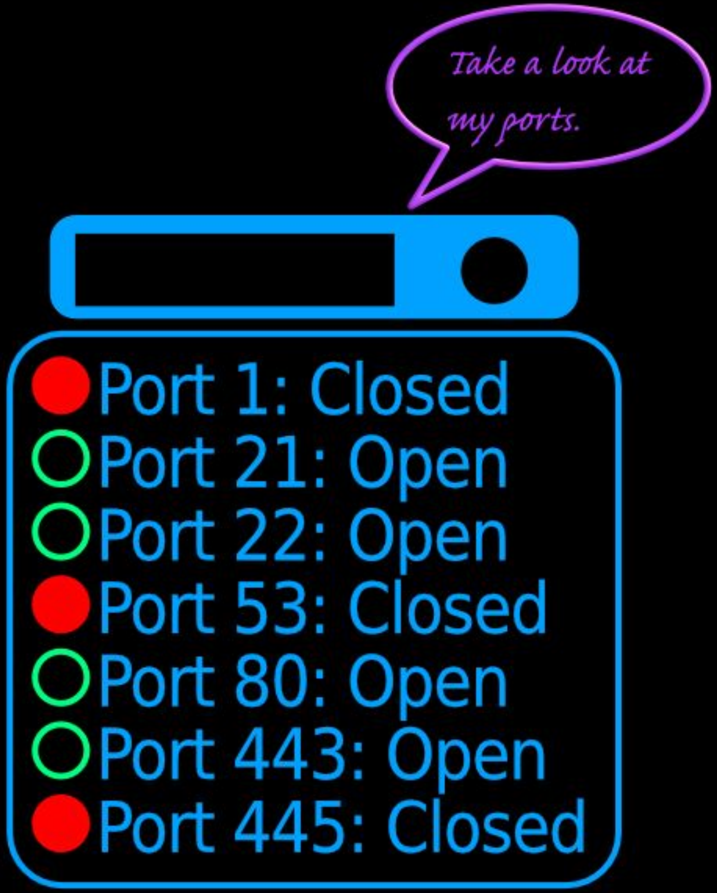
Wait, what's a port?

- A port is a number that identifies a service or a program
- When you connect to another computer, you need both an IP address and a port number
- This allows a computer to provide multiple services, simply by exposing them at different ports



Wait, what's a port?

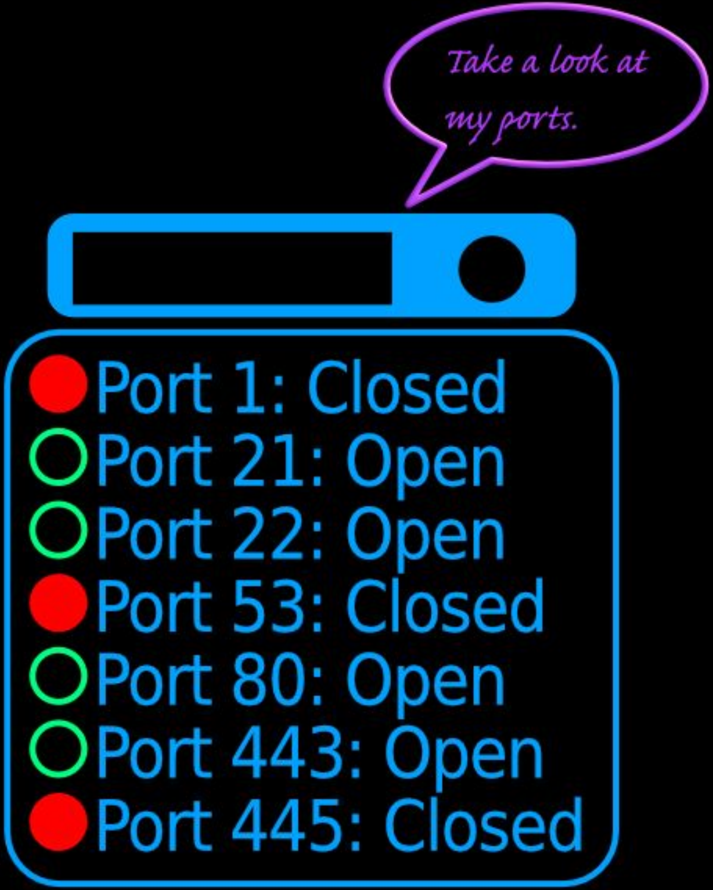
- A port is a number that identifies a service or a program
- When you connect to another computer, you need both an IP address and a port number
- This allows a computer to provide multiple services, simply by exposing them at different ports
- e.g. HTTP uses port 80



● Port 1: Closed
○ Port 21: Open
○ Port 22: Open
● Port 53: Closed
○ Port 80: Open
○ Port 443: Open
● Port 445: Closed

Wait, what's a port?

- **Open port**: a program is running and ready to accept traffic from this port
- **Closed port**: no program is running to accept traffic from this port



● Port 1: Closed
○ Port 21: Open
○ Port 22: Open
● Port 53: Closed
○ Port 80: Open
○ Port 443: Open
● Port 445: Closed

nmap

- A port scanning tool, against a single machine or a network
- Can tell you which ports are open, closed, or filtered
  - And hopefully, what programs are behind the open ports, and what operating system
  - Filtered ports: blocked by a firewall so nmap can’t determine open or closed

- How to install nmap:
  - On Kali Linux: already installed!
  - On Debian/Ubuntu (may be outdated): **`sudo apt-get install nmap`**
  - On a Mac: **`brew install nmap`**

Using nmap: basics

- **nmap -T4 *target.host.com***
  - This finds the open ports of the target
- **nmap -T4** -A ***target.host.com***
  - This additionally finds the OS and version numbers

Nmap example (your own computer!)

```
$ nmap -T5 127.0.0.1
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-17 14:25 PST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0011s latency).
Not shown: 499 closed ports, 495 filtered ports
PORT     STATE SERVICE
111/tcp  open  rpcbind
631/tcp  open  ipp
999/tcp  open  garcon
1021/tcp open  exp1
1023/tcp open  netvenuechat
2049/tcp open  nfs

Nmap done: 1 IP address (1 host up) scanned in 1.72 seconds
```

So nmap told me I have 6 ports open on my laptop among the ones it scanned.

Nmap example (port scanning SEASnet server)

```
$ nmap -A -T5 lnxsrv09.seas.ucla.edu
Starting Nmap 7.60 ( https://nmap.org ) at 2018-11-17 13:47 PST
Nmap scan report for lnxsrv09.seas.ucla.edu (164.67.100.209)
Host is up (0.0039s latency).
Not shown: 954 filtered ports, 45 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   1024 0f:66:9b:9e:db:e0:f7:af:d2:bb:af:53:aa:69:51:d1 (DSA)
|   2048 e3:e4:48:85:c2:81:53:ea:b6:d7:a0:cb:bd:f3:80:f5 (RSA)
|   256 fd:89:e8:84:93:8d:42:21:c3:d3:d2:79:05:6c:61:40 (ECDSA)
|_  256 77:a6:6e:81:c1:da:ed:98:17:9f:7f:7c:1a:af:36:d8 (EdDSA)

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 30.73 seconds
```

More options!

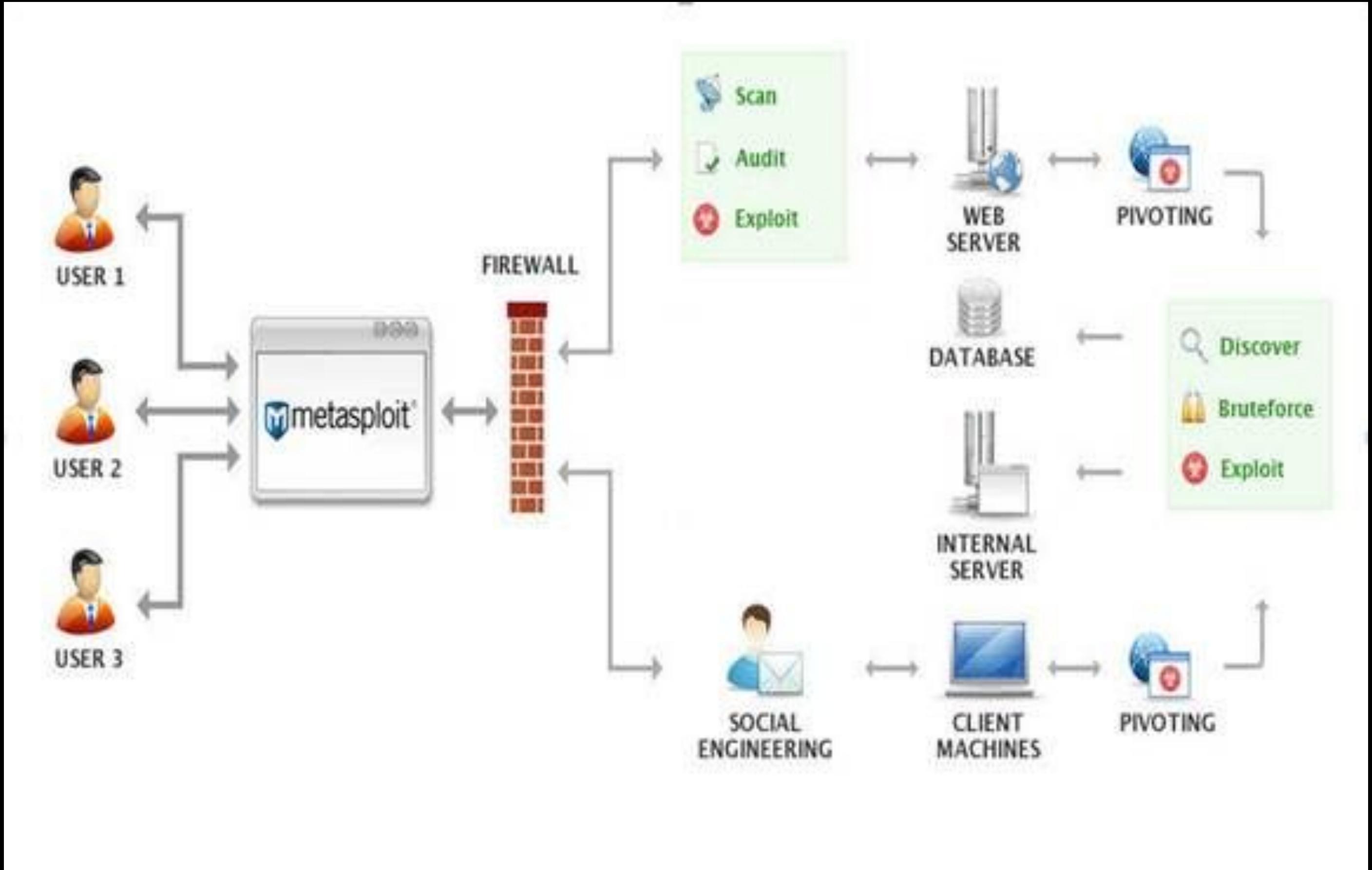
- -p: specify a port or port range to scan
  - -p22: scan only port 22
  - -p1-65535: scan absolutely every single port (slow)
- --spoof-mac: Spoof your MAC Address
- -S: Spoof your IP address
- -A: Enable OS detection, version detection, script scanning, and traceroute
- -T<number> timing:
  - -T0: paranoid: wait five minutes between each scan
  - -T4: aggressive: generally acceptable if you’re not doing anything bad
  - -T5: insane: very aggressive scanning
- Use Nmap with tor or a VPN to stay undetected/safe while using nmap!

Demo

Kahoot!

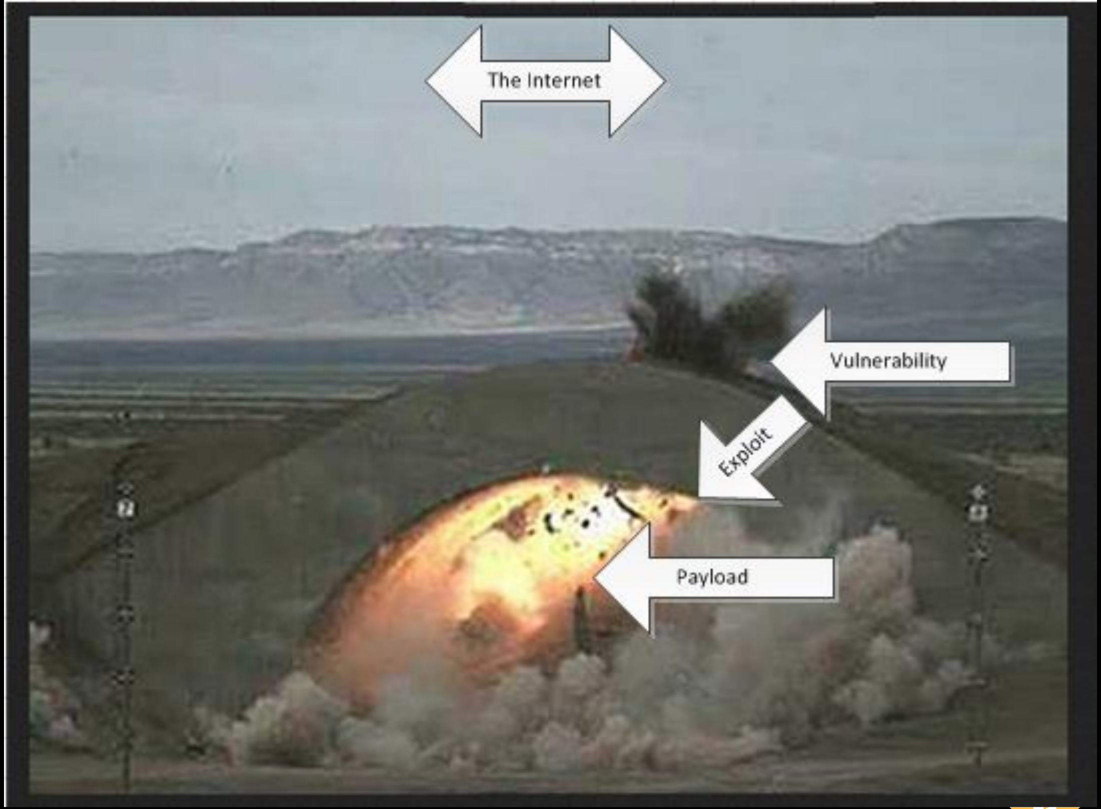
What is Metasploit?

- A tool to develop and execute malicious exploit code against a target machine.
- It has over 1677 exploits!
- Over 495 payloads!


USER 1
USER 2
USER 3
metasploit
FIREWALL
Scan
Audit
Exploit
WEB SERVER
PIVOTING
DATABASE
Discover
Bruteforce
Exploit
INTERNAL SERVER
SOCIAL ENGINEERING
CLIENT MACHINES
PIVOTING

What’s a payload?

- Payloads are **exploit modules**
- Metasploit has payloads in the form of command shell, dynamic payloads and Meterpreter.
- **Exploit** = Delivery system/missile
- **Payload** = Warhead



What does Metasploit do?

- Identify who you’re going to attack
- Find a vulnerability in the remote host you are going to attack
- Configure the payload to exploit the remote host
- Execute the payload

msfconsole: Common Commands

- **help**: Lists all commands and their usage
- **search**: Search for an exploit - can use keywords
- **info**: Find information about the exploit
- **show <parameter>**: Show information about exploits/payloads/info/options etc
- **use <exploit_name>**: Use the exploit, add it to payload
- **exit**: Closes Metasploit console
- **back**: Move from exploit context back to msfconsole

Vocab Time

- **RHOST** (Remote Host): IP address of who you’re attacking
- **RPORT** (Remote Port): Port address of the machine you’re attacking
- **LHOST** (Local Host): Your IP address
- **LPORT** (Local Port): Port address of your machine

Kahoot!

Join our Discord Server !

https://discord.gg/nbgxbjz

Demo

https://tinyurl.com/GuideToMetasploit

Thank you!

tinyurl.com/MetasploitFeedback