Cyber@UC Meeting 40

CEH Networking

If You’re New!

- Join our Slack **ucyber.slack.com**
- **SIGN IN!**
- Feel free to get involved with one of our committees: **Content, Finance, Public Affairs, Outreach, Recruitment**
- **Ongoing Projects:**
  - Malware Sandboxing Lab
  - Cyber Range
  - RAPIDS Cyber Op Center

Announcements

- We will be **running a CTF** at the **RevUC Hackathon**!
- Last Friday was **Board Game/Game Night**!!!
- **Sport Team Updates?**

Public Affairs

- Please fill out Google form for **GroupMe** Numbers! https://goo.gl/forms/94i9kMJgtpDGXsC22

- Our brand new **YouTube** channel has just been made. We will be live streaming meetings, events, etc and posting relevant videos to the channel. Please subscribe! youtube.com/channel/UCWcJuk7A_1nDj4m-cHWvIFw

Follow us on our social media:

Facebook:	facebook.com/CyberAtUC/
Twitter:	twitter.com/UCyb3r
Instagram:	instagram.com/cyberatuc/
Website:	gauss.ececs.uc.edu/UC.yber/

Weekly Content

A few ideas of who to speak with tomorrow

- 5/3 bank: a bank, duh
- Vantiv/Worldpay: credit card processing
- GE: sky boats and other cool stuff
- Future brands: home stuff like cabinets and security
- L3 Technologies: government contractors, offer cyber internship working under csirt manager
- Emerson: automation, had some full time cyber positions
- Intelligrated: materials development, had some cyber internships
- Lendkey: loans company
- Medpace: biomedical company, had some full time cyber jobs

Career fair (continued)

- Cincinnati insurance companies
- Total quality logistics: shipping company
- Military, maybe
- Macaulay-Brown inc.:government consultants
- Northrop Grumman Corporation: gov consultants
- Sogeti: lots of different things including cyber consulting it appears

Workshop 1: Systems Workshop

Insert comment that doesn’t pertain to anything here

The Topics Today Go Something Exactly Like This

- Tool Setup
  - OpenVPN
  - Nmap
  - MacChanger
  - WireShark
- Tool Demonstrations
  - Connect to VPN for UCIT Reasons
  - Nmap everything
  - Stealing someone’s identity with MacChanger and ifconfig
  - Playing in traffic with wireshark
- 127.0.0.1 on the range
  - Slowloris example?
  - Some kind of challenge in which the winner is given a large chunk of aluminum that has been licked by the exec group chat collectively

Put on your ~~3D glasses~~ Linux Distro now

Tool Rundown: OpenVPN

OpenVPN, it’s VPN and it’s Open.

- Remember that VPNs allow multiple computers to share a private network even if they aren’t physically connected
- OpenVPN also uses SSL/TLS certificates to encrypt the traffic between the server and clients
- The PiVPN project on github is a very easy way to setup an OpenVPN instance on mst debian based systems very quickly and easily, I highly recommend
- Install with **sudo apt install openvpn**

Tool Rundown: Nmap

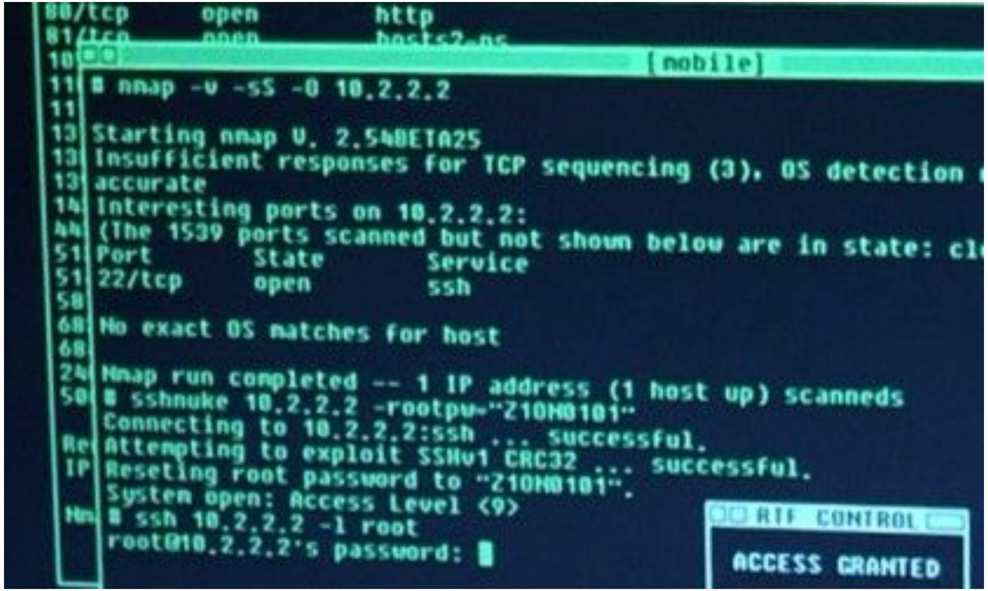
Nmap is the **best tool you will ever use**

Features Include:

- Host discovery via pings
- Port scanning
- Version detection of services
- OS detection
- Install with **sudo apt install nmap**

Tool Rundown: Nmap

Nmap was also featured in the Matrix (1999)



```
80/tcp      open        http
81/tcp      open        hosts2-ns
```

```
# nmap -v -sS -O 10.2.2.2

Starting nmap V. 2.54BETA25
Insufficient responses for TCP sequencing (3). OS detection
accurate
Interesting ports on 10.2.2.2:
(The 1539 ports scanned but not shown below are in state: cl
Port       State       Service
22/tcp     open        ssh

No exact OS matches for host

Nmap run completed -- 1 IP address (1 host up) scanneds
# sshnuke 10.2.2.2 -rootpw="Z10N0101"
Connecting to 10.2.2.2:ssh ... successful.
Attempting to exploit SSHv1 CRC32 ... successful.
Reseting root password to "Z10N0101".
System open: Access Level <9>
# ssh 10.2.2.2 -l root
root@10.2.2.2's password: █
```

ACCESS GRANTED

Tool Rundown: Zenmap

Zenmap is an extension to nmap that creates a GUI, if you have never used nmap before you may want to try Zenmap for now

Features Include:

- Premade Scan types
- Host List and inspection
- Network Graph
- Install with **sudo apt install zenmap**

Tool Rundown: ifconfig

Ifconfig is the de facto interface configuration tool for a lot of debian distro’s

Features:

- Display information about network interfaces
- Edit and modify network interfaces
- Install with **sudo apt-get install net-tools** if you don’t already have it

Tool Rundown: MacChanger

MacChanger is a very simple tool to change your MAC

Features:

- Change your MAC
- Install with **sudo apt-get install macchanger** if you don’t already have it

Tool Rundown: WireShark

A free and open source packet analyzer
Features Include:

- Can be used to intercept and read traffic from a number of protocols
- Supports Decryption
- Supports hundreds of protocols
- Industry standard for packet inspection

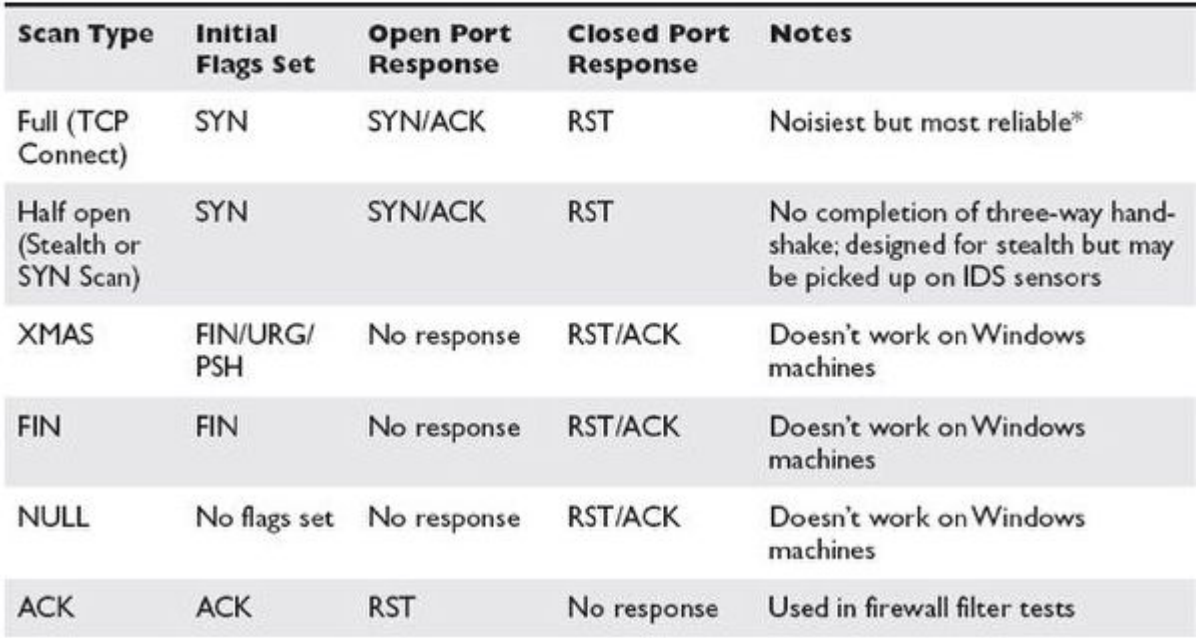
Hands On Demo Goals

- Connect to server via openvpn
- Identify your IP with ifconfig
- Open wireshark and filter on your IP
    - Watch this traffic when you scan
- Scan the network with nmap
    - Scan for OS's
    - Scan for services
- Change your IP with ifconfig
- Change your mac with macchanger

Tool Demonstration: OpenVPN

- The .ovpn files provided are premade for you to just join right away
- Only one machine per key (although not tested)
- **sudo openvpn --config keyfile.ovpn**
- We only have 40 keys ready so if we run out just say so and I’ll make a new one

Tool Demonstration: nmap



Scan Type	Initial Flags Set	Open Port Response	Closed Port Response	Notes
Full (TCP Connect)	SYN	SYN/ACK	RST	Noisiest but most reliable*
Half open (Stealth or SYN Scan)	SYN	SYN/ACK	RST	No completion of three-way handshake; designed for stealth but may be picked up on IDS sensors
XMAS	FIN/URG/ PSH	No response	RST/ACK	Doesn't work on Windows machines
FIN	FIN	No response	RST/ACK	Doesn't work on Windows machines
NULL	No flags set	No response	RST/ACK	Doesn't work on Windows machines
ACK	ACK	RST	No response	Used in firewall filter tests

Tool Demonstration: nmap

- **Ping Host discovery**: *nmap -sn 192.168.1.1-254*
- **Port scanning**: *nmap -p [PORTRANGE] TARGET*
- **Version detection of services**: *nmap -sV TARGET*
- **OS detection:** *nmap TARGET -O*
- **OS, Version, Traceroute, Script Scannning**: *nmap -A TARGET*

You can use multiple commands to make even more powerful scans.

Check out the cheat sheet posted in #links!

Tool Demonstration: Zenmap

Have people use tool for workshop

Tool Demonstration: ifconfig

Change your IP and Netmask: *ifconfig <IN-TER-FAC-E> <IP-/CI-DR>*

Take down/put up an interface: *ifconfig eth0 down/up*

Tool Demonstration: MacChanger

Randomize the Mac of an interface: *macchanger -r eth0*

Set specific Mac address: *macchanger -m b2:aa:0e:56:ed:f7 eth0*

Tool Demonstration: WireShark

Try filtering on your own IP!

Some Basic Commands:

```
ip.addr == 192.168.0.5
```

```
tcp.port == 80 || udp.port == 80
```

Al Level Challenge : Hidden Port

Find the hidden port, on 10.8.0.1, and what service it is running on it

Fun facts about aluminum

- Most abundant metal in the Earth’s crust but not naturally found it metallic form
- Until mass electrolysis became widely available, aluminum was more expensive than gold
- The top of the Washington Monument is an aluminum pyramid
- Aluminum rusts into alumina which is extremely corrosion resistant, allowing aluminum to be left in the elements without protective coating

Attack Demonstration: SloLoris

https://en.wikipedia.org/wiki/Slowloris_(computer_security)

Premise: use TCP to keep a large amount of connections open while using little bandwidth