Please open your **CSC436_Environment** Kali VM!!

Reconnaissance

Yes, we're still doing recon.

Penetration Testing Execution Standard (PTES)

1. Pre-engagement Interactions
2. **Intelligence Gathering / Reconnaissance**
3. Threat Modeling
4. Vulnerability Analysis
5. Exploitation
6. Post-Exploitation
7. Reporting

www.pentest-standard.org

Scanning Is Active Recon!

- Passive Recon == Using a telescope or binoculars to look for doors
  - Looking for anything that might tell us something about the target's network
    - Computers
    - Services
    - Accounts
    - IP Addresses
- Scanning == Actually knocking on the doors
  - Poking the machine to see what is there
    - Open Ports
    - Services
    - Existence of a machine…
    - Vulnerabilities

Active (anything) Requires Permission

- **YOU COULD GO TO JAIL**
- …don’t go to jail, please…
- **BUT YOU COULD GO TO JAIL**
- So make sure you have permission!

Do You Have Permission?

- In the IA Lab, you *generally* have permission.
  - Don't do dumb things.
    - You could still flood things.
    - You could still take systems down.
- On your own system, do what you want.
  - Host Only Mode!
    - You don't want any of this traffic flowing out to the interwebs.
- Stuff on the internet?
  - Just don't.

How do we find stuff?

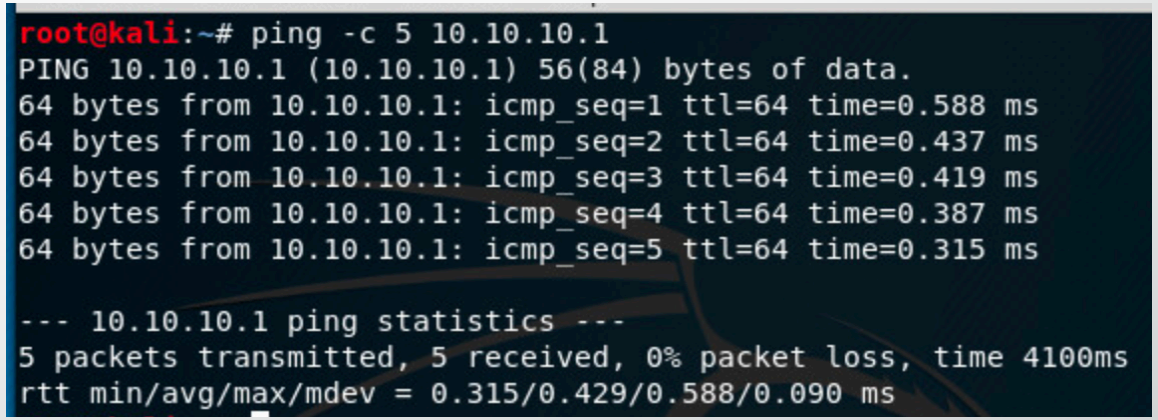
- So, you found all sorts of IP addresses through OSINT.
- Are they valid?
- Do they exist?
- Can you talk to them?
- Are they turned on?

ping

- Utility that allows us to test network comms
  - Reachability of a host
  - Round-trip time
- Internet Control Message Protocol (ICMP)
  - ICMP Echo Request
  - ICMP Echo Reply
- When you send an ICMP Echo Request to a computer, it *should* respond with an ICMP Echo Reply
  - More on that *should* part in a moment…

Let's Test It

- Open your Kali VM
  - CSC436_Environment vApp
- What's your IP address?
  - Should be 10.10.10.X
- Ping your default gateway
  - `ping -c 5 10.10.10.1`



How is it Useful?

- Take each of the IPs we found through OSINT, and ping it.
  - See if it's alive
- Ping a range.
  - This is called a Ping Sweep
  - But that's a lot of typing…

Enter… FPing!

- Built in to Kali, can download for Windows
- Common Switches…
  - -a Only shows systems that are alive
  - -g Generate a list from a netmask, or starting and ending IP.
  - -s Generate statistics at the end
  - Otherwise, `man fping`

Some Gotchya's

- If the computer is temporarily turned off, will it respond?
- Firewalls could block ICMP
  - Network firewalls
  - Host-based firewalls
- This certainly is LOUD. Very well could be logged.
  - Are ping sweeps normal?

Something Else?

We Found Alive Hosts… Now What?

- Deeper scanning.
- Port Scans.

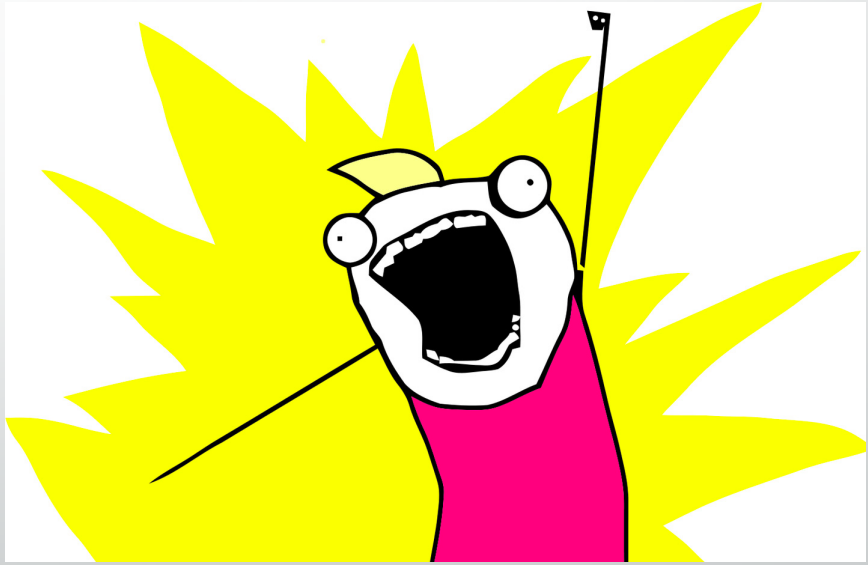
- (This is still active stuff, you require permission.)

What's a Port?

- A door, or pathway into your computer.
- This box has a number of holes, let's call them ports.
- To get in the box, you need to know what shapes are there, what shapes are "open"
  - Same thing with computer ports – you need to know what port is open
- Multiple blocks could enter the cube at the same time
  - Simultaneous communication on your computer.

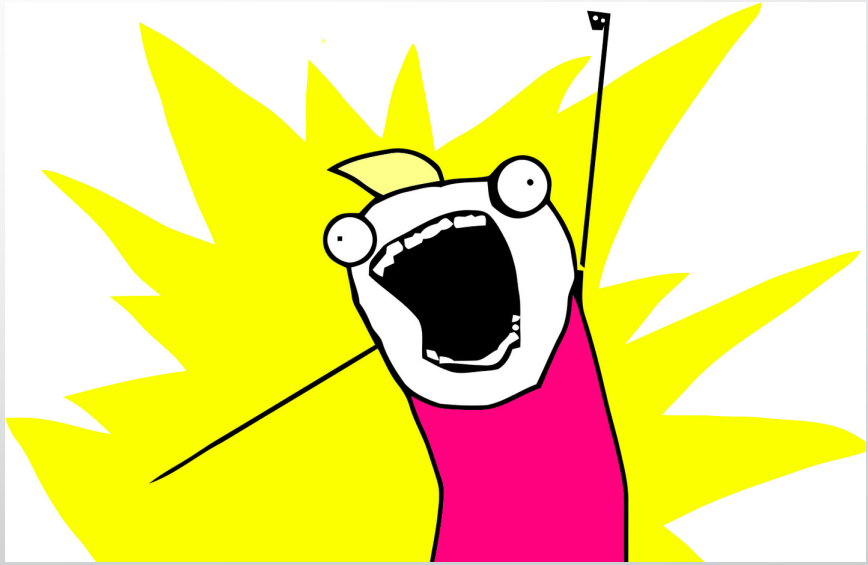
All The Ports

- How many are there?



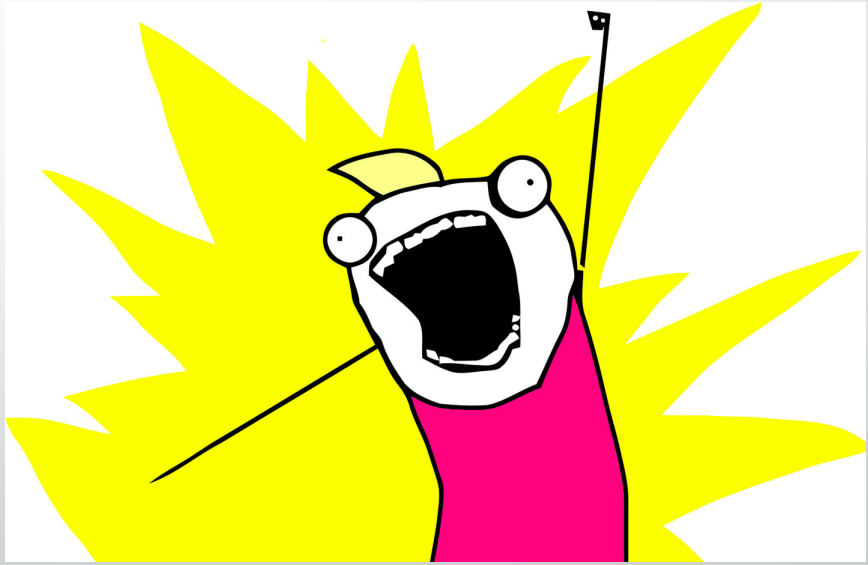
All The Ports

- How many are there?
  - 65,535
- How many ports in a /24 network block?



All The Ports

- How many are there?
  - 65,535
- How many ports in a /24 network block?
  - 256 * 65535 = 16,776,960



Ports -> Services. Sometimes

- Well Known Ports
  - Ports 1024 and below
  - Have a service assigned to the ports

Common Ports -> Services

- 80 -
- 21 –
- 22 –
- 23 –
- 25 –
- 53 -
- 110 –
- 123 –
- 443 –
- 445 -
- 514 –
- 3389 –
- 5500 -

Common Ports -> Services

- 80 - HTTP
- 21 –
- 22 –
- 23 –
- 25 –
- 53 -
- 110 –
- 123 –
- 443 –
- 445 -
- 514 –
- 3389 –
- 5500 -

Common Ports -> Services

- 80 - HTTP
- 21 – FTP
- 22 –
- 23 –
- 25 –
- 53 -
- 110 –
- 123 –
- 443 –
- 445 -
- 514 –
- 3389 –
- 5500 -

Common Ports -> Services

- 80 - HTTP
- 21 – FTP
- 22 – SSH
- 23 –
- 25 –
- 53 -
- 110 –
- 123 –
- 443 –
- 445 -
- 514 –
- 3389 –
- 5500 -

Common Ports -> Services

- 80 - HTTP
- 21 – FTP
- 22 – SSH
- 23 – Telnet
- 25 –
- 53 -
- 110 –
- 123 –
- 443 –
- 445 -
- 514 –
- 3389 –
- 5500 -

Common Ports -> Services

- 80 - HTTP
- 21 – FTP
- 22 – SSH
- 23 – Telnet
- 25 – SMTP
- 53 -
- 110 –
- 123 –
- 443 –
- 445 -
- 514 –
- 3389 –
- 5500 -

Common Ports -> Services

- 80 - HTTP
- 21 – FTP
- 22 – SSH
- 23 – Telnet
- 25 – SMTP
- 53 - DNS
- 110 –
- 123 –
- 443 –
- 445 -
- 514 –
- 3389 –
- 5500 -

Common Ports -> Services

- 80 - HTTP
- 21 – FTP
- 22 – SSH
- 23 – Telnet
- 25 – SMTP
- 53 - DNS
- 110 – POP3
- 123 –
- 443 –
- 445 -
- 514 –
- 3389 –
- 5500 -

Common Ports -> Services

- 80 - HTTP
- 21 – FTP
- 22 – SSH
- 23 – Telnet
- 25 – SMTP
- 53 - DNS
- 110 – POP3
- 123 – NTP
- 443 –
- 445 -
- 514 –
- 3389 –
- 5500 -

Common Ports -> Services

- 80 - HTTP
- 21 – FTP
- 22 – SSH
- 23 – Telnet
- 25 – SMTP
- 53 - DNS
- 110 – POP3
- 123 – NTP
- 443 – HTTP over TLS/SSL (HTTPS)
- 445 -
- 514 –
- 3389 –
- 5500 -

Common Ports -> Services

- 80 - HTTP
- 21 – FTP
- 22 – SSH
- 23 – Telnet
- 25 – SMTP
- 53 - DNS
- 110 – POP3
- 123 – NTP
- 443 – HTTP over TLS/SSL (HTTPS)
- 445 - SMB
- 514 –
- 3389 –
- 5500 -

Common Ports -> Services

- 80 - HTTP
- 21 – FTP
- 22 – SSH
- 23 – Telnet
- 25 – SMTP
- 53 - DNS
- 110 – POP3
- 123 – NTP
- 443 – HTTP over TLS/SSL (HTTPS)
- 445 - SMB
- 514 – Syslog
- 3389 –
- 5500 -

Common Ports -> Services

- 80 - HTTP
- 21 – FTP
- 22 – SSH
- 23 – Telnet
- 25 – SMTP
- 53 - DNS
- 110 – POP3
- 123 – NTP
- 443 – HTTP over TLS/SSL (HTTPS)
- 445 - SMB
- 514 – Syslog
- 3389 – RDP (Microsoft Terminal Server)
- 5500 -

Common Ports -> Services

- 80 - HTTP
- 21 – FTP
- 22 – SSH
- 23 – Telnet
- 25 – SMTP
- 53 - DNS
- 110 – POP3
- 123 – NTP
- 443 – HTTP over TLS/SSL (HTTPS)
- 445 - SMB
- 514 – Syslog
- 3389 – RDP (Microsoft Terminal Server)
- 5500 - VNC

Could I…

- …run a Web Server on port 53?
- …run a DNS server on port 80?
- …connect to a computer over SSH on port 345?

So Many Ports

- Should I scan the top 1024?
  - What about 3389?
  - What about 5500?
  - What about 48293?

Why Are Ports Im***port***ant?

Heh.

- Find what services are offered on the host
- Might help us identify the OS
  - Port 554 anyone?
- Identify Vulnerabilities
- Doorway into the system
  - Launch an exploit

How Is This Useful to Defenders?

- We're looking for holes, doors through which we can exploit, as attackers.
- Defenders should be scanning, too!
  - What's new on the network?
    - New Computers?
    - New Services?
  - Are new things authorized?
    - Rogue devices/services

Angry IP Scanner

- Somewhat automated scanner with a fancy interface.
- Angryip.org
  - 10.10.0.5
- `unzip ipscan_3.5.1_amd64.zip`
- `dpkg -i ipscan_3.5.1_amd64.deb`
- `ipscan`

Pinging Method

- ICMP echo – standard ping method, but may be blocked by firewalls.
- ICMP echo alternative – Windows-specific implementation, after removal of raw socket support
- UDP – sends packets to a port that is likely to be closed. A negative * ICMP response tells us the computer is actually alive and responding
- TCP – Makes a connection attempt to port 80 on the host. Both positive and negative responses mean it's alive.

ARP

Source	Destination	Protocol	Length	Info
Vmware_05:2e:b3	Vmware_05:2e:77	ARP	42	Who has 10.10.10.1? Tell 10.10.10.4
Vmware_05:2e:77	Vmware_05:2e:b3	ARP	60	10.10.10.1 is at 00:50:56:05:2e:77

- Address Resolution Protocol
- Used to map IP addresses to hardware (MAC) addresses

arp-scan

- Scan the local network using arp.
- arp-scan --interface=etho --localnet