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

Scanning with Nmap

Basic Scanning vs. Port Scanning

- Scanning
  - Mapping the network
  - Finding live systems
- Port Scanning
  - Helps figure out the purpose of a system
    - Services
  - Entry points

Ping Sweeps

- Build a list of targets we know are turned on
  - If we get a reply, it's turned on
  - If not, maybe…
- ICMP
  - What if it's blocked?
    - TCP
    - UDP

Perimeter Scanning

- The way in from the outside.
- Typically IPs found during OSINT recon phases will be perimeter IPs…they better be.
- What services do they host?
- Break through, gain access to the internal network.
- Stepping stones

How To Defend Against Scanning?

- Properly configured firewall rules
- Packet filtering
- Block ICMP at the gateway
  - Does the world really need to ping you?
  - Your webserver?
  - Internal hosts?

Nmap

- “Network Mapper”
- THE port scanner
- It’s free! https://nmap.org
- Widely used
  - Multi-platform
- CLI or GUI
  - CLI - you need to know this
  - GUI – fine place to start, but don’t’ get used to it.

Be Careful…

- This is active, get permission.
- You could crash things
  - Some systems may become flooded or crash under the additional load/traffic
    - Printers, VoIP phones, embedded things, depending on load even some servers.

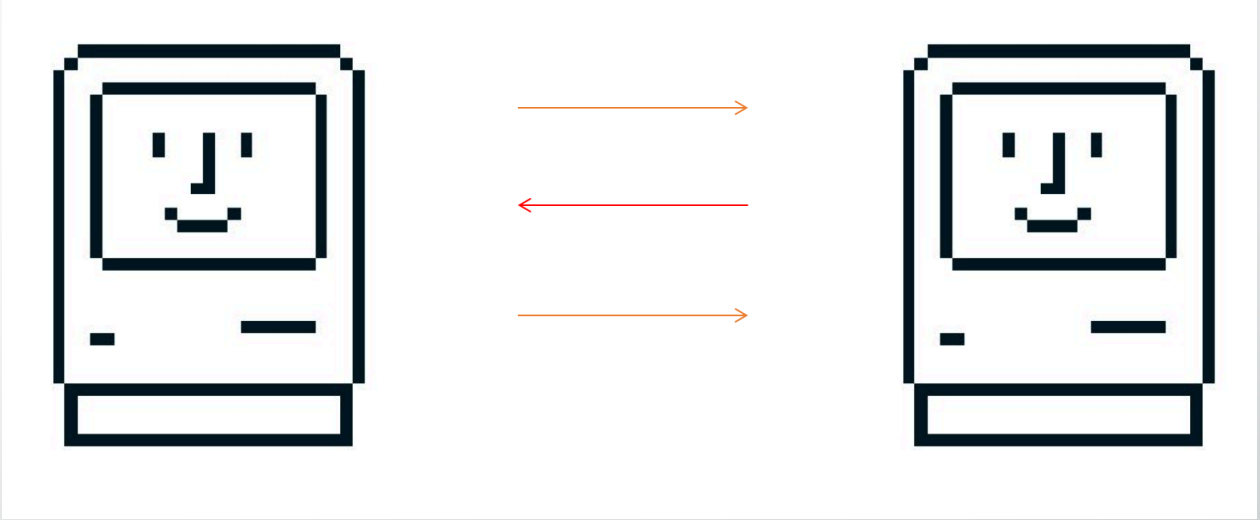
Ping Scan/Host Discovery

- nmap –sP <target>

- Essentially will do the same for us as fping
- ICMP echo request
- TCP Syn to 443
- TCP ACK to 80
- ICMP timestamp request

Three Way Handshake

- Think of a phone call…
- SYN (A -> B)
- SYN-ACK (B->A)
- ACK (A->B)
- Ready for comms!



TCP Connect Scan

- The “polite” scan
- Attempts to complete a 3-way handshake with each port on a target
  - Ends with FIN packet
- Positive
  - Little chance of DoS / network flood / victim crash
  - Normal
- Negative
  - Noisy!
  - Established connection, probably logged!

TCP Connect Scan

- Possible Responses…
  - Host is Down
    - No response
    - Turned off, or firewalled well
  - Port is closed
    - No SYN-ACK
    - RESET, ICMP Port Unreachable, Nothing
  - Port is Up
    - SYN-ACK Response

TCP Connect Scan

- nmap -sT <target>

- What are the results?
- What was the downside to using a connect scan?

Before Nmap Scans Ports…

- It performs a host discovery to find active machines before heavy probing
  - Port scans, version detection, OS detection
- You can turn this off, so Nmap performs the scan you would like, without first checking if the host is up.
  - Treats all hosts as alive
  - **-Pn** switch

More Ports

- If you have time, you should scan all 65,535 ports, not just the top 1000
- **-p-** switch scans all the things
- **-p** switch
  - Specify ports
  - **Nmap –sT –p 22,80**

Host List

- **-iL** input list
  - Could supply a list from fping
    - Fping –a –g > fping.txt
  - Most tools allow a text file as input
  - Better chance you won't fat-finger an IP… Don't scan something you don't have permission to!

TCP SYN Scan

- Slightly stealthier
- Completes 2/3 of the 3 way handshake
  - SYN -> SYN/ACK -> RESET
  - Shutting down the connection before it's completed/started

TCP SYN Scan

- Positive
  - Basic stealth, most end systems only record completed connections
    - Firewalls/IDS/Packet Sniffers may log SYN packets!
  - Speed
- Negative
  - Target system could become flooded with outstanding SYNs
    - Nmap sends RESET to close the connection

TCP SYN Scan

- **nmap –sS <target>**

UDP Scans

- Don’t overlook UDP
- UDP is connectionless, and therefore unreliable
- Used for DHCP, DNS, SNMP, TFTP, etc.
- **nmap –sU <target>**

UDP Scans

- What's the output? What's different about the reporting on ports?
- UDP… Doesn't need to send back a reply, right?
  - How do I know if the port is open or closed?
- Add in **–sV** for a bit more accuracy
- nmap –sUV <target>

Version Scan

- With the scans we've run to this point, we may get a report on the service that's running.
  - But we don't know what version
- **-sV**
- **nmap –sV <target>**

TCP FIN

- FIN scans break the specification by sending unexpected packets
- FIN packets instruct the target that the connection should be torn down
  - …but no connection has been set up!
- Target will still play by the rules
  - If port is closed, it will respond with RESET
  - If it’s open or actively blocked, it won’t respond.

TCP FIN

- **-sF**
- **nmap –sF <target>**
- Can be stealthy, but also lead to false positives.

Xmas Tree Scan

- Sends a packet to the target port with all flags/control bits set:
  - URG, ACK, PSH, RST, SYN, FIN
- Benefit
  - RFC says a packet without SYN/ACK/RST and it's closed, should respond with a RST packet. If open, ignore.
  - Some older IDS's will ignore
- Result
  - If a port is closed, target responds with RESET
  - If it's open or blocked, target responds with nothing.

Xmas Tree Scan

- **-sX**
- **nmap –sX <target>**

TCP Null Scan

- Sends TCP packets with no control bits set
- Positive
  - Very stealthy
  - Among the very minimalist port scans nmap can do
- Results
  - If port is closed, target responds with RESET
  - If port is open (or blocked) target will respond with nothing.

TCP Null Scan

- **-sN**
- **nmap –sN <target>**