
PLEXKITS
30 Minute Lo-Fi Hiphop Beats Study Timer
Copy link
<we will start in>
30:00
Watch on YouTube

CAN YOU HEAR ME NOW?

NETWORK SNIFFING & RECONNAISSANCE

Presented By:
Adrian Cisneros

Date
7/16/2025

VICEROY CTF Prep Series

WHY ARE WE HERE?

Build hands-on cybersecurity skills

Learn core networking and recon concepts

Practice tools used by real professionals

Get ready for CTF challenges & certifications

Learn + Watch + Try

🎯 Network Sniffing & Reconnaissance

WHAT YOU'LL LEARN THIS WEEK:

TCP/IP VS OSI — WHAT'S THE DIFFERENCE?

🌐 What Is the OSI Model?

- OSI = Open Systems Interconnection Model
- It's a conceptual framework that breaks down how data travels over a network — like the layers of a cake.

🌍 What Is the TCP/IP Model?

- TCP/IP = Transmission Control Protocol / Internet Protocol
- It's the real-world model used by the internet. It's simpler and practical, based on protocols in action.

7 Layers of the OSI Model

Layer Number	Layer Name	Description	Example
7	**Application**	Interfaces and protocols used by applications to communicate over a network.	Web browser, email, FTP client
6	**Presentation**	Translates data between the application layer and the network format; handles encryption and compression.	SSL/TLS encryption, JPEG
5	**Session**	Manages sessions and controls dialogues between computers.	Remote login, API sessions
4	**Transport**	Provides reliable data transfer services to the upper layers.	TCP/UDP
3	**Network**	Determines how data is transferred between network devices; handles packet routing.	IP, Routers
2	**Data Link**	Provides node-to-node data transfer and handles error correction from the physical layer.	Ethernet, Switches
1	**Physical**	Transmits raw bit streams over a physical medium.	Ethernet cables, Wi-Fi

Layers 5–7 are user-facing functions

Adrian Cisneros

Layers 1–4 are the delivery system

Adrian Cisneros

4 Layers of TCP/IP

Layer Number	Layer	Maps to OSI Layers	What It Handles	Real-World Examples
4	**Application**	OSI 5–7	Network services & user apps	**Web browsing (HTTP/HTTPS), Email (SMTP), DNS**
3	**Transport**	OSI 4	End-to-end connections, reliability	**TCP** (file downloads, web pages), **UDP** (video calls, gaming)
2	**Internet**	OSI 3	Routing, addressing	**IP Addresses, Routers, Ping, Traceroute**
1	**Network Access**	OSI 1–2	Hardware & local data transfer	**Ethernet cables, Wi-Fi, MAC addresses, Switches**

Key Differences

OSI Model	TCP/IP Model
Conceptual, not implemented directly	Practical, used in real systems
7 layers	4 layers
More academic	More practical

VICEROY

If you're using Wireshark, you'll often see Application-layer protocols like HTTP and DNS.

Adrian Cisneros

Tools like Nmap help probe Transport and Internet layers (TCP/UDP ports, IP addresses).

Adrian Cisneros

Most network attacks target layers 3–7 (like IP spoofing, TCP SYN floods, DNS poisoning, etc.)

Adrian Cisneros

OSI Model is like a detailed textbook:

It breaks down every system (engine, wiring, brakes, etc.) into specific layers so you can study and understand how each part works in isolation.

TCP/IP Model is like the actual car you drive:

It doesn't split everything perfectly, but it works, and it's what manufacturers (network engineers) actually use to build and run systems.

In CTFs and cybersecurity, TCP/IP matters more in practice — but knowing OSI helps you explain or understand where something went wrong.

Why Does This Matter in Cybersecurity?

- You'll encounter network attacks on different OSI layers (e.g., DDoS at Layer 3, MITM at Layer 7)
- Knowing the model helps you analyze packets, design secure systems, and understand tools like Wireshark, Nmap, firewalls, etc.

UNDERSTANDING THE DIGITAL ENTRYWAYS

🏠 What is a Port?

- A port is a numerical identifier for a specific communication process on a computer.
- Think of your device like an apartment building:
- The IP address is the building's street address
- A port is the apartment number
- Ports allow multiple services (web, email, file transfer) to run on the same device without conflict.

💬 What is a Protocol?

- A protocol is a set of rules for formatting and handling data.
- Each protocol is tied to a port, telling computers how to interpret and respond to data coming in or going out.

Quick Port Cheat Sheet

Port	Protocol	Use
80	HTTP	Unencrypted websites
443	HTTPS	Secure websites (SSL/TLS)
22	SSH	Secure shell (remote login)
21	FTP	File transfer
53	DNS	Translates URLs to IPs
25	SMTP	Sending email
110	POP3	Receiving email
3389	RDP	Remote Desktop
23	Telnet	Legacy remote access (insecure)

nmap – Network Mapper

Command	Description
nmap scanme.nmap.org	Basic scan of a target (host discovery + open ports)
nmap -p 80 scanme.nmap.org	Scan only port 80
nmap -p 1-1000 scanme.nmap.org	Scan ports 1 to 1000
nmap -sV scanme.nmap.org	Scan with service/version detection
nmap -O scanme.nmap.org	Attempt to detect the OS
nmap -Pn scanme.nmap.org	Skip host discovery (useful if ping is blocked)
nmap -A scanme.nmap.org	Aggressive scan: OS, version, scripts, traceroute

Try nmap localhost to test on your own machine!

Adrian Cisneros

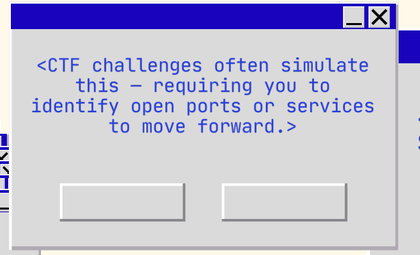
Use Ctrl + F to search for port numbers in the output.

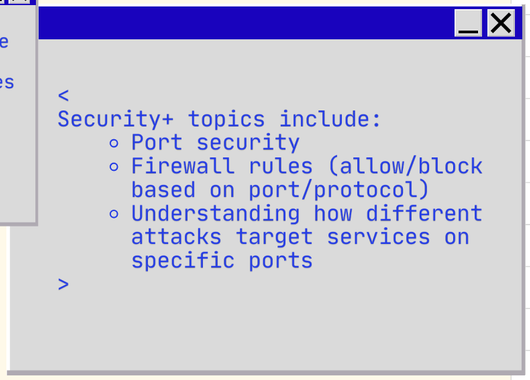
Adrian Cisneros

netstat – Network Statistics

Command	Description
netstat -an	List all connections and listening ports
netstat -aon	Like above, plus process IDs (Windows only)
netstat -tulpn	Linux: Show TCP/UDP ports + program names
netstat -r	Displays routing table
netstat -s	Show network statistics by protocol

TEXAS A&M UNIVERSITY-SAN ANTONIO





⚔️ Practice Tip:

Use Nmap to scan a host for open ports:

nmap -sV [IP address]
Then research what those ports reveal about the system.

Try this on a CTFlearn challenge or local VM!

Adrian Cisneros

PASSIVE VS. ACTIVE RECON

No Direct Interaction with the Target

Passive recon gathers information without touching the target system directly. It's like watching someone through binoculars — quiet and unnoticed. This method avoids detection by firewalls or intrusion detection systems.

Relies on Public or External Sources

You use tools and resources like WHOIS lookups, DNS records, job postings, social media, and Wireshark (if on the same network) to gather intel. It's about connecting dots from freely available data.

Low Risk, Low Noise, but Limited Depth

Since there's no network traffic generated to the target, it's nearly impossible to detect. However, you usually only get surface-level information — not enough for detailed planning.

Direct Communication with the Target

Active recon involves sending packets or signals to the target to gather real-time data. It's like knocking on doors to see who answers. This method gives you deeper insights but can be noisy.

Uses Probing Tools Like Nmap and Netcat

Tools like Nmap, Netcat, and Traceroute are commonly used to find open ports, discover operating systems, and identify running services. These tools build a clear technical map of the target.

High Detail but Detectable

While it provides much richer and more actionable data, active recon may trigger alerts and logs. It's best used when authorized or when stealth isn't the priority.

🛠️ Common Passive Tools:

Tool	Description
Wireshark	Captures packets on your network
whois	Looks up domain registration info
nslookup / dig	Reveals DNS records for a domain
Shodan	Search engine for internet-connected devices
Google	“Google Dorking” for exposed info via search
Social Media	Target research (company, employees, policies)

🛠️ Common Active Tools:

Tool	Description
nmap	Scans ports, detects services and OS
hping3	Custom packet crafting for testing/firewall evasion
traceroute	Maps network hops to the destination
netcat	Manually probe services on specific ports
dirb / gobuster	Brute-force web directories

WIRESHARK

🔍 What is Wireshark?

- Wireshark is a packet sniffer, it captures and displays raw network traffic in real time.
- Used by cybersecurity professionals to analyze protocols, devices, and data flow.
- It helps you visualize what's happening on the wire, down to every single byte.

🎯 Key Uses

- Capture Live Traffic: Monitor everything from web requests to DNS lookups.
- Analyze Packets: Inspect headers, payloads, and protocol details.
- Troubleshoot Issues: Detect abnormal patterns or malicious behavior.

🔍 Common Filters

Filter	What it Does
http	Shows only HTTP traffic
ip.addr == 8.8.8.8	Filters all packets to/from Google DNS
tcp.port == 80	Shows only TCP traffic on port 80 (HTTP)
dns	Filters only DNS queries/responses
ssl or tls	Filters encrypted traffic (HTTPS)

NMAP

🔍 What is Nmap?

- Nmap (Network Mapper) is a powerful open-source tool used to scan networks and discover devices, services, and open ports.
- It’s used by cybersecurity pros to actively probe targets to learn more about them.

🎯 Key Uses

- Actively scans targets to find open ports and services
- Maps networks by identifying live devices
- Reveals potential vulnerabilities
- Like knocking on apartment doors to see which ones open

🔍 Common Filters

Command	Description
nmap <target IP>	Scan a host or IP to find open ports
nmap -sV <target IP>	Identify service versions running on open ports
nmap -O <target IP>	Attempt to detect the operating system
nmap -p 1-1000 <target IP>	Scan a specific range of ports
nmap -A <target IP>	Aggressive scan: detects OS, services, scripts
nmap -Pn <target IP>	Skip host discovery (useful if ICMP is blocked)


DEMO
TIME
LOADING

🔵 1xx – Informational

Server is processing the request.

- **100 Continue: Client should keep sending the request.**

🟢 2xx – Success

The request worked!

- **200 OK: Everything went fine.**
- **201 Created: Something new was created (e.g., file upload).**

🟡 3xx – Redirection

You're being sent somewhere else.

- **301 Moved Permanently: The resource moved to a new URL.**
- **302 Found: Temporary redirect.**
- **304 Not Modified: Use cached version (no need to re-download).**

🔴 4xx – Client Error

You did something wrong.

- **400 Bad Request: Syntax error or malformed request.**
- **401 Unauthorized: You need to log in.**
- **403 Forbidden: You're not allowed, even if logged in.**
- **404 Not Found: The page or file doesn't exist.**
- **418 I'm a teapot: Joke/debug code (from an April Fools spec).**

⚫ 5xx – Server Error

The server messed up.

- **500 Internal Server Error: Generic failure.**
- **502 Bad Gateway: Server got a bad response from upstream.**
- **503 Service Unavailable: Server is overloaded or down for maintenance.**

Command	What it Does	Explanation for Session
nmap scanme.nmap.org	Basic scan to find open ports on the target.	"This scans the target to see which doors (ports) are open."
nmap -sS scanme.nmap.org	SYN (stealth) scan – common fast scan.	"Sends a SYN packet to check if a port responds without completing connection."
nmap -sV scanme.nmap.org	Detect service versions running on open ports.	"Finds what services and versions are behind each open door."
nmap -O scanme.nmap.org	Attempts to detect the operating system.	"Tries to guess what OS the target is running."
nmap -p 22,80,443 scanme.nmap.org	Scan only ports 22 (SSH), 80 (HTTP), and 443 (HTTPS).	"Focuses on specific important ports instead of scanning all."
nmap -A scanme.nmap.org	Aggressive scan: OS detection, service versions, script scan.	"Does all the detailed scanning at once — kind of a 'full inspection'."
nmap -v scanme.nmap.org	Verbose mode: gives more detailed output during scanning.	"Shows you more info as the scan is happening."
nmap -Pn scanme.nmap.org	Skip host discovery; treats host as online.	"Assumes the host is up without pinging first."
nmap -sU scanme.nmap.org	UDP scan to check UDP ports (harder to scan).	"Checks if UDP ports are open, which are often overlooked."
nmap 127.0.0.1	Scan your own computer (localhost).	"Shows which ports your own machine has open."
nmap -sT scanme.nmap.org	TCP connect scan – completes connection to check port.	"Makes full connection to see if port is accepting."
nmap --top-ports 20 scanme.nmap.org	Scan the top 20 most common ports.	"Quick check of the most popular ports."

TRY IT YOURSELF!

A CAPture of a Flag
Passive Recon

🧩 Difficulty: Medium

📌 Relevance:
Practice passive reconnaissanc, examining captured traffic with Wireshark without probing any targets.

🔗 **https://ctflearn.com/challenge/356**

Rock Paper Scissors
Intro to Nmap (Active Recon)

🧩 Difficulty: Medium

📌 Relevance:
Experience active reconnaissance by identifying which service is listening, directly probing a target as taught in Nmap sections.

🔗 **https://ctflearn.com/challenge/855**

Impossible Equation
What's My Port? (Active Recon)

🧩 Difficulty: Easy

📌 Relevance:
Demonstrates active reconnaissance skills, finding an open port and interacting with its service.

🔗 **https://ctflearn.com/challenge/1234**

THANK YOU

FOR YOUR ATTENTION AND PARTICIPATION

https://forms.office.com/r/pFG9GVKjN0

<Have fun Hacking> 😎

VICEROY

TEXAS A&M UNIVERSITY-SAN ANTONIO

1. Official Documentation & Websites

- **Wireshark** — https://www.wireshark.org/docs/
- **Nmap** — https://nmap.org/book/
- **OWASP (Open Web Application Security Project)** — https://owasp.org/
- **CTFlearn** — https://ctflearn.com/

2. Educational Platforms

- **Cybrary** — https://www.cybrary.it/ (free and paid cybersecurity courses)
- **TryHackMe** — https://tryhackme.com/ (interactive hacking labs)
- **Hack The Box** — https://www.hackthebox.eu/ (CTF style challenges)
- **Coursera / edX** (cybersecurity and networking courses)

3. Books & References

- *"The Web Application Hacker's Handbook"* by Dafydd Stuttard and Marcus Pinto
- *"Nmap Network Scanning"* by Gordon "Fyodor" Lyon (creator of Nmap)
- *"Practical Packet Analysis"* by Chris Sanders (Wireshark focus)

4. Trusted Cybersecurity Experts / Influencers

- **Troy Hunt** (creator of "Have I Been Pwned"): https://www.troyhunt.com/
- **Katie Moussouris** (vulnerability disclosure expert)
- **The CyberWire Podcast** — daily cybersecurity news & expert interviews

5. Forums & Communities

- **Stack Exchange Information Security** — https://security.stackexchange.com/
- **Reddit r/netsec** — https://www.reddit.com/r/netsec/