During a real-world investigation, I was tracking some suspicious logins on our network logs. There were multiple failed attempts from weird IPs that didn't match our usual users. That's when it hit me how crucial IP addresses are – without understanding them, you're basically blind. On Day 2 of our cybersecurity training, we dove deep into IPv4 and IPv6, private vs public IPs, domain names, DNS, ports, and protocols. This stuff isn't just theory; it directly helps trace attackers, spot what services are running on targets, and figure out how systems talk over the internet. Let me break it all down like I'm explaining it to a friend over coffee.

IPv4 vs IPv6: The Building Blocks of Addresses

First off, every device on the internet needs an IP address – think of it as a postal address for data packets. IPv4 is the old standard we've been using forever. It's like 192.168.1.10 – four numbers separated by dots, each from 0-255. Super common in logs, but we're running out because there are only about 4 billion possible combos. That's where IPv6 comes in: it's the upgrade with way more space, like 2001:0db8:85a3:0000:0000:8a2e:0370:7334. Hex numbers, colons, and enough addresses for every grain of

sand on Earth.

In investigations, spotting IPv4 vs IPv6 tells you a lot. Old systems or attackers sticking to IPv4 might use tunnels to hide in IPv6 traffic. IPv6 also has built-in security features like IPsec, but misconfigs make it a headache. I sketch this in my notes with two columns: IPv4 (shortage, NAT-heavy) vs IPv6 (future-proof, direct addressing).

Private vs Public IPs: Inside vs Outside the House

Public IPs are what your ISP gives you – visible to the whole internet, like your home's street address. Private IPs are for local networks only, like room numbers in your house. Common private ranges: 192.168.x.x, 10.x.x.x, and 172.16-31.x.x. Your router uses NAT (Network Address Translation) to let tons of private devices share one public IP. Without NAT, hackers could directly ping your fridge or printer.

In that login investigation, the suspicious traffic hit our public IP first, then NAT hid the internal private IPs. Attackers love exposing privates for lateral movement inside networks. Proxies/VPNs let them mask their public

IP. Draw a diagram: Internet cloud → Public IP (router) → Private IPs (devices). Boom, it clicks.

Domain Names: Making IPs Human-Friendly
Nobody memorizes 142.250.190.46 for Google. Domains like blog.google.com fix that. Structure reads right-to-left: .com (TLD – top-level domain, like .com/.org/.in), google (main domain), blog (subdomain). Subdomains are sneaky – attackers hunt forgotten ones like dev.company.com for weak spots.

In probes, DNS logs show domains queried. Suspicious? Like malware phoning home to evil-domain.ru. Table in notes:

Part	Example	What it means
TLD	.com	Commercial site
Domain	google	Main brand
Subdomain	blog	Specific section

DNS: The Internet's Phonebook
DNS translates domains to IPs. Type youtube.com? Your PC asks a DNS resolver (like 8.8.8.8), which checks

caches or root servers, then shoots back the IP. No DNS, internet breaks – you'd memorize IPs for everything.

Risky part: Cache poisoning. Hacker poisons the "phonebook," so bank.com goes to fake site. In investigations, DNS logs are gold: C2 domains, exfil paths. Flowchart: Browser → Resolver → Authoritative DNS → IP back.

Ports & Protocols: Doors and Handshakes
IP gets you to the building; ports are the doors (65,535 total). Services live on specific ones:

- 80/HTTP: Web (unsecure)
- 443/HTTPS: Secure web
- 21/FTP: Files
- 22/SSH: Remote access
- 53/DNS: Queries

Protocols are the rules: TCP (reliable, handshakes like TCP), UDP (fast, fire-and-forget). Connection example: Your browser hits server IP:443 for HTTPS.

Attackers port-scan (Nmap) for open doors. Defenders do too, to close risks. Table:

Port	Service	Protocol
80	HTTP	TCP
443	HTTPS	TCP
22	SSH	TCP

How This Powers Investigations
Tracing Attackers: Correlate logs – IP geolocation, WHOIS for domains, DNS history. VPN? Look for known exit nodes. Chained with ports, you map attack paths.

Identifying Services: Open port 3389? RDP vuln maybe. Nmap banners spill versions/OS. Prioritize exploits.

System Behavior: Normal traffic: Port 443 bursts. Weird? Port 4444 C2 beacon. Protocols show if it's chatty UDP scans or sneaky TCP exfil.

This Day 2 knowledge turned my login hunt from guesswork to systematic. Networking is cybersecurity's

foundation – master comms, master attacks/defense. Built base for Day 3's hacking tools. (4 pages if handwritten with sketches/tables!)