"Day 2 Practitioner Observation Report."

Observation Report: Day 2 – Networking Foundations in Practice

Author: Madire Raju

Date: 29 Dec 2035

Focus: Bridging the gap between network architecture and forensic investigation.

---

1. Executive Summary: The "Why" Behind the Wire

During today's practical sessions, I transitioned from viewing networking as a collection of settings to seeing it as the **digital footprint** of an adversary. In a real-world breach, an IP address is rarely just a number; it is the starting point of a "digital manhunt." My observations today focused on how to decode these signals to map attacker paths and identify compromised assets.

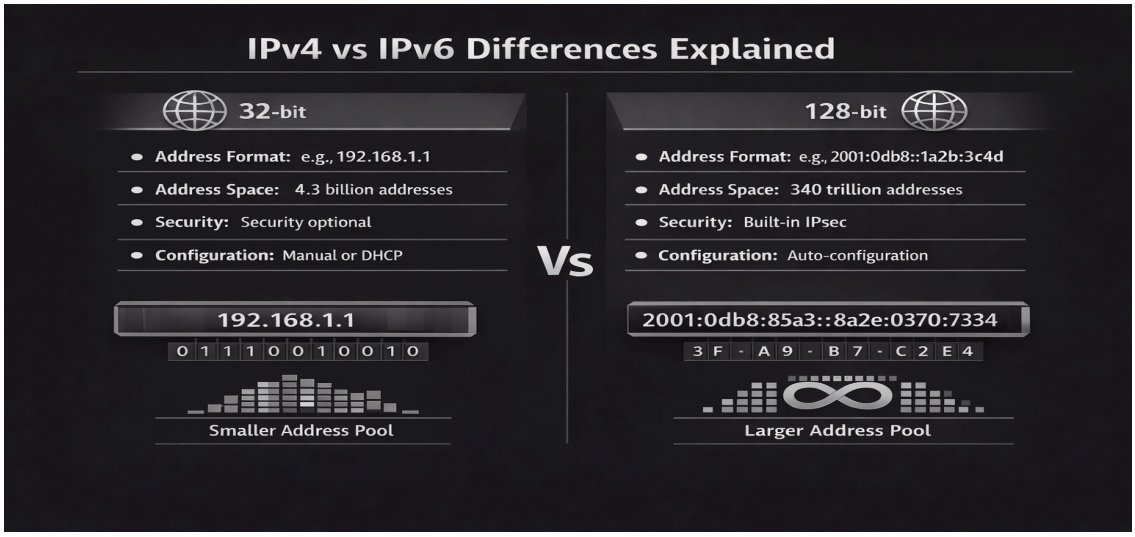
---

2. IP Addressing: Identification and Attribution

IPv4 vs. IPv6 Operational Nuances

I observed that while IPv4 remains the primary language of current logs, IPv6 is no longer "the future"—it is the present.

- **Practical Insight:** Attackers often exploit the fact that many legacy security tools are not configured to monitor IPv6 traffic.
- **Actionable Skill:** I learned to recognize both formats to ensure I am querying threat intelligence databases (like VirusTotal or AlienVault) for the full scope of an attacker’s infrastructure.

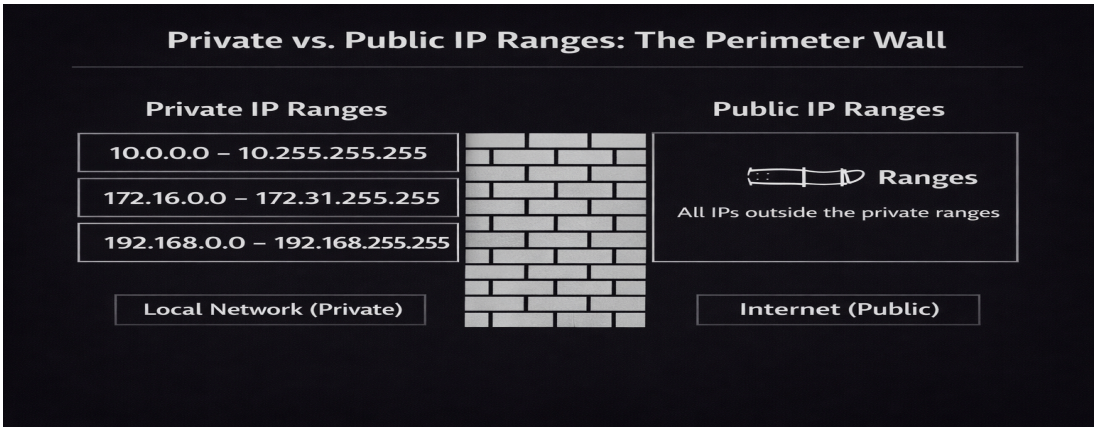


---

3. The Perimeter Wall: Public vs. Private Ranges

Distinguishing between internal and external traffic is the first step in scoping an incident.

- **The Internal Threat:** Seeing a source IP like `192.168.1.15` or `10.0.5.2` in an alert immediately shifts my focus. It suggests **Lateral Movement**—where an attacker has already bypassed the firewall and is moving between internal workstations.
- **The External Threat:** Public IPs (like `8.8.8.8` or a random VPS address) represent the entry point. I practiced using `whois` lookups to determine the owner of a public IP, which helps in identifying if a login is coming from a known "clean" service (like Microsoft) or a suspicious hosting provider used for malicious activity.

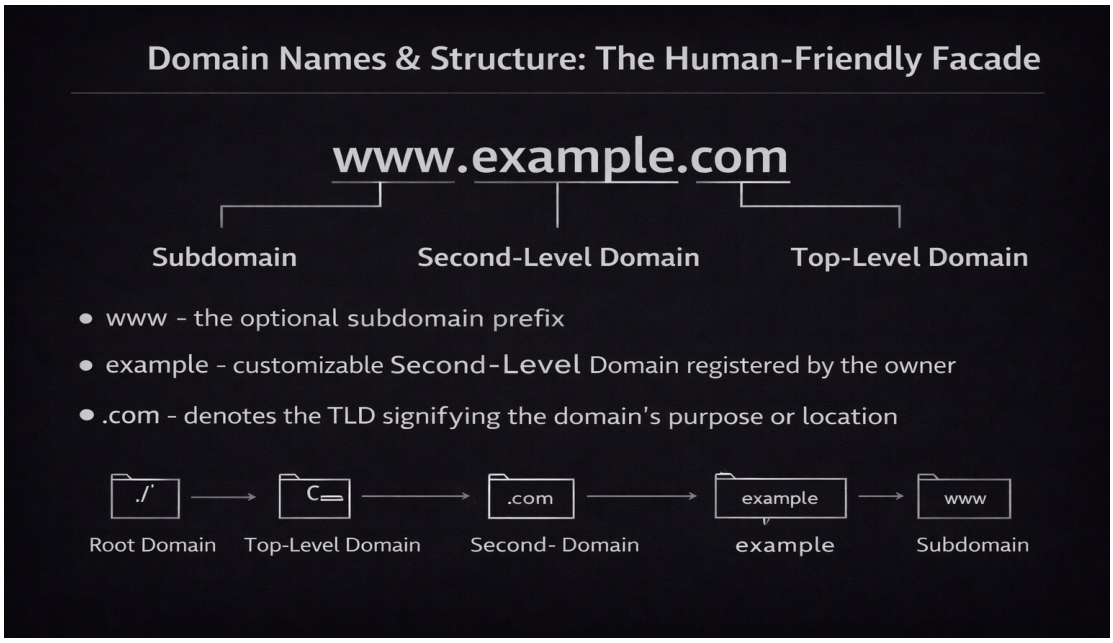


---

4. Domain Analysis: Beyond the Human-Friendly Alias

I analyzed the structure of URLs to detect phishing and "typosquatting."

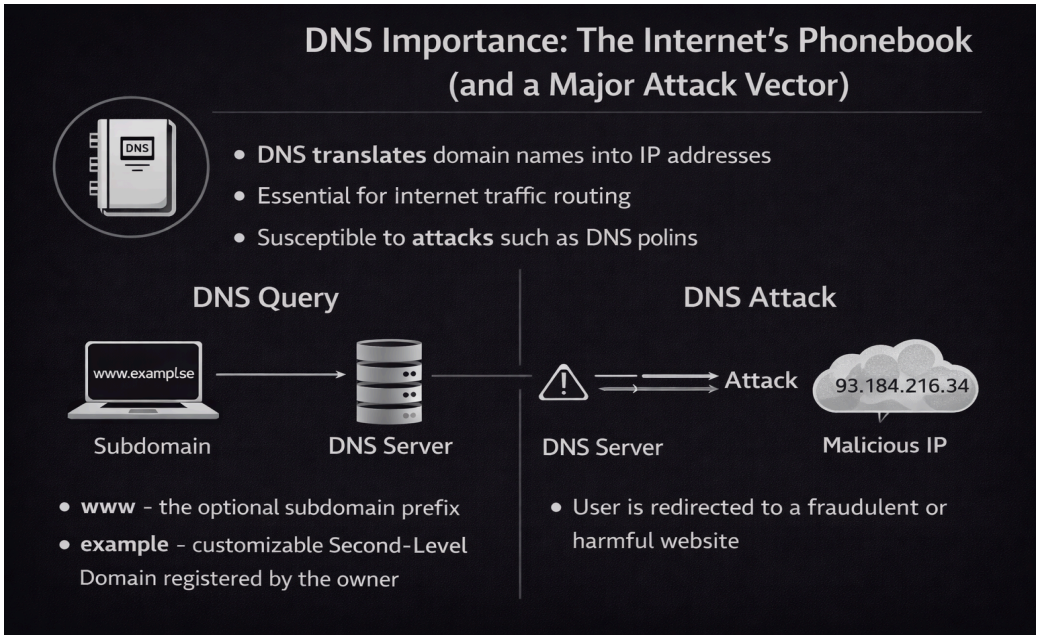
- **The Facade:** An address like `secure-login.raju.com.scam-site.ru` is designed to trick the eye.
- **Observation:** By breaking down the **TLD** (Top-Level Domain) and **SLD** (Second-Level Domain), I can identify that the actual owner of this domain is not "raju.com" but a registrar in a foreign jurisdiction (indicated by `.ru`). This is a critical skill for identifying malicious Command & Control (C2) servers.



5. DNS: Monitoring the Internet's Phonebook

DNS is more than a translation service; it is a major attack vector.

- **DNS Tunneling:** I explored how attackers hide stolen data inside tiny DNS queries to bypass firewalls that otherwise block large file transfers.
- **DGA (Domain Generation Algorithms):** I observed how malware generates random domains (e.g., `x1jf39sdf8.net`) to communicate. Detecting these "nonsense" domain queries in logs is a high-fidelity indicator of a compromised host.

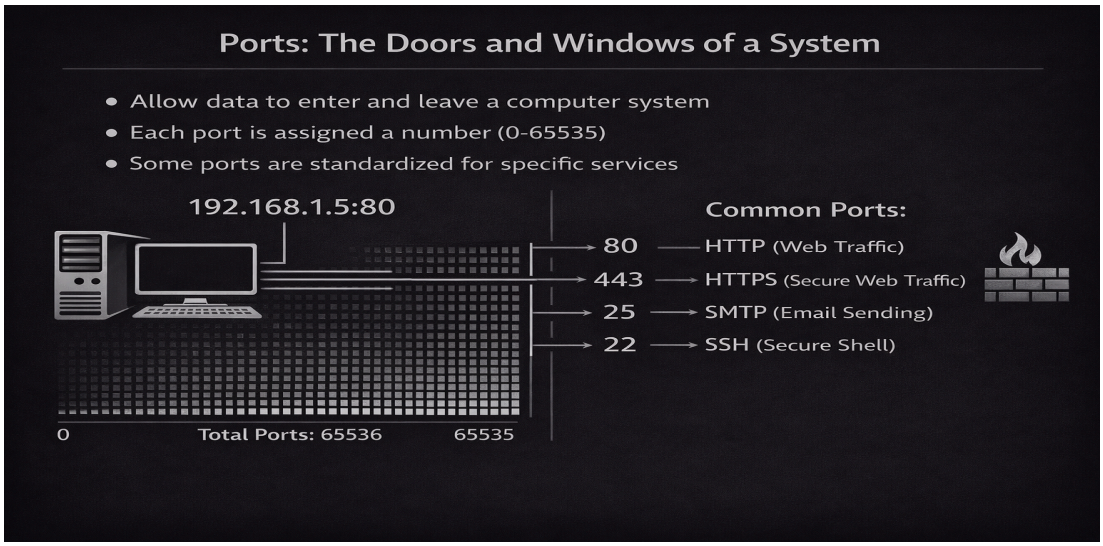


---

6. Ports and Protocols: The Doors and the Language

If the IP is the address, the Port is the door.

- **Port Analysis:** Finding **Port 22 (SSH)** or **Port 3389 (RDP)** open to the public internet is like leaving the front door of a bank unlocked. During a scan, seeing **Port 4444** open immediately flagged a "Payload Handler" (Metasploit), signaling an active compromise.
- **Protocol Analysis:** I used packet captures (PCAPs) to differentiate between **TCP** (reliable, used for data theft) and **UDP** (fast, often used for DoS attacks). Understanding **HTTP vs. HTTPS** allowed me to see where an attacker might have intercepted plaintext credentials.



7. Integrated Case Study: The "raju.com" Investigation

To test these concepts, I walked through a simulated investigation involving the website **raju.com** and a user named **Raju**.

1. **Detection:** Unauthorized funds were moved. Logs showed a successful login from IP `198.51.100.20` via **Port 22 (SSH)**.
2. **Attribution:** A reverse DNS lookup linked that IP to `vps-attackersupply.biz`.
3. **Discovery:** Internal traffic showed the server querying `download.malware-update.cc`.
4. **Conclusion:** By correlating the **Public IP**, the **Malicious Domain**, and the **Port 22 breach**, I was able to recommend a full server reimage and a firewall rule to block all traffic from the identified attacker's TLD.

8. Final Reflection

Day 2 my understanding that networking is the language of security. You cannot defend what you cannot see, and you cannot see what you do not understand. My next step is to apply these "low-level" observations to "high-level" threat-hunting scenarios.