**Using NMAP by Lana Bracken**

**1. What Did You Do?**

To analyze my home network, I downloaded Zenmap, the graphical user interface for the Nmap network scanner. My process involved a structured approach, beginning with initial exploration and progressing to a comprehensive analysis.

First, I downloaded and installed Zenmap from the official Nmap website to ensure I had the most up-to-date version. To gain a foundational understanding, I consulted online resources and the official Nmap documentation to familiarize myself with its core functionalities and the underlying principles of network scanning as I have never performed a network scan before. I then launched the application and began exploring the user interface. I paid close attention to the profile selection dropdown, the target input field, the output tabs (Nmap Output, Hosts, Services, Topology), and the various settings and options available. This exploration allowed me to learn the layout and the different ways I could interact with the tool and provided insight into the tool’s flexibility and power.

Next, I determined the appropriate target IP address range for my home network. To do this, I opened a command prompt in Windows and executed the ipconfig command to identify my local IPv4 Address, Subnet Mask, and Default Gateway (Figure 1). This confirmed my network range as 192.168.1.0/24, covering IPs from 192.168.1.1 to 192.168.1.254.A computer screen with white text

AI-generated content may be incorrect.

Figure 1: ipconfig results

Following this, I planned my scanning strategy by selecting appropriate scan types for different stages of the analysis. I referred to the Nmap documentation to understand the nuances of each scan type and its relevance to my objectives. I decided to perform three distinct scans, each designed to provide a progressively deeper level of network insight:

* **Initial Host Discovery (Ping Scan):** Using nmap -sn 192.168.1.0/24, I performed a ping scan to identify live hosts. The -sn flag skipped port scanning and instead sent ICMP echo and ARP requests. This provided a fast overview of active devices.
* **Detailed Host and Service Enumeration (Intense Scan):** To gather more comprehensive information about each identified host, I executed an "Intense scan." This corresponds to the Nmap command nmap -T4 -A -v 192.168.1.0/24. I carefully selected the -T4 timing template for a balance between speed and accuracy, understanding that it assumes a reasonably reliable network. The -A flag was crucial as it enabled OS detection (-O), version detection (-sV), and script scanning (-sC), providing insights into the operating systems, services, and potential vulnerabilities of the hosts. The -v flag was used to increase verbosity, ensuring detailed output for my analysis. I analyzed the output, paying close attention to open ports, identified services and their versions, OS guesses, and basic vulnerabilities reported by the Nmap scripts.
* **In-Depth Protocol and Vulnerability Analysis (Slow Comprehensive Scan):** For the most detailed analysis, I conducted a slow, detailed scan with nmap -sS -sU -T4 -A -v -PE -PP -PS80,443 -PA3389 -PU40125 -PY -g 53 --script "default or (discovery and safe) or vuln" 192.168.1.0/24. Combining TCP SYN (-sS) and UDP (-sU) scans, this explored both protocol types. Various ping options increased host detection reliability. Spoofing the source port to 53 (-g 53) potentially bypassed some firewalls. The Nmap Scripting Engine (NSE) scripts provided vulnerability assessments. I carefully analyzed output differences, newly discovered services, vulnerabilities, and MAC address details.

Throughout the analysis, I carefully tracked how different Nmap command options influenced the results, helping me grasp both network behavior and possible vulnerabilities. When the output became overwhelming, I used AI tools to help me sort through the data and ensure I didn’t miss any important details.

**2. What are the results?**

The three Nmap scans provided a layered understanding of my home network’s components, protocols, and attack surface. Each scan progressively uncovered more detailed exposures, from basic device presence to deep protocol-level vulnerabilities. This section presents the most significant findings, highlighting how each scan expanded on the previous one and identifying key risks.

**(a) Initial Host Inventory (Ping Scan):** The initial ping scan (nmap -sn 192.168.1.0/24) provided a rapid inventory of active network components. This scan, which completed in 2.61 seconds and scanned 256 IP addresses, identified 12 active devices across the network. These included the Docsis-Gateway (router), multiple IoT devices (Google Home Mini, smart thermostats, iRobot), a Roku streaming stick, a Vizio smart TV, Apple TVs, an HP printer, an iPhone (mobile), and a Windows laptop as detailed in the table below.

Table 1: Devices Identified via Ping Scan

|  |  |  |
| --- | --- | --- |
| IP Address | Device Name | MAC Address / Vendor |
| 192.168.1.1 | Docsis-Gateway | A4:CF:D2:4E:2B:BF (Ubee Interactive) |
| 192.168.1.16 | Google-Home-Mini | 7C:2E:BD:65:4E:79 (Google) |
| 192.168.1.35 | Tstat-73C72C | B8:2C:A0:73:C7:2C (Resideo) |
| 192.168.1.49 | iRobot | 50:14:79:55:D6:3B (iRobot) |
| 192.168.1.61 | RokuStick-663 | B0:EE:7B:C3:94:5B (Roku) |
| 192.168.1.115 | Smart TV | 2C:64:1F:73:75:C8 (Vizio) |
| 192.168.1.121 | Entertanment Room | C0:95:6D:98:A1:FE (Apple) |
| 192.168.1.133 | Apple TV | B8:78:2E:32:0A:4B (Apple) |
| 192.168.1.151 | HP Printer | 3C:52:82:1C:95:C1 (HP) |
| 192.168.1.185 | Tstat-746A10 | B8:2C:A0:74:6A:10 (Resideo) |
| 192.168.1.248 | iPhone | 32:02:7A:CE:E3:67 (Unknown) |
| 192.168.1.46 | LanaB-LP | — |

This foundational scan confirmed the presence of most expected devices. However, two notable anomalies emerged:

* **Missing Device:** The Wi-Fi extender was not detected, which could be due to ICMP blocking, passive bridging mode, or network segmentation isolating it from direct discovery.
* **Google Home Mini Anomaly:** One Google Home Mini was absent from this initial scan but identified in later scans, possibly due to MAC address randomization or temporary disconnection.

This inventory established a baseline for the network's scope, highlighting the devices requiring deeper protocol analysis and vulnerability assessment. While effective for initial host discovery, ping scans may miss devices with strict firewall settings or those configured not to respond to ICMP or ARP probes.

**(b) Detailed TCP Service Enumeration (Intense Scan):** The second phase of analysis involved an Intense Scan (nmap -T4 -A -v 192.168.1.0/24), which provided a more comprehensive view of the network's open TCP ports, active services, and basic operating system fingerprinting. This scan took approximately 5 minutes to complete, balancing speed and detail with the -T4 timing template.

A notable outcome was the detection of the previously missing second Google Home Mini (192.168.1.186), which was not visible during the initial ping scan. This addition demonstrated how devices on a home network can dynamically appear or become discoverable under different scanning techniques.

Key findings included the router (Docsis-Gateway) was found to expose key management and networking services, including HTTP (port 80), HTTPS (port 443), DNS (port 53), and UPnP (ports 49152–49154). These services, especially UPnP, represent potential risks if exposed externally.

Several IoT devices displayed non-standard HTTP services (e.g., ports 8008, 8443, 9000), and the HP printer revealed a variety of services for web management (HTTP/HTTPS on 80/443, IPP on 631, 8080), file sharing via SMB (ports 139/445), and direct print communication (JetDirect on 9100). The Apple TV exposed ports commonly used for media streaming protocols (RTSP on 5000/7000, DAAP on 3689, AirPlay on 7100), while the Windows laptop presented services for file sharing (SMB on 139/445), remote procedure calls (RPC on 135), and a MySQL database (port 3306), alongside potential UPnP (port 5337) and Intel Active Management Technology (AMT on 16992). This scan began to map the attack surface by revealing potential entry points through these open TCP services.

The following table summarizes the most significant findings from the Intense Scan:

Table 2: Intense Scan- Key Findings

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Device Type | IP Address | Key Open Ports | Services/Protocols | Risk Level |
| Router | 192.168.1.1 | 80, 443, 53, UPnP (49152-49154) | HTTP, HTTPS, DNS, UPnP | High |
| Google Home Mini | 192.168.1.16 | 8008, 8009, 8443 | HTTP, SSL, AJP | Medium |
| HP Printer | 192.168.1.151 | 80, 443, 631, 8080, 139, 445, 9100 | HTTP, HTTPS, IPP, SMB, JetDirect | High |
| Apple TV | 192.168.1.133 | 3689, 5000, 7000, 7100 | iTunes DAAP, RTSP, Airplay | Medium |
| Mobile Device | 192.168.1.248 | 62078 | iTunes sync port | Medium |
| Laptop | 192.168.1.46 | 139, 445, 135, 3306, 5357, 16992 | SMB, RPC, MySQL, UPnP, Intel AMT | High |

* **Filtered Ports:** Ports 22 (SSH), 23 (Telnet), 8000, and 9000 were identified as filtered on the router (192.168.1.1). This "filtered" status implies that these ports are not currently accessible, but the underlying services may still be present. Further analysis is required to determine the exact configuration and ensure that these services cannot be reached from external networks. The risk here is the potential for misconfiguration or vulnerabilities that could lead to these services being exposed.
* **Open Port 9000 (cslistener):** A notable discrepancy was observed with port 9000 (cslistener). While filtered on the router, it was found to be open on both Google Home Minis (192.168.1.16 and 192.168.186). Port 9000 is associated with custom applications and has been implicated in malware command-and-control channels. The presence of this open port on the Google Home Minis represents a significant security risk, potentially allowing unauthorized access or control of these devices. This finding warrants immediate investigation and remediation.

**(c) Comprehensive Protocol and Script Analysis (Slow Comprehensive Scan):** The final, most detailed scan was a Slow Comprehensive Scan, executed using an advanced Nmap command integrating TCP SYN (-sS), UDP (-sU), and extensive service/script detection. This scan ran for approximately 18 hours, reflecting the significant time required to uncover deeply hidden services and vulnerabilities. This scan uncovered a deeper layer of network services, many of which were not visible during the faster Intense Scan.

Key findings include the discovery of critical UDP services:

* **DNS (port 53)** on the router, now confirmed to support recursive queries.
* **DHCP (port 67)** on the router and smart thermostats, essential but exploitable.
* **SNMP (port 161)** on the HP printer, which can expose sensitive system data if misconfigured.
* **mDNS (port 5353)** on several devices, enabling device discovery but also potentially usable in multicast attacks.

These UDP services, while essential for network operation, also represent potential attack vectors (e.g., DNS poisoning, DHCP spoofing, SNMP exploits).

Additionally, **TFTP (port 69)** was detected on the router—a protocol known for unauthenticated file transfers, posing risks for unauthorized configuration access.

The execution of Nmap Scripting Engine (NSE) scripts provided further insights:

* The HP printer supported HTTP methods PUT and DELETE, considered risky, and used a self-signed SSL certificate with the deprecated SHA1 algorithm.
* The Windows laptop's open SMB ports and Intel AMT interface were flagged for their vulnerability potential.
* A number of NSE script errors were noted, suggesting hardened configurations or communication issues with certain devices.

Again, scan 3 was a slow, comprehensive scan that included SYN, UDP, and detailed service scans. This scan uncovered additional vulnerabilities and silent services not detected in the faster, intense scan. The comparison below outlines key differences and newly discovered information.

Table 3: Key Enhancements in Scan 3 Compared to Scan 2

|  |  |  |
| --- | --- | --- |
| Category | Found Only in Scan 3 | Notes |
| UDP Ports | 67, 69, 161, 1900, 5353, 502, others | Critical for IoT, DHCP, TFTP, SNMP, mDNS—mostly hidden in Scan 2 |
| SNMP | 161/UDP on HP Printer | Used by printers; may expose system data if misconfigured |
| TFTP | 69/UDP on router | Often unauthenticated; risky for remote configuration access |
| DHCP & DNS | 67/UDP, 53/UDP | DHCP server details and DNS recursion enabled, only partially seen before |
| New HTTP Headers | Detailed redirects, cookies, and SSL certs | Includes router-portal behavior, missing in Scan 2 |
| UPnP Info | Ports 49152–49154 with firmware info | Reveals firmware versions and service descriptors |
| Service Fingerprints | micro\_httpd, SNMPv1, dnsmasq-2.83 | Version-specific details useful for vulnerability matching |

**(d) Combined Attack Surface Analysis and Utility of Scan Results:**

From the combined results of my three scans, I've outlined a multi-faceted attack surface, with these key exposures and recommendations:

* **Router (Docsis-Gateway):** The router is a critical point of failure. The combination of open web interfaces (HTTP/HTTPS), DNS, and UPnP creates multiple attack vectors. The information gathered from the third scan also revealed that TFTP (port 69), a protocol known for unauthenticated file transfers, and confirmed DNS (port 53) supports recursive queries, both of which increase the risk.
  + **Attack Surface:** UPnP (ports 49152-49154) allows potential bypassing of the firewall, and the web interface (ports 80, 443) is a target for remote attacks. TFTP (port 69) and DNS recursion (port 53) increase the risk. The Nmap scan indicates that the router is running dnsmasq (version 2.83) which, by default, allows recursive DNS queries. This means the router will query other DNS servers to resolve domain names on behalf of devices on the local network. If this recursion is not restricted to the internal network, it can be abused in DNS amplification attacks, where attackers send small queries to the router, causing it to send much larger responses to a target, overwhelming it with traffic.
  + **Recommendations:**
    - Disable UPnP to prevent external control via NAT traversal.
    - Secure the web interface with strong credentials and access controls.
    - Disable TFTP if not required and restrict DNS recursion to the internal network. This means configuring the router to only answer DNS queries from devices on the local network, preventing it from being used in DNS amplification attacks.
* **IoT Devices:** IoT devices (Google Home, thermostats, iRobot, Roku, Apple TV, EntertamentRoom) expose a range of services (HTTP, SSL, RTSP, DAAP, AirPlay) on both standard and non-standard ports.
  + **Attack Surface:** These devices often have weak security, exposing management interfaces and creating a significant attack surface. The presence of cslistener on port 9000 on the Google Home Minis is a high-risk indicator for potential malware or unauthorized access. The third scan also highlighted the use of UDP-based protocols like mDNS (port 5353) on several devices, which can be exploited.
  + **Recommendations:**
    - Patch IoT firmware to close known vulnerabilities.
    - Change default credentials and disable unnecessary services.
    - Isolate IoT devices on a separate network segment (VLAN) to limit lateral movement.
    - Investigate and mitigate the cslistener port on the Google Home Minis.
* **Printer (HP1C95C0):** The printer's extensive web interface (HTTP/HTTPS, IPP), file sharing (SMB), and printer-specific protocols (JetDirect, HP-GSG) make it a high-risk device.
  + **Attack Surface:** The web interface is a target for unauthorized access, and open SMB ports allow for potential file access and lateral movement. The third scan detected risky HTTP methods (PUT, DELETE) and a weak SSL certificate (SHA1), confirming significant vulnerabilities.
  + **Recommendations:**
    - Update printer firmware and change default credentials.
    - Restrict network access to the printer and disable unnecessary services.
    - Disable or secure SMB and JetDirect.
    - Disable risky HTTP methods (PUT, DELETE) and update the SSL certificate.
* **Laptop (LanaB-LP**): The laptop's open SMB, RPC, and MySQL services make it a prime target for attacks.
  + **Attack Surface:** Exposed SMB services pose a significant risk of unauthorized file access and lateral movement. The presence of Intel AMT allows for remote management, creating a severe vulnerability if not properly secured.
  + **Recommendations:**
    - Enable a firewall and use strong passwords.
    - Keep the operating system and software up to date.
    - Disable unnecessary services.
    - Secure or disable Intel AMT.
* **Mobile (iPhone):**
  + **Attack Surface:** The open tcpwrapped port (62078) is unusual and requires further investigation. Mobile devices, in general, are vulnerable to malware and can provide access to sensitive network resources.
  + **Recommendations**: Keep the operating system and apps up to date, use a strong passcode, and be cautious about connecting to untrusted Wi-Fi networks.
* **Wireless Network (802.11):**
  + **Attack Surface:** The scans do not provide detailed information about wireless security. However, the prevalence of wireless devices (mobile, IoT, streaming) underscores the importance of strong Wi-Fi security. A compromised Wi-Fi network could grant attackers access to all connected devices.
  + **Recommendations:**
    - Use strong Wi-Fi encryption (WPA3).
    - Implement network segmentation (e.g., guest network) to isolate less trusted devices.
* **Bluetooth and Cloud Components:**
  + **Attack Surface:** Nmap was executed against the local network and did not directly assess Bluetooth or cloud components. Both pose latent risks.
  + **Recommendations:**
    - For Bluetooth, use separate tools to analyze its attack surface. Mitigate risks by disabling Bluetooth when not needed and being cautious about pairing with unknown devices.
    - For cloud services, evaluate account security and privacy settings.

By addressing these vulnerabilities and implementing the recommendations, the network's security posture can be significantly improved. However, due to the dynamic nature of network environments, continuous monitoring remains essential.

**3. What Did You Learn? (Key Takeaways)**

This exercise in mapping and analyzing my home network using Zenmap has provided several valuable insights that have broadened my understanding of network behavior and security assessment.

By exploring how different Nmap command options impacted the results, I learned how specific flags influence scan depth and detail. Tracking these relationships gave me a practical grasp of network analysis nuances and Nmap’s capabilities.

One of the most surprising lessons was the **18-hour runtime** of the comprehensive scan. I initially underestimated how long deep scans could take, even on a home network. This highlighted the critical trade-off between scan speed and thoroughness, especially relevant for business environments where time and resources are limited.

The simple observation of a typographical error in my new Apple TV's network name ("EntertanmentRoom" instead of "EntertainmentRoom") underscores a fundamental aspect of network asset management: even minor inconsistencies can lead to confusion during troubleshooting or security audits. Maintaining accurate and consistent naming conventions is crucial for clear identification and management of network devices, especially in larger organizations.

The absence of my Wi-Fi extender in all scans was a concern. It pointed to either connectivity issues or operation on a different subnet. Such blind spots could hide vulnerabilities, underscoring the need for complete network visibility.

Exploring Nmap's timing templates provided a practical understanding of the trade-offs involved in network scanning. The spectrum from `-T0` (paranoid) to `-T5` (insane) vividly illustrates how scan speed directly correlates with the level of intrusiveness and the potential for detection or instability. For a home network, the aggressive `-T4` offered a reasonable balance, but the explanation of its potential risks on unfamiliar networks was a valuable reminder of ethical considerations and the importance of minimizing disruption during security assessments in professional environments. I now have a better understanding of how to select the appropriate timing template based on the specific context and objectives of the scan.

One powerful takeaway was discovering Zenmap’s ability to save and compare scans over time. This feature is ideal for continuous monitoring, helping detect unauthorized changes or new vulnerabilities—a critical practice for both home and business networks.

I also realized how scan depth must align with network size and objectives. The comprehensive scan revealed the most, but its long runtime showed that efficient, targeted scanning is crucial for larger networks. A phased or script-focused approach might be more practical.

Furthermore, the intense and comprehensive scans revealed weak security configurations on my HP printer. The identification of potentially risky HTTP methods (PUT, DELETE) enabled on its web interface, coupled with the use of a weak SHA1 algorithm for its SSL certificate, raises significant security concerns, especially considering the tendency of printers to retain previously printed and scanned images. If exploited, these weaknesses could allow an attacker to gain unauthorized access to a repository of previously handled documents and images, leading to severe data breaches or the ability to tamper with or intercept future print/scan jobs. This highlights the often-underestimated risk associated with peripheral devices on a network. This would be especially harmful for home printers as most are used to make copies of important documents. The fact that printers on a network can be a significant vulnerability was eye opening.

This exercise wasn’t just about running scans—it deepened my understanding of network dynamics, security implications, and the value of interpreting results critically. From the missing extender to printer vulnerabilities, I saw firsthand how even home networks are complex and require ongoing attention. I also realized the need to upgrade from Windows 10 as support ends and appreciated how AI helped ensure I didn’t overlook key details in the scans output.

Finally, I noticed that my iPhone only responded to pings when unlocked, and as mentioned previously, one Google Home Mini didn’t respond at first—an interesting discovery showing that some devices evade simple scans, reinforcing the need for varied detection methods.