**Abdullrahman Alghanim**

**04/24/2025**

**LAB 13 - Internet of Things (IoT)**

**Network Discovery and IoT Security Assessment**

**1. IoT Devices on My Network**

**I found the following IoT devices connected to my home network:**

* **Smart TV (Samsung)**
* **Smart Thermostat (Google Nest)**
* **Wireless Printer (HP)**
* **Smart Speaker (Amazon Echo)**

**2. Device Configuration and Security Review**

**Google Nest Thermostat**

* **Configuration: Default settings with WPA2 Wi-Fi encryption.**
* **Firmware: Auto-updates enabled; latest version installed.**
* **Accounts: Linked to my Google account.**
* **Vulnerabilities: No known vulnerabilities found.**

**Amazon Echo**

* **Configuration: Auto-updates enabled; strong password set.**
* **Firmware: Latest version installed.**
* **Accounts: Linked to my Amazon account.**
* **Vulnerabilities: No known vulnerabilities found.**

**Samsung Smart TV**

* **Configuration: Remote access features enabled by default.**
* **Firmware: Auto-updates enabled; latest version installed.**
* **Accounts: Linked to my Samsung account.**
* **Vulnerabilities: Remote access features disabled to enhance security.**

**HP Wireless Printer**

* **Configuration: Open web interface initially; secured with a password.**
* **Firmware: Update available; installed the latest version.**
* **Accounts: No account required.**
* **Vulnerabilities: Open port (port 80) secured with a password.**

**3. Network Scanning and Device Identification**

**I used Nmap to scan my local network:**

**bash**

**CopyEdit**

**nmap -sP 192.168.254.0/24**

**This scan revealed several active devices, including my IoT devices.**

**To identify open ports and services, I ran:**

**bash**

**CopyEdit**

**nmap -sV 192.168.254.0/24**

**This provided details on services running on each device.**

**To detect operating systems, I used the -O flag:**

**bash**

**CopyEdit**

**nmap -O 192.168.254.0/24**

**This helped identify the operating systems of connected devices.**

**I also used MAC address lookup tools to identify device manufacturers:**

* **Google Nest Thermostat: Manufacturer: Google**
* **Amazon Echo: Manufacturer: Amazon**
* **Samsung Smart TV: Manufacturer: Samsung**
* **HP Wireless Printer: Manufacturer: HP**

**4. Network Traffic Analysis with Wireshark**

**I captured and analyzed network traffic using Wireshark to understand communication patterns:**

1. **Capture Setup: Selected the appropriate network interface in Wireshark.**
2. **Traffic Filtering: Applied filters to focus on relevant traffic (e.g., ip.addr == 192.168.254.122).**
3. **Analysis: Examined packets for protocols used, data flow, and any unencrypted communications.**

**5. Device Interaction and Analysis**

**I interacted with each IoT device to observe their behavior:**

* **Google Nest Thermostat: Adjusted temperature settings and monitored network traffic.**
* **Amazon Echo: Issued voice commands and observed network responses.**
* **Samsung Smart TV: Streamed content and analyzed data packets.**
* **HP Wireless Printer: Sent print jobs and monitored communication.**

**Wireshark was used to capture and analyze the traffic during these interactions.**

**6. Security Assessment**

**I evaluated the security posture of each IoT device:**

* **Google Nest Thermostat: Utilized WPA2 encryption; no default credentials.**
* **Amazon Echo: Enabled automatic updates; strong password required.**
* **Samsung Smart TV: Remote access features disabled; no default credentials.**
* **HP Wireless Printer: Secured web interface with a password; previously had an open port.**

**I assessed common security issues such as weak authentication, default credentials, and insecure communication.**

**7. Secure Configuration**

**I implemented the following security measures:**

* **Google Nest Thermostat: Enabled WPA2 encryption; changed default password.**
* **Amazon Echo: Enabled automatic updates; set a strong password.**
* **Samsung Smart TV: Disabled remote access features; changed default password.**
* **HP Wireless Printer: Secured web interface with a password; updated firmware.**

**8. Access Control and Authentication**

**I enhanced access control and authentication mechanisms:**

* **Google Nest Thermostat: Enabled two-factor authentication for my Google account.**
* **Amazon Echo: Enabled two-factor authentication for my Amazon account.**
* **Samsung Smart TV: Set up a unique PIN for accessing settings.**
* **HP Wireless Printer: Restricted access to the web interface to trusted IP addresses.**

**9. Conclusion**

**Through this assignment, I discovered and analyzed the IoT devices on my network, assessed their security configurations, and implemented necessary measures to enhance their security. This exercise provided valuable insights into the importance of securing IoT devices in a home network environment**

