Home Network Penetration Test Report

CSIA 440 Cyber Testing and Penetration

May 25, 2025

Samuel Mendez

Columbia basin college  Professor Eric Robinson

**Introduction**

Testing Team:

5/19/2025

Sam Mendez

(509) 380 – 5555

Unexperience Cyber Security Professional with hands on experience on Linux and Windows system administration, Nmap, and vulnerable scanning tools.

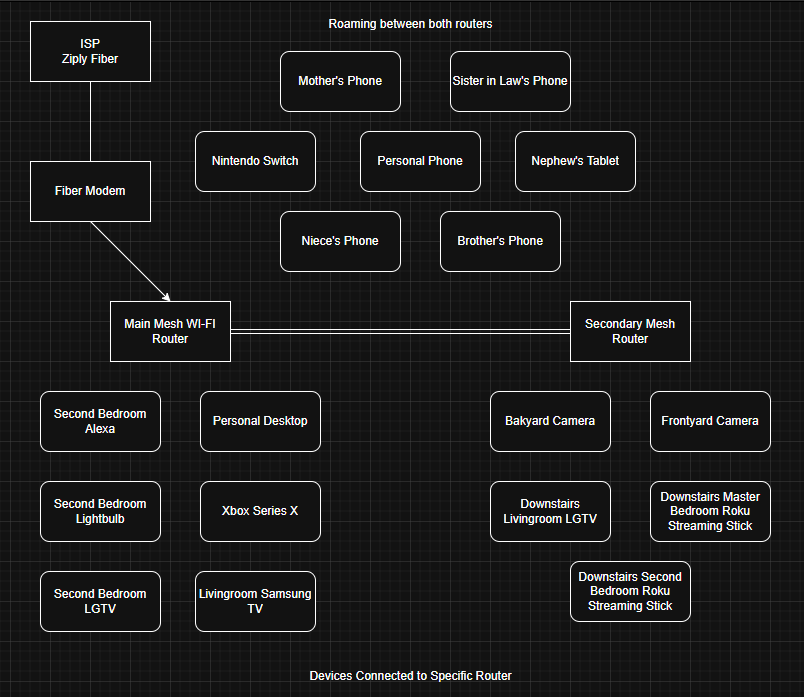
Purpose:

The purpose of this test is to evaluate the current security posture of my home network and identify vulnerabilities that could potentially be exploited by attackers. The findings will be used to strengthen the network's defenses and enhance cybersecurity awareness.

Test Type:

This test will be conducted as a White-Box Vulnerability Assessment, meaning the tester has full knowledge of the network and its assets. The goal is to identify misconfigurations, weak points, and exposed services without performing exploitative actions.

Network Details:



|  |  |  |  |
| --- | --- | --- | --- |
| **DNS Name** | **IP Address** | **OS Description** | **Purpose** |
| Personal Phone | 192.168.68.54 | Android | Smart Phone |
| Backyard Camera | 192.168.68.65 | unknown | Surveillance |
| Second Bedroom LGTV | 192.168.68.67 | WebOS | Smart TV |
| Front yard Camera | 192.168.68.56 | unknown | Surveillance |
| Personal Desktop | 192.168.68.60 | Windows | PC |
| Mother's Phone | 192.168.68.74 | Android | Smart Phone |
| Xbox Series X | 192.168.68.51 | Windows | Video Game Console |
| Second Bedroom Lightbulb | 192.168.68.59 | unknown | IoT |
| Second Bedroom Alexa | 192.168.68.52 | unknown | IoT |
| Living Room Samsung TV | 192.168.68.61 | Tizen OS | Smart TV |
| Nintendo Switch | 192.168.68.62 | Horizon | Video Game Console |
| Niece's Phone | 192.168.68.58 | iOS | Smart Phone |
| Downstairs Master Bedroom Roku Streaming Stick | 192.168.68.50 | Roku OS | Streaming Device |
| Sister in Law's Phone | 192.168.68.63 | iOS | Smart Phone |
| Nephew's Tablet | 192.168.68.53 | iOS | Tablet |
| Brother's Phone | 192.168.68.64 | iOS | Smart Phone |
| Downstairs Second Bedroom Roku Streaming Stick | 192.168.68.69 | Roku OS | Streaming Device |
| Downstairs Livingroom LGTV | 192.168.68.55 | WebOS | Smart TV |

**Executive Summary**

Risk Analysis:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Risk** | **Device** | **Issue** | **Likelihood** | **Impact** |
| R1 | Personal Desktop (Windows) | May have open RDP (3389) or SMB (445) ports vulnerable to attacks | High | High |
| R2 | LGTV / Samsung TV | Smart TVs with outdated WebOS/Tizen may have exploitable web services | Medium | Medium |
| R3 | Lightbulb, Alexa, Camera | Unknown OS/patch level on IoT makes them harder to secure | Low | Low |

R1: Open Ports on Windows Desktop

The personal desktop (192.168.68.60), running Windows, may have ports such as RDP (3389) or SMB (445) open, which are commonly targeted by attackers. If exposed or improperly secured, these ports could allow unauthorized access to the system.  
Recommendation: Disable unused ports, apply strict firewall rules, and restrict RDP to internal IP addresses only.

R2: Smart TVs with Outdated OS

Smart TVs such as the Second Bedroom LGTV, Livingroom Samsung TV, and Downstairs Livingroom LGTV may run outdated firmware or insecure versions of WebOS or Tizen OS. These devices are often overlooked in updates and could expose remote services or vulnerabilities.  
Recommendation: Ensure all Smart TVs are updated with the latest firmware and isolate them on a guest or IoT VLAN.

R3: IoT Devices with Unknown OS

Devices such as the Second Bedroom Lightbulb, Alexa, and surveillance cameras use unknown or proprietary operating systems and may not receive regular updates. These devices often lack visibility and can be exploited or leveraged in DDoS attacks.

Recommendation: Place IoT devices on a segregated network, disable UPnP, and monitor their traffic for anomalies.

**Technical Summary**

Reconnaissance:

Tool 1: Google Search

A Google search of my name “Samuel Mendez, Pasco Wa” only reveals public social profiles. No other sensitive personal information was found.

Tool 2: Whois Lookup

My public IP shows I’m using Ziply fiber with a location near Kennewick, WA. No personally identifiable information was exposed.

Tool 3: Shodan

Shodan identified my ASUS (motherboard) router as being accessible on ports **7547** and **8443**. Port 8443 hosts the HTTPS web interface for the router's admin panel, potentially exposing it to remote attacks if not secured. Port 7547 is commonly used for ISP remote management (TR-069), which could also be a risk if misconfigured.

Tool 4: Censys

I searched my public IP address on Censys.io and found no publicly accessible services listed. The IP is associated with Ziply Fiber (AS-WHOLESAIL), located in Highland, Washington. This confirms that the host may be protected by NAT, firewalls, or the services are simply not exposed to the public internet.

Tool 5: Have I Been Pwned

I used HaveIBeenPwned.com to check if my email address had been exposed in any known data breaches. The tool reported **zero data breaches**, meaning my email address has not been involved in any leaks as of now.

Physical Assessment:

|  |  |
| --- | --- |
| **Control** | **Description** |
| 1. **Router Placement** | The modem is placed in my bedroom in the of an entertainment set. The door and window have locks, so when I leave the house, my room is inaccessible. |
| 2. **Security Cameras** | Front yard and backyard cameras are actively monitoring entry points to detect unauthorized access attempts. |
| 3. **Limited Physical Access to Network Hardware** | Network hardware such as main mesh Wi-Fi router, and secondary mesh router are all placed in locations that are not easily accessible to guests or children. This reduces the likelihood of accidental unplugging, tampering, or reset attempts. Main Mesh Router is in my room which is inaccessible when I leave the house since door and window are locked. |

Wireless Network Scan:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **SSID** | **Encryption Type** | **Signal Strength** | **Mode** | **Max Rate (Mbps)** |
| The Casita | WPA2/WPA3 | -27 dBm | b/g/n/ac/ax | 1,531.30 |
| [HIDDEN] on The Casita | WPA2/WPA3 | -27 dBm | b/g/n/ac/ax | 1,020.80 |
| SpectrumSetup-CB | WPA2 | -50 dBm | b/g/n/ac/ax | 2,402.00 |

The scan detected multiple wireless networks nearby. My network, **The Casita**, had the strongest signal at -27 dBm and uses WPA2/WPA3 encryption with a dual-band configuration supporting Wi-Fi 6 (ax), offering a max rate of 1,531.3 Mbps.  
Nearby networks such as **SpectrumSetup-CB** and **[HIDDEN] on The Casita** also had strong signal levels, but **SpectrumSetup-CB** reports a higher theoretical maximum rate of 2,402 Mbps.  
All three networks use modern encryption (WPA2 or higher) and support high-speed protocols, though hidden SSIDs may indicate attempts to obscure network visibility.

Nmap Scan:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| DNS Name | IP Address | OS Description | Purpose | Open TCP Ports | Risk Analysis |
| Downstairs Master Bedroom Roku Streaming Stick | 192.168.68.50 | Roku OS | Streaming Device | 7000 | Port 7000 used by AirTunes; could be vulnerable if service is outdated. Fix: Restrict access and keep firmware updated. |
| Xbox Series X | 192.168.68.51 | Windows | Video Game Console | 80, 554, 8888, 10000 | Ports 554 and 10000 suggest streaming and admin services. Risk: Stream hijacking or unauthorized configuration. Fix: Secure interface and restrict external access. |
| Second Bedroom Alexa | 192.168.68.52 | Linux (Amazon) | IoT | 1080, 8888, 10001 | Port 1080 (SOCKS) could be abused for tunneling. Fix: Block or monitor access; secure the device. |
| Nephew's Tablet | 192.168.68.53 | iOS | Tablet | 49152, 62078 | Common iOS/macOS service ports; risk of exposure if used improperly. Fix: Disable unused services. |
| Frontyard Camera | 192.168.68.56 | Linux/nginx | Surveillance | 49152, 62078 | Likely IP camera ports. Risk: Remote view/control if not secured. Fix: Disable remote access or secure with strong passwords. |
| Niece's Phone | 192.168.68.58 | iOS | Smart Phone | 2869 | Used by Microsoft UPnP. Risk: Could expose device info. Fix: Disable UPnP unless required. |
| Second Bedroom Lightbulb | 192.168.68.59 | IwIP Stack | IoT | 6668 | Common port for Tuya IoT devices. Risk: Vulnerable to botnets. Fix: Isolate device and block WAN access. |
| Personal Desktop | 192.168.68.60 | Windows | PC | 1102, 1113, 3000, 3001, 7000, 8008, 8009, 8443, 9080, 15002 | Various media and control ports. Risk: Potential remote access or media interception. Fix: Disable unnecessary services. |
| Living Room Samsung TV | 192.168.68.61 | Tizen OS | Smart TV | 135, 139, 445, 5357 | Windows ports for file sharing and HTTP. Risk: Vulnerable to exploits like EternalBlue. Fix: Block externally and patch OS. |
| Nintendo Switch | 192.168.68.62 | Horizon | Video Game Console | 4000, 8001, 8002, 8080, 9080, 32768, 32772, 32773, 32774 | Various admin or RPC services. Risk: Could be entry points if unpatched. Fix: Limit access and monitor traffic. |
| Sister in Law's Phone | 192.168.68.63 | iOS | Smart Phone | 80, 554, 8888, 10000 | Similar to surveillance setup. Risk: Unauthorized stream or admin access. Fix: Secure credentials and block internet access. |

Vulnerable Scan:

Nessus Essentials Vulnerability Scan:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **DNS Name** | **IP Address** | **OS Description** | **Purpose** | **Vulnerability** | **Risk Analysis** |
| Samsung TV | 192.168.68.61 | Tizen OS | Smart TV | TLS Version 1.0 Protocol Detection | TLS 1.0 is deprecated and vulnerable to downgrade and cipher attacks. Fix: Disable TLS 1.0 and enable TLS 1.2/1.3 in settings or isolate the device. |
| Xbox Series X | 192.168.68.51 | Windows-based | Game Console | HTTP Server on Port 10000 Detected | Port 10000 is commonly used for admin interfaces and may allow remote access. Fix: Restrict access to LAN or disable remote access features if not in use. |
| Alexa Device | 192.168.68.52 | Linux (Amazon) | IoT Assistant | Web Server Transmits Cleartext Credentials | Login data may be intercepted over HTTP. Fix: Force HTTPS or block web interface externally. |
| Roku Stick | 192.168.68.50 | Roku OS | Streaming Device | Open Web Interface Detected (Port 8060) | May allow unauthorized control or browsing. Fix: Disable remote HTTP interface or place behind firewall. |
| Personal Desktop | 192.168.68.60 | Windows | PC | Unsupported Windows Services Detected | Older Windows services may be unpatched or exposed. Fix: Disable unnecessary services and apply system updates. |

**Annexes**

Methodology:

To complete this home network penetration test, a structured approach was taken to identify potential vulnerabilities, assess risks, and recommend mitigations. The steps followed were:

1. **Network Identification**: Using the mesh Wi-Fi app and Nmap, all devices on the network were identified and their IP addresses recorded.
2. **Reconnaissance**: Five open-source intelligence tools were used (Google, Whois, Shodan, Censys, HaveIBeenPwned) to gather external information about the network and personal exposure.
3. **Physical Assessment**: Photos and notes were taken on physical security controls protecting the network and access to hardware.
4. **Wireless Scan**: inSSIDer was used to scan local wireless networks and assess encryption strength, signal quality, and network visibility.
5. **Port & Service Scanning**: Nmap was used to scan the internal network and document open ports, device roles, and OS information.
6. **Vulnerability Assessment**: Nessus Essentials was configured and run against the internal network. Results were analyzed, and the most relevant vulnerabilities were documented in the report.
7. **Documentation**: Data from each tool was collected, organized, and translated into actionable risk and mitigation recommendations.

Reflection:

This process enhanced my practical skills in using cybersecurity tools like Nmap and Nessus, and improved my understanding of how vulnerable everyday home networks can be. I gained valuable experience in identifying weak points, interpreting scan data, and thinking like a security professional when making recommendations.

Results:

Wireless Network Scan Results

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **SSID** | **Encryption Type** | **Signal Strength** | **Mode** | **Max Rate (Mbps)** |
| The Casita | WPA2/WPA3 | -27 dBm | b/g/n/ac/ax | 1,531.30 |
| [HIDDEN] on The Casita | WPA2/WPA3 | -27 dBm | b/g/n/ac/ax | 1,020.80 |
| SpectrumSetup-CB | WPA2 | -50 dBm | b/g/n/ac/ax | 2,402.00 |

Nmap Scan Results

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| DNS Name | IP Address | OS Description | Purpose | Open TCP Ports | Risk Analysis |
| Downstairs Master Bedroom Roku Streaming Stick | 192.168.68.50 | Roku OS | Streaming Device | 7000 | Port 7000 used by AirTunes; could be vulnerable if service is outdated. Fix: Restrict access and keep firmware updated. |
| Xbox Series X | 192.168.68.51 | Windows | Video Game Console | 80, 554, 8888, 10000 | Ports 554 and 10000 suggest streaming and admin services. Risk: Stream hijacking or unauthorized configuration. Fix: Secure interface and restrict external access. |
| Second Bedroom Alexa | 192.168.68.52 | Linux (Amazon) | IoT | 1080, 8888, 10001 | Port 1080 (SOCKS) could be abused for tunneling. Fix: Block or monitor access; secure the device. |
| Nephew's Tablet | 192.168.68.53 | iOS | Tablet | 49152, 62078 | Common iOS/macOS service ports; risk of exposure if used improperly. Fix: Disable unused services. |
| Frontyard Camera | 192.168.68.56 | Linux/nginx | Surveillance | 49152, 62078 | Likely IP camera ports. Risk: Remote view/control if not secured. Fix: Disable remote access or secure with strong passwords. |
| Niece's Phone | 192.168.68.58 | iOS | Smart Phone | 2869 | Used by Microsoft UPnP. Risk: Could expose device info. Fix: Disable UPnP unless required. |
| Second Bedroom Lightbulb | 192.168.68.59 | IwIP Stack | IoT | 6668 | Common port for Tuya IoT devices. Risk: Vulnerable to botnets. Fix: Isolate device and block WAN access. |
| Personal Desktop | 192.168.68.60 | Windows | PC | 1102, 1113, 3000, 3001, 7000, 8008, 8009, 8443, 9080, 15002 | Various media and control ports. Risk: Potential remote access or media interception. Fix: Disable unnecessary services. |
| Living Room Samsung TV | 192.168.68.61 | Tizen OS | Smart TV | 135, 139, 445, 5357 | Windows ports for file sharing and HTTP. Risk: Vulnerable to exploits like EternalBlue. Fix: Block externally and patch OS. |
| Nintendo Switch | 192.168.68.62 | Horizon | Video Game Console | 4000, 8001, 8002, 8080, 9080, 32768, 32772, 32773, 32774 | Various admin or RPC services. Risk: Could be entry points if unpatched. Fix: Limit access and monitor traffic. |
| Sister in Law's Phone | 192.168.68.63 | iOS | Smart Phone | 80, 554, 8888, 10000 | Similar to surveillance setup. Risk: Unauthorized stream or admin access. Fix: Secure credentials and block internet access. |

Vulnerability Scan Results

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **DNS Name** | **IP Address** | **OS Description** | **Purpose** | **Vulnerability** | **Risk Analysis** |
| Samsung TV | 192.168.68.61 | Tizen OS | Smart TV | TLS Version 1.0 Protocol Detection | TLS 1.0 is deprecated and vulnerable to downgrade and cipher attacks. Fix: Disable TLS 1.0 and enable TLS 1.2/1.3 in settings or isolate the device. |
| Xbox Series X | 192.168.68.51 | Windows-based | Game Console | HTTP Server on Port 10000 Detected | Port 10000 is commonly used for admin interfaces and may allow remote access. Fix: Restrict access to LAN or disable remote access features if not in use. |
| Alexa Device | 192.168.68.52 | Linux (Amazon) | IoT Assistant | Web Server Transmits Cleartext Credentials | Login data may be intercepted over HTTP. Fix: Force HTTPS or block web interface externally. |
| Roku Stick | 192.168.68.50 | Roku OS | Streaming Device | Open Web Interface Detected (Port 8060) | May allow unauthorized control or browsing. Fix: Disable remote HTTP interface or place behind firewall. |
| Personal Desktop | 192.168.68.60 | Windows | PC | Unsupported Windows Services Detected | Older Windows services may be unpatched or exposed. Fix: Disable unnecessary services and apply system updates. |