Home Network Vulnerability Assessment Checklist (Draft)

1. Network Access and Router Security

Router Access Control

- ☐ Change the default router login username and password.
- ☐ Disable remote management of the router if not necessary.
- ☐ Regularly update the router firmware to patch security vulnerabilities.

Wi-Fi Security Settings

- ☐ Use WPA3 encryption for Wi-Fi (WPA2 if WPA3 is not available).
- ☐ Set a strong, unique Wi-Fi password (minimum 12 characters with a mix of letters, numbers, and symbols).
- ☐ Hide the network SSID (optional for added security but may reduce convenience).
- ☐ Create a separate guest network for visitors, limiting guest access to local devices.

Device Whitelisting

- ☐ Enable MAC address filtering to restrict which devices can join the network.

2. Device Security

Device Inventory

- ☐ List all devices connected to the network (e.g., computers, phones, smart TVs, IoT devices).
- ☐ Check if any unknown or unauthorized devices are on the network.

Device Software and Firmware Updates

- ☐ Ensure all devices have the latest software and firmware updates.
- ☐ Enable automatic updates on devices whenever possible.

Device Passwords and Authentication

- ☐ Set strong, unique passwords for each device.
- ☐ Enable multi-factor authentication (MFA) for services and accounts when available.

IoT Device Security

- [ ] Change default passwords on all IoT devices.
- [ ] Disable unused or insecure features, like remote access or universal plug and play (UPnP).

3. Network Monitoring and Logging

Router Logs

- [ ] Enable logging on the router to track any unusual activity.
- [ ] Review logs periodically for unknown devices or suspicious activity.

Firewall and Intrusion Detection

- [ ] Enable the router's firewall and ensure it's configured correctly.
- [ ] If available, activate intrusion detection or prevention systems (IDS/IPS).

4. Data Privacy and Protection

Encryption

- [ ] Enable encryption for sensitive files and communications, especially over public networks.
- [ ] Use a VPN for added privacy and security when accessing the internet on public networks.

Personal Data Protection

- [ ] Disable unnecessary file sharing between devices.
- [ ] Ensure that sensitive files are not stored in easily accessible locations or shared folders.

5. Remote Access and External Connections

VPN for Remote Access

- [ ] Use a VPN if remote access to the home network is needed.
- [ ] Avoid using public Wi-Fi for accessing home network services directly.

Disable Unused Ports and Services

- [ ] Disable any open ports or services not in use.
- [ ] Check for open ports using a tool like GRC's ShieldsUP! or Nmap to assess exposure.

6. Physical Security

Router and Device Placement

- ☐ Place the router in a secure location where unauthorized individuals cannot access it physically.
- ☐ Restrict access to sensitive devices (such as computers and storage drives).

7. Regular Maintenance

Periodic Checks

- ☐ Review this checklist every 6–12 months or after any significant network changes.
- ☐ Run periodic vulnerability scans (e.g., with tools like Nessus Essentials or OpenVAS) to detect any potential issues.

Backup and Recovery

- ☐ Regularly backup important data to an external hard drive or secure cloud storage.
- ☐ Ensure backup files are protected with encryption and only accessible by authorized devices.

Notes and Observations

Additional Observations:

- ☐ Note any unusual behaviors, recurring issues, or additional security recommendations observed during the assessment.