HOME NETWORK
SECURITY AUDIT

Prepared by: Sanjeel Shrestha

IT Graduate | Cybersecurity Enthusiast

Sydney, NSW, Australia

May 2026

Cisco Introduction to Cybersecurity — Portfolio Project

Introduction

A network security audit is a structured review of a network system to assess its privacy and security. For everyday households, it is essential for maintaining and strengthening the protection against unauthorized access and cyber threats. This report audits the home network of a fictional Australian household, identifying vulnerabilities and providing recommendations to improve their overall security posture.

Audit Subject

Name: The Smith Household

Location: Sydney, NSW, Australia

Internet Provider: Telstra

Router Model: TP-Link Archer AX55

Number of Devices: 8 — 2 Laptops, 3 Phones, 1 Smart TV, 1 Gaming Console, 1 Smart Doorbell

Findings

Finding 1 — Default Router Password

⚠️ **Status: At Risk**

Finding: The router password has not been changed from the factory default "admin".

Risk: Anyone with physical or network access can log into the router and change settings, intercept traffic, or lock out the owner.

Recommendation: Change the router password immediately to a strong, unique password of at least 12 characters containing uppercase, lowercase, numbers and symbols.

Finding 2 — WiFi Password Set to Home Address

⚠️ **Status: At Risk**

Finding: The password for the WiFi is set to the household's home address.

Risk: The password is easy to crack as it is based on a basic personal detail of the owner. It makes guessing easy for anyone attempting to access the network.

Recommendation: Change the password to something strong and unique with at least 12 characters including uppercase, lowercase, numbers and symbols.

Finding 3 — No Guest Network

⚠️ **Status: At Risk**

Finding: There is no separate WiFi network for guests.

Risk: This gives external users direct access to the central WiFi network, allowing them to make unwanted changes or access shared devices.

Recommendation: Set up a separate guest WiFi network with a different password and name, to be provided only to visitors.

Finding 4 — Firmware 2 Years Out of Date

⚠️ **Status: At Risk**

Finding: The router firmware update has been pending for two years.

Risk: The router is not protected by the latest security patches and remains vulnerable to known exploits that have since been fixed.

Recommendation: Update the router firmware immediately and enable automatic updates to ensure ongoing protection.

Finding 5 — WPA2 Instead of WPA3

⚠️ **Status: At Risk**

Finding: The WiFi is using WPA2 encryption, which is an older standard.

Risk: WPA2 is a weaker encryption standard compared to WPA3 and is easier to compromise using modern attack techniques.

Recommendation: Upgrade to WPA3 encryption through the router settings for stronger, more modern WiFi security.

Finding 6 — Remote Management Turned On

⚠️ **Status: At Risk**

Finding: The remote management setting on the router has been left enabled.

Risk: Anyone with network access can make changes to the router settings from any location, increasing the attack surface significantly.

Recommendation: Disable remote management in the router settings to restrict configuration access to the local network only.

Finding 7 — Unrecognised Device — Smart Doorbell

⚠️ **Status: At Risk**

Finding: There is an 8th device — a smart doorbell — connected to the network that the family did not knowingly connect.

Risk: An unrecognised device on the network is a potential security risk. It may have been connected without authorisation and could be used to monitor or intercept network traffic.

Recommendation: Identify the device through the router's connected devices list. If it cannot be verified, remove its network access immediately and investigate further.

Summary

Finding	Status	Priority
Default Router Password	At Risk	**High**
WiFi Password Weak	At Risk	**High**
No Guest Network	At Risk	**Medium**
Firmware Outdated	At Risk	**High**
WPA2 Instead of WPA3	At Risk	**High**
Remote Management On	At Risk	**Medium**
Unrecognised Device	At Risk	**Medium**

Conclusion

The audit shows that the Smith household network is indeed at risk. Several severe risks — including the outdated firmware, weak passwords, and an unrecognised device — need to be addressed immediately. Moving forward, the household should schedule regular firmware updates, adopt stronger encryption standards, and periodically review all connected devices to maintain a secure network environment.