

Investigate, Analyse and Demonstrate the Importance of Network Security in a Home Network

Joshua J. Harries • BSc (Hons) Computing (Computer Networks and Cybersecurity)
Supervisor: Carlene Campbell • September 2025



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Home networks increasingly resemble small enterprises: dozens of devices, cloud connected services, and mixed trust users. This project investigates how a focused set of low cost, platform agnostic controls—segmentation, service minimisation, credential hygiene, timely updates, and right sized monitoring—changes the security posture of a typical UK home.

Methodology

Using a before/after experimental design, we built a Baseline configuration and a Hardened configuration, then ran repeatable tests (external exposure checks, internal discovery, default/weak credential abuse, lateral movement from IoT, UPnP/remote admin exposure, exploit attempts, and detection).

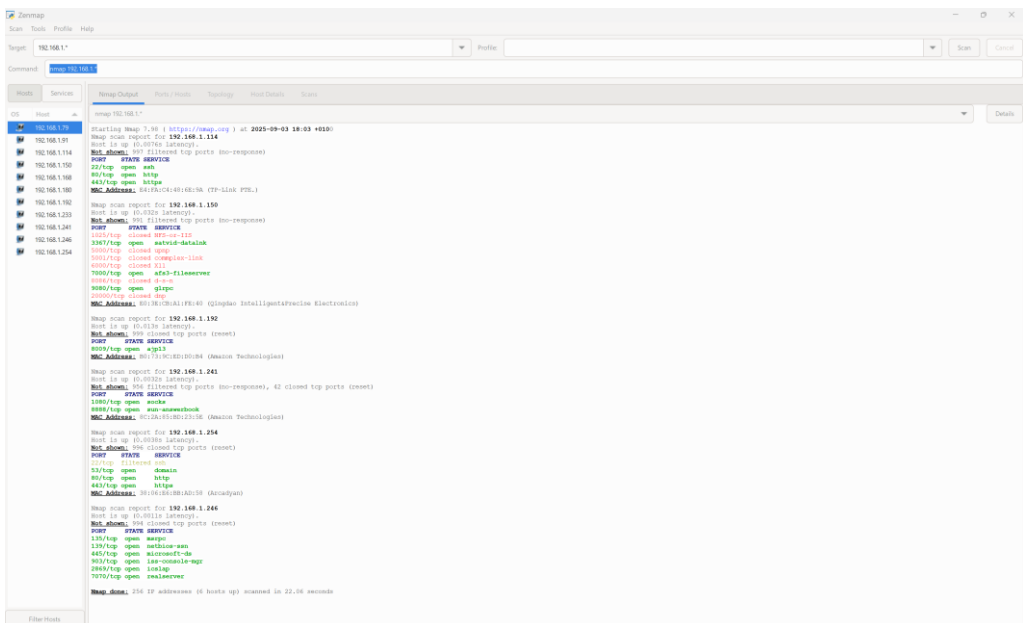
Findings

Results show a marked reduction in reachable attack surface and scanner visible risk, prevention of trivial compromises and lateral movement, and timely detection of reconnaissance/brute force activity. The findings align with current UK guidance (NCSC) and are feasible on consumer-grade equipment.

Thank you Stephen, Carlene, Gaynor, and the wider TSD / SOAC team for all your support.

Recommendations

- Disable UPnP and WAN-side admin; use HTTPS/SSH for management.
- Rotate unique passwords; remove vendor defaults; enable MFA where available.
- Apply firmware/OS updates on a regular cadence.
- Adopt three segments (Trusted/IoT/Guest) with default-deny inter-VLAN initiation.
- Enable client isolation on guest SSIDs; prefer WPA3; disable WPS.



Screenshot of a non-segmented home network on nmap where all devices, including IoT devices, are present and accessible.

Selected References

NCSC home device guidance; Network security fundamentals
PSTI regulations (DSIT/OPSS) for consumer connectable products
ETSI EN 303 645 baseline for consumer IoT security
CIS Critical Security Controls v8.1
MITRE ATT&CK techniques: T1078.001, T1110, T1133, T1046, T1557.001
ENISA Threat Landscape 2024
NIST SP 800-115 (testing & assessment)