Review report of network scanning of macbook

This project demonstrates network reconnaissance on a router using Nmap, identifying open services such as DNS and RTSP and analyzing their security posture.

Observations

- Two active hosts were detected on the network
- The router was reachable and responsive
- Port 53 (DNS) was open and providing name resolution services
- Port 5000 (RTSP) was open and associated with Apple AirTunes / AirPlay
- Services returned 403 Forbidden, indicating access restriction

Security Analysis

- DNS services should be monitored to prevent spoofing or amplification attacks
- RTSP streaming services should be restricted to trusted local devices only
- No unnecessary ports were exposed

Conclusion

This experiment demonstrates how Nmap can be used for network reconnaissance to identify services and analyze network exposure. Such analysis helps improve defensive security measures.

Ethical Disclaimer

All scans were performed on my own local network for educational purposes only. No unauthorized systems were scanned.