Alex’s Thoughts

1. Research Question/Literacy Review:
   1. What are the most common security vulnerabilities in consumer networking equipment and how can they be mitigated?
   2. How secure are the default confs and firmware of popular networking equipment?
      1. Are there hidden backdoors or hardcoded credentials?
   3. What are the most effective attack vectors against consumer networking equipment and how can users protect themselves?
   4. How susceptible are they to remote exploits and unauthorized access?
   5. IoT devices connected to routers introduce additional risk?
      1. Default or weak passwords and lack of encryption due to size
      2. Can be used to access router config
   6. Consumer behavior that impacts security of the networking device?
   7. How many people change their security settings from default?
   8. Supply chain/manufacture concerns
2. Device Routers, modems, IoT
   1. Outdated Models or ones with known security flaws
   2. Ensure compliance with security testing of device
   3. Proposal for the device
      1. TP-Link Archer AX21, Archer C50 V4, Archer AX3000, Archer AX5400, TP-Link TL-WR841N
         1. In 2024 it was investigated due to national security risk and cyberattacks from Chinese hacking groups
         2. Chinese manufacturer
      2. Netgear R7000 (nighthawk) CVE-2016-10001, hardcoded password
3. Technical - Research Tools
   1. Port scanners
      1. Nmap, Unicornscan, Masscan
   2. Web Interface Scanners
      1. Postman, Burpsuite,
   3. Firmware Analysis
      1. Extract – Binwalk, Firmadyne
         1. binwalk -e firmware.bin
      2. Sensitive file search
         1. grep -r “password” extracted\_firmware/
            1. Check in /etc/shadow, etc/password, config files
      3. Binaries – Reverse engineer
         1. IDA pro (tool), Ghidra
            1. Buffer overflows, command injections, backdoors
      4. Debugging/Emulation
         1. GDB, QEMU (Firmware emulation)
      5. Password Cracking
         1. Hashcat, John the Ripper, Volatility (memory forensics)
   4. Wireless
      1. Reaver – exploit vulnerabilities in wifi that use WPS
         1. reaver -I wlan0mon -b <BSSID> -vv
      2. Aircrack-ng
      3. RFExploit
   5. Exploit
      1. Manual
         1. Try default passwords, injection attacks, buffer overflow
         2. Use CVE database for model to test for those
      2. Tools
         1. Metasploit, routerSploit
   6. Mitigation/disclosure
      1. If found, contact vendor
   7. Suggest security improvements based on findings (pwds, updates, ports, etc)
      1. General security recommendations
         1. Firmware updates – a way to automate this instead of manual process?
         2. Default credentials
         3. Disable unused services
         4. Set secure wireless
         5. Segment of network for IoT and normal