Full Project Write-Up – Home Network Reconnaissance and Security Audit:

Introduction:

This project was designed to conduct an internal network reconnaissance and vulnerability analysis using a popular network port scanner Nmap. The objective of this project was to identify actively running devices on my home network, scan for open ports and exposed services, and evaluate each systems attack surface. While this was conducted in a home environment, this process mirrors what security analysts do when assessing internal networks for any sort of potential risk.

Tools & Setup:

- Operating System: Conducting this test involved executing scans from Kali Linux (running in UTM and on a 2020 MacBook Pro).

- Scanner: Nmap (Version 7.94) a popular open-source tool used for network discovery was used to conduct each scan.

- Target Network Range: The network range was given in CIDR (Classless Inter-Domain Routing) notation as 192.168.X.X/24.

- Scan Flags: During the scans, certain flags were utilized such as -A and -Pn. The flag -A is known as an aggressive scan, which collects information on OS detection, version detection, and script scanning. -Pn is used for skipping host discovery, and useful for devices that block ping.

Note: Screenshots of the terminal output for each scan are included in the project's main repository in pdf format along with a README file summarizing the project and findings.

Devices Scanned:

Device	Purpose	Services Found
2020 MacBook Pro	Main workstation	SSH, DNS, AirPlay
2023 Apple iPhone 15 Plus	Mobile device	iTunes sync (tcpwrapped)
2013 Original Xbox One	Gaming console	UPnP (Universal Plug and Play)
2017 HP Envy 7158	Wireless printer	HTTP(S), IPP, JetDirect
AT&T DSL Router	Internet gateway	DNSMasq, lighttpd admin

Device Findings:

2020 MacBook Pro:

- **Open Ports**: 22 (SSH), 53 (DNS), 5000 & 7000 (Airplay / RTSP).

- **Observations**:
    - SSH likely enabled for remote terminal use.
    - RTSP ports exposed due to AirPlay.
    - DNS port may indicate Bonjour/mDNS behavior.

- **Security Insight**: No critical risks, but these services should be disabled if unused.

2023 iPhone 15 Plus:

- **Open Port**: 62078

- **Service**: Lockdownd (used by iTunes/Finder for syncing)

- **Notes**: Nmap reported the service as 'tcpwrapped,' meaning it blocked deeper inspection which is typical for IOS devices.

- **Security Insight**: Very minimal exposure. This is a good example of a locked-down consumer device.

2013 Original Xbox One:

- **Open Port**: 2869
- **Service**: UPnP via Microsoft IIS httpd
- **OS Fingerprint**: Guessed as Windows 11 or Server 2008, makes sense given Xbox's Windows-based operating system.
- **Security Insight**: UPnP is not dangerous itself, but in enterprise environments it's often disabled due to abuse potential. No major risks identified here.

2017 HP ENVY Photo 7158:

- **Open Ports:** 80 (HTTP), 443 (HTTPS), 631 (IPP), 8080, 9100 (JetDirect)
- **Services:** Multiple nginx web interfaces, printing protocols, and raw job handling.
- **Security Insight:**
    - Port 9100 allows raw tcp print jobs with no sort of authentication. This is an old common vector for potential denial-of-service attacks.
    - Admin panel lacks authentication and uses a self-signed certificate.

AT&T DSL Router:

- **Open Ports:** 53 (DNSMasq), 80 (HTTP), 443 (HTTPS).
- **Filtered:** Port 111 (RPCBind) is blocked, which is a good sign.
- **Service Info:**
    - DNSMasq 2.89 handles internal name resolution.
    - Web admin panel accessible over both HTTP and HTTPS.
- **Security Insight:**
    - Self-signed certificate from Arris Group, this is expected but not secure for remote use.
    - Ensure remote management is disabled, and credentials are strong.

Summary of Risks:

Risk	Affected Devices	Explanation
Admin Panels Exposed	Printer, Router	Web logins accessible over LAN without rate limiting.
UPnP Running	Xbox One	Abused in network pivoting.
JetDirect Open (9100)	Printer	Unauthenticated printing.
Streaming Protocols Exposed	MacBook	AirPlay services open on LAN.

Recommendations:

- Disable unnecessary services (AirPlay, UPnP, JetDirect) where possible.
- Require authentication on printer web panels and admin pages.
- Disable remote management on router if not in use.
- Use HTTPS where available and replace self-signed certs if deploying externally.
- Keep firmware updated for router and printer.
- Place high-risk devices (e.g., smart printers) on a segmented VLAN.

FINAL NOTE:

- Even simple home networks can expose multiple services and management interfaces without the user realizing it.
- Default configurations on devices like printers and routers leave them discoverable and, in some cases, interactable.
- Basic internal enumeration can provide valuable insight into overall network posture, especially for IoT-heavy environments.
- Tools like Nmap are not just for offensive security, they're essential in risk assessment, system hardening, and ongoing monitoring.