Nmap Scan Results

Linux

IMAGE REMOVED FOR SECURITY

FreeBSD

IMAGE REMOVED FOR SECURITY

macOS

IMAGE REMOVED FOR SECURITY

Windows

IMAGE REMOVED FOR SECURITY

Services Identified

Linux

- Port 22 (SSH): OpenSSH 9.7 running on Linux with protocol 2.0

FreeBSD

- Port 22 (SSH): OpenSSH 9.7 running on Linux with protocol 2.0

macOS

- Port 5000: AirTunes RTSP version 775.3.1
- Port 7000: AirTunes RTSP version 775.3.1

Windows

- Port 22 (SSH): OpenSSH for Windows 8.6 with protocol 2.0
- Port 135 (MSRPC): Microsoft Windows RPC service
- Port 139 (NetBIOS-SSN): Microsoft Windows NetBIOS session service
- Port 445 (Microsoft-DS): Microsoft Windows SMB service
- Port 2179 (VMRDP): Virtual Machine Remote Desktop Protocol (VMRDP)

Metasploit has not explicitly shown any vulnerabilities. However, there are some potential vulnerabilities that could exist.

Recommendations

Linux

I. Potential Risks:
   a. Brute-force attacks: It could be vulnerable to brute-force password attacks
   b. Outdated versions: OpenSSH 9.7 is a relatively recent patch, but it’s important to continuously stay updated with the latest version.

II. Recommendations:
   a. Enable key-based authentication: Disable password-based login and require SSH keys
   b. Rate-limiting: Ensure to limit login attempts
   c. Regular updates: Keep OpenSSH up to date with security patches

FreeBSD

I. Potential Risks:
   a. Brute-force attacks: It could be vulnerable to brute-force password attacks
   b. Outdated versions: OpenSSH 9.5 is a relatively recent patch, but it’s important to continuously stay updated with the latest version.

II. Recommendations:
   a. Enable key-based authentication: Disable password-based login and require SSH keys
   b. Rate-limiting: Ensure to limit login attempts
   c. Regular updates: Keep OpenSSH up to date with security patches

macOS

I. Potential Risks:
   a. Denial of Service (DoS): RTSP services might be vulnerable to DOS attacks
   b. Unauthorized Access: Without proper access control, the RTSP stream could be accessed by unauthorized users.

II. Recommendations:
   a. Network Segmentation: Restrict RTSP services to trusted networks
   b. Encryption: user secure protocols for RTSP streaming
   c. Regular updates: Keep AirTunes up to date with security patches

Windows

I. Potential Risks:
   a. Remote code execution: It could be exploited through unpatched services
   b. Ransomware attacks: It could be conducted via SMB if unpatched
   c. Unauthorized RDP access: It could be conducted if weak passwords or outdated versions

II. Recommendations:
   a. Disable unnecessary services: Disable unnecessary services to minimize potential vulnerabilities as much as possible
   b. Regular updates: Ensure all Windows services, especially SMB and RPC, are up to date
   c. Strong RDP settings: Restrict RDP access with network-level authentication and strong passwords
   d. Firewalls: Block external access to SMB and RDP