Activity Report: Nmap Vulnerability Scan on 192.168.1.148

Date and Time: April 22, 2025, 17:51 - 18:01 UTC

User: root@parrot

Location: /home/user

Tool Used: Nmap 7.94SVN

Target: 192.168.1.148

Command Executed: sudo nmap -sV --script=vuln 192.168.1.148

Overview

The user performed a vulnerability scan on the IP address 192.168.1.148 using Nmap with the -sV (service version detection) and --script=vuln (vulnerability scanning) options. The scan was initiated at 17:51 UTC and completed multiple iterations, with the final results captured at 18:01 UTC. The scan identified open ports, services, and potential vulnerabilities on the target host.

Scan Details

- **Target Host:** 192.168.1.148 (1 host up)
- **Scan Duration:**
  - Initial scan: 0.21 seconds (17:51 UTC)
  - Subsequent scans: 0.41 seconds (17:52 UTC), 1.68 seconds (18:00 UTC), 1.68 seconds (18:01 UTC)
- **Ports Scanned:** 999 TCP ports (closed/reset)
- **Open Ports and Services:**
  - **Port 53/tcp:** Open, running dnsmasq 2.90

Vulnerabilities Identified

The Nmap vulnerability script (--script=vuln) flagged several potential vulnerabilities on the target host. Below is a summary of the findings:

1. **DNS Service (dnsmasq 2.90 on Port 53/tcp):**
   - No specific vulnerabilities were directly tied to the DNS service in the output.
2. **General Vulnerabilities (not tied to a specific port):**
   - **CVE-2017-14494:** Severity 5.9 (Medium) - Link
   - **CVE-96622:** Severity 5.0 (Medium) - Link
   - **EXPLOITPACK:** C0456C7DF1625677A211CB799B879F9A - Link
   - **CVE-2013-0198:** Severity 5.0 (Medium) - Link

- **CVE-2012-3411:** Severity 5.0 (Medium) - Link
- **1337DAY-ID-28726:** Severity 5.0 (Medium) - Link
- **SSV:96621:** Severity 4.3 (Medium) - Link
- **SSV:12173:** Severity 4.3 (Medium) - Link
- **EXPLOITPACK: 22D470FAF79A3DB8978CC3F8766C759:** Severity 4.3 (Medium) - Link
- **CVE-2009-2958:** Severity 4.3 (Medium) - Link
- **CB73EF2D-AB5B-5110-A374-4A5ADE9AC91A:** Severity 4.0 (Medium) - Link
- **1337DAY-ID-28725:** Severity 4.3 (Medium) - Link
- **CVE-2021-3448:** Severity 4.0 (Medium) - Link
- **CVE-2020-25686:** Severity 3.7 (Low) - Link
- **CVE-2020-25685:** Severity 3.7 (Low) - Link
- **CVE-2020-25684:** Severity 3.7 (Low) - Link
- **CVE-2019-14834:** Severity 3.7 (Low) - Link
- **PACKETSTORM:144480:** Severity 0.0 (Informational) - Link
- **PACKETSTORM:144479:** Severity 0.0 (Informational) - Link
- **PACKETSTORM:144473:** Severity 0.0 (Informational) - Link
- **PACKETSTORM:144471:** Severity 0.0 (Informational) - Link
- **PACKETSTORM:144468:** Severity 0.0 (Informational) - Link
- **PACKETSTORM:144462:** Severity 0.0 (Informational) - Link
- **1337DAY-ID-6998:** Severity 0.0 (Informational) - Link

3. **Additional Exploits Identified in Later Scans:**
   - **2C119FFA-ECE0-5E14-4AA4-354A2C38071A:** Severity 10.0 (Critical) - Link
   - **EDB-ID:42943:** Severity 9.8 (Critical) - Link
   - **EDB-ID:42942:** Severity 9.8 (Critical) - Link
   - **EDB-ID:42941:** Severity 9.8 (Critical) - Link
   - **CVE-2017-14493:** Severity 9.8 (Critical) - Link
   - **CVE-2017-14492:** Severity 9.8 (Critical) - Link
   - **CVE-2017-14491:** Severity 9.8 (Critical) - Link
   - **CVE-2020-25682:** Severity 8.1 (High) - Link
   - **CVE-2020-25681:** Severity 8.1 (High) - Link
   - **SSV:96623:** Severity 7.8 (High) - Link
   - **EXPLOITPACK:708148DF89AFEA44750A98B84E292A6B9:** Severity 7.8 (High) - Link
   - **EXPLOITPACK:E661AE0D6AF5BCC1565D1CBOF9878E40B:** Severity 7.5 (High) - Link
   - **EXPLOITPACK:95340EB39AF331E01096F2B1CF71DE2:** Severity 7.5 (High) - Link
   - **EXPLOITPACK:572F56450883EECA41007EF1833848B:** Severity 7.5 (High) - Link
   - **CVE-2023-50387:** Severity 7.5 (High) - Link
   - **CVE-2023-49441:** Severity 7.5 (High) - Link
   - **CVE-2023-29450:** Severity 7.5 (High) - Link
   - **CVE-2022-0934:** Severity 7.5 (High) - Link
   - **CVE-2019-14513:** Severity 7.5 (High) - Link
   - **CVE-2017-15107:** Severity 7.5 (High) - Link

- **CVE-2017-13704:** Severity 7.5 (High) - Link
- **CVE-2015-8899:** Severity 7.5 (High) - Link
- **CVE-2005-0877:** Severity 7.5 (High) - Link
- **CE8366BE-F17D-552A-B1B4-C2DBD31482C0:** Severity 7.5 (High) - Link
- **BB688F8F-CEE2-5DD1-8561-8F76501DE2D4:** Severity 7.5 (High) - Link
- **790688EF-A572-5A8A-88D0-177524BDAAFE:** Severity 7.5 (High) - Link
- **5EFDF373-FBD1-5C09-A612-00ADBFE574CF:** Severity 7.5 (High) - Link
- **1337DAY-ID-28724:** Severity 7.5 (High) - Link
- **1337DAY-ID-28723:** Severity 7.5 (High) - Link
- **1337DAY-ID-28720:** Severity 7.5 (High) - Link

Additional Observations

- **Pre-Scan Scripts:** The user ran scripts like broadcast-avahi-dos to discover hosts, which identified 224.0.0.251 as a potential target for an Avahi packet DoS (CVE-2011-1002).
- **Host Status:** The target host (192.168.1.148) was up with minimal latency (0.000001s).
- **Service Detection:** Confirmed the presence of dnsmasq 2.90 on port 53/tcp.
- **Nmap Warning:** At 17:51 UTC, Nmap issued a warning: "No targets were specified, so 0 hosts scanned." This suggests an initial misconfiguration or lack of target specification before the correct command was executed.

Recommendations

1. **Patch Management:** Address the identified vulnerabilities, especially the critical ones (e.g., CVE-2017-14493 with a severity of 9.8). Update dnsmasq to the latest version to mitigate known exploits.
2. **Further Investigation:** Investigate the high-severity vulnerabilities (e.g., 2C119FFA-ECE0-5E14-4AA4-354A2C38071A, severity 10.0) for potential exploitation risks.
3. **Network Hardening:** Close unnecessary ports and services to reduce the attack surface.
4. **Reporting:** As advised by Nmap, report any incorrect results to https://nmap.org/submit/.

Conclusion

The scan revealed that the target host (192.168.1.148) is running a DNS service (dnsmasq 2.90) on port 53/tcp and is potentially vulnerable to multiple exploits, ranging from low to critical severity. Immediate action is recommended to address the critical and high-severity vulnerabilities to prevent potential exploitation.

End of Report