

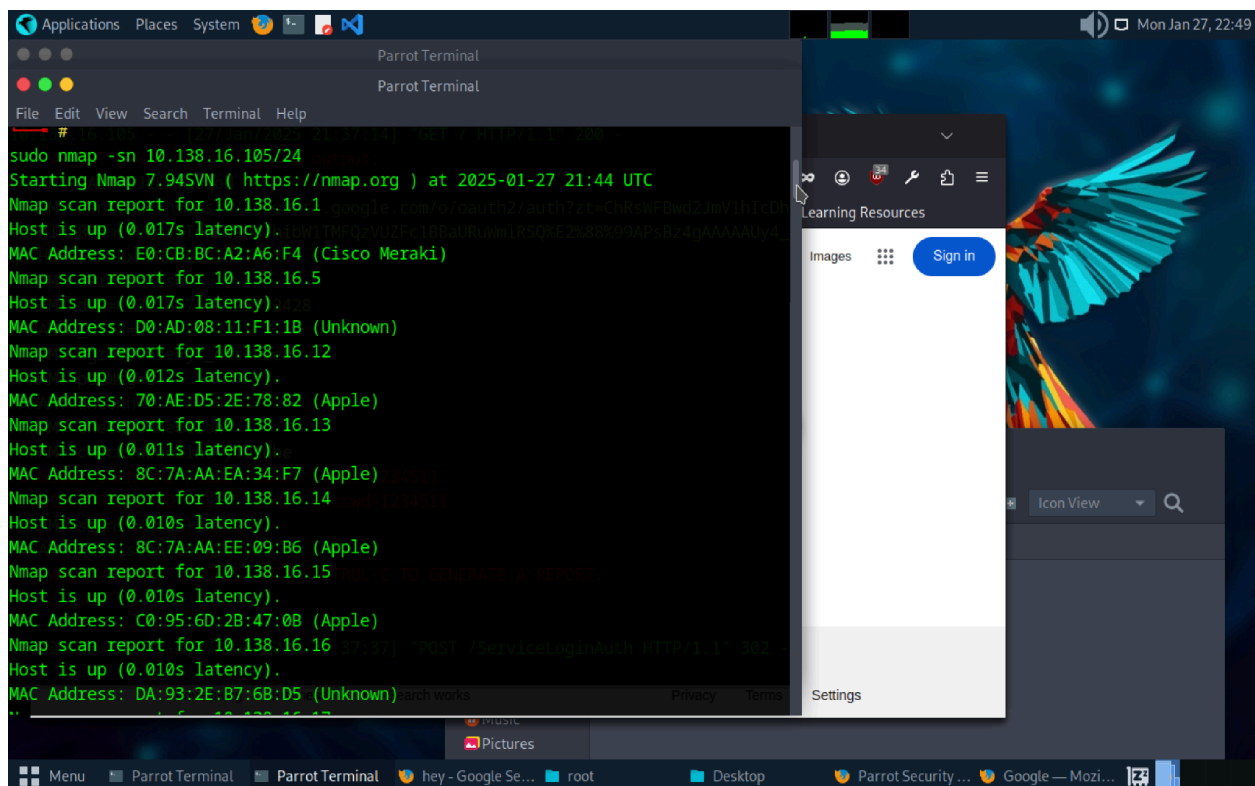
1. Introduction

This report presents an analysis of vulnerabilities identified through a network vulnerability scan. The objective is to assess risks, prioritize two critical vulnerabilities, and provide recommendations for mitigation and ongoing risk monitoring.

2. Identified Risks from Vulnerability Scan

The network vulnerability scan identified multiple risks. The two most critical vulnerabilities are:

2.1 Critical Risk #1: Unfiltered Open Ports (TCP/68, DHCP Service Exposure)

A screenshot of a Parrot OS desktop environment. In the foreground, a Parrot Terminal window displays the output of an Nmap scan for the 10.138.16.0/24 network. The scan results show several hosts are up, including 10.138.16.1 (Cisco Meraki), 10.138.16.5 (Unknown), 10.138.16.12 (Apple), 10.138.16.13 (Apple), 10.138.16.14 (Apple), 10.138.16.15 (Apple), and 10.138.16.16 (Unknown). The terminal also shows the command 'sudo nmap -sn 10.138.16.0/24'. In the background, a web browser window is open, displaying a 'Learning Resources' page with a 'Sign in' button. The desktop background features a colorful parrot illustration. The system clock in the top right corner indicates 'Mon Jan 27, 22:49'.

Risk Description:

- The scan detected an exposed DHCP port (TCP/68), which could allow an attacker to exploit unauthorized DHCP services.
- This vulnerability can lead to DHCP spoofing attacks, where a rogue DHCP server issues incorrect IP configurations, leading to potential man-in-the-middle (MITM) attacks.

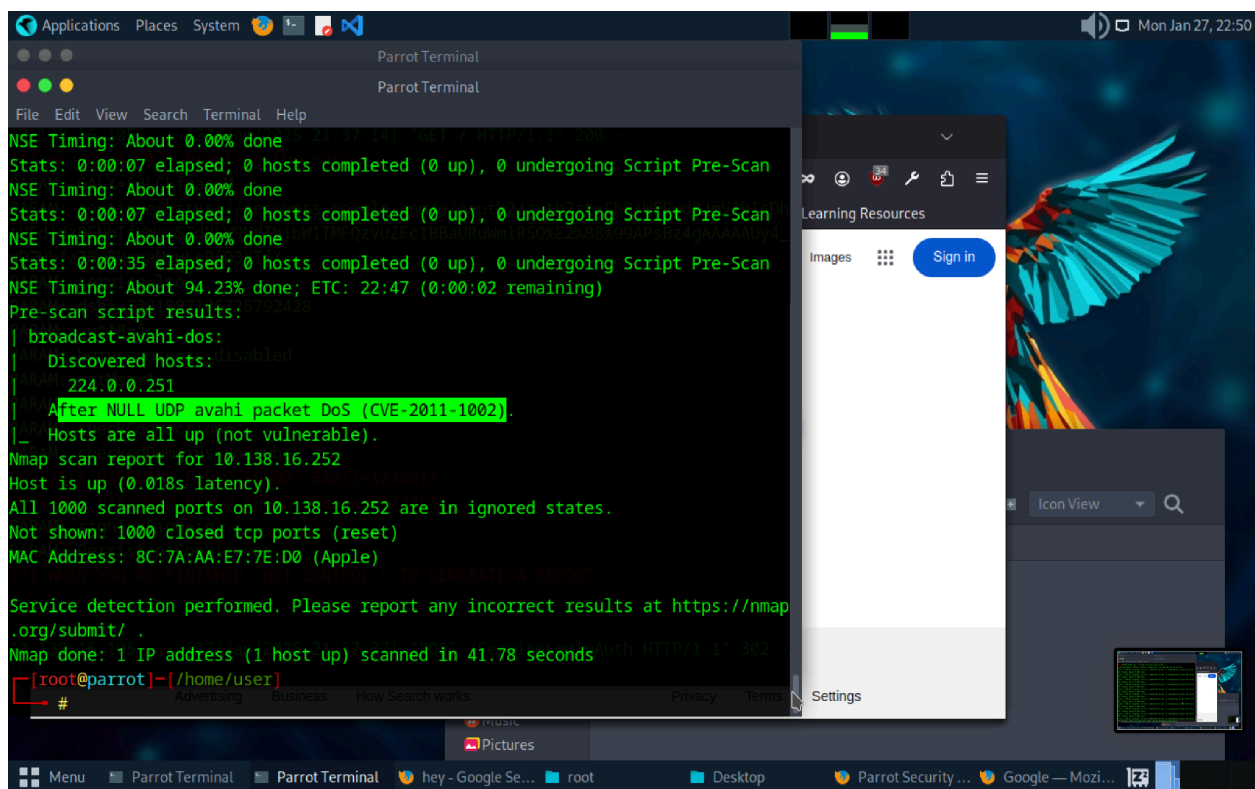
Treatment Recommendations:

- Restrict DHCP server access using firewall rules to limit exposure.
- Implement DHCP snooping to detect and prevent rogue DHCP servers.
- Monitor network traffic for unauthorized DHCP responses.

Mitigation Steps:

1. Configure firewall rules to block unauthorized access to DHCP ports.
2. Enable DHCP snooping on network switches.
3. Regularly audit DHCP server configurations.

2.2 Critical Risk #2: CVE-2011-1002 (Avahi NULL UDP Packet DoS Vulnerability)



```

NSE Timing: About 0.00% done
Stats: 0:00:07 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 0.00% done
Stats: 0:00:07 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 0.00% done
Stats: 0:00:35 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 94.23% done; ETC: 22:47 (0:00:02 remaining)
Pre-scan script results:
| broadcast-avahi-dos:
|_ Discovered hosts:
|_ 224.0.0.251
|_ After NULL UDP avahi packet DoS (CVE-2011-1002).
|_ Hosts are all up (not vulnerable).
Nmap scan report for 10.138.16.252
Host is up (0.018s latency).
All 1000 scanned ports on 10.138.16.252 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 8C:7A:AA:E7:7E:D0 (Apple)
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 41.78 seconds
[root@parrot]-(/home/user)
#
  
```

Risk Description:

- The scan detected the presence of the Avahi daemon, which is vulnerable to a NULL UDP packet-based Denial of Service (DoS) attack.
- Attackers could exploit this vulnerability to flood the network with malformed packets, causing service disruptions.

Treatment Recommendations:

- Update Avahi to the latest patched version.
- Disable Avahi if it is not required for the network.

- Implement network segmentation to limit the impact of potential exploits.

Mitigation Steps:

1. Apply vendor patches for Avahi.
2. Disable Avahi on systems where it is unnecessary.
3. Restrict UDP traffic on the vulnerable ports using firewall rules.

3. Risk Monitoring Procedure

Objective: Implement a structured monitoring process to track identified vulnerabilities and prevent future exploits.

Procedure for Risk Tracking

1. **Logging and Documentation:**
 - Maintain a risk register documenting identified vulnerabilities, their impact, and mitigation status.
 - Use security information and event management (SIEM) tools to log suspicious activities related to identified vulnerabilities.
2. **Regular Vulnerability Scans:**
 - Conduct weekly automated vulnerability scans to track changes in risk exposure.
 - Compare new scan results with previous findings to assess risk trends.
3. **Incident Response Planning:**
 - Define response protocols for detected exploits or repeated vulnerability detections.
 - Assign responsibilities for patching and remediation to designated IT security personnel.
4. **Network Traffic Analysis:**
 - Use intrusion detection systems (IDS) to monitor traffic for exploitation attempts.
 - Set up alerts for unusual activities on high-risk ports.

4. Conclusion

The vulnerability scan revealed critical security risks that could lead to unauthorized access and service disruption. By implementing the recommended mitigation steps and the outlined risk monitoring procedure, the organization can reduce exposure to threats and improve network security.

5. Justification of Decisions

- **Prioritization of Risks:** The identified vulnerabilities were categorized as critical based on their exploitability and potential impact on network operations.

- **Mitigation Approaches:** Solutions were chosen based on best security practices, feasibility of implementation, and effectiveness in reducing risk.
- **Risk Monitoring:** A structured monitoring approach ensures continuous assessment and proactive threat response.