**Network Discovery and Mapping Report**

Date: 13 / 07 / 2024

Prepared by: Kushagra Pandurang Pitre

**1. Introduction**

The purpose of this report is to provide a comprehensive analysis of the organization's network through the processes of network discovery and mapping. Network discovery is the identification of all devices and assets connected to the network, while the network map creates a visual representation of their connections and communication channels.

**2. Network Discovery and Mapping**

2.1 Tools Used

Nmap: For network scanning and host discovery.

Zenmap: For visual network mapping.

Netdiscover: For discovering live hosts.

OpenVAS: For vulnerability assessment.

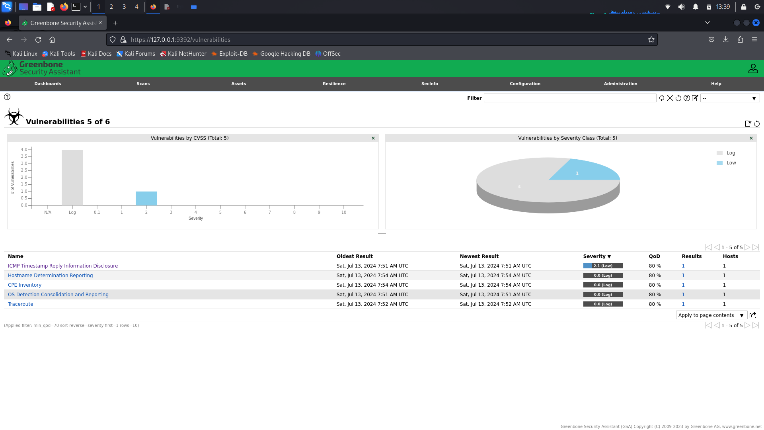
2.2 Methodology

Initial Scan: Used Nmap to identify live hosts and open ports. A screenshot of a computer

Description automatically generated

Detailed Scan: Conducted OS and service version detection using Nmap.

Network Mapping: Created a visual representation of the network using Zenmap.

Vulnerability Assessment: Performed using OpenVAS.

.

2.3 Network Topology Map

The network topology map generated from the scans is shown below:

A diagram of a network

Description automatically generated

**3. Vulnerability Assessment Results**

3.1 Summary of Findings

Total Hosts Scanned: 4

Total Vulnerabilities Identified: 5

Critical Vulnerabilities: None

High Vulnerabilities: None

Medium Vulnerabilities: None

Low Vulnerabilities: 1

3.2 Detailed Vulnerability Report

Host: 192.168.1.2

Open Ports: 53/tcp (domain) ,80/tcp (http),443/tcp (https),5555/tcp (freeciv)

Operating System: Linux

Vulnerabilities:

CVE-1999-0524: low – The remote host responded to an ICMP timestamp request

Host: 192.168.1.2

Open Ports: 65000/tcp filtered unk

Operating System: linux kernel

Vulnerabilities:

Insight :- The Timestamp reply is an ICMP message which replies to a Timestamp message , It consist of the originating timestamp sent by the sender of the Timestamp as well as receive timestamp and a transmit timestamp

4. **Risk Assessments**

4.1 Risk Assessment Criteria

Likelihood of Exploitation: High

Impact on Network: High

4.2 Risk Analysis

1. ICMP Echo Request (Ping) Flooding

• Risk Level: High

• Justification: There is a high likelihood and severity associated with this attack, as it has the potential to cause significant disruptions to network services.

2. ICMP Redirect Attack

• Risk Level: High

• Justification: While the likelihood of this attack is medium, the severity is high due to the serious security breaches and data interception that could occur.

3. ICMP Unreachable Attack

• Risk Level: Medium

• Justification: This attack poses a medium level of risk in terms of likelihood and severity, as it has the potential to disrupt services.

4. ICMP Timestamp Request Attack

• Risk Level: Low to Medium

• Justification: Although the likelihood of this attack is low, the severity is medium because it could aid in further attacks by leaking information.

5. ICMP Fragmentation Attack

• Risk Level: High

• Justification: With a medium likelihood and high severity, this attack has the potential to bypass security measures and facilitate data exfiltration.

**Impact**: This information could theoretically be use to exploit weak time – based random number generators in other services

Description: If an attacker can predict or know the exact time when the RNG was seeded, they can replicate the random number generation process, leading to the prediction of supposedly random values.

5. **Recommendations**

1. Cryptographically Secure Random Number Generators (CSPRNGs) are specifically designed to offer a high level of entropy and unpredictability, making them suitable for applications that require a high level of security.

2. It is important to seed RNGs with high-entropy sources to ensure that the output is unpredictable. Using low entropy seeds can make the output of the RNG predictable.

3. Regularly reseeding RNGs is essential to maintain their unpredictability over time. This can be achieved by scheduling regular reseeding intervals using diverse and high-entropy sources.

4. It is crucial to manage entropy pools to ensure a continuous supply of high-quality entropy. This can be done by using system utilities to feed the entropy pool and monitoring its health to ensure it is adequately replenished.

5. To minimize the risk of vulnerabilities due to poor implementation, it is advisable to use well-reviewed and widely accepted RNG libraries. This can be achieved by choosing RNG libraries from reputable sources and keeping them updated to benefit from security patches and improvements.

6**. Conclusion**

**Network** discovery and mapping activities revealed several critical and **critical** vulnerabilities that require immediate attention. By addressing these vulnerabilities and implementing the recommended security measures, the security posture of the network can be significantly improved.