Name : Patel Dhruv Nirmalkumar
Email : dhruvpatel.00700@gmail.com
Phone : 9426176903
Task : 9

Network Vulnerability Scanning Report

Introduction

This report details the findings of a network reconnaissance and vulnerability scan performed on the local sandbox environment. The primary objective was to identify active hosts, open ports, running services, and the operating system of the target hosts, following the provided **Hints / Mini Guide**.

The scan identified two active hosts: the local machine (169.254.0.21) and the network gateway (169.254.0.22). The local machine was found to be running **Ubuntu 22.04.5 LTS** with several services exposed, most notably **SSH (Port 22)** and **VNC (Port 5900)**. The gateway system showed all commonly scanned ports as closed.

The exposed services on the local host represent potential attack vectors if not properly secured. Overall, the activity demonstrates the successful application of basic network reconnaissance and risk analysis skills.

Tools Used: Nmap

Scan Local Network

The reconnaissance process began by identifying the local network range.

- **Network Range:** 169.254.0.20/30
- **Tool Used:** Nmap
- **Scan Type:** Ping scan (-sn)
- **Purpose:** Discover active hosts on the network

Active Hosts Identified

IP Address	Status	Description
169.254.0.21	Up	Local sandbox host (analyzed further via 127.0.0.1)
169.254.0.22	Up	Network gateway / router

Identify Open Ports

Gateway (169.254.0.22)

- **Tool Used:** Masscan (ports 1–65535)
- **Result:** Inconclusive
- **Follow-up:** Nmap fast scan (-F)

Outcome:

- All 100 common ports were **closed**

Interpretation:

- The gateway is either heavily filtered or intentionally not exposing services.

Local Host (127.0.0.1)

- **Tool Used:** Nmap
- **Purpose:** Identify open ports on the local system

Port	Protocol	Service	Status
22	TCP	SSH	Open
5900	TCP	VNC	Open

Detect Services

Port	Protocol	Service / Program	Description
22	TCP	sshd	Secure Shell remote access
5900	TCP	x11vnc	Remote desktop access
8329	TCP	node	Node.js application
8330	TCP	start_server	Internal server process
8340	TCP	upgrade	Internal upgrade service
9222	TCP	chromium-browse	Browser debugging port
9330	TCP	start_server	Internal server process

Identify Operating System

The operating system was identified using system commands.

- **Operating System:** Ubuntu 22.04.5 LTS (Jammy Jellyfish)
- **Kernel Version:** Linux 6.1.102

Analyze Vulnerabilities

- An Nmap vulnerability script scan was attempted.
- The scan did not complete successfully.
- Vulnerability analysis was based on exposed services and common attack risks.

Save Scan Results

- Scan outputs were manually reviewed and documented.
- Results were structured into tables for clarity and reporting.

Interpret Risks

Service	Risk Level	Risk Description
SSH (Port 22)	Medium	Vulnerable to brute-force attacks if weak credentials are used
VNC (Port 5900)	Medium	Often unencrypted, allowing possible interception
Internal Services	Low	Bound to local interfaces and not externally accessible

Document Findings and Mitigation

Service	Recommended Mitigation
SSH	Use key-based authentication, strong passwords, disable root login
VNC	Use SSH tunneling and strong authentication
Internal Services	Ensure services remain bound to localhost only