Assignment No: 7 Vulnerability Analysis using Nessus

Title: Conduct a vulnerability scan on a virtual machine using Nessus. Identify vulnerabilities and suggest fixes.

Objective: To learn the process of conducting an automated vulnerability assessment using the Nessus tool, analyze the output, and propose remediation strategies for identified security flaws.

Tool Used: Tenable Nessus Essentials

Target System (VM): IP Address: 10.25.28.229 (Based on scan report msl2_9tiyf3.pdf)

1. Introduction

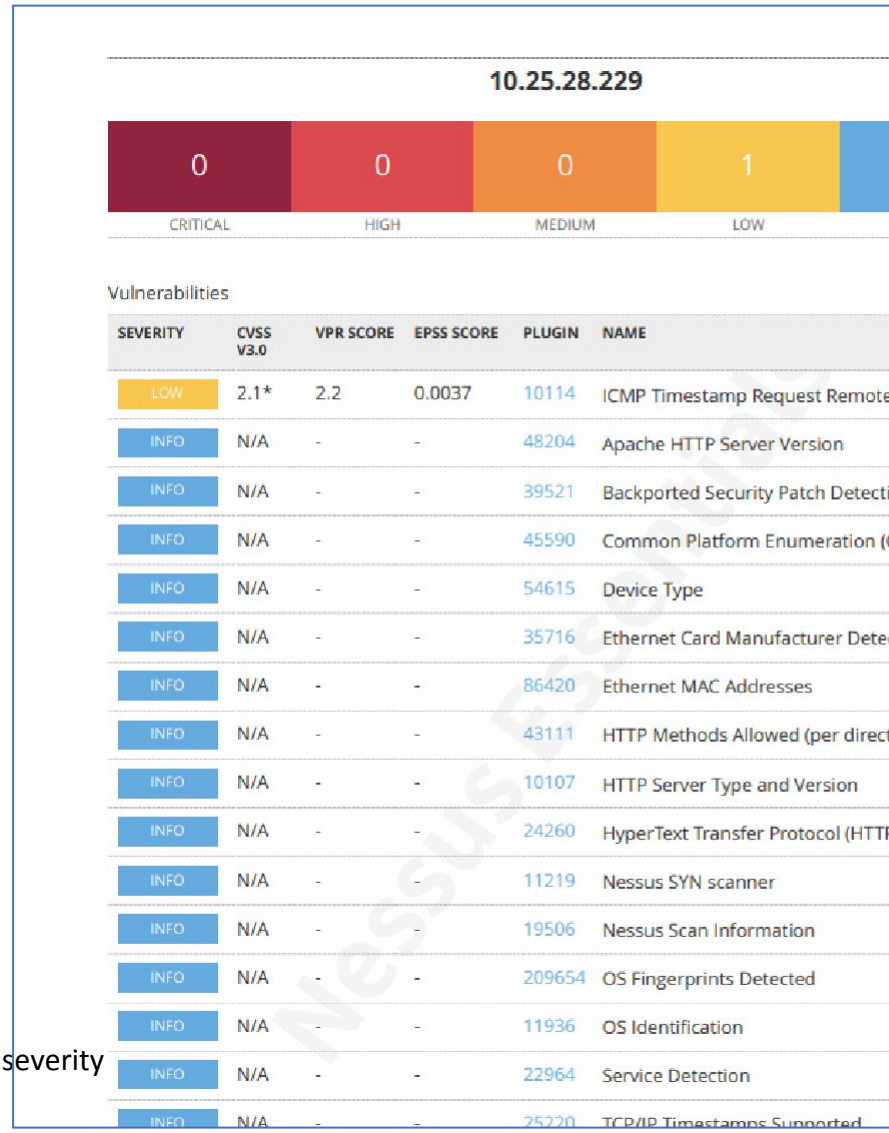
Vulnerability scanning is a crucial component of information security, involving automated tools to proactively identify security weaknesses in network assets. This practical focused on using **Tenable Nessus**, a widely recognized vulnerability scanner, to assess the security posture of a target Virtual Machine (VM). The process involved configuring a scan, executing it against the target VM, analyzing the resulting report, and prioritizing the identified risks.

2. Theory and Methodology

Nessus Workflow

1. **Installation and Setup:** Nessus was installed and configured on the attacking machine.
2. **Scan Configuration:** A new basic network scan was created, targeting the VM's IP address (10.25.28.229).
3. **Execution:** The scan was run, which performed various checks, port scans, and service enumerations.
4. **Reporting:** Nessus generated a detailed report summarizing all discovered findings.

Types of Findings



10.25.28.229

0	0	0	1
CRITICAL	HIGH	MEDIUM	LOW

Vulnerabilities

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
LOW	2.1*	2.2	0.0037	10114	ICMP Timestamp Request Remote
INFO	N/A	-	-	48204	Apache HTTP Server Version
INFO	N/A	-	-	39521	Backported Security Patch Detecti
INFO	N/A	-	-	45590	Common Platform Enumeration (C
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Dete
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	43111	HTTP Methods Allowed (per direct
INFO	N/A	-	-	10107	HTTP Server Type and Version
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	209654	OS Fingerprints Detected
INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	22964	Service Detection
INFO	N/A	-	-	25220	TCP/IP Timestamps Supported

The results are typically categorized by severity (Info).

Vulnerability: A weakness that an attacker can exploit to gain unauthorized access or cause harm.

Informational (Info): Data points that do not pose an immediate risk but provide valuable intelligence to an attacker (e.g., OS version, running services).

3. Scan Results Analysis

The scan report for the target VM (10.25.28.229) identified a total of **18 findings**.

Vulnerability Summary

Severity Level	Count	Status
CRITICAL	0	None found
HIGH	0	None found
MEDIUM	0	None found
LOW	1	Vulnerability Identified
INFO	17	Informational findings identified
Total Findings	**18**	—

Detailed Findings

A. Key Vulnerability (LOW Severity)

The scan successfully identified one specific security issue:

Plugin ID	Plugin Name	Severity	CVSS v2.0 Score	Suggested Fix Priority
10114	**ICMP Timestamp Request Remote Date Disclosure**	LOW	2.1	Moderate

Description of Vulnerability: The target system responds to ICMP Timestamp Request packets. An attacker can use this feature to determine the exact date and time of the system, which can aid in other attacks that rely on time synchronization or predict system maintenance windows. This is considered an information leak.

B. Key Informational Findings

The majority of the findings (17) were informational, providing enumeration details:

- **Service & Version Enumeration:** Apache HTTP Server Version, HTTP Server Type and Version. (This allows an attacker to search for known vulnerabilities specific to that version).
- **Protocol Information:** HTTP Methods Allowed (per directory), HyperText Transfer Protocol (HTTP) Information.
- **Host Data:** OS Identification, Ethernet MAC Addresses, Device Type.

4. Suggested Fixes and Remediation

Remediation steps must address both the low-severity vulnerability and the informational leaks to improve the overall security posture of the VM.

A. Fix for LOW Vulnerability (ICMP Timestamp Request)

Vulnerability	Remediation Strategy	Implementation Steps
ICMP Timestamp Request Remote Date Disclosure (Plugin ID 10114)	**Disable ICMP Timestamp Responses.**	Configure the operating system's firewall (e.g., iptables on Linux or Windows Firewall) to explicitly drop all incoming ICMP messages of type 13 (Timestamp Request). This prevents the system from disclosing its internal clock time to external hosts.

B. Fixes for Informational Leaks (Hardening)

Finding Category	Remediation Strategy	Implementation Steps
Service Version Disclosure	Suppress Banner Information	Modify httpd.conf for Apache: set ServerSignature Off and ServerTokens Prod to prevent version leakage in headers and error pages.
Unnecessary Services / Ports	Disable or Filter Unused Ports/Protocols	Review detected services. Disable unused ones (e.g., mDNS Detection) or apply strict firewall rules to block external access to their ports.

General Patching	Establish a Patch Management Routine	Regularly update OS and applications to patch zero-day or newly disclosed vulnerabilities, reducing future detection in Nessus scans.

5. Conclusion

The Nessus scan showed no critical issues, but one low-severity vulnerability and several informational findings. By disabling ICMP timestamp responses and hiding server version details, the system can be better protected from attackersand reconnaissance attempts. Basic hardening steps will improve overall security.