Nessus Vulnerability Assessment

Prepared By:
Kazim Ali Obad

Supervisor:
Anmar Mohammed

Table of Contents

Scenario Description

Your security operations team has been tasked with performing a **basic vulnerability assessment** on a newly discovered Linux server within the internal network. The objective of this assessment is to evaluate the server's exposure to security threats and to identify obvious security weaknesses. The assessment focuses on understanding vulnerability scan results rather than exploiting any weaknesses.

Objectives

The primary objectives of this assessment are to:

- Identify running services on the target system
- Perform a basic vulnerability scan using Nessus
- Understand vulnerability severity levels
- Explain why certain vulnerabilities pose significant security risks

Rules and Constraints

To ensure ethical and academic compliance, the following rules must be followed:

- No exploitation of any identified vulnerabilities
- Nessus must be the only tool used for scanning
- The assessment must focus on analysis and understanding of scan results, not on attacking the system

Student Tasks

Students are required to complete the following tasks:

1. Configure a basic Nessus vulnerability scan against the target system
2. Execute the scan and monitor its progress until completion
3. Review and analyze the discovered vulnerabilities
4. Categorize findings by severity level (Critical, High, Medium, Low)
5. Select and analyze the top five most important vulnerabilities

1. Introduction

This assessment aims to perform a vulnerability assessment of Linux server within an internal network. The purpose of the assessment is to identify exposed services, detect known vulnerabilities, and evaluate the security of the system using Nessus software.

The target system for this assessment is Metasploitable , a Linux virtual machine commonly used for security training and testing.

2. Methodology

In this assessment we will follow a standard vulnerability management practices:

1. Identification of the target system and its network address
2. Configuration of a Basic Network Scan using Nessus
3. Execution of the vulnerability scan and monitoring of progress
4. Review and analysis of discovered vulnerabilities
5. Classification of findings based on severity levels

3. Target System

The target system for this assessment is Metasploitable a Linux virtual machine operating within a private internal network.

Using standard system identification methods, the target was found to have an IPv4 address of: 192.168.100.42

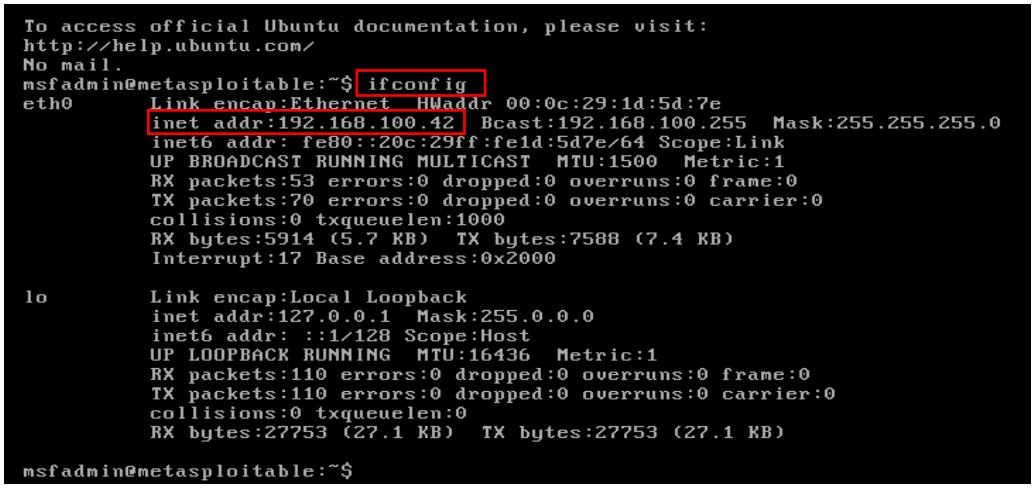

Figure (1) shows the ipv4 address of the target machine

This IP address was used as the target for the Nessus vulnerability scan.

4. Scan Configuration (Nessus)

The Basic Network Scan allows Nessus to:

- Discover open ports and running services on the target system
- Identify known vulnerabilities by matching discovered services with Nessus plugin signatures
- Categorize vulnerabilities based on severity levels (Critical, High, Medium, and Low)

During the scan configuration, the following parameters were defined:

- Scan Type: Basic Network Scan
- Scan Name: Test
- Target: 192.168.100.42
- Scan Settings: left on default

The vulnerability scan was configured using the Basic Network Scan in Nessus.

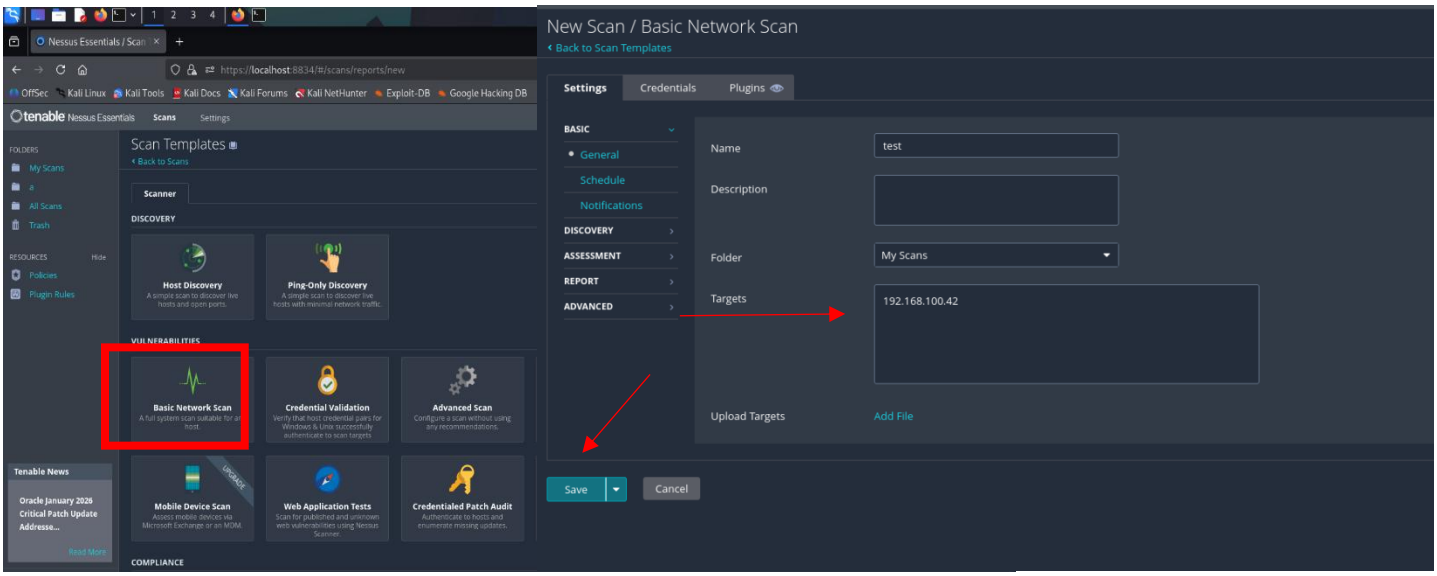

Figure (2) Nessus scan configuration

5.Scan Results and Vulnerability Analysis

After the completion of the Nessus Basic Network Scan, the results were reviewed to identify discovered vulnerabilities and assess their severity.

The scan results indicate that the Metasploitable system contains vulnerabilities across all severity levels, including Critical, High, Medium, Low, and Informational findings.

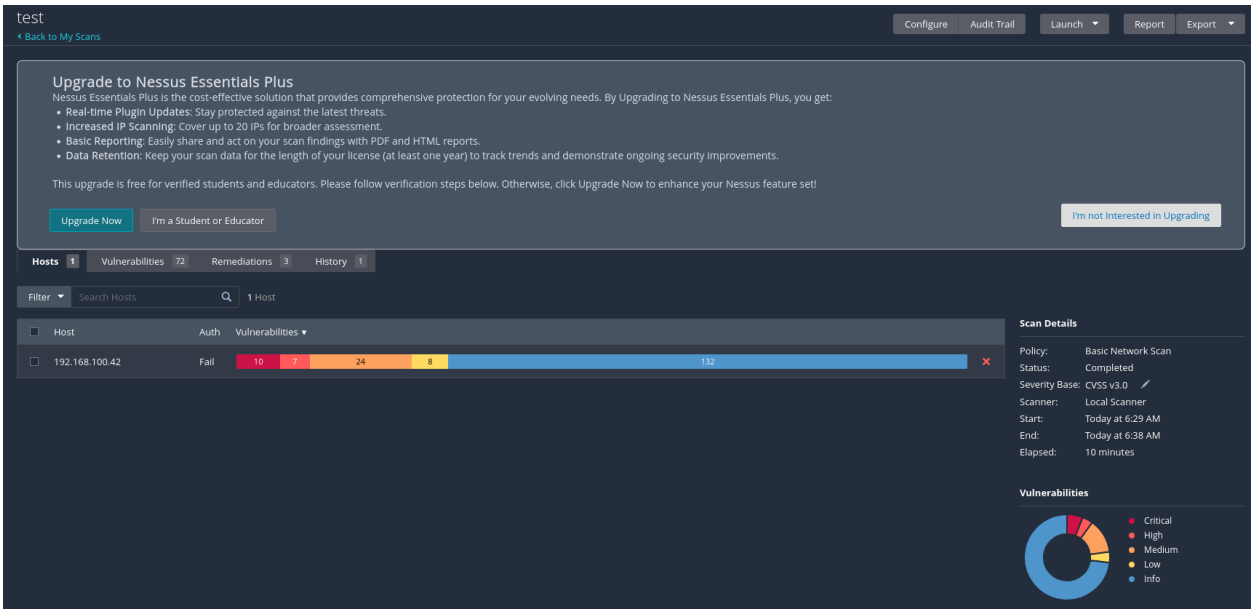

Figure (3) shows the vulnerability summary generated by Nessus after scan completion.

6.Vulnerability Severity Levels

Nessus categorizes vulnerabilities based on the CVSS v3.0 scoring system, which helps prioritize risks according to their potential impact. The discovered vulnerabilities were categorized into the following severity levels:

Severity Level	*Description*	*Number of Findings*
Critical	Vulnerabilities that may lead to full system compromise	10
High	Vulnerabilities that can allow unauthorized access or privilege escalation	7
Medium	Vulnerabilities that may assist attackers or weaken system defenses	24
Low	Minor misconfigurations or low-impact security weaknesses	8
Informational	Informational findings that do not pose an immediate security risk	132

TABLE (1) the distribution of vulnerabilities identified during the Nessus vulnerability

The presence of multiple Critical and High severity vulnerabilities indicates that the system is at a very high risk of compromise .

7.Identification of Running Services

The Nessus Basic Network Scan successfully identified multiple running services on the target system. These services were discovered through open port detection

The identified services include:

- FTP
- SSH
- Telnet
- HTTP (Apache Web Server)
- Samba (SMB)
- NFS
- DNS
- IRC

Sev	CVSS	VPR	EPSS	Name	Family	Count
CRITICAL	10.0 *	7.4	0.8622	UnrealIRCd Backdoor Detection	Backdoors	1
CRITICAL	10.0			Canonical Ubuntu Linux SEoL (8.04.x)	General	1
CRITICAL	10.0 *			VNC Server 'password' Password	Gain a shell remotely	1
CRITICAL	9.8	8.9	0.9447	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1
CRITICAL	9.8			SSL Version 2 and 3 Protocol Detection	Service detection	2
CRITICAL	9.8			Bind Shell Backdoor Detection	Backdoors	1
CRITICAL	...	...	...	SSL (Multiple Issues)	Gain a shell remotely	3
HIGH	7.5 *	6.7	0.5006	rlogin Service Detection	Service detection	1
HIGH	7.5 *	6.7	0.5006	rsh Service Detection	Service detection	1
HIGH	7.5	5.9	0.7714	Samba Badlock Vulnerability	General	1
HIGH	7.5			NFS Shares World Readable	RPC	1
MIXED	...	...	...	SSL (Multiple Issues)	General	28
MIXED	...	...	...	ISC Bind (Multiple Issues)	DNS	5
MEDIUM	6.5			TLS Version 1.0 Protocol Detection	Service detection	2
MEDIUM	6.5			Unencrypted Telnet Server	Misc.	1
MEDIUM	5.9	4.4	0.027	SSL Anonymous Cipher Suites Supported	Service detection	1
MEDIUM	5.9	3.6	0.8991	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Misc.	1
MIXED	...	...	...	ISC Bind (Multiple Issues)	DNS	5
MEDIUM	6.5			TLS Version 1.0 Protocol Detection	Service detection	2
MEDIUM	6.5			Unencrypted Telnet Server	Misc.	1
MEDIUM	5.9	4.4	0.027	SSL Anonymous Cipher Suites Supported	Service detection	1
MEDIUM	5.9	3.6	0.8991	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Misc.	1
MIXED	...	...	...	DNS (Multiple Issues)	DNS	5
MIXED	...	...	...	HTTP (Multiple Issues)	Web Servers	3
MIXED	...	...	...	SMB (Multiple Issues)	Misc.	2
MIXED	...	...	...	TLS (Multiple Issues)	Misc.	2
MIXED	...	...	...	TLS (Multiple Issues)	SMTP problems	2
LOW	3.7	3.9	0.939	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Misc.	1
LOW	2.6 *			X Server Detection	Service detection	1
LOW	2.1 *	2.2	0.0037	ICMP Timestamp Request Remote Date Disclosure	General	1
MIXED	...	...	...	SSH (Multiple Issues)	Misc.	3
INFO	...	...	...	SMB (Multiple Issues)	Windows	7
INFO	...	...	...	TLS (Multiple Issues)	General	4
INFO	...	...	...	FTP (Multiple Issues)	Service detection	3
INFO	...	...	...	VNC (Multiple Issues)	Service detection	3
INFO	...	...	...	Apache HTTP Server (Multiple Issues)	Web Servers	2

Figure (4) Nessus Vulnerability Scan Results Showing Identified Vulnerabilities

Table: Top 5 Critical Vulnerabilities Identified

No.	Vulnerability Name	Severity	Affected Service / Port	Why It Is Dangerous
1	UnrealIRCd Backdoor Detection (CVE-2010-2075)	Critical	IRC / TCP 6667	Contains a built-in backdoor that allows unauthenticated attackers to execute arbitrary commands with root privileges, leading to full system compromise.
2	Canonical Ubuntu Linux End of Life (8.04.x)	Critical	Operating System	The operating system is no longer supported and receives no security updates, leaving all services permanently vulnerable to known and future exploits.
3	VNC Server Weak Password	Critical	VNC / TCP 5900	The VNC service is protected by a weak password, allowing unauthorized remote users to log in and gain full graphical control of the system.
4	SSL Version 2 and 3 Protocol Enabled	Critical	Multiple Services (SSL/TLS)	Outdated SSL protocols are vulnerable to cryptographic attacks, enabling attackers to intercept or decrypt sensitive communications.
5	Bind Shell / Remote Shell Exposure	Critical	Remote Shell Services	Exposes a remote shell interface that allows attackers to execute commands directly on the system, resulting in immediate system takeover.

TABLE (2)The top five vulnerabilities identified by Nessus

8. Conclusion

This assessment successfully conducted a baseline vulnerability assessment of a Linux server using Nessus in accordance with the defined objectives and constraints. The results revealed that the Metasploitable system contains a large number of security weaknesses across all severity levels, with a particularly high concentration of Critical and High vulnerabilities. These findings indicate that the system is highly exposed and lacks essential security controls.

The identified vulnerabilities include outdated and unsupported software, insecure network services, weak authentication mechanisms, and the presence of backdoors that allow remote access. Such weaknesses significantly increase the risk of full system compromise if the server were deployed in a real production environment. The assessment demonstrates the importance of regular vulnerability scanning, proper system patching, and service hardening in reducing an organization's attack surface.

Overall, this exercise highlights how vulnerability assessment tools such as Nessus can be effectively used to identify security risks, prioritize remediation efforts, and improve the overall security posture of Linux-based systems without exploiting any vulnerabilities.