NAME: FERDAUS, JANNATUL

ID:20-42843-1

SECTION: C

Vulnerability Assessment Report

Target Host Information:

Hostname: Metasploitable 2

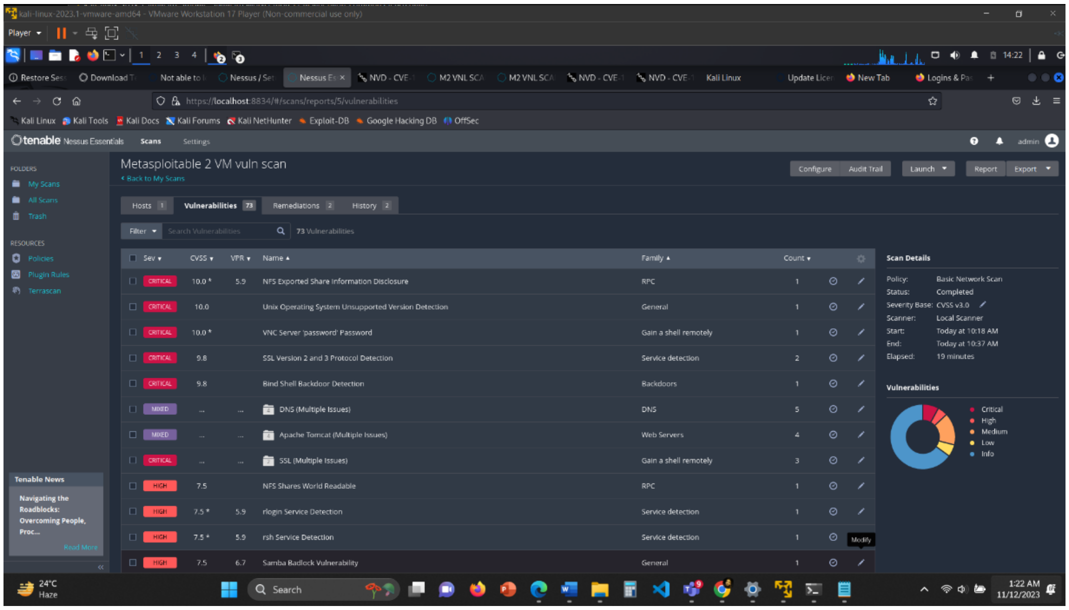
IP Address: 192.168.44.129

Scan Date: November 11, 2023

Summary:

This report explores the high-threat vulnerability findings for the host Metasploitable 2 that was scanned on November 11, 2023. For three of these high-threat vulnerabilities, the report summarizes the vulnerable service, what exploit might the vulnerability allow, and what mitigation is required to reduce or eliminate the vulnerability. The report also records at least three Common Vulnerability Exposure (CVE) identifiers for later investigation and provides links to known attacks that may work against the found vulnerabilities.

Scan Results :



Metasploitable 2 VM vuln scan

73 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1
CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1
CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1
CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2
CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1
MIXED	...	...	DNS (Multiple Issues)	DNS	5
MIXED	...	...	Apache Tomcat (Multiple Issues)	Web Servers	4
CRITICAL	...	...	SSL (Multiple Issues)	Gain a shell remotely	3
HIGH	7.5		NFS Shares World Readable	RPC	1
HIGH	7.5 *	5.9	rlogin Service Detection	Service detection	1
HIGH	7.5 *	5.9	rsh Service Detection	Service detection	1
HIGH	7.5	6.7	Samba Badlock Vulnerability	General	1

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 10:18 AM
End: Today at 10:37 AM
Elapsed: 19 minutes

Vulnerabilities

Risk Assessment :

This report identifies security risks that could have significant impact on mission-critical applications used for day-to-day business operations.

Critical Severity	High Severity	Medium Severity	Low Severity
12	7	25	8

Vulnerability Findings:

The following table summarizes the high-threat vulnerability findings for the host [Host Name]:

CVE Identifier	Vulnerability Description	Exploit	Mitigation
CVE-1999-0170	NFS Exported Share Information Disclosure	At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.	Configure NFS on the remote host so that only authorized hosts can mount its remote shares.
CVE-2020-1745	Apache Tomcat AJP Connector Request Injection (Ghostcat)	A file read/inclusion vulnerability was found in AJP connector. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and gain remote code execution (RCE).	Update the AJP configuration to require authorization and/or upgrade the Tomcat server to 7.0.100, 8.5.51, 9.0.31 or later.
CVE-2008-1447	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning	The remote DNS resolver does not use random ports when making queries to third-party DNS servers. An unauthenticated, remote attacker can exploit this to poison the remote DNS server, allowing the attacker to divert legitimate traffic to arbitrary sites.	Contact your DNS server vendor for a patch.

Known Attacks and Exploits:

1. CVE-1999-0170

Link to Known Attacks: https://localhost:8834/#/scans/reports/5/vulnerabilities/11356

Link to Mitigation Details: https://nvd.nist.gov/vuln/detail/CVE-1999-0170

2. CVE-2020-1745

Link to Known Attacks: https://localhost:8834/#/scans/reports/5/vulnerabilities/134862

Link to Mitigation Details: https://nvd.nist.gov/vuln/detail/CVE-2020-1745

3. CVE-2008-1447

Link to Known Attacks: https://localhost:8834/#/scans/reports/5/vulnerabilities/33447

Link to Mitigation Details: https://nvd.nist.gov/vuln/detail/CVE-2008-1447

Conclusion:

This report has explored the high-threat vulnerability findings for the host Metasploitable 2 that was scanned on November 11, 2023. The report has summarized three of these high-threat vulnerabilities in detail and provided links to known attacks that may work against the found vulnerabilities. It is strongly recommended that the vulnerabilities listed in this report be remediated as soon as possible.