



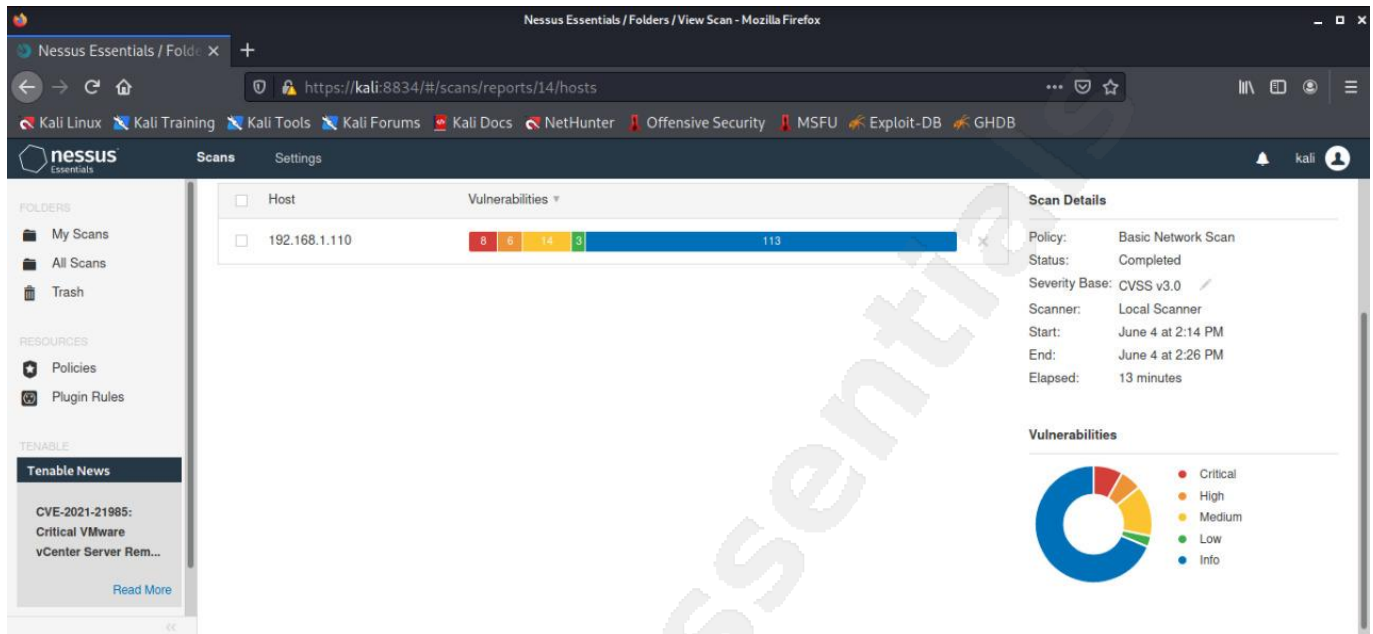
## **METASPLOIT MACHINE**

**Submitted by:**  
**Shirshak kumar kafle**

## TABLE OF CONTENTS

### Hosts Executive Summary

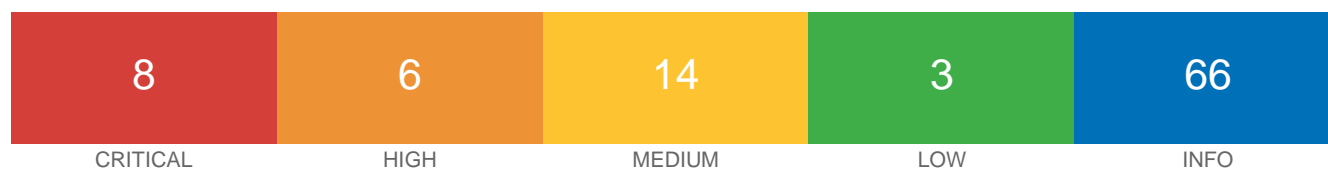
- 192.168.1.110.....4



## Hosts Executive Summary

# vulnerability

192.168.1.110



## Vulnerabilities

Total: 97

SEVERITY	CVSS V3.0	PLUGIN	NAME
CRITICAL	9.4	33447	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning
CRITICAL	7.5	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	7.5	34460	Unsupported Web Server Detection
CRITICAL	10.0	51988	Bind Shell Backdoor Detection
CRITICAL	10.0	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0	61708	VNC Server 'password' Password
HIGH	7.8	136808	ISC BIND Denial of Service
HIGH	7.1	20007	SSL Version 2 and 3 Protocol Detection
HIGH	6.8	90509	Samba Badlock Vulnerability
HIGH	5.0	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	5.0	42256	NFS Shares World Readable
HIGH	5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	6.1	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.8	42263	Unencrypted Telnet Server

MEDIUM	5.0	<a href="#">12085</a>	Apache Tomcat Default Files
MEDIUM	5.0	<a href="#">12217</a>	DNS Server Cache Snooping Remote Information Disclosure
MEDIUM	5.0	<a href="#">11213</a>	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.0	<a href="#">57608</a>	SMB Signing not required
MEDIUM	5.0	<a href="#">15901</a>	SSL Certificate Expiry
MEDIUM	5.0	<a href="#">45411</a>	SSL Certificate with Wrong Hostname
MEDIUM	4.3	<a href="#">90317</a>	SSH Weak Algorithms Supported
MEDIUM	4.3	<a href="#">65821</a>	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	4.3	<a href="#">78479</a>	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
MEDIUM	4.0	<a href="#">139915</a>	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
LOW	2.6	<a href="#">70658</a>	SSH Server CBC Mode Ciphers Enabled
LOW	2.6	<a href="#">71049</a>	SSH Weak MAC Algorithms Enabled
LOW	2.6	<a href="#">10407</a>	X Server Detection
INFO	N/A	<a href="#">10223</a>	RPC portmapper Service Detection
INFO	N/A	<a href="#">21186</a>	AJP Connector Detection
INFO	N/A	<a href="#">18261</a>	Apache Banner Linux Distribution Disclosure
INFO	N/A	<a href="#">48204</a>	Apache HTTP Server Version
INFO	N/A	<a href="#">39446</a>	Apache Tomcat Detection
INFO	N/A	<a href="#">84574</a>	Backported Security Patch Detection (PHP)
INFO	N/A	<a href="#">39520</a>	Backported Security Patch Detection (SSH)
INFO	N/A	<a href="#">39521</a>	Backported Security Patch Detection (WWW)
INFO	N/A	<a href="#">45590</a>	Common Platform Enumeration (CPE)
INFO	N/A	<a href="#">10028</a>	DNS Server BIND version Directive Remote Version Detection
INFO	N/A	<a href="#">11002</a>	DNS Server Detection
INFO	N/A	<a href="#">72779</a>	DNS Server Version Detection

INFO	N/A	<a href="#">35371</a>	DNS Server hostname.bind Map Hostname Disclosure
INFO	N/A	<a href="#">54615</a>	Device Type
INFO	N/A	<a href="#">10092</a>	FTP Server Detection
INFO	N/A	<a href="#">10107</a>	HTTP Server Type and Version
INFO	N/A	<a href="#">24260</a>	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	<a href="#">11156</a>	IRC Daemon Version Detection
INFO	N/A	<a href="#">117886</a>	Local Checks Not Enabled (info)
INFO	N/A	<a href="#">10397</a>	Microsoft Windows SMB LanMan Pipe Server Listing Disclosure
INFO	N/A	<a href="#">10785</a>	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	<a href="#">11011</a>	Microsoft Windows SMB Service Detection
INFO	N/A	<a href="#">100871</a>	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	<a href="#">106716</a>	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
INFO	N/A	<a href="#">10719</a>	MySQL Server Detection
INFO	N/A	<a href="#">10437</a>	NFS Share Export List
INFO	N/A	<a href="#">11219</a>	Nessus SYN scanner
INFO	N/A	<a href="#">19506</a>	Nessus Scan Information
INFO	N/A	<a href="#">11936</a>	OS Identification
INFO	N/A	<a href="#">10919</a>	Open Port Re-check
INFO	N/A	<a href="#">50845</a>	OpenSSL Detection
INFO	N/A	<a href="#">48243</a>	PHP Version Detection
INFO	N/A	<a href="#">66334</a>	Patch Report
INFO	N/A	<a href="#">118224</a>	PostgreSQL STARTTLS Support
INFO	N/A	<a href="#">26024</a>	PostgreSQL Server Detection
INFO	N/A	<a href="#">22227</a>	RMI Registry Detection
INFO	N/A	<a href="#">11111</a>	RPC Services Enumeration

INFO	N/A	<a href="#">53335</a>	RPC portmapper (TCP)
INFO	N/A	<a href="#">70657</a>	SSH Algorithms and Languages Supported
INFO	N/A	<a href="#">149334</a>	SSH Password Authentication Accepted
INFO	N/A	<a href="#">10881</a>	SSH Protocol Versions Supported
INFO	N/A	<a href="#">10267</a>	SSH Server Type and Version Information
INFO	N/A	<a href="#">56984</a>	SSL / TLS Versions Supported
INFO	N/A	<a href="#">45410</a>	SSL Certificate 'commonName' Mismatch
INFO	N/A	<a href="#">10863</a>	SSL Certificate Information
INFO	N/A	<a href="#">70544</a>	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	<a href="#">21643</a>	SSL Cipher Suites Supported
INFO	N/A	<a href="#">57041</a>	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	<a href="#">25240</a>	Samba Server Detection
INFO	N/A	<a href="#">104887</a>	Samba Version
INFO	N/A	<a href="#">96982</a>	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	<a href="#">22964</a>	Service Detection
INFO	N/A	<a href="#">11153</a>	Service Detection (HELP Request)
INFO	N/A	<a href="#">110723</a>	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	<a href="#">10281</a>	Telnet Server Detection
INFO	N/A	<a href="#">10287</a>	Traceroute Information
INFO	N/A	<a href="#">11154</a>	Unknown Service Detection: Banner Retrieval
INFO	N/A	<a href="#">19288</a>	VNC Server Security Type Detection
INFO	N/A	<a href="#">65792</a>	VNC Server Unencrypted Communication Detection
INFO	N/A	<a href="#">10342</a>	VNC Software Detection
INFO	N/A	<a href="#">135860</a>	WMI Not Available

INFO	N/A	<a href="#">20108</a>	Web Server / Application favicon.ico Vendor Fingerprinting
INFO	N/A	<a href="#">11422</a>	Web Server Unconfigured - Default Install Page Present
INFO	N/A	<a href="#">11424</a>	WebDAV Detection
INFO	N/A	<a href="#">10150</a>	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	<a href="#">52703</a>	vsftpd Detection



# Remiadation:

Thank You for Registerin

Temp Mail - Disposable

Nessus Essentials / Folders / View Scan

https://kali:8834/#/scans/reports/14/remediations

Kali LinuxKali TrainingKali ToolsKali ForumsKali DocsNetHunterOffensive SecurityMSFUExploit-DBGHDB

nessusEssentials

ScansSettings

kali

FOLDERS

My Scans

All Scans

Trash

RESOURCES

Policies

Plugin Rules

TENABLE

Tenable News

macOS Installer Local Privilege Escalation

Read More

metasploitable

ConfigureAudit TrailLaunchReportExport

Back to My Scans

Hosts1Vulnerabilities57Remediations3VPR Top ThreatsHistory1

Search Actions3 Actions

Action	Vulns	Hosts
ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS: Upgrade to BIND 9.11.22, 9.16.6, 9.17.4 or later.	3	1
Apache Tomcat AJP Connector Request Injection (Ghostcat): 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.	2	1
Samba Badlock Vulnerability: Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.	0	1

Scan Details

Policy: Basic Network Scan

Status: Completed

Severity Base: CVSS v3.0

Scanner: Local Scanner

Start: Today at 2:14 PM

End: Today at 2:26 PM

Elapsed: 13 minutes

# VPR Top Threat:

Thank You for Registerin

Temp Mail - Disposable

Nessus Essentials / Folders / View Scan

+

https://kali:8834/#/scans/reports/14/prioritization

Kali Linux

Kali Training

Kali Tools

Kali Forums

Kali Docs

NetHunter

Offensive Security

MSFU

Exploit-DB

GHDB

nessusEssentials

Scans

Settings

kali

FOLDERS

My Scans

All Scans

Trash

RESOURCES

Policies

Plugin Rules

TENABLE

Tenable News

Microsoft Teams

macOS Installer Local

Privilege Es...

Read More

VPR Severity	Name	Reasons	VPR Score	Hosts
CRITICAL	Apache Tomcat AJP Connector Request Injection (G...Social Media; Security Researc...		9.6	1
HIGH	Debian OpenSSH/OpenSSL Package Random Num...	No recorded events	7.4	1
HIGH	Debian OpenSSH/OpenSSL Package Random Num...	No recorded events	7.4	1
MEDIUM	Samba Badlock Vulnerability	No recorded events	6.7	1
MEDIUM	SSLv3 Padding Oracle On Downgraded Legacy Enc...	Hacker Forum	5.4	1
MEDIUM	Multiple Vendor DNS Query ID Field Prediction Cac...	No recorded events	5.2	1
MEDIUM	ISC BIND Service Downgrade / Reflected DoS	No recorded events	5.2	1
MEDIUM	SSL Medium Strength Cipher Suites Supported (SW...	No recorded events	4.4	1
MEDIUM	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	No recorded events	4.4	1

Scanner: Local Scanner  
Start: Today at 2:14 PM  
End: Today at 2:26 PM  
Elapsed: 13 minutes

Thank You for Registerin

Temp Mail - Disposable

Nessus Essentials / Folders / View Scan

+

https://kali:8834/#/scans/reports/14/prioritization

Kali Linux

Kali Training

Kali Tools

Kali Forums

Kali Docs

NetHunter

Offensive Security

MSFU

Exploit-DB

GHDB

nessusEssentials

Scans

Settings

kali

FOLDERS

My Scans

All Scans

Trash

RESOURCES

Policies

Plugin Rules

TENABLE

Tenable News

Microsoft Teams

macOS Installer Local

Privilege Es...

Read More

CRITICAL	Apache Tomcat AJP Connector Request Injection (G...Social Media; Security Researc...		9.6	1
HIGH	Debian OpenSSH/OpenSSL Package Random Num...	No recorded events	7.4	1
HIGH	Debian OpenSSH/OpenSSL Package Random Num...	No recorded events	7.4	1
MEDIUM	Samba Badlock Vulnerability	No recorded events	6.7	1
MEDIUM	SSLv3 Padding Oracle On Downgraded Legacy Enc...	Hacker Forum	5.4	1
MEDIUM	Multiple Vendor DNS Query ID Field Prediction Cac...	No recorded events	5.2	1
MEDIUM	ISC BIND Service Downgrade / Reflected DoS	No recorded events	5.2	1
MEDIUM	SSL Medium Strength Cipher Suites Supported (SW...	No recorded events	4.4	1
MEDIUM	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	No recorded events	4.4	1
MEDIUM	ISC BIND Denial of Service	No recorded events	4.4	1

Elapsed: 13 minutes

Thank you.....