nessus®

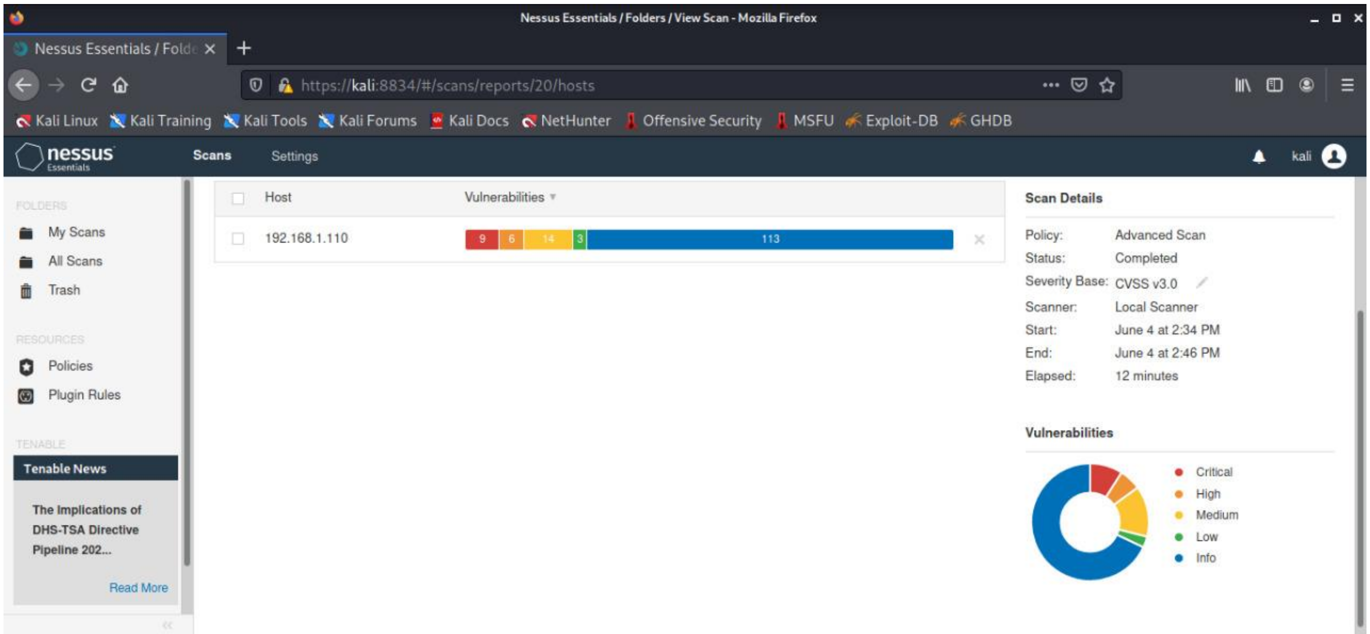
METASPLOIT

Submitted by:

Shirshak kumar kafle

Report generated by Nessus™ Fri, 04 Jun 2021 14:46:28 IST

TABLE OF CONTENTS



Host	Vulnerabilities
192.168.1.110	9 6 14 3 113

Scan Details

Policy:	Advanced Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	June 4 at 2:34 PM
End:	June 4 at 2:46 PM
Elapsed:	12 minutes

Vulnerabilities

Hosts Executive Summary

Vaulnerablity

192.168.1.110

9	6	14	3	68
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities

Total: 100

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	46882	UnrealIRCd Backdoor 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

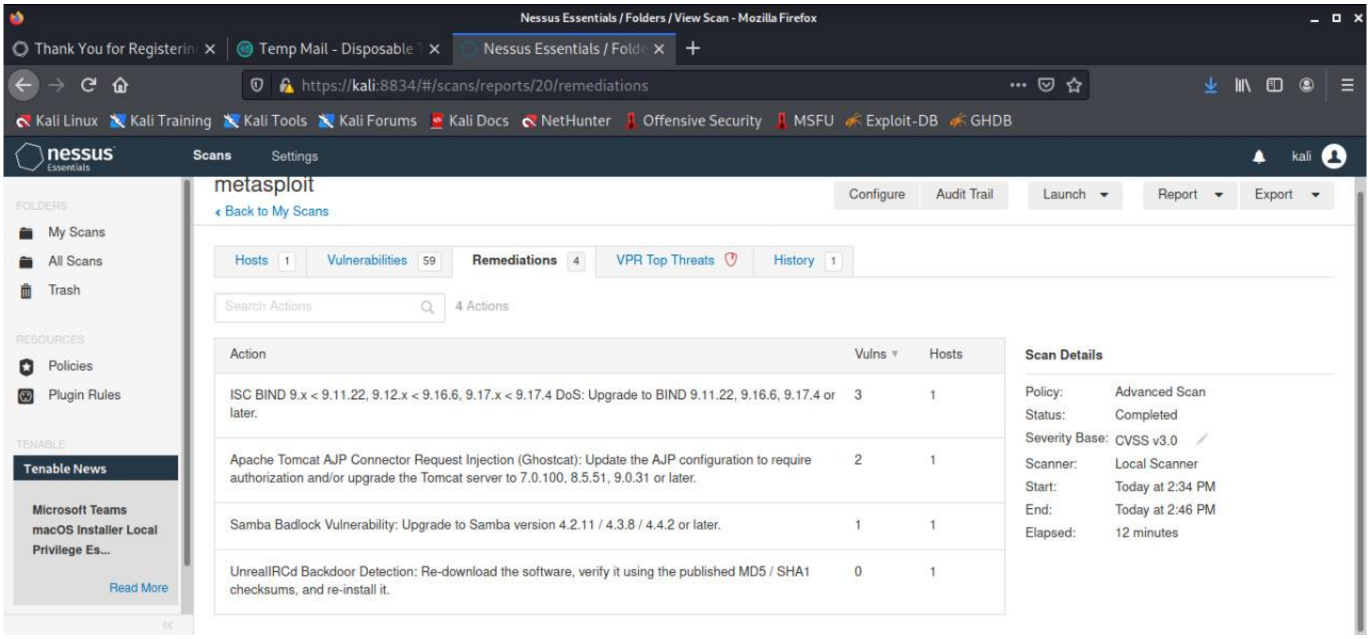
MEDIUM	5.8	42263	Unencrypted Telnet Server
MEDIUM	5.0	12085	Apache Tomcat Default Files
MEDIUM	5.0	12217	DNS Server Cache Snooping Remote Information Disclosure
MEDIUM	5.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.0	57608	SMB Signing not required
MEDIUM	5.0	15901	SSL Certificate Expiry
MEDIUM	5.0	45411	SSL Certificate with Wrong Hostname
MEDIUM	4.3	90317	SSH Weak Algorithms Supported
MEDIUM	4.3	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	4.3	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
MEDIUM	4.0	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
LOW	2.6	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6	71049	SSH Weak MAC Algorithms Enabled
LOW	2.6	10407	X Server Detection
INFO	N/A	10223	RPC portmapper Service Detection
INFO	N/A	21186	AJP Connector Detection
INFO	N/A	18261	Apache Banner Linux Distribution Disclosure
INFO	N/A	48204	Apache HTTP Server Version
INFO	N/A	39446	Apache Tomcat Detection
INFO	N/A	84574	Backported Security Patch Detection (PHP)
INFO	N/A	39520	Backported Security Patch Detection (SSH)
INFO	N/A	39521	Backported Security Patch Detection (WWW)
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	10028	DNS Server BIND version Directive Remote Version Detection
INFO	N/A	35373	DNS Server DNSSEC Aware Resolver

INFO	N/A	11002	DNS Server Detection
INFO	N/A	72779	DNS Server Version Detection
INFO	N/A	35371	DNS Server hostname.bind Map Hostname Disclosure
INFO	N/A	54615	Device Type
INFO	N/A	10092	FTP Server Detection
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	11156	IRC Daemon Version Detection
INFO	N/A	117886	Local Checks Not Enabled (info)
INFO	N/A	10397	Microsoft Windows SMB LanMan Pipe Server Listing Disclosure
INFO	N/A	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	11011	Microsoft Windows SMB Service Detection
INFO	N/A	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
INFO	N/A	10719	MySQL Server Detection
INFO	N/A	10437	NFS Share Export List
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	11936	OS Identification
INFO	N/A	10919	Open Port Re-check
INFO	N/A	50845	OpenSSL Detection
INFO	N/A	48243	PHP Version Detection
INFO	N/A	66334	Patch Report
INFO	N/A	118224	PostgreSQL STARTTLS Support
INFO	N/A	26024	PostgreSQL Server Detection

INFO	N/A	22227	RMI Registry Detection
INFO	N/A	11111	RPC Services Enumeration
INFO	N/A	53335	RPC portmapper (TCP)
INFO	N/A	70657	SSH Algorithms and Languages Supported
INFO	N/A	149334	SSH Password Authentication Accepted
INFO	N/A	10881	SSH Protocol Versions Supported
INFO	N/A	10267	SSH Server Type and Version Information
INFO	N/A	56984	SSL / TLS Versions Supported
INFO	N/A	45410	SSL Certificate 'commonName' Mismatch
INFO	N/A	10863	SSL Certificate Information
INFO	N/A	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	21643	SSL Cipher Suites Supported
INFO	N/A	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	25240	Samba Server Detection
INFO	N/A	104887	Samba Version
INFO	N/A	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	22964	Service Detection
INFO	N/A	17975	Service Detection (GET request)
INFO	N/A	11153	Service Detection (HELP Request)
INFO	N/A	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	10281	Telnet Server Detection
INFO	N/A	10287	Traceroute Information
INFO	N/A	11154	Unknown Service Detection: Banner Retrieval
INFO	N/A	19288	VNC Server Security Type Detection

INFO	N/A	65792	VNC Server Unencrypted Communication Detection
INFO	N/A	10342	VNC Software Detection
INFO	N/A	135860	WMI Not Available
INFO	N/A	20108	Web Server / Application favicon.ico Vendor Fingerprinting
INFO	N/A	11422	Web Server Unconfigured - Default Install Page Present
INFO	N/A	11424	WebDAV Detection
INFO	N/A	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	52703	vsftpd Detection

Remidation:

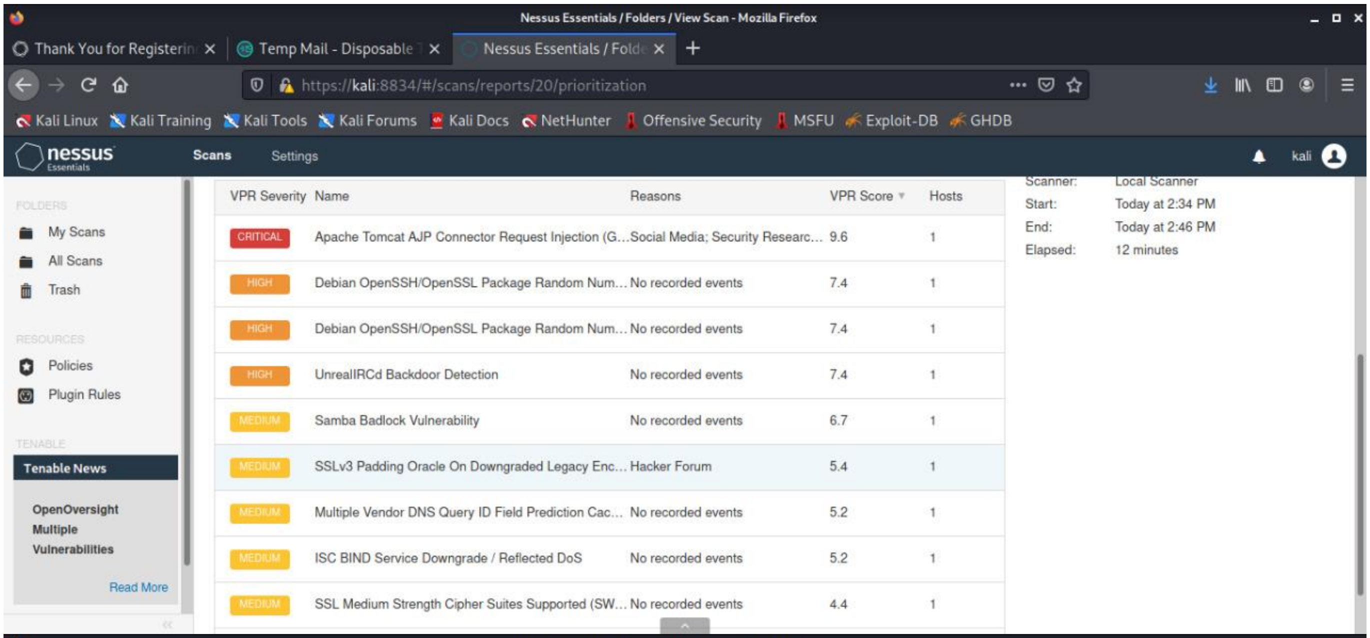


Action	Vulns	Hosts
ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS: Upgrade to BIND 9.11.22, 9.16.6, 9.17.4 or later.	3	1
Apache Tomcat AJP Connector Request Injection (Ghostcat): Update the AJP configuration to require authorization and/or upgrade the Tomcat server to 7.0.100, 8.5.51, 9.0.31 or later.	2	1
Samba Badlock Vulnerability: Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.	1	1
UnrealIRCd Backdoor Detection: Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.	0	1

Scan Details

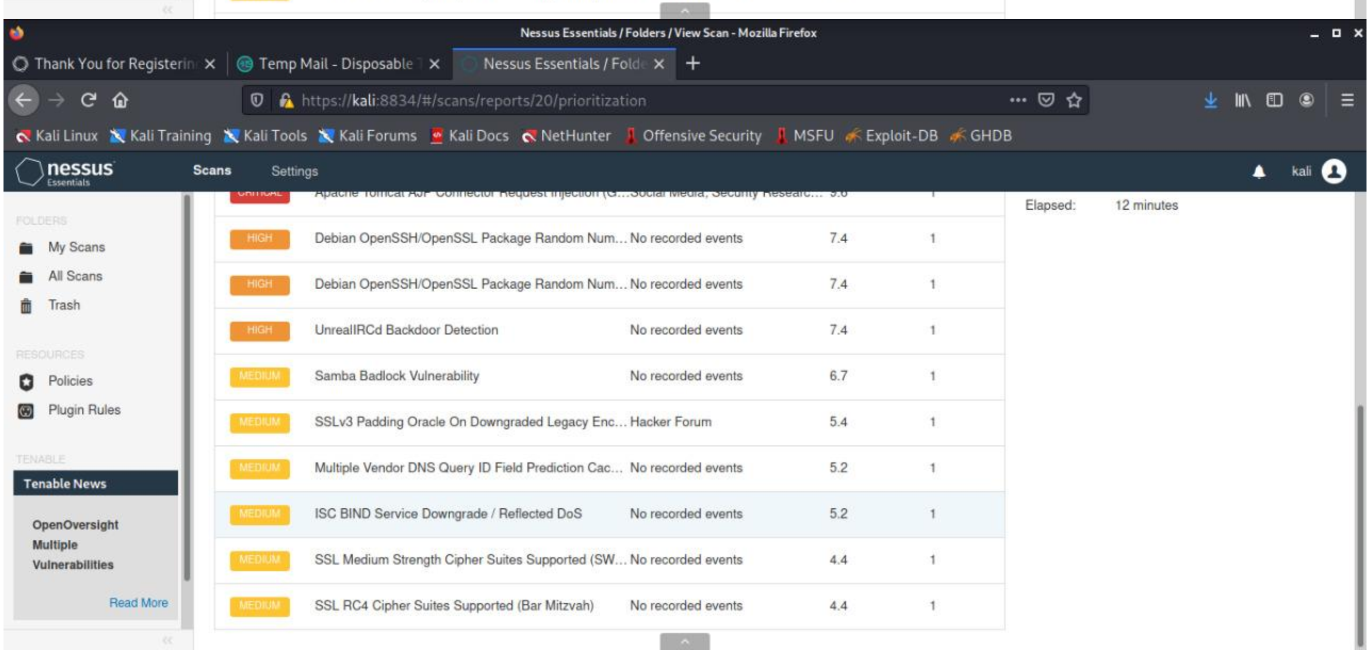
Policy:	Advanced Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 2:34 PM
End:	Today at 2:46 PM
Elapsed:	12 minutes

VPR TOP THREATS:



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
HIGH	UnrealIRCd Backdoor Detection	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

Scanner: Local Scanner
Start: Today at 2:34 PM
End: Today at 2:46 PM
Elapsed: 12 minutes



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
HIGH	UnrealIRCd Backdoor Detection	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

Elapsed: 12 minutes

Thank you…………..