Task 3 : Perform a Basic Vulnerability Scan on Your PC.

Objective: Use free tools to identify common vulnerabilities on your computer.

Tools: OpenVAS Community Edition (free vulnerability scanner) or Nessus Essentials.

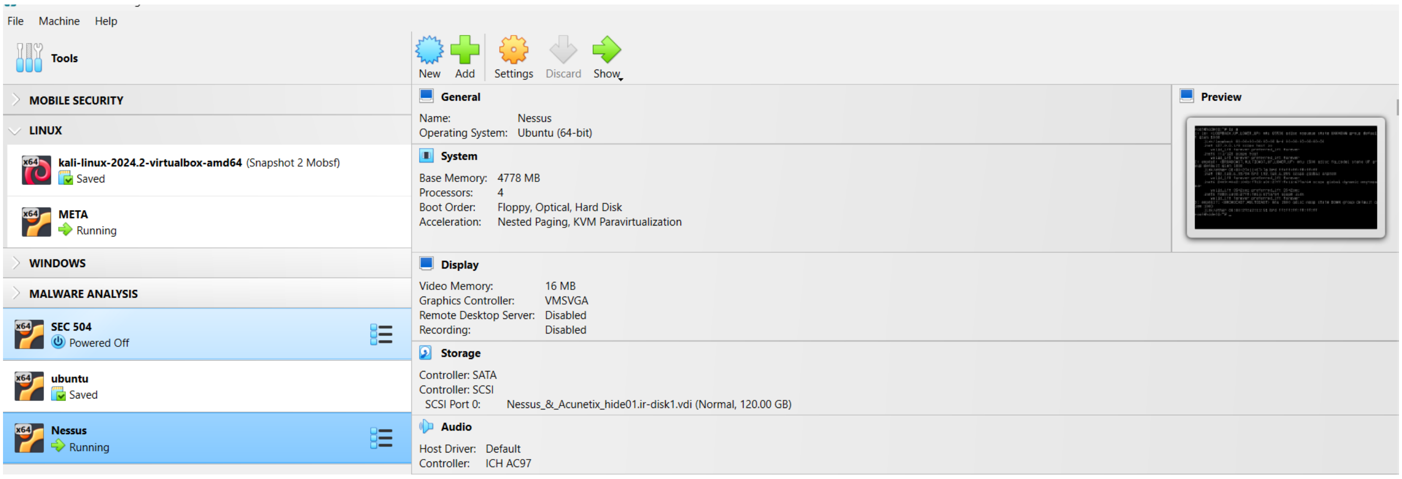
Deliverables: Vulnerability scan report with identified issues.

Nessus installed in a Ubuntu machine, which is accessible in the windows host though the bridged networking mode.

Network range is : 192.168.6.0/24

Nessus IP : 192.168.6.33

Metasploitable IP : 192.168.6.132



kali-linux-2024.2-virtualbox-amd64 (Snapshot 2 Mobsf) Saved

META Running

SEC 504 Powered Off

ubuntu Saved

Nessus Running

General
Name: Nessus
Operating System: Ubuntu (64-bit)

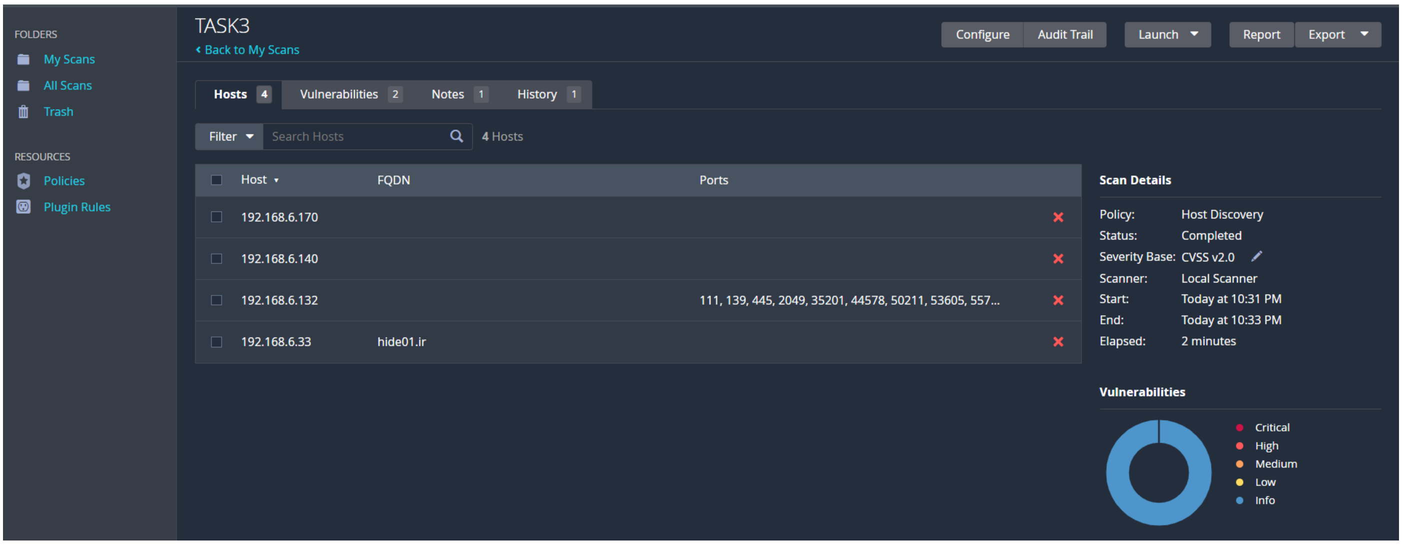
System
Base Memory: 4778 MB
Processors: 4
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, KVM Paravirtualization

Display
Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage
Controller: SATA
Controller: SCSI
SCSI Port 0: Nessus_&_Acunetix_hide01.ir-disk1.vdi (Normal, 120.00 GB)

Audio
Host Driver: Default
Controller: ICH AC97

Here I have ran a Host identification scan which is used to identify the machine or host present in the network at the time of scanning the network



TASK3

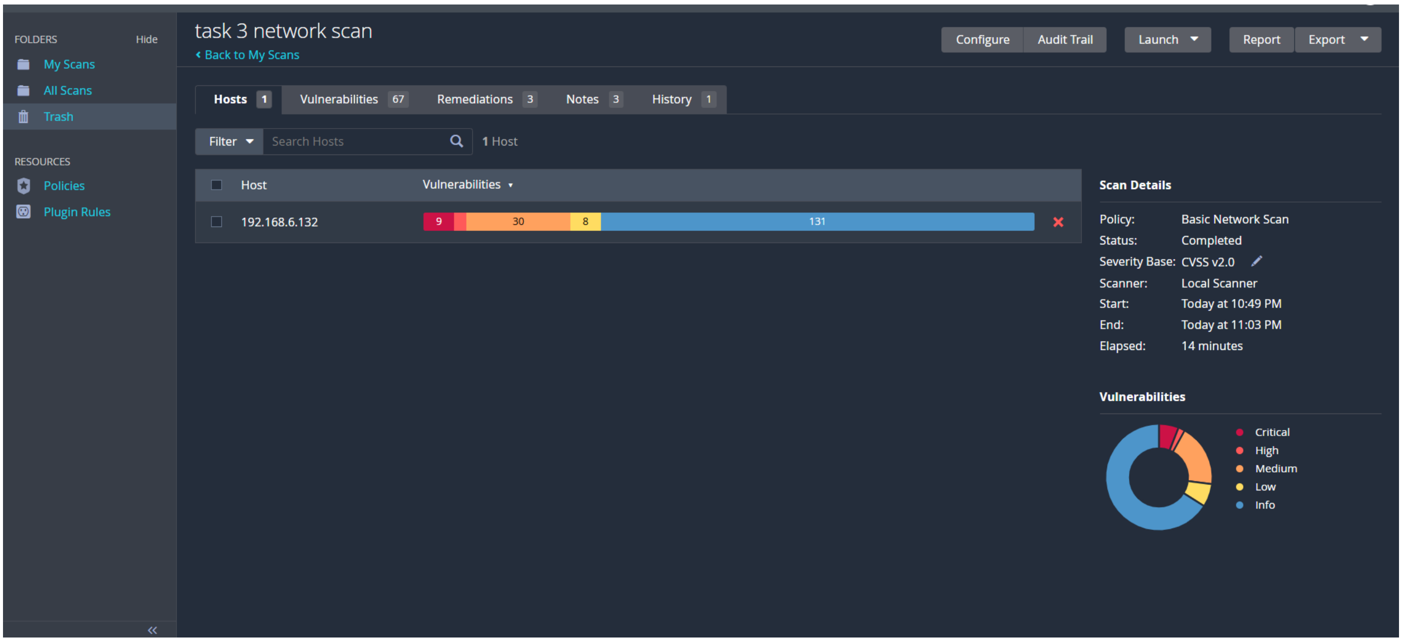
Host	FQDN	Ports
192.168.6.170		
192.168.6.140		
192.168.6.132		111, 139, 445, 2049, 35201, 44578, 50211, 53605, 557...
192.168.6.33	hide01.ir	

Scan Details

Policy: Host Discovery
Status: Completed
Severity Base: CVSS v2.0
Scanner: Local Scanner
Start: Today at 10:31 PM
End: Today at 10:33 PM
Elapsed: 2 minutes

Vulnerabilities

Nessus Network scan which I ran on the Metasploitable machine



task 3 network scan

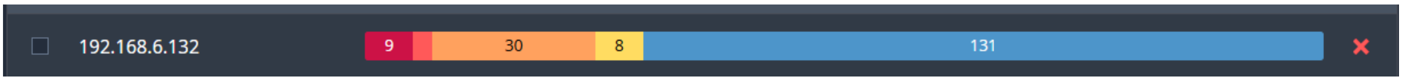
1 Host

Host	Vulnerabilities ▾
192.168.6.132	9 30 8 131

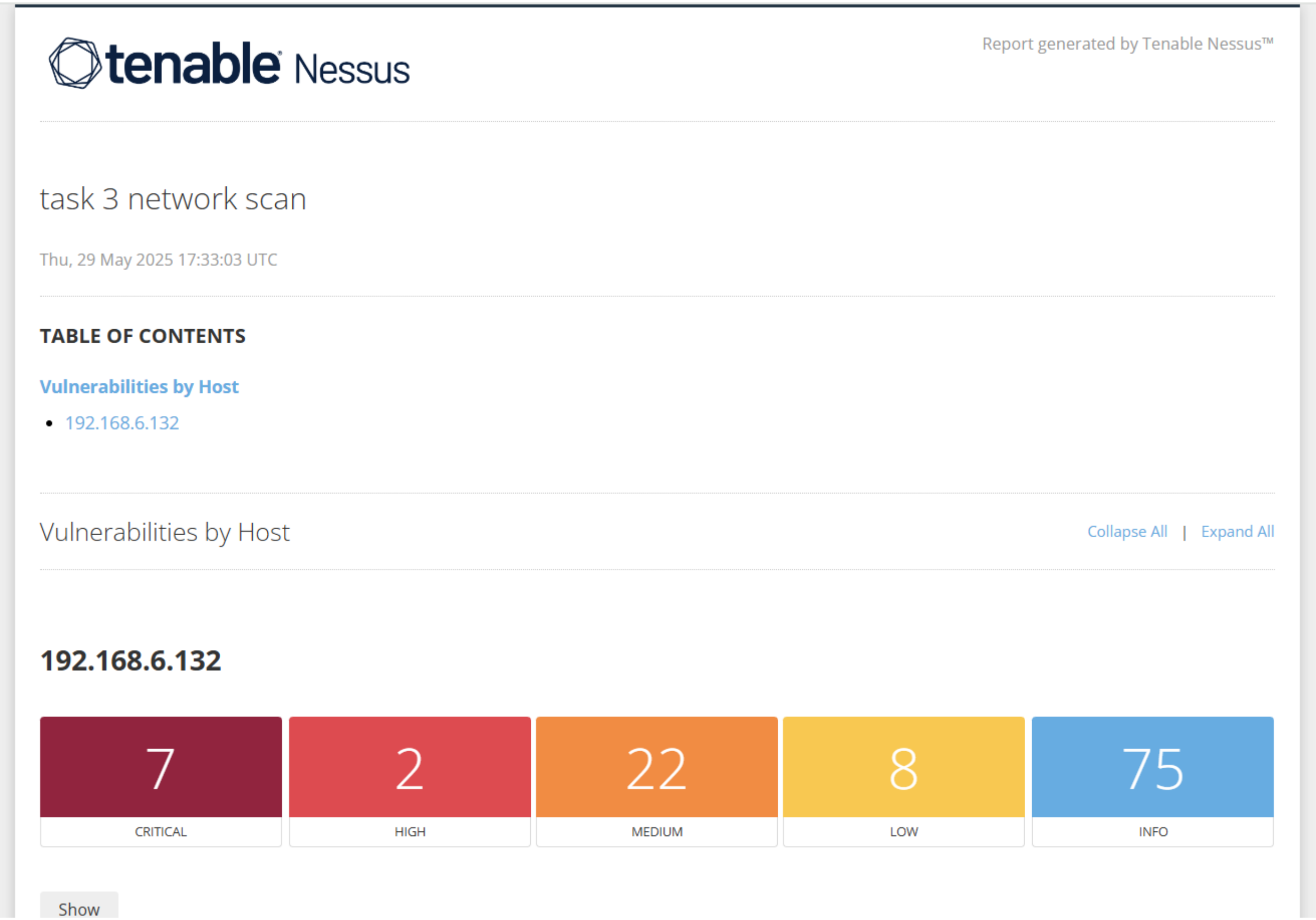
Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v2.0
Scanner: Local Scanner
Start: Today at 10:49 PM
End: Today at 11:03 PM
Elapsed: 14 minutes

Vulnerabilities



192.168.6.132 9 30 8 131



Report generated by Tenable Nessus™

task 3 network scan

Thu, 29 May 2025 17:33:03 UTC

TABLE OF CONTENTS

Vulnerabilities by Host

Collapse All | Expand All

192.168.6.132

7	2	22	8	75
CRITICAL	HIGH	MEDIUM	LOW	INFO

Show

Severity	CVSS v2.0	Plugin ID	Plugin Name
Critical	10.0	171340	Apache Tomcat SEoL (<= 5.5.x)
Critical	10.0	51988	Bind Shell Backdoor Detection
Critical	10.0	32314	Debian OpenSSH/OpenSSL Package RNG Weakness
Critical	10.0	32321	Debian OpenSSH/OpenSSL RNG Weakness (SSL check)
Critical	10.0	20007	SSL Version 2 and 3 Protocol Detection
Critical	10.0	46882	UnrealIRCd Backdoor Detection
Critical	10.0	61708	VNC Server 'password' Password
High	7.5	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
High	7.5	10205	rlogin Service Detection
Medium	6.8	90509	Samba Badlock Vulnerability
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	11213	HTTP TRACE / TRACK Methods Allowed
Medium	5.0	136769	ISC BIND Service Downgrade / Reflected DoS
Medium	5.0	42256	NFS Shares World Readable
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	5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
Medium	4.3	136808	ISC BIND Denial of Service
Medium	4.3	90317	SSH Weak Algorithms Supported
Medium	4.3	89058	SSL DROWN Attack Vulnerability
Medium	4.3	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
Medium	4.3	26928	SSL Weak Cipher Suites Supported

Severity	CVSS v2.0	Plugin ID	Plugin Name
Medium	4.3	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
Medium	4.3	78479	SSLv3 Padding Oracle Vulnerability (POODLE)
Medium	4.0	139915	ISC BIND DoS (< 9.11.22, < 9.16.6, < 9.17.4)
Medium	4.0	52611	SMTP STARTTLS Plaintext Command Injection
Low	2.6	70658	SSH Server CBC Mode Ciphers Enabled
Low	2.6	153953	SSH Weak Key Exchange Algorithms Enabled
Low	2.6	71049	SSH Weak MAC Algorithms Enabled
Low	2.6	31705	SSL Anonymous Cipher Suites Supported
Low	2.6	83875	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
Low	2.6	83738	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites
Low	2.6	10407	X Server Detection
Low	2.1	10114	ICMP Timestamp Request Remote Date Disclosure