**Name: Samarth Jain**

**USN: 4SU20CS081**

**Course: Cybersecurity**

**Trainer: Bharath Kumar**

**Date: 23/08/2023**

**Assignment Details**

Assigned Date: 22/08/2023

Due Date: 23/08/2023

Topic: Vulnerability Scanning

**Introduction**

Vulnerability scanning is a proactive security practice that involves using specialized tools to identify weaknesses and security gaps within computer systems, networks, and applications. It scans for known vulnerabilities, misconfigurations, and outdated software versions that could potentially be exploited by malicious actors. The goal of vulnerability scanning is to provide organizations with insights into their security posture, enabling them to prioritize and remediate vulnerabilities before they are exploited, thereby reducing the risk of cyberattacks and data breaches. Regular vulnerability scanning is an essential component of maintaining a strong cybersecurity strategy.

**Content**

**METASPLOITABLE2**

**Scan Details**

Policy: Basic Network Scan

Status: completed

Severity Base: CVSS v3.0

Scanner: Local Scanner

Start: Today at 08:48 PM

End: Today at 09:08 PM

Elapsed: 20 minutes

**Host Details**

IP: 10.0.2.5

MAC: 08:00:27:8D:55:32

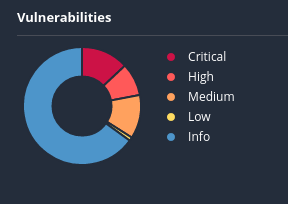
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

Start: Today at 8:48 PM

End: Today at 9:08 PM

Elapsed: 20 minutes

**Vulnerabilities**



Critical: 13 (7%)

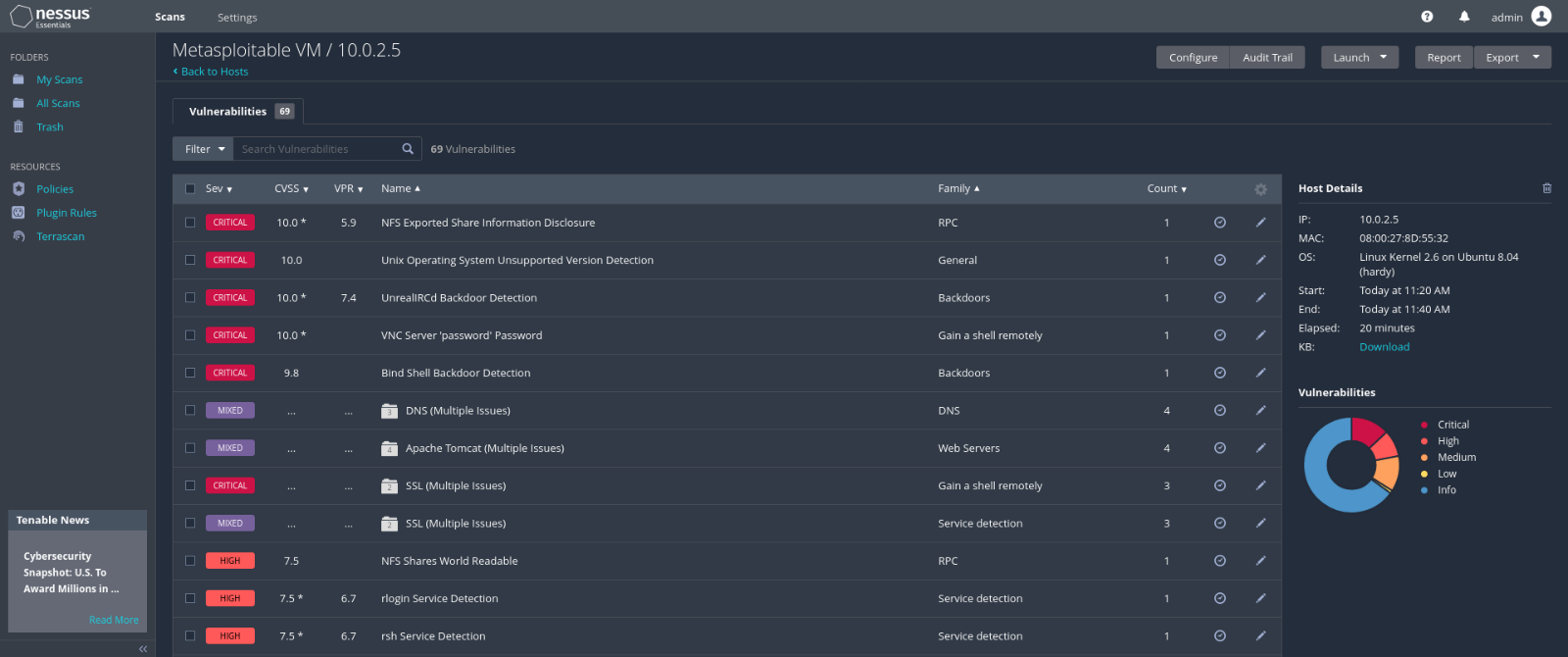
High: 7 (3%)

Medium: 25 (14%)

Low: 7 (3%)

Info: 134 (73%)

Metasploitable is a purposely vulnerable virtual machine (VM) that's used for training, practicing, and demonstrating various cybersecurity techniques and tools, particularly penetration testing and ethical hacking. It's designed to simulate a range of security vulnerabilities and weaknesses commonly found in real-world systems, making it an ideal environment for security professionals, students, and researchers to learn about and practice exploiting vulnerabilities in a controlled and safe setting.



1. **NFS Exported Share Information Disclosure [CRITICAL]**

ID: 11356

Description:

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.

Solution:

Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

Port: 2049 / udp / rpc-nfs

Tools to exploit: Metasploit (NFS Mount Scanner)

CVE:  [CVE-1999-0170](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0170), [CVE-1999-0211](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0211), [CVE-1999-0554](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0554)

1. **Unix Operating System Unsupported Vesrsion Detected [CRITICAL]**

ID**:** 33850

Description:

According to its self-reported version number, the Unix operating system running on the remote host is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

Solution:

Upgrade to a version of the Unix operating system that is currently supported.

Port: N/A

Tools to exploit: N/A

1. **UnrealIRCD Backdoor Detection [CRITICAL]**

ID: 46882

Description:

The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host.

Solution:

Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.

Port: 6667 / tcp / irc

Tools to exploit: Metasploit (UnrealIRCD 3.2.8.1 Backdoor Command Execution), CANVAS ()

CVE: [CVE-2010-2075](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2075)

1. **VNC Server ‘password’ Password [CRITICAL]**

ID: 61708

Port: 5900 / tcp / vnc

1. **Bind Shell Backdoor Detection [CRITICAL]**

ID: 51988

Port: 1524 / tcp / wild\_shell

1. **SSL (Multiple Issues) [CRITICAL]**
2. **Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check) [CRITICAL]**

ID: 32321

Port: 5432 / tcp / postgresql

25 / tcp / smtp

Tools to exploit: Core Impact

CVE: [CVE-2008-0166](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-0166)

**b) Debian OpenSSH/OpenSSL Package Random Number Generator Weakness [CRITICAL]**

ID: 32314

Port: 22 / tcp / ssh

Tools to exploit: Core Impact

CVE: [CVE-2008-0166](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-0166)

1. **NFS Shares World Readable [HIGH]**

ID: 42256

Port: 2049 / tcp / rpc-nfs

1. **rlogin Service Detection [HIGH]**

ID: 10205

Port: 513 / tcp / rlogin

1. **rsh Service Detection [HIGH]**

ID: 10245

Port: 514 / tcp / rsh

Tools to exploit: Metasploit (rlogin Authentication Scanner)

CVE: [CVE-1999-0651](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0651)

1. **Samba Badlock Vulnerability [HIGH]**

ID: 90509

Port: 445 / tcp / cifs

Tools to exploit: No known exploits are available

CVE: [CVE-2016-2118](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-2118)

1. **TLS Version 1.0 Protocol Detection [MEDIUM]**

ID: 104743

Port: 5432 / tcp / postgresql

25 / tcp / smtp

1. **Unencrypted Telnet Server [MEDIUM]**

ID: 42263

Port: 23 / tcp / telnet

1. **SSL Drown Attack Vulnerability (Decrypting RSA with Obsolete and Weakend eNcryption) [MEDIUM]**

ID: 89058

Port: 25 / tcp / smtp

Tools to exploit: No known exploits are available

CVE: [CVE-2016-0800](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0800)

**WINDOWS7**

**Scan Details**

Policy: Basic Network Scan

Status: completed

Severity Base: CVSS v3.0

Scanner: Local Scanner

Start: Today at 5:37 PM

End: Today at 5:42 PM

Elapsed: 5 minutes

**Host Details**

IP: 10.0.2.4

MAC: 08:00:27:9E:37:29

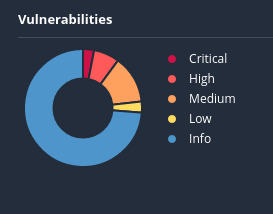
OS: Microsoft Windows 7 Ultimate

Start: Today at 5:37 PM

End: Today at 5:42 PM

Elapsed: 5 minutes

**Vulnerabilities**



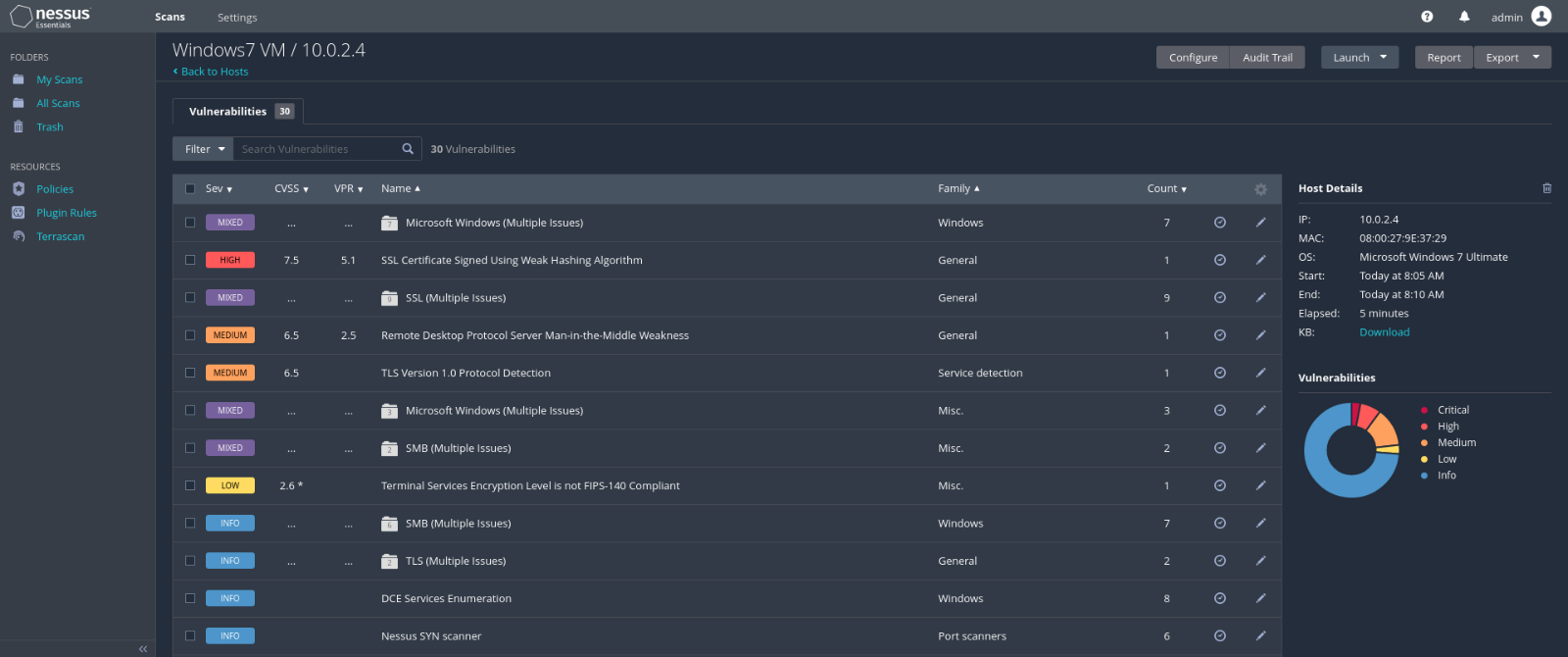
Critical: 3 (5%)

High: 4 (6%)

Medium: 9 (14%)

Low: 1 (2%)

Info: 49 (73%)



1. **SSL Certificate Signed Using Weak Hashing Algorithm [HIGH]**

ID: 35291

Port: 3389 / tcp

CVE: [CVE-2004-2761](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-2761)

1. **Remote Desktop Protocol Server Man-in-the-Middle Weakness [MEDIUM]**

ID: 18405

Port: 3389 / tcp

Tools for exploit: No known exploits are available

CVE: [CVE-2005-1794](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-1794)

1. **TLS Version 1.0 Protocol Detection [MEDIUM]**

ID: 104743

Port: 3389 / tcp

**scanme.nmap.org (Website)**

**Scan Details**

Policy: Web Application Tests

Status: completed

Severity Base: CVSS v3.0

Scanner: Local Scanner

Start: Today at 8:50 PM

End: Today at 9:17 PM

Elapsed: 27 minutes

**Host Details**

IP: 45.33.32.156

DNS: scanme.nmap.org

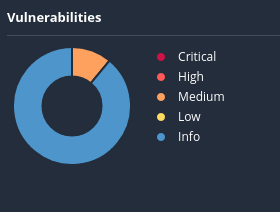
OS: Linux Kernel 3.13 on Ubuntu 14.04 (trusty)

Start: Today at 8:50 PM

End: Today at 9:17 PM

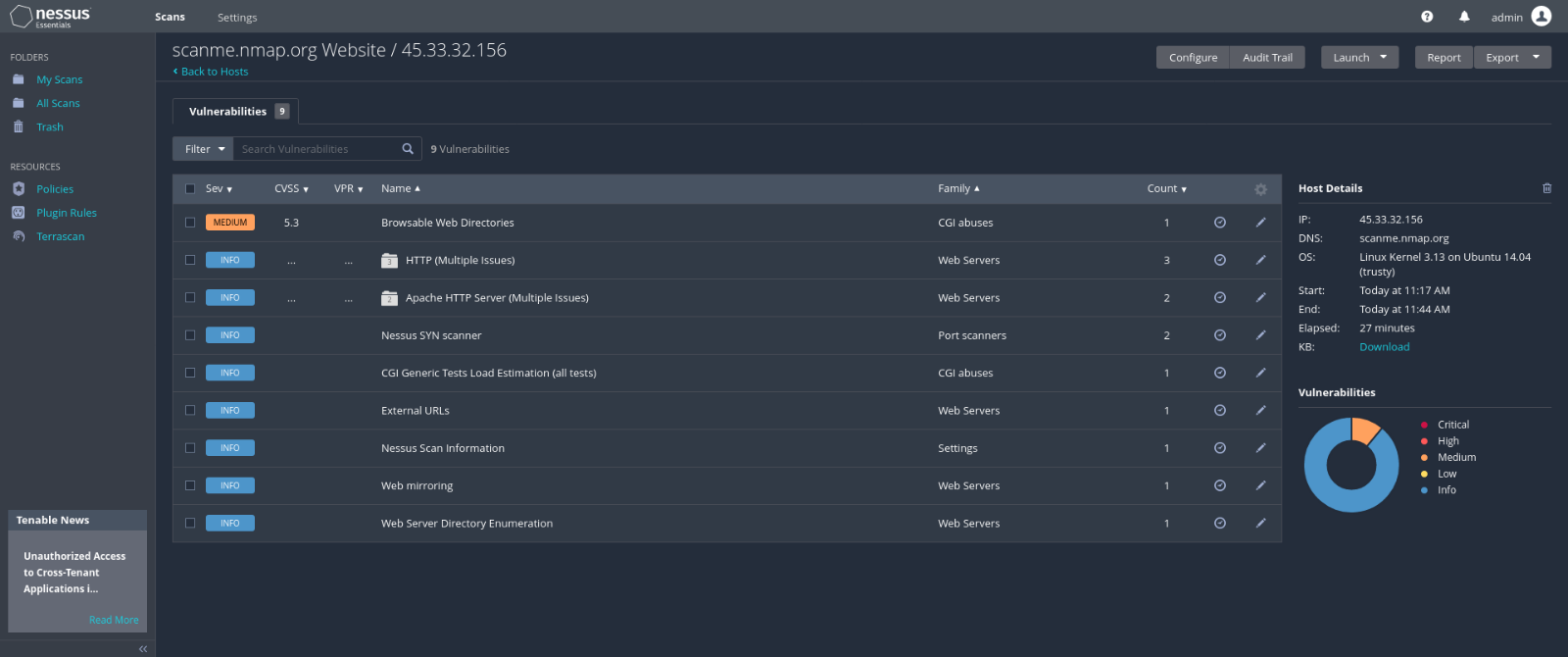
Elapsed: 27 minutes

**Vulnerabilities**



Medium: 1 (8%)

Info: 12 (92%)



1. **Browsable Web Directories [MEDIUM]**

Description

Multiple Nessus plugins identified directories on the web server that are browsable.

Solution

Make sure that browsable directories do not leak confidential information or give access to sensitive resources. Additionally, use access restrictions or disable directory indexing for any that do.

ID: 40984

Port: 80 / tcp

**Analysis**

The project report examines the implementation of vulnerability scanning utilizing Nessus as the primary tool. It delves into the process of configuring and running scans across a network to identify potential security weaknesses. The analysis highlights the effectiveness of Nessus in pinpointing vulnerabilities, discusses the significance of prompt remediation, and underscores its role in enhancing overall cybersecurity posture.

**Conclusion**

The project report examines the implementation of vulnerability scanning utilizing Nessus as the primary tool. It delves into the process of configuring and running scans across a network to identify potential security weaknesses. The analysis highlights the effectiveness of Nessus in pinpointing vulnerabilities, discusses the significance of prompt remediation, and underscores its role in enhancing overall cybersecurity posture.

**References**

[An InfoSec Blog for anyone interested to learn security and Hacking (wordpress.com)](https://hackwithbkob.wordpress.com/)

[Nmap: the Network Mapper - Free Security Scanner](https://nmap.org/)