

Cybersecurity Content Specialist Assignment: Vulnerability Scanning Report

Candidate Name: Vedant Adhikari

Submission Date: May 27, 2025

Tools Used: Kali Linux, Nmap, Metasploitable2

1. Introduction to Vulnerability Scanning

Vulnerability scanning is a crucial component of a robust cybersecurity strategy. It involves the automated process of identifying security weaknesses and misconfigurations within an organization's networks, systems, applications, and devices.

2. Methodology Used to Conduct the Scan

To demonstrate the process of vulnerability scanning, a controlled and ethical environment was established. The following steps outline the methodology employed:

2.1. Environment Setup:

- **Attacker Machine:** A Kali Linux Virtual Machine (VM) was used as the scanning platform.



- **Target Machine:** Metasploitable2, an intentionally vulnerable Linux-based virtual machine, was selected as the target system for the scan.

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:14:37:e5
          inet addr:11.0.0.9  Bcast:11.0.0.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe1d:37e5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5 errors:0 dropped:0 overruns:0 frame:0
          TX packets:34 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:983 (983.0 B)  TX bytes:4000 (3.9 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:96 errors:0 dropped:0 overruns:0 frame:0
          TX packets:96 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:21437 (20.9 KB)  TX bytes:21437 (20.9 KB)

msfadmin@metasploitable:~$
```

- **Network Configuration:** Both the Kali Linux VM and Metasploitable2 were configured within an isolated internal virtual network. This setup ensures that the scanning activities do not interfere with external networks and maintains a secure testing environment.

2.2. Nmap Tool Selection and Rationale: Nmap (Network Mapper) was chosen for this vulnerability scan due to its versatility, power, and widespread adoption in the cybersecurity community..

2.3. Scan Execution: The following Nmap command(s) were executed from the Kali Linux terminal against the Metasploitable2 target's IP address:

- **Initial Port and Service Discovery Scan:**

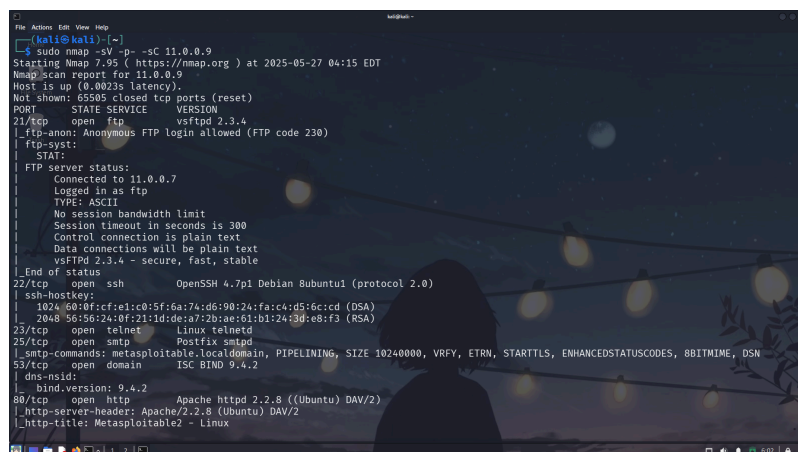
```
nmap -sV -sC -p- 11.0.0.9
```

-sV: Attempts to determine service/version info on open ports.

-sC: Runs default Nmap scripts, which include some basic vulnerability checks and enumeration.

-p-: Scans all 65535 ports.

2.4. Results Analysis: The output from the Nmap scans was carefully analyzed to identify open ports, the services running on them, their versions, and any vulnerabilities detected by the NSE scripts.



```

(kali@kali)~$ sudo nmap -sV -p- -sC 11.0.0.9
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-27 04:15 EDT
Nmap scan report for 11.0.0.9
Host is up (0.0023s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|_STAT:
|_FTP server status:
|_  Connected to 11.0.0.7
|_  Logged in as ftp
|_  TYPE: ASCII
|_  No session bandwidth limit
|_  Session timeout in seconds is 300
|_  Control connection is plain text
|_  Data connections will be plain text
|_vsftpd 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_ssh-hostkey:
|_  1024 6010f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_smtp_commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
33/tcp    open  domain       ISC BIND 9.4.2
|_dns-nsid:
|_bind.version: 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux

```

3. Key Vulnerabilities Identified During the Scan

The Nmap scan on Metasploitable2 revealed numerous open ports and services, many of which are known to be intentionally vulnerable.

- **Vulnerability 1: FTP Anonymous Login Allowed (Port 21)**

- **Description:** The Nmap scan identified an FTP service running on port 21. Analysis confirmed that this service allows anonymous login, granting unauthorized access to the FTP server without credentials.
- **Potential Impact (CIA Triad):** Primarily compromises **Confidentiality** and **Integrity**.

```
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|_STAT:
|_FTP server status:
|_Connected to 11.0.0.7
|_Logged in as ftp
|_TYPE: ASCII
|_No session bandwidth limit
|_Session timeout in seconds is 300
|_Control connection is plain text
|_Data connections will be plain text
|_vsFTPD 2.3.4 - secure, fast, stable
|_End of status
```

- **Vulnerability 2: Outdated Apache Tomcat Version (Port 8180)**

- **Description:** The scan detected an Apache Tomcat web server running on port 8180.
- **Potential Impact (CIA Triad):** High risk to **Confidentiality**, **Integrity** and **Availability**.

```
8180/tcp  open  unknown
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
```

- **Vulnerability 3: Default/Weak Credentials for Databases (e.g., MySQL on Port 3306, PostgreSQL on Port 5432)**

- **Description:** The Nmap scan identified open database ports (e.g., 3306 for MySQL, 5432 for PostgreSQL)..
- **Potential Impact (CIA Triad):** Critical impact on **Confidentiality**, **Integrity** and **Availability**.

```

3306/tcp open  mysql      MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 8
|   Capabilities flags: 43564
|   Some Capabilities: SwitchToSSLAfterHandshake, LongColumnFlag, Support41Auth, SupportsTransactions, ConnectWithDatabase, Speaks41Pro
SupportsCompression
|   Status: Autocommit
|   Salt: #heDb?VpR+{OWIE 0o^j

```

```

5432/tcp open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outsi
me=XX
| Not valid before: 2010-03-17T14:07:45
| Not valid after:  2010-04-16T14:07:45
|_ ssl-date: 2025-05-27T08:19:19+00:00; +15s from scanner time.

```

- **Vulnerability 4: Remote Login Services with Default Credentials (e.g., SSH on Port 22, Telnet on Port 23)**
 - **Description:** The scan identified open remote login services such as SSH (port 22) and Telnet (port 23). SSH might be susceptible to brute-force attacks due to weak configurations.
 - **Potential Impact (CIA Triad):** High CIA risk, especially due to plaintext Telnet.

```

22/tcp open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp open  telnet   Linux telnetd

```

- **Vulnerability 5: Unpatched Samba Services (Port 445/139)**
 - **Description:** Nmap detected Samba services running on ports 445 (SMB) and 139 (NetBIOS). It could be vulnerable to known exploits like EternalBlue (MS17-010).
 - **Potential Impact (CIA Triad):** High risk to **Confidentiality, Integrity and Availability**..

```

139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)

```

4. Recommended Actions to Mitigate or Address the Identified Vulnerabilities

Addressing identified vulnerabilities is crucial for improving a system's security posture. For each of the key vulnerabilities found, the following mitigation strategies are recommended, aligned with established cybersecurity frameworks like NIST and ISO 27001.

- **For FTP Anonymous Login Allowed:**
 - **Action:** Disable anonymous FTP access entirely if not absolutely necessary. If required, restrict anonymous access to read-only for specific, non-sensitive

directories. Configure the FTP server to require strong authentication for all write access.

- **For Outdated Apache Tomcat Version:**

- **Action:** Immediately update Apache Tomcat and all other outdated software components to their latest stable versions. Implement a regular patch management schedule as part of a continuous vulnerability management program.

- **For Default/Weak Credentials for Databases:**

- **Action:** Change all default credentials for database services (e.g., MySQL, PostgreSQL) to strong, unique passwords. Implement a robust password policy requiring complexity, length, and regular rotation. Where possible, use stronger authentication mechanisms like multi-factor authentication (MFA) or key-based authentication.

- **For Remote Login Services with Default Credentials (SSH/Telnet):**

- **Action:** Disable Telnet entirely due to its inherent insecurity (cleartext transmission). For SSH, enforce strong password policies, disable root login, prefer SSH key-based authentication, and configure SSH to use only strong cryptographic ciphers. Restrict SSH access to trusted IP addresses only.

- **For Unpatched Samba Services:**

- **Action:** Apply all available security patches for the Samba service. Ensure regular updates for all network services. If the service is not strictly required, disable it following the principle of least functionality.

5. Case studies and real world examples

- In 2017, it was reported that **Samsung's SmartThings hub** was vulnerable to FTP anonymous login, potentially exposing firmware information and device details to unauthorized users.
- In 2017, the **Equifax data breach**, which exposed personal data of millions, was largely attributed to the exploitation of a known vulnerability in the Apache Struts framework (CVE-2017-5638).

- The **Mirai botnet** in 2016 notoriously leveraged default and weak credentials on IoT devices (like routers, IP cameras, and DVRs) to gain control of them.
- The **WannaCry ransomware attack** of May 2017, which impacted hundreds of thousands of computers globally, exploited the EternalBlue vulnerability (MS17-010) in unpatched Windows systems (specifically targeting SMB services on port 445).

6. Conclusion

Vulnerability scanning, as demonstrated through the Nmap scan of Metasploitable2, is an indispensable practice for any organization aiming to protect its digital assets. Furthermore, the recommended mitigation strategies are directly aligned with internationally recognized **cybersecurity frameworks like NIST and ISO 27001**, underscoring a commitment to structured and comprehensive security management.

References:

1. Nmap.org Official Documentation.
2. National Institute of Standards and Technology (NIST) (Specify revision if you use a particular one, e.g., Rev. 5). Available at:
<https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>
3. International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection*.