Project Report

Basic Vulnerability Assessment for a Small Business Network

Intern Name: Jaishri Mahalia
Organization/Institution: Infotact Solution
Internship Duration: 05/05/2025 – 04/06/2025
Supervisor/Mentor:
Submission Date: 05/06/2025

Table of Contents

1. Executive Summary

This project simulates a real-world vulnerability assessment for a small business IT infrastructure. The objective is to identify potential security risks, prioritize them based on severity using CVSS scores, and provide mitigation strategies to improve the network's security posture. Over a four-week period, a virtual lab was set up with vulnerable machines and scanning tools to detect, analyze, and document real-world threats.

2. Project Objectives

- Set up a simulated small business IT infrastructure
- Learn and apply vulnerability assessment techniques
- Perform scanning and enumeration using professional tools
- Map vulnerabilities to public CVEs
- Recommend practical mitigation strategies

3. Week-wise Work Summary

Week 1: Virtual Lab Setup

- Installed VirtualBox and configured internal network
- Deployed Kali Linux (attacker) and Metasploitable2 (target)
- Verified inter-VM communication

Week 2: Network Scanning & Initial Analysis

- Conducted host discovery and port scanning using Nmap
- Performed service enumeration on open ports
- Launched vulnerability scans using OpenVAS
- Collected and documented initial scan data

Week 3: Vulnerability Assessment and CVE Research

- Matched discovered services to known vulnerabilities
- Researched CVEs and assessed CVSS scores
- Identified critical and high-severity threats in FTP, SSH, MySQL, and HTTP services

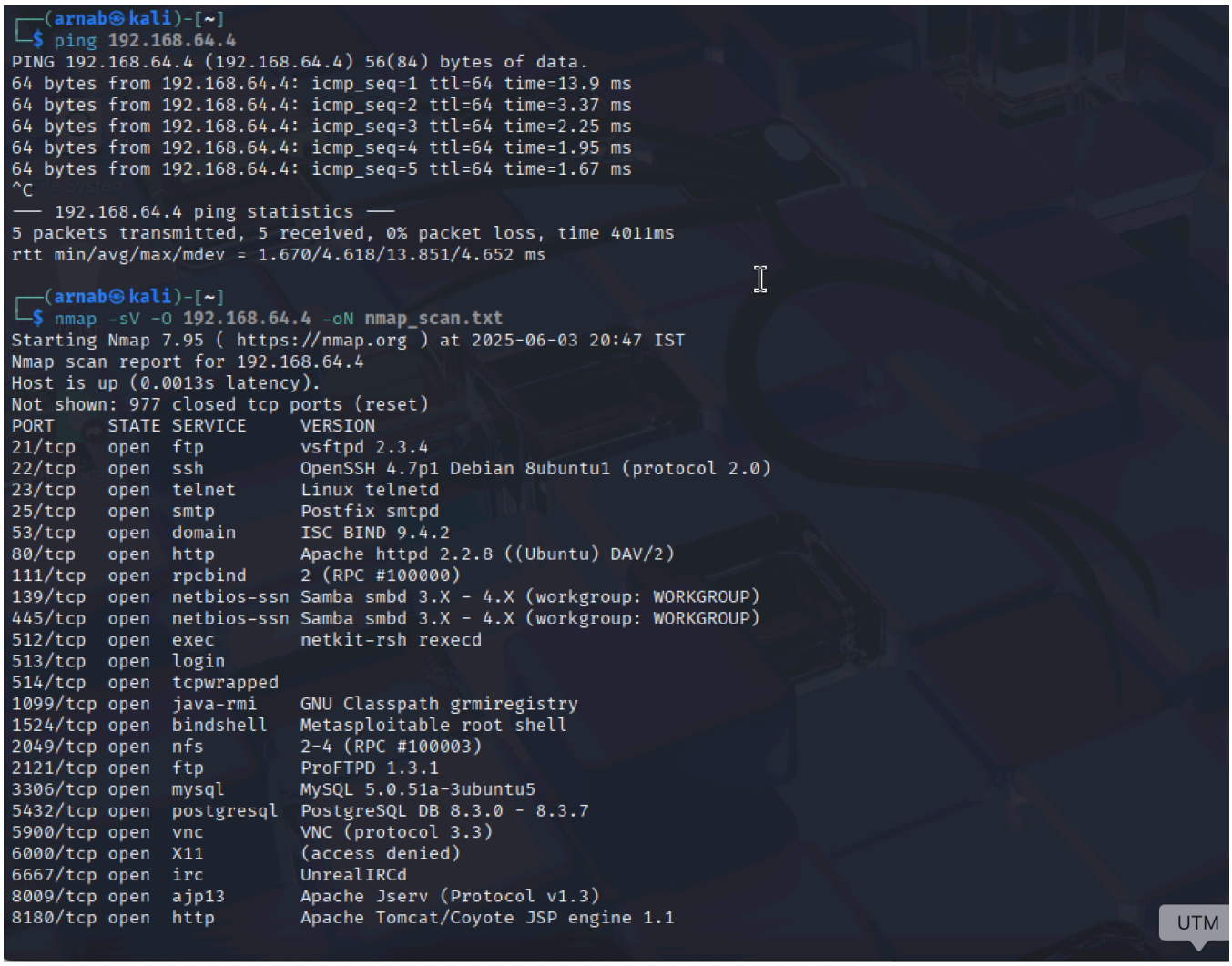
Week 4: Mitigation Planning and Documentation

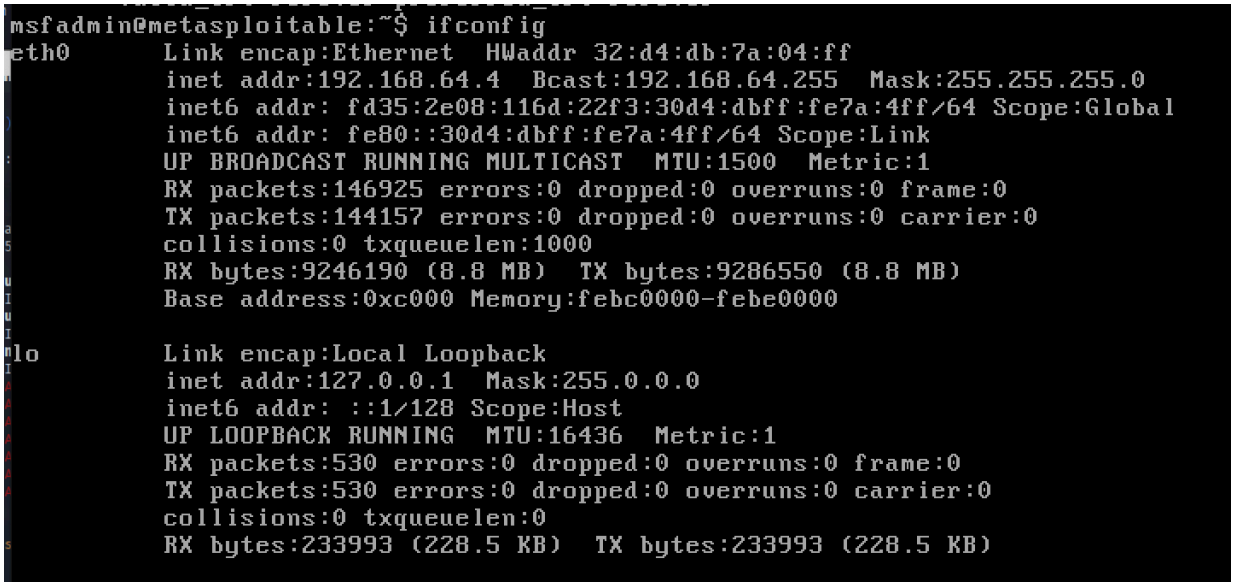
- Recommended fixes and configuration updates for each vulnerability
- Structured the final report with references and screenshots
- Prepared presentation slides for a simulated client review

4. Tools and Technologies Used

- **Virtualization:** UTM
- **Operating Systems:** Kali Linux, Metasploitable 2
- **Scanning Tool:** Nmap
- **Analysis:** CVE Reference Database, CVSS Calculator

Screenshots of the scanning done by nmap in kali in UTM , also metasploitable 2





```
┌──(arnab㉿kali)-[~]
└─$ nmap -p 21,22,53,44820,514 192.168.64.4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-03 20:50 IST
Nmap scan report for 192.168.64.4
Host is up (0.00057s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
53/tcp    open  domain
514/tcp   open  shell
44820/tcp open  unknown
MAC Address: 32:D4:DB:7A:04:FF (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds

┌──(arnab㉿kali)-[~]
└─$ nmap -A 192.168.64.4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-03 20:54 IST
Nmap scan report for 192.168.64.4
Host is up (0.0014s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.64.3
|      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
```

```
┌──(root㉿kali)-[/home/arnab]
└─# msfconsole
Metasploit tip: Use the analyze command to suggest runnable modules for
hosts

  Metasploit Park, System Security Interface
  Version 4.0.5, Alpha E
  Ready ...
  > access security
  access: PERMISSION DENIED.
  > access security grid
  access: PERMISSION DENIED.
  > access main security grid
  access: PERMISSION DENIED....and ...
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!


       =[ metasploit v6.4.56-dev                          ]
+ -- --=[ 2504 exploits - 1291 auxiliary - 393 post       ]
+ -- --=[ 1607 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search vsftpd 2.3.4

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution
```

Nmap Scan Report - Scanned at Wed Jun 4 21:23:42 2025

Scan Summary | 192.168.64.4

Scan Summary

Nmap 7.95 was initiated at Wed Jun 4 21:23:42 2025 with these arguments:
/usr/lib/nmap/nmap -v -sV -A -p1-65535 -oX ports.xml 192.168.64.4

Verbosity: 1; Debug level 0

Nmap done at Wed Jun 4 21:26:34 2025; 1 IP address (1 host up) scanned in 172.27 seconds

192.168.64.4

Address

- 192.168.64.4 (ipv4)
- 32:D4:DB:7A:04:FF (mac)

Ports

The 65505 ports scanned but not shown below are in state: **closed**

- 65505 ports replied with: **reset**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
21	tcp	open	ftp	syn-ack	vsftpd	2.3.4	
	ftp-anon	Anonymous FTP login allowed (FTP code 230)					
	ftp-syst	STAT: FTP server status: Connected to 192.168.64.3 Logged in as ftp TYPE: ASCII No session bandwidth limit					

Go to top
Toggle Closed Ports

		SSL2_RC2_128_CBC_WITH_MD5 SSL2_RC4_128_EXPORT40_WITH_MD5					
53	tcp	open	domain	syn-ack	ISC BIND	9.4.2	
	dns-nsid	bind.version: 9.4.2					
80	tcp	open	http	syn-ack	Apache httpd	2.2.8	(Ubuntu) DAV/2
	http-methods	Supported Methods: GET HEAD POST OPTIONS					
	http-server-header	Apache/2.2.8 (Ubuntu) DAV/2					
	http-title	Metasploitable2 - Linux					
111	tcp	open	rpcbind	syn-ack		2	RPC #100000
	rpcinfo	program version port/proto service 100000 2 111/tcp rpcbind 100000 2 111/udp rpcbind 100003 2,3,4 2049/tcp nfs 100003 2,3,4 2049/udp nfs 100005 1,2,3 50964/tcp mountd 100005 1,2,3 59761/udp mountd 100021 1,3,4 56696/tcp nlockmgr 100021 1,3,4 60005/udp nlockmgr 100024 1 40680/udp status 100024 1 55731/tcp status					
139	tcp	open	netbios-ssn	syn-ack	Samba smbd	3.X - 4.X	workgroup: WORKGROUP
445	tcp	open	netbios-ssn	syn-ack	Samba smbd	3.0.20-Debian	workgroup: WORKGROUP
512	tcp	open	exec	syn-ack	netkit-rsh rexecd		
513	tcp	open	login	syn-ack			
514	tcp	open	tcpwrapped	syn-ack			
1099	tcp	open	java-rmi	syn-ack	GNU Classpath grmiregistry		
1524	tcp	open	bindshell	syn-ack	Metasploitable root shell		
2049	tcp	open	nfs	syn-ack		2-4	RPC #100003
2121	tcp	open	ftp	syn-ack	ProFTPD	1.3.1	
3306	tcp	open	mysql	syn-ack	MySQL	5.0.51a-3ubuntu5	

Go to top
Toggle Closed Ports
Toggle Filtered Ports

39663	tcp	open	java-rmi	syn-ack	GNU Classpath grmiregistry		
50964	tcp	open	mountd	syn-ack		1-3	RPC #100005
55731	tcp	open	status	syn-ack		1	RPC #100024
56696	tcp	open	nlockmgr	syn-ack		1-4	RPC #100021

Remote Operating System Detection

- Used port: **21/tcp** (**open**)
- Used port: **1/tcp** (**closed**)
- Used port: **39374/udp** (**closed**)
- OS match: **Linux 2.6.9 - 2.6.33** (**100%**)

Host Script Output

Script Name	Output
smb-os-discovery	OS: Unix (Samba 3.0.20-Debian) Computer name: metasploitable NetBIOS computer name: Domain name: localdomain FQDN: metasploitable.localdomain System time: 2025-06-04T11:55:51-04:00
nbstat	NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown) Names: METASPLOITABLE<00> Flags: <unique><active> METASPLOITABLE<03> Flags: <unique><active> METASPLOITABLE<20> Flags: <unique><active> \x01\x02__MSBROWSE__\x02<01> Flags: <group><active> WORKGROUP<00> Flags: <group><active> WORKGROUP<1d> Flags: <unique><active> WORKGROUP<1e> Flags: <group><active>
clock-skew	mean: 59m59s, deviation: 1h59m59s, median: 0s
smb-security-mode	account_used: <blank> authentication_level: user challenge_response: supported message_signing: disabled (dangerous, but default)

Tog

Tog

5. Findings and Analysis

Vulnerability	Target System	CVSS Score	Details
OpenSSH 4.7 (CVE-2008-1657)	Metasploitable	7.5	Weak login control enabling remote exploitation
Apache 2.2.8 (CVE-2007-6388)	Metasploitable	6.8	Susceptible to denial-of-service
MySQL Default Auth (CVE-2012-2122)	Metasploitable	10.0	Permits root access without password

6. Recommendations

Vulnerability	Mitigation Strategy
MySQL Blank Password	Set a strong root password; restrict remote access
OpenSSH 4.7	Upgrade OpenSSH to the latest stable version
Apache 2.2.8 DoS	Update Apache to a secure version or configure mod_security

7. Learning Outcomes

Technical Skills:

- Configuration of virtual lab environments
- Nmap and OpenVAS scanning
- CVE identification and risk evaluation
- Cybersecurity reporting and documentation

Soft Skills:

- Research and analysis
- Time management and planning
- Professional documentation

8. Conclusion

This project effectively demonstrated the process of a basic vulnerability assessment in a small business environment. Key threats were discovered and mapped to known CVEs, and practical mitigations were proposed. The simulated lab and professional tools provided hands-on experience that mirrors real-world practices in network security.

9. Appendices

Nmap Commands Used:

- `nmap -sn <target>` — Host discovery
- `nmap -sS -sV <target>` — Port scan and service detection
- `nmap -O <target>` — OS detection
- `nmap -A <target>` — Aggressive scan with version detection

CVE Reference Links:

- CVE-2008-1657 – OpenSSH 4.7
- CVE-2007-6388 – Apache 2.2.8 DoS
- CVE-2012-2122 – MySQL Blank Password