

Project Report

Basic Vulnerability Assessment for a Small Business Network

Intern Name: Arnab Nath

Organization/Institution: Infotact Solution

Internship Duration: 05/05/2025 – 04/06/2025

Supervisor/Mentor:

Submission Date: 05/06/2025

Table of Contents

1. Summary Overview
2. Aims and Goals
3. Weekly Progress Breakdown
4. Tools & Platforms Utilized
5. Assessment Outcomes
6. Strategic Suggestions
7. Knowledge Gained
8. Wrap-Up
9. Supporting Material

1. Summary Overview

This report outlines a simulated cybersecurity exercise aimed at examining potential security flaws within a small business-style IT setup. Over a span of four weeks, the project involved deploying a virtual testing lab, identifying network vulnerabilities using advanced tools, and suggesting effective defenses. The initiative followed an organized plan to replicate real-life penetration testing and risk evaluation.

2. Aims and Goals

- Emulate a business IT environment for penetration testing
- Explore and practice vulnerability discovery methods
- Conduct scanning operations to uncover exposed services
- Link discovered weaknesses to official CVEs
- Advise on remediation actions using best practices

3. Weekly Progress Breakdown

Week 1: Virtual Lab Construction

- Set up VirtualBox with a dedicated internal network
- Installed Kali Linux for penetration testing purposes
- Deployed vulnerable targets: Metasploitable2
- Tested inter-device communication and configured static IPs

Week 2: Discovery and Mapping

- Identified devices on the network using Nmap tools
- Scanned for active services and open ports
- Performed vulnerability scans using OpenVAS suite
- Began compiling findings into draft notes

Week 3: CVE-Based Threat Analysis

- Cross-referenced vulnerabilities with public CVE databases
- Analyzed risks using the CVSS scoring system
- Focused on issues found in services like FTP, SSH, MySQL, and Apache

Week 4: Security Planning and Documentation

- Wrote detailed remediation steps for each threat identified
- Completed the full documentation and added illustrative evidence
- Created a client-style presentation highlighting key issues and solutions

4.Tools & Platforms Utilized

- **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)-[~]
$ ping 192.168.64.4
PING 192.168.64.4 (192.168.64.4) 56(84) bytes of data:
64 bytes from 192.168.64.4: icmp_seq=1 ttl=64 time=13.9 ms
64 bytes from 192.168.64.4: icmp_seq=2 ttl=64 time=3.37 ms
64 bytes from 192.168.64.4: icmp_seq=3 ttl=64 time=2.25 ms
64 bytes from 192.168.64.4: icmp_seq=4 ttl=64 time=1.95 ms
64 bytes from 192.168.64.4: icmp_seq=5 ttl=64 time=1.67 ms
^C
— 192.168.64.4 ping statistics —
5 packets transmitted, 5 received, 0% packet loss, time 401ms
rtt min/avg/max/mdev = 1.670/4.618/13.851/4.652 ms

(arnab@kali)-[~]
$ nmap -sV -O 192.168.64.4 -oN nmap_scan.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-03 20:47 IST
Nmap scan report for 192.168.64.4
Host is up (0.0013s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
```

UTM

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 32:d4:db:7a:04:ff
          inet addr:192.168.64.4  Bcast:192.168.64.255  Mask:255.255.255.0
          inet6 addr: fd35:2e08:116d:22f3:30d4:dbff:fe7a:4ff/64 Scope:Global
          inet6 addr: fe80::30d4:dbff:fe7a:4ff/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:146925 errors:0 dropped:0 overruns:0 frame:0
          TX packets:144157 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:9246190 (8.8 MB)  TX bytes:9286550 (8.8 MB)
          Base address:0xc000 Memory:febc0000-febe0000

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:530 errors:0 dropped:0 overruns:0 frame:0
          TX packets:530 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:233993 (228.5 KB)  TX bytes:233993 (228.5 KB)
```

```

(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
arnab@kali: ~
(arnab@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 Tue Jun 3 11:07:57 2025

Scan Summary | 192.168.64.4

Scan Summary

Nmap 7.95 was initiated at Tue Jun 3 11:07:57 2025 with these arguments:
usr/lib/nmap/nmap -v -sV -A -p1-65535 -oX port.xml 192.168.64.4
Verbosity: 1; Debug level 0
Nmap done at Tue Jun 3 11:10:46 2025; 1 IP address (1 host up) scanned in 168.53 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 [o] filtered [f])	Service	Reason	Product	Version	Extra info
21	tcp	open	ftp	syn-ack	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					
	ftp-anon	Anonymous FTP login allowed (FTP code 230)					

Go to top
Toggle Closed Ports
Toggle Filtered Ports

	ftp-anon	Anonymous FTP login allowed (FTP code 230)					
22	tcp	open	ssh	syn-ack	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	syn-ack	Linux telnetd		
25	tcp	open	smtp	syn-ack	Postfix smtpd		
	ssl-date	2025-05-27T07:15:19+00:00; -6d22h25m24s from scanner time.					
	smtp-commands	metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN					
	sslv2	SSLv2 supported ciphers: SSL2 DES_64_CBC_WITH_MD5 SSL2 RC4_128_WITH_MD5 SSL2 RC2_128_CBC_WITH_MD5 SSL2 RC2_128_CBC_EXPORT40_WITH_MD5 SSL2 DES_192_EDE3_CBC_WITH_MD5 SSL2 RC4_128_EXPORT40_WITH_MD5					
	ssl-cert	Subject: commonName=ubuntu804-base.localdomain/organizationName=OC0SA/stateOrProvinceName=There is no such thing outside US/countryName=XX Issuer: commonName=ubuntu804-base.localdomain/organizationName=OC0SA/stateOrProvinceName=There is no such thing outside US/countryName=XX Public Key type: rsa Public Key bits: 1024 Signature Algorithm: sha1WithRSAEncryption Not valid before: 2010-03-17T14:07:45 Not valid after: 2010-04-16T14:07:45 MD5: dcd9:ad90:6c8f:2f73:74af:383b:2540:8828 SHA-1: ed09:3088:7066:03bf:d5dc:2373:99b4:98da:2d4d:31c6					
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-server-header	Apache/2.2.8 (Ubuntu) DAV/2					
	http-methods	Supported Methods: GET HEAD POST OPTIONS					

Go to top
Toggle Closed Ports
Toggle Filtered Ports

Remote Operating System Detection

- Used port: 21/tcp (open)
- Used port: 11/tcp (closed)
- Used port: 34339/udp (closed)
- OS match: Linux 2.6.9 - 2.6.33 (100%)

Host Script Output

Script Name	Output
smb2-time	Protocol negotiation failed (SMB2)
smb-os-discovery	OS: Unix (Samba 3.0.20-Debian) Computer name: metasploitable NetBIOS computer name: Domain name: localdomain FQDN: metasploitable.localdomain System time: 2025-05-27T03:14:44-04:00
clock-skew	mean: -6d21h25m23s, deviation: 2h00m00s, median: -6d22h25m24s
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_MSBR0WSE_\x02<01> Flags: <group><active> WORKGROUP<00> Flags: <group><active> WORKGROUP<1d> Flags: <unique><active> WORKGROUP<1e> Flags: <group><active>
smb-security-mode	account_used: <blank> authentication_level: user challenge_response: supported message_signing: disabled (dangerous, but default)

5. Assessment Outcomes

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. Strategic Suggestions

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. Knowledge Gained

Practical Expertise:

- Hands-on virtual network deployment
- Executing Nmap and OpenVAS scans
- Investigating vulnerabilities through CVE data
- Drafting formal security evaluation reports

Professional Development:

- Time-bound project execution
- Research and analysis of public exploits
- Crafting structured documentation and presentations

8. Wrap-Up

This project offered a realistic experience of assessing and reporting IT vulnerabilities in a controlled business simulation. Each week contributed to a complete assessment cycle—planning, scanning, analysis, and resolution. The result is a thorough understanding of identifying security weaknesses and formulating targeted solutions.

9. Supporting Material

Network Commands Used:

- `nmap -sn <target>` — Network discovery
- `nmap -sS -sV <target>` — Port and version scan
- `nmap -O <target>` — Identify operating system
- `nmap -A <target>` — Complete host profile scan

Key CVEs Referenced:

- [CVE-2008-1657 – OpenSSH 4.7](#)
- [CVE-2007-6388 – Apache 2.2.8 DoS](#)
- [CVE-2012-2122 – MySQL Blank Password](#)