



ITSY 2359

SECURITY ASSESSMENT AND AUDITING

COMPANY BEING AUDITED NAME
SECURITY Penetration Test REPORT



Timothy Zellers
Sr. Auditor
FortifyNet Solutions
987 Watchtower Street
Digital City, Protectorsville 13579
Secure Province

TABLE OF CONTENTS

Note: Complete TOC with appropriate page numbers

	Page
1.0 Executive Summary	
2.0 Purpose	
3.0 Scope	
4.0 Tools and Methodologies	
5.0 Findings	
5.1 Reconnaissance	
5.2 Network Vulnerability Research	
5.3 Network Exploitation	
5.4 Operating System Exploitation	
5.5 Web Application Exploitation	
6.0 Summary	
6.1 Analysis	
6.2 Recommendations	
7.0 Points of Contact	
8.0 Distribution List	
9.0 Appendices	

FIGURES AND TABLES

	Page
Table 5.1.1.1	
Table 5.2.1.1	
Table 5.3.1.1	
Table 7.1 Points of Contact	
Table 8.1 Distribution List	
Figure <i>XXXX Note Add Figures included in document</i>	

APPENDICES

	Page
Appendix A. Reconnaissance OneNote Documentation	
Appendix B. Network Vulnerability scans and OneNote Documentation	
Appendix C. Network and OS Attacks OneNote Documentation Obtained Documents	
Appendix D. Web-Database Attacks OneNote Documentation Obtained Documents	

1.0 Executive Summary

2.0 Purpose

The purpose of the penetration test was to assess the network environment's defensive posture, utilizing tools listed in **3.0 Tools and Methodologies**. The findings aimed to assist the company in enhancing its security measures, protecting against potential threats, and safeguarding critical assets and data.

3.0 Scope

The Penetration test consisted of an assessment of the following items:

- Windows 2019 Server (Web Server)
- Ubuntu Machine (Apache Version 2.2.8)

4.0 Tools and Methodologies

- Nmap
- Metasploit
- Cyber Chef

5.0 Findings

With social engineering User name and Password was obtained for Pepper Pots. User name: SWilson, Password: OnYourLeft!.

During the course of the Pentest, two IP addresses were discovered vulnerable. A Windows 2019 Server with the IP address of 172.20.50.10 using Microsoft IIS httpd 10.0 Web Sever was discovered. This server has Active Directory Domain Services with a Domain name of "HackMe.loc0". An Ubuntu machine with the IP address of 172.20.50.54 hosting Apache 2.2.8 Services on port 80 was also discovered on the network. Both devices were vulnerable to Enumeration.

With enumeration, other domain accounts from the Windows 2019 Server were discovered with a Lockout tries setting of 0 and Passwordmin set to 7. Along with domain accounts linking the Windows 2019 Server to the Ubuntu machine services listed in **Lab 3.1.4 Network Enumeration** of **Appendix A**.

5.1 Reconnaissance

- Showdan.com
- Whois.com
- Social Engineering

5.2 Network Evaluation

5.3 OS Evaluation

5.4 Web Applications

6.0 Summary

6.1 Analysis

6.2 Recommendations

7.0 POINTS OF CONTACT

Table 7.1 provides the Points of Contact for this Document. *Note: Complete the table.*

Table 7.1 Points of Contact

Name	Title	Email	Phone #
Timothy Zellers	Senior Auditor	tlzellers113509@mymail.tstc.edu	713-516-8683
Robert Zellers	Owner	rzellers@yahoo.com	713-504-1249

8.0 DISTRIBUTION LIST

Table 8.1 provides the Distribution list for this Document. *Note: Complete the table.*

Table 8.1 Distribution List

Recipient Name	Recipient Organization	Distribution Method
Emily Reynolds	Comptia/Network Security Analyst	<i>Electronic Copy</i>
Michael Anderson	Comptia/IT Systems Administrator	<i>Electronic Copy</i>
Olivia Thompson	Comptia/Cybersecurity Engineer	<i>Electronic Copy</i>
Benjamin Matthews	Comptia/Information Security Officer	<i>Electronic Copy</i>
Sophia Roberts	Comptia/Incident Response Manager	<i>Electronic Copy</i>

APPENDICIES

Appendix A.

Lab 3.1.1 Passive Reconnaissance

PART A:

Shodan.com

172.65.218.150 - USA, San Francisco

TLSv1, TLSv1.1, TLSv1.2

DigiCert Inc

172.65.248.163 - USA, San Francisco "Possible"

TLSv1, TLSv1.1, TLSv1.2

DigiCert Inc

PART B:

Whois.com

2 Name Servers:

armando.ns.cloudflare.com

jade.ns.cloudflare.com

Creation date of the record:

1995-08-15

PART C:

NSLOOKUP:

Non-authoritative answer:

Name: comptia.org

Addresses: 2606:4700::6812:111d

2606:4700::6812:101d

104.18.16.29

104.18.17.29

PART D:

Dig in linux

—(timz@MyMachine)-[~]

└─\$ dig www.hackme.loc

; <<>> DiG 9.18.16-1-Debian <<>> www.hackme.loc

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 59662

;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 4096
;; QUESTION SECTION:
; www.hackme.loc.          IN      A

;; AUTHORITY SECTION:
.          5      IN      SOA      a.root-servers.net. nstld.verisign-grs.com. 2023071101 1800 900 604800 86400

;; Query time: 11 msec
;; SERVER: 192.168.157.2#53(192.168.157.2) (UDP)
;; WHEN: Tue Jul 11 18:50:41 CDT 2023
;; MSG SIZE rcvd: 118
```


Appendix A.

Lab 3.1.2 Social Engineering

The Malware link for Pepper Pots

VXNIcm5hbWU6IFBQb3R0cwpQYXNzd29yZDogSUxvdmVZb3UzMDAwIQ==

Credentials to analyze with Cyber Chef

VXNIcm5hbWU6IFBQb3R0cwpQYXNzd29yZDogSUxvdmVZb3UzMDAwIQ==

Username: SWilson

Password: OnYourLeft!

Appendix A.

Lab 3.1.3 Active Reconnaissance

PART A:

Potential targets in Metasploit

172.20.50.50
172.20.50.51
172.20.50.52
172.20.50.53
172.20.50.54
172.20.50.56

PART B:

Nmap scan potential targets

Nmap scan report for 172.20.50.10

Host: CYBER-DC

OS: Windows

(Note: Domain HackMe.loc0)

Nmap Scan report for 172.20.50.11

Host: DC

OS: Windows Server 2016

(Note services: kerberos-sec, kpasswd5, ldap.)

Nmap Scan report for 172.20.50.50

Host: no host name

OS: Linux (Ubuntu)

Nmap Scan report for 172.20.50.54

Host: metasploitable.localdomain

OS: Linux (Debian)

(Note: MySQL, Samba smbd, telnet)

Nmap Scan report for 172.20.50.104

Host: no host name

OS: Windows 10

Nmap Scan report for 172.20.50.52

Host: no host name

OS: Linux 2.6.x

(Note: services: xrdp)

Appendix A.

Lab 3.1.4 Network Enumeration

PART A:

#Telnet Probing

172.20.50.10

Vulnerable *

Web Server:

Microsoft IIS httpd 10.0

172.20.50.54

Vulnerable *

Web Server:

Apache httpd 2.2.8 ((Ubuntu) DAV/2)

Note Worthy:

Apache/2.2.8 (Ubuntu) DAV/2 Server at metasploitable.localdomain Port 80</address>

2 Hosts Vulnerable...

PART B:

#smb_enumshares exploit SMB scan with Metasploit

Rhost set to 172.20.50.10 for the Windows server

Scan results:

```
[ - ] 172.20.50.10:139    - Login Failed: Unable to negotiate SMB1 with the remote host: Not a valid SMB packet
[ * ] 172.20.50.10:445    - Windows 2019 (Unknown)
[ * ] 172.20.50.10:445    - No shares collected
[ * ] 172.20.50.10:      - Scanned 1 of 1 hosts (100% complete)
[ * ] Auxiliary module execution completed
```

SMB User credentials set to:

Username: SWilson

Password: OnYourLeft!

Scan results after credentials:

```
[ - ] 172.20.50.10:139    - Login Failed: Unable to negotiate SMB1 with the remote host: Not a valid SMB packet
[ * ] 172.20.50.10:445    - Windows 2019 (Unknown)
[ + ] 172.20.50.10:445    - ADMIN$ - (DISK) Remote Admin
[ + ] 172.20.50.10:445    - C$ - (DISK) Default share
[ + ] 172.20.50.10:445    - IPC$ - (IPC) Remote IPC
[ + ] 172.20.50.10:445    - NETLOGON - (DISK) Logon server share
[ + ] 172.20.50.10:445    - Private - (DISK)
```

```
[+] 172.20.50.10:445 - Public - (DISK) Public
[+] 172.20.50.10:445 - SYSVOL - (DISK) Logon server share
[*] 172.20.50.10: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

#smb_enumusers exploit SMB scan with Metasploit

Rhost set to 172.20.50.10

Scan results:

```
[*] 172.20.50.10: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Note Insufficient results. Proceeding with providing a valid account.

SMB User credentials set to:

Username: SWilson

Password: OnYourLeft!

Scan results after credentials:

```
[+] 172.20.50.10:445 - HACKME [ Administrator, Guest, krbtgt, dev, NRomanoff, PPotts, SWilson, WMaximoff,
BBanner, SRogers, WWilson, SLee, PBlart, SLang, TStark, SStrange, JHammer, CJanssen, PPhillips ] ( LockoutTries=0
PasswordMin=7 )
[*] 172.20.50.10: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Note New account user names discovered as well as Lockout tries is 0 and Passwordmin is set to 7.

PART C:

#Use nmap script to scan for SMB-related info on Metasploitable host:

Note Syntax used in nmap:

Nmap -script=smb-enum-shares 172.20.50.54

Scan results:

Nmap scan report for 172.20.50.54

Host is up (0.0023s latency).

Not shown: 978 closed ports

PORT STATE SERVICE

21/tcp open ftp

22/tcp open ssh

23/tcp open telnet

25/tcp open smtp

80/tcp open http

111/tcp open rpcbind

139/tcp open netbios-ssn

445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown

Host script results:

| smb-enum-shares:
| account_used: <blank>
| [\\172.20.50.54\ADMIN\\$](smb://172.20.50.54/ADMIN$):
| Type: STYPE_IPC
| Comment: IPC Service (metasploitable server (Samba 3.0.20-Debian))
| Users: 1
| Max Users: <unlimited>
| Path: C:\tmp
| Anonymous access: <none>
| [\\172.20.50.54\IPC\\$](smb://172.20.50.54/IPC$):
| Type: STYPE_IPC
| Comment: IPC Service (metasploitable server (Samba 3.0.20-Debian))
| Users: 1
| Max Users: <unlimited>
| Path: C:\tmp
| Anonymous access: READ/WRITE
| [\\172.20.50.54\opt](smb://172.20.50.54/opt):
| Type: STYPE_DISKTREE
| Comment:
| Users: 1
| Max Users: <unlimited>
| Path: C:\tmp
| Anonymous access: <none>
| [\\172.20.50.54\print\\$](smb://172.20.50.54/print$):
| Type: STYPE_DISKTREE
| Comment: Printer Drivers
| Users: 1
| Max Users: <unlimited>
| Path: C:\var\lib\samba\printers
| Anonymous access: <none>
| [\\172.20.50.54\tmp](smb://172.20.50.54/tmp):
| Type: STYPE_DISKTREE
| Comment: oh noes!

```
| Users: 1
| Max Users: <unlimited>
| Path: C:\tmp
|_ Anonymous access: READ/WRITE
```

Nmap done: 1 IP address (1 host up) scanned in 17.55 seconds

Recorded for comment in share \tmp:

```
\172.20.50.54\tmp:
| Type: STYPE_DISKTREE
| Comment: oh noes!
| Users: 1
| Max Users: <unlimited>
| Path: C:\tmp
|_ Anonymous access: READ/WRITE
```

#Nmap script smb-enum-users.nse

Results of script scan smb-enum-users.nse

Starting Nmap 7.91 (<https://nmap.org>) at 2023-07-12 00:55 CDT

Nmap scan report for 172.20.50.54

Host is up (0.0046s latency).

Not shown: 978 closed ports

PORT STATE SERVICE

```
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown
```

Host script results:

```
| smb-enum-users:
| METASPLOITABLE\backup (RID: 1068)
|   Full name: backup
|   Flags:    Account disabled, Normal user account
| METASPLOITABLE\bin (RID: 1004)
|   Full name: bin
|   Flags:    Account disabled, Normal user account
| METASPLOITABLE\bind (RID: 1210)
|   Flags:    Account disabled, Normal user account
| METASPLOITABLE\daemon (RID: 1002)
|   Full name: daemon
|   Flags:    Account disabled, Normal user account
| METASPLOITABLE\dhcp (RID: 1202)
|   Flags:    Account disabled, Normal user account
| METASPLOITABLE\distccd (RID: 1222)
|   Flags:    Account disabled, Normal user account
| METASPLOITABLE\ftp (RID: 1214)
|   Flags:    Account disabled, Normal user account
| METASPLOITABLE\games (RID: 1010)
|   Full name: games
|   Flags:    Account disabled, Normal user account
| METASPLOITABLE\gnats (RID: 1082)
|   Full name: Gnats Bug-Reporting System (admin)
|   Flags:    Account disabled, Normal user account
| METASPLOITABLE\irc (RID: 1078)
|   Full name: ircd
|   Flags:    Account disabled, Normal user account
| METASPLOITABLE\klog (RID: 1206)
|   Flags:    Account disabled, Normal user account
| METASPLOITABLE\libuuid (RID: 1200)
|   Flags:    Account disabled, Normal user account
| METASPLOITABLE\list (RID: 1076)
|   Full name: Mailing List Manager
|   Flags:    Account disabled, Normal user account
| METASPLOITABLE\lp (RID: 1014)
|   Full name: lp
|   Flags:    Account disabled, Normal user account
| METASPLOITABLE\mail (RID: 1016)
|   Full name: mail
|   Flags:    Account disabled, Normal user account
| METASPLOITABLE\man (RID: 1012)
|   Full name: man
|   Flags:    Account disabled, Normal user account
| METASPLOITABLE\msfadmin (RID: 3000)
|   Full name: msfadmin,,,
|   Flags:    Normal user account
| METASPLOITABLE\mysql (RID: 1218)
|   Full name: MySQL Server,,,
|   Flags:    Account disabled, Normal user account
```

```

| METASPLOITABLE\news (RID: 1018)
|   Full name: news
|   Flags:   Account disabled, Normal user account
| METASPLOITABLE\nobody (RID: 501)
|   Full name: nobody
|   Flags:   Account disabled, Normal user account
| METASPLOITABLE\postfix (RID: 1212)
|   Flags:   Account disabled, Normal user account
| METASPLOITABLE\postgres (RID: 1216)
|   Full name: PostgreSQL administrator,,,
|   Flags:   Account disabled, Normal user account
| METASPLOITABLE\proftpd (RID: 1226)
|   Flags:   Account disabled, Normal user account
| METASPLOITABLE\proxy (RID: 1026)
|   Full name: proxy
|   Flags:   Account disabled, Normal user account
| METASPLOITABLE\root (RID: 1000)
|   Full name: root
|   Flags:   Account disabled, Normal user account
| METASPLOITABLE\service (RID: 3004)
|   Full name: ,,,
|   Flags:   Account disabled, Normal user account
| METASPLOITABLE\sshd (RID: 1208)
|   Flags:   Account disabled, Normal user account
| METASPLOITABLE\sync (RID: 1008)
|   Full name: sync
|   Flags:   Account disabled, Normal user account
| METASPLOITABLE\sys (RID: 1006)
|   Full name: sys
|   Flags:   Account disabled, Normal user account
| METASPLOITABLE\syslog (RID: 1204)
|   Flags:   Account disabled, Normal user account
| METASPLOITABLE\telnetd (RID: 1224)
|   Flags:   Account disabled, Normal user account
| METASPLOITABLE\tomcat55 (RID: 1220)
|   Flags:   Account disabled, Normal user account
| METASPLOITABLE\user (RID: 3002)
|   Full name: just a user,111,,
|   Flags:   Normal user account
| METASPLOITABLE\uucp (RID: 1020)
|   Full name: uucp
|   Flags:   Account disabled, Normal user account
| METASPLOITABLE\www-data (RID: 1066)
|   Full name: www-data
|_  Flags:   Account disabled, Normal user account

```

Nmap done: 1 IP address (1 host up) scanned in 17.32 seconds

#Questions in #4 of part C:

Recorded results:

- A. Yes, there is an account named "nobody"
- B. Yes, there is an account named "www-data"
- C. No, there is NOT an account name "1337"

Appendix B. *Note. Label and separate each appendix on separate pages.*

Appendix C. *Note. Label and separate each appendix on separate pages.*

Appendix D. *Note. Label and separate each appendix on separate pages.*