

Active Information Gathering

Table of Contents

Executive Summary.....	3
Overview of issues.....	3
Business impact of issues.....	3
Metasploitable 2 Findings.....	4
Attack surface of open ports and services.....	4
Vulnerabilities discovered.....	5
Win7 Pen Test Findings.....	5
Attack surface of open ports and services.....	5
Vulnerabilities discovered.....	6
Recommendations.....	7
Tactical recommendations.....	7
Strategic recommendations.....	7
Methodology.....	8
Appendices.....	10
Bibliography.....	15

Executive Summary

Overview of issues

This report documents findings from active information gathering performed in a penetration test. The targets of the scans are Metasploitable 2 and Windows 7. The significant issues covered for each system are presented in relevant “Findings” sections, including an overview of open ports gathered from NMAP and Netcat scans. These overviews of attack surfaces are followed by analyses of vulnerabilities associated with each system, obtained from OpenVAS scans. Following these analyses, tactical recommendations are made, proposing suggestions such as upgrading software and closing ports. Strategic recommendations are then suggested, to provide tangible steps to improve the security posture of these systems. Finally, the steps taken to conduct this analysis are covered in a methodology section, followed by specific findings displayed in relevant appendices.

Business impact of issues

The impact of these issues are crucial. Some of the issues presented in this report include vulnerabilities such as open ports, weak encryption, outdated software, and susceptible applications across both systems. Malicious actors may exploit these vulnerabilities to gain unauthorized access to sensitive information, and may either tamper existing data or continue to passively monitor incoming data in each system. Protecting against these threats will ensure organizational success to a high extent by creating a lower attack surface. Continued vigilance is an essential cornerstone of a strong cybersecurity policy, and this report suggests important steps which must be taken to protect against attacks.

Metasploitable 2 Findings

Attack surface of open ports and services

From the port scan in Appendix 1.1 and Appendix 1.2, several open ports are identified. While open ports are not inherent vulnerabilities in the system, they may offer attackers points of entry into a system if unmonitored. Port 21 is a file transfer protocol (FTP) port that allows users to send and receive files from servers (Schrader). This protocol is insecure, and can be exploited by attackers through brute-forcing passwords, or through anonymous authentication such as using “anonymous” as the username and password. Port 22 can be exploited through leaked SSH keys or brute forced credentials; however, this port is less susceptible to attacks. Port 23 is the default Telnet port; since Telnet has been succeeded by SSH and is considered outdated, it may be vulnerable to brute forcing or credential sniffing attacks (Speedguide). Port 53 handles DNS, and as a result may increase the likelihood of DDoS attacks, or DNS amplification attacks.

Port 80 is an unencrypted port, which may leave an open door and clear data for attackers to exploit in order to gain and retain access to the system. Port 111 is open; it may be dangerous to leave this port open, particularly if this service is opened to the internet. An attacker may, in this circumstance, query information related to this port without needing to authenticate themselves. Port 139 is also open, and is utilized by the NetBIOS Session service (manageengine). Having this port open could lead to shared resources such as files being accessed by any entity across the internet, resulting in a scope for attack. This vulnerability is shared with leaving Port 445 open as well.

Vulnerabilities discovered

Many high-severity vulnerabilities were discovered upon completing the OpenVAS scan of the Metasploitable 2 machine. A sample of these vulnerabilities are included in Appendix 2.2. The operating system on this device is past its end of life, opening the system up to a host of vulnerabilities. A lack of security updates and patches would expose this system to increasingly sophisticated attacks, with little to no means to defend. A backdoor installed on the remote host was also identified, which may provide an attacker with a means to re-enter the system, allowing that attacker to launch new attacks or gain information passively. The Twiki software is being used on this system, a software susceptible to cross-site scripting. An attacker who exploits this vulnerability will be able to execute arbitrary code, and this vulnerability can be addressed by upgrading the Twiki software. Additionally, a source package, vsftpd, is used in this system. This source code contains a backdoor which opens a shell on Port 6200.

The Appendix 2.2 includes a list of ports associated with vulnerabilities, ranked in descending order from high to medium severity and scored on a scale of 1-10. These ports should be hardened, and closed if necessary, to decrease the threats posed against the system. Three applications, also documented in the Appendix, are identified as high-severity vulnerabilities. Upgrading the operating system would ensure these applications are patched.

Win7 Pen Test Findings

Attack surface of open ports and services

Several open ports are detected in the Windows 7 machine. Port 135 may pose security vulnerabilities in the event it is exposed to the internet, but is otherwise considered a port safe to remain open on the internal network. The vulnerability with Port 139 being open is covered in

the previous section; this open port is a commonality between both the Metasploitable 2 and Windows 7 machines. Port 445 should also remain closed to external networks, and the vulnerability associated with keeping this port open is shared with Port 139. Other attack surfaces revealed in Appendix 2.2 include open ports which do not have major associated security vulnerabilities, other than Port 3389 which is associated with the TLSv1.0 protocol. This open port may be vulnerable to man-in-the-middle attacks.

Vulnerabilities discovered

A wide range of vulnerabilities were discovered using OpenVAS. Four high-severity, three medium-severity, and two low-severity vulnerabilities were identified and included in Appendix 2.2. The most prominent vulnerability is that the host operating system, Windows 7, has reached its end of life. A host of security concerns arise when considering the vulnerabilities associated with using an operating system past its end of life. The second high-severity vulnerability discovered was the ability to gain access via the SMB protocol (Ports 139 and 445) using user:user credentials, also documented in Appendix 2.2. This vulnerability confirms the need to close Ports 139 and 445. The third high-severity vulnerability detected lent insight into errors in input validation while processing SMB errors, and a lacking cryptography entropy existing during SMB authentication, allowing for the authentication mechanism to be bypassed. The most important step in addressing this vulnerability is to upgrade the operating system, as it is not present in modern Windows operating systems.

Some additional vulnerabilities present included weak cipher suites such as RC4 in place in the TLSv1.0 protocol, associated with open Port 3389 identified in the port scan. Furthermore, cryptographically weak hashing algorithms were detected in the SSL/TLS certificate chain of the service.

In contrast to the Metasploitable 2 machine, only three ports in the Windows 7 system are identified as vulnerable, with only one port, Port 445, marked as a high severity vulnerability. No vulnerable applications were detected.

Recommendations

Tactical recommendations

The first, and most important, recommendation suggested is to upgrade the operating systems of both systems. Since both operating systems have reached (and extended past) their end-of-lives, upgrading to newer operating systems will lower the attack surface significantly since the manufacturer of each operating system will provide periodic security patches and software updates. With new threats constantly surfacing, attackers are able to exploit vulnerable systems. The Windows 7 system must be upgraded in order to avoid incidents such as the WannaCry ransomware attack, for instance, which targeted systems running on outdated Windows software.

The next recommendation is to close Ports 139 and 445. These ports are identified as open in both systems, and result in high-severity vulnerabilities in both systems as well. Additional open ports, particularly in the Metasploitable 2 system, marked as open in Appendix 1.2 or high-severity in Appendix 2.2 should be reviewed and closed unless their need to remain open can be adequately justified. A whole cleanup of both systems is also recommended.

Strategic recommendations

In addition to upgrading the operating systems of both the Windows 7 and Metasploitable 2 machines, it is highly recommended for periodic upgrades to take place moving forward. Once

Windows 7 is upgraded to an updated software, Microsoft's monthly Patch Tuesday program will ensure critical security updates are provided to the system automatically.

It is also recommended for frequent security audits to take place, examining open ports, packet captures, and vulnerabilities. As mentioned, while there is no risk with a port simply being open, there is a high risk in keeping a port without understanding the risks and vulnerabilities, and the types of attacks, that specific port is susceptible to. Performing regular security audits will ensure that attempts to exploit these ports and vulnerabilities are detected.

Encrypting data and protecting against brute-force attacks, by implementing input validation and sanitization frameworks, will also significantly lower the vulnerabilities associated with both systems, and particularly the Metasploitable 2 system.

Methodology

For both the Metasploitable 2 and Windows 7 tests, insights were drawn in accordance with the following methodology:

1) Bash script: the `./ping.sh` command was used to perform a ping to each virtual machine. This was used to verify connection between the Kali Linux machine and the two machines from which we intended to gather information. The following commands were used:

```
vi ping.sh
```

```
ping 127.0.0.1 (for Metasploitable 2)
```

```
ping 192.168.64.7 (for Windows 7)
```

```
Press esc, then type :wq
```

```
./ping.sh
```


2) Nmap: the following commands were used to launch Nmap scans on each machine from the Kali Linux command line, run simultaneously with Wireshark to perform packet captures:

```
sudo apt-get install nmap
```

```
nmap 127.0.0.1 (Metasploitable 2)
```

```
nmap 192.168.64.7 (Windows 7)
```

3) NetCat: the following NC commands were used:

```
nc -v -n -z -w1 127.0.0.1 100-1000
```

```
nc -v -n -z -w1 192.168.64.7
```

4) OpenVAS: OpenVAS was used to identify vulnerabilities in targets. Since the GUI was used, the commands run are not included in this section; the only commands used were to set up the GUI, which was then used to generate a report on the vulnerabilities associated with each system. After being set up, the scan was eventually run using the command `sudo gvm-start`.

Appendices

Appendix 1.1: Metasploitable 2 port scan

```
Enter a remote host to scan: 192.168.28.116
Please wait, scanning remote host 192.168.28.116
Port 21: Open
Port 22: Open
Port 23: Open
Port 25: Open
Port 53: Open
Port 80: Open
Port 111: Open
Port 139: Open
Port 445: Open
Port 512: Open
Port 513: Open
Port 514: Open
Scanning Completed in: 0:00:00.527641
```

Appendix 1.2: Windows 7 port scan

```
(kali@kali)-[~]
$ nmap 192.168.64.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-04 23:30 EST
Nmap scan report for 192.168.64.7
Host is up (0.00030s latency).
Not shown: 986 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
554/tcp    open  rtsp
2869/tcp   open  iclslap
3389/tcp   open  ms-wbt-server
5357/tcp   open  wsdapi
10243/tcp  open  unknown
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
49157/tcp  open  unknown
Nmap done: 1 IP address (1 host up) scanned in 1.98 seconds
```

Appendix 1.3: Windows 7 Netcat scan













```
(kali㉿kali)-[~]  
$ nc -v -n -z -w1 192.168.64.7 10-1000  
(UNKNOWN) [192.168.64.7] 554 (rtsp) open  
(UNKNOWN) [192.168.64.7] 445 (microsoft-ds) open  
(UNKNOWN) [192.168.64.7] 139 (netbios-ssn) open  
(UNKNOWN) [192.168.64.7] 135 (epmap) open
```

Appendix 1.4: Metasploitable 2 NetCat scan

```
(kali㉿kali)-[~]  
$ nc -v -n -z -w1 192.168.1.94 10-1000  
(UNKNOWN) [192.168.1.94] 514 (shell) open  
(UNKNOWN) [192.168.1.94] 513 (login) open  
(UNKNOWN) [192.168.1.94] 512 (exec) open  
(UNKNOWN) [192.168.1.94] 445 (microsoft-ds) open  
(UNKNOWN) [192.168.1.94] 139 (netbios-ssn) open  
(UNKNOWN) [192.168.1.94] 111 (sunrpc) open  
(UNKNOWN) [192.168.1.94] 80 (http) open  
(UNKNOWN) [192.168.1.94] 53 (domain) open  
(UNKNOWN) [192.168.1.94] 25 (smtp) open  
(UNKNOWN) [192.168.1.94] 23 (telnet) open  
(UNKNOWN) [192.168.1.94] 22 (ssh) open  
(UNKNOWN) [192.168.1.94] 21 (ftp) open
```















Appendix 2.1: Metasploitable 2 OpenVAS

A sample of results are included below

Vulnerability		Severity ▾	QoD	Host IP	Name	Location	Created
Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities		10.0 (High)	99 %	192.168.1.94		8787/tcp	Tue, Mar 5, 2024 4:45 AM UTC
Operating System (OS) End of Life (EOL) Detection		10.0 (High)	80 %	192.168.1.94		general/tcp	Tue, Mar 5, 2024 4:43 AM UTC
Possible Backdoor: Ingreslock		10.0 (High)	99 %	192.168.1.94		1524/tcp	Tue, Mar 5, 2024 4:47 AM UTC
TWiki XSS and Command Execution Vulnerabilities		10.0 (High)	80 %	192.168.1.94		80/tcp	Tue, Mar 5, 2024 4:44 AM UTC
vsftpd Compromised Source Packages Backdoor Vulnerability		9.8 (High)	99 %	192.168.1.94		21/tcp	Tue, Mar 5, 2024 4:46 AM UTC
vsftpd Compromised Source Packages Backdoor Vulnerability		9.8 (High)	99 %	192.168.1.94		6200/tcp	Tue, Mar 5, 2024 4:46 AM UTC
DistCC RCE Vulnerability (CVE-2004-2687)		9.3 (High)	99 %	192.168.1.94		3632/tcp	Tue, Mar 5, 2024 4:45 AM UTC
VNC Brute Force Login		9.0 (High)	95 %	192.168.1.94		5900/tcp	Tue, Mar 5, 2024 4:44 AM UTC
PostgreSQL Default Credentials (PostgreSQL Protocol)		9.0 (High)	99 %	192.168.1.94		5432/tcp	Tue, Mar 5, 2024 4:45 AM UTC
UnrealIRCd Authentication Spoofing Vulnerability		8.1 (High)	80 %	192.168.1.94		6697/tcp	Tue, Mar 5, 2024 4:30 AM UTC
UnrealIRCd Backdoor		7.5 (High)	70 %	192.168.1.94		6697/tcp	Tue, Mar 5, 2024 4:46 AM UTC

Greenbone

Security Assistant

Dashboards	Scans	Assets	Resilience	SecInfo	Configuration	Administration	Help
Twiki Cross-Site Request Forgery Vulnerability (Sep 2010)		<div><div>6.8 (Medium)</div></div>	80 %	192.168.1.94		80/tcp	Tue, Mar 5, 2024 4:44 AM UTC
Anonymous FTP Login Reporting		<div><div>6.4 (Medium)</div></div>	80 %	192.168.1.94		21/tcp	Tue, Mar 5, 2024 4:30 AM UTC
jQuery < 1.9.0 XSS Vulnerability		<div><div>6.1 (Medium)</div></div>	80 %	192.168.1.94		80/tcp	Tue, Mar 5, 2024 4:44 AM UTC
Twiki Cross-Site Request Forgery Vulnerability		<div><div>6.0 (Medium)</div></div>	80 %	192.168.1.94		80/tcp	Tue, Mar 5, 2024 4:44 AM UTC
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection		<div><div>5.9 (Medium)</div></div>	98 %	192.168.1.94		25/tcp	Tue, Mar 5, 2024 4:34 AM UTC
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection		<div><div>5.9 (Medium)</div></div>	98 %	192.168.1.94		5432/tcp	Tue, Mar 5, 2024 4:34 AM UTC
SSL/TLS: Report Weak Cipher Suites		<div><div>5.9 (Medium)</div></div>	98 %	192.168.1.94		5432/tcp	Tue, Mar 5, 2024 4:34 AM UTC
Check if Mailserver answer to VRFY and EXPN requests		<div><div>5.0 (Medium)</div></div>	99 %	192.168.1.94		25/tcp	Tue, Mar 5, 2024 4:34 AM UTC
SSL/TLS: Certificate Expired		<div><div>5.0 (Medium)</div></div>	99 %	192.168.1.94		25/tcp	Tue, Mar 5, 2024 4:33 AM UTC
SSL/TLS: Certificate Expired		<div><div>5.0 (Medium)</div></div>	99 %	192.168.1.94		5432/tcp	Tue, Mar 5, 2024 4:33 AM UTC
awiki <= 20100125 Multiple LFI Vulnerabilities - Active Check		<div><div>5.0 (Medium)</div></div>	99 %	192.168.1.94		80/tcp	Tue, Mar 5, 2024 4:47 AM UTC
VNC Server Unencrypted Data Transmission		<div><div>4.8 (Medium)</div></div>	70 %	192.168.1.94		5900/tcp	Tue, Mar 5, 2024 4:31 AM UTC
FTP Unencrypted Cleartext Login		<div><div>4.8 (Medium)</div></div>	70 %	192.168.1.94		21/tcp	Tue, Mar 5, 2024 4:30 AM UTC
FTP Unencrypted Cleartext Login		<div><div>4.8 (Medium)</div></div>	70 %	192.168.1.94		2121/tcp	Tue, Mar 5, 2024 4:30 AM UTC
Cleartext Transmission of Sensitive Information via HTTP		<div><div>4.8 (Medium)</div></div>	80 %	192.168.1.94		80/tcp	Tue, Mar 5, 2024 4:43 AM UTC

Greenbone Security Assistant (GSA) Copyright © 2009-2023 by Greenbone AG, www.greenbone.org

Vulnerable ports:

Information	Results (45 of 388)	Hosts (1 of 1)	Ports (13 of 23)	Applications (16 of 16)	Operating Systems (1 of 1)	CVEs (21 of 21)	Closed CVEs (0 of 0)	TLS Certificates (2 of 2)	Error Messages (0 of 0)	User Tags (0)	
<div>⏪ ⏩ 1 - 13 of 13 ⏪ ⏩</div>											
Port						Hosts					Severity ▼
80/tcp						1					10.0 (High)
1524/tcp						1					10.0 (High)
8787/tcp						1					10.0 (High)
21/tcp						1					9.8 (High)
6200/tcp						1					9.8 (High)
3632/tcp						1					9.3 (High)
5432/tcp						1					9.0 (High)
5900/tcp						1					9.0 (High)
6697/tcp						1					8.1 (High)
25/tcp						1					6.8 (Medium)
23/tcp						1					4.8 (Medium)
2121/tcp						1					4.8 (Medium)
22/tcp						1					4.3 (Medium)
<div>⏪ ⏩ 1 - 13 of 13 ⏪ ⏩</div>											
<div>(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort=reverse=severity)</div>											

Vulnerable Applications:

Information	Results (45 of 388)	Hosts (1 of 1)	Ports (13 of 23)	Applications (16 of 16)	Operating Systems (1 of 1)	CVEs (21 of 21)	Closed CVEs (0 of 0)	TLS Certificates (2 of 2)	Error Messages (0 of 0)	User Tags (0)
										1 - 16 of 16
Application CPE										Severity ▼
cpe:/a:beasts:vsftpd:2.3.4	1									9.8 (High)
cpe:/a:postgresql:postgresql:8.3.1	1									9.0 (High)
cpe:/a:unrealircd:unrealircd:3.2.8.1	1									8.1 (High)
cpe:/a:apache:http_server:2.2.8	1									4.3 (Medium)
cpe:/a:mysql:mysql:5.0.51a	1									N/A

Appendix 2.2: Windows 7 OpenVAS

Vulnerability	Severity ▼	QoD	Host IP	Name	Location	Created
Operating System (OS) End of Life (EOL) Detection	10.0 (High)	80 %	192.168.64.7		general/tcp	Tue, Mar 5, 2024 3:51 AM UTC
SMB Brute Force Logins With Default Credentials	10.0 (High)	99 %	192.168.64.7		445/tcp	Tue, Mar 5, 2024 4:05 AM UTC
Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)	10.0 (High)	98 %	192.168.64.7		445/tcp	Tue, Mar 5, 2024 4:09 AM UTC
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)	8.1 (High)	95 %	192.168.64.7		445/tcp	Tue, Mar 5, 2024 4:09 AM UTC
SSL/TLS: Report Weak Cipher Suites	5.9 (Medium)	98 %	192.168.64.7		3389/tcp	Tue, Mar 5, 2024 3:57 AM UTC
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80 %	192.168.64.7		135/tcp	Tue, Mar 5, 2024 4:05 AM UTC
SSL/TLS: Certificate Signed Using A Weak Signature Algorithm	4.0 (Medium)	80 %	192.168.64.7		3389/tcp	Tue, Mar 5, 2024 3:57 AM UTC
TCP Timestamps Information Disclosure	2.6 (Low)	80 %	192.168.64.7		general/tcp	Tue, Mar 5, 2024 3:51 AM UTC
ICMP Timestamp Reply Information Disclosure	2.1 (Low)	80 %	192.168.64.7		general/icmp	Tue, Mar 5, 2024 3:51 AM UTC



Summary

A number of known default credentials are tried for the login via the SMB protocol.

Detection Result

It was possible to login with the following credentials via the SMB protocol to the 'IPC\$' share. <User>:<Password>

User:user

Detection Method

Tries to login with a number of known default credentials via the SMB protocol.

Details: [SMB Brute Force Logins With Default Credentials OID: 1.3.6.1.4.1.25623.1.0.804449](#)

Version used: 2024-02-09T14:47:30Z

Solution

Solution Type: ↶ Mitigation
Change the password as soon as possible.

References

- CVE [CVE-1999-0503](#)
[CVE-1999-0504](#)
[CVE-1999-0505](#)
[CVE-1999-0506](#)
[CVE-2000-0333](#)

Greenbone Security Assistant (GSA) Copyright (C) 2009-2024

Vulnerable Ports:

⏪ ⏩ 1 - 3 of 3 ⏪ ⏩		
Port	Hosts	Severity ▼
445/tcp	1	10.0 (High)
3389/tcp	1	5.9 (Medium)
135/tcp	1	5.0 (Medium)
(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort=reverse=severity)		
⏪ ⏩ 1 - 3 of 3 ⏪ ⏩		

Bibliography

“How to Disable NetBIOS Port 139 (TCP) | NetBIOS Session Service.” *Manage Engine*, Zoho, www.manageengine.com/vulnerability-management/misconfiguration/windows-firewall/how-to-disable-netbios-port-139-tcp-netbios-session-service.html#:~:text=Port%20139%20is%20utilized%20by,port%20139%20in%20the%20Firewall. Accessed 5 Mar. 2024.

Schrader, Dirk. “Open Port Vulnerabilities List.” *Netwrix*, Netwrix Corporation, 4 Aug. 2022, [blog.netwrix.com/2022/08/04/open-port-vulnerabilities-list/#:~:text=Ports%2020%20and%201%20\(FTP,Brute%2Dforcing%20passwords](https://blog.netwrix.com/2022/08/04/open-port-vulnerabilities-list/#:~:text=Ports%2020%20and%201%20(FTP,Brute%2Dforcing%20passwords).

SpeedGuide. “Port 21 (TCP/UDP).” *SpeedGuide*, Speed Guide, Inc., www.speedguide.net/port.php?port=21. Accessed 5 Mar. 2024.