**Information on Writing a White Paper[[1]](#footnote-1) and Use of this Document**

**“A white paper is a persuasive essay that uses facts and logic to promote a certain product, service, or viewpoint**.”[[2]](#footnote-2) In this case you are promoting what you have done in your coursework.

* Remember **do** **not** **to write in the first person** in any section of your report.
* All sections should be numbered.
* Any Figures should be numbered. E.g. Figure 1: Showing xxx

**How to use this form:**

This document is a template. You shouldchange the content under the sub-headers and replace it with your own material if you think it is necessary.

**Checklist before you submit your white paper:**

* Proof read your document and use the spell/grammar check and correct any mistakes
* Check the format, e.g. are any images, tables, diagrams legible etc.
* Check whether your white paper looks professional, there should not be large areas of white space; spacing is consistent etc.
* Make sure you refer to figures, tables and references in the body of the text.(see Appendix C for examples for the format of figures and tables)



|  |
| --- |
| **Investigation and penetration testing of Network**  *Searching and utilising vulnerabilities and exploits on older Active Directory software and systems.*  **Adam Board**  CMP210: Ethical Hacking 1  2021/22 |

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

Abstract (not more than around 400 words)

This paper was created for an organisation to conduct a penetration test to gain access to their inner systems. There are two servers and a client on the network, with credentials to client being provided to the penetration tester. This account is a standard level account with the aim that, from here the system should be penetrated and full unrestrained access should be obtained. Once successful provide findings and recommendations to the company.

A full penetration test was conducted within scope given to the penetration tester. The test had four different stages: Scanning the system for services and open ports, Enumerating the services found to search for any vulnerabilities, searching for user groups and the password policy, Exploiting the known vulnerabilities to breach the server and escalate to administrator and, finally, Post exploitation where the general discussion and recommendations will be for actions going forwards. Each section goes in depth for each of the tools used with information about each tool and why it was used. Nessus was provided by the organisation for vulnerability scanning to assist in the process of finding vulnerabilities.

The results found from the penetration test were that this network in completely insecure and had multiple vulnerabilities. Furthermore, the organisations password policy was far under the standard that a company should have for passwords. From the gathered information, if an attacker was to breach their systems it would not be complicated to escalate to administrator and gain persistence on the server. The recommendations given were to patch the software and services, update the firewall and windows defender and implement a strict password policy, with passwords that need to be changed every month. The company should look to invest in training the security team or hiring an external security team to deal with these security issues, as it would benefit them more since the financial costs of having their network breached would far excel the costs of hiring or training a security team.

Contents

[1 Introduction 1](#_Toc82239455)

[1.1 Background 1](#_Toc82239456)

[1.2 Aim 1](#_Toc82239457)

[2 Procedure 2](#_Toc82239458)

[2.1 Overview of Procedure 2](#_Toc82239459)

[2.2 Sub-Heading 2](#_Toc82239460)

[3 Discussion 4](#_Toc82239461)

[3.1 General Discussion 4](#_Toc82239462)

[3.2 Countermeasures 4](#_Toc82239463)

[3.3 Future Work 4](#_Toc82239464)

[References 5](#_Toc82239465)

[Appendices 7](#_Toc82239466)

[Appendix A 7](#_Toc82239467)

[Appendix B 7](#_Toc82239468)

[Appendix C - Suggestions for formatting figures/tables/screenshots in the body of the text 7](#_Toc82239469)

# Introduction

## Background

E-commerce takes up at least 13-14% of all retail sales in the United States and has risen to a third of all retail sales in the United Kingdom (smartinsights, 2021). From just these statistics alone, the impact that E-Commerce has had on the world of business is apparent, which is why cyber-security has become essential to every business that is on the internet. That’s where penetration tests come in.

The National Cyber Security Centre (NCSC) describes Penetration testing as “a method for gaining assurance in your organisation's vulnerability assessment and management processes, not as a primary method for identifying vulnerabilities” (ncsc.gov, 2022) or in other words, an ethical hacker will act as a black-hat hacker and attempt to breach the businesses network. Vulnerabilities occur through software that is not regularly updated to latest patches by the security or development team, misconfigurations occur in the initial setup of networks and software when default settings have not been changed (like passwords) and security options are left unticked (SMB signing).

Penetration testing is important due to the frequency of black hat attacks, since there is a new attack on the internet every 39 seconds (2,244 breaches every day) (techJury, 2022). Even one of these attacks could be enough to put a small business out of work and could significantly harm a medium to large sized business.

These Tests are carried out because there will always be black-hat hackers that want to disrupt businesses or institutes for varied reasons including financial, political or malice; A real-world showcase of the severity black-hat hackers cause is WannaCry Ransomware, which was used against the NHS to take complete control of all user access to the systems (The WannaCry attack cost the NHS £92 million) (Health Executive webpage, 2018). For this reason, the tests allow for these critical vulnerabilities to be found and patched by the security team before a catastrophic event can even occur. However, if they cannot be fixed, then the security will have extensive monitoring on the service that has this unfixable vulnerability.

One of the earliest recorded penetration tests was in 1972 by James P. Anderson, where he outlined steps that had to be taken by a group known as tiger team to ensure a thorough test was being done to test the system’s resilience and security. The first steps included identifying the vulnerability and afterwards designing an attack based on that vulnerability. Even today, this fundamental method is continuously used as the backbone of penetration tests (infosecinstitute, 2019).

## Aim

A small organisation has requested a penetration test on their network to evaluate the security level of their network and systems.

This Active Directory network consists of two servers (192.168.10.1 and 192.168 10.2) and a client (192.168.10.10), for this scenario of the network, access has been given to client to simulate a network breach of a low privilege account. To call this penetration test successful both servers need to be exploited and have access to privileges of SYSTEM and Administrator, which will most likely be through a horizontal privilege escalation into a vertical privilege escalation depending on the vulnerability.

For the penetration test, the firstbase techie’s methodology is being used as a guideline to follow to assist the process of getting to SYSTEM privilege; It starts off with Footprinting, which does not need to be done because, as mentioned before, access is already granted to the client machine. The next step is Scanning, the active recon stage. At this stage, information about ports, services and the OS are scanned so all attack vectors can be looked upon and further investigated for what they do and whether those services have any vulnerabilities in them in the Enumeration stage.

Once all the Enumeration is done, the System Hacking phase can begin, this is where all scanning comes into use to exploit the vulnerabilities that were found within the services. Once the exploits have been exploited and system access has been accomplished to the point of being within server1, these exploits can be taken to the advanced phase where access to either Administrator or SYSTEM is obtained and allow to gather all the data that resides within the two servers. Once all of this is complete, the feedback stage will take place.

All the information that has been gathered will be transferred to the company with step by steps of how each exploitation happened and a possible way of patching the vulnerability or advice if unsure of how to fix it.

# Procedure

## Overview of Procedure

The penetration test made use of the Firstbase Techies methodology as its basic structure, the methodology consists of 5 separate stages; Footprinting, Scanning, Enumeration, System Hacking, and finally “Advanced” stage which, going forward, will be known as essentially the post-Exploitation stage.

While these are the main headings for each stage, they have been broken down into separate sub-headings depending on the stage, the Scanning stage has been broken down into its different tools that are being used and System Hacking will be broken down into two categories, exploiting vulnerabilities to gain unauthorised access to both servers and exploiting vulnerabilities to achieve privilege escalation to a user with more permissions.

The first stage was Footprinting, which for this penetration test was out of scope since the tester had complete access to the client already. In Footprinting, normally social engineering and physically searching the perimeters either in person or on google maps would be carried out. It can even be going to a café where an employee goes to and listening in on their conversations or looking at their screen over their shoulder.

With Footprinting completed next comes Scanning. The tester at this stage started to scan the ports through Nmap and HPing3 to find any services that are on open facing ports. This was used to discover what they needed to be able to allow them to do further scanning.

Now that Scanning was finished, Enumeration came next. The best tool for this process was Nessus and Metasploit’s Searchsploit since these allowed quick searching of what exploits would work with the versions that were found.

Now that all the exploits were found it was time to begin exploiting them in the System Hacking stage. The tester was now ready to start acting upon those found exploits. Using Metasploit allowed the attacks to be done automatically without having the code being rewritten to another language which would’ve taken too much time for the tester in the short timeframe that was given to do Proof of Concept coding.

The final stage that the tester has done was the Post-Exploit Stage, where all the exploits that have been successful have been discussed and evaluated so the company could look at to work on these if they chose to act on the information that was given to them.

## Footprinting

While footprinting was out of scope for this penetration test, it is still crucial to discuss what would have taken place if it was in scope of the test. The penetration tester would have done research through google maps about the building itself where the servers are kept or where the employees go to work, then an in person investigation would have taken place and a set of OSINT tools would have been used to investigate all the employees that could be seen going in and out of the building during the in-person investigation; OSINT tools would be used to search through their social medias, emails, work accounts and any other information they put on the internet. Social engineering techniques could have been attempted as well to gain access to a low-level account; Techniques like phishing, whaling, and tailing may have been used if they were in scope of the project.

Phishing is when a fraudulent message like an email is sent to one of the employees which could have malware that gives a reverse shell to the machine they work on, which in turn would have given the tester access to the client machine they have access to now.

Whaling is when a higher-up in the company is targeted for phishing attempts since they could have access to an admin account or secretive information could accidentally be leaked by them in. If this had been attempted and was successful, higher level of privilege could have been a starting point which would lead to an easier time exploiting the entire active directory network.

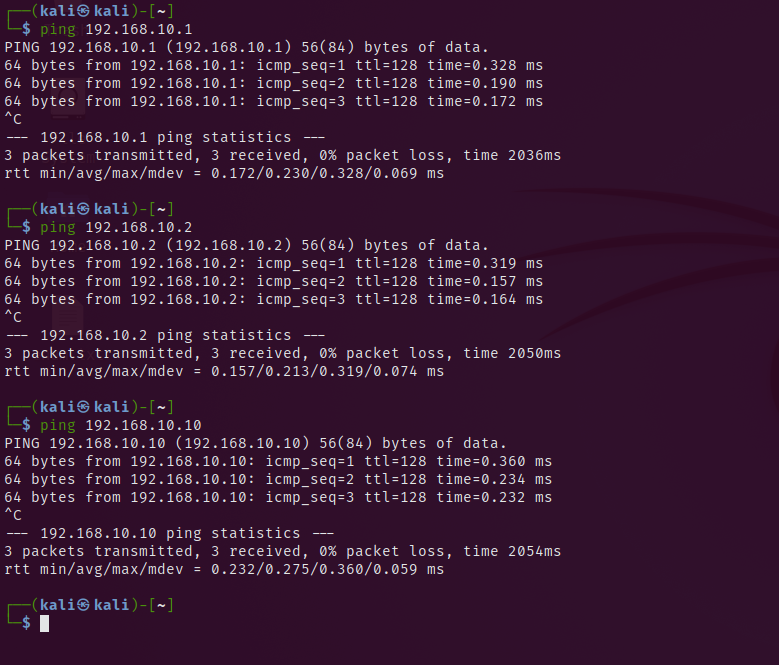
Tailing could be the tester dressed up in similar work attire and following an employee through the physical front doors of the building until they can get access to an unlocked pc when someone has gone away to the bathroom or on lunch break for example. This technique is preying on human decency to hold doors for other people as a physical weakness to company security.

This alone can reveal the scale of a company and what kind of security measures they have in place physically, which can sometimes help give an estimation for the tester on how hight their security will be virtually as well. This will not always be the case however.

## Scanning

Scanning is the first stage of the penetration test and with it being the starting point, the tester had made the decision to first ensure the system is online and ready to be penetrated. So, the tester used the PING command on Kali Linux; Ping sends a packet to the IP address that was included in the command and requests a packet back for the attacking machine to receive.

ping 192.168.10.1, ping 192.168.10.2, and ping 192.168.10.10



(Figure 1 – Replies from ping command from all machines)

The tester was certain that all machines on the network were live and ready for testing. It was then time to scan for information other than the system being live.

This section has been broken down to the two main tools used and the file shares manual searching method.

The tester used the credentials given for accessing client1 and begun to investigate the file shares as these could have had information relating to usernames or possible passwords for Enumeration or System Hacking further down the line.

To do this, the tester typed \\<IP Address> inside of the file explorer search bar to gain access to the file shares on the servers. Then the shares were searched thoroughly.

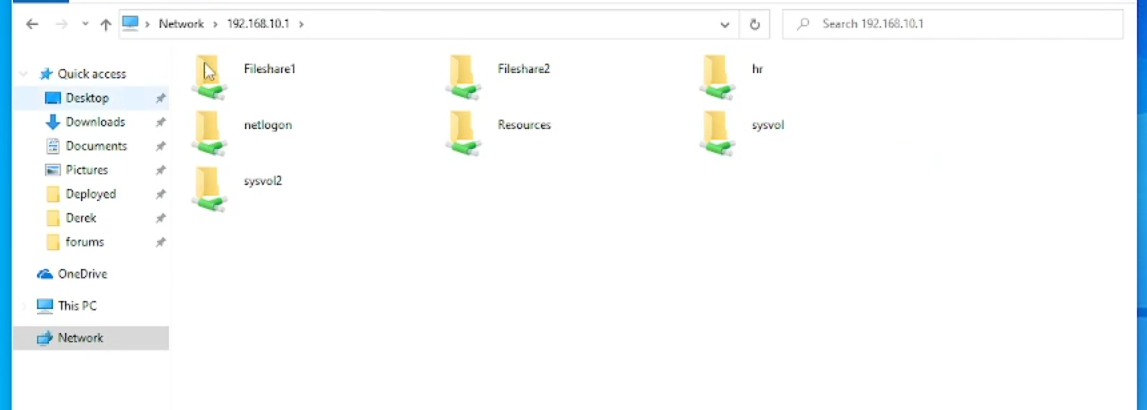
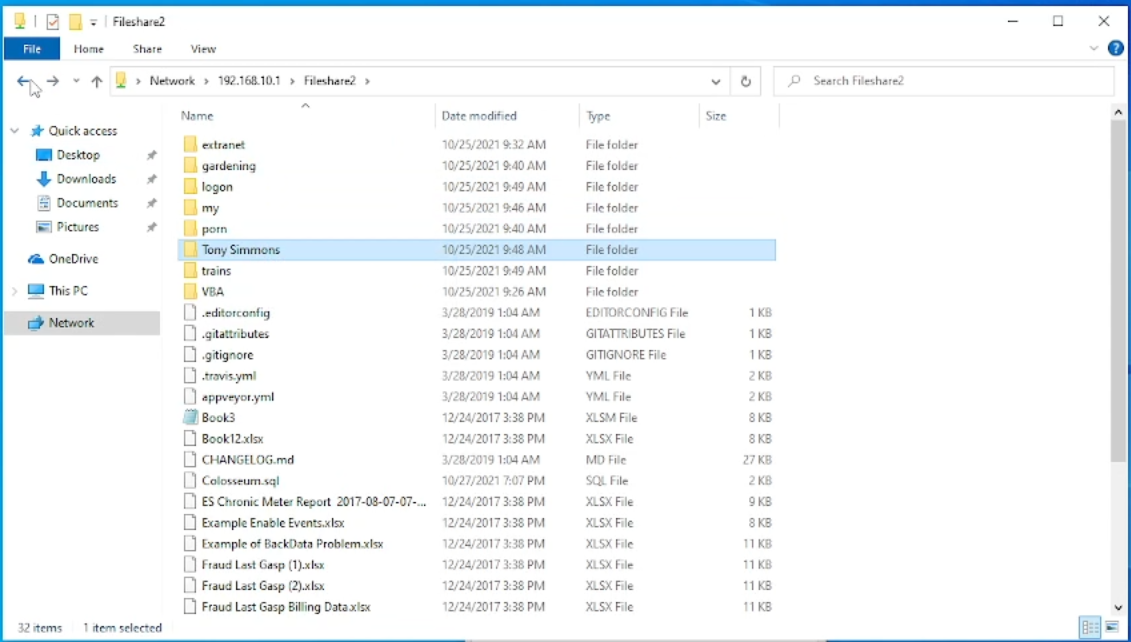


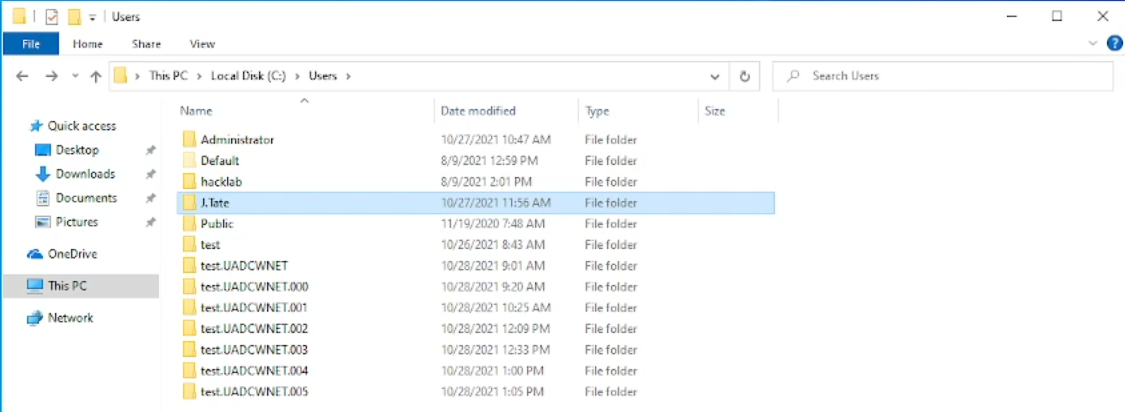
Figure 2 – all the file shares were in 192.168.10.1)

The best places to check were FileShare1 and FileShare2 since this is where the lower privilege level employees would be able to share information with each other, so it wouldn’t be out of the realm of reality for an accidental password or username slip throughout the files here.



(Figure 3 – Tony Simmons username found in fileshare2)

After only going inside of FileShare2 There was a folder named Tony Simmons which seems like the name of one of the workers on this network. Once going through the rest of the file shares and no useful information was found regarding the penetration test was completed, the next place that was beneficial to go to would be the Users folder to find out who logged onto this machine during work hours.



(Figure 4 – J.Tate, Administrator and other usernames were found in the Users folder of client1)

Inside of the Users folder two usernames were found, Administrator J.Tate. The layout of usernames was discovered as well, so now there was a known format for usernames in the company; So to turn Tony Simmons into a user name it then became T.Simmons.

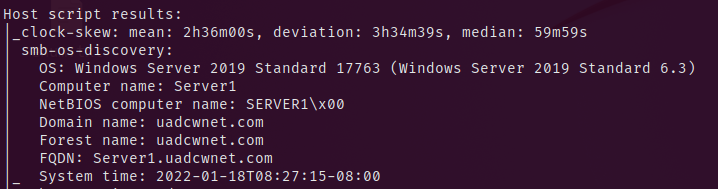
Once all the shares had been looked into in server1, server2 and client1, three usernames stuck out to the tester as these would most likely be usernames which could be used for the server: J.Tate, T.Simmons and Administrator. These could have been used for brute-forcing password attempts but it is better to leave brute-forcing as a last resort.

### Nmap

Network mapper or Nmap for short is a free and opensource tool that can be used for network scanning. Nmap is an industry standard tool for network mapping, and as such the information from the scans conducted will be used multiple times throughout this report due to the nature of the scan that was run.

The first and only scans that was needed to be ran was “nmap 192.168.10.1 -vv -A -p1-10000” and “nmap 192.168.10.2 -vv -A -p1-10000”

These commands scanned the first 10,000 ports on server1 and server2 in an aggressive manner while providing verbose information about exactly what happened during scanning the servers. For the first server there was 9980 ports closed out of 10,000 scanned. Some of the notable ports on server1 were, port 22 which is typically used for SSH, port 80 as this is a web server running on HTTP rather than HTTPS, finally port 2081 which ran a HTTP server. These services have been further enumerated in the Enumeration phase. Due to the -A switch that was used in the scan, the Operating System and its version was searched for. However, this switch also makes the scan much more invasive of the servers so it will most likely get flagged by the company’s blue team in a realistic scenario. (nmap.org, 2022)



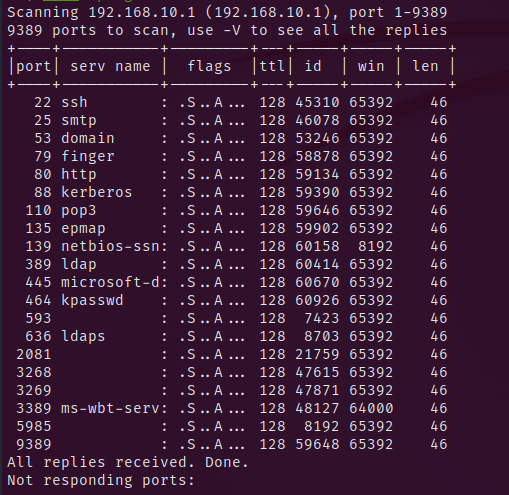
(Figure 5 – Discovery of Server1 Operating System)

For server2 when the same scan ran only one port had stuck out, which had been port 80 as this would have been another web server running on HTTP. The OS was the same for both servers. The tester would be able to use this data for the enumeration stage.

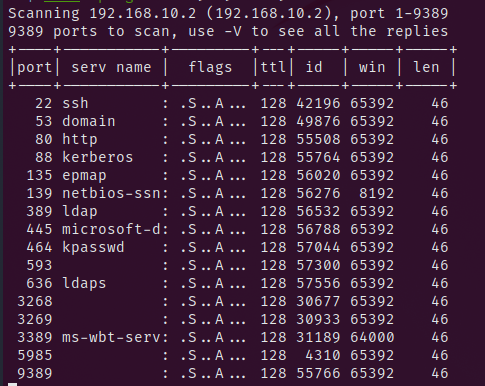
(The screenshots for the port scanning of server1 and server2 is in Appendix A)

### HPing3

HPing3 allows the tester to send custom packets to the network to see what affects it would have had on the server. However, in this case it had been used to check for services and the ports they were on. The tester found multiple services open and has used these to cross reference the services that Nmap had picked up from its port and service scanning.



(Figure 6 - The Scans above are from 192.168.10.1)



(Figure 6 - The Scans above are from 192.168.10.2)

The tester found the services found from the HPing3 scan are near enough the same as the Nmap scans, so it confirms the ports and services running are correct. The tester chose to move onto Enumeration stage due to finding all the information they needed to proceed.

## Enumeration

The Enumeration phase is where the tester has scraped as much information as possible from the services that have found to be running. The tester had also made use of the software Nessus, which has been discussed later in the Enumeration phase. The purpose of this Phase for the tester is to find any vulnerabilities or weaknesses in the security of the network so when moving towards the System Hacking stage there will be an exploit available to try to gain access to server1 and server2.

The tester investigated port 2081 on server1 and port 80 on both server1 and server2 since web servers are prone to having exploits like remote command execution, cross site scripting or SQL injection.

### Nessus Scan

The tester chose first to use Nessus to do vulnerability scanning. Nessus is a professional level vulnerability scanner which the tester had access to due to the essentials account that was given by the organisation that requested the penetration test.

Some information about Nessus as a whole, there is 5 different levels of vulnerabilities found within the Nessus scanner. In order:

Crictical – These vulnerabilities should be investigated by the company immediately after being told about it as these could have a detrimental impact on the company and its systems. These vulnerabilities are what the tester would go for if looking for vulnerabilities

High

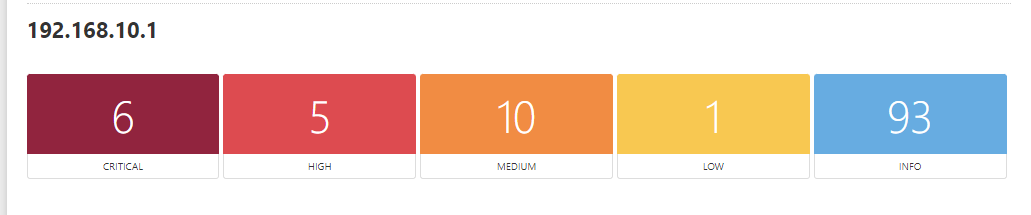
Medium

Low

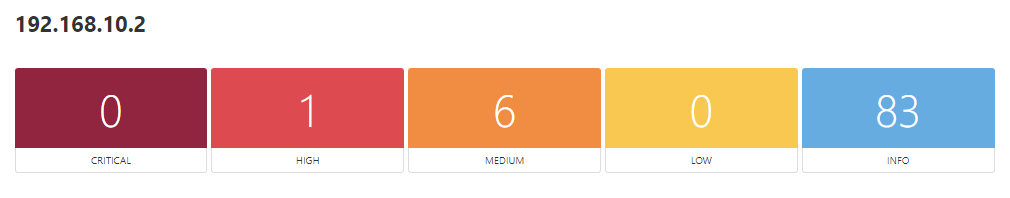
Info – Vulnerabilties of this calibre either have very little or even no use for the attacker but should still be investigated when they arise.

Nessus also has a full run down on the vulnerabilities that were found within the system and uses the CVE that matches the vulnerability to help explain how it works. For the tester this means they could look within these exploits and have a source of where to go next with the System Hacking.

Here are the results of the Nessus scans as a collective:



(Figure 7 – server1 Nessus scan results)



(Figure 8 – server2 Nessus scan results)

(All of the data for the Nessus scans are in the separate html file that was given with submission)

From the following screenshots of the scans there is

Server1 - 6 critical, 5 high, 10 medium, 1 low, and 93 info

Server2 – 0 critical, 1 high, 6 medium, 0 low, and 83 info

The tester is aware the most vulnerable server was server1 and this was most likely where the first attack vector was going to start. These 6 critical vulnerabilities would be a good place to start for the System Hacking (tenable, 2022)

### 192.168.10.1 - Port 2081 -HTTPFileServer 2.3

From the tester’s further analysis on the web-service at address 192.168.10.1:2081 An out-of-date version of HTTPFileServer was found which had been checked by the tester on Metasploit’s ExploitDB search tool in a later sub-heading.



(Figure 9 – Image of webpage that was found)

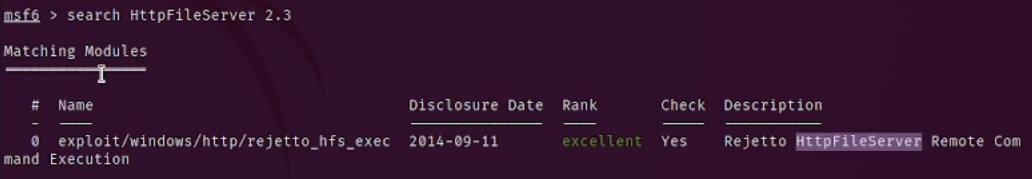
### 192.168.10.2 – Port 80 – Webserver Apache

From the Nmap scan that was done on server2 as well as server1, A web service was shown to be running on port 80 so the tester decided to investigate this further to check for any places where Remote Code Injection could be possible. Upon further investigation all that was found was a web page that had a text file which said, “Nothing to see here.”. Even after inspecting element of the whole page nothing was found. Which meant this was a dead end, so it didn’t make it to the System Hacking phase.

### MSFCONSOLE – Search

Msfconsole is a part of the Metasploit framework and is the Command Line Interface for Metasploit. Metasploit is an opensource and free framework that can be used for probing vulnerabilities all the way to completely exploiting a system and getting to root or SYSTEM, depending on the Operating System. The Graphical user interface version is called Armitage but isn’t used in industry standard meaning its better to stick to the CLI rather than the GUI.

the tester used the framework’s search functionality to discover exploits that would work on the vulnerabilities based on the version of the HTTPFileServer which had still been at version 2.3.

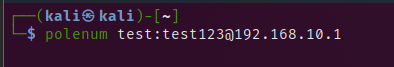


(Figure 10 – Found exploit for HTTPFileServer)

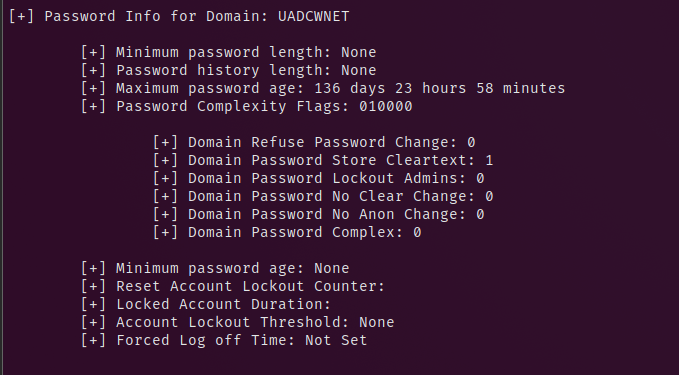
From the search the tester had found one exploit that should work against the file server. The exploit was a remote code execution exploit which would mean the code that is submitted to the page would run on the target machine (in this case server1) and can give access to the tester.

### Polenum

The tester had already found a small amount of exploits they could try so next was to find out about the company’s password policy, which was done with the password policy tool polenum. The information that had been found using this tool will be vital if password cracking was attempted since it gives details about how long a password must be, how long it is allowed to be alive before being changed, how many attempts for guessing before being locked out and if there is a duration of being locked out depending on if there a maximum number of tries before being locked out.



(Figure 11 – command for executing polenum tool)



(Figure 12 - Details for password policy)

Now that the enumeration for the policy had been completed the tester could see that this system had no min password length, a high password age, no minimum account lockout counter. This information makes brute-forcing the admin password possible since there is an unlimited number of attempts allowed, however this could take a while, so the tester would’ve run the password cracker in the background if they wanted to take the password cracking approach.

### Enum4Linux

Enum4Linux is a tool for doing a complete analysis of windows machines and does a thorough and advanced enumeration of windows through one command line, the -u and -p switches allow for usage of a username and password as well to help with the enumeration process. The tester ran this to find more users and user groups so they could create a user list file for a brute-force attack if it came to that being the only attack vector.

(Output of command will be in Appendix B)

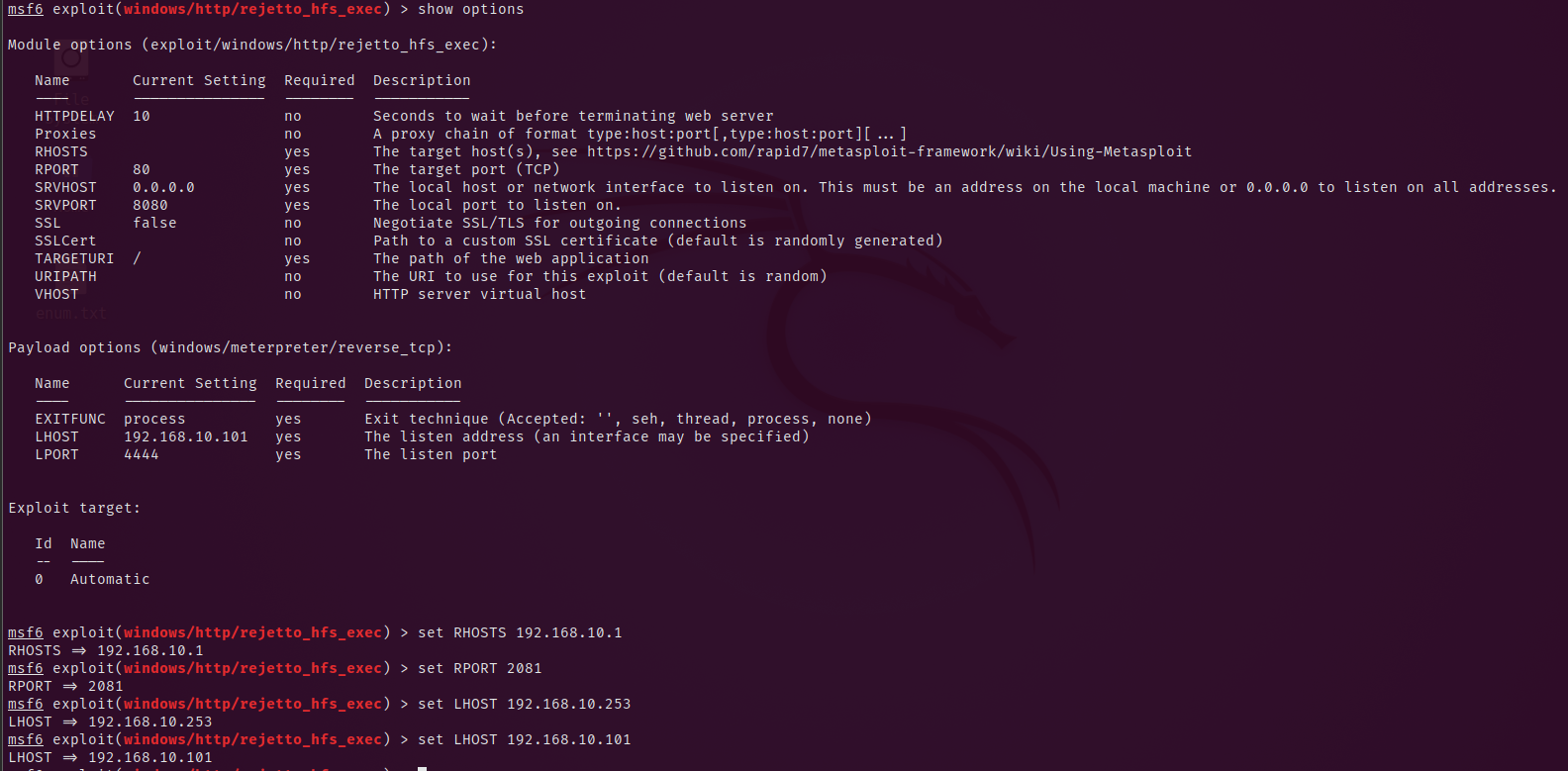
## System Hacking

Now that the tester had scanned the network and gotten possible attack vectors, it was time to attempt the exploits to try gain access into server1 then Privilege escalate vertically into a high-level account and from that account gain access to server2 since they are both domain controllers (server1 being main domain controller and server2 being secondary domain controller) that relay information to each other regularly for updating, meaning if any changes occur like username or password changes then both servers will update those credentials to ensure it stays in sync with each other.

The exploit path the tester is going to try is gain access from the service on port 2081 since there is a well-known Metasploit exploit on that service.

### HFS Exploitation

The tester goes back to msfconsole and loads up the exploit for HTTPFileServer. (Metasploit.com, 2022)



(Figure 13 – showing and Setting options to get exploit ready for exploiting)

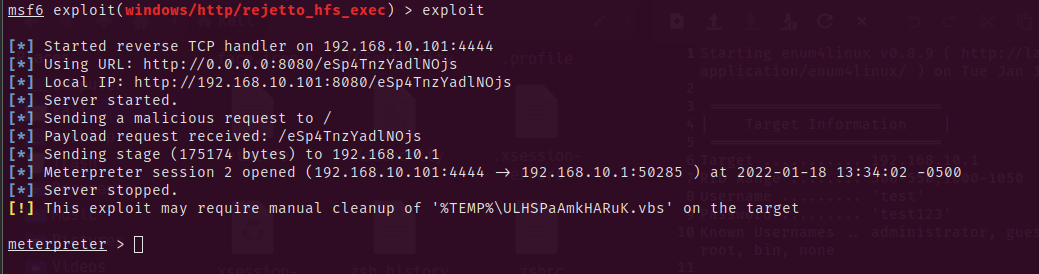
To run the exploit the tester had to show what options needed to be set and then set the values. RHOST need to be set to the IP address of the target machine.

RPORT needed to be set to the port of the target machine where the service was being run.

LHOST is the tester’s Kali machine IP address.

LPORT has been set to whatever the tester would like, so they had left it as default 4444. Bear in mind that depending on the firewall sometimes it will block ports that aren’t from common service ports so it may need to be changed to solve that.

Once all the values had been set by the tester, the tester typed exploit and ran it.



(Figure 14 – Meterpreter shell on server1)

The tester then got a Meterpreter shell into the system and was ready to start privilege escalation.

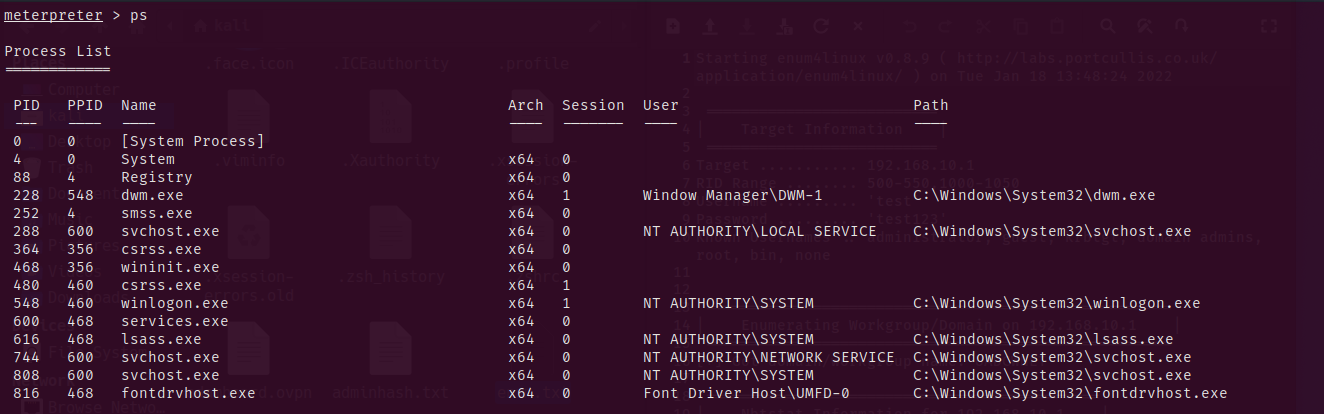
Meterpreter is Metasploit’s own shell payload that was created by them, Meterpreter has many applications that can be important once access has been gained, two of these commands were used in the upcoming sub-headings.

### Privilege Escalation

The tester had access to the server1 as a lower-level account and needed to privilege escalate to a higher-level account. The process for this would have been complicated for the tester but thankfully meterpreter can do the heavy lifting of getting to a higher privilege account with ease.

First the tester wrote the command PS which reveals all the currently running processes on the server1.

(Full list of running processes can be found in Appendix D)



(Figure 15 – A small sample of all processes running on server1)

The vital piece of information within the processes is what user was the process running as. This could be found in the User heading; the tester would want to be NT AUTHORITY\SYSTEM since this is the highest possible level of privileges. Getting access as one of these Users would have been the tricky part but Meterpreter makes it easy by having a simple command to do it. The tester wrote the command migrate <PID> which will move the tester’s shell to that process so the tester can run commands as that User. The tester in this case will use the PID 4368.



(Figure 16 – Process that is being migrated to)

The tester is now successfully privilege escalated to SYSTEM. The next step was to dump the hashes and crack them.

### Hash Cracking

The tester can run the second command that makes Meterpreter a shell that is better than most shells, once access has been gained the tester typed the command hashdump to dump all the user hashes, then they have been inputted into a text file using vim.

The tester then used the file and inserted it into a tool called JohnTheRipper; JohnTheRipper is a hash cracking tool used typically in Capture the Flags (CTF) and can change its format depending on the hash.

Since windows uses NTLM hashes the format would be NT for the window hashes. A wordlist is also required for the hash to be checked against, Rockyou.txt was used since it was the ideal wordlist considering how many passwords are contained within Rockyou.txt.



(Figure 17 – Command for john the ripper to crack and display the passwords)



(Figure 18 – Command for john the ripper to show the already cracked passwords)

(All of the cracked hashes are in Appendix C)

Now that there is cracked passwords, the tester goes for access to server2. Administrator’s hash didn’t get cracked but there is another way of entry the tester had in mind. (Openwall, 2022)

### Access to server2

Finally, to complete exploitation phase Access to server2 has been gained.

Before the proper process can be done, meterpreter needed to load powershell through two commands

Load powershell

Powershell\_shell

These commands set up and runs a powershell shell on the meterpreter shell.

The process for doing this is the tester had created their own account and added it to administrators and the Remote Desktop Group through these three commands from powershell.

net user hacker ihackedyou /add

net localgroup Administrators hacker /add

net localgroup "Remote Desktop Users" hacker /add

Next step is to enable Remote Desktop Protocol (RDP) and allow it through windows defender for external access. The tester done this to gain persistent access to the machine.

Set-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Control\Terminal Server' -name "fDenyTSConnections" -value 0

Enable-NetFirewallRule -DisplayGroup "Remote Desktop"

Finally, persistent access is used by doing these two commands.

The program required was installed through the command below

sudo apt install xfreerdp-x11

The second command gained RDP access to both server1 and server2 when the IP address is changed

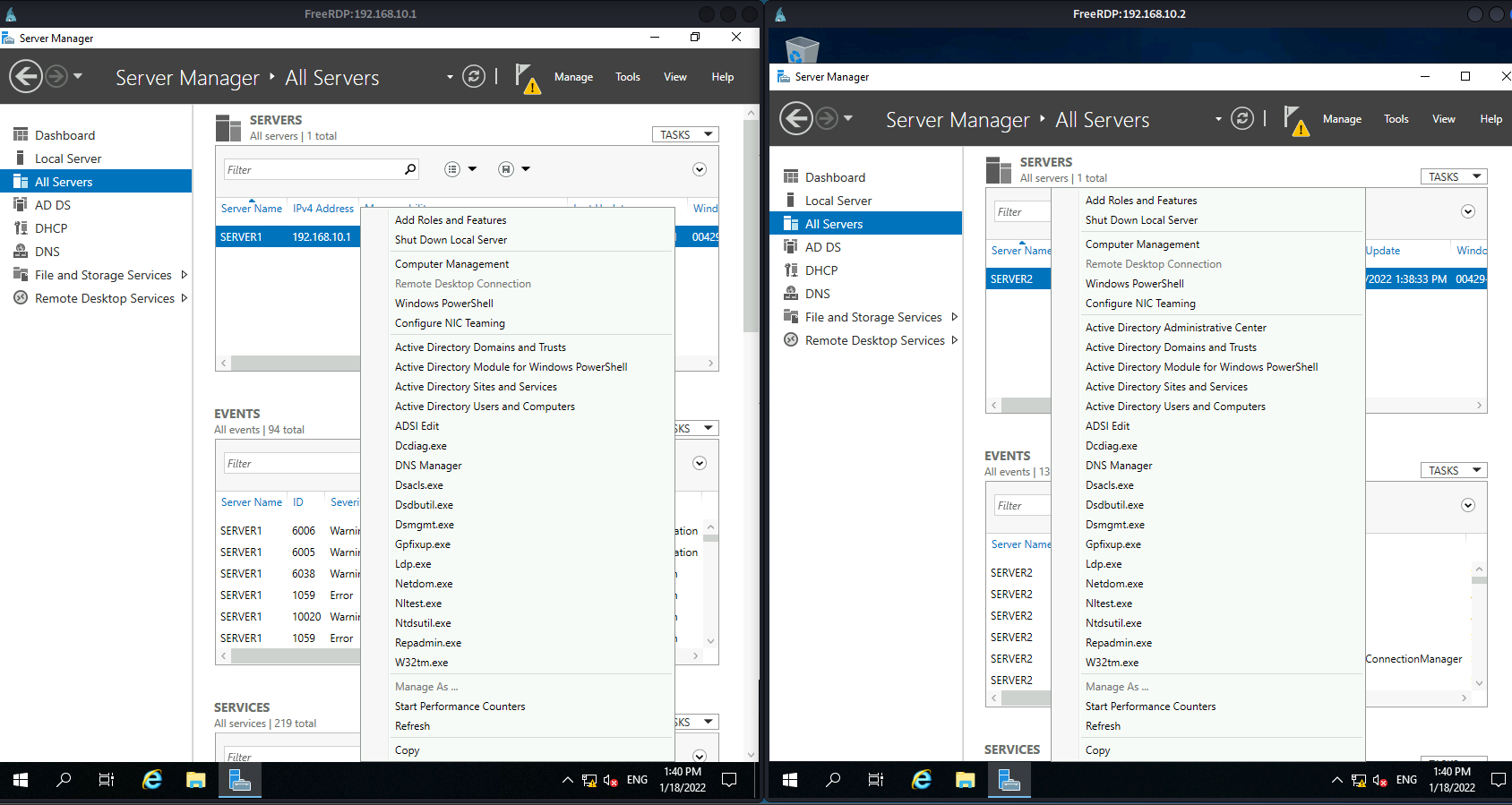
xfreerdp /v:192.168.10.1 /u:hacker /p:ihackedyou /dynamic-resolution +clipboard /drive:/usr/share/windows-resources,share

xfreerdp /v:192.168.10.2 /u:hacker /p:ihackedyou /dynamic-resolution +clipboard /drive:/usr/share/windows-resources,share

The tester Gained access to both servers and had obtained highest privilege in both servers. (Nekrotic, 2021)

### Post-Exploit

The tester reached the final stage of the methodology and had complete control over the entirety of the active directory network. The options shown below is all the options that can be done with server manager since the tester is obtained administrator of the whole network.



(Figure 19 – Access to server manager for both server1 and server2 with a list of all options they can inspect and mess around with)

# Discussion

## General Discussion

The tester was able to gain access in under 10 hours which was a third of time allotted for the penetration test. All the this was done from the low-level account of test and obtained access to a high-level privileged account on server1, server2 and client1. The tester was able to get to this position in a short amount of time with very little obstacles in the way. This section discusses general findings within the network and during the penetration test. The tester’s recommendation would be to follow the Nessus scan and this report to assist in increasing the security of the network as it was somewhat lacking, this was continued later in countermeasures.

This penetration test was made simpler as its starting point was within the internal network already and made the first step in the Firstbase Techies methodology null and void. Depending on the companies firewalls and physical security, the first step could have made this penetration test significantly harder so long as they had no major blind spots within their external and physical security.

Furthermore, the tester scanned the network from both internally and externally to see if the firewall would pick up from external scans and to no surprise it blocked access to seeing the services and ports from external access, so the information was not publicly available and only available from internally.

During the Enumeration phase multiple critical vulnerabilities were found and even without the Nessus scan as proof the out-of-date HFS service wasn’t seen in the Nessus report and was still vulnerable. Nessus altogether across both servers had 205 vulnerabilities, whereas the ideal number of vulnerabilities would be 0 but in a realistic outlook isn’t possible so settling for lower than 10 is also ideal.

Next was the exploitation phase where the vulnerabilities found were exploited, namely the HFS exploit which had happened because of the out-of-date service on port 2081. Brute-forcing the passwords was not done by the tester since it would be seen as a last resort as mentioned throughout the entirety of the report. However, the capability to brute-force the passwords is there since there Is no minimum length for passwords and no lockout feature had been enabled for too many password attempts.

From the passwords the tester did find they were simple enough passwords that were found through RockYou.txt; RockYou.txt is one of the biggest data breaches with 14.3 million unique passwords which shows how simplistic some employees passwords are considering they had been found within this wordlist.

Finally, the windows defender should have caught the Meterpreter shell when it was being uploaded however, the tester found that it was not caught and because of this slip through security, the tester obtained their own admin account on the network with full access to everything within. The tester recommends the organisation to do research into the vulnerabilities found and either hire an external security team or train up current security team if available to keep systems up to date, hardened and monitored.

## Countermeasures

From the section before, the tester was able to see the vulnerabilities at each stage and they are completely transparent and throughout this section each vulnerability will be listed with its countermeasure below.

The Nmap scan from the scanning phase should be done by the company itself on a regular basis to scan for unknown open ports or services. These open ports could be backdoors or malware planted by black-hat hackers.

The company should also investigate investing into a firewall that is up to date and updated with new Vulnerabilities from windows threat intelligence and assume any incoming external connections are malicious unless proven otherwise as it will be more beneficial.

Finally, the vulnerabilities that were found from Nessus and the pen test should be patched, like the out-of-date PHP web server on port 80 and the HFS that is out of date on port 2081. Both require immediate updates and if not possible then should be monitored intensely to ensure any incoming suspicious connections can be cut off immediately.

There was also the weak password policy which should be updated to have a minimum length, at least on special character, one capital letter and one number. And decrease the password age to 30 days at a minimum at it will require passwords to be fresh each month.

## Future Work

The organisation could have made the penetration test harder by including the Footprinting stage as it would require some level of social engineering, and the company may have blind spots to these social engineering techniques. Continuing, the tools given to the tester were more than sufficient to be able to complete a full penetration test, especially with Nessus and Metasploit. However, if more tools were to be chosen here is a few that come to the tester’s mind:

Full access to the entirety of the Nessus pro database to assist in finding more vulnerabilities, Reports that would have a generator of responses depending on the vulnerability to remove human error within the report and have exact definitions of what is needed to fix the vulnerability, and the last thing would be a way to keep the tools up indefinitely since they had turned off a few times and the whole exploitation process had to be restarted to get back to where the tester was.

If there was more time, then a test against obfuscated code that is handwritten rather than with use of Metasploit would be more than accepted as it would test the limits of even windows defender since Meterpreter is a well-known payload currently so it would normally get flagged by up-to-date systems and the connection wouldn’t go through.

## Conclusion

In conclusion, a penetration test against this organisation’s whole network was successful in being carried out by the tester, there was a magnitude of vulnerabilities found within the network and each one was given some level of a solution. If the penetration test had not been carried out by the tester, then sooner or later the company would have been attacked by a black-hat hacker and the impact towards the company would be detrimental to any goals or success plans they may have planned. The financial damages alone could have unimaginable amounts of damage that would take years to recover from if they do recover.

Active directory for the organisation is not secure. And everything recommended within this paper should be taken into thought when securing the systems as there would be no downside to securing the system.

# References

2022. [online] Available at: <https://www.nationalhealthexecutive.com/News/wannacry-cyber-attack-cost-the-nhs-92m-after-19000-appointments-were-cancelled> [Accessed 15 January 2022].

2022. [online] Available at: <https://techjury.net/blog/what-is-a-black-hat-hacker/#gref> [Accessed 9 January 2022].

Infosec Resources. 2022. *The history of penetration testing - Infosec Resources*. [online] Available at: <https://resources.infosecinstitute.com/topic/the-history-of-penetration-testing/> [Accessed 11 January 2022].

Metasploit. 2022. *Metasploit | Penetration Testing Software, Pen Testing Security | Metasploit*. [online] Available at: <https://www.metasploit.com/> [Accessed 17 January 2022].

Ncsc.gov.uk. 2022. *Penetration Testing*. [online] Available at: <https://www.ncsc.gov.uk/guidance/penetration-testing#section\_4> [Accessed 12 January 2022].

Nekrotic -. 2022. *Active Directory Setup – The Basics - Nekrotic*. [online] Available at: <https://nekrotic.co.uk/2021/09/12/active-directory-setup-the-basics/> [Accessed 15 January 2022].

Nmap.org. 2022. *Nmap: the Network Mapper - Free Security Scanner*. [online] Available at: <https://nmap.org/> [Accessed 17 January 2022].

Openwall.com. 2022. *John the Ripper password cracker*. [online] Available at: <https://www.openwall.com/john/> [Accessed 18 January 2022].

Smart Insights. 2022. *E-commerce growth statistics - UK, US and Worldwide forecasts*. [online] Available at: <https://www.smartinsights.com/digital-marketing-strategy/online-retail-sales-growth/#:~:text=As%20demonstrated%20by%20these%20charts,between%20Q3%202020%20%2D%20Q2%202021.> [Accessed 14 January 2022].

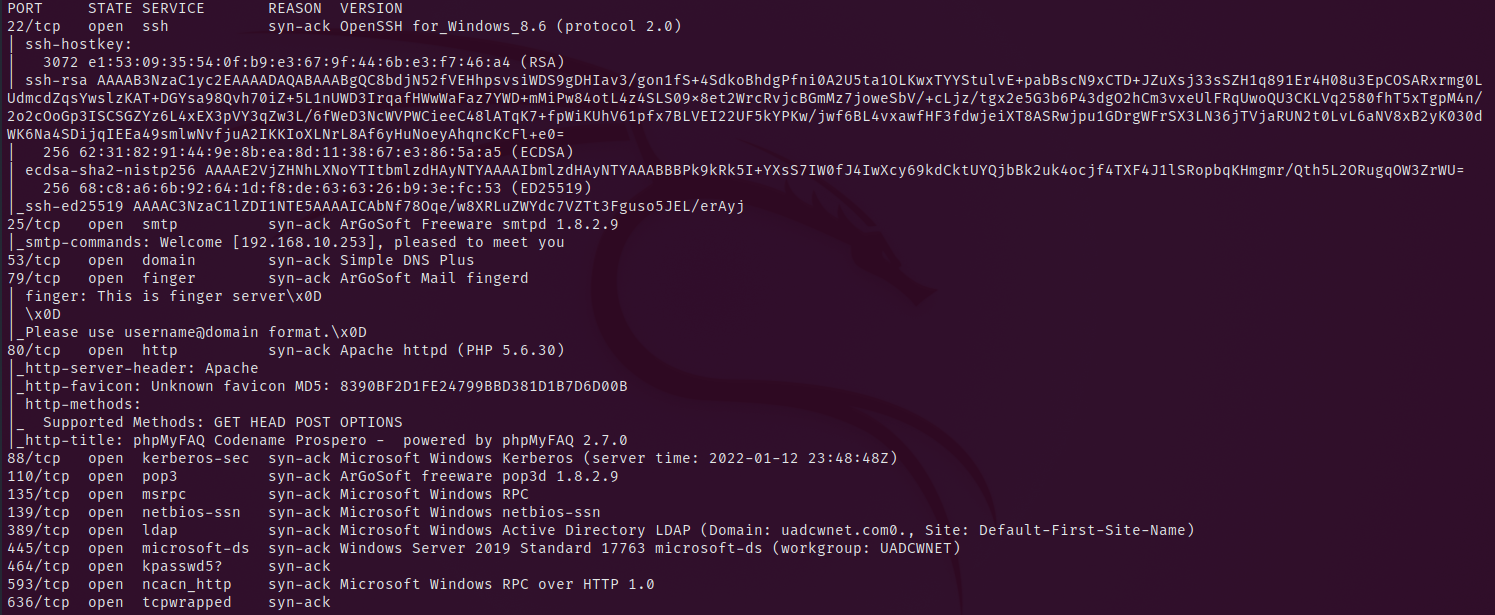
Tenable®. 2022. *Tenable® - The Cyber Exposure Company*. [online] Available at: <https://www.tenable.com/> [Accessed 17 January 2022].

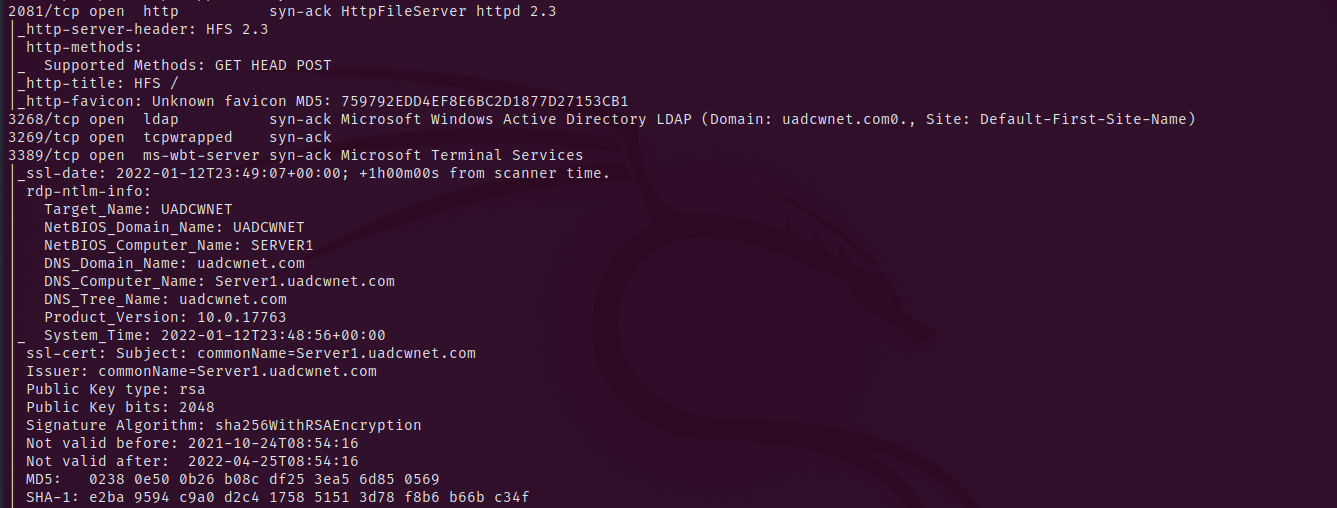
# Appendices

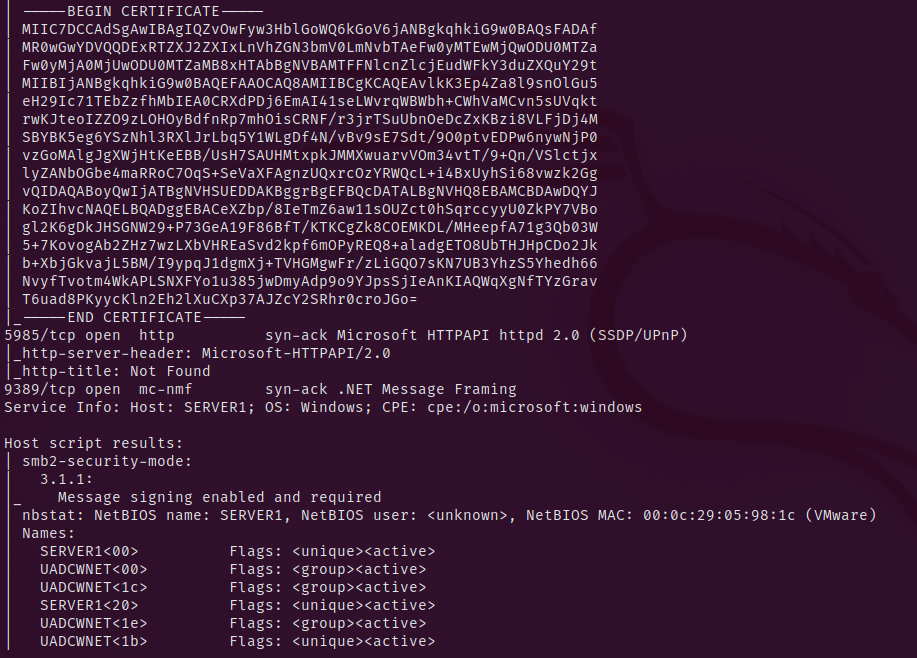
Note that Appendices should be referenced in the main body of the text.

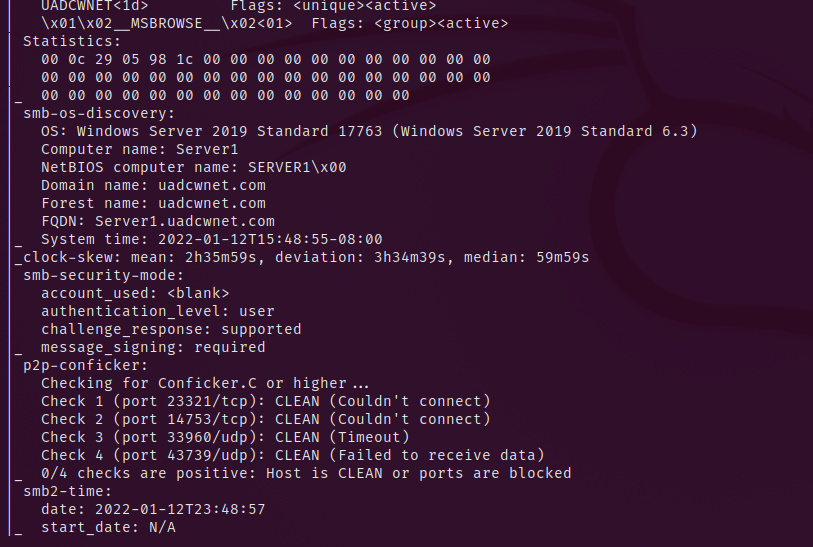
## Appendix A – Nmap scan for both servers

Nmap – 192.168.10.1

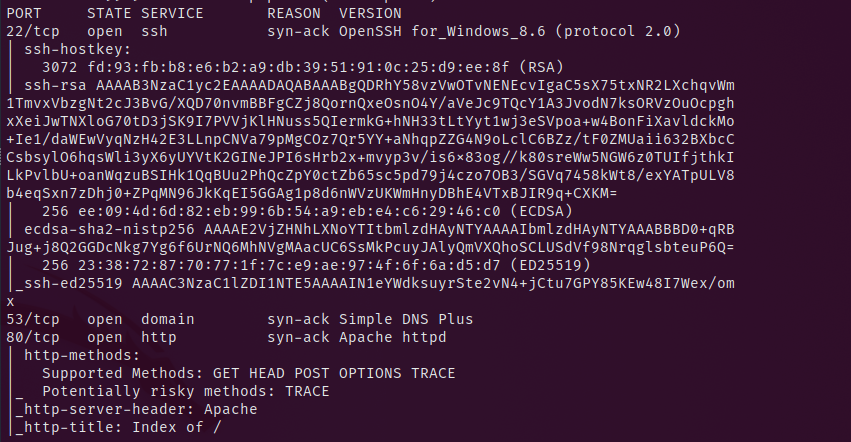


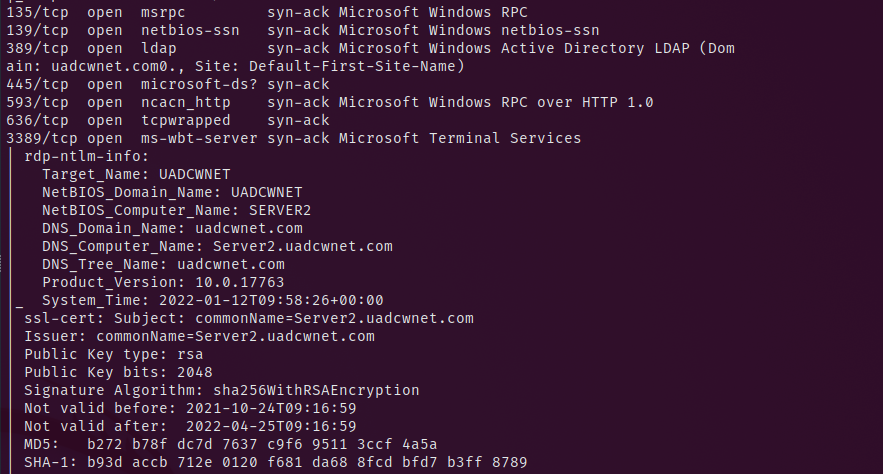


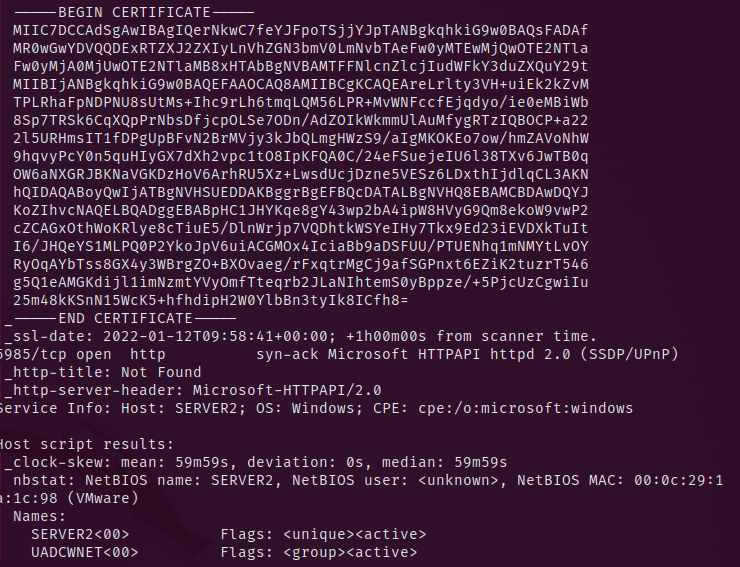


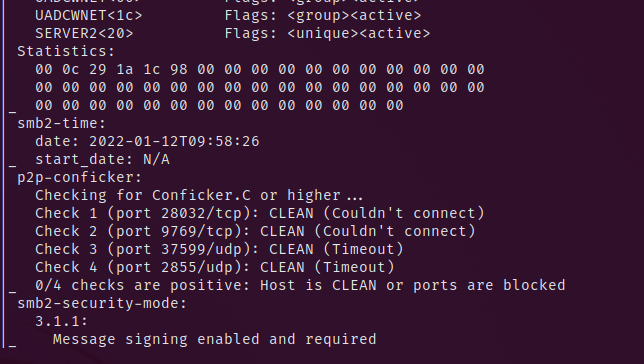


Nmap – 192.168.10.2









## Appendix B – Enum4Linux scan results

## Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Tue Jan 18 13:48:24 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 = 00-0C-29-05-98-1C

## =====================================

## | 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: 0x8176 RID: 0x8176 acb: 0x00000210 Account: A.Benson Name: Alma Benson Desc: evangel

## 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: 0x8163 RID: 0x8163 acb: 0x00000210 Account: A.Pearson Name: Arthur Pearson Desc: fertile

## 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: 0x8156 RID: 0x8156 acb: 0x00000210 Account: B.Brown Name: Boyd Brown Desc: bobbing

## 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: 0x8152 RID: 0x8152 acb: 0x00000210 Account: C.Watkins Name: Clarence Watkins Desc: dahlia

## index: 0x8170 RID: 0x8170 acb: 0x00000210 Account: C.Welch Name: Craig Welch Desc: each

## index: 0x6bec RID: 0x6bec acb: 0x00000210 Account: C.Willis Name: Carl Willis Desc: wavelength

## index: 0x8155 RID: 0x8155 acb: 0x00000210 Account: D.Berry Name: Diane Berry Desc: tallow

## index: 0x8165 RID: 0x8165 acb: 0x00000210 Account: D.Doyle Name: Doreen Doyle Desc: glossary

## index: 0x6be2 RID: 0x6be2 acb: 0x00000210 Account: D.Dunn Name: Daniel Dunn Desc: pinnacle

## index: 0x816b RID: 0x816b acb: 0x00000210 Account: D.Ford Name: Dexter Ford Desc: snowstorm

## index: 0x6be7 RID: 0x6be7 acb: 0x00000210 Account: D.Gross Name: Deborah Gross Desc: gorse

## index: 0x8166 RID: 0x8166 acb: 0x00000210 Account: D.Sandoval Name: Dwight Sandoval Desc: imposture

## index: 0x816d RID: 0x816d acb: 0x00000210 Account: E.Blake Name: Ellen Blake Desc: eureka

## index: 0x6bd9 RID: 0x6bd9 acb: 0x00000210 Account: E.Elliott Name: Elmer Elliott Desc: Todd

## index: 0x815f RID: 0x815f acb: 0x00000210 Account: E.Fields Name: Evan Fields Desc: tideland

## 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: 0x8169 RID: 0x8169 acb: 0x00000210 Account: F.Stokes Name: Florence Stokes Desc: prowl

## index: 0x815b RID: 0x815b acb: 0x00000210 Account: G.Adkins Name: Guadalupe Adkins Desc: poi

## index: 0x8162 RID: 0x8162 acb: 0x00000210 Account: G.Francis Name: Gretchen Francis Desc: thirty

## 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: 0x814e RID: 0x814e acb: 0x00000210 Account: H.Graham Name: Hannah Graham Desc: Landis

## index: 0x8157 RID: 0x8157 acb: 0x00000210 Account: H.Scott Name: Hope Scott Desc: serviceberry

## index: 0x817c RID: 0x817c acb: 0x00000010 Account: hacker Name: (null) Desc: (null)

## index: 0x6bd2 RID: 0x6bd2 acb: 0x00000210 Account: J.Ballard Name: Johnnie Ballard Desc: gassy

## index: 0x816c RID: 0x816c acb: 0x00000210 Account: J.Farmer Name: Jacob Farmer Desc: jury

## index: 0x816a RID: 0x816a acb: 0x00000210 Account: J.Gonzales Name: Jessie Gonzales Desc: angelies

## 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: 0x814f RID: 0x814f acb: 0x00000210 Account: J.Norton Name: Jessica Norton Desc: way

## 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: 0x8173 RID: 0x8173 acb: 0x00000210 Account: J.Rhodes Name: Julie Rhodes Desc: corruption

## index: 0x8158 RID: 0x8158 acb: 0x00000210 Account: J.Stevenson Name: Jody Stevenson Desc: Feeney

## index: 0x69dd RID: 0x69dd acb: 0x00000210 Account: J.Tate Name: Juanita Tate Desc: pastoral

## index: 0x8161 RID: 0x8161 acb: 0x00000210 Account: J.Wagner Name: Jake Wagner Desc: rightward

## index: 0x8171 RID: 0x8171 acb: 0x00000210 Account: J.Wilkerson Name: Jennifer Wilkerson Desc: pwd:MtiJW92hYspZ61fAmK

## index: 0x8175 RID: 0x8175 acb: 0x00000210 Account: K.Castillo Name: Krista Castillo Desc: squint

## index: 0x817b RID: 0x817b acb: 0x00000210 Account: K.Cohen Name: Kristen Cohen Desc: euphemist

## index: 0x815e RID: 0x815e acb: 0x00000210 Account: K.Mcgee Name: Kimberly Mcgee Desc: Rousseau

## index: 0x69e3 RID: 0x69e3 acb: 0x00010210 Account: K.Patrick Name: Kelvin Patrick Desc: methionine

## index: 0x816f RID: 0x816f acb: 0x00000210 Account: K.Russell Name: Kristopher Russell Desc: flogging

## 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: 0x8164 RID: 0x8164 acb: 0x00000210 Account: L.Mcguire Name: Lonnie Mcguire Desc: just

## index: 0x8178 RID: 0x8178 acb: 0x00000210 Account: L.Nguyen Name: Lamar Nguyen Desc: tongue

## 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: 0x8168 RID: 0x8168 acb: 0x00000210 Account: M.Boyd Name: Mattie Boyd Desc: vacant

## 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: 0x8154 RID: 0x8154 acb: 0x00000210 Account: M.Davidson Name: Mercedes Davidson Desc: Replication Account

## 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: 0x8179 RID: 0x8179 acb: 0x00000210 Account: M.Murphy Name: Marsha Murphy Desc: Bogota

## index: 0x8172 RID: 0x8172 acb: 0x00000210 Account: M.Patterson Name: Myra Patterson Desc: arsine

## index: 0x8151 RID: 0x8151 acb: 0x00000210 Account: M.Phillips Name: Marion Phillips Desc: southwest

## index: 0x6bd1 RID: 0x6bd1 acb: 0x00000210 Account: N.Colon Name: Nichole Colon Desc: Proust

## index: 0x8177 RID: 0x8177 acb: 0x00000210 Account: N.Hogan Name: Nicole Hogan Desc: Thor

## index: 0x8174 RID: 0x8174 acb: 0x00000210 Account: N.Norman Name: Nicolas Norman Desc: formatting

## index: 0x8150 RID: 0x8150 acb: 0x00000210 Account: N.Wells Name: Nettie Wells Desc: Muir

## index: 0x6bda RID: 0x6bda acb: 0x00000210 Account: O.Parker Name: Oliver Parker Desc: indelible

## index: 0x815a RID: 0x815a acb: 0x00000210 Account: P.Cain Name: Pam Cain Desc: keg

## index: 0x8160 RID: 0x8160 acb: 0x00000210 Account: R.Baker Name: Rodney Baker Desc: schooner

## index: 0x814d RID: 0x814d acb: 0x00010210 Account: R.Beck Name: Roman Beck Desc: Graves

## index: 0x69e4 RID: 0x69e4 acb: 0x00000210 Account: R.Bridges Name: Randy Bridges Desc: fair

## index: 0x817a RID: 0x817a acb: 0x00000210 Account: R.Holloway Name: Ryan Holloway Desc: insurrect

## 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: 0x8167 RID: 0x8167 acb: 0x00000210 Account: S.Daniels Name: Sharon Daniels Desc: lustful

## index: 0x8153 RID: 0x8153 acb: 0x00000210 Account: S.Franklin Name: Sidney Franklin Desc: hireling

## index: 0x69e2 RID: 0x69e2 acb: 0x00000210 Account: S.Glover Name: Sean Glover Desc: rye

## index: 0x815d RID: 0x815d acb: 0x00000210 Account: S.Hicks Name: Sergio Hicks Desc: buggy

## 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: 0x815c RID: 0x815c acb: 0x00000210 Account: T.Gibson Name: Troy Gibson Desc: flatworm

## 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: 0x816e RID: 0x816e acb: 0x00000210 Account: V.Lawson Name: Virginia Lawson Desc: sunder

## index: 0x8159 RID: 0x8159 acb: 0x00000210 Account: Y.Burton Name: Yvonne Burton Desc: pliant

## 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:[0x814d]

## user:[H.Graham] rid:[0x814e]

## user:[J.Norton] rid:[0x814f]

## user:[N.Wells] rid:[0x8150]

## user:[M.Phillips] rid:[0x8151]

## user:[C.Watkins] rid:[0x8152]

## user:[S.Franklin] rid:[0x8153]

## user:[M.Davidson] rid:[0x8154]

## user:[D.Berry] rid:[0x8155]

## user:[B.Brown] rid:[0x8156]

## user:[H.Scott] rid:[0x8157]

## user:[J.Stevenson] rid:[0x8158]

## user:[Y.Burton] rid:[0x8159]

## user:[P.Cain] rid:[0x815a]

## user:[G.Adkins] rid:[0x815b]

## user:[T.Gibson] rid:[0x815c]

## user:[S.Hicks] rid:[0x815d]

## user:[K.Mcgee] rid:[0x815e]

## user:[E.Fields] rid:[0x815f]

## user:[R.Baker] rid:[0x8160]

## user:[J.Wagner] rid:[0x8161]

## user:[G.Francis] rid:[0x8162]

## user:[A.Pearson] rid:[0x8163]

## user:[L.Mcguire] rid:[0x8164]

## user:[D.Doyle] rid:[0x8165]

## user:[D.Sandoval] rid:[0x8166]

## user:[S.Daniels] rid:[0x8167]

## user:[M.Boyd] rid:[0x8168]

## user:[F.Stokes] rid:[0x8169]

## user:[J.Gonzales] rid:[0x816a]

## user:[D.Ford] rid:[0x816b]

## user:[J.Farmer] rid:[0x816c]

## user:[E.Blake] rid:[0x816d]

## user:[V.Lawson] rid:[0x816e]

## user:[K.Russell] rid:[0x816f]

## user:[C.Welch] rid:[0x8170]

## user:[J.Wilkerson] rid:[0x8171]

## user:[M.Patterson] rid:[0x8172]

## user:[J.Rhodes] rid:[0x8173]

## user:[N.Norman] rid:[0x8174]

## user:[K.Castillo] rid:[0x8175]

## user:[A.Benson] rid:[0x8176]

## user:[N.Hogan] rid:[0x8177]

## user:[L.Nguyen] rid:[0x8178]

## user:[M.Murphy] rid:[0x8179]

## user:[R.Holloway] rid:[0x817a]

## user:[K.Cohen] rid:[0x817b]

## user:[hacker] rid:[0x817c]

## =========================================

## | Share Enumeration on 192.168.10.1 |

## =========================================

## do\_connect: Connection to 192.168.10.1 failed (Error NT\_STATUS\_RESOURCE\_NAME\_NOT\_FOUND)

## Sharename Type Comment

## --------- ---- -------

## ADMIN$ Disk Remote Admin

## C$ Disk Default share

## Fileshare1 Disk

## Fileshare2 Disk

## HR Disk

## IPC$ IPC Remote IPC

## NETLOGON Disk Logon server share

## Resources Disk

## SYSVOL Disk Logon server share

## SYSVOL2 Disk

## Reconnecting with SMB1 for workgroup listing.

## Unable to connect with SMB1 -- no workgroup available

## [+] 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 'Pre-Windows 2000 Compatible Access' (RID: 554) has member: NT AUTHORITY\Authenticated Users

## Group 'Guests' (RID: 546) has member: UADCWNET\Guest

## Group 'Guests' (RID: 546) has member: UADCWNET\Domain Guests

## 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 'Administrators' (RID: 544) has member: UADCWNET\hacker

## Group 'Remote Desktop Users' (RID: 555) has member: UADCWNET\hacker

## Group 'Windows Authorization Access Group' (RID: 560) has member: NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS

## 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 'IIS\_IUSRS' (RID: 568) has member: NT AUTHORITY\IUSR

## [+] 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\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

## 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 '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 'Domain Users' (RID: 513) has member: UADCWNET\hacker

## 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\test

## 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\J.Norton

## Group 'Legal' (RID: 1104) has member: UADCWNET\L.Mcguire

## Group 'Legal' (RID: 1104) has member: UADCWNET\D.Sandoval

## Group 'Legal' (RID: 1104) has member: UADCWNET\M.Boyd

## Group 'Legal' (RID: 1104) has member: UADCWNET\J.Gonzales

## Group 'Legal' (RID: 1104) has member: UADCWNET\K.Russell

## Group 'Legal' (RID: 1104) has member: UADCWNET\J.Rhodes

## Group 'Legal' (RID: 1104) has member: UADCWNET\N.Norman

## Group 'Legal' (RID: 1104) has member: UADCWNET\N.Hogan

## 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\N.Wells

## Group 'Engineering' (RID: 1106) has member: UADCWNET\S.Franklin

## Group 'Engineering' (RID: 1106) has member: UADCWNET\T.Gibson

## Group 'Engineering' (RID: 1106) has member: UADCWNET\S.Hicks

## Group 'Engineering' (RID: 1106) has member: UADCWNET\R.Baker

## Group 'Engineering' (RID: 1106) has member: UADCWNET\J.Wilkerson

## Group 'Engineering' (RID: 1106) has member: UADCWNET\L.Nguyen

## Group 'Schema Admins' (RID: 518) has member: UADCWNET\Administrator

## Group 'Sales' (RID: 1107) has member: UADCWNET\N.Colon

## 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\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\R.Beck

## Group 'Sales' (RID: 1107) has member: UADCWNET\M.Davidson

## Group 'Sales' (RID: 1107) has member: UADCWNET\A.Pearson

## Group 'Sales' (RID: 1107) has member: UADCWNET\D.Doyle

## Group 'Sales' (RID: 1107) has member: UADCWNET\S.Daniels

## Group 'Sales' (RID: 1107) has member: UADCWNET\F.Stokes

## Group 'Sales' (RID: 1107) has member: UADCWNET\E.Blake

## Group 'Sales' (RID: 1107) has member: UADCWNET\V.Lawson

## Group 'Sales' (RID: 1107) has member: UADCWNET\M.Murphy

## 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 'Finance' (RID: 1105) has member: UADCWNET\L.Vasquez

## 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\M.Phillips

## Group 'Finance' (RID: 1105) has member: UADCWNET\C.Watkins

## Group 'Finance' (RID: 1105) has member: UADCWNET\J.Stevenson

## Group 'Finance' (RID: 1105) has member: UADCWNET\G.Adkins

## Group 'Finance' (RID: 1105) has member: UADCWNET\G.Francis

## Group 'Finance' (RID: 1105) has member: UADCWNET\D.Ford

## Group 'Enterprise Admins' (RID: 519) has member: UADCWNET\Administrator

## 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\C.Romero

## 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\H.Graham

## Group 'Human Resources' (RID: 1103) has member: UADCWNET\B.Brown

## Group 'Human Resources' (RID: 1103) has member: UADCWNET\H.Scott

## Group 'Human Resources' (RID: 1103) has member: UADCWNET\P.Cain

## Group 'Human Resources' (RID: 1103) has member: UADCWNET\K.Mcgee

## Group 'Human Resources' (RID: 1103) has member: UADCWNET\E.Fields

## Group 'Human Resources' (RID: 1103) has member: UADCWNET\J.Wagner

## Group 'Human Resources' (RID: 1103) has member: UADCWNET\C.Welch

## Group 'Human Resources' (RID: 1103) has member: UADCWNET\M.Patterson

## Group 'Human Resources' (RID: 1103) has member: UADCWNET\K.Castillo

## Group 'Human Resources' (RID: 1103) has member: UADCWNET\R.Holloway

## Group 'Human Resources' (RID: 1103) has member: UADCWNET\K.Cohen

## Group 'Group Policy Creator Owners' (RID: 520) has member: UADCWNET\Administrator

## Group 'Domain Guests' (RID: 514) has member: UADCWNET\Guest

## Group 'Domain Controllers' (RID: 516) has member: UADCWNET\SERVER1$

## Group 'Domain Controllers' (RID: 516) has member: UADCWNET\SERVER2$

## 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\D.Berry

## Group 'Information Technology' (RID: 1108) has member: UADCWNET\Y.Burton

## Group 'Information Technology' (RID: 1108) has member: UADCWNET\J.Farmer

## Group 'Information Technology' (RID: 1108) has member: UADCWNET\A.Benson

## 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$

## =======================================================================

## | 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-1-5-80 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-1-5-21-2407547381-1006735410-685985656 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-1-5-21-2373017989-4057782597-2990666611 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)

## =============================================

## | Getting printer info for 192.168.10.1 |

## =============================================

## No printers returned.

## enum4linux complete on Tue Jan 18 13:48:41 2022

## Appendix C

Guest::501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

J.Tate:knobber:27101:aad3b435b51404eeaad3b435b51404ee:837c84468f8017b3a35e327ce0202597:::

M.Johnston:Odyssey:27102:aad3b435b51404eeaad3b435b51404ee:1289b7b2efe2b3e03412466314572946:::

K.Patrick:playoff:27107:aad3b435b51404eeaad3b435b51404ee:1b8f094544191757435cbf13ea6f8122:::

J.Kelly:menopause:27112:aad3b435b51404eeaad3b435b51404ee:da631a4b29c99dbb3bf80c13e383a4d6:::

N.Colon:climate:27601:aad3b435b51404eeaad3b435b51404ee:30f4e47da897170bb3fe87e0a8d558d0:::

C.Munoz:feinberg:27608:aad3b435b51404eeaad3b435b51404ee:3c4d1baf9bf5eae2a1221893329a3fab:::

O.Parker:clogging:27610:aad3b435b51404eeaad3b435b51404ee:7514f4a16511b4ce99866ab68d73a149:::

J.Patton:croydon:27617:aad3b435b51404eeaad3b435b51404ee:1ae931f85d4f76e448808ecaa2316901:::

S.Brock:voracity:27625:aad3b435b51404eeaad3b435b51404ee:3f20e243fb1b8e2b7fecbabcd98a5aad:::

L.Sharp:metamorphic:27626:aad3b435b51404eeaad3b435b51404ee:9656c417d3ff3aa3742209ea4c9fd46c:::

G.Lambert:workhorse:27627:aad3b435b51404eeaad3b435b51404ee:b2f27ae7d5f449c70468e933d58db932:::

C.Willis:handwritten:27628:aad3b435b51404eeaad3b435b51404ee:329b732aa252bd2684fe004a3b4765f5:::

J.Poole:pitchfork:27633:aad3b435b51404eeaad3b435b51404ee:f13c86afe974bf0cf506a673c05d6286:::

B.Blair:Peugeot:27634:aad3b435b51404eeaad3b435b51404ee:ac8a5244c76ab50203f22b65c05005c1:::

test:test123:27637:aad3b435b51404eeaad3b435b51404ee:c5a237b7e9d8e708d8436b6148a25fa1:::

J.Norton:Lincoln:33103:aad3b435b51404eeaad3b435b51404ee:34ad9ec59c02c6feeac9ef1c414bab46:::

N.Wells:embryology:33104:aad3b435b51404eeaad3b435b51404ee:8dc38e447cd5592bcf71e1ab1e62eead:::

C.Watkins:choirmaster:33106:aad3b435b51404eeaad3b435b51404ee:8cc43f4179f99a697003943ebb1486ae:::

Y.Burton:hawaiian:33113:aad3b435b51404eeaad3b435b51404ee:7272029b2d64c6e3df194e4d81c53302:::

T.Gibson:Patagonia:33116:aad3b435b51404eeaad3b435b51404ee:6734eb9bb8cb79b4f000a545055583c2:::

R.Baker:obfuscate:33120:aad3b435b51404eeaad3b435b51404ee:4a2d05ebd8d60f5c7a37d0e93929781d:::

A.Pearson:patriarch:33123:aad3b435b51404eeaad3b435b51404ee:73108c205623bf29eb4423c5b1b6eead:::

L.Mcguire:Sherrill:33124:aad3b435b51404eeaad3b435b51404ee:df9a732051587cae8b73201262fa8b46:::

D.Sandoval:masturbate:33126:aad3b435b51404eeaad3b435b51404ee:6086514d8af2e27c7b353e35846a23d5:::

M.Boyd:crankshaft:33128:aad3b435b51404eeaad3b435b51404ee:9063edf579410320651c778c7feeaa6e:::

E.Blake:Patagonia:33133:aad3b435b51404eeaad3b435b51404ee:6734eb9bb8cb79b4f000a545055583c2:::

K.Russell:apparatus:33135:aad3b435b51404eeaad3b435b51404ee:09fd1934b9ed97d6d1ad3bb0914b7e39:::

K.Cohen:accidental:33147:aad3b435b51404eeaad3b435b51404ee:6b17f3c0d3eae470f68e114ba186578a:::

hacker:ihackedyou:33148:aad3b435b51404eeaad3b435b51404ee:006f22ea5bfa5d57c317a90873cfef14:::

MSSQL4$:qualities:27641:aad3b435b51404eeaad3b435b51404ee:f93796520a25a3c5c68bd4332306c407:::

## Appendix D

0 0 [System Process]

4 0 System x64 0

88 4 Registry x64 0

228 548 dwm.exe x64 1 Window Manager\DWM-1 C:\Windows\System32\dwm.exe

252 4 smss.exe x64 0

288 600 svchost.exe x64 0 NT AUTHORITY\LOCAL SERVICE C:\Windows\System32\svchost.exe

364 356 csrss.exe x64 0

468 356 wininit.exe x64 0

480 460 csrss.exe x64 1

548 460 winlogon.exe x64 1 NT AUTHORITY\SYSTEM C:\Windows\System32\winlogon.exe

600 468 services.exe x64 0

616 468 lsass.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\lsass.exe

744 600 svchost.exe x64 0 NT AUTHORITY\NETWORK SERVICE C:\Windows\System32\svchost.exe

808 600 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\svchost.exe

816 468 fontdrvhost.exe x64 0 Font Driver Host\UMFD-0 C:\Windows\System32\fontdrvhost.exe

828 548 fontdrvhost.exe x64 1 Font Driver Host\UMFD-1 C:\Windows\System32\fontdrvhost.exe

840 3956 cmd.exe x86 0 NT AUTHORITY\SYSTEM C:\Windows\SysWOW64\cmd.exe

868 600 svchost.exe x64 0 NT AUTHORITY\LOCAL SERVICE C:\Windows\System32\svchost.exe

920 600 svchost.exe x64 0 NT AUTHORITY\NETWORK SERVICE C:\Windows\System32\svchost.exe

1000 600 svchost.exe x64 0 NT AUTHORITY\LOCAL SERVICE C:\Windows\System32\svchost.exe

1004 548 LogonUI.exe x64 1 NT AUTHORITY\SYSTEM C:\Windows\System32\LogonUI.exe

1080 600 svchost.exe x64 0 NT AUTHORITY\LOCAL SERVICE C:\Windows\System32\svchost.exe

1124 600 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\svchost.exe

1176 600 svchost.exe x64 0 NT AUTHORITY\NETWORK SERVICE C:\Windows\System32\svchost.exe

1328 600 svchost.exe x64 0 NT AUTHORITY\LOCAL SERVICE C:\Windows\System32\svchost.exe

1432 600 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\svchost.exe

1468 600 vm3dservice.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\vm3dservice.exe

1516 3904 TjtlZXBpzyTmbcW.exe x86 0 NT AUTHORITY\SYSTEM C:\Windows\Temp\rad3057F.tmp\TjtlZXBpzyTmbcW.exe

1632 1516 cmd.exe x86 0 NT AUTHORITY\SYSTEM C:\Windows\SysWOW64\cmd.exe

1648 600 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\svchost.exe

1684 600 svchost.exe x64 0 NT AUTHORITY\LOCAL SERVICE C:\Windows\System32\svchost.exe

1852 1432 cmd.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\cmd.exe

1972 1432 UniController.exe x86 0 NT AUTHORITY\SYSTEM C:\Users\Administrator\Desktop\UniServerZ\UniController.exe

2080 600 svchost.exe x64 0 NT AUTHORITY\NETWORK SERVICE C:\Windows\System32\svchost.exe

2208 1852 conhost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\conhost.exe

2396 1972 mysqld\_z.exe x86 0 NT AUTHORITY\SYSTEM C:\Users\Administrator\Desktop\UniServerZ\core\mysql\bin\mysqld\_z.exe

2440 600 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\svchost.exe

2520 1972 httpd\_z.exe x86 0 NT AUTHORITY\SYSTEM C:\Users\Administrator\Desktop\UniServerZ\core\apache2\bin\httpd\_z.exe

2540 2520 httpd\_z.exe x86 0 NT AUTHORITY\SYSTEM C:\Users\Administrator\Desktop\UniServerZ\core\apache2\bin\httpd\_z.exe

3312 600 spoolsv.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\spoolsv.exe

3368 600 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\svchost.exe

3376 600 dfsrs.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\dfsrs.exe

3384 600 Microsoft.ActiveDirectory.WebServices.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\ADWS\Microsoft.ActiveDirectory.WebServices.exe

3392 600 dns.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\dns.exe

3400 600 svchost.exe x64 0 NT AUTHORITY\NETWORK SERVICE C:\Windows\System32\svchost.exe

3420 600 ismserv.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\ismserv.exe

3488 600 snmp.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\snmp.exe

3500 600 dfssvc.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\dfssvc.exe

3516 600 sshd.exe x64 0 NT AUTHORITY\SYSTEM C:\openSSH\sshd.exe

3528 1632 conhost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\conhost.exe

3564 600 VGAuthService.exe x64 0 NT AUTHORITY\SYSTEM C:\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuthService.exe

3588 600 vmtoolsd.exe x64 0 NT AUTHORITY\SYSTEM C:\Program Files\VMware\VMware Tools\vmtoolsd.exe

3904 4484 wscript.exe x86 0 NT AUTHORITY\SYSTEM C:\Windows\SysWOW64\wscript.exe

3944 808 WmiPrvSE.exe x64 0 NT AUTHORITY\NETWORK SERVICE C:\Windows\System32\wbem\WmiPrvSE.exe

3956 5036 kVVdNTFDYxWxlE.exe x86 0 NT AUTHORITY\SYSTEM C:\Windows\Temp\rad67165.tmp\kVVdNTFDYxWxlE.exe

4056 600 dllhost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\dllhost.exe

4136 600 msdtc.exe x64 0 NT AUTHORITY\NETWORK SERVICE C:\Windows\System32\msdtc.exe

4360 1852 mailserver.exe x86 0 NT AUTHORITY\SYSTEM C:\Program Files (x86)\ArGo Software Design\Mail Server\mailserver.exe

4368 1852 cmd.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\cmd.exe

4376 840 conhost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\conhost.exe

4380 1852 2005335.exe x86 0 NT AUTHORITY\SYSTEM C:\Windows\students\info\2005335.exe

4388 4368 conhost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\conhost.exe

4464 600 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\svchost.exe

4484 4368 hfs.exe x86 0 NT AUTHORITY\SYSTEM C:\temp\hfs.exe

5036 4484 wscript.exe x86 0 NT AUTHORITY\SYSTEM C:\Windows\SysWOW64\wscript.exe

1. Document prepared and revised by Natalie Coull, Colin McLean, Andrea Szymkowiak [↑](#footnote-ref-1)
2. Graham, G., 2005. *The White Paper FAQ (Frequently Asked Questions)/That White Paper Guy – Gordon Graham*. [online] Available at <<https://www.thatwhitepaperguy.com/white-paper-faq-frequently-asked-questions/#what_is>> [Accessed 9 May 2016]. [↑](#footnote-ref-2)