

|  |
| --- |
| **Penetration Testing: Unveiling Common**  **Vulnerabilities**  *A Comprehensive Penetration Test and Vulnerability Assessment*  **David Dandie**  CMP210  2023/24 |

Abstract

As the world becomes increasingly digital, it is crucial for individuals and organizations to adopt and maintain robust security practices. This report delves into the ever-growing threat posed by widely recognized vulnerabilities and poor security protocols. Through an extensive penetration test, using an array of prevalent exploits and techniques, the tester not only unveils vulnerabilities but also draws the similarities between the simulated scenario and the grim reality of real-world attacks. The targeted servers were susceptible to Apache and eternal blue exploits just like the real-world attacks that happened in 2017, namely, the *notpetya* attack and the *Equifax data breach.*

The objective of this penetration test was twofold, to highlight how critical it is for robust security practices and protocols, and to shed light on the ease with which a malicious actor could gain root access to a targeted system. It was highlighted that both servers have outdated software versions and a poor password policy. Within a matter of hours, the tester, using a common attacking methodology consisting of scanning, enumeration, and system hacking, in conjunction with a variety of commonly used attacking techniques and tools was able to infiltrate the targeted network, gaining root access to both servers. The results of the penetration test demonstrate the insecurity of the network and provide a number of recommendations to ensure no such attack is possible in the future. It is imperative that not only is this report used to increase the robustness of the organizations network security, but also a reminder that poor security practices can have catastrophic consequences.

Top of Form

Contents

[1 Introduction 1](#_Toc155262844)

[1.1 Background 1](#_Toc155262845)

[1.2 Aim 2](#_Toc155262846)

[2 Procedure 4](#_Toc155262847)

[2.1 Overview of Procedure 4](#_Toc155262848)

[2.2 Foot Printing 5](#_Toc155262849)

[2.3 scanning 5](#_Toc155262850)

[2.3.1 network scan 5](#_Toc155262851)

[2.3.2 Vulnerability scanning 7](#_Toc155262852)

[2.4 Enumeration 9](#_Toc155262853)

[2.5 system hacking 15](#_Toc155262854)

[2.5.1 Password Cracking 15](#_Toc155262855)

[2.5.2 System Exploitation 20](#_Toc155262856)

[3 General Discussion 24](#_Toc155262857)

[3.1 Countermeasures 25](#_Toc155262858)

[3.2 Conclusion 26](#_Toc155262859)

[3.3 Future work 26](#_Toc155262860)

[References 28](#_Toc155262861)

[Appendices 30](#_Toc155262862)

[3.4 Appendix A 30](#_Toc155262863)

[3.4.1 Network Scan 30](#_Toc155262864)

[3.4.2 Vulnerability Scan Nessus 37](#_Toc155262865)

[3.4.3 NMAP vulnerability scan full report. 40](#_Toc155262866)

[3.5 Appendix B - Enumeration 49](#_Toc155262867)

[3.5.1 Enum4Linux Output 49](#_Toc155262868)

[3.6 Appendix C – System hacking 78](#_Toc155262869)

[3.6.1 Hash-Dump 78](#_Toc155262870)

# Introduction

## Background

In the modern digital landscape, the importance of robust digital security cannot be overstated. Organizations worldwide face a continuing threat from malicious actors with the intent to steal, disrupt and destroy. It is crucial for most organizations to keep their data secure. However, as the modern world edges forward more to a digital age, this brings with it an increasing level of financial and data security risk. There are a variety of methods a malicious actor can use to penetrate a network and steal valuable information. One of these methods caused catastrophic financial and reputational damage to a well-known credit agency, Equifax.

Information provided by csoonline (Fruhlinger.J,2020) shows that in 2017 Equifax fell victim to a cyber-attack, Hackers exploited a vulnerability in Equifax’s website software also known as CVE-2017-5638 an Apache vulnerability, compromising the personal information of 143 million individuals which is more than 40% of the United States population. The compromised data encompassed highly sensitive information such as individual’s names, addresses, dates of birth and social security numbers. Notably 200,000 of these accounts also contained full credit card information.

Although this data breach was devastating to the individual, the breach also cost Equifax over $1 billion in *“clean-up costs”* andit could have been entirely prevented had Equifax followed more robust security practices. The breach was a result of both system failures and human error. Administrators had failed to apply patches when advised and system scans, targeted at detecting vulnerabilities proved ineffective identifying the intrusion. The Equifax breach highlighted the devastating consequences of overlooking and remedying system vulnerabilities in a timely manner. *(see figure 1).*

A diagram of a network

Description automatically generated

Figure shows the timeline of events of the Equifax data breach.

Hackers don’t always want to steal, sometimes they just wish to cause as much damage as possible. Information provided by the National Cyber Security Center (2018) shows that in 2017 the world faced a catastrophic cyber-attack known as the *notpetya* attack, a malicious software that wreaked havoc globally with Ukraine the primary target. The attack crippled the government and other key infrastructure institutions. Disguised as ransomware the attack spread through trusted systems rather than over the internet, allowing it to bypass security systems in place to prevent such attacks.

Disguised under the façade of ransomware, a cyber-attack typically employed for financial gain through decryption methods, this malicious software was meticulously engineered to obliterate data, highlighting the attackers deliberate intent to cause maximum damage. Despite the primary target being Ukraine, the ramifications of this attack rippled around Europe and beyond, resulting in damages amounting to hundreds of millions of pounds. The UK government believe this attack was carried out by Russian forces, implicating the use of sophisticated techniques, specifically, the eternal blue and eternal romance exploits, exploiting vulnerabilities within SMB protocols. This incident serves as a stark reminder of the increasing cyber threats faced globally and emphasizes the need for enhanced cyber security practices and international cooperation.

With such devastating cyber-attacks taking place around the globe, pro-active measures are needed to safeguard individuals and corporations alike. Penetration testing emerges as a crucial strategy. The National Cyber Security Council (2017) defines penetration testing as "A method for gaining assurance in the security of an IT system by attempting to breach some or all of that system's security, using the same tools and techniques as an adversary might”. Penetration testing serves as a defensive weapon, employed to fortify the security of individual and corporate systems. By simulating real world cyber-attacks, organizations can identify vulnerabilities and strengthen their overall digital defense’s, ultimately mitigating the risk posed by malicious adversaries.

## Aim

The aim of this project is to conduct a comprehensive penetration test on a targeted small network by simulating real world cyber-attacks. The network consists of two servers and one client to which the login credentials have been provided, *(see table 1 and 2 respectively).*

|  |  |
| --- | --- |
| Machine Name | IP Address |
| Server1 | 192.168.10.1 |
| Server2 | 192.168.10.2 |
| Client Machine | 192.168.10.10 |

Table 1 shows the machines being targeted.

|  |  |
| --- | --- |
| Username | Password |
| test | test123 |

Table 2 shows the user credentials for the client machine.

**Additional focus areas for the penetration test:**

* **Identify vulnerabilities:** Uncover vulnerabilities and weaknesses within the network through simulating real world cyber threats, utilizing scanning and enumeration tools such as Nmap and Nessus to identify potential security gaps.
* **Exploitation techniques:** Use a wide range of common hacking techniques, using tools such as Metasploit to attack any vulnerabilities found, breaching the system with the primary objective of achieving root access.
* **Evaluate existing security measures:** Assess the effectiveness of current security measures such as but not limited to software versions, hardware configurations and password policies.
* **Emphasize robust security practices:** Highlight the importance of robust security practices, including proactive measures such as but not limited to, regular security updates, system scans, strong password policy, and user training.
* **Provide feedback and recommendations:** based on the results of the penetration test, offer comprehensive feedback and recommendations to fortify the network’s security. These recommendations should cover areas that need improvement so that no such attack should be possible in the future.

# Procedure

## Overview of Procedure

The penetration test was conducted following the industry standard 5 steps process,

* Foot Printing (open-source Intelligence)
* Network Scanning
* Enumeration
* Vulnerability Scanning
* System Hacking

Throughout this document these 5 phases are set out under several subheadings in a particular order to make more systematic sense to the reader. Network scanning and vulnerability scanning is under the “scanning” section, with sections such as “Password Hacking” and “system exploitation” under system hacking.

**Foot Printing:** A passive and effective method of collecting crucial information on an individual or organization. However, for the purposes of the following report, foot printing was not necessary as this penetration test was conducted within a controlled lab environment and key information was provided to allow a suitable foundation for a successful penetration process. Nonetheless, as it is such a crucial and effective method of gaining information on a potential target, a subheading has been included explaining OSINT in more detail.

**Scanning**: The next part of the test was the scanning phase, a critical part of any penetration test. Network scanning allows the identification of live hosts and identifies open ports and active services and versions on the hosts network. Using tools such as Nmap the networks topology was able to be mapped out, laying the foundation for further penetration activities like vulnerability scanning. Vulnerability scanning tools like NESSUS check the versions of these discovered services and reference them against databases of known vulnerabilities. The combination of both these scanning methods provided a complete insight into the targets network and allowed for further advanced attacking capabilities.

**Enumeration:** Following the scanning phase enumeration on both servers was performed allowing for more detailed information to be collected. This crucial step can unveil details such as usernames and password policies, laying the groundwork for potential brute force attacks. Additionally, the enumeration process provided valuable insights into domain information and structure. Revealing administrator user account names, allowing for more a more precise and targeted approach for future testing phases.

**System Hacking:** The next phase was the attacking phase also known as “system Hacking”. The objective of this phase was to obtain root access of the targeted system using all the information gathered from all previous stages. Beginning with password cracking, the tester utilizes tools such as hydra to brute force SMB protocols and John the ripper to crack passwords gained from hash dumping. These credentials provide a wider attack surface and more access points into the targeted system. The next phase of system hacking, “system exploitation” utilizes all previously discovered vulnerabilities to attack the system head on with the primary objective of gaining full system control.

Following the penetration test the tester then provided one of the most crucial parts of any penetration test, reporting. The report sectioned as “Discussion” discusses what the tester found during the process and the potential consequences of any vulnerabilities and system access points. Followed by “Countermeasures”, recommendations so that future attacks can become less likely, followed by any “Future work” that may be carried out using the information gathered from this penetration test.

## 2.2 Foot Printing

According to eccouncil.org(2022) open-Source Intelligence also known as “Foot printing” is primarily the first step of any penetration test, involving the collection and analysis of publicly available information to gain valuable insight into a target organization’s network. Foot printing can provide valuable data such as IP addresses, domain names, employee information and their role within the organization. It can also be used to obtain information from social media platforms, public databases, and official government websites to provide vital information to help an attacker choose a potential avenue of attack on the given organization. For the purposes of this report foot printing was not required.

## scanning

### network scan

The first step of the penetration test is to establish if the targeted servers are up. To ascertain this the tester performed a ping scan using Nmap *(see figure 1).* Nmap is a networking mapping tool used to ascertain open ports, services and versions running on targeted ports and vulnerability detection.

A screen shot of a computer

Description automatically generated

Figure 1 shows that both servers 192.168.10.1 and 192.168.10.2 are live.

In Nmap the **-sn** flag is used to perform a ping only scan it tells Nmap to skip the port scanning phase and only send an ICMP *(Internet Control Message Protocol)* to the target host, these types of scans are more commonly used when more intrusive scans are not required.

Once the tester established that the servers are live a more informative network scan was performed using the following command in Nmap. *(see figure 2).*



Figure 2 shows the command used to execute a more informative version detection scan.

The Flags used in this command by the tester where:

* **-p-:** This scans all 65535 ports, although it takes longer it ensures no open ports are missed.
* **-sV**: This flag allows for version detection on any services running on open ports.
* **-A**: This flag allows for aggressive detection of OS and service versions as well as traceroute and script scanning.
* **T5:** This flag is to set the timing to the fastest so there is minimal delay between requests. Use this flag with caution as it will be easier to detect from security systems.

Using these flags, a more comprehensive landscape of the targeted network became apparent showing which ports were open and what services were running on said ports *(see figure 3).* For full scan results for both servers see ***Appendix A*.**

**A screen shot of a computer program

Description automatically generated**

Figure 3 displays open ports, services, and their versions.

### Vulnerability scanning

### 

The next phase of the process was to gain insight into any potential vulnerabilities the target servers may have. The tester runs a series of vulnerability scans to determine this using Nessus and NMAP. Nessus, a software application owned by Tenable network security, is an advanced application used to detect misconfigurations and vulnerabilities in a target system, it comes with a variety of capabilities from basic scans to more advanced features depending on the need of the user. For the purposes of this process the tester used the basic features to scan both networks. It’s worth noting the following information to make better understanding of the Nessus output. Vulnerabilities are categorized based on a common vulnerability scoring system score. The CVSS is a numerical value given to a vulnerability based on several factors. These scores are used by security professionals, providing a points comparison allowing prioritization of vulnerability remediation. Nessus categorizes these as followed:

* **Critical:** CVSS score 9.0 – 10.0
* **High:** CVSS score 7.0 – 8.9
* **Medium:** CVSS score 4.0 – 6.9
* **Low:** CVSS score 0.0 - 3.9
* **Info:** Information that may not necessarily be vulnerability based but could contain other system weaknesses or misconfigurations.

A blue and white stripes

Description automatically generated

Figure shows the initial Nessus scan results for both servers.

Information from the Nessus scan shows that server 1 has 6 critical, 5 high, 14 medium, and 2 low vulnerabilities while having 111 information alerts *(see figure 5)*. Server 2 has 6 critical, 5 high, 11 medium, and 1 low while having 95 information alerts. On further investigation the tester realized that both servers have almost identical PHP vulnerabilities, suggesting that these servers are most likely running webservers. Refer to ***appendix A*** for full scan results for both servers.

A screenshot of a computer

Description automatically generated

Figure shows the most severe vulnerabilities for server 1.

The tester then decided to run a further vulnerability scan using Nmap to determine if any further vulnerability information could be ascertained. (*see figure 6)*

A computer screen shot

Description automatically generated

Figure shows the flags used to perform a vulnerability scan using NMAP.

The information provided by the Nmap vulnerability scan confirms that web servers are indeed running on server 1 and server 2, it also provided the tester with additional details on the contents of the server 1 webserver*. (see figure 7).*

A screen shot of a computer screen

Description automatically generated

Figure shows potentially interesting folders on server 1 port 90.

The server 1 webserver has several “interesting folders” that can be traversed for further information, notably though, the server is using an ajax file manager. Using the search function at vulners.com *(x-sisadane,2015),* the tester was able to ascertain that there was a potential exploit that can be used on this web server, *(CVE:2011-4825).*

Furthermore, the tester was also able to ascertain that web servers running on port 2025 on server 1 and port 2033 on server 2 were running an outdated and vulnerable version of an HTTP file management server, *(see figure 8)*.

A subsequent search on vulners.com (*Metasploit,2014)* uncovered the rejetto remote command exploit *(CVE:2014-6287)*, introducing another potential avenue for exploitation. For the full scan report for both servers please refer to ***appendix A.***

A screen shot of a computer

Description automatically generated

Figure shows that there is a vulnerable webserver on server 2.

The information gathered from the scanning phase has proven invaluable and provided the tester with multiple avenues of potential system exploitation for both servers. The next step entailed a detailed investigation to gather as much system information as possible.

## Enumeration

The next stage of the penetration testing process is enumeration, the enumeration stage is a deeper investigative stage that involves extracting specific details about the targeted system including but not limited to users group information, web server information, file and directory structures and system security policies and configurations. The information provided in the scanning phase provides the tester with a starting point for further investigations, the web servers. Firstly, the tester browsed one of “potentially interesting folders the README.txt. This provides the tester with login information to gain admin access to the web page. *(See figure 9).*

A screenshot of a computer program

Description automatically generated

Figure shows the login information for the web page as well as confirming the ajax file manager software.

From accessing the web server with the provided credentials, the tester was able to manipulate all aspects of the webpage, including file management and page addition as well as all aspects of security control, for before and after pictures of gained access *(see figure 10 and figure 11 respectively)*.

A screenshot of a website

Description automatically generated

Figure 0 shows the before web page on server 1 port 90.

A screenshot of a computer

Description automatically generated

Figure 11 shows the webpage after tester accessed and customized using credentials.

The confirmation of the webserver on server 1 was subsequently followed by the testers verification that there was also a file management web server port open on server 2 running an outdated version of HTTP file manager as discovered in the scanning phase. *(see figure 12).*

A screenshot of a computer

Description automatically generated

Figure 12 shows the presence of an HTTP file server on server 2 Port 2033.

The subsequent step in the enumeration process was to ascertain if the DNS zone transfer was misconfigured, if not configured correctly this can provide a wide range of valuable information such as but not limited to domain names and corresponding Ip addresses, internal naming conventions, server types and system configurations. This allows a malicious actor to refine their strategy, increasing the risk of a successful attack. Fortunately for the targeted network, the configuration did not allow for DNS zone transfers *(see figure 13).*

A screenshot of a computer

Description automatically generated

Figure 13 shows that DNS zone transfer was unsuccessful on both server 1 and server 2.

In the final stages of the enumeration phase, the main objective was to obtain a comprehensive understanding of the user landscape in the targeted system. Various enumeration techniques are available for this purpose noteworthy among them are *Polenum* and *NBTEnum,* each serving a unique purpose in unraveling specific aspects of user information.

**Polenum:** A specialized enumeration tool used for extracting detailed password policy information from a windows machine. By conducting analysis of the password guidelines on the targeted machine, polenum can uncover detailed configurations such as, password length requirements, complexity rules or expiration and lockout policies. This allows for further system target analysis and can increase the possibility of successful exploitation.

**NBTEnum**: NBTEnum on the other hand serves as a powerful tool focused on identifying users and unraveling their group affiliations within the targeted system. It reveals not only the user’s identities but also to which group they belong. This information is vital for understanding user permissions and access levels.

However, a strategic decision led the tester to use a separate technique, Enum4Linux. Enum4linux is a one size fits all enumeration tool for gaining insight into the user landscape of a targeted system, combining the enumeration power of both Polenum and NBTEnum enum4linux provides a trove of user information on a targeted system. Using the following flags, an in-depth look at the user ecosystem was uncovered. (*see figure 14).*

A close up of a computer screen

Description automatically generated

Figure 14 shows the flags used for enum4linux.

Using enum4linux the tester now has a full comprehensive insight of every user on the targeted system and their access levels. This would prove invaluable in subsequent stages of this process. The scan not only provided valuable insight into the password policy on the targeted system, knowledge that would become crucial in the password cracking aspect of this process, *(see figure 15)* but also revealed which users had domain administrative access. *(see figure 16*). For the full comprehensive enum4linux scans for both servers refer to ***appendix B****.*

A screenshot of a computer

Description automatically generated

Figure 15 shows the password policy on server 1.

A screen shot of a computer screen

Description automatically generated

Figure 16 shows all users on server 1 who have domain admin rights.

The tester performed one more enumeration scan on ports 139 and 445 to determine if the network would be potentially vulnerable to an exploit that was discussed at the beginning of this paper, eternal blue. Information from Avast(2023) shows that the eternal blue exploit takes advantage of the SMBv1 vulnerabilities and that any network running this version of SMB is at risk of potential exploitation. *(See figure 17).* For the scan results for server 2 please refer to***Appendix B***

A computer screen with white text

Description automatically generated

Figure 17 shows the SMB version that server 1 is running.

The scan shows that server 1 is running on SMBv1. This critical finding not only identifies the SMB version but also presents the tester with a potential immediate avenue of attack. Now armed with a wealth of information about the target servers the tester decided that they could proceed to the next stage of the penetration test.

## system hacking

### Password Cracking

Initially in the password cracking phase, the tester will attempt to crack as many passwords as viably possible in the attempt to gain system access and gain more information to aid further system exploitation. The tester will employ information gathered in the enumeration stage, specifically the password policy, which upon examination reveals the absence of lockout restrictions. Recognizing this vulnerability, the tester determines that a dictionary attack on the SMB services would be the most effective approach, allowing the tester to systematically attempt login an infinite number of times without lockout repercussions, maximizing the success of gaining access.

Using text files containing domain admin usernames acquired from the enum4linux scan and a compilation of the top 100 thousand most used passwords (Newsome,2023), the tester utilizes Hydra, a powerful and versatile tool integrated into kali Linux specifically designed for brute force attacks and password cracking. The tester configures hydra with the appropriate configuration to target the SMB services on the targeted system. Specifically, leveraging the tool to iteratively try combinations of domain admin usernames and passwords from the provides lists, systematically checking if any of the passwords match *(see figure 18).* Noteworthy, although this method is highly effective, it may not be the most optimal choice in all situations. Not only does it impose a significant strain on the system resources, but the heightened volume of login attempts may raise suspicions to system administrators.

*A screen shot of a computer

Description automatically generated*

figure 18 shows there was a successful login attempt of an admin user on server 1.

Using the newly acquired login credentials the tester then proceeded to log into the targeted system to confirm a successful breach. *(see figure 19).*

A screenshot of a computer

Description automatically generated

Figure 19 shows that the login credentials where correct and the tester now had full admin control of server 1.

Now that the tester had full domain admin access to the server, the objective was to maintain access. To assure this the tester provided the test account with maximum admin rights, allowing for full domain control. *(see figure 20).*

A screenshot of a computer

Description automatically generated

Figure 20 shows the test account being accredited enterprise admin access allowing for maximum access across both servers.

With maximum admin rights now obtained, it was time to acquire as many passwords for user accounts as feasibly possible. The tester will use a tool known as Metasploit. Metasploit is an open-source penetration testing platform used for developing, testing, and executing exploits on a target system. It simplifies the process of penetration testing by automating many tasks associated with the exploitation of vulnerabilities. It does this by using a variety of built in payloads to gain unauthorized access, perform post exploitation activities, and assess the overall security posture of the target system.

For the purposes of this objective the tester will use the SMB/PSexec exploit, an exploit that takes advantage of SMB vulnerabilities. Used in conjunction with the beefed-up admin test account this exploit will allow traversal through the system remotely without raising too much suspicion*. (see figure 21).*

*A screenshot of a computer

Description automatically generated*

Figure 21 shows the configuration used to gain a system shell on server 1 using the test account.

Now that the tester had full remote system access, traversal through the system can be done without detection as valid admin credentials were used. The next step was to perform a hash dump to collect all stored password hashes on the targeted system, allowing for further account compromission. To achieve this the tester attempted the ***hashdump*** command but soon realized it could not be done via the current privileges of the user (*see figure 22)*.



Figure 22 shows the hash dump command failed.

The tester then decided to migrate to another system process that has the appropriate privileges. Using the ***Ps*** command the tester was able to show a list of running system services and choose the appropriate one using the ***Migrate*** command, in this instance the service was ***dllhost.exe****.* The tester then needed to escalate the privileges of this process to system using the ***Getsystem*** command. With the appropriate permissions the tester was able to extract all stored password hashes. *(see figure 23).* For the full list of hashed passwords obtained please refer to ***Appendix C***.

A screen shot of a computer screen

Description automatically generated

Figure 23 shows that the hashdump extraction was successful.

For the next phase of the password cracking process, John the Ripper, a versatile password cracking tool renowned for its multifaceted capabilities, was employed. Specifically, it was used to execute a dictionary attack. The tool operated by using two text files, one containing the target password hashes and the other comprising a wordlist. John the Ripper systematically compared each hash against the entries in the wordlist. Upon identifying a match, the corresponding password would be considered successfully cracked. *(see figure 24).*

A computer screen shot of a program

Description automatically generated

Figure 24 shows that 14 passwords were cracked in total.

The results show that an additional 2 domain admin passwords were successfully cracked:

* **W. Holt**
* **I. Robinson**

In addition, 11 user accounts were also compromised. Although the user accounts do not have any admin rights, they can still be used to cause widespread chaos within the system, and if needed, privileges could be escalated. The tester now feels that enough evidence has been obtained to conclude the password cracking phase.

### System Exploitation

The next crucial step involved leveraging vulnerabilities identified during scanning and enumeration to exploit the targeted systems. As revealed in the enumeration stage, it was identified that server 1 was running SMBv1. Although the vulnerability scan did not detect an eternal blue vulnerability, recognizing the inherent risks associated with this version, the tester opted to employ the eternal blue exploit anyway. *(see figure 25).*

A computer screen shot of a computer

Description automatically generated

Figure 25 shows the configuration setup for the eternal blue exploit on server 1.

The tester attempted this exploit several times without success, this is a known issue with running this exploit *(see figure 26)*. However, persistence was key. After several attempts on this configuration the tester acquired a shell on the targeted system. From here the tester was able to traverse the system. *(see figure 27).*

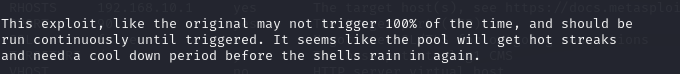
**

Figure 26 shows that multiple exploit attempts are needed for this exploit to work.

*A blurry image of a person's head

Description automatically generated*

Figure 27 shows that the tester gained shell access to server 1.

In the Nmap vulnerability scan it was also ascertained that server 1 and server 2 both had outdated HTTP file servers (version 2.3) on ports 2025 and 2033 respectively, this version as previously discussed in the scanning phase is vulnerable to the rejetto exploit, The rejetto exploit is a remote code execution exploit that facilities the execution of a payload through a meticulously crafted HTTP request(*cvedetails.com,2021*), enabling the attacker to attain root access. For the purposes of this exploit the tester decided to use server 2 as the target system*. (see figure 28).*

A screen shot of a computer

Description automatically generated

Figure 28 shows the configuration for the rejetto exploit on server 2.

With this configuration the tester was able to gain root access to the targeted system and traverse freely as a system authority. To provide evidence of breach mid-way through the system exploitation stage the tester created a text file on the test accounts desktop.  *(see figure 29 and 30 respectively).*

A screenshot of a computer

Description automatically generated

Figure 29 shows that the tester obtained root access on server 2 as a system authority using the rejetto exploit and created a text file.

A screenshot of a computer

Description automatically generated

Figure 30 shows the text file created by tester to prove system breach on the test admin account.

In the conclusive phase of system exploitation, further insights from the enumeration stage were instrumental, particularly the log1 CMS data. This valuable information revealed that the web server operated a 3rd party application, namely Ajax File Manager, responsible for the file management on the server. As previously discovered, vulners.com revealed a documented vulnerability within this software called the ajax\_create\_folder vulnerability. This vulnerability is a security flaw that can be exploited by a hacker to gain unauthorized access and manipulate files on the webserver. This can be utilized to send payloads via HTTP requests to gain remote access to the targeted system. *(see figure 31).*

A screenshot of a computer

Description automatically generated

Figure 31 shows that the tester was able to gain root access using the configuration settings shown.

The tester during the system hacking phase was able to crack numerous admin and user credentials and utilize the information gathered during the scanning and enumeration phases to gain root access both to server 1 and 2. With this in mind, the tester felt they had enough information to construct a comprehensive report, concluding the physical element of the penetration test.

# General Discussion

It was highlighted at the outset of this report, the damage that can be done with system exploits using known vulnerabilities. The similarities between Equifax’s Apache Vulnerability and the penetration tests PHP vulnerabilities highlight the relevance and persistence of these threats. Similarly, the SMBv1 vulnerabilities identified in the penetration test on server 1, where root access was obtained mirror that of the Not Petya attack that occurred in 2017. These similarities within this test are a stark reminder to system administrators that robust security practices and vulnerability awareness is needed to mitigate the damage caused by these threats.

System root access was also obtained using remote command execution exploits, namely through port 2033 on server 2 and port 90 on server 1. It is worth noting that although both where critical vulnerabilities, the ajax file manager was not flagged specifically as such via the Nmap or the Nessus vulnerability scan, it was only on further investigation that the tester was able to capitalize on the readme file discovered during the scanning process which highlighted the services and their version number. Both these vulnerabilities where possible only due to their versions being outdated. These findings highlight the importance of not only system scanning but also updating software in a timely manner.

The password cracking phase highlighted the importance of robust password policies. The fact there was no lockout restrictions allowed the tester to perform a dictionary attack on SMB services on server 1, coupled with the admin usernames acquired from the enumeration stage, the tester was able to acquire a domain admins login credential in under 4 hours. The compromised admin credentials were then used for further system exploitation, highlighting the impact of a single security lapse. The evidence shows the need for implementation of more effective password policies.

While the test conducted provided valuable insight into the security stature of the targeted network, it is important to note that there were limitations. The test was conducted within a lab environment with supplied client credentials. Because of this, target information gathering was not required. Foot printing is a fundamental and tedious part of any penetration test and had this been required, the results of the test may have differed. Additionally, the penetration test focused on known vulnerabilities. The identification zero-day vulnerabilities which are vulnerabilities not yet known and not addressed by security patches was beyond the scope of this test, however real-world attackers could use these vulnerabilities to gain system access (Stouffer, C 2023).

The purpose of this penetration test was to evaluate the targeted systems security using several widely used tools and techniques to simulate a real-world cyber-attack. The identified vulnerabilities and successful system exploitation has demonstrated the effectiveness of the penetration test, simulating, and finding potential security gaps within the targeted system. The results provided valuable insight into areas for improvement and highlighted the need for preventative security measures as well as security best practice compliance.

## Countermeasures

The report highlighted the potential avoidance of system exploits uncovered in this penetration test through regular software updates. Specifically, the HTTP file server operating on version 3.2 and Ajax file manager version 1.0 exhibited vulnerabilities to remote command execution. According to guidelines from the National Institute of Standards and Technology *(2011,2021*), applying patches beyond version 1.0 for Ajax file manager and version 2.3 for the HTTP file manager could effectively nullify the danger of this exploit.

It was also previously discussed that server 1 was only vulnerable to eternal blue due to the server running SMB protocols through SMBv1 as default. Through the SMB enumeration scan however, it was discovered that the server supports up to 3.X, with this in mind it is highly recommended that system administrators utilize the guide provided by Microsoft (Microsoft,2023) removing SMBv1 while upgrading to a more secure version to mitigate the risk any further eternal blue exploitation.

The penetration test also highlighted the importance of having a strong password policy for increasing system security. Drawing information from Microsoft 365 (Microsoft,2023), the focus is on resisting common attacks, containing successful attacks, and understanding human behavior in password creation. Admins are advised to keep passwords at least 8 characters long, avoid unnecessary complexity and eliminate periodic resets. Banning common passwords and educating users against password reuse are additional measures to increase organizations cyber defenses. In addition to robust user password rules, implementing effective lockout restrictions into an organization’s password policy is crucial for enhancing security. Lockout restrictions prevent unauthorized access by temporarily locking user accounts after a certain number of failed attempts. This mechanism serves as a deterrent to brute force attack, by limiting the number of unsuccessful login attempts, organizations can significantly reduce the risk of unauthorized system access and protect against credential-based threats. Combining effective lockout restrictions with strong user password conditions creates a formidable password policy and increases the security stature of any organization.

In Addition to the above recommendations, it is also suggested that system administrators conduct periodic internal penetration tests. It is important to know that penetration testing alone is not a quick fix but rather an enhancement to organizations process for assessing and managing vulnerabilities. As has been discovered throughout this report a penetration test can be crucial in understanding a network’s security stature and allow for remedial action to be taken on discovered vulnerabilities. While there are no guarantees in cyber security due to the dynamic nature of the cyber world, systematically utilizing the mentioned recommendations would dramatically increase the security stature of the tested network and mitigate the risk of any further similar attacks from taking place in the future.

## Conclusion

In conducting this penetration test, several critical vulnerabilities were discovered within the target network. The tester was able to utilise the outdated software versions to exploit and gain root access to the system through a variety of exploits while the inadequate password policy allowed for brute force attacks to obtain administrator user credentials and gain full system control.  
  
The penetration test conducted also emphasises the threat faced by real world organisations and the short amount of time required to gain access to a vulnerable network. it is imperative that network administrators follow the remedial action outlined in this report to ensure network fortification and counteract any further similar system breaches.

## Future work

Throughout the penetration test there were several things that were unable to be investigated due to time constraints. Some of the following services, given more time could have been exploited:

* **FTP server:** if the FTP server has weak authentication methods this could allow for easy brute force attacks.
* **DNS server:** Although this test highlighted that DNS zone transfers where not possible it may be possible to subject the DNS servers to other types of exploits such as DDos attacks (Denial of service attacks)
* **Working active directory**: Exploiting AD services could potentially lead to privilege escalation, allowing attackers to gain control over user accounts, especially if strong password policies are not in place allowing for simple brute force attacks.

While several post exploitation activities took place within this penetration test such as hash dumping, creating files and privilege escalation, If the tester had more time further activities could have been performed such as:

* **Data exfiltration:** Extracting further data such as customer details, proprietary data or other intellectual property could have been transferred to an external device owned by the attacker.
* **Network persistence:** Implementing persistent access to ensure control over the targeted system, using techniques like registry modification or back doors to ensure access even if the system is reset.
* **Disabling real time monitoring:** disable security services within the network to avoid detection while performing further activities.
* **Time stomping:** Manipulate the timestamps on files to make it difficult for network analysts to detect when files were created, modified, or accessed, complicating forensic investigations.

These are just some of the further activities the tester could have performed had more resources and time been granted. It is important to acknowledge however, scope is crucial for any penetration test and any penetration tester must work ethically and within the scope of the agreed boundaries. Additional work, if any, must have authorization from the network owner before being executed.

# References

*CSO Online. (n.d.). Equifax data breach FAQ: What happened, who was affected, what was the impact? [online] Available at:* [*https://www.google.com/amp/s/www.csoonline.com/article/567833/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html/amp/*](https://www.google.com/amp/s/www.csoonline.com/article/567833/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html/amp/)*.[Accessed 23 Nov. 2023].*

*National Cyber Security Centre (2018). Russian military ‘almost certainly’ responsible for destructive 2017 cyber-attack. [online] www.ncsc.gov.uk. Available at:* [*https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack*](https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack)*. [Accessed 23 Nov. 2023].*

*National Cyber Security Centre (2017). Penetration Testing. [online] Ncsc.gov.uk. Available at:* [*https://www.ncsc.gov.uk/guidance/penetration-testing*](https://www.ncsc.gov.uk/guidance/penetration-testing)*. [Accessed 23 Nov. 2023].*

*EC-Council (2022). Understanding the Steps of Footprinting: A Guide for Penetration Testers. [online] Cybersecurity Exchange. Available at:* [*https://www.eccouncil.org/cybersecurity-exchange/penetration-testing/footprinting-steps-penetration-testing/*](https://www.eccouncil.org/cybersecurity-exchange/penetration-testing/footprinting-steps-penetration-testing/)*.[ Accessed 23 Nov. 2023].*

*X-Cisadane (2011). Ajax File Manager File Upload Vulnerability - exploit database | Vulners.com. [online] Vulners Database. Available at:* [*https://vulners.com/zdt/1337DAY-ID-17204*](https://vulners.com/zdt/1337DAY-ID-17204) *[Accessed 23 Nov. 2023]*

*Metasploit (2014). Rejetto HTTP File Server (HFS) - Remote Command Execution (Metasploit... - exploit database | Vulners.com. [online] Vulners Database. Available at:* [*https://vulners.com/exploitdb/EDB-ID:34926*](https://vulners.com/exploitdb/EDB-ID:34926) *[Accessed 29 Nov 2023].*

*Burdova, C. (2020). What Is EternalBlue and Why Is the MS17-010 Exploit Still Relevant? [online] What Is EternalBlue and Why Is the MS17-010 Exploit Still Relevant? Available at:* [*https://www.avast.com/c-eternalblue*](https://www.avast.com/c-eternalblue)*. [Accessed 29 Nov 2023].*

*Newsome, T.C. (2023). SleepTheGod/100-000-Common-Passwords. [online] GitHub. Available at:* [*https://github.com/SleepTheGod/100-000-Common-Passwords*](https://github.com/SleepTheGod/100-000-Common-Passwords)*.[ Accessed 29 Nov 2023].*

*www.cvedetails.com. (n.d.). CVE-2014-6287 : The findMacroMarker function in parserLib.pas in Rejetto HTTP File Server (aks HFS or HttpFileServer) 2.3x before 2.3c a. [online] Available at:* [*https://www.cvedetails.com/cve/CVE-2014-6287/*](https://www.cvedetails.com/cve/CVE-2014-6287/)*[ Accessed 29 Nov 2023].*

*‌us.norton.com. (n.d.). What is a zero-day exploit? Definition and prevention tips – Norton. [online] Available at:* [*https://us.norton.com/blog/emerging-threats/zero-day-exploit*](https://us.norton.com/blog/emerging-threats/zero-day-exploit)*. [ Accessed 29 Nov 2023].*

*nvd.nist.gov. (n.d.). NVD - CVE-2011-4825. [online] Available at:* [*https://nvd.nist.gov/vuln/detail/CVE-2011-4825*](https://nvd.nist.gov/vuln/detail/CVE-2011-4825)*.[Accessed 12 Dec 2023].*

*nvd.nist.gov. (n.d.). NVD - CVE-2020-13432. [online] Available at:* [*https://nvd.nist.gov/vuln/detail/CVE-2020-13432*](https://nvd.nist.gov/vuln/detail/CVE-2020-13432)*. [Accessed 12 Dec 2023].*

*Deland-Han (2023). How to detect, enable and disable SMBv1, SMBv2, and SMBv3 in Windows. [online] learn.microsoft.com. Available at:* [*https://learn.microsoft.com/en-us/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3?tabs=server*](https://learn.microsoft.com/en-us/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3?tabs=server)*. [Accessed 12 Dec 2023].*

*KwekuA (2023). Password policy recommendations - Microsoft 365 admin. [online] learn.microsoft.com. Available at:* [*https://learn.microsoft.com/en-us/microsoft-365/admin/misc/password-policy-recommendations?view=o365-worldwide*](https://learn.microsoft.com/en-us/microsoft-365/admin/misc/password-policy-recommendations?view=o365-worldwide)*. [Accessed 12 Dec 2023].*

# Appendices

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

## Appendix A

### Network Scan

# Nmap 7.92 scan initiated Tue Dec 5 00:02:21 2023 as: nmap -p- -sV -A -T5 -oN /home/kali/Desktop/scan\_results.txt 192.168.10.1 192.168.10.2

Nmap scan report for 192.168.10.1

Host is up (0.00050s latency).

Not shown: 65500 closed tcp ports (reset)

PORT STATE SERVICE VERSION

21/tcp open ftp

| ftp-syst:

|\_ SYST: Internet Component Suite

|\_ftp-bounce: bounce working!

| fingerprint-strings:

| GenericLines:

| 220-Wellcome to Home Ftp Server!

| Server ready.

| command not understood.

| command not understood.

| Help:

| 220-Wellcome to Home Ftp Server!

| Server ready.

| 'HELP': command not understood.

| NULL, SMBProgNeg:

| 220-Wellcome to Home Ftp Server!

| Server ready.

| SSLSessionReq:

| 220-Wellcome to Home Ftp Server!

| Server ready.

|\_ command not understood.

| ftp-anon: Anonymous FTP login allowed (FTP code 230)

| drw-rw-rw- 1 ftp ftp 0 Oct 06 2022 . [NSE: writeable]

| drw-rw-rw- 1 ftp ftp 0 Oct 06 2022 .. [NSE: writeable]

|\_-rw-rw-rw- 1 ftp ftp 15 Apr 19 2017 DefaultFTP.txt [NSE: writeable]

22/tcp open ssh OpenSSH for\_Windows\_8.6 (protocol 2.0)

| ssh-hostkey:

| 3072 3a:35:12:6e:d6:62:a9:72:7e:33:94:89:b0:72:4a:b2 (RSA)

| 256 28:d7:ce:b1:78:2c:bb:2c:03:52:d6:73:c3:5d:25:b7 (ECDSA)

|\_ 256 86:89:76:b5:64:9e:8d:5b:0a:9c:d2:6d:e5:63:5c:7f (ED25519)

25/tcp open smtp ArGoSoft Freeware smtpd 1.8.2.9

|\_smtp-commands: Welcome [192.168.10.253], pleased to meet you

53/tcp open domain Simple DNS Plus

79/tcp open finger?

| finger: This is finger server\x0D

| \x0D

|\_Please use username@domain format.\x0D

| fingerprint-strings:

| FourOhFourRequest:

| This is finger server

| Sorry, user GET /nice%20ports%2C/Tri%6Eity.txt%2ebak HTTP/1.0 not found

| GenericLines:

| This is finger server

| GetRequest:

| This is finger server

| Sorry, user GET / HTTP/1.0 not found

| HTTPOptions:

| This is finger server

| Sorry, user OPTIONS / HTTP/1.0 not found

| Help:

| This is finger server

| Sorry, user HELP not found

| LPDString:

| This is finger server

| Sorry, user

| default not found

| RTSPRequest:

| This is finger server

| Sorry, user OPTIONS / RTSP/1.0 not found

| SIPOptions:

| This is finger server

|\_ Sorry, user OPTIONS sip:nm SIP/2.0 not found

80/tcp open http ArGoSoft Mail Server Freeware httpd 1.8.2.9

|\_http-title: ArGoSoft Mail Server

88/tcp open kerberos-sec Microsoft Windows Kerberos (server time: 2023-12-05 05:02:46Z)

90/tcp open http Apache httpd (PHP 5.6.30)

|\_http-server-header: Apache

|\_http-title: log1 CMS

110/tcp open pop3 ArGoSoft freeware pop3d 1.8.2.9

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

389/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: uadcwnet.com0., Site: Default-First-Site-Name)

445/tcp open microsoft-ds Windows Server 2019 Standard 17763 microsoft-ds (workgroup: UADCWNET)

464/tcp open kpasswd5?

593/tcp open ncacn\_http Microsoft Windows RPC over HTTP 1.0

636/tcp open tcpwrapped

2025/tcp open http HttpFileServer httpd 2.3

|\_http-server-header: HFS 2.3

|\_http-title: HFS /

3268/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: uadcwnet.com0., Site: Default-First-Site-Name)

3269/tcp open tcpwrapped

3389/tcp open ms-wbt-server Microsoft Terminal Services

| rdp-ntlm-info:

| Target\_Name: UADCWNET

| NetBIOS\_Domain\_Name: UADCWNET

| NetBIOS\_Computer\_Name: SERVER1

| DNS\_Domain\_Name: uadcwnet.com

| DNS\_Computer\_Name: Server1.uadcwnet.com

| DNS\_Tree\_Name: uadcwnet.com

| Product\_Version: 10.0.17763

|\_ System\_Time: 2023-12-05T05:04:44+00:00

| ssl-cert: Subject: commonName=Server1.uadcwnet.com

| Not valid before: 2023-09-20T08:09:25

|\_Not valid after: 2024-03-21T08:09:25

|\_ssl-date: 2023-12-05T05:05:08+00:00; -1s from scanner time.

5985/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

|\_http-title: Not Found

|\_http-server-header: Microsoft-HTTPAPI/2.0

9389/tcp open mc-nmf .NET Message Framing

47001/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

|\_http-server-header: Microsoft-HTTPAPI/2.0

|\_http-title: Not Found

49664/tcp open msrpc Microsoft Windows RPC

49665/tcp open msrpc Microsoft Windows RPC

49666/tcp open msrpc Microsoft Windows RPC

49667/tcp open msrpc Microsoft Windows RPC

49669/tcp open msrpc Microsoft Windows RPC

49670/tcp open ncacn\_http Microsoft Windows RPC over HTTP 1.0

49671/tcp open msrpc Microsoft Windows RPC

49672/tcp open msrpc Microsoft Windows RPC

49676/tcp open msrpc Microsoft Windows RPC

49679/tcp open msrpc Microsoft Windows RPC

49685/tcp open msrpc Microsoft Windows RPC

49703/tcp open msrpc Microsoft Windows RPC

2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :

==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============

SF-Port21-TCP:V=7.92%I=7%D=12/5%Time=656EAEF7%P=x86\_64-pc-linux-gnu%r(NULL

SF:,35,"220-Wellcome\x20to\x20Home\x20Ftp\x20Server!\r\n220\x20Server\x20r

SF:eady\.\r\n")%r(GenericLines,79,"220-Wellcome\x20to\x20Home\x20Ftp\x20Se

SF:rver!\r\n220\x20Server\x20ready\.\r\n500\x20'\r':\x20command\x20not\x20

SF:understood\.\r\n500\x20'\r':\x20command\x20not\x20understood\.\r\n")%r(

SF:Help,5A,"220-Wellcome\x20to\x20Home\x20Ftp\x20Server!\r\n220\x20Server\

SF:x20ready\.\r\n500\x20'HELP':\x20command\x20not\x20understood\.\r\n")%r(

SF:SSLSessionReq,89,"220-Wellcome\x20to\x20Home\x20Ftp\x20Server!\r\n220\x

SF:20Server\x20ready\.\r\n500\x20'\x16\x03\0\0S\x01\0\0O\x03\0\?G\xd7\xf7\

SF:xba,\xee\xea\xb2`~\xf3\0\xfd\x82{\xb9\xd5\x96\xc8w\x9b\xe6\xc4\xdb<=\xd

SF:bo\xef\x10n\0\0\(\0\x16\0\x13\0':\x20command\x20not\x20understood\.\r\n

SF:")%r(SMBProgNeg,35,"220-Wellcome\x20to\x20Home\x20Ftp\x20Server!\r\n220

SF:\x20Server\x20ready\.\r\n");

==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============

SF-Port79-TCP:V=7.92%I=7%D=12/5%Time=656EAEFC%P=x86\_64-pc-linux-gnu%r(Gene

SF:ricLines,19,"This\x20is\x20finger\x20server\r\n\r\n")%r(GetRequest,3F,"

SF:This\x20is\x20finger\x20server\r\n\r\nSorry,\x20user\x20GET\x20/\x20HTT

SF:P/1\.0\x20not\x20found\r\n")%r(Help,35,"This\x20is\x20finger\x20server\

SF:r\n\r\nSorry,\x20user\x20HELP\x20not\x20found\r\n")%r(HTTPOptions,43,"T

SF:his\x20is\x20finger\x20server\r\n\r\nSorry,\x20user\x20OPTIONS\x20/\x20

SF:HTTP/1\.0\x20not\x20found\r\n")%r(RTSPRequest,43,"This\x20is\x20finger\

SF:x20server\r\n\r\nSorry,\x20user\x20OPTIONS\x20/\x20RTSP/1\.0\x20not\x20

SF:found\r\n")%r(FourOhFourRequest,62,"This\x20is\x20finger\x20server\r\n\

SF:r\nSorry,\x20user\x20GET\x20/nice%20ports%2C/Tri%6Eity\.txt%2ebak\x20HT

SF:TP/1\.0\x20not\x20found\r\n")%r(LPDString,39,"This\x20is\x20finger\x20s

SF:erver\r\n\r\nSorry,\x20user\x20\x01default\x20not\x20found\r\n")%r(SIPO

SF:ptions,47,"This\x20is\x20finger\x20server\r\n\r\nSorry,\x20user\x20OPTI

SF:ONS\x20sip:nm\x20SIP/2\.0\x20not\x20found\r\n");

MAC Address: 00:0C:29:06:40:42 (VMware)

Aggressive OS guesses: Microsoft Windows 10 1709 - 1909 (96%), Microsoft Windows 10 1709 - 1803 (94%), Microsoft Windows Vista SP1 (93%), Microsoft Windows Server 2012 (92%), Microsoft Windows Longhorn (92%), Microsoft Windows Server 2012 R2 Update 1 (91%), Microsoft Windows Server 2016 build 10586 - 14393 (91%), Microsoft Windows 7, Windows Server 2012, or Windows 8.1 Update 1 (91%), Microsoft Windows Server 2012 or Server 2012 R2 (90%), Microsoft Windows 7 Enterprise SP1 (90%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 1 hop

Service Info: Hosts: Wellcome, SERVER1; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:

| smb2-time:

| date: 2023-12-05T05:04:50

|\_ start\_date: N/A

| smb-security-mode:

| account\_used: <blank>

| authentication\_level: user

| challenge\_response: supported

|\_ message\_signing: required

| smb-os-discovery:

| OS: Windows Server 2019 Standard 17763 (Windows Server 2019 Standard 6.3)

| Computer name: Server1

| NetBIOS computer name: SERVER1\x00

| Domain name: uadcwnet.com

| Forest name: uadcwnet.com

| FQDN: Server1.uadcwnet.com

|\_ System time: 2023-12-04T21:04:47-08:00

|\_nbstat: NetBIOS name: SERVER1, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:06:40:42 (VMware)

|\_clock-skew: mean: 1h36m00s, deviation: 3h34m41s, median: 0s

| smb2-security-mode:

| 3.1.1:

|\_ Message signing enabled and required

TRACEROUTE

HOP RTT ADDRESS

1 0.50 ms 192.168.10.1

Nmap scan report for 192.168.10.2

Host is up (0.00044s latency).

Not shown: 65505 closed tcp ports (reset)

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH for\_Windows\_8.6 (protocol 2.0)

| ssh-hostkey:

| 3072 45:6a:c2:a8:e9:68:bb:73:31:88:e8:d9:7c:a2:fa:1e (RSA)

| 256 24:64:ff:32:88:4c:e0:b3:6c:61:d5:cc:b7:3e:4d:da (ECDSA)

|\_ 256 6e:71:34:62:3a:94:81:66:da:67:a8:6f:8a:ef:d3:d8 (ED25519)

53/tcp open domain Simple DNS Plus

88/tcp open kerberos-sec Microsoft Windows Kerberos (server time: 2023-12-05 05:02:46Z)

90/tcp open http Apache httpd (PHP 5.6.30)

|\_http-server-header: Apache

|\_http-title: Site doesn't have a title (text/html; charset=UTF-8).

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

389/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: uadcwnet.com0., Site: Default-First-Site-Name)

445/tcp open microsoft-ds?

464/tcp open kpasswd5?

593/tcp open ncacn\_http Microsoft Windows RPC over HTTP 1.0

636/tcp open tcpwrapped

2033/tcp open http HttpFileServer httpd 2.3

|\_http-server-header: HFS 2.3

|\_http-title: HFS /

3268/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: uadcwnet.com0., Site: Default-First-Site-Name)

3269/tcp open tcpwrapped

3389/tcp open ms-wbt-server Microsoft Terminal Services

|\_ssl-date: 2023-12-05T05:05:08+00:00; -1s from scanner time.

| ssl-cert: Subject: commonName=Server2.uadcwnet.com

| Not valid before: 2023-09-20T08:09:33

|\_Not valid after: 2024-03-21T08:09:33

| rdp-ntlm-info:

| Target\_Name: UADCWNET

| NetBIOS\_Domain\_Name: UADCWNET

| NetBIOS\_Computer\_Name: SERVER2

| DNS\_Domain\_Name: uadcwnet.com

| DNS\_Computer\_Name: Server2.uadcwnet.com

| DNS\_Tree\_Name: uadcwnet.com

| Product\_Version: 10.0.17763

|\_ System\_Time: 2023-12-05T05:04:48+00:00

5985/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

|\_http-server-header: Microsoft-HTTPAPI/2.0

|\_http-title: Not Found

9389/tcp open mc-nmf .NET Message Framing

47001/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

|\_http-server-header: Microsoft-HTTPAPI/2.0

|\_http-title: Not Found

49664/tcp open msrpc Microsoft Windows RPC

49665/tcp open msrpc Microsoft Windows RPC

49666/tcp open msrpc Microsoft Windows RPC

49667/tcp open msrpc Microsoft Windows RPC

49669/tcp open msrpc Microsoft Windows RPC

49670/tcp open ncacn\_http Microsoft Windows RPC over HTTP 1.0

49671/tcp open msrpc Microsoft Windows RPC

49672/tcp open msrpc Microsoft Windows RPC

49676/tcp open msrpc Microsoft Windows RPC

49682/tcp open msrpc Microsoft Windows RPC

49703/tcp open msrpc Microsoft Windows RPC

55306/tcp open msrpc Microsoft Windows RPC

MAC Address: 00:0C:29:77:ED:8D (VMware)

Aggressive OS guesses: Microsoft Windows 10 1709 - 1909 (96%), Microsoft Windows 10 1709 - 1803 (94%), Microsoft Windows Server 2012 (93%), Microsoft Windows Vista SP1 (93%), Microsoft Windows Longhorn (92%), Microsoft Windows Server 2012 R2 Update 1 (91%), Microsoft Windows Server 2016 build 10586 - 14393 (91%), Microsoft Windows 7, Windows Server 2012, or Windows 8.1 Update 1 (91%), Microsoft Windows 10 1703 (91%), Microsoft Windows Server 2012 R2 (91%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 1 hop

Service Info: Host: SERVER2; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:

|\_nbstat: NetBIOS name: SERVER2, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:77:ed:8d (VMware)

| smb2-security-mode:

| 3.1.1:

|\_ Message signing enabled and required

| smb2-time:

| date: 2023-12-05T05:04:48

|\_ start\_date: N/A

TRACEROUTE

HOP RTT ADDRESS

1 0.44 ms 192.168.10.2

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

# Nmap done at Tue Dec 5 00:05:10 2023 -- 2 IP addresses (2 hosts up) scanned in 168.95 seconds

### Vulnerability Scan Nessus

**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**

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

### NMAP vulnerability scan full report.

**# Nmap 7.92 scan initiated Sun Dec 10 22:22:45 2023 as: nmap -p- -sV -T5 --script vuln -oN /home/kali/Desktop/vuln\_results.txt 192.168.10.1 192.168.10.2**

**mass\_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers**

**Nmap scan report for 192.168.10.1**

**Host is up (0.00076s latency).**

**Not shown: 65500 closed tcp ports (reset)**

**PORT STATE SERVICE VERSION**

**21/tcp open ftp**

**| fingerprint-strings:**

**| GenericLines:**

**| 220-Wellcome to Home Ftp Server!**

**| Server ready.**

**| command not understood.**

**| command not understood.**

**| Help:**

**| 220-Wellcome to Home Ftp Server!**

**| Server ready.**

**| 'HELP': command not understood.**

**| NULL, SMBProgNeg:**

**| 220-Wellcome to Home Ftp Server!**

**| Server ready.**

**| SSLSessionReq:**

**| 220-Wellcome to Home Ftp Server!**

**| Server ready.**

**|\_ command not understood.**

**22/tcp open ssh OpenSSH for\_Windows\_8.6 (protocol 2.0)**

**25/tcp open smtp ArGoSoft Freeware smtpd 1.8.2.9**

**| smtp-vuln-cve2010-4344:**

**|\_ The SMTP server is not Exim: NOT VULNERABLE**

**53/tcp open domain Simple DNS Plus**

**79/tcp open finger ArGoSoft Mail fingerd**

**80/tcp open http ArGoSoft Mail Server Freeware httpd 1.8.2.9**

**|\_http-server-header: ArGoSoft Mail Server Freeware, Version 1.8 (1.8.2.9)**

**| http-fileupload-exploiter:**

**|**

**| Couldn't find a file-type field.**

**|**

**|\_ Couldn't find a file-type field.**

**|\_http-csrf: Couldn't find any CSRF vulnerabilities.**

**|\_http-stored-xss: Couldn't find any stored XSS vulnerabilities.**

**|\_http-dombased-xss: Couldn't find any DOM based XSS.**

**88/tcp open kerberos-sec Microsoft Windows Kerberos (server time: 2023-12-11 03:23:12Z)**

**90/tcp open http Apache httpd (PHP 5.6.30)**

**| http-sql-injection:**

**| Possible sqli for queries:**

**| http://192.168.10.1:90/lightbox/js/?C=D%3BO%3DA%27%20OR%20sqlspider**

**| http://192.168.10.1:90/lightbox/js/?C=S%3BO%3DA%27%20OR%20sqlspider**

**| http://192.168.10.1:90/lightbox/js/?C=M%3BO%3DA%27%20OR%20sqlspider**

**| http://192.168.10.1:90/lightbox/js/?C=N%3BO%3DD%27%20OR%20sqlspider**

**| http://192.168.10.1:90/lightbox/js/?C=D%3BO%3DD%27%20OR%20sqlspider**

**| http://192.168.10.1:90/lightbox/js/?C=S%3BO%3DA%27%20OR%20sqlspider**

**| http://192.168.10.1:90/lightbox/js/?C=N%3BO%3DA%27%20OR%20sqlspider**

**| http://192.168.10.1:90/lightbox/js/?C=M%3BO%3DA%27%20OR%20sqlspider**

**| http://192.168.10.1:90/lightbox/js/?C=D%3BO%3DA%27%20OR%20sqlspider**

**| http://192.168.10.1:90/lightbox/js/?C=N%3BO%3DA%27%20OR%20sqlspider**

**| http://192.168.10.1:90/lightbox/js/?C=M%3BO%3DA%27%20OR%20sqlspider**

**| http://192.168.10.1:90/lightbox/js/?C=S%3BO%3DD%27%20OR%20sqlspider**

**| http://192.168.10.1:90/lightbox/js/?C=D%3BO%3DA%27%20OR%20sqlspider**

**| http://192.168.10.1:90/lightbox/js/?C=S%3BO%3DA%27%20OR%20sqlspider**

**| http://192.168.10.1:90/lightbox/js/?C=N%3BO%3DA%27%20OR%20sqlspider**

**|\_ http://192.168.10.1:90/lightbox/js/?C=M%3BO%3DD%27%20OR%20sqlspider**

**|\_http-dombased-xss: Couldn't find any DOM based XSS.**

**| http-phpself-xss:**

**| VULNERABLE:**

**| Unsafe use of $\_SERVER["PHP\_SELF"] in PHP files**

**| State: VULNERABLE (Exploitable)**

**| PHP files are not handling safely the variable $\_SERVER["PHP\_SELF"] causing Reflected Cross Site Scripting vulnerabilities.**

**|**

**| Extra information:**

**|**

**| Vulnerable files with proof of concept:**

**| http://192.168.10.1/db/head/feed.php/%27%22/%3E%3Cscript%3Ealert(1)%3C/script%3E**

**| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.10.1**

**| References:**

**| http://php.net/manual/en/reserved.variables.server.php**

**|\_ https://www.owasp.org/index.php/Cross-site\_Scripting\_(XSS)**

**| http-csrf:**

**| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.10.1**

**| Found the following possible CSRF vulnerabilities:**

**|**

**| Path: http://192.168.10.1:90/**

**| Form id: qsearch**

**| Form action: index.php**

**|**

**| Path: http://192.168.10.1:90/index.php**

**| Form id: qsearch**

**| Form action: index.php**

**|**

**| Path: http://192.168.10.1:90/admin/**

**| Form id:**

**| Form action: index.php**

**|**

**| Path: http://192.168.10.1:90/admin/index.php**

**| Form id:**

**|\_ Form action: index.php**

**|\_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)**

**|\_http-stored-xss: Couldn't find any stored XSS vulnerabilities.**

**| http-cookie-flags:**

**| /admin/:**

**| PHPSESSID:**

**| httponly flag not set**

**| /admin/index.php:**

**| PHPSESSID:**

**| httponly flag not set**

**| /Admin/:**

**| PHPSESSID:**

**| httponly flag not set**

**| /admin/libraries/ajaxfilemanager/ajaxfilemanager.php:**

**| PHPSESSID:**

**|\_ httponly flag not set**

**| http-enum:**

**| /admin/: Possible admin folder**

**| /admin/index.php: Possible admin folder**

**| /Admin/: Possible admin folder**

**| /admin/libraries/ajaxfilemanager/ajaxfilemanager.php: Log1 CMS**

**| /db/: BlogWorx Database**

**| /README.txt: Interesting, a readme.**

**| /db/: Potentially interesting folder**

**| /functions/: Potentially interesting folder**

**| /icons/: Potentially interesting folder w/ directory listing**

**|\_ /templates/: Potentially interesting folder**

**|\_http-trace: TRACE is enabled**

**|\_http-server-header: Apache**

**110/tcp open pop3 ArGoSoft freeware pop3d 1.8.2.9**

**135/tcp open msrpc Microsoft Windows RPC**

**139/tcp open netbios-ssn Microsoft Windows netbios-ssn**

**389/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: uadcwnet.com0., Site: Default-First-Site-Name)**

**445/tcp open microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: UADCWNET)**

**464/tcp open kpasswd5?**

**593/tcp open ncacn\_http Microsoft Windows RPC over HTTP 1.0**

**636/tcp open tcpwrapped**

**2025/tcp open http HttpFileServer httpd 2.3**

**|\_http-stored-xss: Couldn't find any stored XSS vulnerabilities.**

**| http-method-tamper:**

**| VULNERABLE:**

**| Authentication bypass by HTTP verb tampering**

**| State: VULNERABLE (Exploitable)**

**| This web server contains password protected resources vulnerable to authentication bypass**

**| vulnerabilities via HTTP verb tampering. This is often found in web servers that only limit access to the**

**| common HTTP methods and in misconfigured .htaccess files.**

**|**

**| Extra information:**

**|**

**| URIs suspected to be vulnerable to HTTP verb tampering:**

**| /~login [GENERIC]**

**|**

**| References:**

**| http://www.imperva.com/resources/glossary/http\_verb\_tampering.html**

**| http://capec.mitre.org/data/definitions/274.html**

**| https://www.owasp.org/index.php/Testing\_for\_HTTP\_Methods\_and\_XST\_%28OWASP-CM-008%29**

**|\_ http://www.mkit.com.ar/labs/htexploit/**

**| http-vuln-cve2011-3192:**

**| VULNERABLE:**

**| Apache byterange filter DoS**

**| State: VULNERABLE**

**| IDs: BID:49303 CVE:CVE-2011-3192**

**| The Apache web server is vulnerable to a denial of service attack when numerous**

**| overlapping byte ranges are requested.**

**| Disclosure date: 2011-08-19**

**| References:**

**| https://www.securityfocus.com/bid/49303**

**| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192**

**| https://www.tenable.com/plugins/nessus/55976**

**|\_ https://seclists.org/fulldisclosure/2011/Aug/175**

**|\_http-server-header: HFS 2.3**

**| http-fileupload-exploiter:**

**|**

**|\_ Couldn't find a file-type field.**

**|\_http-csrf: Couldn't find any CSRF vulnerabilities.**

**|\_http-dombased-xss: Couldn't find any DOM based XSS.**

**3268/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: uadcwnet.com0., Site: Default-First-Site-Name)**

**3269/tcp open tcpwrapped**

**3389/tcp open ms-wbt-server Microsoft Terminal Services**

**5985/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)**

**|\_http-csrf: Couldn't find any CSRF vulnerabilities.**

**|\_http-stored-xss: Couldn't find any stored XSS vulnerabilities.**

**|\_http-dombased-xss: Couldn't find any DOM based XSS.**

**|\_http-server-header: Microsoft-HTTPAPI/2.0**

**9389/tcp open mc-nmf .NET Message Framing**

**47001/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)**

**|\_http-stored-xss: Couldn't find any stored XSS vulnerabilities.**

**|\_http-server-header: Microsoft-HTTPAPI/2.0**

**|\_http-csrf: Couldn't find any CSRF vulnerabilities.**

**|\_http-dombased-xss: Couldn't find any DOM based XSS.**

**| http-slowloris-check:**

**| VULNERABLE:**

**| Slowloris DOS attack**

**| State: LIKELY VULNERABLE**

**| IDs: CVE:CVE-2007-6750**

**| Slowloris tries to keep many connections to the target web server open and hold**

**| them open as long as possible. It accomplishes this by opening connections to**

**| the target web server and sending a partial request. By doing so, it starves**

**| the http server's resources causing Denial Of Service.**

**|**

**| Disclosure date: 2009-09-17**

**| References:**

**| http://ha.ckers.org/slowloris/**

**|\_ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750**

**49664/tcp open msrpc Microsoft Windows RPC**

**49665/tcp open msrpc Microsoft Windows RPC**

**49666/tcp open msrpc Microsoft Windows RPC**

**49667/tcp open msrpc Microsoft Windows RPC**

**49669/tcp open msrpc Microsoft Windows RPC**

**49670/tcp open ncacn\_http Microsoft Windows RPC over HTTP 1.0**

**49671/tcp open msrpc Microsoft Windows RPC**

**49672/tcp open msrpc Microsoft Windows RPC**

**49676/tcp open msrpc Microsoft Windows RPC**

**49679/tcp open msrpc Microsoft Windows RPC**

**49685/tcp open msrpc Microsoft Windows RPC**

**49703/tcp open msrpc Microsoft Windows RPC**

**1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :**

**SF-Port21-TCP:V=7.92%I=7%D=12/10%Time=657680A0%P=x86\_64-pc-linux-gnu%r(NUL**

**SF:L,35,"220-Wellcome\x20to\x20Home\x20Ftp\x20Server!\r\n220\x20Server\x20**

**SF:ready\.\r\n")%r(GenericLines,79,"220-Wellcome\x20to\x20Home\x20Ftp\x20S**

**SF:erver!\r\n220\x20Server\x20ready\.\r\n500\x20'\r':\x20command\x20not\x2**

**SF:0understood\.\r\n500\x20'\r':\x20command\x20not\x20understood\.\r\n")%r**

**SF:(Help,5A,"220-Wellcome\x20to\x20Home\x20Ftp\x20Server!\r\n220\x20Server**

**SF:\x20ready\.\r\n500\x20'HELP':\x20command\x20not\x20understood\.\r\n")%r**

**SF:(SSLSessionReq,89,"220-Wellcome\x20to\x20Home\x20Ftp\x20Server!\r\n220\**

**SF:x20Server\x20ready\.\r\n500\x20'\x16\x03\0\0S\x01\0\0O\x03\0\?G\xd7\xf7**

**SF:\xba,\xee\xea\xb2`~\xf3\0\xfd\x82{\xb9\xd5\x96\xc8w\x9b\xe6\xc4\xdb<=\x**

**SF:dbo\xef\x10n\0\0\(\0\x16\0\x13\0':\x20command\x20not\x20understood\.\r\**

**SF:n")%r(SMBProgNeg,35,"220-Wellcome\x20to\x20Home\x20Ftp\x20Server!\r\n22**

**SF:0\x20Server\x20ready\.\r\n");**

**MAC Address: 00:0C:29:06:40:42 (VMware)**

**Service Info: Hosts: Wellcome, SERVER1; OS: Windows; CPE: cpe:/o:microsoft:windows**

**Host script results:**

**|\_smb-vuln-ms10-061: NT\_STATUS\_ACCESS\_DENIED**

**|\_smb-vuln-ms10-054: false**

**Nmap scan report for 192.168.10.2**

**Host is up (0.00074s latency).**

**Not shown: 65505 closed tcp ports (reset)**

**PORT STATE SERVICE VERSION**

**22/tcp open ssh OpenSSH for\_Windows\_8.6 (protocol 2.0)**

**53/tcp open domain Simple DNS Plus**

**88/tcp open kerberos-sec Microsoft Windows Kerberos (server time: 2023-12-11 03:23:12Z)**

**90/tcp open http Apache httpd (PHP 5.6.30)**

**|\_http-csrf: Couldn't find any CSRF vulnerabilities.**

**|\_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)**

**|\_http-stored-xss: Couldn't find any stored XSS vulnerabilities.**

**|\_http-dombased-xss: Couldn't find any DOM based XSS.**

**|\_http-trace: TRACE is enabled**

**| http-enum:**

**| /test.php: Test page**

**| /css/: Potentially interesting folder w/ directory listing**

**| /icons/: Potentially interesting folder w/ directory listing**

**|\_ /js/: Potentially interesting folder w/ directory listing**

**|\_http-server-header: Apache**

**135/tcp open msrpc Microsoft Windows RPC**

**139/tcp open netbios-ssn Microsoft Windows netbios-ssn**

**389/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: uadcwnet.com0., Site: Default-First-Site-Name)**

**445/tcp open microsoft-ds?**

**464/tcp open kpasswd5?**

**593/tcp open ncacn\_http Microsoft Windows RPC over HTTP 1.0**

**636/tcp open tcpwrapped**

**2033/tcp open http HttpFileServer httpd 2.3**

**|\_http-csrf: Couldn't find any CSRF vulnerabilities.**

**|\_http-dombased-xss: Couldn't find any DOM based XSS.**

**| http-vuln-cve2011-3192:**

**| VULNERABLE:**

**| Apache byterange filter DoS**

**| State: VULNERABLE**

**| IDs: BID:49303 CVE:CVE-2011-3192**

**| The Apache web server is vulnerable to a denial of service attack when numerous**

**| overlapping byte ranges are requested.**

**| Disclosure date: 2011-08-19**

**| References:**

**| https://www.securityfocus.com/bid/49303**

**| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192**

**| https://www.tenable.com/plugins/nessus/55976**

**|\_ https://seclists.org/fulldisclosure/2011/Aug/175**

**| http-fileupload-exploiter:**

**|**

**|\_ Couldn't find a file-type field.**

**|\_http-stored-xss: Couldn't find any stored XSS vulnerabilities.**

**| http-method-tamper:**

**| VULNERABLE:**

**| Authentication bypass by HTTP verb tampering**

**| State: VULNERABLE (Exploitable)**

**| This web server contains password protected resources vulnerable to authentication bypass**

**| vulnerabilities via HTTP verb tampering. This is often found in web servers that only limit access to the**

**| common HTTP methods and in misconfigured .htaccess files.**

**|**

**| Extra information:**

**|**

**| URIs suspected to be vulnerable to HTTP verb tampering:**

**| /~login [GENERIC]**

**|**

**| References:**

**| http://www.imperva.com/resources/glossary/http\_verb\_tampering.html**

**| http://capec.mitre.org/data/definitions/274.html**

**| https://www.owasp.org/index.php/Testing\_for\_HTTP\_Methods\_and\_XST\_%28OWASP-CM-008%29**

**|\_ http://www.mkit.com.ar/labs/htexploit/**

**| http-slowloris-check:**

**| VULNERABLE:**

**| Slowloris DOS attack**

**| State: LIKELY VULNERABLE**

**| IDs: CVE:CVE-2007-6750**

**| Slowloris tries to keep many connections to the target web server open and hold**

**| them open as long as possible. It accomplishes this by opening connections to**

**| the target web server and sending a partial request. By doing so, it starves**

**| the http server's resources causing Denial Of Service.**

**|**

**| Disclosure date: 2009-09-17**

**| References:**

**| http://ha.ckers.org/slowloris/**

**|\_ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750**

**|\_http-server-header: HFS 2.3**

**3268/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: uadcwnet.com0., Site: Default-First-Site-Name)**

**3269/tcp open tcpwrapped**

**3389/tcp open ms-wbt-server Microsoft Terminal Services**

**5985/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)**

**|\_http-csrf: Couldn't find any CSRF vulnerabilities.**

**|\_http-dombased-xss: Couldn't find any DOM based XSS.**

**|\_http-stored-xss: Couldn't find any stored XSS vulnerabilities.**

**|\_http-server-header: Microsoft-HTTPAPI/2.0**

**9389/tcp open mc-nmf .NET Message Framing**

**47001/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)**

**|\_http-stored-xss: Couldn't find any stored XSS vulnerabilities.**

**|\_http-csrf: Couldn't find any CSRF vulnerabilities.**

**|\_http-dombased-xss: Couldn't find any DOM based XSS.**

**| http-slowloris-check:**

**| VULNERABLE:**

**| Slowloris DOS attack**

**| State: LIKELY VULNERABLE**

**| IDs: CVE:CVE-2007-6750**

**| Slowloris tries to keep many connections to the target web server open and hold**

**| them open as long as possible. It accomplishes this by opening connections to**

**| the target web server and sending a partial request. By doing so, it starves**

**| the http server's resources causing Denial Of Service.**

**|**

**| Disclosure date: 2009-09-17**

**| References:**

**| http://ha.ckers.org/slowloris/**

**|\_ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750**

**|\_http-server-header: Microsoft-HTTPAPI/2.0**

**49664/tcp open msrpc Microsoft Windows RPC**

**49665/tcp open msrpc Microsoft Windows RPC**

**49666/tcp open msrpc Microsoft Windows RPC**

**49667/tcp open msrpc Microsoft Windows RPC**

**49669/tcp open msrpc Microsoft Windows RPC**

**49670/tcp open ncacn\_http Microsoft Windows RPC over HTTP 1.0**

**49671/tcp open msrpc Microsoft Windows RPC**

**49672/tcp open msrpc Microsoft Windows RPC**

**49676/tcp open msrpc Microsoft Windows RPC**

**49682/tcp open msrpc Microsoft Windows RPC**

**49703/tcp open msrpc Microsoft Windows RPC**

**55306/tcp open msrpc Microsoft Windows RPC**

**MAC Address: 00:0C:29:77:ED:8D (VMware)**

**Service Info: Host: SERVER2; OS: Windows; CPE: cpe:/o:microsoft:windows**

**Host script results:**

**|\_samba-vuln-cve-2012-1182: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR**

**|\_smb-vuln-ms10-054: false**

**|\_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR**

**Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .**

**# Nmap done at Sun Dec 10 22:34:10 2023 -- 2 IP addresses (2 hosts up) scanned in 684.37 seconds**

## Appendix B - Enumeration

### Enum4Linux Output

**┌──(root㉿kali)-[~]**

**└─# enum4linux -a -u test -p test123 192.168.10.1**

**Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Tue Dec 12 04:44:50 2023**

**=========================================( 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-29-06-40-42**

**===================================( 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 )===================================**

**[E] Can't get OS info with 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: 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]**

**=================================( 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 Writing: N/A**

**//192.168.10.1/C$ Mapping: DENIED Listing: N/A Writing: N/A**

**//192.168.10.1/Fileshare1 Mapping: OK Listing: OK Writing: N/A**

**//192.168.10.1/Fileshare2 Mapping: OK Listing: OK Writing: N/A**

**//192.168.10.1/HR Mapping: OK Listing: OK Writing: N/A**

**[E] Can't understand response:**

**NT\_STATUS\_NO\_SUCH\_FILE listing \\***

**//192.168.10.1/IPC$ Mapping: N/A Listing: N/A Writing: N/A**

**//192.168.10.1/NETLOGON Mapping: OK Listing: OK Writing: N/A**

**//192.168.10.1/Resources Mapping: OK Listing: OK Writing: N/A**

**//192.168.10.1/SYSVOL Mapping: OK Listing: OK Writing: N/A**

**//192.168.10.1/SYSVOL2 Mapping: OK Listing: OK Writing: N/A**

**============================( 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: 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**

**[+] Retieved partial password policy with rpcclient:**

**Password Complexity: Disabled**

**Minimum Password Length: 7**

**=======================================( 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: Administrators' (RID: 544) has member: UADCWNET\Administrator**

**Group: Administrators' (RID: 544) has member: UADCWNET\Enterprise Admins**

**Group: Administrators' (RID: 544) has member: UADCWNET\Domain Admins**

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

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

**Group: Pre-Windows 2000 Compatible Access' (RID: 554) has member: NT AUTHORITY\Authenticated Users**

**Group: Users' (RID: 545) has member: NT AUTHORITY\INTERACTIVE**

**Group: Users' (RID: 545) has member: NT AUTHORITY\Authenticated Users**

**Group: Users' (RID: 545) has member: UADCWNET\Domain Users**

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

**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\W.Holt**

**[+] 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 Computers' (RID: 515) has member: UADCWNET\marketplace$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\pc28$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\range86-130$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\nt4$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\cust84$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\devserver$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\about$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\helponline$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\sanantonio$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\inbound$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\customer$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\ir$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\announce$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\iris$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\dev1$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\cust24$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\mx$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\vader$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\cust53$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\mv$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\mickey$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\ptld$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\tool$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\uninet$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\houstin$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\CLIENT1$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL1$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL2$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL3$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL4$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL5$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL6$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL7$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL8$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL9$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL10$**

**Group: '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\test**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\K.Thompson**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\V.Nelson**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\L.Gill**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\N.May**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\W.Holt**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\J.Wheeler**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\F.Payne**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\T.Oliver**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\J.Poole**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\N.Wells**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\N.Hogan**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\M.Adams**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\Y.Marshall**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\W.Wolfe**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\A.Kennedy**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\T.Fuller**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\L.Washington**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\S.Shelton**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\J.Farmer**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\M.Paul**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\B.Wong**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\D.Ford**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\M.Daniel**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\D.Brooks**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\B.Rice**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\P.Powers**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\S.Wright**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\L.Williamson**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\G.Malone**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\M.Harrington**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\H.Mclaughlin**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\G.Turner**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\P.Rodriquez**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\L.Thornton**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\D.Murray**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\A.Peters**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\M.Padilla**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\J.Becker**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\K.Perkins**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\M.Murphy**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\S.Higgins**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\B.Lewis**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\F.Sanders**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\R.Soto**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\I.Robinson**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\B.Yates**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\E.Frazier**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\G.Francis**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\J.Shaw**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\G.Adkins**

**Group: 'Domain Admins' (RID: 512) has member: UADCWNET\Administrator**

**Group: 'Domain Admins' (RID: 512) has member: UADCWNET\W.Holt**

**Group: 'Domain Admins' (RID: 512) has member: UADCWNET\L.Washington**

**Group: 'Domain Admins' (RID: 512) has member: UADCWNET\M.Padilla**

**Group: 'Domain Admins' (RID: 512) has member: UADCWNET\I.Robinson**

**Group: 'Domain Admins' (RID: 512) has member: UADCWNET\B.Yates**

**Group: 'Domain Admins' (RID: 512) has member: UADCWNET\J.Shaw**

**Group: 'Information Technology' (RID: 1108) has member: UADCWNET\test**

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

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

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

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

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

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

**==================( 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-1-5-21-2373017989-4057782597-2990666611**

**[I] Found new SID:**

**S-1-5-32**

**[I] Found new SID:**

**S-1-5-32**

**[I] Found new SID:**

**S-1-5-32**

**[I] Found new SID:**

**S-1-5-32**

**[I] Found new SID:**

**S-1-5-32**

**[I] Found new SID:**

**S-1-5-32**

**[I] Found new SID:**

**S-1-5-32**

**[I] Found new SID:**

**S-1-5-21-2373017989-4057782597-2990666611**

**[+] Enumerating users using SID S-1-5-80 and logon username 'test', password 'test123'**

**[+] Enumerating users using SID S-1-5-90 and logon username 'test', password 'test123'**

**[+] Enumerating users using SID S-1-5-32 and logon username 'test', password 'test123'**

**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-1-5-32-548 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)**

**[+] Enumerating users using SID S-1-5-80-3139157870-2983391045-3678747466-658725712 and logon username 'test', password 'test123'**

**[+] 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-1-5-21-2373017989-4057782597-2990666611-512 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)**

**[+] Enumerating users using SID S-1-5-21-3909509232-362358561-949330273 and logon username 'test', password 'test123'**

**S-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)**

**===============================( Getting printer info for 192.168.10.1 )===============================**

**No printers returned.**

**Server 2 Enum4linux**

**┌──(root㉿kali)-[~]**

**└─# enum4linux -a -u test -p test123 192.168.10.2**

**Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Tue Dec 12 04:47:12 2023**

**=========================================( Target Information )=========================================**

**Target ........... 192.168.10.2**

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

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

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

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

**============================( Enumerating Workgroup/Domain on 192.168.10.2 )============================**

**[+] Got domain/workgroup name: UADCWNET**

**================================( Nbtstat Information for 192.168.10.2 )================================**

**Looking up status of 192.168.10.2**

**SERVER2 <00> - B <ACTIVE> Workstation Service**

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

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

**SERVER2 <20> - B <ACTIVE> File Server Service**

**MAC Address = 00-0C-29-77-ED-8D**

**===================================( Session Check on 192.168.10.2 )===================================**

**[+] Server 192.168.10.2 allows sessions using username 'test', password 'test123'**

**================================( Getting domain SID for 192.168.10.2 )================================**

**Domain Name: UADCWNET**

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

**[+] Host is part of a domain (not a workgroup)**

**===================================( OS information on 192.168.10.2 )===================================**

**[E] Can't get OS info with smbclient**

**[+] Got OS info for 192.168.10.2 from srvinfo:**

**192.168.10.2 Wk Sv BDC Tim NT**

**platform\_id : 500**

**os version : 10.0**

**server type : 0x801033**

**=======================================( Users on 192.168.10.2 )=======================================**

**index: 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]**

**=================================( Share Enumeration on 192.168.10.2 )=================================**

**do\_connect: Connection to 192.168.10.2 failed (Error NT\_STATUS\_RESOURCE\_NAME\_NOT\_FOUND)**

**Sharename Type Comment**

**--------- ---- -------**

**ADMIN$ Disk Remote Admin**

**C$ Disk Default share**

**IPC$ IPC Remote IPC**

**NETLOGON Disk Logon server share**

**SYSVOL Disk Logon server share**

**Reconnecting with SMB1 for workgroup listing.**

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

**[+] Attempting to map shares on 192.168.10.2**

**//192.168.10.2/ADMIN$ Mapping: DENIED Listing: N/A Writing: N/A**

**//192.168.10.2/C$ Mapping: DENIED Listing: N/A Writing: N/A**

**[E] Can't understand response:**

**NT\_STATUS\_NO\_SUCH\_FILE listing \\***

**//192.168.10.2/IPC$ Mapping: N/A Listing: N/A Writing: N/A**

**//192.168.10.2/NETLOGON Mapping: OK Listing: OK Writing: N/A**

**//192.168.10.2/SYSVOL Mapping: OK Listing: OK Writing: N/A**

**============================( Password Policy Information for 192.168.10.2 )============================**

**[+] Attaching to 192.168.10.2 using test:test123**

**[+] Trying protocol 139/SMB...**

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

**[+] Trying protocol 445/SMB...**

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

**[+] UADCWNET**

**[+] Builtin**

**[+] Password Info for Domain: UADCWNET**

**[+] Minimum password length: 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**

**[+] Retieved partial password policy with rpcclient:**

**Password Complexity: Disabled**

**Minimum Password Length: 7**

**=======================================( Groups on 192.168.10.2 )=======================================**

**[+] Getting builtin groups:**

**group:[Administrators] rid:[0x220]**

**group:[Users] rid:[0x221]**

**group:[Guests] rid:[0x222]**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**group:[Replicator] rid:[0x228]**

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

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

**group:[Server Operators] rid:[0x225]**

**[+] Getting builtin group memberships:**

**Group: Administrators' (RID: 544) has member: UADCWNET\Domain Admins**

**Group: Administrators' (RID: 544) has member: UADCWNET\Enterprise Admins**

**Group: Administrators' (RID: 544) has member: UADCWNET\Administrator**

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

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

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

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

**Group: Users' (RID: 545) has member: UADCWNET\Domain Users**

**Group: Users' (RID: 545) has member: NT AUTHORITY\Authenticated Users**

**Group: Users' (RID: 545) has member: NT AUTHORITY\INTERACTIVE**

**Group: Pre-Windows 2000 Compatible Access' (RID: 554) has member: NT AUTHORITY\Authenticated Users**

**[+] Getting local groups:**

**group:[Cert Publishers] rid:[0x205]**

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

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

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

**group:[DnsAdmins] rid:[0x44d]**

**[+] Getting local group memberships:**

**Group: DnsAdmins' (RID: 1101) has member: UADCWNET\W.Holt**

**Group: Denied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Cert Publishers**

**Group: Denied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Domain Admins**

**Group: Denied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Schema Admins**

**Group: Denied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Enterprise Admins**

**Group: Denied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Group Policy Creator Owners**

**Group: Denied RODC Password Replication Group' (RID: 572) has member: UADCWNET\krbtgt**

**Group: Denied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Domain Controllers**

**Group: Denied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Read-only Domain Controllers**

**[+] Getting domain groups:**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**group:[DnsUpdateProxy] rid:[0x44e]**

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

**group:[Legal] rid:[0x450]**

**group:[Finance] rid:[0x451]**

**group:[Engineering] rid:[0x452]**

**group:[Sales] rid:[0x453]**

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

**[+] Getting domain group memberships:**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\krbtgt**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\Administrator**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\test**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\K.Thompson**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\V.Nelson**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\L.Gill**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\N.May**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\W.Holt**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\J.Wheeler**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\F.Payne**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\T.Oliver**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\J.Poole**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\N.Wells**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\N.Hogan**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\M.Adams**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\Y.Marshall**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\W.Wolfe**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\A.Kennedy**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\T.Fuller**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\L.Washington**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\S.Shelton**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\J.Farmer**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\M.Paul**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\B.Wong**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\D.Ford**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\M.Daniel**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\D.Brooks**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\B.Rice**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\P.Powers**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\S.Wright**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\L.Williamson**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\G.Malone**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\M.Harrington**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\H.Mclaughlin**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\G.Turner**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\P.Rodriquez**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\L.Thornton**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\D.Murray**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\A.Peters**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\M.Padilla**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\J.Becker**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\K.Perkins**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\M.Murphy**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\S.Higgins**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\B.Lewis**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\F.Sanders**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\R.Soto**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\I.Robinson**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\B.Yates**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\E.Frazier**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\G.Francis**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\J.Shaw**

**Group: 'Domain Users' (RID: 513) has member: UADCWNET\G.Adkins**

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

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

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\marketplace$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\pc28$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\range86-130$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\nt4$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\cust84$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\devserver$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\about$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\helponline$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\sanantonio$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\inbound$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\customer$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\ir$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\announce$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\iris$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\dev1$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\cust24$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\mx$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\vader$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\cust53$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\mv$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\mickey$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\ptld$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\tool$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\uninet$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\houstin$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\CLIENT1$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL1$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL2$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL3$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL4$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL5$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL6$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL7$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL8$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL9$**

**Group: 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL10$**

**Group: 'Information Technology' (RID: 1108) has member: UADCWNET\test**

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

**Group: 'Domain Admins' (RID: 512) has member: UADCWNET\Administrator**

**Group: 'Domain Admins' (RID: 512) has member: UADCWNET\W.Holt**

**Group: 'Domain Admins' (RID: 512) has member: UADCWNET\L.Washington**

**Group: 'Domain Admins' (RID: 512) has member: UADCWNET\M.Padilla**

**Group: 'Domain Admins' (RID: 512) has member: UADCWNET\I.Robinson**

**Group: 'Domain Admins' (RID: 512) has member: UADCWNET\B.Yates**

**Group: 'Domain Admins' (RID: 512) has member: UADCWNET\J.Shaw**

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

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

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

**==================( Users on 192.168.10.2 via RID cycling (RIDS: 500-550,1000-1050) )==================**

**[I] Found new SID:**

**S-1-5-21-2373017989-4057782597-2990666611**

**[I] Found new SID:**

**S-1-5-21-2373017989-4057782597-2990666611**

**[I] Found new SID:**

**S-1-5-32**

**[I] Found new SID:**

**S-1-5-32**

**[I] Found new SID:**

**S-1-5-32**

**[I] Found new SID:**

**S-1-5-32**

**[I] Found new SID:**

**S-1-5-32**

**[I] Found new SID:**

**S-1-5-32**

**[I] Found new SID:**

**S-1-5-32**

**[I] Found new SID:**

**S-1-5-21-2373017989-4057782597-2990666611**

**[+] Enumerating users using SID S-1-5-32 and logon username 'test', password 'test123'**

**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-1-5-32-548 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)**

**[+] Enumerating users using SID S-1-5-90 and logon username 'test', password 'test123'**

**[+] Enumerating users using SID S-1-5-21-4039629344-2512537879-3147035361 and logon username 'test', password 'test123'**

**S-1-5-21-4039629344-2512537879-3147035361-500 SERVER2\Administrator (Local User)**

**S-1-5-21-4039629344-2512537879-3147035361-501 SERVER2\Guest (Local User)**

**S-1-5-21-4039629344-2512537879-3147035361-503 SERVER2\DefaultAccount (Local User)**

**S-1-5-21-4039629344-2512537879-3147035361-504 SERVER2\WDAGUtilityAccount (Local User)**

**S-1-5-21-4039629344-2512537879-3147035361-513 SERVER2\None (Domain Group)**

**[+] Enumerating users using SID S-1-5-80-3139157870-2983391045-3678747466-658725712 and logon username 'test', password 'test123'**

**[+] 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-1-5-21-2373017989-4057782597-2990666611-512 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)**

**[+] Enumerating users using SID S-1-5-80 and logon username 'test', password 'test123'**

**===============================( Getting printer info for 192.168.10.2 )===============================**

**No printers returned.**

**enum4linux complete on Tue Dec 12 04:47:41 2023**

**enum4linux complete on Tue Dec 12 04:45:18 2023**

**A computer screen shot of a program

Description automatically generated**

## Appendix C – System hacking

### Hash-Dump

**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:0637b59972afd98cce4e82a489c6ab38:::**

**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:ab5f6d7688ffe080bea5d7908f30ab89:::**

**CLIENT1$:1601:aad3b435b51404eeaad3b435b51404ee:c85db885f072fc084f3acc041947c427:::**

**MSSQL1$:2691:aad3b435b51404eeaad3b435b51404ee:781dacd2eb93ba3d94306bd5e3f1c059:::**

**MSSQL2$:2692:aad3b435b51404eeaad3b435b51404ee:49367e9c86ffead10e6f03c93655e9cb:::**

**MSSQL3$:2693:aad3b435b51404eeaad3b435b51404ee:ae008065775102ea4d5cfedea2a81a06:::**

**MSSQL4$:2694:aad3b435b51404eeaad3b435b51404ee:d4d903dd474c0934b422622bf746a682:::**

**MSSQL5$:2695:aad3b435b51404eeaad3b435b51404ee:93117b81ef394634afaabf37630ccf05:::**

**MSSQL6$:2696:aad3b435b51404eeaad3b435b51404ee:ff9605652929b00769f74958f6645ebe:::**

**MSSQL7$:2697:aad3b435b51404eeaad3b435b51404ee:a6603c971c056a913dbaea13ff533814:::**

**MSSQL8$:2698:aad3b435b51404eeaad3b435b51404ee:93dac4cc23b4e6346114dee976226337:::**

**MSSQL9$:2699:aad3b435b51404eeaad3b435b51404ee:5f976c01fe34c7fb28d4bea18e5e7078:::**

**MSSQL10$:2700:aad3b435b51404eeaad3b435b51404ee:d9f9018c7ca05566fd73a2a5a2551a9d:::**