

|  |
| --- |
| **Network Penetration Testing**  White paper for Ethical Hacking 1 module  **Luke Burgess**  CMP210: Professional Project Development & Delivery  BSc Ethical Hacking Year 2  2018/19 |

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

Abstract

This whitepaper takes the reader through the actions taken to successfully penetration test the Typical Company network and investigate any identified security risks using a trusted methodology. Each step in the process will be fully document with reference to appendices.

After initial information gathering, completed nmap scans revealed a number of open TCP and UDP ports for both Server1 and Server2 which were vulnerable to both DOS attacks and Eternal Blue through the use of Metasploit.

Nbtenum v3.3 results provided information on the name/domain for all users and user groups. After exploiting both servers with Eternal Blue, password hashes were dumped to text files, of which many user’s passwords were uncovered with the use of Cain dictionary attacks. Once compared to the Nbtenum findings, admin accounts were then logged in to and used to escalate privileges of the test account to be part of the admin groups. A .txt file was also left to confirm successful exploit.

Conclusions were drawn that netbios-ssn port 139 was unsafe and easily exploitable and that many users had insecure and weak passwords.

+Contents

[1 Introduction 1](#_Toc532922144)

[1.1 Background 1](#_Toc532922145)

[1.2 Aim 2](#_Toc532922146)

[2 Procedure and Results 3](#_Toc532922147)

[2.1 Overview of Procedure 3](#_Toc532922148)

[2.2 Footprinting 3](#_Toc532922149)

[2.3 Scanning 3](#_Toc532922150)

[2.3.1 Ping 3](#_Toc532922151)

[2.3.2 TRACERT 4](#_Toc532922152)

[2.3.3 NETSTAT 5](#_Toc532922153)

[2.3.4 TELNET 5](#_Toc532922154)

[2.3.5 NMAP TCP 6](#_Toc532922155)

[2.3.6 NMAP UDP 7](#_Toc532922156)

[2.3.7 NMAP OS 9](#_Toc532922157)

[2.3.8 Nessus 10](#_Toc532922158)

[2.4 Enumeration 13](#_Toc532922159)

[2.4.1 NMAP Vulnerability Scans 13](#_Toc532922160)

[2.4.2 NBT Enumeration 14](#_Toc532922161)

[2.4.3 RPCClient 14](#_Toc532922162)

[2.5 System Hacking 15](#_Toc532922163)

[2.5.1 Eternal Blue 15](#_Toc532922164)

[2.5.2 Cain Password Cracker 19](#_Toc532922165)

[2.6 Advanced Phases 21](#_Toc532922166)

[2.6.1 Hash Dump 21](#_Toc532922167)

[2.6.2 Cain Password Cracker 22](#_Toc532922168)

[3 Discussion 25](#_Toc532922169)

[3.1 General Discussion 25](#_Toc532922170)

[3.2 Countermeasures 25](#_Toc532922171)

[3.3 Conclusions 26](#_Toc532922172)

[3.4 Future Work 26](#_Toc532922173)

[3.5 Call to action 26](#_Toc532922174)

[4 Bibliography 27](#_Toc532922175)

[Appendices 28](#_Toc532922176)

[Appendix A – NBTENUM Server1 28](#_Toc532922177)

[Appendix B – nbtenum Server2 35](#_Toc532922178)

[Appendix C 42](#_Toc532922179)

[Appendix D 46](#_Toc532922180)

[Appendix C 51](#_Toc532922181)

[Appendix C 51](#_Toc532922182)

[Appendix D - Include your project deliverables and requirements sheet 52](#_Toc532922183)

# Introduction

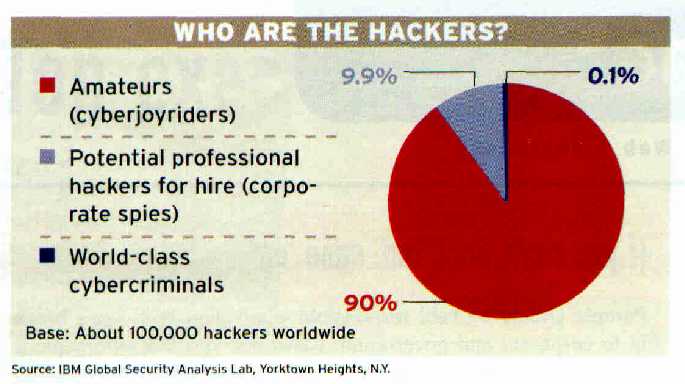
## Background

This network penetration testing report, completed for Typical Co. is written as a comprehensive analysis of the network with the use of information gathering and hacking tools to exploit and report on the level of security it provides. This is to be carried out from the position of a malicious attacker with access to a user account with no special privileges.

Security reviews are a vital task to be completed for every IT company, regardless of the size. A common misconception is that small businesses are not a priority to hackers however according to (Solutions, 2018), “43% of cyber-attacks target small business”. These costs businesses hundreds of millions of pounds every year, often due to security flaws which can be easily prevented.

As shown in figure 1 (Csciwww, 2018), the vast majority of hackers are amateur hackers, which would suggest taking precautions and employing professional penetration testers to review your security is a very effective measure to protect both the company and the individual person’s data to prevent monetary loss and comply with the Data Protection Act 2018 and prevent hackers who may intend to gain “Unauthorised access to computer material” (Legislation.gov.uk, 2018) as per the Computer Misuse Act 1990.

**Figure 1:**



All findings are kept confidential and will not be documented outside of this report as agreed under contract and in accordance with the Data Protection Act 2018. No attempts are to be made on any networks, client desktops or servers not detailed by the Typical Co. as Server1, Server2, Client1, Client2.

The most common faults in the integrity of a security system is user error – employees using insecure passwords or setting up software incorrectly – and also outdated software being used for example, a version of Windows operating system which is no longer supported and updated by Microsoft.

## Aim

The aim of this penetration test is to gather information about the network and find any security flaws, to report and highlight vulnerabilities and attempt to exploit them to access admin accounts and give the test account the admin privileges. Following this, countermeasures are to be researched and reported on to prevent this happening in a malicious attack.

# Procedure and Results

## Overview of Procedure

The Firstbase Techies methodology is implemented for testing and reporting on the network provided. This methodology implements Footprinting, Scanning, Enumeration, System Hacking and Advanced Phase stages to successfully identify security flaws and pitfalls while reporting on this with appendices and solutions to these issues.

This methodology was chosen because it is great and also is a tried and tested method used by the first base company which is a large business in the industry, and also due to its very clear steps taken through.

## Footprinting

For this task, footprinting cannot be completed as the penetration testing was on an offline network, and therefore it will not exist in search engines or websites. The methods in which you would use for this part of this methodology would include using regional IP registries for example RIPE or ARIN. There is also whois and other domain searches which will provide information in regards to a domain/IP such as DNSstuff.com and also sub domain tools such as DNSdumpster.com and censys.io.

## Scanning

### Ping

This is a command which is used to send a packet to the target IP address to use the three-way handshake to confirm if a computer or server is online by encouraging it to reply with an acknowledgement packet. It also shows the time it took for packets to be sent back. Please see figures below for ping requests. This was carried out on the three other IPs not already logged in to.

Figure 2

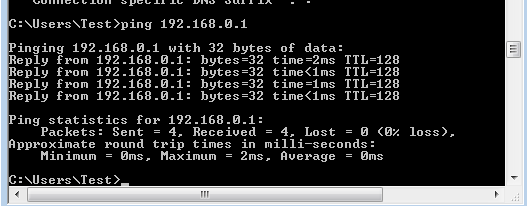


Figure 3

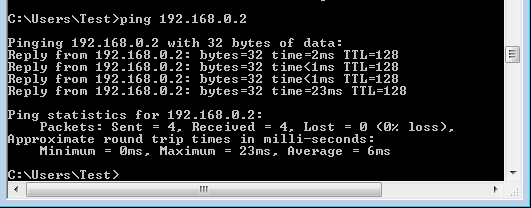
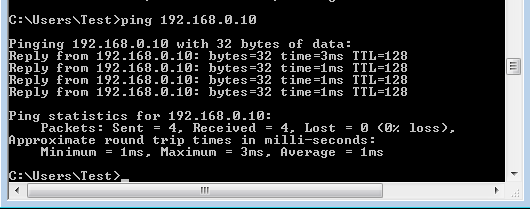


Figure 4



### TRACERT

This command is short for trace route and in a literal sense, traces the route a packet takes from the origin source to the target IP. This was carried out on Server1, Server2, and Client1 as shown in this figures below. This was a direct route to the destination as it is on a small closed network.

Figure 5

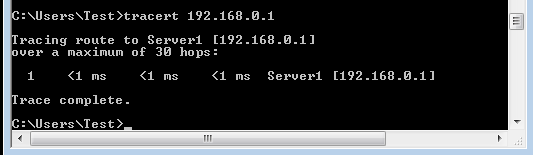
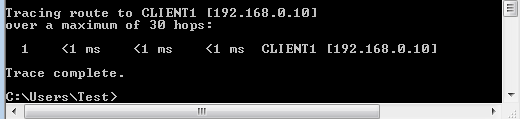


Figure 6



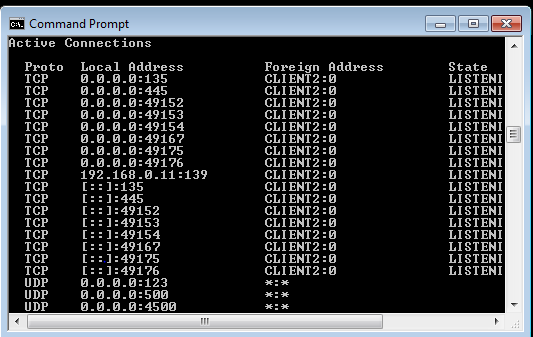
Figure 7



### NETSTAT

The netstat command is used to gather information on active connections a computer/server has. This was run on server 1 which showed an active connection with client 2 which I was using as shown in figure 8 below with a connection with 192.168.0.11 (client 2) using port 139.

Figure 8



I thereafter searched for uses for port 139 which revealed “Once an attacker has located an active Port 139 on a device, he can run **NBSTAT** a diagnostic tool for NetBIOS over TCP/IP” (thewindowsclub, 2018).

### TELNET

TELNET command will confirm if a computer is running Telnet, this was used as a means to confirm if the targets were using it. This was confirmed for Server1 and Server2 only as show below.

Figure 9

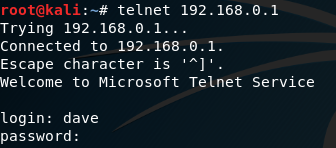


Figure 10

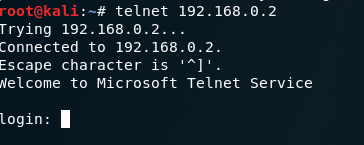
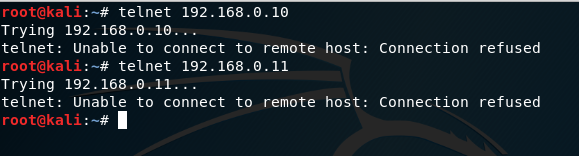


Figure 11



### NMAP TCP

NMAP scans can have many different purposes. A NMAP -sT scan was run to see which TCP ports were open for each IP. This confirmed Server1 port 139 had the service netbios – ssn which as previously discovered is vulnerable to attacks. It also showed the telnet service which may be of use later. This is shown in figure 9.

Figure 12

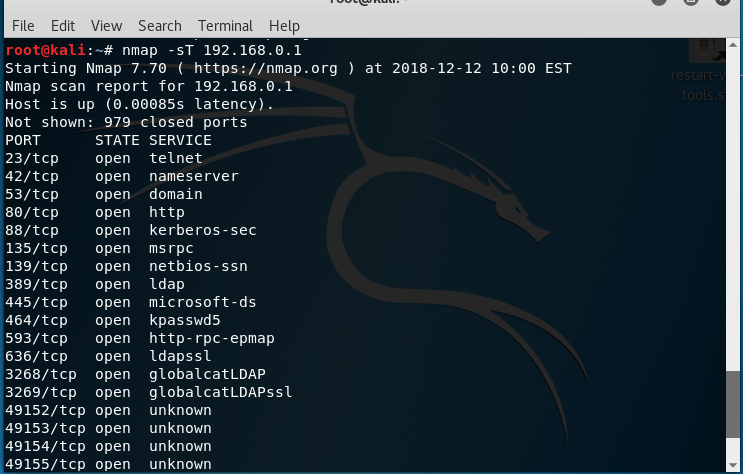


Figure 13

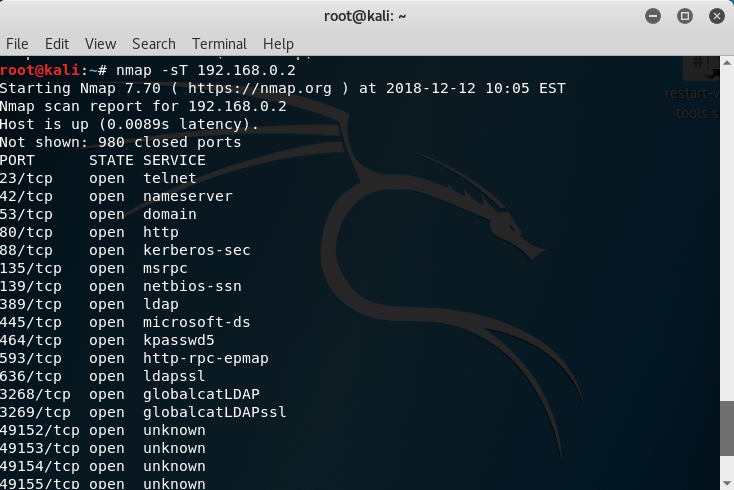
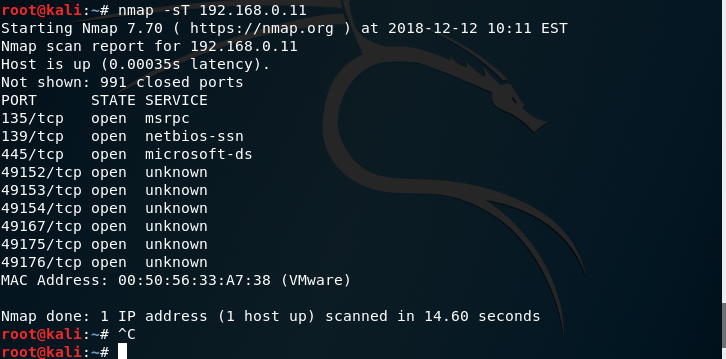


Figure 14



Figure 15



### NMAP UDP

The nmap – sU command may be used to check which UDP ports on an IP are currently running. This was also run on all computers as shown in the figures below.

Figure 16

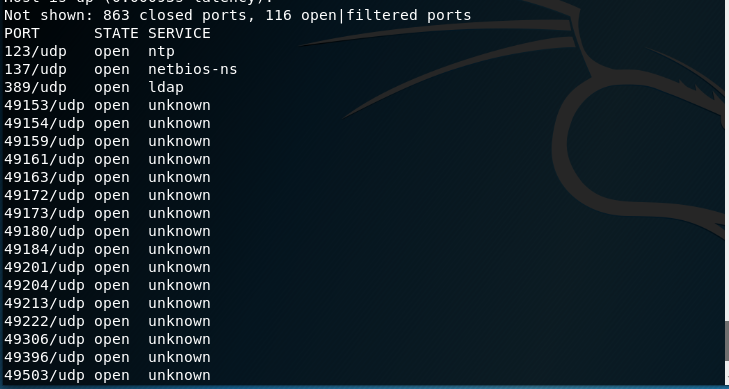


Figure 17

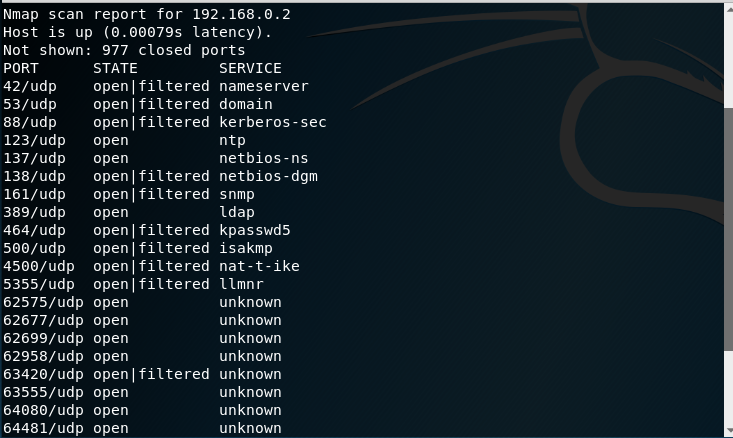


Figure 18

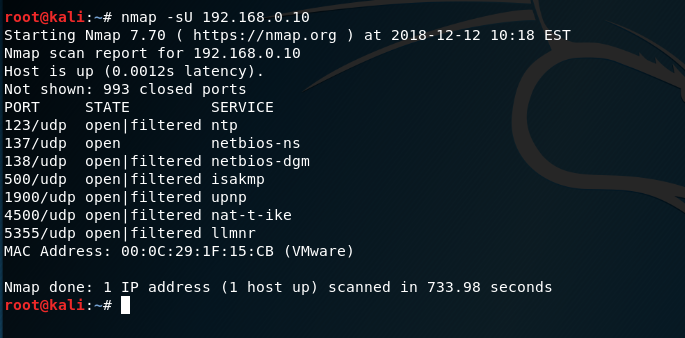
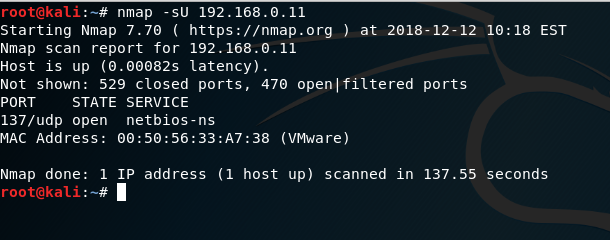


Figure 19



### NMAP OS

The nmap –O scans were completed to attempt to find out which operating system the computers were running on. It showed that all computers were likely running on Windows 7, 8.1 or Windows Server 2008 as per figures below.

Figure 20

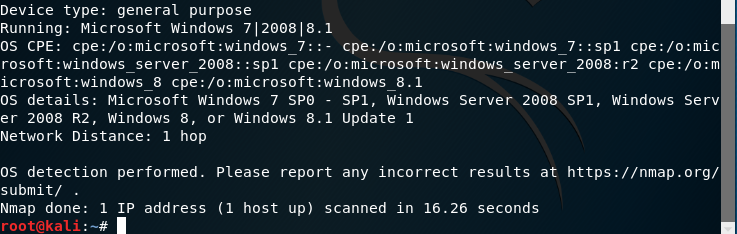
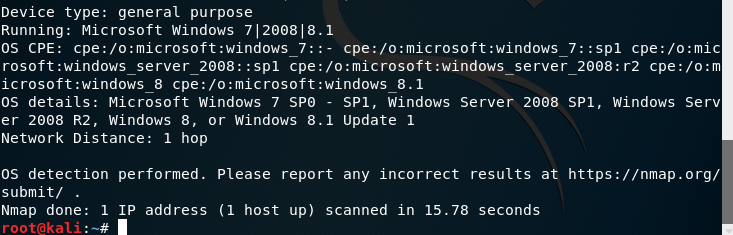


Figure 21



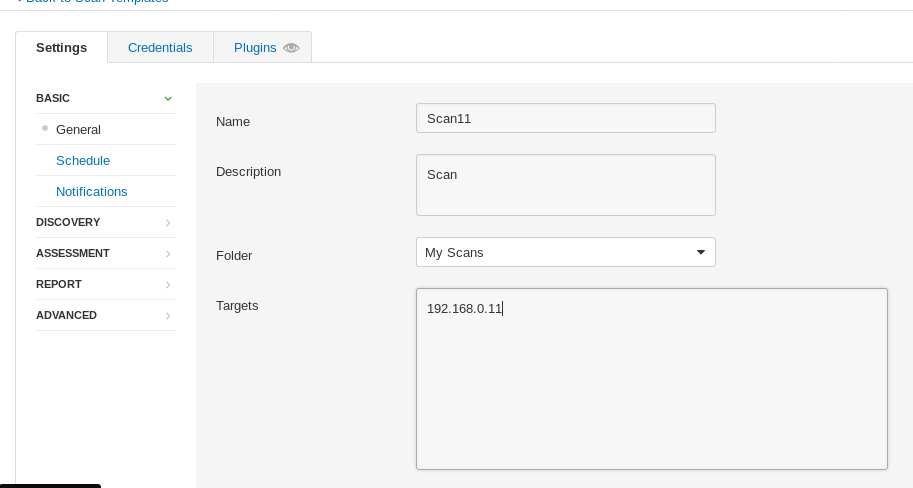
Figure 21.5



### Nessus

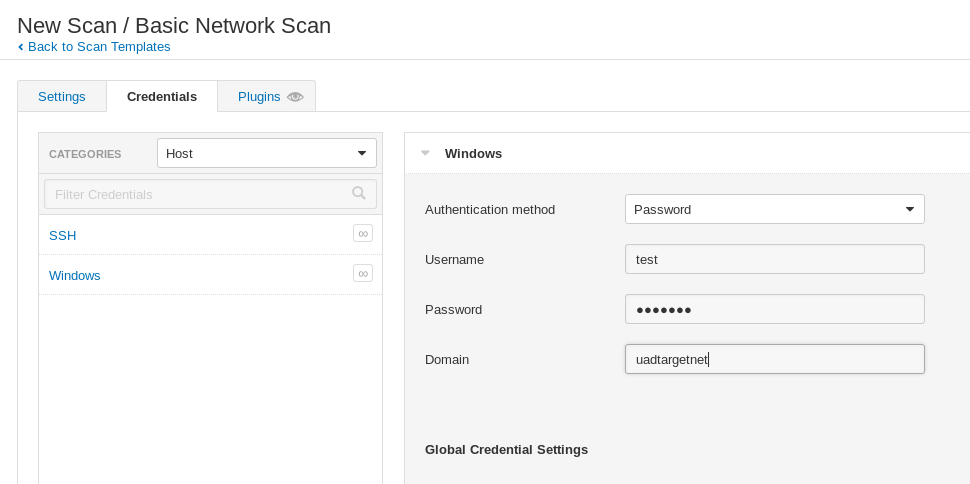
Nessus is a tool to scan IP addresses within a network for vulnerabilities. It provides in depth details on the vulnerabilities and also solutions to them. This is set by navigating to <https://127.0.0.1:8834> and signing in to your account and starting a scan. The first page of scan setup requires information about the scan including scan name, details and the IP address or IP range you wish to check.

Figure 22



The user must then select the credentials tab, select Windows and then enter in the test accounts name and password along with the network name “uadtargetnet”

Figure 22.1



After this is complete, press save and you will be brought back to “My Scans”. Here you will need to press the play button to begin the scan.

Figure 22.2

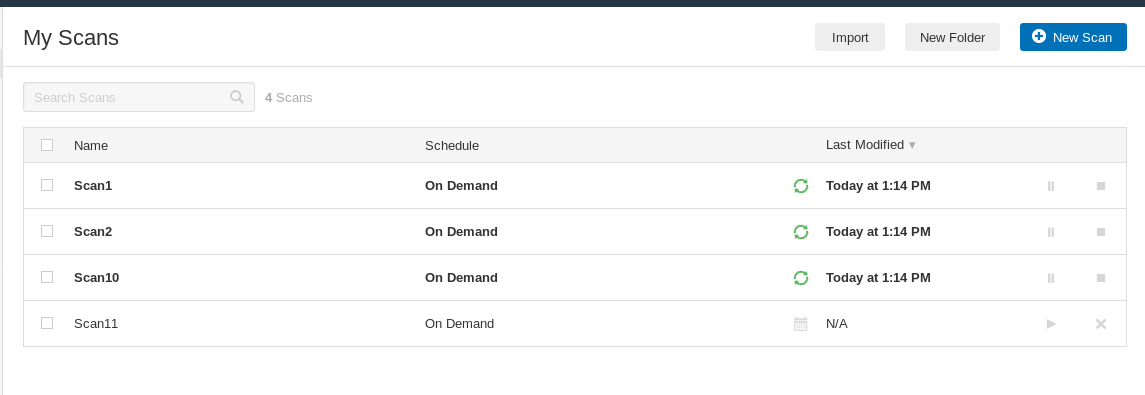
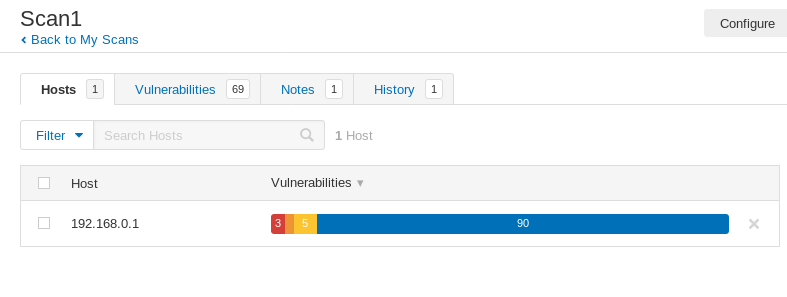


Figure 22.3



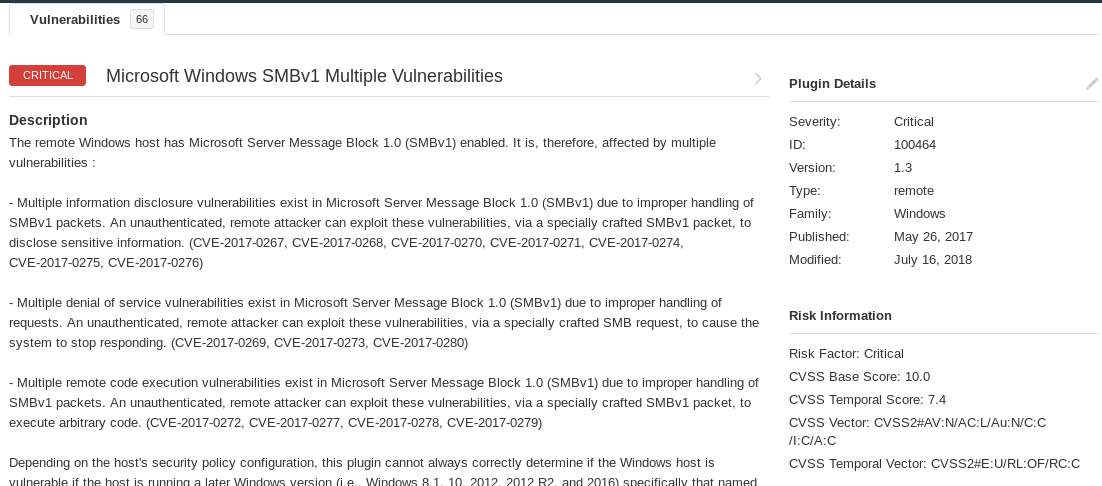
Once a scan is complete, it can be clicked on to show its findings. You then click on the red section of the bar to view the most critical vulnerabilities.

Figure 22.4



The most critical vulnerabilities are shown to the user and they may be clicked to show more specific details on the individual one chosen.

Figure 22.5



On this page, solutions will also be shown to fix vulnerabilities, usually in the form of windows patches.

## Enumeration

### NMAP Vulnerability Scans

The command nmap –script vuln was run to identify any vulnerabilities the computers had. This quickly revealed that Server1 was likely vulnerable to a Slowloris Denial Of Service attack (CVE-2017-6750)(figure 20) and had a vulnerability in SMB v1 (CVE-2017-0143)(figure 21). Server2 also had the same SMB vulnerability (CVE-2017-0143).

Figure 23

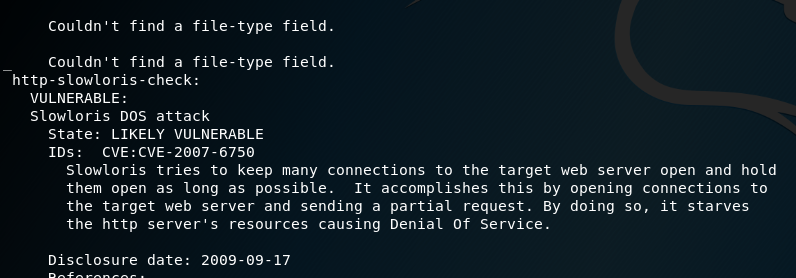
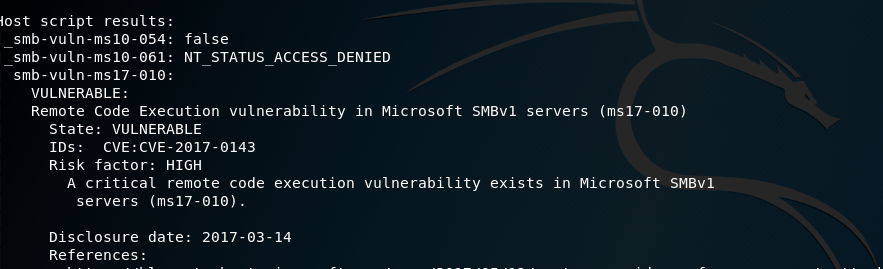


Figure 24



After doing some research, it was found that the SMB vulnerability was exploitable by Eternal Blue, a hack used within Metasploit. The website (Rapid7, 2018) stated: “A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests. An attacker who successfully exploited the vulnerability could gain the ability to execute code on the target server.”.

### NBT Enumeration

The enumeration tool nbtenum 3.3 is used to gather specific information regarding the users and user groups on a network. This can be a vital step in obtaining information on users and user privileges. The command nbtenum.exe -q 192.168.0.1 UADTARGETNET\test test123 was used with the parameters including the IP address of the target and the log in details of the test account are needed to complete this task. The results of this can be found in appendix A and appendix B.

### RPCClient

RPC client is a kali linux method of finding out details about users based on their privileges, aka 500 for administrators. The command rpcclient –U “test” 192.168.0.1 would gather this information for Server1. The results are shown in the two figures below.

Figure 25

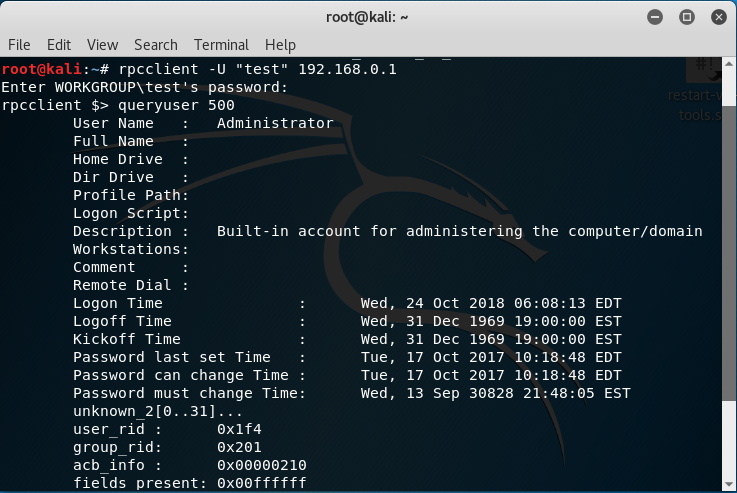
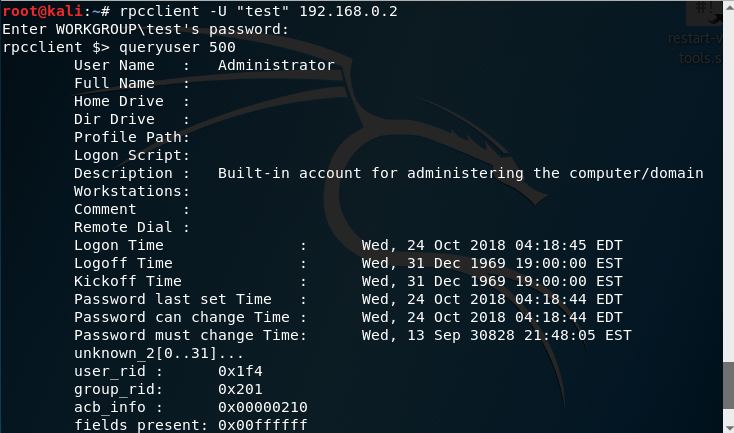


Figure 26



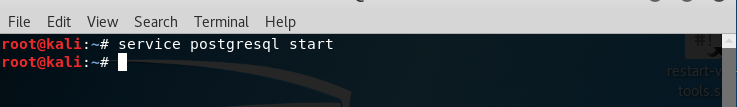
## System Hacking

### Eternal Blue

Eternal Blue is an exploit used through Metasploit which can take advantage of SMB vulnerabilities. This was used as it was previously discovered that port 139 netbios –ssn SMB service was vulnerable (CVE-2017-0143)

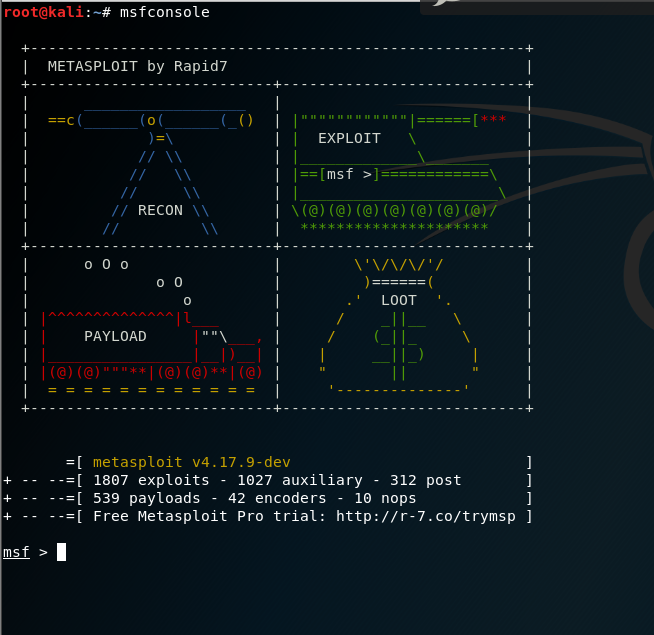
The first step was to start the postgresql service to speed up searching for the exploit.

Figure 27



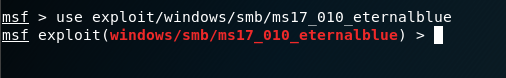
The command “msfconsole” was then used to start metasploit.

Figure 28



The command “use exploit/windows/smb/ms17\_010\_eternalblue” was then entered to instruct Metasploit to use the Eternal Blue exploit.

Figure 29



Then Metasploit is instructed to use the reverse shell payload. A reverse shell is when a shell is opened on the target computer and is instructed to send results to the attacker’s computer.

Figure 30

C:\Users\amg\Desktop\Ethical Hacking 1\Screenshots\Reverse Shell.PNG

It is then instructed to instruct Metasploit where the reverse shell is being sent to.

Figure 31

C:\Users\amg\Desktop\Ethical Hacking 1\Screenshots\Lhost.PNG

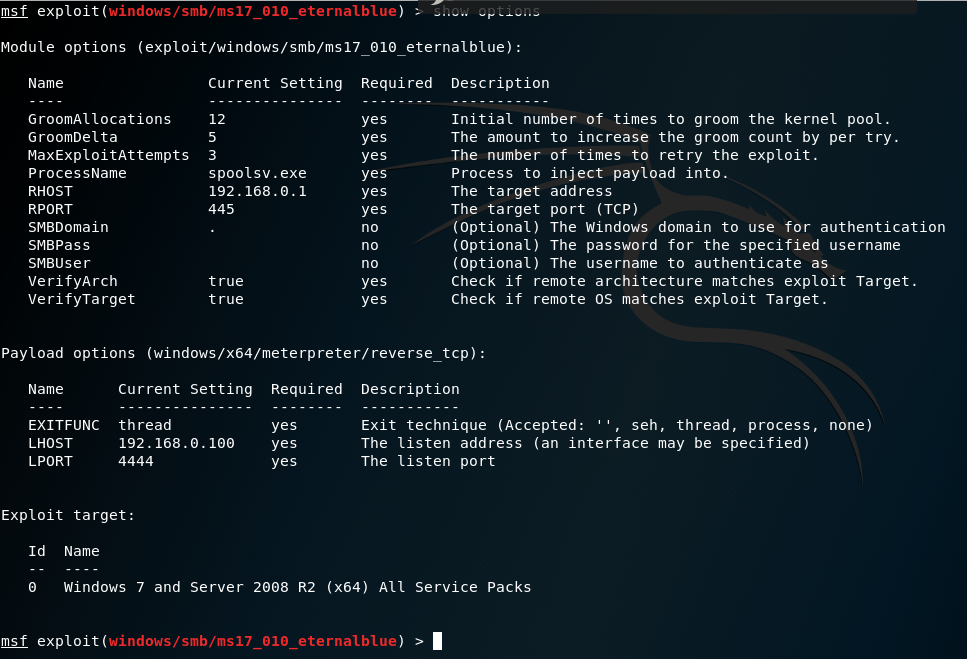
Metasploit is then instructed as to the IP address of the targets computer.

Figure 32

C:\Users\amg\Desktop\Ethical Hacking 1\Screenshots\Rhost.PNG

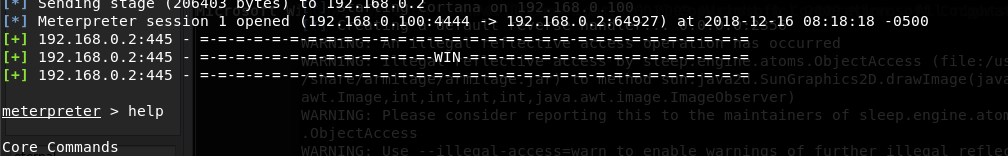
“show options” is then entered to confirm that the exploit will run with the correct parameters.

Figure 33



The command “exploit” then executes the exploit. If successful, the following message will be shown.

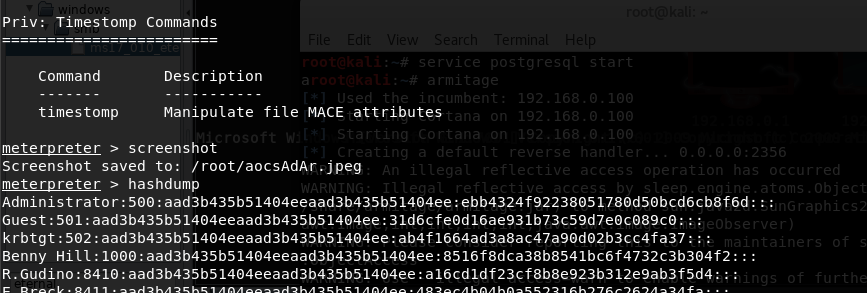
Figure 34



After successful exploit, the “help” command can be used to display options.

The “hashdump” command can then be used to get the hashed passwords for every user as shown below. The full data can be seen in appendix C and appendix D.

Figure 35



### Cain Password Cracker

Cain is a password cracker which can use multiple different ways of cracking including brute force, dictionary attacks and crypto analysis for hashed passwords. The hashed passwords were imported into Cain and thereafter a dictionary attack for NTLM hashes was used to uncover multiple passwords.

Figure 36

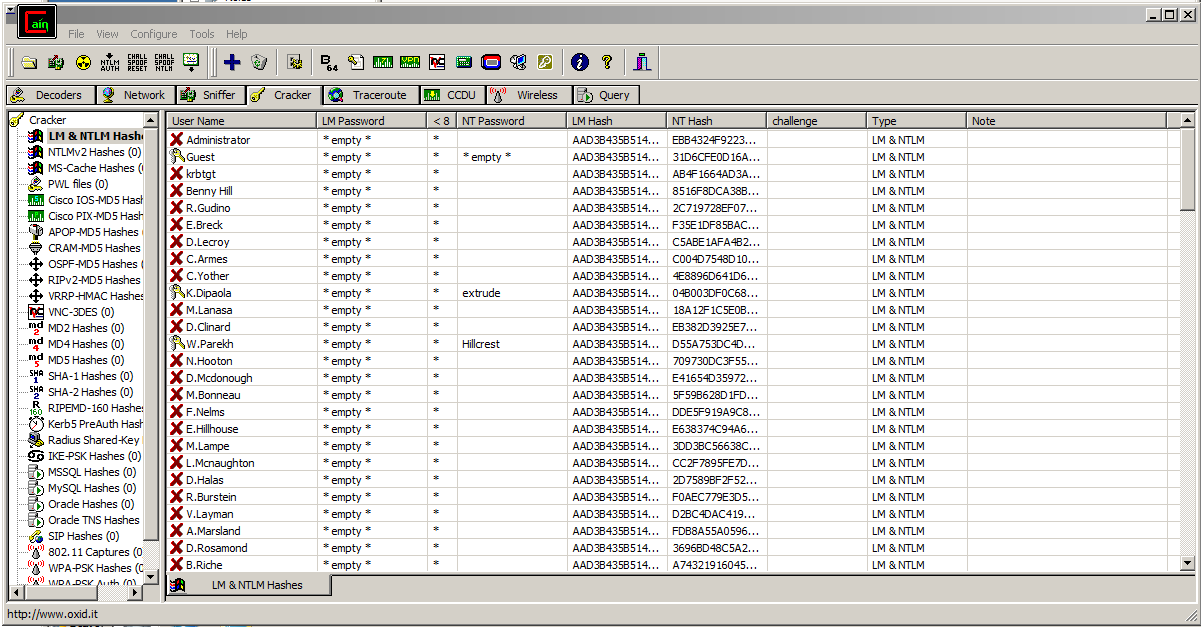
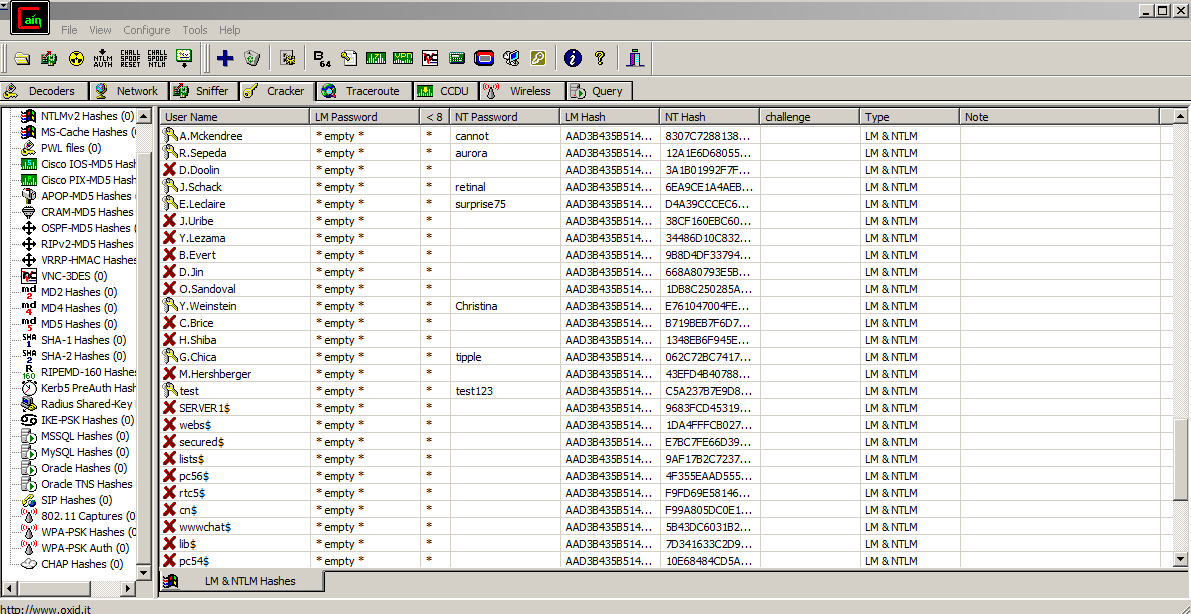


Figure 37



These were then compared to the web files created by the nbtenum3.3 to discover admins “W.Parekh” for Server1 and “G.Chica” for Server2 has insecure passwords that were cracked.

Both servers were then logged into as the admins with cracked passwords and then the Active Directory Administrative Center the servers were used to escalate privileges of the test account to admin by adding them to the “Enterprise Admins” user group.

Figure 38

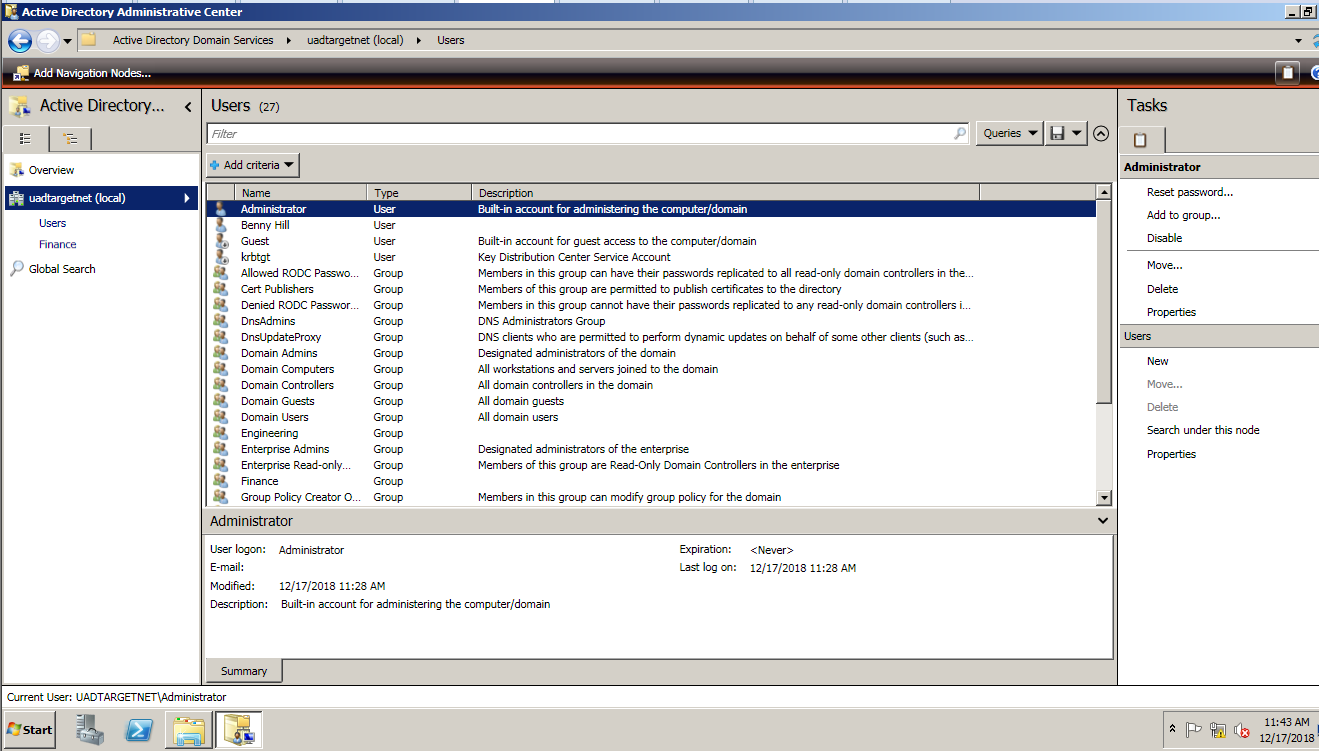
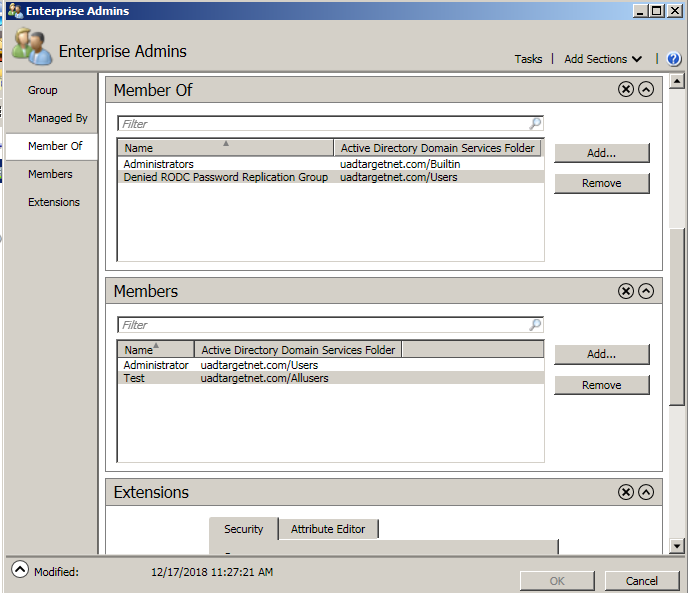


Figure 39



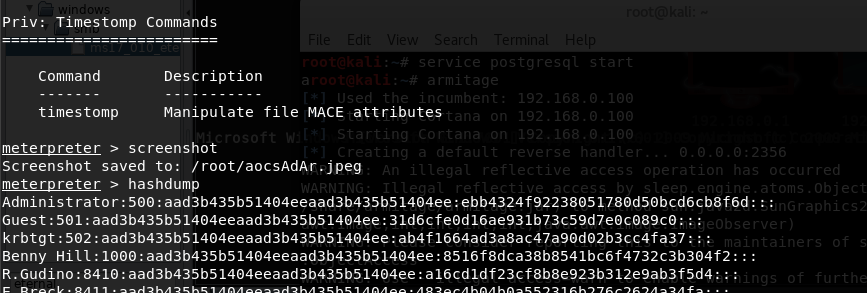
Both servers were then logged in to as the test account and confirmation was gained that this was now an admin account.

## Advanced Phases

### Hash Dump

The “hashdump” command can then be used on successful exploit via Eternal blue to get the hashed passwords for every user as shown below. The full hashed passwords data can be seen in appendix C and appendix D.

Figure 35



### Cain Password Cracker

Cain is a password cracker which can use multiple different ways of cracking including brute force, dictionary attacks and crypto analysis for hashed passwords. The hashed passwords were imported into Cain and thereafter a dictionary attack for NTLM hashes was used to uncover multiple passwords.

Figure 36

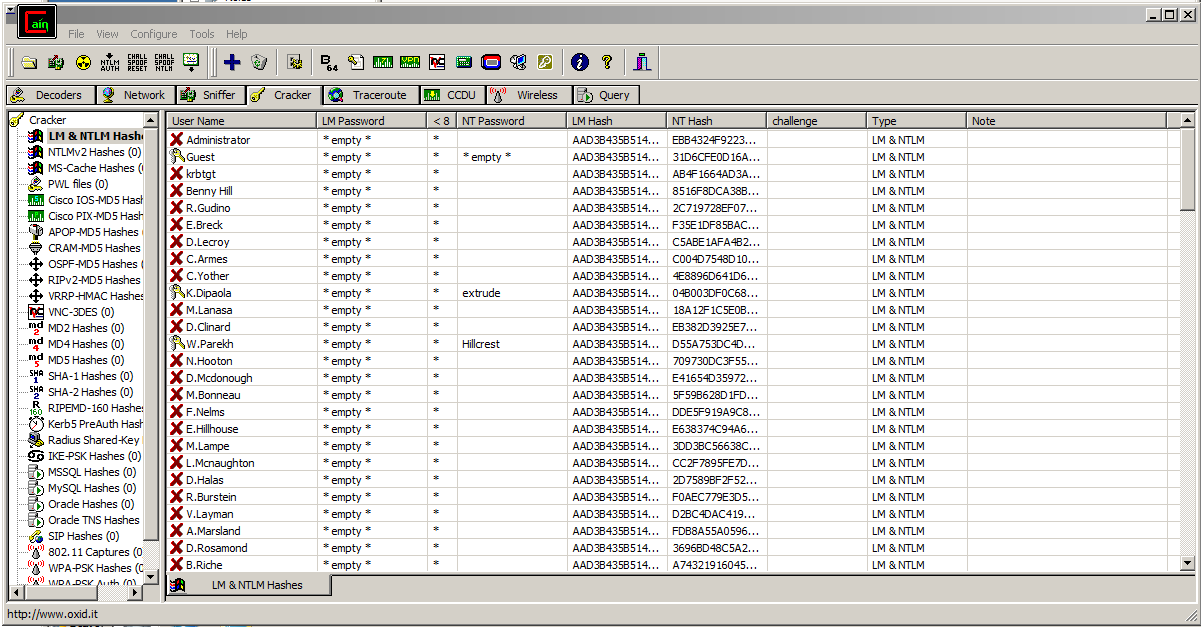
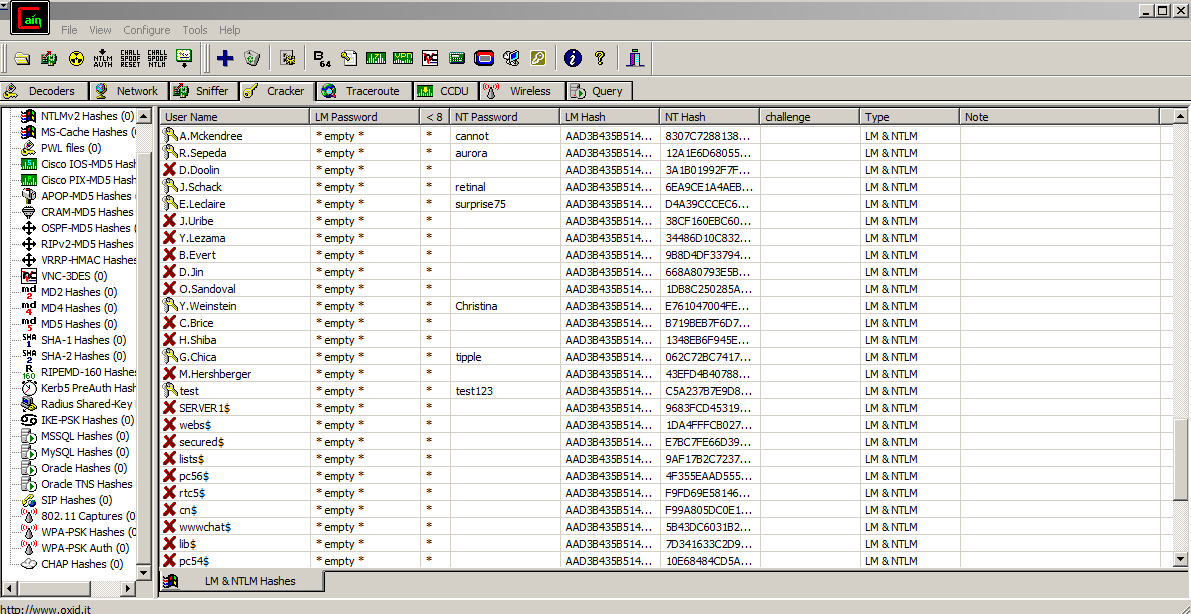


Figure 37



These were then compared to the web files created by the nbtenum3.3 to discover admins “W.Parekh” for Server1 and “G.Chica” for Server2 has insecure passwords that were cracked.

Both servers were then logged into as the admins with cracked passwords and then the Active Directory Administrative Center the servers were used to escalate privileges of the test account to admin by adding them to the “Enterprise Admins” user group.

Figure 38

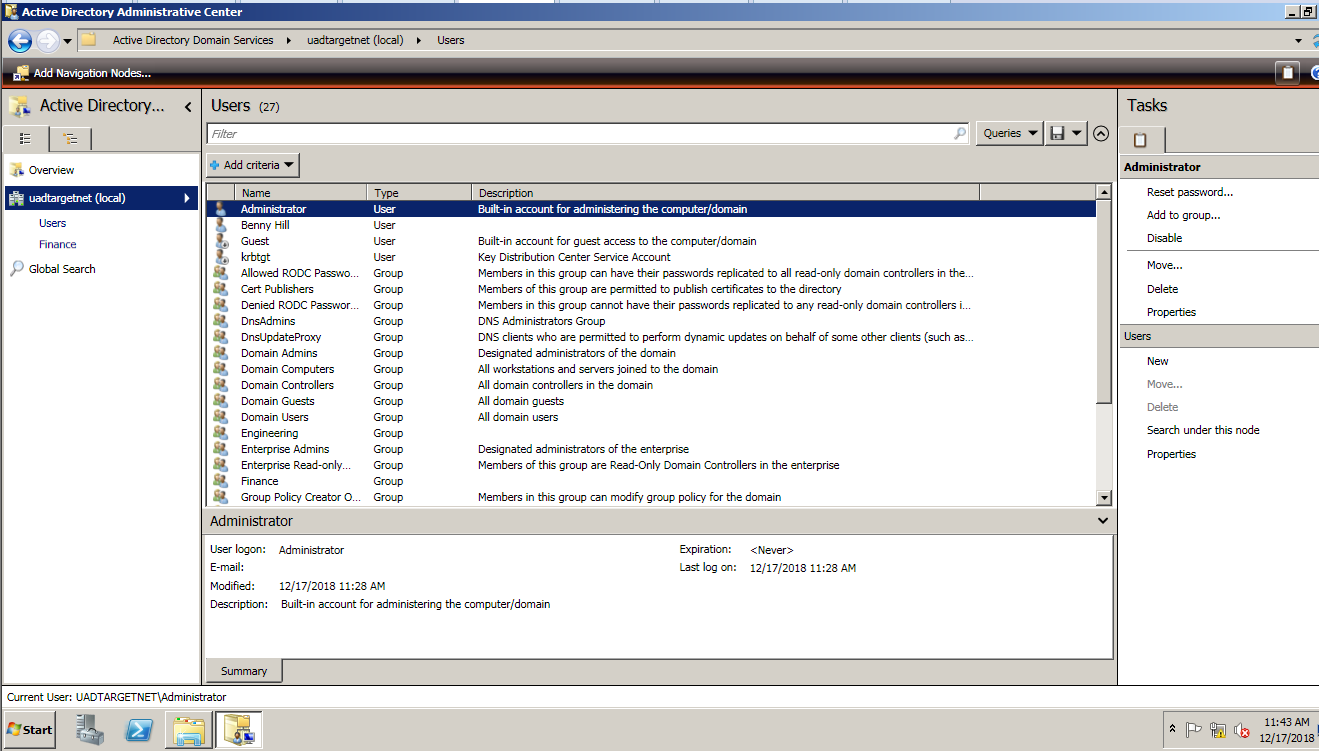
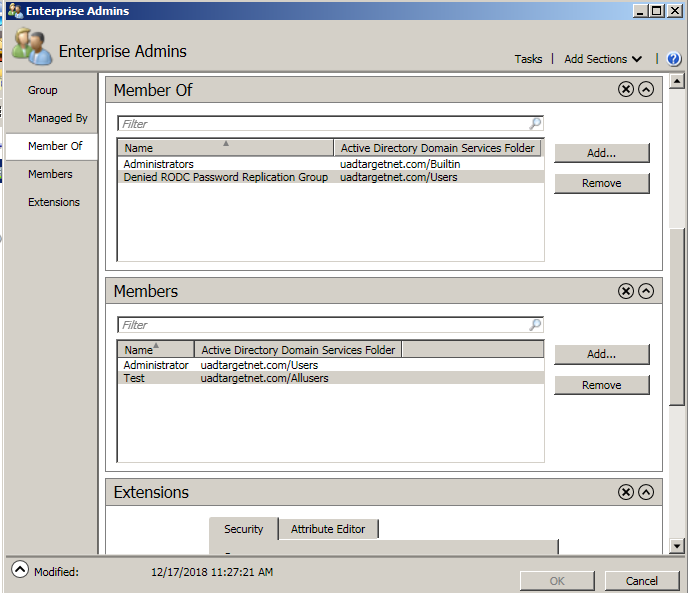


Figure 39



Both servers were then logged in to as the test account and confirmation was gained that this was now an admin account.

# Discussion

## General Discussion

Here, you want to discuss your results/outcomes.

* What does it all mean? Discuss anything of interest. How does this relate to other work in this area (if relevant)?

* Relate the findings back to your aims - how well have you met your aim?
* Discuss, for example, return on investment (ROI), usability, adherence to standards, and speed of implementation. Ensure that you make clear you understand your client’s pain and can relieve it.

## Countermeasures

The Nessus scans gave solutions to the vulnerabilities fund during this penetration testing. The figures below show that windows patches are required to be installed to prevent further exploit.

Figure 40

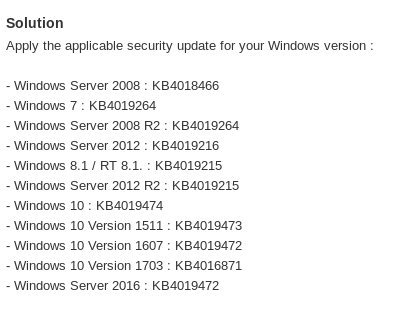
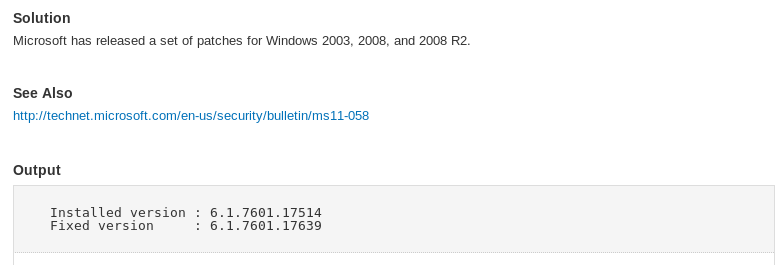


Figure 41



It would also be strongly advisable to ensure the password creation applications are updated to ensure users create more secure passwords. For example, it could require users to contain 8 or more characters, upper case and lower case, with numbers and special characters, avoiding the use of dictionary words where possible.

## Conclusions

It can be concluded that a number of vulnerabilities exist within the Typical Company’s network that need to be addressed. The windows versions are older and appear outdated and unpatched, which leaves it vulnerable to attacks. Microsoft IIS always requires updating.

The current password policy for staff also appears to be too lenient on what is accepted. This allows attackers to crack passwords with ease.

## Future Work

Given more time, longer periods of time cracking passwords could be done to ensure other staff have secure passwords. It would be possible to run other password cracking tools such as “Hydra” as well. This is a tool which sends requests to the server in an attempt to try and crack passwords. Due to the fact it communicates with the server, this method takes longer to complete.

“Ophcrack” is a tool that uses rainbow tables to crack windows passwords. Given more time this tool could also be tested against the network.

## Call to action

Burgess Inc. can offer maintenance packages to provide penetration testing services and regularly update software to ensure that your network has minimal vulnerabilities to drastically reduce the likelihood of exploit.

# Bibliography

Csciwww. (2018). *Statistics on Cyber-terrorism*. Retrieved from http://csciwww.etsu.edu/gotterbarn/stdntppr/stats.htm

Legislation.gov.uk. (2018). *Computer Misuse Act 1990*. Retrieved from https://www.legislation.gov.uk/ukpga/1990/18/section/1

Rapid7. (2018). *CVE-2017-0143 Microsoft CVE-2017-0143: Windows SMB Remote Code Execution Vulnerability | Rapid7*. Retrieved from Rapid 7: https://www.rapid7.com/db/vulnerabilities/msft-cve-2017-0143

Solutions, C. (2018). *13 Alarming Cyber Security Facts and Stats | Cybint*. Retrieved from https://www.cybintsolutions.com/cyber-security-facts-stats/

thewindowsclub. (2018). *What is an SMB port? What is Port 445 and Port 139 used for?* Retrieved from The Windows Club: https://www.thewindowsclub.com/smb-port-what-is-port-445-port-139-used-for

# Appendices

## Appendix A – NBTENUM Server1

|  |
| --- |
| 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 |

|  |
| --- |
|  |

## Appendix B – nbtenum Server2

|  |
| --- |
| 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 |

## Appendix C

Hash Dump for Server1

Administrator:500:aad3b435b51404eeaad3b435b51404ee:ebb4324f92238051780d50bcd6cb8f6d:::

Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

krbtgt:502:aad3b435b51404eeaad3b435b51404ee:ab4f1664ad3a8ac47a90d02b3cc4fa37:::

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

R.Gudino:8410:aad3b435b51404eeaad3b435b51404ee:2c719728ef075775d9645c97168e18b1:::

E.Breck:8411:aad3b435b51404eeaad3b435b51404ee:f35e1df85bacb525a805d5a8368c4f62:::

D.Lecroy:8412:aad3b435b51404eeaad3b435b51404ee:c5abe1afa4b210af38e70c8345a6660a:::

C.Armes:8413:aad3b435b51404eeaad3b435b51404ee:c004d7548d10c3607aea63b4783579cf:::

C.Yother:8414:aad3b435b51404eeaad3b435b51404ee:4e8896d641d6237eea7ec9a48a3b557d:::

K.Dipaola:8415:aad3b435b51404eeaad3b435b51404ee:04b003df0c68398456184f04fa8ccf6e:::

M.Lanasa:8416:aad3b435b51404eeaad3b435b51404ee:18a12f1c5e0bfbc51ecfb20b9cb75f78:::

D.Clinard:8417:aad3b435b51404eeaad3b435b51404ee:eb382d3925e7a940819bc9ab65c19cd5:::

W.Parekh:8418:aad3b435b51404eeaad3b435b51404ee:d55a753dc4d951b3f296e7636149fa31:::

N.Hooton:8419:aad3b435b51404eeaad3b435b51404ee:709730dc3f558310a005f25d534d6ede:::

D.Mcdonough:8420:aad3b435b51404eeaad3b435b51404ee:e41654d359729c89ae0fc2dff5c5fe0b:::

M.Bonneau:8421:aad3b435b51404eeaad3b435b51404ee:5f59b628d1fd944945f7d9fa34e80eb0:::

F.Nelms:8422:aad3b435b51404eeaad3b435b51404ee:dde5f919a9c87ad76d670c366bc9ca00:::

E.Hillhouse:8423:aad3b435b51404eeaad3b435b51404ee:e638374c94a682337b8db912550c6f7e:::

M.Lampe:8424:aad3b435b51404eeaad3b435b51404ee:3dd3bc56638c2be7e36e0ba8518160b5:::

L.Mcnaughton:8425:aad3b435b51404eeaad3b435b51404ee:cc2f7895fe7de33e5c6399ab1017ffc0:::

D.Halas:8426:aad3b435b51404eeaad3b435b51404ee:2d7589bf2f528ad82bfb342d82781a25:::

R.Burstein:8427:aad3b435b51404eeaad3b435b51404ee:f0aec779e3d5e3d2c4c8cc3d34815e8b:::

V.Layman:8428:aad3b435b51404eeaad3b435b51404ee:d2bc4dac419a84c2ba03e1247621aa5e:::

A.Marsland:8429:aad3b435b51404eeaad3b435b51404ee:fdb8a55a0596c4fa89f0c47b5b6a8a23:::

D.Rosamond:8430:aad3b435b51404eeaad3b435b51404ee:3696bd48c5a2b84ce6626db82f771872:::

B.Riche:8431:aad3b435b51404eeaad3b435b51404ee:a7432191604554bc1432c78835034664:::

J.Wiste:8432:aad3b435b51404eeaad3b435b51404ee:4c6be6c27d1733687ac556911ac7cb33:::

T.Lefebre:8433:aad3b435b51404eeaad3b435b51404ee:8071bb547c15f5812eccc7d66847700d:::

S.Dalrymple:8434:aad3b435b51404eeaad3b435b51404ee:1579cc963e773689d21694c536d346ac:::

R.Stoneking:8435:aad3b435b51404eeaad3b435b51404ee:9a1fecbe6026ffc4fe7da70019711ce9:::

S.Russom:8436:aad3b435b51404eeaad3b435b51404ee:2a97f213a2d4ef9606b0347127bd6057:::

M.Maxwell:8437:aad3b435b51404eeaad3b435b51404ee:2f32bf67f628d991a143fe73e7a83632:::

Z.Sowders:8438:aad3b435b51404eeaad3b435b51404ee:2c3eaca482910782289141023f75b5e7:::

M.Hoy:8439:aad3b435b51404eeaad3b435b51404ee:d41977b8c2ed7e5377c83b10ba6adbc7:::

C.Selzer:8440:aad3b435b51404eeaad3b435b51404ee:5385ea2b21a1729e83de74799416d6cf:::

K.Leiker:8441:aad3b435b51404eeaad3b435b51404ee:6e294f8648c008cb09ad6e4f929bdd7e:::

S.Gerst:8442:aad3b435b51404eeaad3b435b51404ee:09f2763188abd3fc5b75ba3a90d222c9:::

D.Kennemer:8443:aad3b435b51404eeaad3b435b51404ee:0e8d3c52b2c976ac0a2bd2e5bb00979c:::

L.Angelo:8444:aad3b435b51404eeaad3b435b51404ee:d2edf9ec8fde361f9584144e579567f5:::

L.Gamino:8445:aad3b435b51404eeaad3b435b51404ee:70fdb9838cf05b0265b70c929e50f607:::

S.Tacey:8446:aad3b435b51404eeaad3b435b51404ee:fd4a62c4f3df7cc1274d8c23a78a6858:::

E.Bouknight:8447:aad3b435b51404eeaad3b435b51404ee:d794f1d2e3d78cd5856ac02ad55c8852:::

L.Soriano:8448:aad3b435b51404eeaad3b435b51404ee:81197fc3601b55ce333951cd530979c9:::

M.Wentz:8449:aad3b435b51404eeaad3b435b51404ee:c13272b5fd22589254a2b93b899f1ebf:::

G.Fuller:8450:aad3b435b51404eeaad3b435b51404ee:ce3b6a64b3a13a0b4c8b4c8f7341d41b:::

C.Linen:8451:aad3b435b51404eeaad3b435b51404ee:187996eb0144f70a62ae59e3cb28fec1:::

J.Murrell:8452:aad3b435b51404eeaad3b435b51404ee:2be574578fe4e5b236c2e89248b62dee:::

A.Eisenmenger:8453:aad3b435b51404eeaad3b435b51404ee:cab4559de87687f943f17ace8b774b14:::

S.Poore:8454:aad3b435b51404eeaad3b435b51404ee:9ccb954ce8e85ab05d40679927c4a5ef:::

A.Fritzler:8455:aad3b435b51404eeaad3b435b51404ee:46eb0774ffbf96be63c6ac191f4a289d:::

M.Otter:8456:aad3b435b51404eeaad3b435b51404ee:c8c984497573ce4fb649d7ac4d925467:::

S.Kerfoot:8457:aad3b435b51404eeaad3b435b51404ee:aab99eaf82f0280cbe637042c2cee3b3:::

B.Saari:8458:aad3b435b51404eeaad3b435b51404ee:0a61c82a7ebff9e84ef3e80d734d61be:::

M.Colberg:8459:aad3b435b51404eeaad3b435b51404ee:47fc975afaf6b3a6f79346e65684c046:::

V.Reighard:8460:aad3b435b51404eeaad3b435b51404ee:ac109cff8a2f00851eaf7f44c7806b01:::

S.Leverich:8461:aad3b435b51404eeaad3b435b51404ee:15c91a110eff6be1bb32697424c50c67:::

C.Hernadez:8462:aad3b435b51404eeaad3b435b51404ee:e66caffeae89b519beefade05b901172:::

E.Bolander:8463:aad3b435b51404eeaad3b435b51404ee:1bf672f24ca641cf61c623f1b903dd7e:::

S.Abercrombie:8464:aad3b435b51404eeaad3b435b51404ee:9c16a93d03340a844731c2fa83cd5920:::

D.Kawasaki:8465:aad3b435b51404eeaad3b435b51404ee:0dfb05055627ee78741114aee00d0aea:::

J.Killion:8466:aad3b435b51404eeaad3b435b51404ee:db4e9833cddb903e3b67aff17494dd4d:::

C.Spann:8467:aad3b435b51404eeaad3b435b51404ee:095585e9e04d7d94fdd53a12f8d389da:::

E.Bascom:8468:aad3b435b51404eeaad3b435b51404ee:6c76358139d1529bb6ccc2fda24d5bb2:::

W.Haakenson:8469:aad3b435b51404eeaad3b435b51404ee:311c1ee5fd20bda1e04be3453ddb7724:::

K.Corney:8470:aad3b435b51404eeaad3b435b51404ee:2f2e7d658fcff4609cde0e8013f04e0c:::

K.Husby:8471:aad3b435b51404eeaad3b435b51404ee:769af9c36787ee48fafa0b0f54c92b23:::

R.Avina:8472:aad3b435b51404eeaad3b435b51404ee:80fee42f76624ee0f2441ee93d6f95bf:::

C.Corpuz:8473:aad3b435b51404eeaad3b435b51404ee:6028945c172a53aeb39f0e3574883d28:::

M.Tilman:8474:aad3b435b51404eeaad3b435b51404ee:12dc52f5077d75e3b7bdbc3319b2f5d4:::

T.Blass:8475:aad3b435b51404eeaad3b435b51404ee:7945702642617ef4275d1959730a50a7:::

B.Schweitzer:8476:aad3b435b51404eeaad3b435b51404ee:da9754a21f6b2370b9077552ccde16fe:::

W.Loch:8477:aad3b435b51404eeaad3b435b51404ee:96915301bef02368514403da3fcd03f8:::

N.Broady:8478:aad3b435b51404eeaad3b435b51404ee:4b8ea66764d5efa3704b3ff5a545ecdc:::

L.Sarver:8479:aad3b435b51404eeaad3b435b51404ee:6184d151318a3629a296ad216c104058:::

F.Ousley:8480:aad3b435b51404eeaad3b435b51404ee:cf8cd80dbcbdbacd18a8c1ce70d922f8:::

T.Prestidge:8481:aad3b435b51404eeaad3b435b51404ee:e5c1cd33e3dbb3f8de77c208f5e92ad7:::

G.Nordeen:8482:aad3b435b51404eeaad3b435b51404ee:a670d566f94848b6de962afd1153fb2b:::

G.Youngberg:8483:aad3b435b51404eeaad3b435b51404ee:30c874cd3f2bea10ca44509491de638d:::

R.Zoll:8484:aad3b435b51404eeaad3b435b51404ee:cdde1022a3b946692db0a3fb4858aa10:::

M.Thiel:8485:aad3b435b51404eeaad3b435b51404ee:b2f1b6a710fb60fb24a660b2b34c520e:::

N.Bitterman:8486:aad3b435b51404eeaad3b435b51404ee:978fe87f970a58ff08b805ffdc5fc2e2:::

V.Teran:8487:aad3b435b51404eeaad3b435b51404ee:99ab6b701390782dddce13db09f5be80:::

M.Pascucci:8488:aad3b435b51404eeaad3b435b51404ee:db16e484ba92131363584b9367ec98ab:::

F.Lu:8489:aad3b435b51404eeaad3b435b51404ee:8dd2598c133641334602ea8b14af6ec5:::

I.Cortright:8490:aad3b435b51404eeaad3b435b51404ee:964914313d49733466c6de1f6b692f92:::

M.Birdwell:8491:aad3b435b51404eeaad3b435b51404ee:b417fef67ec6776ce28ab6c423a98753:::

E.Mogan:8492:aad3b435b51404eeaad3b435b51404ee:c7b2c6b68f9d851132064c49d94b5625:::

F.Lietz:8493:aad3b435b51404eeaad3b435b51404ee:a83754d0f607ccfa00e05f3622fb537a:::

A.Mckendree:8494:aad3b435b51404eeaad3b435b51404ee:29b4a946ccc7be2bbe58d79683fb6c09:::

R.Sepeda:8495:aad3b435b51404eeaad3b435b51404ee:8d19fe04e0db994b42ffbfc10693a8e6:::

D.Doolin:8496:aad3b435b51404eeaad3b435b51404ee:073d5025927b13827194f61697e3203a:::

J.Schack:8497:aad3b435b51404eeaad3b435b51404ee:1e428e58bf4a8b1af5008d83916186fd:::

E.Leclaire:8498:aad3b435b51404eeaad3b435b51404ee:711274cddb31bbc22a9c37c17071f5d9:::

J.Uribe:8499:aad3b435b51404eeaad3b435b51404ee:a8bdf1af95033d887c53860b491edf35:::

Y.Lezama:8500:aad3b435b51404eeaad3b435b51404ee:cbe8ce77a578d3426b8d4c58e70e44d7:::

B.Evert:8501:aad3b435b51404eeaad3b435b51404ee:cce1c32173b9507ba62f209bb726daa1:::

D.Jin:8502:aad3b435b51404eeaad3b435b51404ee:f035e2b964c95cc0d009431951c8e5c6:::

O.Sandoval:8503:aad3b435b51404eeaad3b435b51404ee:8bc129e04cb2fd644a903ec770a7eca7:::

Y.Weinstein:8504:aad3b435b51404eeaad3b435b51404ee:e2bd4085feab5d1dda165ff143ffda60:::

C.Brice:8505:aad3b435b51404eeaad3b435b51404ee:a01c76abb2ba744aa51a8b62ba13eaa5:::

H.Shiba:8506:aad3b435b51404eeaad3b435b51404ee:19b08eec9e420866c96e31772a189f81:::

G.Chica:8507:aad3b435b51404eeaad3b435b51404ee:b574de5f7863a12f053723da38fef17f:::

M.Hershberger:8508:aad3b435b51404eeaad3b435b51404ee:29be1d810a610bf6f9fc78bd2d74ee1e:::

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:::

## Appendix D

Hash Dump for Server2:

Administrator:500:aad3b435b51404eeaad3b435b51404ee:ebb4324f92238051780d50bcd6cb8f6d:::

Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

krbtgt:502:aad3b435b51404eeaad3b435b51404ee:ab4f1664ad3a8ac47a90d02b3cc4fa37:::

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

R.Gudino:8410:aad3b435b51404eeaad3b435b51404ee:a16cd1df23cf8b8e923b312e9ab3f5d4:::

E.Breck:8411:aad3b435b51404eeaad3b435b51404ee:483ec4b04b0a552316b276c2624a34fa:::

D.Lecroy:8412:aad3b435b51404eeaad3b435b51404ee:c53064e9887a83f8a4d5cbfcef972305:::

C.Armes:8413:aad3b435b51404eeaad3b435b51404ee:854b0771463f88f7bc24a4725f84e8cb:::

C.Yother:8414:aad3b435b51404eeaad3b435b51404ee:676035f793cc21d58a224011ea06bab2:::

K.Dipaola:8415:aad3b435b51404eeaad3b435b51404ee:97bab9d5bece0fcc4f1e4276b86b7cd2:::

M.Lanasa:8416:aad3b435b51404eeaad3b435b51404ee:6b9e4e4fe9908b12391c41ef35b7b1c3:::

D.Clinard:8417:aad3b435b51404eeaad3b435b51404ee:81fdfb48450ad4f3864d741a01ca2e21:::

W.Parekh:8418:aad3b435b51404eeaad3b435b51404ee:24e4ac391f7c5d4378f792253e356f22:::

N.Hooton:8419:aad3b435b51404eeaad3b435b51404ee:a6339833fd0bcf84a3ab10a42fa7b59a:::

D.Mcdonough:8420:aad3b435b51404eeaad3b435b51404ee:ce1dc95c9d025db2e1f3ea85c40236be:::

M.Bonneau:8421:aad3b435b51404eeaad3b435b51404ee:c8772704bdf47b48a33804df97f67850:::

F.Nelms:8422:aad3b435b51404eeaad3b435b51404ee:f64237b0e85352bd41ce8eed475d8421:::

E.Hillhouse:8423:aad3b435b51404eeaad3b435b51404ee:f62a557ef50f7784877e4f9a56e159e6:::

M.Lampe:8424:aad3b435b51404eeaad3b435b51404ee:d8d5907791e5a47726e83e5e46f2af40:::

L.Mcnaughton:8425:aad3b435b51404eeaad3b435b51404ee:24b5431395c05f8b51ea696b56a753d5:::

D.Halas:8426:aad3b435b51404eeaad3b435b51404ee:4096de2eb2481c54b9434504a6bd2626:::

R.Burstein:8427:aad3b435b51404eeaad3b435b51404ee:dbd5e86f519091ee6bd8493ab5a11495:::

V.Layman:8428:aad3b435b51404eeaad3b435b51404ee:43bcce94858487616e05d95296ede293:::

A.Marsland:8429:aad3b435b51404eeaad3b435b51404ee:73e649125bc403926b144d55afb39b93:::

D.Rosamond:8430:aad3b435b51404eeaad3b435b51404ee:70e0448c608d9a2c9063f843a67e19ea:::

B.Riche:8431:aad3b435b51404eeaad3b435b51404ee:889f1e1dda555e1dbf1dd2fddeab883d:::

J.Wiste:8432:aad3b435b51404eeaad3b435b51404ee:bd2ec47441828680d9e0505cf0459e5c:::

T.Lefebre:8433:aad3b435b51404eeaad3b435b51404ee:4b4e6698bfe9dc66f21fccee2b3a716f:::

S.Dalrymple:8434:aad3b435b51404eeaad3b435b51404ee:0e22d6c69b26a876faae86c723e905fc:::

R.Stoneking:8435:aad3b435b51404eeaad3b435b51404ee:68ca4d1dd6450dee4940a9bcb4ce8423:::

S.Russom:8436:aad3b435b51404eeaad3b435b51404ee:3ef78cda39b74b1c181814af284fb3f1:::

M.Maxwell:8437:aad3b435b51404eeaad3b435b51404ee:840a1f2263dd7dffdf4d0ac22dcc6f49:::

Z.Sowders:8438:aad3b435b51404eeaad3b435b51404ee:8519eb53ce4e373f984a0e38f4b810fb:::

M.Hoy:8439:aad3b435b51404eeaad3b435b51404ee:a7b07e7189039642f865bb96a9c35570:::

C.Selzer:8440:aad3b435b51404eeaad3b435b51404ee:d275a92aeef9d6b958d22dd34e2d33cb:::

K.Leiker:8441:aad3b435b51404eeaad3b435b51404ee:9ca781b2c9b0e2db50ac628846f852f5:::

S.Gerst:8442:aad3b435b51404eeaad3b435b51404ee:a2eb2c7035aaf261e099a4f345f14980:::

D.Kennemer:8443:aad3b435b51404eeaad3b435b51404ee:bba45f0275135400fe21015d52d937b1:::

L.Angelo:8444:aad3b435b51404eeaad3b435b51404ee:c4342458001cd63d599b200ad74cb09e:::

L.Gamino:8445:aad3b435b51404eeaad3b435b51404ee:eb48f0585453625ec4e4ed116977042e:::

S.Tacey:8446:aad3b435b51404eeaad3b435b51404ee:edccee80b5097606b5e1a991ff20d0ab:::

E.Bouknight:8447:aad3b435b51404eeaad3b435b51404ee:53124ae8313a8f4b6e28eec9b978e41c:::

L.Soriano:8448:aad3b435b51404eeaad3b435b51404ee:fede29a42ffcb3cf0955d8f7ca567955:::

M.Wentz:8449:aad3b435b51404eeaad3b435b51404ee:9568d16ab2ccf3f4801678eda8bc749d:::

G.Fuller:8450:aad3b435b51404eeaad3b435b51404ee:e65f96ff47fbb707c4af42aced95d43b:::

C.Linen:8451:aad3b435b51404eeaad3b435b51404ee:99b6dd12c417c650d1f968b8afdde36e:::

J.Murrell:8452:aad3b435b51404eeaad3b435b51404ee:3fabd7fc9b1a83b16370168f7fbc741e:::

A.Eisenmenger:8453:aad3b435b51404eeaad3b435b51404ee:583018f6618d5cb7004b6af75eadf510:::

S.Poore:8454:aad3b435b51404eeaad3b435b51404ee:2ece90083724c6050f1d7d54b57c13e0:::

A.Fritzler:8455:aad3b435b51404eeaad3b435b51404ee:6ac6a6fd88899f637cde5f2e6564a1e1:::

M.Otter:8456:aad3b435b51404eeaad3b435b51404ee:86439a616978705185f584bf350cf5dc:::

S.Kerfoot:8457:aad3b435b51404eeaad3b435b51404ee:8cb3522398cbe3dbd0abe6a26a87478e:::

B.Saari:8458:aad3b435b51404eeaad3b435b51404ee:53b1fd8b95ec2299731c623d948276c6:::

M.Colberg:8459:aad3b435b51404eeaad3b435b51404ee:1ac6ed1b576eb48ddf6676d0bb2aa3e5:::

V.Reighard:8460:aad3b435b51404eeaad3b435b51404ee:467e2d0e0e8daaf270d82b9dcc7124c6:::

S.Leverich:8461:aad3b435b51404eeaad3b435b51404ee:b5b73b1984e9c951d4e95924a1cbc34f:::

C.Hernadez:8462:aad3b435b51404eeaad3b435b51404ee:e4e95bee1e9e9b4d49020c3b659d85f3:::

E.Bolander:8463:aad3b435b51404eeaad3b435b51404ee:c6504719856851983a0ccc47f009ae96:::

S.Abercrombie:8464:aad3b435b51404eeaad3b435b51404ee:5375fdb80376829e2a30271aa81640c1:::

D.Kawasaki:8465:aad3b435b51404eeaad3b435b51404ee:08d8ed1eaeea3c8fd7acc06314976e36:::

J.Killion:8466:aad3b435b51404eeaad3b435b51404ee:6117435384806d5c98df5c4e3d0ae712:::

C.Spann:8467:aad3b435b51404eeaad3b435b51404ee:8d4aed79e85b97d730a06b0bea01a085:::

E.Bascom:8468:aad3b435b51404eeaad3b435b51404ee:1f4ad2c305a1624d9e53bf1c34ad6977:::

W.Haakenson:8469:aad3b435b51404eeaad3b435b51404ee:2cbec3d1df634a653b2b2a07e411a11a:::

K.Corney:8470:aad3b435b51404eeaad3b435b51404ee:071650fb910bcf433f0944c2a48234f5:::

K.Husby:8471:aad3b435b51404eeaad3b435b51404ee:9ba3b63f93788a77e9cd5ae290e35f9c:::

R.Avina:8472:aad3b435b51404eeaad3b435b51404ee:280635941483e80a3ba540cae061754d:::

C.Corpuz:8473:aad3b435b51404eeaad3b435b51404ee:c18f63bfcf49f049c9a4ea12fa5150b7:::

M.Tilman:8474:aad3b435b51404eeaad3b435b51404ee:47b55ceed18efe45582bab180dcc6ce3:::

T.Blass:8475:aad3b435b51404eeaad3b435b51404ee:8b121c8bc35ba87546985582f3329b8d:::

B.Schweitzer:8476:aad3b435b51404eeaad3b435b51404ee:00860eb7c07bd00e9945faa01877b89a:::

W.Loch:8477:aad3b435b51404eeaad3b435b51404ee:90584e3a0a419f3e208da1b39b2ec98a:::

N.Broady:8478:aad3b435b51404eeaad3b435b51404ee:ce055cd6aca06cb629bce80c7bcae5d2:::

L.Sarver:8479:aad3b435b51404eeaad3b435b51404ee:bf99adbdc97c1f9a1ad9f4efc4dd4be3:::

F.Ousley:8480:aad3b435b51404eeaad3b435b51404ee:53effa66137a652ea07b6a6b8451ac6e:::

T.Prestidge:8481:aad3b435b51404eeaad3b435b51404ee:f7d460e1c769b6a8a68ca878cfedf5ce:::

G.Nordeen:8482:aad3b435b51404eeaad3b435b51404ee:05a3d4704d52997e255c4dc0ba3fae1c:::

G.Youngberg:8483:aad3b435b51404eeaad3b435b51404ee:e1f0f84ff05796020ef43891709cfc77:::

R.Zoll:8484:aad3b435b51404eeaad3b435b51404ee:129e6028e32aac47d9fd5bfc91be3911:::

M.Thiel:8485:aad3b435b51404eeaad3b435b51404ee:17ad717e4fb4ee6f547a72b64bdc3c75:::

N.Bitterman:8486:aad3b435b51404eeaad3b435b51404ee:fcc3b78f9abf782da2ba68d9bc6902f5:::

V.Teran:8487:aad3b435b51404eeaad3b435b51404ee:af0e992f816167feebe71d57db83e0c2:::

M.Pascucci:8488:aad3b435b51404eeaad3b435b51404ee:a010c0cf64975ce361e428b701b15c91:::

F.Lu:8489:aad3b435b51404eeaad3b435b51404ee:b6e4332e1cebf538eb367127203c71ba:::

I.Cortright:8490:aad3b435b51404eeaad3b435b51404ee:9c12c32215cdf257506d6623c676a4e5:::

M.Birdwell:8491:aad3b435b51404eeaad3b435b51404ee:d6795acdd456261a959f67837d28886a:::

E.Mogan:8492:aad3b435b51404eeaad3b435b51404ee:79e84653d30fe67c7b5ae45eb3c6eb48:::

F.Lietz:8493:aad3b435b51404eeaad3b435b51404ee:6dd01db8c84aa3ae833f1c4cce0d7f98:::

A.Mckendree:8494:aad3b435b51404eeaad3b435b51404ee:8307c7288138647ab7691e1674819b63:::

R.Sepeda:8495:aad3b435b51404eeaad3b435b51404ee:12a1e6d68055762e2d8fc61d9215b3ee:::

D.Doolin:8496:aad3b435b51404eeaad3b435b51404ee:3a1b01992f7f12d79d1775148bac1775:::

J.Schack:8497:aad3b435b51404eeaad3b435b51404ee:6ea9ce1a4aeb73e7ddd4a194a4dbafd2:::

E.Leclaire:8498:aad3b435b51404eeaad3b435b51404ee:d4a39cccec6bcff8acec23b572a2dd9e:::

J.Uribe:8499:aad3b435b51404eeaad3b435b51404ee:38cf160ebc6020e49a91f9a0472a281a:::

Y.Lezama:8500:aad3b435b51404eeaad3b435b51404ee:34486d10c832e47a9ae1e5af73cdfc19:::

B.Evert:8501:aad3b435b51404eeaad3b435b51404ee:9b8d4df3379439d96bcc45426f70f9d2:::

D.Jin:8502:aad3b435b51404eeaad3b435b51404ee:668a80793e5bef2b6aaee72e00d59355:::

O.Sandoval:8503:aad3b435b51404eeaad3b435b51404ee:1db8c250285adcfdb68169bfacf09119:::

Y.Weinstein:8504:aad3b435b51404eeaad3b435b51404ee:e761047004fe0282a9222b27784fd8de:::

C.Brice:8505:aad3b435b51404eeaad3b435b51404ee:b719beb7f6d7473e4f5ee57687b9b7e5:::

H.Shiba:8506:aad3b435b51404eeaad3b435b51404ee:1348eb6f945ebb332f6d69a3b8f4f7c1:::

G.Chica:8507:aad3b435b51404eeaad3b435b51404ee:062c72bc7417f9bafdaf0625003435f2:::

M.Hershberger:8508:aad3b435b51404eeaad3b435b51404ee:43efd4b4078817357c3bafed63f13dd9:::

test:8510:aad3b435b51404eeaad3b435b51404ee:c5a237b7e9d8e708d8436b6148a25fa1:::

SERVER1$:1001:aad3b435b51404eeaad3b435b51404ee:9683fcd45319937ac8d7d4428e94f6d5:::

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:6b9f633c31350397bf612730006ec8a5:::

CLIENT2$:8533:aad3b435b51404eeaad3b435b51404ee:60ae5045c905b7f56e9bffbc9de99352:::

SERVER2$:8534:aad3b435b51404eeaad3b435b51404ee:987e2eb29c51ab1b58cbee8392ca8321:::

## Appendix C

## Appendix C

**Figure 1-1** A diagram of the system that was used in the security test.

**Table 1-1** Advantages of the X versus Y

|  |  |
| --- | --- |
| **Advantage Description** | |
| **1** | Can be programmed easier. |
| **2** | More flexible that the traditional system. |
| **3** | More secure than the traditional setup. |



**Figure 1-1** Snippets of code can be formatted like this.

## Appendix D - Include your project deliverables and requirements sheet