Abertay University

Company Network Investigation

By: Nick Nesterenko

CMP210: Ethical Hacking 1

2020/21

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

Abstract

This paper describes the process of the penetration testing. The final goal of the test is to gain full root access to the given network which consists of two servers:

- Server1, 192.168.0.1.
- Server2, 192.168.0.2.

The penetration testing was conducted using a planned set of tools which could potentially lead to the achievement of the final goal.

In this project, the penetration testing process was divided into five sections:

1. Foot printing.
2. Scanning.
3. Enumeration.
4. Vulnerability Scanning.
5. System Hacking.

At each stage of the penetration testing a set of relevant tools were used to achieve the final goal:

1. Nmap – port and software version scanning.
2. Enum4Linux – enumeration tool.
3. NBTEnum – another enumeration tool.
4. Nessus – possible vulnerability and exploit scanner.
5. Hydra – password cracking tool.
6. Fgdump.exe – tool used for dumping the user passwords.
7. Armitage – Metasploit framework GUI, used to run exploits on target device.
8. Cain – password recovery tool, in this case used as password hash cracker.

Using the tools and the structure above it was possible to achieve the final goal which is the root access to the system on both servers. The full list of users and user groups was obtained from the enumeration process. The overall security of the system was relatively poor due to the ability of anyone gaining the access without advanced skill, the tools that were used are also mainly available for free, which makes the root access available to anyone. Overall, the penetration test was successful.

+Contents

1 Introduction

1.1 Background

Nowadays, organizing a network for the company/business needs is essential, such networks provide a significant improvement in communication and productivity no matter what type the business is. The number of networks set up worldwide is constantly growing and a wide majority of tasks within the businesses is completed through such networks. Alongside with the popularity of custom networks, the number of cyber-attacks is growing proportionally. For past 10 years the number of malware infections only grew more than 2000% (Figure 1):

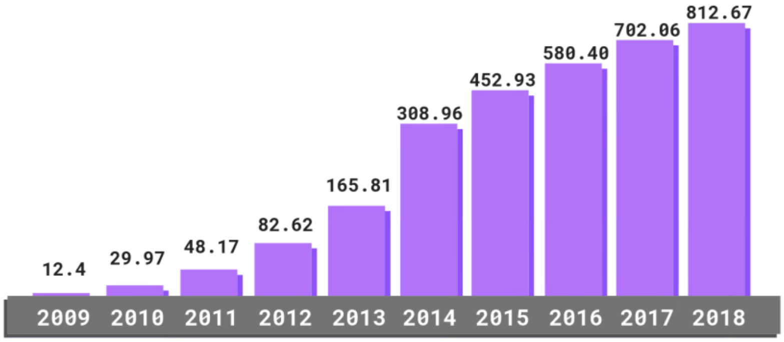


Figure 1: Total Malware infection Growth Rate

The factors mentioned above form an important business problem: “How to protect your Business’s Network”. One of the solutions to that problem is conducting regular network penetration tests to find possible misconfigurations or errors of the network that, if not taken care of, may result in theft of confidential information such as identity, passwords, other important for the business information, or faults in business operation.

1.2 AIM

The aim of this project is to conduct a standard penetration test and find possible vulnerabilities of the given network, with the final goal of gaining root access to the system. In order to reach the final goal, a list of tools was used, including:

- Nmap.
- Enum4Linux.
- NBTEnum.
- Nessus.
- Fgdump.exe
- Hydra.
- Armitage.
- Cain.

The list of tools mentioned above should allow the root access to be gained. For the penetration test, the user credentials were provided (username: test, password: test123), as well as the IP range of the network.

2 PROCEDURE

2.1 OVERVIEW OF PROCEDURE

This penetration test was performed using the standard structure of any penetration test against given servers (Server1 also referred as 192.168.0.1, Sever2 also referred as 192.168.0.2), the structure is:

1. **Foot printing** – this stage includes the research of the basic information which can be obtained from public sources and without any intrusive methods. Such information can include the physical location of the networks, details about the employees of the business, possible IP ranges, etc. This intel can help the penetration tester when moving on to the intrusive methods of testing. In this project, the foot printing step is skipped since there is no publicly available information due to the fact that the given network was specifically implemented for this project.
2. **Scanning** – at this stage, the use of intrusive methods begins. During the scanning stage, information about the opened ports on the network are checked, as well as the versions of the software which is ran on the network. This information can provide the idea for possible vulnerabilities in the network. In this project, the following software was used:
    - **Nmap** software was used to check for the opened ports as well as the versions of the software which were run by the Server1 and Server2, including the Operating system.
3. **Enumeration** – this is the main information gathering stage, which includes gaining the list of users/usernames, the list of user groups, etc. In this project, the following software were used:
    - **Enum4Linux** was used to find the description of the user accounts which gave the idea about the passwords used.
    - **NBTEnum** was used to get the full list of users as well as the user groups which helped to identify the accounts with administrator rights.
4. **Vulnerability Scanning** – at this stage, the network is checked for devices or software which are open to known vulnerabilities. In this project, the following software were used:
    - **Nessus** – was used to find possible vulnerabilities of the network.
    - **Nmap scripts** – alongside the scanning which can be done using Nmap, this application also supports scripts which can also be used for identifying possible vulnerabilities of the network.

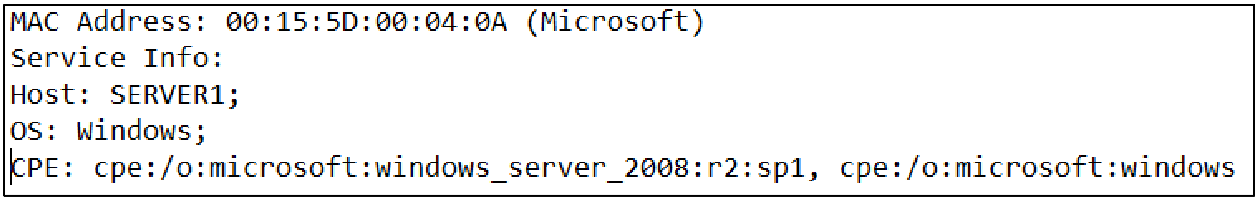
5. **System Hacking** – at this stage, after identifying the vulnerabilities, a known exploit is used in order to gain access to the target. In this project, the following software were used:
    - **Hydra** – was used to crack passwords using given password dictionaries. Unfortunately, did not give positive results.
    - **Fgdump.exe** – software which allowed to dump user password hashes, which later was used with **Cain** to get the passwords in plain hashed. 3 accounts with administrator rights were compromised.
    - **Armitage/Metasploit** – Armitage is a software which essentially provides the graphical user interface for the Metasploit. Metasploit is a penetration testing framework which provides information about known vulnerabilities as well as the database of known exploits. This application was used to gain full access to the network using "EternalBlue" exploit.

2.2 NMAP (SCANNING)

Nmap is a free and open-source network scanning application which is used to identify hosts and services on a computer network by sending packets and analyzing the results.

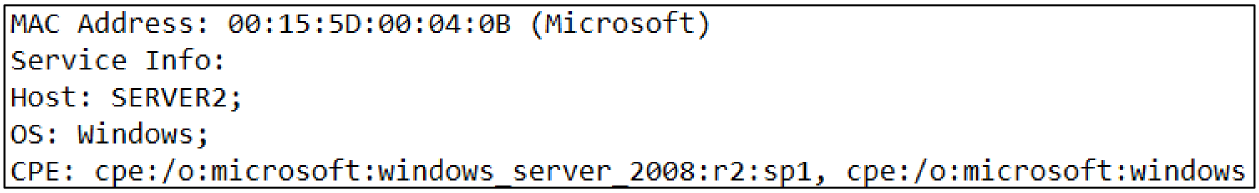
Running Nmap scans on Server1 and Server2 provided a range of important information:

- **The Operating System** was the most useful in this case since gave ability to utilize critical vulnerability (Figure 2, Figure 3):



```
MAC Address: 00:15:5D:00:04:0A (Microsoft)
Service Info:
Host: SERVER1;
OS: Windows;
CPE: cpe:/o:microsoft:windows_server_2008:r2:sp1, cpe:/o:microsoft:windows
```

Figure 2: Operating System of Server1



```
MAC Address: 00:15:5D:00:04:0B (Microsoft)
Service Info:
Host: SERVER2;
OS: Windows;
CPE: cpe:/o:microsoft:windows_server_2008:r2:sp1, cpe:/o:microsoft:windows
```

Figure 3: Operating System of Server2

- **The opened ports and versions of software** were not as useful since the possible vulnerabilities were not critical.

2.3 ENUM4LINUX

Enum4Linux is software for Linux which is used for enumerating data from Windows and Samba hosts.

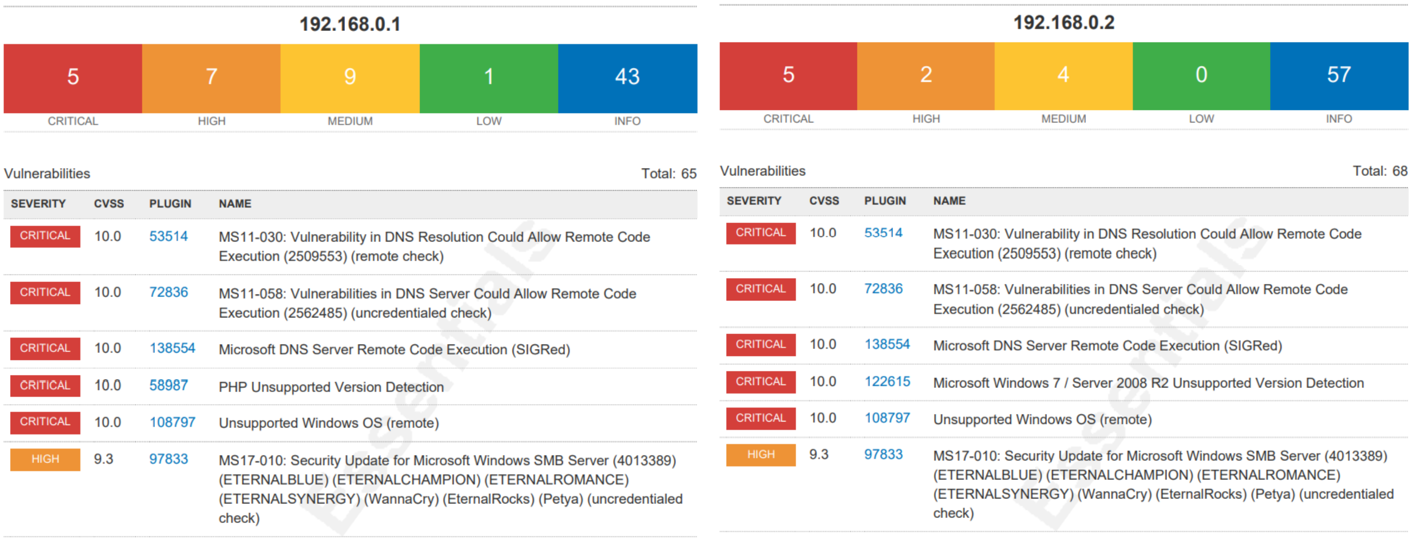
Running Enum4Linux enumeration provided a wide range of usable information including the description of the user accounts, the full list of usernames, the list of shared directories, user groups and user SIDs. The Server1 had correct configuration so enumeration for this server was not possible, however, Server2 provided the full range of information.

2.4 NBTENUM

NBTEnum or NetBIOS enumeration tool, is also used for enumerating data on various type of hosts. It provides a simple organized layout of output which makes it very effective when using. For this project, this application was redundant since Enum4Linux provides similar information, however NBTEnum outline the accounts with administration rights, which are the primary targets of this penetration test.

2.5 Nessus

Nessus is a vulnerability scanner which provides a range of vulnerabilities and exposures of the scanned network, it outlines most of the vulnerabilities which could allow unauthorized access to the sensitive data, the misconfigurations of the system and denials of service vulnerabilities. Nessus outlined that the version of operating system which was installed on both servers was highly vulnerable to the "EternalBlue" exploit (Figure 4). This exploit could provide root access to the network.



192.168.0.1

CRITICAL	HIGH	MEDIUM	LOW	INFO
5	7	9	1	43

Vulnerabilities — Total: 65

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	138554	Microsoft DNS Server Remote Code Execution (SIGRed)
CRITICAL	10.0	58987	PHP Unsupported Version Detection
CRITICAL	10.0	108797	Unsupported Windows OS (remote)
HIGH	9.3	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)

192.168.0.2

CRITICAL	HIGH	MEDIUM	LOW	INFO
5	2	4	0	57

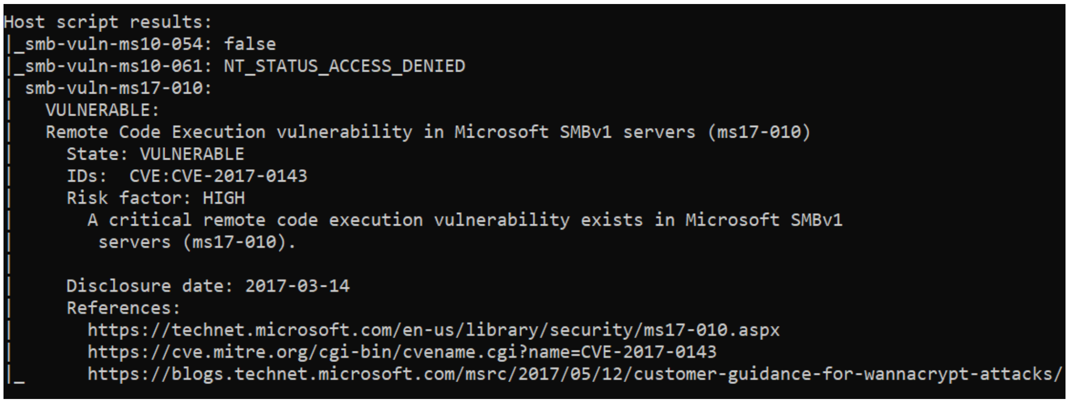
Vulnerabilities — Total: 68

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	138554	Microsoft DNS Server Remote Code Execution (SIGRed)
CRITICAL	10.0	122615	Microsoft Windows 7 / Server 2008 R2 Unsupported Version Detection
CRITICAL	10.0	108797	Unsupported Windows OS (remote)
HIGH	9.3	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)

Figure 4: Nessus most important results

2.6 Nmap (Scripts)

In this project the "--script vuln" Nmap scan was used to find known vulnerabilities of both servers, just like Nessus, Nmap identified critical vulnerability at the version of operating system installed (Figure 5):



```
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://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
```

Figure 5: Nmap Vulnerability

2.7 HYDRA

Hydra is a password cracking software for Linux which can be used with or without password dictionaries.

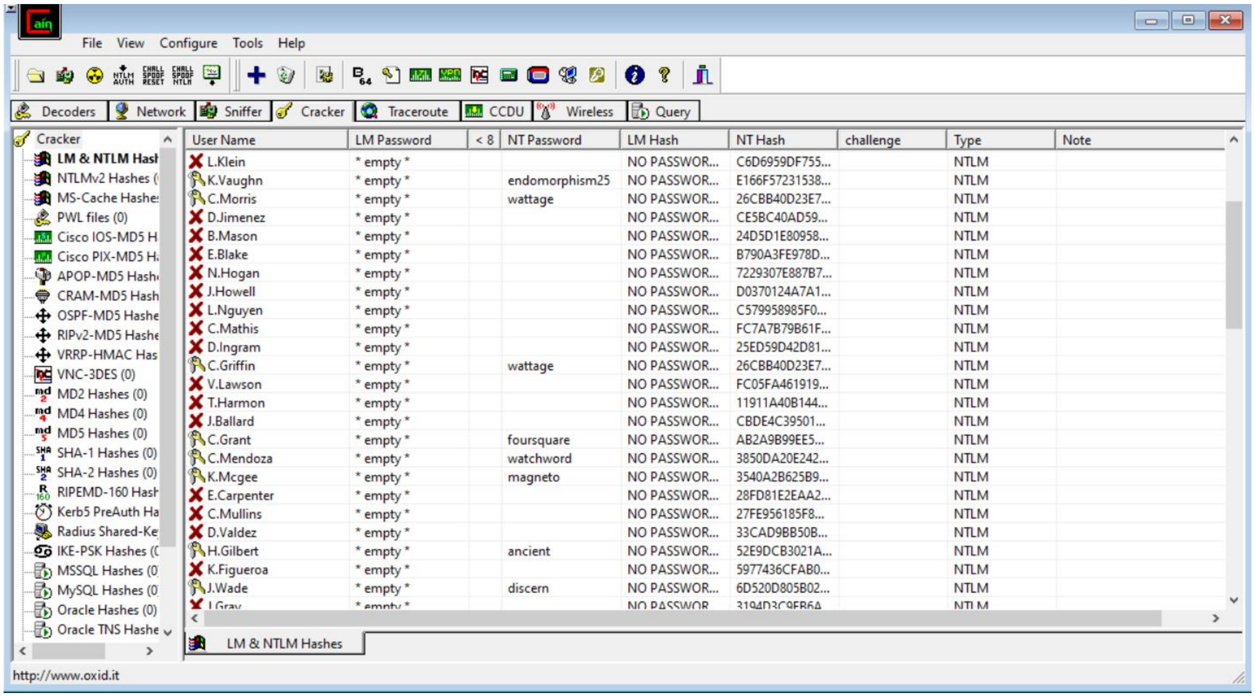
In this project using two different sets of password dictionaries did not provide any user password. The brute force functionality was not used due to the limited performance of the used hardware.

2.8 FGDUMP.EXE AND CAIN

Fgdump.exe is a Windows program that output the LM and NTLM password hashes of local user accounts from the Security Account Manager (SAM).

Cain is a password recovery tool that has a wide range of functionality like packet sniffing, decoding, etc. In this case the password cracking using a set of NTLM hashes was used.

In this project, the combination of the two software applications provided a set of cracked passwords with 3 of them having administration rights (Figure 6):



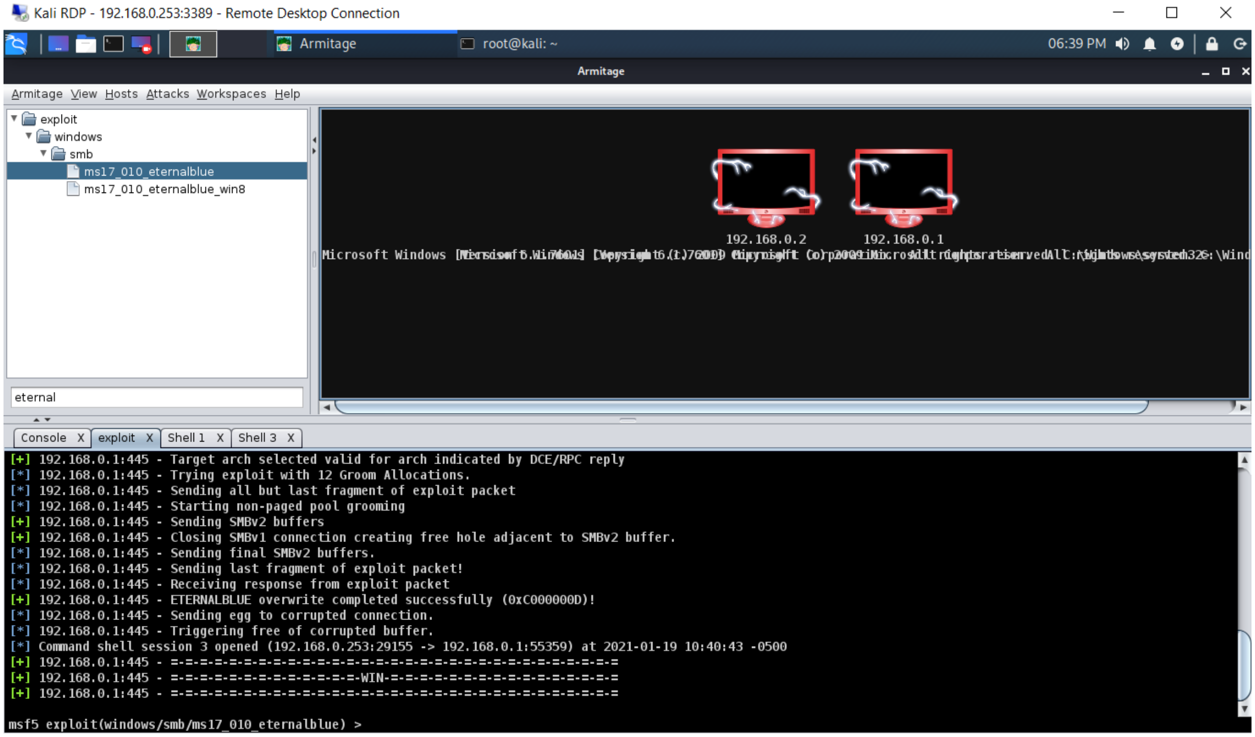
User Name	LM Password	< 8	NT Password	LM Hash	NT Hash	challenge	Type	Note
✗ L.Klein	* empty *			NO PASSWOR...	C6D6959DF755...		NTLM	
🔑 K.Vaughn	* empty *		endomorphism25	NO PASSWOR...	E166F57231538...		NTLM	
🔑 C.Morris	* empty *		wattage	NO PASSWOR...	26CBB40D23E7...		NTLM	
✗ D.Jimenez	* empty *			NO PASSWOR...	CE5BC40AD59...		NTLM	
✗ B.Mason	* empty *			NO PASSWOR...	24D5D1E80958...		NTLM	
✗ E.Blake	* empty *			NO PASSWOR...	B790A3FE978D...		NTLM	
✗ N.Hogan	* empty *			NO PASSWOR...	7229307E887B7...		NTLM	
✗ J.Howell	* empty *			NO PASSWOR...	D0370124A7A1...		NTLM	
✗ L.Nguyen	* empty *			NO PASSWOR...	C579958985F0...		NTLM	
✗ C.Mathis	* empty *			NO PASSWOR...	FC7A7B79B61F...		NTLM	
✗ D.Ingram	* empty *			NO PASSWOR...	25ED59D42D81...		NTLM	
🔑 C.Griffin	* empty *		wattage	NO PASSWOR...	26CBB40D23E7...		NTLM	
✗ V.Lawson	* empty *			NO PASSWOR...	FC05FA461919...		NTLM	
✗ T.Harmon	* empty *			NO PASSWOR...	11911A40B144...		NTLM	
✗ J.Ballard	* empty *			NO PASSWOR...	CBDE4C39501...		NTLM	
🔑 C.Grant	* empty *		foursquare	NO PASSWOR...	AB2A9B99EE5...		NTLM	
🔑 C.Mendoza	* empty *		watchword	NO PASSWOR...	3850DA20E242...		NTLM	
🔑 K.Mcgee	* empty *		magneto	NO PASSWOR...	3540A2B625B9...		NTLM	
✗ E.Carpenter	* empty *			NO PASSWOR...	28FD81E2EAA2...		NTLM	
✗ C.Mullins	* empty *			NO PASSWOR...	27FE956185F8...		NTLM	
✗ D.Valdez	* empty *			NO PASSWOR...	33CAD9BB50B...		NTLM	
🔑 H.Gilbert	* empty *		ancient	NO PASSWOR...	52E9DCB3021A...		NTLM	
✗ K.Figueroa	* empty *			NO PASSWOR...	5977436CFAB0...		NTLM	
🔑 J.Wade	* empty *		discern	NO PASSWOR...	6D520D805B02...		NTLM	
✗ J.Gray	* empty *			NO PASSWOR...	3194D3C9EB6A		NTLM	

Figure 6: The cracked passwords using Cain

2.9 ARMITAGE/METASPLOIT

Metasploit is an exploit framework which includes the database of common exploitable Common Vulnerabilities and Exposures (also known as CVE's) for penetration tests. Armitage provides a user interface for Metasploit.

After running Armitage Root using the "EternalBlue" exploit, the root access was obtained on both servers. Through this exploit, the attacker is able to perform nearly anything, including creating new admin users, in case of this project the privileges of the user "test" were escalated to administrator. New files and directories can be created, a remote desktop or command prompt shell (which allows the attacker to view a list of installed patches) can be organized. Armitage/Metasploit also is able to clear system logs with a single command once system-level access is gained, which would allow an attacker to cover their tracks very effectively. The evidence of the full root access can be found below (Figure 7)



```
[+] 192.168.0.1:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.0.1:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.0.1:445 - Sending all but last fragment of exploit packet
[*] 192.168.0.1:445 - Starting non-paged pool grooming
[+] 192.168.0.1:445 - Sending SMBv2 buffers
[+] 192.168.0.1:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.0.1:445 - Sending final SMBv2 buffers.
[*] 192.168.0.1:445 - Sending last fragment of exploit packet!
[*] 192.168.0.1:445 - Receiving response from exploit packet
[+] 192.168.0.1:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.0.1:445 - Sending egg to corrupted connection.
[*] 192.168.0.1:445 - Triggering free of corrupted buffer.
[*] Command shell session 3 opened (192.168.0.253:29155 -> 192.168.0.1:55359) at 2021-01-19 10:40:43 -0500
[+] 192.168.0.1:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.0.1:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.0.1:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

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

Figure 7: Root access screenshot

3 DISCUSSION

3.1 GENERAL DISCUSSION

The final goal of this report was achieved successfully, the full root access was obtained using Metasploit and the “Eternal Blue” exploit. The only stages that were necessary for such result was basic Nmap vulnerability script or Nessus scan that show which can be done by anyone without advanced skills in cyber security. The enumeration process for the Server2 was also relatively straight forward as it was misconfigured, unlike Server1 which did not enumerate with user account without elevated privileges. The users have decent passwords as the attempt to crack them using password dictionaries failed. However, there were some accounts which had password hints in them, and some of the passwords were cracked by using the dumped password hashes.

All in all, the ability to get data by enumeration and critical vulnerability to popular exploits makes the security of the given network relatively poor, however, it should be noted that Server1 was slightly more secure as it was enumeration resistant.

3.2 COUNTERMEASURES

The best way to improve security of any computer system is to keep the software up to date by installing the latest patches and updates. Having updated software makes it harder to find vulnerabilities as due to the short time from release, the public is not able to publish/find the vulnerabilities and by the time they do, the new patch will likely cover them.

Setting up decoy administrator accounts will make it more difficult for the hacker to identify the targets of the attack which can win the necessary time to locate the intruder or change the password.

It is important to configure the software as well as the hardware of the networking systems professionally, the stricter and more limited the access to certain aspects of the network is, the more secure it will be.

2-Factor authentication can be implemented to bring the possibility of gaining the unauthorized access to the network using the credentials of an existing user close to none.

Critical networking structure of the company can be localized, e.g. not being connected to the internet. This will limit the risk of the network being attacked outside of the physical location of the network.

Password policies can be introduced to make brute forcing more challenging and time consuming.

3.3 FUTURE WORK

There is a wide range of opportunities of future work with this project, such include:

- Brute forcing password of every user.
- Using other possible exploits so gain root access in different ways, using different vulnerabilities.
- Exploring files stored on the network to gain more clues about the network and the users, possibly physical addresses, emails, bank details, etc.

4 REFERENCES

Offensive security. 2021. Meterpreter basics. [ONLINE] Available at: https://www.offensive-security.com/metasploit-unleashed/meterpreter-basics/. [Accessed 18 January 2021].

Purplesec. 2021. Cyber Security Statistics. [ONLINE] Available at: https://purplesec.us/resources/cyber-security-statistics/. [Accessed 18 January 2021].

Tenable. 2021. Nessus overview. [ONLINE] Available at: https://www.tenable.com/cyber-exposure. [Accessed 18 January 2021].

Wikipedia. 2021. Nessus. [ONLINE] Available at: https://en.wikipedia.org/wiki/Nessus_(software). [Accessed 18 January 2021].

Wikipedia. 2021. Metasploit. [ONLINE] Available at: https://en.wikipedia.org/wiki/Metasploit_Project. [Accessed 18 January 2021].

Wikipedia. 2021. Nmap. [ONLINE] Available at: https://en.wikipedia.org/wiki/Nmap. [Accessed 18 January 2021].

Wikipedia. 2021. Pwdump. [ONLINE] Available at: https://en.wikipedia.org/wiki/Pwdump. [Accessed 18 January 2021].

Wikipedia. 2021. Cain_and_Abel_(software). [ONLINE] Available at: https://en.wikipedia.org/wiki/Cain_and_Abel_(software). [Accessed 18 January 2021].

Wikipedia. 2021. Hydra_(software). [ONLINE] Available at: https://en.wikipedia.org/wiki/Hydra_(software). [Accessed 18 January 2021].

APPENDICES

APPENDIX A

The Full result files of this penetration test can be found in the results.zip file, which is attached to the submission.