

Is Our Company Network Safe?

Checking for vulnerabilities within the network by using various application and preventing attacks from malicious attackers

Constantinos Sakkas

CMP210: Penetration Testing

BSc (Hons) Cybersecurity

Year 2

2023/24

**ABSTRACT**

As the world of technology rapidly changes throughout the decades and evolves, there are more dangers to new methods of attacks on company networks, which often contain sensitive data about employees, bank details, etc. Sensitive information about the company could be released and potentially damage the company’s reputation. The purpose of this report is to help reduce security vulnerabilities while increasing security standards for better infrastructure within the company network. The tests conducted in this penetration test helped find many forms of vulnerabilities, either open ports, poor password complexities, or easy access to usernames using simple exploit tools through Kali terminal or Windows Command Prompt.

Hours of testing on both Server 1 and Server 2 have shown me that both servers are poorly configured when it comes to security, with lots of vulnerabilities regarding security infrastructure. In a real-world scenario, both servers would have been hacked very soon, which goes to show that if a server is poorly configured, sensitive data can be easily stolen from a skilled malicious attacker. This penetration has helped future-proof both networks by patching the vulnerabilities and exploits that were found, which can help other companies with their networks. Help prepare future penetration testers to improve from the last penetration testers, so no misconfiguration of a server is repeated.

Contents

1.1 Background .............................................................................................................................4  
1.2 Aim ..........................................................................................................................................5  
2.1 Overview of Procedure.............................................................................................................6  
2.2.1 Setting Up VMware................................................................................................................6  
2.2.2 Packet Tracing........................................................................................................................7  
2.2.3 Scanning ................................................................................................................................7  
2.2.4 Emulation..............................................................................................................................12  
2.2.5 More Scanning .....................................................................................................................18

2.2.6 System Hacking .....................................................................................................................21  
3 Discussion ...................................................................................................................................25

3.1 General Discussion....................................................................................................................25

3.2 Countermeasures.....................................................................................................................25

3.3 Future Work ..............................................................................................................................25  
References .....................................................................................................................................26  
Appendices ....................................................................................................................................27  
Appendix A.................................................................................................................................... 27  
Appendix B…………………………………….............................................................................................. 31

1.1 Background

Background:

In the modern business world, the use of network-based technology is crucial to ensuring that everything is in order. However, as different corporations continue to digitize their operations and update any other systems that may be seen as obsolete these days, the dangers of cyber threats have unfortunately improved. With advancements in malicious insider threats, which pose a danger for most business enterprises, as well as external threats, Data breaches are an occurrence that never stops but continues. LinkedIn faced a data breach in 2021 where 700 of their users' data was stolen. The hacker then put the stolen data for sale in a forum called RaidForums two months after the attack, but although LinkedIn denied any user data being stolen, it faced another similar attack back in April 2021 when 500 million leaked. Data breaches are a serious matter, and security needs to always be high, as other companies have faced similar data breaches in the past, such as Google, Microsoft, etc.

**Example of data breaches:**

A diagram of a cause

Description automatically generated with medium confidence

Figure illustrator – Top 100 Largest Breaches (<https://www.nightfall.ai/blog/mega-breaches15-year-data-breach-report#analyzing-the-causes-of-the-top-100-largest-data-breaches>)

* Main causes being external threats or misconfiguration.

The Danger of Malicious Insiders:

People who have authorization to access various internal organization groups, called malicious insiders, can easily take advantage of any visible or known vulnerabilities in ways that external threats could not in a brief time but may take months. Whether through physical infiltration, etc., these insiders present a risk to the security of the organization. Their actions can cause information breaches or disrupt important services.

Purpose of Investigation:

The goal of this penetration check is to comprehend and cope with the dangers posed by way of malicious insiders. By simulating the moves of an insider with unauthorized access the purpose is to perceive any vulnerabilities in the organisation network and identify those vulnerabilities for them to patched as soon as possible so there are no repeats.

**1.2 Aim**

This penetrating test will be concentrating on both Servers 1 and a Server 2, which are imperative components of the company’s infrastructure. We will be conducting several penetration tests to fully find out what vulnerabilities are present within the company’s network. This evaluation is crucial for bolstering the company's defences against malicious insiders and even outside attacks as well.

**Wireless Network Vulnerabilities**:

* Examine the configuration of Server 1 and Server 2 to find any potential exploits.
* Any entry ports example ports which could be used to the advantage of malicious insiders who have a direct wireless connection to those servers.

**Physical Security:**

* Check both servers physically to examine the security which are in place as of conducting this research.
* Check for any physical vulnerabilities which may be beneficial to the insider attacker.

**Potential Recommendations to improve security:**

* Give advice and recommendations after the research has been concluded to strengthen security for future proofing security.

**Expectation of the penetration testing:**

* The expectation of this report is helping to fortify the company's defences against malicious attackers either from the inside or outside even though they would have a harder time gaining access to the servers. Also concentrating on both physical and wireless vulnerabilities, which will give us a better comprehension in understanding of the potential risks associated with Servers 1 and 2. The report will help guide current and future Network Administrators, in achieving a more secure network for the coming years and ensure a robust defence against vicious attackers of any type.

2.1 Overview of The Procedure

* The following procedures will be demonstrating what was undertaken and will walk you through the whole process this penetration test which targets Server 1 and Server 2. The investigation itself is all wireless with no physical components with the expectation of the PC that was used to conduct this penetration test.
* **The four steps that will be undertaken:**
* Packet Tracing
* Footprinting (in a real-world scenario this would be a part of a penetration testing but as its fictional this step cannot be done)
* Scanning
* Emulation
* System Hacking
* **Software and OS’s used for the penetration tasting:**

OS’s: Windows 11 and Kali GNU/Linux Rolling

Software Applications and tools: VMware Workstation (Windows), Wireshark (Kali), Command Prompt (Windows), Terminal Emulator (Kali), PUTY(Windows), Angry Scanner (Windows), Packet Tracing (Windows), Hydra (Kali), Nessus (Kali), ENUM4linux (Kali Terminal), Metasploit (Kali Terminal), Cain(Widows).

2.2.1 Setting Up VMware:

* Setting up VMware is very straight forward, you will first need to go to the [VMware website](https://www.vmware.com/uk/products/workstation-pro.html) , after downloading it you will need to acquire a licence to use it then proceed to set up the virtual machine thank you see the provided OneDrive link available on the MLS website where you can download the virtual machines from there but will need 7zip application to combine the files as they are broken up to files then extract them.
* Once everything has been properly configured by following the set-up sheet form, from the one drive link in MLS on how to configure VMware through the, then the penetration testing can begin, it should look something like in figure 1.

(Refer to figure 1 in Appendix A for layout)

2.2.2 Packet Tracing:

Wireshark (Kali)

A screenshot of a computer

Description automatically generated

(Figure.2)

* Figure 2 shows all three connected devises connected to the targeted network eth0, 192.168.10.1, 192.168.10.2, 192.168.10.10. The Ip addresses belong to the following 192.168.10.1 is Server 1, 192.168.10.2 is Server 2, 192.168.10.10 is the Client1 but it already has access to it.

2.2.3 Scanning:

Command Prompt:

.Tracert

A screenshot of a computer program

Description automatically generated

(Figure.3)

* Figure 3 shows when using Tracert on each Ip address displays their destination by sending packets to those machines and then there is response indicating they are both ON and what there is destination.

.Fping

A computer screen with white text

Description automatically generated

(Figure.4)

* Figure 4 shows that they are indeed ON by pinging them and both Sever 1 and Server 2 reply including Client1 as well.

Angry IP Scanner:

A screenshot of a computer

Description automatically generated

(Figure.5)

* Figure 5 shows when using angry scanner and specifying the Ip address it returns with 3 active devises with port 80 being open.

Kali Linux:

* Now from kali’s side and see what we get when the same type of tasks that are performed.

NMAP Ping Scanning:

* Nmap sort for Network is a useful utility built in the kali terminal which can help map a network, identify ports etc.

.sudo nmap -sn 192.168.10.1/192.168.10.2

A screenshot of a computer screen

Description automatically generated

(Figure.6)

* Figure 6 shows when using kali terminal there is more detail given on each Ip address.

Port Scans (Kali):

sudo nmap -sT 192.168.10.1

A screen shot of a computer

Description automatically generated

(Figure.7)

* Figure 7 shows nineteen open TCP ports meaning 19 vulnerabilities or ways for a malicious to gain access with the right tools.

.sudo nmap -sT 192.168.10.2

A screenshot of a computer

Description automatically generated

(Figure.8)

* Figure 8 has the same the same issue as in Figure6 with fourteen open TCP ports.

.Sudo nmap -A 192.168.10.1

A screenshot of a computer

Description automatically generated

(Figure.9)

* In figure 9 by using the above command you can see the IP addresses name, user, operating system version and security level but by using -A command it performs different attacks but can easily be detected, not ideal if you are trying to remain undetected although effective best to use -O command although it may not be able the operating system depending on how secure it is.

.Sudo nmap -A 192.168.10.2

A computer screen shot of a computer

Description automatically generated

(Figure.10)

* In figure 10 it is the same as figure 9.

**2.2.4 Emulation:**

* Like scanning but with more detailed information on the chosen target.

Windows Command Prompt:

.Nslookup

A screenshot of a computer

Description automatically generated

(Figure.11)

* In figure we can see all the DNS associated with each IP address.

Kali Linux:

Terminal Emulator:

.Nbtscan -v -t :192.168.10.1

A screen shot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

(Figure.12)

* In figure 12 we can see a more detailed NETBIOS names for both Server 1 and 2.

SMBMAP:

* Using this command can help retrieve any networked shared files which can prove to be useful to an attacker as these files can contain passwords etc.

.smbmap -u test -p test123 -H 192.168.10.1

(Refer to Appendix A for Figure.13 to see the screenshot)

* Figure 13 displays all the files on Server 1 which can be accessed remotely although they are read only.

(Refer to Appendix A for Figure.14 to see the screenshot)

* Figure 14 shows the files on Server 1 when typing //192.168.10.1 in file explorer search bar (in a real-world scenario we would not have the credentials to be able to view the actual files but only view them through the terminal itself).

(Refer to Appendix A for Figure.15 to see the screenshot)

* Figure 15 is the same process as Figure 14 with different files.

A screenshot of a computer

Description automatically generated

(Figure.16)

* Figure 16 shows netlogon is only accessible by an admin account which we do not have the credentials to yet.

**User Accounts:**

* Using this command below will help display all the user account names for Server 1.

.rpcclient -U "test" 192.168.10.1

(Refer to Appendix A for Figure.17 to see the screenshot)

* Figure 17 displays User Accounts names.

(Refer to Appendix A for Figure.18 to see the screenshot)

* Figure 18 shows the Server 2 User Accounts as well.

**Password Length**:

.polenum test:test123@192.168.10.1

A computer screen shot of a person

Description automatically generated

(Figure.19)

* Figure 19 is targeted to the admin account and shows in detail of password length and domains.

A computer screen shot of a person

Description automatically generated

(Figure.20)

* Figure 20 is the same as Figure 19.

**Note:**

* Keep in mind that the administrator account has 500 as part of its SID at the end SID \\S 1 5 21 3909509232 36235851 949330273 500.

Which and how many accounts have admin permissions??

* Figure 21 below shows four local groups and one administrator.

A computer screen shot of a computer program

Description automatically generated

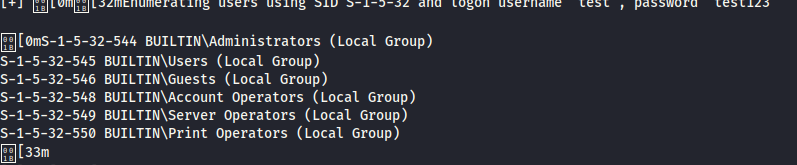
(Figure.21)

**Target Group:**

**ENUM4linux:**

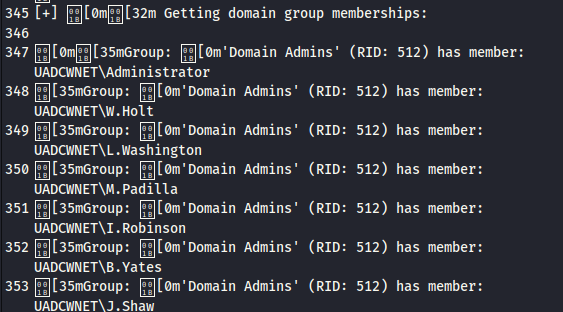
.enum4linux -a -u test -p test123 192.168.10.1 >/home/kali/Desktop/enum.txt

**The Five Local Groups:**

****

(Figure 22)

* Figure 22 lists all five groups in Server 1.



(Figure 23)

* Figure 23 shows all the different user groups, but the admins are the target give us the attackers full access to the Servers.

A screen shot of a computer

Description automatically generated

(Figure 24)

* Figure 24 is the same as figure 23.

**2.2.5 MORE SCANNING:**

**Nessus:**

* A useful tool that can help identify any existing vulnerable security issues and often used for penetration testing to resolve these issues through patches etc.

**Getting Started:**

* Go to this link <https://localhost:8834/> through a kali web browser where you will be prompted to login using the credentials of admin and password hacklab shown in Figure 25.

A screenshot of a computer

Description automatically generated

(Figure.25)

* After you login you will choose a new scan then proceed to Basic Network Scan, then type the IP address and through windows enter the test credentials and domain as well, shown in Figure 26.

A screenshot of a computer program

Description automatically generated

(Figure.26)

**Runing the scan:**

A screenshot of a computer

Description automatically generated

(Figure.27)

* Figure 27 illustrates that Server 1 has more variabilities compared to Server 2

Results:

Server 1:

A screenshot of a computer

Description automatically generated

(Figure.28)

* Figure 28 shows that there 105 vulnerabilities in total

Server 2:

A chart with different colors

Description automatically generated with medium confidence

(Figure.29)

* Figure 29 has fewer vulnerabilities compared to figure 28 with 98 vulnerabilities.

**Server 1 Sample Results:**

(Refer to Appendix B for Figure.30 to see the screenshots)

**Server 2 Sample Results:**

(Refer to Appendix B for Figure.31 to see the screenshots)

2.2.6 System Hacking:

Password Hacking:

Using Hydra:

* Hydra is a password cracker utilising txt files to crack online passwords or usernames. Although using it can potentially take a couple of hours to crack a password or username.

**Attempt 1(Failed):**

A screen shot of a computer

Description automatically generated

(Figure.32)

* Figure 32 shows on the first attempt using the small text file did not work.

Attempt 2(Success):

. hydra -V -L users.txt -P "cain.txt" smb://192.168.10.1

A screen shot of a computer program

Description automatically generated

(Figure.33)

* Figure 33 illustrates when using cain txt we managed to get a password match, but the process took more that 3 hours to complete.

**Using Metasploit:**

**Hashdump:**

(Refer to Appendix B for Figure.34 to see the screenshot)

* When using **getsystem, hashdump,** an error occurs and have to **migrate** it to a system in order to get hash by typing **ps** then finding SYSTEM, doing this can resolve the issue as shown in Figure 34.

**Using Cain:**

* Useful tool to crack hashes by copying the hashes from kali terminal then store them to text file where through cain select Cracker then add to list by right clicking and selecting the hash text file and selecting cain text file and the output being as shown in Figure 35.

A screenshot of a computer

Description automatically generated

(Figure.35)

Accessing Server 1 with user credentials:

Using J. Shaw account credentials, we gain full access to server 1 as shown in Figure 36.

A computer screen with a white screen

Description automatically generated

(Figure.36)

**Password Guessing the Administrator Account:**

* Password guessing can be effective but time-consuming, but as this is a fictitious network, cracking it was not too hard, and using the password Thisisverysecret1 from the tutorial network, through trial and error produced different versions of Thisisverysecret1, for example, Thisisverysecret123, Thisisverysecret12, and Thisisverysecret19. The password was **Thisisverysecret21**, which gives access to both administrator accounts on Server 1 and Server 2, as shown in figures 37 and 38.

**Server 1:**

**A screenshot of a computer

Description automatically generated**

(Figure37)

**Server 2:**

**A screenshot of a computer

Description automatically generated**

(Figure.38)

**3 DISCUSSIONs**

**3.1 GENERAL DISCUSSION:**

* After hours of extensive work and constant testing through trial and error due to Kali or Windows not being able to communicate with the server on occasion (they did after a bit of network configuration), the testing has shown that both Server 1 and Server 2 had many vulnerabilities regarding security. Server 1, which contained the most sensitive data such as usernames and other files of different natures, had the most vulnerabilities due to its crucial issue of having 19 open ports, compared to Server 2, which only had 14. Although being unable to verify security protocols being public, hacking into both servers had some challenges compared to a real-life scenario where it would have been far more complex, and the servers were configured intentionally to have so many vulnerabilities to make it easier to gain access to them. No system hacking was done due to password guessing the administrator password and the same password being used on both servers. By just gaining access to both administrator accounts, there was no need for system hacking, considering the administrator accounts have access to all sensitive data. Because the whole network was fictitious, not all results produced can be seen as real, and my aim to fortify the company’s network cannot fully become a reality due to it being fictitious and not to scale of a real company network, but regardless, the penetration test has helped to show what could possibly happen if a network is not set up correctly and what data can be potentially stolen. Additionally, both servers OS were out of date, making them more prone to malicious attacks as well.

**3.2 COUNTERMEASURES:**

* When setting up new a network always be sure it is being set up by a qualified specialist then processed to test the network infrastructure to check for any potential vulnerabilities before it's integrated into the company's network which could act as backdoor access for malicious attackers.
* When interviewing a new employer double check their history and be sure they can be trusted if their position will have access to sensitive company data.
* Implement encryption protocols for sensitive data.
* Routine inspection of the networks to possible identify new vulnerabilities.
* Train new or current stuff to be up to date.

**3.3 FUTURE WORK:**

* With more time and resources, the penetration test would have been more complex meaning more testing, even gather a group of people to expand this test and see how far we could take this and what the limit is by hiring professionals. See if we discover new forms of attacks. Even work with other large tech companies.

References:

* VMware(Broadcom Inc)( <https://www.vmware.com/uk/products/workstation-pro.html>) (Accessed 29 of November 2023).
* Tenable”,Inc ([https://localhost:8834/)](https://localhost:8834/)%20(Accessed) (Accessed 10th of December 2023).
* Lee Mathews. 2021 x86 Details on 700 million LinkedIn Users For Sale On Notorious Hacking Forum [Blog] 29 Jun. Available from (<https://www.forbes.com/sites/leemathews/2021/06/29/details-on-700-million-linkedin-users-for-sale-on-notorious-hacking-forum/>) (Accessed 27th November 2023).
* Figure Illustrator - Michael Osakwe.2021 x86 The Anatomy of Mega-Breaches: An Analysis of the Top 100 largest Data Breaches of the Past 15+ Years [Blog] (<https://www.nightfall.ai/blog/mega-breaches15-year-data-breach-report#analyzing-the-causes-of-the-top-100-largest-data-breaches>) (Accessed 12th of December 2023).

**APPENDICES**

APENDIX A:

**VMWARE LAYOUT:**

**A screenshot of a computer

Description automatically generated**

(Figure.1)

SMBMAPA screen shot of a person

Description automatically generated

(Figure.13)

A screenshot of a computer

Description automatically generated

(Figure.14)

A screen shot of a person taking a selfie

Description automatically generated

(Figure.15)

**User Accounts:**

A screen shot of a computer screen

Description automatically generated

(Figure.17)

A screen shot of a computer screen

Description automatically generated

(Figure.18)

APENDIX B

**NESUS**

**Server 1 Sample Results**

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

(Figure.30)

**Server 2 Sample Results:**

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

(Figure.31)

**Hashdump**

A computer screen shot of a computer program

Description automatically generated

(Figure.34)