

|  |
| --- |
| **Penetration Test Report**  *This report is being produced for a company that has requested a penetration test to be done on their network, this will go through what vulnerabilities were found and what can be done to fix them.*  **Snow White**  CMP210: Ethical Hacking  2023/24 |

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

Abstract

This paper will be about a penetration test done on a company, to see what vulnerabilities they may have and how these can be rectified. This paper will also include ways to keep the company safe and to mitigate any vulnerabilities they may have.

This paper will include the ways in which the pen tester got into the network/machine and if anything was found. Which included using things like nmap to find out what machines were also on the companies’ network and what operating systems and what versions were being run, which then allowed the pen tester a way to see if that software had any vulnerabilities that would allow them in.

When the pen tester got into the network/machine their findings included things like an outdated operating system that hasn’t been updated. The mail server hasn’t been updated so is also vulnerable to being exploited by using the authentication bypass. There were also serval vulnerabilities in the php which could be used to get into these machines. Another one of these vulnerabilities found was a critical one that had several vulnerabilities, it was Oracle Java.

There was also a high vulnerability with the Windows DNS Server with an RCE number attached which is RCE (CVE-2020-1350).

These findings have shown the pen tester that this company has vulnerabilities that need to be addressed and sorted immediately to make sure that they are not vulnerable to any of these types of attacks.

Contents

[1 Introduction 1](#_Toc153568078)

[1.1 Background 1](#_Toc153568079)

[1.2 Aim 2](#_Toc153568080)

[2 Procedure 3](#_Toc153568081)

[2.1 Overview of Procedure 3](#_Toc153568082)

[2.2 Scanning 4](#_Toc153568083)

[2.3 Vulnerability Scanning 6](#_Toc153568084)

[2.4 Enumeration 8](#_Toc153568085)

[2.5 Password Hacking 9](#_Toc153568086)

[2.6 System Hacking 10](#_Toc153568087)

[3 Discussion 16](#_Toc153568088)

[3.1 General Discussion 16](#_Toc153568089)

[3.2 Countermeasures 17](#_Toc153568090)

[3.3 Future Work 18](#_Toc153568091)

[4 References 19](#_Toc153568092)

[Appendices 20](#_Toc153568093)

[Appendix A 20](#_Toc153568094)

[21](#_Toc153568095)

[23](#_Toc153568096)

[23](#_Toc153568097)

[Appendix B 24](#_Toc153568098)

[25](#_Toc153568099)

[25](#_Toc153568100)

[Appendix C 26](#_Toc153568101)

[Appendix D 36](#_Toc153568102)

# Introduction

## Background

This report is going to be for a penetration test, that is going to be carried out on a company’s system/servers.

This is going to be done by following a pen test methodology which consists of several stages. Normally the pen test would include Footprinting but as that is not in the scope of works for this pen test it will not be done this time around.

There are several different types of penetration test methodologies out there but the one that will be used for this pen test is:

* Scanning
* Vulnerability Scanning
* Enumeration
* Password Hacking
* System Hacking

This pen test is to see if there are any vulnerabilities and weaknesses that can be exploited to gain unlawful access to their systems or information they hold. This pen test will be checking to see if there are vulnerabilities, and then will come up with countermeasures for any that are found like updating vulnerable software.

A pen test is something that companies/organizations/governments can have done either in house or by a third-party cyber security company. It is an authorized simulated attack which is performed on a computer system to determine its security. Pen testers will use the same tools, techniques and processes as attackers to find and demonstrate the impacts this will have on the business due to the weaknesses in the system. (Synopsys, n.d.).

According to NCSC (Penetration Testing, 2017) pen testing is a core tool for analyzing the security of IT systems, but it’s not a magic bullet. Even with doing pen tests regularly, companies/organizations can still be vulnerable to attacks on their network. A pen test will help to mitigate these things from happening, it will not stop it completely but will reduce the risks. As shown below in figure 1, these are the benefits of Penetration testing. It is a very important thing that companies/organizations should have in place to keep them safe.

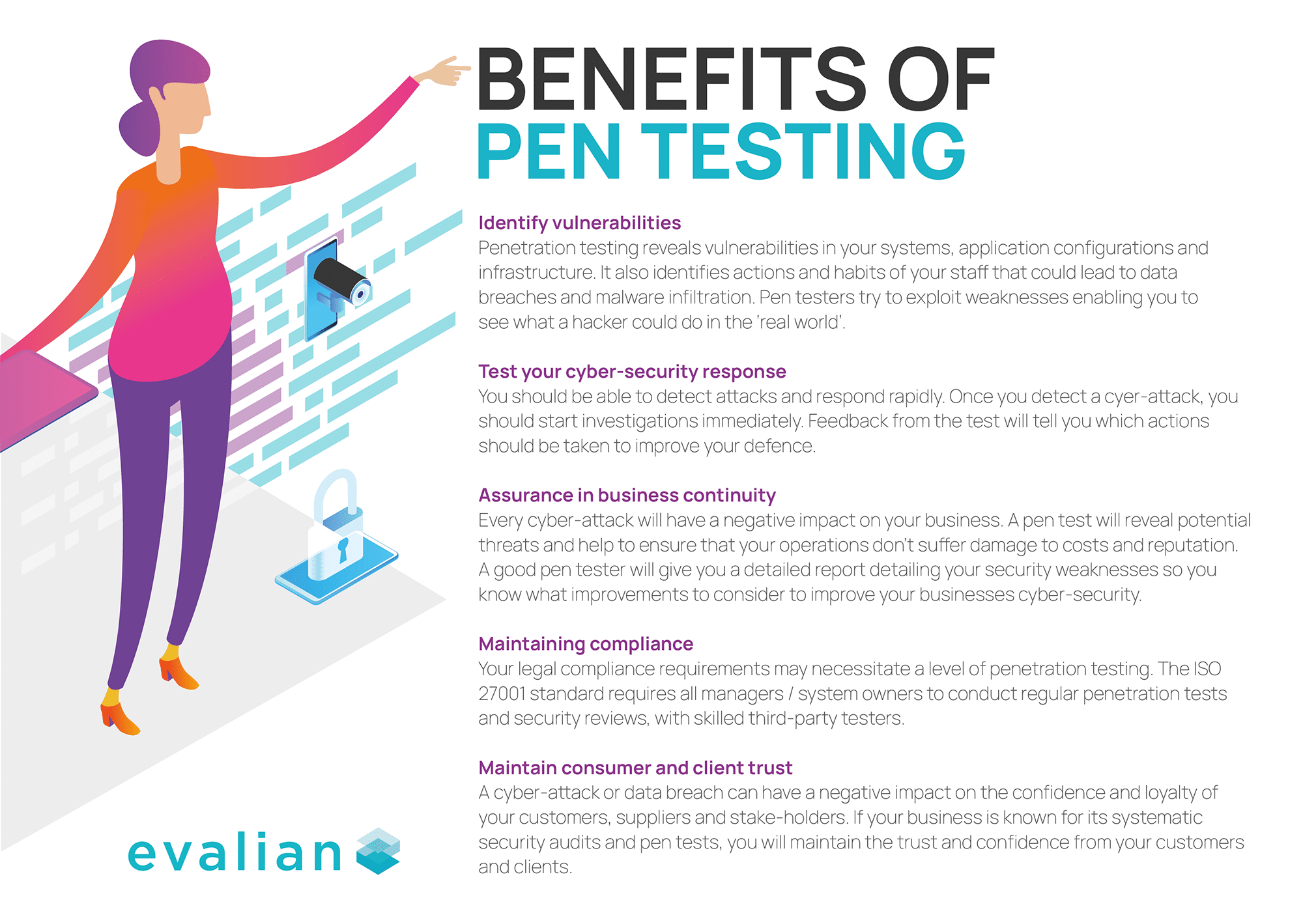


Figure 1 A Picture of the benefits of Penetration Testing

Source(<https://evalian.co.uk/the-benefits-of-penetration-testing/)>

## Aim

The aim of this paper is to do a penetration test for a company to see what vulnerabilities they have or may have. This will be done by:

* Scanning their network/computers to see how many vulnerabilities there are.
* To see if the machine/network can be broken into
* What can be done to these machines/network if these can be broken into?
* Report back the findings of the pen test.
* Suggest any ways to mitigate this from happening in the future.
* And discuss any future work that could be carried out.

# Procedure

## Overview of Procedure

For this paper, the pen tester was given access to a client machine with user credentials, and as per the scope of works was tasked to see what vulnerabilities were available on any machines on this network like server1 and server2.

This pen test will be done in several stages. In this pen test the stage Footprinting will not be done as this pen test is going to focus on the 2 server machines that the pen tester was given to try and gain access to.

The stages covered in this part of the report are going to be the Scanning Stage, Vulnerability Scanning, Enumeration Stage, Password Hacking and System Hacking Stage.

The Scanning Stage is where the pen test is started which includes scanning the network/computers and seeing what info was gleamed from these scans.

The Vulnerability Scanning Stage is where a Nessus Scan is being run on any ips that were found in the Scanning Stage to get a full list of any vulnerabilities they may have, this will break down the vulnerabilities into critical, high, medium and low vulnerabilities.

The Enumeration Stage is where the pen tester is going to try and find user accounts that can be used to gain access to the target machines and help find any other useful information that will help the pen tester as well as looking at the vulnerabilities that were found in the Scanning Stage.

The Password Hacking Stage is where the pen tester will be trying to crack passwords of any user accounts that were found to have admin access to gain access to the target machines.

The System Hacking Stage is where the pen tester has gained access into the system via an exploit using metaspoilt in a kali linux machine and then showing what can be done in the remote shell that has been opened which can will include things like keylogging, setting up a persistence script etc.

## Scanning

A screenshot of a computer

Description automatically generatedThe first thing that was done was log into the client machine and run an ipconfig which gave the pen tester the ip address 192.168.10.10 that was being used by the client machine. Shown in Figure 2 below.

Figure 2 Picture of Scan Run on Client Machine

Once the ip was found, the pen tester logged into Kali Linux to run a nmap scan on the ip address that was found in the client machine to see if there were any other machines or servers on those ip addresses by using a specific command which is nmap 192.168.10.10/24. This is the information that was received from this scan, it was found that there are 2 other machines using an ip in this range, which are 192.168.10.1 and 192.168.10.2 which can be assumed to be server 1 and server 2, in Figure 3 and Figure 3.1 shown below is a screenshot of the information found from the nmap scan.

A computer screen with white text

Description automatically generated

Figure 3 – Screenshot information found from the nmap scan of the first ip that was found.

A screen shot of a computer

Description automatically generated

Figure 3.1 – Screenshot of information found from second ip found.

As there were 2 other ips found by doing the first nmap scan , which are 192.168.10.1 and 192.168.10.2 the next move is to do a another set of nmaps on these ips that have been found which will give more information with things like open ports and operating systems. The nmaps on both ips has also revealed the names of both these machine which are server 1 and server 2 as shown in Figure 3.2 and 3.3 below , which means the pen tester has found the target machines they were tasked to look for.

A screen shot of a computer

Description automatically generated

Figure 3.2 – Screenshot of the machine name for ip 192.168.10.1

A screen shot of a computer

Description automatically generated

Figure 3.3 – Screenshot of the machine name for ip 192.168.10.2

For the full scan results of server 1 and server2 see Apendix A but shown below in Figure 4 is a snip of the most important information that was found which gives the operating system Windows Server 2019 Standard and it’s build number which is 17763 as well as the mail server which is ArGoSoft Mail Server Freeware and its build number which is Version 1.8(1.8.2.9).

A screenshot of a computer program

Description automatically generatedFigure 4 A screenshot of information found in nmap scan

The next step the pen tester is going to be doing is a vulernability scan using something called Nessus which will be done in the next section.

## Vulnerability Scanning

The next stage that is going to be done is vulnerability scanning which is going to be done by using a piece of software called Nessus, which is going to do a scan on the ips that were found in the nmap scans in the scanning stage.

By using the credentials, the client has given the pen tester for the client machine which are test and tes123, this will be used when going into nessus to setup the scan for server 1 and server 2 ips.

A screenshot of a computer

Description automatically generatedOnce the pen tester has logged into Nessus, there will be a choice of different types of scans that can be run but for this pen test it is just a normal basic scan that was chosen. Once that has been decided it will come up with a form to input information like the ips to be scanned and any user credentials as shown in Figure 5 and 5.1 below

A screenshot of a computer

Description automatically generatedFigure 5 – A screenshot of a Nessus scan being setup

Figure 5.1 – A screenshot of user credentials being inputted in the Nessus Scan settings.

Once these details have been saved, the scan is ready to be run.

Now that the scan has been run, Nessus will produce a report of all the vulnerabilities that server 1 and server 2 have and give the levels of how dangerous they are from critical to low.

On Server 1 there were 45 Critical, 37 High, 21 Medium and 2 Low vulnerabilities found by the Nessus scan.

On Server 2 there were 37 Critical, 27 High, 12 Medium and 1 Low vulnerability found by the Nessus scan.

In Appendix C will be the full report of the vulnerabilities. Below in Figure 6 and Figure 6.1 are screenshots of some of the most important vulnerabilities that were identified.

A screenshot of a computer program

Description automatically generated

Figure 6 – Screenshot of the Critical vulnerabilities

A screenshot of a computer

Description automatically generated

Figure 6.1 – Screenshot continued of the Critical vulnerabilities found by the Nessus Scan.

Now that those scans have been completed , the pen tester has taken the information that was found in these scans as well as the information found in the nmap scans and used it to do some internet searches to see if any of these pieces of software are vulnerable to being exploited or broken into.

Which they are vulnerable to several exploits, that can be used to gain access to the target machines. This will be discussed in depth in the Discussion section where the results of the internet searches will be spoken about in terms of what was found from these vulnerabilities and if there are any exploits that could be used to gain access to these machines.

## Enumeration

Now that a few vulnerabilities have been found, the pen tester is going to look at enumeration.

The pen tester is going to look at using enum4linux in kali linux. By running a command and using the username test and password test123 on the ip from server 1 to see what user accounts can be found. This will show us the account name and any descriptions attached to it which can then be used later. In Figure 7 shown below is a small section of what was found for by running this command, for the full amount of user accounts found see Appendix B.

A screenshot of a computer

Description automatically generated

Figure 7 A screenshot of information found during the enun4linux scan.

One of the next things the pen tester did was to run a command called a smtp-user-enum to check if these users do exist as shown in Figure 8 below.

A screenshot of a computer

Description automatically generated

Figure 8 – A screen snip of the smtp on user J. Shaw

The next step was to go onto the client’s machine that the pen tester was given access to and by using NetBIOS to see if the user accounts that were found had admin privileges, as well as looking at things like any password policies in place or any password lockouts on the accounts. The pen tester checked the account of J. Shaw as shown Figure 9 below.

A screen shot of a computer

Description automatically generated

Figure 9 – A screenshot of the results of J. Shaw user account.

This information enables the pen tester to identify that J. Shaw possesses admin access. Additionally, since there are no specified login hours for the user, it reduces the likelihood of IT flagging their account for usage outside of office hours.

## Password Hacking

Now that the pen tester has an account name and an ip to use ,the pen tester will use a password cracker on the kali machine called hydra to see if that will give a password to J. Shaw ‘s account.

In the kali machine the pen tester opened a text file and put in J. Shaw’s name and saved it under users.txt. Once that was done the pen tester opened a terminal in kali and ran a command to run Hydra which was hydra -V -L users.txt -P "small.txt" smb://192.168.10.1. This was using a small dictionary file and didn’t gain any results so the pen tester then ran it against the dictionary word list called cain.txt which is a bigger dictionary file to see if that would gain any results which is shown in Figure 10 below.

Figure 10 – Screenshot of the hydra results

Once this password was found the pen tester wanted to try and see if they could access that machine remotely from the client’s machine and see what shares had been made from those ip addresses as well as seeing the files etc. Screenshots below of Figure 11 and Figure 11.1 show them gaining successful access to this machine via command prompt.

A screen shot of a computer

Description automatically generated

Figure 11 – Screenshot showing access gained on ip 192.168.10.2

A black background with white text

Description automatically generatedFigure 11.1 – Screenshot showing access acquired.

Now that the pen tester has a password for the user account J. Shaw, it was used to see if it would allow access to server 1 which it did.

Now that pen tester has been able to login into the machine via the user account that was found during the enumeration stage, it is now possible to be able to do things like add new admin user accounts, put malicious files on the machine that when a user opens them it will infect the machine with malware or ransomware as well as gain a remote shell from a document.

Now that the pen tester has gained access via password cracking, it is time to move on to system hacking so see if it is possible to gain access via metaspoilt in Kali Linux. Which will be done in the next section called System Hacking.

## System Hacking

The pen tester has found a way to get into this machine by using metaspoilt to run an SMB exploit to gain a meterpreter session into the targets machine.

Before this exploit can be run the pen tester needs to turn off the windows defender on the target machines as Windows Defender recognizes the metaspoilt payload and deletes it. The way around this is to run a command prompt from the client machine to turn Windows Defender off with tools that the pen tester has in a folder.

The command for this is cd C:\Users\admin\Desktop\tools\PSTools, which has put the pen tester in the PSTOOLS folder, then the next command the pen tester will use is psexec -u J.Shaw -p howsomever \\192.168.10.1 cmd and the next command that was inputted was powershell. Then to stop windows defender from running the powershell command that was input was Set-MpPreference -DisableRealtimeMonitoring $true , this is shown in Figure 12 below.

A computer screen with white text

Description automatically generated

Figure 12 – A screenshot of turning the Windows Defender off in the target machine

Now that windows defender has been successfully turned off the pen tester can continue with trying to exploit the target machine.

Refer to Appendix D for the full Metaspoilt images.

In the kali terminal the pen tester has opened a terminal and ran the msfconsole command to start up metaspoilt to try and run the exploit.

Once that loaded up, the pen tester entered in the command use exploit/windows/smb/psexec and hit enter once that has been done , then the pen tester entered in show options which gave the pen tester information on current settings as show in Figure 13 below.

A computer screen shot of a computer screen

Description automatically generated

Figure 13 – A screenshot of what information is needed for the SMB psexec exploit.

This demonstrates the configuration parameters required for executing the exploit. The pen tester proceeds by setting the SMBDomain to the identified domain, which is 'uadtargetnet.com.' Subsequently, the SMBpass is set to the discovered password ('howsomever'), followed by configuring SMBuser as 'J. Shaw.' The RHOSTS is then set to the target IP address, 192.168.10.1, while the LHOST is configured to the Kali IP, 192.168.10.253.

Figure 13.1 illustrates this process, showcasing the penetration tester successfully gaining access to the target machine.

A screenshot of a computer program

Description automatically generated

Figure 13.1 – Screenshot of the pen tester getting in through SMB exploit.

The pen tester has been able to get into the targets machine as they are vulnerable to an SMB exploit in metaspoilt. One of the first things the pen tester did was to run a sysinfo command to make sure it is the target machine that has been breached which is shown in Figure 14 below.

A screen shot of a computer program

Description automatically generated

Figure 14– Screenshot of the sysinfo command

Now that the pen tester has confirmed that the correct machine has been breached, several actions were taken to extract more information using various enumeration commands.

One of the enumeration things to run is an enum gather command on applications which will give the pen tester all the applications running on the target machine as well as build/version numbers which can give more information on if the operating system gets patched, the pen tester could see if any of these applications are vulnerable . As shown in Figure 15 below this is a screenshot of what was found on the target machine using this command.

A computer screen shot of a computer program

Description automatically generated

Figure 15 – Screenshot of result from the enum gather applications command.

The next enum is an enum shares command which will show what has been shared from the targets machine as shown in Figure 16 below.

A screenshot of a computer

Description automatically generated

Figure 16 – Screenshot of the enum shares command.

A couple of things that can be done now that the pen tester has gotten into the target machine are things like running a keylogger through meterpreter which will pick up any keystrokes on the target machine. Shown below in Figure 17 and Figure 17.1 are 2 screenshots, one from the target machine showing a sentence that was typed and then a screenshot from the pen testers meterpreter dumping the keystrokes.

A screenshot of a computer

Description automatically generated

Figure 17 – Target machine showing text that has been typed when a keylogger is running.

A screenshot of a computer screen

Description automatically generatedFigure 17.1 – Pen tester using keylogger and showing the results from targets machine.

The pen tester has also executed a persistence script, enabling a reconnection without repeating the entire exploit phase, as illustrated in Figure 18 below.

A computer screen shot of a computer program

Description automatically generated

Figure 18 – A screenshot of the persistence script.

There were ways that the pen tester could clear their tracks so that the victim didn’t know they were there. For example, the pen tester can use a command called clearev (Mastering Metasploit, n.d.).

The pen tester cleared the Application, System, and Security logs from the victim’s machine. Figure 19 below shows the pen tester using the clearev command to eliminate their tracks.

A blue background with white text

Description automatically generated

Figure 19 – Clearev command clearing the track of the pen tester.

Now that all stages of the penetration test have been complete, the report will now move on to discuss the results that have been found throughout the pen test.

# Discussion

## General Discussion

Now that the pen test has been completed, the results can be discussed. There are a lot of vulnerabilities in both machines that could be used to gain access to them.

The pen tester has completed the aims of their pen test, which was to see if server 1 and server 2 were vulnerable to an attack which they are.

The pen tester was able to access server 1 and server 2 with both password cracking and using an exploit in metaspoilt on a kali linux machine.

The pen tester has proven that both machines are vulnerable to attack as well as the whole company network due to there not being a strong password policy in place as well as out of date software being used.

In the Scanning and Vulnerability Stage one of the bigger vulnerabilities that was found was the fact that both machines had an operating system and software that was missing security updates which means it is vulnerable to being attacked. In the nmap scans it gave a build number for the operating system and mail server which in a google search has found several vulnerabilities to these versions.

A google search has found that the Windows Server 2019 Standard build number 17763(Windows Server 2019 Standard 6.3) has several known vulnerabilities than can be used to get into this machine and one of them being SMB (Microsoft Server Message Block 2.0). A remote code execution vulnerabilty exists on this Windows Sever 2019 Standard build number 17763 , which deals with how the Microsoft Server Message Block 2.0 (SMBv2) server handles certain requests which means that an attacker can gain access to the targets machine by exploiting this vulnerabilty.

There are also several ways to do Windows Privilege Escalations (dualfade, 2022) on this version due to a vulnerability in this build of the operating system. When researching the operating system , the pen tester also found this website which gives details and also shows how to use the privilege vulernablity in this software. It shows what do in metaspoilt to get into a machine running this build of software. (NCC Group, 2019)

The mail server that is being used is also using out of date software, that when searched about has an Authentication Bypass which makes it extremely vulnerable to an attack.

By doing a google search on the Argo soft mail server, which has serval known vulnerabilities but 1.8 .x has an authentication bypass, (ArGoSoft 1.8.- Authenication Bypass , 2003)which basically fails to carry out the suffiencient authentication before granting access to the user management interface.

In the Enumeration and Password Cracking Stage this was where a user account with admin privileges was found to have a weak password that was able to be cracked by using enum4linux in metaspoilt. This user account was used to gain access to the target machine. The user account did have aspects of a good password but lacked the use of upper-case letters, special characters and numbers which made it easier to crack using a password cracker.

In the System Hacking Stage, the pen tester knows from the research that has been carried out that these target machines are vulnerable to SMBv2 exploits.

The pen tester in the kali machine was then able to use the SMBv2 exploit that was found to gain access to the target machines.

The pen tester had gained access to the target machines with a meterpreter session, which allowed things like running a keylogger on the target machine. Gaining more in-depth information about the target machines like applications on the machines with their current build numbers which could give an attacker a way to get back into the machines if the current exploit was patched. The attacker can also use a command called clearev to clear their tracks which could make it hard to see what was done after the fact.

As both these machines are vulnerable to an attack through metaspoilt, in meterpreter there is a script that can be run called persistence which when used will create an auto reconnecting persistent back door on these machines which will allow the attacker to gain access every time this machine is turned on (How to Make the Metasploit Meterpreter Persistent, n.d.).

If these machines had been updated to have the latest operating system with security patches installed this would not have been possible as these vulnerabilities have since been patched in newer versions of the Microsoft Server 2019 Standard version.

## Countermeasures

With the vulnerabilities that have been found in both server 1 and server 2 there are some countermeasures that need to be put into place to mitigate any breaches that could happen in the future it will not stop them completely, but it will help lessen the risk to you and your customers/clients.

* Have a clear and robust password policy, make sure to have a minimum length to the password as well as special characters, upper- and lower-case letters and numbers in the passwords (Password Policy Best Practices for Strong Security in AD, n.d.).
* Implement a robust update policy for operating systems and software to ensure the timely installation of security patches (Delvalle, n.d.).
* Keep up to date with things like OWASP (Open Web Application Security Project) who provide tools resources and best practices to help organisations develop and maintain secure web applications and WASC (Web Application Security Consortium) are a non-profit organisation that focuses on improving security of web applications. They also provide information, tools resources to help organisations enhance security of their web applications.
* Make sure to keep an eye out for any new threats or vulnerabilities on websites like CVE, exploit database.
* Close all unnecessary ports, if the port does not need to be open then close it to stop any potential breaches happening.
* Have current and up-to-date anti-virus software running and have a firewall configured with allow and deny rules in place.
* Conduct Penetration tests every 6 to 12 months either done via a third party or in-house.
* Staff training in Cyber Security, make sure to have refresher training every 6 months.

These are just some of the countermeasures that can be put in place, there are a lot of other measures that can be implemented. There are a lot of good articles online about measures to put in place one that is good is (12 tips for mitigating cyberattacks, 2022)

Once these steps are in place and have been taken the company/organization will be more secure than it previously was.

## Future Work

If there was more time available, the pen tester would have spent more time researching more about the vulnerabilities that were present, not just the most critical ones. To see if the less severe vulnerabilities would allow them a way in.

As well as looking at doing a black box pen test which would include them acting like hackers which would include them doing things like Footprinting and Reconnaissance. Seeing what weakness these might reveal if the company/organization is vulnerable to social engineering and other things.

Another thing, the pen tester would have spent more time looking at the other exploits that could be used to get into the machines via a Kali Linux machine.

Also if there was more time available, the pen tester would have tested more than just the 2 machines they would have maybe looked at the Networks or the Cloud environment that is being used.

# References

*12 tips for mitigating cyberattacks*. (2022, September 29). Retrieved from J.P Morgan: https://www.jpmorgan.com/insights/cybersecurity/ransomware/12-tips-for-mitigating-cyber-risk

*ArGoSoft 1.8.- Authenication Bypass* . (2003, 05 15). Retrieved from Exploit Database: https://www.exploit-db.com/exploits/22604

Delvalle, E. (n.d.). *Behind the Hack: The Importance of Software Updates & Patches*. Retrieved from 46 Solutions: https://www.46solutions.com/blog/behind-the-hack-the-importance-of-software-updates-patches/

dualfade. (2022). *Microsoft Windows Server 2019 Standard ( 10.0.17763 N/A Build 17763 ) - WD / BL Evasion - Priv Esc Lateral Move*. Retrieved from Github Gist: https://gist.github.com/dualfade/48c45fb47ff273a3996c9a4f10ac9d72

*How to Make the Metasploit Meterpreter Persistent*. (n.d.). Retrieved from Hackers Arise: https://www.hackers-arise.com/how-to-make-the-meterpreter-persistent

*Mastering Metasploit*. (n.d.). Retrieved from oreilly: https://www.oreilly.com/library/view/mastering-metasploit/9781788990615/a8fcda41-1bfc-4054-a8a9-7f128b1da37b.xhtml

NCC Group, h. b.-r. (2019, 11 12). *Microsoft UPnP Local Privilege Elevation Vulnerability - Metasploit*. Retrieved from Infosecmatters.com: https://www.infosecmatter.com/metasploit-module-library/?mm=exploit/windows/local/comahawk

*Password Policy Best Practices for Strong Security in AD*. (n.d.). Retrieved from netwrix: https://www.netwrix.com/password\_best\_practice.html

*Penetration Testing*. (2017, 08 08). Retrieved from NCSC: https://www.ncsc.gov.uk/guidance/penetration-testing

*Synopsys*. (n.d.). Retrieved from Penetration Testing - Penetration Testing Buyer's Guide: https://www.synopsys.com/glossary/what-is-penetration-testing.html

# Appendices

## Appendix A

Nmap scan from 192.168.10.1

A computer screen shot of a computer program

Description automatically generated

A screenshot of a computer screen

Description automatically generated

## A computer screen shot of a program Description automatically generated

Nmap Scan from 192.168.10.2

A screen shot of a computer

Description automatically generated

## A screen shot of a computer program Description automatically generated

## A computer screen with white text Description automatically generated

## Appendix B

A screenshot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

## A screen shot of a computer Description automatically generated

## A computer screen shot of white text Description automatically generated

## Appendix C

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

## Appendix D

A computer screen shot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated

A screenshot of a computer program

Description automatically generated