**Abstract**

This is an individual coursework for module ‘Digital Investigation and E-Discovery’. This report consists of well documented demonstration of Metasploit and its application in pen test and anti-forensics along with its investigation.

All the activities done in this coursework is for educational purposes. Some activities carried out might be illegal but they are done for small demonstration. No such activity is encouraged through this coursework.

Table of Contents

[1. Introduction 5](#_Toc123890315)

[1.1. Subject Matter 5](#_Toc123890316)

[1.2. Aims and Objectives 7](#_Toc123890317)

[**1.2.1.** **Aims** 7](#_Toc123890318)

[**1.2.2.** **Objective** 7](#_Toc123890319)

[1.3. Report structure 7](#_Toc123890320)

[**1.3.1.** **Background** 7](#_Toc123890321)

[**1.3.2.** **Recommendation** 7](#_Toc123890322)

[**1.3.3.** **Conclusion** 7](#_Toc123890323)

[2. Background 7](#_Toc123890324)

[2.1. Brief History 7](#_Toc123890325)

[**2.1.1.** **Metasploit Filesystem** 8](#_Toc123890326)

[**2.1.2.** **Metasploit Libraries** 9](#_Toc123890327)

[2.2. Literature Review 9](#_Toc123890328)

[**2.2.1.** **Case Study** 9](#_Toc123890329)

[**2.2.2.** **Analysis** 10](#_Toc123890330)

[**2.2.3.** **Description of vulnerability** 10](#_Toc123890331)

[2.3. Attack Techniques 11](#_Toc123890332)

[**2.3.1.** **Exploitation** 11](#_Toc123890333)

[**2.3.2.** **Post Exploitation** 12](#_Toc123890334)

[2.4. Anti-forensics 12](#_Toc123890335)

[**2.4.1.** **Using VIRUSTOTAL to scan malicious file** 12](#_Toc123890336)

[**2.4.2.** **Event Viewer** 14](#_Toc123890337)

[3. Recommendation 15](#_Toc123890338)

[4. Conclusion 15](#_Toc123890339)

[Works Cited 16](#_Toc123890340)

[5. Appendix 16](#_Toc123890341)

[5.1. Appendix 1: Exploitation 16](#_Toc123890342)

[5.2. Appendix 2: Post Exploitation 20](#_Toc123890343)

**List of Figures**

[Figure 1: Metasploit Architecture 8](#_Toc123897278)

[Figure 2: Opening Metasploit frame work 11](#_Toc123897279)

[Figure 3: Victims command prompt 11](#_Toc123897280)

[Figure 4: Screenshot result of scan 12](#_Toc123897281)

[Figure 5: Screenshot of web research 13](#_Toc123897282)

[Figure 6: Screenshot event viewer 14](#_Toc123897283)

[Figure 7: searching Modules 16](#_Toc123897284)

[Figure 8: Selecting desired module 16](#_Toc123897285)

[Figure 9: Viewing options 17](#_Toc123897286)

[Figure 10: Creating payloads 17](#_Toc123897287)

[Figure 11: Accessing payload 18](#_Toc123897288)

[Figure 12: Setting payload 18](#_Toc123897289)

[Figure 13: Exploiting payload 19](#_Toc123897290)

[Figure 14: Creating a .txt file and a folder named HeyYou 19](#_Toc123897291)

[Figure 15: Victim opening the folder made by attacker 20](#_Toc123897292)

# **Introduction**

## **Subject Matter**

A penetration test is also known as pen test, simulates a cyberattack on our computer system in order to look for exploitable flaws. Penetration testing is frequently utilized in conjunction with a web application firewall to improve Web Application Firewall (WAF). In order to test the security of the company, a penetration test is made up of a variety of techniques or instructions. Because it helps identify weaknesses and determines if an attacker or hacker will be able to take advantage of them and be successful in getting unauthorized access, this test has greatly shown to be beneficial for many organizations. (pp\_pankaj, 2022)

Metasploit is a framework that can be used by cybercriminals as well as ethical hackers to probe systematic vulnerabilities on the network and servers. It is the most powerful tool that can be easily customized and used with most operating systems. This framework makes hacking simple for both attackers and defenders. It is a versatile, incredibly resilient, modern penetration testing platform built on Ruby that allows you to design, test, and run attack code. It offers a ton of tools to carry out both straightforward and intricate tasks. (tiwari, 2022)

Some of the modules that are available in Metasploit framework are listed below:

* **Exploits:** The framework’s primary objective is to provide exploits for vulnerabilities. We use an exploit on the target system to benefit from the vulnerabilities existing in the target system. An exploit is a piece of code that takes advantage of a software weakness or security fault. Metasploit has more than 1,800 exploits that can be classified into 17 categories. (tiwari, 2022)
* **Payloads:** As we already know an exploit is a piece of code that can be utilized against the component that is vulnerable. The payload defines what we want to do when the attack is successful, even if the exploit code runs successfully. A payload can be defined as the action that must be carried out after the complete execution of an exploit. (tiwari, 2022)
* **Auxiliary function:** The modules that make Metasploit so simple to use are the auxiliary functions. A Metasploit auxiliary is a piece of code created to carry out a certain task. It can be used to determine whether we have anonymous access to an FTP server or to check if the web server is vulnerable to a heart bleed attack. Metasploit contains more than 1000 auxiliary modules that carry out variety of functions including scanning, fuzzing, sniffing and many other things. There are 19 different classifications for these auxiliary modules. (tiwari, 2022)
* **Encoders:** Metasploit helps us to create a broad range of payloads that we can deliver to the target in various ways to carry out any operation. It’s highly conceivable that any antivirus or any other security software installed on the target device will find our payload. Encoders are useful in this situation. Encoders conceal the payload using a variety of algorithms and methods so that any antivirus couldn’t detect it. (tiwari, 2022)
* **Post-Exploitation Code:** Once we obtain basic access to our target system using one of the various exploits, we can utilize the post modules to further compromise the system. Here we are talking about advanced access. Most of these operations are carried out in Cyber Events with full access, and must be carried out ethically. (tiwari, 2022)
* **Evasion:** With the use of this module, users can create a windows EXE that gets by Windows Defender. To do this, a variety of strategies are utilized, including anti-emulation, shellcode encryption, source code obfuscation and Metsam. In order to avoid the payload network traffic being better detected by antivirus, users should always aim to employ payloads that utilise more secure channels, such as HTTPS or RC4. (tiwari, 2022)
* **Nops:** This module acts as an instruction that keep the payload from crashing. (tiwari, 2022)

## **Aims and Objectives**

### **Aims**

The purpose of this coursework is to demonstrate how to use Metasploit framework by performing an attack and using several forensic methods to detect that particular attack.

### **Objective**

* To have a clear knowledge about the Metasploit framework.
* To show the impact of Metasploit framework in penetration testing.
* To show an attack using Metasploit.
* To run different exploits using payload.

## **Report structure**

### **Background**

In this part of the report a brief history about Metasploit, case study, attack techniques with detection and investigation are explained. The attack is explained in this part.

### **Recommendation**

In this part the precautions and safety methods for the victim is recommended and how can we mitigate such attack is explained.

### **Conclusion**

In this part the report is summarized and the learning about this coursework is explained.

# **Background**

## **Brief History**

The Metasploit was first introduced by H.D. Moore with the help from core developer Matt Miller in 2003 which is to be used as a portable pearl-based network tool. By 2007, it had been entirely converted to Ruby, and Rapid7 purchased the license in 2009, adding it to its toolkit of targeted remote exploit, fuzzing, anti-forensic, and evasion techniques. Rapid7 is a Boston-based start-up. (Buckbee, 2020)

Open-source project Metasploit provides resources to create scripts and investigate security flaws. It enables network managers to identify security concerns on their network and to describe which vulnerability needs to be defined first. (Javapoint, 2020) The architecture of Metasploit is described below with their particular filesystem and libraries that are being used in the Metasploit.

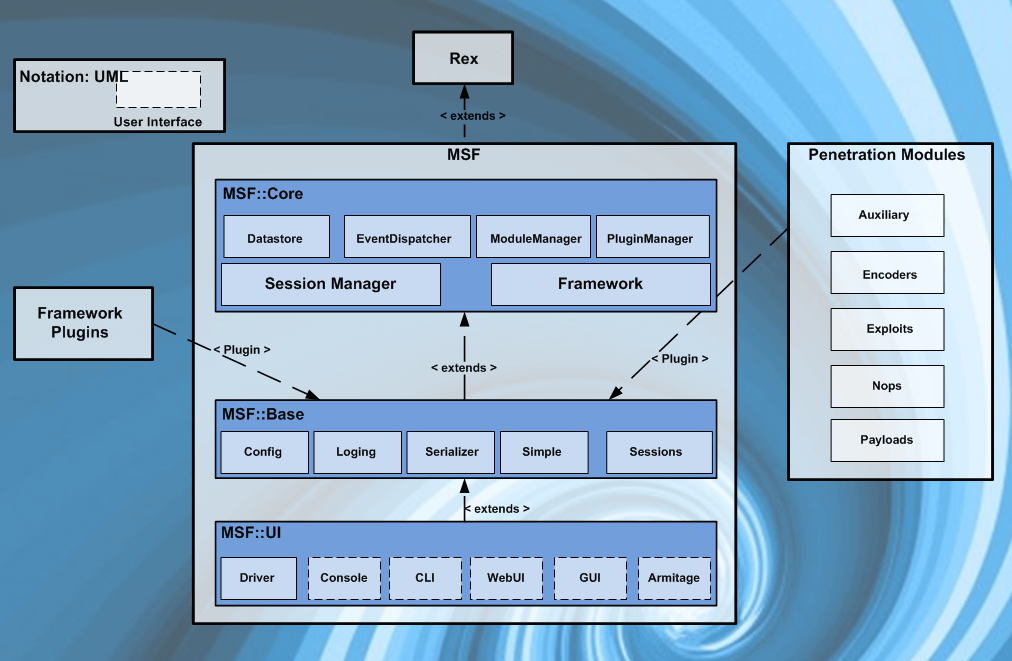


Figure 1: Metasploit Architecture

### **Metasploit Filesystem**

The MSF filesystem is structured by directory and has an intuitive organized directory. The Metasploit-framework package comes with Kali Linux and installs Metasploit in the /usr/share/Metasploit-framework directory. (Heynik, 2020) Some of the important directories are briefly described below.

* **Data:** The data directory contains editable files that Metasploit uses to store word lists, pictures, word exploit binaries and more.
* **Documentation:** The documentation directory contains the framework’s available documentation.
* **LIB:** The LIB directory contains the ***‘meat’*** of the framework codebase.
* **Modules:** The actual MSF modules for exploits, auxiliary and post modules, payloads, encoders, and NOP generators are located in the modules directory.
* **Plugins:** Metasploit contains many plugins that we will find in the Metasploit-framework directory.
* **Scripts:** The scripts directory contains Meterpreter and other scripts.
* **Tools:** This directory contains various useful command-line utilities.

### **Metasploit Libraries**

Many MSF libraries enable us to launch our exploits without having to create extra code for elementary tasks like HTTP queries or payload encoding. (Heynik, 2020) The following list contains some of the most important libraries.

* **REX:** Almost all core task, including configuring formatting, connections, sockets, and other tasks, are handled by REX.
* **MSF Base:** MSF base provide users the capability for accessing Metasploit in so many different ways (web and CLI for instance).
* **MSF core:** MSF core offers the common API and the original core that defines the framework.

## **Literature Review**

### **Case Study**

According to a CERT-Bund press release, a remote, anonymous attacker might use a vulnerability to run arbitrary code, cause a denial of service, reveal information, or change files.

According to German security agency CERT-bund, the popular open-source VLC media player has a Remote Code Execution (RCE) vulnerability that allows hacker to install, modify or run any software on a victim’s device without their consent and could also be used to reveal files on the host system. (Lobo, 2019)

### **Analysis**

In the above case study, it is found that though the VLC media player hacker can use vulnerability to access in the target’s device.

After analysing the case study, a reverse shell payload is created and embedded in .mkv files and sent to victim’s device. VLC player file fails when the malicious .mkv file is opened by the victim, and the payload runs in the background to get the remote access to the victim’s command prompt. An attach shell is a payload that ‘binds’ a command prompt to a listening port on the target system, to which the attacker will then communicate, as opposed to a reverse shell, which establishes a connection as a windows command prompt from the target machine back to the attacker.

### **Description of vulnerability**

**CVE-ID:** CVE-2018-11529

**Vulnerable software version:** VLC Media Player 2.0.0 – 2.2.8

A Use-After-Free vulnerability in VideoLAN VLC Media Player 2.2.x allows an attacker to use specially crafted MKV files to execute arbitrary code. Failures in exploit efforts will probably result in VLC crashing.

Insecure older version of VLC can be used by hackers to crash the device and remotely run malicious code. The modus operandi is extremely prevalent. If we play a video on VLC after unknowingly downloading an AVI or MKV attack file, it will give the hackers total control of our device. These assault files may have a source other than Facebook, Twitter, or Instagram, such as video torrents. (opswat, 2019)

## **Attack Techniques**

In this report, a reverse shell payload is created and embedded in .mkv files and sent to victim’s device. VLC player file fails when malicious .mkv file is opened by the victim, and the payload runs in the background to get the remote access to the victim’s command prompt. An attach shell is a payload that ‘binds’ a command prompt to a listening port on the target system, to which the attacker will then communicate, as opposed to a reverse shell, which establishes a connection as a windows command prompt from the target machine back to the attacker.

### **Exploitation**

For the attack, VLC vulnerability CVE-2018-11529 is used to exploit the victim’s machine using Metasploit framework.

**Step1:** Metasploit framework is opened using command ***“msfconsole”*** in command terminal.

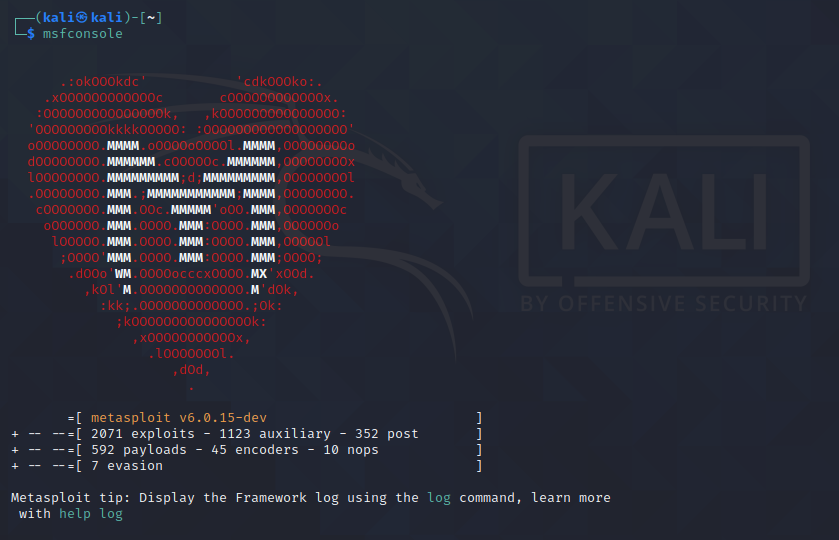


Figure 2: Opening Metasploit frame work

[**Appendix1**](#_Appendix_1:_Exploitation)

### **Post Exploitation**

After the successful exploitation, below we can see that the attacker has got access to the victims command prompt.

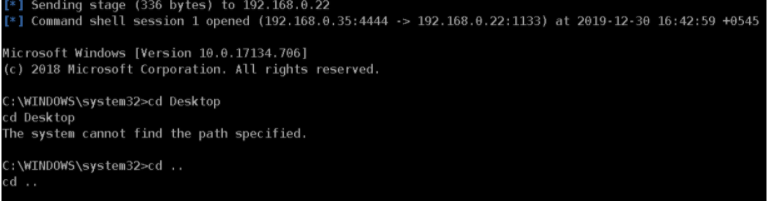


Figure 3: Victims command prompt

[**Appendix2**](#_Appendix_2:_Post)

## **Anti-forensics**

Cybercrime investigations and the search for concrete proof of computer assisted crime both benefit from the use of digital forensics. When it was still known as computer forensics, the idea of digital forensics first emerged in the late 1990s and early 200s. Digital forensics is typically related to cybercrime detection and prevention. Given both of them center on digital issues, it is connected to digital security. Digital forensics focuses on reactive measures, whereas digital security emphasizes preventive ones. Forensic analysis identifies the pieces of the puzzle needed to solve computer crimes. Utilizing efficient tool is necessary. There are currently variety of software tools accessible for forensic investigators with training. Using a variety of methods, analysts perform research in accordance with the fundamentals of forensic science.

### **Using VIRUSTOTAL to scan malicious file**

The suspicious files (phwhk-part1.mkv and phwk-part2.mkv) are compressed in order to be uploaded to and scanned by VIRUSTOTAL, an online service that analyses files and URLs to enable the detection of viruses, worms, trojan horses, and other types of malicious content using antivirus engines and website scanners.

The below screenshot is the result of scan:

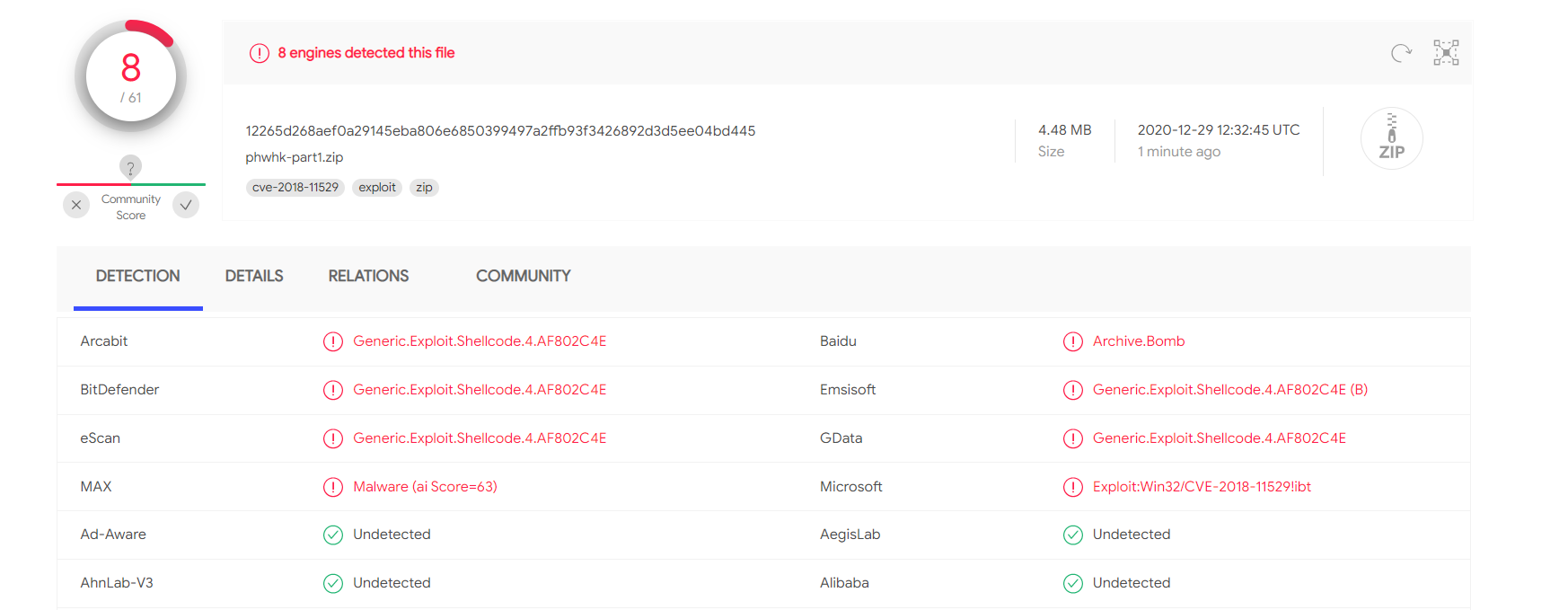


Figure 4: Screenshot result of scan

It is clear from the scan that the file contains shellcode, a payload that starts in a command shell and allows the attacker complete access over the infected system.

**Screenshot of the web search:**

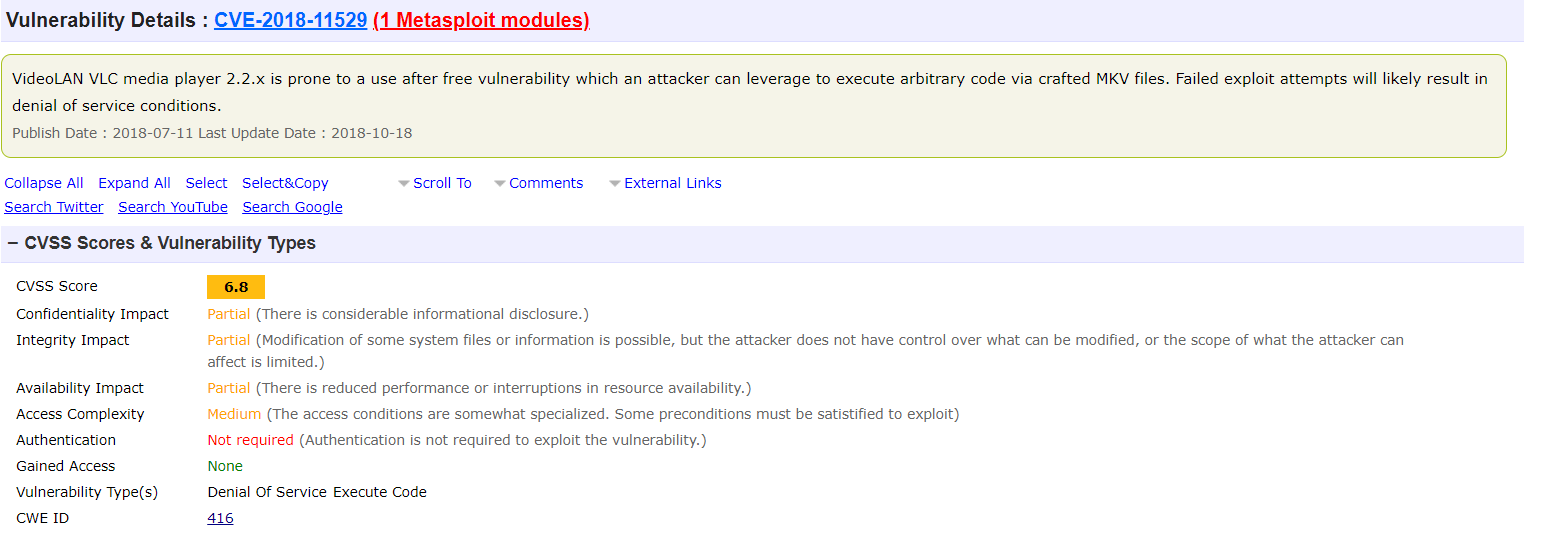


Figure 5: Screenshot of web research

### **Event Viewer**

From the above step, It is clear that the vulnerability’s main goal is to remotely access victim’s computer and failing exploit efforts will lead to a denial of service scenario. Event viewer is employed to record the attack’s trail.

The built-in Windows utility known as Event Viewer provides detailed information about major events that have occurred on our computer, such as a log of system and application messages, including error, information messages, and warnings.

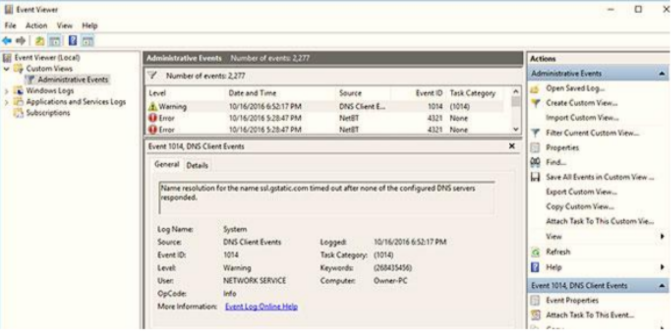


Figure 6: Screenshot event viewer

Events: How the event happened

Error: Major problem, perhaps including data loss

Warning: Not necessarily significant, but could indicate a brewing of problem

# **Recommendation**

In this report, the attacker was able to get full access of the victim’s machine through which the attacker can perform any task in the victim’s computer. The attacker was able to access all the crucial part of the victim’s computer in which he can get access to any file that he wanted to access and can get every information regarding his all-personal details and passwords saved in the device. When the victim opened the VLC player file the file created an error and injected the exploit in the victim’s machine and gave access to the attacker to access the command prompt and each an every system information through which the attacker can get access to all the valuable information of the victim’s machine.

If the victim had kept his system updated, Windows Defender and Firewall would have notified the user about the malware in .mkv file. When the victim noticed the file downloading from a link and looked at the file’s format, he should have been aware. The finest advice may be to be alert while browsing the web. There may be different procedures to follow in order to be safe. The user must be aware that one click could result in the download of a file and possible system compromise. Everyone works for a living; thus, user should be aware of this type of phasing attack. The user should investigate caution and find out what kind of the file they have downloaded.

# **Conclusion**

Metasploit is a framework that can be used by cybercriminals as well as ethical hackers to probe systematic vulnerabilities on the network and servers. It is the most powerful tool that can be easily customized and used with most operating systems. This framework makes hacking simple for both attackers and defenders. (tiwari, 2022)

This report clarified the purpose and use of the Metasploit tools that is utilized for pretesting. In this report, what can be done if the attacker is able to insert payload is made clearer. People should be aware of problems and prepare for future attacks if they want to stay secure from this kind of behaviour. This report makes it clear that we shouldn’t click anywhere that we can see. A small file can result in a significant loss if it is phishing. To protect ourselves from attacks, we can develop prevention strategies.

# Works Cited

pp\_pankaj. (2022, November 23). *Geeksforgeeks*. Retrieved from geeksforgeeks: https://www.geeksforgeeks.org/software-testing-penetration-testing/

tiwari, l. m. (2022, November 29). *geeksforgeeks*. Retrieved from geeksforgeeks: https://www.geeksforgeeks.org/what-is-metasploit/

Buckbee, M. (2020, March 29). *Varonis*. Retrieved from Varonis: https://www.varonis.com/blog/what-is-metasploit

Lobo, S. (2019, July 25). *Packt hub*. Retrieved from Packt hub: https://hub.packtpub.com/vlc-media-player-affected-by-a-major-vulnerability-in-a-3rd-library-libebml-updating-to-the-latest-version-may-help/

opswat. (2019, November 14). *opswat*. Retrieved from opswat: https://www.opswat.com/blog/remote-code-execution-vulnerability-in-vlc-detection-remediation-with-opswat

Javapoint. (2020). *Javapoint*. Retrieved from javapoint: https://www.javatpoint.com/what-is-metasploit

Heynik. (2020, August 22). *Medium*. Retrieved from Medium: https://medium.com/cyberxerx/metasploit-framework-introduction-b25c0f9ded37

# **Appendix**

## **Appendix 1: Exploitation**

**Step2:** To discover the module of VLC ***“Search VLC”*** command is used. From the result we can see the list of VLC vulnerabilities with their disclosure date and ranked according to their effectiveness.

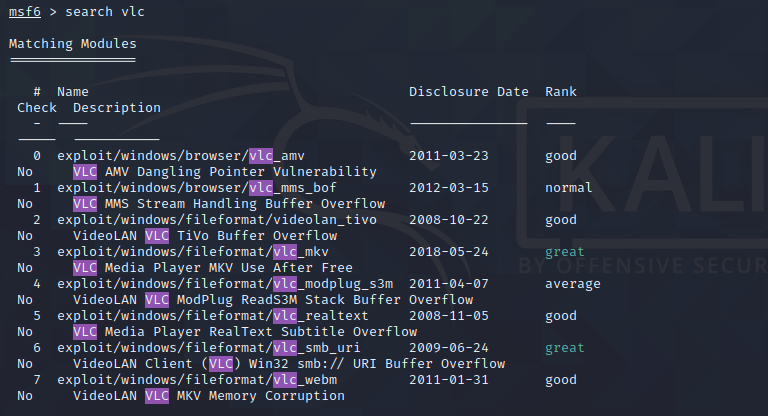


Figure 7: searching Modules

**Step3:** By creating a listening address with the IP address of the attack machine in the module (exploit/windows/fileformat/vlc\_mkv). vlc\_mkv module is selected and the attack is carried out.



Figure 8: Selecting desired module

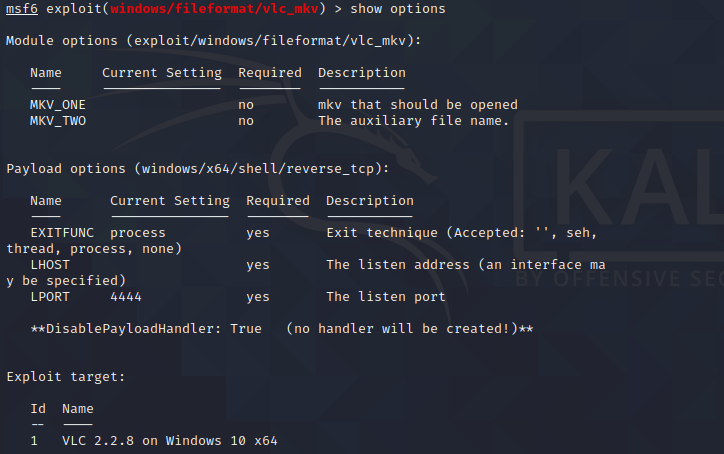


Figure 9: Viewing options

**Step4:** After the exploit was launched in the module (exploit/windows/fileformat/vlc\_mkv), where two payloads are created in the file location /home/kali/msf4/local/. The first .mkv file contains the main vulnerability and heap spray. The second .mkv file is required in order to take the vulnerable code path and should be places under the same directory as the first .mkv file.

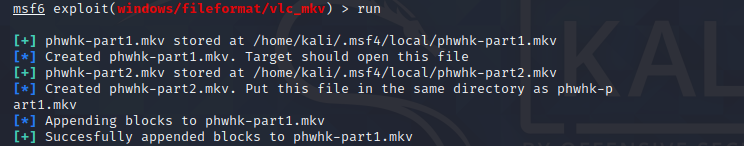


Figure 10: Creating payloads

**Step 5:** A payload is created of windows/x64/shell/reverse\_tcp and the module exploit/multi/handler was accessed.

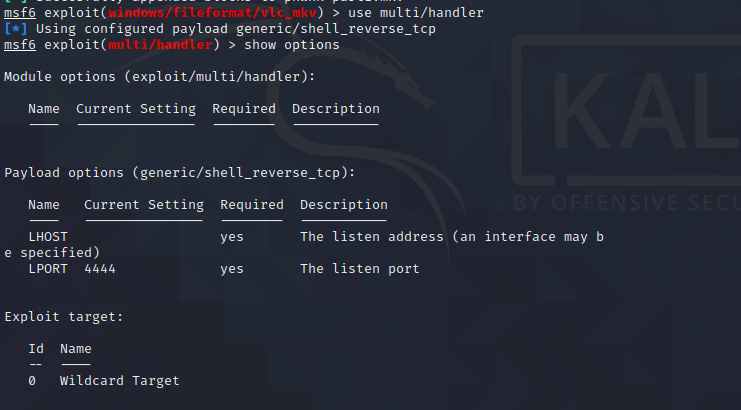


Figure 11: Accessing payload

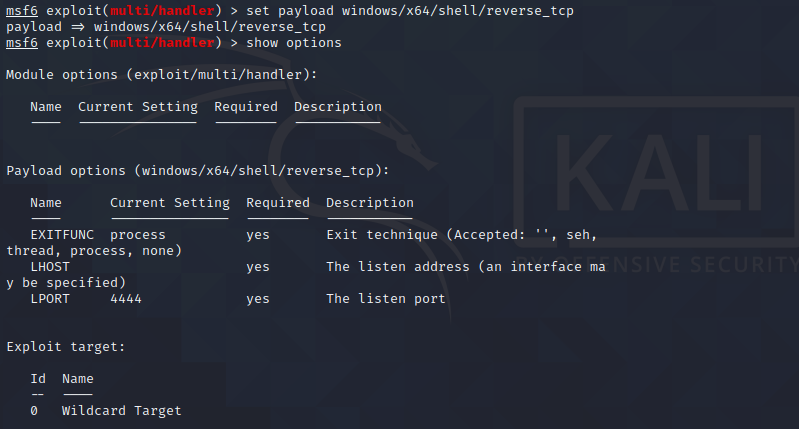


Figure 12: Setting payload

**Step 6:** The access to the victim’s machine is seen after the exploitation. Before, the module exploit/multi/handler, the listening address was created with the IP of the attacker’s machine and the payload was exploited.

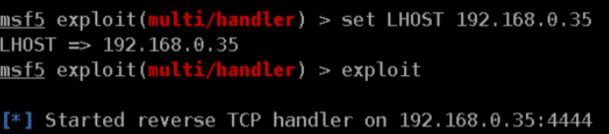


Figure 13: Exploiting payload

## **Appendix 2: Post Exploitation**

Below we can see that the attacker can create the folder and have got the full access to the victim’s machine.



Figure 14: Creating a .txt file and a folder named HeyYou

Below we can see that the attacker can create the folder named ***“Hey you”*** and have got the full access to the victim’s machine. And have created a .txt file saying the message ***“You have been hacked”.***



Figure 15: Victim opening the folder made by attacker