REVERSE BACKDOOR

Enrol. No. (s) - 20103123, 20103315, 20103305

Name of Student (s) - Vineet Mathur, Aryan Garg, Dhruv Gupta

December - 2022

Submitted In Partial Fulfilment of The Degree Of

Bachelor Of Technology

In

Computer Science Engineering

TABLE OF CONTENTS

DECLARATION

We ARYAN GARG, VINEET MATHUR, DHRUV GUPTA hereby declare that this project submission is our own work and that to the best of my knowledge and belief, it contains no material previously published or written by another person nor material which has been accepted for the award of any other degree or diploma of the university or other institute of higher learning, except where due acknowledgment has been made in the text.

STUDENT ID	STUDENT NAME	SIGNATURE
2010123	Vineet Mathur	
20103315	Aryan Garg	
20103305	Dhruv Gupta	

CERTIFICATE

This is to certify that the work titled “Reverse Backdoor” submitted by “Vineet Mathur, Aryan Garg, Dhruv Gupta” in partial fulfilment for the award of degree of B.Tech of Jaypee Institute of Information Technology, Noida has been carried out under my supervision. This work has not been submitted partially or wholly to any other University or Institute for the award of any other degree or diploma.

Name of Supervisor - Dr. Taj Alam
Designation - Assistant Professor (Senior Grade)
Date - 5th December 2022

ACKNOWLEDGEMENT

STUDENT ID	STUDENT NAME	SIGNATURE
2010123	Vineet Mathur	
20103315	Aryan Garg	
20103305	Dhruv Gupta	

Chapter 1 Introduction

1.1 General Introduction

A backdoor is a typically covert method of bypassing normal authentication or encryption in a computer, product, embedded device (e.g. a home router), or its embodiment (e.g. part of a cryptosystem, algorithm, chipset, or even a "homunculus computer" —a tiny computer-within-a-computer such as that found in Intel's AMT technology). Backdoors are most often used for securing remote access to a computer, or obtaining access to plaintext in cryptographic systems. From there it may be used to gain access to privileged information like passwords, corrupt or delete data on hard drives, or transfer information within autoschediastic networks. A backdoor may take the form of a hidden part of a program, a separate program (e.g. Back Orifice may subvert the system through a rootkit), code in the firmware of the hardware, or parts of an operating system such as Windows.Trojan horses can be used to create vulnerabilities in a device. A Trojan horse may appear to be an entirely legitimate program, but when executed, it triggers an activity that may install a backdoor. Although some are secretly installed, other backdoors are deliberate and widely known. These kinds of backdoors have "legitimate" uses such as providing the manufacturer with a way to restore user passwords. Many systems that store information within the cloud fail to create accurate security measures. If many systems are connected within the cloud, hackers can gain access to all other platforms through the most vulnerable system.

1.2 Problem Statement

In the past few years, a lot of research has been focused on backdoor attacks and defence mechanisms. Many types of the backdoor defences have been proposed, but there are still a lot of challenges unresolved. New attacks are proposed and created regularly, which makes defending even harder. Many defences can be bypassed by attackers as well. Also, no defence mechanism that protects deep learning models against all types of backdoor attacks has been proposed. One of the problems is that we do not know how much impact the used dataset has on a defence or how one defence would perform on different models. Because of that, in this work, we investigate how backdoor attacks work with different models, would that affect their performance and is there some defence that would always perform well.

Chapter 2

Literature Survey

2.1 Summary of Paper Studied

Backdoor attacks are not always malicious. For instance, the United States Government Organization FBI requested Apple to build a backdoor for the iPhone that belongs to an assailant.

But Apple refused to do so, showing it to be against the user data privacy agreement of Apple and its customers. Nonetheless, the FBI managed to build a backdoor with the help of a third party. In this case, accessing the data is important as it could help in gathering information about the assailant. Therefore, backdoor attacks play a crucial role in today's world. The experiment performed is on utilising an existing vulnerability to create a backdoor in the Windows operating system and is achieved by using Armitage open-source tool. Armitage tool uses the Metasploit framework in which a lot of exploits are outdated as industries are frequently updating their software against security threats. But the advantage that comes with the Metasploit framework is the development of new exploits. Therefore, the Metasploit framework is helpful to organisations that need to design their exploit against their tool to check the vulnerability. The attack is conducted to help organisations for achieving the legal purposes like the above example. Overall, such an implementation could be easily incorporated into a foundational cybersecurity course for enhanced student learning.

2.2 Integrated Summary of The Literature Study

In this paper, it presents an implementation of remotely hacking into the Windows system with reverse TCP payload using an open-source tool. Reverse TCP opens a backdoor on the victim system which is remotely operated by the attacker without the victim's notice. The firewall only scans the incoming traffic and doesn't examine the outgoing traffic which is the flaw that leads to the back door. The victim must initiate the connection in the reverse TCP payload. Armitage is an open-source tool that provides Graphical User Interface (GUI) to the Metasploit. The Metasploit framework is another open-source framework which aims to provide information about the vulnerabilities and aids in performing penetration testing. Metasploit contains an extensive database of exploits, payloads, and vulnerabilities that vary for different kinds of systems. In the implemented attack, the attacker can access the files, take a screenshot, monitor screen, sniff packets, and take shots using the webcam. We demonstrate these attacks which can be used in the offering of a foundational cybersecurity course.

Chapter 3

Requirement Analysis and Solution Approach

3.1 Overall Description of The Project

Remotely hacking into the Windows system with reverse TCP payload using an open-source tool. Reverse TCP opens a backdoor on the victim system which is remotely operated by the attacker without the victim's notice. The firewall only scans the incoming traffic and doesn't examine the outgoing traffic which is the flaw that leads to the back door.

- Access file system.
- Execute system commands.
- Download & upload files
- Running Executables Silently
- Persistence
- Running Programs on Start-up
- Creating a Trojan by Embedding Files in Program Code
- Bypassing Anti-Virus Programs
- Adding an Icon to Generated Executables
- Spoofing File Extension

3.2 Requirement Analysis

Virtual Machine

VMs are used in cyber security extensively for several reasons including access to tools across multiple platforms, and — if properly configured and isolated from the network — can also be used for malware analysis. Using a VM is also a great way to safely test new things without causing problems on the 'host'.

Why To Use Kali Linux

There is a wide array of reasons as to why one should use Kali Linux. Let me list down a few of them:

1. As Free as It Can Get – Kali Linux has been and will always be free to use.
2. More Tools Than You Could Think Of – Kali Linux comes with over 600 different penetration testing and security analytics related tool.

3. Open-Source – Kali, being a member of the Linux family, follows the widely appreciated open-source model. Their development tree is publicly viewable on Git and all of the code is available for your tweaking purposes.
4. Multi-Language Support – Although penetration tools tend to be written in English, it has been ensured that Kali includes true multilingual support, allowing more users to operate in their native language and locate the tools they need for the job.
5. Completely Customizable – The developers at offensive security understand that not everyone will agree with their design model, so they have made it as easy as possible for the more adventurous user to customise Kali Linux to their liking, all the way down to the kernel.

Socket Programming

A socket is a communications connection point (endpoint) that you can name and address in a network. Socket programming shows how to use socket APIs to establish communication links between remote and local processes.

The processes that use a socket can reside on the same system or different systems on different networks. Sockets are useful for both stand-alone and network applications. Sockets allow you to exchange information between processes on the same machine or across a network, distribute work to the most efficient machine, and they easily allow access to centralised data. Socket application program interfaces (APIs) are the network standard for TCP/IP. A wide range of operating systems support socket APIs. Sockets support multiple transport and networking protocols. Socket system functions and the socket network functions are thread safe.

Why Windows as Target Machine

Windows has always been a bigger target for hackers than Linux for a variety of reasons. First and foremost, Windows is by far the most popular operating system in the world, with a market share of over 90%. That means there are a lot more Windows users out there for hackers to target. Another reason Windows is a bigger target is that it is generally less secure than Linux. While there are plenty of security measures you can take to secure your Windows system, the fact is that Windows is just inherently less secure than Linux.

This is due to a number of factors, including the fact that Windows is a proprietary operating system with closed-source code, while Linux is open source.

3.3 Solution Approach

Backdoors are difficult to detect. Everyday users can’t discover a backdoor just by opening the Task Manager. But there are a few easy steps you can take to keep your device safe from backdoors virus attacks, such as:

Use an Antivirus

Always use advanced antivirus software that can detect and prevent a wide range of malware, including trojans, crypto hackers, spyware, and rootkits. An antivirus will detect backdoor viruses and eliminate them before they can infect your computer. Good antivirus software like Norton 360 also includes tools like Wi-Fi monitoring, an advanced firewall, web protection, and microphone and webcam privacy monitoring to ensure you’re as safe as possible online.

Download With Care

Backdoors are often bundled with seemingly legitimate free software, files, and applications. When downloading any file from the internet, check to see if you’re only getting the file you wanted, or if there are some nasty hitchhikers coming along for the ride. Even a file that behaves like the file you’re looking for could be a trojan. Make sure to always download from official websites, avoid pirate sites, and install an antivirus with real-time protection that can flag malware files before you even download them onto your system.

Use a Firewall

Firewalls are essential for anti-backdoor protection — they monitor all incoming and outgoing traffic on your device. If someone outside of your approved network is trying to get into your device, the firewall will block them out, and if an app on your device is trying to send data out to an unknown network location, the firewall will block that app, too. Advanced firewalls can detect unauthorised backdoor traffic even when your device’s malware detection has been fooled. Windows and macOS both have pretty decent built-in firewalls, but they’re not good enough. There are a few antivirus programs with good firewalls (McAfee has excellent network protections) and you can also consider purchasing a smart firewall, which is a physical device that you connect to your router to keep your network as safe as possible.

Use a Password Manager

Password managers generate and store login information for all your accounts and even help you log into them automatically. All of this information is securely encrypted using 256-bit AES encryption and locked behind a master password. Advanced password managers like Dash lane can even enhance your password vault's security using biometric login or 2FA tools like TOTP generators and USB tokens. Because they generate random, complex passwords, password managers make it a lot harder for hackers to get into your network or spread across your network in the event that you get a backdoor installed on your system.

Stay on Top of Security Updates/Patches

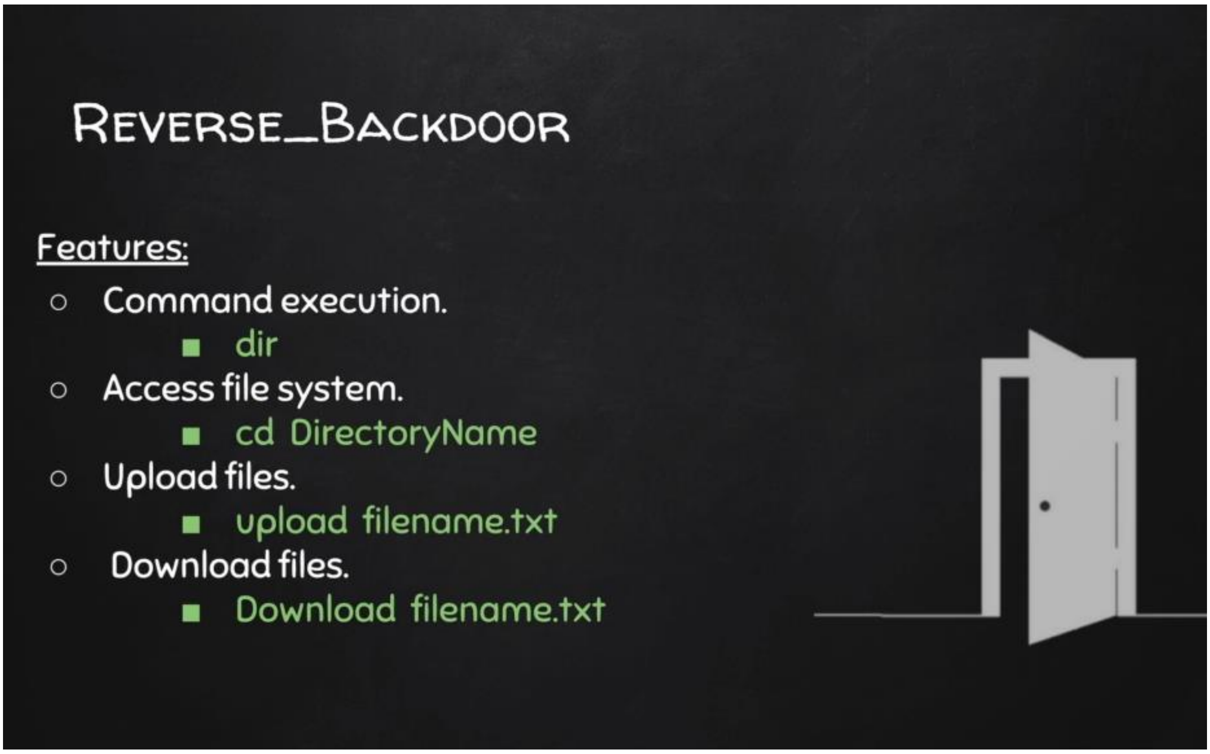
Zero-day attacks are pretty rare, and most hackers just recycle the same exploits and malware because it's cheap and easy for them to do so. Plus, it works. One in three IT professionals (34%) in Europe admitted that their company had been breached as a result of an unpatched vulnerability.

Software developers frequently publish new patches to fix the vulnerabilities in their software, and it's not hard to install those updates. Many programs even include an auto-update option. If you're a macOS or Windows user, navigate to your settings and turn "Automatic Updates" on — it's especially important to keep your OS updated because backdoors depend on fooling your operating system.

Chapter-4

Modelling And Implementation Details

First, We Implement Connection Form Target Machine to Hacker Machine



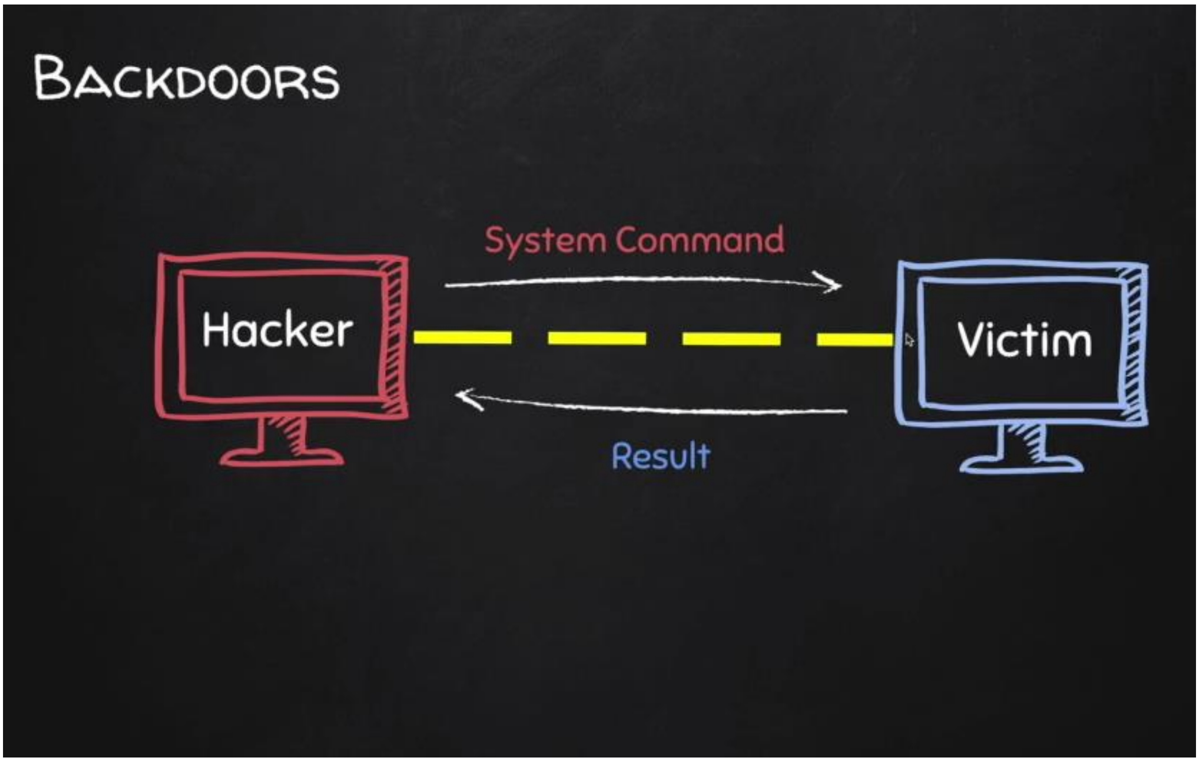
REVERSE_BACKDOOR

Features:

- ○ Command execution.
  - ■ dir
- ○ Access file system.
  - ■ cd DirectoryName
- ○ Upload files.
  - ■ upload filename.txt
- ○ Download files.
  - ■ Download filename.txt

Transfer Data Over Tcp Ipv4 Connection with Reliability.

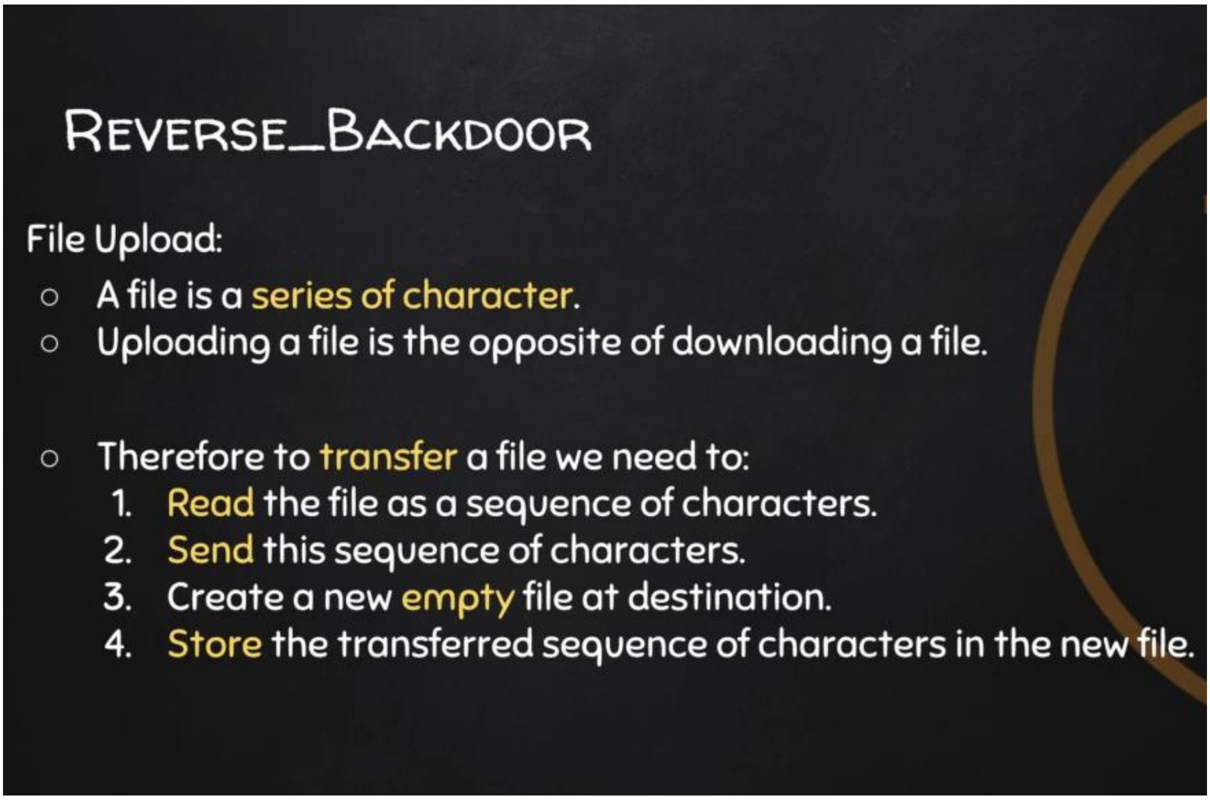
Access File System & Executing System Commands.



BACKDOORS

Upload Files and Download-

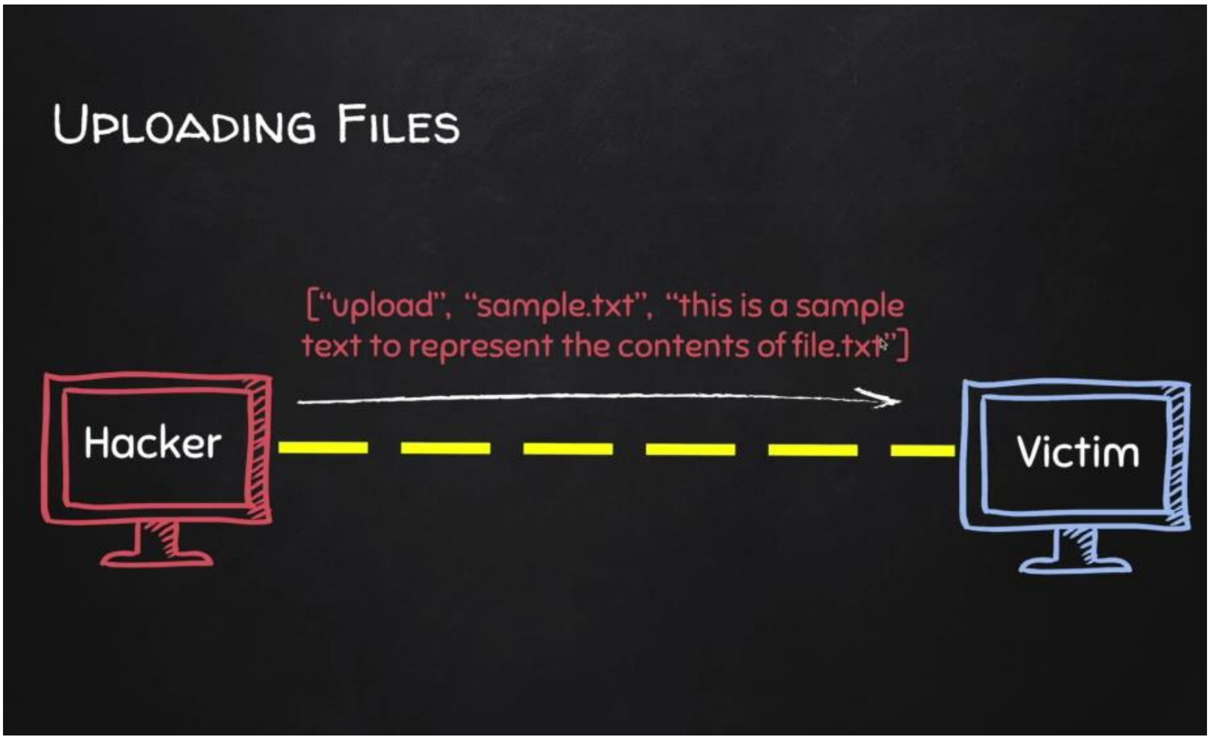
In almost every application there is functionality for uploading files. This file may be in the form of text, video, image, etc. However, many applications do not have proper security checks during uploading files and this results in a vulnerability called File Upload Vulnerability.



REVERSE_BACKDOOR

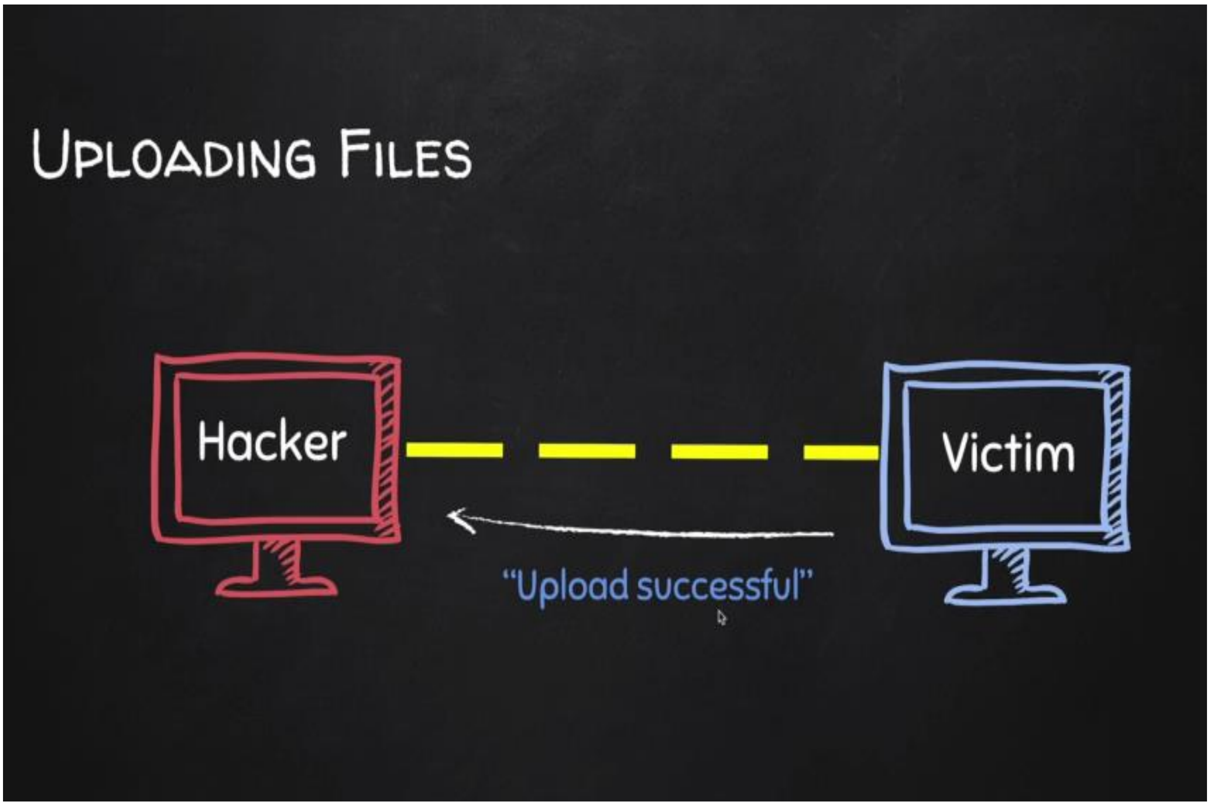
File Upload:

- A file is a series of character.
- Uploading a file is the opposite of downloading a file.
- Therefore to transfer a file we need to:
  1. Read the file as a sequence of characters.
  2. Send this sequence of characters.
  3. Create a new empty file at destination.
  4. Store the transferred sequence of characters in the new file.

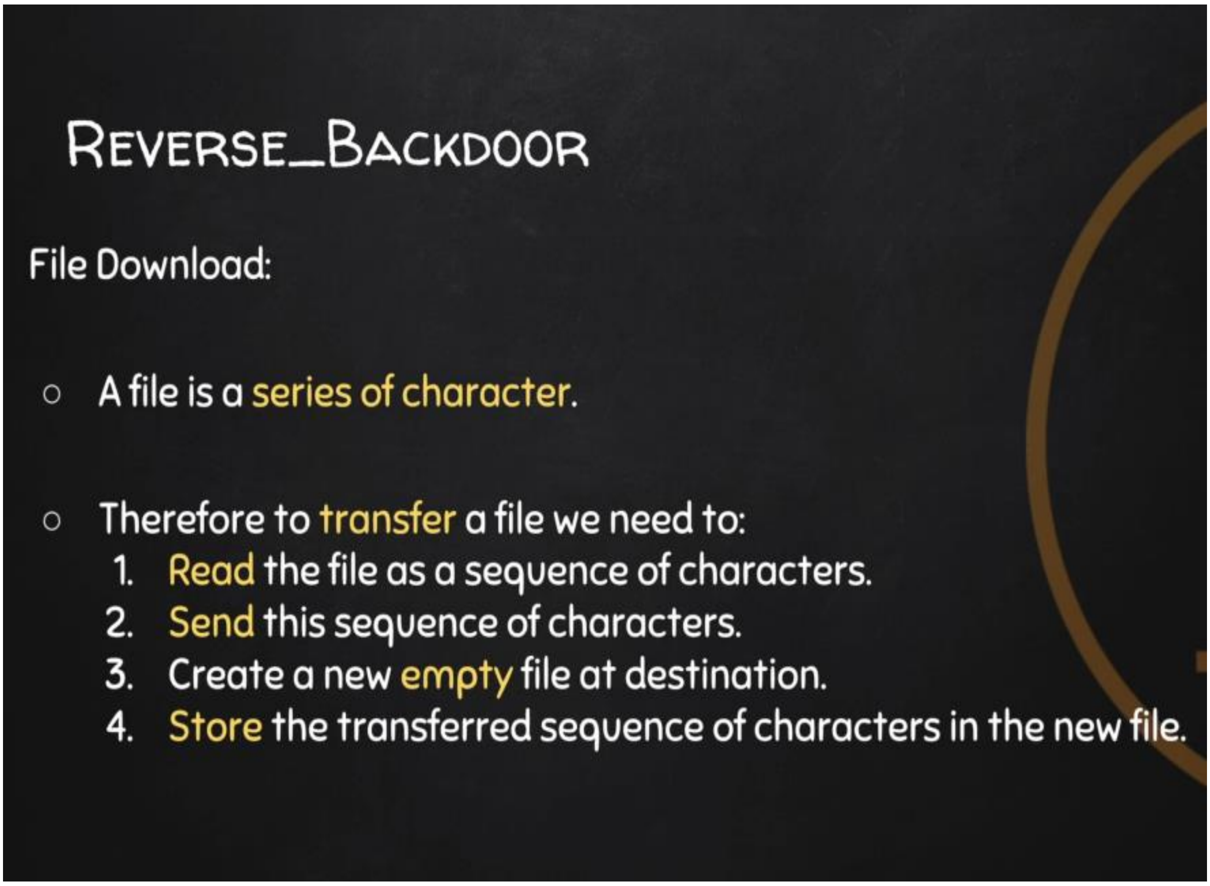


UPLOADING FILES

["upload", "sample.txt", "this is a sample text to represent the contents of file.txt"]



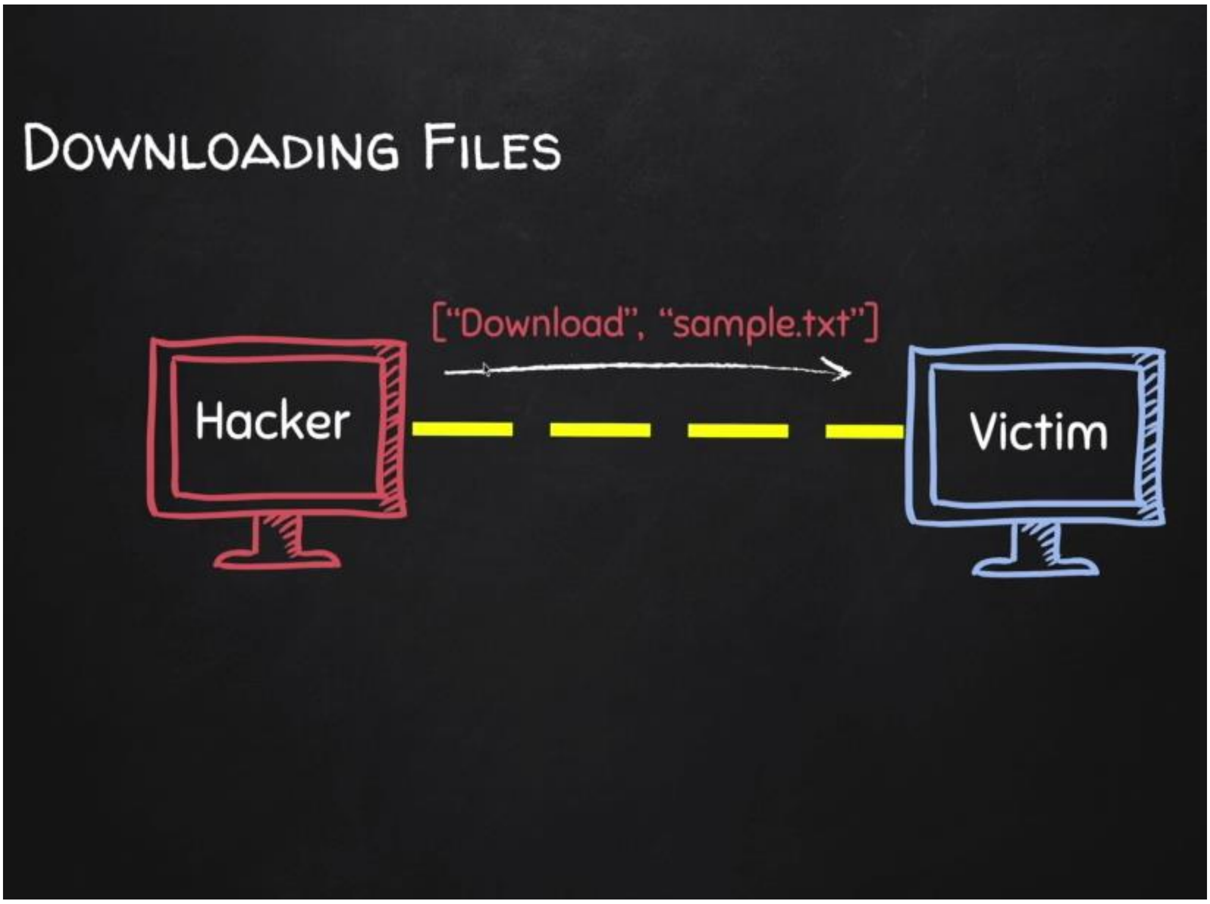
Uploading Files



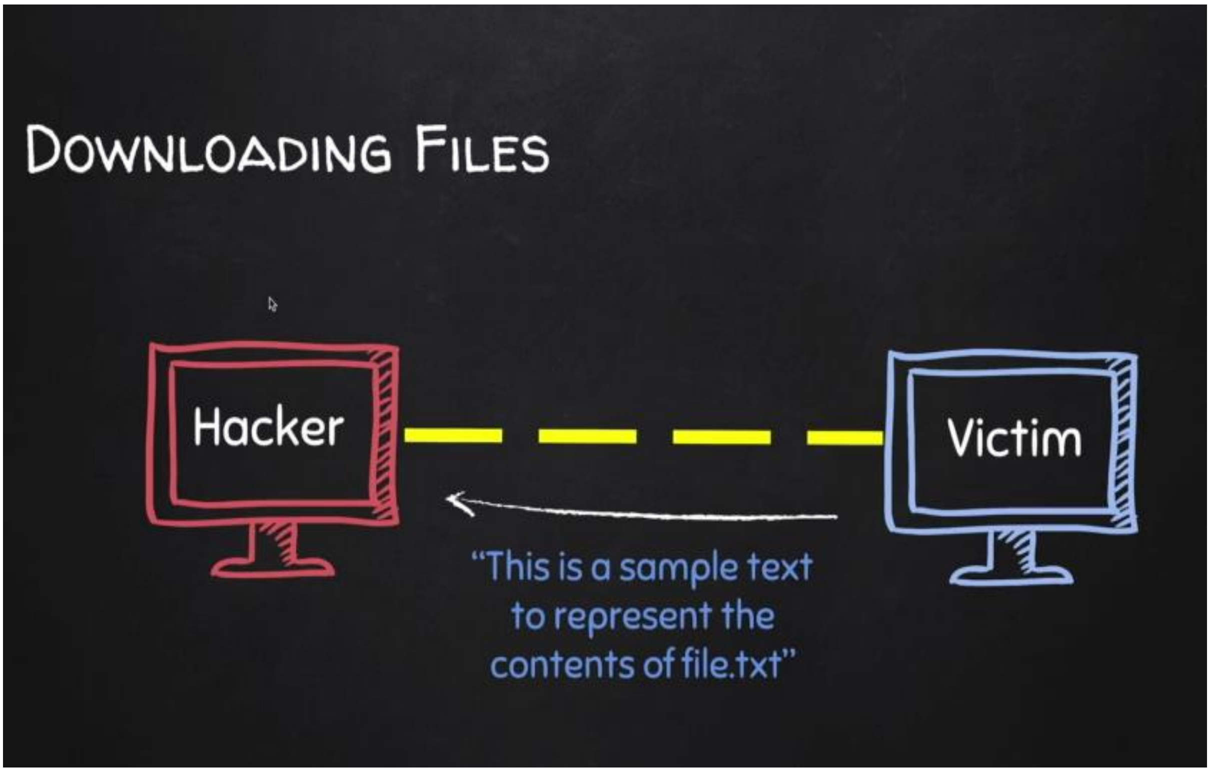
Reverse_Backdoor

File Download:

- A file is a series of character.
- Therefore to transfer a file we need to:
  1. Read the file as a sequence of characters.
  2. Send this sequence of characters.
  3. Create a new empty file at destination.
  4. Store the transferred sequence of characters in the new file.



Downloading Files



Downloading Files

Hacker
Victim
"This is a sample text to represent the contents of file.txt"

Why We Use Tcp

Transmission Control Protocol (TCP) is a type of communication protocol that interconnects different networking devices. It is the basic way of how applications are going to communicate across a network (Allowing communication over large distances). Some of the examples for them are TCP/IP, HTTP, HTTPS and FTP. Even if you have an unreliable network, the TCP has the capability to offer reliable and end-to-end byte stream.

Features Of Tcp

1. Data Re-Transmission

During every handshake, TCP segments are being transmitted from sender to receiver. Sometimes in between the transport, the segments may get lost failing to reach its destination. Due to this an acknowledgement will be sent to the sender from the receiver, so that the sender can re transmit the segment back again.

2. Congestion Control

In order for avoiding congestions, TCP uses a separate congestion control policy. Basically, congestion happens when the sender sends out too many data packets in a given time. For preventing these the receiver sends signals to the sender in order for slowing the process down or delaying the transmission. Right amount of data is being transmitted to keep the network saturated.

3. Unique Identification

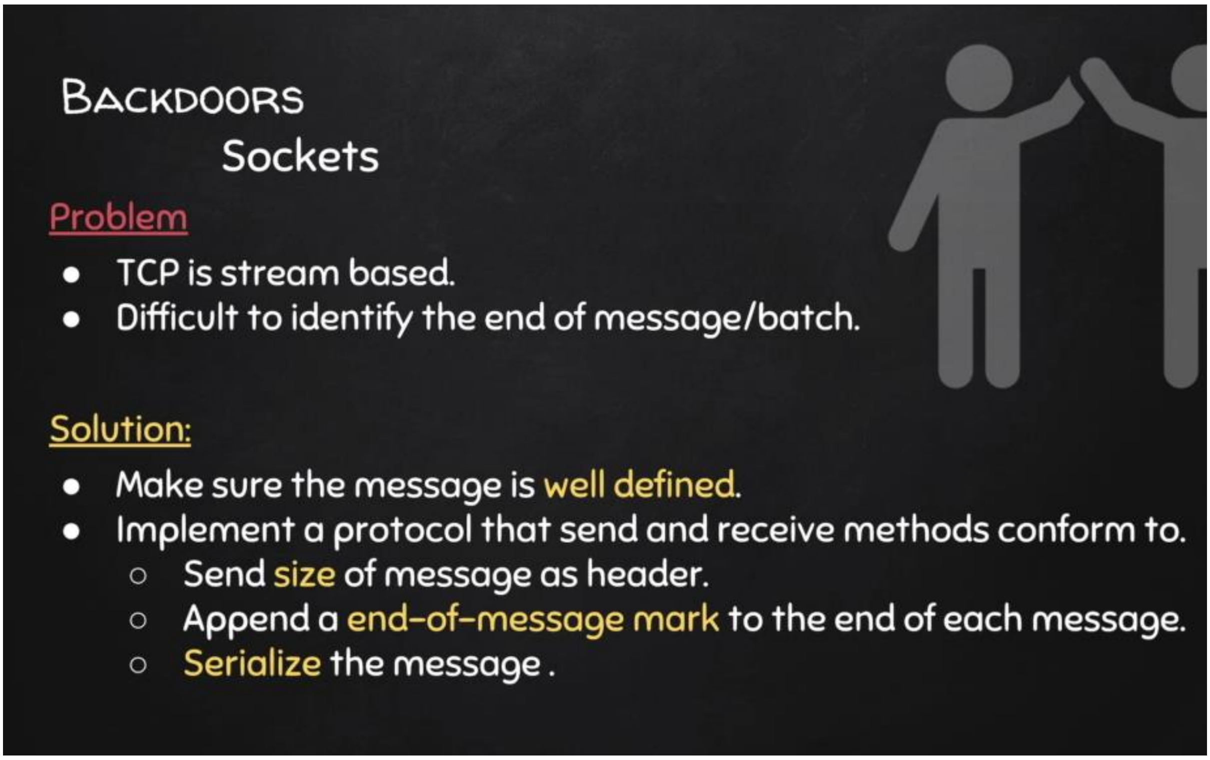
In TCP each computer on the network has been assigned with a unique IP address making it identifiable over the network. Besides that, each domain is assigned with a name. Therefore, ultimately TCP provides benefits of name and address resolution services.

4. In Order Delivery

Whenever a packet is sent, it cannot be guaranteed that it will be in order once it reaches its host. The order might get lost in between. Therefore, before reaching the application, TCP takes necessary steps to rearrange them in order.

5. Error Detection

Error in the TCP can negatively impact performance and connectivity services. Detecting errors like corrupted and missing segments is relatively easy in TCP. It is generally done through 3 steps. Those are the checksum, re transmission and acknowledgement.



BACKDOORS

Sockets

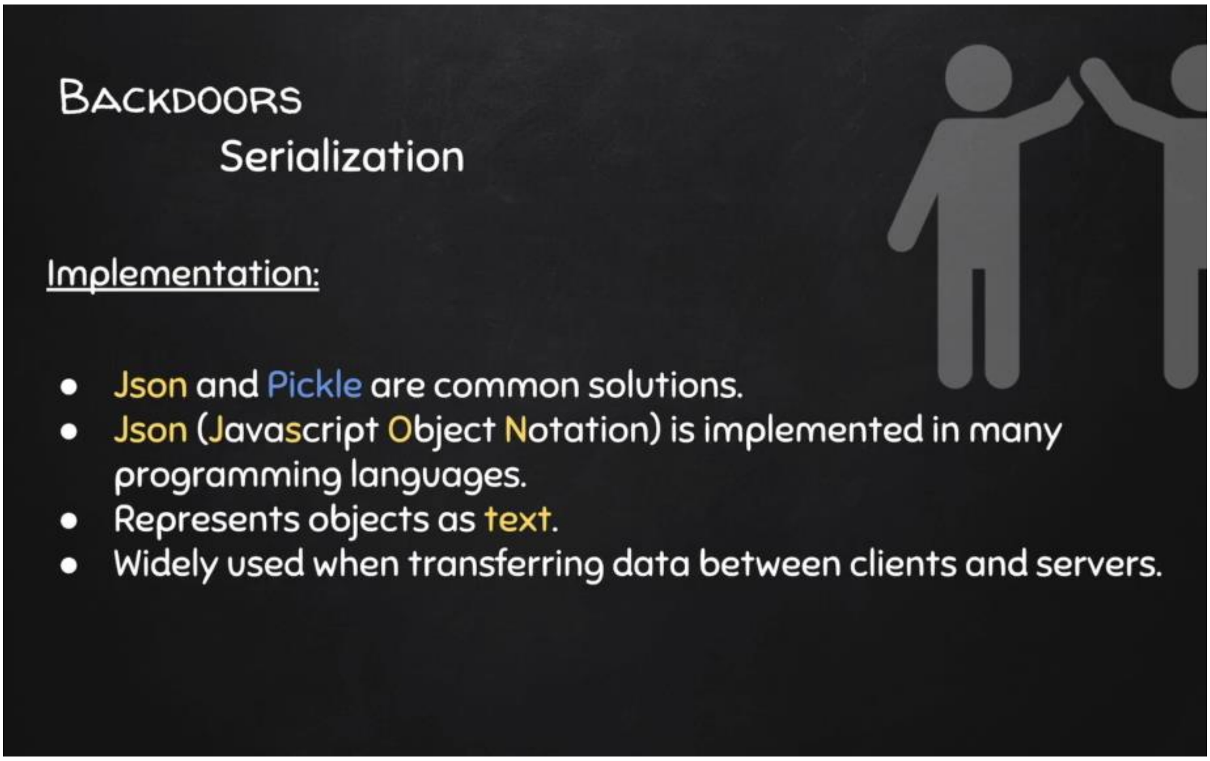
Problem

- TCP is stream based.
- Difficult to identify the end of message/batch.

Solution:

- Make sure the message is well defined.
- Implement a protocol that send and receive methods conform to.
  - Send size of message as header.
  - Append a end-of-message mark to the end of each message.
  - Serialize the message .

Why We Use Json Object with Tcp and Ipv4 Addressing.

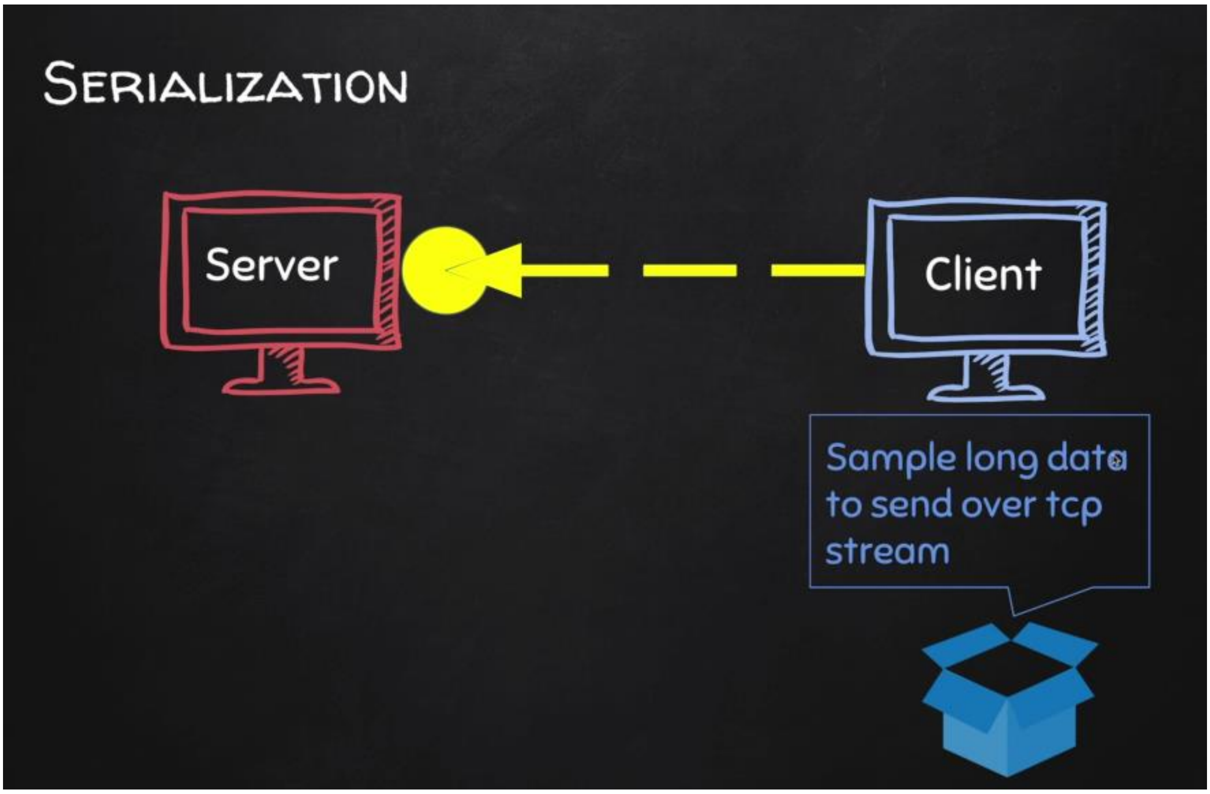


BACKDOORS

Serialization

Implementation:

- Json and Pickle are common solutions.
- Json (Javascript Object Notation) is implemented in many programming languages.
- Represents objects as text.
- Widely used when transferring data between clients and servers.

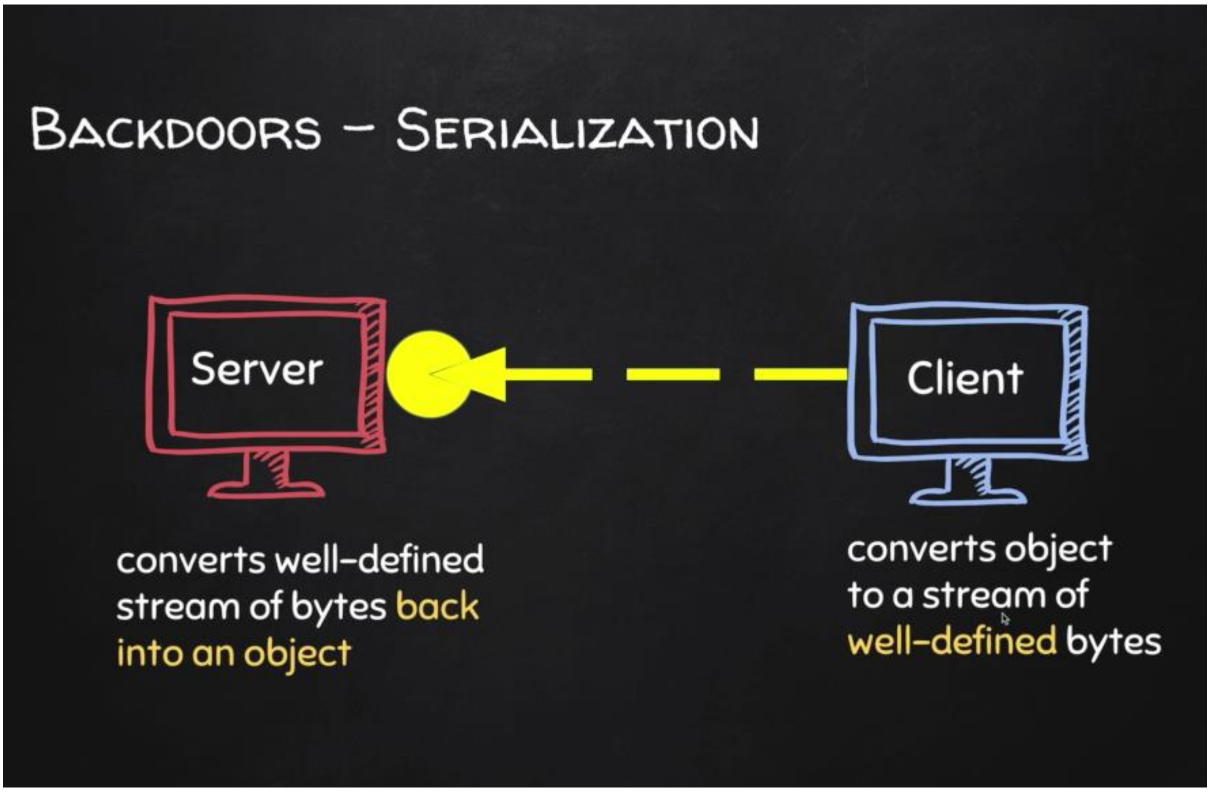


Serialization

Server

Client

Sample long data to send over tcp stream



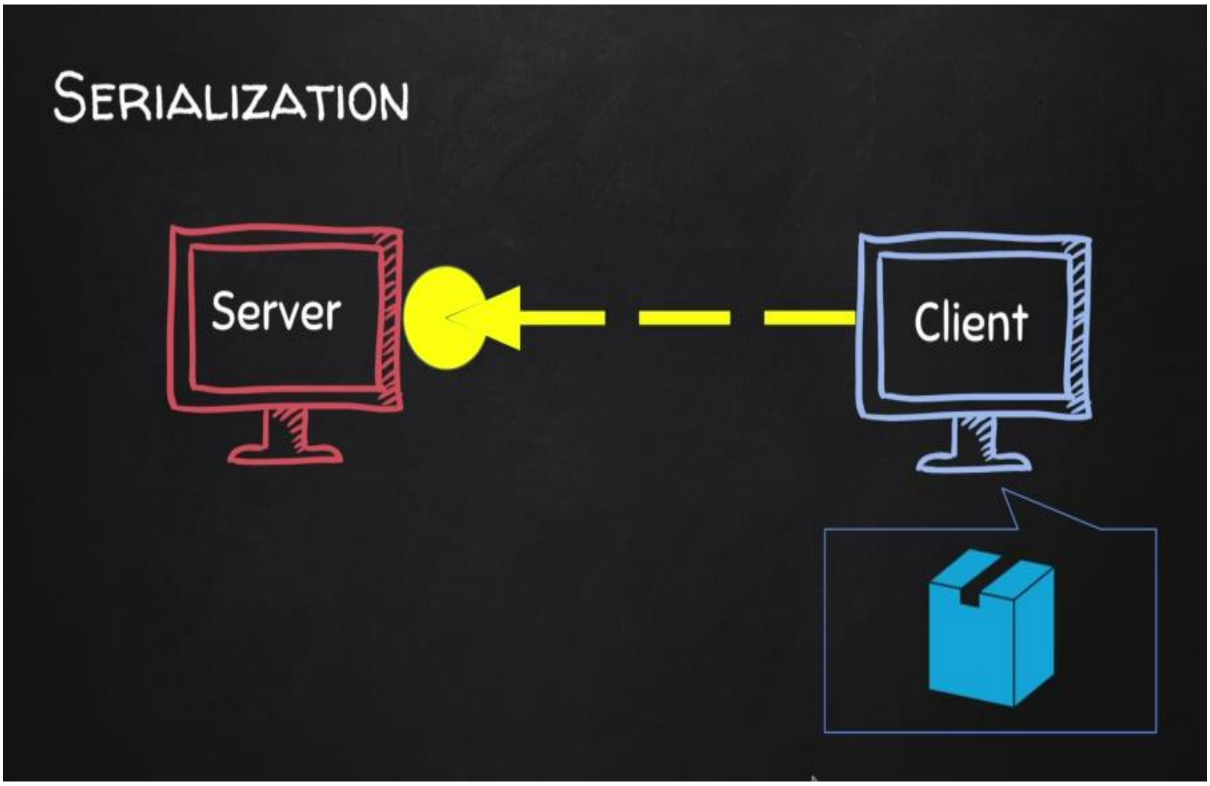
Backdoors - Serialization

Server

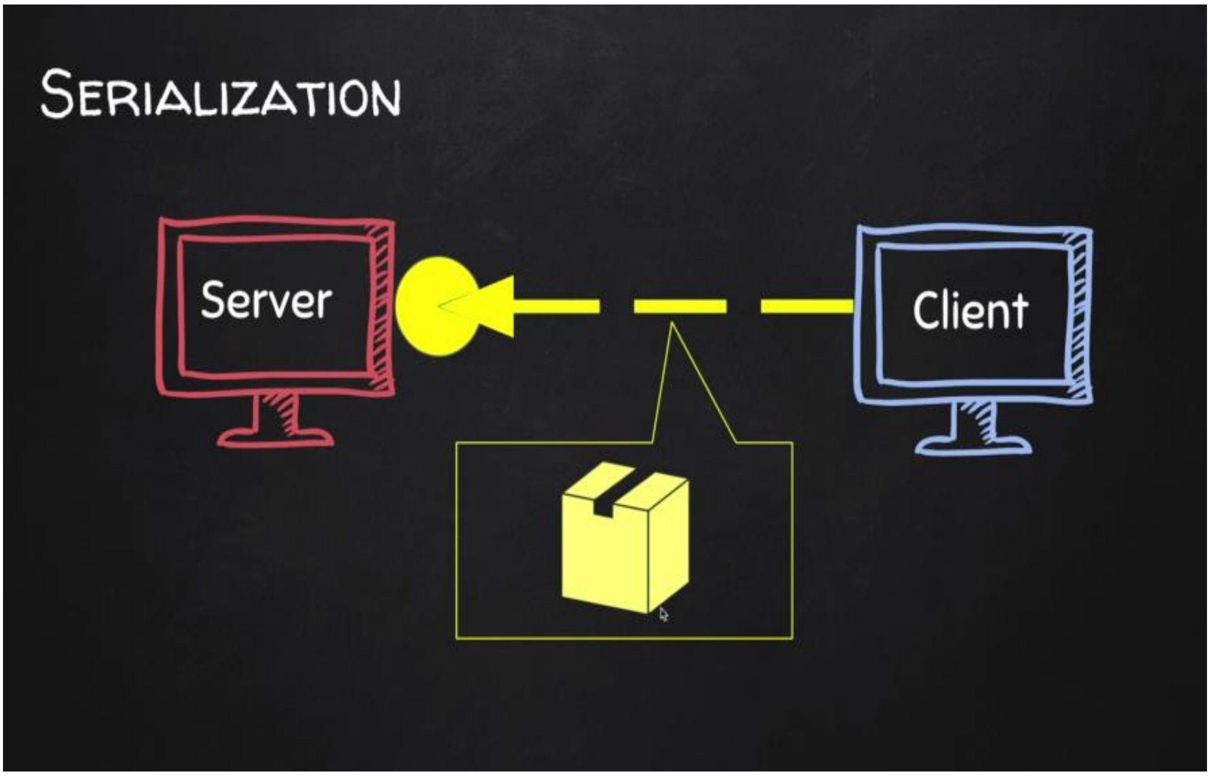
Client

converts well-defined stream of bytes back into an object

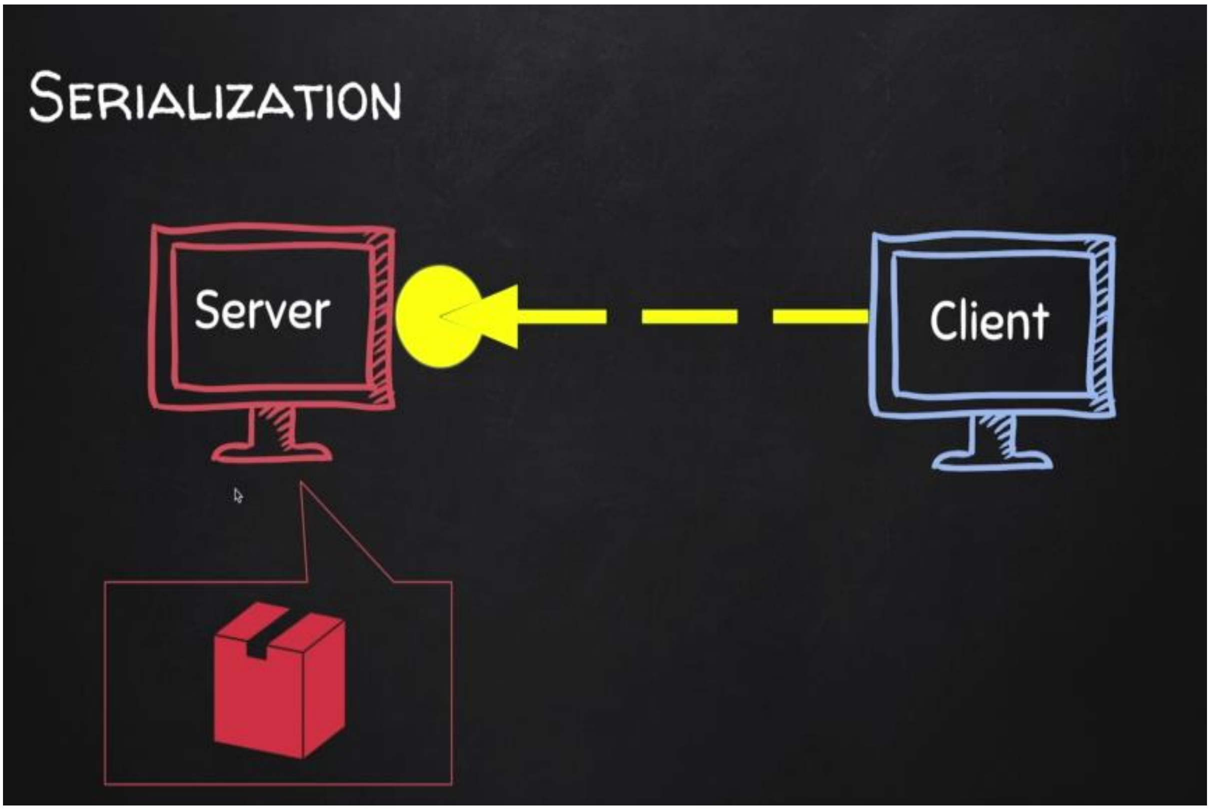
converts object to a stream of well-defined bytes



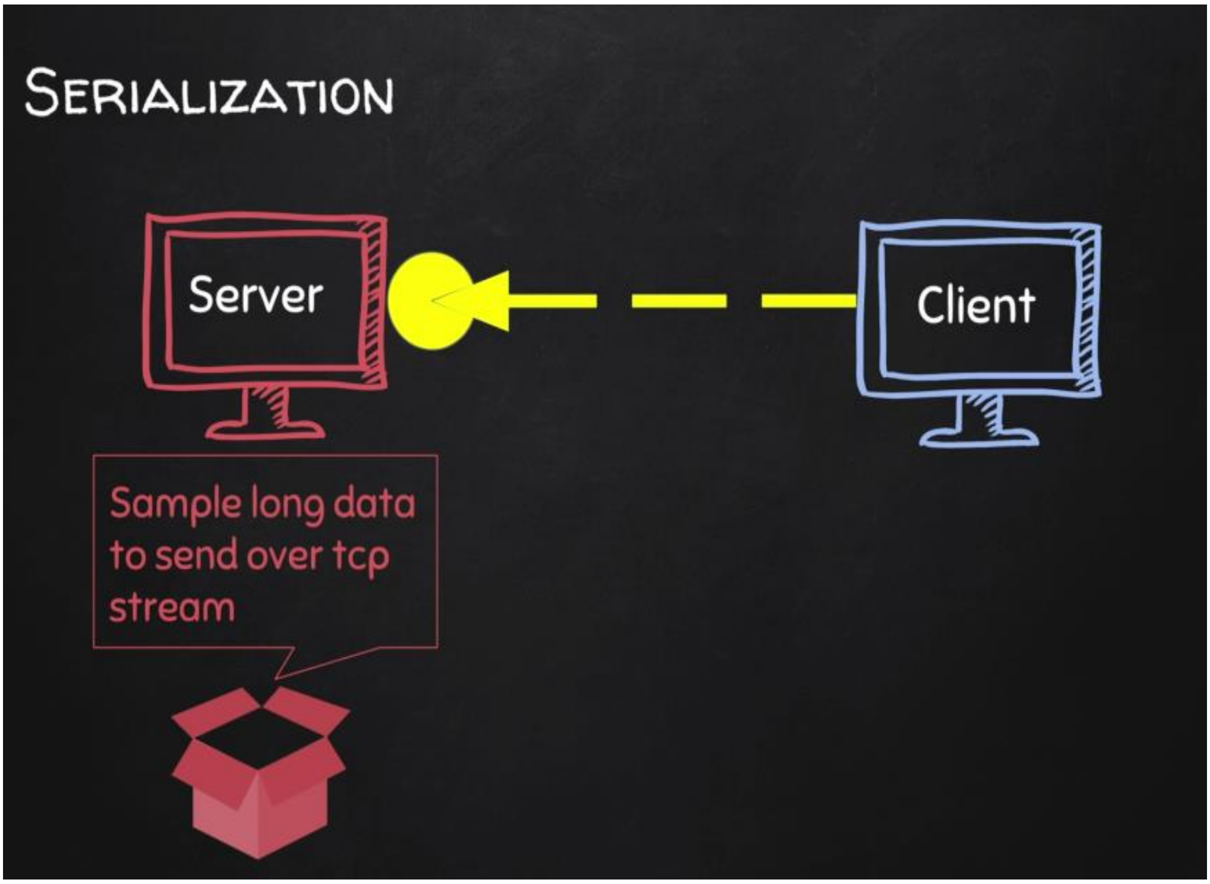
SERIALIZATION



SERIALIZATION

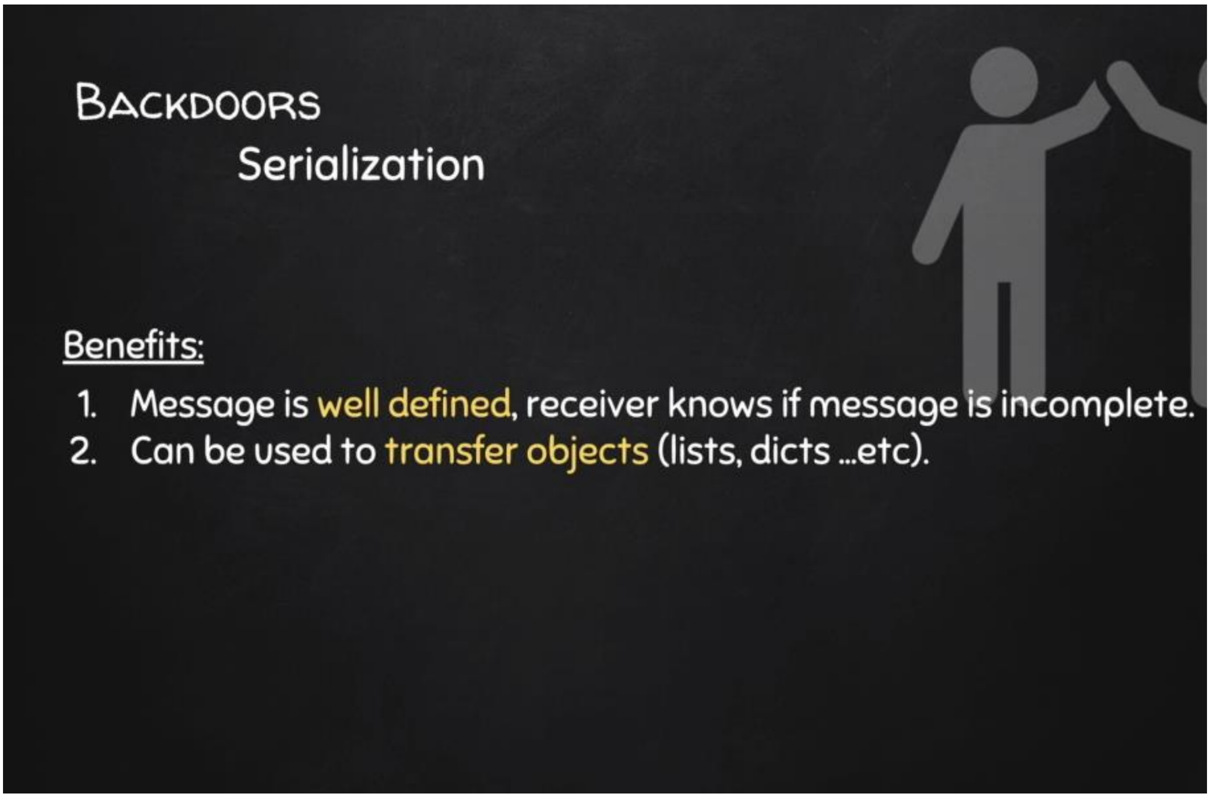


SERIALIZATION



SERIALIZATION

Sample long data to send over tcp stream



BACKDOORS

Serialization

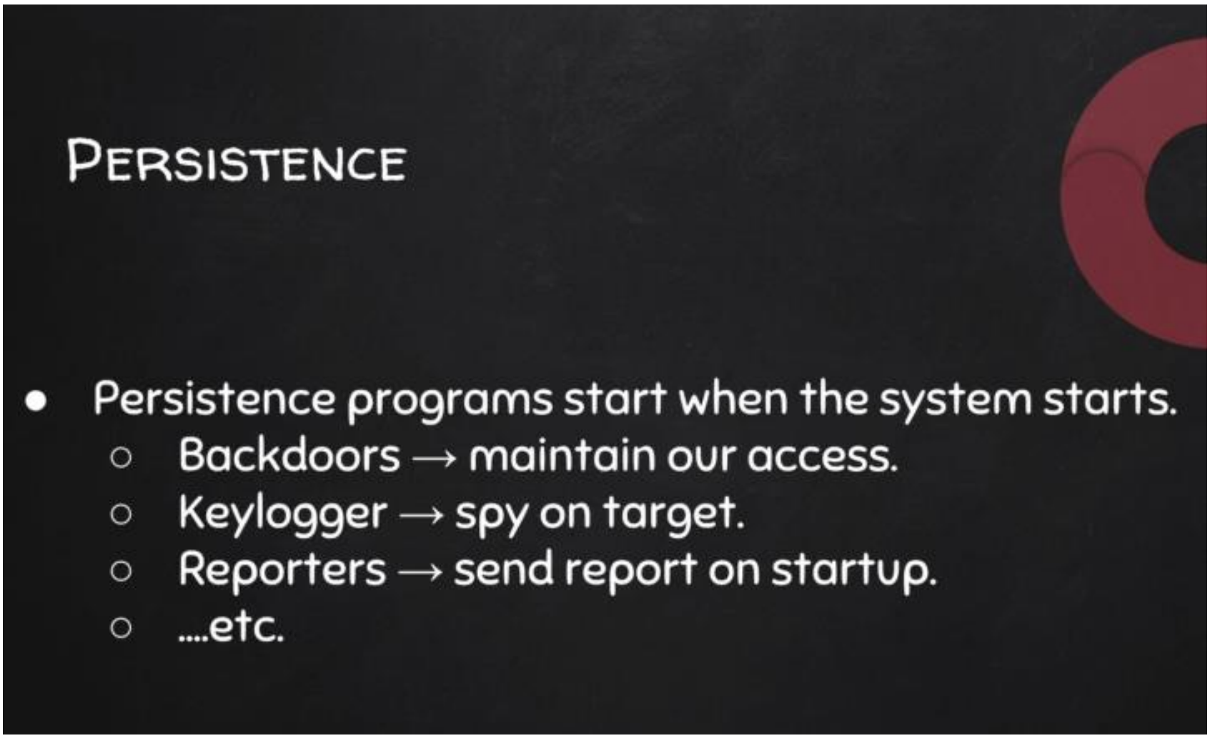
Benefits:

1. Message is well defined, receiver knows if message is incomplete.
2. Can be used to transfer objects (lists, dicts ...etc).

Running Executables Silently

Making An Entry in The Windows Registry of Auto Start-up Programs.

Persistence

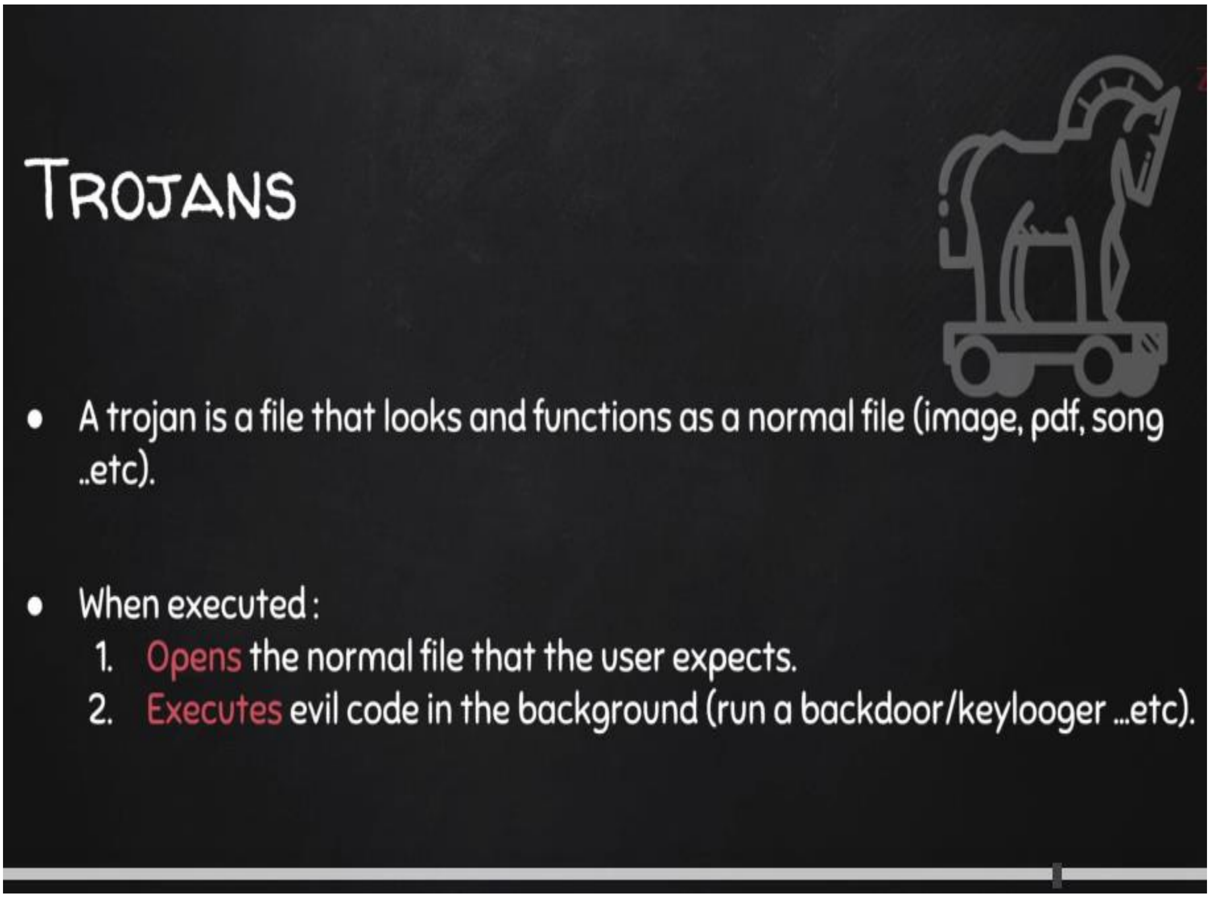


PERSISTENCE

- Persistence programs start when the system starts.
  - Backdoors → maintain our access.
  - Keylogger → spy on target.
  - Reporters → send report on startup.
  - ....etc.

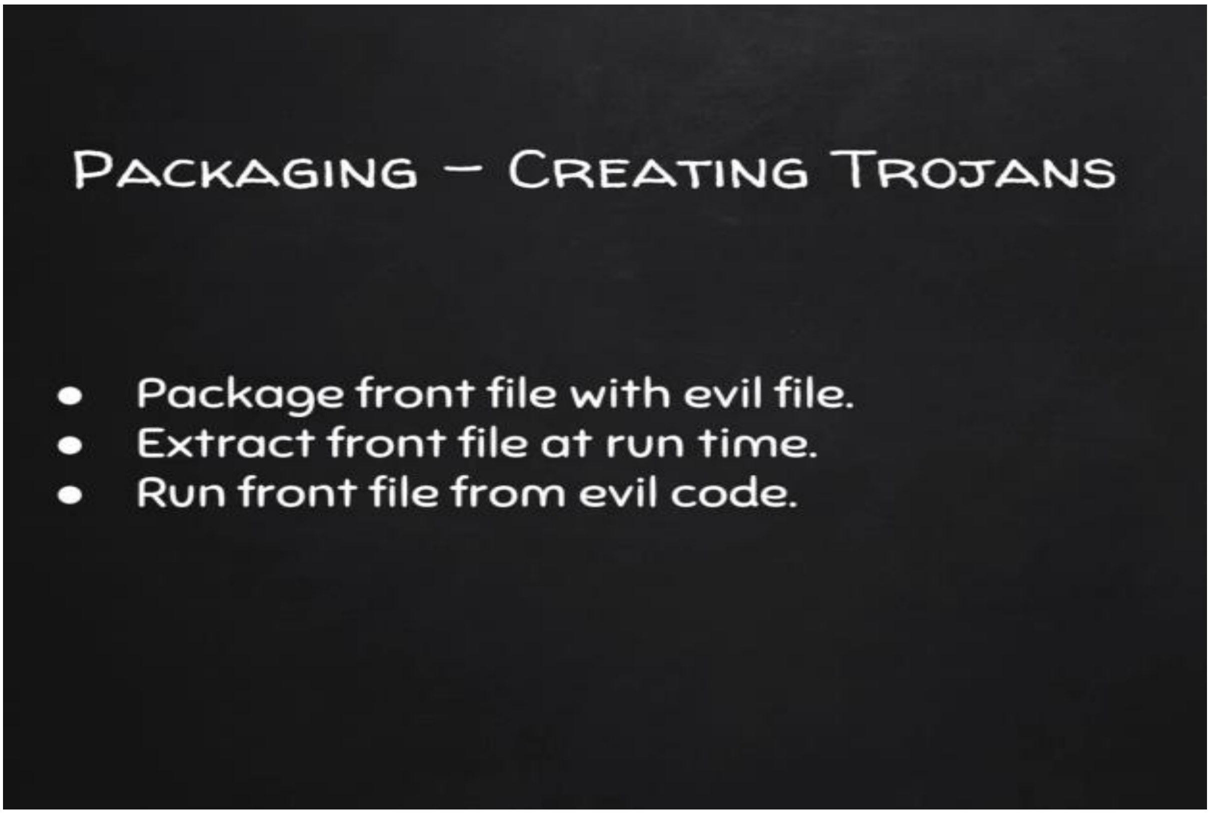
Running Programs on Start-up

Creating a Trojan by Embedding Files in Program Code



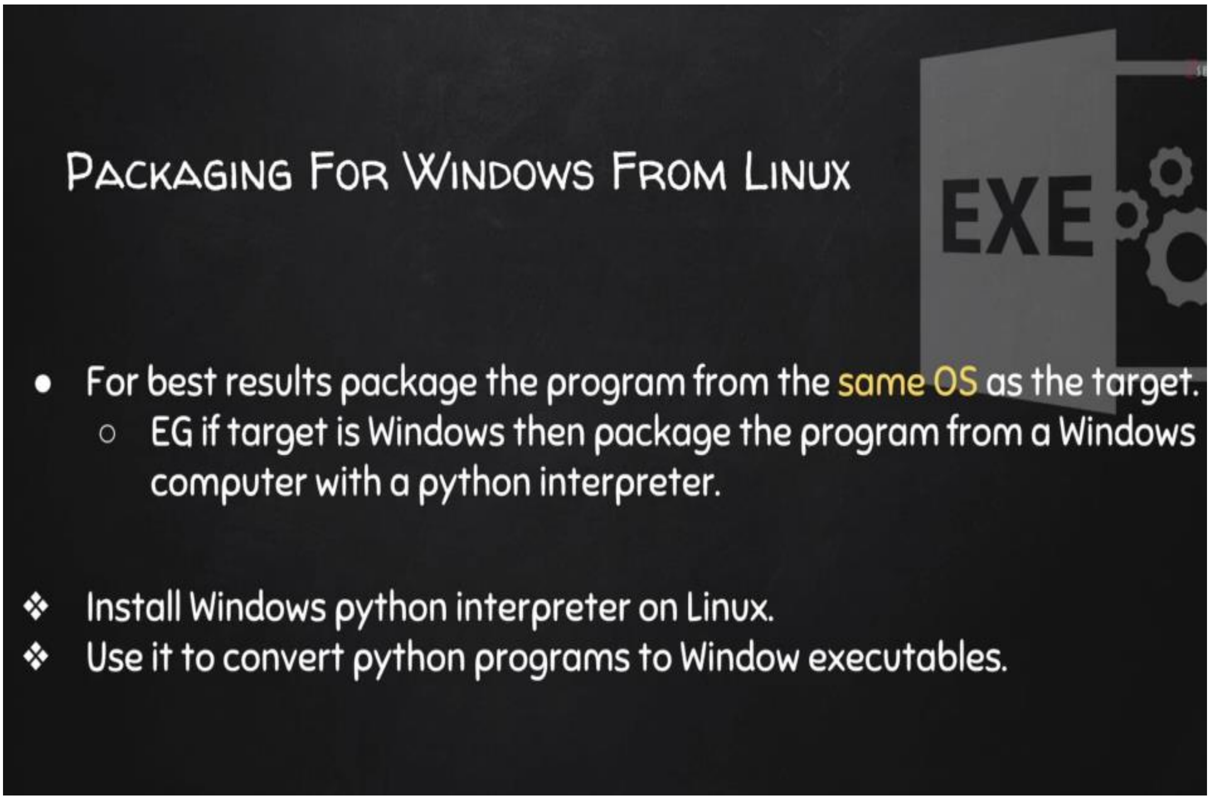
TROJANS

- A trojan is a file that looks and functions as a normal file (image, pdf, song ..etc).
- When executed :
  1. Opens the normal file that the user expects.
  2. Executes evil code in the background (run a backdoor/keylooger ...etc).



Packaging – Creating Trojans

- Package front file with evil file.
- Extract front file at run time.
- Run front file from evil code.

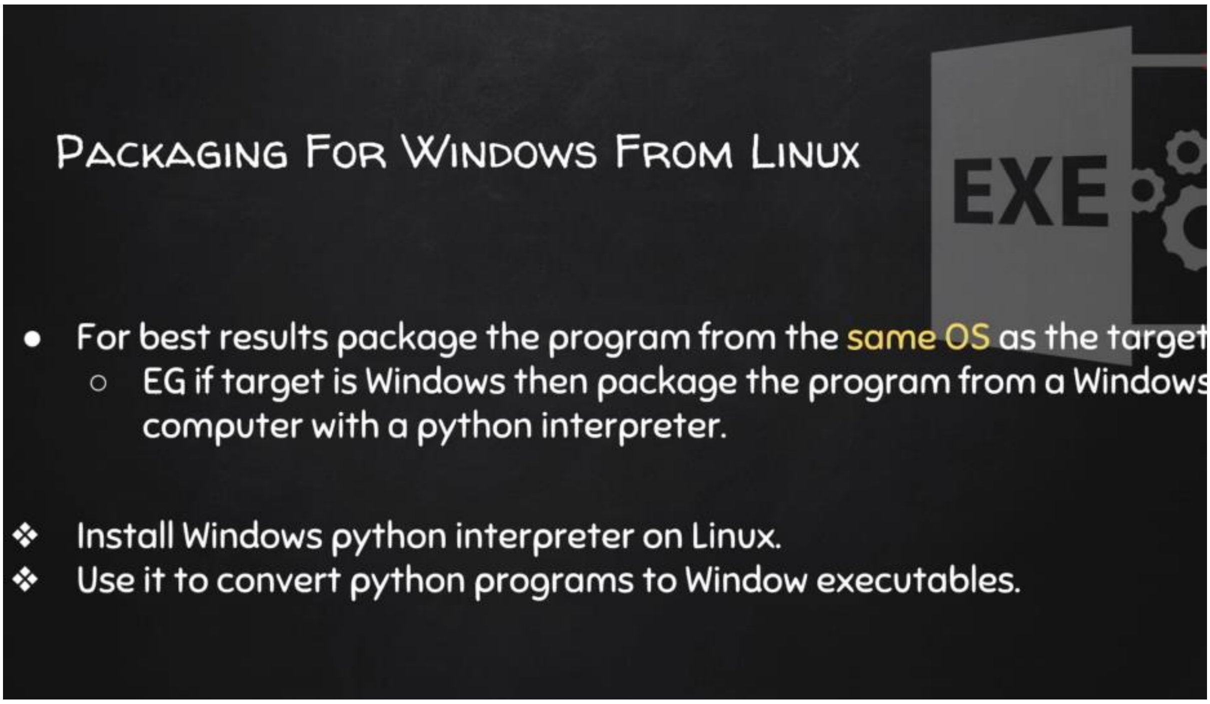


Packaging For Windows From Linux

- For best results package the program from the same OS as the target.
  - EG if target is Windows then package the program from a Windows computer with a python interpreter.

❖ Install Windows python interpreter on Linux.

❖ Use it to convert python programs to Window executables.



Packaging For Windows From Linux

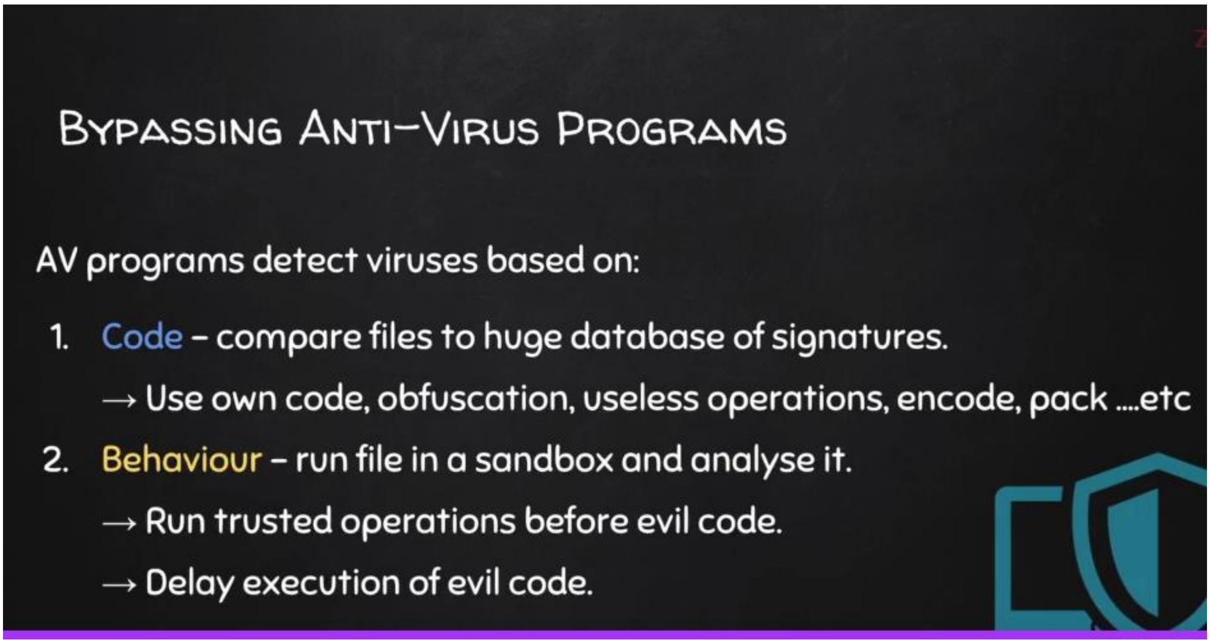
- For best results package the program from the same OS as the target
  - EG if target is Windows then package the program from a Windows computer with a python interpreter.

❖ Install Windows python interpreter on Linux.
❖ Use it to convert python programs to Window executables.

Bypassing Anti-Virus Programs-

You may need to bypass antivirus software in two situations:

- during an attack. In such cases, the payload is run either by a vulnerable application or, more often, by the user (social engineering). In most cases, this gives you a foothold and ensures your persistence in the system. The most important thing is to avoid detection; or
- during post-exploitation. In this case, it is you who runs the program on the compromised PC. It may be a sniffer, a privilege escalator, or other hacking software used to advance you through the network. For the post-exploitation purposes, the program has to be run by all means – even if you failed to launch it on the first try and the antivirus has raised several alarms.



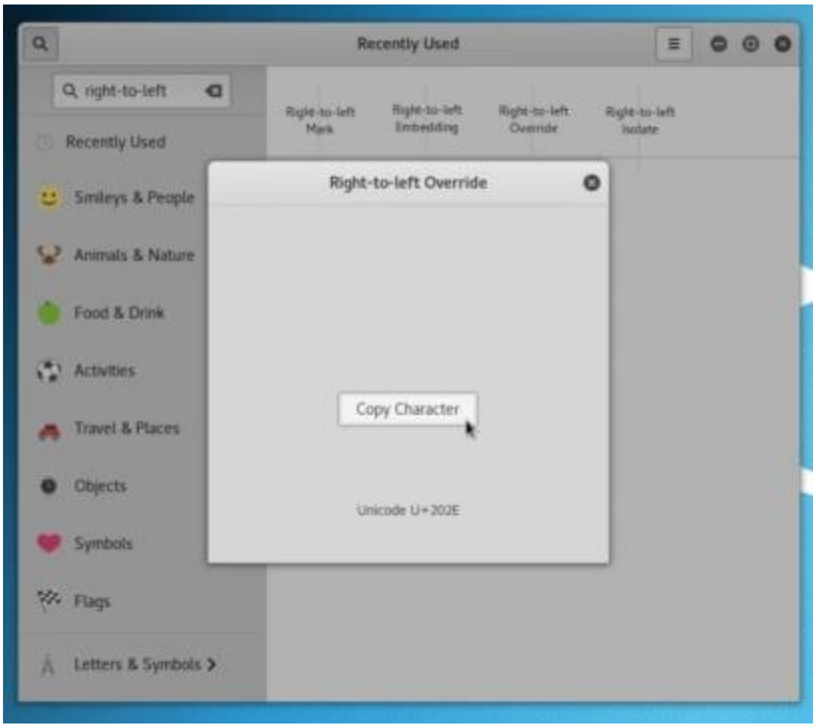
Bypassing Anti–Virus Programs

AV programs detect viruses based on:

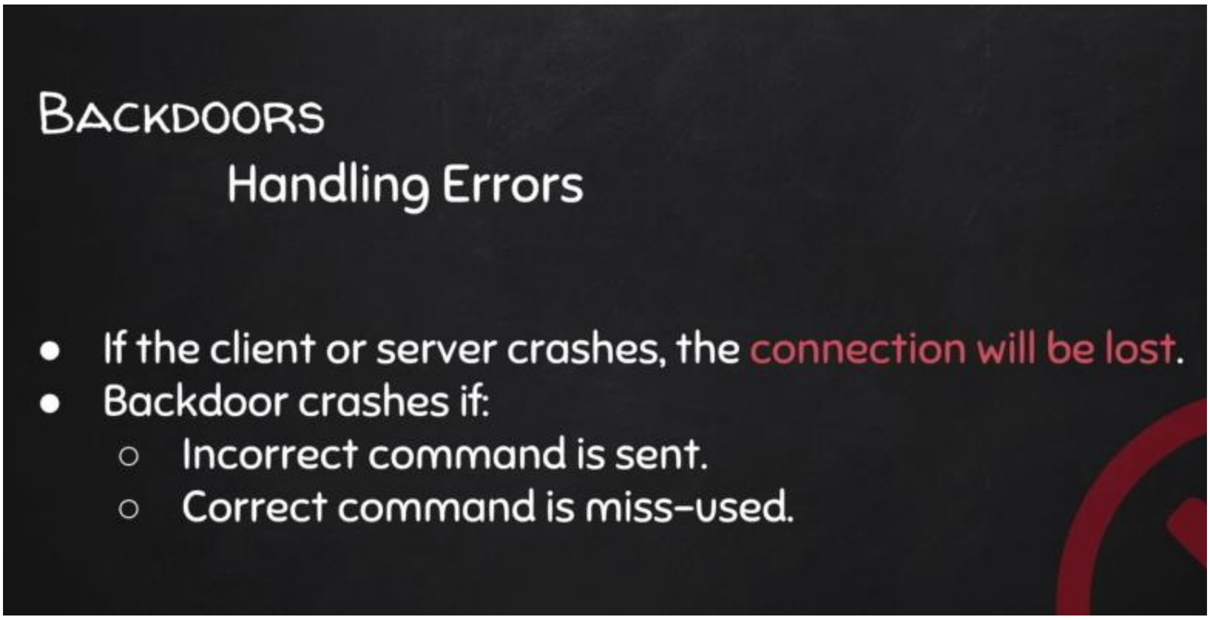
1. Code – compare files to huge database of signatures.
   → Use own code, obfuscation, useless operations, encode, pack ....etc
2. Behaviour – run file in a sandbox and analyse it.
   → Run trusted operations before evil code.
   → Delay execution of evil code.

Adding an Icon to Generated Executables

Spoofing File Extension



Backdoor Error Handling

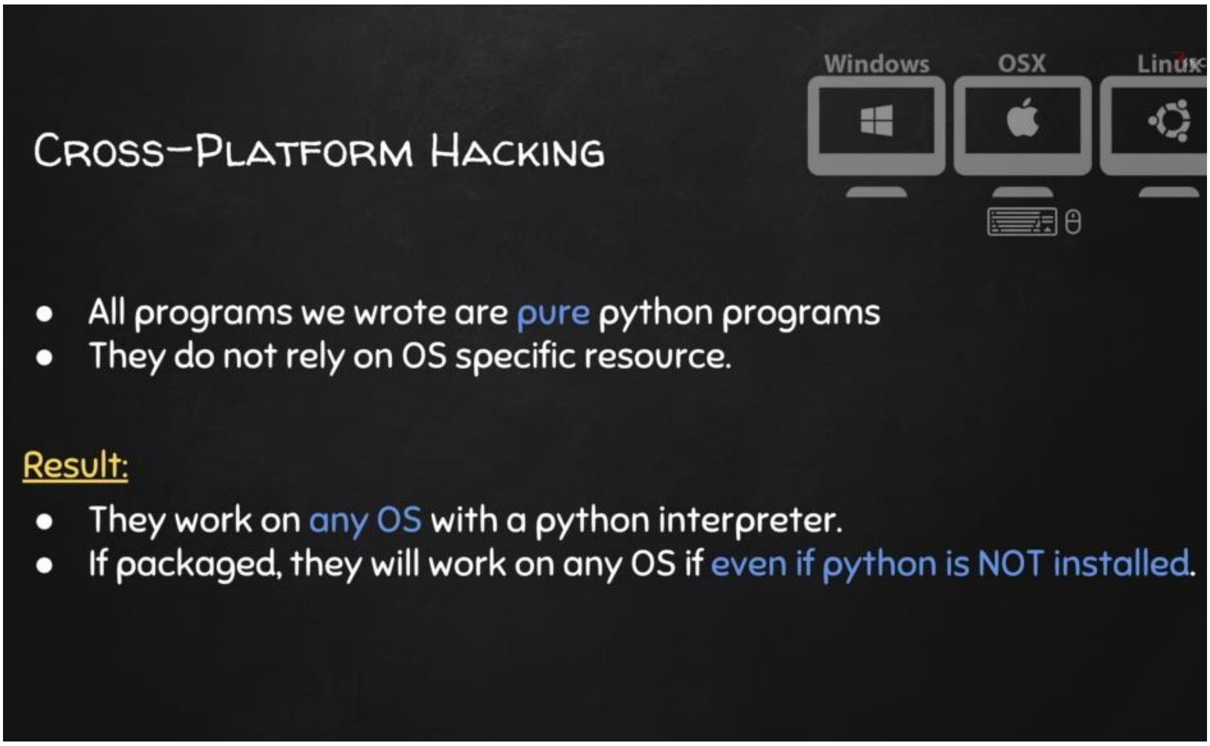


Backdoors

Handling Errors

- If the client or server crashes, the connection will be lost.
- Backdoor crashes if:
  - Incorrect command is sent.
  - Correct command is miss-used.

Cross Platform Compatibility



CROSS-PLATFORM HACKING

- All programs we wrote are pure python programs
- They do not rely on OS specific resource.

Result:

- They work on any OS with a python interpreter.
- If packaged, they will work on any OS if even if python is NOT installed.

Why We Use Pyinstaller

PyInstaller is a package in Python which bundles all the dependencies of Python applications in a single package.

We don’t need to install different packages or modules for different applications.

PyInstaller reads and analyses our code and then discovers the modules that our program requires in order to execute. It then packages them into a single folder or a single executable file.

It is used to create .exe files for windows, .app files for Mac and distributable packages for Linux.

PyInstaller can also create a one-file app for our Python script. It contains an archive of all Python modules required by our python program.

- **Subprocess-** Subprocess is the task of executing or running other programs in Python by creating a new process. We can use subprocess when running a code from Github or running a file storing code in any other programming language like C, C++, etc**.**

- **JSON (JavaScript Object Notation)-** is a file that is mainly used to store and transfer data mostly between a server and a web application. It is popularly used for representing structured data. In this article, we will discuss how to handle JSON data using Python. Python provides a module called json which comes with Python's standard built-in utility.

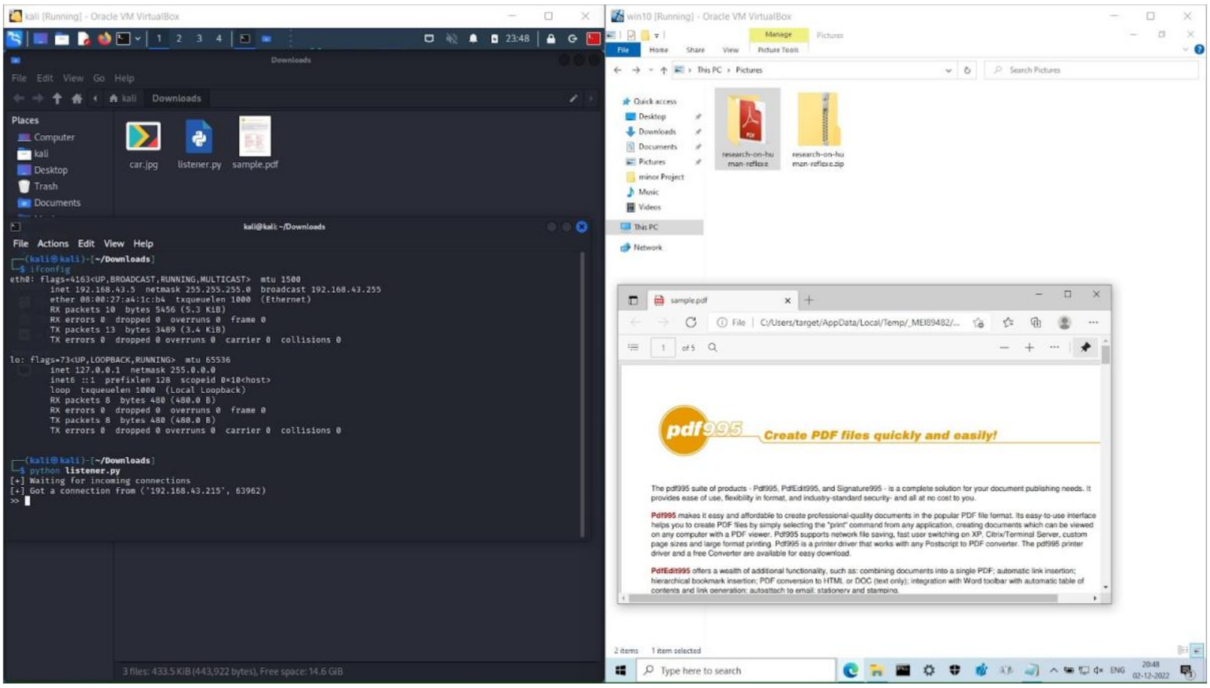
- **OS**-The OS module in Python provides functions for interacting with the operating system. OS comes under Python's standard utility modules. This module provides a portable way of using operating system-dependent functionality. The os and os.path modules include many functions to interact with the file system.

- **Base64 -**The Base64 encoding is used to convert bytes that have binary or text data into ASCII characters. Encoding prevents the data from getting corrupted when it is transferred or processed through a text-only system.

- **sys -**The sys module in Python provides various functions and variables that are used to manipulate different parts of the Python runtime environment. It allows operating on the interpreter as it provides access to the variables and functions that interact strongly with the interpreter.

- **Shutil-**The shutil is a module that offers several functions to deal with operations on files and their collections. It provides the ability to copy and removal of files.

Chapter - 5 Testing



```
┌──(kali㉿kali)-[~/Downloads]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.43.5  netmask 255.255.255.0  broadcast 192.168.43.255
        ether 08:00:27:a4:1c:b4  txqueuelen 1000  (Ethernet)
        RX packets 10  bytes 5456 (5.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 13  bytes 3489 (3.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~/Downloads]
└─$ python listener.py
[+] Waiting for incoming connections
[+] Got a connection from ('192.168.43.215', 63962)
>> 
```

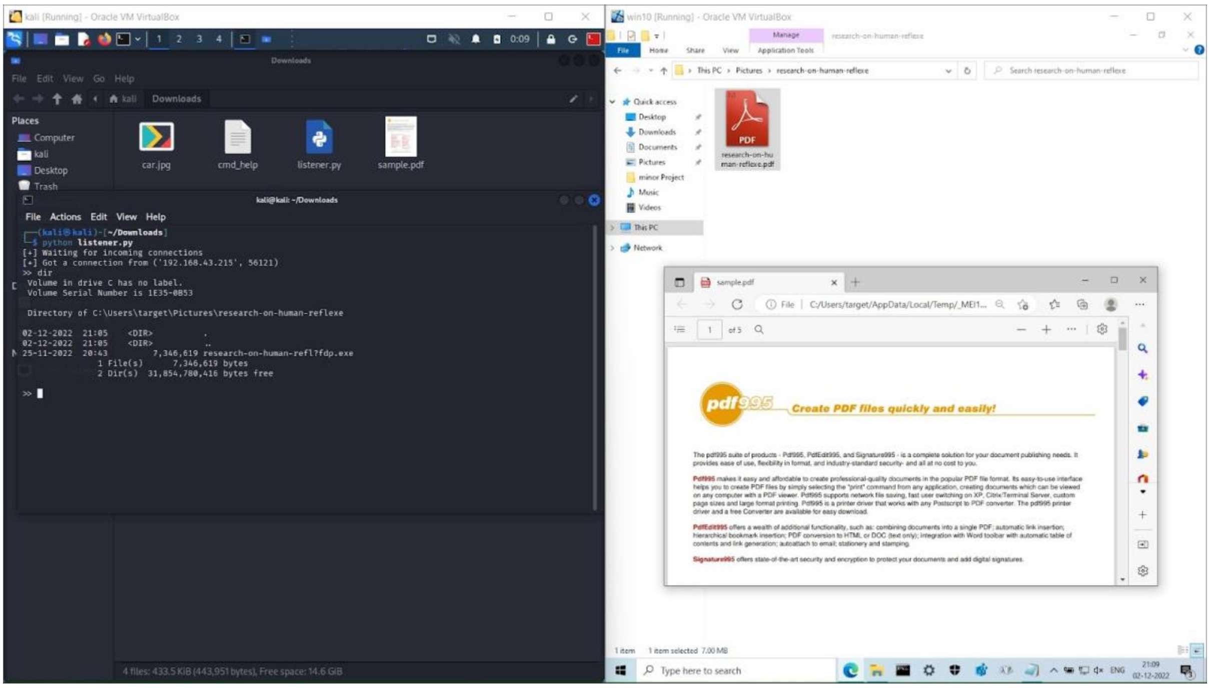
Create PDF files quickly and easily!

The pdf995 suite of products - Pdf995, PdfEdit995, and Signature995 - is a complete solution for your document publishing needs. It provides ease of use, flexibility in format, and industry-standard security- and all at no cost to you.

Pdf995 makes it easy and affordable to create professional-quality documents in the popular PDF file format. Its easy-to-use interface helps you to create PDF files by simply selecting the "print" command from any application, creating documents which can be viewed on any computer with a PDF viewer. Pdf995 supports network file saving, fast user switching on XP, Citrix/Terminal Server, custom page sizes and large format printing. Pdf995 is a printer driver that works with any Postscript to PDF converter. The pdf995 printer driver and a free Converter are available for easy download.

PdfEdit995 offers a wealth of additional functionality, such as: combining documents into a single PDF; automatic link insertion; hierarchical bookmark insertion; PDF conversion to HTML or DOC (text only); integration with Word toolbar with automatic table of contents and link generation; autoattach to email; stationery and stamping.

kali [Running] - Oracle VM VirtualBox
win10 [Running] - Oracle VM VirtualBox
Downloads
car.jpg
listener.py
sample.pdf
kali@kali: ~/Downloads
3 files: 433.5 KiB (443,922 bytes), Free space: 14.6 GiB
This PC › Pictures
research-on-human-reflexe
research-on-human-reflexe.zip
sample.pdf
C:/Users/target/AppData/Local/Temp/_MEI89482/...
2 items   1 item selected
Type here to search
20:48
02-12-2022



```
┌──(kali㉿kali)-[~/Downloads]
└─$ python listener.py
[+] Waiting for incoming connections
[+] Got a connection from ('192.168.43.215', 56121)
>> dir
 Volume in drive C has no label.
 Volume Serial Number is 1E35-0B53

 Directory of C:\Users\target\Pictures\research-on-human-reflexe

02-12-2022  21:05    <DIR>          .
02-12-2022  21:05    <DIR>          ..
25-11-2022  20:43         7,346,619 research-on-human-refl?fdp.exe
               1 File(s)      7,346,619 bytes
               2 Dir(s)  31,854,780,416 bytes free

>> 
```

Create PDF files quickly and easily!

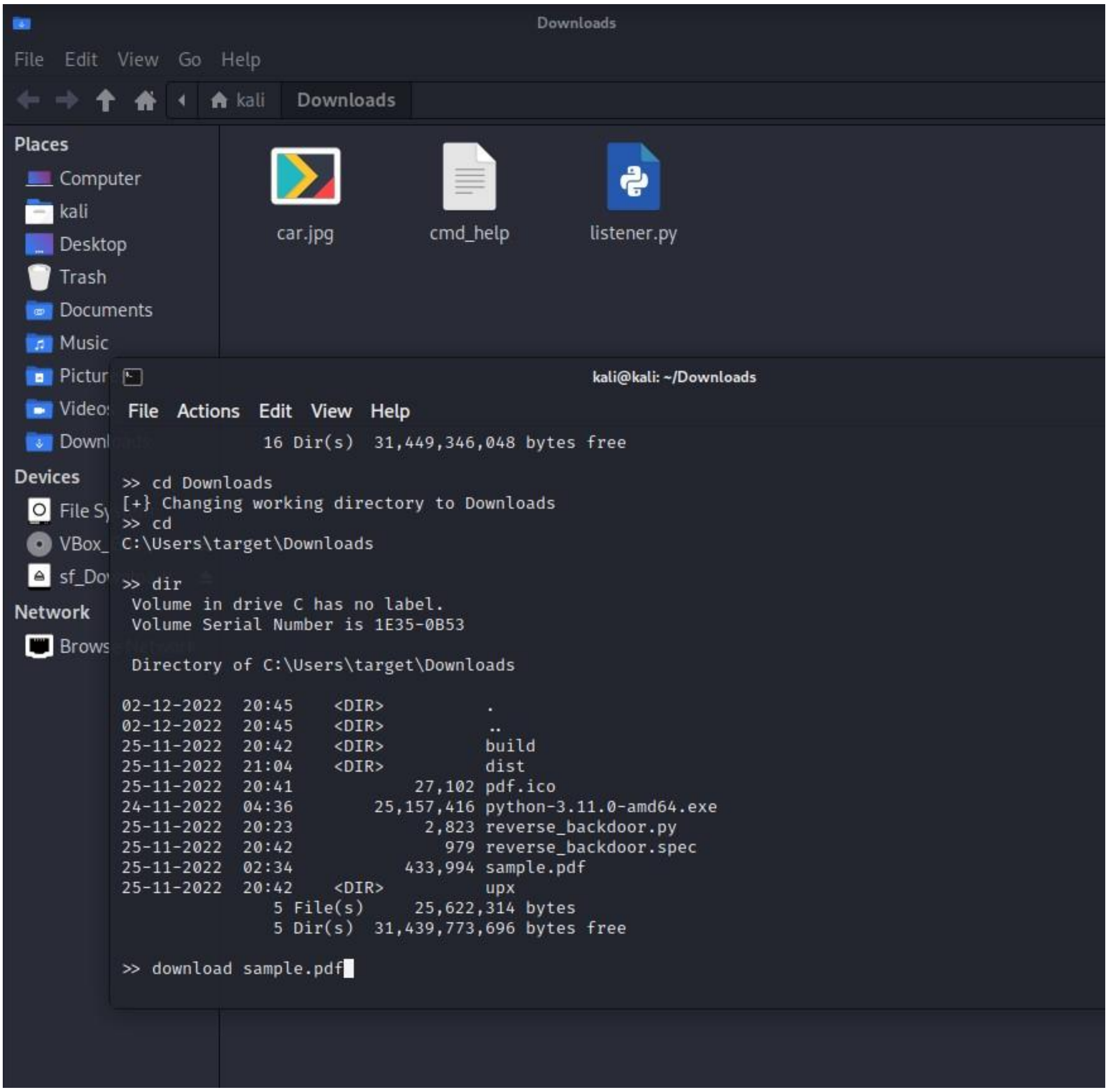
The pdf995 suite of products - Pdf995, PdfEdit995, and Signature995 - is a complete solution for your document publishing needs. It provides ease of use, flexibility in format, and industry-standard security- and all at no cost to you.

Pdf995 makes it easy and affordable to create professional-quality documents in the popular PDF file format. Its easy-to-use interface helps you to create PDF files by simply selecting the "print" command from any application, creating documents which can be viewed on any computer with a PDF viewer. Pdf995 supports network file saving, fast user switching on XP, Citrix/Terminal Server, custom page sizes and large format printing. Pdf995 is a printer driver that works with any Postscript to PDF converter. The pdf995 printer driver and a free Converter are available for easy download.

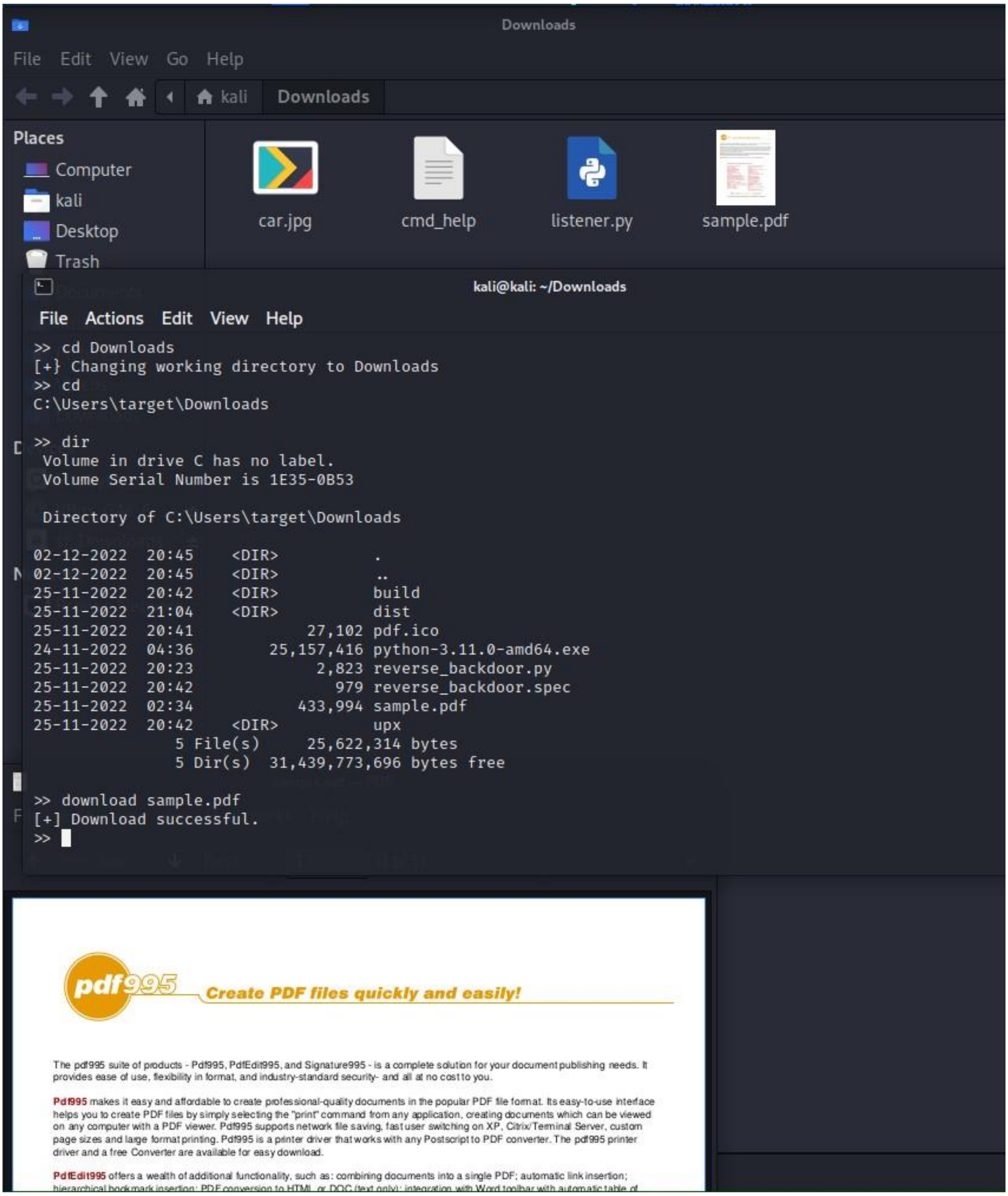
PdfEdit995 offers a wealth of additional functionality, such as: combining documents into a single PDF; automatic link insertion; hierarchical bookmark insertion; PDF conversion to HTML or DOC (text only); integration with Word toolbar with automatic table of contents and link generation; autoattach to email; stationery and stamping.

Signature995 offers state-of-the-art security and encryption to protect your documents and add digital signatures.

kali [Running] - Oracle VM VirtualBox
win10 [Running] - Oracle VM VirtualBox
Downloads
car.jpg
cmd_help
listener.py
sample.pdf
kali@kali: ~/Downloads
4 files: 433.5 KiB (443,951 bytes), Free space: 14.6 GiB
This PC › Pictures › research-on-human-reflexe
research-on-human-reflexe.pdf
sample.pdf
C:/Users/target/AppData/Local/Temp/_MEI1...
1 item   1 item selected 7.00 MB
Type here to search
21:09
02-12-2022



```
              16 Dir(s)  31,449,346,048 bytes free

>> cd Downloads
[+] Changing working directory to Downloads
>> cd
C:\Users\target\Downloads

>> dir
 Volume in drive C has no label.
 Volume Serial Number is 1E35-0B53

 Directory of C:\Users\target\Downloads

02-12-2022  20:45    <DIR>          .
02-12-2022  20:45    <DIR>          ..
25-11-2022  20:42    <DIR>          build
25-11-2022  21:04    <DIR>          dist
25-11-2022  20:41            27,102 pdf.ico
24-11-2022  04:36        25,157,416 python-3.11.0-amd64.exe
25-11-2022  20:23             2,823 reverse_backdoor.py
25-11-2022  20:42               979 reverse_backdoor.spec
25-11-2022  02:34           433,994 sample.pdf
25-11-2022  20:42    <DIR>          upx
               5 File(s)     25,622,314 bytes
               5 Dir(s)  31,439,773,696 bytes free

>> download sample.pdf
```

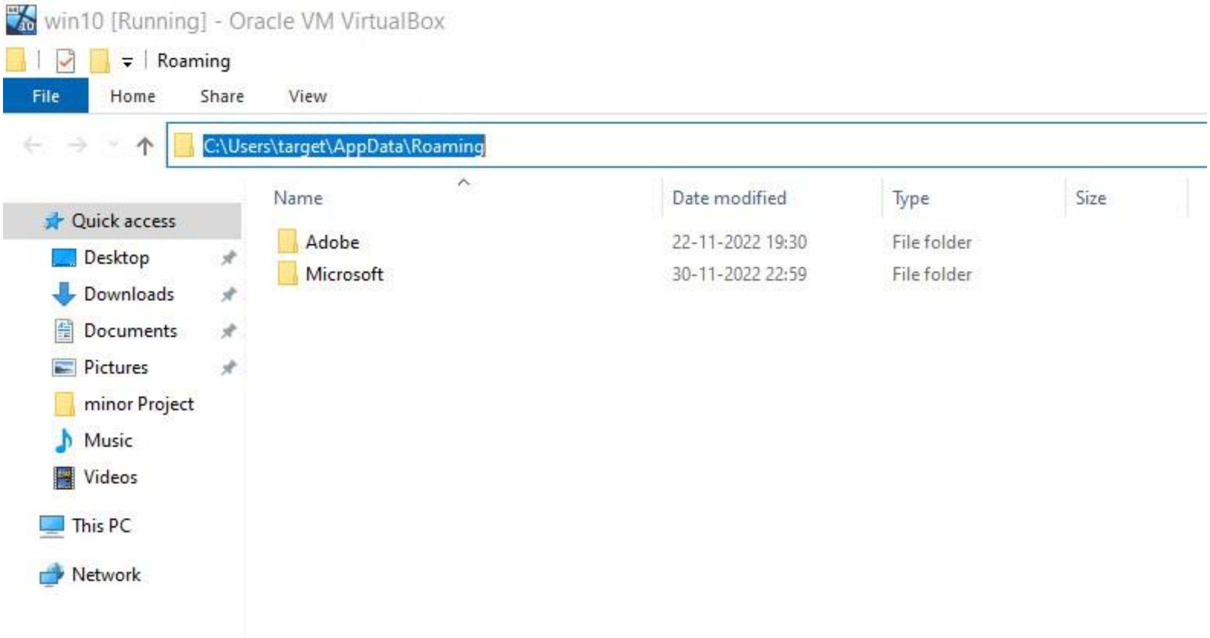


```
>> cd Downloads
[+} Changing working directory to Downloads
>> cd
C:\Users\target\Downloads

>> dir
 Volume in drive C has no label.
 Volume Serial Number is 1E35-0B53

 Directory of C:\Users\target\Downloads

02-12-2022  20:45    <DIR>          .
02-12-2022  20:45    <DIR>          ..
25-11-2022  20:42    <DIR>          build
25-11-2022  21:04    <DIR>          dist
25-11-2022  20:41            27,102 pdf.ico
24-11-2022  04:36        25,157,416 python-3.11.0-amd64.exe
25-11-2022  20:23             2,823 reverse_backdoor.py
25-11-2022  20:42               979 reverse_backdoor.spec
25-11-2022  02:34           433,994 sample.pdf
25-11-2022  20:42    <DIR>          upx
               5 File(s)     25,622,314 bytes
               5 Dir(s)  31,439,773,696 bytes free

>> download sample.pdf
[+] Download successful.
>> 
```

The pdf995 suite of products - Pdf995, PdfEdit995, and Signature995 - is a complete solution for your document publishing needs. It provides ease of use, flexibility in format, and industry-standard security- and all at no cost to you.

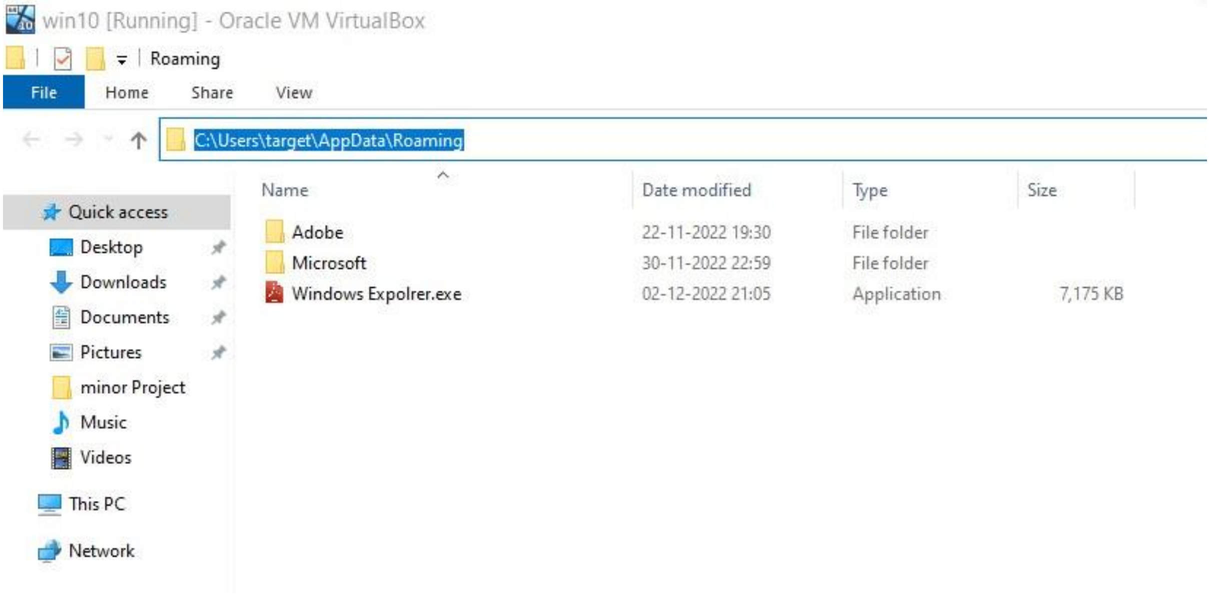
Pdf995 makes it easy and affordable to create professional-quality documents in the popular PDF file format. Its easy-to-use interface helps you to create PDF files by simply selecting the "print" command from any application, creating documents which can be viewed on any computer with a PDF viewer. Pdf995 supports network file saving, fast user switching on XP, Citrix/Terminal Server, custom page sizes and large format printing. Pdf995 is a printer driver that works with any Postscript to PDF converter. The pdf995 printer driver and a free Converter are available for easy download.

PdfEdit995 offers a wealth of additional functionality, such as: combining documents into a single PDF; automatic link insertion; hierarchical bookmark insertion; PDF conversion to HTML or DOC (text only); integration with Word toolbar with automatic table of



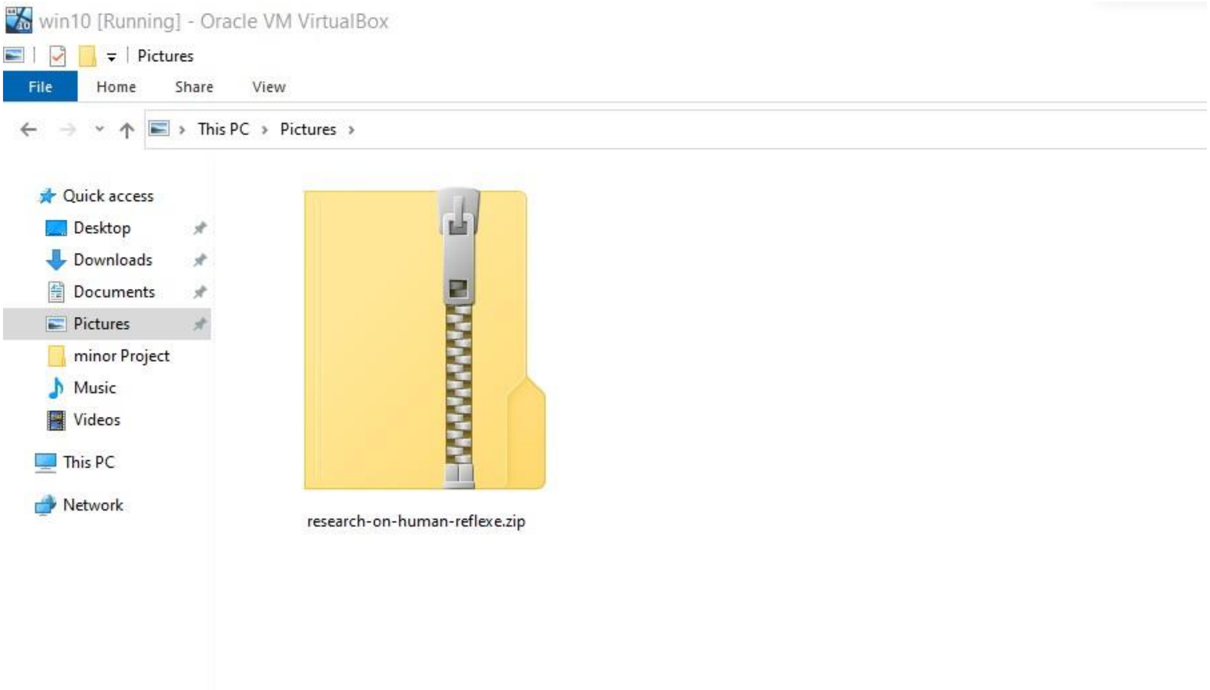
C:\Users\target\AppData\Roaming

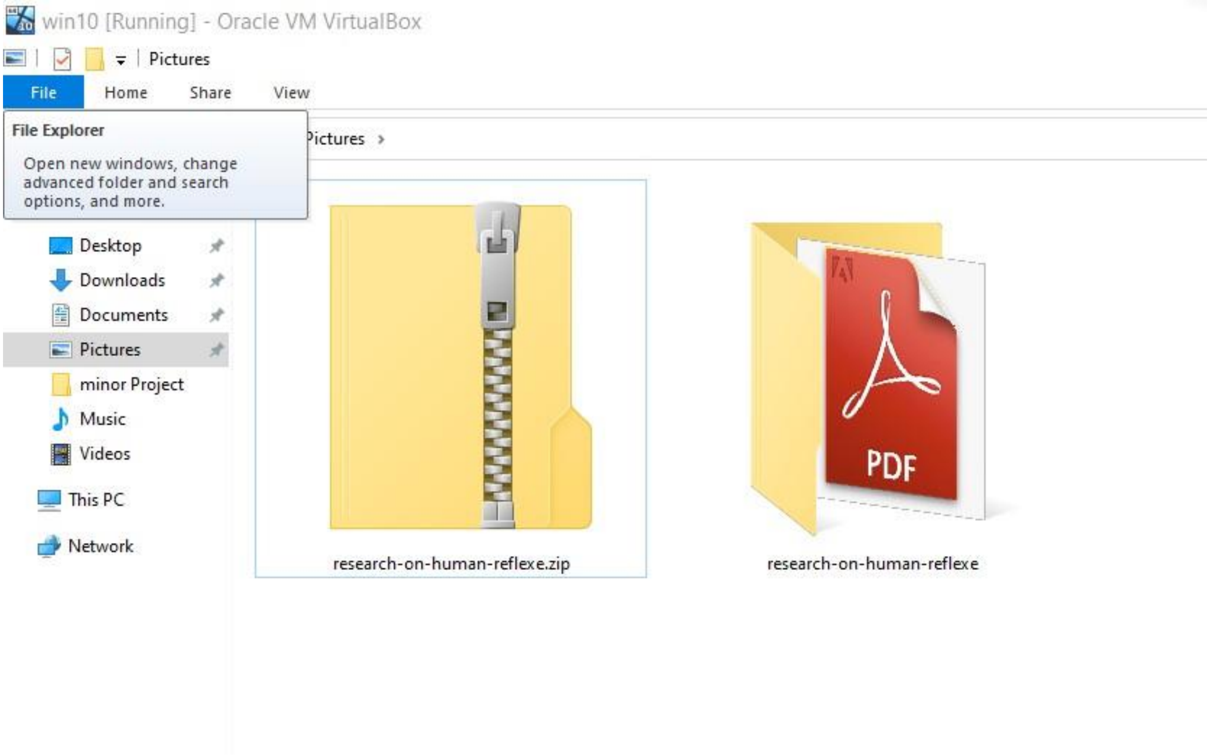
Name	Date modified	Type	Size
Adobe	22-11-2022 19:30	File folder	
Microsoft	30-11-2022 22:59	File folder	



C:\Users\target\AppData\Roaming

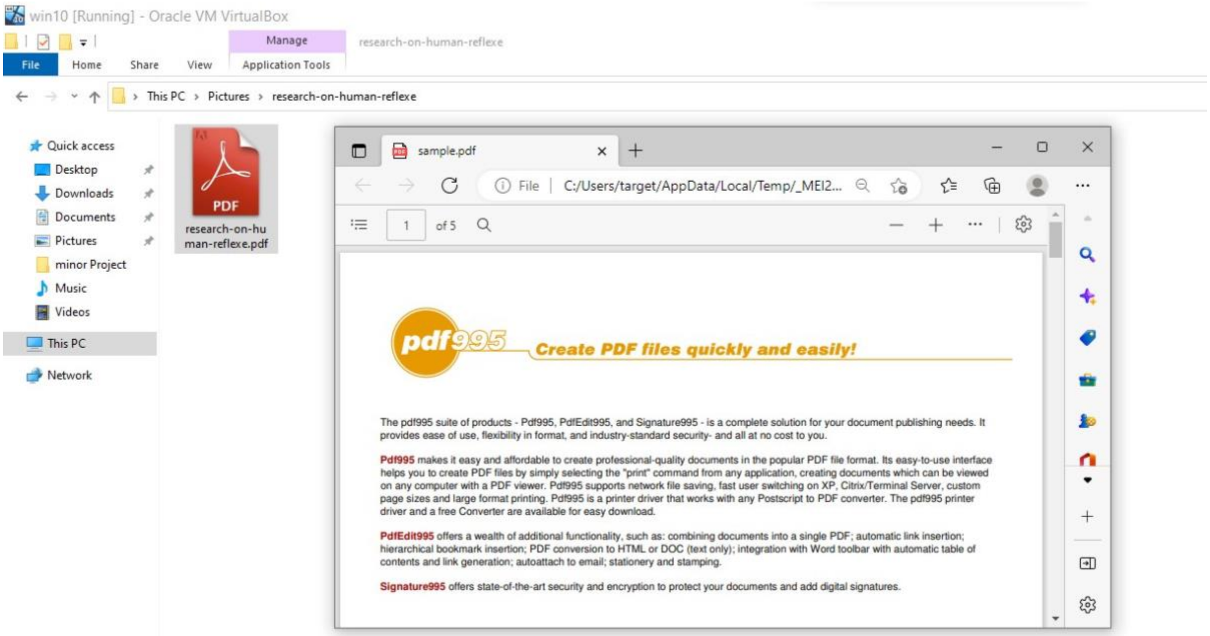
Name	Date modified	Type	Size
Adobe	22-11-2022 19:30	File folder	
Microsoft	30-11-2022 22:59	File folder	
Windows Expolrer.exe	02-12-2022 21:05	Application	7,175 KB





File Explorer

Open new windows, change advanced folder and search options, and more.


win10 [Running] - Oracle VM VirtualBox
Manage
research-on-human-reflexe
File
Home
Share
View
Application Tools
This PC › Pictures › research-on-human-reflexe
Quick access
Desktop
Downloads
Documents
Pictures
minor Project
Music
Videos
This PC
Network
PDF
research-on-human-reflexe.pdf
sample.pdf
File
C:/Users/target/AppData/Local/Temp/_MEI2...
1
of 5

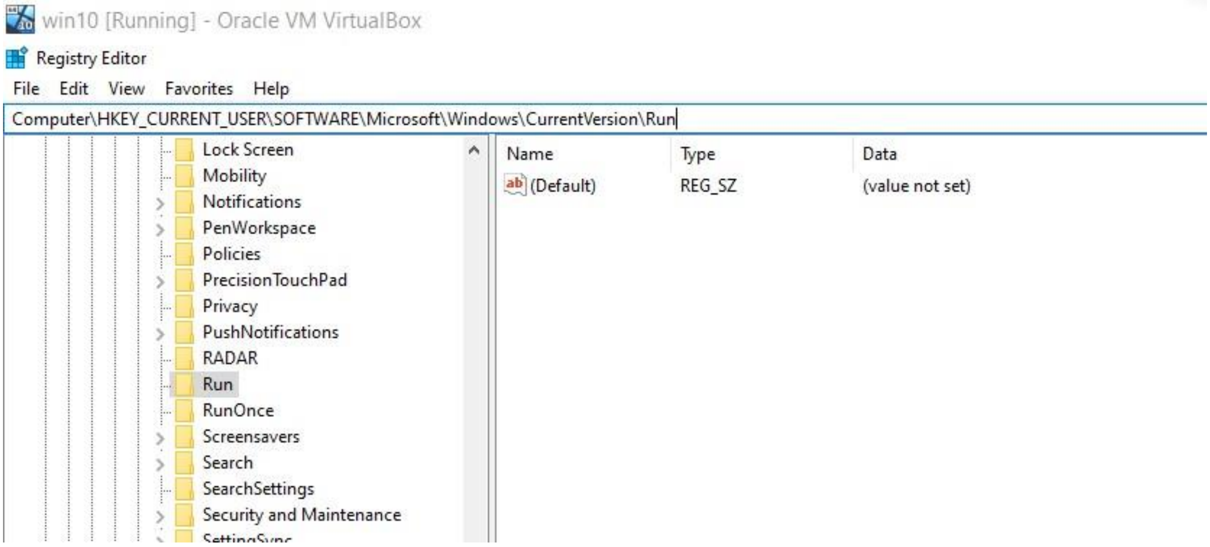
pdf995 Create PDF files quickly and easily!

The pdf995 suite of products - Pdf995, PdfEdit995, and Signature995 - is a complete solution for your document publishing needs. It provides ease of use, flexibility in format, and industry-standard security- and all at no cost to you.

Pdf995 makes it easy and affordable to create professional-quality documents in the popular PDF file format. Its easy-to-use interface helps you to create PDF files by simply selecting the "print" command from any application, creating documents which can be viewed on any computer with a PDF viewer. Pdf995 supports network file saving, fast user switching on XP, Citrix/Terminal Server, custom page sizes and large format printing. Pdf995 is a printer driver that works with any Postscript to PDF converter. The pdf995 printer driver and a free Converter are available for easy download.

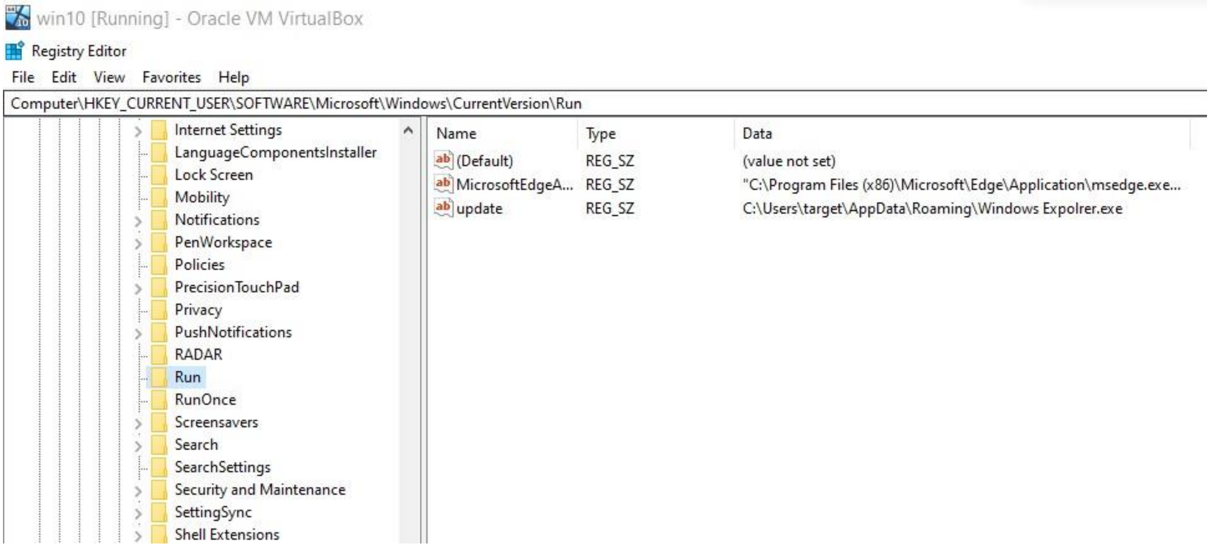
PdfEdit995 offers a wealth of additional functionality, such as: combining documents into a single PDF; automatic link insertion; hierarchical bookmark insertion; PDF conversion to HTML or DOC (text only); integration with Word toolbar with automatic table of contents and link generation; autoattach to email; stationery and stamping.

Signature995 offers state-of-the-art security and encryption to protect your documents and add digital signatures.



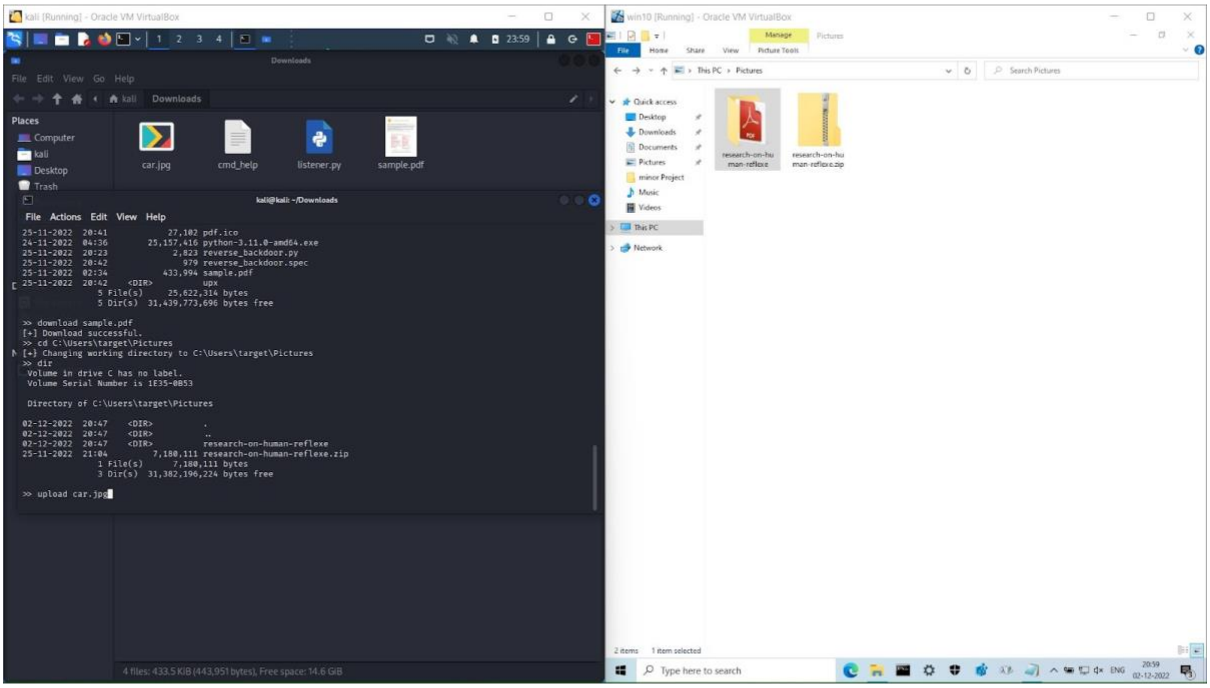
Computer\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Name	Type	Data
(Default)	REG_SZ	(value not set)

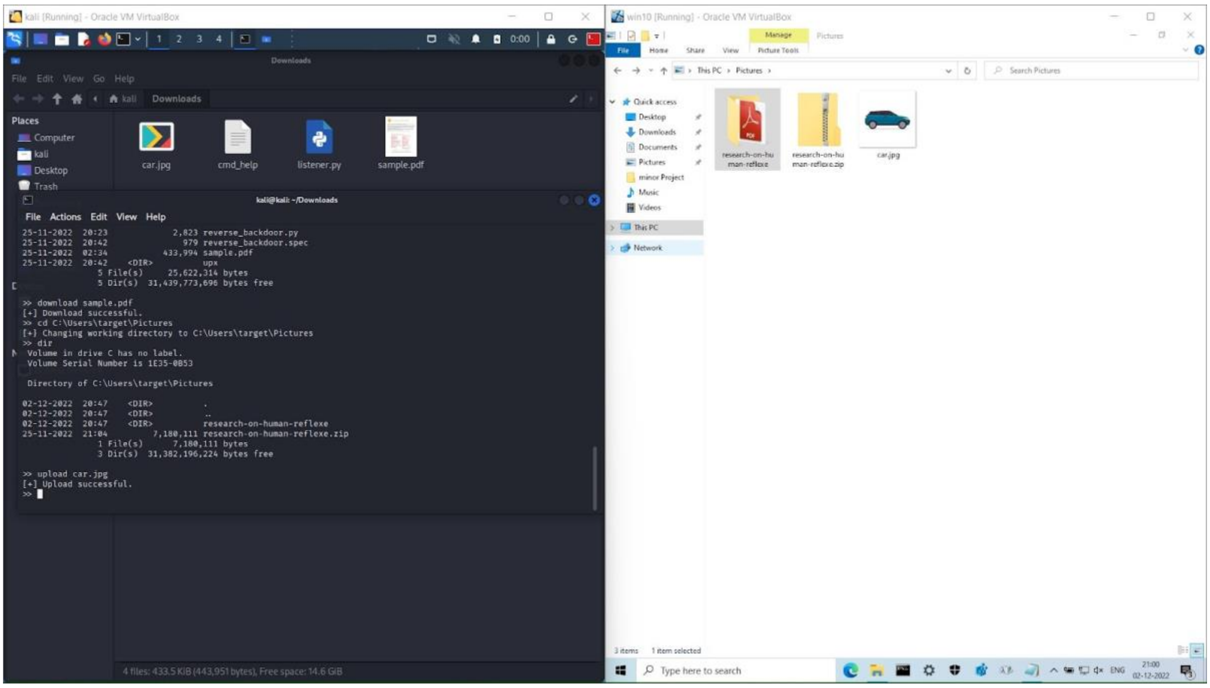


Computer\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Name	Type	Data
(Default)	REG_SZ	(value not set)
MicrosoftEdgeA...	REG_SZ	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe...
update	REG_SZ	C:\Users\target\AppData\Roaming\Windows Expolrer.exe



```
25-11-2022  20:41            27,102 pdf.ico
24-11-2022  04:36        25,157,416 python-3.11.0-amd64.exe
25-11-2022  20:23             2,823 reverse_backdoor.py
25-11-2022  20:42               979 reverse_backdoor.spec
25-11-2022  02:34           433,994 sample.pdf
25-11-2022  20:42    <DIR>          upx
               5 File(s)     25,622,314 bytes
               5 Dir(s)  31,439,773,696 bytes free

>> download sample.pdf
[+] Download successful.
>> cd C:\Users\target\Pictures
[+] Changing working directory to C:\Users\target\Pictures
>> dir
 Volume in drive C has no label.
 Volume Serial Number is 1E35-0B53

 Directory of C:\Users\target\Pictures

02-12-2022  20:47    <DIR>          .
02-12-2022  20:47    <DIR>          ..
02-12-2022  20:47    <DIR>          research-on-human-reflexe
25-11-2022  21:04         7,180,111 research-on-human-reflexe.zip
               1 File(s)      7,180,111 bytes
               3 Dir(s)  31,382,196,224 bytes free

>> upload car.jpg
```



```
25-11-2022  20:23             2,823 reverse_backdoor.py
25-11-2022  20:42               979 reverse_backdoor.spec
25-11-2022  02:34           433,994 sample.pdf
25-11-2022  20:42    <DIR>          upx
               5 File(s)     25,622,314 bytes
               5 Dir(s)  31,439,773,696 bytes free

>> download sample.pdf
[+] Download successful.
>> cd C:\Users\target\Pictures
[+] Changing working directory to C:\Users\target\Pictures
>> dir
 Volume in drive C has no label.
 Volume Serial Number is 1E35-0B53

 Directory of C:\Users\target\Pictures

02-12-2022  20:47    <DIR>          .
02-12-2022  20:47    <DIR>          ..
02-12-2022  20:47    <DIR>          research-on-human-reflexe
25-11-2022  21:04         7,180,111 research-on-human-reflexe.zip
               1 File(s)      7,180,111 bytes
               3 Dir(s)  31,382,196,224 bytes free

>> upload car.jpg
[+] Upload successful.
>>
```

Chapter – 6

- **Results -** Once a system has been compromised with a backdoor or Trojan horse, such as the Trusting Trust compiler, it is very hard for the "rightful" user to regain control of the system – typically one should rebuild a clean system and transfer data (but not executables) over. However, several practical weaknesses in the Trusting Trust scheme have been suggested. For example, a sufficiently motivated user could painstakingly review the machine code of the untrusted compiler before using it. As mentioned above, there are ways to hide the Trojan horse, such as subverting the disassembler; but there are ways to counter that defense, too, such as writing a disassembler from scratch.

- **Conclusion** - Continuous Monitoring of Security System: Monitoring the system network helps in checking loopholes that may turn into potential entry points for backdoor attacks. Having Strong firewalls in Computer Network: Firewall filters the traffic in a computer network and a strong firewall can prevent attackers from getting into the system. Protection of computer networks through Strong Passwords: Having a strong password helps in establishing the strong security of the system. Users should never stick to default passwords and should always have passwords that are difficult to crack.

- **Further Work on Backdoor-**Deep learning models are known to be vulnerable to various adversarial manipulations of the training data, model parameters, and input data. In particular, an adversary can modify the training data and model parameters to embed backdoors into the model, so the model behaves according to the adversary's objective if the input contains the backdoor features (e.g., a stamp on an image). The poisoned model's behaviour on clean data, however, remains unchanged. Many detection algorithms are designed to detect backdoors on input samples or model activation functions, in order to remove the backdoor. These algorithms rely on the statistical difference between the latent representations of backdoor-enabled and clean input data in the poisoned model. In the future work, we design an adversarial backdoor embedding algorithm that can bypass the existing detection algorithms including the state-of-the-art techniques. We design a strategic adversarial training that optimizes the original loss function of the model, and also maximizes the indistinguishability of the hidden representations of poisoned data and clean data. We show the effectiveness of our attack on multiple datasets and model architectures. This work calls for designing adversary-aware defence mechanisms for backdoor detection algorithms.

REFERENCES

- **https://www.geeksforgeeks.org/**
- **https://www.geeksforgeeks.org/python-sys-module/**
- **https://www.geeksforgeeks.org/encoding-and-decoding-base64-strings-in-python/**
- **https://ieeexplore.ieee.org/document/8614801**
- **https://www.imperva.com/learn/application-security/backdoor-shell-attack/**
- **https://www.wallarm.com/what/what-is-a-backdoor-attack**
- **https://arxiv.org/pdf/2007.08745.pdf**
- **https://www.wordfence.com/learn/finding-removing-backdoors/**
- **https://www.elastic.co/security-labs/a-peek-behind-the-bpfdoor**
- **https://www.malwarebytes.com/backdoor**
- **https://study.com/academy/lesson/what-is-a-backdoor-virus-definition-removal-example.html**
- **https://www.trendmicro.com/vinfo/us/security/definition/backdoor**
- **https://techterms.com/definition/backdoor**
- **https://www.google.com/amp/s/www.cybereason.com/blog/case-study-software-company-detects-and-closes-year-old-webmail-server-backdoor%3fhs_amp=true**
- **https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.osti.gov/servlets/purl/1266888&ved=2ahUKEwj26Ia9meD7AhWo4nMBHdwLAOo4ChAWegQIBRAB&usg=AOvVaw36G1qrWuNg2C7h760yiaOn**
- **https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.andrew.cmu.edu/user/md4l/practices/documents/CSSC-CaseStudy-001.pdf&ved=2ahUKEwj9hP6hmuD7AhX__3MBHSbGCF8QFnoECCcQAQ&usg=AOvVaw1InUlt5PBAFN7oALjy3tTN**
- **https://www.thecasesolutions.com/building-a-backdoor-to-the-iphone-an-ethical-dilemma-2-150533**