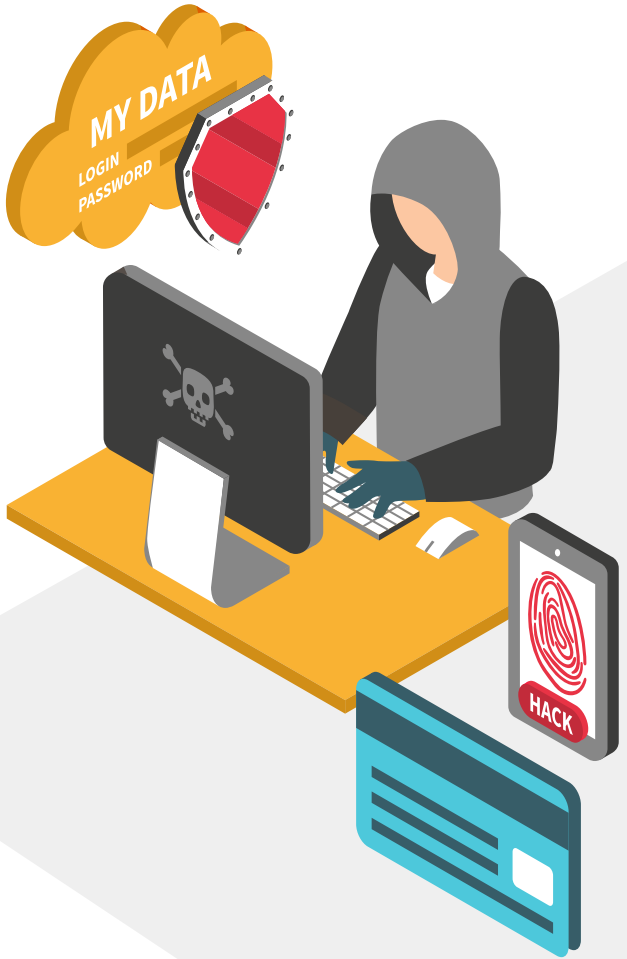
MALWARE CREATION, ANALYSIS AND EXPLOITATION IN VIRTUAL ENVIRONMENT



Jnyandeep (HU21CSEN0101342)

TABLE OF CONTENTS

01
INTRODUCTION
Introduction to cybersecurity

02
VIRTUALIZATION
Creating virtual machines

03
MALWARE CREATION
Types and creation of malware

04
EXPLOITATION
MySQL database exploitation

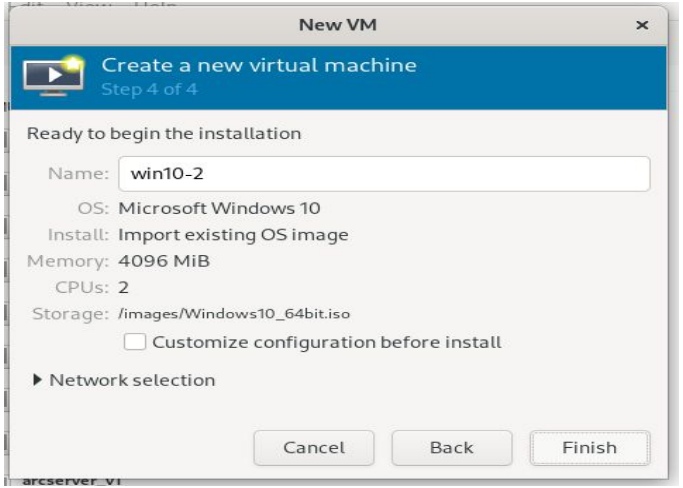
05
ANALYSIS
Different types of analysis and frameworks

06
CONCLUSION
Importance of this project

INTRODUCTION

Cybersecurity involves protecting computer systems, networks, and data from digital attacks, unauthorized access, and damage.

VIRTUALIZATION



VIRTUAL MACHINE(WINDOWS 10)

DESCRIPTION

Creating a virtual version of hardware, storage, or network resources.

ADVANTAGES

1. Enhanced security
2. Resource Optimization
3. Flexibility

INTRODUCTION TO MALWARE

TROJANS

Disguised as legitimate software.

VIRUSES

Replicate by attaching to other programs.

WORMS

Self-replicating and spread independently.

RANSOMWARE

Encrypts files and demands ransom.

SPYWARE

Secretly monitors activities.

ADWARE

Displays unwanted advertisements.

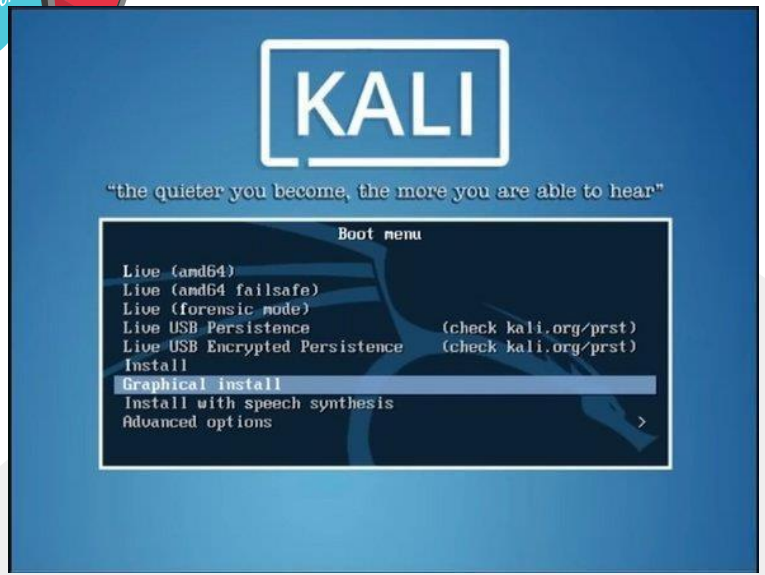
MALWARE CREATION WITH BATCH FILES

Batch files are text files containing a series of commands executed by the command-line interpreter.Often used to automate repetitive tasks, including malicious activities.

Example:To stop someone's internet access.
Code:**@Echo off**
pconfig /release

KALI IINUX

Kali Linux is a Debian-based Linux distribution designed for digital forensics and penetration testing.Comes with numerous pre-installed tools for security testing. Widely used by cybersecurity professionals for ethical hacking and security assessments.



EXPLOITATION OF MySQL USING KALI

OVERVIEW

MySQL is a widely-used database management system, which can be targeted for exploitation if misconfigured or vulnerable.

TOOLS

Metasploit

STEPS

1. Scan for MySQL Server
2. Identify MySQL Version
3. Brute Force Attack
4. Exploit with Metasploit

POST-EXPLOITATION

Access databases and tables.Extract sensitive information or upload a backdoor for persistent access.

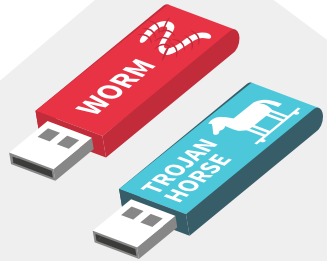
MALWARE ANALYSIS

STATIC ANALYSIS

- Examination of code or binaries without executing them.
- Uses tools like virustotal, IDA for code review.
- Detects vulnerabilities early in the development cycle.
- Provides a comprehensive code review.

DYNAMIC ANALYSIS

- Analysis by executing code in a controlled environment.
- Uses tools like Cuckoo Sandbox for monitoring.
- Identifies runtime errors and detects malicious behavior
- Requires a controlled environment and is more time-consuming



Using Virustotal(Static)

Access VirusTotal

Open and navigate to VirusTotal website

1

Upload the File

Click "Choose file" and select file

2

Submit the File

Click "Confirm upload" to start analysis

3

Analyze Results

Review scan results from multiple antivirus engines

4

Review

Explore file behavior, comments, and history

5

Using Cuckoo Sandbox(Dynamic)

Install Cuckoo Sandbox

Download and install Cuckoo Sandbox software

1

Set Up Environment

Configure virtual machines for isolated analysis

2

Submit the File

Upload the suspicious file to Cuckoo

3

Run Analysis

Execute file within the sandbox environment

4

Review

Examine detailed analysis results and logs

5

MITRE ATT&CK FRAMEWORK

PURPOSE

Helps organizations understand and combat cybersecurity threats

COMPONENTS

Consists of tactics, techniques, and procedures (TTPs)

USAGE

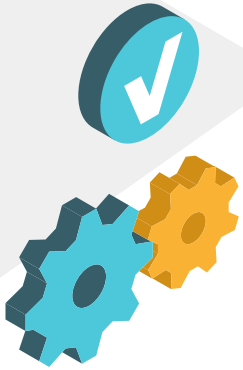
Used for threat detection, response, and mitigation

BENEFITS

Enhances security posture and incident response capabilities

Understanding cybersecurity, virtualization, and malware is crucial for safeguarding digital environments. Continuous learning ensures we can defend against emerging threats and optimize resource use.

—CONCLUSION



THANK YOU