INTRODUCTION

Cyber security refers to every aspect of protecting an organization and its employees and assets against cyber threats. As cyberattacks become more common and sophisticated and corporate networks grow more complex, a variety of cyber security solutions are required to mitigate corporate cyber risk.

Malware Analysis is the practice of determining and analyzing suspicious files on endpoints and within networks.

ABSTRACT

The purpose of malware analysis is to obtain and provide the information needed to rectify a network or system intrusion.

When we analyze potential malware, the intended result is typically

to determine what a suspected malware can do,

how to detect it once it is in our network, and

how to measure and contain the damage.

Once we identify which files require full analysis, we develop signatures to detect malware infections on our network.

PROBLEM STATEMENT

To analyze a provided malware sample and identify its behaviour, functionality, and potential impact

They will also be required to suggest countermeasures and best practices to prevent future attacks.

TYPES OF MALWARE

Malware, or malicious software, is a term for any kind of computer software with malicious intent.

Ransomware is software that uses encryption to disable a target’s access to its data until a ransom is paid.

Fileless malware makes changes to files that are native to the operating system, such as PowerShell or WMI.

Spyware collects information about users’ activities without their knowledge or consent.

Adware tracks a user’s surfing activity to determine which ads to serve them

A Trojan disguises itself as desirable code or software. Once downloaded, the Trojan can take control of victims’ systems for malicious purposes.

Worms target vulnerabilities in operating systems to install themselves into networks.

A virus is a piece of code that inserts itself into an application and executes when the app is run.

A rootkit is software that gives malicious actors remote control of a victim’s computer with full administrative privileges.

MALWARE ANALYSIS

The study or process of determining the functionality, origin and potential impact of a given malware sample .Malware or malicious software is any computer software intended to harm the host operating system or to steal sensitive data from users, organizations or companies.

Malware may include software that gathers user information without permission.

TYPES OF MALWARE ANALYSIS

Basic static analysis does not require that the code is actually run. Instead, static analysis examines the file for signs of malicious intent. It can be useful to identify malicious infrastructure, libraries or packed files.

Technical indicators are identified such as file names, hashes, strings such as IP addresses, domains, and file header data can be used to determine whether that file is malicious.

Dynamic malware analysis executes suspected malicious code in a safe environment called a sandbox. This closed system enables security professionals to watch the malware in action without the risk of letting it infect their system or escape into the enterprise network.

Dynamic analysis provides threat hunters and incident responders with deeper visibility, allowing them to uncover the true nature of a threat

Reverse Engineering malware involves disassembling a software program. Through this process, binary instructions are converted to code mnemonics so that engineers can look at what the program does and what systems it impacts. Only by knowing its details are engineers then able to create solutions that can mitigate the program’s intended malicious effects.

STEPS FOR MALWARE ANALYSIS

Before the actual analysis, you need access to a malicious piece of code in an uncompressed format.

A malware analysis lab is a safe environment where you can test different malware functionalities without any risk to nearby files.

You can use several tools to analyze malware, including open-source and paid options. There is plenty of support to be found on GitHub.

Before running the malware, assess the operating environment and document it as your baseline.

There are several phases involved in the investigation step. Some require intense manual involvement, while others can gain from automation tools.

Depending on the tools you’re using, you will have detailed information on malware behavior, tendencies, and interaction patterns with its surrounding digital environment.