Practical 4

What is malware?
malware, or malicious software, is any program or file that is intentionally harmful to a computer network or server.

Types of malware include computer viruses, worms, Trojan horses ransomware and spyware

What does malware do?
malware can infect networks and devices and is designed to harm those devices, networks and their user in some way. Depending on the type of malware and its goal, this harm might present itself differently to the user or endpoint.

malware can typically perform the following harmful actions:

- Data exfiltration :- Data exfiltration is a common objective of malware. During data exfiltration once a system is infected with malware,

threat actors can steal sensitive information stored on the system is infected information stored on the system, such as emails passwords, intellectual property financial information and login credentials.

Service disruption :- malware can disrupt services in several ways. for example it can lock up computers and make them unusable or hold them hostage for financial gain by peforming a ransomware attack.

Data espionage : A type of malware know as spyware peform data espionage by spying on users. Typically hackers use keyloggers to record keystokes access web cameras and micro-phones and capture screenshots

Identity theft :- malware can be used to steal person data which

can be used to impersonate victims, commit fraud or gain access to additional resources

stealing resources :- malware can use stolen system resources to send spam emails operate botnets and run cryptomining software also know as cryptojacking

system damage :- Cetain types of malware such as computer worms can damage deleting data or changing system settings. This damage can lead to an unstable or unusable system.

Types of malware

Different types of malware have the following unique traits and characteristics.

- Virus :- A virus is the most common type of malware that can execute itself and spread by infecting other program or files.

Worm :- A worm can self-replicate without a host program and typically spreads without any interaction from the malware authors.

Trojan horse :- A Trojan horse is designed to appear as a legitimate software program to gain access to a system.

Spyware :- Spyware collects information and data on the device and user as well as observes that user activity without their knowledge

Ransomware :- Ransomware infects a user's system and encrypts its data.

Rootkit :- A rootkit obtains administrator-level access to the victim's system. once installed, the program gives threat actors root or privileged access to the system.

Backdoor virus :- A backdoor virus or remote access trojan secretly creates a backdoor into an infected computer system that lets threat actors remotely access it without alerting the user or the systems security programs.

Adware :- Adware tracks a user's browser and download history with the intent to display pop-up or banner advertisements that lure the user into making a purchase.

Keyloggers :- Keyloggers, also called system monitors, tracks nearly everything a user does on their computer. This includes writing emails, opening webpages, accessing computer programs and typing keystrokes.

Logic bombs :- This type of malicious malware is designed to cause harm and typically gets inserted

into a system once specific condition are met.

Exploits :- computer exploits take advantage of existing vulnerabilities flaws or weaknesses in a system's hardware or software

How to remove malware and which tools to use

many security sofware products are designed to detect and prevent malware as well as remove it from infected system.

Bitdefender Gravity Zone :- This tool offers an intuitive risk analysis engine That protects agaunt malware attacks

Cisco secure Endpoint :- Formerly known as Cisco Amp for Endpoints It uses advanced threat detection techniques

ESET Protect :- ESET protect provides endpoint protection agints various threats such as malware, ransomware and viruses.

F-secure Total :- F-secure Total is a comprehensive internet security suite that provides internet security, virtual private network and password management in one subscription.

Kaspersky premium :- This tool provides endpoint protection automated Threat removal and vpn services

Sophos intercept x :- Sophos x uses a combination of signature-based detection

Symantec Enterprise cloud :- This tool provides data-centric hybrid security for large and complex organization.

ThreatDown Endpoint protection :-
Formerly malwarebytes Endpoint protection, This tool offers a layered protection approach

Trend micro cloud one :- trend micro cloud one is designed to offer protection for various workload, including physical servers, virtual, cloud and containers.

Webroot managed Detection and Response :- Webroot MDR is designed to provide proactive defense against evolving threats. It achieves this through continous monitoring and by using expert analysis and actionable workflows.

Practical 2

IDA Pro :-

IDA pro is a powerful and versatile tool for reverse engineers security researchers and software analysts its robust features such as disassembly, code analysis its pro debugging and support for various processor architectures and file formats enable in-depth analysis and understanding of binary code.

Pratical 3

Types of malware Analysis

There are several types of malware analysis. you can use one or a combination before or after an attack, depending on the situation your organization faces.

Static malware analysis

Static malware analysis looks for files that may harm your system without actively running the malware code, making it a safe tool for exposing malicious libraries or packaged files.

Dynamic malware analysis

Dynamic malware analysis uses a sandbox which is a secure isolated, virtual environment where you can run suspected dangerous code.

Hybrid malware analysis

Hybrid malware analysis combines both static and dynamic techniques. For example if malicious code makes changes to a computer's memory, dynamic analysis can detect that activity. Then static analysis can determine exactly what changes were made.

Practical 4

4 Stages of malware Analysis

You can break down the malware analysis process into four stages.

static properties analysis

static properties refer to strings of code embedded inside the malware file, hashes, header details and metadata.

Interactive behavior analysis

interactive behavior analysis involves a security analyst interacting with malware running in a lab, making observations

regarding its behavior

Fully automated analysis
Fully automated analysis scans suspected malware files using automated tools, focusing on what the malware can do once inside your system.

manual code reversing
manual code reversing breaks down the code used to build the malware to learn how it works and what is capable of doing.

Practical 5

malware analysis use cases

malware analysis can be used in a variety of cybesecurity situation such as

Incident response

For remediation and recovery to be successful, incident response team must move quickly and This is where malware analysis is especially useful.

malware research and detection

To best safeguard your organization identifying malicious code and understanding how it differs from benevolent code is extremely important

Indicator of compromise extration

with malware analysis you can extract indicator of compromise

to better understand how malware can attack your system.

Threat hunting

Threat hunting use malware analysis to identify previously unknown cyberthreats.

Threat alerts and triage

malware analysis enables IT team to better understand how threat work and then use this information to react faster. The right malware analysis tool can send you alerts prioritizing them according to severity.

Practical 6

Tools for malware analysis

several malware analysis tools are available on the market and here are some of the most well-known.

process hacker

Process Hacker enables analysts to understand the processes that are running on any given device on the network.

Fiddler

Fiddler can observe and study malicious traffic because it serves as a proxy accepting and managing network traffic

Limon

Limon is controlled sandbox enviroment for studying malware that attacks Linux system, enabling

IT teams to monitor how the malware behaves and determine what it was designed to do.

pestudio

Pestudio identifies potentially suspicious file by analyzing what is happening on your system.

Ghidra

Ghidra disassemble malware instead of merely identifying it it then takes whatever it finds in the malware code and translates it into something a human can read.

Cuckoo Sandbox

Cuckoo sandbox studies malware in a safe sandbox environement recording its activity and then generating a report.

Crowdstrike Falcon insight

crowdStrike Falcon automatically analyzes malware by combining crowdstrike's Threat intelligence with a sandbox environment.

IDA :-

IDA offers a privilege opportunity to see IDA in action. This light but powerfull tool can quickly analyze the binary code samples and users can save and looks closer at the analysis result

Practical 7

strings command :- Extracts printable characher sequences from binary files

IDA Pro :- A powerful disasemble and debuggyer for static analysis of binary code.

Findcrypt2 :- An IDA pro plugin to identify known cryptographic constants and algorithms

Krypto ANalyzer (KANAL) :- A tool similar to Findcrypt2 for identifying cryptographic routines

Wireshark :- A network protocal andyzer for deep inspection of network packets

Process monitor :- A windows utility that shows real-time file system, Registry and process / thread activity.

Process Hacker :- A free powerful multi-purpose tool that helps you monitor system resources debug software, and detect malware

Frida :- A dynamic instrumentation toolkit for developers, reverse engineers and security researchers to inject scripts into running processes

Practical 8

IDA pro :- A powerful disassembler and debugger for static analysis of binary code.

Wireshark :- A network protocol analyzer for deep inspection and capture of network packets.

Fiddler :- A web debugging proxy used to capture and analyze HTTP / HTTPS network traffic.

Sandbox :- A secure, isolated virtual environment to safely execute and observe malware behavior

Debugger :- A software tool used to analyze and trace RE execution of programs at runtime.