Pract 1:

**What is malware?**

Malware, or malicious software, is any program or file that's intentionally harmful to a computer, network or server.

Types of malware include computer [viruses](https://www.techtarget.com/searchsecurity/definition/virus), worms, Trojan horses, [ransomware](https://www.techtarget.com/searchsecurity/definition/ransomware) and spyware. These malicious programs steal, encrypt and delete sensitive data; alter or hijack core computing functions; and monitor end users' computer activity.

**What does malware do?**

Malware can infect networks and devices and is designed to harm those devices, networks and their users in some way. Depending on the type of malware and its goal, this harm might present itself differently to the user or [endpoint](https://www.techtarget.com/whatis/definition/endpoint-device). In some cases, the effect of malware is relatively mild and benign, and in others, it can be disastrous.

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, such as emails, passwords, intellectual property, financial information and login credentials. Data exfiltration can result in monetary or reputational damage to individuals and organizations.
* **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 performing a ransomware attack. Malware can also target critical infrastructure, such as power grids, healthcare facilities or transportation systems to cause service disruptions.
* **Data espionage.**A type of malware known as [spyware](https://www.techtarget.com/searchsecurity/definition/spyware) performs data espionage by spying on users. Typically, hackers use keyloggers to record keystrokes, access web cameras and microphones and capture screenshots.
* **Identity theft.**Malware can be used to [steal personal data](https://www.techtarget.com/whatis/feature/How-do-cybercriminals-steal-credit-card-information) which can be used to impersonate victims, commit fraud or gain access to additional resources. According to the IBM X-Force Threat Intelligence Index 2024, there was a 71% rise in cyberattacks using stolen identities in 2023 compared to the previous year.
* **Stealing resources.** Malware can use stolen system resources to send spam emails, operate [botnets](https://www.techtarget.com/searchsecurity/definition/botnet) and run cryptomining software, also known as *[cryptojacking](https://www.techtarget.com/whatis/definition/cryptojacking)*.
* **System damage.** Certain types of malware, such as [computer worms](https://www.techtarget.com/searchsecurity/definition/worm), can damage devices by corrupting the system files, 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 programs 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](https://www.techtarget.com/searchsecurity/definition/Trojan-horse) is designed to appear as a legitimate software program to gain access to a system. Once activated following installation, Trojans can execute their malicious functions.
* **Spyware.** Spyware collects information and data on the device and user, as well as observes the user's activity without their knowledge.
* **Ransomware.** Ransomware infects a user's system and encrypts its data. Cybercriminals then demand a ransom payment from the victim in exchange for decrypting the system's data.
* **Rootkit.** A [rootkit](https://www.techtarget.com/searchsecurity/definition/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](https://www.techtarget.com/searchsecurity/definition/back-door) virus or remote access Trojan ([RAT](https://www.techtarget.com/searchsecurity/definition/RAT-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 system's security programs.
* **Adware.** [Adware](https://www.techtarget.com/searchsecurity/definition/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. For example, an advertiser might use cookies to track the webpages a user visits to better target advertising.
* **Keyloggers.** Keyloggers, also called system monitors, track 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 conditions are met. [Logic bombs](https://www.techtarget.com/searchsecurity/definition/logic-bomb) stay dormant and are triggered when a certain event or condition is met, such as when a user takes a specific action on a certain date or time.
* **Exploits.** [Computer exploits](https://www.techtarget.com/searchsecurity/definition/exploit) take advantage of existing vulnerabilities, flaws or weaknesses in a system's hardware or software. Instead of depending on [social engineering](https://www.techtarget.com/searchsecurity/definition/social-engineering) tactics to execute, they exploit technical vulnerabilities to gain unauthorized access and perform other malicious activities such as executing arbitrary code inside a system.

**How to remove malware and which tools to use**

Many security software products are designed to detect and prevent malware, as well as remove it from infected systems. Running antimalware tools is the best option to remove malware.

According to networking expert Andrew Froehlich, Westgate Networks, the following is a sampling of [enterprise-grade antimalware tools](https://www.techtarget.com/searchsecurity/tip/10-antimalware-tools-for-ransomware-protection-and-removal) that include ransomware protection. These tools, which are listed in alphabetical order, are designed for organizations of all sizes:

* **Bitdefender GravityZone.** This tool offers an intuitive risk analysis engine that protects against malware attacks and also ensures adherence to corporate protocols, including patch management, disk encryption and device control.
* **Cisco Secure Endpoint.** Formerly known as Cisco AMP for Endpoints, it uses advanced threat detection techniques, including [machine learning](https://www.techtarget.com/searchenterpriseai/definition/machine-learning-ML) and behavioral analysis, to identify and block malware, ransomware and other malicious activities in real time.
* **ESET Protect.** ESET Protect provides endpoint protection against 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 ([VPN](https://www.techtarget.com/searchnetworking/definition/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, machine learning and behavioral analysis to proactively identify and block malware, ransomware and other cyber threats before they can cause harm to endpoints.
* **Symantec Enterprise Cloud.** This tool provides data-centric hybrid security for large and complex organizations.
* **ThreatDown Endpoint Protection.** Formerly Malwarebytes Endpoint Protection, this tool offers a layered protection approach with simplified security management and scalability options for IT organizations.
* **Trend Micro Cloud One.** Trend Micro Cloud One is designed to offer protection for various workloads, 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 continuous monitoring and by using expert analysis and actionable workflows.

Pract 2:

### **[IDA Pro](https://www.hex-rays.com/products/%20ida" \l ":~:text=IDA%20Pro%20is%20a%20complete,to%20enhance%20IDA%20Pro's%20functionalities.)**

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

Pract 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. Static malware analysis can uncover clues regarding the nature of the malware, such as filenames, hashes, IP addresses, domains, and file header data. The malware can be observed using a variety of tools, such as network analyzers.

### Dynamic malware analysis

Dynamic malware analysis uses a [**sandbox**](https://www.fortinet.com/resources/cyberglossary/what-is-sandboxing), which is a secure, isolated, virtual environment where you can run suspected dangerous code. Security professionals can closely monitor the malware in the sandbox without worrying about infecting the rest of the system or network, allowing them to gather more information about the malware.

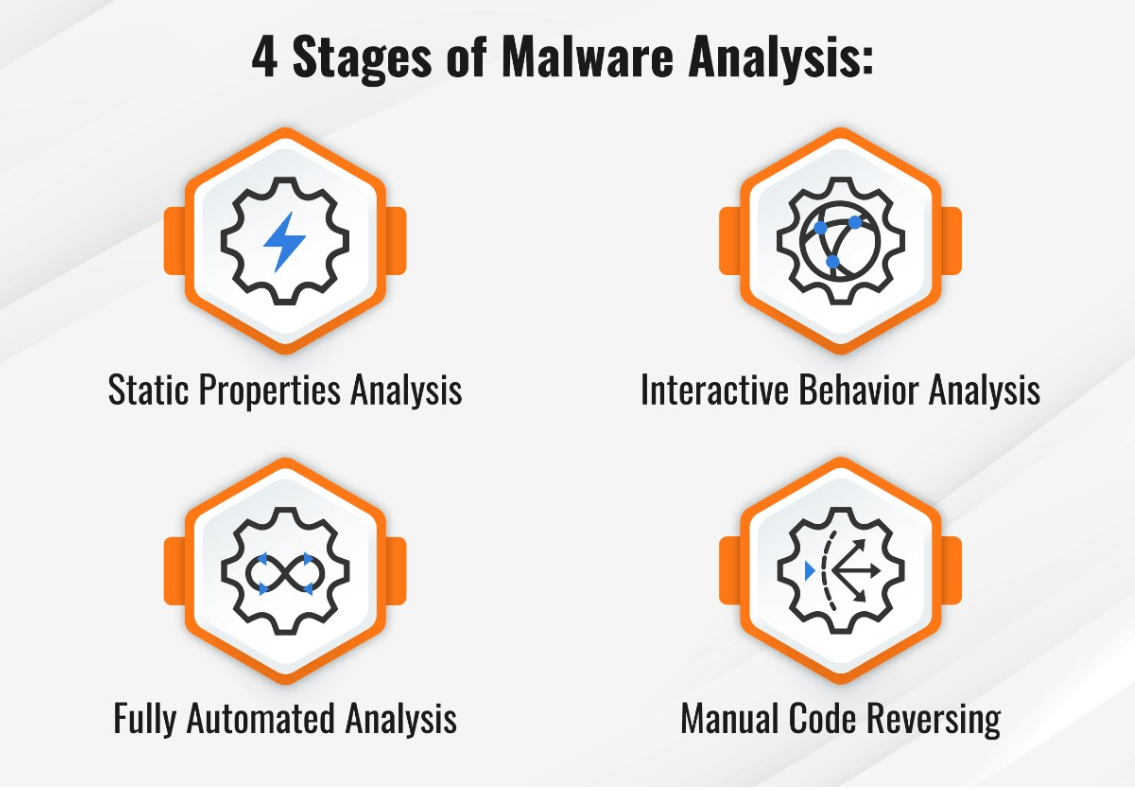
### Hybrid malware analysis

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.

Pract 4:

## 4 Stages of Malware Analysis

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

**[[](https://www.fortinet.com/content/dam/fortinet/images/cyberglossary/types-malware-analysis.png)](https://www.fortinet.com/content/dam/fortinet/images/cyberglossary/types-malware-analysis.png)**

**[Click to See Larger Image](https://www.fortinet.com/content/dam/fortinet/images/cyberglossary/types-malware-analysis.png)**

### Static properties analysis

Static properties refer to strings of code embedded inside the malware file, hashes, header details, and metadata. Static properties analysis provides a quick and easy way to gather helpful information about malware because the malware does not have to be executed for you to study it.

### Interactive behavior analysis

Interactive behavior analysis involves a security analyst interacting with malware running in a lab, making observations regarding its behavior. In this way, you can better understand how malware uses different elements of a computer system, such as its memory.

### Fully automated analysis

Fully automated analysis scans suspected malware files using automated tools, focusing on what the malware can do once inside your system. After the analysis, you get a report outlining the potential damage to assets connected to your network.

### Manual code reversing

Manual code reversing breaks down the code used to build the malware to learn how it works and what it is capable of doing. This is a time-consuming process that requires significant skill. However, when used correctly, manual code reversing can reveal valuable information about the malware.

Pract 5:

## Malware Analysis Use Cases

Malware analysis can be used in a variety of cybersecurity situations, such as:

### Incident response

For remediation and recovery to be successful, [**incident response**](https://www.fortinet.com/resources/cyberglossary/incident-response) teams must move quickly, and this is where malware analysis is especially useful. By giving incident responders applicable information for ongoing and upcoming incidents, malware analysis enables them to contain and prevent attacks.

### Malware research and detection

To best safeguard your organization, identifying malicious code and understanding how it differs from benevolent code is extremely important. For example, by knowing which sites transmit malicious code, you can blacklist websites that propagate threats.

### Indicator of Compromise (IOC) extraction

With malware analysis, you can extract [**indicators of compromise (IOCs)**](https://www.fortinet.com/resources/cyberglossary/indicators-of-compromise) to better understand how malware can attack your system. An IOC is data indicating that a system breach or attack has occurred. You can use this data to understand how your system reacts to attacks, making it easier to detect attacks in the future.

### Threat hunting

[**Threat hunters**](https://www.fortinet.com/resources/cyberglossary/threat-hunting) use malware analysis to identify previously unknown cyberthreats. For example, if you set up a honey trap, which is designed to attract malware and confine it to a homeless area of your network, you can study how the malware behaves and potentially discover a new threat. Using malware analysis in this way may reveal threats that can get past your defenses.

### Threat alerts and triage

Malware analysis enables IT teams to better understand how threats work and then use this information to react faster. The right malware analysis tool can send you alerts, prioritizing them according to severity. This way, instead of wasting time tracking down false positives, your security team can focus their energies on the threats that really matter.

Pract 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. This can be very useful as you allow malware to execute because you can watch the processes it impacts. With this information, you can determine how different computers react when malware is introduced to your system.

### Fiddler

Fiddler can observe and study malicious traffic because it serves as a proxy, accepting and managing network traffic. Running Fiddler enables malware analysts to study the code and locate the hardcoded malicious sites that will be used to download the malware.

### Limon

Limon is a controlled sandbox environment for studying malware that attacks Linux systems, enabling IT teams to monitor how the malware behaves and determine what it was designed to do.

### PeStudio

PeStudio identifies potentially suspicious files by analyzing what is happening on your system. After it identifies malicious files, it quarantines them and assigns each a hash. You can then use each hash to access the malware and run it in a safe environment to learn how it behaves.

### Ghidra

Ghidra disassembles 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. In this way, it shows you what the malware designer might have been thinking while writing the malicious code.

### Cuckoo sandbox

Cuckoo Sandbox studies malware in a safe sandbox environment, recording its activity and then generating a report. This provides IT teams with data outlining how the malware attempts to impact your system.

### CrowdStrike Falcon insight

CrowdStrike Falcon automatically analyzes malware by combining CrowdStrike’s threat intelligence with a sandbox environment. By comparing the malware’s behavior in the sandbox to information from CrowdStrike’s threat intelligence, Falcon Insight can determine whether the malware already exists or is new to the threat landscape.

[IDA](https://hex-rays.com/ida-free/):

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