SCHOOL OF COMPUTER SCIENCE

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
DEHRADUN, UTTARAKHAND

DIGITAL FORENSICS

ASSIGNMENT FILE - 4

(2024-2025)

For

Vth Semester

Submitted To:
Prof. Subhranil Das
Assistant Professor S.S.
[Vth Semester]
School of Computer Sciences

Submitted By:
Mr. Akshat Negi
500106533(SAP ID)
R2142220414(Roll No.)
B.Tech. CSF (Batch-1)

ASSIGNMENT FILE – 4

1. ***Compare and contrast static analysis and dynamic analysis in the context of malware analysis.***

Static analysis and dynamic analysis are two core methodologies used in malware analysis. Each has its advantages, limitations, and use cases, depending on the level of detail and safety required. Here's a comparison and contrast between the two:

1. Static Analysis

Definition:

- Static analysis involves examining the malware's code, structure, or binary without executing it.

Key Techniques:

- **Disassembly**: Decompiling the binary code to view assembly instructions.
- **Strings Analysis**: Searching for readable strings within the binary that might reveal clues like URLs, IP addresses, or commands.
- **Dependency Analysis**: Examining the imports and exports to identify APIs or libraries used.
- **Control Flow Graph Analysis**: Understanding the logical flow of the program.

Advantages:

- **Safety**: It doesn't require execution, avoiding potential harm to the analysis environment.
- **Speed**: Faster for identifying known signatures or obvious indicators of compromise (IOCs).
- **Comprehensive Code Insight**: Provides an overview of the malware's capabilities by analyzing its code.

Limitations:

- **Evasion Techniques**: Malware may use obfuscation, encryption, or packing to hide its true functionality.
- **No Runtime Behaviour Insights**: Cannot reveal dynamic behaviour like network activity or interaction with the environment.

2. Dynamic Analysis

Definition:

- Dynamic analysis involves executing the malware in a controlled environment (sandbox or virtual machine) to observe its behaviour in real-time.

Key Techniques:

- **Behaviour Monitoring**: Tracking file modifications, registry changes, network connections, and system calls.

- **Network Traffic Analysis**: Observing communication with command-and-control (C&C) servers.
- **Memory Dump Analysis**: Capturing runtime data from memory for deeper inspection.

Advantages:

- **Runtime Behaviour Insight**: Reveals how the malware operates and its interaction with the host system and network.
- **Bypasses Obfuscation**: Execution often exposes hidden functionality or dynamically decrypted code.
- **Identifies Unknown Threats**: Effective against novel or polymorphic malware.

Limitations:

- **Risk**: Potentially dangerous if the malware escapes the controlled environment.
- **Resource-Intensive**: Requires setting up and maintaining isolated environments.
- **Limited by Anti-Analysis Features**: Some malware detects sandbox environments and alters its behaviour to evade detection.

Comparison Summary:

Aspect	**Static Analysis**	**Dynamic Analysis**
Execution Requirement	Not required	Required
Safety	Safer, no execution needed	Riskier, requires strict containment
Time Efficiency	Faster for initial triage	Slower, due to execution and observation
Behaviour Insights	Limited to code capabilities	Full insight into runtime behavior
Evasion Resistance	Susceptible to obfuscation and packing	Can uncover obfuscated/dynamic functionality
Setup Complexity	Requires tools for code analysis	Needs controlled sandbox environments

Conclusion:

Static analysis is best for quickly understanding the structure of malware and identifying initial IOCs, while dynamic analysis is ideal for uncovering runtime behaviors and detecting more sophisticated threats. A combined approach often yields the most comprehensive understanding of malware.

2. ***Explain the process of behavioral analysis in malware investigation.***

Behavioral analysis in malware investigation involves executing a malware sample in a controlled and isolated environment to observe its runtime behavior. This process begins with setting up a secure environment, such as a sandbox or virtual machine, to prevent the malware from causing unintended harm. Analysts use monitoring tools to track the malware's interactions with the host system, including changes to files, processes, registry keys, and system services. Network monitoring tools are employed to observe outbound communication, such as attempts to contact command-and-control (C&C) servers, identify protocols and ports used, and analyze data payloads. Memory snapshots may be taken during execution to uncover decrypted code, hidden processes, or additional payloads. Throughout this process, analysts document Indicators of Compromise (IOCs), such as IP addresses, domains, file paths, and registry keys, while being mindful of anti-analysis techniques employed by the malware, like sandbox detection or delayed execution. This detailed understanding of the malware's behavior helps inform mitigation strategies, incident response, and the development of detection mechanisms.

3. ***Describe the role of network forensics in detecting and mitigating network intrusions.***

Network forensics plays a critical role in detecting and mitigating network intrusions by analyzing network traffic to identify suspicious activities, trace the origin of attacks, and gather evidence for response and prevention. It involves capturing, recording, and analyzing network packets to uncover malicious activities such as unauthorized access, data exfiltration, and malware communications.

Network forensics tools, such as packet sniffers, intrusion detection systems (IDS), and traffic analyzers, are used to monitor traffic in real-time and retrospectively. By analyzing patterns in network data, analysts can identify anomalies like unusual traffic spikes, connections to known malicious domains, or the use of non-standard ports. These insights help detect ongoing intrusions or attempts at lateral movement within a network.

Once an intrusion is detected, network forensics aids in mitigation by providing actionable intelligence. Analysts can trace the attack's source, isolate compromised devices, and block malicious IP addresses or domains. The forensic data also serves as evidence for legal proceedings and is used to refine security policies and rules to prevent future breaches. Overall, network forensics is an essential component of an organization's cybersecurity strategy, enabling timely detection, effective response, and continuous improvement of network defenses.