Indian Institute of Technology Kanpur

Proposal for a New Course

1. Course No: A **200 level** number requested**.**
2. Course Title: **Malware Analysis**
3. No. of Lectures per week: 0 (L), Tutorial: 1 (T), Laboratory: 3 (P), Additional Hours: 3 (A),

   Credits (3*L+2*T+P+A): 08 Duration of Course: Full Semester
4. Proposing Department/IDP : WSAIS

   Other Departments/IDPs which may be interested in the proposed course: CSE

   Other faculty members interested in teaching the course: Somitra Sanadhya, Manindra Agrawal
5. Proposing Instructor: DUGC (WSAIS)
6. Course Description:

A) Objectives: The objective of this practical-based course is to impart hands-on training in malware analysis, including malware fundamentals, safe malware handling, static and dynamic analysis, memory and network-based analysis, basic reverse engineering concepts, and malware reporting, using standard tools and safe analysis methodologies.

B) Contents: **(for 13 weeks of labs, tutorials, and additional work)**

S. No	Type	Broad Title	Topics	Tools	Duration
1	Theory	Introduction to Malware & Forensics Lab Setup and Safety	Malware concepts and lifecycle, Threat landscape overview, Importance of isolation, snapshots, and safety controls, Legal and ethical boundaries of malware handling	Manual	1 Hour

	Practical	Lab 1: Malware & Forensics Lab Setup	**Objectives:** Understand safe malware lab design and isolation principles. Configure isolated virtual environments. Establish operational safety and legal compliance. **No live malware execution outside the controlled lab environment.** **Tasks:** Create Windows analysis VM. Create Linux utility VM (network tools only). Configure host-only networking and isolation. Disable clipboard and drag-and-drop. Install Wireshark, Autopsy, Sysinternals tools. Take baseline snapshots and document safety rules.	VirtualBox, Autopsy, Wireshark, Sysinternals	3 Hours
2	Theory	Malware Types, Infection Vectors & Identification Basics	Malware delivery mechanisms (phishing, drive-by, supply chain). Malware classification: virus, worm, trojan, ransomware, spyware, botnets, rootkits. Early indicators of malicious files.	Manual	1 Hour
	Practical	Lab 2: Malware Identification & Artefact Awareness	**Objectives:** Identify suspicious files using basic indicators. Understand hash-based identification limits. **Tasks:** Copy the given suspicious executable into the analysis VM Generate MD5 and SHA-256 hashes. Compare hash values using Virus Total, Identify filename, size, and entropy anomalies. Instructor-led VirusTotal demonstration (read-only).	Open-source hash tools, VirusTotal (demo only)	3 Hours

			Discuss false positives and reputation limits.		
3	Theory	Malware Analysis Methodology & Initial Triage	Static vs dynamic vs memory analysis. Triage decision-making under time constraints. IOC concepts and prioritisation.	Manual	1 Hour
	Practical	Lab 3: Windows Triage & Evidence Collection	**Objectives:** Perform live system triage. Collect volatile and logical evidence safely. **Tasks:** Capture running processes, users, and network connections. Collect logs, browser artefacts, and user directories. Document chain-of-custody and triage notes.	Autopsy, Windows built-in tools	3 Hours
4	Theory	Static Malware Analysis I – File Structure	PE file format overview. Headers, sections, imports, timestamps. Limits of static analysis.	Manual	1 Hour
	Practical	Lab 4: Static Analysis – File Profiling	**Objectives:** To perform static malware analysis using REMnux tools in order to: • Identify file type and structure • Extract metadata and strings • Detect obfuscation and packing • Analyze documents, scripts, and binaries without	Tools under REmnux • file • stat • hashdeep • ssdeep • imphas • strings • rabin2 • floss • grep / egrep • bulk_extractor • peframe • pefile • bulk_extractor • yara	3 Hours

			execution **Tasks:** • Installation of REmnux VM • File Identification & Hashing • Strings Analysis • Metadata Analysis, • Packed & Obfuscated File Detection, • PE Header Analysis, • URL & IP Extraction, • Entropy Analysis	• 7z • pdfid	
5	Theory	Static Malware Analysis II – Packing & Obfuscation	Packers and obfuscation techniques. Entropy-based detection. Signature detection limitations. Introduction to YARA.	Manual	1 Hour
	Practical	Lab 5: Packing Detection & YARA Introduction	**Objectives:** Identify packed binaries. Introduce detection logic using YARA. **Tasks:** Perform entropy analysis. Identify packed sections and suspicious strings. Draft simple YARA rules.	REmnux VM, Detect It Easy (DiE), YARA	3 Hours
6	Theory	Dynamic Malware Analysis I – Runtime Behaviour	Runtime execution model. Sandboxing concepts. Process, file, and registry monitoring.	Manual	1 Hour
	Practical	Lab 6: Dynamic Analysis – Host Behaviour	**Objectives:** To analyze **runtime behavior of suspicious files** on a Windows system by observing: • Process creation • File system changes • Registry	Tools available in FLARE-VM: • Process Monitor • Process Explorer • Regshot • Autoruns • TCPView • Fake malware samples / test binaries	3 Hours

			modifications • Network activity • Persistence techniques **Tasks:** Install Flare VM for Dynamic Analysis, Restore VM snapshot. Execute sample in isolation. Monitor process, file, and registry activity. Summarise observed behaviour.		
7	Theory	Dynamic Malware Analysis II – Persistence & Internals	Persistence mechanisms. Services, autoruns, scheduled tasks. Introductory Windows internals for malware.	Manual	1 Hour
	Practical	Lab 7: Persistence Mechanism Analysis	**Objectives:** Identify persistence techniques. **Tasks:** Capture baseline using Regshot. Identify autorun entries and scheduled tasks. Compare baseline vs infected state.	Autoruns, Regshot	3 Hours
8	Theory	Malware Network Behaviour & C2 Concepts	Command-and-Control models. DNS abuse, beaconing, tunnelling. Encrypted traffic evasion.	Manual	1 Hour
	Practical	Lab 8: Network Behaviour Analysis	**Objectives:** Capture and analyse malware network traffic. **Tasks:** Capture traffic in isolated network. Filter DNS, HTTP, HTTPS traffic. Extract IPs, domains, and IOCs.	Wireshark, Zeek	3 Hours
9	Theory	Memory-Based Malware & Fileless Attacks	Fileless malware concepts. Memory artefacts. Process hollowing and injection.	Manual	1 Hour

	Practical	Lab 9: Memory Forensics	**Objectives:** Analyse memory artefacts linked to malware. **Tasks:** Load memory image. Run Volatility plugins (processes, DLLs, network). Identify suspicious processes.	Volatility, FTK Imager	3 Hours
10	Theory	Disk Forensics & Timeline Reconstruction	Disk artefact relevance. Prefetch, LNK, USB artefacts. Timeline analysis concepts.	Manual	1 Hour
	Practical	Lab 10: Disk Forensics Mini-Case	**Objectives:** Reconstruct user activity from disk artefacts. **Tasks:** Analyse provided disk image. Reconstruct execution and USB timeline. Extract supporting artefacts.	Autopsy/Belka soft	3 Hours
11	Theory	Reverse Engineering Foundations	Disassembly vs de-compilation. Ethics and legal boundaries. Tool overview.	Manual	1 Hour
	Practical	Lab 11: Introductory Reverse Engineering	**Objectives:** Understand binary structure and control flow. **Tasks:** Load sample into Ghidra. Identify entry point, strings, suspicious functions.	Ghidra, radare2	3 Hours
12	Theory	Detection Engineering & IOC Development	Indicators of compromise. Detection vs analysis. False-positive considerations.	Manual	1 Hour
	Practical	Lab 12: Detection Artefacts Creation	**Objectives:** Convert analysis results into detection logic. **Tasks:** Write YARA rules from IOCs. Draft conceptual IDS rules. Discuss false-positive reduction.	YARA	3 Hours
13	Theory	Integrated Malware Investigation & Reporting	End-to-end investigation workflow. Professional reporting standards.	Manual	1 Hour

	Practical	Lab 13: Final Case Study & Reporting	**Objectives:** Conduct full malware investigation and reporting. **Tasks:** Integrated static, dynamic, network, and memory analysis. Prepare structured forensic report. Oral walkthrough / viva.	All open-source tools used	3 Hours

C) Pre-requisites:

- Basic computer usage
- Working knowledge of Windows and Linux
- Basic networking concepts
- Familiarity with virtual machines
- Introductory cyber security knowledge

D) Short summary for including in the Courses of Study Booklet: Fundamentals of Malwares – how they are designed, Safe malware handling, Static and dynamic analysis, Memory and network-based analysis, Basic reverse engineering concepts, and malware reporting, using standard tools and safe analysis methodologies.

7. Recommended books:
   • Tools which will be used are already listed in the weekly description.

Dated: 17 July 2026; Proposer: DUGC, WSAIS

Dated: ; DUGC Convener (WSAIS):_____

The course is approved / not approved

_____

Chairperson, SUGC

Dated:_____