Malware Analysis	**L**	**1**	**1**	**-**
	3	**1**	**0**	

Course Objective: To introduce fundamentals of malware and to set up a protected static and dynamic malware analysis environment. Learn various malware behavior monitoring tools and actionable detection signatures from malware indicators. Learn how to trick malware into exhibiting behaviors that only occur under special conditions.

S. NO	Course Outcomes (CO)
CO1	To list the goals of Malware Analysis and to define Malware Analysis techniques.
CO2	To employ and illustrate static malware analysis techniques.
CO3	To employ and illustrate dynamic malware analysis techniques.
CO4	To classify and describe malware functionalities and behaviors
CO5	To be able to examine malwares with reverse engineering.
CO6	To be able to examine malwares with reverse engineering.

S. NO	Contents	Contact Hours
UNIT 1	Introduction to malware, OS security concepts, malware threats, evolution of malware, malware types viruses, worms, rootkits, Trojans, bots, spyware, adware, logic bombs, malware analysis, static malware analysis, dynamic malware analysis.	**6**
UNIT 2	X86 Architecture- Main Memory, Instructions, Opcodes and Endianness, Operands, Registers, Simple Instructions, The Stack, Conditionals, Branching, Rep Instructions, C Main Method and Offsets. Antivirus Scanning, Fingerprint for Malware, Portable Executable File Format, The PE File Headers and Sections, The Structure of a Virtual Machine, Reverse Engineering- x86 Architecture, recognizing c code constructs in assembly, c++ analysis, Analysing Windows programs, Anti-static analysis techniques-obfuscation, packing, metamorphism, and polymorphism.	**8**
UNIT 3	Live malware analysis, dead malware analysis, analyzing traces of malware-system-calls, api-calls, registries, network activities. Anti-dynamic analysis techniques-anti-vm, runtime-evasion techniques, , Malware Sandbox, Monitoring with Process Monitor, Packet Sniffing with Wire shark, Kernel vs. User-Mode Debugging, OllyDbg, Breakpoints, Tracing, Exception Handling, Patching	**7**
UNIT 4	Downloader, Backdoors, Credential Stealers, Persistence Mechanisms, Privilege Escalation, Covert malware launching- Launchers, Process Injection, Process Replacement, Hook Injection, Detours, APC injection.	**8**

UNIT 5	Signature-based techniques: malware signatures, packed malware signature, metamorphic and polymorphic malware signature Non-signature based techniques: similarity-based techniques, machine-learning methods, invariant inferences	**7**
UNIT 6	Malware Characterization, Case Studies – Plankton, DroidKungFu, AnserverBot, Smartphone (Apps) Security	**6**
	Total	**42**