MALWARE ANALYSIS LAB SYLLABUS

1. Examining PE Files using PEview, PE explorer and Resource Hacker

   Disassembling Portable Executable (PE32)

   imports, exports, functions, main address, malicious string locations

2. Sandboxing malware using SANDBOX tool, Virus Total Analysis, Anyrun Analysis

3. Basic malware analysis: file compilation date imports/ exports, suspicious strings run-time effect procmon filter hist -based signatures revealing files registry keys, processes, services network-based signatures

4. Advanced static malware analysis find address of main, code constructs, suspicious strings, imported functions, their tasks, intention of the malware impact of the malware via hex code

5. Analyze the malware using IDA Pro for reverse-engineering the malware: strings analysis, local variables, graph mode to cross-references, Analyzing Functions

6. Analyze the malware using OllyDbg: Debug the malware, Viewing Threads and Stacks, OllyDbg Code-Execution Options, Breakpoints, Loading DLLs, Exception Handling

7. Advanced analysis of Windows programs for processes, interactive remoteshell, uploaded file, address of the subroutine, return value, Windows APIs

8. Malware behavior analysis finding the source of malware persistence mechanism, multiple instances replication mechanisms, hiding strategies API calls for keylogging, constants involved post-infection actions of the malware, mutex, SendMessage API structure

9. Malware self-defense, packing and unpacking, obfuscation and de-obfuscation using Packers and obfuscation tools

10. Anti-disassembly and anti-debugging techniques used in the binary by patching the PE, set a breakpoint in the malicious subroutine

11. Analyzing malicious Microsoft Office and Adobe PDF documents to locate malicious embedded code such as shellcode, VBA macros or JavaScript, disassemble and/ or debug, shellcode analysis