PIS220: REVERSE ENGINEERING MALWARE

L	T	P	Cr
3	0	2	4.0

Course Objectives: To familiarize with the practice of reverse engineering suspicious files by utilizing static and dynamic tactics, techniques, and procedures in order to gain an understanding as to what impact the suspicious file may have on a particular computer system when executed.

Introduction to Malware, Analysis, and Trends, Malware taxonomy and characteristics: Introduction to Reverse Engineering Software Reverse Engineering: Reversing Applications, The Reversing Process: System-Level Reversing and Code-Level Reversing. Tools :System-Monitoring Tools ,Disassemblers, Debuggers, Decompilers. Malware Trends, naming and characteristics**:** Classification by attack areas-Boot sectors, Files, Macros, Classification by self-concealment ways- No Concealment, Encryption, Stealth, Oligomorphism, Polymorphism, Metamorphism, Strong Encryption.

Understanding Malware Threats : Malware indicators, Malware Classification, Examining Existing ClamAV Signature , Creating a Custom ClamAV Database, Detecting Malware Capabilities with YARA, Converting ClamAV Signatures to YARA, Identifying Packers with YARA and PEiD, File Type Identification and Hashing in Python.

Fundamentals of Malware Analysis (MA) : Reverse Engineering Malware (REM) Methodology , Introduction to key MA tools and techniques , Behavioural Analysis vs. Code Analysis

Resources for Reverse-Engineering Malware (REM):Initial Infection Vectors and Malware Discovery, Sandboxing Executables and Gathering Information from Runtime Analysis, The Portable Executable (PE32) File Format, Identifying Executable Metadata, Executable Packers and Compression, and Obfuscation, Techniques.Utilizing Software Debuggers to Examine Malware, triggering exploits by Emulating Browser DOM Elements. Extracting JavaScript from PDF Files with pdf.py, Triggering Exploits by Faking PDF Software Versions, Leveraging Didier Stevens's PDF Tools, Determining which Vulnerabilities a PDF File Exploits Disassembling Shell code with DiStorm, Analysing Microsoft Office Files with OfficeMal Scanner, Debugging Office Shellcode with DisView and MalHost-setup, Extracting HTTP Files from Packet Captures with Jsunpack, Graphing URL Relationships with Jsunpack, Automating the Reverse Engineering Process.

Laboratory Work: To explore the static and dynamic reverse engineering tools, creating custom CLAMAV and YARA signatures and patching executables using debuggers.

Recommended Books

1. Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code, Michael Ligh, Steven Adair, Blake Hartstein, and Matthew Richard ,Wiley,1st Edition,2010.
2. Practical Malware Analysis, Michael Sikorski and Andrew Honig, No Starch Press, 1st edition,2012
3. Computer Viruses and Malware, John Aycock,Wiley, Reprint 2010
4. Reversing: Secrets of Reverse Engineering, Eldad Eilam ,Wiley, 1st Edition, 2005