Department of Computer Science & Engineering

Session 23-24

Course Outcomes (COs):

1. Due to the dependence on online operations, social media usage, emerging technologies like IoT, IIoT, and IoE, digitization, and the pervasiveness of mobile devices, the course on malware analysis is crucial in today's digital era.
2. Safe gadget handling and secure online operations are urgently needed. To prevent being a victim of cybercrimes, it is imperative to grasp the security problems as well as the best practices.
3. At the end of this course, students will demonstrate the ability to Possess the skills necessary to carry out independent analysis of modern malware samples using both static and dynamic analysis techniques.
4. Identify and analyze various malware types by static, dynamic analysis and reverse engineering.

VAC-CSE-101: Malware Analysis

Chapter 1: Introduction to need for malware analysis, objective behind developing malwares, the dangerous effect of Malwares. Some of the use case caused by malware. (2 Hours)

Chapter 2: Malware threats- Malware analysis methodologies, Legal considerations, Identifying and protecting against malware, Malware hiding places. (3 Hours)

Chapter 3: Malware analysis types, Static, Dynamic and Hybrid type of malware analysis with examples. (2 Hours)

Chapter 4: Static Analysis: Detailed file analysis -Database of file hashes. Identifying file compile date Identifying packing/ obfuscation (2 Hours)

Chapter 5: Dynamic Analysis: System baselining - Host integrity - Monitor - Installation monitor - Process monitor - File monitor - Registry analysis/ monitoring - Network traffic monitoring/ analysis - Port monitor. (6 Hours)

Chapter 6: Code Analysis: Reverse engineering malicious code - Identifying malware, Introduction to IDA, Olly Dbg, Advanced malware analysis Virus, Trojan. Parsing Basic analysis of an APK. (5 Hours)

Chapter 7: Malware Challenges and advanced solutions (2 Hours)

Chapter 8: Mobile Malware Analysis: Need for mobile application penetration testing methodology Android and iOS Vulnerabilities - Exploit Prevention. (4 Hours).

Chapter 9: Live demo on Realtime malware analysis cases Mobile, social media. (2 Hour)

Chapter 10: Identifying malware in dead system Malware Analysis Environment: Virtual machine - Real systems - Malware analysis Identifying malware in dead system Malware Analysis Environment: Virtual machine - Real systems - Malware analysis tools ProcMon, CFF Explorer, ProcExplore, BinText, FileAlyzer, OllyDbg tools ProcMon, CFF Explorer, ProcExplore, BinText, FileAlyzer, OllyDbg. (4 Hours Practice)

BOOKS AND REFERENCES

1. https://heimdalsecurity.com/pdf/cyber_security_for_beginners_ebook.pdf

Certificates

- **A course Assessment and MCQ questions**
- **Candidates who complete all the assignments and Exam successfully are eligible to get the Certificate**