INFOSOFT IT SOLUTIONS

Training | Projects | Placements

Revathi Apartments, Ameerpet, 1st Floor, Opposite Annapurna Block, Info

soft it solutions Software Training& Development 905968394,918254087

MALWARE ANALYSIS TRAINING

1: Introduction to Malware

- Definition and types of malware
- Malware lifecycle and stages
- Goals and objectives of malware analysis

2: Malware Collection and Handling

- Sources of malware samples
- Legal and ethical considerations
- Handling and storing malware safely

3: Static Analysis Techniques

- File identification and classification
- File format analysis (PE, ELF, etc.)
- Strings and metadata extraction

4: Dynamic Analysis Techniques

- Setting up a virtual environment
- Monitoring system behavior
- Analyzing network traffic

5: Behavioral Analysis

- Identifying malware behaviors
- Process and memory analysis
- Registry and file system monitoring

6: Code Analysis

- Disassembly and decompilation
- Code execution flow analysis
- Identifying anti-analysis techniques

7: Malware Families and Variants

- Common malware families (viruses, worms, Trojans, etc.)
- Variant analysis and similarities
- Indicators of compromise (IOCs)

8: Reverse Engineering Basics

- Introduction to reverse engineering
- Tools and techniques for reverse engineering
- Practical exercises in reverse engineering malware

9: Malware Mitigation and Defense

- Prevention strategies and best practices
- Incident response and handling
- Case studies of recent malware attacks

10: Emerging Threats and Trends

- IoT malware
- Ransomware and cryptojacking
- AI and machine learning in malware

11: Legal and Ethical Issues

- Laws and regulations related to malware analysis
- Ethics of malware research
- Responsible disclosure

ADVANCE TOPIICS ;-

1: Advanced Static Analysis

- Advanced file format analysis (e.g., dissecting complex file structures)
- Code obfuscation and anti-reversing techniques
- Advanced string analysis and encoding schemes
- Identifying and analyzing embedded executables and shellcode

2: Advanced Dynamic Analysis

- Evading malware detection mechanisms (sandbox evasion, anti-VM techniques)
- Advanced malware behavior analysis (e.g., polymorphism, metamorphism)
- Deep packet inspection and protocol analysis for network traffic
- Automated dynamic analysis frameworks and tools

3: Advanced Code Analysis

- Advanced disassembly techniques (e.g., IDA Pro, Ghidra)
- Analyzing complex malware execution flows
- Debugging malware with advanced techniques (e.g., kernel debugging)
- Unpacking and deobfuscation of packed and encrypted malware

4: Memory Forensics

- Introduction to memory forensics and its importance in malware analysis
- Analyzing volatile data for malware artifacts
- Detecting and analyzing rootkits and kernel-level malware
- Memory analysis tools and frameworks (e.g., Volatility)

5: Malware Reverse Engineering

- Advanced techniques in malware reverse engineering
- Reverse engineering complex algorithms and cryptographic routines
- Identifying and analyzing anti-analysis and anti-debugging techniques
- Automating reverse engineering tasks with scripting (e.g., Python, IDAPython)

6: Advanced Malware Families

- Analysis of advanced malware families (e.g., advanced persistent threats, nation-state malware)
- Case studies of complex malware incidents and forensic analysis
- Behavioral analysis of multi-stage and multi-vector malware campaigns
- Creating YARA rules for detecting advanced malware variants

7: Exploit Kits and Exploit Analysis

- Understanding exploit kits and their role in malware distribution
- Analyzing exploit payloads and exploit techniques
- Reverse engineering exploit code and payloads
- Case studies of recent exploit kit campaigns

8: Advanced Incident Response

- Advanced incident response methodologies for malware incidents
- Threat hunting techniques for identifying malware in the network
- Incident response playbook development and execution
- Collaboration with law enforcement and third-party incident response teams

9: Malware Analysis in IoT and Embedded Systems

- Analyzing malware targeting IoT devices and embedded systems
- Challenges and techniques in firmware analysis
- Case studies of IoT malware attacks and forensic analysis

10: Malware Analysis Automation

- Automating malware analysis workflows with scripting and orchestration tools
- Building custom analysis tools and plugins
- Integration of threat intelligence feeds with automated analysis pipelines
- Scalability and performance considerations in automated malware analysis