Malware Analysis

Training and Certification

Cyber Security Educational Courses Professional Sessions

ABOUT US

We offer Cyber Security and Information Security training and Certification in Delhi for Cyber Security and Information Technology aspirants. Since Decade, we have been in the Information Technology and Cybersecurity industry. You can learn more about cybersecurity, Techniques, and Tools to choose a better career path.

DESCRIPTION

For getting the best-in-class information regarding the Malware Analysis Course in Delhi NCR through the most skilled and experienced teaching professionals in the proximity of New Delhi and its adjoining areas, you can join Bytecode Security in the upcoming batches at Saket and Laxmi Nagar institutions.

Duration - 40Hrs

Language - Hindi & English

Mode - Online & Offline

BENEFITS

1. Basic to Advanced Courses
2. Interview Cracking and Proposal-Making Sessions
3. Transparent Syllabus
4. Career-Oriented Courses and Certifications
5. International Accreditation

SAMPLE CERTIFICATE

CRAW ACADEMY

SAKET ADDRESS

1st Floor, Plot no. 4, Lane no. 2,
Kehar Singh Estate, Westend Marg,
Behind Saket Metro Station,
Saidulajab New Delhi - 110030

LAXMI NAGAR ADDRESS

R31/ 32, 2nd floor Jandu Tower,
Vikas marg, Shakarpur,
New Delhi -110092

www.craw.in

+91 951 380 5401

Malware Analysis

Training and Certification

Cyber Security Educational Courses Professional Sessions

MALWARE ANALYSIS COURSE MODULE

Module 1: Malware Development

Tools: Pe Bear, CFF explorer, x64dbg, MSVC and Sysinternals Suite
Prerequisites: Proficiency in basic C programming and a foundational understanding of Windows internals.

1.1: Foundations of Malware Development

overview

- Definition and objectives of malware in offensive security
- Role in red teaming and penetration testing

1.2: Windows Executable Formats

Portable Executable (PE) File Format

- PE file structure: headers and sections (.text, .data, .rdata, etc.)
- Tools for analyzing PE files (e.g., Pe Bear, CFF Explorer)

EXE vs. DLL

- Structural and behavioral differences
- Use cases in offensive tooling

1.3: Shellcode and Execution

Shellcode Fundamentals

- Definition and role in exploitation
- Storage options for shellcode
- Obfuscation techniques: encryption and encoding
- Win32 APIs: threads, handles, and process structures
- Native API vs. Win32 API differences

Shellcode Runners

- Concept and purpose of shellcode runners
- Primitives for building a custom shellcode runner
- Writing a custom shellcode runner
- Loading shellcode into memory from remote locations

1.4: Code Injection Techniques

Introduction to Code Injection

- Purpose and advantages of injecting code into remote processes
- Core primitives for code injection

Injection Methods

- Classic CreateRemoteThread
- QueueUserAPC (identifying alertable threads)
- SetThreadContext
- Section mapping and views
- EarlyBird injection
- Module Stomping
- Allocating executable image commit memory

DLL Injection

- Classic DLL injection
- Reflective DLL injection
- sRDI: Converting DLLs to shellcode
- Loading PE files as shellcode in current and remote processes

Malware Analysis

Training and Certification

Cyber Security Educational Courses Professional Sessions

MALWARE ANALYSIS COURSE MODULE

1.5: Payload Execution Control

Execution Management

- Preventing multiple executions of the same payload
- Implementing guardrails:
  - Environment checks (hostname, domain, user, etc.)
  - Avoiding execution on unintended systems

Module 2: Defense Evasion

Tools: Pe Bear, CFF explorer, x64dbg, MSVC and Sysinternals Suite
Prerequisites: Proficiency in basic C programming and a foundational understanding of Windows internals.

2.1: Function Call Obfuscation

Obfuscation Techniques

- Hiding shellcode execution or injection primitives
- Creating PE files without an Import Address Table (IAT)
- Camouflaging IAT to mimic legitimate binaries

2.2: Event Tracing for Windows (ETW) Evasion

Silencing ETW

- Understanding ETW and its role in detection
- Patching internal functions to disable ETW in user space
- Techniques for silencing ETW in remote processes

2.3: Bypassing EDR Hooks

Hook Management

- Role of hooks in EDR/XDR systems
- Unhooking techniques:
- Classic unhooking method
- Dual copy technique using ntdll.dll
- Perun's Fart technique for stealth unhooking

System Calls

- Direct vs. indirect system calls
- Hell's Gate and Halo's Gate techniques
- Transitioning to indirect syscalls for process unhooking
- Limitations of user-space unhooking against kernel-level hooks

2.4: Disrupting Endpoint Protection Platforms (EPPs)

Neutralizing EPP Communication

- Using Windows Firewall rules to block EPP communication
- Modifying system routing tables to disrupt connectivity

2.5: Event Log Evasion

Blinding Event Logs

- Identifying event log service threads
- Suspending or terminating threads to disable logging

2.6: Parent Process ID (PPID) Spoofing

Spoofing Techniques

- Classic spoofing via CreateProcess APIs
- Advanced spoofing using Windows Management Instrumentation (WMI)

Malware Analysis

Training and Certification

Cyber Security Educational Courses Professional Sessions

MALWARE ANALYSIS COURSE MODULE

2.7: Neutralizing Microsoft Sysmon

Sysmon Evasion

- Detecting hidden Sysmon instances
- Silent Gag technique to neutralize Sysmon

Terminating the Sysmon process

2.7: PowerShell Security Controls

Introduction to AMSI

- Bypassing AMSI by String Obfuscation

Patching internal functions & structures to break AMSI

Module3: Initial Access

Tools: Pe Bear, CFF explorer, x64dbg, MSVC and Sysinternals Suite
Prerequisites: Proficiency in basic C, and VBA programming is helpful but not required.

3.1: Function Call Obfuscation

overview

- Defining initial access in red team operations

3.2: Event Tracing for Windows (ETW) Evasion

Pretexting

- Crafting effective social engineering scenarios

HTML Smuggling

- Techniques for delivering malicious payloads via HTML

3.3: Malicious File Formats

Office Macros

- VBA stomping techniques
- Bypassing Protected View and Macro Security

LNK Files

- Using LNK files as initial access vectors

Windows Script Host (WSH)

- Leveraging JScript and VBScript
- Tools: dotnet2jscript and gadget2jscript
- Introduction to Sharpshooter framework

Other Formats

- HTA, CHM, and CPL files as attack vectors

3.4: Credential Theft

Exploiting Built-in Internet Functionality

- Techniques for stealing credentials via native Windows features

3.5: Bypassing Security Controls

Mark of the Web (MOTW) and SmartScreen

- Understanding MOTW and SmartScreen
- Bypassing MOTW and SmartScreen protections

Introduction to Containerization

- Why use containerization?
- ISO
- Compression Formats like Zip, 7z

Application Whitelisting Environments

- Phishing strategies in locked-down environments

Malware Analysis

Training and Certification

Cyber Security Educational Courses Professional Sessions

MALWARE ANALYSIS COURSE MODULE

3.6: Infection Chains

Complex Infection Chains

- Designing multi-stage infection chains for perimeter breaches

Module 4: Windows Persistence

Tools: Pe Bear, CFF explorer, x64dbg, MSVC and Sysinternals Suite
Prerequisites: Proficiency in basic C programming and a foundational understanding of Windows internals.

4.1: Foundations of Persistence overview

- Importance of persistence in red team operations

4.2: Medium Integrity Persistence Techniques

- Startup Folder
- Registry Keys
- Logon Scripts
- Shortcut Modifications
- Screensavers
- PowerShell Profile
- DLL Proxying

4.2: High Integrity Persistence Techniques

- Elevated Scheduled Tasks
- Multi-Action Tasks
- Creating and modifying services
- Image File Execution Options (IFEO) - Silent Process Exit
- WMI Event Subscription
- Netsh Helper DLLs
- Winlogon: SHELL and USERINIT modifications
- Time Providers
- Port Monitors

CRAW SECURITY

LEARN | RESEARCH | INNOVATE

SAKET ADDRESS

1st Floor, Plot no. 4, Lane no. 2, Kehar Singh Estate, Westend Marg, Behind Saket Metro Station, Saidulajab New Delhi - 110030

LAXMI NAGAR ADDRESS

R31/ 32, 2nd floor Jandu Tower, Vikas marg, Shakarpur, New Delhi -110092

www.craw.in +91 951 380 5401 @crawsec