



## DEFENCE INSTITUTE OF ADVANCED TECHNOLOGY (DU)

An Autonomous Organization funded by  
Department of Defence  
Research & Development,  
Ministry of Defence, Government of India



### SALIENT FEATURES OF THE COURSE

- 200 hours of training materials.
- The training sessions are offered by the leading academicians, experts from DRDO, industry, and cyber security Think Tanks.
- Live interaction sessions with instructors.
- Advanced Topics like Malware Analysis, Vulnerability Discovery, BYOD Security, Drone & Anti-Drone technology, etc.
- Practical demo on Kernel programming, UEFI device driver programming, Reverse Engineering, Exploit writing, Full-stack debugging of an android application, VAPT, SQL Injection, etc.

### DIAT CERTIFIED INFORMATION ASSURANCE PROFESSIONAL

### An Online Training & Certification Course (OTCC) on Cyber Security

**16 weeks online course**  
**Around 200 hours of course**  
**content plus demonstration**

### STRUCTURE OF THE COURSE:

10 Modules:

- Fundamentals of Cyber Security
- Forensics and Incident Response
- Cryptography
- System/ Driver Programming and OS Internals
- Reverse Engineering
- Malware Analysis
- Vulnerability Discovery Module for Windows, Linux, and iOS
- Vulnerability Analysis & Penetration Testing
- Tools and Techniques for Cyber Security Professionals
- Must-know Basics of Emerging Cyber Security Domain

## GENESIS OF THE COURSE

Information Assurance is the need of the hour. There is a strong demand for the experts in the fields of red teaming, cyber compliance and resilience in the organizations, industry and business. The programme is launched with a goal of building the next gen cyber warriors' force for the nation, to fulfil the immediate and growing requirement for the trained professionals competent in the state-of-the-art security tools and techniques.

## IMPORTANT DATES

- **Last date of Registration : 25 May 2023**
- **Last date of payment of fees: 05 June 2023**
- **Commencement of course: 12 June 2023**

## REGISTRATION LINK

<https://forms.gle/ngYR78hzXjs9yeTp6>

## TARGET AUDIENCE

Graduates from any discipline aiming for successful career in information security, IT professionals who wish to enhance their information assurance capabilities, Officers from Tri-services, R&D professionals, or anyone who wants to develop the skill set for information assurance. Students pursuing graduation may apply.

## CERTIFICATE

The entrance test ensures the qualification for enrolling in the course. DIAT Certified Information Assurance Professional will be awarded after successful completion, to claim your state-of-the-art skill set.

## ADVISORS

- Dr. CP Ramanarayanan, VC, DIAT
- Shri Amit Sharma, Director , O/o Advisor (Cyber), Ministry of Defence
- Dr. Manisha J Nene, Director, SoCE&MS, DIAT
- Shri Dinesh Bareja, CISA, CISM, ITIL, ISMS (LA, LI)



*"DREAM IS NOT THAT WHICH YOU SEE WHILE SLEEPING, IT IS SOMETHING THAT DOES NOT LET YOU SLEEP."*


## CANDIDATES ARE SUPPOSED TO HAVE UNDERSTANDING OF

- Fundamentals of OS: memory management, kernel architecture, IPC, process management, device management, file management, practical knowledge of BSD based OS, shell programming, Windows 32/64 APIs.
- Networking: OSI, TCP/IP, socket programming, win32 socket APIs, server messaging block, application and ports, TLS/SSL including TLS1.3, Firewalls, UTM, routing protocols, core/edge routers, ASN, IPv4/v6.
- System Software: basic knowledge of assembly, x86 instruction set, addressing modes, registers, and main memory space.
- Data Structures: Knowledge of programming language C/C++/Java/any Object-Oriented language, any one scripting language – PHP/python/ruby/Perl.

## FEES DETAILS

Fees for the Course: **Rs. 35,400/-** (including GST @18%)

## CONTACT US:

 +91 2024604533 / +91 2024604538

 [csdiat@gmail.com](mailto:csdiat@gmail.com)

 <https://www.diat.ac.in/online-certificate-courses/>

## FUNDAMENTALS OF CYBER SECURITY

Basics of computer, Evolution in computing environments; Basic constructs of cyber security; Computer networks; Network security; Firewall config, UTM, Wire-shark dump analysis, PCAP analysis, IDS/IPS- SNORT, ASL, OSSEC (file system); Attacks- snooping, spoofing, DPI techniques; Traffic reconstruction; Intro to virtual machines and hypervisors; Intro to cloud computing; Intro to cyber-crime.

## FORENSIC & INCIDENT RESPONSE

Stages of forensics; Memory forensics- evidence collection acquisition/imaging of onboard memory, Practical- FTK, Encase; Online and Live forensics, File system forensics, Network forensics- intrusion detection form Internet logs, monitoring and analysis, network traffic analysis, Incident response - Using Process Explorer, Windows sysinternals to look for malware, Cloud forensics, Database forensics - Metadata extraction & analysis.

## CRYPTOGRAPHY

Data Security & Privacy; Modular Arithmetic, Mathematics of Cryptography; Symmetric Key Cryptography, Stream Cipher A5, Asymmetric Key Cryptography, RSA; Elliptic Curve based Cryptography; Hash Functions, Digital Signature.

# SYLLABUS DETAILS

## SYSTEM/ DRIVER PROGRAMMING AND OS INTERNALS

Basics of compiler, linker and build processes, Basics Kernel programming, user-kernel mode communication, Interrupt handling & input subsystems, ring architecture; Windows OS Internals- System Architecture; Linux Internals- Linux Kernel, File Descriptors; SSDT, IDT, IAT (hands-on hooking); Linux boot process; NDIS Device driver programming- protocol, miniport; Windows boot process debugging, UEFI device driver programming, MBR, programming; File system filter driver programming; Secure boot, measure boot, trust boot ;Introduction to ARMv7 & V8 instructions; Introduction to ARM ABI convention, writing simple assembly files, its calling & its functionality; Recovery partitions; WMI programming & power shell.

## REVERSE ENGINEERING

Reversing basics, Execution Environments, Static & Dynamic reverse engineering; Assembly language primer; x86 & x86-64 architectures; Assembly language primer; Executable file formats- PE & ELF; Reversing program binaries- offline code analysis; Reversing program binaries; Reversing program binaries- live code analysis; Kernel Debugging (hands-on Windows crash dump analysis); Reversing tools: Disassemblers, Debuggers, System monitoring tools; Reversing '.NET',

De-compilation; Anti-reversing techniques: Breaking protections, Confusing Disassemblers, Anti-Debugger Techniques, VM- detection techniques

## MALWARE ANALYSIS

Static & Dynamic malware analysis techniques; Packing, unpacking, Sandboxing executables, Runtime analysis in VM; Advanced Static Analysis- Analyzing malicious Windows Programs; Advanced Dynamic Analysis- Debugging, Kernel Debugging with WinDbg; Dynamic data flow tracking (DFT); Process injection, API hooking, DLL injection; Reflective DLL loading, Dynamic API loading, 64- bit Malware, File-less Malware; AV obfuscation techniques; Covert Malware Launching; Data Encoding; Malware Focused Network Signatures; Shellcode Analysis; Reversing firmware; Android, iOS architecture; Android Reverse Engineering; Android application architecture understanding; Tools for reversing of application (jadx, apktool, backsmali, dextojar); Obfuscation Techniques of android applications, Deobfuscation Techniques; Smali code understanding, code injection techniques; iOS Application Security; iOS Security Mechanisms & Security Architecture; Secure Boot Chain, Data Encryption & Network Security; iOS File System isolation, Application Sandbox, iOS device Architecture; Automated Malware Analysis using Cuckoo, Yara; Malware As A Service.

## VULNERABILITY DISCOVERY MODULE FOR WINDOWS, LINUX AND IOS

Writing shell code for Arm and x86\_64; Software vulnerabilities: buffer overflow, integer overflow, heap overflow, Use after free, double free, null pointer dereference, race condition; Out-of-bounds and pool overflow, Vulnerability discovery and Exploit writing, hands on for both windows and Linux (android); Return oriented programming; SEH exploit; heap splaying; stack overflow prevention; ASLR, DEP bypass, canary bits, egg hunting; Fuzzing with Metasploit: Simple FTP fuzzer; Android Fuzzing (AFL for android, SyzKaller for kernel); Full-stack debugging of an android application, with remote gdb, adb and android studio; Advance kernel Exploitation Windows/Linux; KSLR bypass, SMEP bypass, token stealing shell code; Privilege escalation techniques; iOS Kernel Debugging: Panic Dumps, Using the KDP Kernel Debugger (hands on tasks limited to 30 pin devices); Extending the Kernel Debugger (KDP++); Debugging with own Patches; Kernel Heap Debugging/Visualization (new software package); Patch Diffing, One-Day Exploits, and Return-Oriented Shell-code; Advanced Persistent Threat (APT) life-cycle; Introduction to VAPT methodology; Introduction to Red Teaming, Mitre Framework; Essential Tools for VAPT;

## SYLLABUS DETAILS

Passive Information Gathering: OSINT/Search Engines, DNS Enumeration, DNS Tools (dnsenum, dnsrecon, dnsdumpster); Active Information Gathering: Intro to TCP/UDP, Port Scanning using NMAP, Nmap Scripting Engine, Service Detection and Banner Grabbing; Service Enumeration: NetBIOS, SMTP, SNMP, Other Services; Sniffing and MITM attacks: ARP Tools, MITM; Exploits: Searching for Exploits, Customizing Exploits; Client Side Attacks: Spear Phishing, Phishing, Social Engineering; Anonymity using TOR, VPNs and Proxies; Common Web Services: HTTP, HTTPS, FTP, WebSockets; Web Discovery: Fuzzing using wfuzz, dirbuster, dirb and web crawling; Web Exploitation Tools: Burpsuite, Firefox Add-ons.

## TOOLS AND TECHNIQUES FOR CYBER SECURITY PROFESSIONALS

IEEE standards; Technical report writing; SOC maintenance; Overview of fail-safe and fault-tolerant systems; Commercial grid security-BYOD security; Corporate security implementation overview - threat analysis, risk assessment; Indicators of Compromise (IoC), Indicators of attack; Tactics, Techniques, and Procedures (TTP) - method of analyzing an APT operation, analyzing the performance of APT; Disaster recovery- tier 1, 2; Business Continuity Plan (BCP).

## VULNERABILITY ANALYSIS AND PEN TESTING

SQL Injection, Login Bypass using SQL Injection; Advanced SQL Injection: WAF and advanced queries; File Inclusion, File Upload Bypass; Cross-Site Scripting and other OWASP top 10 vulnerabilities; Post-Exploitation and Lateral Movement; File Transfer: tftp, ftp, encoded, echo, download clients; Hydra, NCrack, Medusa, John the Ripper; Maintaining access: web shells, reverse shells and payloads; Privilege escalation: password attacks, security misconfiguration, exploitable software, escalation exploits; Windows Authentication Weaknesses; Port Redirection, Tunneling, Pivoting and Proxies; Escalation and Lateral Movement in AD environments; Exploitation Frameworks: Metasploit.

## MUST-KNOW BASICS OF EMERGING CYBER SECURITY DOMAINS

Cloud Security, Drone & Anti-Drone technologies, Concept of block-chain, cyber terrorism, cyber warfare, virtual currency, & utilization in dark web, TOR, VPN, social media threats; Cyber Physical Systems (CPS) and Security in CPS.