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

DIAT CERTIFIED INFORMATION ASSURANCE PROFESSIONAL

An Online Training & Certification Programme by
Defence Institute of Advanced Technology (DIAT)

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.

Structure of the Course
During this 12 weeks intensive course, the experts will teach the fundamentals of cyber security and advanced topics including digital forensics, reverse engineering, malware analysis, vulnerability analysis, exploit mitigation and tools and techniques for Cyber Security professionals. The sessions include theory as well as hands-on practice sessions for the topics. Syllabus of the course is designed by a team of academicians, DRDO experts and Cyber security advisors.

Online mode of course.
Learn from anywhere, without leaving your home or your job.

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.

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.

Eligibility
Graduate from any discipline. Students from final year may apply. Need to qualify the entrance test.

Be prepared to learn the advanced skills and sharpen your edge.

Prerequisite for the course - Syllabus for Entrance Test

- **Fundamentals of OS:** memory management, IPC, kernel architecture, 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, 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 Entrance Test: **Free**
- Fees for the Course: **Rs. 15000/- (Excluding GST @18%)**
  [Need to be paid after qualifying the Entrance Test]

Important Dates

- Registration for Test: **28th January 2021 to 15th February 2021**
  [Link: onlinecourse.diat.ac.in]
- Date of Entrance Test: **21th February2021**
- Date of Result Declaration: **22nd February 2021**
- Last date of payment of fees: **26th February** [After qualifying]
- Date of Commencement of Course: **28th February 2021**

Duration

- **12** weeks online course
- **120** contact hours
- **[2** hours/day & **5** days/week]

Advisors

- **Dr. CP Ramanarayanan, VC, DIAT**
- **Amit Sharma, Advisor (Cyber), Ministry of Defence**
- **Prof. KP Ray, DIAT**
- **Dinesh Bareja, CISA, CISM, ITIL, ISMS (LA, LI)**

Trainers

The training sessions are offered by the leading academicians, experts from DRDO, industry, cyber security think tank.

For information

Contact: **cs@diat.ac.in** Website: **onlinecourse.diat.ac.in**; http://diat.ac.in;

Course framework

(1) Cyber Security Essentials
(2) Forensics and Incident Response
(3) System/ Driver Programming and OS Internals
(4) Reverse Engineering and Malware Analysis
(5) Vulnerability Discovery Module for Windows, Linux and iOS
(6) Vulnerability Analysis & Penetration Testing
(7) Tools and Techniques for Cyber Security Professionals

Syllabus Details

Cyber Security Essentials: Basic constructs of security, Cryptography– Modular Arithmetic, Mathematics of Cryptography, Symmetric Key Cryptography, Stream Cipher A5, Asymmetric Key Cryptography, RSA; Elliptic Curve based Cryptography, Hash Functions, Digital Signature, Hands-on class– Wire-shark dump analysis, PCAP analysis, IDS/IPS– SNORT based practical, ASL, ossec (file system), firewall config; UTM; Attacks- snooping, spoofing, DPI techniques– practical aspects, traffic reconstruction, Intro to virtual machines and hypervisors, Intro to cloud computing, Cloud Security; Intro to cyber crime, cyber terrorism, cyber warfare, virtual currency, & utilization in dark web, TOR, VPN, social media threats.

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.

System/ Driver Programming & 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 & Malware Analysis: 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 (IDA, GDB, GEF, Ghidra), Disassemblers, Debuggers, System monitoring tools; Reversing '.NET', De-compilation; Anti-reversing techniques: Breaking protections, Confusing Disassemblers, Anti-Debugger Techniques, VM- detection techniques; 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 (jadax, 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; OutOfBound 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 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; 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.

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.

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 performance of APT; Disaster recovery- tier 1, 2; Business Continuity Plan (BCP).