CA401: Linux Operations

24 Instructional Hours 61 CPEs 37 Labs

LIVE ONLINE OR ON-DEMAND ACCESS OR IN PERSON

BEGINNER TO INTERMEDIATE

This course provides a comprehensive introduction to Linux system administration and command-line operations with an emphasis on practical, real-world usage. The course covers foundational Linux concepts, including filesystem structure, shell commands, text editors, permissions, and user management, before progressing to advanced topics such as process control, system boot mechanisms, package management, networking, automation with cron, and shell scripting. Students gain hands-on experience configuring, managing, and troubleshooting Linux systems, including secure remote access, network analysis, and system services using systemd. The course also introduces widely used security and networking tools and concludes with a capstone challenge designed to reinforce operational and cybersecurity-relevant skills essential for modern IT and security professionals.

You Will Be Able To

- Navigate and manage Linux systems confidently using essential shell commands and filesystem concepts.
- Create, edit, and manage files safely using common Linux text editors and command-line tools.
- Administer users, groups, and permissions (including ownership and privilege elevation with sudo) to support secure operations.
- Monitor and control system processes, understand the Linux boot process, and manage services with systemd.
- Apply Linux networking fundamentals for troubleshooting, secure remote access (SSH/SCP), and practical system management tasks.

Who Should Attend

This course is designed for a broad audience interested in working with Linux systems and the command-line environment. It is appropriate for students, entry-level professionals, and experienced practitioners who want to develop or reinforce practical skills in system navigation, administration, networking, automation, and troubleshooting. The course supports learners across IT, cybersecurity, software development, cloud, and engineering disciplines, and is structured to be accessible while still providing depth applicable to real-world technical environments.

Relevant Combat Roles

- IT Support
- Systems Administrator (Junior to Mid-Level)
- Linux Administrator
- Cybersecurity Analyst (Entry-Level)
- Network Operations Technician

Topics Covered

Linux command line foundations, filesystem structure, and working efficiently in he terminal (navigation, wildcards, I/O redirection, pipelines).

Administration fundamentals: users/groups, permissions, ownership, archiving/backup, and package management concepts.

Operations and security workflow: processes/signals, boot process + systemd services, networking utilities, SSH/SCP, and task automation with cron and shell scripting.

Labs

User & Group Administration
(configure Linux users/groups, manage permissions and ownership, apply sudo/SUID privileges, and validate access control using chmod/chown/id/su/sudo CLI tools)

Process Monitoring & Service Management
(monitor and control running processes using ps/top/kill/signals, inspect system services with systemctl, and analyze Linux process behavior and resource usage)

Task Automation & Bash Scheduling
(create bash automation workflows, schedule recurring jobs with cron/systemd timers, automate backups and log collection, and validate execution through logs and script output)

CA301: Cryptography

30 Instructional Hours 46 CPEs 16 Labs

LIVE ONLINE OR ON-DEMAND ACCESS OR IN PERSON

INTERMEDIATE

This course provides a comprehensive and practical exploration of cryptography, covering both foundational principles and advanced applications in modern security systems. It begins with core concepts such as confidentiality, integrity, and availability, and progresses through symmetric and asymmetric encryption techniques, cryptographic algorithms, and real-world implementations. Learners are introduced to essential topics including key management, hashing, digital signatures, cryptographic protocols, and network security mechanisms like TLS and VPNs. The course also addresses emerging areas such as quantum cryptography, cryptanalysis, and steganography, while emphasizing secure implementation practices and common pitfalls. With a strong focus on applied learning, the material integrates theoretical knowledge with hands-on examples and real-world scenarios to prepare learners for practical cybersecurity challenges.

You Will Be Able To

- Apply symmetric and asymmetric encryption techniques to secure data in real-world scenarios
- Analyze and select appropriate cryptographic algorithms, modes of operation, and protocols
- Implement secure key management, hashing, and authentication mechanisms
- Identify and mitigate common cryptographic vulnerabilities and implementation flaws
- Evaluate modern cryptographic systems, including TLS, PKI, and secure communication protocols
- Understand and assess emerging threats such as quantum computing and advanced cryptanalysis

Who Should Attend

This course is designed for students, cybersecurity professionals, and IT practitioners who want to build a strong foundation in cryptography and its real-world applications. It is suitable for individuals with a basic understanding of networking or security concepts who are looking to deepen their knowledge in secure communications, encryption technologies, and data protection. The course is particularly valuable for those pursuing roles in cybersecurity, secure software development, or network defense.

Relevant Combat Roles

- Network Security Engineer
- Cryptanalyst
- Key Management Officer
- Cryptography Engineer

Topics Covered

Fundamentals & Core Principles
(CIA triad, AAA model, terminology)

Cryptographic Methods & Algorithms
(keyless, symmetric—DES/AES/stream ciphers/modes, asymmetric—RSA/Diffie-Hellman/ECC/digital signatures)

Hashing, Passwords & Security Practices
(hash functions, MACs, bcrypt/scrypt/Argon2, randomness, key derivation, IVs/nonces, encoding pitfalls)

Protocols, Infrastructure & Network Security
(PKI, certificates, authentication protocols, TLS/SSL, VPNs, secure communication)

Attacks & Advanced Topics
(cryptanalysis—brute force, frequency, padding oracles; steganography, quantum & post-quantum cryptography)

Labs

Symmetric Encryption & OpenSSL Operations
(OpenSSL DES/AES encryption, ECB/CBC modes, encryption and decryption workflows)

Public-Key Cryptography & Digital Signatures
(RSA key generation, asymmetric encryption/decryption, and digital signatures)

TLS Analysis & Certificate Inspection
(TLS configuration analysis, certificate chain inspection, and weak cipher detection)

Password Hashing & Key Derivation Security
(password hashing, salting, PBKDF2/scrypt/Argon2 key derivation)

Password Cracking & Cryptographic Attack Analysis
(weak password cracking, rainbow tables, and brute-force analysis)

Steganography & Hidden Data Analysis
(image/audio steganography, hidden data extraction, and steganalysis)

CA302: Operational Cyber Defense

26 Instructional Hours 46 CPEs 20 Labs

LIVE ONLINE OR ON-DEMAND ACCESS OR IN PERSON

INTERMEDIATE

This course provides a comprehensive and practical exploration of Blue Team operations within modern cybersecurity environments. It covers the structure, roles, and responsibilities of defensive teams, along with the operational frameworks of Security Operations Centers (SOCs). Learners are introduced to core defensive disciplines such as network monitoring, endpoint security, threat intelligence, detection engineering, incident response, and vulnerability management. The material emphasizes real-world application through structured workflows, tools (SIEM, EDR/XDR), and industry frameworks like MITRE ATT&CK, enabling learners to build, operate, and improve defensive security capabilities in organizational settings.

You Will Be Able To

- Monitor and analyze security events using SOC processes and tools such as SIEM and EDR
- Detect, triage, and respond to security incidents using structured playbooks and workflows
- Implement network and endpoint security controls to defend against common attack vectors
- Perform vulnerability management and prioritize remediation based on risk

Who Should Attend

This course is designed for individuals seeking to build or strengthen defensive cybersecurity skills, particularly those interested in Security Operations Center (SOC) roles. It is suitable for beginners to intermediate learners, including IT professionals, system administrators, and aspiring cybersecurity analysts who want hands-on knowledge of monitoring, detection, and incident response. It is also valuable for professionals transitioning from general IT into specialized security roles or aiming to understand real-world Blue Team operations.

Relevant Combat Roles

- SOC Analyst
- Incident Responder / Incident Handler
- Threat Hunter / Threat Intelligence Analyst
- Security Operations Engineer
- Vulnerability Management Analyst

Topics Covered

Blue Team Operations & SOC Fundamentals
(defensive principles, SOC architecture, governance, and metrics)

Threat Intelligence & Detection Engineering
(IOC vs IOA, intel-to-action workflows, detection engineering, alert triage)

Monitoring, Logging & Security Automation
(network security monitoring, SIEM, SOAR, logging, traffic analysis)

Endpoint & Network Security
(EDR/XDR capabilities, segmentation, response playbooks)

Vulnerability Management & Threat Hunting
(exposure management, risk prioritization, threat hunting, MITRE ATT&CK)

Labs

SOC Operations & Incident Response
(SOC alert triage, incident classification, and response playbooks using SIEM tools such as Splunk/ELK)

Network Security Monitoring & Traffic Analysis
(Wireshark traffic analysis, DNS/HTTP(S) attack investigation, network architecture, and access control with IPTables)

Detection Engineering & IDS/IPS
(Snort and Suricata setup, rule creation, and YARA-based detection)

Endpoint Detection & Response (EDR)
(endpoint investigation, host isolation, process termination, and forensic data collection)

SIEM, Logging & Security Analytics
(Splunk, ELK stack setup, log analysis, and security monitoring)

CA501: Web Application Security

60 Instructional Hours 80 CPEs 20 Labs

LIVE ONLINE OR ON-DEMAND ACCESS OR IN PERSON

ADVANCED

This course provides a comprehensive and practical exploration of web application security, focusing on the principles, methodologies, and tools required to identify, assess, and mitigate vulnerabilities. It covers foundational cybersecurity concepts, web technologies such as HTTP and APIs, and progresses into advanced security testing techniques including vulnerability assessment, penetration testing, and exploitation methods. Learners are introduced to industry standards such as OWASP, NIST, and PTES, and gain hands-on understanding of both manual and automated testing approaches. The course blends theoretical knowledge with real-world application, equipping learners with the skills needed to analyze, test, and secure modern web applications effectively.

You Will Be Able To

- Identify and analyze common web application vulnerabilities and attack vectors
- Perform structured vulnerability assessments and penetration testing activities
- Understand and manipulate HTTP protocols, requests, and responses for security testing
- Use industry-standard tools (e.g., Burp Suite, OWASP ZAP, Nessus) for web security testing
- Evaluate authentication, authorization, and session management mechanisms for weaknesses
- Apply security testing methodologies aligned with OWASP, NIST

Who Should Attend

This course is designed for individuals with a foundational understanding of cybersecurity who want to specialize in web application security. It is suitable for aspiring penetration testers, security analysts, and developers seeking to understand how applications are attacked and secured. The course is also valuable for IT professionals and engineers responsible for securing web-based systems and applications, as well as those preparing for roles in offensive or defensive cybersecurity.

Relevant Combat Roles

- Web Application Penetration Tester
- Security Analyst
- Application Security Engineer
- Red Team Operator
- Vulnerability Assessment Specialist
- Cybersecurity Consultant

Topics Covered

Cybersecurity & Web Fundamentals
(threats, vulnerabilities, risks, exploits, payloads, web architecture, HTTP protocol, APIs including REST/SOAP/GraphQL)

Security Testing Methodologies & Standards
(information gathering, enumeration, vulnerability assessment, penetration testing, OWASP Top 10, ASVS, NIST, OSSTMM, PTES, SAST/DAST tools)

Authentication, Authorization & Session Management
(OAuth, AWS Cognito, weak password policies, authentication bypass, privilege escalation, IDOR, session attacks, JWT, CSRF, brute force, cookie security)

Input Validation & Injection Attacks
(XSS—stored/reflected/DOM, SQL/NoSQL injection, command injection, SSRF, XXE, template injection, LDAP/XML/XPath injection, file inclusion, HTTP smuggling)

Client-Side & Server-Side Vulnerabilities
(CORS, clickjacking, browser storage, client-side manipulation, business logic flaws, WAF bypass, access control issues, error handling and misconfigurations)

Advanced Attacks & Security Risks
(RCE, insecure deserialization, DoS/DDoS, dependency confusion, zero-day hunting, advanced exploitation techniques)

Labs

Web Application Enumeration & Testing
(information gathering, endpoint discovery, basic vulnerability assessment)

Authentication & Access Control Attacks
(weak passwords, authentication bypass, IDOR, privilege escalation)

Session Management & Web Attacks
(session fixation, CSRF, cookie analysis, JWT attacks)

Injection Attacks Lab
(SQL injection, XSS (stored/reflected), command injection, file inclusion)

Client-Side & API Security Testing
(DOM XSS, CORS issues, API testing with REST/GraphQL)

Advanced Web Exploitation Lab
(SSRF, RCE concepts, WAF bypass techniques, security misconfigurations)

CA303: Cyber Threat Intelligence

25 Instructional Hours 38 CPEs 13 Labs

LIVE ONLINE OR ON-DEMAND ACCESS OR IN PERSON

INTERMEDIATE

This course provides a comprehensive exploration of Threat Intelligence (CTI) and Open-Source Intelligence (OSINT), focusing on how organizations collect, analyze, and operationalize intelligence to defend against evolving cyber threats. It covers the full intelligence lifecycle, threat actor profiling, malware analysis, and the integration of intelligence into security operations. Learners will gain both foundational knowledge and advanced insights into frameworks such as MITRE ATT&CK and the Cyber Kill Chain, along with practical techniques for intelligence-driven defense, threat hunting, and OSINT investigations. The course emphasizes actionable intelligence, real-world use cases, and the importance of context, relevance, and operational application in modern cybersecurity environments.

You Will Be Able To

- Apply the threat intelligence lifecycle to transform raw data into actionable intelligence
- Analyze and profile threat actors based on motivations, tactics, and behavior
- Conduct malware analysis using static, dynamic, and behavioral techniques
- Integrate threat intelligence into SOC workflows, SIEM, and incident response processes
- Perform OSINT investigations using structured methodologies and validated sources
- Develop intelligence-driven detection and response strategies aligned with real-world threats

Who Should Attend

This course is designed for cybersecurity professionals, analysts, and students who want to build or enhance their skills in threat intelligence and OSINT. It is suitable for individuals working in security operations, incident response, or threat hunting, as well as those interested in digital investigations and cyber defense. The course is also valuable for professionals seeking to transition into intelligence-focused roles, as it combines both technical and analytical perspectives with practical applications.

Relevant Combat Roles

- Threat Intelligence Analyst
- Incident Responder / DFIR Specialist
- Threat Hunter
- Cybersecurity Analyst
- Vulnerability Management Specialist

Topics Covered

Threat intelligence fundamentals – lifecycle, workflows, and types (tactical, operational, strategic)

Threat actors & context – motivations, categories, and real-world case studies

Malware analysis basics – common types and intro to analysis techniques

Applying intelligence in security – SIEM/SOAR use, MITRE ATT&CK, and threat hunting

OSINT methods & tools – data collection, verification, and online investigations

Labs

Malware Analysis & Sandbox Investigation (static/dynamic malware analysis, sandbox behavior analysis, and IOC identification)

Threat Detection & MITRE ATT&CK Mapping (MITRE ATT&CK mapping, SIEM detection rules, and threat behavior analysis)

OSINT Investigation & Digital Footprint Analysis (social media investigations, public data analysis, and digital footprint validation)

Threat Intelligence Operations & SOC Enrichment (alert enrichment, intelligence-driven incident prioritization, and SOC threat analysis)

CA202: Python Programming Language

16 Instructional Hours 24 CPEs 8 Labs

LIVE ONLINE OR ON-DEMAND ACCESS OR IN PERSON

BEGINNER

This course provides a comprehensive introduction to Python programming, covering both foundational concepts and practical applications. It begins with core syntax, data types, and control structures, then progresses into functions, modules, file handling, and data structures. The course also explores object-oriented programming, exception handling, and advanced topics such as threading and networking. Throughout the learning journey, hands-on "Cyberdrome" exercises reinforce concepts with real-world cybersecurity use cases, enabling learners to apply Python in automation, data processing, and security-related tasks.

You Will Be Able To

- Write and execute Python scripts using proper syntax, variables, and data types
- Implement control flow, loops, and functions to build structured programs
- Manipulate files, directories, and structured data formats such as CSV and JSON
- Apply object-oriented programming principles including classes, inheritance, and polymorphism
- Handle exceptions and debug programs effectively for reliable execution
- Develop basic cybersecurity-related scripts such as IP filtering, password validation, and port scanning

Who Should Attend

This course is designed for beginners and early-stage learners who want to build a solid foundation in Python programming. It is suitable for students, aspiring developers, and cybersecurity enthusiasts who have little to no prior programming experience. The course is also appropriate for individuals seeking to transition into technical roles where scripting, automation, and data handling are essential skills.

Relevant Combat Roles

- Cybersecurity Analyst
- SOC Analyst (Tier 1 / Tier 2)
- Automation / Scripting Engineer
- Penetration Tester

Topics Covered

Network & Sockets Labs
Build TCP client/server apps and monitor connections to detect unusual port activity.

Data Protection & File Security
Implement DLP checks, file integrity monitoring, and audit access to sensitive files.

Security Automation with Python
Develop scripts for IP blocking, password auditing, phishing detection, and rule-based alerts.

Library Hijacking & Serialization Labs
Explore Python import behavior, unsafe dependency handling, and serialization/deserialization risks in controlled lab scenarios.

Malware Analysis & OCR Libraries
Use Python for safe malware analysis concepts in sandboxed environments and work with OCR libraries to extract and process text from images.

Data Handling & Ethical Web Use
Process CSV/JSON logs and perform compliant web scraping on approved sources.

Labs

Python Automation & Web Scraping Development
(web scraping, data collection, and structured data storage using Python)

Computer Vision & OpenCV Projects
(face detection systems, image processing, and OpenCV-based automation)

Security Monitoring & Exfiltration Detection
(network traffic analysis, anomaly detection, and suspicious transfer monitoring)

Safe Malware Simulation & Code Mutation Demonstrations
(polymorphic code structure demonstrations in isolated lab environments)

Remote Administration & Secure Lab Tooling
(controlled remote command execution tools for authorized testing environments)

CA402: Network Security

35 Instructional Hours 58 CPEs 23 Labs

LIVE ONLINE OR ON-DEMAND ACCESS OR IN PERSON

INTERMEDIATE

This course provides a comprehensive and practical foundation in network security, combining core networking principles with modern defensive strategies. It begins with essential networking concepts such as network architecture, devices, protocols, and addressing, then progresses into security-focused topics including segmentation, firewall management, intrusion detection, and secure network design. The material emphasizes real-world application by integrating defensive techniques, monitoring strategies, and incident response practices. Learners develop both theoretical understanding and operational skills required to design, secure, and troubleshoot modern network environments.

You Will Be Able To

- Analyze network architectures using OSI and TCP/IP models to understand data flow and security implications
- Configure and secure network components including firewalls, NAT/PAT, and access controls
- Design secure network architectures using segmentation, DMZs, and defense-in-depth strategies
- Identify and mitigate common network-based attacks such as ARP poisoning, DHCP attacks, and DNS spoofing
- Monitor and investigate network activity using logging, telemetry, and packet analysis tools

Who Should Attend

This course is designed for individuals seeking a strong foundation in both networking and network security. It is suitable for beginners entering cybersecurity, IT students, and professionals transitioning into network defense roles. It is also valuable for system administrators and IT support personnel who want to deepen their understanding of how networks operate and how to secure them against modern threats. The course accommodates learners with basic technical knowledge and progressively builds toward more advanced defensive concepts.

Relevant Combat Roles

- Network Security Analyst
- SOC (Security Operations Center) Analyst
- Network Engineer (Security-focused)
- Cyber Defense Analyst
- Incident Response Analyst

Topics Covered

Network Fundamentals & Models
Network types (LAN/WAN/MAN), devices (switches, routers, NICs), and core concepts like encapsulation. Includes OSI vs TCP/IP models and data flow across layers.

Ethernet & Infrastructure
Ethernet standards, switching, frame structure, and cabling types (UTP, fiber, coax) with categories (Cat5e–Cat8).

Protocols & Addressing
Key protocols (HTTP, DNS, SMTP, TCP/UDP), plus IPv4/IPv6, subnetting, CIDR, ARP, and NAT/PAT.

Secure Architecture & Defense
Segmentation, DMZ, trust boundaries, and traffic flow (north-south vs east-west) with defense-in-depth design.

Security Controls & Monitoring
Firewalls, NAC, VPNs, DHCP snooping, ARP defense, plus logging (Syslog), NetFlow, SIEM, IDS/IPS.

Troubleshooting & Wireless
Tools (Wireshark, ping, traceroute), monitoring, and Wi-Fi security (WPA2/WPA3, common attacks).

Labs

Network Traffic Analysis & Wireshark Operations
(packet capture, protocol analysis, anomaly detection, and traffic inspection using Wireshark)

Firewall Configuration & Policy Enforcement
(Linux iptables/firewalld, Windows Defender Firewall, inbound/outbound filtering, and rule auditing)

Secure Network Architecture & Segmentation
(VLAN design, DMZ implementation, trust boundaries, east-west vs north-south traffic control, and bastion host placement)

Network Attack Simulation & Defensive Analysis
(ARP poisoning, DHCP spoofing/starvation simulations, IDS/IPS detection, telemetry collection, and incident response workflows)

Network Monitoring & Detection Engineering
(Syslog, NetFlow/sFlow/IPFIX, SPAN/TAP capture strategies, SIEM integration, and PCAP-based investigations)

CA403: Windows Security

39 Instructional Hours 57 CPEs 18 Labs

LIVE ONLINE OR ON-DEMAND ACCESS OR IN PERSON

INTERMEDIATE

This course provides a comprehensive introduction to the core components, architecture, and operational principles of the Windows operating system. It explores both theoretical concepts and practical administration tasks, including system architecture, command-line usage, graphical interface navigation, process and memory management, and virtualization. Learners will also gain insight into system startup processes, storage management, file systems, and security mechanisms such as BitLocker and Active Directory. The course is designed to build a strong foundational understanding of how Windows operates internally and how to manage, troubleshoot, and secure Windows-based environments effectively.

You Will Be Able To

- Explain Windows architecture, including kernel and user mode operations
- Use command-line tools and scripting to automate system tasks
- Manage processes, applications, and system performance using built-in tools
- Configure storage, file systems, and disk management features
- Analyze system logs and troubleshoot issues using Event Viewer
- Implement basic Windows security measures, including encryption and access control

Who Should Attend

This course is intended for beginners to intermediate learners who want to build a solid foundation in Windows operating systems. It is suitable for students, IT support staff, aspiring system administrators, and cybersecurity learners who need practical knowledge of Windows internals, system management, and security fundamentals. No prior advanced experience is required, but basic computer literacy is recommended.

Relevant Combat Roles

- Windows System Administrator
- IT Support Specialist
- SOC Analyst (Tier 1)
- Cybersecurity Analyst

Topics Covered

Core system architecture & operation: Windows architecture (kernel, processes, threads, HAL), startup/boot process (BIOS, UEFI, Boot Manager, WinRE), and overall system components

User interaction & interfaces: Command-Line Interface (CLI), command shell with I/O redirection, and Graphical User Interface (GUI) including Windows 11 system applications

Process & performance management: Process management, Task Manager usage, and system performance monitoring tools

Storage & file systems: Storage management (basic/dynamic disks, storage spaces, disk tools) and file systems (NTFS, FAT, exFAT) with related utilities

System monitoring & automation: Event logging with Event Viewer and PowerShell fundamentals including basic scripting

Security & enterprise features: Windows security concepts (BitLocker, UAC, firewall basics), virtualization with Hyper-V, and Active Directory basics with authentication (Kerberos overview)

Labs

Windows Command-Line Operations & Automation
(Command Prompt usage, I/O redirection, piping, command chaining, scripting, and task automation with cmd)

Windows Performance & Process Analysis
(Task Manager monitoring, process management, startup analysis, CPU/memory utilization, and Performance Monitor diagnostics)

Windows Logging & Troubleshooting
(Event Viewer usage, event filtering, Security/Application/System log analysis, Event ID investigation, and troubleshooting workflows)

Windows Identity & Access Management
(Active Directory deployment, domain controller configuration, OU/user/group management, Kerberos authentication, and Group Policy administration)

Windows Account Administration & Credential Management
(User account provisioning, password resets, administrative account control, permissions, access tokens, and authentication management)

PowerShell Administration & Automation
(PowerShell cmdlets, scripting fundamentals, loops, conditional logic, automation workflows, environment variables, and Windows configuration management)

CA304: Cloud Security

29 Instructional Hours 47 CPEs 18 Labs

LIVE ONLINE OR ON-DEMAND ACCESS OR IN PERSON

INTERMEDIATE

This course provides a comprehensive and practical introduction to cloud security, focusing on how modern cloud environments are designed, deployed, and protected. It explores core cloud computing concepts, service and deployment models, and the shared responsibility framework, while diving deeply into real-world implementations using platforms such as AWS and Azure. Learners gain hands-on exposure to identity and access management, cloud networking, secure SaaS architecture, serverless computing, data protection, and security operations. The course emphasizes a practical, lab-driven approach, enabling participants to build, secure, monitor, and assess cloud infrastructures while understanding real-world vulnerabilities, attack surfaces, and defensive strategies.

You Will Be Able To

- Explain cloud computing models, architectures, and the shared responsibility model
- Configure and secure cloud environments using IAM, networking, and storage controls
- Design and analyze secure SaaS and serverless architectures
- Detect, monitor, and respond to cloud-based threats using native security tools
- Perform basic cloud penetration testing and identify common misconfigurations
- Implement security best practices across AWS, Azure, and containerized environments

Who Should Attend

This course is designed for students, IT professionals, and cybersecurity practitioners seeking to understand and secure cloud environments. It is particularly suitable for individuals pursuing roles in cybersecurity, cloud engineering, DevOps, or system administration. A basic understanding of networking and computing concepts is recommended, as the course builds progressively from foundational cloud principles to advanced security practices and real-world implementations.

Relevant Combat Roles

- Cloud Security Engineer
- Security Operations Analyst (SOC Analyst)
- Cloud / DevOps Engineer
- Penetration Tester (Cloud Specialist)
- Threat Detection and Incident Response Analyst

Topics Covered

Cloud Foundations & Architecture: Cloud computing models (IaaS, PaaS, SaaS, FaaS), SaaS architecture design, multi-tenancy, and secure cloud architecture principles

Identity, Access & Security Models: IAM (users, roles, policies, least privilege), shared responsibility model, and core cloud security principles

Core AWS Services & Infrastructure: AWS IAM, EC2, S3, VPC, Organizations, along with cloud networking (VPCs, subnets, routing, gateways)

Serverless & Infrastructure as Code: AWS Lambda, API Gateway, Terraform, and AWS SAM for scalable and automated deployments

Data Protection & Observability: Data storage (S3), encryption (KMS), secrets management (Secrets Manager), monitoring (CloudWatch), logging, metrics, and tracing

Security Operations & Advanced Topics: CloudTrail, GuardDuty, threat detection, penetration testing, container security (Docker, Kubernetes), and Azure fundamentals & security controls

Labs

Deploy and secure a cloud environment
(Create a VPC with public/private subnets, configure EC2 instances, implement secure access controls, bastion host, security groups)

Implement IAM security
(Create users, groups, and policies, apply least privilege, and test access control scenarios)

Build a serverless API
(Deploy a Lambda-backed API using API Gateway and store data securely in S3 using IAM roles and Secrets Manager)

Monitor and investigate activity
(Configure CloudTrail and CloudWatch, analyze logs, and detect suspicious actions within a cloud environment)

CA203: Mobile Penetration Testing

15 Instructional Hours 27 CPEs 12 Labs

LIVE ONLINE OR ON-DEMAND ACCESS OR IN PERSON

BEGINNER TO INTERMEDIATE

This course provides a comprehensive and practical exploration of mobile application penetration testing, focusing on both Android and iOS platforms. It covers foundational concepts such as mobile security threats, operating system architectures, and security models, before progressing into hands-on techniques for identifying and exploiting vulnerabilities. Learners will gain experience in setting up a professional pentesting environment, performing static and dynamic analysis, intercepting network traffic, and applying OWASP Mobile Security guidelines. The course emphasizes real-world attack vectors, tools, and methodologies used by security professionals to assess and secure mobile applications in modern threat landscapes.

You Will Be Able To

- Analyze mobile application architectures (Android and iOS) to identify potential security weaknesses
- Perform static and dynamic analysis on mobile applications using industry tools
- Capture and inspect network traffic to detect insecure communications and vulnerabilities
- Identify and exploit common mobile vulnerabilities aligned with OWASP Mobile Top 10
- Set up and configure a complete mobile pentesting environment using tools like Genymotion, ADB, and Burp Suite
- Assess mobile applications against real-world attack vectors including insecure storage, authentication flaws, and data leakage

Who Should Attend

This course is designed for cybersecurity professionals, penetration testers, and developers who want to build or strengthen their expertise in mobile application security. It is also suitable for IT professionals and security enthusiasts seeking practical, hands-on experience in identifying and mitigating vulnerabilities in Android and iOS applications. A basic understanding of networking, operating systems, and security concepts is recommended for optimal learning outcomes.

Relevant Combat Roles

- Mobile Application Penetration Tester
- Cybersecurity Analyst (Mobile Security Focus)
- Red Team Operator
- Security Engineer (Application Security)
- Vulnerability Researcher
- Mobile Security Consultant

Topics Covered

Fundamentals of mobile penetration testing, threat landscape, and common attack vectors (data at rest/in motion, device-level threats)

Android & iOS security: architecture, sandboxing, security models, rooting and jailbreaking concepts

Setting up pentesting environments (Genymotion, Android Studio, ADB) and app deployment/debugging techniques

Network traffic analysis using tools like Burp Suite and proxy configurations

Static & dynamic analysis: APK decompilation (JADX, APKTool, MobSF), Frida, drozer, and runtime/log analysis

OWASP Mobile Top 10 risks, secure development practices, and real-world exploitation scenarios

Labs

Mobile Pentesting Lab Setup & Android Testing Environment
(Genymotion installation, Android Studio integration, Android SDK configuration, ADB setup, emulator deployment, and virtual device management for mobile security testing)

Android Application Deployment & Device Interaction
(Deploying APKs to Genymotion using ADB, drag-and-drop installation, emulator connectivity, and Android Debug Bridge workflows)

Android Static Analysis & Reverse Engineering
(Decompiling APKs, JADX usage, APKTool analysis, identifying hardcoded secrets, insecure storage, binary protections, and reverse engineering Android applications)

Mobile Traffic Interception & API Security Testing
(Burp Suite proxying, network traffic interception, insecure communication analysis, API attack-surface mapping, authentication testing, session management testing, and OWASP Mobile Top 10 validation)

Android Dynamic Analysis & Runtime Instrumentation
(Using Frida for runtime manipulation, dynamic hooking, SSL pinning bypass, drozer deployment, runtime testing, log analysis with Logcat, and behavioral analysis of Android applications)

Mobile Vulnerability Assessment & Exploitation Techniques
(Analyzing insecure communication, insecure storage, weak cryptography, security misconfigurations, certificate pinning bypass, deep link abuse, and advanced mobile attack vectors)

CA305: Enterprise Pentesting

31 Instructional Hours 41 CPEs 10 Labs

LIVE ONLINE OR ON-DEMAND ACCESS OR IN PERSON

INTERMEDIATE TO ADVANCED

This course provides a comprehensive introduction to enterprise penetration testing, focusing on how large organizations assess and strengthen their cybersecurity posture through simulated real-world attacks. It explores the evolution, importance, and methodologies of penetration testing, including reconnaissance techniques, vulnerability exploitation, and adversary emulation. Learners are guided through both theoretical foundations and practical tools used in modern security assessments, such as Nmap, Shodan, and recon-ng. The course also emphasizes real-world considerations, including legal constraints, responsible disclosure, and the role of advanced persistent threats (APTs), equipping learners with a holistic understanding of enterprise-level offensive security practices.

You Will Be Able To

- Conduct structured enterprise penetration testing engagements using industry-recognized phases and methodologies
- Perform passive and active reconnaissance using OSINT techniques and specialized tools
- Identify, analyze, and exploit vulnerabilities to assess real-world security risks
- Differentiate between penetration testing and vulnerability assessments and apply both appropriately
- Understand and emulate adversary behavior using MITRE ATT&CK and adversary emulation frameworks
- Apply ethical, legal, and responsible disclosure practices in cybersecurity engagements

Who Should Attend

This course is designed for aspiring and intermediate cybersecurity professionals who want to develop practical skills in penetration testing within enterprise environments. It is suitable for individuals with a basic understanding of networking and operating systems who are looking to transition into offensive security roles or enhance their ability to assess and defend complex IT infrastructures. The course is also valuable for security analysts and IT professionals seeking to understand attacker methodologies and improve organizational security posture.

Relevant Combat Roles

- Penetration Tester (Ethical Hacker)
- Red Team Operator
- Cybersecurity Analyst
- Threat Intelligence Analyst
- Security Consultant
- Incident Response Analyst

Topics Covered

Foundations of enterprise penetration testing, including its importance and the impact of corporate data breaches

Penetration testing methodologies, engagement phases, and types (black-box, gray-box, white-box)

Comparison of penetration testing and vulnerability assessment, along with legal considerations and responsible disclosure

Digital reconnaissance, OSINT techniques, and use of tools such as Nmap, Shodan, WHOIS, and Nikto

Network scanning, enumeration, vulnerability identification, and adversary emulation with threat modeling

Advanced concepts including APTs, attack lifecycle, MITRE ATT&CK framework, and security assessment limitations

Labs

Adversary Emulation & MITRE ATT&CK Operations
(CALDERA automation, ATT&CK mapping, and ATT&CK Navigator usage)

Enterprise Reconnaissance & Network Enumeration
(OSINT investigations, Nmap scanning, DNS enumeration, and infrastructure discovery)

Post-Exploitation & Defense Evasion Techniques
(PowerShell Empire usage, obfuscation techniques, and stealth operations)

Advanced Exploitation & Windows Tradecraft
(buffer overflow exploitation, LOLBins abuse, and privilege escalation)

CA306: Security of Emerging Intelligent System

27 Instructional Hours 33 CPEs 6 Labs

LIVE ONLINE OR ON-DEMAND ACCESS OR IN PERSON

INTERMEDIATE

This course provides a comprehensive and practical exploration of securing modern intelligent systems, including artificial intelligence, autonomous platforms, and cyber-physical infrastructure. It examines how these systems integrate sensing, decision-making, and physical actuation, and how vulnerabilities across these layers can lead to real-world consequences. Learners are introduced to foundational concepts such as system architecture, trust modeling, and threat analysis, as well as advanced topics including adversarial machine learning, supply chain security, IoT ecosystems, and resilience engineering. The course emphasizes a consequence-aware approach to cybersecurity, equipping learners with frameworks and methodologies to analyze, defend, and design secure, resilient intelligent systems operating in dynamic and high-risk environments.

You Will Be Able To

- Analyze the architecture of intelligent systems across physical, sensing, control, decision, and coordination layers
- Identify and evaluate security risks in AI, autonomous systems, and cyber-physical environments
- Assess adversarial threats such as evasion attacks, data poisoning, and model exploitation
- Design secure deployment strategies and resilient defenses for AI and IoT systems
- Apply threat modeling techniques considering state, timing, and real-world consequences
- Evaluate supply chain risks and implement trust and provenance mechanisms

Who Should Attend

This course is designed for cybersecurity professionals, AI practitioners, engineers, and students with a foundational understanding of computing or security who want to specialize in securing intelligent systems. It is particularly suitable for individuals seeking to expand into areas such as AI security, IoT, autonomous systems, and critical infrastructure protection. The course is also valuable for researchers and technical analysts aiming to understand how digital vulnerabilities translate into physical-world risks and operational consequences.

Relevant Combat Roles

- AI Security Engineer
- Cyber-Physical Systems Security Analyst
- Threat Intelligence Analyst (AI/IoT focus)
- Autonomous Systems Security Specialist
- Industrial Control Systems (ICS/OT) Security Engineer
- Red Team / Adversarial ML Specialist

Topics Covered

Foundations & Architecture: Layered system design, trust and threat modeling, and consequence-aware security.

AI/ML Risks: Vulnerabilities across the lifecycle—from data to deployment.

Adversarial & Agentic AI: Attacks like evasion/poisoning and risks from autonomous decision-making.

Autonomous & Cyber-Physical Systems: Securing navigation, control, sensors, and critical infrastructure.

IoT & Supply Chain: Hardware trust, secure updates, and SBOM/HBOM transparency.

Monitoring & Resilience: Anomaly detection, automated response, and fail-safe system design.

Labs

Intelligent System Threat Modeling & Attack Surface Analysis
(system architecture mapping, attack path identification, and consequence surface analysis)

Adversarial Machine Learning & Model Security Testing
(evasion attacks, data poisoning simulations, and defensive technique evaluation)

IoT Security Assessment & Protocol Analysis
(protocol weaknesses, trust analysis, and IoT botnet exposure assessment)

Autonomous System Incident Response & Compromise Analysis
(navigation spoofing investigations, command injection analysis, and incident response operations)

CA204: Cyber Security Reporting

7 Instructional Hours 10 CPEs 3 Labs

LIVE ONLINE OR ON-DEMAND ACCESS OR IN PERSON

BEGINNER

This course provides a comprehensive foundation in academic writing, technical documentation, and cybersecurity reporting. It guides learners through essential research practices, literature analysis, structured writing techniques, and proper formatting and referencing standards. Additionally, it introduces AsciiDoc as a modern tool for technical documentation and explores its practical use in creating structured, publishable content. The course concludes with applied cybersecurity reporting concepts, including vulnerability assessments and standardized frameworks such as CVE, CWE, and CVSS. Overall, it equips learners with the skills needed to produce clear, professional, and evidence-based reports in both academic and cybersecurity contexts.

You Will Be Able To

- Apply appropriate research methods (qualitative, quantitative, and mixed) to gather and analyze data
- Conduct structured literature reviews to identify trends, gaps, and insights in existing research
- Produce well-organized academic and technical documents with clear structure, tone, and style
- Use proper formatting and referencing techniques (APA, MLA, Chicago) to maintain academic integrity
- Create professional technical documentation using AsciiDoc and compile it into multiple formats
- Develop cybersecurity reports, including vulnerability assessments and risk scoring using CVSS

Who Should Attend

This course is designed for students, researchers, and professionals who need to develop strong writing and reporting skills, particularly in technical or cybersecurity domains. It is suitable for individuals involved in academic research, technical documentation, or security assessments who want to improve clarity, structure, and professionalism in their written communication. No advanced writing background is required, but a basic understanding of research or IT concepts will be beneficial.

Relevant Combat Roles

- Cybersecurity Analyst
- Penetration Tester / Ethical Hacker
- Threat Intelligence Analyst
- Technical Writer (Cybersecurity / IT)
- Security Operations Center (SOC) Analyst
- Research Analyst

Topics Covered

Academic Writing & Research
Basics of academic writing, clarity, and key research methods (qualitative & quantitative).

Literature Review
Finding, analyzing, and evaluating existing research for relevance and credibility.

Structure, Style & Referencing
Proper document organization, formal tone, and citation styles (APA, MLA, Chicago).

Plagiarism & Ethics
Avoiding plagiarism through correct citation, paraphrasing, and integrity practices.

Technical Documentation & AsciiDoc
Clear technical writing, AsciiDoc syntax, theming, and documentation tools.

Cybersecurity Reporting & Quality
Reporting principles, CVE/CWE/CVSS frameworks, and best practices for quality assurance.

Labs

Academic Research & Professional Reporting
(research methods, academic report writing, and structured technical documentation)

AsciiDoc Technical Documentation & Publishing
(AsciiDoc formatting, tables, code snippets, and PDF/HTML document compilation)

Cybersecurity Assessment & Professional Reporting
(vulnerability assessments, executive summaries, technical findings, and remediation reporting)

CVSS Risk Assessment & Vulnerability Scoring
(CVSS scoring, vulnerability severity analysis, and risk rating justification)

CA201: Digital Forensic and Incident Response

18 Instructional Hours 27 CPEs 9 Labs

LIVE ONLINE OR ON-DEMAND ACCESS OR IN PERSON

BEGINNER / INTERMEDIATE

This course provides a comprehensive, hands-on introduction to Digital Forensics and Incident Response (DFIR), focusing on the structured identification, collection, analysis, and preservation of digital evidence within modern security operations. It covers both foundational and advanced concepts, including detection and triage, incident response lifecycle, evidence acquisition, host and memory forensics, threat intelligence integration, and real-world investigation workflows. Learners are guided through practical methodologies used in enterprise environments, emphasizing analytical reasoning, evidence correlation across systems, and defensible decision-making during active security incidents.

You Will Be Able To

- Conduct structured digital investigations from alert triage to full incident reconstruction
- Acquire, preserve, and validate digital evidence while maintaining chain of custody
- Analyze host, disk, and memory artifacts to identify attacker behavior
- Apply threat intelligence and MITRE ATT&CK to guide investigations and detection
- Perform incident response activities including containment, eradication, and recovery
- Correlate multi-source evidence (endpoint, network, identity, cloud) to build attack timelines

Who Should Attend

This course is designed for students and cybersecurity professionals with a foundational understanding of security concepts who want to specialize in DFIR. It is suitable for aspiring incident responders, SOC analysts, and digital forensic practitioners seeking practical, real-world skills in investigating and responding to cyber incidents. It is also valuable for professionals transitioning into blue team roles or aiming to deepen their investigative and analytical capabilities.

Relevant Combat Roles

- SOC Analyst (Tier 1–3)
- Incident Responder
- Digital Forensic Analyst
- Threat Hunter
- Cyber Threat Intelligence Analyst
- Security Operations Engineer

Topics Covered

DFIR Basics: Mindset, workflows, SOC roles

Detection & Intel: Triage, ATT&CK, threat intelligence

Incident Response: Lifecycle, containment, recovery

Forensics & Evidence: Collection, validation, analysis

Threat Analysis: Malware, phishing, lateral movement

Advanced & Reporting: Hunting, automation, reporting

Labs

DFIR Lab Environment Design & Setup
(virtual machines, logging pipelines, Autopsy, FTK Imager, and Volatility setup)

Disk Forensics & Evidence Analysis
(forensic imaging, deleted file recovery, file-system artifact analysis, and SleuthKit/Autopsy investigations)

Incident Triage & Investigation Operations
(alert triage, affected system scoping, attacker activity reconstruction, and telemetry analysis)

Memory Forensics & Timeline Reconstruction
(RAM capture, Volatility analysis, process investigation, anomaly detection, and attack timeline creation)

Digital Forensics & Memory Analysis
(Volatility, Autopsy, Foremost, Windows artifacts, and memory forensics)

CA404: Adversary Emulation with MITRE ATT&CK

41 Instructional Hours 51 CPEs 10 Labs

LIVE ONLINE OR ON-DEMAND ACCESS OR IN PERSON

ADVANCED

This course delivers a comprehensive, hands-on introduction to adversary emulation (AE), focusing on replicating real-world attacker behavior using the MITRE ATT&CK framework. Participants will learn how advanced persistent threats (APTs) operate, how to model their tactics, techniques, and procedures (TTPs), and how to assess organizational defenses against realistic threat scenarios. The course bridges the gap between red and blue teams by integrating cyber threat intelligence (CTI), enabling organizations to evaluate security holistically across people, processes, and technology.

You Will Be Able To

- Conduct adversary emulation engagements based on real-world threat intelligence
- Map cyber threat intelligence to the MITRE ATT&CK framework
- Develop adversary profiles and build TTP-based attack scenarios
- Plan, implement, and execute adversary emulation operations
- Evaluate detection and response capabilities across the attack lifecycle
- Use tools such as ATT&CK Navigator, Caldera, and Atomic Red Team
- Measure defensive effectiveness and identify security gaps
- Produce actionable reports to improve organizational resilience

Who Should Attend

This course is designed for cybersecurity professionals who want to simulate real adversary behavior and improve defensive capabilities, including:

- Red Team Operators
- Blue Team / SOC Analysts
- Threat Hunters
- Cyber Threat Intelligence Analysts
- Penetration Testers transitioning to advanced assessments
- Security Engineers and Architects
- Incident Responders

Relevant Combat Roles

- Red Team Operator
- Purple Team Practitioner
- SOC Analyst (Tier 2–3)
- Threat Intelligence Analyst
- Detection Engineer
- Security Operations Engineer
- Cyber Defense Analyst

Topics Covered

Adversary Emulation Fundamentals and Methodology

Advanced Persistent Threats (APTs) and attacker motivations

MITRE ATT&CK Framework (tactics, techniques, procedures)

Adversary lifecycle: reconnaissance impact

Cyber Threat Intelligence (collection, enrichment, mapping)

ATT&CK-based detection and defense strategies

Visualization using ATT&CK Navigator

Engagement planning and rules of engagement

TTP development, implementation, and execution

Measuring detection, prevention, and response effectiveness

Real-world adversary emulation plans (FIN6, APT3, APT29)

Labs

Adversary Emulation Lab & Environment Operations
(Splunk Attack Range setup, lab deployment, and adversary emulation environments)

Threat Intelligence & MITRE ATT&CK Mapping
(real-world CTI mapping, ATT&CK techniques, and ATT&CK Navigator visualization)

Adversary Profiling & TTP Development
(adversary profiles, threat actor research, and TTP outline creation)

Initial Access & Exploitation Simulations
(phishing simulations, exploitation scenarios, and initial access techniques)

Post-Exploitation & Lateral Movement Operations
(lateral movement, credential access, persistence, and privilege escalation techniques)

Command & Control (C2) & Data Exfiltration Simulations
(C2 communications, data exfiltration, and adversary tradecraft simulations)

Adversary Emulation Automation & Detection Validation
(Atomic Red Team, CALDERA automation, detection analysis, and defensive control validation)

Professional Adversary Emulation Reporting
(emulation findings, remediation recommendations, and security assessment reporting)