Cybersecurity Bootcamp (Ethical Hacking, Digital Forensics and SOC)

Go from curious to job-ready blue and red team operator who can hack, hunt and investigate across the full attack lifecycle.

Duration: multi-track bootcamp | Certificate: NUEXUS Cybersecurity Bootcamp certificate | Format: Online or onsite, 1-on-1 or batch | NUEXUS certificate on completion

OVERVIEW

The Cybersecurity Bootcamp is a multi-track, hands-on program that trains you across three career-defining disciplines: offensive security (ethical hacking and penetration testing), digital forensics and incident response, and Security Operations Center (SOC) analysis and threat detection. You learn by attacking, defending and investigating in real lab environments built by practicing security professionals, not by watching slides. It is mentor-led by certified trainers, delivered online from anywhere or onsite in Islamabad, in a batch or 1-on-1, and scheduled on weekends or weekday evenings so it fits around work. You finish with a portfolio of real work, a working command of industry-standard tools, and a NUEXUS completion certificate.

SKILLS YOU WILL GAIN

Networking Fundamentals | Linux | Security Concepts | Threat Analysis | SOC Operations | Vulnerability Assessment | Ethical Hacking Basics | Incident Response | Tooling | Reporting

WHAT YOU WILL BE ABLE TO DO

- Set up and safely operate a security lab with Kali Linux and industry-standard tooling, and understand the legal and ethical boundaries of authorized testing
- Run a full penetration test workflow: reconnaissance, scanning, enumeration, exploitation of common web and network vulnerabilities, and clear reporting of findings
- Detect, triage and respond to security incidents as a SOC analyst using SIEM log analysis, alerting and the MITRE ATT&CK framework
- Perform core digital forensics: acquire and preserve evidence, analyze disk and memory artifacts, and reconstruct what an attacker did while maintaining chain of custody
- Identify and explain common vulnerabilities such as the OWASP Top 10, weak authentication, misconfigurations and phishing, and recommend practical fixes
- Produce professional security reports and an incident write-up you can show employers as portfolio evidence

WHO IT IS FOR

- Career switchers and fresh graduates who want a structured, hands-on entry into cybersecurity across offense, defense and investigation
- IT support, sysadmin, help desk and networking staff who want to move into a security role
- Aspiring SOC analysts, penetration testers or incident responders who want practical, tool-driven skills rather than theory alone
- Students and self-taught learners who have dabbled in security and want a guided, lab-based path to job readiness
- Developers and DevOps engineers who want to understand how attackers think and how defenders detect them

PREREQUISITES

- Comfortable using a computer and the internet; able to install software and follow technical instructions
- Basic familiarity with networking concepts (IP addresses, ports, what a firewall does) is helpful but not required; we cover the essentials
- No prior hacking, forensics or SOC experience needed, this bootcamp is beginner-friendly and starts from fundamentals
- Willingness to spend time in hands-on labs outside live sessions to build real muscle memory

WHAT'S INCLUDED

- Mentor-led live sessions, online or onsite, in batch or 1-on-1
- Hands-on labs and real-world projects, not slides alone
- Recordings of your own sessions to revisit anytime
- Exam-aligned study material and practice questions
- Doubt-clearing and revision support through the program
- A verifiable NUEXUS completion certificate
- Career and next-step guidance after you finish

COURSE CURRICULUM

1 Cybersecurity Foundations and Lab Setup

- Core security concepts: CIA triad, threats, vulnerabilities, risk and attack surface
- Building your home lab with virtualization, Kali Linux and vulnerable target machines
- Linux and Windows command-line essentials for security work
- Networking refresher: TCP/IP, ports, protocols, DNS and how traffic flows
- Law, ethics, authorization and rules of engagement for any authorized testing

2 Networking, Systems and Cryptography Essentials

- Network architecture, firewalls, VPNs and network segmentation
- Common services and protocols and how they are attacked and defended
- Cryptography basics: hashing, symmetric and asymmetric encryption, TLS and PKI
- Authentication, authorization, identity and access management fundamentals
- Secure configuration and hardening of hosts and services

3 Ethical Hacking: Reconnaissance and Scanning

- Passive and active reconnaissance and open-source intelligence (OSINT)
- Footprinting a target and mapping the attack surface
- Network scanning and host discovery with Nmap
- Service enumeration and vulnerability scanning
- Documenting findings and building an attack plan

4 Ethical Hacking: Exploitation and Web Application Attacks

- The OWASP Top 10: injection, broken authentication, XSS, misconfigurations and more
- Exploiting common network and service vulnerabilities with Metasploit and manual techniques
- Web app testing with Burp Suite: intercepting, tampering and testing requests
- Password attacks, credential harvesting and privilege escalation basics
- Social engineering and phishing concepts and how they are used in real attacks

5 Post-Exploitation, Reporting and Vulnerability Management

- Privilege escalation on Linux and Windows and maintaining access concepts
- Pivoting and lateral movement fundamentals
- Writing a clear, professional penetration test report with risk ratings and remediation
- Vulnerability management: prioritization, patching and retesting
- Mapping attacker techniques to the MITRE ATT&CK framework

6 SOC Analysis: Monitoring, SIEM and Threat Detection

- The SOC role, tiers, workflows and analyst day-to-day
- Log sources, log analysis and building detections
- Working with a SIEM to search, correlate and alert on suspicious activity
- Detecting common attacks: brute force, malware, phishing and lateral movement
- Using threat intelligence and MITRE ATT&CK to guide detection

7 Incident Response and Threat Hunting

- The incident response lifecycle: preparation, detection, containment, eradication, recovery, lessons learned
- Alert triage, escalation and severity classification
- Proactive threat hunting hypotheses and techniques
- Endpoint and network telemetry analysis
- Building an incident timeline and communicating findings to stakeholders

8 Digital Forensics and Evidence Analysis

- Forensic fundamentals, chain of custody and evidence handling
- Disk imaging and file system analysis with tools such as Autopsy
- Memory forensics and volatile data acquisition
- Recovering deleted files, browser, log and registry artifacts
- Malware artifact analysis basics and reconstructing attacker activity

9 Capstone: End-to-End Attack, Detect and Investigate

- Run an authorized penetration test against a provided target environment
- Detect and triage the same activity from the SOC and SIEM perspective
- Perform a forensic investigation and reconstruct the attacker's steps
- Produce a full deliverable set: pentest report, incident report and forensic findings
- Present and defend your findings to your mentor and cohort

CAREER OUTCOMES

SOC Analyst | Security Analyst | Junior Penetration Tester | IT Security Associate | Blue Team Member

CERTIFICATION

On finishing the bootcamp and completing the practical assessment and capstone project, you earn the NUEXUS Cybersecurity Bootcamp certificate, evidence that you have hands-on skills across ethical hacking, digital forensics and SOC operations. The bootcamp is also strong preparation and a solid foundation if you later pursue industry certifications such as CEH, CompTIA Security+ or blue-team credentials, but there are no guarantees of a certification pass or a job; the certificate reflects the work you complete and the skills you demonstrate.