TAAS IT
Academy

Cybersecurity Engineering

Penetration Testing With Generative AI & Real World Projects

Course Curriculum

www.taasitacademy.com

Contents

Tools we're going to use during the course

- **Kali Linux –** Ready-made OS packed with all essential pentesting and security tools. Saves setup time and ensures compatibility.
- **Metasploit –** Framework to safely simulate attacks on systems. Helps understand vulnerabilities and their impact.
- **Nmap –** Discovers devices, open ports, and services on networks. Essential for mapping and assessing network security.
- **Zenmap –** GUI version of Nmap. Makes network scanning easier and more visual for analysis.
- **Wireshark –** Captures and inspects network traffic. Helps detect anomalies and malicious activity.
- **Snort –** Monitors network traffic in real time. Alerts on suspicious behavior to prevent attacks.
- **Burp Suite –** Intercepts and analyzes web traffic. Detects vulnerabilities in authentication, sessions, and input validation.
- **SQLmap –** Automates detection and exploitation of SQL injection flaws. Secures databases against attackers.
- **Gobuster –** Finds hidden directories, files, and subdomains. Identifies potential attack surfaces on web servers.
- **Hydra –** Performs password-cracking attacks. Tests authentication strength and identifies weak credentials.
- **Ethical Hacker ChatGPT / PentesterGPT – AI tools for automating security tasks, analyzing vulnerabilities, and simulating attacks efficiently.**

Abstract

Course Insights

6 months
(5 Months Course + 1 Month Real World Project)
80+ Hours
Placement Assistance- Until Hired

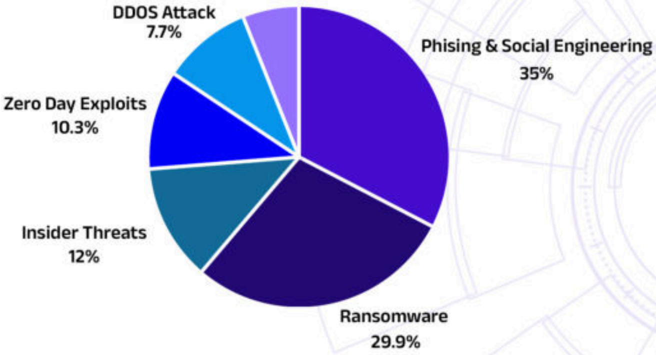
The Fullstack Cybersecurity Engineering curriculum offers a complete, hands-on learning journey through core cybersecurity concepts, operating system fundamentals, network defense, and offensive security. Students gain practical experience with tools like Kali Linux, Wireshark, Metasploit, and Burp Suite while learning to identify and mitigate vulnerabilities, perform penetration tests, and respond to real-world threats through red and blue team operations.

The program also covers modern topics like AIpowered security, bug bounty hunting, and OSINT investigations, along with interactive Capture the Flag (CTF) challenges to build realworld problem-solving skills. With a strong focus on career readiness, it includes capstone projects, resume and portfolio building, and freelancing guidance—making it ideal for launching or advancing a career in today's fastgrowing cybersecurity field.

This curriculum equips students with holistic cybersecurity expertise, combining offensive and defensive strategies with cutting-edge AI integration. Learners not only gain hands-on technical skills but also build professional portfolios and prepare for global certifications. Whether aiming for roles in SOC, Red Teaming, threat intel, or freelance bounty hunting, this program offers a strategic entry point into a high-demand industry. It's future-proof, practical, and career-focused— perfect for launching a cybersecurity career or upskilling in a rapidly evolving threat landscape.

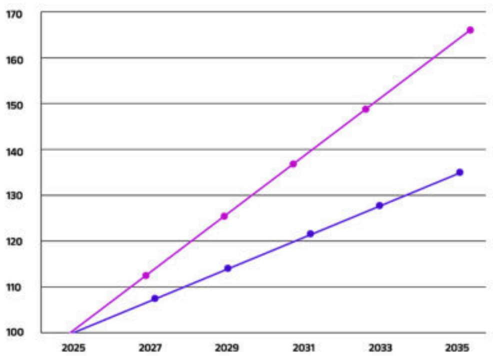
The Era of Cyber Security with Gen AI

We are at the dawn of a new age in cybersecurity— one shaped not just by evolving threats but by the tools used to fight them. With the integration of Generative AI into both offensive and defensive cyber capabilities, the landscape is shifting rapidly. Organizations now face not only known threats but an entirely new class of AI-augmented attacks capable of morphing and adapting in real-time. In response, cybersecurity professionals must leverage the same technolo-



Global Cyber Threat Distribution 2024

Cyberattacks are becoming increasingly sophisticated and damaging. Phishing remains the leading threat, accounting for 31% of breaches, followed by ransomware at 28%, often targeting critical sectors like healthcare and government. Zero-day exploits and insider threats have surged by more than 20% year-over-year, many now powered by AI tools and LLMs, making detection and response more challenging than ever.



Projected Job Growth Index (Year 2025 - 2035)

- 🟪 Regular Cybersecurity Engineer
- 🟪 Cybersecurity Engineer With Gen AI Knowledge

From **2025 to 2035**, demand for cybersecurity engineers is projected to grow by **35%**, while roles requiring generative AI expertise are expected to surge by **65%**. As AI reshapes cyber defense, professionals skilled in both cybersecurity and GenAI will lead the next wave of innovation and impact.

Cybersecurity is no longer a traditional IT function. it has become a dynamic, AI-augmented battlefield. As generative AI continues to evolve, so too does the complexity and speed of cyber threats. In this rapidly shifting landscape, the future of cyber defense will be defined by those who not only understand these technologies but also know how to harness and innovate with them. This course is designed to equip learners not just with technical tools but with the mindset, automation skills, and strategic vision required to lead in this new era of cybersecurity.

Module 1

Cybersecurity Foundations & Principles

Develop a thorough understanding of the mindset, methodologies, and principles essential to modern cybersecurity practices. This module establishes a foundation for strategic thinking and effective defense in today's threat landscape.

Developing the Cybersecurity Mindset

Explore the attacker vs. defender paradigm and cultivate a proactive, risk-aware approach to Cybersecurity. Learn how to think like both attackers and defenders to anticipate threats and strengthen defenses.

Cybersecurity Terminologies & Acronyms

Familiarize yourself with key terminology and acronyms used in the Cybersecurity field. This ensures clear communication within technical teams, management, and across organizations.

Common Cybersecurity Attack Types

Gain insights into prevalent and emerging attack vectors, including phishing, malware, denial-of-service (DoS), and zero-day exploits. Understand techniques used by attackers and learn strategies to prevent and mitigate attacks.

The CIA Triad: Confidentiality, Integrity, and Availability

Delve into the foundational security model that informs secure system design and policy-making. Analyze its real-world impact on protecting sensitive information and ensuring service reliability.

Encoding & Data Representation Fundamentals

Learn the basics of character encoding, URL encoding, and Base64. Understand how data is represented, transmitted, and processed—essential knowledge for web security, secure data handling, and recognizing manipulation attempts by attackers.

Introduction to Cybersecurity Framework, Policy, and Compliance (NIST, ISO, GDPR, HIPAA, PCI-DSS)

Learn the fundamentals of Cybersecurity frameworks, organizational policies, and regulatory requirements. Explore how frameworks like NIST and ISO provide best practices, how internal policies enforce these practices, and how compliance with standards such as GDPR, HIPAA, and PCI-DSS ensures legal obligations are met. Understand how adopting these measures helps protect sensitive data, strengthen security posture, and reduce organizational risk.

Cybersecurity Career Pathways

Discover the diverse career opportunities within Cybersecurity, including roles in Red Teaming, Blue Teaming, Governance, Risk & Compliance (GRC), and emerging fields like AI-driven security. Understand the skills and pathways to enter these roles.

Potential Job Role By Module:

- ▶ Cybersecurity Intern / IT Intern
- ▶ Cybersecurity Assistant / IT assistant

Module 2

Operating system Fundamentals for Cybersecurity

This module introduces learners to the core concepts of operating systems and their role in Cybersecurity. Students will explore Linux and Windows environments, understand file systems and permission models, manage users, groups, and processes securely, and learn basic command-line operations. The module also covers virtualization for safe testing and introduces Python scripting for security automation.

Introduction to Operating Systems

Understand what an operating system is and how it manages hardware, software, users, and processes. Learn the key differences between Linux and Windows and why operating system security is critical in modern Cybersecurity.

Introduction to virtualization

Understanding the concept of virtualization and why used them as isolated lab environments. Further Importance of safe testing without affecting the real systems

Command line interface

Develop basic proficiency with Linux and Windows command-line interfaces. Learn essential commands to navigate directories, view files, and interpret system output. These are skills required for working with Cybersecurity tools and servers.

Linux Fundamentals for Cybersecurity

Get introduced to Linux concepts . Learn why Kali Linux is widely used in security training and gain familiarity with the Linux environment without requiring prior Linux experience.

File systems and Permission Structures

Understand how file systems are organized and how permission models work. Learn to configure access controls that prevent unauthorized access and privilege escalation

User, group and Process Management

Effectively manage users, groups and system processes to minimize vulnerabilities and ensure a secure operational environment

Introduction to windows system security

Explore security mechanism within windows environment including User account control , group policy objects and windows event system.

Learning python for security automation

Write and deploy scripts to create security tools, routine security tasks like system updates and configuration audits

Potential Job Role By Module:

- IT Support
- System Admin
- Junior Security Analyst
- SOC Analyst

Module 3

Networking Fundamentals & Network Security

This module covers networking and network security fundamentals. Students will learn how data flows, key network components, and gain hands-on skills in scanning, traffic analysis, firewalls, VPNs, and intrusion detection using tools like Nmap, Zenmap, Wireshark, and Snort, preparing them for entry-level cybersecurity roles.

Understanding the OSI & TCP/IP Models

Learn how data traverses through layered models in the day-to-day life of computers. This foundational knowledge is crucial for understanding cybersecurity operations.

Basics of Networking

Explore key components such as topologies, protocols, ports, and the client-server model. Understand these concepts from an IT and cybersecurity perspective for a deeper understanding of networks.

IP Addressing, Subnetting, and Routing

Master IP addressing and subnetting to segment networks effectively. Learn routing fundamentals to manage data flow and establish security boundaries.

Network Scanning with Nmap & Zenmap

Use industry-standard reconnaissance tools to scan networks, discover open ports and services, and identify potential vulnerabilities.

Traffic Analysis with Wireshark

Capture and dissect network packets using Wireshark. Gain hands-on experience with OSI and TCP/IP concepts. Analyze DNS traffic and other protocols, detect anomalies, and identify signs of malicious activity.

Firewall Concepts and Implementation

Understand principles of packet filtering, stateful inspection, proxy firewalls, host-based firewalls, and next-generation firewalls. Learn how these tools create robust perimeter defense.

VPNs and Secure Communication

Study virtual private networks (VPNs) and how they protect sensitive data during transmission, ensuring secure communication over public networks.

Network Access Control (NAC)

Learn NAC strategies that enforce role-based and identity-aware access, ensuring only authorized users and devices connect to the network.

DNS and Network Protocol Analysis

Analyze DNS traffic and other network protocols to detect anomalies, identify misuse, and uncover signs of malicious activity.

Intrusion Detection and Prevention Systems (IDS/IPS)

Explore IDS and IPS concepts, tools that detect threats in real-time, issue alerts, and prevent attacks. Gain hands-on experience with the high-demand tool Snort.

Key Tools : nmap, zenmap, and snort

Potential Job Role By Module:

- Network Security Analyst (Entry-Level)
- Junior SOC Analyst
- Network Support Technician

Module 4

Red Team Operations – Web Application Security & Bug Bounty Hunting

Explore the offensive side of web application security through real-world penetration testing techniques and responsible vulnerability disclosure. This module immerses students in the bug bounty ecosystem, focusing on high-impact web vulnerabilities and practical ex-

Foundations of Web Technologies

Gain a thorough understanding of the web stack —HTTP/HTTPS, cookies, sessions, and authentication —and how these components play a critical role in application security.

Web Reconnaissance and Target Profiling

Apply both passive and active reconnaissance techniques,including OSINT, subdomain enumeration, and directory brute-forcing to uncover potential entry points.

Exploitation of Common Web Vulnerabilities

Hands-on exploitation of widespread web flaws such as business logic vulnerabilities, authentication and authorization bypass , directory traversal , Broken access conrtol (BAC), SQLi and Cross-Site Scripting (XSS),with proof-of-concept demonstrations.

Web Penetration Testing Tools

Develop hands-on experience with essential web security testing tools such as Burp Suite, SQLmap, Gobuster, and Hydra to identify, test, and validate common web application vulnerabilities.

Manual Testing vs. Automated Scanning

Compare the effectiveness of manual testing for logic flaws and complex bugs versus the speed and coverage of automated scanners.

Bug Bounty Program Case Studies

Analyze real-world vulnerability submissions to platforms like HackerOne and Bugcrowd, highlighting techniques, communication, and payout strategies.

Effective Bug Report Writing

Learn to structure and submit professional-quality vulnerability reports that clearly communicate i mpact, reproduction steps, and mitigation guidance.

Potential Job Role By Module:

- Bug Hunter
- Web application penetration tester
- Application freelance tester

Module 5

Vulnerability Assessment & CVE Fundamentals

Learn the basics of software vulnerabilities, how CVEs track them, and how severity is measured with CVSS. Explore vulnerability databases, assessment tools like Nessus and OpenVAS, and understand patching, remediation, and responsible disclosure. Gain foundational knowledge in threat intelligence and managing security risks.

CVSS Scoring System

Understand how vulnerabilities are scored using CVSS (Common Vulnerability Scoring System) to measure severity and risk.

Vulnerability Databases & Reporting

Gain a deep understanding of SIEM architecture and functionalities. Learn how to centralize data collection and perform real-time threat correlation for situational awareness.

Vulnerability Assessment Techniques

Introduction to scanning tools (like Nessus, OpenVAS, Nmap scripts) and how to identify vulnerabilities in systems and web apps.

Patch Management & Remediation

Understand how vulnerabilities are fixed, patching best practices, and tracking mitigations.

Responsible Disclosure & Threat Intelligence

Learn how vulnerabilities are reported responsibly, how organizations track them, and how threat intelligence is used to prioritize remediation.

Ley tools : NVD, Nessus, OpenVAS and Nmap

Potential Job Role By Module:

- Vulnerability Analyst
- Junior Security Analyst
- Threat Intelligence Intern

Module 6

Blue Team Operations

This module introduces students to the defensive side of Cybersecurity, focusing on monitoring, threat detection, and incident response. Learners will explore the structure and function of Security Operations Centers (SOC), log management in Windows and Linux, and the use of SIEM tools. The module also covers threat intelligence using the MITRE ATT&CK framework, basic malware analysis, and hands-on exercises such as phishing email analysis to strengthen real-world defensive skills.

Introduction to Cyber Defense, SOC & SOC Structures

Understand the critical role of Blue Teams in defending organizations against cyber threats. Learn how SOCs operate, the structure of SOC tiers (Tier 1, Tier 2, Tier 3), and the responsibilities of security analysts in monitoring, investigating, and responding to security events.

Foundations of Windows & Linux Log Management

Explore how logs are generated and collected in Windows and Linux systems. Learn about common log sources such as system events, application logs, and network activity, and understand how monitoring logs helps detect anomalies, policy violations, and security incidents

Introduction to SIEM Tools and Their Usage

Learn the purpose and capabilities of Security Information and Event Management (SIEM) platforms. Gain hands-on knowledge of basic SIEM functions including log ingestion, searching, alerting, and simple correlation to detect suspicious behavior.

Understanding Threat Intelligence (MITRE ATT&CK)

Learn how threat intelligence helps organizations anticipate and respond to attacks. Explore the MITRE ATT&CK framework to understand attacker tactics, techniques, and procedures (TTPs), and how analysts use this knowledge to map, detect, and mitigate threats.

Malware Fundamentals & Detection Basics

Understand common types of malware such as viruses, trojans, ransomware, and spyware. Learn their typical behaviors, indicators of compromise (IOCs), and basic detection and response techniques used in enterprise environments.

Use Case: Phishing Email Analysis

Apply defensive techniques to analyze phishing emails. Identify indicators of compromise, social engineering tactics, malicious attachments or links, and practice effective response and reporting procedures.

Potential Job Role By Module:

- ▶ SOC Analyst (Tier 1)
- ▶ Incident Response Analyst (Junior)
- ▶ Security Monitoring Analyst
- ▶ Digital Forensics Assistant

Module 7

Generative AI for Cybersecurity

This module introduces students to the growing role of Generative AI in cybersecurity. Learners will understand the fundamentals of AI models like LLMs and transformers, and explore practical applications in security operations, threat detection, report automation, and simulation. The module emphasizes hands-on use of AI tools for cybersecurity, ethical considerations, and safe usage practices. Students will also explore emerging trends and career opportunities where AI complements

Introduction to Generative AI and Security Applications

Understand the basics of generative AI, including LLMs and transformer models. Explore how AI is being applied in cybersecurity tasks such as automating analysis, simulating attacks, and generating actionable insights.

Using Prompt Engineering for Security Outcomes

Learn how to craft effective prompts to guide AI tools toward producing accurate and relevant outputs for cybersecurity tasks. Explore AI tools specifically fine-tuned for security, including Ethical Hacker ChatGPT, PentesterGPT, and HackerGPT Lite, for tasks like vulnerability discovery, reporting, and simulation exercises.

AI in Cybersecurity Use Cases

Learn how AI is applied in real-world cybersecurity operations. Explore practical applications such as automating threat detection and log analysis, generating security reports or vulnerability summaries, and assisting in detecting phishing attacks and social engineering attempts.

Ethics, Bias & Safe AI Usage

Understand the potential risks of AI, including bias, inaccuracies, and misuse. Learn best practices for using AI responsibly in security operations and how to validate AI-generated outputs.

Future of AI in Cybersecurity

Discover emerging trends in AI-driven cybersecurity, including its role in automation, threat intelligence, and offensive security simulations. Discuss career opportunities combining AI and cybersecurity expertise.

Key tools : Chatgpt, Ethical Hacker ChatGPT, PentesterGPT, and HackerGPT Lite

Potential Job Role By Module:

- AI security analyst
- Cybersecurity Automaton Engineer
- Security Aanalyst with GenAI specialization
- Prompt Engineer (Cybersecurity Focus)

Module 8

Open Source Intelligence (OSINT)

Master the art of gathering actionable intelligence from publicly accessible sources. This module prepares you to conduct structured Cyber investigations, analyze digital footprints, and leverage open data for profiling, attribution, and threat validation

Introduction to OSINT and Its Role in Cybersecurity

Gain a foundational understanding of OSINT, its importance in threat intelligence, cybercrime investigations, and its ethical and legal boundaries

OSINT Investigation Methodologies

Apply structured methodologies used by law enforcement and threat analysts, including the intelligence cycle and investigative frameworks.

Search Engine Intelligence and Google Dorking

Leverage advanced search operators to uncover hidden or misconfigured content indexed by search engines.

Email, Username, and Phone Number Tracing

Track digital identities by linking email addresses, usernames, and phone numbers across platforms and data leaks.

Social Media Intelligence (SOCMINT)

Extract behavioral insights, relationship networks, and threat indicators from social media profiles and public interactions.

Domain, DNS, and WHOIS Investigations

Perform infrastructure reconnaissance to identify ownership, hosting providers, and DNS anomalies.

Metadata Analysis of Digital Files

Analyze images, documents, and media files to uncover embedded metadata such as geolocation, timestamps, and device information.

Real-World OSINT Case Studies

Review notable case studies showcasing how open-source data was used to uncover cyber threats, track malicious actors, and support law enforcement.

Types of OSINT: Technical, Human, Social, Geo, and Dark Web

Explore various OSINT domains—from infrastructure analysis to human behavior monitoring—and learn how to correlate them for comprehensive investigations.

Potential Job Role By Module:

- Threat Intelligence Analyst (Junior)
- OSINT Investigator
- Cybersecurity Research Assistant

Module 9

Capture the Flag

Master the art of gathering actionable intelligence from publicly accessible sources. This module prepares you to conduct structured cyber investigations, analyze digital footprints, and leverage open data for profiling, attribution, and threat validation.

Introduction to CTFs and Practice Platforms

Understand the structure and goals of various CTF formats—Jeopardy-style, Attack-Defense, and Hybrid—and get hands-on with platforms like TryHackMe, Hack The Box, and PicoCTF.

Cryptography Challenges

Decrypt classical and modern encryption schemes to uncover hidden data, enhancing your grasp of cryptographic principles.

Web Exploitation Labs

Engage in live exploitation of vulnerable web applications to simulate real-world attacks in isolated environments.

Team-Based CTF Competitions

Collaborate with peers in offensive (red team) and defensive (blue team) roles to solve timed challenges and simulate adversarial scenarios.

OSINT and Reconnaissance-Based CTFs

Utilize open-source intelligence techniques to investigate digital trails, perform reconnaissance, and uncover hidden assets.

Forensics and Steganography Challenges

Investigate digital evidence and extract concealed data from files, images, and metadata using forensic and steganographic analysis.

Core Platforms: TryHackMe, Hack The Box, PicoCTF

Master CTF skills using leading cybersecurity training platforms designed to build real-world technical expertise.

Potential Job Role By Module:

- ▶ CTF Competitor / Intern
- ▶ Cybersecurity Lab Assistant
- ▶ Red Team Trainee
- ▶ Security Testing Intern

Module 10

Capstone Projects & Career Preparation

Real Time Cybersecurity Projects

Web Application Security Assessment & Penetration Testing

This capstone project simulates a real-world web application penetration testing engagement. Students assess an intentionally vulnerable web application in a controlled lab environment, applying industry-standard tools, methodologies, and ethical testing practices.

Students perform testing from a virtualized attack environment (VM-based attack box) to ensure safe and isolated execution. Using tools such as Nmap, Burp Suite, Gobuster, and Nessus, learners conduct reconnaissance, vulnerability discovery, and controlled proof-of-concept exploitation.

The project concludes with a professional penetration testing report, documenting findings, risk severity, business impact, and remediation recommendations—suitable for inclusion in a resume or Cybersecurity portfolio.

Cybersecurity Resume Development

Learn to identify and exploit input validation weaknesses that allow attackers to extract, alter, or compromise sensitive data.

LinkedIn and GitHub Profile Enhancement and Personal Branding

Develop a professional online presence designed to attract recruiters and establish your credibility within the cybersecurity community.

Create and maintain a public portfolio featuring your code repositories, research, and project write-ups to validate your technical proficiency.

AI-Driven Security Tool or Automation Development

Conceptualize, build, and document an AI-integrated Cybersecurity tool or automation script, showcasing innovation and applied AI in security workflows.

Introduction to Cybersecurity Freelancing Platforms

Explore platforms such as Hackerone, Bugcrowd and Intigrity where you can monetize your cybersecurity skills through freelance and bug bounty opportunities.

Interview Preparation: Technical and Behavioral

Prepare for interviews with targeted practice on technical problem-solving questions and behavioral scenarios to excel in hiring processes.

Certification Pathways and Planning

Develop a strategic roadmap for pursuing advanced industry certifications like Sec+, CEH, OSCP, CISSP, and others that elevate your professional qualifications.

Potential Job Role By Module:

- Cybersecurity Generalist (Entry-Level)
- Freelance Cybersecurity Consultant
- Career-Ready Security Analyst
- Security Content Developer

For Contacts

Address; 4201 W 3rd St, Los Angeles, California, United States, 90020

Website : www.taasitacademy.com

Email : info@taasitacademy.com

☎ Phone : +1 818-514-3007

f facebook.com/taasitacademy