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** – Provides a ready-made environment with all essential pentesting and security tools in one OS. Saves setup time and ensures compatibility.

- **Nmap** – Used for network discovery and mapping. Helps identify live hosts, open ports, and services—a critical first step in assessing network security.

- **Metasploit** – Exploitation framework to safely simulate attacks on vulnerable systems. Helps testers understand vulnerabilities and their potential impact.

- **SQLMap** – Automates detection and exploitation of SQL injection flaws in web applications. Essential for securing databases against attackers.

- **Gobuster** – Finds hidden directories, files, and subdomains. Helps identify possible attack surfaces on web servers.

- **Nikto** – Scans web servers for misconfigurations, outdated software, and known vulnerabilities .Supports proactive server hardening.

- **Burp Suite** – Intercepts and analyzes web traffic to detect security flaws. Critical for testing authentication, sessions, and input validation in web apps.(Add this info before the module start)

Abstract

Course Insights

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

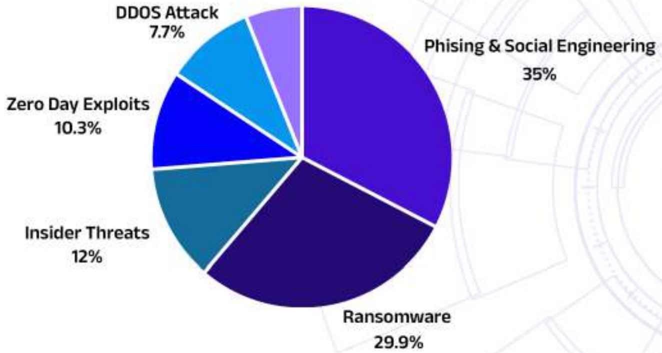
The Fullstack Cybersecurity Engineering curriculum offers a complete, hands-on learning journey through core cybersecurity concepts, operating system fundamentals, network defense, and offensive security. Students gain practical experience with tools like Kali Linux, Wireshark, Metasploit, and Burp Suite 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.

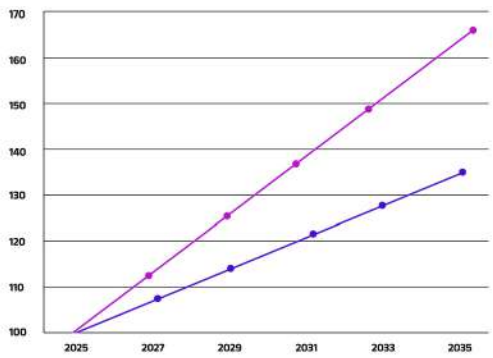
The Era of Cyber Security with Gen AI

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-versus-defender paradigm and cultivate a proactive, risk-aware approach to cybersecurity, an essential mindset for addressing evolving digital threats.

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.

Threats, Vulnerabilities, and Risk Assessment

Differentiate between threat actors, vulnerabilities, and exploits. Learn to apply structured risk assessment frameworks to evaluate and prioritize cybersecurity defenses.

Common Cybersecurity Attack Types

Gain insights into prevalent and emerging attack vectors, including phishing, malware, denial-of-service (DoS), and zero-day exploits, along with their techniques and prevention strategies.

Security Policies and Governance

Understand the critical role of governance through well-defined security policies, standards, and procedures. Learn how these align cybersecurity initiatives with broader business goals.

Introduction to Virtualization and Cloud Security

Explore the fundamentals of securing virtualized and cloud-based environments. Learn about shared responsibility models, hypervisor-level risks, and cloud-native security considerations.

Introduction to Virtualization and Cloud Security

Understand the critical role of governance through well-defined security policies, standards, and procedures. Learn how these align cybersecurity initiatives with broader business goals.

Cybersecurity Terminologies & Acronyms

Familiarize yourself with the key terminology and acronyms used in the cybersecurity field to ensure clear communication within technical teams and organizations.

Introduction to Compliance Frameworks (GDPR, HIPAA, ISO 27001)

Gain foundational knowledge of major global compliance standards and their implications for data protection, security policy enforcement, and organizational accountability.

Cybersecurity Career Pathways

Discover the diverse career opportunities within cybersecurity, including roles in Red Teaming, Blue Teaming, Governance, Risk and Compliance (GRC), and emerging fields like AI-driven security.

Potential Job Role By Module:

- ▶ Cybersecurity Intern
- ▶ IT Security Assistant
- ▶ Compliance Assistant (GRC)
- ▶ Compliance Assistant (GRC)

Module 2

Operating Systems & System Security

Effective cybersecurity begins with a deep understanding of the underlying operating systems and the assets they support. This module equips learners with hands-on skills in both Linux and Windows environments, while introducing foundational practices in system auditing, automation, and asset management.

Linux Operating System Fundamentals (Kali Linux)

Gain practical experience with industry-relevant Linux distributions. Learn to navigate, configure, and secure systems using Kali—cornerstones of cybersecurity labs and real-world environments.

Command Line Interface (CLI) Proficiency

Develop fluency in the Linux and Windows CLI to efficiently manage files, directories, permissions, and system processes—critical for any cybersecurity professional.

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.

Bash Scripting for Security Automation

Write and deploy Bash scripts to automate routine security tasks such as log analysis, system updates, and configuration audits.

Introduction to Windows System Security

Explore the security mechanisms within Windows environments, including User Account Control (UAC), Group Policy Objects (GPOs), and the Windows Event Log system.

System Logs and Monitoring Essentials

Familiarize yourself with the key terminology and acronyms used in the cybersecurity field to ensure clear communication within technical teams and organizations.

Asset Discovery and Inventory Management

Leverage both open-source and commercial tools to identify and manage IT assets. Learn to detect unauthorized devices and maintain a complete inventory for audit and compliance.

Potential Job Role By Module:

- System Administrator (Junior)
- IT Support Analyst
- Security Operations Assistant

Module 3

Networking Fundamentals & Network Security

Secure networks are essential for a cybersecurity strategy. This module provides foundational networking concepts and critical tools and techniques for defending enterprise environments against various threats.

Introduction to Networking Concepts

Explore key networking components—topologies, protocols, and the client-server model—from a cybersecurity perspective.

Understanding the OSI and TCP/IP Models

Learn how data traverses the network through layered models, and identify where and how to implement effective security controls.

IP Addressing, Subnetting, and Routing

Master IP addressing and subnetting to segment networks effectively, and grasp routing fundamentals for managing data flow and ensuring security boundaries.

Network Scanning with Nmap & Zenmap

Use industry-standard reconnaissance tools to map network assets, discover open ports and services, and identify potential vulnerabilities.

Traffic Analysis with Wireshark

Capture and dissect network packets to uncover anomalies, detect signs of compromise, and track attacker movement across the network.

Firewall Concepts and Implementation

Understand the principles of stateful inspection, access control rules, and next-generation firewall features for robust perimeter defense.

VPNs and Secure Communication Protocols

Study virtual private networks (VPNs), tunneling protocols, and encryption standards that protect sensitive data during transmission.

Encryption and Encoding Fundamentals

Gain insight into symmetric and asymmetric encryption, hashing algorithms, and encoding techniques critical for securing data in motion and at rest.

Network Access Control (NAC)

Implement 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)

Learn how to deploy and configure IDS/IPS tools to detect threats in real-time, issue alerts, and prevent potential attacks through signature and behavior-based analysis.

Potential Job Role By Module:

▶ Network Security Analyst (Entry-Level)

▶ Junior SOC Analyst

▶ Network Support Technician

Module 4

Red Team Operations

This module encourages students to adopt an adversary's mindset to learn about real-world attacks. It emphasizes offensive security techniques, allowing students to ethically identify and exploit vulnerabilities through simulated scenarios.

Developing the Cybersecurity Mindset

Explore the attacker-versus-defender paradigm and cultivate a proactive, risk-aware approach to cybersecurity, an essential mindset for addressing evolving digital threats.

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.

Threats, Vulnerabilities, and Risk Assessment

Differentiate between threat actors, vulnerabilities, and exploits. Learn to apply structured risk assessment frameworks to evaluate and prioritize cybersecurity defenses.

Common Cybersecurity Attack Types

Gain insights into prevalent and emerging attack vectors, including phishing, malware, denial-of-service (DoS), and zero-day exploits, along with their techniques and prevention strategies.

Security Policies and Governance

Understand the critical role of governance through well-defined security policies, standards, and procedures. Learn how these align cybersecurity initiatives with broader business goals.

Introduction to Virtualization and Cloud Security

Explore the fundamentals of securing virtualized and cloud-based environments. Learn about shared responsibility models, hypervisor-level risks, and cloud-native security considerations.

Introduction to Virtualization and Cloud Security

Understand the critical role of governance through well-defined security policies, standards, and procedures. Learn how these align cybersecurity initiatives with broader business goals.

Cybersecurity Terminologies & Acronyms

Familiarize yourself with the key terminology and acronyms used in the cybersecurity field to ensure clear communication within technical teams and organizations.

Introduction to Compliance Frameworks (GDPR, HIPAA, ISO 27001)

Gain foundational knowledge of major global compliance standards and their implications for data protection, security policy enforcement, and organizational accountability.

Cybersecurity Career Pathways

Discover the diverse career opportunities within cybersecurity, including roles in Red Teaming, Blue Teaming, Governance, Risk and Compliance (GRC), and emerging fields like AI-driven security.

Potential Job Role By Module:

- ▶ Cybersecurity Intern
- ▶ IT Security Assistant
- ▶ Compliance Assistant (GRC)
- ▶ Compliance Assistant (GRC)

Module 5

Blue Team Operations

Master cyber defense by enhancing monitoring, detection, and response capabilities. This module emphasizes building a resilient security infrastructure and improving incident response readiness in enterprise environments.

Log Management and Analysis

Design and implement effective logging pipelines. Develop search queries and correlation logic to identify suspicious activities, policy violations, and indicators of compromise.

Security Information and Event Management (SIEM)

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

Threat Detection with Splunk

Work hands-on with Splunk to build dashboards, query security data, and visualize trends. Detect, investigate, and respond to threats using structured analysis.

Foundations of Digital Forensics

Learn essential forensic procedures including evidence acquisition, timeline reconstruction, data integrity verification, and preservation for legal compliance.

Security Monitoring Solutions

Deploy and configure endpoint detection and response (EDR), network monitoring, and cloud-based security tools to achieve comprehensive visibility across systems and environments.

Malware Detection and Analysis

Explore static and dynamic malware analysis techniques to dissect suspicious files, identify malware families, and extract actionable indicators of compromise (IOCs).

Incident Response Planning and Execution

Design and implement incident response playbooks aligned with the NIST Incident Response Lifecycle. Practice handling breaches from identification to containment and recovery.

Threat Hunting Methodologies

Adopt a proactive defense posture through behavior-based threat hunting. Use hypothesis-driven techniques to detect stealthy adversaries and persistent threats.

Applying the NIST Cybersecurity Framework

Operationalize the NIST Cybersecurity Framework by integrating the five core functions—Identify, Protect, Detect, Respond, and Recover—into your security operations model.

Automation and AI in Defensive Security

Leverage automation, machine learning, and AI-enhanced tools to reduce detection times, eliminate noise, and accelerate incident triage and response.

Potential Job Role By Module:

- SOC Analyst (Tier 1)
- Incident Response Analyst (Junior)
- Digital Forensics Assistant
- SIEM Analyst

Module 6

Generative AI for Cybersecurity

Leverage the transformative power of generative AI to enhance cybersecurity efficiency, precision, and adaptability. This module explores how AI—particularly large language models (LLMs)—can be responsibly integrated into defensive and offensive security workflows.

Introduction to Generative AI and Security Applications

Understand the fundamentals of generative AI, including LLMs and transformer models, and examine their emerging roles in cybersecurity use cases such as automation, analysis, and simulation.

Prompt Engineering for Security Outcomes

Master prompt engineering techniques to effectively guide AI tools toward generating accurate, secure, and actionable outputs tailored to cybersecurity tasks.

Utilizing ChatGPT for Security Automation

Deploy ChatGPT to streamline repetitive tasks such as report writing, code review, documentation, and alert triage, boosting productivity in SOC and DevSecops environments.

Hands-On with OpenAI Playground

Experiment with OpenAI's playground and APIs to build practical integrations for automated workflows, threat detection, and vulnerability analysis.

Integrating AI Into Cybersecurity Workflows

Incorporate AI into existing workflows to support real-time log analysis, threat classification, incident enrichment, and automated response through intelligent pipelines.

AI-Powered Reporting and Threat Intelligence

Generate high-quality, compliance-ready reports, executive summaries, and threat intelligence documents with speed and clarity using AI-driven content generation.

Phishing Detection and Simulation with AI

Use AI to identify indicators of phishing in emails and messages, and create realistic simulation scenarios for employee security awareness training.

Ethical Considerations and Responsible AI Use

Examine the implications of AI in cybersecurity, including bias, misinformation (hallucinations), prompt injection attacks, and ethical safeguards for responsible deployment.

Key Tools: Chatgpt, Pentesrergpt, Hackergpt, Deepseek

Potential Job Role By Module:

- ▶ AI Security Analyst
- ▶ Cybersecurity Automation Engineer
- ▶ Security Analyst with GenAI Specialization
- ▶ Prompt Engineer (Cybersecurity Focus)

Module 7

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 exploitation.

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 Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), and Server-Side Request Forgery (SSRF) with proof-of-concept demonstrations.

Common Cybersecurity Attack Types

Gain insights into prevalent and emerging attack vectors, including phishing, malware, denial-of-service (DoS), and zero-day exploits, along with their techniques and prevention strategies.

Building a Professional Bug Bounty Portfolio

Document responsibly disclosed vulnerabilities to showcase your skills, build industry credibility, and create a pathway into security careers.

Authentication & Authorization Bypass

Investigate weaknesses in session management, broken access controls, and logic flaws that allow unauthorized access and privilege escalation.

Business Logic Vulnerabilities

Identify non-technical flaws in application workflows that can lead to financial abuse, information leakage, or broken functionality.

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 impact, reproduction steps, and mitigation guidance.

Key Tools: Burp Suite, OWASP ZAP, NUCLEI

Potential Job Role By Module:

- ▶ Bug Bounty Hunter
- ▶ Web Application Penetration Tester
- ▶ Application Security Researcher
- ▶ Freelance Security Tester

Module 8

Capture the Flag (CTF)

Apply your cybersecurity knowledge in dynamic, hands-on scenarios that replicate real-world environments. This module emphasizes experiential learning through gamified CTF challenges, lab-based exercises, and collaborative team competitions.

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 (Caesar,XOR, AES)

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

Building Your CTF Portfolio

Document your participation, techniques, and solved challenges to create a professional portfolio that showcases your practical skills to recruiters and employers.

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.

Building a Professional Bug Bounty Portfolio

Document responsibly disclosed vulnerabilities to showcase your skills, build industry credibility, and create a pathway into security careers.

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 9

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 10

Capstone Projects & Career Preparation

Real Time Cybersecurity Projects

Mail Server Security Challenge

Mission: Break into your mind, not the system! Analyze and secure a mail server like a pro.

What You'll Do: Hunt for vulnerabilities, lock down access, and implement best practices for email security.

Tools In Action:

Kali Linux, Nmap, Metasploit, Nikto, Burp Suite.

File Server Defense Project

Mission: Become the guardian of files! Assess and harden a file server.

What You'll Do: Test access controls, fix misconfigurations, and protect sensitive data from intruders.

Tools in Action: Kali Linux, Nmap, Metasploit, Gobuster, SQLMap.

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 Bugcrowd, Synack, and Upwork 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 OSCP, CISSP, and others that elevate your professional qualifications.

Cybersecurity Career Pathways

Develop a strategic roadmap for pursuing advanced industry certifications like 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

Our Instructor

MD. ANISUR RAHMAN
Faculty, Cybersecurity, TAAS IT
MSC IN INFORMATION TECHNOLOGY

For Contacts

Address; 141 South Berendo Street , 308, Los Angeles, CA, United States, California

Website : www.taasitacademy.com

Email : info@taasitacademy.com

☎ Phone : +1 (213) 619-7232

facebook.com/taasitacademy