About A&T Edutech (Panvel)

‘Your go-to partner for education upgrading and upskilling with current, industry-relevant courses that unleash your employment potential and make you production-ready to fit the tech market demand!’

A&T Edutech is democratizing access to high-quality education at an affordable price. We are playing our part in helping the country meet the growing demand for talent across segments. We follow an outcome-oriented approach while not compromising on either quality or affordability. Our emphasis is to become a bridge and fill the employment gap in our country by increasing the employment quotient of students and enabling them to access premium jobs.

About the program

A cybersecurity course is an educational program designed to provide individuals with the knowledge, skills, and expertise necessary to understand and address issues related to cybersecurity. Cybersecurity courses cover a broad range of topics aimed at protecting computer systems, networks, and data from unauthorized access, attacks, and damage.

A&T
Edu Tech
SINCE 1998

Operating Systems and Networking Fundamentals

Day 1: Basics of Linux

Topics

- What is an Operating System?
- Linux Operating System
- Linux Distributions
- Linux Architecture

Day 2: Linux Essentials

Topics

- Linux Commands
- Linux File System
- Linux Regular Expressions

Day 3: User Administration

Topics

- Users And Group Management
- Process Management
- Domain Name System

Day 4: Cybersecurity Tools in Kali Linux – I

Day 5: Cybersecurity Tools in Kali Linux – II

Topics

- Reverse Engineering
- Exploitation Tools
- Sniffing and Spoofing
- Forensic Tools
- Maintaining Access
- Hardware Hacking
- Stress Testing
- Reporting Tools

Day 6: System Management and Security - I

Topics

- Advanced Packet Tool
- APT Key Management Utility
- dpkg
- System Security and Protection
- Multics

Day 7: System Management and Security - II

Topics

- Access Matrix
- Access Control

Day 8: Operating System Security - I

Topics

- Security in Systems
- Security Problems
- Levels of Security Measures
- User Authentication

Day 9: Operating System Security - II

Topics

- Firewall System Protection
- Protection and Security in Operating System
- What is a Computer Network?

Day 10: Computer Network Fundamentals - I

Topics

- Network Topologies
- Network Structures
- IP and MAC Address

Day 11: Computer Network Fundamentals - II

Topics

- OSI Model
- TCP/IP Model

Day 12: Computer Network Fundamentals – III

Topics

- Addressing
- Subnetting
- IPv4 Packet Structure

Day 13: Network Protocols

Topics

- Network Protocols
- ARP
- RARP
- GARP
- HTTP
- HTTPS
- SSL
- ICMP
- DHCP

14: IPv6 & Network Security Basics Day

Topics

- IPv6 Packet Structure
- IPv4 vs. IPv6
- Introduction to Network Security
- Need for Network Security

Day 15: Network Security Attacks

Topics

- Network Security Attacks
- Code Execution Intrusion
- Stack Buffer Overflow
- Heap Buffer Overflow

Day 16: Network Security

Topics

- Network Security
- Intrusion Detection Systems
- Intrusion Prevention Systems

Day 17: Interview Preparation and Assessment – Operating Systems and Networking Fundamentals

Topics

- Interview Preparation on Operating Systems and Networking Fundamentals
- Assessment on Operating Systems and Networking Fundamentals

Day 18: Project – Secure User Access Management in Linux

The Secure User Access Management project in Linux enhances system security by implementing robust authentication mechanisms and offering fine-grained control over user permissions, thereby safeguarding against unauthorized access.

Cryptography and Application Security

Day 19: Cryptography – I

Topics

- Types of cryptography
- Symmetric cryptography
- Asymmetric cryptography

Day 20: Cryptography – II

Topics

- Hash functions
- Digital signatures
- Public Key Infrastructure (PKI)
- Attacks on cryptosystems

Day 21: Authentication

Topics

- Input Validation
- What is Authentication?
- Two Factor and Three Factor Authentication
- Web Application Authentication
- Securing Password Based Authentication
- Secure Authentication Best Practices

A&T
Edu Tech
SINCE 1998

Day 22: Secure Web Authentication Practices and Authorization

Topics

- Identity Access Management
- Privilege Access and Identity Management
- Customer Identity Access Management
- Social Login
- Fundamentals of Authorization
- Authorization Layers
- Securing Web application Authorization
- Custom Authorization Mechanism
- Client-Side Attacks
- TOCTTOU Exploits
- Attacks Against Authorization
- Introduction to Access Control

Day 23: Session Management

Topics

- Session management
- Session tracking methods
- Session functionalities
-

Day 24: Session Data and Security

Topics

- Handling session data
- Session security
- Session management flows
- Session vulnerabilities

Day 25: Web Security

Topics

- Session attacks and their mitigation
- Best practices for secure session management
- Web Application and its Components
- Structure of Web Application
- Document Object Model (DOM)
- HTTPS, SSL/TLS, and WAF

Day 26: Miscellaneous Web Technology Security - I

Topics

- Same Origin Policy (SOP)
- Cross-origin Resource Sharing (CORS)

Day 27: Miscellaneous Web Technology Security - II

Topics

- Web Browser Security
- Web Server Hardening
- Securing Web Services
- Some Common Web Security Methods

Day 28: Database Security - I

Topics

- Database Security
- Database Threats
- Security Risks Specific to NoSQL Databases
- Deploying Database Security

Day 29: Database Security - II

Topics

- Data Validation and Sanitization
- Data Perturbation, Data Masking, and Tokenization
- Protecting Data with Tokenization
- Database Auditing and Monitoring
- Database Encryption
- Setting Database Privileges

Day 30: File Security

Topics

- Different Types of Files
- Accessing Files
- Inserting Malicious Files

Day 31: File Security and Best Practices

Topics

- File Tampering
- File Security Best Practices
- Code Obfuscation
- Antivirus Protection: Types of Scans

Day 32: Mobile Security - Android

Topics

- Mobile operating system
- Android
- Android Security Features

Day 33: Mobile Security - IOS

Topics

- IOS
- IOS Security features
- Enterprise Mobile Security Methods
- Mobile Threats and Mitigation

Day 34: Interview Preparation and Assessment – Cryptography and Application Security

Topics

- Interview Preparation on Cryptography and Application Security
- Assessment on Cryptography and Application Security

Day 35: Project - Web Application Source Code Vulnerability Analysis

The Web Application Source Code, Vulnerability Analysis project, focuses on identifying and mitigating security weaknesses in web application code. It employs advanced scanning tools to detect potential vulnerabilities like SQL injection or cross-site scripting. This proactive approach ensures the security and integrity of web applications by addressing issues before they can be exploited.

Cyber Security Tools

Day 36: Secure Development Methodologies – I

Topics

- What is a Secure Software?
- Factors that Influence Secure Software Properties
- Common Security Flaws in a Software
- Security Principles
- Software Development Models

Day 37: Secure Development Methodologies – II

Topics

- Common Threat Modelling Methodologies
- Secure Development Lifecycle Phases
- Secure Coding Best Practices
- Security Testing
- The Penetrate-and-Patch Approach

Day 38: Introduction to Cyber Security

Topics

- Secure development methodologies and maturity models
- Cybersecurity
- CIA Triad

Day 39: Security Architecture & Policies

Topics

- Security Architecture & Policies
- Ethical Hacking
- Phases of Ethical Hacking

Day 40: Introduction to Ethical Hacking

Topics

- Scenario: Avco’s Tale
- Scenario: Zomato Hacked
- Phases of Ethical Hacking
- Findings in Each Phase
-

Day 41: Penetration Testing

Topics

- Penetration Testing
- Phases of Penetration Testing
- Types of Penetration Testing
- What Makes a Good Penetration Test?
- Essential Skills for Ethical Hacking
- Information Security

Day 42: Advanced Ethical Hacking

Topics

- Information security policies
- Laws
- Standards

Day 43: Incident Management

Topics

- Incident management
- What is anonymity
- Need for anonymity

Day 44: Anonymity and Tools - I

Topics

- Anonymity online using Tor browser
- Onion Routing
- Comodo Dragon Browser
- Browser Extensions

Day 45: Anonymity and Tools – II

Topics

- Spoofing MAC Address: TMac
- Anonymity using VPN
- Anonymity in DNS
- Proxy

Day 46: Anonymity and Tools – III

Topics

- Anonymity using OS
- Anonymity in Search Engine
- Anonymous Email and Communication
- Anonymous File Sharing and Backup

Day 47: Information Gathering – I

Topics

- What is Information Gathering
- Footprinting through search engines

Day 48: Information Gathering – II

Topics

- Footprinting using Advanced Google hacking techniques
- Footprinting through Social Networking Sites

Day 49: Reconnaissance and Tools – I

Topics

- Website Footprinting
- Email Footprinting
- Competitive Intelligence
- Whois Footprinting

Day 50: Reconnaissance and Tools - II

Topics

- DNS Footprinting
- Network Footprinting
- Footprinting Countermeasures
- Footprinting Pen Testing

Day 51: Network Scanning Tools - I

Topics

- TCP flags
- Packet crafting

Day 52: Network Scanning Tools - II

Topics

- Scanning ICMP services
- Scanning TCP services
- Scanning UDP services

Day 53: Network Scanning Tools – III

Topics

- Banner grabbing
- Network diagram
- IDS/Firewall evasion techniques

Day 54: Enumeration – I

Topics

- Introduction to enumeration
- Techniques of enumeration

Day 55: Enumeration - II

Topics

- NetBIOS enumeration
- SNMP enumeration

Day 56: Enumeration on Different technologies - I

Topics

- LDAP enumeration
- NTP enumeration
- SMTP enumeration

Day 57: Enumeration on Different technologies - II

Topics

- DNS enumeration
- VoIP, IPSec, RPC enumeration
- Various enumeration countermeasures
- Enumeration in Pen Testing

Day 58: Interview Preparation and Assessment – Cyber Security Tools

Topics

- Interview Preparation on Cyber Security Tools
- Assessment on Cyber Security Tools

Day 59: Project – Information Gathering on Websites Using Linux

The Information Gathering on Websites Using Linux project utilizes Linux tools for web data extraction and analysis, aiding in cybersecurity and market research by providing insights into website structures and security.

Web Application Hacking

Day 60: Vulnerability Analysis - I

Topics

- Vulnerability Assessment Concepts
- Vulnerability Management Life-Cycle
- Vulnerability Assessment Solutions

Day 61: Vulnerability Analysis - II

Topics

- Vulnerability Assessment Tools
- Vulnerability Scoring System
- Vulnerability Assessment Report
- Vulnerability Scanning Tools

Day 62: Introduction to Web Application Hacking - I

Topics

- How Web Applications Work?
- Web Applications Architecture
- Attack Surfaces
- Types of attack surfaces

Day 63: Introduction to Web Application Hacking – II

Topics

- Vulnerabilities of Digital Surfaces
- Web Server Vulnerabilities
- Backend Induced Vulnerabilities
- Web Cache Poisoning
- Core Defense Mechanisms of Web Application
- Web Application Hacking Methodology
- Footprinting

Day 64: Advanced Web Application Hacking - I

Topics

- Web Application Hacking: Application Logic
- Bypass Client-Side Control
- Attack Hidden HTML Form Fields
- Web Application Hacking: Access Handling
- Attack Authentication Mechanism
- Attack Session Management
- Web Application Hacking: Input Handling
- Attack Data Connectivity

Day 65: Advanced Web Application Hacking – II

Topics

- Attack Back-End Components
- Web Server Attacks
- Web Application Hacker’s Toolkit
- Integrated Testing Suites
- Components of Testing Suites
- Vulnerability Scanners
- Countermeasures to Web Application Hacking

Day 66: Overview of OWASP

Topics

- What is OWASP?
- Top 10 OWASP Vulnerabilities
- Application Security Risks
- OWASP Risk Rating
- Injection Attacks
- Code Injection
- OS Command Injection
- Command Injection Attacks

Day 67: OWASP Terminologies

Topics

- SQL Injection (SQLi)
- Host Header Injection
- CRLF (Carriage Return and Line Feed) Injection
- Cross-site Scripting (XSS)
- XPath Injection
- Email Header Injection
- Prevent Injection Attacks
- Broken Authentication
- Session Hijacking
- Types of Broken Authentication Vulnerabilities
- How to Prevent Broken Authentication?

Day 68: SQL Injection - I

Topics

- Sensitive Data Exposure
- What is vulnerable?
- How to Prevent Sensitive Data Exposure
- SQL Injection
- Working of SQL Query
- Working of a Malicious SQL Query

Day 69: SQL Injection - II

Topics

- SQL Injection Methodology
- Launch SQL Injection Attacks
- Advanced SQL Injection Attacks
- Types of SQL Injection

Day 70: Tools and Advanced SQL Injection

Topics

- SQL injection tools
- Testing of SQL injection
- SQL injection countermeasures

Day 71: Session Hijacking - I

Topics

- Session Hijacking
- Active Attack
- Passive Attack
- Application-Level Session Hijacking
- Session Fixation Attack

Day 72: Session Hijacking – II

Topics

- Network-level session hijacking
- Single sign-on
- JWT tokens

Day 73: OWASP – I

Topics

- XML External Entities
- What is Extensible Markup Language (XML)?
- Types of XML Entities
- XML External Entities (XXE)
- Types of XXE Attacks
- Broken Access Control
- Privilege Escalation
- Directory Traversal
- How to Detect Broken Access Control?

Day 74: OWASP – II

Topics

- Security Misconfigurations
- Types of Security Misconfiguration
- Web Server Misconfiguration
- Parameter/Form Tampering
- Detecting Security Misconfigurations
- File Upload Vulnerabilities
- Insecure Storage
- Types of File Upload Attacks

Day 75: OWASP - III

Topics

- Cross-Site Scripting (XSS) Attack
- Impact of XSS
- How XSS Works?
- Types of XSS
- XSS Mitigation Techniques

Day 76: OWASP – IV

Topics

- Insecure Deserialization
- Serialization
- Deserialization
- Insecure Deserialization
- Oracle, Kentico Vulnerable to Insecure Deserialization
- Impact of Insecure Deserialization
- Application Vulnerable
- Insufficient Logging and Monitoring
- Mitigation Techniques

Day 77: Social Engineering – I

Topics

- Social Engineering
- Introduction to Phishing
- Differentiating Phishing and Original Webpages

Day 78: Social Engineering - II

Topics

- Tools to Detect Phishing Websites: Netcraft
- Tools to Detect Phishing websites: PhishTank
- Insider Threats
- Social Networking Threats
- Risks of Social Networking to Corporate Networks
- Identity Theft
- Identity Theft Countermeasures

Day 79: Interview Preparation and Assessment – Web Application Hacking

Topics

- Interview Preparation on Web Application Hacking
- Assessment on Web Application Hacking

Day 80: Project – CTF Challenge

The CTF (Capture the Flag) Challenge project is centered around hosting cybersecurity competitions, where participants solve security-related puzzles and tasks. These challenges range from cryptography and reverse engineering to network security and ethical hacking. The project aims to enhance cybersecurity skills and knowledge through practical, hands-on experience in a controlled environment.

Professional Development

- Day 81 and 82: Capstone Project – Ethically Hacking an E-Commerce Website
- Day 83: Mock Exam and Real-world Use Cases
- Day 84: Final Assessment
- Day 85 and 86: Profile Building
- Day 87 and 88: Logical Reasoning
- Day 89 and 90: Aptitude
- Day 91 and 92: Communication Skills
- Day 93 to 96: Mock Interviews

A&T
Edu Tech
SINCE 1998

For further assistance contact

Call: 89766 95898 / 99606 71421

Visit: JK Plaza, Shop no.24, 2nd Floor,
Opp. Tanishq Jewellers, Above Unnati Hospital,
Shivaji Chowk, Old Panvel

Our website www.aandtedutech.com