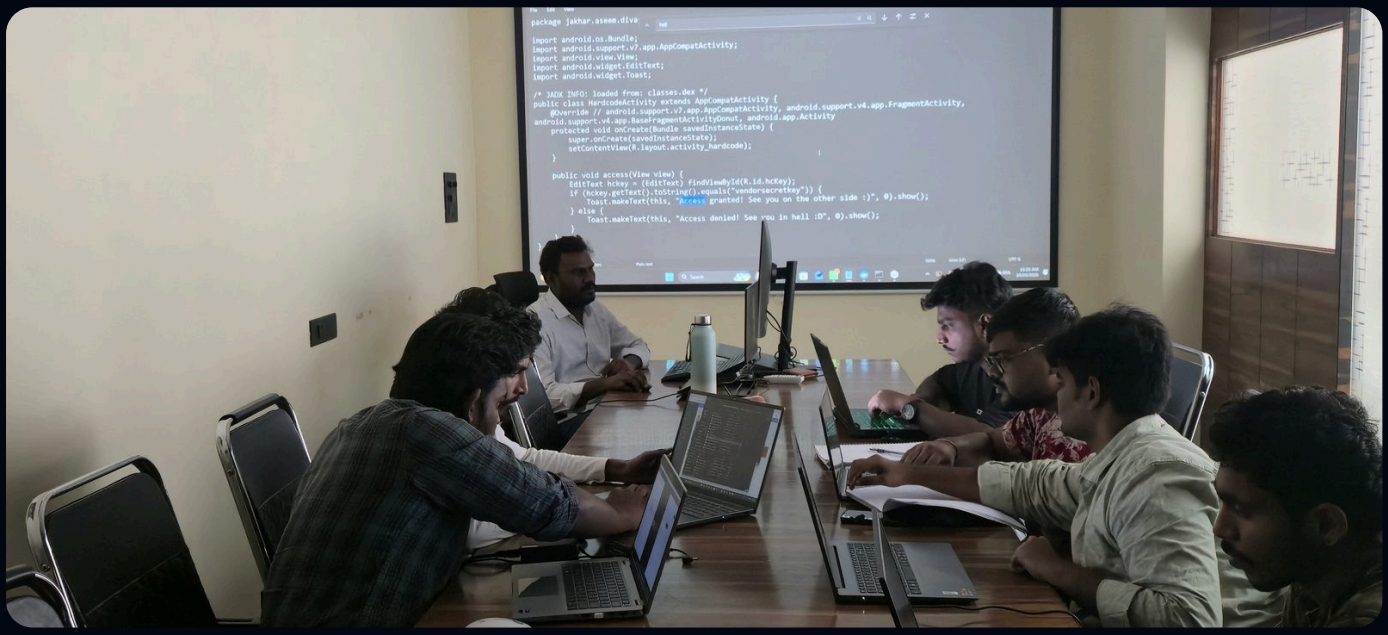
HACKING TRAINER ACADEMY
AMEERPET · HYDERABAD

Classroom in Ameerpet and live online

Course syllabus: every module, hour by hour

Three 6-week cyber security courses, each from beginner to advanced. For each module: what you learn, what you do in the lab, what you hand in, and about which week it falls in.



3
courses, each beginner to advanced

90 h
guided hours in each course

35
modules, each with a lab and a deliverable

3 h
a day, Monday to Friday, or weekends

+91 86868 92922
hackingtrainer.com · info@hackingtrainer.com

Syllabus as of 13 November 2026. Start dates and fees are always on the website.

WHICH COURSE FIRST

Pick the course that fits your goal

Every course runs from beginner to advanced level, so choose by what you want to do. Each card shows where it starts, what it assumes and where it ends. Taken in order, the three courses are 18 weeks and 270 guided hours.

SEPARATE COURSE

Beginner to advanced

HTA-103 · SOC Analyst and DFIR

STARTS WITH

Cybersecurity and network defense fundamentals (10 hours)

BEFORE YOU START

Basic computer skills. The first module covers networking, Linux and Windows fundamentals. Freshers are welcome.

ENDS WITH

Capstone: incident simulation (10 hours)

ROLES IT PREPARES YOU FOR

SOC analyst (L1), Security analyst, Incident response associate

TRACK, WEEKS 1 TO 6

Beginner to advanced

HTA-101 · Application Security

STARTS WITH

Linux fundamentals for security testing (5 hours)

BEFORE YOU START

Basic computer skills. The course starts with Linux, Windows and networking fundamentals, then web and API fundamentals. A short admissions check confirms your starting point.

ENDS WITH

Capstone assessment (10 hours)

ROLES IT PREPARES YOU FOR

Application security tester, Web and API penetration tester, Mobile application security tester

TRACK, WEEKS 7 TO 12

Beginner to advanced

HTA-102 · Network and Active Directory

STARTS WITH

Virtualization fundamentals (3 hours)

BEFORE YOU START

Basic computer skills. The course starts with virtualization, lab setup and Linux, networking and Windows fundamentals before any attacks. A short admissions check confirms your starting point.

ENDS WITH

Capstone assessment (9 hours)

ROLES IT PREPARES YOU FOR

Network penetration tester, VAPT analyst, Junior red team operator

Where should I start?

Fresher, graduate or non-IT background	**HTA-103**
Developer or software tester	**HTA-101**
Network, system or IT support engineer	**VAPT Track**

Admissions runs a short check on your starting point.

Fees for the path

HTA-103 on its own	₹20,000 + GST
VAPT Track (HTA-101 then HTA-102)	₹30,000 + GST
All three, in order	**₹50,000 + GST**

The last line is the two published prices added together; there is no separate fee for all three.

How every class runs, and how you are assessed

Instructor-led live classes, with practice support and guidance after class. Every class is recorded, with one year of replay from your admission date. Each course ends with a graded report and a technical oral exam. Missed a class? Free backup classes.

The certificate is a Hacking Trainer course certificate, not an EC-Council or other vendor certification. We do not provide job placement or placement assistance. We give you the skill, graded reports to show employers, and interview preparation. The employer decides who to hire.

HTA-103 · Beginner to advanced

SOC Analyst and DFIR

The core concepts of EC-Council's CCT, CSA, ECIH and CHFI, taught hands-on with Splunk, Wazuh and forensics tools.

6 weeks
90 guided hours

9 modules
each with a lab

Beginner to advanced
Level

₹20,000 + GST
₹23,600 with GST

THE 6 WEEKS AT A GLANCE



Bar widths are the module hours. On a weekday batch (15 hours a week) the weeks are approximate; the trainer confirms the pace for your batch.

Before you start

Basic computer skills. The first module covers networking, Linux and Windows fundamentals. Freshers are welcome.

Prepares you for

SOC analyst (L1), Security analyst, Incident response associate, Junior forensic analyst

Lab tools: Splunk, Microsoft Sentinel (orientation), Wazuh, Sysmon, Wireshark, Autopsy, Volatility, MISP (concepts)

Note: The core concepts of EC-Council's CCT, CSA, ECIH and CHFI, taught hands-on. It is not EC-Council courseware and does not include exam vouchers.

MODULE BY MODULE

M1

10 hours
About week 1

Cybersecurity and network defense fundamentals

Explain how attacks work and how networks and systems are defended, in the terms every security team uses.

- Threats, vulnerabilities, attacks and controls; confidentiality, integrity and availability
- Networking for analysts: TCP/IP, DNS, DHCP, HTTP, SMTP and VPN
- Network defense: firewalls, IDS/IPS, proxies, segmentation and what each one logs
- Windows and Linux essentials and hardening
- Identity and access management, cryptography and PKI basics
- Wireless, cloud and IoT security basics

IN THE LAB
Capture and read traffic in Wireshark; Harden a Windows and a Linux machine against a checklist

YOU HAND IN
Network defense notes and a hardening checklist

M2

10 hours

About weeks 1 to 2

SOC operations and log sources

Work inside a SOC and read the logs it depends on: know which source answers which question.

- L1, L2 and L3 roles, shifts, ticketing, SLAs, escalation and shift handover
- Frameworks: Cyber Kill Chain, MITRE ATT&CK, IOCs vs IOAs and the Pyramid of Pain
- Windows Security events, PowerShell logging and Sysmon
- Active Directory and Kerberos events; Linux authentication, syslog and auditd
- Firewall, proxy, DNS and web server logs; Entra ID sign-in and AWS CloudTrail logs (introduction)
- Parsing, normalization, time zones and ingestion health

IN THE LAB

Triage a queue of sample alerts and write ticket notes; Trace one attack across Windows, Sysmon, firewall and DNS logs

YOU HAND IN

Ticket notes, a shift handover and a log-source reference sheet

M3

12 hours

About weeks 2 to 3

SIEM investigation: Splunk and Microsoft Sentinel

Investigate alerts in Splunk, build searches, dashboards and alerts, and read the same investigation in Sentinel's KQL.

- Splunk search language (SPL): searching, fields, stats, lookups and knowledge objects
- Dashboards, reports and scheduled alerts
- Investigating authentication, endpoint and network events
- Correlation searches and use cases
- Microsoft Sentinel and KQL: the same investigation in Microsoft's SIEM (orientation and trainer demonstration)

IN THE LAB

Investigate a brute-force-to-compromise case in Splunk; Build a dashboard and a scheduled alert

YOU HAND IN

Splunk investigation notes

M4

8 hours

About week 3

Endpoint monitoring, EDR and threat intelligence

Monitor endpoints with Wazuh and Sysmon, investigate an endpoint alert the way EDR analysts do, and enrich it with threat intelligence.

- Wazuh manager, agents, decoders and rules; file integrity monitoring and vulnerability detection
- EDR concepts: process trees, isolation and response, as in tools such as Microsoft Defender and CrowdStrike
- Active response and alert tuning
- Threat intelligence: feeds, reputation services, MISP concepts and enrichment

IN THE LAB

Deploy agents, generate activity, investigate the alerts and tune a noisy rule; Enrich indicators from an alert

YOU HAND IN

Endpoint investigation and tuning notes

M5

12 hours

About weeks 3 to 4

Alert triage, detection engineering and threat hunting

Work the common L1 alert types with playbooks, write detections mapped to ATT&CK, and hunt for what the detections miss.

- Triage playbooks: phishing email analysis (headers, SPF, DKIM, DMARC, links and attachments), brute force and password spraying, malware and ransomware alerts, suspicious PowerShell and account compromise
- Sigma rules mapped to MITRE ATT&CK
- Baselines and false-positive reduction
- Hypothesis-driven threat hunting on replayed network and Active Directory attacks
- SOAR and automation concepts

IN THE LAB

Analyze real-world-style phishing emails; Write and test Sigma detections; Run a hypothesis-driven hunt

YOU HAND IN

Detection rules and a hunt report

M6

10 hours

About weeks 4 to 5

Incident handling and response

Handle an incident from detection to recovery, and communicate it clearly to management and to authorities where required.

- The incident handling and response process: preparation, detection and analysis, containment, eradication, recovery and lessons learned
- Playbooks for malware, email, web application, network, insider and cloud incidents
- First response, evidence preservation and escalation
- CERT-In six-hour reporting and data breach duties under India's DPDP Act
- Incident communication and the incident report

IN THE LAB

Run a tabletop exercise; Contain and eradicate a simulated malware incident

YOU HAND IN

Incident handling report

M7

14 hours

About weeks 5 to 6

Digital forensics and malware analysis

Prove what happened: acquire and analyze disk, memory, network and email evidence, examine suspicious files, and build a defensible timeline.

- The forensic investigation process, chain of custody and order of volatility
- Disk acquisition and analysis with Autopsy; Windows file systems and artifacts
- Memory forensics with Volatility
- Network and email forensics
- Linux forensics basics
- Malware analysis basics: static and dynamic analysis in a sandbox, and extracting indicators of compromise
- Anti-forensics awareness, timelines and the forensic report

IN THE LAB

Investigate a disk image and a memory image from a simulated breach; Analyze a suspicious file in a sandbox

YOU HAND IN

DFIR investigation report

M8

4 hours

About week 6

AI in the SOC

Use an AI assistant to work faster on alerts and notes, without letting it make the decision.

- Summarizing alerts, explaining log events and drafting incident notes with an LLM assistant
- Drafting search queries and Sigma rules with AI, then testing them against real events
- Limits: hallucinations, privacy of log data and a human decision on every escalation
- Watching AI applications for prompt injection and misuse

IN THE LAB

Draft and verify a detection with AI help

YOU HAND IN

Verified AI-assisted detection

M9

10 hours

About week 6

Capstone: incident simulation

Handle a live, timed multi-alert shift, from first alert to forensic findings, escalation and handover.

- A timed multi-alert simulation with written investigations
- CTF challenges on detection, investigation and forensics
- An incident case with evidence, a timeline, a shift handover and an escalation
- Technical oral exam on your investigation

IN THE LAB

Timed simulation

YOU HAND IN

SOC monitoring and detection report, and DFIR report

HTA-101 · Beginner to advanced

Application Security (Web, API, Android, Thick Client)

Test web applications, APIs, Android apps and thick-client software by method, then report and retest.

6 weeks
90 guided hours

11 modules
each with a lab

Beginner to advanced
Level

₹20,000 + GST
₹23,600 with GST

THE 6 WEEKS AT A GLANCE



Week 1 | Week 2 | Week 3 | Week 4 | Week 5 | Week 6

Bar widths are the module hours. On a weekday batch (15 hours a week) the weeks are approximate; the trainer confirms the pace for your batch.

Before you start

Basic computer skills. The course starts with Linux, Windows and networking fundamentals, then web and API fundamentals. A short admissions check confirms your starting point.

Prepares you for

Application security tester, Web and API penetration tester, Mobile application security tester, VAPT analyst

Lab tools: Burp Suite, OWASP ZAP, ffuf, SQLmap, Postman, Semgrep, Android emulator and ADB, jadx, apktool, MobSF, Frida, objection, Sysinternals, dnSpyEx or ILSpy, Wireshark

MODULE BY MODULE

M1

5 hours
About week 1

Linux fundamentals for security testing

Work comfortably on the Linux command line, the system most security tools run on.

- The Linux file system, users, groups and permissions
- Navigating, searching and editing from the command line: ls, cd, grep, find, pipes and redirection
- Processes, services and logs
- Installing and updating security tools
- Bash scripting basics and SSH

IN THE LAB

Complete a set of command-line tasks on a Kali Linux machine; Write a Bash script that automates a repeated task

YOU HAND IN

Linux command and script notes

M2

4 hours

About week 1

Windows fundamentals for security testing

Understand how a Windows system is organized, because desktop and server applications run on it.

- Windows users, groups, services and the registry
- File and folder permissions, and network shares
- The command prompt and PowerShell basics
- Windows event logs and the Sysinternals tools

IN THE LAB

Explore a Windows machine from the command prompt and PowerShell; Read the permissions on a service and a shared folder

YOU HAND IN

Windows command and PowerShell notes

M3

5 hours

About week 1

Networking fundamentals for security testing

Explain how data moves across a network, and read ports, addresses and protocols the way a tester does.

- TCP/IP, IP addressing, subnets and routing
- Ports, protocols and the TCP handshake
- DNS, DHCP, ARP and ICMP
- Common services and their ports: HTTP, HTTPS, SSH, SMB and RDP
- Firewalls, NAT and proxies, and what they hide from a tester

IN THE LAB

Map a small network by hand with ping, traceroute and Netcat; Capture and read a web request in Wireshark

YOU HAND IN

Network notes and a labelled diagram

M4

9 hours

About weeks 1 to 2

Web and API fundamentals, mapping and test planning

Map an application and its APIs completely, and plan a test that covers every role, endpoint and risk category.

- HTTP and HTTPS, TLS, cookies, headers, the same-origin policy and CORS basics
- Burp Suite set-up: proxy, scope, site map, Repeater and Intruder
- Content discovery with ffuf, and reading client-side JavaScript
- REST, SOAP and GraphQL; OpenAPI and schemas; building an API inventory
- Standards: OWASP Top 10:2025, OWASP API Security Top 10:2023, WSTG and ASVS
- Engagement scope, rules of engagement and the endpoint-and-role coverage matrix

IN THE LAB

Map a multi-role web application and its API; Build the coverage matrix you will use all course

YOU HAND IN

Application map and coverage matrix

M5

10 hours

About weeks 2 to 3

Authentication, sessions and access control

Break login, session and permission controls, including the object, property and function-level flaws most common in APIs.

- Authentication, MFA and password-reset flows; session handling and logout
- JWT handling, OAuth 2.0 and OpenID Connect
- Horizontal and vertical access control; IDOR and BOLA
- Mass assignment and property-level authorization (BOPLA); function-level authorization (BFLA)
- Multi-role and multi-tenant testing
- CSRF, CORS misconfiguration and clickjacking

IN THE LAB

Two-account access-control testing across the coverage matrix; Forge and tamper with JWTs in a vulnerable API

YOU HAND IN

Access-control findings with evidence

M6

10 hours

About week 3

Injection and server-side attacks

Find, confirm and explain injection and server-side flaws, and show developers exactly how to fix them.

- SQL injection, including careful use of SQLmap; NoSQL injection
- OS command injection, server-side template injection and insecure deserialization
- Cross-site scripting (reflected, stored and DOM-based) and Content Security Policy
- File upload, path traversal and file inclusion
- XXE, and SSRF including cloud metadata services

IN THE LAB

Exploit each class in authorized labs, then write the fix; Chain SSRF to reach an internal service

YOU HAND IN

Injection findings with reproduction steps and fixes

M7

8 hours

About weeks 3 to 4

Business logic, advanced web attacks and GraphQL

Test what scanners cannot: business workflows, race conditions, request-level attacks and GraphQL APIs.

- Business logic and sensitive workflows; limits, quotas and resource consumption
- Race conditions and state transitions
- Host-header attacks, request smuggling, cache poisoning and cache deception
- WebSockets and client-side prototype pollution
- GraphQL: introspection, resolver-level authorization, batching and query depth

IN THE LAB

Exploit a race condition in a checkout flow; Test a GraphQL API

YOU HAND IN

Business-logic and GraphQL findings

M8

12 hours

About weeks 4 to 5

Android application penetration testing

Test an Android app end to end: unpack and read it, find insecure storage and components, bypass client-side controls and test its back-end API.

- Android architecture, the APK format, permissions and the app sandbox
- Lab set-up: Android emulator, ADB and a rooted test device image
- OWASP Mobile Top 10 (2024), MASVS and MASTG
- Static analysis with jadx, apktool and MobSF: hardcoded secrets, insecure configuration and weak cryptography
- Insecure data storage: shared preferences, databases, logs and backups
- Exported activities, services, content providers, intents, deep links and WebViews
- Intercepting app traffic with Burp; certificate pinning and root-detection bypass with Frida and objection
- Testing the mobile back-end API

IN THE LAB

Assess intentionally vulnerable Android apps in an emulator; Bypass certificate pinning and test the app's API

YOU HAND IN

Android application penetration test findings

M9

8 hours

About week 5

Thick-client application penetration testing

Assess a desktop application and its server: traffic, local storage, binaries and the Windows environment it runs in.

- Two-tier and three-tier thick-client architectures; .NET and Java desktop applications
- Information gathering with Sysinternals tools such as Process Monitor
- Intercepting HTTP and non-HTTP traffic between the client and its server
- Insecure local storage: configuration files, the registry, hardcoded credentials and database connection strings
- Decompiling .NET applications with dnSpyEx or ILSpy, and patching client-side checks
- DLL hijacking and insecure file and service permissions
- Direct database access and injection through the client
- OWASP Desktop App Security Top 10

IN THE LAB

Assess an intentionally vulnerable thick-client application end to end

YOU HAND IN

Thick-client assessment findings

M10

9 hours

About weeks 5 to 6

Secure code review, DevSecOps and AI application security

Read code for security flaws, use SAST and DAST tools with judgment, and test AI features for prompt injection and data leaks.

- Threat modeling with STRIDE
- Secure code review basics: spotting injection and authorization flaws in code
- SAST with Semgrep and DAST with OWASP ZAP and Burp's scanner; dependency and secrets scanning
- How chat assistants, RAG and agents sit behind web and API endpoints
- OWASP Top 10 for LLM Applications 2025: prompt injection, improper output handling, sensitive information disclosure and excessive agency
- AI-assisted testing: payload ideas and report drafting, verified by hand

IN THE LAB

Review a vulnerable code base and confirm the flaws in the running app; Attack an intentionally vulnerable chat assistant with a knowledge base and tools

YOU HAND IN

Code-review notes and AI feature test notes

M11

10 hours

About week 6

Capstone assessment

Assess unseen targets against the clock, report them professionally and verify the fixes in a formal retest.

- Assess an unseen web application and its API, plus an Android app or a thick-client application
- CTF challenges on web, API and mobile flaws
- Complete coverage matrix and an explanation of false positives
- Fix representative flaws, report and run a formal retest
- Technical oral exam on your findings

IN THE LAB

Timed practical assessment and retest

YOU HAND IN

Web, API, Android and thick-client reports (R-01 to R-04)

HTA-102 · Beginner to advanced

Network and Active Directory Penetration Testing

Become a network penetration tester: advanced enumeration, exploitation, pivoting and Active Directory forest attacks.

6 weeks
90 guided hours

15 modules
each with a lab

Beginner to advanced
Level

₹20,000 + GST
₹23,600 with GST

THE 6 WEEKS AT A GLANCE



Bar widths are the module hours. On a weekday batch (15 hours a week) the weeks are approximate; the trainer confirms the pace for your batch.

Before you start

Basic computer skills. The course starts with virtualization, lab setup and Linux, networking and Windows fundamentals before any attacks. A short admissions check confirms your starting point.

Prepares you for

Network penetration tester, VAPT analyst, Junior red team operator

Lab tools: Nmap, Nessus, Metasploit, BloodHound, Impacket, NetExec, Certipy, Hashcat, John the Ripper, Chisel, Ligolo-ng

MODULE BY MODULE

M1

3 hours
About week 1

Virtualization fundamentals

Run and manage the virtual machines the whole course is built on.

- Hypervisors: VirtualBox and VMware
- Virtual machines, disks, snapshots and clones
- Virtual networking: NAT, host-only, internal and bridged
- What your laptop needs to run the lab, and keeping the lab off your own network
- Backing up and moving lab machines

IN THE LAB

Install a hypervisor and create a Linux and a Windows machine; Take a snapshot, break the machine and roll it back

YOU HAND IN

Working virtual machines with snapshots

M2

4 hours

About week 1

Penetration testing lab setup

Set up the segmented lab with a multi-domain Active Directory forest that you test in for the rest of the course.

- Lab design: segmented subnets and an attacker machine
- Linux and Windows target hosts
- A multi-domain Active Directory forest
- Isolating the lab and rebuilding it from snapshots

IN THE LAB

Import the lab machines, build the Windows machines from the guides, configure the networks and snapshot the lab

YOU HAND IN

Lab diagram and a working lab

M3

5 hours

About week 1

Linux fundamentals for security testing

Work comfortably on the Linux command line and read a Linux system the way an attacker and a defender do.

- The Linux file system, users, groups and permissions
- Command line skills: text processing, grep, find, pipes and redirection
- Processes, services, cron jobs and logs
- Package management and installing tools
- Bash scripting basics, SSH and file transfer

IN THE LAB

Complete command-line tasks on a Kali Linux and an Ubuntu machine; Write a Bash script that automates a repeated task

YOU HAND IN

Linux command and script notes

M4

6 hours

About weeks 1 to 2

Networking fundamentals for security testing

Explain how traffic crosses a segmented network, and read addresses, ports and protocols the way a tester does.

- TCP/IP, subnets and routing
- Ports, protocols and the TCP handshake
- DNS, DHCP, ARP and ICMP
- Common services and their ports: SMB, SSH, RDP, SMTP and databases
- Firewalls, NAT and VLANs, and how segmentation limits an attacker
- Reading a network diagram

IN THE LAB

Map the lab network by hand; Test reachability between segments with ping, traceroute and Netcat

YOU HAND IN

Network diagram of the lab

M5

9 hours

About week 2

Linux service enumeration and exploitation

Enumerate and compromise Linux hosts and their network services, then escalate to root.

- Passive OSINT and internet-wide search engines, checked against scope
- Nmap in depth: discovery, TCP and UDP scans, version detection and the scripting engine
- Service enumeration: SMB, SNMP, NFS, SMTP, SSH, HTTP and databases
- Common service misconfigurations and default credentials
- Metasploit, and manual exploitation with public exploit code
- Linux privilege escalation: sudo, SUID, cron, capabilities and kernel issues
- Python for testers: automating enumeration

IN THE LAB

External attack-surface map of a fictional company; Full enumeration of the segmented lab; Exploit a Linux target with and without Metasploit and escalate to root; Write a Python script that parses Nmap output

YOU HAND IN

Attack-surface inventory and Linux exploitation evidence

M6

4 hours

About weeks 2 to 3

Network traffic analysis and sniffing

Capture and read network traffic, find what leaks in clear text, and understand man-in-the-middle attacks.

- Wireshark: capture and display filters
- Protocol analysis: HTTP, FTP, Telnet, SMTP, DNS and SMB
- Finding clear-text credentials
- Capturing traffic on a switched network and man-in-the-middle attacks, in an isolated lab
- What TLS protects, and what it does not

IN THE LAB

Capture a login and find the credentials; Intercept traffic between two lab machines

YOU HAND IN

Packet-capture analysis notes

M7

5 hours

About week 3

Windows fundamentals for security testing

Understand how a Windows system is organized and administered, before attacking one.

- Windows users, groups, SIDs, services and the registry
- File and folder permissions, and network shares
- The command prompt and PowerShell
- Windows event logs, Sysmon and the Sysinternals tools
- Windows networking: SMB, RDP and WinRM

IN THE LAB

Explore a Windows machine from the command prompt and PowerShell; Write a PowerShell script that lists users and services

YOU HAND IN

Windows command and PowerShell notes

M8

9 hours

About week 3

Windows exploitation and post-exploitation

Compromise Windows machines: attack passwords, escalate privileges and move to other hosts.

- Windows exploitation and common service misconfigurations
- Password attacks: spraying and brute force within agreed limits, and hash cracking with Hashcat and John the Ripper
- Pass-the-hash and credential reuse
- Windows privilege escalation: services, scheduled tasks, stored credentials and token privileges
- Lateral movement: WinRM, PsExec-style execution, WMI and RDP
- Persistence concepts, cleaning up after a test, and how defenders see your activity in Sysmon

IN THE LAB

Exploit a Windows target and escalate to administrator; Crack captured hashes with rules and masks; Move from one Windows host to another

YOU HAND IN

Windows exploitation and lateral movement evidence

M9

5 hours

About week 4

Active Directory fundamentals

Explain how an Active Directory domain is built and how it authenticates users, before attacking one.

- Domains, trees, forests and trusts
- Domain controllers, LDAP and DNS in Active Directory
- Kerberos and NTLM authentication in outline
- Users, groups, organizational units, GPOs and ACLs
- Administrative tiers and delegation of control

IN THE LAB

Explore the lab domain with Active Directory Users and Computers and PowerShell; Read a GPO and trace a user's group memberships

YOU HAND IN

Map of the lab forest

M10

13 hours

About weeks 4 to 5

Active Directory security assessment

Take a multi-domain forest from a low-privilege user to domain and forest admin, and recommend the fixes that break each path.

- Enumeration with NetExec (nxc), LDAP queries and BloodHound attack-path analysis
- Kerberoasting, AS-REP roasting, NTLM relay and authentication coercion
- ACL abuse with bloodyAD
- Delegation attacks: unconstrained, constrained and resource-based constrained delegation
- Active Directory Certificate Services (AD CS) attacks with Certipy
- DCSync, golden and silver ticket concepts, and attacks across forest trusts
- Hybrid identity with Entra ID (introduction); hardening: tiered administration, Windows LAPS, gMSA, SMB and LDAP signing

IN THE LAB

Attack the lab forest from a low-privilege user to forest admin; Exploit a misconfigured certificate template

YOU HAND IN

Attack-path diagram and hardening plan

M11

6 hours

About week 5

Vulnerability assessment, configuration review and wireless

Run credentialed and uncredentialed scans, validate and prioritize the results, review configurations against benchmarks and assess wireless security.

- Nessus: scan policies, credentialed and uncredentialed scans
- Triage: false positives, manual validation and business context; old vulnerabilities on legacy Windows systems and how to eliminate false positives with Nessus and Metasploit
- Prioritization with CVSS v4, EPSS and CISA's Known Exploited Vulnerabilities catalog
- Configuration review against CIS Benchmarks for Windows, Linux and network devices
- Wireless assessment: WPA2 and WPA3, handshake capture and cracking, rogue access points (lab demonstration)

IN THE LAB

Credentialed scan with manual validation of the top findings; Scan legacy Windows systems with Nessus, then confirm or reject each finding with Metasploit; CIS benchmark review of a Windows server

YOU HAND IN

Validated vulnerability assessment summary

M12

5 hours

About week 5

Pivoting and tunneling

Reach hosts you cannot connect to directly by tunneling through a machine you already control.

- Tunneling and pivoting: SSH, SOCKS proxies, Chisel and Ligolo-ng, including double pivots
- Port forwarding and proxychains
- Attacking an isolated subnet through a foothold
- How tunnels look to defenders

IN THE LAB

Pivot through two subnets to reach an isolated host

YOU HAND IN

Attack-path evidence across the segmented network

M13

3 hours

About weeks 5 to 6

Engagement management, methodology and law

Run an engagement the professional way: scope, authorization, method and evidence.

- Law and ethics: the IT Act, written authorization, scope and rules of engagement
- Why clients commission VAPT: ISO 27001, PCI DSS, CERT-In, RBI and SEBI requirements
- Methodology: PTES and NIST SP 800-115; internal, external and assumed-breach tests
- CVE, CWE and CVSS v4; evidence handling and note-taking
- Cyber Kill Chain and MITRE ATT&CK: describing an attack in the common language of defenders

IN THE LAB

Draft the rules of engagement for a sample client

YOU HAND IN

Rules-of-engagement document

M14

4 hours

About week 6

AI-assisted testing and professional reporting

Use an AI assistant safely to speed up analysis and writing, and turn findings into a report managers and engineers can act on.

- Using an LLM assistant to summarize scan output, suggest next steps and draft commands, then verifying every answer in the lab
- Client data and confidentiality: what never goes into a public AI service
- Report structure: executive summary, scope, methodology, findings and remediation
- Writing a finding: impact, evidence, reproduction steps, CVSS v4 rationale and a specific fix
- Mapping each finding to a MITRE ATT&CK technique and a Cyber Kill Chain stage, so a client can compare it with their own detections
- Peer review, and presenting findings to a client

IN THE LAB

Rewrite a weak finding into a reviewed one; Summarize a large scan export with AI, then check it against the evidence

YOU HAND IN

Peer-reviewed report sections

M15

9 hours

About week 6

Capstone assessment

Show you can do the job: compromise an unseen segmented network and forest against the clock, then defend your report.

- Assess an unseen segmented network and Active Directory forest end to end
- CTF challenges across the course's tools and techniques
- Technical and management report with an attack-path diagram
- Technical oral exam on your findings

IN THE LAB

Timed practical assessment

YOU HAND IN

Network and Active Directory penetration test reports (R-05, R-06)

FEES, IN FULL

OPTION	LENGTH	FEE	WITH 18% GST
Any one course above	6 weeks, 90 hours	₹20,000 + GST	₹23,600
VAPT Track (HTA-101 then HTA-102; in full or 2 installments)	12 weeks, 180 hours	**₹30,000 + GST**	**₹35,400**

Each EC-Council certification fee includes one exam attempt. Course fees do not include an EC-Council exam. Certification fees: hackingtrainer.com/certifications/

HOW TO JOIN

1. **Call or WhatsApp** +91 86868 92922, or send the form on our website.
2. **Sit in 3 to 5 classes free** in a running batch, in the room or online.
3. **Choose your course and batch.** We confirm batch, time, mode and fee in writing.
4. **Pay and get your receipt.**
5. **Start.** Bring a laptop with 16 GB RAM (32 GB recommended).

REFUND AND CANCELLATION

We cancel or move your batch	Full refund, or a seat in another batch
You cancel before your batch starts	Your fee back, less a ₹1,000 processing fee
You leave in the first 5 class days	The part of the fee for classes not yet held, less ₹1,000
After the first 5 class days	No refund; one free move to a later batch within 12 months
EC-Council exam voucher already bought	No refund for the voucher

Full policy: hackingtrainer.com/refund-policy

BATCHES

Monday to Friday: Online, morning (India and US) 7:30 to 9 AM; Hybrid class (classroom and online) 11 AM to 12:30 PM; Practice support at the center 1:30 to 8:30 PM; Online, evening (India and US) 7:30 to 9 PM (IST). Weekend: Saturday and Sunday, class 11 AM to 1 PM, then 2 hours of practice.

Start dates change every few weeks, so they are not printed here: hackingtrainer.com/upcoming-batches-schedule/

Our classes use training environments built by others: Metasploitable from Rapid7, the OWASP Broken Web Applications project, and the GOAD (Game of Active Directory) lab from Orange Cyberdefense. We set them up for class. We did not create them, and we are not affiliated with or endorsed by these organizations.

Our honest answer on placement

We do not provide job placement or placement assistance. We give you the skill, graded reports to show employers, and interview preparation. The employer decides who to hire.

+91 86868 92922 · call or WhatsApp
info@hackingtrainer.com · hackingtrainer.com
Ground Floor, G-3, Sri Venkatasai Nest, Kallu Compound Road, Nagarjuna Nagar Colony, Yella Reddy Guda, Ameerpet, Hyderabad, Telangana 500073
Open 7 days: Monday to Friday 8:30 AM to 8:30 PM IST; Saturday and Sunday 10 AM to 6 PM IST · Scan to WhatsApp us