ASD ACADEMY

HACKER VLOG

EKLAVYA BATCH WITH AI

6 MONTH ONLINE COURSE

Introducing..

"CyberGuard AI Academy: Mastering Defense in the Age of Intelligence."

POWERED BY

PODCAST

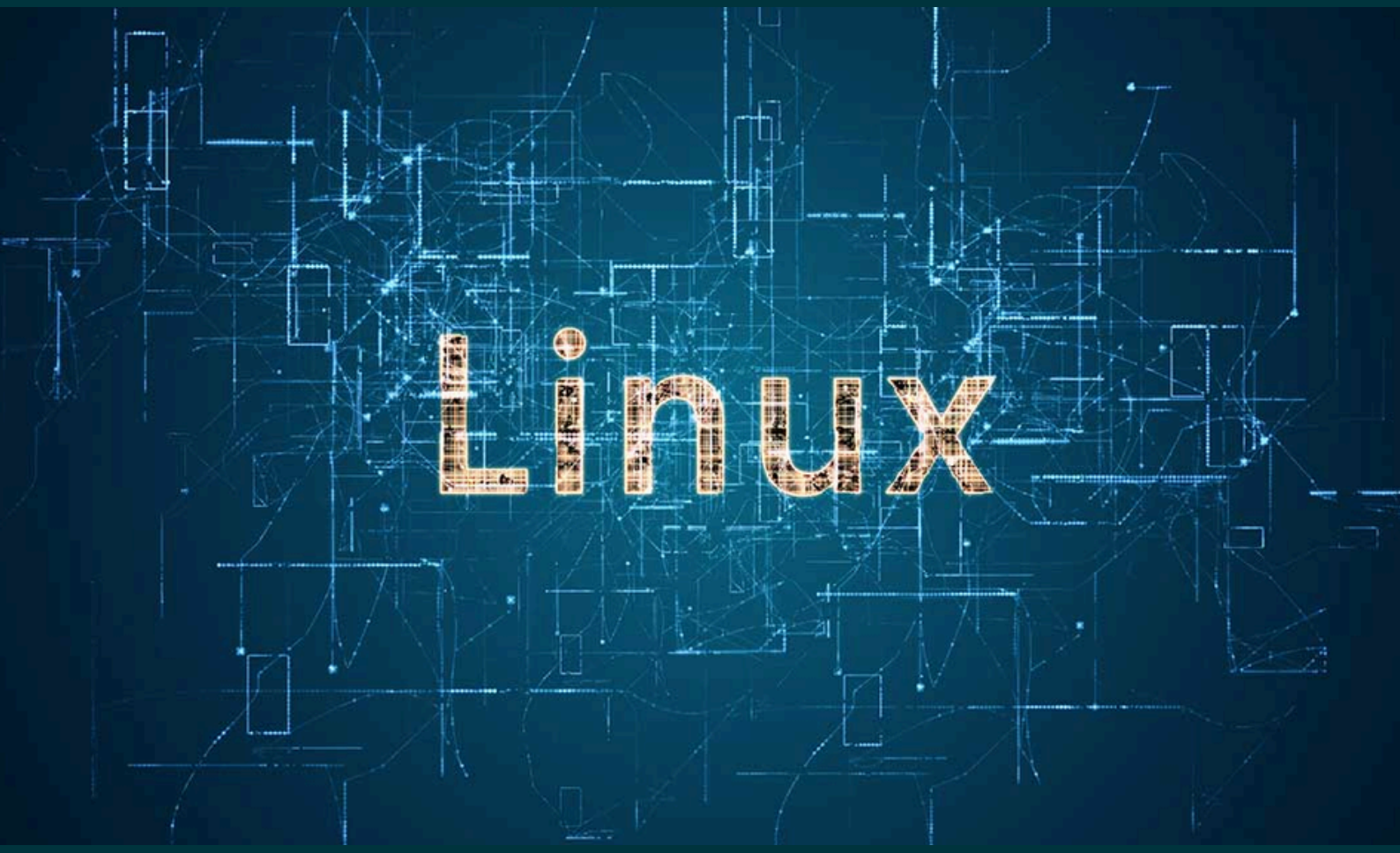
REGISTERED BY

iSTART

Linux for Hackers

Course Syllabus

S.No	Topic Name	Sub-Topics Covered
1	**Architecture & Precision Navigation**	The Shell & Directory Structure: /etc (configs), /tmp (writable space), /var/log (traces) — attacker's perspective.
2	**Users, Groups & the 'Root' Goal**	Identity Recon: Using whoami, id, and groups to see what you've compromised.
3	**Networking & Remote Access**	Network Enumeration: Using ip a, netstat -antp (checking for open ports), and ss to see who the machine is talking to.
4	**Processes, Persistence & Hardening**	Process Hunting: Using ps aux, top, and kill to find and stop defensive software or hidden miners



Networking

Course Syllabus

S.No	Topic Name	Sub-Topics Covered
1	**Introduction to Networking & CCNA Lab Setup**	Overview of Networking, Lab Setup Basics, Packet Tracer/Simulation Tools.
2	**Types of Networks, Wired vs Wireless Communication**	LAN, WAN, MAN, Wired Media Types, Wireless Standards.
3	**IPv4 Addressing**	Address Classes, Public vs Private IPs, Subnet Mask.
4	**Subnetting**	FLSM, VLSM, Subnet Calculations.
5	**CIDR & VLSM**	CIDR Notation, Route Aggregation, VLSM Planning.
6	**Networking Devices & Security Devices**	Router, Switch, Hub, Firewall, IDS/IPS.
7	**Network Cables**	Coaxial, Twisted Pair, Fiber Optic.
8	**OSI Model**	7 Layers, Functions of Each Layer.
9	**TCP/IP Model & Protocols**	4 Layers, Important Protocols per Layer.
10	**Device Management**	Console Access, SSH/Telnet Configuration.
11	**Switch Operations**	MAC Table, Switching Logic & Forwarding.
12	**VLANs & Inter-VLAN Routing**	VLAN Concepts, Router on a Stick.
13	**DTP & VLAN Ports**	Trunk vs Access Ports, DTP Negotiation.
14	**Spanning Tree Protocol**	Loops in Switching, STP Types (STP, RSTP, PVST).
15	**Switching Security & Redundancy**	Port Security, Redundancy Protocols.
16	**Static & Default Routing**	Static Routes, Default Routes, Floating Routes.
17	**RIP & EIGRP Basics**	Distance Vector Protocols, Metrics & Configuration.
18	**OSPF**	OSPF Areas, LSA Types, DR/BDR Election.

S.No	Topic Name	Sub-Topics Covered
19	**ACLs (Access Control Lists)**	Standard ACLs, Extended ACLs, Named ACLs.
20	**NAT & PAT Concepts**	Types of NAT, PAT Working Principle.
21	**NAT Configuration**	Static NAT, Dynamic NAT, Overload (PAT).
22	**Remote Device Access**	SSH, Telnet, VTY Line Configuration.
23	**Wireless Devices & Standards**	802.11 Standards, Access Points, Wireless Security.
24	**Final Lab – Campus & Branch Setup**	Campus Topology, Branch Connectivity.

Course Highlights

24 Modules	Packet Tracer Labs	Hands-on Projects
CCNA Foundation Coverage	Simulation Tools Included	Campus & Branch Lab

CEH

Course Syllabus

S.No	Topic Name	Sub-Topics Covered
1	**Introduction to Ethical Hacking**	Learn The Fundamentals And Key Issues in Information Security, Including The Basics of Ethical Hacking, Information Security Controls, Relevant Laws, And Standard Procedures.
2	**Footprintingand Reconnaissance**	Learn How to Use The Latest Techniques And Tools For Footprinting And Reconnaissance, a Critical Pre-Attack Phase of Ethical Hacking.
3	**Scanning Networks**	Learn Different Network Scanning Techniques And Countermeasures.
4	**Enumeration**	Learn Various Enumeration Techniques, Including Border Gateway Protocol (BGP) and Network File Sharing (NFS) Exploits and Associated Countermeasures.
5	**Vulnerability Analysis**	Learn How to Identify Security Loopholes in a Target Organization's Network, Communication Infrastructure, and Systems. Diferent Types of Vulnerability Assessment and Vulnerability Assessment Tools are Also Included.
6	**System Hacking**	Learn About The Various System Hacking Methodologies Used to Discover System and Network Vulnerabilities, Including Steganography, Steganalysis Attacks, and How to Cover Tracks.
7	**Malware Threats**	Learn About Different Types of Malware (Trojan, Viruses, Worms, etc.), APT and Fileless Malware, Malware Analysis Procedures, And Malware Countermeasures.
8	**Sniffing**	Learn About Packet Sniffing Techniques And Their Uses For Discovering Network Vulnerabilities, Plus Countermeasures to Defend Against Snifing Attacks.
9	**Social Engineering**	Learn Social Engineering Concepts and Techniques, Including How to Identify The Attempts, Audit Human-Level Vulnerabilities, and Suggest Social Engineering Countermeasures.
10	**Denial-of-Service**	Learn about different Denial of Service (DoS) and Distributed Dos (DDoS) attack techniques, plus the tools used to audit a target and devise DoS and DDoS countermeasures and protections.

S.No	Topic Name	Sub-Topics Covered
11	**Session Hijacking**	Learn the Various Session-Hijacking Techniques Used to Discover Network-Level Session Management, Authentication, Authorization, and Cryptographic Weaknesses and Associated Countermeasures.
12	**EvadingIDS, Firewalls, and Honeypots**	Learn About Firewalls, Intrusion Detection Systems (IDS), and Honeypot Evasion Techniques; The Tools Used to Audita Network Perimeter For Weaknesses; and Countermeasures.
13	**Hacking Web Servers**	Learn About Web Server Attacks, Including a Comprehensive Attack Methodology Used to Audit Vulnerabilities in Web Server Infrastructures and Countermeasures.
14	**Hacking Web Applications**	Learn About Web Application Attacks, Including a Comprehensive Hacking Methodology For Auditing Vulnerabilities in Web Applications and Countermeasures.
15	**SQL Injection**	Learn About SQL Injection Attack Techniques, Evasion,Techniques, and SQL Injection Counter Measures.
16	**Hacking Wireless Networks**	Learn About Different Types of Encryption, Threats, Hacking Methodologies, Hacking Tools, Security Tools, and Countermeasures For Wireless Networks.
17	**HackingMobile Platforms**	Learn Mobile Platform Attack Vectors, Android and ios Hacking, Mobile Device Management, Mobile Security Guidelines, and Security Tools.
18	**loT Hacking**	Learn Different Types of Internet of Things (IoT) and Operational Technology (OT) Attacks, Hacking Methodologies, Hacking Tools, and Countermeasures.
19	**Cloud Computing**	Learn Different Cloud Computing Concepts, Such as Container Technologies and Serverless Computing. Various Cloud Computing Threats, Attacks, Hacking Methodologies, and Cloud Security Techniques and Tools.
20	**Cryptography**	Learn About Encryption Algorithms, Cryptography Tools, Public Key Infrastructure (PKI), Email Encryption, Disk Encryption, Cryptography Attacks, and Cryptanalysis Tools.

WAPT

Course Syllabus

S.No	Topic Name	Sub-Topics Covered
1	**Introduction to Web Application Testing**	Basics of testing web applications to identify security flaws and vulnerabilities.
2	**Burp Suite**	Learn to intercept, analyze, and modify HTTP requests using Burp Suite.
3	**ZAP Proxy & NetSparker**	Use automated tools to scan and detect web application vulnerabilities.
4	**Convert VA Report into PT**	Transform vulnerability assessment findings into a structured penetration testing report.
5	**Application Walkthrough, Identify Functionality & Report Writing**	Understand application flow, identify features, and document security findings.
6	**Security Headers**	Analyze HTTP security headers to enhance application protection.
7	**Cookies & SSL Vulnerabilities**	Identify risks related to cookies and SSL/TLS misconfigurations.
8	**SQL Injection & XSS**	Detect and exploit database injection and cross-site scripting flaws.
9	**CSRF & Clickjacking**	Understand attacks that trick users into performing unintended actions.
10	**DOM-Based Vulnerabilities & CORS**	Identify client-side vulnerabilities and misconfigured cross-origin policies.
11	**XXE & SSRF**	Exploit server-side request handling and XML parsing weaknesses.
12	**OS Command Injection & Path Traversal**	unauthorized access by executing system commands or accessing restricted files.
13	**Access Control Vulnerabilities & Authentication**	Find flaws in user permissions and authentication mechanisms.
14	**Insecure Deserialization & Information Disclosure**	Identify risks from unsafe data handling and leakage of sensitive information.
15	**Business Logic Vulnerabilities & HTTP Host Header Attacks**	Exploit application logic flaws and header manipulation issues.
16	**OAuth Authentication & File Upload Vulnerabilities**	Analyze weaknesses in third-party login systems and file upload features.
17	**JWT & Introduction to API Testing**	Understand token-based authentication and basics of testing APIs.

API Security

Course Syllabus

S.No	Topic Name	Sub-Topics Covered
1	**Broken Object Level Authorization**	APIs Tend to Expose Endpoints That Handle Object Identifiers, Creating a Wide Attack Surface of Object Level Access Control Issues.
2	**Broken Authentication**	Authentication Mechanisms are Often Implemented Incorrectly, Allowing Attackers to Compromise Authentication Tokens or to Exploit Implementation Flaws to Assume Other User's Identities Temporarily or Permanently.
3	**Broken Object Property Level Authorization**	Focusing on The Root Cause: The Lack of or Improper Authorization Validation at The Object Property Level.
4	**Unrestricted Resource Consumption**	Satisfying API Requests Requires Resources Such as Network Bandwidth, CPU, Memory, and Storage.
5	**Broken Function Level Authorization**	Complex Access Control Policies With Different Hierarchies, Groups, and Roles.
6	**Unrestricted Access to Sensitive Business Flows**	A Vulnerability Where an API Endpoint is Functionally Correct But Lacks Safeguards to Prevent Bots or Users From Excessively Exploiting The Business Logic.
7	**Server Side Request Forgery**	Server-Side Request Forgery (SSRF) Flaws can Occur When an API is Fetching a Remote Resource Without Validating The User-Supplied URI.
8	**Security Misconfiguration**	APIs and The Systems Supporting Them Typically Contain Complex Configurations, Meant to Make The APIs More Customizable. Software and DevOps Engineers Can Miss These Configurations.
9	**Improper Inventory Management**	APIs Tend to Expose More Endpoints Than Traditional Web Applications, Making Proper and Updated Documentation Highly Important.
10	**Unsafe Consumption of APIs**	Developers Tend to Trust Data Received From Third-Party APIs More Than User Input, and So Tend to Adopt Weaker Security Standards.

OWASP Top 10 FOR LLM

Course Syllabus

S.No	Topic Name	Sub-Topics Covered
1	**Prompt Injection**	Malicious Input Designed to Manipulate an AI Model Into Ignoring Instructions or Revealing Sensitive Data.
2	**Sensitive Information Disclosure**	Exposure of Confidential Data (like Passwords, API keys, or Personal info) Through insecure AI Responses.
3	**Supply Chain**	Risks Arising From Third-Party Tools, Libraries, or APIs that can introduce Vulnerabilities into AI Systems.
4	**Data and Model Poisoning**	Attacks Where Training Data or Models are Tampered With to Produce Biased or Harmful Outputs.
5	**Improper Output Handling**	Failure to Validate or Sanitize AI Outputs, Leading to Security Risks Like Code Injection or Misinformation.
6	**Excessive Agency**	Granting AI Systems too Much Autonomy, Allowing Them to Perform Actions Beyond Intended Permissions.
7	**System Prompt Leakage**	Accidental Exposure of Hidden System Instructions That Guide AI Behavior.
8	**Vector and Embedding Weaknesses**	Exploiting Flaws in Vector Databases or Embeddings to Retrieve or Manipulate Sensitive Information.
9	**Misinformation**	Generation of Incorrect or Misleading Information That Appears Credible.
10	**Unbounded Consumption**	Lack of Limits on AI Usage (API Calls, Tokens, etc.), Leading to Resource Exhaustion or High Costs.

SOC

Course Syllabus

S.No	Topic Name	Sub-Topics Covered
1	**Cyber security and SOC**	Introduction to Cyber Security, SOC Roles & Responsibilities, SOC Workflow.
2	**OS's role in SOC**	Windows Event Logs, Linux Log Files, OS Hardening Basics.
3	**SIEM**	SIEM Architecture, Log Ingestion, Correlation Rules.
4	**Splunk**	Searching & Reporting, Dashboards, Splunk Architecture.
5	**Splunk Admin Tasks**	User Management, Indexing, Data Onboarding.
6	**Cyber Kill Chain**	Reconnaissance, Weaponization, Delivery, Exploit & Installation.
7	**MITRE ATT&CK Framework**	Tactics, Techniques, Mitigation & Detection.
8	**Logs**	Types of Logs, Log Sources, Log Normalization.
9	**SPL**	Search Syntax, Commands, Use Cases.
10	**Use cases in SIEM**	Brute Force, Malware Detection, Privilege Escalation Alerts.
11	**Custom Alerts**	Threshold Alerts, Behavior-Based Alerts, Use-case Mapping.
12	**Threat Hunting**	Hypothesis Creation, Threat Intel Usage, Hunting Techniques.
13	**Ticketing Tools**	Jira, ServiceNow, Ticket Lifecycle.
14	**RCA Report**	Problem Analysis, Timeline Creation, Mitigation Steps.
15	**Capstone Project**	Project Design, Documentation.

Contact Us:

Website: www.asdacademy.in

Email: training@asdacademy.in

Phone: 8233150687 / 9680100687

Hacker Vlog

Hacker Vlog Podcast

@hackervlogofficial / @hackervlog / @cyberexpert.riddhisoral

Address:

AkanshaDeep Heights,18thFloor, No. 1841-1842, Kunadi, Kota (Rajasthan),
Pin Code - 324008

www.skilltrack.top

SCAN ME

ASD ACADEMY
India's Most Advanced
Hacking & Coding Academy

Thank You