



ETHICAL

HACKING

LEARN TO PROTECT YOUR SELF NOW

HOW DO WE EDUCATE



ONLINE

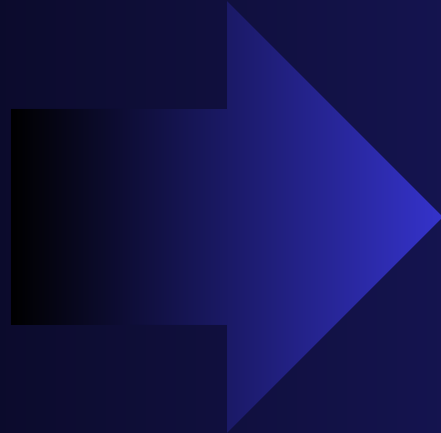


OFFLINE



WORKSHOPS

BECOME
HACKER



**1 MONTHS GLOBLE CERTIFICATION TRAININGS
+
CERTIFICATE OF TRAINING
+
INTERNSHIP**

Hey There,

I am AJAY BHASKAR SIDDI

**Founder & CEO of ABcyberpro
Certified Ethical Hacker , India Book
Of Records holder**



I'm Ajay Bhaskar Siddi, the Founder and CEO of ABcyberpro, and I'm passionate about cybersecurity. I'm a Certified Ethical Hacker and hold a record in the India Book of Records as the youngest Certified Ethical Hacker, where I achieved a score of 124 out of 125. With over five years of experience, I've dedicated myself to cybersecurity since the mind, and I've successfully completed 50+ projects and solved 20+ cases in ethical hacking and cybersecurity.

My Journey in Cybersecurity

I have a hands-on approach to cybersecurity and enjoy contributing to meaningful work in the field. I'm also a trainer at APCID, where I've had the opportunity to solve various cases and guide others in handling cyber threats. Over the years, my experience has expanded to include a range of cybersecurity areas, including:

- Web and Application Penetration Testing
- Ethical Hacking
- Network Security

- IoT and Automotive Security
- Cloud Security
- Digital Forensics
- SIEM Tools

My Skills and Expertise

I'm proficient with a variety of cybersecurity tools, like Nmap, Metasploit, Nessus, and Wireshark. I work in areas including threat analysis, vulnerability assessment, API security, and ISO 27001 Lead Auditing. My goal is always to create innovative, customized solutions that offer the highest level of security for my clients.

About ABcyberpro

At ABcyberpro, I'm focused on delivering excellent cybersecurity services. I'm dedicated to quality and put my clients' needs first, striving to make ABcyberpro a trusted partner in cybersecurity. Through advanced tools, strategic insights, and a results-driven approach, I work to offer tailored solutions that fit each client's unique requirements.

My Mission and Vision

My mission is to raise cybersecurity awareness and help build resilient systems that protect valuable assets in today's digital world. My vision is to make ABcyberpro a leader in cybersecurity solutions, empowering organizations and individuals to thrive securely in a complex digital environment.

What is this Course about ?

Ethical Hacking & WAPT

Ethical hacking is the practice of testing computer systems, networks, or web applications for security vulnerabilities with the permission of the system owner. It involves simulating real-world cyber attacks to identify weaknesses that malicious actors could exploit. Ethical hackers use various tools and techniques to assess security posture and recommend measures to mitigate risks. Web application testing specifically focuses on evaluating the security of web-based applications, including websites and web services. It aims to uncover vulnerabilities such as SQL injection, cross-site scripting (XSS), and insecure authentication mechanisms. Through thorough testing, ethical hackers help organizations enhance their cybersecurity defenses, protect sensitive data, and prevent unauthorized access. This proactive approach to security helps organizations stay ahead of potential threats and ensures the integrity and confidentiality of their digital assets.



WHAT WILL YOU LEARN ?

ETHICAL HACKING

HACKER LAB SETUP

- **VMWARE SETUP IN PC**
- **KALI LINUX INSTALLATION IN VMWARE**
- **METASPLOITABLE – VULNERABLE WEB SERVER**
- **DVWA SETUP**

KALI LINUX FOR HACKERS

- **KALI LINUX OVERVIEW**
- **KALI LINUX SETTINGS AND CONFIGURATION**
- **KALI LINUX READ, WRITE AND EXTRACT PERMISSIONS**
- **KALI LINUX BASIC COMMANDS**

INTRODUCTION TO ETHICAL HACKING

- **TYPES OF HACKERS**
- **ETHICAL HACKING PHASES**
- **HACKING CONCEPTS SECURITY RESEARCHERS, ANALYSTS, AUDITORS ETC...**

INFORMATION GATHERING (FOOTPRINTING)

- **WEBSITE FOOT-PRINTING**
- **WHO IS**
- **VIRUS TOTAL**
- **SHODAN**
- **GHDB (GOOGLE HACKING DATA BASE)**
- **THE HARVESTER TOOL**
- **INFORMATION GATHERING FROM SOCIAL MEDIA**
- **VOIP AND VPN FOOTPRINTING**
- **MALTEGO - ADVANCED TOOL**
- **IMAGE METADATA**

NMAP SCANNING (NETWORK SCANNING)

- **NETWORK SCANNING WITH NMAP**
- **SERVER SCANNING WITH NMAP HOST DISCOVERY PORT DISCOVERY**
- **SERVICE VERSION DETECTION OS DISCOVERY**

NET CAT (POWERFUL TOOL FOR PENTESTERS)

- **PORT SCANNING WITH NETCAT (TCP AND UDP)**
- **CHATTING BETWEEN TWO USERS (INITIATOR AND LISTENER)**
- **BANNER GRABBING (FTP AND SSH) WITH NETCAT**
- **FILE TRANSFER WITH NETCAT**
- **GRABBING THE HTTP BANNER**
- **WINDOWS REVERSE CONNECTION**

METASPLOIT (PENTESTER TOOL)

- **SERVER ENUMERATION WITH METASPLOIT**
- **DETAIL EXPLANATION OF MODULES -1.EXPLOIT
MODULE 2.PAYLOAD MODULE 3.AUXILIARIES
MODULE 4.ENCODER MODULE 5.EVASIONS MODULE
6.POST MODULE**

WEB SERVER HACKING

- **SCANNING WITH NMAP USING SEARCHSPLOIT TOOL
FOR FINDING CVE**
- **FINDING THE EXPLOIT IN RAPID7**
- **USING PEN TESTING TOOL (METASPLOIT)**

SYSTEM HACKING

- **OS BYPASSING**
- **ERROR GENERATION METHOD (CRACKING
PASSWORD)**
- **NGROK CONFIGURATION**
- **WINDOWS REVERSE SHELL**
- **WINDOWS MACHINE HACKING**
- **GETTING THE LIVE SCREEN WITH VNC**

MOBILE HACKING

- **INTRODUCTION TO MOBILE OS ,CREATING REVERSE
SHELL WITH MSFVENOM ,BINDING THE REVERSE
SHELL ,TUNNEL FORWARDING WITH OPEN-SOURCE
TOOL ,GETTING ACCESS IN WAN CONNECTION**
- **GETTING ACCESS IN LAN CONNECTION ,EXPLOITING
THE MOBILE PLATFORMS**

MALWARE

- **TYPES OF MALWARE**
- **VIRUS**
- **WORMS TROJANS**

SNIFFING

- **INTRODUCTION TO SNIFFING**
- **INTRODUCTION TO WIRESHARK TOOL**
- **ANALYZING THE DATA PACKETS FROM WIRESHARK**
- **PERFORMING MAC FLOODING ATTACK**
- **MAN-IN-THE-MIDDLE ATTACK – ARP POISONING**

DOS/DDOS (DISTRIBUTED DENIAL-OF-SERVICE ATTACK)

- **INTRODUCTION TO DENIAL-OF-SERVICE ATTACK**
- **INTRODUCTION TO DISTRIBUTED DENIAL-OF-SERVICE ATTACK**

WIRELESS HACKING

- **WIRELESS ENCRYPTIONS- WEP (WIRED EQUIVALENT PRIVACY) ,WPA (WI-FI PROTECTED ACCESS), WPA2 (WI-FI PROTECTED ACCESS)**
- **HACKING WI-FI NETWORKS**
- **BRUTE FORCING THE WI-FI NETWORKS**
- **WI-FI DEAUTHER ATTACK**
- **INTRODUCTION TO SERVICE DEFINED RADIO**

SOCIAL ENGINEERING

- **INTRODUCTION TO SOCIAL ENGINEERING**
- **TYPES OF SOCIAL ENGINEERING**
- **HUMAN-BASED SOCIAL ENGINEERING**
- **COMPUTER BASED SOCIAL ENGINEERING**
- **INSIDER ATTACKS**
- **EXTERNAL ATTACKS**

PASSWORD CRACKING

- **HACK WINDOWS PASSWORD**
- **USING CMD**
- **HACK LINUX PASSWORD**
- **CRACK SSH PASSWORD**
- **CRACK TELNET PASSWORD**

CRYPTOGRAPHY

- **TYPES OF CRYPTOGRAPHY**
- **SYMMETRIC KEY**
- **ASYMMETRIC KEY**
- **ENCRYPTION ALGORITHMS**

NETWORKING

INTRODUCTION TO NETWORKING

- TYPES OF NETWORK
- NETWORK TOPOLOGIES
- NETWORKING MODELS
- COMPONENTS TO BUILD NETWORKS

PROTOCOLS / PORTS

- TCP
- UDP
- BASIC PROTOCOLS
- BASIC PORTS
- FUNCTIONS OF PROTOCOLS
- SERVICES OF PORTS

TCP/IP MODEL

- APPLICATION LAYER
- TRANSPORT LAYER
- NETWORK LAYER

OSI MODEL

- APPLICATION LAYER
- PRESENTATION LAYER
- SESSION LAYER
- TRANSPORT LAYER
- NETWORK LAYER
- DATA-LINK LAYER
- PHYSICAL LAYER

HANDSHAKING MODELS

- THREE WAY HANDSHAKING TCP/IP

TCP FLAGS / HEADERS

- URG
- ACK
- PUSH
- RST
- SYN
- FIN

WEB APPLICATION PENETRATION TESTING

INTRODUCTION ABOUT WAPT

- **WHAT IS WEB APPLICATION PENETRATION TESTING**
- **VULNERABILITY ASSESSMENTS**
- **PENETRATION TESTING**
- **DVTA SETUP**
- **BWAPP SETUP**
- **BUG HUNTING METHODOLOGY**

CRYPTOGRAPHY

- **TYPES OF CRYPTOGRAPHY**
- **SYMMETRIC KEY**
- **ASYMMETRIC KEY**
- **ENCRYPTION ALGORITHMS**
- **DECODING AND ENCODING**
- **HIDE PLAIN TEXT IN FILES (STEGANOGRAPHY)**

BROKEN AUTHENTICATION AND SESSION MANAGEMENT

- **A01:2021-BROKEN ACCESS CONTROL**
- **A02:2021-CRYPTOGRAPHIC FAILURES**
- **A03:2021-INJECTION**
- **A04:2021-INSECURE DESIGN**
- **A05:2021-SECURITY MISCONFIGURATION**
- **A06:2021-VULNERABLE AND OUTDATED COMPONENTS**
- **A07:2021-IDENTIFICATION AND AUTHENTICATION**
- **A8:2021-SOFTWARE AND DATA INTEGRITY FAILURES**

BURPSUITE

- **REPEATER**
- **WEB CRAWLING**
- **PROXY CONFIGURATION**
- **TARGET SCANNING**

WEB APPLICATION PENETRATION TESTING

XSS (CROSS-SITE SCRIPTING)

- REFLECTED XSS
- STORED XSS
- DOM BASED XSS
- XSS VIA XXE
- XSS THROUGH FILE UPLOADING
- SSRF TO XSS

SQL INJECTION

- ERROR BASED SQL INJECTION
- UNION BASED SQL INJECTION
- BLIND SQL INJECTION
- MANUAL INJECTION
- AUTOMATED SCANNING
- SQLMAP TOOL

FILE INCLUSIONS

CRYPTOGRAPHIC FAILURES

- COLDFUSION VULNERABILITY
- BREACH ATTACK VULNERABILITY
- HEART BLEED VULNERABILITY
- MISSING HSTS
- POODLE ATTACK VULNERABILITY

BROKEN AUTHENTICATION AND SESSION MANAGEMENT

- CREDENTIAL STUFFING
- IMPROPER ADMINISTRATIVE LOGIN
- INSECURE LOGIN FORMS
- INSECURE LOGOUT MANAGEMENT
- SESSION HIJACKING
- SESSION ID EXPOSURE IN URL

CSRF (CROSS SITE REQUEST FORGERY)

- COOKIES ,SESSION ID'S
- SAME ORIGIN POLICY ,CSRF EXPLOITATION

WEB APPLICATION PENETRATION TESTING

SSRF (SERVER-SIDE REQUEST FORGERY)

- NGROK CONFIGURATION
- BLIND SSRF
- BURP COLLABORATOR
- SSRF EXPLOITATION
- SSRF TO XSS

SHELL & COMMAND EXECUTIONS

- FILE UPLOAD VULNERABILITY
- REMOTE CODE EXECUTION
- OS COMMAND INJECTION

XXE (XML EXTERNAL ENTITY)

- INTRODUCTION TO XML
- INTRODUCTION TO XXE INJECTION
- WHAT IS AN ENTITY?
- WHAT IS THE DOCUMENT TYPE DEFINITION (DTD)?

- XXE BILLION LAUGH ATTACK-DOS
- XXE USING FILE UPLOAD
- XXE TO REMOTE CODE EXECUTION
- XSS VIA XXE

ADDITIONAL VULNERABILITIES

- IDOR (INSECURE DIRECT OBJECT REFERENCE)
- HOST HEADER ATTACK
- HTTP REQUEST SMUGGLING
- HTML INJECTION
- OPEN REDIRECTION
- PATH TRAVERSAL
- DIRECTORY TRAVERSAL I
- NSECURE CORS CONFIGURATION
- CLICKJACKING
- NO RATE LIMIT
- PARAMETER OR DATA TAMPERINGCSRF

CONTACT US



+91 9347223943



<https://abcyberpro.com>



abcyberpro81024@gmail.com