GS2
CYBER SECURITY

SYLLABUS

ETHICAL HACKING TRAINING

INTRODUCTION

COURSE DESCRIPTION

Our Ethical Hacking Course is designed to offer an immersive experience in the world of cybersecurity and ethical hacking. This program covers the fundamental skills and knowledge needed to protect organizations against cyber threats and vulnerabilities. Through a hands-on approach, participants will learn to think like hackers to defend against future attacks. This course is ideal for aspiring cybersecurity professionals seeking to enhance their skills in network security, system penetration testing, and ethical hacking.

PREREQUISITES OF ETHICAL HACKING

- ✓ Basic understanding of networking concepts.
- ✓ Familiarity with operating systems, especially Windows and Linux.
- ✓ A keen interest in cybersecurity and ethical hacking.

TARGET AUDIENCE

- ✓ IT professionals who are seeking to transition into cybersecurity roles.
- ✓ Network administrators and engineers.
- ✓ Security officers and practitioners.
- ✓ College students and recent graduates looking to enter the cybersecurity field.
- ✓ Anyone who is willing to know more about the ethical hacking course.

WILL I GET A CERTIFICATE ?

Upon successful completion of the course and passing the examination, participants will receive a certification from GS2 Cyber Security.

ETHICAL HACKING TRAINING

COURSE CONTENT

Ethical hacking training is to introduce candidates to the concept of discovering vulnerabilities.You will learn how to manage security exploits, find vulnerabilities and process issues, and modern pentesting tools.

Module 01 Basics of Networking

Module 02 Linux Essentials - Kali

Module 03 Introduction to Ethical Hacking

Module 04 Web Application Security

Module 05 Viruses, Trojans, Malwares, and OS Level Attacks and Counter Measures

Module 06 Mobile Application Security

Module 07 Advance Penetration Testing & Network VAPT

Module 1 : Basics of Networking

Lesson 01: Introduction to Networking

- What is a Network?
- Local Area Network (LAN) Explained
- Wide Area Network (WAN) Explained
- Type of Mode
- Type of Communication

Lesson 02: Open Systems Interconnection (OSI) Model

- What is Open Systems Interconnection (OSI)
- Why we Need Open Systems Interconnection (OSI)
- Open Systems Interconnection (OSI) Layers
- Transmission Control Protocol (TCP) / User Datagram Protocol (UDP)
- 3 Way Hand Shake

Lesson 03: Transmission Control Protocol (TCP) / Internet Protocol (IP) Model

- What is Transmission Control Protocol (TCP) / Internet Protocol (IP)
- Why we Need Transmission Control Protocol (TCP) / Internet Protocol (IP) Model
- Transmission Control Protocol (TCP) / Internet Protocol (IP) Layer

Lesson 04: Sub Netting

- Subnetting Explained
- Classless Inter-Domain Routing (CIDR)
- Create Subnets
- Understanding Variable Length Subnet Masks (VLSM)
- Private Internet Protocol (IP) Addresses Explained

Lesson 05: Packet Flow in Same & Different Network

- What is Domain Name System (DNS) and How Does it Work?
- Map Hostnames to Internet Protocol (IP) Addresses
- Configure Cisco Device as Domain Name System (DNS) Client
- How to Configure a Cisco Router as a DNS Server?
- no Internet Protocol (IP) domain-lookup Command
- Address Resolution Protocol (ARP) Explained
- Address Resolution Protocol (ARP) Table on a Cisco Router

Lesson 06: Information about Networking Device

- Network Devices
- Network Hubs Explained
- Network Switch Explained
- Carrier Sense Multiple Access with Collision Detection (CSMA CD)
- Collision & Broadcast Domain
- How Switches Work
- Layer 2 Switching
- Network Router Explained
- What Is Layer 3 Switch and how it Works in Our Network?

Lesson 07: Internet Protocol (IP) / Internet Control Message Protocol (ICMP)

- Internet Control Message Protocol (ICMP)
- Ping Explained
- Extended Ping Command
- Traceroute Explained
- Traceroute Command
- Show processes Command

Lesson 08: Automatic Private IP Addressing (APIPA)

- What is Automatic Private IP Addressing (APIPA)
- Why we Need Automatic Private IP Addressing (APIPA)
- Automatic Private IP Addressing (APIPA)

Lesson 09: Address Resolution Protocol (ARP)

- What is Address Resolution Protocol (ARP)
- Why we Need Address Resolution Protocol (ARP)
- Type of Address Resolution Protocol (ARP)

Lesson 10: Dynamic Host Configuration Protocol

- Dynamic Host Configuration Protocol (DHCP) & Domain Name System (DNS)
- Configure Cisco Router as Dynamic Host Configuration Protocol (DHCP) Server
- Dynamic Host Configuration Protocol (DHCP) Relay Agent
- Configure Cisco Router as a Dynamic Host Configuration Protocol (DHCP) Client
- Automatic Private IP Addressing (APIPA)

Lesson 11: Telnet & Secure Shell (SSH)

- What is Telnet & Secure Shell (SSH)
- Why we Need Telnet & Secure Shell (SSH)
- Telnet & Secure Shell (SSH)
- Setting Up Telnet
- Setting Up Secure Shell (SSH)

Module 2: Linux Essentials - Kali

Lesson 01: Getting Started with Kali Linux

- What Is Linux?

Lesson 02: Accessing the Command Line

- Access the Command Line
- Access the Command Line with the Desktop
- Execute Commands with the Bash Shell
- Lab: Access the Command Line

Lesson 03: Managing Files from the Command Line

- Describe Linux file system Hierarchy Concepts
- Specify Files by Name
- Manage Files with Command-line Tools
- Make Links Between Files
- Match File Names with Shell Expansions
- Lab: Manage Files from the Command Line

Lesson 04: Getting Help in Kali Linux

- Lab: Get Help in Kali Linux

Lesson 05: Creating, Viewing & Editing Test Files

- Redirect Output to a File or Program
- Edit Text Files from the Shell Prompt
- Change the Shell Environment
- Lab: Create, View, and Edit Text Files

Lesson 06: Managing Local Users and Groups

- Describe User and Group Concepts
- Gain Superuser Access
- Manage Local User Accounts
- Manage Local Group Accounts
- Manage User Passwords
- Lab: Manage Local Users and Groups

Lesson 07: Controlling Access to Files

- Interpret Linux File System Permissions
- Manage File System Permissions from the Command Line
- Manage Default Permissions and File Access
- Lab: Control Access to Files

Lesson 08: Monitoring and Managing Linux Process

- Process States and Lifecycle
- Control Jobs
- Kill Processes
- Monitor Process Activity
- Lab: Monitor and Manage Linux Processes

Lesson 09: Controlling Services and Daemons

- Identify Automatically Started System Processes
- Control System Services
- Lab: Control Services and Daemons

Lesson 10: Configuring and Securing SSH

- Access the Remote Command Line with Secure Shell (SSH)
- Configure Secure Shell (SSH) Key-based Authentication
- Customize Open Secure Shell (SSH) Service Configuration
- Lab: Configure and Secure Shell (SSH)

Lesson 11: Installing and Updating Software Packages

- Install and Update Software Packages
- Register Systems for Kali Support
- Explain and Investigate RPM Software Packages
- Install and Update Software Packages with Differential Network Flow (DNF)
- Enable Differential Network Flow (DNF) Software Repositories
- Lab: Install and Update Software Packages

Lesson 12: Accessing Linux File System

- Identify File Systems and Devices
- Mount and Unmount File Systems
- Locate Files on the System
- Lab: Access Linux File Systems

Module 3 : Ethical Hacking

Lesson 01: Introduction to Basics of Ethical Hacking

- Intro To Ethical Hacking
- Types of Attacks
- Hacking Methodology
- Cyber Kill Chain
- Types of Attackers
- Confidentiality, Integrity, and Availability (CIA) Traid
- Risk Management
- Cyber Laws

Lesson 02: Foot-printing Active (Tool-Based Practical)

- What is Active Footprinting
- Different kinds of information gathered in Footprinting
- Tools for Active Footprinting = nmap, hping, Masscan

Lesson 03: Foot-printing Passive (Passive Approach)

- What is passive footprinting
- Footprinting Through Whois
- Footprinting Through Website / Web services
- Footprinting Through search engine
- Footprinting Through DNS
- Footprinting Through Email
- Footprinting Through Network
- Footprinting Through Social Media
- Tools for Passive Footprinting – Google dorks, shodan, netcraft

Lesson 04: In-depth Network Scanning

- Overview of Network Scanning
- Scanning Methodology
- Host Discovery
- Port Scanning Techniques
- Scanning tools – nmap, netdiscover, arp-scan -1

Lesson 05: Enumeration User Identification

- Enumeration Concepts
- Network Basic Input Output System (NetBIOS) Enumeration
- Simple Network Management Protocol (SNMP) Enumeration
- Lightweight Directory Access Protocol (LDAP) Enumeration
- Simple Mail Transport Protocol (SMTP) Enumeration
- Domain Name System (DNS) Enumeration

Lesson 06: System Hacking Password Cracking & Bypassing

- Authentication
- Gaining Access
- Password cracking
- Password Cracking Techniques
- Steganography

Lesson 07: Web Session Hijacking

- Session Hijacking Concepts
- Session Hijacking Techniques
- Session Hijacking Tools

Lesson 08: Hacking Wireless Networks Manual CLI Based

- Wireless Network Basics
- Manual Hacking Techniques for Wi-Fi Networks
- Command Line Tools for Wireless Hacking
- Automated Wireless Hacking Tools
- Wireless Network Exploitation Methods
- Wireless Security Best Practices

Lesson 09: Honey pots

- Introduction on Honeypots
- Types Of Honeypots
- Install Of Honeypot (KF Sensor)

Lesson 10: Buffer Overflow

- Introduction to Buffer Overflow

Lesson 11: Cryptography

- What is cryptography, encryption, decryption
- Types of cipher – substitution (Caesar) and Transposition (rail fence) techniques
- Keys in cryptography – asymmetric and symmetric
- What is encoding
- Example of encoding
- What is hashing
- Example of hashes of a string

Module 4 : Viruses, Trojans, Malwares, and OS Level Attacks and Counter Measures

Lesson 01: Malware

- Introduction to Malware
- Types of Viruses
- Types of Worms
- Types of Trojans
- Components Of a Trojan
- Introduction to Botnets
- Characteristics of Botnets
- Practical of Androrat

Lesson 02: Sniffers MITM with Kali

- Introduction to Ettercap and Bettercap
- Practical on Ettercap
- Practical on Bettercap
- Introduction to Wireshark
- Practical on Wireshark

Lesson 03: Social Engineering Techniques Theoretical Approach

- Types of Social Engineering Attacks
- Human Based Social Engineering Attacks
- Computer Based Social Engineering Attacks
- Mobile Based Social Engineering Attacks

Lesson 4: Social Engineering Toolkit Practical Based Approach

- Practical on zphisher
- Practical on Social Engineering Toolkit (SET)

Lesson 5: Denial of Service (DOS) & Distributed Denial-of-Service (DDOS) Attacks

- Denial of Service (DOS) / Distributed Denial-of-Service (DDOS) Concepts
- Denial of Service (DOS) / Distributed Denial-of-Service (DDOS) Attack Techniques
- Denial of Service (DOS) / Distributed Denial-of-Service (DDOS) Tools
- Denial of Service (DOS) / Distributed Denial-of-Service

Module 5 : Web Application Security

Lesson 01: Introduction

- Networking and protocols
- Hypertext Transfer Protocol (HTTP) & Hypertext Transfer Protocol Secure (HTTPS)

Lesson 02: OWASP Top 10

- Briefing about various frameworks
- Explaining the OWASP top 10

Lesson 03: Recon for bug hunting

- Subdomains enumeration
- Domains filtration
- Endpoints enumeration
- Grepping responses

Lesson 04: Advanced SQL Injection

- Union based SQLI
- SQL Authentication Bypass
- Error based SQLI
- Time-based SQLI
- In-band and out-of-band SQLI
- Create our own script to automate the process of Blind SQLi

Lesson 05: Command injection

- DVWA source code review
- PHP command injection with various functions
- Filter bypass

Lesson 06: Session Management and Broken Authentication Vulnerability

- Cookie hijacking
- HSTS policy bypass

Lesson 07: Cross-Site Request Forgery (CSRF)

- protection bypass

Lesson 08: Server Site Request Forgery (SSRF)

- Filter bypass
- Server-side configuration check

Lesson 09: Cross-Site Scripting (XSS)

- Explaining JavaScript
- Reflected JavaScript
- Stored JavaScript
- DOM-based JavaScript

Lesson 10: Insecure Direct Object Reference (IDOR)

- Universally Unique Identifier(UUID) protection

Lesson 11: Sensitive Data Exposure and Information Disclose

- GIT source code disclosure
- Client-side source code review

Lesson 12: Server Site Template Injection (SSTI)

- Template engine Explaining
- Various exploitation techniques with various Template engine

Lesson 13:Multi-Factor Authentication Bypass

- Brute-force attacks
- Creating wordlists
- Logic errors bypass

Lesson 14: HTTP Request Smuggling

- Explaining HTTP/1.1 and HTTP/2
- CL-TE attack
- TE-CL attack
- TE-TE attack

Lesson 15: External Control of File Name or Path

- Whitelisting and blacklisting
- Bypassing blacklisting
- Brief on regex

Lesson 16: Local File Inclusion (LFI) and Remote File Inclusion (RFI)

- Traversal payload
- Bypass WAF
- Reading and inclusion difference

Lesson 17: Directory Path Traversal

- Path traversal payload to read the file

Lesson 18: HTML Injection

- Explaining HTML web page
- Reflected HTML injection
- Stored HTML injection

Lesson 19: Host Header Injection

- Apache Config Brief
- Host header Explaining

Lesson 20: File Upload Vulnerability

- POST method explain
- Encoded POST method
- Various headers related to file upload

Module 6 : Mobile Application Security

Lesson 01: Introduction to Mobile Penetration Testing

- Scope
- Methodology
- Tools

Lesson 02: Lab Setup

- Kali lab setup
- Burp suite setup
- Mobile penetration testing lab setup

Lesson 03: Android Architecture

- Layers of Android architecture
- Key Components
- Application lifecycle
- Security Model

Lesson 04: Apl File structure

- Core components
- Common file structure patterns
- File structure example

Lesson 05: Reversing App with Apktool

- Overviews
- Functionality
- Installation
- Usage
- Common usage case

Lesson 06: Reversing App with MobSf

- Overviews
- Functionality
- Installation and setup
- Feature and Capabilities
- Scan the app with mobsf

Lesson 07: Static Analysis

- Types of static analysis
- Tools and techniques
- Benefits
- How to perform static analysis

Lesson 08: Scanning Vulnerability with Drozer

- Overviews
- Dynamic analysis
- Injection attacks
- Exploitation

Lesson 09: Improper Platform Usage

- Definition
- attacks
- Impact
- Mitigation
- Tools and resources

Lesson 10: Insecure Data Storage

- Definition
- Storing passwords in plain text
- Unprotected databases
- Impact
- Mitigation
- Tools and resources

Lesson 11: Insecure Communication

- Definition
- Unencrypted protocols
- Missing or misconfigured SSL/TLS
- Impact
- Mitigation
- Tools and resources

Lesson 12: Insecure Authentication

- Definition
- Weak password policies
- Lack of multi-factor authentication
- Impact
- Mitigation
- Tools and resources

Lesson 13: Insufficient Cryptography

- Common vulnerability
- Impact
- Prevention and Mitigation
- Continuous monitoring and updates

Lesson 14: Insecure Authorization

- Common vulnerability
- Impact
- Prevention and Mitigation

Lesson 15: Client Code Quality
- Important of client code quality
- Code structure and Organization
- Readability and Maintainability

Lesson 16: Code Tampering
- Objective
- Techniques
- Detection and Prevention
- Implications

Lesson 17: Reverse Engineering
- Purpose
- Techniques
- Tools
- Reversing Malware

Lesson 18: Extraneous Functionality
- Security risks
- User Experience (UX) issues
- Code review and refactoring
- Automated Analysis tools

Lesson19: SSLPinning
- Publickey Pinning
- Certificate Pinning
- Benefits of SSL pinning
- Certificate Authority (CA)

Lesson 20: Intercepting the Network Traffic
- Packet Capture
- Network sniffing
- Protocol Analysis
- Traffic Decryption

Lesson 21: Dynamic Analysis
- Introduction to Dynamic Analysis
- How to perform dynamic analysis
- Dynamic Debugging
- Dynamic Decomplication

Lesson 22: Report Preparation
- Consider the objective of the report
- The test compiles a comprehensive report
- Detailing their findings of vulnerability

Lesson 23: IOS Penetration: Basics

- Introduction to IOS Penetration testing
- IOS structure
- How to secure you application

Lesson 24: Report Writing

- Proof of Concept (POC)
- Executive and Management Report
- Technical Report For IT and security Department

Module 7 : Advance Penetration Testing & Network VAPT

Lesson 01: Introduction to Penetration Testing
- What is Advanced Penetration Testing (APT)
- Types of Penetration Testing & Areas
- Demo Report Understanding

Lesson 02: In-Depth Scanning
- Lesson 01 : Scan All Top 20 Ports

Lesson 03: Exploitation
- Basics of Exploitations

Lesson 04: Command Line Fun
- Basic of LinuxCommands
- Permission Commands

Lesson 05: Getting Comfortable with Kali Linux
- Introduction to Kali Linux

Lesson 06: Bash Scripting
- Introduction to Bash Scripting
- Bash Scripting Fundamentals
- Tool Creation - Password Generator
- Functions

Lesson 07: Practical Tools
- Essential Tools

Lesson 08: Active Information Gathering
- Domain Name System (DNS) Enumerations
- Automating Lookups
- Domain Name System (DNS) Zone Transfers
- NMAP and Masscan
- Port Enumeration

Lesson 09: Passive Information Gathering
- Website Recon
- Netcraft, Shodan, Email Harvesting
- Open Source Intelligence (OSINT) Framework

Lesson 10: Locating Public Exploits
- Find Exploits on Google Hacking Database
- Find Exploits on GitHub

Lesson 11: Antivirus Evasion

- Introduction to Antivirus Evasion
- Working of Antivirus Evasion
- Obfuscation Techniques

Lesson 12: File Transfers

- File Transfers Using FTP, Telnet, SSH, PHP, Python

Lesson 13: Windows Privilege Escalation

- Service Exploits - Insecure Service Permissions
- Service Exploits - Unquoted Service Path
- Service Exploits - Weak Registry Permissions
- Service Exploits - Insecure Service Executables
- Registry – Auto Runs, etc.

Lesson 14: Linux Privilege Escalation

- Service Exploits
- Weak File Permissions - Readable /etc/shadow
- Weak File Permissions - Writable /etc/shadow
- Weak File Permissions - Writable /etc/passwd
- Sudo - Shell Escape Sequences, etc.

Lesson 15: Password Attacks

- Password Spraying and Dictionary Attack

Lesson 16: Port Redirection and Tunneling

- Port Redirection and Tunneling Using Chisel

Lesson 17: Active Directory Attacks

- Introduction of Active Directory (AD)
- Basics of Active Directory (AD)
- Enumeration of Active Directory (AD)

Lesson 18: Power Shell Empire

- Introduction of Empire
- Getting Shell Using Empire

07 Modules

07 Month Duration

Language : Hindi /English

Mon to Fri 8 PM to 9 PM

ABOUT US

We offer Cyber Security and Information Security training and Certification for Cyber Security and Information Technology aspirants. Since decade, we have been in the Information Technology and Cyber Security Industry. You can learn more about cybersecurity, Techniques, and Tools to choose a better career path. **GS2 Cyber Security** also provide a vast range of VAPT Services, SOC Services and other Cyber Security Services.

GS2 CYBER SECURITY is one of the most trusted and reliable training providers in cyber security, providing exceptional unmatched Hands-on practical training to individuals and corporate worldwide.

We have a large number of professional instructors who are specialized and experienced in various Information/Cyber Security domains. Our Instructors holds a wide range of accreditation like OSCP, OSWE, eWPTX, CEH, CISSP, CISA.

We emphasize more on hands-on practical training which gives our clientsand candidate an edge to grow and advance professionally in theirrespective career(s).

Contact Details :

GS2 CYBER SECURITY

info@gs2cybersec.com

Block B1/632, 2nd Floor,
Janakpuri, Delhi-110058,
India

SCAN ME

/gs2cybersec /gs2cyber **7307970448** www.gs2cybersec.com