Ethical Hacking

Introduction

This Ethical Hacking Certificate is the desired information security training programme that any information security expert will ever want to be in. You must become a hacker, but an ethical one, in order to master hacking technologies. It offers cutting-edge hacking tools and methods that information security experts and hackers alike utilize to breach a business. It is a known fact that to fight a hacker, you need to think like a hacker. To fight against such attacks, this certification will completely immerse you in the hacker mindset. Any organization's security mindset must extend beyond the silos of a specific vendor, technology, or piece of machinery. You will be thought the five phases of ethical hacking and thought how you can approach including Reconnaissance, Gaining Access, Enumeration, Maintaining Access, and covering your tracks.

REQUIREMENTS:

- Learners must have the Basic IT knowledge
- Should be able to read English
- Minimum education required: Intermediate with experience | Graduate Preferable

CURRICULUM:

Sr. No.	Contents

1	**Basic Security Concepts**
	• Security Fundamentals
	  ◦ Security goals: confidentiality, integrity, availability
	  ◦ Risk assessment and management
	  ◦ Security controls: preventive, detective, corrective
	• Security Principles and Models
	  ◦ Bell-LaPadula model
	  ◦ Biba integrity model
	  ◦ Clark-Wilson integrity model
	• Security Policies and Procedures
	  ◦ Access control policies
	  ◦ Acceptable use policies
	  ◦ Change management procedures
	• Security Awareness and Training
	  ◦ Employee training programs
	  ◦ Security awareness campaigns
	  ◦ Social engineering awareness

Sr. No.	Contents

2	**Information Security Terminology**
	
	• Authentication Mechanisms
	  ◦ Passwords, biometrics, multi-factor authentication
	  ◦ Single Sign-On (SSO) concepts
	• Authorization Concepts
	  ◦ Role-based access control (RBAC)
	  ◦ Attribute-based access control (ABAC)
	• Cryptography Basics
	  ◦ Symmetric and asymmetric encryption
	  ◦ Digital signatures and certificates
	• Network Security Concepts
	  ◦ Firewalls, IDS/IPS, VPNs
	  ◦ Security appliances: proxies, gateways
	• Incident Response Terminology
	  ◦ Incident identification, containment, eradication, recovery

3	**Malware Classifications**
	
	• Authentication Mechanisms
	  ◦ File and boot sector viruses
	  ◦ Polymorphic and metamorphic viruses
	• Worm Propagation Techniques
	  ◦ Network and email-based spreading
	  ◦ Self-replicating mechanisms
	• Trojan Horse Functionalities
	  ◦ Information theft, backdoor access
	  ◦ Remote control and surveillance
	• Ransomware Encryption Mechanisms
	  ◦ Cryptographic algorithms used
	  ◦ Bitcoin and cryptocurrency payments
	• Spyware and Adware Behaviors
	  ◦ Information gathering, user tracking
	• Rootkit Installation and Concealment
	  ◦ Kernel-level rootkits
	  ◦ User-mode rootkits

Sr. No.	Contents

4	**Types of Malware**
	• Detailed Analysis
	  ◦ Anatomy of a virus: infection, payload, spread
	  ◦ Behavioral patterns of worms and trojans
	  ◦ Ransomware attack scenarios
	  ◦ Spyware and adware detection techniques
	  ◦ Rootkit detection and removal tools

5	**Server-Side Web Application Attacks**
	• Cross-Site Scripting (XSS) Variations
	  ◦ Stored XSS, reflected XSS, DOM-based XSS
	  ◦ Impact on web applications
	• SQL Injection Techniques and Defenses
	  ◦ Union-based, time-based, error-based
	  ◦ Parameterized queries and prepared statements
	• Cross-Site Request Forgery (CSRF) Prevention Measures
	  ◦ Anti-CSRF tokens
	  ◦ SameSite cookie attribute

6	**Planning and Policy**
	• Developing Security Policies
	  ◦ Policy creation and documentation
	  ◦ Security policy enforcement
	• Incident Response Planning and Execution
	  ◦ Incident detection and reporting
	  ◦ Forensic analysis and reporting
	• Business Continuity and Disaster Recovery Planning
	  ◦ Business impact analysis (BIA)
	  ◦ Continuity of operations planning (COOP)
	• Legal and Regulatory Compliance
	  ◦ GDPR, HIPAA, PCI DSS
	  ◦ Compliance auditing and reporting

Sr. No.	Contents

7	**Network Protocols and Service Models**
	• In-Depth Understanding of TCP/IP and OSI Layers
	  ◦ Packet structure and encapsulation
	  ◦ TCP handshake process
	• Specific Protocols
	  ◦ HTTP/HTTPS request-response cycle
	  ◦ DNS query and resolution process
	  ◦ SMTP email communication
	• Network Services
	  ◦ DHCP for IP address assignment
	  ◦ NAT for private network addressing

8	**Transport Layer Security**
	• SSL/TLS Protocols and Versions
	  ◦ Handshake protocols: SSL, TLS
	  ◦ TLS 1.2 and TLS 1.3 improvements
	• Public-Key and Symmetric-Key Cryptography
	  ◦ Certificate authorities and digital certificates
	  ◦ Key exchange mechanisms
	• Certificate Authorities and Digital Certificates
	  ◦ Certificate lifecycle
	  ◦ Certificate Revocation Lists (CRLs)

9	**Network Layer Security**
	• IPsec Protocols
	  ◦ Authentication Header (AH) and Encapsulating Security Payload (ESP)
	  ◦ Tunnel mode and transport mode
	• VPN Types and Implementations
	  ◦ Site-to-site VPNs
	  ◦ Remote access VPNs

Sr. No.	Contents

10	**Wireless Security**
	• Evolution of Wireless Security Standards
	  ◦ WEP to WPA3 advancements
	  ◦ Wi-Fi Alliance certifications
	• Wireless Encryption Protocols
	  ◦ WEP vulnerabilities and weaknesses
	  ◦ WPA2 and WPA3 improvements
	• Wireless Security Best Practices
	  ◦ Strong passphrase selection
	  ◦ Regular firmware updates

11	**Cloud & IoT Security**
	• Cloud Deployment Models
	  ◦ Public, private, hybrid cloud
	  ◦ Community cloud considerations
	• Wireless Encryption Protocols
	  ◦ Infrastructure as a Service (IaaS)
	  ◦ Platform as a Service (PaaS)
	  ◦ Software as a Service (SaaS)
	• Wireless Security Best Practices
	  ◦ Device authentication and authorization
	  ◦ Data encryption in transit and at rest

Outcomes:

- Prevent malicious hacking attempts
- Analyzing and exploiting vulnerabilities on a website
- Scanning Networks with Nmap
- Identify legal and ethical issues related to vulnerability and penetration testing

BENEFITS:

- Understanding of advanced hacking skills
- Become a cyber security professional
- Master Information gathering and footprinting

Affiliation & Collaboarations

PBTE PSDA