ELYSIUM ACADEMY®
Milestone of Cognizance

Since 2007

VERSION 2.0

PROFESSIONAL

CERTIFIED HACKING DEFENDER

ELYSIUM ACADEMY

CERTIFIED HACKING DEFENDER

SR. CODE

EAPL/PROF/PRTC19

COURSE CODE

EAPHD

SUB CATEGORY

CYBER SECURITY AND NETWORKING

TOTAL DURATION	THEORY TAKEN	PRACTICAL TAKEN
90 HOURS	18 HOURS	72 HOURS

ELYSIUM ACADEMY CERTIFIED HACKING DEFENDER

COURSE DESCRIPTION

Their programmes are created to offer thorough ethical hacking and penetration testing training and cover a range of subjects. One of the most well-liked courses is ethical hacking, which is a result of people's growing interest in internet security and techniques for protecting their personal security. In general, there are three key themes covered in ethical hacking courses.

COURSE GOALS

Find weaknesses and vulnerabilities in security through penetration testing.
Find areas where sensitive data could be compromised in a cyber attack.
Attempt to exploit vulnerabilities as a malicious hacker would.
Give recommendations for protection.

FUTURE SCOPE

Paladion Networks, Tata Consultancy Services Limited, InfoSys Limited, Wipro Technologies Ltd. and others are the best recruiters for the ethical hacker. These top recruiters either hire candidates from institutions with good salary packages to recruit a qualified ethical hacker to their company. Below are some organizations in India that hire ethical hackers

ELYSIUM ACADEMY®
Milestone of Cognizance

Since 2007

01
CHAPTER

BASIC OF COMPUTER AND NETWORKING HARDWARE

07 HRS 00 MINS

04 HRS 00 MINS

01.Computer Hardware

a.Mother Board
b.Ram
c. Storage
d.Mobile Equipment
e. Laptop
f. Processor

02. Network Devices

a.Routers
b.Switches
c. Access Points
d.Firewall
e. Hub
f. Power over Ethernet(PoE)
g.Injectors
h.Cable Modem
i. Network Interface Card
j. Protocols for Router and Switch
k.Logical Ports

03. Hacking:

a.What is Hacking
b.Types of Hackers
c. Who is called Hackers
d.Life Cycle of Hacking

ELYSIUM ACADEMY®
Milestone of Cognizance

Since 2007

02 CHAPTER

GETTING STARTED

04 HRS 00 MINS

06 HRS 00 MINS

01. About Ethical Hacking

a. What is Ethical Hacking?
b. What is Ethics?
c. Engagements and Reports
d. Terminology crash
e. Confidentiality
f. Integrity
g. Availability
h. Legal considerations

02. Ethics and Legality

a. Define the job role of an ethical hacker
b. Understand ethical hacking terminology
c. Understand the different phases involved in ethical hacking
d. Identify different types of hacking technologies
e. List the 5 stages of ethical hacking
f. What is hacktivism?
g. List different types of hacker classes
h. Define the skills required to become an Ethical hacker
i. What is vulnerability research?
j. Describe the ways of conducting ethical hacking
k. Understand the legal implications of hacking

03. Review of Everything

a. Number systems
b. Networking

c. TCP/IP
d. Subnetting
e. Domain Name
f. Dp Address
g. Employee Information
h. Emails

04. Footprint

a. What is footprint?
b. Purpose of footprints
c. Types of footprints

03 CHAPTER

FINGERPRINT, SCANNING

4.5 HRS
8.5 HRS

01. Reconnaissance

a. What is Reconnaissance?
b. Reconnaissance methodology
c. Information Gathered Through Foot printing
d. Surveying the attack surface
e. Recon types and goals
f. Passive recon pt. 1
g. Passive recon pt. 2
h. Active recon
i. Recon walk-through and tools summary Gather initial information
j. Determine the network range

k. Identify active machines
l. Discover open ports and access points
m. Fingerprint the operating system
n. Uncover services on ports
o. Map the network

02. Ethical Fingerprint

a. What is Fingerprint in ethical?
b. Purpose of fingerprint
c. Types of fingerprints
d. TTL
e. Window Size
f. DF
g. TOS

03. Scanning Networks

a. What is scanning networks?
b. Purpose of scanning networks
c. Types of scanning in ethical hacking
d. Scanning Methodology
e. Ping Sweep Techniques
f. nmap Command Switches
g. Syn, Stealth, Xmas, Null, IDLE & FIN Scans
h. Proxy Servers & Attack
i. HTTP Tunneling Techniques
j. DP Spoofing Techniques
k. List the Scanning Tools

04. Enumeration

a. What is Enumeration in ethical hacking?
b. Purpose of Enumeration in ethical hacking
c. DNS enumeration
d. NTP enumeration
e. SNMP enumeration
f. Linux/Windows enumeration
g. SMB enumeration

04
CHAPTER

HACKING, DOS

05 HRS 00 MINS

08 HRS 00 MINS

01. System Hacking

a. Understanding password cracking techniques.
b. Understanding different types of passwords.
c. Identify various password cracking tools.
d. Understand escalating privileges.
e. Understanding keyloggers and other spyware technologies.
f. Understand how to hide files.
g. Understand rootkits.
h. Understand steganography technologies.
i. Understand how to cover your tracks and erase evidence.

O2. Trojans and Backdoors

a. What is a Trojan?
b. What is meant by overt and covert channels?
c. List the different types of Trojans
d. What are the indications of a Trojan attack?
e. Understand how "Netcat" Trojan works
f. What is meant by "wrapping"?
g. How do reverse connecting Trojans work?
h. What are the countermeasure techniques in preventing Trojans?
i. Understand Trojan evading techniques

O3. Sniffing

a. Understand the protocol susceptible to sniffing
b. Understand active and passive sniffing
c. Understand ARP poisoning
d. Understand Ethereal capture and display filters
e. Understand MAC flooding
f. Understand DNS spoofing techniques
g. Describe sniffing countermeasures

O4. Denial of Service

a. Understand the types of DoS Attacks
b. Understand how DDoS attack works
c. Understand how BOTs/BOTNETs work
d. What is a "Smurf" attack?
e. What is "SYN" flooding?
f. Describe the DoS/DDoS countermeasures

ELYSIUM ACADEMY®
Milestone of Cognizance

Since 2007

05

CHAPTER

WEB APPLICATION VULNERABILITIES

05 HRS 00 MINS

08 HRS 00 MINS

01. Social Engineering

a. What is social engineering?
b. What are the common types of attacks?
c. Understand dumpster diving
d. Understand reverse social engineering
e. Understand insider attacks
f. Understand identity theft
g. Describe phishing attacks
h. Understand online scams
i. Understand URL obfuscation
j. Social engineering countermeasures

02. Session Hijacking

a. Understand spoofing vs. hijacking
b. List the types of session hijacking
c. Understand sequence prediction
d. What are the steps in performing session hijacking?
e. Describe how you would prevent session hijacking

03. Hacking Web Servers

a. List the types of web server vulnerabilities
b. Understand the attacks against web servers
c. Understand IIS Unicode exploits
d. Understand patch management techniques
e. Understand Web Application Scanner
f. What is the Metasploit Framework?
g. Describe web server hardening methods

04. Web Application Vulnerabilities

a. Understanding how a web application works
b. Objectives of web application hacking
c. Anatomy of an attack
d. Web application threats
e. Understand Google hacking
f. Understand web application countermeasures

06 CHAPTER

WIRELESS HACKING

06 HRS 00 MINS

07 HRS 00 MINS

01. Web-Based Password Cracking Techniques

a. List the authentication types
b. What is a password cracker?
c. How does a password cracker work?
d. Password attacks – classification
e. Password cracking counter measures

02. SQL Injection

a. What is SQL injection?
b. Understand the steps to conduct SQL injection
c. Understand SQL Server vulnerabilities
d. Describe SQL injection countermeasures

03. Wireless Hacking

a. Overview of WEP, WPA authentication systems and cracking techniques

b. Overview of wireless sniffers and SSID, MAC spoofing
c. Understand rogue access points
d. Understand wireless hacking techniques
e. Describe the methods of securing wireless networks

04. Virus and Worms

a. Understand the difference between a virus and a worm
b. Understand the types of viruses
c. How a virus spreads and infects the system
d. Understand antivirus evasion techniques
e. Understand virus detection methods

07 CHAPTER

LINUX HACKING

04 HRS 00 MINS

08 HRS 00 MINS

01. Physical Security

a. Physical security breach incidents
b. Understanding physical security
c. What is the need for physical security?
d. Who is accountable for physical security?
e. Factors affecting physical security

02. Linux Hacking

a. Understand how to compile a Linux kernel
b. Understand GCC compilation commands
c. Understand how to install LKM modules
d. Understand Linux hardening methods

03. Evading IDS, Honeypots, & Firewalls

a. List the types of intrusion detection systems

b. Evasion techniques
c. List firewall and honeypot evasion techniques

04. Buffer Overflows

a. Overview of stack-based buffer overflows
b. Identify the different types of buffer overflows
c. Methods of detection
d. Overview of buffer overflow mutation techniques

08 CHAPTER

CRYPTOGRAPHY

02 HRS 00 MINS

01. Cryptography

a. Overview of cryptography
b. Encryption techniques
c. Describe how public and private keys are generated
d. Overview of MD5, SHA, RC4, RC5, Blowfish algorithms

03 HRS 00 MINS

02. Penetration Testing Methodologies

a. Overview of penetration testing methodologies
b. List the penetration testing steps
c. Overview of the pen-test legal framework
d. Overview of the pen-test deliverables
e. List the automated penetration testing tools

03. Cloud Computing

a. What is Cloud Computing in ethical hacking?
b. Types of cloud computing
c. Methodologies in ethical hacking
d. Role of Ethical Hackers in the Cloud Computing Industry

04. Covering tracks

a. What is covering tracks?

b. Deleting logs

c. Modifying log files

d. Hiding malware or backdoors

ELYSIUM ACADEMY®
Milestone of Cognizance

Since 2007

Placement Assistance 100%

135+ Professional Courses

Practical Sessions 90%

67+ Global Pacts

Corporate Placements 65%

170+ IT Companies Tie-Up

ELYSIUM GROUP OF COMPANIES

ELYSIUM ACADEMY PRIVATE LIMITED

Authorized International Partners

Microsoft · CompTIA · Cisco · aws · Google · SUSE · Rocheston · C++