ETHICAL HACKING AND CYBER SECURITY

This course is meant for those who are looking for comprehensive and total knowledge in the security domain. This is the only course which teaches both hacking and prevention techniques. And in keeping with industrial standards, this course is entirely hand's on and real time oriented. And need we say, the instructor is infosec enthusiast, Ethical Hacker, and Web Developer. He has helped few organizations in improving their website security by penetration testing. And gave trainings in several universities, colleges, companies and trained 2,000+ students nationally and internationally.

KARTHEEK CHANDA

Certified Ethical Hacker

Brief Table Of Content

(including networking, system basics and OWASP TOP 10)

14· SQL Injection

15· Hacking Wireless Networks

16· Evading IDS, Firewalls and Honey pots

17· Hacking Mobile Application Platforms

18. IoT Hacking

19· Cloud Computing

20· Cryptography

OWASP TOP 10 :-

1. Injection
2. Broken Authentication
3. Sensitive data exposure
4. XML External Entities (XXE)
5. Broken Access control
6. Security misconfigurations
7. Cross Site Scripting (XSS)
8. Insecure Deserialization
9. Using Components with known vulnerabilities
10. Insufficient logging and monitoring

Table Of Content

Who are at the risk of Hacking attacks
Effects of Computer Hacking on an organization
The Security, Functionality & Usability Triangle
What is Ethical Hacking
Why Ethical Hacking is Necessary
Scope & Limitations of Ethical Hacking

5.Foot printing and Reconnaissance

What is Foot Printing
Objectives of Foot Printing
Finding a company's details
Finding a company's domain name
Finding a company's Internal URLs
Finding a company's Server details
Finding the details of domain registration
Finding the range of IP Address
Finding the DNS information
Finding the location of servers
Traceroute analysis
Tracking e-mail communications

6.Scanning

What is network scanning
Objectives of network scanning

Finding the default passwords of network devices and softwares
Password cracking methods o Online password cracking
Man-in-the-middle attack
Password guessing o Offline password cracking
Brute force cracking
Dictionary based cracking
USB password stealers
Elcomsoft Distributed password recovery tools
Active password changer
What is a keylogger
How to deploy a keylogger to a remote pc
How to defend against a keylogger

16.Mobile Hacking

What is mobile Hacking
Goals of mobile Hacking
Countermeasures

17.Sniffers

What is a sniffer
How sniffer works
Types of sniffing
Active sniffing
Passive Sniffing

Finding the live hosts in a network
SNMP Enumeration
SMTP Enumeration
DNS Enumeration
Finding open ports on a server
Finding the services on a server
OS fingerprinting
Server Banner grabbing tools
What is a Vulnerability Scanning
What is a proxy server
How does proxy server work
Why do hackers use proxy servers
What is a TOR network
Why hackers prefer to use TOR networks

7.Hacking Web Servers & Web Applications

What is a web server
Different webserver applications in use
Why are webservers hacked & its consequences
Directory traversal attacks
Website defacement
Website password brute forcing

8.Cross site scripting

What is ARP
ARP poison attack
Threats of ARP poison attack
How MAC spoofing works
MAC Flooding
How to defend against MAC Spoofing attacks
How to defend against Sniffers in network

18.Wireless Hacking

Types of wireless networks
Finding a Wi-Fi network
Types of Wi-Fi authentications
Using a centralized authentication server
Using local authentication
Types of Wi-Fi encryption methods
1.WEP
2.WPA
3.WPA2
How does WEP work
Weakness of WEP encryption
How does WPA work
How does WPA2 work
Hardware and software required to crack Wi-Fi networks
How to crack WEP encryption
How to crack WPA encryption
How to crack WPA2 encryption

Persistent XSS, where the malicious input originates from the website's database.
Reflected XSS, where the malicious input originates from the victim's request.
DOM-based XSS, where the vulnerability is in the client-side code rather than the server-side code.

9.SQL Injection

What is SQL Injection
Effects of SQL Injection attacks
Types of SQL Injection attacks
SQL Injection detection tools

10.Session Hijacking

What is session hijacking
Dangers of session hijacking attacks
Session hijacking techniques
How to defend against session hijacking

11.Denial of Service

What is a DoS attack
What is a DDoS attack
Symptoms of a Dos attack
DoS attack techniques
What is a Botnet
How to defend against Wi-Fi cracking attack

19.Malware Threats

What is malware
Types of malware

Virus

What is a virus program
What are the properties of a virus program
How does a computer get infected by virus
Types of virus
Virus making tools
How to defend against virus attacks

Worm

What is a worm program
How worms are different from virus

Trojan

What is a Trojan horse
How does a Trojan operate
How to defend against Trojans

Spyware

What is a spyware
Types of spywares
How to defend against spyware

Rootkits

What is a Rootkit
Types of Rootkits
How does Rootkit operate

12.Social Engineering Phishing What is Phishing How Phishing website is hosted How victims are tricked to access Phishing websites How to differentiate a Phishing webpage from the original webpage How to defend against Phishing attacks Homograph attack	How to defend against Rootkits **20.OWASP TOP 10** Injection Broken Authentication Sensitive data exposure XML External Entities (XXE) Broken Access control Security misconfigurations Cross Site Scripting (XSS) Insecure Deserialization Using Components with known vulnerabilities Insufficient logging and monitoring

Job Profiles

1) Ethical Hacker
2) Penetration Tester
3) Information Security Analyst
4) Information Security Manager
5) Security Analyst
6) Security Consultant, (Computing / Networking / Information Technology)