CODEVIRUS SECURITY

PRESENTS

Diploma Courses Structure

In this Presentation

Here's what we'll cover:-

1. Certified Ethical Hacker
2. IOT Penetration
3. Android Penetration
4. Cloud Security
5. Penetration Testing Module
6. Web Penetration Testing
7. Python Programming
8. Networking

Certified Ethical Hacker

MODULES

- Module 01 Introduction to Ethical Hacking
- Module 02 Footprinting and Reconnaissance
- Module 03 Scanning Networks
- Module 04 Enumeration
- Module 05 Vulnerability Analysis
- Module 06 System Hacking
- Module 07 Malware Threats
- Module 08 Sniffing
- Module 09 Social Engineering
- Module 10 Denial-of-Service

MODULES

- Module 11 Session Hijacking
- Module 12 Evading IDS, Firewalls, and Honeypots
- Module 13 Hacking Web Servers
- Module 14 Hacking Web Applications
- Module 15 SQLInjection
- Module 16 Hacking Wireless Networks
- Module 17 Hacking Mobile Platforms
- Module 18 IoT and OTHacking
- Module 19 Cloud Computing
- Module 20 Cryptography

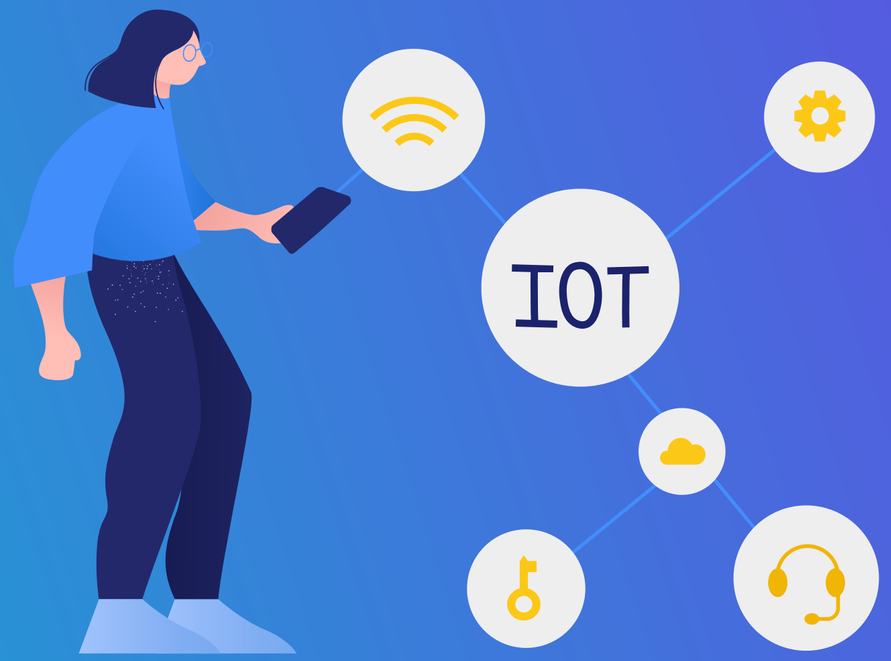
What Will You Learn?

- Key issues include plaguing the information security world, ethical hacking, information security controls,laws, and standards.
- Perform footprinting and reconnaissance using the latest footprinting techniques and tools as a critical pre attack phase required in ethical hacking.
- Network scanning techniques and scanning countermeasures.
- Enumeration techniques and enumeration countermeasures.
- Vulnerability analysis to identifysecurity loopholes in the target organization's network, communication infrastructure and end systems.

- Different types of malware(Trojan, Virus, worms, etc.) system auditing for malware attacks, malware analysis,and countermeasures.
- Packet sniffing techniques to discover network vulnerabilities and countermeasures to defend sniffing.
- Social engineering techniques and how to identify theft attacks to audit human-level vulnerabilities and suggest social engineering countermeasures.
- DoS/DDoS attack techniques and tools to audit a target and DoS/DDoS
- Session hijacking techniques to discover Network-level session management, authentication/authorization, cryptographic weaknesses and countermeasures.
- System hacking methodology, steganography, steganalysis attacks, and covering tracks to discover system and network vulnerabilities.

- Wireless encryption, wireless hacking methodology, wireless hacking tools,and Wi-Fi security tools.
- Mobile platform attack vector, android vulnerability exploitations, mobile security guidelines and tools.
- Firewall, IDS and honeypot evasion techniques, evasion tools and techniques to audit a network perimeter for weaknesses, and countermeasures.
- Cloud computing concepts(Container technology, serverless computing), various threats/attacks, and security techniques and tools.
- Penetration testing, security audit, vulnerability assessment, and penetration testing roadmap.
- Threats to IoT and OT platforms and learn how to defend IoT and OT devices securely.
- Cryptography ciphers, Public Key Infrastructure (PKI), cryptography attacks, and cryptanalysis tools.

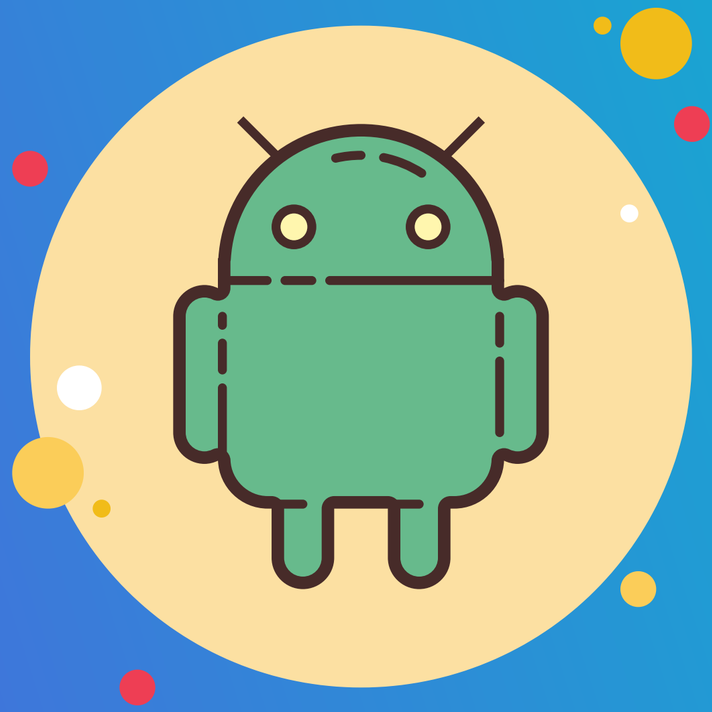
IoT Penetration



MODULES

- Analytic Engine for IoT
- Scope of the penetration testing engagement.
- What are your biggest fears regarding security of your solution.
- Your organization's current security posture.
- Overview of Why IoT is so important
- Machine learning for intelligent IoT
- Introduction to Mobile app platform & Middleware for IoT
- Expected time duration and financials.
- Explaining about our penetration testing methodology for your product.
- Conceiving a new IoT Product Requirement document for IoT.

Android Penetration



MODULES

- Android Architecture Fundamentals
- Android Application Architecture
- Decompiling Android Application
- Android Application File Structure
- Important Security Controls in Android
- Real Time Application Analysis Vulnerability Testing on Test Application
- Bug Hunting Approach on Live Applications
- Android Permission Structure

MODULES

- OWASP Top 10 2014
- OWASP Top 10 2016
- Analyze Application Traffic
- Static Analysis
- Dynamic Analysis
- Log Analysis
- Effective Bug Bounty Report Writin

Cloud Security

MODULES

- How to build AWS application infrastructures to protect against security threats.
- How to identify and mitigate threats for Apps and Data.
- AWS shared security responsibility model.
- How to protect data at rest.
- How to perform security assessment tests for making sure that simple vulnerabilities are resolved.
- Applying security checks to conduct an automated and reproducible infrastructure.
- Encryption technique.

Penetration Testing

MODULES

- Security Analysis and Penetration Testing Methodologies
- TCP IP Packet Analysis
- Pre-penetration Testing Steps
- Information Gathering Methodology
- Vulnerability Analysis
- External Network Penetration Testing Methodology
- Internal Network Penetration Testing Methodology
- Firewall Penetration Testing Methodology
- IDS Penetration Testing Methodology
- SQL Penetration Testing Methodology
- Database Penetration Testing Methodolog

Web Pentration Testing

MODULES

- Module 1 - Introduction
- Module 2 - Tools
- Module 3 - Packets
- Module 4 - HTTP Basics
- Module 5 - Why Sites Get Hacked
- Module 6 - Why Sites Get Hacked
- Module 7 - Why Sites Get Hacked
- Module 8 - Why Sites Get Hacked
- Module 9 - Why Sites Get Hacked
- Module 10 - Best Practices
- Module 11 - Best Practices
- Module 12 - Environment Setup

MODULES

- 2.1 What is SQL Injection
- 2.2 Spidering
- 2.3 Spidering
- 2.4 Spidering
- 2.5 Spidering
- 2.6 Discovering SQLI
- 2.7 Discovering SQLI
- 2.8 Discovering SQLI
- 2.9 Discovering SQLI
- 2.10 Discovering SQLI
- 2.11 Discovering SQLI
- 2.12 Exploiting SQLI
- 2.13 Exploiting SQLI
- 2.14 Exploiting SQLI
- 2.15 Exploiting SQLI
- 2.16 SQLI Lab

MODULES

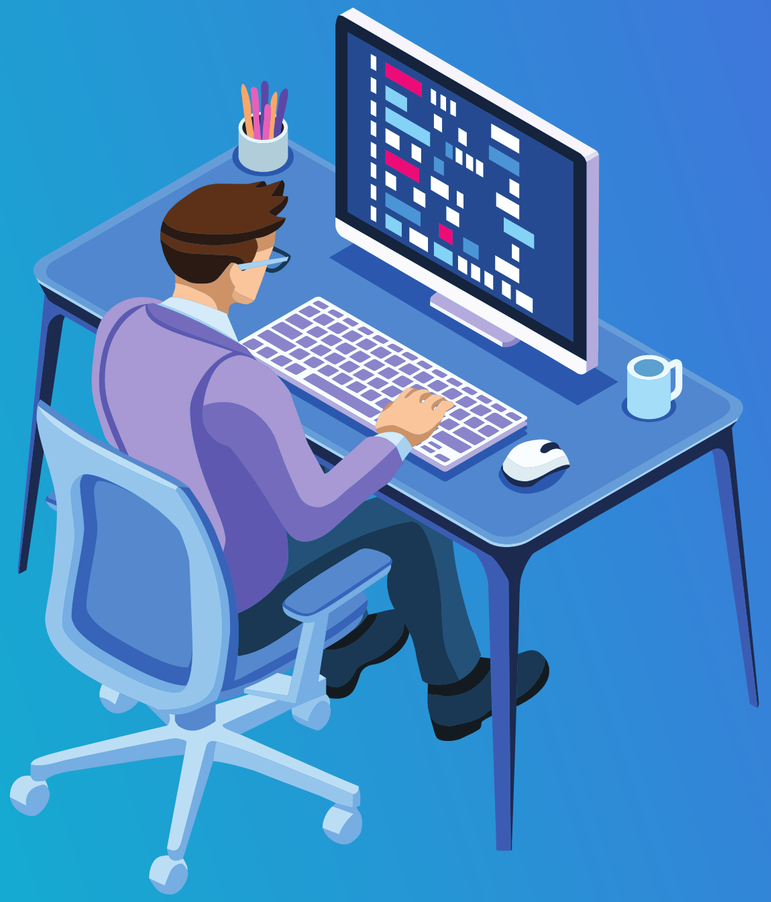
- 3.1 What is XSS
- 3.2 What is XSS
- 3.3 Discovering XSS
- 3.4 Discovering XSS
- 3.5 Discovering XSS
- 3.6 Discovering XSS
- 3.7 Discovering XSS
- 3.8 Discovering XSS
- 3.9 Exploiting XSS
- 3.10 Exploiting XSS
- 3.11 XSS Lab

MODULES

- 4.1 LFI & RFI
- 4.2 LFI & RFI
- 4.3 LFI & RFI
- 4.4 LFI & RFI Lab

- 5.1 Report Creation
- 5.2 Report Creation
- 5.3 Wrap Up
- Owasp Concept

Python Programming



MODULES

- About Python or Python History
- Conditional Statement
- Learn how to Interacting with Networks
- How to debug python programs
- Common Gateway Interface
- How statistical modelling relates to machine learning and how to compare them.
- Loop and string
- Control Statement
- Input / Output
- Functions and Module
- Unsupervised learning algorithms, including Clustering and Dimensionality Reduction.

Networking

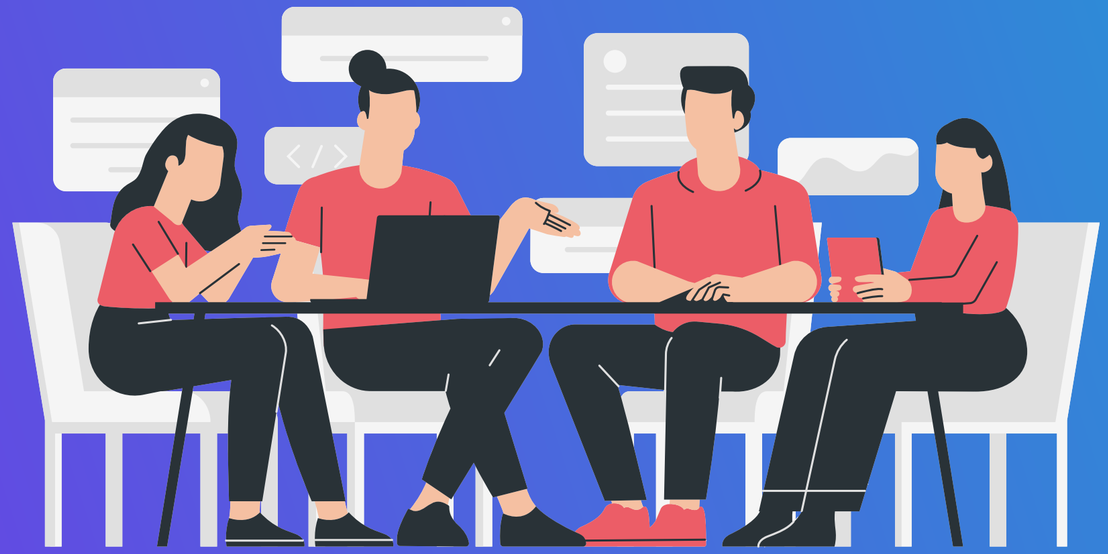
MODULES

- Introduction to Networking
- OSI Model
- TCP/IP Model
- Subnetting/Summarisation
- Packet Flow in Same & Different Network
- Information About Networking Device
- IP/ICMP
- APIPA
- ARP
- Routing Protocols(Static & Dynamic)

MODULES

- Static : Next hop/Exit Interface
- Dynamic : RIP/EIGRP/OSPF & BGP
- Wan Technologies
- NAT
- ACL
- Dynamic Host Configuration Protocol
- Telnet & SSH
- Load Balancing Protocol
- Layers 2 Protocols
- VLAN
- Different Types of STP
- Ether Channel(L2)
- Port Security

CODEVIRUS SECURITY



REGISTER NOW

+91 90267 64985

CODEVIRUSSEC.IN