2 Year Course of Cyber Security

1. Computer Basics – 1st Semester -3 weeks

Introduction to Computers
Computer hardware and software
Operating systems Basics
File management
Internet Basics
Introduction to algorithms and problem solving.
MS Office

HTML

1. Introduction to HTML
2. HTML Tags and Attributes
3. Semantic HTML
4. HTML Forms
5. HTML 5 Features

CSS

1. Introduction to CSS
2. CSS Selectors
3. Box model and layout
4. CSS Flexbox
5. CSS Grid

2. Networking Basics - 1st Semester

Module 01 : Computer Networking
Module 04 : Subnet Mask, CIDR and Subnetting
Module 03 : IPV4 and IPV6
Module 06 : OSI MODEL
Module 05 : VLSM, Wild Card, Summarization
Module 08 : Network Devices, Cabling & Packet Tracer
Module 07 : TCP / IP MODEL
Module 10 : Packet Flow
Module 09 : ARP and ICMP
Module 12 : Static Routing - Next HOP IP & Exit Interface
Module 11 : Routing - Static and Dynamic
Module 13 : Dynamic - RIP
Module 14 : EIGRP
Module 16 : Redistribution
Module 15 : OSPF
Module 18 : DHCP
Module 17 : Remote Services (Telnet and SSH)
Module 20 : Switching
Module 19 : ACL
Module 22 : Ether - Channel
Module 21 : L2 Protocols - CDP, VLAN, STP, DTP, VTP
Module 23 : Port Security

3. Linux Essentials - 1st Semester

Module 01 : Getting Started with Red Hat Enterprise Linux
Module 02 : Accessing the Command Line
Module 03 : Managing Files from the command Line
Module 04 : Getting Help in Red Hat Enterprise Linux
Module 05 : Creating, Viewing & Editing Test Files
Module 06 : Managing Local Users and Groups
Module 07 : Controlling Access to Files
Module 08 : Monitoring and Managing Linux Process
Module 09 : Controlling Services and Daemons
Module 10 : Configuring and Securing SSH
Module 11 : Analyzing and Storing Logs
Module 12 : Managing Networking
Module 13 : Archiving and Transferring Files
Module 14 : Installing and Updating Software Packages
Module 15 : Accessing Linux File System
Module 16 : Analyzing Servers and Getting Support

4. Python Programming – 2nd Semester

Module 01 : Python - An Introduction
Module 02 : Comparisons of Python with other Language
Module 03 : Python Variables & Data Types
Module 04 : Operators
Module 05 : Python Conditional Statements
Module 06 : Python Looping Concept
Module 07 : Control Statements
Module 08 : Data Type Casting
Module 09 : Python Number
Module 10 : String
Module 11 : Python List
Module 12 : Python Tuple
Module 13 : Python Dictionary
Module 14 : Python Array
Module 15 : Python Date & Time
Module 16 : File Handling (Input / Output)
Module 17 : Multithreading
Module 18 : Python Mail Sending Program
Module 19 : Database Connection
Module 20 : OOPs Concepts

5. Ethical Hacking – 2nd Semester

Module 01 : Introduction to Basics of Ethical Hacking
Module 02 : Foot-printing Active (Tool Based Practical)
Module 03 : Foot-printing Passive (Passive Approach)
Module 04 : In-depth Network Scanning
Module 05 : Enumeration User Identification
Module 06 : System Hacking Password Cracking & Bypassing
Module 07 : Viruses and Worms
Module 08 : Trojan and Back door
Module 09 : Bots and Botnets
Module 10 : Sniffers MITM with Kali
Module 11 : Sniffers MITM with Windows
Module 12 : Social Engineering Techniques Theoretical Approach
Module 13 : Social Engineering Toolkit Practical Based Approach
Module 14 : Denial of Service DOS & DDOS Attacks
Module 15 : Web Session Hijacking
Module 16 : SQL Injection Manual Testing
Module 17 : SQL Injection Automated Tool Based Testing
Module 18 : Basics of Web App Security
Module 19 : Hacking Web servers Server Rooting
Module 20 : Hacking Wireless Networks Manual CLI Based
Module 21 : Hacking Wireless Network

Module 22 : Evading IDS, Firewall
Module 23 : Honey pots
Module 24 : Buffer Overflow
Module 25 : Cryptography
Module 26 : Penetration Testing: Basics
Module 27 : Mobile Hacking
Module 28 : Internet of Things (IOT) Hacking
Module 29 : Cloud Security and many more

6. Advance Penetration Testing – 3rd Semester

Module 01 : Introduction
Module 02 : In-Depth Scanning
Module 03 : Exploitation
Module 04 : Command Line Fun
Module 05 : Getting Comfortable with Kali Linux
Module 06 : Bash Scripting
Module 07 : Practical Tools
Module 08 : Active Information Gathering
Module 09 : Passive Information Gathering
Module 10 : Introduction to Buffer Overflows
Module 11 : Buffer Overflows
Module 12 : Fixing Exploits
Module 13 : Locating Public Exploits
Module 14 : Antivirus Evasion
Module 15 : File Transfers
Module 16 : Windows Privilege Escalation
Module 17 : Linux Privilege Escalation
Module 18 : Password Attacks
Module 19 : Port Redirection and Tunnelin
Module 20 : Active Directory Attacks
Module 21 : Power Shell Empire
Module 22 : Trying Harder : The Labs
Module 23 : Penetration Test Breakdown

7. Cyber Forensics Investigation – 3rd Semester

Module 01 : Computer Forensics in today's World
Module 02 : Computer Forensics Investigation Process
Module 03 : Hard-Disk and File-System
Module 04 : Data-Acquisition and Duplication
Module 05 : Defeating Anti-Forensics Techniques
Module 06 : Windows Forensics
Module 07 : Linux Forensics
Module 08 : Network Forensics
Module 09 : Web-Forensics
Module 10 : Dark Web Forensics
Module 11 : Cloud forensics
Module 12 : Email-Forensics
Module 13 : Malware Forensics
Module 14 : Mobile forensics
Module 15 : IOT forensics
Module

8. Web Application Security – 4th Semester

01 : Introduction
Module 02 : Owasp Top 10
Module 03 : Recon for Bug Hunting
Module 04 : Advanced SQL Injection
Module 05 : Command Injection
Module 06 : Session Management and Broken Authentication Vulnerability
Module 07 : CSRF - Cross Site Request Forgery
Module 08 : SSRF - Server Site Request Forgery
Module 09 : XSS - Cross Site Scritpting
Module 10 : IDOR - Insecure Direct Object Reference

Module 11 : Sensitive Data Exposure and Information Disclose
Module 12 : SSTI - Server Site Template Injection
Module 13 : Multi Factor Authentication Bypass
Module 14 : HTTP Request Smuggling
Module 15 : XXE - XML External Entities
Module 16 : LFI - Local File Inclusion and RFI - Remote File Inclusion
Module 17 : Source Code Disclousre
Module 18 : Directory Path Traversal
Module 19 : HTML Injection
Module 20 : Host Header Injection
Module 21 : SQL Authentication Bypass
Module 22 : File Upload Vulnerability
Module 23 : JWT Token Attack
Module 24 : Security Misconfiguration
Module 25 : URL Redirection
Module 26 : Flood Attack on Web

9. Web Application Security – 4th Semester

Module 01 : Introduction to Mobile Penetration Testing
Module 02 : Lab Setup
Module 03 : Android Architecture
Module 04 : APK file Structure
Module 05 : Reversing App with APK tool
Module 06 : Reversing App with MobSf
Module 07 : Static Analysis
Module 08 : Scanning Vulnerability with Drozer
Module 09 : Improper Platform Usage
Module 10 : Insecure Data Storage
Module 11 : Insecure Communication
Module 12 : Insecure Authentication
Module 13 : Insufficient Cryptography
Module 14 : Insecure Authorization
Module 15 : Code Tampering
Module 16 : Reverse Engineering
Module 17 : Extraneous Functionality
Module 18 : SSL Pinning
Module 19 : Intercepting the Network Traffic
Module 20 : Dynamic Analysis
Module 21 : Report Preparation
Module 22 : IOS Penetration Basics

10. Internet of Things (IOT) Pentesting – 5th Semester

Module 01 : Overview of Why IoT is so important
Module 02 : Introduction of IoT
Module 03 : Introduction to Sensor Network & Wireless protocol
Module 04 : Review of Electronics Platform, Production & Cost Projection
Module 05 : Conceiving a new IoT product- Product Requirement document for IoT
Module 06 : Introduction to Mobile app platform & Middleware for IoT
Module 07 : Machine learning for intelligent IoT
Module 08 : Analytic Engine for IoT
Module 09 : Iaas/Paas/Saas-IoT data, platform and software as a service revenue model

11. End Point Security – 5th Semester

Module 01 : Implementing Internet Security Anti Virus
Module 02 : Two-Factor Authentication Implementation
Module 03 : Mobile Device Management For Industry
Module 04 : Data Loss Prevention Overview & Implementation
Module 05 : Security Information and Event Management (SIEM)
Module 06 : APT- Attack
Module 07 : MITRE Framework
Module 08 : EDR
Module 09 : MDR
Module 10 : Next Generation Firewall
Module 11 : Unified Threat Management
Module 12 : Physical Security
Module 13 : ISO 27001 Lead Auditor Guidelines

12. AWS Associate – 6th Semester

Module 01 : Designing Highly Available, cost effective, scalable systems
(a) Planning and Design (b) Monitoring and Logging
(c) Hybrid IT Architectures (d) Elasticity and Scalability

Module 02 : Implementation and Deployment
(a) Amazon EC2 (b) Amazon S3
(c) Amazon Web Service Cloud Formation (d) Amazon Web Service VPS
(e) Amazon Web Service IAM

Module 03 : Data Security

(a) AWS IAM (Identify and Access Management)
(b) Amazon Web Service VPC
(c) Encryption Solutions
(d) Cloud watch logs
(e) Disaster Recovery
(f) Amazon Route 53
(g) AWS Storage Gateway
(h) Amazon Web Service Import/Export

Module 04 : Troubleshooting

13. AWS Security – 6th Semester

Module 01 : Given an AWS Abuse Notice, Evaluate a Suspected Compromised Instance or Exposed Access Key
Module 02 : Verify that the Incident Response plan includes relevant AWS services
Module 03 : Evaluate the Configuration of Automated Alerting and Execute Possible Remediation of Security-Related Incidents and Emerging Issues
Module 04 : Design and implement security monitoring and alerting
Module 05 : Troubleshoot security monitoring and alerting
Module 06 : Design and Implement a Logging Solution
Module 07 : Design Edge Security on AWS
Module 08 : Troubleshoot Logging Solutions
Module 09 : Design and implement a secure network infrastructure
Module 10 : Troubleshoot a secure network infrastructure
Module 11 : Design and implement host-based security
Module 12 : Design and Implement a Scalable Authorization and Authentication System to Access AWS Resources
Module 13 : Troubleshoot an Authorization and Authentication System to Access AWS Resources
Module 14 : Design and implement key management and use
Module 15 : Troubleshoot key management
Module 16 : Design and implement a data encryption solution for data at rest and data in transit

1 Year Course of Cyber Security

1. Computer Basics

Introduction to Computers
Computer hardware and software
Operating systems Basics
File management
Internet Basics
Introduction to algorithms and problem solving.
MS Office

HTML

Introduction to HTML
HTML Tags and Attributes
Semantic HTML
HTML Forms
HTML 5 Features

CSS

Introduction to CSS
CSS Selectors
Box model and layout
CSS Flexbox
CSS Grid

2. Networking Basics

Module 01 : Computer Networking
Module 04 : Subnet Mask, CIDR and Subnetting
Module 03 : IPV4 and IPV6
Module 06 : OSI MODEL
Module 05 : VLSM, Wild Card, Summarization
Module 08 : Network Devices, Cabling & Packet Tracer
Module 07 : TCP / IP MODEL
Module 10 : Packet Flow
Module 09 : ARP and ICMP
Module 12 : Static Routing - Next HOP IP & Exit Interface
Module 11 : Routing - Static and Dynamic
Module 13 : Dynamic - RIP
Module 14 : EIGRP
Module 16 : Redistribution
Module 15 : OSPF
Module 18 : DHCP
Module 17 : Remote Services (Telnet and SSH)
Module 20 : Switching
Module 19 : ACL
Module 22 : Ether - Channel
Module 21 : L2 Protocols - CDP, VLAN, STP, DTP, VTP
Module 23 : Port Security

3. Linux Essentials

Module 01 : Getting Started with Red Hat Enterprise Linux
Module 02 : Accessing the Command Line
Module 03 : Managing Files from the command Line
Module 04 : Getting Help in Red Hat Enterprise Linux
Module 05 : Creating, Viewing & Editing Test Files
Module 06 : Managing Local Users and Groups
Module 07 : Controlling Access to Files
Module 08 : Monitoring and Managing Linux Process
Module 09 : Controlling Services and Daemons
Module 10 : Configuring and Securing SSH
Module 11 : Analyzing and Storing Logs
Module 12 : Managing Networking
Module 13 : Archiving and Transferring Files
Module 14 : Installing and Updating Software Packages
Module 15 : Accessing Linux File System
Module 16 : Analyzing Servers and Getting Support

4. Python Programming

Module 01 : Python - An Introduction
Module 02 : Comparisons of Python with other Language
Module 03 : Python Variables & Data Types
Module 04 : Operators
Module 05 : Python Conditional Statements
Module 06 : Python Looping Concept
Module 07 : Control Statements
Module 08 : Data Type Casting
Module 09 : Python Number
Module 10 : String
Module 11 : Python List
Module 12 : Python Tuple
Module 13 : Python Dictionary
Module 14 : Python Array
Module 15 : Python Date & Time
Module 16 : File Handling (Input / Output)
Module 17 : Multithreading
Module 18 : Python Mail Sending Program
Module 19 : Database Connection
Module 20 : OOPs Concepts
Module 21 : Interacting with Networks
Module 22 : Graphical User Interface
Module 23 : Python Web Scraping
Module 24 : Python for Image Processing
Module 25 : Python Data Science
Module 26 : Intro with Python Machine Learning
Module 27 : Intro with Python Artificial Intelligence
Module 28 : Functions

5. Ethical Hacking

Module 01 : Introduction to Basics of Ethical Hacking
Module 02 : Foot-printing Active (Tool Based Practical)
Module 03 : Foot-printing Passive (Passive Approach)
Module 04 : In-depth Network Scanning
Module 05 : Enumeration User Identification
Module 06 : System Hacking Password Cracking & Bypassing
Module 07 : Viruses and Worms
Module 08 : Trojan and Back door
Module 09 : Bots and Botnets
Module 10 : Sniffers MITM with Kali
Module 11 : Sniffers MITM with Windows
Module 12 : Social Engineering Techniques Theoretical Approach
Module 13 : Social Engineering Toolkit Practical Based Approach

Module 14 : Denial of Service DOS & DDOS Attacks
Module 15 : Web Session Hijacking
Module 16 : SQL Injection Manual Testing
Module 17 : SQL Injection Automated Tool Based Testing
Module 18 : Basics of Web App Security
Module 19 : Hacking Web servers Server Rooting
Module 20 : Hacking Wireless Networks Manual CLI Based
Module 21 : Hacking Wireless Network
Module 22 : Evading IDS, Firewall
Module 23 : Honey pots
Module 24 : Buffer Overflow
Module 25 : Cryptography
Module 26 : Penetration Testing: Basics
Module 27 : Mobile Hacking
Module 28 : Internet of Things (IOT) Hacking
Module 29 : Cloud Security and many more

6. Advance Penetration Testing

Module 01 : Introduction
Module 02 : In-Depth Scanning
Module 03 : Exploitation
Module 04 : Command Line Fun
Module 05 : Getting Comfortable with Kali Linux
Module 06 : Bash Scripting
Module 07 : Practical Tools
Module 08 : Active Information Gathering
Module 09 : Passive Information Gathering
Module 10 : Introduction to Buffer Overflows
Module 11 : Buffer Overflows
Module 12 : Fixing Exploits
Module 13 : Locating Public Exploits
Module 14 : Antivirus Evasion
Module 15 : File Transfers
Module 16 : Windows Privilege Escalation
Module 17 : Linux Privilege Escalation
Module 18 : Password Attacks
Module 19 : Port Redirection and Tunnelin
Module 20 : Active Directory Attacks
Module 21 : Power Shell Empire
Module 22 : Trying Harder : The Labs
Module 23 : Penetration Test Breakdown

7. Cyber Forensics Investigation

Module 01 : Computer Forensics in today’s World
Module 02 : Computer Forensics Investigation Process
Module 03 : Hard-Disk and File-System
Module 04 : Data-Acquisition and Duplication
Module 05 : Defeating Anti-Forensics Techniques
Module 06 : Windows Forensics
Module 07 : Linux Forensics
Module 08 : Network Forensics
Module 09 : Web-Forensics
Module 10 : Dark Web Forensics
Module 11 : Cloud forensics
Module 12 : Email-Forensics
Module 13 : Malware Forensics
Module 14 : Mobile forensics
Module 15 : IOT forensics

8. Web Application Security

Module 01 : Introduction
Module 02 : Owasp Top 10

Module 03 : Recon for Bug Hunting
Module 04 : Advanced SQL Injection
Module 05 : Command Injection
Module 06 : Session Management and Broken Authentication Vulnerability
Module 07 : CSRF - Cross Site Request Forgery
Module 08 : SSRF - Server Site Request Forgery
Module 09 : XSS - Cross Site Scritpting
Module 10 : IDOR - Insecure Direct Object Reference
Module 11 : Sensitive Data Exposure and Information Disclose
Module 12 : SSTI - Server Site Template Injection
Module 13 : Multi Factor Authentication Bypass
Module 14 : HTTP Request Smuggling
Module 15 : XXE - XML External Entities
Module 16 : LFI - Local File Inclusion and RFI - Remote File Inclusion
Module 17 : Source Code Disclousre
Module 18 : Directory Path Traversal
Module 19 : HTML Injection
Module 20 : Host Header Injection
Module 21 : SQL Authentication Bypass
Module 22 : File Upload Vulnerability
Module 23 : JWT Token Attack
Module 24 : Security Misconfiguration
Module 25 : URL Redirection
Module 26 : Flood Attack on Web

9. Mobile Application Security

Module 01 : Introduction to Mobile Penetration Testing
Module 02 : Lab Setup
Module 03 : Android Architecture
Module 04 : APK file Structure
Module 05 : Reversing App with APK tool
Module 06 : Reversing App with MobSf
Module 07 : Static Analysis
Module 08 : Scanning Vulnerability with Drozer
Module 09 : Improper Platform Usage
Module 10 : Insecure Data Storage
Module 11 : Insecure Communication
Module 12 : Insecure Authentication
Module 13 : Insufficient Cryptography
Module 14 : Insecure Authorization
Module 15 : Code Tampering
Module 16 : Reverse Engineering
Module 17 : Extraneous Functionality
Module 18 : SSL Pinning
Module 19 : Intercepting the Network Traffic
Module 20 : Dynamic Analysis
Module 21 : Report Preparation
Module 22 : IOS Penetration Basics

6 Months Specialization Courses of Cyber Security

Networking (CCNA) – 6 Months

Module 01 : Computer Networking
Module 04 : Subnet Mask, CIDR and Subnetting
Module 03 : IPV4 and IPV6
Module 06 : OSI MODEL
Module 05 : VLSM, Wild Card, Summarization
Module 08 : Network Devices, Cabling & Packet Tracer
Module 07 : TCP / IP MODEL
Module 10 : Packet Flow
Module 09 : ARP and ICMP
Module 12 : Static Routing - Next HOP IP & Exit Interface
Module 11 : Routing - Static and Dynamic
Module 13 : Dynamic - RIP
Module 14 : EIGRP
Module 16 : Redistribution
Module 15 : OSPF
Module 18 : DHCP
Module 17 : Remote Services (Telnet and SSH)
Module 20 : Switching
Module 19 : ACL
Module 22 : Ether - Channel
Module 21 : L2 Protocols - CDP, VLAN, STP, DTP, VTP
Module 23 : Port Security

Linux (RHCSA) – 6 Months

Module 01 : Getting Started with Red Hat Enterprise Linux
Module 02 : Accessing the Command Line
Module 03 : Managing Files from the command Line
Module 04 : Getting Help in Red Hat Enterprise Linux
Module 05 : Creating, Viewing & Editing Test Files
Module 06 : Managing Local Users and Groups
Module 07 : Controlling Access to Files
Module 08 : Monitoring and Managing Linux Process
Module 09 : Controlling Services and Daemons
Module 10 : Configuring and Securing SSH
Module 11 : Analyzing and Storing Logs
Module 12 : Managing Networking
Module 13 : Archiving and Transferring Files
Module 14 : Installing and Updating Software Packages
Module 15 : Accessing Linux File System
Module 16 : Analyzing Servers and Getting Support

Certified Ethical Hacking (CEHv12) – 6 Months

Module 01 : Introduction to Basics of Ethical Hacking
Module 02 : Foot-printing Active (Tool Based Practical)
Module 03 : Foot-printing Passive (Passive Approach)
Module 04 : In-depth Network Scanning
Module 05 : Enumeration User Identification
Module 06 : System Hacking Password Cracking & Bypassing
Module 07 : Viruses and Worms
Module 08 : Trojan and Back door
Module 09 : Bots and Botnets
Module 10 : Sniffers MITM with Kali
Module 11 : Sniffers MITM with Windows
Module 12 : Social Engineering Techniques Theoretical Approach

Module 13 : Social Engineering Toolkit Practical Based Approach
Module 14 : Denial of Service DOS & DDOS Attacks
Module 15 : Web Session Hijacking
Module 16 : SQL Injection Manual Testing
Module 17 : SQL Injection Automated Tool Based Testing
Module 18 : Basics of Web App Security
Module 19 : Hacking Web servers Server Rooting
Module 20 : Hacking Wireless Networks Manual CLI Based
Module 21 : Hacking Wireless Network
Module 22 : Evading IDS, Firewall
Module 23 : Honey pots
Module 24 : Buffer Overflow
Module 25 : Cryptography
Module 26 : Penetration Testing: Basics
Module 27 : Mobile Hacking
Module 28 : Internet of Things (IOT) Hacking
Module 29 : Cloud Security and many more

Certified Forensics Specialist (CHFI) – 6 Months

Module 01 : Computer Forensics in today's World
Module 02 : Computer Forensics Investigation Process
Module 03 : Hard-Disk and File-System
Module 04 : Data-Acquisition and Duplication
Module 05 : Defeating Anti-Forensics Techniques
Module 06 : Windows Forensics
Module 07 : Linux Forensics
Module 08 : Network Forensics
Module 09 : Web-Forensics
Module 10 : Dark Web Forensics
Module 11 : Cloud forensics
Module 12 : Email-Forensics
Module 13 : Malware Forensics
Module 14 : Mobile forensics
Module 15 : IOT forensics

Web Application Penetration Testing – 6 Months

Module 01 : Introduction
Module 02 : Owasp Top 10
Module 03 : Recon for Bug Hunting
Module 04 : Advanced SQL Injection
Module 05 : Command Injection
Module 06 : Session Management and Broken Authentication Vulnerability
Module 07 : CSRF - Cross Site Request Forgery
Module 08 : SSRF - Server Site Request Forgery
Module 09 : XSS - Cross Site Scritpting
Module 10 : IDOR - Insecure Direct Object Reference
Module 11 : Sensitive Data Exposure and Information Disclose
Module 12 : SSTI - Server Site Template Injection
Module 13 : Multi Factor Authentication Bypass
Module 14 : HTTP Request Smuggling
Module 15 : XXE - XML External Entities
Module 16 : LFI - Local File Inclusion and RFI - Remote File Inclusion
Module 17 : Source Code Disclousre
Module 18 : Directory Path Traversal
Module 19 : HTML Injection
Module 20 : Host Header Injection
Module 21 : SQL Authentication Bypass
Module 22 : File Upload Vulnerability
Module 23 : JWT Token Attack

Module 24 : Security Misconfiguration
Module 25 : URL Redirection
Module 26 : Flood Attack on Web

Mobile Application Penetration Testing – 6 Months

Module 01 : Introduction to Mobile Penetration Testing
Module 02 : Lab Setup
Module 03 : Android Architecture
Module 04 : APK file Structure
Module 05 : Reversing App with APK tool
Module 06 : Reversing App with MobSf
Module 07 : Static Analysis
Module 08 : Scanning Vulnerability with Drozer
Module 09 : Improper Platform Usage
Module 10 : Insecure Data Storage
Module 11 : Insecure Communication
Module 12 : Insecure Authentication
Module 13 : Insufficient Cryptography
Module 14 : Insecure Authorization
Module 15 : Code Tampering
Module 16 : Reverse Engineering
Module 17 : Extraneous Functionality
Module 18 : SSL Pinning
Module 19 : Intercepting the Network Traffic
Module 20 : Dynamic Analysis
Module 21 : Report Preparation
Module 22 : IOS Penetration Basics

Internet of Things (IOT) Pentesting – 6 Months

Module 01 : Overview of Why IoT is so important
Module 02 : Introduction of IoT
Module 03 : Introduction to Sensor Network & Wireless protocol
Module 04 : Review of Electronics Platform, Production & Cost Projection
Module 05 : Conceiving a new IoT product- Product Requirement document for IoT
Module 06 : Introduction to Mobile app platform & Middleware for IoT
Module 07 : Machine learning for intelligent IoT
Module 08 : Analytic Engine for IoT
Module 09 : Iaas/Paas/Saas-IoT data, platform and software as a service revenue model

AWS Cloud Associate and Security – 6 Months

Associate :-

Module 01 : Designing Highly Available, cost effective, scalable systems
(a) Planning and Design
(b) Monitoring and Logging
(c) Hybrid IT Architectures
(d) Elasticity and Scalability

Module 02 : Implementation and Deployment
(a) Amazon EC2
(b) Amazon S3
(c) Amazon Web Service Cloud Formation
(d) Amazon Web Service VPS
(e) Amazon Web Service IAM

Module 03 : Data Security
(a) AWS IAM (Identify and Access Management)
(b) Amazon Web Service VPC
(c) Encryption Solutions
(d) Cloud watch logs
(e) Disaster Recovery
(f) Amazon Route 53

(g) AWS Storage Gateway (h) Amazon Web Service Import/Export

Module 04 : Troubleshooting

Security :-

Module 01 : Given an AWS Abuse Notice, Evaluate a Suspected Compromised Instance or Exposed Access Key
Module 02 : Verify that the Incident Response plan includes relevant AWS services
Module 03 : Evaluate the Configuration of Automated Alerting and Execute Possible Remediation of Security-Related Incidents and Emerging Issues
Module 04 : Design and implement security monitoring and alerting
Module 05 : Troubleshoot security monitoring and alerting
Module 06 : Design and Implement a Logging Solution
Module 07 : Design Edge Security on AWS
Module 08 : Troubleshoot Logging Solutions
Module 09 : Design and implement a secure network infrastructure
Module 10 : Troubleshoot a secure network infrastructure
Module 11 : Design and implement host-based security
Module 12 : Design and Implement a Scalable Authorization and Authentication System to Access AWS Resources
Module 13 : Troubleshoot an Authorization and Authentication System to Access AWS Resources
Module 14 : Design and implement key management and use
Module 15 : Troubleshoot key management
Module 16 : Design and implement a data encryption solution for data at rest and data in transit