INFORMATION SECURITY TRAINING

Course Content

Course Duration: 45 days

Pre-Requisite: Basic Knowledge of Internet

Course Fee: ₹ 15,000 (Online Examination Fee, Books, Certification, Tools & Software's Included)

Module 1

CCNA

The Cisco Certified Network Associate (CCNA) course consists of days 1 to 5 of the Cisco Networking Academy Programme.

1. OSI model and industry standards
2. Network topologies
3. IP addressing, including subnet masks
4. Networking components
5. Basic network design
6. Beginning router configurations
7. Routed and routing protocols
8. Advanced router configurations
9. LAN switching theory and VLANs
10. Advanced LAN and LAN switched design
11. Novell IPX
12. Threaded case studies
13. WAN theory and Design
14. WAN technology, PPP, Frame Relay, ISDN
15. Network troubleshooting
16. National SCANS Skills
Module 2

BCSE (Byte code Certified Security Expert) V.2

BCSE is a most famous, well prepared and recognised certification in ethical hacking for beginners, which is very useful and demandable in Information Security & technology world, the program covers the all types of ethical hacking concepts which is very useful for this industry, its the only way to start your career in cyber security or in IT world.

1 History of Hacking
2 Basics of internet, Networking & Hacking
3 Windows & Linux Basics
4 Basics of Hacking & Ethics
5 Google Hacking, Yahoo Hacking
6 Scanning
7 Foot printing
8 Email Hacking
9 System Hacking
10 Trojans hacking
11 Sniffers
12 DOS attacks
13 Attacks & Types
14 Social Engineering

17. Threaded case study
15 Session Hijacking
16 Hacking Web Servers
17 Compromised Systems
18 Advanced PHP Injection
19 Advanced SQL Injection
20 Physical Security
21 Firewalls & Honeypots
22 Cryptography
23 Cyber Forensics
24 Cyber Crimes & Laws
25 Financial Frauds Online
26 Hardware Hacking
27 Email Hacking
28 Password Hacking
29 Password Sniffing
30 Mobile Phone Hacking
31 Bluetooth Hacking
32 Wireless Devices & Wi-Fi Hacking
34 Penetration Testing
35 Website & Web Hacking
36 Website & Web Security
37 Viruses & Worms
38 Vulnerability Scanning & Assessments
39 Backtrack Training
40 Steganography & Cyber Forensics
41 Security Auditing Methodologies
42 Remote & Desktop Root Vulnerability Exploitation
43 Metasploit Training
44 Brute Forcing
45 XSS Hacking
46 Defensive Techniques
47 Desktop exploitation
48 Routers & Firewall Hacking
49 PHP - Shell Hacking
50 Hacking With Mobile OS’s

MODULE 3

CEH (Certified Ethical Hacker) V.7

CEHv7 provides a comprehensive ethical hacking and network security-training program to meet the standards of highly skilled security professionals. Hundreds of SMEs and authors have contributed towards the content presented in the CEHv7 courseware. Latest tools and exploits uncovered from the underground community are featured in the new package. Our researchers have invested thousands of man hours researching the latest trends and uncovering the covert techniques used by the underground community.

1. Understand the issues plaguing the information security world
2. Gain knowledge on various hacking terminologies
3. Learn the basic elements of information security
4. Understand the security, functionality and ease of use triangle
5. Know the 5 stages of ethical hacking
6. Understand the different types and implications of hacker attacks
7. Understand hactivism and understand the classification of hackers
8. Understand who is an ethical hacker
9. Gain Information on how to become an ethical hacker
10. Learn the profile of a typical ethical hacker
11. Understand scope and limitations of ethical hacking
12. Understand vulnerability research and list the various vulnerability research tools
13. Learn the different ways an ethical hacker tests a target network
14. Understand penetration testing and the various methodologies used
15. Understand the term Footprinting
16. Learn the areas and information that hackers seek
17. Gain knowledge on information gathering tools and methodology
18. Understand the role of financial websites in footprinting
19. Understand competitive intelligence and its need
20. Understand DNS enumeration
21. Understand Who is
22. Learn different types of DNS records
23. Understand how trace route is used in Foot printing
24. Recognize the Role of search engines in foot printing
25. Learn the website mirroring tools
26. Understand how e-mail tracking works
27. Understand Google hacking and its tools
28. Learn the countermeasures to be taken in footprinting
29. Understand pen testing
30. Understand the term port scanning, network scanning and vulnerability scanning
31. Understand the objectives of scanning
32. Learn the CEH scanning methodology
33. Understand Ping Sweep techniques
34. Understand the Fire walk tool
35. Gain knowledge on Nmap command switches
36. Understand the three way handshake
37. Understand the following Scans:
38. SYN, Stealth, XMAS, NULL, IDLE, FIN, ICMP Echo, List, TCP Connect, Full Open, FTP Bounce, UDP, Reverse Indent, RPC, Window
39. Learn TCP communication flag types
40. Gain knowledge on War dialling techniques
41. Understand banner grabbing using OS fingerprinting, Active Stack Fingerprinting, Passive Fingerprinting and other techniques and tools
42. Learn vulnerability scanning using BidiBlah and other hacking tools
43. Learn to draw network diagrams of vulnerable hosts using various tools
44. Understand how proxy servers are used in launching an attack
45. Gain insights on working of anonymizers
46. Identify HTTP tunnelling techniques
47. Identify IP spoofing techniques
48. Understand various scanning countermeasures
49. Learn the system hacking cycle
50. Understand Enumeration and its techniques
51. Understand null sessions and its countermeasures
52. Understand SNMP enumeration and its countermeasures
53. Describe the steps involved in performing enumeration
54. Understand the different types of passwords
55. Identify the different types of password attacks
56. Identify password cracking techniques
57. Understand Microsoft Authentication mechanism
58. Describe password sniffing
59. Identifying various password cracking tools
60. Identify various password cracking countermeasures
61. Understand privilege escalation
62. Gain insights on key loggers and other spyware technologies
63. Learn how to defend against spyware
64. Identify different ways to hide files
65. Understanding rootkits
66. Learn how to identify rootkits and steps involved
67. Understand Alternate Data Streams
68. Understand Steganography technologies and tools used
69. Understand covering tracks, tools used and erase evidences
70. Define a Trojan
71. Identify overt and covert channels
72. Understand working of Trojans
73. Identify the different types of Trojans
74. What do Trojan creators look for
75. Identify the different ways a Trojan can infect a system
76. How to indicate a Trojan attack
77. Identify the ports used by Trojan
78. Identify listening ports using netstat
79. Understand “wrapping”
80. Understand Reverse Shell Trojan
81. Understand ICMP tunneling
82. Identify various classic Trojans
83. Learn windows start up monitoring tools
84. Understand the Trojan horse constructing kit
85. Learn Trojan detection techniques
86. Learn Trojan evading techniques
87. Learn how to avoid a Trojan infection
88. Understand virus and its history
89. Characteristics of a virus
90. Learn the working of a virus
91. Understand the motive behind writing a virus
92. Understand how does a computer get infected by viruses
93. Gain insights on virus hoax
94. Understand virus analysis
95. Understand the difference between a virus and a worm
96. Understand the life cycle of virus
97. Identify the types of viruses
98. Understand how a virus spreads and infects the system
99. Understand the storage pattern of virus
100. Identify various types of classic virus found in the wild
101. Virus writing technique
102. Virus construction kits
103. Understand antivirus evasion techniques
104. Understand Virus detection methods and countermeasures
105. Understand worm analysis
106. Understand sniffing and protocols vulnerable to it
107. Identify types of sniffing
108. Understand Address Resolution Protocol (ARP)
109. Understanding the process of ARP Spoofing
110. Understand active and passive sniffing
111. Understand ARP poisoning
112. Understand MAC duplicating
113. Learn ethereal capture and display filters
114. Understand MAC flooding
115. Understand DNS spoofing techniques
116. Identify sniffing countermeasures
117. Know various sniffing tools
118. Identify sniffing detection and defensive techniques
119. Understand Social Engineering
120. Understand human weakness
121. Identify the different types of social engineering
122. Learn warning signs of an attack
123. Understand Dumpster Diving
124. Understand Human-based Social Engineering
125. Understand Insider attacks and its countermeasures
126. Gain insights on Social Engineering threats and defense
127. Comprehend Identity Theft
128. Understand Phishing Attacks
129. Identify Online Scams
130. Understand URL obfuscation
131. Understand social engineering on social networking sites
132. Identify Social Engineering countermeasures
133. Understand a Denial of Service Attack
134. Gain insights on Distributed Denial of Service Attacks
135. Examine the working of Distributed Denial of Service Attacks
136. Analyze Symptoms of a DoS Attack
137. Understand Internet Chat Query (ICQ)
138. Understand Internet Relay Chat (IRC)
139. Assess DoS Attack Techniques
140. Understand Botnets
141. Assess DoS/DDoS Attack Tools
142. Describe Detection Techniques
143. Identify DoS/DDoS Countermeasure Strategies
144. Analyze Post-Attack Forensics
145. Identify DoS/DDoS Protection Tools
146. Understand DoS/DDoS Penetration Testing
147. Understand what is Session Hijacking
148. Identify Key Session Hijacking Techniques
149. Understand Brute Forcing Attack
150. Understand HTTP Referrer Attack
151. Spoofing vs. Hijacking
152. Understand Session Hijacking Process
153. Identify types of Session Hijacking
154. Analyze Session Hijacking in OSI Model
155. Understand Application Level Session Hijacking
156. Discuss Session Sniffing
157. Describe Man-in-the-Middle Attack
158. Understand Man-in-the-Browser Attack
159. Examine Steps to Perform Man-in-the-Browser Attack
160. Understand Client-side Attacks
161. Understand Cross-site Script Attack
162. Understand Session Fixation Attack
163. Describe Network Level Session Hijacking
164. Understand TCP/IP Hijacking
165. Identify Session Hijacking Tools
166. Identify Countermeasures of Session Hijacking
167. Understand Session Hijacking Pen Testing
168. Understand Open Source Webserver Architecture
169. Examine IIS Webserver Architecture
170. Understand Website Defacement
171. Understand why Web Servers are compromised
172. Analyze Impact of Webserver Attacks
173. Examine Webserver Misconfiguration
174. Understand Directory Traversal Attacks
175. Learn regarding HTTP Response Splitting Attack
176. Understand Web Cache Poisoning Attack
177. Understand HTTP Response Hijacking
178. Discuss SSH Bruteforce Attack
179. Examine Man-in-the-Middle Attack
180. Learn Webserver Password Cracking Techniques
181. Identify Web Application Attacks
182. Understand Webserver Attack Methodology
183. Identify Webserver Attack Tools
184. Identify Counter-measures against Webserver Attacks
185. Understand Patch Management
186. Assess Webserver Security Tools
187. Understand Webserver Pen Testing
188. Understand Introduction to Web Applications
189. Identify Web Application Components
190. Understand working of Web Applications
191. Examine Web Application Architecture
192. Assess Parameter/Form Tampering
193. Understand Injection Flaws
194. Discuss Hidden Field Manipulation Attack
195. Describe Cross-Site Scripting (XSS) Attacks
196. Understand Web Services Attack
197. Understand Web Application Hacking Methodology
198. Identify Web Application Hacking Tools
199. Understand how to Defend Against Web Application Attacks
200. Identify Web Application Security Tools
201. Understand Web Application Firewalls
202. Gain insights on Web Application Pen Testing
203. Understand SQL Injection
204. Examine SQL Injection Attacks
205. Understand working of Web Applications
206. Identify Server Side Technologies
207. Understand SQL Injection Detection
208. Discuss SQL Injection Black Box Pen Testing
209. Types of SQL Injection
210. Understand Blind SQL Injection
211. Learn SQL Injection Methodology
212. Understanding SQL Query
213. Examine Advanced Enumeration
214. Describe Password Grabbing
215. Discuss Grabbing SQL Server Hashes
216. Identify SQL Injection Tools
217. Understand Evasion Techniques for SQL Injection
218. Understand Defensive strategies Against SQL Injection Attacks
219. Identify SQL Injection Detection Tools
220. Understand Wireless Networks
221. Gain Insights on Wireless Networks
222. Understand various types of Wireless Networks
223. Understand Wi-Fi Authentication Modes
224. Identify types of Wireless Encryption
225. Understand WEP Encryption
226. Understand WPA/WPA2
227. Discuss Wireless Threats
228. Understand Wireless Hacking Methodology
229. Assess Wireless Hacking Tools
230. Understand Bluetooth Hacking
231. Understand how to Defend Against Bluetooth Hacking
232. Understand how to Defend against Wireless Attacks
233. Identify Wi-Fi Security Tools
234. Examine Wireless Penetration Testing Framework
235. Understand Intrusion Detection Systems (IDS)
236. Learn Ways to Detect an Intrusion
237. Acquire knowledge on various types of Intrusion Detection Systems
238. Understand what is a Firewall
239. Types of Firewall
240. Identify Firewall Identification Techniques
241. Understand Honeypot
242. Assess various types of Honeypot
243. Understand how to Set up a Honeypot
244. Understand IDS, Firewall and Honeypot System
245. Examine Evading IDS
246. Understand Evading Firewall
247. Learn detecting Honeypots
248. Identify Firewall Evading tools
249. Identify Countermeasures
250. Analyze Firewall and IDS Penetration Testing
251. Understand Buffer Overflows (BoF)
252. Understand Stack-Based Buffer Overflow
253. Know Heap-Based Buffer Overflow
254. Understand Stack Operations
255. Identify Buffer Overflow Steps
256. Analyze attacking a Real Program
257. Examine Smashing the Stack
258. Examples of Buffer Overflow
259. Understand how to Mutate a Buffer Overflow Exploit
260. Learn how to identify Buffer Overflows
261. Testing for Heap Overflow Conditions: heap.exe
262. Understand steps for Testing Stack Overflow in OllyDbg Debugger
263. Identify Buffer Overflow Detection Tools
264. Understand Defense Against Buffer Overflows
265. Identify Buffer Overflow Countermeasures Tools
266. Understand Buffer Overflow Pen Testing
267. Understand Cryptography
268. Learn various types of Cryptography
269. Understand Ciphers
270. Gain insights on Advanced Encryption Standard (AES)
271. Understand RC4, RC5, RC6 Algorithms
272. Examine RSA (Rivest Shamir Adleman)
273. Explain Message Digest Function: MD5
274. Understand Secure Hashing Algorithm (SHA)
275. Identify Cryptography Tools
276. Understand Public Key Infrastructure (PKI)
277. Understand Email Encryption
278. Identify Digital Signature
279. Describe SSL (Secure Sockets Layer)
280. Examine Disk Encryption
281. Identify Disk Encryption Tools
282. Understand Cryptography Attacks
283. Identify Cryptanalysis Tools
284. Understand Penetration Testing (PT)
285. Identify Security Assessments
286. Examine Risk Management
287. Understand various types of Penetration Testing
288. Understand Automated Testing
289. Understand Manual Testing
290. Understand Penetration Testing Techniques
291. Know the Penetration Testing Phases
292. Understand Enumerating Devices
293. Understand Penetration Testing Roadmap
294. Understand Denial of Service Emulation
295. Outsourcing Pen Testing Services
296. Identify various Penetration testing tools

**MODULE 4**

**Network Security**

The course will make heavy use of hands-on exercises. It will conclude with a large defensive exercise, reinforcing the lessons learned throughout the week.

1. Preparing to Secure Information
2. Explaining How Assets Are Attacked
3. Explaining How Assets Are Secured
4. Implementing Security-Enhanced Computing Baselines
5. Introduction to Trusted Computing Bases
6. Establishing a Security Baseline
7. Monitoring a Security Baseline
8. Helping to Secure Computers Physically
9. Maintaining a Security Baseline
10. Helping to Protect Information Using Authentication and Access Control
11. Introduction to Access Control
12. Implementing an Authentication Strategy
13. Implementing an Access Control Strategy
14. Using Cryptography to Help Protect Information
15. Introduction to Cryptography
16. Using Symmetric Encryption
17. Using Hash Functions
18. Using Public Key Encryption
19. Securing Internet Applications and Components
20. Helping to Protect Web Servers
22. Configuring Security for Web Browsers
23. Configuring Security for Databases
24. Real threats that impact cybersecurity
25. Hackers inside and out
26. Eavesdropping
27. Spoofing
28. Sniffing
29. Trojan horses
30. Viruses
31. Wiretaps
32. A cybersecurity policy: the foundation of your protection
33. Defining your information assurance objectives
34. Assessing your exposure
35. A Cryptography Primer
36. Securing data with symmetric encryption
37. Choosing your algorithm: DES, AES, RC4 and others
38. Assessing key length and key distribution
39. Solving key distribution issues with asymmetric encryption
40. Generating keys
41. Encrypting with RSA
42. PGP and GnuPG
43. Evaluating Web of Trust and PKI
44. Ensuring integrity with hashes
45. Hashing with MD5 and SHA
46. Protecting data in transit
47. Building the digital signature
48. Verifying User and Host Identity
49. Assessing traditional static password schemes
50. Creating a good quality password policy to prevent password guessing and cracking
51. Protecting against social engineering attacks
52. Encrypting passwords to mitigate the impact of password sniffing
53. Evaluating strong authentication methods
54. Challenge-response to prevent man-in-the-middle attacks
55. Preventing password replay using one-time and tokenized passwords
56. Employing biometrics as part of two-factor authentication
57. Authenticating hosts
58. Shortcomings of IP addresses
59. Address-spoofing issues and countermeasures
60. Solutions for wireless networks
61. Preventing System Intrusions
62. Discovering system vulnerabilities
63. Searching for operating system holes
64. Discovering file permission issues
65. Limiting access via physical security
66. Encrypting files for confidentiality
67. Encryption with application-specific tools
68. Recovering encrypted data
69. Hardening the operating system
70. Locking down user accounts
71. Securing administrator's permissions
72. Protecting against viruses
73. Guarding Against Network Intrusions
74. Scanning for vulnerabilities
75. Restricting access to critical services
76. Preventing buffer overflows
77. Reducing denial-of-service (DoS) attacks
78. Securing DNS
79. Limiting the impact of common attacks
80. Deploying firewalls to control network traffic
81. Contrasting firewall architectures
82. Preventing intrusions with filters
83. Implementing cybersecurity policy
84. Building network firewalls
85. Evaluating firewall features
86. Selecting an architecture and a personal firewall
87. Ensuring Network Confidentiality
88. Threats from the LAN
89. Sniffing the network
90. Mitigating threats from connected hosts
91. Partitioning the network to prevent data leakage
92. Identifying wireless LAN vulnerabilities
93. Confidentiality on external connections
94. Ensuring confidentiality with encryption
95. Securing data-link layer with PPTP and L2TP
96. Middleware information assurance with SSL and TLS
97. Deploying SSH (the Secure Shell)
98. Protecting data with IPsec
99. Authenticating remote locations
100. Tunneling traffic between sites
101. Exchanging keys
102. Managing Your Organization’s Security
103. Developing a security plan
104. Responding to incidents
105. Enumerating the six critical steps

For more information or query please feel free to contact us:

**Byte Code Cyber Securities**

**Address:** 72-B, 3rd Floor,
Vikas Marg, Laxmi Nagar,
New Delhi: 110092
Near Nirman Vihar Metro Station, Opposite Pillar No.50
Telephone: +91-64601115, +91-9210001115
Website: www.bytec0de.com
Email: info@bytec0de.com