ETHICAL HACKING TRAINER

MODEL - ETHHACK100

This trainer has been designed with a view to provide practical and experimental knowledge of Ethical Hacking Technology used to prevent Cyber attacking.

SPECIFICATIONS

FEATURES

A. Introduction :

This course is designed to learn complete ethical hacking topics with real-time scenarios Welcome this Latest tactics, techniques of Complete Ethical Hacking course .This course Designed from scratch to professional with latest tools and techniques and ethical hacking concepts along with Web application, network, wireless, cloud, server, and system/endpoint based pentesting in this course you'll learn + ethical hacking modules with NO prior Experience & knowledge and end of this course you'll become a Security Expert & Pentesting Professional

This course is both theory and practical sessions first, we explain Kali Linux's complete setup, architecture, File-systems, and effective usage of commands and servers in Linux machines, then we'll give you to an ethical hacking theory party along with practical hands-on sessions and each session Tools are attached, you can learn how to install tool and practical while learning also.

You'll learn web applications, network scanning & exploitations, wireless, servers, system hacking & endpoint exploitation and cloud pentesting also we understand student view that's why we divided this course into two sections (Theory and practical).

At the end of the course you will learn latest ethical hacking tactics, techniques and tools used for hacking and penetration testing in various levels.

B. Topics covered in this course

1. Lab Setup (Kali Linux & windows VMware installation and configuration)
2. Complete kali Linux course (commands, architecture, file-system, services, and servers)
3. Practical Shell scripting & Pentesting automation scripts (you'll learn how to create automation scripts using shell scripting)
4. Understand Ethical hacking overview & Footprinting
5. Understanding network security and network scanning techniques (using NMAP, angry ip scanner, Ping, HPING other tools)
6. Understanding enumeration process and create active connections
7. System hacking (Windows, Unix using latest tools and techniques)
8. Understanding Sniffing and MITM attacks (Wireshark)

9. Understanding Social Engineering and Phising, Smishing, and Spear-phishing attacks
10. Understanding Vulnerability analysis using automation and manual
11. Denial of service and distributed denial of service attacks and mitigation process
12. Session hijacking in web applications and mitigation steps and counter attacks
13. understanding Web application pentesting and OWASP top
14. Learn Practical SQL Injection (error, boolean, time based, union, and blind Injections)
15. Understanding server exploitations and mitigation steps
16. Understanding Wireless attacks and latest tools with countermeasures
17. Understanding Android and IOS exploitation and working with backdoors to gain unauthorized access
18. Understanding Cloud attacks and deployments
19. Cryptography techniques

C. What you'll learn

1. Learn Complete Kali Linux Commands, File systems, servers, and services
2. Learn how to set up an Ethical hacking lab (Kali Linux, Windows VMs, Qualys Guard, Pentesting etc..
3. Learn how to exploit systems using payloads from Metasploit, and gain access using meterpreter
4. Learn in-depth sniffing techniques & MITM attacks (Wireshark, Filters, airodumping)
5. Learn NMAP techniques to identify the open ports, services versions and their vulnerabilities
6. Learn SQL injection to exploit web applications using latest exploits
7. You will Learn Practical Ethical Hacking and Cyber Security key concepts with practical approach
8. 18+ Ethical hacking modules with + 140 practical labs
9. Practical ethical hacking and enterprise defense tools
10. Learn Qualys Guard deployment, cloud agent, and Web application scanning
11. Learn how to hack wireless security with practical approach
12. Learn about the tools used for cracking passwords (John the Ripper, Hydra, Metasploit, Netcat)

EXPERIMENTS

1. Ethical Hacking Lab Setup

1. Course Introduction
2. Kali Linux Virtual Machine Setup
3. Windows Virtual machine setup

2. OSI Layers Explanation

4. Data Link layer
5. Network Layer
6. Transport Layer
7. Presentation Layer
8. Application Layer
9. Physical Layer
10. TCP Handhsake - Practical approach
11. Download Practical - Tools

3. Kali Linux Command-Line & Shell Scripting

12. Directories in Kali Linux
13. Services in Kali Linux
14. Servers in kali Linux
15. Users management
16. Metasploit Framework
17. Important Tools in Cyber Security
18. Cat Command
19. Cal Command (calendar)
20. CD Command
21. cmp diff Command
22. cp command (copy files)
23. Date command
24. Egrep Command
25. File Permissions
26. Find command
27. Find files by names command
28. Find files by type and perm
29. grep command
30. ls command (List)

31. Mkdir command (make the directory)
32. Modes command
33. Paste command
34. pwd command (present working directory)
35. Unix vi editor
36. rm command (to remove the files)
37. Sort command
38. touch command
39. tr command (translate)
40. Uname command
41. uniq command
42. Users_last command
43. unix filter commands
44. w command (who)
45. wc command (word count)
46. whereis command
47. whoami command
48. who command
49. who-is-logged command
50. unix communication commands
51. Shell Scripting introduction
52. Shell Scripting Command line Arguments
53. Shell Scripting operators
54. Shell scripting functions
55. Shell Scripting Control Statements
56. Shell Scripting Loops
57. Pentest automate - Project -1
58. Pentest automate - Project -2
59. Pentest automate - Project -3

4. Working with Footprinting and Reconnaissance

60. Footprinting Concepts
61. Footprinting through Search Engines
62. Footprinting through Web Services
63. Footprinting through Social Networking Sites
64. Website Footprinting

65. Email Footprinting
66. Whois Footprinting
67. DNS Footprinting
68. Network Footprinting
69. Footprinting through Social Engineering
70. Footprinting Tools
71. Footprinting Penetration Testing
72. Lab 1 - Open Source Information Gathering Using Windows Command Line Utilities
73. Lab 2 - Collecting Information About a Target Website Using Firebug
74. Lab 3 - Mirroring Website Using HTTrack Web Site Copier
75. Lab 3 - Advanced Network Route Tracing Using Path Analyzer Pro
76. Lab 5 - Information Gathering Using Metasploit
77. Download Practical Tools

5. Working with Scanning Networks and Exploiting Networks

78. Network Scanning Concepts
79. Scanning Tools
80. Scanning Techniques part -1
81. Scanning Techniques part -2
82. Scanning Beyond IDS and Firewall part -1
83. Scanning Beyond IDS and Firewall part -2
84. Banner Grabbing
85. Draw Network Diagrams
86. Scanning Pen Testing
87. Lab-01 - UDP and TCP Packet Crafting Techniques using HPING
88. Lab-02 - Scanning The Network Using The Colasoft Packet Builder
89. Lab-03 - Basic Network Troubleshooting Using MegaPing
90. Lab-04 - Understanding Network Scanning Using Nmap
91. Lab-05 - Exploring Various Network Scanning Techniques
92. Lab-06 - Scanning a Network Using NetScan Tools Pro
93. Lab-07 - Avoiding Scanning Detection using Multiple Decoy IP Addresses
94. Lab-08 - Drawing Network Diagrams Using Network Topology Mapper
95. Lab-09 - Checking for Live Systems Using Angry IP Scanner
96. Lab-10 - Scanning for Network Traffic Going Through a Computer's Adapter Using
97. Lab-11 - Identify Target System OS with TTL and TCP Window Sizes using Wireshark
98. Download Tools – Practical

6. Working with Enumeration Techniques & Exploiting Services

99. Enumeration Concepts
100. NetBIOS Enumeration
101. SNMP Enumeration
102. LDAP Enumeration
103. NTP Enumeration
104. SMTP and DNS Enumeration
105. Other Enumeration Techniques
106. Enumeration Pen Testing
107. Lab-01 - NetBIOS Enumeration Using Global Network Inventory
108. Lab-02 - Enumerating Network Resources Using Advanced IP Scanner
109. Lab-03 - Performing Network Enumeration Using SuperScan
110. Lab-04 - Enumerating Resources in a Local Machine Using Hyena
111. Lab-05 - Performing Network Enumeration Using NetBIOS Enumerator
112. Lab-06 - Enumerating a Network Using SoftPerfect Network Scanner
113. Lab-07 - Enumerating a Target Network using Nmap and Net Use
114. Lab-08 - Enumerating Services on a Target Machine
115. Lab-09 - SNMP Enumeration Using snmp_enum
116. Lab-10 - LDAP Enumeration Using Active Directory Explorer (ADExplorer)
117. Lab-11 - Enumerating information from Windows and Samba host using Enumlinux
118. Download Tools – Practical

7. Exploiting Systems and Hacking Points

119. System Hacking Concepts
120. Cracking Passwords part -1
121. Cracking Passwords part -2
122. Cracking Passwords part -3
123. Escalating Privileges
124. Steganography
125. Penetration Testing
126. Lab-01 - Dumping Cracking SAM Hashes to Extract Plaintext Passwords
127. Lab-02 - Auditing System Passwords Using LOphtCrack
128. Lab-04 - Hacking Windows using Metasploit, and Post-Exploitation using Meterpr
129. Lab-05 - Web Activity Monitoring and Recording using Power Spy

130. Lab-06 - Hiding Files Using NTFS Streams
131. Lab-07 - Hiding Data Using White Space Steganography
132. Lab-08 - Image Steganography Using Openstego
133. Download tools to explore and practice

8. Working with Practical Wireshark

134. Wireshark Installation
135. Wireshark Features
136. Working with Wireshark
137. Useful filters
138. Regular Expressions - 1
139. Regular Expressions - 2
140. Packet Colorization
141. Hex Values
142. ICMP ping-sweep Walkthrough
143. ICMP ping-sweep Practical
144. Wifi Packet analysis
145. TCP Reverse Shell - Walkthrough
146. performing registry entry monitoring
147. TCP Handshake
148. Startup Program Monitoring
149. Stealth Scan - NMAP detection
150. Null Scan - NMAP detection
151. HTTP Steal credentials from unencrypted channels
152. HTTP Tunneling
153. ARP - Address resolution protocol (Detecting arp packets)
154. Detecting Suspicious Downloads in your network
155. Download Wireshark Tool

9. Working with Malwares, Trojans, Backdoors, Rootkits and Virus Detection

156. Malware Concepts
157. Trojan Concepts part -1
158. Trojan Concepts part -2
159. Trojan Concepts part -3
160. Virus and Worm Concepts part -1
161. Virus and Worm Concepts part -2

162. Virus and Worm Concepts part -3
163. Malware Analysis part -1
164. Malware Analysis part -2
165. Malware Analysis part -3
166. Countermeasures
167. Anti-Malware Software
168. Malware Penetration Testing
169. Lab-01 - Gaining Control Over a Victim Machine Using njRAT
170. Lab-02 - Creating a Virus Using the JPS Virus Maker Tool
171. Lab-03 - Creating a Worm Using Internet Worm Maker Thing
172. Lab-04 - Virus Analysis Using OllyDbg
173. Lab-05 - Detecting Trojans
174. Lab-06 - Monitoring TCP/IP Connections Using the Currports
175. Lab-07 - Performing Registry Entry Monitering
176. Lab-08 - Startup Program Monitering Tool
177. Download Practical Tools

10. Sniffing and Man-in-the-Middle Attacks

178. Sniffing Techniques part -1
179. Sniffing Techniques part -2
180. Sniffing Techniques part -3
181. Sniffing tools
182. Sniffing Detection Techniques
183. Sniffing Pen Testing
184. Lab01 - Sniffing Passwords Using Wireshark
185. Lab-02 - Spoofing MAC Address Using SMAC
186. Lab-03 - Performing Man-in-the-Middle Attack using cain & Abel
187. Lab-04 - Detecting ARP Attacks with XArp Tool
188. Download Practical Tools

11. Working with Social Engineering

189. Social Engineering Concepts
190. Social Engineering Techniques
191. Insider Threats
192. Impersonation on Social Networking Sites
193. Identity Theft

194. Lab-01 - Sniffing Website Credentials Using Social Engineering Toolkit (SET)

12. Working with Denial-of-Service and DDOS Attack

195. DOS/DDoS Concepts
196. DOS/DDOS Attack Techniques
197. Botnets
198. DDoS Case Study
199. DoS/DDOS Attack Tools
200. DoS/DDoS Protection Tools
201. DoS/DDoS Penetration Testing
202. Lab-01 - SYN Flooding a Target Host Using Metasploit
203. Lab-02 - SYN Flooding a Target Host Using hping
204. Lab-03 - Performing Distributed Denial of Service Attack Using HOIC

13. Web Application Vulnerability Assessment and Penetration testing

205. Web App Concepts
206. Web App Threats
207. Web App Hacking Tools
208. Countermeasures
209. Web App Security Testing Tools
210. Web App Pen Testing
211. Lab-01 - Exploiting Parameter Tampering and XSS Vulnerabilities in web Application
212. Lab-02 - Enumerating and Hacking a Web Application Using WPScan and Metasploit
213. Lab-03 - Exploiting Remote Command Execution Vulnerability to Compromise a Target
214. Lab-04 - Exploiting File Upload Vulnerability at Different Security Levels
215. Lab-05 - Performing Cross-Site Request Forgery (CSRF) Attack

14. Exploiting SQL Injection Vulnerabilities (Practical Approach)

216. SQL Injection Concepts
217. Types of SQL Injection
218. SQL Injection Methodology part
219. SQL Injection Methodology part
220. SQL Injection Tools
221. Evasion Techniques
222. Lab-01 - SQL Injection Attacks on an MS SQL Database

223. Lab02 - Scanning Web Applications Using N-Stalker Tool

15. Hacking Wireless Networks

224. Wireless Concepts
225. Wireless Encryption
226. Wireless Threats
227. Wireless Hacking Tools
228. Wireless Hacking Methodology part -1
229. Wireless Hacking Methodology part -2
230. Bluetooth Hacking
231. Wireless Security Tools
232. Wireless Pen Testing
233. Lab-01 - WiFi Packet Analysis using Wireshark
234. Lab-02 - Cracking a WEP with Aircracking
235. Lab-03 - Cracking a WPA (Wi-Fi Protected Access) with Aircracking

16. Working Hacking Mobile Platforms

236. Mobile Platform Attack Vectors
237. Hacking Android OS part -1
238. Hacking Android OS part -2
239. Hacking iOS
240. Mobile Spyware
241. Mobile Device Management
242. Mobile Security Guidelines and Tools
243. Mobile Pen Testing
244. Lab-01 - Creating Binary Payloads using Kali Linux to Hack Android
245. Lab-02 - Harvesting the user's credentials using the Social Engineering

17. Working with Cryptography Techniques

246. Cryptography Concepts
247. Encryption Algorithms
248. Cryptography Tools
249. Public Key Infrastructure (PKI)
250. Email Encryption
251. Disk Encryption
252. Cryptanalysis

253. Lab-01 - Calculating One-Way Hashes Using HashCalc
254. Lab-02 - Calculating MD5 Hashes Using MD5 Calculator
255. Lab-03 - Creating and Using Self-Signed Certificate
256. Lab-04 - Basic Disk Encryption Using VeraCrypt

18. Web application Scanning - QualysGuard

257. Qualys Web Application overview
258. Qualys Knowledge base and search lists
259. Basic Web application setup
260. Scheduled Scans
261. Option profile
262. Web Application knowledge base
263. Tagging
264. User management
265. WAS site map
266. WAS Search lists
267. WAS Reporting

19. Qualys Vulnerability Management (VM)

268. Vulnerability Management Introduction
269. Account & Application setup
270. Qualys Knowledge Base
271. Lab-01 - Account Setup & Application
272. Knowledge base & Search Lists
273. Lab-02 - Working with Knowledge base
274. Lab-03 - Working with SeachLists
275. Lab-04 - Working with Asset tags
276. Lab-05 - Working with Asset Search
277. Asset & Asset inventory
278. Asset Groups
279. Asset Tagging
280. Using Asset tags
281. Using Asset groups
282. Lab-Working with Asset groups
283. Scan by Hostname
284. Vulnerability Assessment

285. VM Life cycle and Sensors
286. Lab-06 - Working with Vulnerability Assessment
287. Lab-07 - Authentication Records
288. Lab-08 - Launch Scan
289. Scan Configuration
290. Scheduling Assessment Scans
291. View Scan results
292. Lab-09 - Scheduled Scans
293. User management
294. Lab-10 - Creating user account
295. Vulnerabilities Remediation
296. Lab-11 - Assign Vulnerability to User.
297. Lab-12 - Ignore Vulnerabilities
298. Lab-Create Remediation Report
299. Report overview
300. Report Templates
301. Lab-13 - Reporting
302. Lab-14 - Scheduled Reports
303. Lab-15 - Custom Report templates

CLASS ROOM TRAINING – ONLINE AND OFFLINE

The training includes Single user Classroom / laboratory teaching, learning and simulation software module. The content has easy explanation of various complex topics with animation and simulation for ease of student learning. It also supports learning through videos, graphs, charts, along with mandatory rich content and theory to understand fundamental concepts, interactive learning objects, FAQ, MCQ etc. The content is supplied in digital online access or license protection.

Contact US

Registered Office

SIGMA TRAINERS AND KITS
E-113, Jai Ambe Nagar,
Near Udgam School,
Drive-in Road,
Thaltej,
AHMEDABAD-380054. INDIA.

Factory

SIGMA TRAINERS AND KITS
B-6, Hindola Complex,
Below Nishan Medical Store,
Lad Society Road,
Near Vastrapur Lake,
AHMEDABAD-380015. INDIA.

Contact Person
Prof. D R Luhar – Director
Mobile : 9824001168
Whatsapp : 9824001168

Phones:
Office : +91-79-26852427
Factory : +91-79-26767512
+91-79-26767648
+91-79-26767649

E-Mails :
sales@sigmatrainers.com
drluhar@gmail.com