Cyber Security, Ethical Hacking & Information Security Course Syllabus

Course Brochure

1) **Understanding Ethical Hacking and Cybersecurity, various domains of Information Security.**
   - Different types of penetration testing, various information security standards, key issues pertaining in today's information security world and various technologies used to suffice information security requirements.
2) Deep dive into Networking and understanding the OSI layer and protocols.
   - **TCP Packets, IP Packets, TCP/IP 3 way handshaking, OSI layer in details, various other protocols, ports and services.**
3) Understanding the concepts behind Kali Linux OS and various ethical hacking tools.
   - **Information Gathering tools, social networking tools, social engineering tools, password bruteforcers, reverse engineering tools etc.**
4) Hands-on into Foot printing and Reconnaissance.
   - **Perform footprinting and reconnaissance using the latest footprinting techniques and tools.**
5) Demonstration of conducting Network scanning using tools like Nmap.
   - **Nmap various command usage and nse scripts.**
6) Learning Vulnerability Assessment and using tools like Nexpose, OpenVAS for discovering vulnerabilities.
   - **How to configure and run the tools for vulnerability assessment, generate reports etc.**
7) Sniffing network traffic and understanding the packet flow using tools like Wireshark.
   - **Wireshark promiscuous and non-promiscuous mode, network traffic capture and analysis of network packet.**
8) Understanding Cryptography Concepts, Encryption Algorithms, Cryptography Tools like gnupg, bcrypt etc, Public Key Infrastructure (PKI), Email-Encryption, Disk Encryption.
   - **Ciphers, Difference between encoding, encryption and hashing, Different types of encryption, public and private keys, encrypting files using gnupg and bcrypt encryptions, performing disk encryption.**
9) Understanding the usage of Social Engineering techniques and tools like Social Engineer Toolkit (SET).
   - **Learning social engineering techniques and using Social engineer tools to launch social engineering attacks.**
10) Learning about Denial of service/Distributed Denial of service concepts, tools and botnets.
    - **DoS/DDoS attack techniques and tools to asses a target and DoS/DDoS countermeasures.**
11) Understanding Malware/Ransomware, Trojan, Virus and Worms? Anti-malware Software, Malware Creation Tool and USB Password Stealers.
    - **Different types of malware (Trojan, Virus, worms, etc.), performing system auditing for malware attacks, malware analysis, and countermeasures.**
12) Understanding Wireless Concepts and Types of Wireless networks, Wireless Hacking Techniques and Hacking Tools like Aircrack-ng, Reaver, Crunch, Machanger etc., Wireless Encryption, Threats and Security Tools.
13) Understanding the Concepts of Firewall, Web application firewall, IDS, IPS and Honeypots.
    - **Firewall, IDS and honeypot evasion techniques, evasion tools and techniques.**

14) Learning the concepts of Internet of Things (IOT) and OWASP top 10 IOT vulnerabilities.
    - **What is Internet of Things (IOT), different IOT products and top 10 vulnerabilities in IOT systems and remediation techniques.**
15) Deep dive into different cloud environments like SAAS/IAAS/PAAS. Steps to conduct Cloud security assessment.
    - **Vulnerabilities in cloud applications and remediation measures.**

16) Understanding the System hacking methodology, usage of Metasploit framework and usage to hack a system and gain meterpreter session.
17) Understanding the concepts of web application and its components like HTML, CSS, JS, Content management systems like Drupal, Wordpress etc.
18) Steps or Procedures needs to be adopted for conducting web application penetration testing activities. What are false positives and false negatives?
19) Learning threat profiling of the vulnerabilities. Concepts of different vulnerability scoring/rating methodologies like DREAD, CVSS score etc.
20) Deep dive into HTTP protocol and HTTP status codes.
    - About HTTP protocol
    - HTTP status codes like 100, 200, 300, 400 and 500 series
    - HTTP request methods like GET, POST, TRACE, PUT, HEAD, DELETE etc.
21) Understanding the OWASP Top 10 vulnerabilities and practical demonstration of web application vulnerabilities.
    - SQL injection
    - XSS
    - Session Management Flaws
    - Server Misconfiguration
    - XXE
    - Malicious File Upload
    - Insecure Deserialization
    - LFI, RFI
    - Bruteforce attacks and many more

22) Deep dive into different modules present in Burpsuite like Intruder, Repeater, Sequencer, Decoder, Comparer, Extender etc. Sub domain scanners, crawlers, directory busters, brute forcing tools like Hydra to be covered.
23) Learning SQL injection attack techniques in details, Different types of SQL injection, injection detection tools (SQLmap) to detect SQL injection exploits, and countermeasures to prevent SQL injection.

24) Session hijacking techniques to discover network-level session management, authentication/authorization, cryptographic weaknesses, and countermeasures.
25) Conducting automated web application scanning using open source tools like OWASP Zap.
26) Learning concepts of SOAP and REST APIs. Differences between them.
27) Learning the steps to conduct manual API security assessment. Practical Demonstration of API vulnerabilities exploitation using sample application like dvws node app and OWASP Top 10 API list.
    - Broken Object Level Authorization
    - Broken User Authentication
    - Excessive Data Exposure
    - Lack of Resources & Rate Limiting
    - Broken Function Level Authorization
    - Mass Assignment
    - Security Misconfiguration
    - Injection Flaws
    - Improper Assets Management
28) Understanding the Mobile app penetration testing overview. Learning Static secure code analysis of mobile apps using tools like MOBSF and Dynamic security testing of mobile apps
29) Introduction to Information Security Governance and Risk Management.
30) CIA triad, Risk analysis using formulas like Single Loss Expectancy, Annual Rate of Occurrence (ARO), Annualized Loss Expectancy (ALE) etc.
31) Information security standards like PCI DSS, ISO 27001, HIPPA, SOX, FISMA etc.

Prerequisite Tools:

1) KALI LINUX VM
2) Bwapp application downloaded from http://www.itsecgames.com/
3) Windows 10 VM from https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/
4) VMWare workstation player