Cyber Security, Ethical Hacking & Information Security Course Syllabus

APPONIX academy SINCE 2013

Course Brochure

Introduction to Cybersecurity

- CIA Triad, Separation of Duties, Org Structure, Top Down and Bottom-up approach

Information Availability

- Recovery Time Objective/Recovery Point Objective/Maximum Tolerable Downtime, SLA

Disclosure, Alteration and Destruction of Data

IAAAA protocols

- Identification, Authentication, Authorization, Accountability and Auditing

Corporate Governance and Plans

- Introduction to corporate Governance, Strategic, Tactical and Operational Plans, Policies, Standards, Procedures and Guidelines

Data Protection Mechanism

- Data Layering, Abstraction, Data Hiding, Encryption

Data Classification methodologies

- Confidential, Sensitive, Top Secret, Private, Public, Unclassified

Risk Management

- Asset Management, Threat and Vulnerability, Threat, Threat Agent, Exploit, Quantitative and Qualitative Risk Assessment

Risk Management lifecycle

- Assessment, Analysis, Mitigation and Response

Risk Management Framework

- ISO27001, ISO31000, ISO27000, Steps involved in risk management framework

Internal Controls

- Preventive, Detective and Corrective controls

Threat Identification Model

- STRIDE
- DREAD

Disaster Recovery and Business Continuity Management

- Contingency Plans, BCP documentation and DR documentation, Types of tests

Information Systems Laws

- Criminal, Civil and Administrative laws, Computer Security Act, Computer Fraud and Abuse Act, Government Information Security Reform Act, Federal Information Security Management Act

Information Systems Regulations

- PCI-DSS, GDPR, HIPAA, Hi-Trust, SOX, ISO series etc.

Intellectual Property

- Copyright, Trademark, Patents, Trade Secrets

Data Security Controls and Data ownership

- Data in Use, Data in Rest, Data in Transit, Data Custodian, Data Processor, Data Controller, System owners, Administrators, End Users

Data Destruction Mechanism

- Sanitize, Degaussing, Erase, Overwrite

Security Architecture Framework and Security Models

- Zachman Framework, Sherwood Applied Business Security Architecture (SABSA), Information Technology Infrastructure Library (ITIL), State Machine Models, Multilevel Lattice Models, Information Flow Models

Mobile Security

- Device Encryption
- Remote wiping
- Remote lock out
- Internal locks (voice, face recognition, pattern, pin, password)
- Application installation control
- Asset tracking (IMIE)
- Mobile Device Management
- Removable storage (SD CARD, Micro SD etc.)

IoT and Internet Security

- Network Segmentation (Isolation)
- Logical Isolation (VLAN)
- Physical isolation (Network segments)
- Application firewalls
- Firmware updates

Physical Security

- Various threats to Physical Security

System Virtualization

- Guest OS, Virtualization Threats, Cloud Computing Models, Cloud Computing Threats

Web Security

- OWASP, OWASP Top 10, SQL Injection, XSS, CSRF

Cryptography

- Goals of Cryptography, Symmetric and Asymmetric Encryption, Decryption, Digital Signature, Hashing, Cryptography Algorithms (DES, AES, IDEA, two fish)

Network Security

- OSI Model, Attacks in OSI Layers, Network Types, Network Methods and Standards, Hardware devices, VPN protocols,

Firewall and Perimeter security

- Firewall, Types of Firewalls, DMZ, Honey Pot, Honey Net

Different types of Network attacks

- Virus, Worms, Logic Bomb, Trojan, Backdoor, Sniffing, Zero Day attack, Ransomware, Rootkit, Spyware, DoS, DDos, Botnet etc.

Email Security

- LDAP, SASL, S/MIME

Identity and Access Management

- 3 factor authentication, SSO, Authorization, Federated Identity, Access Control Models, Access Control Categories, Access control types

Vulnerability Assessment and Pen Test

- Steps involved, Test Types, Test Strategies, Reporting

Software Development and Testing

- Development Models, Development lifecycle, Testing types, Code review and testing

Security Operations and Incident Management

- Evidence Life Cycle, IDS, IPS, Backup, SIEM, Hardening Process

Threat Hunting and Attack Framework

- Cyber Kill Chain Process, Mitre Attack framework, Threat Hunting benefits

Social Engineering attacks

- Phishing, Spear Phishing, Whaling, Piggybacking, Watering Hole

Assessment and Knowledge test

Viva and Interview preparation