CYBROTACADEMY

Enterprise Information Security

support@cybrotacademy.com | www.cybrotacademy.com

DESCRIPTION

Cybersecurity attacks continue to grow at a rapid pace. Therefore, more job roles are required to equip with baseline security readiness and response to modern-day security threats. Welcome to this comprehensive course on Fundamentals of Cyber Security. This Session covers all the objectives of the baseline security certificates including the principles of protecting a system against attack and managing risk. Important topics such as access control, identity management and cryptography will be covered in detail. These baseline Cybersecurity skills applicable across most of today's job roles.

AUDIENCE

- **Anybody interested in learning cyber security**
- **Any Beginner who wants to start Job in cyber security.**
- **Trainer who are willing to start teaching Cyber Security.**
- **Any cyber security professional and student.**
- **Ethical Hackers who want to learn fundamentals of cyber security.**
- **Beginners in Cyber Security Industry for Analyst Position**
- **Anyone who is preparing for CompTIA Security+ Certification**

PROGRAM FEATURES

- 45 hours of instructor-led training
- Course completion certificate
- Study Material
- Life Time Access to recorded Session
- Weekend as well as weekdays classes

COURSE CURRICULAM

Threats, Attacks and Vulnerabilities

1. Overview and Introduction
2. What is Threat, Attack and Vulnerability?
3. Difference between Threat, Attack and Vulnerability with example.
4. Security concerns associated with different types of vulnerabilities.
5. Get familiar with Cloud-based vs. on-premises infrastructure and vulnerabilities.
6. Malware and types
7. Host Threats
8. Weak Configurations
9. Third-Party Risks
10. Improper or weak patch management.

Governance, Risk, and Compliance:

11. CIA Triad
12. Security Principles
13. Threat Actors
14. Risk and Enterprise Risk Management
15. Complete Guide to the Risk Assessment Process
16. ISO 27001 and ISO 27005
17. Security controls and it's type
18. Security Principles
19. IT Security Governance
20. Security Policies
21. Frameworks
22. Quantitative Risk Calculations
23. Business Impact Analysis
24. Third-Party Agreements

Securing the System

25. Host Threats
26. System Resiliency
27. RAID
28. NAS and SAN
29. IDS and IPS
30. DAM
31. DLP
32. EPO
33. Data Destruction
34. SIEM
35. LOG Management Cycle

Understand Corporate Network Infrastructures

36. LAN vs MAN vs WAN
37. Network Topologies Review
38. Network Devices
39. DMZ
40. Network Access Controls
41. Firewalls and their types
42. Proxy Servers
43. Honeypots
44. Virtual Private Networks
45. NIDS NIPS
46. Cloud and Types and their security
47. Demo of Network Topology

Operations and Incident Response

36. Business Continuity Process
37. Disaster Recovery
38. Incident Response
39. Contingency Planning
40. Backups

Infrastructure Testing

41. Passive and Active Reconnaissance
42. Vulnerability Assessment Process
43. Penetration Testing Process
44. Vulnerability Scanning Tools

Cryptography and PKI

45. Introduction to Cryptography
46. Cryptosystems
47. Cryptographic Methods
48. Public Key Infrastructure
49. Hashing
50. Steganography
51. Digital Signal
52. Cryptographic Attacks

Identity and Access Management (IAM)

53. Introduction to Access Management overview

54. Different types of Identity Management

55. Single Sign On

56. Difference between Authentication and authorization

Course Instructor

Aman Dubey is an Information Security researcher and founder of cybrot.com and cybrotacademy.com . He has done Master of Cyber law and Information Security from National Law University Bhopal. He holds CEH and ISO 27001 LA/LI certificates. Currently he is working in the global security department of a renowned organization. His area of expertise includes Information Security Audits, Risk Assessment and Application Security.

Teamcybrot