SecureHack
Making Internet Safe

Advance Implementation of Cyber Security (AICS)

Introduction:

Starting from the basics, this cybersecurity course provides a solid foundation for students from any stream at any level entering the field. No prior knowledge or experience is required, making it accessible to beginners who are eager to learn. The course begins by emphasizing the significance of cybersecurity in today's interconnected world. The course has been designed with a practical approach so that students will gain a clear understanding of the threats and attack vectors that jeopardize our digital systems and personal information. These topics cover the foundational aspects of cybersecurity and provide a solid understanding of key concepts, technologies, and practices.

Course outcome: The course outcomes of these topics aim to equip students with the knowledge and skills necessary to understand, mitigate, and respond to cybersecurity threats effectively. Upon completing the training program, students should be able to implement security measures, assess risks, protect data, and contribute to a secure computing environment.

Mode: Online/Offline

Duration: 6 Months

System Requirements:

Operating System:
Windows 10, macOS, or Linux (based on the training program and tools being used)
Processor:
Intel Core i5 or equivalent (or higher)
RAM:
Minimum of 8 GB RAM (16 GB or higher recommended for better performance)
Storage:
At least 256 GB of available storage space
Network Connectivity:
Ethernet or Wi-Fi capability for internet access and networking tasks
Virtualization:
If virtualization software like VMware or VirtualBox is used, the system should support hardware virtualization technology (e.g., Intel VT-x or AMD-V)

Tools :

1. **Virtualization Software:**
   VMware Workstation
   VirtualBox
2. **Network Security Tools:**
   Wireshark
   Nmap
   tcpdump
3. **Penetration Testing Tools:**
   Metasploit Framework
   Kali Linux (including its various tools)
4. **Intrusion Detection and Prevention Systems (IDS/IPS)**
   Snort
5. **Forensics and Incident Response Tools:**
   EnCase
   Autopsy

Course Content:

1. **Introduction to Cybersecurity**
   Overview of cybersecurity concepts, principles, and challenges.
   Introduction to different types of cyber threats and attacks.
2. **Basic of Linux**
   Installation of Linux
   Basic commands
   Introduction of Linux and tools
3. **Basic networks**
   Important protocols and their header in-depth
   TCP
   UDP
   IP
   ICMP
   Ports and their basic

4. **Network Security**
   Fundamentals of network security.
   Network architecture and design considerations.
   Network security protocols and encryption techniques.
5. **Operating System Security**
   Securing different operating systems (Windows, Linux, macOS).
   User management and access controls.
   Patch management and software updates.
6. **Application Security**
   Web application security principles.
   Common web vulnerabilities and secure coding practices.
   Application security testing techniques.
7. **Data Security and Privacy**
   Data classification and protection.
   Encryption techniques and data loss prevention strategies.
   Privacy laws and regulations.
8. **Security Operations and Incident Management**
   Security operations center (SOC) functions and roles.
   Incident response planning and procedures.
   Threat intelligence and analysis.
9. **Risk Management and Compliance**
   Risk assessment and management methodologies.
   Compliance frameworks and security auditing.
   Business continuity and disaster recovery planning.
10. **Ethical Hacking**
    Introduction to ethical hacking.
    Wi-Fi ethical hacking and security.
11. **Penetration Testing**
    Penetration testing methodologies and tools.
    Vulnerability assessment and exploitation techniques.
12. **Cryptography and Cryptanalysis**
    Principles of cryptography and encryption.
    Cryptographic algorithms and protocols.
    Cryptanalysis techniques and countermeasures.
13. **Wireless Network Security**
    Securing wireless networks (Wi-Fi) and mitigating risks.

Wireless network encryption protocols.
Wireless intrusion detection and prevention systems (WIDS/WIPS).

14. Cloud Security

Introduction to cloud computing security.
Cloud deployment models and security considerations.

15. Incident Response and Digital Forensics

Incident response processes and procedures.
Digital forensics principles and techniques.
Preservation and analysis of digital evidence.

16. Social Engineering and Physical Security

Understanding social engineering techniques.
Mitigating social engineering attacks through awareness and training.
Physical security measures and access controls.

17. Mobile Security

Mobile device security threats and vulnerabilities.
Mobile application security best practices.
Mobile device management and security policies**.**

18. Network Defense and Intrusion Detection

Network defense strategies and techniques.
Intrusion detection systems (IDS) and intrusion prevention systems (IPS).
Network traffic analysis and incident response.

19. Industrial Control Systems (ICS) Security

Introduction to industrial control systems and their security challenges.
ICS security frameworks and standards.
Securing critical infrastructure and SCADA systems.

20.Virtualization and Cloud Security

Virtualization technologies and security considerations.
Cloud security risks and countermeasures.
Securing virtual environments and hypervisors.