Arjunvision
Vision that leads you

4-Week Introduction to Cyber Security Course Syllabus

- **Week 1: Fundamentals of Cyber Security**

- Day 1: Introduction to Cyber Security - Definition and importance of cyber security - Key concepts: confidentiality, integrity, and availability (CIA triad) - Types of cyber threats and attacks
- Day 2: Cyber Security Terminologies - Understanding malware: viruses, worms, trojans - Phishing, social engineering, and other attack vectors - Common vulnerabilities and exposure (CVE)
- Day 3: Networking Basics for Cyber Security - Basic networking concepts: IP addresses, DNS, TCP/IP - Firewalls, routers, and switches - Network security principles
- Day 4: Cyber Security Tools and Techniques - Introduction to encryption and cryptography - Authentication methods: passwords, biometrics, multi-factor authentication - Overview of security tools: antivirus, IDS/IPS, VPNs

Week 2: Threats and Attack Vectors

Day 5: Malware and Ransomware

- Deep dive into malware types and behavior

- Ransomware: how it works and prevention strategies

- Case studies of recent malware attacks

Day 6: Social Engineering Attacks

- Types of social engineering attacks: phishing, spear phishing, baiting

- Techniques to identify and prevent social engineering
- Real-world examples and case studies

Day 7: Network Security Threats

- Common network attacks: DoS, DDoS, Man-in-the-Middle (MitM)
- Securing wireless networks
- Network security monitoring and incident response

Day 8: Web Application Security

- Introduction to web application vulnerabilities: SQL injection, XSS, CSRF
- Secure coding practices and OWASP Top 10
- Web application firewalls (WAFs) and their role

Week 3: Defensive Cyber Security

Day 9: Endpoint Security

- Securing desktops, laptops, and mobile devices
- Endpoint protection strategies and tools
- Patching and vulnerability management

Day 10: Identity and Access Management (IAM)

- Understanding IAM: concepts and components
- Role-based access control (RBAC) and least privilege principle
- IAM solutions and best practices

Day 11: Incident Response and Recovery

- Incident response lifecycle: preparation, detection, containment, eradication, recovery
- Creating an incident response plan
- Disaster recovery and business continuity planning

Day 12: Cyber Security Frameworks and Compliance

- Introduction to NIST, ISO/IEC 27001, GDPR, and other frameworks
- Importance of compliance in cyber security

- Auditing and risk management

Week 4: Advanced Topics and Practical Application

Day 13: Cloud Security

- Understanding cloud security challenges
- Best practices for securing cloud infrastructure
- Cloud security tools and services

Day 14: Penetration Testing and Ethical Hacking

- Introduction to penetration testing: tools and techniques
- Ethical hacking concepts and methodologies
- Conducting vulnerability assessments

Day 15: Emerging Threats and Future Trends

- Overview of emerging cyber threats: AI-driven attacks, IoT vulnerabilities
- The future of cyber security: quantum computing, blockchain
- Preparing for future challenges in cyber security

Day 16: Final Project and Review

- Hands-on project: setting up a secure network or conducting a vulnerability assessment
- Review and wrap-up: key takeaways and next steps
- Final assessment and certification