Course Name: Cybersecurity for Beginners

CONTENTS

Course Name: Cybersecurity for Beginners

About the course: The Cybersecurity for Beginners course is designed to provide learners with a strong foundation in networking concepts, cybersecurity fundamentals, and Security Operations Center (SOC) practices. The programme introduces learners to cyber threats, network security mechanisms, ethical hacking basics, and incident response processes through a blend of theory and hands-on practical sessions. By the end of the course, learners will be equipped with the skills required to understand, monitor, and protect IT systems against cyber threats and pursue entry-level cybersecurity roles.

Programme Outcomes:

Upon successful completion of the course, learners will be able to:

1. Understand core networking concepts and protocols
2. Identify common cyber threats, vulnerabilities, and attack vectors
3. Understand SOC operations and incident response workflows
4. Work with firewalls, IDS/IPS, VPNs, and endpoint security tools
5. Perform basic vulnerability assessment and ethical hacking tasks
6. Analyze logs and security alerts for threat detection
7. Apply cybersecurity best practices in real-world scenarios

Eligibility Criteria: Pursuing/ completed Graduation/ Diploma in IT or related field

- Students / Graduates
- Basic computer knowledge is preferred
- Suitable for beginners with no prior cybersecurity background

Duration of the programme: 65 Hours (Theory 35 Hours / Practical 30 Hours / Mini project 5 Hours)

Mode of Training : Online

Course Syllabus

Module 1 – Introduction to Cybersecurity

Unit 1 – Cybersecurity and its applications
Introduce learners to the concept of cybersecurity, its importance in the digital era, and its applications across industries, enabling awareness of cyber risks and protection mechanisms.

Module 2 – Network Devices: Purpose & Functions

Unit 1 – Overview of network components and devices
Explain the purpose and functionality of cables, connectors, NICs, repeaters, hubs, bridges, switches, and routers, enabling learners to understand basic network infrastructure and data flow.

Module 3 – OSI and TCP/IP Models

Unit 1 – Introduction to networking models
Introduce the concept of networking models, their purpose, and the need for standardized communication frameworks.

Unit 2 – Model representation and implementation
Explain how networking models are represented and implemented in real-world communication systems.

Unit 3 – OSI model layers and functions
Describe each layer of the OSI model, their functions, and role in network communication.

Unit 4 – Computer addressing formats
Introduce addressing mechanisms used in networks to identify devices and services.

Unit 5 – Binary, decimal, and hexadecimal conversions
Enable learners to perform number system conversions essential for networking and cybersecurity.

Unit 6 – Encapsulation and Protocol Data Units (PDU)
Explain data encapsulation and the role of PDUs in layered communication.

Unit 7 – MAC addressing (OUI & Vendor Assigned)
Introduce MAC addresses, their structure, and role in device identification.

Unit 8 – Comparison of OSI and TCP/IP models
Compare OSI and TCP/IP models to help learners understand similarities, differences, and practical relevance.

Module 4 – TCP/IP Protocol Suite

Unit 1 – Protocol header fields and functions
Explain TCP, UDP, IPv4, IPv6, Ethernet, ARP, and ICMP protocols, focusing on header fields and their functional roles.

Module 5 – Enterprise Network Infrastructure Design

Unit 1 – Network fundamentals and classification
Introduce network concepts, functions, types, and classifications.

Unit 2 – Enterprise network designs (CAN, DC, WAN)
Explain campus, data center, and wide-area network architectures used in enterprises.

Unit 3 – Network design models
Introduce 2-tier, 3-tier, and spine–leaf design models used in modern enterprise networks.

Module 6 – IPv4 Basics

Unit 1 – IPv4 addressing fundamentals
Explain IP classes, subnet masks, prefixes, network bits, and host bits.

Unit 2 – Network and host calculations
Teach calculation of number of networks, hosts, network address, broadcast address, first and last host addresses.

Module 7 – Class C Subnetting

Unit 1 – Public and private IP addressing
Introduce public and private IP address ranges and their usage.

Unit 2 – CIDR notation and subnet calculations
Explain CIDR, network bits, subnet bits, and address planning.

Unit 3 – Subnet masks and magic number concept
Teach subnet mask calculation and magic number methodology.

Unit 4 – Subnet address calculations
Cover first and last subnet network and broadcast address calculations.

Unit 5 – Full subnet range table (FRT)
Guide learners in creating and using subnet range tables.

Unit 6 – Host address allocation
Explain host address distribution within subnets.

Module 8 – FLSM, VLSM & IPv6 Basics

Unit 1 – Fixed and Variable Length Subnet Masking
Explain FLSM and VLSM concepts and their practical applications.

Unit 2 – Introduction to IPv6
Introduce IPv6 addressing, structure, and benefits over IPv4.

Module 9 – BD / CD Exercises

Unit 1 – Learning on broadcast domains and collision domains
Exploring concepts of broadcast domains and collision domains in detail

Module 10 – SOC Concepts

Unit 1 – Security roles, responsibilities, and CIA model
Introduce security roles, responsibilities, terminologies, and the CIA models.

Unit 2 – Network security controls and devices

Explain firewalls (NGFW), IDS/IPS, VPNs, ISE (AAA), WSA, ESA, and endpoint security.

Unit 3 – Operating system security
Cover Windows and Unix/Linux security fundamentals.

Unit 4 – Web application fundamentals
Introduce basic web application architecture and security considerations.

Module 11 – Security Operations and Management

Unit 1 – Security management and operations
Explain security governance and operational practices.

Unit 2 – Security Operations Center (SOC)
Introduce SOC concepts, structure, and objectives.

Unit 3 – SOC operations and workflows
Explain SOC workflows and daily operational processes.

Unit 4 – SOC components and models
Describe people, process, technology, and different SOC models.

Unit 5 – SOC implementation
Explain steps involved in implementing and operating a SOC.

Module 12 – Cyber Threats and Attack Methodology

Unit 1 – Cyber threats and attacker intent
Introduce cyber threats and attacker motivations.

Unit 2 – Tactics, Techniques, and Procedures (TTPs)
Explain attacker methodologies and behavior patterns.

Unit 3 – Vulnerabilities and weaknesses
Explain how vulnerabilities are identified and exploited.

Unit 4 – Indicators of Compromise (IoCs)
Teach identification of compromise indicators.

Unit 5 – Hacking methodologies
Introduce ethical and malicious hacking methodologies.

Module 13 – Incidents, Events, and Logging

Unit 1 – Security incidents and events
Differentiate between incidents and events.

Unit 2 – Logging fundamentals
Explain logs, their necessity, and typical formats.

Unit 3 – Logging approaches
Introduce centralized and distributed logging mechanisms.

Module 14 – Threat Intelligence and Incident Response

Unit 1 – Threat intelligence-driven SOC
Explain the importance of threat intelligence in SOC operations.

Unit 2 – Vulnerability management
Cover vulnerability scanning, remediation, and patching.

Unit 3 – Ethical hacking basics
Introduce ethical hacking concepts and tools.

Module 15 – Incident Response

Unit 1 – Incident response teams and collaboration
Explain IRT roles and collaboration with SOC.

Unit 2 – Incident response process
Introduce incident response lifecycle and handling procedures.

Module 16 – Mini Project

Enable learners to apply networking and cybersecurity concepts through a guided mini project, including implementation, documentation, and presentation.

Certification process: After completing the course and submitting the mini project the students have to attend a final assessment. Upon successful completion of the final assessment the students will be certified.

Certificate awarded by: ASAP Kerala