Duration: 6 Months

DIPLOMA IN CYBERSECURITY

Overview:

The Diploma in Cyber Security and Ethical Hacking is a comprehensive program designed to equip participants with the knowledge and skills required to pursue a career in cybersecurity. The course covers a wide range of topics including Linux fundamentals, networking basics, programming with Python, advanced ethical hacking techniques, penetration testing methodologies for web, mobile, and network environments, as well as security considerations for cloud and Internet of Things (IoT) technologies.

What you'll learn

➢ In this module, you will learn the foundational principles of Linux operating systems, mastering essential commands and administration tasks.

➢You'll delve into the basics of networking, understanding IP addressing, protocols, and network configurations.

➢ Additionally, you'll gain proficiency in Python programming, covering syntax, data structures, and automation techniques.

➢ Furthermore, you'll advance into the realms of ethical hacking, exploring penetration testing methodologies across web, mobile, and network domains.

➢Lastly, you'll explore the intricate landscapes of cloud computing and IoT security, understanding the unique challenges and strategies to safeguard digital assets in modern computing environments.

Benifits

➢**Hands-on practical:** Engage in real-world exercises to apply theoretical knowledge directly.

➢**Internship opportunity:** Gain practical experience through internships to enhance skills and build a professional network.

➢**Expert trainers:** Receive guidance and instruction from seasoned professionals with extensive experience in the field.

➢**Job assistance:** Access support and resources to secure employment opportunities aligned with acquired skills. and expertise.

You can reach us at:

www.cyberous.in
info@cyberous.in
cyberous_
cyberous

Month :- 1

LINUX FUNDAMENTALS

Course Outline:

Module 01: Linux Basics

- History and philosophy
- Different distributions
- Command line interaction

Module 02: File System Navigation

- Commands: cd, pwd, ls
- Permissions
- Manipulating files: mkdir, touch, rm, mv

Module 03: File Manipulation

- Text editing: nano, vim
- Searching: grep
- Compression: gzip, tar, zip

Module 04: User and Group Management

- Commands: useradd, usermod, passwd
- Permissions
- Group management

Module 05: Process Management

- Commands: ps, top, kill
- Background and foreground processes
- Priority and scheduling: nice, renice

Module 06: Package Management

- Package managers: apt, yum, pacman
- Searching and repositories
- Dependencies and conflicts

Module 07: Networking Basics

- Configuration: ifconfig, ip
- Troubleshooting
- Protocols: TCP/IP

Module 08: System Administration

- Services: systemctl, service
- Startup/shutdown
- Performance monitoring

Module 09: Shell Scripting

- Scripting basics
- Variables, conditionals, loops
- Task automation

Module 10: File System Permissions

- Ownership and permissions
- chmod
- chown, chgrp

Module 11: Text Processing Tools

- sed, awk
- Text manipulation
- Regular expressions

Module 12: File System Hierarchy

- Structure overview
- Important directories
- Navigation

Module13: Backup and Restore

- Backup tools: tar, rsync
- Strategies
- Restoration

Module 14: File System Integrity

- Checksums
- Error detection and repair
- Journaling

Module15: Security Essentials

- Firewalls
- Authentication
- Log monitoring

Module 16: Remote Access

- SSH
- File transfer: SCP, SFTP
- Remote desktop

Module 17: System Updates and Upgrades

- Package
- updates System
- upgradesRepositories

Module 18: Shell Customization

- Prompt customization
- Aliases, functions
- Configuration files

Module 19: Virtualization and Containers

- Virtualization: VirtualBox, VMware
- Containers: Docker, Podman
- Management

Module 20: Monitoring and Performance Tuning

- Performance tools: sar, vmstat
- Bottleneck identification
- System tuning

Month :- 2

BASIC OF NETWORKING

Course Outline:

Module 01: Networking Basics

- OSI/TCP/IP models
- LAN/WAN/WLAN
- Networking devices: routers, switches, modems

Module 02: Network Protocols

- TCP/IP suite: IPv4, IPv6, TCP, UDP
- Application layer: HTTP, FTP, SMTP
- Data link layer: Ethernet, ARP

Module 03: IP Addressing

- IPv4: classes, subnetting, CIDR
- IPv6: addressing scheme, types
- DHCP: dynamic IP allocation

Module 04: Routing and Switching

- Routing: tables, protocols
- Switching: MAC, VLANs
- Protocols: OSPF, BGP, RIP

Module 05: Network Security

- Firewalls: types
- VPN: tunneling, encryption
- IDS/IPS: detection, prevention

Module 06: Wireless Networking

- Wi-Fi standards: 802.11
- Security: WPA, WPA2
- Access points, SSIDs

Module 07: Network Services

- DNS: resolution
- DHCP: IP allocation
- NAT: address translation

Module 08: Network Troubleshooting

- Ping, traceroute
- Wireshark: traffic analysis
- Connectivity issues

Module 09: Network Design

- Scalability, redundancy
- Topologies: star, mesh
- VLANs, virtual switches

Module 10: Quality of Service (QoS)

- Bandwidth management
- Traffic prioritization
- QoS techniques: shaping, scheduling

Module 11: Network Monitoring

- SNMP: management protocol
- Monitoring tools: Nagios
- Performance metrics: throughput, latency

Module 12: Cloud Networking

- VPC setup
- Direct Connect, ExpressRoute
- Hybrid cloud networking

Module 13: SDN

- Architecture
- OpenFlow
- Use cases

Module 14: Network Virtualization

- VLANs
- VPNs
- NFV

Module 15: Network Access Control (NAC)

- Authentication
- Deployment
- Solutions/vendors

Module 16: Network Performance Optimization

- Bandwidth optimization
- Traffic shaping
- Load balancing

Module 17: IPv6 Implementation

- Addressing
- Transition
- Adoption challenges

Module 18: VoIP and Unified Communications

- VoIP protocols
- Unified comms platforms
- QoS for VoIP

Module 19: Network Automation

- Configuration management
- Automation frameworks
- Benefits, challenges

Module 20: IoT Networking

- IoT protocols
- Security considerations
- Scalability challenges

Month :- 3

BASIC OF PYTHON

Course Outline:

Module 01: Python Basics
- Syntax and data types
- Control flow
- Functions and modules

Module 02: Data Structures
- Lists, tuples, dictionaries
- Operations and methods
- Mutability and immutability

Module 03: File Handling
- Opening, reading, writing
- files Exception handling
- Context managers

Module 04: Object-Oriented Programming (OOP)
- Classes and objects
- Inheritance
- Encapsulation, polymorphism

Module 05: Pythonic Idioms
- List comprehensions
- Generators, iterators
- Decorators

Module 06: String Manipulation

- String methods
- String formatting
- Regular expressions

Module 07: Exception Handling

- Try-except blocks
- Handling specific exceptions
- Finally block

Module 08: Debugging Techniques

- Print statements
- Debugging tools: pdb
- Tracebacks

Module 09: Functional Programming

- Lambda functions
- Map, filter, reduce
- Recursion

Module 10: Concurrency and Parallelism

- Threading, multiprocessing
- Thread synchronization
- GIL

Module 11: Database Interaction

- SQLite, ORM frameworks
- CRUD operations
- Connection management

Module 12: Web Development with Python

- Flask, Django frameworks
- Routing, views
- Templating engines

Module 13: API Integration

- RESTful APIs
- HTTP requests: requests library
- Authentication, authorization

Module 14: Data Analysis and Visualization

- Pandas: data manipulation
- Matplotlib, Seaborn: plotting
- Jupyter Notebooks

Module 15: Testing in Python

- Unit testing: unittest
- Test-driven development
- (TDD) Mocking, patching

Module 16: Python Packaging and Distribution

- Creating packages
- PyPI distribution
- Virtual environments

Module 17: Asynchronous Programming

- Asyncio library
- Async/await syntax
- Event loops, coroutines

Module 18: Machine Learning with Python

- Scikit-learn: ML algorithms
- TensorFlow, PyTorch: deep learning
- Model evaluation, deployment

Module 19: Deployment and Automation

- Creating executables
- Docker containerization
- CI/CD pipelines: Jenkins, GitLab CI

Module 20: Documentation and Best Practices

- Docstrings
- PEP 8: style guide
- Code review, version control

Month :- 4

ADVANCE ETHICAL HACKING

Course Outline:

Module 01: Ethical Hacking Fundamentals
- Ethical concepts
- Legal considerations
- Distinction from malicious hacking

Module 02: Footprinting and Reconnaissance
- Information gathering
- OSINT tools
- Footprinting methodologies

Module 03: Scanning Networks
- Port scanning
- Network mapping
- Vulnerability scanning

Module 04: Enumeration
- Service enumeration
- User enumeration
- SNMP enumeration

Module 05: System Hacking
- Exploiting vulnerabilities
- Privilege escalation
- Password cracking

Module 06: Malware Threats

- Types of malware
- Malware analysis
- Antivirus evasion

Module 07: Sniffing and Spoofing

- Packet sniffing
- ARP/DNS spoofing
- Sniffing tools

Module 08: Social Engineering

- Psychological manipulation
- Phishing
- Social engineering toolkits

Module 09: Web Application Hacking

- SQL injection
- XSS
- Session hijacking

Module 10: Wireless Network Hacking

- WLAN security
- Cracking keys
- Rogue APs

Module 11: Evading IDS, Firewalls, Honeypots

- IDS evasion
- Firewall evasion
- Honeypot detection

Module 12: Cryptography

- Encryption algorithms
- Cryptanalysis
- Steganography

Module 13: Penetration Testing Methodologies

- Planning
- Execution
- Reporting

Module 14: Post-Exploitation Techniques

- Maintaining access
- Covering tracks
- Pivoting

Module 15: IoT Hacking

- Device vulnerabilities
- Exploitation.
- Penetration testing

Module 16: Cloud Computing Security

- Cloud infrastructure flaws
- AWS/Azure/GCP security
- Cloud pen testing

Module 17: Mobile Application Hacking

- Android/iOS security
- Reverse engineering
- Exploiting vulnerabilities

Module 18: Physical Security

- Social engineering attacks
- Lock picking
- Physical security audits

Module 19: Red Team Operations

- Simulating attacks
- Covert ops
- Adversarial tactics

Module 20: Ethical Hacking Best Practices

- Responsible disclosure
- Continuous learning
- Upholding ethical standards

Month :-5

PENTERATION TESTING

Course Outline:

Module 01: Introduction to Penetration Testing

- Methodologies & Principles Overview
- Cybersecurity Importance
- Hands-on Demonstrations

Module 02: Legal and Ethical Considerations

- Laws, Regulations, Ethics
- Ethical & Legal Guidelines
- Case Studies on Legal Issues

Module 03: Web Application Basics

- Architecture & Components
- Common Protocols
- Interactive Web App Lab

Module 04: Web Application Penetration Testing

- Identify & Exploit Vulnerabilities
- Tools & Methodologies
- Practical Web App Testing Exercises

Module 05: Mobile Application Basics

- Architecture & Platforms
- Security Considerations
- Mobile App Development Overview

Module 06: Mobile Application Penetration Testing

- Assess Security
- Vulnerabilities & Attacks
- Mobile App Testing Lab

Module 07: Network Fundamentals

- TCP/IP, OSI Model
- Infrastructure Basics
- Network Configuration Lab

Module 08: Network Penetration Testing

- Identify & Exploit Vulnerabilities
- Tools & Methodologies
- Network Pen Testing Simulation

Module 09: Wireless Network Security

- Risks & Securing
- Testing Techniques
- Wireless Network Lab

Module 10: Social Engineering

- Techniques & Mitigation
- Countermeasures
- Social Engineering Simulation

Module 11: Physical Security Assessment

- Controls & Vulnerabilities
- Unauthorized Access
- Physical Security Assessment Lab

Module 12: Reporting and Documentation

- Best Practices
- Writing Reports
- Report Writing Workshop

Module 13: Post-Exploitation Techniques

- Maintaining Access
- Cleanup & Remediation
- Post-Exploitation Scenario Analysis

Module 14: Incident Response and Handling

- Response Process
- Roles & Responsibilities
- Incident Response Simulation

Module 15: Penetration Testing Tools

- Popular Tools Overview
- Hands-on Exercises
- Tool Integration Lab

Module 16: Advanced Penetration Testing Techniques

- Advanced Exploits
- Red Teaming
- Advanced Exploitation Lab

Module 17: Case Studies and Practical Exercises

- Real-world Examples
- Hands-on Labs
- Live Penetration Testing Engagements

Month :-6

CLOUD AND IoT SECURITY

Course Outline:

Module 01: Introduction to Cloud Computing

- Overview of cloud computing models (IaaS, PaaS, SaaS)
- Understanding cloud deployment models (public, private, hybrid)
- Benefits and challenges of cloud computing

Module 02: IoT Fundamentals

- Introduction to Internet of Things (IoT) architecture and components
- IoT communication protocols (e.g., MQTT, CoAP)
- Common IoT devices and use cases

Module 03: Security Challenges in Cloud Computing

- Data breaches and data loss in cloud environments
- Insider threats and unauthorized access
- Compliance and regulatory concerns

Module 04: Security Considerations for IoT Devices

- Limited computational resources and constrained environments
- Firmware and software vulnerabilities
- Physical security of IoT devices

Module 05: Cloud Security Controls

- Identity and access management (IAM) in the cloud
- Encryption and key management for data protection
- Network security measures (firewalls, VPNs) in cloud environments

Module 06: Securing IoT Networks

- Network segmentation for IoT devices
- Authentication and authorization mechanisms
- Secure bootstrapping and provisioning

Module 07:Cloud Data Security

- Data classification and encryption
- Secure data storage and backup strategies
- Data loss prevention (DLP) in the cloud

Module 08: IoT Data Privacy

- Privacy implications of IoT data collection and processing
- GDPR and other privacy regulations relevant to IoT
- Anonymization and pseudonymization techniques

Module 09: Cloud Security Monitoring and Incident Response

- Intrusion detection and prevention systems (IDPS)
- Logging and auditing in cloud environments
- Incident response planning and execution

Module 10: IoT Device Lifecycle Management

- Secure device provisioning and onboarding
- Patch management and firmware updates
- Decommissioning and disposal of IoT devices

Module 11: Cloud Service Provider Security

- Evaluating cloud service provider security measures
- Service level agreements (SLAs) and security responsibilities
- Third-party risk management in cloud environments

Module 12:IoT Authentication and Authorization

- Role-based access control (RBAC) for IoT devices
- Mutual authentication and certificate-based authentication
- Access control policies and enforcement

Module 13: Cloud Compliance and Governance

- Regulatory compliance frameworks (e.g., HIPAA, PCI DSS)
- Auditing and compliance monitoring in cloud environments
- Cloud governance best practices

Module 14: Secure Cloud Migration Strategies

- Planning and executing cloud migration securely
- Risk assessment and mitigation during
- migration Data sovereignty and jurisdiction considerations

Module 15: IoT Security Standards and Frameworks

- Overview of IoT security standards (e.g., NIST IoT Cybersecurity Framework, ISA/IEC 62443)
- Implementing security-by-design principles in IoT development
- Conformance testing and certification programs

Module 16: Cloud Disaster Recovery and Business Continuity

- Backup and recovery strategies for cloud-based services
- Disaster recovery planning and testing
- Ensuring business continuity in the event of cloud service disruptions

Module 17: IoT Communication Security

- Secure communication protocols and encryption techniques
- Securing wireless IoT communications (e.g., Wi-Fi, Bluetooth, Zigbee)
- Man-in-the-middle (MITM) attack prevention

Module 18: Cloud Security Automation and Orchestration

- DevSecOps principles for cloud security
- Continuous integration and deployment (CI/CD) pipelines for security
- Security automation tools and frameworks

Module 19: IoT Security Testing

- Vulnerability assessment and penetration testing of IoT devices
- Fuzzing and reverse engineering IoT protocols
- Red teaming exercises to assess IoT device security posture

Module 20: Emerging Trends in Cloud & IoT Security

- Edge computing and its security implications
- Quantum computing and its impact on cloud and IoT security
- AI and machine learning for threat detection and mitigation in cloud and IoT environments