# Diploma in Cybersecurity

Duration: 6 Month

## Overview:

Our comprehensive cybersecurity training program covers a range of essential topics to equip participants with the skills and knowledge needed to excel in the field. From mastering Linux fundamentals to delving into web and network penetration testing,mobille app security participants gain hands-on experience in identifying vulnerabilities and securing systems. They also learn about bug bounty programs, mobile application penetration testing, and corporate training initiatives, preparing them for real-world challenges. Culminating in a Diploma in Cybersecurity, this program ensures a well- rounded understanding of cybersecurity principles and practices, empowering graduates to thrive in today's evolving threat landscape.

### What you'll learn:

➢Aspiring cybersecurity professionals seeking a comprehensive understanding of cybersecurity principles and practices.

➢ IT professionals specializing in Linux fundamentals, web, and network penetration testing, aiming to enhance their skills and credentials.

➢Bug bounty hunters interested in formalizing their knowledge and gaining a broader perspective on cybersecurity.

➢ Mobile application developers and testers looking to specialize in mobile application penetration testing.

➢ Corporate teams responsible for enhancing their organization's cybersecurity posture through structured training and education initiatives.

### Target Audience:

The Diploma in Cybersecurity training course will significantly benefit:

➢The Diploma in Cybersecurity training course caters to security officers.

➢ethical hackers, network administrators, engineers.

➢system administrators, and individuals focused on network integrity.

### Prerequisite Knowledge:

➢ Participants in this course are assumed to be familiar with a foundational understanding of computer systems and networks.

## You can reach us:


Cyberous

info@cyberous.in

cyberous_

@Cyberous

Month :-1

# Linux Fundamentals Modules

## Course Outline:

### Module 01 Introduction to Linux

- History: Linus Torvalds, GNU
- Project Distributions: Ubuntu,
- Fedora, CentOS Components: Kernel, GNU utilities, Shell

### Module 02  Fundamentals of Command Line

- Navigation: cd, ls, pwd
- File Operations: cp, mv, rm
- Input/Output Redirection: >, >>, <

### Module 03: File System Hierarchy

- Root Directory: /
- Special Directories: /bin, /etc, /home, /var
- File Permissions: chmod, chown, chgrp

### Module 04: User and Group Management

- User Administration: useradd, usermod, userdel
- Group Administration: groupadd, groupmod,
- groupdel User Permissions: sudo, su, chown

### Module 05: Package Management

- Package Installation: apt, yum, dnf
- Package Queries: dpkg, rpm
- Dependency Management: apt-get, yum, dnf

### Module 06: Networking Basics

- Network Configuration: ifconfig, ip
- Network Troubleshooting: ping, traceroute,
- netstat Network Services: systemctl, service, netstat

## Module 07: Process Management

- Process Identification: ps, pgrep,
- pidof Process Manipulation: kill,
- pkill, killall Process Prioritization: nice, renice, top

## Module 08: Shell Scripting

- Script Creation: touch, nano, vim
- Variable Usage: $var, ${var}, environment
- variables Conditional Statements: if, else, elif

## Module 09: System Administration Basics

- Service Management: systemctl,
- service System Monitoring: top, htop, free
- Backup Tools: rsync, tar, dd

## Module 10: Security Fundamentals

- User Authentication: passwd, su, sudo
- File Permissions: chmod, chown, chgrp
- Firewall Configuration: iptables, firewalld, ufw

## Module 11: Text Processing Tools

- sed, awk.
- Text manipulation. Regular expressions.

## Module 12: File System Hierarchy

- Structure overview.
- Important directories. Navigation.

## Module 13: Backup and Restore

- Backup tools: tar, rsync.
- Strategies.
- Restoration.

## Module 14:File System Integrity

- Checksums.
- Error detection and repair.
- Journaling.

## Module 15: 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 upgrades.
- Repositories.

## Module 18:Shell Customization

- Prompt customization.
- Aliases, functions.
- Configuration files.

## Module 19: Virtualization and Containers

- Virtualization: VirtualBox, VMware.
- ontainers: Docker, Podman.
- Management.

## Module 20: Monitoring and Performance Tuning

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

Month :-2

# Network Penetration Testing Modules

## Course Outline:

### Module 1: Reconnaissance

- Network Discovery
- ServiceEnumeration OS
- Fingerprinting

### Module 2: Vulnerability Scanning

- Automated Scanning
- Manual Verification
- Patch Management Review

### Module 3: Exploitation

- Exploit Development
- Privilege Escalation
- Post-Exploitation Activities

### Module 4: Password Cracking

- Password Hash Retrieval
- Password Cracking Techniques
- Password Policy Assessment

### Module 5: Wireless Security Assessment

- Wireless Network Discovery
- Wireless Protocol Analysis
- Wireless Authentication Testing

### Module 6: Social Engineering

- Phishing Attacks
- Phone-based Attacks
- Physical Security Testing

### Module 7: Network Device Testing

- Router and Switch Configuration
- Review Firewall and IDS/IPS Testing
- VPN Security Assessment

## Module 8: Traffic Analysis

- Packet Capture
- Protocol Analysis
- Anomaly Detection

## Module 9: DNS Security Assessment

- DNS Enumeration
- DNS Cache Poisoning
- DNSSEC Implementation Review

## Module 10: Reporting and Remediation

- Vulnerability Reporting
- Remediation Recommendations Prioritization of Remediation Efforts Post-Testing Validation
- Continuous Monitoring

## 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

# Web Penetration Testing Modules

## Course Outline:

### Module 1: Information Gathering

- Domain Enumeration
- Web Application Discovery
- Open Source Intelligence (OSINT) Network Mapping
- Technology Profiling

### Module 2: Vulnerability Analysis

- Automated Scanning Manual Testing
- Source Code Review
- Fingerprinting
- Threat Modeling

### Module 3: Authentication and Session Management

- Authentication Testing
- Session Management Testing Password Cracking
- Cookie Manipulation
- CAPTCHA Bypassing

### Module 4: Authorization Testing

- Role-Based Access Control (RBAC)
- Insecure Direct Object References (IDOR)
- Privilege Escalation
- Business Logic Testing

### Module 5: Session Management and Security Configuration

- Session Fixation
- Session Timeout
- Security Headers
- Secure Cookie Flags
- HTTP Strict Transport Security (HSTS)

## Module 6: Data Validation and Input Handling

- Input Validation Testing
- Output Encoding
- File Upload Security
- SQL Injection Testing
- NoSQL Injection Testing

## Module 7: Error Handling and Logging

- Error Handling Testing
- Logging and Monitoring
- Error-based SQL Injection
- Information Leakage
- Testing Stack Trace Analysis

## Module 8: Client-Side Security

- Cross-Site Scripting (XSS)
- Cross-Origin Resource Sharing (CORS)
- Content Security Policy (CSP)
- Clickjacking Testing
- Browser Extension Analysis

## Module 9: API Security

- API Authentication
- Input Validation
- Rate Limiting and Throttling
- API Parameter Manipulation
- Business Logic Flaws in APIs

## Module 10: Reporting and Remediation

- Vulnerability Reporting
- Remediation Guidance
- Retesting
- Secure Coding Guidelines
- Incident Response Planning

## Module 11:Social Engineering Testing

- Phishing.
- Pretexting.
- Physical bypass.

## Module 12: Physical Security Testing

- Tailgating.
- Lock picking.
- Physical assessments.

## Module 13:Cloud Infrastructure Testing

- Security configurations.
- IAM permissions.
- Data exposure testing.

## Module 14:Mobile Application Testing

- iOS/Android security.
- Reverse engineering.
- API security.

## Module 15: IoT Testing

- Device vulnerabilities.
- Protocol exploitation.
- Network reconnaissance.

## Module 16: Red Team Exercises

- Real-world simulations.
- Defensive capability assessment.
- Incident response evaluation.

## Module 17: Report Writing and Documentation

- Findings documentation.
- Vulnerability prioritization.
- Remediation recommendations.

## Module 18: . Continuous Testing and Monitoring

- Continuous testing implementation.
- Vulnerability monitoring.
- Security posture assessment.

## Module 19: Advanced Techniques and Tools

- Exploitation advancements.
- Custom tool development.
- Exploit creation.

## Module 20: Ethical and Professional Conduct

- Ethical adherence.
- Professionalism.
- Confidentiality respect.

Month :-4

# Bug Bounty Modules

## Course Outline:

### Module 1: Platform Selection

- Choose a bug bounty platform.
- Review program policies and rewards.

### Module 2: Scope Identification

- Define program scope and testing techniques.
- Specify allowed targets and prohibited activities.

### Module 3: Target Reconnaissance

- Gather information about the target organization.
- Identify potential attack vectors.

### Module 4: Vulnerability Discovery

- Assess vulnerabilities using automated and manual testing.
- Identify security flaws like SQL injection and XSS.

### Module 5: Exploitation and Proof of Concept

- Develop proof-of-concept exploits.
- Verify exploitability and impact.

### Module 6: Submission and Reporting

- Document findings accurately.
- Submit reports following program guidelines.

### Module 7: Communication and Collaboration

- Maintain open communication with the organization.
- Collaborate with program administrators.

### Module 8: Rewards and Recognition

- Receive monetary rewards or recognition.
- Participate in acknowledgments.

## Module 9: Vulnerability Remediation

- Work with the organization to resolve vulnerabilities.
- Verify remediation effectiveness.

## Module 10: Continuous Learning and Improvement

- Stay updated on security threats.
- Participate in bug bounty community events.

## Module 11: Legal and Ethical Considerations

- Adhere to ethical guidelines and legal requirements.
- Obtain appropriate authorization.

## Module 12: Feedback and Program Evaluation

- Provide feedback for program improvement.
- Evaluate bug bounty experiences.

## Module 13:Rewards and Incentive Structures

- Reputation and Recognition Systems
- Bug Severity and Reward Correlation

## Module 14:Non-Monetary Rewards and Recognition

- Access to Exclusive Resources and Tools
- Professional Development Opportunities

## Module 15: Custom Rewards Tailored to Individual Hunter Preferences

- Preference Assessment and Profiling
- Flexible Reward Options

## Module 16: Educational Opportunities as Rewards

- Training Workshops and Webinars
- Certification Programs

## Module 17:Access to Exclusive Resources or Tools

- Specialized Vulnerability Scanning Tools:
- Private Bug Bounty Program Invitations:

## Module 18: Invitation to Private Programs as a Reward

- Higher Payout Opportunities:
- Access to Exclusive Targets:

## Module 19:Feedback and Mentorship as Incentives

- Personalized Feedback on Submissions:
- Technical Guidance and Support:

## Module 20:Transparent Reward Structures to Build Trust and Motivation

- Clear and Consistent Reward Guidelines:
- Publicly Available Reward Tiers and Payout Scales:

Month :-5

# Mobile Application Penetration Testing Modules

## Course Outline:

### Module 1: Pre-Assessment Preparation

- Understand app purpose and platforms.
- Obtain necessary permissions.
- Define testing objectives and scope.

### Module 2: Reconnaissance

- Gather app information.
- Analyze network traffic.
- Identify API endpoints and backend infrastructure.

### Module 3: Static Analysis

- Review source code for vulnerabilities.
- Check third-party libraries for security issues.
- Assess data storage mechanisms and encryption.

### Module 4: Dynamic Analysis

- Test runtime behavior for vulnerabilities.
- Assess server-side security controls.
- Evaluate session management and token handling.

### Module 5: Authentication and Authorization

- Test authentication mechanisms thoroughly.
- Evaluate authorization controls for weaknesses.
- Assess multi-factor authentication implementation.

### Module 6: Data Storage and Transmission

- Evaluate local data storage security.
- Assess data transmission over network protocols.
- Check for insecure data caching mechanisms.

## Module 7: Input Validation and Injection

- Test all input fields for injection vulnerabilities.
- Validate input data to prevent exploitation.
- Assess client-side and server-side input validation.

## Module 8: Session Management

- Review session handling mechanisms.
- Test for session fixation and hijacking vulnerabilities.
- Assess session timeout and token rotation policies.

## Module 9: Cryptography

- Assess cryptographic algorithms and key management.
- Check for insecure storage of cryptographic keys.
- Evaluate SSL/TLS implementation for security.

## Module 10: API Security

- Test API endpoints for security vulnerabilities.
- Assess API authentication mechanisms.
- Evaluate API rate limiting and throttling.

## Module 11: Push Notification and Cloud Integration

- Evaluate push notification security mechanisms.
- Assess cloud storage and integration security.
- Review permissions and access controls.

## Module 12: Reverse Engineering and Code Review

- Reverse engineer app binary for vulnerabilities.
- Perform static and dynamic code analysis.
- Check for sensitive information leakage.

## Module 13: Device-specific Security

- Test for device-specific vulnerabilities (e.g., jailbreak/root detection).
- Assess app behavior under different device configurations.
- Evaluate app's adherence to platform-specific security guidelines.

## Module 14: Inter-Component Communication

- Test security of inter-component communication channels.
- Assess broadcast receivers, content providers, and intents for vulnerabilities.
- Check for insecure data sharing between app components.

## Module 15: Client-Side Security

- Assess client-side security mechanisms.
- Evaluate app permissions and data access controls.
- Check for insecure data storage on the device.

## Module 16: Offline Security

- Test app security in offline mode.
- Assess data encryption and protection mechanisms when offline.
- Evaluate app behavior when network connectivity is lost.

## Module 17: Webview Security

- Assess security of webviews within the app.
- Check for vulnerabilities such as XSS and CSRF.
- Evaluate webview configuration and sandboxing.

## Module 18: Error Handling and Logging

- Assess error handling mechanisms.
- Review logging practices for security issues.
- Check for sensitive information leakage in error messages.

## Module 19: Biometric Security

- Test biometric authentication mechanisms.
- Assess biometric data storage and protection.
- Evaluate resistance to biometric spoofing attacks.

## Module 20: Localization and Internationalization

- Test app behavior under different language and region settings.
- Assess security implications of localization and internationalization features.
- Check for vulnerabilities related to language-specific inputs.

Month :-6

# Corporate Training Modules

## Course Outline:

### Module 1: Onboarding Training

- Introduction to company culture and policies.
- Familiarization with job roles and expectations.

### Module 2: Compliance Training

- Legal and regulatory requirements.
- Data privacy and workplace safety.

### Module 3: Technical Skills Training

- Software tools and job-specific skills.
- Coding and IT certifications.

### Module 4: Soft Skills Training

- Communication and leadership skills.
- Time management and problem-solving.

### Module 5: Customer Service Training

- Active listening and conflict resolution.
- Building rapport and empathy.

### Module 6: Sales and Marketing Training

- Sales techniques and digital marketing.
- Product knowledge and CRM.

### Module 7: Project Management Training

- Planning and risk management.
- Agile methodologies and communication.

### Module 8: Financial Literacy Training

- Understanding financial statements.
- Budgeting and risk management.

## Module 9: Cybersecurity Awareness Training

- Phishing awareness and secure practices.
- Remote work security and updates.

## Module 10: Change Management Training

- Adapting to organizational changes.
- Effective communication of change.

## Module 11: Team Building and Collaboration

- Trust-building and teamwork.
- Conflict resolution and accountability.

## Module 12: Innovation and Creativity Training

- Idea generation and design thinking.
- Encouraging experimentation and risk-taking.

## Module 13: Performance Management and Feedback

- Goal setting and constructive feedback.
- Performance appraisals and recognition.

## Module 14: Remote Work and Virtual Collaboration

- Remote tools and time management.
- Cybersecurity and work-life balance.

## Module 15: Ethical Conduct and CSR

- Ethics and corporate values.
- Social responsibility and sustainability.

## Module 16: Health and Wellness Programs

- Stress management and mindfulness.
- Fitness and mental health support.

## Module 17: DEI Training

- Bias awareness and inclusivity.
- Celebrating diversity and accessibility.

## Module 18: Leadership Development

- Executive coaching and strategic planning.
- Leadership skills for change and growth.

## Module 19: Continuing Education

- Professional certifications and workshops.
- Ongoing skill development and conferences.

## Module 20: Evaluation and Feedback

- Assessing training effectiveness and surveys.
- Continuous improvement based on data.