Duration: 2 Months

NETWORK PENETRATION TESTING

Overview:

Network penetration testing mimics cyberattacks on a company's network infrastructure to uncover vulnerabilities and evaluate its security stance. Testers utilize diverse techniques to exploit weaknesses in systems, applications, and configurations, furnishing organizations with critical insights to fortify their defense strategies and alleviate risks. This training voucher delivers thorough guidance on executing penetration tests, empowering participants with the expertise required to shield networks from looming threats effectively.

What you'll learn

➢In the Network Penetration Testing module, you will learn how to identify and exploit vulnerabilities in network infrastructure, such as routers, switches, and servers.

➢You'll gain hands-on experience with tools and techniques for port scanning, vulnerability assessment, and exploitation.

➢Additionally, you'll develop the skills to conduct thorough penetration tests, assess network security posture, and provide actionable recommendations for remediation.

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

Course Outline:

Module 01: Understanding Network Security

- Importance
- Threat landscape
- Security objectives

Module 02: Firewalls

- Types (stateful, stateless)
- Access control lists (ACLs)
- IDS/IPS

Module 03: Network Segmentation

- VLANs
- Subnetting
- DMZ setup

Module 04: Encryption

- VPN
- SSL/TLS
- IPsec

Module 05: Access Control

- User authentication
- RBAC
- NAC

Module 06: Wireless Security

- WPA3/WPA2
- SSID hiding
- MAC filtering

Module 07: Network Monitoring

- Traffic analysis
- Log monitoring
- Behavior analysis

Module 08: Intrusion Detection/Prevention

- Signature-based
- Anomaly-based
- Real-time blocking

Module 09: Vulnerability Management

- Scanning
- Patching
- Updates

Module 10: Network Hardening

- Service disablement
- Least privilege
- Strong passwords

Module 11: DNS Security

- DNSSEC
- Filtering
- DDoS protection

Module 12: Network Forensics

- Incident response
- Analysis
- Evidence gathering

Module 13: Virtualization Security

- Hypervisor security
- VM isolation
- Migration security

Module 14: Cloud Network Security

- Firewall setup
- API security
- Data transfer security

Module 15: Network Access Control (NAC)

- Compliance checks
- Authentication
- Access enforcement

Module 16: Secure Protocols

- SSH
- HTTPS
- SNMPv3

Module 17: Network Device Security

- Router/switch hardening
- Firmware updates
- Access control

Module 18: Web Application Firewalls (WAF)

- Protection
- Filtering
- Updates

Module 19: BYOD Security

- MDM
- Containerization
- Data segregation

Module 20: Network Security Best Practices

- Audits
- Training
- Incident response planning