Duration: 2 Month

Network Penetration Testing Modules

Overview:

Performing network penetration testing involves simulating cyber attacks on a company's network infrastructure to identify vulnerabilities
and assess its security posture. Testers employ various techniques to exploit weaknesses in systems, applications, and configurations, providing organizations with
valuable insights to bolster their defense mechanisms and mitigate potential risks. This training voucher offers comprehensive instruction on conducting penetration
tests, equipping participants with the skills needed to safeguard networks against potential threats.

What you'll learn:

➢In a network penetration test, I will gather insights into the security posture of the target network by identifying vulnerabilities, assessing their severity, and exploiting them to gain unauthorized access.

➢Through thorough analysis, I aim to provide actionable recommendations to bolster the network's defenses

➢Mitigate potential risks effectively.

Target Audience:

The Network Penetration Testing training course will significantly benefit:

➢The Network Penetration Testing Training course caters to security officers.

➢Ethical hackers, Network administrators, engineers.

➢Network 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

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.