Kore Infotech
Intelligent IT Solutions
Passionate People

Advanced Network Security Course

This **Advanced Network Security** course provides an in-depth understanding of how to secure, monitor, and test network infrastructures against evolving cyber threats. Learners will gain practical experience in network scanning, vulnerability assessment, intrusion detection, and penetration testing techniques using industry-standard tools such as Nmap, Wireshark, Snort, and proxy analyzers.

The course also covers firewalls, IDS/IPS configuration, network topology discovery, and troubleshooting methods essential for maintaining a secure network environment. By the end of this course, participants will be equipped to identify vulnerabilities, analyze risks, and implement effective defence mechanisms to safeguard networked systems.

Who Should Attend This Course:

This course is ideal for:

- **Network administrators** and **system engineers** responsible for securing IT infrastructure.
- **Cybersecurity professionals** and ethical hackers seeking practical skills in network defence and penetration testing.
- **IT support technicians** and students in computer science or information technology aiming to build a foundation in network security operations.

Pre-Requisites:

- Basic understanding of computer networks and operating systems.
- Familiarity with TCP/IP concepts and general IT infrastructure.
- Prior exposure to command-line interfaces and networking tools is recommended but not mandatory.

Course Duration:

This course will be conducted over a period of 4 Days (9.30 am to 5.30 pm)

Objectives:

1. **Understand core concepts of network security** — goals, functions, and best practices for protecting communication systems.
2. **Identify and analyze network threats and attacks**, including password attacks, spoofing, ARP poisoning, and malware intrusions.
3. **Perform network scanning and sniffing** using tools like Nmap and Wireshark to detect vulnerabilities and suspicious activities.
4. **Conduct vulnerability assessments and penetration tests** on internal and external networks following structured methodologies.
5. **Configure and test firewalls, IDS, and IPS** to detect, prevent, and respond to network intrusions effectively.
6. **Monitor and troubleshoot network performance** using system monitoring, traffic analysis, and reporting tools.

Kore Infotech
Intelligent IT Solutions
Passionate People

Course Content

1. **Network Security**
   - 1.1. Overview of Network Security
   - 1.2. The need for network security
   - 1.3. The goals of network security
   - 1.4. Security awareness
   - 1.5. Functions of Network security
   - 1.6. administrator
   - 1.7. Network Security at Transmission
   - 1.8. Security

2. **Network Attacking Terminology**
   - 2.1. Network Security Best Practices
   - 2.2. Network Attacks
   - 2.3. Social Engineering
   - 2.4. Identifying Network Attacks
   - 2.5. Looking at Password Attacks
   - 2.6. System Security Threats
   - 2.7. Identifying Physical Threats
   - 2.8. Looking at Malicious Software
   - 2.9. Threats Against Hardware

3. **User and End System Authentication**
   - 3.1. Desktop Firewall
   - 3.2. Centralized Policy Management
   - 3.3. Automatic Policy Updating
   - 3.4. Role and Time Based Network Access Control
   - 3.5. Activity and Network Log

4. **Network Scanning and Sniffing**
   - 4.1. Check for Live Systems by using Ping, Ping Sweep
   - 4.2. Check for Open and Closed Ports using Nmap
   - 4.3. Various Scanning Techniques by using Nmap
   - 4.4. Network Scanning Tools
   - 4.5. Understanding MAC Attacks
   - 4.6. Understanding DHCP Attacks
   - 4.7. Understanding ARP Poisoning
   - 4.8. Understanding MAC Spoofing Attacks
   - 4.9. Understanding DNS Poisoning
   - 4.10. Sniffing Tools-Wireshark
   - 4.11. Techniques to detect Sniffing

5. **Network Vulnerability Assessment**
   - 5.1. Vulnerability Scanning Tools
   - 5.2. Drawing Network Diagrams
   - 5.3. Network Discovery Tools
   - 5.4. Understanding Proxy Servers, Proxy Chaining
   - 5.5. Understanding IP Spoofing, MAC
   - 5.6. Spoofing and various Detection Techniques
   - 5.7. System Monitoring Tools
   - 5.8. Performance Measurement Tool

6. **Network Penetration Testing**
   - 6.1. External Penetration Testing
   - 6.2. External Intrusion Test & Analysis
   - 6.3. How is it done?
   - 6.4. Clients Benefits
   - 6.5. External Pen-Testing Steps
   - 6.6. Internal Network Penetration Testing
   - 6.7. Internal Pen-Testing
   - 6.8. Internal Pen-Testing Steps

7. **Intrusion Detection and Prevention System**
   - 7.1. What is an Intrusion Detection System?
   - 7.2. Types of IDS
   - 7.3. Multi-Layer IDS
   - 7.4. Wireless IDS
   - 7.5. Common Techniques to Evade IDS
   - 7.6. IDS Products & Services
   - 7.7. Snort Analysis
   - 7.8. IDS Penetration Testing Steps
   - 7.9. What is an Intrusion Prevention System?
   - 7.10. Types of IPS
   - 7.11. IPS Products & Services

8. **Firewall Penetration Testing**
   - 8.1. Firewall
   - 8.2. What does Firewall do?
   - 8.3. Packet Filtering Firewall
   - 8.4. What can't a Firewall do?
   - 8.5. How does a Firewall work?
   - 8.6. Firewall Operations
   - 8.7. Firewall Logging Functionality
   - 8.8. Firewall Policy
   - 8.9. Firewall Implementation
   - 8.10. Maintenance & Management of a Firewall
   - 8.11. Types of Firewall
   - 8.12. Steps for Firewall Penetration Testing

9. Resource Discovery

9.1. Network Topology
9.2. Asset Management
9.3. Configuration Management
9.4. Performance Management
9.5. Fault Management
9.6. Traffic Analysis
9.7. SLA Management
9.8. Report Generation

10. Network Reporting & Troubleshooting

10.1. Reporting on Bandwidth Usage and Other
10.2. Metrics
10.3. Collecting Data for Analysis
10.4. Understanding SNMP
10.5. Troubleshooting Network Problems
10.6. Additional Troubleshooting Tools
10.7. System Monitoring Tools
10.8. Troubleshooting Network Communication
10.9. Performance Measurement