Net Inspect

Course outline

Module 1: Network Security Basics

Module 1: Network Security Basics is an introductory course for the Net Inspect certification program. It covers the fundamentals of network security, including topics such as firewalls, intrusion detection systems, encryption, authentication, and access control. It also provides an overview of the different types of threats and vulnerabilities that can affect a network, as well as the best practices for mitigating them.

Lessons

- Introduction to Network Security
- Types of Network Security
- Network Security Protocols
- Network Security Tools
- Firewalls and Intrusion Detection Systems
- Network Access Control
- Network Security Policies
- Network Security Auditing
- Cryptography and Encryption
- Network Security Best Practices

After completing this module, students will be able to:

- Understand the fundamentals of network security and the importance of protecting data.
- Identify common threats to networks and how to protect against them.
- Implement basic security measures such as firewalls, antivirus software, and encryption.
- Utilize network security tools to monitor and detect suspicious activity.

Module 2: Network Protocols and Standards

Module 2 of the Net Inspect course covers the fundamentals of network protocols and standards. It provides an overview of the different types of protocols and standards used in networking, including TCP/IP, Ethernet, Wi-Fi, and more. It also covers the basics of network security, including encryption, authentication, and access control. Finally, it provides an introduction to network troubleshooting and monitoring tools.

Lessons

- Introduction to Network Protocols and Standards
- TCP/IP Protocol Suite
- IPv4 and IPv6 Addressing
- Network Layer Protocols: ICMP, IGMP, ARP
- Transport Layer Protocols: TCP and UDP
- Application Layer Protocols: HTTP, FTP, SMTP, DNS
- Network Security Protocols: SSL/TLS, SSH
- Network Management Protocols: SNMP, NetFlow
- Network Troubleshooting and Diagnostics
- Network Performance Monitoring and Optimization

After completing this module, students will be able to:

- Understand the fundamentals of network protocols and standards, such as TCP/IP, Ethernet, and Wi-Fi.
- Identify and troubleshoot common network issues related to network protocols and standards.
- Analyze network traffic using packet sniffers and other network analysis tools.
- Configure and manage network devices to ensure optimal performance and security.

Module 3: Network Topologies and Architectures

Module 3 of the Net Inspect course covers the fundamentals of network topologies and architectures. It provides an overview of the different types of network topologies, such as bus, star, ring, and mesh, and explains the advantages and disadvantages of each. It also covers the basics of network architectures, including the OSI model, TCP/IP model, and network protocols. Finally, it provides an introduction to network security and troubleshooting.

Lessons

- Introduction to Network Topologies
- Types of Network Topologies
- Network Architectures
- Network Design Considerations
- Network Security
- Network Troubleshooting
- Network Performance Monitoring
- Network Management Tools
- Network Virtualization
- Network Automation

After completing this module, students will be able to:

- Understand the different types of network topologies and architectures, such as bus, star, mesh, and ring.
- Identify the advantages and disadvantages of each type of network topology and architecture.
- Analyze the performance of a network based on its topology and architecture.
- Design and implement a network topology and architecture that meets the requirements of a given

scenario.

Module 4: Network Monitoring and Troubleshooting

Module 4 of the Net Inspect course covers the fundamentals of network monitoring and troubleshooting. It provides an overview of the different types of network monitoring tools and techniques, as well as how to use them to identify and resolve network issues. It also covers the basics of network troubleshooting, including how to diagnose and resolve common network problems.

Lessons

- Introduction to Network Monitoring
- Network Performance Monitoring
- Network Troubleshooting Techniques
- Network Security Monitoring
- Network Traffic Analysis
- Network Configuration Management
- Network Fault Management
- Network Capacity Planning
- Network Automation and Orchestration
- Network Monitoring Tools and Technologies

After completing this module, students will be able to:

- Understand the fundamentals of network monitoring and troubleshooting.
- Identify and diagnose common network issues.
- Utilize network monitoring tools to detect and resolve network problems.
- Develop strategies for proactive network maintenance and optimization.

Module 5: Network Performance Analysis

Module 5 of the Net Inspect course focuses on Network Performance Analysis. It covers topics such as network performance metrics, network performance monitoring, and network performance optimization. Students will learn how to identify and troubleshoot network performance issues, as well as how to use various tools and techniques to improve network performance.

Lessons

- Introduction to Network Performance Analysis
- Network Performance Metrics
- Network Performance Monitoring Tools
- Network Performance Troubleshooting
- Network Performance Optimization
- Network Performance Tuning
- Network Performance Reporting
- Network Performance Capacity Planning
- Network Performance Security

- Network Performance Best Practices

After completing this module, students will be able to:

- Understand the fundamentals of network performance analysis and how to use tools to measure and analyze network performance.
- Identify and troubleshoot common network performance issues.
- Utilize network performance analysis tools to identify and resolve network performance problems.
- Develop strategies to optimize network performance and ensure quality of service.

Module 6: Network Traffic Analysis

Module 6 of the Net Inspect course focuses on network traffic analysis. It covers topics such as packet analysis, network forensics, and intrusion detection. Students will learn how to identify malicious traffic, analyze network traffic, and use tools to detect and respond to security incidents. The module also covers topics such as network security policies, network security monitoring, and incident response.

Lessons

- Introduction to Network Traffic Analysis
- Network Traffic Analysis Tools
- Analyzing Network Traffic Patterns
- Analyzing Network Traffic Performance
- Analyzing Network Traffic Security
- Analyzing Network Traffic Volume
- Analyzing Network Traffic Quality
- Analyzing Network Traffic Congestion
- Analyzing Network Traffic Flows
- Analyzing Network Traffic Anomalies
- Analyzing Network Traffic Trends
- Analyzing Network Traffic Profiles
- Analyzing Network Traffic Correlations
- Analyzing Network Traffic Optimization
- Analyzing Network Traffic Forensics

After completing this module, students will be able to:

- Identify and analyze network traffic patterns and anomalies.
- Utilize network traffic analysis tools to detect malicious activity.
- Interpret network traffic data to identify potential security threats.
- Develop strategies to mitigate network traffic-related security risks.

Module 7: Network Intrusion Detection and Prevention

Module 7 of the Net Inspect course covers Network Intrusion Detection and Prevention. It provides an overview of the different types of network intrusions, the methods used to detect them, and the strategies

used to prevent them. It also covers the use of intrusion detection systems (IDS) and intrusion prevention systems (IPS) to detect and prevent malicious activity. Finally, it provides an introduction to the use of honeypots and honeynets to detect and respond to malicious activity.

Lessons

- Overview of Network Intrusion Detection and Prevention
- Types of Network Intrusions
- Network Intrusion Detection System (NIDS)
- Network Intrusion Prevention System (NIPS)
- Signature-Based Intrusion Detection
- Anomaly-Based Intrusion Detection
- Host-Based Intrusion Detection
- Network Access Control
- Firewalls and Network Security
- Network Security Policies and Procedures
- Network Security Auditing
- Network Security Monitoring
- Incident Response and Management
- Best Practices for Network Intrusion Detection and Prevention

After completing this module, students will be able to:

- Understand the fundamentals of network intrusion detection and prevention systems.
- Identify and analyze malicious network traffic.
- Develop strategies to protect networks from malicious attacks.
- Implement network intrusion detection and prevention systems.

Module 8: Network Access Control

Module 8 of the Net Inspect course covers Network Access Control, which is the process of controlling who can access a network and what they can do once they are connected. It includes topics such as authentication, authorization, and encryption, as well as methods for controlling access to the network, such as firewalls, intrusion detection systems, and virtual private networks.

Lessons

- Introduction to Network Access Control
- Types of Network Access Control
- Network Access Control Protocols
- Network Access Control Policies
- Network Access Control Authentication
- Network Access Control Authorization
- Network Access Control Auditing
- Network Access Control Best Practices
- Network Access Control Troubleshooting
- Network Access Control Security Considerations

After completing this module, students will be able to:

- Understand the fundamentals of network access control and its importance in network security.
- Implement network access control policies and procedures to protect the network from unauthorized access.
- Utilize network access control tools to monitor and control user access to the network.
- Troubleshoot and resolve network access control issues.

Module 9: Network Forensics

Module 9 of the Net Inspect course covers the fundamentals of network forensics. It provides an overview of the tools and techniques used to investigate network-related incidents, including packet capture and analysis, log analysis, and malware analysis. It also covers the legal and ethical considerations of network forensics.

Lessons

- Introduction to Network Forensics
- Network Traffic Analysis
- Network Packet Analysis
- Network Log Analysis
- Investigating Network Intrusions
- Investigating Malware Activity
- Investigating Denial of Service Attacks
- Investigating Web-Based Attacks
- Investigating Email-Based Attacks
- Investigating Wireless Network Attacks
- Investigating Mobile Device Attacks
- Investigating Cloud-Based Attacks
- Investigating Botnets
- Investigating Social Engineering Attacks
- Investigating Insider Threats
- Investigating Data Leakage
- Investigating Network Abuse
- Investigating Network Misconfigurations
- Investigating Network Performance Issues
- Investigating Network Security Breaches

After completing this module, students will be able to:

- Understand the fundamentals of network forensics and its importance in network security.
- Identify and analyze network traffic to detect malicious activity.
- Utilize network forensics tools to investigate and analyze network traffic.
- Develop strategies to prevent and respond to network security incidents.

Module 10: Network Vulnerability Assessment and Management

Module 10 of the Net Inspect course focuses on network vulnerability assessment and management. It covers topics such as identifying and assessing network vulnerabilities, developing and implementing security policies, and using tools to detect and mitigate security threats. The module also provides an overview of the different types of security threats and how to respond to them.

Lessons

- Understanding Network Vulnerability Assessments
- Identifying Network Vulnerabilities
- Network Security Best Practices
- Network Vulnerability Scanning Tools
- Network Vulnerability Remediation Strategies
- Network Vulnerability Management Processes
- Network Vulnerability Risk Management
- Network Vulnerability Auditing
- Network Vulnerability Reporting
- Network Vulnerability Mitigation Techniques

After completing this module, students will be able to:

- Identify and assess network vulnerabilities.
- Develop and implement strategies to mitigate network vulnerabilities.
- Utilize tools and techniques to detect and respond to network security threats.
- Monitor and analyze network traffic for malicious activity.