



Performing Network Security Auditing

Risk Management and Tools



Introduction

- Network security auditing is a critical process for assessing and improving the security of a network infrastructure.
- This presentation explores the importance of risk management in network audits and discusses popular network audit and security assessment tools.

Risk Management in Network Audits

Understanding Risk Management

- 1 Risk management involves identifying, assessing, and mitigating potential risks to the network infrastructure.
- 2 In network audits, risk management helps prioritize security measures and allocate resources effectively.

Key Components of Risk Management

1 Risk Identification

Identifying potential threats, vulnerabilities, and security weaknesses in the network.

2 Risk Assessment

Evaluating the likelihood and impact of identified risks to determine their significance.

3 Risk Mitigation

Implementing controls and measures to reduce or eliminate identified risks.

4 Risk Monitoring

Continuously monitoring the network for new risks and reassessing existing risks.



Network Audit Tools

SolarWinds

SolarWinds offers a range of network auditing tools, including Network Performance Monitor and Network Configuration Manager.

These tools provide comprehensive network monitoring, configuration management, and vulnerability assessment capabilities.

Open-Audit

Open-Audit is an open-source network auditing tool that automates the discovery and inventory of network devices.

It provides detailed information about network assets, including hardware, software, and configuration data.

Nmap

Nmap is a widely-used network scanning tool that helps identify open ports, services, and potential vulnerabilities.

It offers advanced scanning techniques and can be used for both security auditing and network mapping purposes.

NetformX

NetformX is a network design and documentation tool that assists in auditing network configurations and ensuring compliance.

It provides visual representations of network topologies, device configurations, and connectivity information.

Security Assessment Tools

Nessus

Nessus is a popular vulnerability scanning tool that helps identify security weaknesses in network devices and systems.

It offers comprehensive vulnerability assessments, compliance checks, and remediation guidance.

Nipper

Nipper is a network security auditing tool that analyzes network device configurations for potential security risks.

It provides detailed reports and recommendations for improving the security posture of network devices.

Wireshark

Wireshark is a powerful network protocol analyzer that captures and analyzes network traffic in real-time.

It helps identify network anomalies, troubleshoot issues, and detect potential security breaches.



Conclusion

- Performing network security audits is crucial for maintaining a secure network infrastructure.
- By implementing effective risk management practices and utilizing network audit and security assessment tools, organizations can identify vulnerabilities, mitigate risks, and enhance their overall network security.



Information Security Buzz

Discover more at our InfoSec Knowledge Hub