Experiment No. 6

Date: 03/09/2025

Title: Network Security Audit Checklist

Objective:

To perform a network security audit by creating suitable audit questionnaires for two IT companies and preparing a 10-step checklist to evaluate and improve network security.

Apparatus / Software Required:

- Network documentation and security policy documents
- Network monitoring tools (Wireshark, SolarWinds, Nagios)
- Access logs and server configurations
- Audit checklist and questionnaire sheets

Theory:

A Network Security Audit is a systematic evaluation of an organization's IT infrastructure. It identifies vulnerabilities, assesses controls, and ensures compliance with security standards. It helps organizations take their network from being uncomfortably vulnerable to confidently secure by reviewing devices, policies, access, data handling, and recovery systems.

10-Step Network Security Audit Process:

Step No.	Audit Step	Purpose
1	Define the Scope of the Audit	Identify all network components to include (devices, OS, access layers).
2	Determine Threats	List possible cyber threats (malware, phishing, insider threats).
3	Review and Edit Internal Policies	Verify and update company policies (security, privacy, backup).
4	Ensure Safety of Sensitive Data	Check data access restrictions and secure storage.
5	Inspect the Servers	Verify server configurations, DNS, and

		backup systems.
6	Examine Training Logs and Log Monitoring	Ensure proper employee training and log auditing.
7	Safe Internet Access	Check encryption, malware protection, and firewall settings.
8	Penetration Testing	Perform vulnerability testing for all access points.
9	Share the Audit Report	Communicate audit results transparently with the IT team.
10	Regular Network Audits	Schedule periodic (annual or semi-annual) audits.

Network Security Audit Checklist (Sample Format):

Sr. No.	Audit Questionnaire	Company A (Yes/No)	Company B (Yes/No)	Remarks
1	Security camera has been installed to monitor the data center?	Yes	No	Company A: Monitored 24x7; Company B lacks surveillance.
2	Do you maintain register for entry/exit to data center?	Yes	Yes	Both maintain entry logs.
3	Do you have electronic access control (Swipe Card) mechanism?	Yes	No	Company B uses manual register.
4	Do you have UPS system to backup your	Yes	Yes	3-hour backup available in

	data center electricity?			both.
5	Do you have Disaster Recovery plan in place for Data center?	Yes	No	Company B yet to implement DRP.

Sample Questionnaire (Detailed):

Physical Security

Sr. No.	Audit Questionnaire	Document Available (Yes/No)
1	Do you have policy that addresses the physical security of the Data Center?	Yes
2	Do you maintain register for entry/exit to data center?	Yes
3	Do you have electronic access control (Swipe Card) mechanism for entry/exit to data center?	Yes
4	Do you take access control review, at what frequency?	Yes
5	Do you allow temporary access to data center? Is it recorded?	Yes
6	Do you escort visitors to the data center?	Yes
7	Do you have control on door automatic lock with alarm system?	Yes
8	Security camera installed to monitor data center? Check monitoring and retention details.	Yes

Observation:

- Company A maintains better documentation, access control, and data safety mechanisms.
- Company B needs improvement in patch management, audit frequency, and policy updates.
- Both companies have adequate firewall and encryption measures.
- Incident management and DRP compliance are satisfactory.

Result:

A detailed Network Security Audit Checklist was successfully prepared for two IT companies. The audit process helped in identifying weaknesses, ensuring policy compliance, and improving network security posture.

Conclusion:

Network security audits are essential for maintaining the confidentiality, integrity, and availability of organizational data. Regular audits help detect vulnerabilities early and strengthen overall cyber defense.

Remarks:

Company A: Compliant with most security standards.
Company B: Needs improvement in documentation and patch updates.