Experiment - 6

Date: 17/9/25

NETWORK SECURITY AUDIT CHECKLIST

Aim:

To perform a Network Security Audit Checklist for two IT companies by creating suitable audit questionnaires based on the 10 essential steps of network auditing. The objective is to evaluate the current security posture and recommend improvements to ensure network security.

Procedure:

The steps followed in this experiment are:

1. Define the scope of the audit – Decide devices, OS, and access layers to be included.
2. Determine threats – Identify possible cyber threats like malware, DDoS, BYOD risks.
3. Review and edit internal policies – Review current company policies and suggest updates.
4. Ensure the safety of sensitive data – Restrict access and storage to secure systems.
5. Inspect the servers – Verify configurations, DNS, WINS, backups, and software updates.
6. Examine training logs and log monitoring – Ensure training, log monitoring, and automation.
7. Safe internet access – Apply encryption, malware scanning, and access restrictions.
8. Penetration testing – Perform static and dynamic testing to locate vulnerabilities.
9. Share audit results – Discuss audit findings with the team transparently.
10. Regular audits – Perform audits at least twice a year to ensure continuous improvement.

Network Security Audit Checklist:

Sr. No.	Audit Questionnaire	Company A (Yes/No)	Company B (Yes/No)	Remarks
1	Security camera installed to monitor data center?	Yes	No	Monitored by admin, recording stored for 30 days.
2	Are malware protection and DDoS prevention	Yes	Yes	Both companies use firewalls and IDS/IPS.

	implemented?			
3	Is there a network security and remote access policy?	Yes	No	Company B needs to update policies.
4	Is sensitive data stored securely and restricted?	Yes	Yes	Data stored in encrypted servers.
5	Are servers configured properly and updated?	Yes	Yes	DNS, WINS verified, regular patch updates applied.
6	Are employees trained and logs monitored regularly?	Yes	No	Company B lacks proper training logs.
7	Is internet usage monitored and encrypted?	Yes	Yes	VPNs and malware filters enabled.
8	Is penetration testing conducted regularly?	Yes	No	Company B has not yet implemented penetration tests.
9	Are audit results shared with the IT/security team?	Yes	Yes	Both companies share results with teams.
10	Are audits conducted 1–2 times per year?	Yes	No	Company B should plan periodic audits.

Result:

Thus, the network security audit checklist was successfully prepared for two IT companies. The audit identified strengths such as proper server configuration and secure data storage, and weaknesses such as lack of penetration testing and irregular audits in Company B.