Network Security Monitoring Report

Overview

This report provides an account of network security monitoring activities conducted from [Start Date] to [End Date]. It highlights security events, details one identified incident, and outlines the steps taken for incident response.

1. Monitoring Process

Network traffic and security logs were monitored using tools such as [Tool Names] to detect anomalies and potential threats. Key metrics observed include:

- Intrusion Detection System (IDS) alerts
- Unusual login attempts
- Data transfer anomalies

2. Identified Security Incident

On [Date], a security incident was identified involving unauthorized access to [System Name]. The event was detected by [Tool Name], which flagged unusual login attempts from IP address [IP Address].

3. Incident Response Steps

The following steps were taken to respond to the incident:

1. Isolation of the affected system to prevent further access.
2. Identification of compromised accounts and resetting of credentials.
3. Blocking of the malicious IP address at the firewall level.
4. Review and analysis of logs to determine the extent of the breach.
5. Implementation of additional security measures to prevent recurrence.

4. Supporting Logs and Screenshots

Below are the key logs and screenshots captured during the monitoring and incident response

process.

[Insert logs and screenshots here.]

Example: Screenshot of flagged IDS alert, log snippet of unusual login attempts, etc.