IT Incident Report Example

Incident Details

Incident ID: 2021-001

Date: January 3, 2021

Time: 02:30 PM

Reported By: John Doe

Incident Description

An unauthorized user was detected attempting to gain root access to our primary server. The attacker tried to exploit a known vulnerability in our system to escalate their privileges.

Detected Threat

The threat was identified as a privilege escalation attack. The attacker attempted to gain higher-level privileges, which could allow them full access to the system.

Incident Response

The IT team was alerted immediately. They successfully thwarted the attempt and cut off the attacker's access to the system. A full system check was carried out to ensure no malicious software was installed.

Impact

No data was compromised during this incident. The server was offline for two hours during the investigation.

Next Steps

We are updating our system to patch the vulnerability exploited in this incident. We will also be enhancing our security measures to prevent similar incidents in the future.