Re: Incident #

Team #

February 8th, 2025

# Incident Summary

* **Time:** 2025-02-08 at 15:00
* **Source IP Address:** 10.x.x.x
* **Destination IP Address:** 10.x.x.x

# Timeline of Activity

1. **15:00** – Attackers brute-forced the password on 10.x.x.x.
2. **15:02** – Attackers opened a reverse shell to 10.x.x.x.
3. **15:05** – All database contents on 10.x.x.x were dumped.

# Effects

## Compromised Credentials

1. SSH password on 10.x.x.x.
2. Database password on 10.x.x.x.

## Compromised Information

1. Database contents on 10.x.x.x.

## Access obtained

1. Remote access on 10.x.x.x from 15:00-15:10

# Remediation

To avoid this attack succeeding in the future, Team # will…