

# Black Sabre Response IRTx Presentation

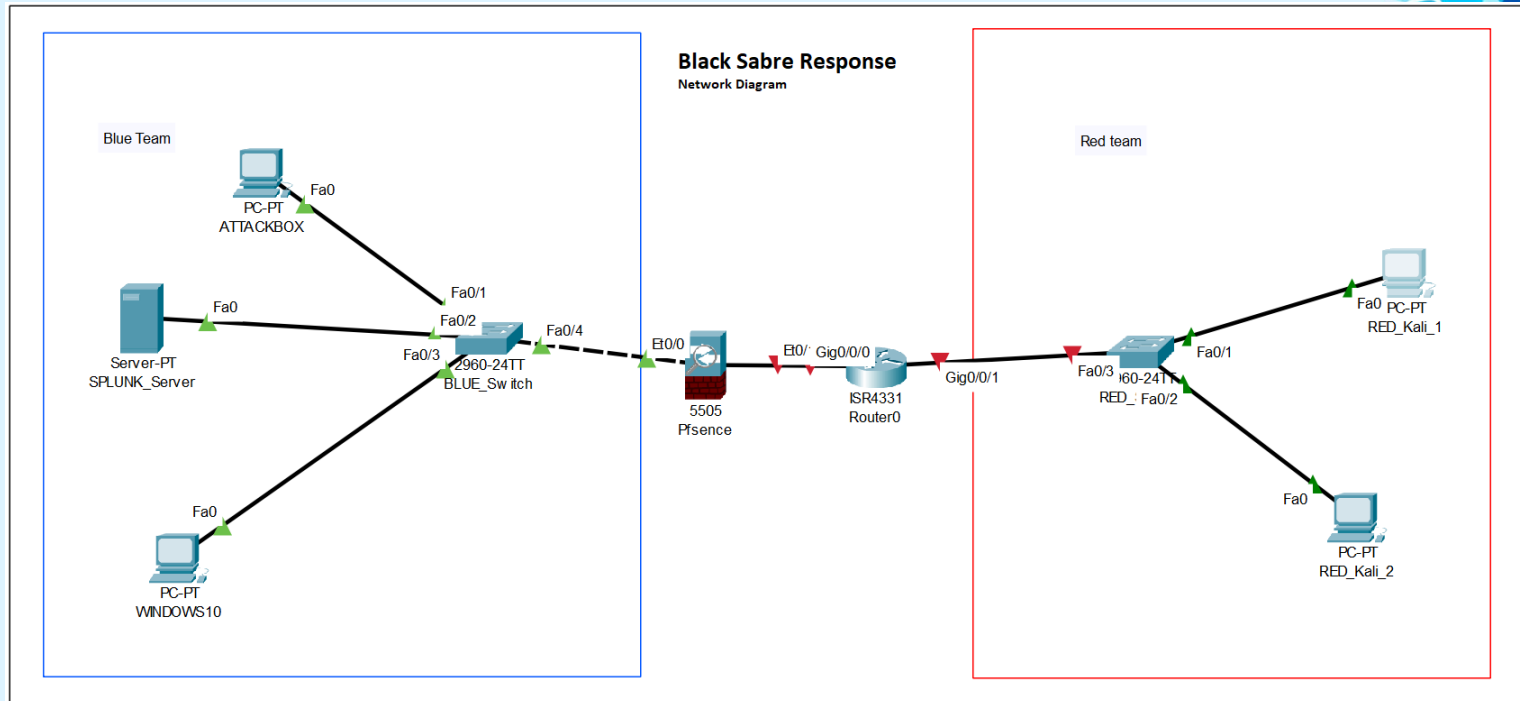




# Overview

- Environment setup
- Scenario Overview
- Lessons Learnt
- Summary

# Environment





# Scenario Overview

- Blue team playbooks x3
- Red team playbooks x3

## Attacks:

- Misconfigured Jenkins
- SQL injections
- Vulnerable file upload

# Red Team Lessons

The background of the slide features a blue and white abstract design. On the right side, there is a graphic with binary code (0s and 1s) in a light blue color. A black globe icon is positioned near the top right. Below the globe, there are several black gears of different sizes, some of which are interlocked. The overall aesthetic is technical and digital.

## Positives

Attacks successful

- Reverse shell X2
- Database dump with credentials

## Negatives

Reverse shell code stored on desktop

MSF module failed





# Blue Team Lessons

## Positives

- Detection of all attacks

- Dashboard to assist in monitoring

## Negatives

- Detection only, no remediation

- Detection for Jenkins based on console process

# Lessons Learnt: Syed

The background of the slide features a blue and white abstract design. It includes a stylized globe in the upper right corner, surrounded by floating binary digits (0s and 1s). Below the globe, there are several interlocking gears, suggesting a mechanical or engineering theme. The overall aesthetic is modern and tech-oriented.

- How projects management works with tools like Gantt chart, draw.io
- Learning how to setup Splunk, Pfsense and network configuration
- How real-life SOC setup looks like



# Lessons Learnt: Dylan

How to create IRP/how it works

How to setup PFSense





# Project Lessons

## Positives

Effective communication

Teamwork

## Negatives

Incorrect project timeline

Members not always present

# Summary

- Successful IRTx
- Red and blue team completed tasks
- Lessons learnt from both teams



# Team Members

Project Manager – Syed

Communication Manager – Muzamil?

Blue Team Lead – Braedyn

Red Team Lead – Dylan





THANKYOU