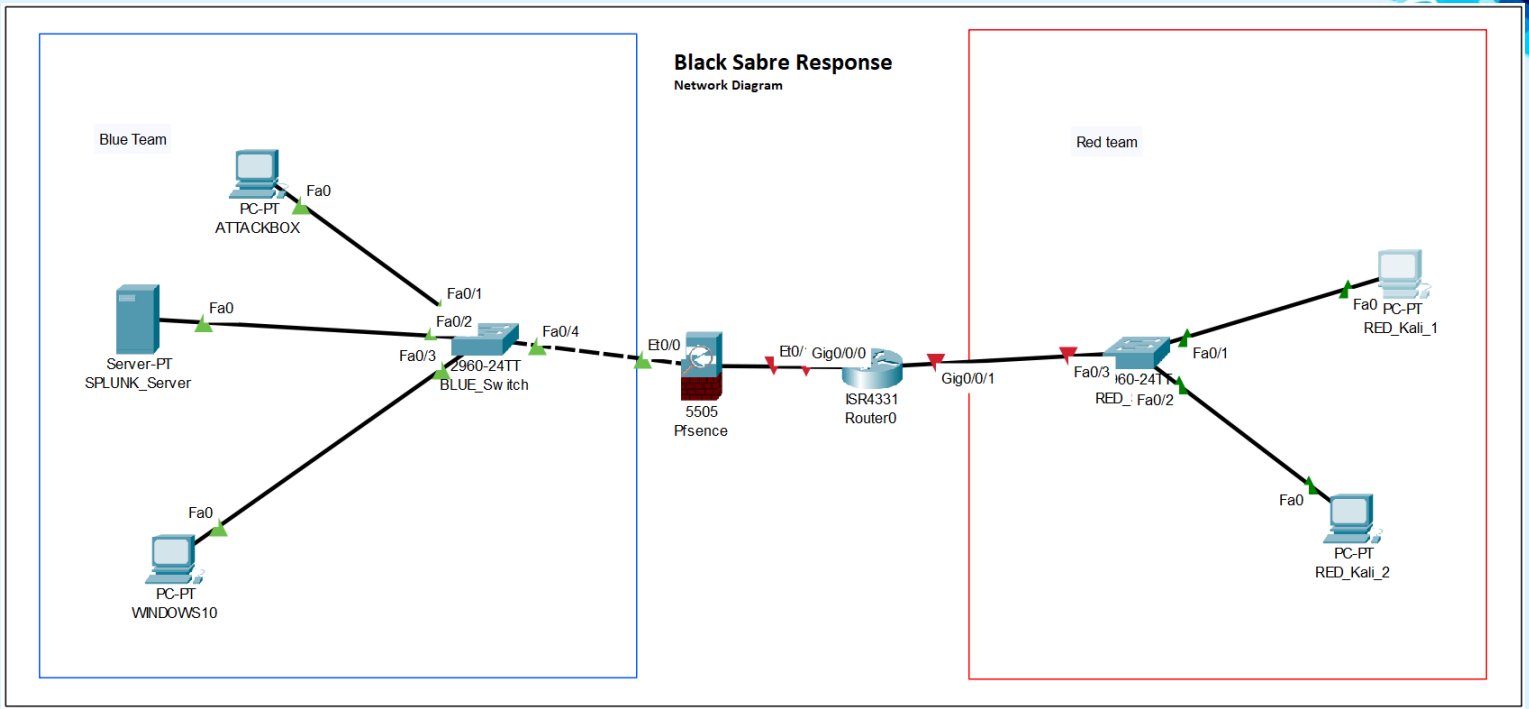
Black Sabre Response

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

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

- 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