# Blue Team: Summary of Operations

## Table of Contents

* Network Topology
* Description of Targets
* Monitoring the Targets
* Patterns of Traffic and Behavior

## Network Topology

The following machines were identified on the network:

**[Kali]**

* Operating System: Debain 5.4.13 – 1kali1
* Purpose: Pentester, Attacking Machine
* IP Address: 192.168.1.90/24

**[ELK]**

* Operating System: Ubuntu 18.04.4 LTS
* Purpose: Logs Purpose (FileBeat, MetricBeat, PacketBeat)
* IP Address: 192.168.1.100/24

**[Capstone]**

* Operating System: Ubuntu 18.04.1 LTS
* Purpose: Webserver/Capstone
* IP Address: 192.168.1.105/24

**[Target 1]**

* Operating System: Debian 3.16.57-2 / Linux
* Purpose: Vulnerable Target Machine
* IP Address: 192.168.1.110/24

**[Target 2]**

* Operating System: Debian 3.16.57-2 / Linux
* Purpose: Vulnerable Target Machine
* IP Address: 192.168.1.115/24

Diagram

Description automatically generated

## 

## Description of Targets

Fill in the following:

* Two VMs on the network were vulnerable to attack: Target 1 [192.168.1.110/24] and Target 2 [192.168.1.115/24].
* Each VM functions as an Apache web server and has SSH enabled, so ports 80(http) 22(ssh) and 111(rpcbind) are possible ports of entry for attackers.

## 

## Monitoring the Targets

This scan identifies the services below as potential points of entry:

Our assessment uncovered the following critical vulnerabilities in **Target 1**

|  |  |  |
| --- | --- | --- |
| **Vulnerability** | **Description** | **Impact** |
| Brute Force | Web site is vulnerable to brute force attacks | Was able to crack multiple passwords |
| Insecure Configuration Files | Configuration Files are easily accessible | Database passwords were retrieved from insecure config files |
| Password Policy | Users are using weak passwords that are easily crackable | Were able to guess or brute force several passwords |

Traffic to these services should be carefully monitored. To this end, we have implemented the alerts below: (Note: Add at least three alerts. You can add more if time allows.)

**SSH Alert**

SSH Connection Alert is implemented as follows:

* Metric: PacketBeat
* Threshold: 5
* Reliability: Medium

Graphical user interface, website

Description automatically generated

**Brute Force Alert**

Brute Force Alert is implemented as follows:

* Metric: PacketBeat
* Threshold: >1
* Reliability: This alert generate lot of false positives when user forget password, medium

Graphical user interface, text, application, email

Description automatically generated

**Wordpress Login Alert**

Wordpress Login Alert is implemented as follows:

* Metric: Packetbeat
* Threshold: ≥ 1
* Reliability: Low