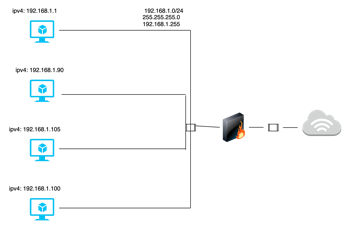
# **Blue-Team: Summary of Operations.**

## Table of Contents

* Network Topology
* Description of Targets
* Monitoring the Targets
* Proposed Alarms
* Mitigation Strategies

## Network Topology

The following machines were identified on the network:



The vulnerable network discovered:

Nmap scan report for 192.168.1.105 (192.168.1.105) - IP address discovered...with open port.

Host is up

Not shown: 998 closed ports

PORT STATE SERVICE

22/tcp open ssh

80/tcp open http

## Description of Targets

Fill in the following:

* One VM on the network is vulnerable to attack: Target 1 [192.168.1.105].

## Monitoring the Targets

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

A screenshot of a computer

Description automatically generated

Traffic to these services should be carefully monitored. To this end, we have implemented the alerts below:

**Proposed Alarms & Mitigation**

**Blocking Port Scan**

**Alarm**

**System Hardening**

**Configure firewalls to detect and shut down port scans**

**Patching: updating system to latest version**

**Whitelisting IP addresses**

**Load Balancer**

**Whitelisting only accepts connections from trusted IP address ranges.**

**Installing a load balancer will help lighten traffic burden.**

**Finding request for hidden directory**

**Alarm**

**System Hardening**

Patch: Invalid credential lock out

Whitelisting IP addresses

Load Balancer

Invalid credential lockout – Prevents excess login attempts. Can be implemented by activating lockout/timeout.

Whitelisting- System should only accept connection from trusted IP address ranges.

**Preventing Brute Force Attacks**

**Alarm**

Excessive HTTP errors

HTTP requests

Threshold: Above 300 for the last 5 minutes

Threshold: above 2500 for the last minute

**System Hardening**

Patch: Invalid credentials lock out

Whitelisting IP addresses

Invalid credentials lock out prevents excessive login attempts

Installation: By implementing an account lockout system

Whitelisting- System should only accept connection from trusted IP address ranges.

**Detecting the WebDav connection**

**Alarm**

**System Hardening**

Patch: Invalid credential lock out

Whitelisting IP addresses

Invalid credential lockout – Prevents excess login attempts. Can be implemented by activating lockout/timeout.

Whitelisting- System should only accept connection from trusted IP address ranges

**Identifying Reverse shell uploads**

**Alarm**

Machine Learning: A machine learning rule can be set which creates an alert when machine learning job creates an anomaly.

Security: packetbeat looks for unusual web browsing url activity that could indicate execution.

Threshold: field: source: IP address outside whitelist.

**System Hardening**

Patch: Invalid credential lock out

Whitelisting IP addresses

Invalid credential lockout – Prevents excess login attempts. Can be implemented by activating lockout/timeout.

Whitelisting- System should only accept connection from trusted IP address ranges.