# Blue Team: Summary of Operations

## Table of Contents

* Network Topology
* Description of Targets
* Monitoring the Targets
* Patterns of Traffic and Behavior
* Suggestions for Going Further

## Network Topology

The following machines were identified on the network:

**[Target 1]**

* Operating System: Debian GNU/Linux
* Purpose: The first target.
* IP Address: 192.168.1.110

**[Target 2]**

* Operating System: Debian GNU/Linux
* Purpose: The second target.
* IP Address: 192.168.1.255

Including a Gliffy or draw.io diagram is optional but highly encouraged.

## Description of Targets

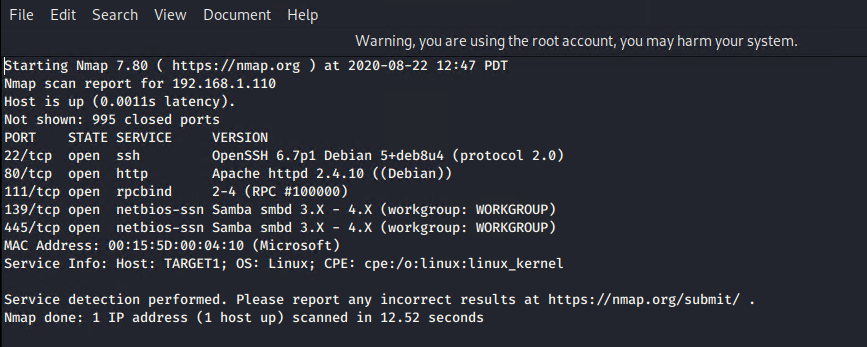
Fill in the following:

* Two VMs on the network were vulnerable to attack: Target 1 [192.168.1.110] and Target 2 [192.168.1.255].
* Each VM functions as an Apache web server and has SSH enabled, so ports 80 and 22 are possible ports of entry for attackers.

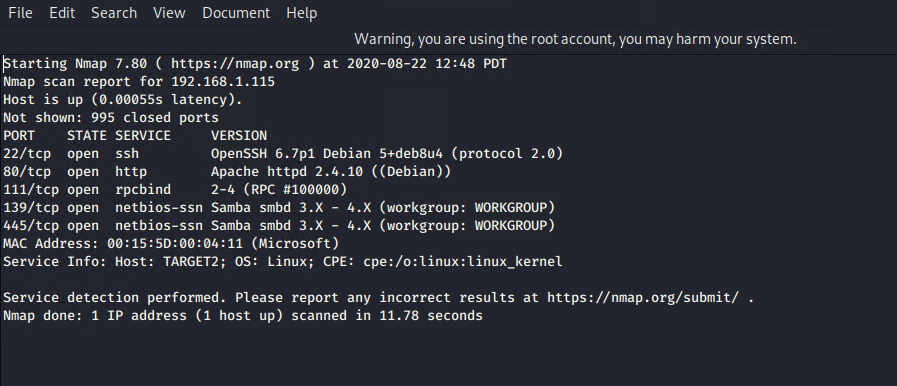
## Monitoring the Targets

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

* **Target 1**



* **Target 2**



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

**Excessive HTTP Errors**

[Excessive HTTP Errors] is implemented as follows:

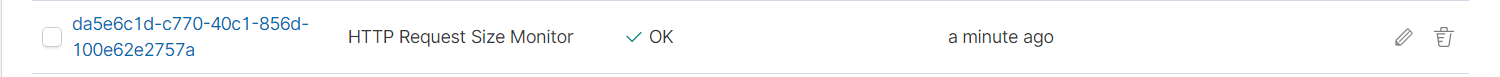
* Metric: HTTP Errors
* Threshold: Above 400 for the last 5 minutes
* Vulnerability Mitigated: Brute Force Attacks. Resource Usage Issues.
* Reliability: High Reliability



**HTTP Request Size Monitor**

[HTTP Request Size Monitor] is implemented as follows:

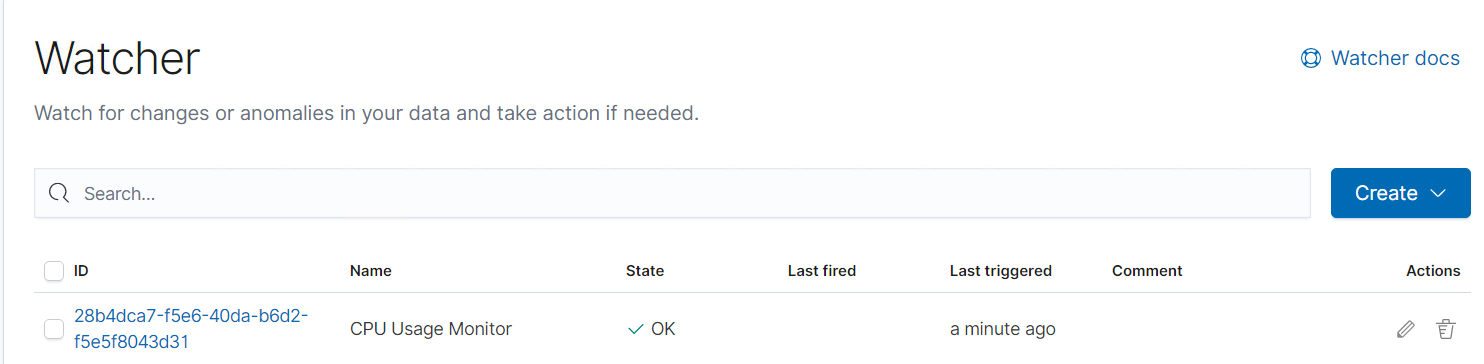
* Metric: http.request.bytes
* Threshold: Above 3500 for the last minute
* Vulnerability Mitigated: DOS (Denial of Service) Attacks.
* Reliability: High Reliability.



**CPU Usage Monitor**

[CPU Usage Monitor] is implemented as follows:

* Metric: system.process.cpu.total.pct
* Threshold: Above 0.5 for the last 5 minutes.
* Vulnerability Mitigated: Resource Management, Excessive CPU Usage.
* Reliability: Medium Reliability.



## Suggestions for Going Further

**Suggest a patch for each vulnerability identified by the alerts above.** Remember: alerts only detect malicious behavior. They do not prevent it.It is not necessary to explain how to implement each patch.

The logs and alerts generated during the assessment suggest that this network is susceptible to several active threats. In addition to watching for occurrences of such threats, the network should be hardened against them. The Blue Team suggests that IT implement the fixes below to protect the network:

**Vulnerability 1: Brute Force Attacks**

* Patch: Invalid Credentials Lock out. Limit activity/Whitelist to a specified IP address or range. Monitor server logs.
* Why It Works: It limits the number of attempts the attacker can commit. Only allows connections from trusted addresses.

**Vulnerability 2: DOS Attacks**

* Patch: Install a Load Balancer.
* Why It Works: Distributes requests amongst a number of servers which lightens the traffic burden on each server.

**Vulnerability 3: Excessive CPU Usage**

* Patch: Create different levels of alert for CPU Usage. Limit max cpu usage for each core.
* Why It Works: Different levels of alerts can help monitor CPU usage. Power Core Management.