# 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

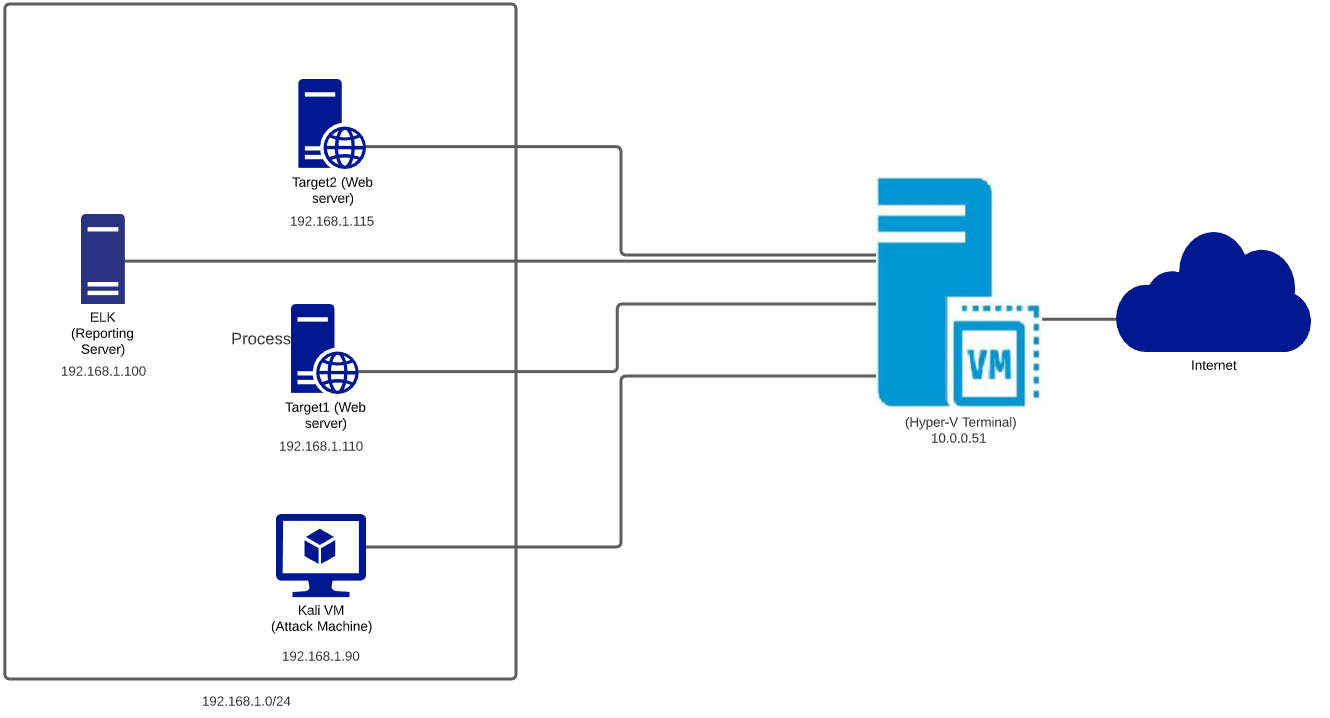
The following machines were identified on the network:

**[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: 192.168.1.115



## Description of Targets

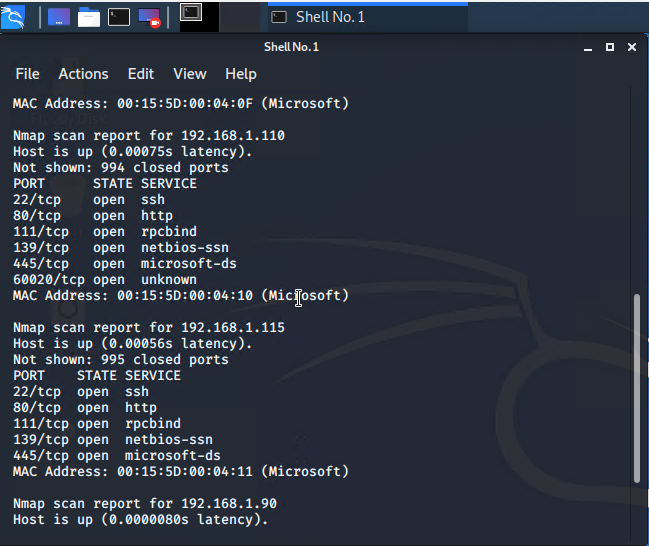
Fill in the following:

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

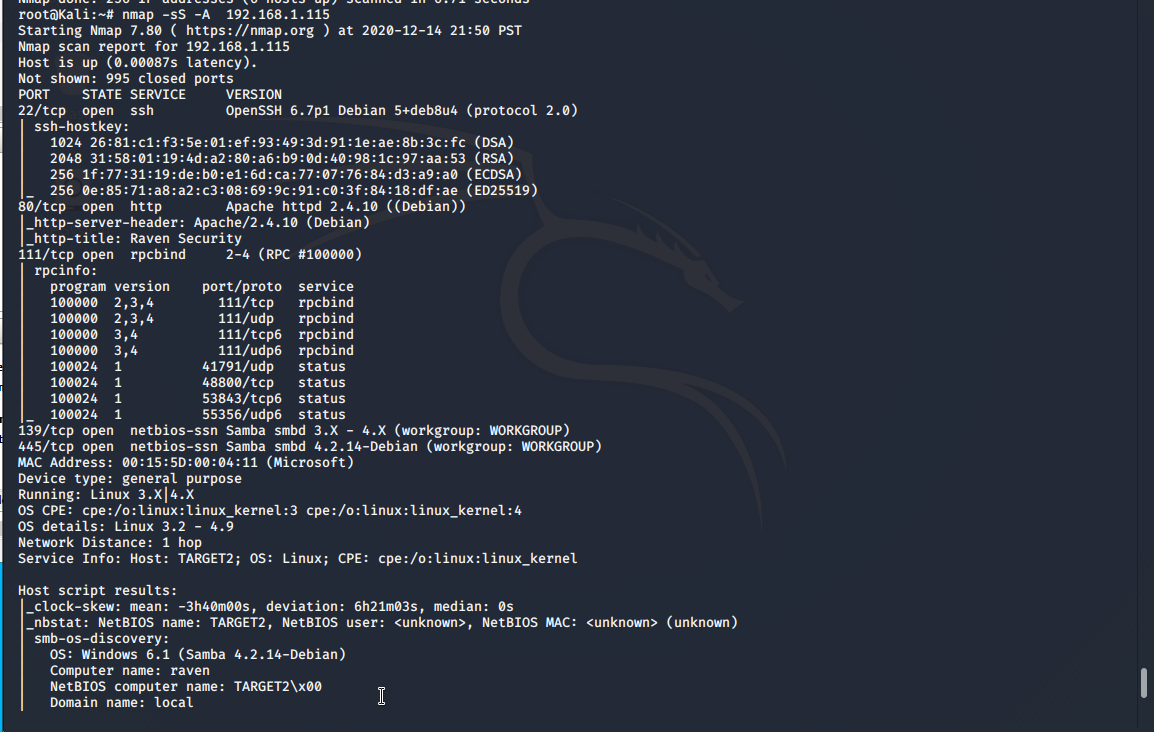
## Monitoring the Targets

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:

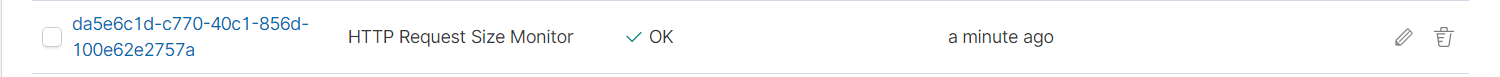
* Metric: HTTP Errors
* Threshold: Above 200 for the last 5 minutes
* Vulnerability Mitigated: Brute Force Attacks. Resource Usage Issues.
* Reliability: High Reliability



**HTTP Request Size Monitor**

[HTTP Request Size Monitor] is implemented as follows:

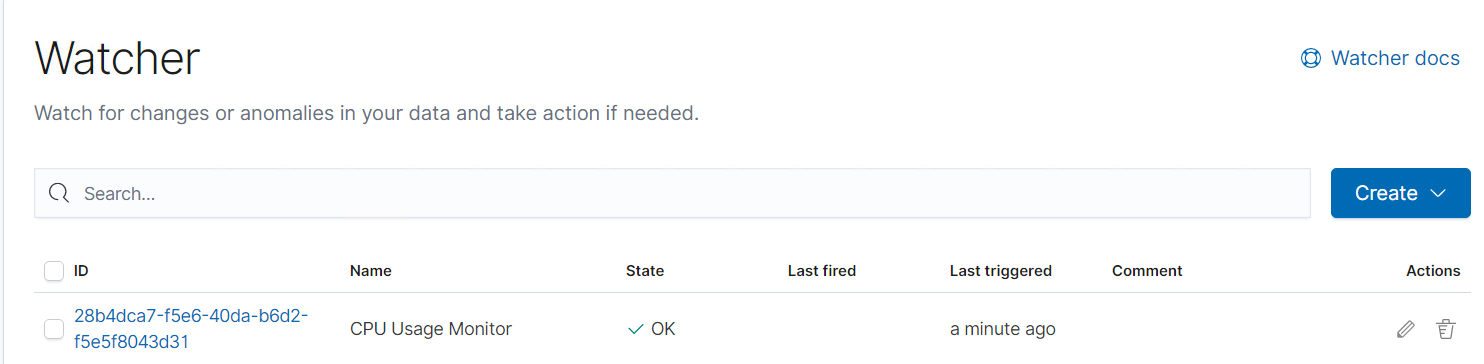
* Metric: http.request.bytes
* Threshold: Above 2000 for the last minute
* Vulnerability Mitigated: DOS (Denial of Service) Attacks.
* Reliability: High Reliability.



**CPU Usage Monitor**

[CPU Usage Monitor] is implemented as follows:

* Metric: system.process.cpu.total.pct
* Threshold: Above 0.02 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: CVE-2008-5161 SSH Login and Brute Force Attacks**

* Patch: Invalid Credentials Lock out. Limit activity/Whitelist to a specified IP address or range. Monitor server logs.

Disable ssh. This can be done by logging in as the root user on the server(s) and accessing the /etc/ssh/sshd\_config file.

Why It Works: It limits the number of attempts the attacker can commit. Only allows connections from trusted addresses. Disabling SSH from outside network will prevent anyone to login to the server

**Vulnerability 2: CVE-2019-15653 -Proprietary information including hashed passwords is viewable in plaintext on html pages within the wordpress site.**

* Patch: Notify developers of the error and have it corrected.
* Why It Works: The web developers can correct the code prevents exposing the hashed password within the wordpress site

**Vulnerability 3: CWE-548-Exposure of Information Through Directory Listing**

* Patch: The web developers must disable the Directory Listing in all web projects.
* Why It Works: This will restrict the attacker to find out the directory details of the web server

**Vulnerability 4: Users can access files they shouldn't be able to. User Steven has ability to run python scripting through his login**.

* Patch: chmod 700 to these files
* Why It Works: This will restrict access to root only read/write access

**Mandatory Hardening:**

* Install auditd, tripwire and lynis as part of the hardening process for both Target 1 and Target2
* Highly recommend to harden the machines as per CIS benchmark