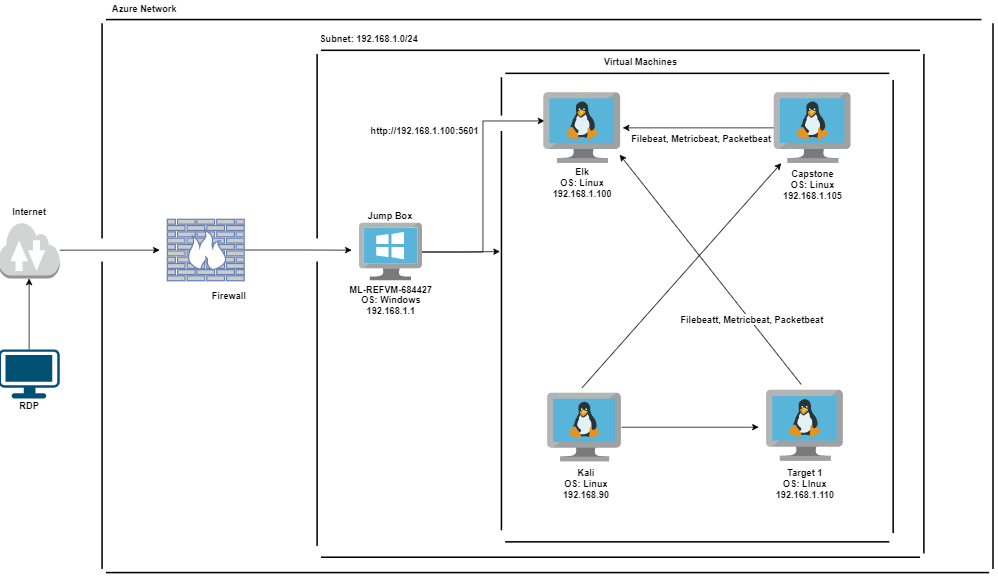
# Blue Team: Summary of Operations

## 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:

Azure VM

* Operating System: Windows
* Purpose: Host Machine
* IP Address: 192.68.1.1

Capstone

* Operating System: Linux
* Purpose: Test Alerts
* IP Address: 192.168.1.105

Elk

* Operating System: Linux
* Purpose: Gathers Logs and Hosts the Kibana Dashboard
* IP Address: 192.168.100

Kali

* Operating System: Linux
* Purpose: Attack Machine
* IP Address: 192.168.1.90

Target 1

* Operating System: Linux
* Purpose: Target Machine
* IP Address: 192.168.1.110

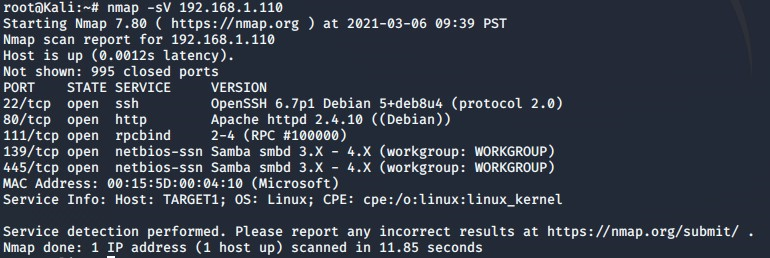
## Description of Target

The target of this attack was:

Target 1 (192.168.1.110). Target 1 is an Apache web server and has SSH enabled, so ports 80 and 22 are possible ports of entry for attackers. As such, the following alerts have been implemented.

## Monitoring the Targets

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



* **Target 1**
  + Port 22 ssh
  + Port 80 http
  + Port 111 rpcbind
  + Port 139 netbios-ssn
  + Port 445 netbios-ssn

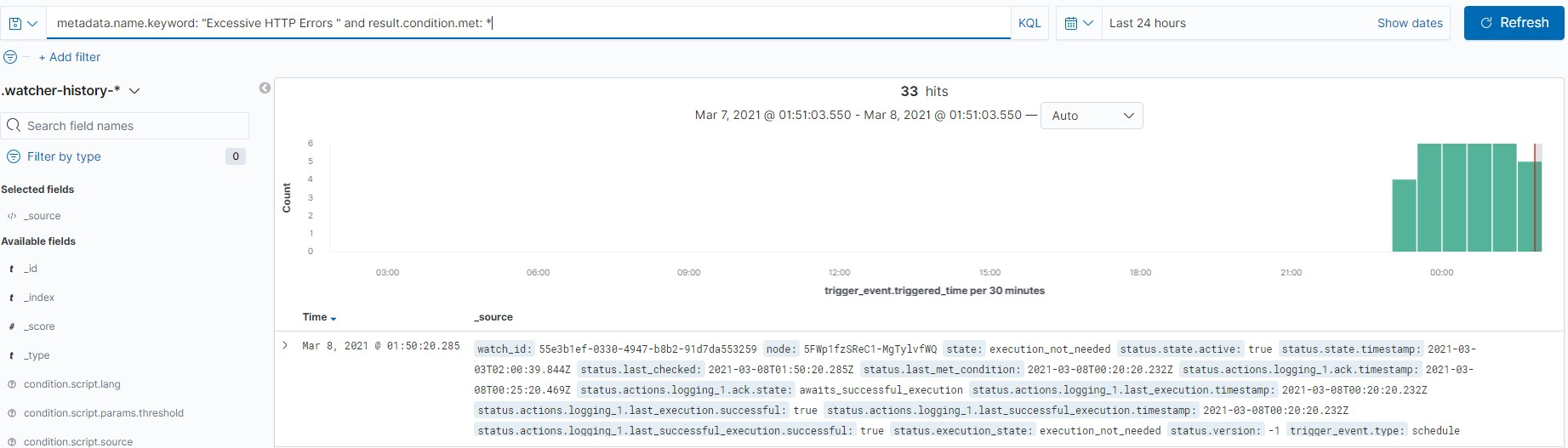
Traffic to these services should be carefully monitored. To this end, we have implemented the alerts below.

**Excessive HTTP Errors**

Excessive HTTP Errors is implemented as follows:

* Metric: Packetbeat data of http.response.status\_code
* Threshold: 5 HTTP Response Code 400 in 5 minutes
* Vulnerability Mitigated: Yes, WordPress enumeration detected
* Reliability: Moderate, threshold could be lowered and still detect attack

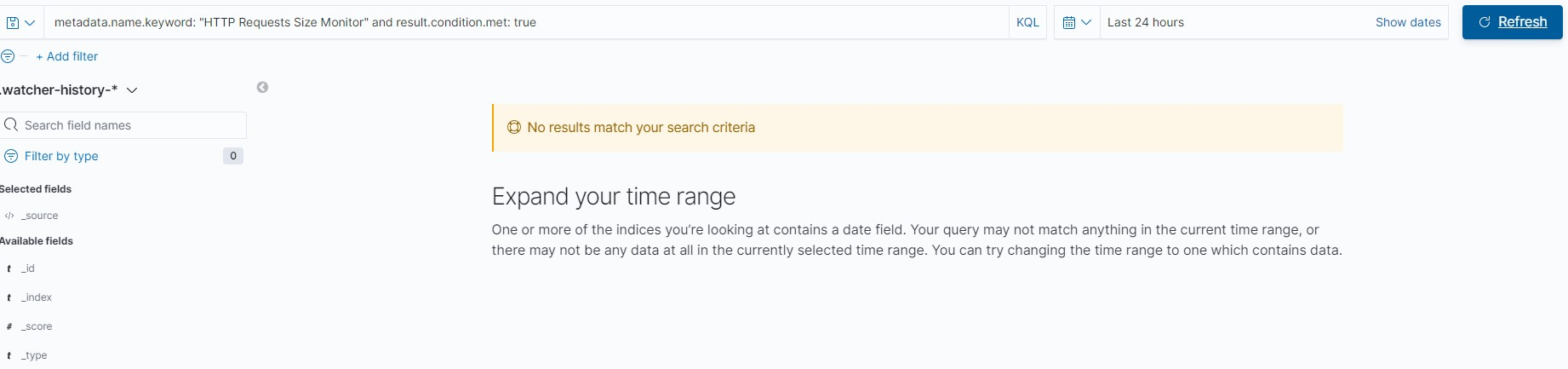




**HTTP Requests Size Monitor**

HTTP Requests Size Monitor is implemented as follows:

* Metric: Metricbeat data of http.request.bytes
* Threshold: Sum total of HTTP request bytes exceeds 3500 in one minute
* Vulnerability Mitigated: No, password hash dump and download not detected
* Reliability: Low

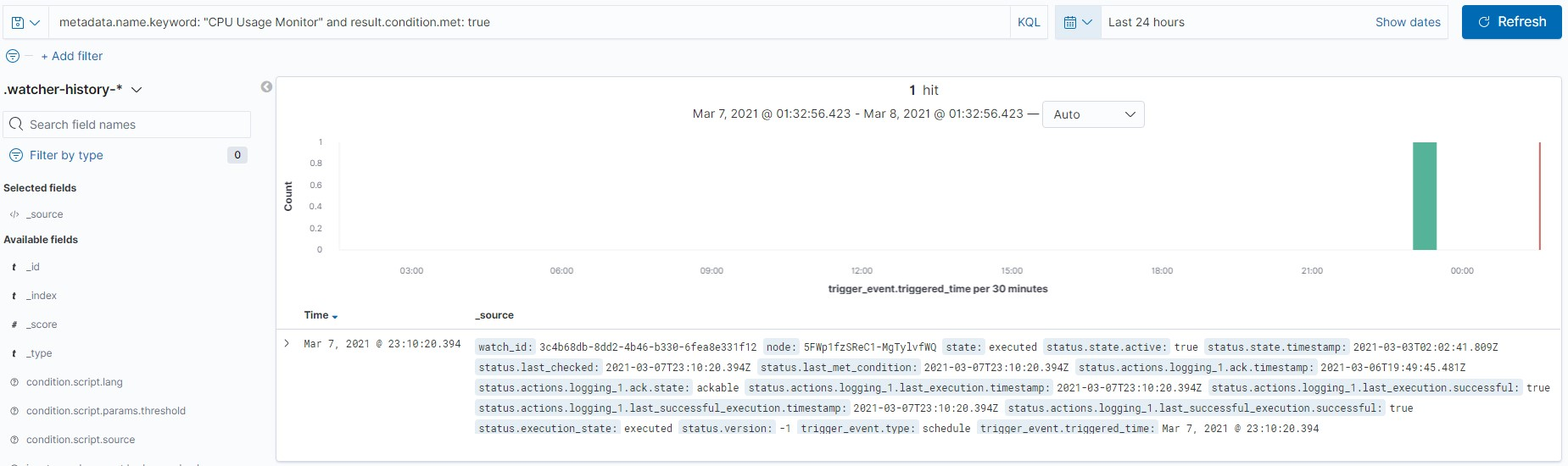




**CPU Usage Monitor**

CPU Usage Monitor is implemented as follows:

* Metric: Metricbeat data of system.process.cpu.total.pct
* Threshold: CPU usage of machine exceeds 50% for the last 5 minutes
* Vulnerability Mitigated: Yes, brute force attack detected
* Reliability: Moderate, threshold could be lowered and still detect attack





## 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 - Open Port 22 SSH**

* Patch: Close Port 22 so it is not discoverable by outside forces
* Why It Works: This prevents an attacker from gaining a SSH connection to the server

**Vulnerability 2 - Privilege Escalation**

* Patch: Change user rules on privileges and secure the root access with more authentication
* Why It Works: This prevents an attacker from escalating there privileges up to root after gaining access to the server

**Vulnerability 3 - Outdated WordPress**

* Patch: Update WordPress to the newest version
* Why It Works: The current version of WordPress patches many of the vulnerabilities that we were able to exploit thereby hardening the system