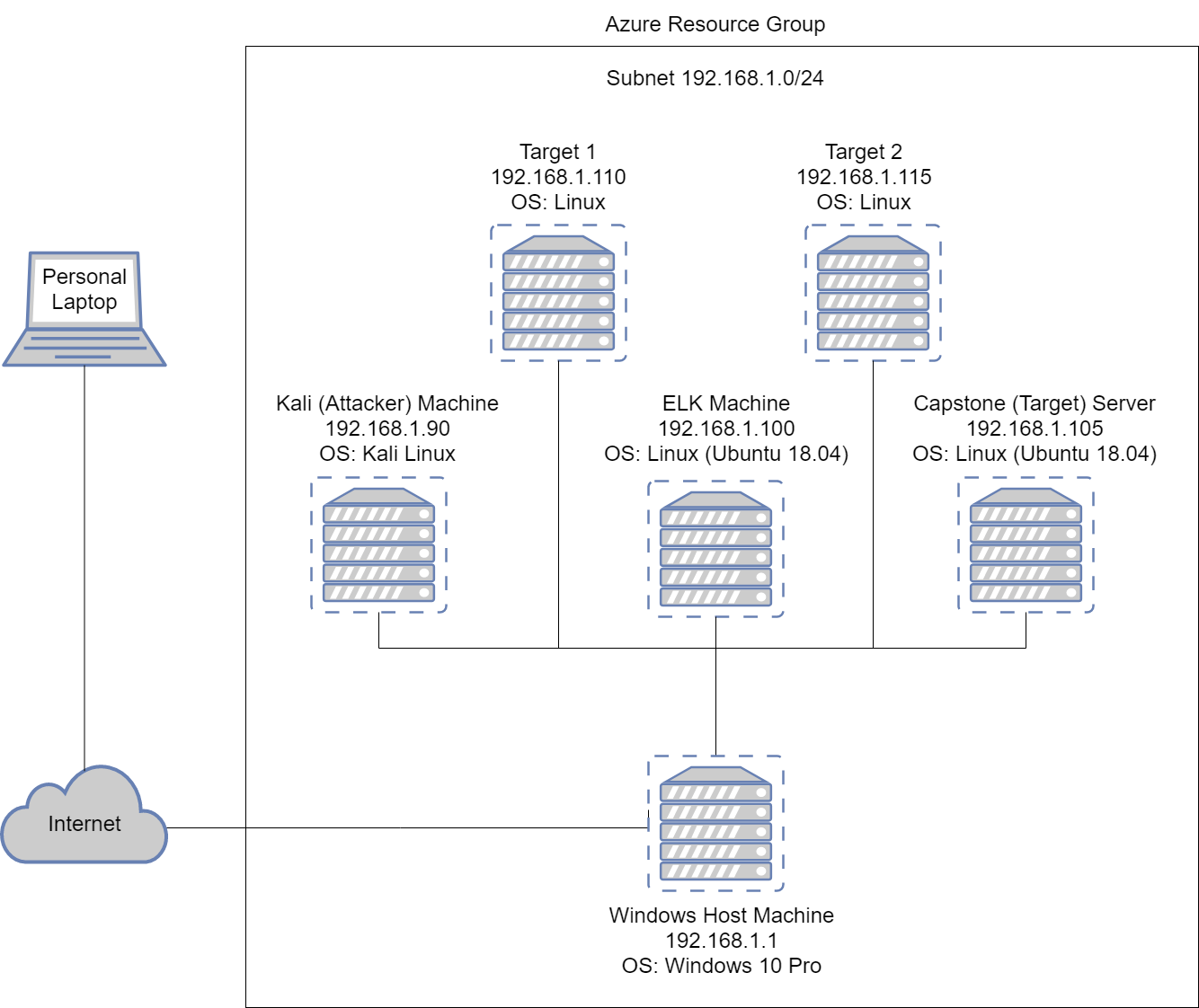
# Blue Team: Summary of Operations

## 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:



**Windows Host Machine**

* Operating System: Windows 10 Pro
* Purpose: Azure Cloud Environment
* IP Address: 192.168.1.1

**Kali**

* Operating System: Kali Linux
* Purpose: Attacker machine
* IP Address: 192.168.1.90

**ELK**

* Operating System: Linux (Ubuntu 18.04)
* Purpose: Collects Kibana logs
* IP Address: 192.168.1.100

**Target 1**

* Operating System: Linux
* Purpose: Target machine 1
* IP Address: 192.168.1.110

**Target 2**

* Operating System: Kali Linux
* Purpose: Target machine 2
* IP Address: 192.168.1.115

**Capstone**

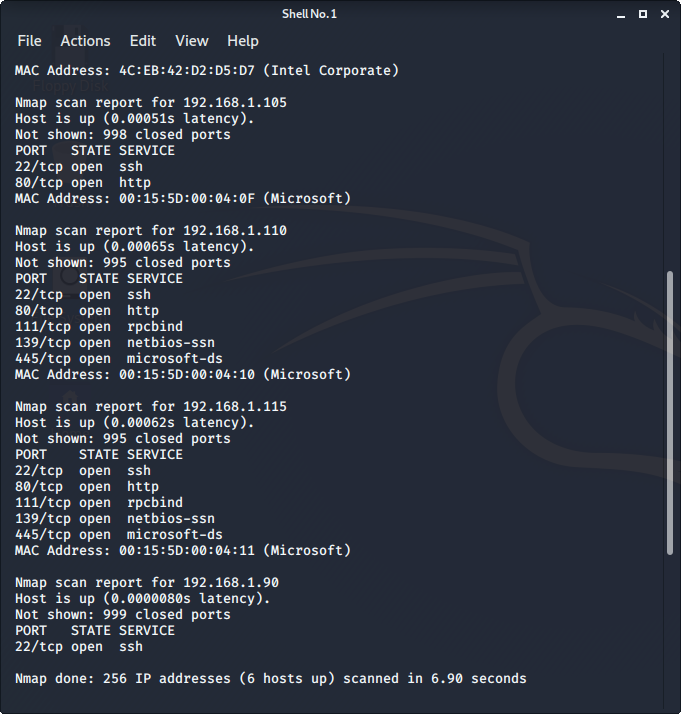
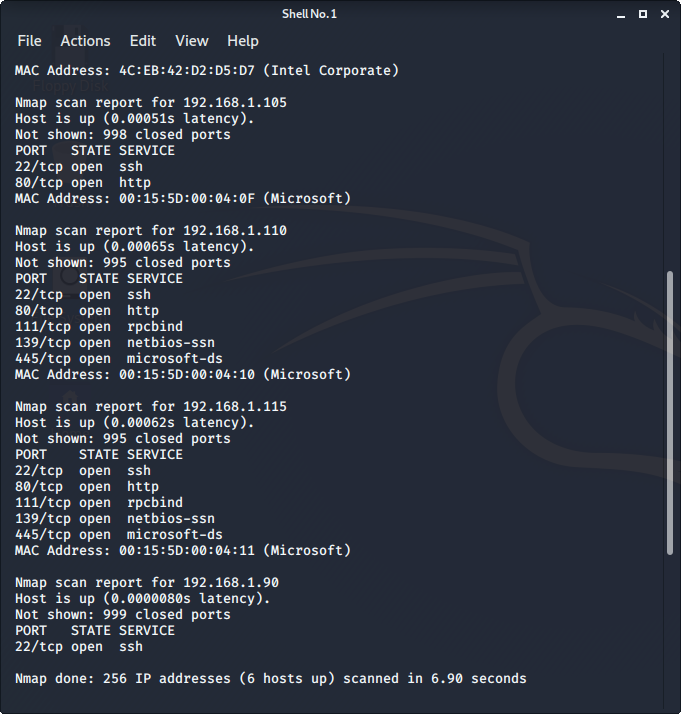
* Operating System: Linux (Ubuntu 18.04)
* Purpose: Original target machine
* IP Address: 192.168.1.105

## 

## 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. Port 445 is also a common point of entry for attackers and is often used to execute ransomware attacks.



## 

## Monitoring the Targets

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

* **Target 1**
  + Port 22: ssh into a system
  + Port 80: HTTP access
  + Port 445: File-sharing ability
* **Target 2**
  + Port 22: ssh into a system
  + Port 80: HTTP access
  + Port 445: File-sharing ability

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

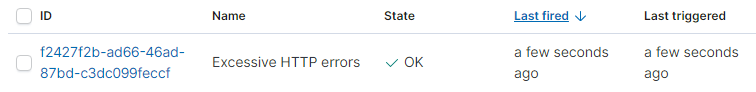
**Excessive HTTP Errors**

Excessive HTTP Errors is implemented as follows:

* Metric: Count of top 5 http response status codes over the last 5 minutes
* Threshold: 400
* Vulnerability Mitigated:
  + CWE-307: Improper Restriction of Authentication Attempts

[https://cwe.mitre.org/data/definitions/307.html](https://cwe.mitre.org/data/definitions/200.html)

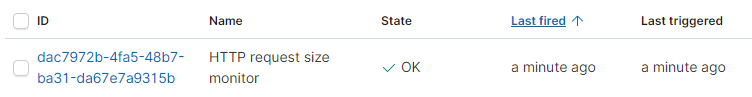
* + CWE-200: Exposure of Sensitive Information to an Unauthorised Actor: htt[ps://cwe.mitre.org/data/definitions/200.html](https://cwe.mitre.org/data/definitions/200.html)
* Reliability: High - this alert was triggered during all of my brute force attempts



**HTTP Request Size Monitor**

HTTP Request Size Monitor is implemented as follows:

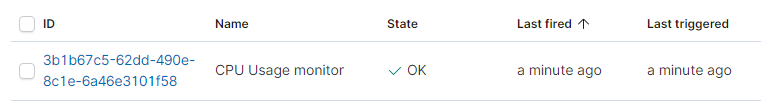
* Metric: Sum of http request bytes for the last minute
* Threshold: 3500
* Vulnerability Mitigated:
  + CWE-284: Improper Access Control [https://cwe.mitre.org/data/definitions/284.html](https://cwe.mitre.org/data/definitions/200.html)
  + DDOS attack risk
* Reliability: High



**CPU Usage Monitor**

CPU Usage Monitor is implemented as follows:

* Metric: max system processes cpu total percentage for the last 5 minutes
* Threshold: 0.5%
* Vulnerability Mitigated:
  + CWE-307: Improper Restriction of Authentication Attempts [https://cwe.mitre.org/data/definitions/307.html](https://cwe.mitre.org/data/definitions/200.html)
* Reliability: High



## 

## Suggestions for Going Further

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:

##### **CWE-521:Weak Password Requirements; CWE-306: Missing Authentication for Critical Function; CWE-307: Improper Restriction of Excessive Authentication Attempts**

* Patch:
  + Adjust Password parameters
  + Password lockout after 3 attempts
  + Set an alarm that is activated if the number of 401 HTTP status codes issued in 10 second intervals reaches 5.
  + Set an alarm that is activated if the “user\_agent.original” field detects “hydra” in its result.
* Why It Works:
  + Adjusting password parameters and setting a password lockout inhibits brute force attacks
  + An alarm will alert for a brute force attack and allow the company to act quickly and stop the attack and block the attacking IP from further attacks.

##### 

##### **CWE-200: Exposure of Sensitive Information to an Unauthorized Actor; CWE-284: Improper Access Control; CWE-552: Files or Directories Accessible to External Parties**

* Patch:
  + Secure installation of MYSQL with cmd: sudo-mysql-secure-installation
  + Proper encryption of sensitive data
  + An alarm that alerts when any non-specified IP address requests access to a hidden directory.
* Why It Works:
  + Secure installation of MYSQL will harden the MYSQL database in a cost effective and efficient way. It secures passwords and allows for encryption of information on the database.
  + Properly encrypting sensitive data will stop hackers from gaining access to files or directories that may have been password protected but the passwords were located somewhere else and improperly encrypted
  + An alarm enables someone to act quickly and identify information about the incoming attack, stop it from happening, and block it from occurring in the future

**CWE-261: Weak Encoding for Password;**

**CWE-326: Inadequate Encryption Strength;**

**CWE-328: Reversible One-Way Hash;**

**CWE-916: Use of Password Hash with Insufficient Computational Effort**

* Patch:
  + Better encryption of sensitive documents such as RSA keys
  + An alarm that is activated if the number of 401 HTTP status codes issued in 10 second intervals reaches 5.
* Why It Works:
  + RSA keys and other encryption techniques are a much stronger way of encrypting data than a reversible one-way hash. Implementing these forms of encryption ensures there is no unauthorised access to sensitive data and at the very least acts as a deterrent to potential attackers.
  + If hashes are used for encrypting sensitive data, this alarm will inhibit the hash from being cracked via brute force by john the ripper.

The system needs to have all security and integrity patches installed and it is strongly suggested to use a recognised public source of guidance for hardened builds, such as the Centre for Internet Security.