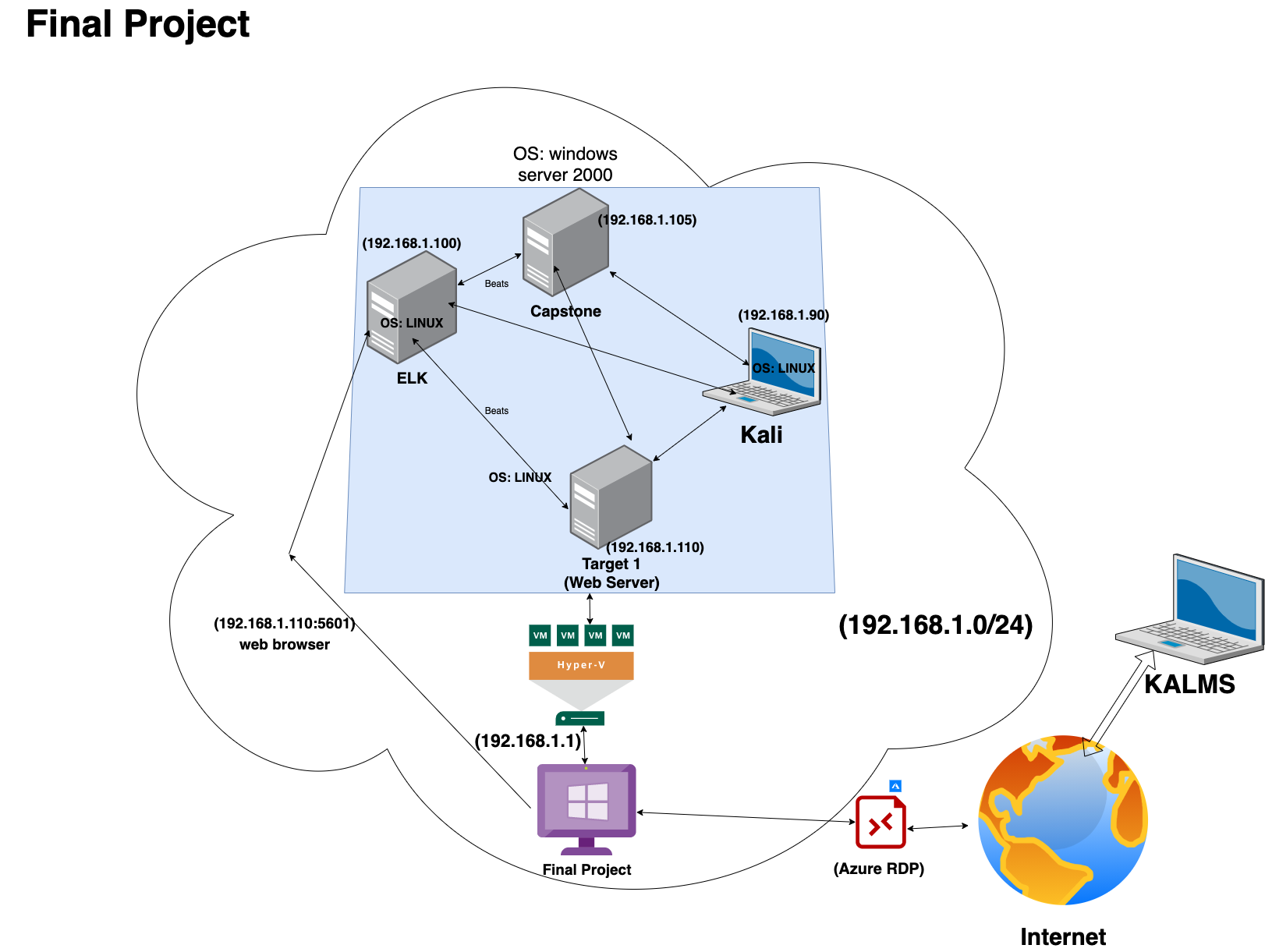
# **Blue Team: Summary of Operations**

## **Table of Contents**

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

### **Network Topology**

**Network

Address Range:192.168.1.0/24

Netmask:255.255.255.0

Gateway:192.168.1.1

The following machines were identified on the network:

* Name of VM 1: ELK
  + **Operating System**:Linux
  + **Purpose**:Monitoring
  + **IP Address**:192.168.1.100
* Name of VM 2: Target 1
  + **Operating System**:Linux
  + **Purpose**:runs alerts
  + **IP Address**:192.168.1.110
* Name of VM 3: Capstone
  + **Operating System**:Windows
  + **Purpose**:alerts implemented
  + **IP Address**:192.168.1.105
* Name of VM 4:Kali
  + **Operating System**:Kali Linux
  + **Purpose**:attacking machine
  + **IP Address**:192.168.1.90.

### **Description of Targets**

The target of this attack was: Target 1 ( IP Address ; 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**

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

#### **Excessive HTTP Errors** (This alert Triggers when the grouped count over top 5 https status response code exceeds 400 in the last 5 minutes)

Alert 1 is implemented as follows:

* **Metric**: Packetbeat
* **Threshold**: 400
* **Vulnerability Mitigated**: Brute force attack (CWE-307): An attacker could perform an arbitrary number of authentication attempts using different passwords, and eventually gain access to the targeted account.
* **Reliability**: high reliability.

#### **HTTP Request Size Monitor**

Alert 2 is implemented as follows:

* **Metric**: Packetbeat-7.7.0-2021.03.19-000001
* **Threshold**: Total Http requests bytes is above 3500 for last minute
* **Vulnerability Mitigated**: SQL Injection (CWE-89)
* **Reliability**: medium to high reliability.

#### 

*CPU Usage Monitor*

Alert 3 is implemented as follows:

* **Metric**: Metricbeat
* **Threshold**: 0.5 (When max() of system.process.cpu.total.pct over all documents is above 0.5 for the last 5 minutes)
* **Vulnerability Mitigated**: DDOS (CWE400)Crash, Exit, or Restart; DoS: Resource Consumption (CPU); DoS: Resource Consumption (Memory); DoS: Resource Consumption (Other)
* **Reliability**: TODO: Does this alert generate lots of false positives/false negatives? Rate as low, medium, or high reliability.

### **Suggestions for Going Further (Optional)**

* Each alert above pertains to a specific vulnerability/exploit. Recall that alerts only detect malicious behavior, but do not stop it. For each vulnerability/exploit identified by the alerts above, suggest a patch. E.g., implementing a blocklist is an effective tactic against brute-force attacks. 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, identified by the alerts above. 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 Attack**

* **Patch:** Ensure passwords are complex, use two factor authentication, and make the root user inaccessible via SSH
* **Why It Works:** Complex passwords are harder to guess and take much longer to guess. Using two factor authentication makes it much harder for malicious parties to get access to the clients server and finally, hackers that can log in to the server through roots account via SSH can cause damage and so it saves trouble to disallow root access via SSH
* **How to install it :**

nano /etc/ssh/sshd\_config

(change) #PermitRootLogin yes (to) PermitRootLogin no

/etc/init.d/sshd restart

systemctl restart sshd

service sshd restart

**Vulnerability:** DDOS Attack

* **Patch:** There are no reliable patches or software updates that have been proven to control DDOS attacks but there are DDoS mitigation services, e.g cloudflare.
* **Why It Works:** DDOS mitigation services, detect suspected DDOS attacks, reroute them, and use machine learning to adapt to the attack pattern. There are so many services offering this real time DDOS protection but for a price of $20/month minimum.

**Patch Commands**

* sudo apt update && sudo apt -y upgrade (Update/Upgrade Software)
* sudo apt purge application (Removing and Re-Installing apps)
* sudo apt update
* sudo apt install application

Some of the issue to high CPU usage can be related to not updated/upgraded software that might have new patches that make the software more efficient. Another problem could be improperly installed code. By using the patch above one can update all the system software. If this does not work then we can move on by uninstalling and reinstalling the given program, to see if the issue was a problem in the way it was originally installed.