**Blue Team: Summary of Operations**

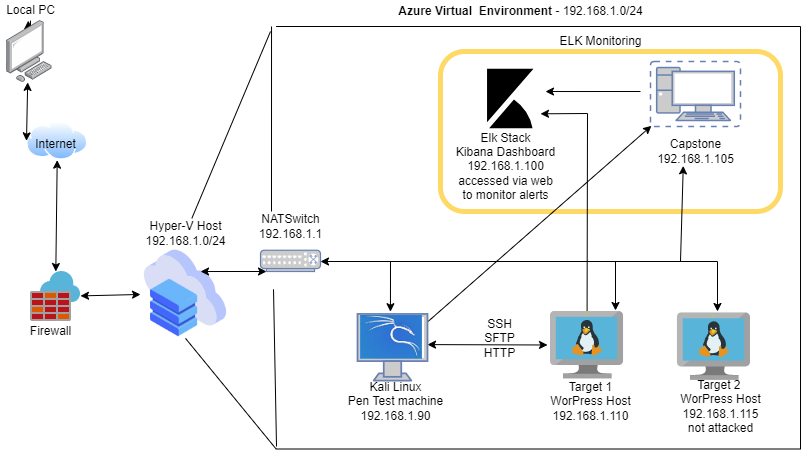
**Table of Contents**

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

**Network Topology**

The following machines were identified on the network:

* Name of VM1: Kali
  + **Operating System**: Kali Linux 5.4.0
  + **Purpose**: attacking vulnerable machines
  + **IP Address**: 192.168.1.90
* Name of VM2: ELK
  + **Operating System**: Linux
  + **Purpose**: Hold Kibana/Elasticsearch dashboards for monitoring
  + **IP Address**:192.168.1.100
* Name of VM3: Capstone
  + **Operating System**: Linux
  + **Purpose**: track system logs through Filebeat and Metricbeat and forward those logs to the ELK machine
  + **IP Address**: 192.168.1.105
* Name of VM4: Target1
  + **Operating System**: Linux 3.16.0 - Debian
  + **Purpose**: target machine – Wordpress host
  + **IP Address**: 192.168.1.110
* Name of VM5: Target 2
  + **Operating System**: Linux 3.2 – 4.9
  + **Purpose**: target machine
  + **IP Address**: 192.168.1.115

****

**Description of Targets**

The target of this attack was: 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**

Alert 1 is implemented as follows:

* **Metric**: when count is grouped over the top 5 ‘http.response.status.code’
* **Threshold**: above 400 for the last 5 minutes
* **Vulnerability Mitigated**: enumeration and brute force attacks
* **Reliability**: This alert is highly reliable. Monitoring by 400 and above error codes will filter normal traffic. Error codes 400 and above are either client or server error responses

A group of computer screens

Description automatically generated with medium confidence

**HTTP Request Size Monitor**

Alert 2 is implemented as follows:

* **Metric**: when sum of http.request.bytes over all documents
* **Threshold**: above 3500 for the last 1 minute
* **Vulnerability Mitigated**: This helps to mitigate against Denial of Service attacks as well as Malicious software uploads.
* **Reliability**: Reliability is rated as medium as some false positives may arise. It is possible that large, viable, non-malicious HTTP traffic could occur, but it is safer to monitor large sized HTTP traffic.

**CPU Usage Monitor**

Alert 3 is implemented as follows:

* **Metric**: when max of system.process.cpu.total.pct over all documents
* **Threshold**: is above .5 for the last 5 minutes
* **Vulnerability Mitigated**: Alert is used to mitigate malicious software uploads, manage resource availability and SYN Flood attacks, which can keep resources occupied, limiting resource availability.
* **Reliability**: This is medium-high reliability. Monitoring CPU usage helps ensure the network is up and running allowing for normal traffic speeds.

**Suggestions for Going Further**

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:

* Port scan
  + **Patch**: Install or strengthen firewalls and internal reporting
  + **Why It Works**: firewalls help protect the internal network and can block outside sources from scanning for available ports.
* Sudo Commands
  + **Patch**: configure sudoers file to limit root access
    - Specifically for this example, remove Steven’s access to python
  + **Why It Works**: A properly configured sudoers file restricts privilege escalation, limiting how much a user can access and change.

A group of computer screens

Description automatically generated with low confidence

* Brute Force attack
  + **Patch**: Establish strong password policy, requiring:
    - Minimum length at least 15 characters, discourage using personal factors
    - Password history of at least 10
    - Minimum password age of at least 3 days
    - Enable multi-factor authentication
  + **Why It Works**: Establishing stronger password policies reduces the risk of brute force attacks. Longer passwords are less susceptible to brute force attacks. Combining password history and minimum age for passwords reduces the risk of quick re-use of an older password. Multi-factor authentication helps to mitigate the risk of lost or stolen passwords.