Blue Team: Summary of Operations Chad Skeen

#### 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:

- ELK Stack

- Operating System: Ubuntu 18.04.4 LTS ELKK tty1

- Purpose: Store logs, access, and visualize data in a program using KBL

- IP Address: 192.168.1.100

- Capstone

- \*\*Operating System\*\*: Linux server1 4.15.0-108-generic

- \*\*Purpose\*\*: Testing the alerts

- \*\*IP Address\*\*: 192.168.1.105

- Kali Linux

- \*\*Operating System\*\*: Linux Kali 5.4.0-kali3-amd64 #1 SMP

- \*\*Purpose\*\*: Penetration Testing

- \*\*IP Address\*\*: 192.168.1.90

- Target 1

- \*\*Operating System\*\*: Linux target1 3.16.0-6-amd64 SMP

- \*\*Purpose\*\*: Wordpress server

- \*\*IP Address\*\*: 192.168.1.110

#### Description of Targets

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

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() GROUPED OVER top 5 ‘http.response.status\_code’ IS ABOVE 400 FOR THE LAST 5 minutes

- Threshold: 400 Instances

- Vulnerability Mitigated: Alerts and protects from brute force activity

- Reliability: This alert is reliable and recommended strategy of cyber defense. High level of reliability.

HTTP Request Size Monitor:

Alert 2 is implemented as follows:

- Metric: WHEN sum() OF http.request.bytes OVER all documents IS ABOVE 3500 FOR THE LAST 1 minute

- Threshold: 3500 Bytes of information or 3.5KB

- Vulnerability Mitigated: Alerts and protects from malicious network activity deemed irregular for our purposes.

- Reliability: Medium rate of reliability, some activity may be generated by administrators, threat actors should trigger alerts.

CPU Usage Monitor

Alert 3 is implemented as follows:

- Metric: WHEN max() OF system.process.cpu.total.pct OVER all documents IS ABOVE 0.5 FOR THE LAST 5 minutes

- Threshold: 0.5

- Vulnerability Mitigated: Any activity that can generate heat over 0.5 is known to be irregular and should be triggered by threat actors.

- Reliability: Medium rate of reliability, some activity like updates and maintenance could trigger this.

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

- Patch: Tracing and reporting the known IP addresses the attack is coming from in an automated process or application. Active monitoring as well greatly increases the chances of having security breaches go undetected.

- Why It Works: Active monitoring ensures real-time reports and services can be provided to the network infrastructure.

- Vulnerability 2

- Patch: Custom baseline dashboard in SIEM tools.

- Why It Works: Establishing a baseline in these tools mitigates the risk of brute force activity or any irregular traffic the administrators identify.

- Vulnerability 3

- Patch: Active CPU Thermal Monitoring

- Why It Works: Some breaches done over the network can be extremely small and difficult to trace over live-monitoring. Establishing programs that monitor the CPU temperature of the servers and databases ensures that malicious software installed onto the machine are not capable of utilizing extra resources without notifying administrators.