Final Project: Blue Team-Summary of Operations

**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:

* Azure VM (ML-RefVm-684427)
  + **Operating System**: Windows
  + **Purpose**: Azure VM (ML-RefVm-684427) is used to connect to all of the virtual machines.
  + **IP Address**: 192.168.1.1

A screenshot of a computer

Description automatically generated with medium confidence



Kali

* + **Operating System**: Linux
  + **Purpose**: Kali is used to attack the Target 1 machine and access it’s data.
  + **IP Address**: 198.162.1.90

A screen shot of a computer

Description automatically generated with low confidence

**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:

Text

Description automatically generated

**Monitoring the Targets**

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

**Name of Alert 1**

Alert 1 is implemented as follows: HTTP Request Size Monitor (cd2f862d-380a-4cb4-98ee-a95bdc82f472)

* **Metric**: HTTP Request Size within the last minute
* **Threshold**: 3500
* **Vulnerability Mitigated**: Nmap
* **Reliability**: During the course of attacking target 1 there were a total of 21 hits exceeding the threshold. The rate of reliability is high.

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

**Name of Alert 2**

Alert 2 is implemented as follows: CPU Usage Monitor ( 80134c0b-d18e-4954-ba3b-f96dfff0f5a3)

* **Metric**: CPU Processing usage
* **Threshold**: 0.5 within the last 5 minutes
* **Vulnerability Mitigated**: CPU Meltdown
* **Reliability**: During the course of attacking target 1 there were 30 hits for CPU usage exceeding the threshold of 0.5 for CPU Usage. This resulted in a lot of false positives. This makes reliability of the alerts medium. The threshold should be changed to a higher threshold for more accurate results.

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

**Name of Alert 3**

Alert 3 is implemented as follows: Excessive HTTP Errors (fc4df62f-dbbd-4d57-ac73-bd55ad47c774)

* **Metric**: HTTP Errors
* **Threshold**: Above 400 within the last 5 minutes
* **Vulnerability Mitigated**: XSS
* **Reliability**: During the attack on target 1 there were a total of 39 hits meaning a higher rate of false positives. The reliability of this alert is very low and should be changed for more accurate results.

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

**Suggestions for Going Further (Optional)**

*TODO*:

* 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: Nmap
  + **Patch**: Turning off the organizations ICMP would result in no port information being exposed.
  + **Why It Works**: With the ICMP being turned off to outside sources this makes it harder for a breach or attack because port and system information isn’t exposed.
* Vulnerability 2
  + **Patch**: All data should be moved form WordPress (MySQL) to a more secure database.
  + **Why It Works**: Wordpress is an open-source CMS with hundreds of vulnerabilities making it easier for attackers to get privileged information to be able to remotely log into the organizations servers to access data.
* Vulnerability 3
  + **Patch**: User log in information should be changed regularly, have special requirements (length, characters, capital letter etc.) and a lock out policy.
  + **Why It Works**: Using brute force tools such as John the Ripper makes user log in information susceptible for attacker to access.