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

TODO: Fill out the information below.

The following machines were identified on the network:

**Target 1**

* Operating System: WIN 6.1 (Samba 4.2.14-Debian)
* Purpose:
* IP Address: 192.168.1.110

**[Name of VM 2]**

* Operating System:
* Purpose:
* IP Address: 192.168.1.115
* Etc.

Including a Gliffy or draw.io diagram is optional but highly encouraged.

Description of Targets

Fill in the following:

* Two VMs on the network were vulnerable to attack: Target 1 IP192.168.1.110 and Target 2 IP192.168.1.115
* Each VM functions as an Apache web server and has SSH enabled, so ports 80 and 22 are possible ports of entry for attackers.

Monitoring the Targets

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

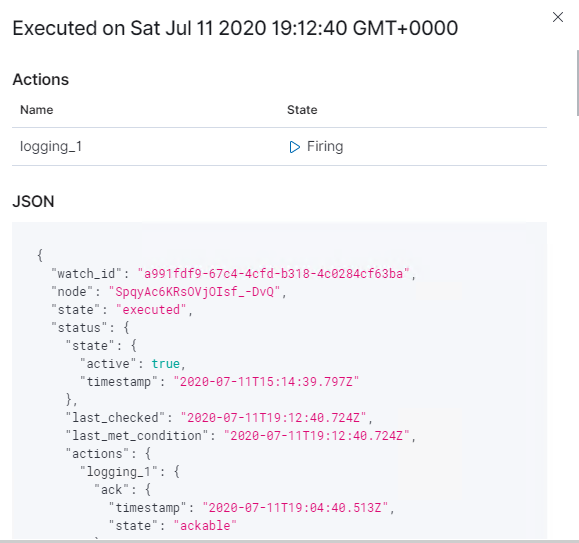
* **Target 1**
  + List ofPotentially vulnerableServices: SSH, HTTP
* **Target 2**
  + List of Potentially vulnerable Services: SSH, HTTP

Traffic to these services should be carefully monitored. To this end, we have implemented the alerts below: (Note: Add at least three alerts. You can add more if time allows.)

**Alert 1**

**HTTP Request Size** **Monitor** is implemented as follows:

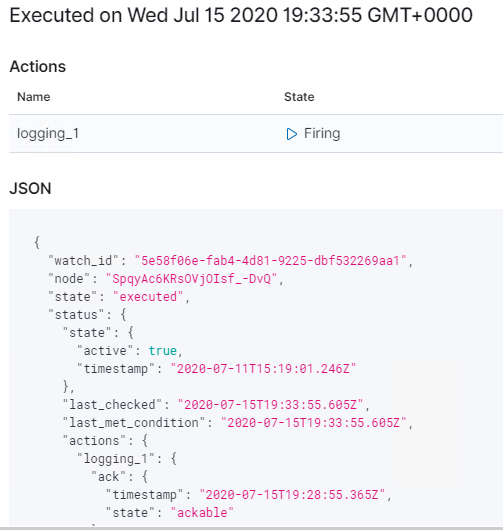
* Metric: http request bytes
* Threshold: >3500 per 1 minute
* Vulnerability Mitigated: Identify potentially malicious file transfers.
* Reliability: TODO: Does this alert generate lots of false positives/false negatives? I would say yes, b/c I see it firing at times when it should not have.
* LOW RELIABILITY



**Alert 2**

**CPU Usage Monitor** is implemented as follows:

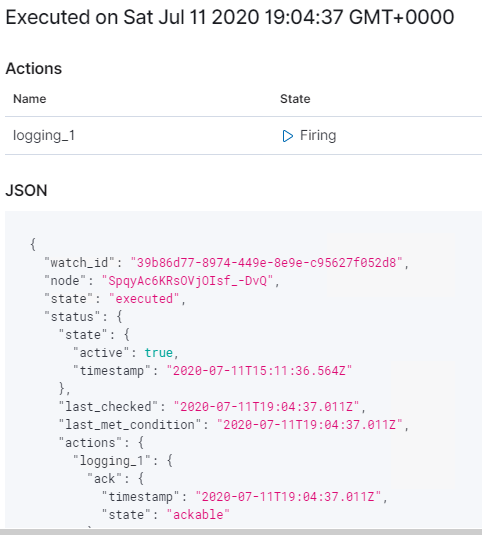
* Metric: system cpu total pct
* Threshold: > .5 (>50% usage) per 5 minutes
* Vulnerability Mitigated: Identifies when a machine might go offline, or when a malicious user is hijacking it for their own purposes.
* Reliability: TODO: Does this alert generate lots of false positives/false negatives? Low number of false positives, I see some times when it fires and it should not have.
* MEDIUM RELIABITY



**Alert 3**Excessive HTTP Errors is implemented as follows:

* Metric: HTTP Error responses
* Threshold: >400 over 5 minutes
* Vulnerability Mitigated: Identifies brute force attacks, directory enumerations, etc..
* Reliability: TODO: Does this alert generate lots of false positives/false negatives? No false positives.

HIGH RELIABILITY



Suggestions for Going Further

**Suggest a patch for each vulnerability identified by the alerts above.** Remember: alerts only detect malicious behavior. They do not prevent it.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. 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:

**PHPMailer 5.2.18**

* Patch: CVE 2016-10033
* Why It Works: This vulnerability constitutes [CVE-2016-10033](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-10033), and was thought to be resolved by applying [escapeshellarg()](http://php.net/manual/en/function.escapeshellarg.php) to the address, and released as PHPMailer 5.2.20, with a subsequent cleanup in [PHPMailer 5.2.21](https://github.com/PHPMailer/PHPMailer/releases/tag/v5.2.21).

**Password Policy**

* Patch: require more secure passwords and store in db with salted hashes.
* Why It Works: passwords were either easy to guess or easy to crack from the available hash.