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 VM 1** Hyper V Host Manager
  - Operating System: **Windows 10**
  - Purpose: **Contains the vulnerable machines and the attacking machine**
  - IP Address: **192.168.1.1**
- **Name of VM 2** Kali
  - Operating System: **Linux 5.4.0**
  - Purpose: **Used as attacking machine**
  - IP Address: **192.168.1.90**
- **Name of VM 3** Capstone
  - Operating System: **Linux (Ubuntu 18.04.1 LTS)**
  - Purpose: **Used as a testing system for alerts**
  - IP Address: **192.168.1.100**
- **Name of VM 4** ELK
  - Operating System: **Linux (Ubuntu 18.04.1 LTS)**
  - Purpose: **Used for gathering information from the victim machine using Metricbeat, Filebeats, and Packetbeats**
  - IP Address: **192.168.1.100**
- **Name of VM 5** Target 1
  - Operating System: **Linux 3.2 - 4.9**
  - Purpose: **The VM with WordPress as a vulnerable server**
  - IP Address: **192.168.1.110**
- **Name of VM 6** Target 2
  - Operating System: **Linux 3.2 - 4.9**
  - Purpose: **The VM with WordPress as a vulnerable server**
  - 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

- ***Metric**: WHEN count() GROUPED OVER top 5 http.response.status_code*
- ***Threshold**: IS ABOVE 400*
- ***Vulnerability Mitigated**: Enumeration/Brute Force*
- ***Reliability**: The alert is highly reliable. Measuring by error codes 400 and above will filter out any normal or successful responses. 400+ codes are client and server errors which are of more concern. Especially when taking into account these error codes going off at a high rate.*

HTTP Request Size Monitor

- ***Metric**: WHEN sum() of http.request.bytes OVER all documents*
- ***Threshold**: IS ABOVE 3500*
- ***Vulnerability Mitigated**: Code injection in HTTP requests (XSS and CRLF) or DDOS*
- ***Reliability**: Alert could create false positives. It comes in at medium reliability. There is a possibility for a large non malicious HTTP request or legitimate HTTP traffic.*

CPU Usage Monitor

- ***Metric**: WHEN max() OF system.process.cpu.total.pct OVER all documents*
- ***Threshold**: IS ABOVE 0.5*
- ***Vulnerability Mitigated**: Malicious software, programs (malware or viruses) running taking up resources*

- ***Reliability****: The alert is highly reliable. Even if there isn't a malicious program running this can still help determine where to improve on CPU usage.*

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:

- ***Excessive HTTP Errors***
  - ***Patch****: TODO: E.g., install* `special-security-package` *with* `apt-get`
  - ***Why It Works****: TODO: E.g.,* `special-security-package` *scans the system for viruses every day*
- ***HTTP Request Size Monitor***
  - ***Patch****: TODO: E.g., install* `special-security-package` *with* `apt-get`
  - ***Why It Works****: TODO: E.g.,* `special-security-package` *scans the system for viruses every day*
- ***CPU Usage Monitor***
  - ***Patch****: TODO: E.g., install* `special-security-package` *with* `apt-get`
  - ***Why It Works****: TODO: E.g.,* `special-security-package` *scans the system for viruses every day*
-