Blue Team: Summary of Operations

Table of Contents

Network Topology

The following machines were identified on the network:

[RAVEN 1 / Target 1]

- Operating System: Microsoft Windows
- Purpose: Wordpress Server
- IP Address: 192.168.1.110

[RAVEN 2 / Target 2]

- Operating System: Microsoft Windows
- Purpose: Wordpress Server (Hardened)
- IP Address: 1192.168.1.115

Description of Targets

Fill in the following:

- Two VMs on the network were vulnerable to attack: Target 1 [192.168.1.110] and Target 2 [192.168.1.115].

- 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**
  - SSH - 22
  - HTTP - 80
  - 445 – Microsoft SMB

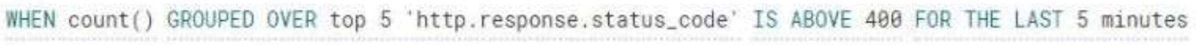
- **Target 2**
  - SSH - 22
  - HTTP - 80
  - 445 – Microsoft SMB

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

Excessive HTTP Errors

[Excessive HTTP Errors] is implemented as follows:

- Metric: By timestamp
- Threshold: 400 + HTTP requests within 5 minutes for HTTP codes in 400+ range
- Vulnerability Mitigated: Mitigation to brute force HTTP password attacks
- Reliability: As the alert was recently implemented, further analysis will be required to ensure the 400 + alerts within 5 minutes is not an excessive allowance causing attacks to go un-noticed.

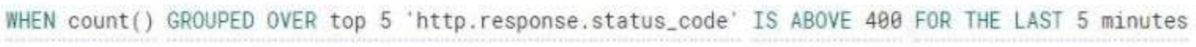


```
WHEN count() GROUPED OVER top 5 'http.response.status_code' IS ABOVE 400 FOR THE LAST 5 minutes
```

HTTP Request Size Monitor

[HTTP Request Size Monitor] is implemented as follows:

- Metric: By sum
- Threshold: HTTP request bytes of all documents is about 3500 within 1 minute
- Vulnerability Mitigated: Serves as post exploit indicator
- Reliability: In this scenario the alert proves invaluable in order to isolate relevant data to paint a picture of target and methodology used. Clear display of scouring the webserver to find vulnerabilities to further exploit the server

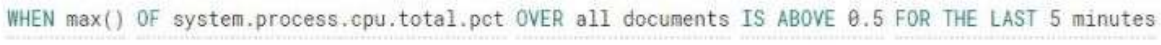


```
WHEN count() GROUPED OVER top 5 'http.response.status_code' IS ABOVE 400 FOR THE LAST 5 minutes
```

CPU Usage Monitor

[CPU Usage Monitor] is implemented as follows:

- Metric: usage maximum
- Threshold: System CPU total usage is above 50 percent for 5 minutes
- Vulnerability Mitigated: Indicator of high resource access or usage beyond normal traffic
- Reliability: The reliability of alert is highly dependent on timing and whether maintenance or modifications are being performed. These circumstances might create false alerts.



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

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:

Vulnerability 1 - SSH

- Patch: Rather than using password based SSH login, implement secure keys
- Why It Works: Even if password to be leaked or carelessly phished, it would be useless without secure key pair to access server creating a more hardened access.

Vulnerability 2 - HTTP

- Patch: Remove server version banner and directory browser listing
- Why It Works: Does not remove vulnerability but does increase time and effort required for enumeration. This also deters novice attacks as vulnerability identification is more difficult.

Vulnerability 3 – Samba SMBD

- Patch: Use host-based protection and IPC$ share deny
- Why It Works: Allowing remote connections from specific IP ranges prevents unauthorized users to access files on server. IPC$ share deny prevents remote users from seeing what shares are available on servers.