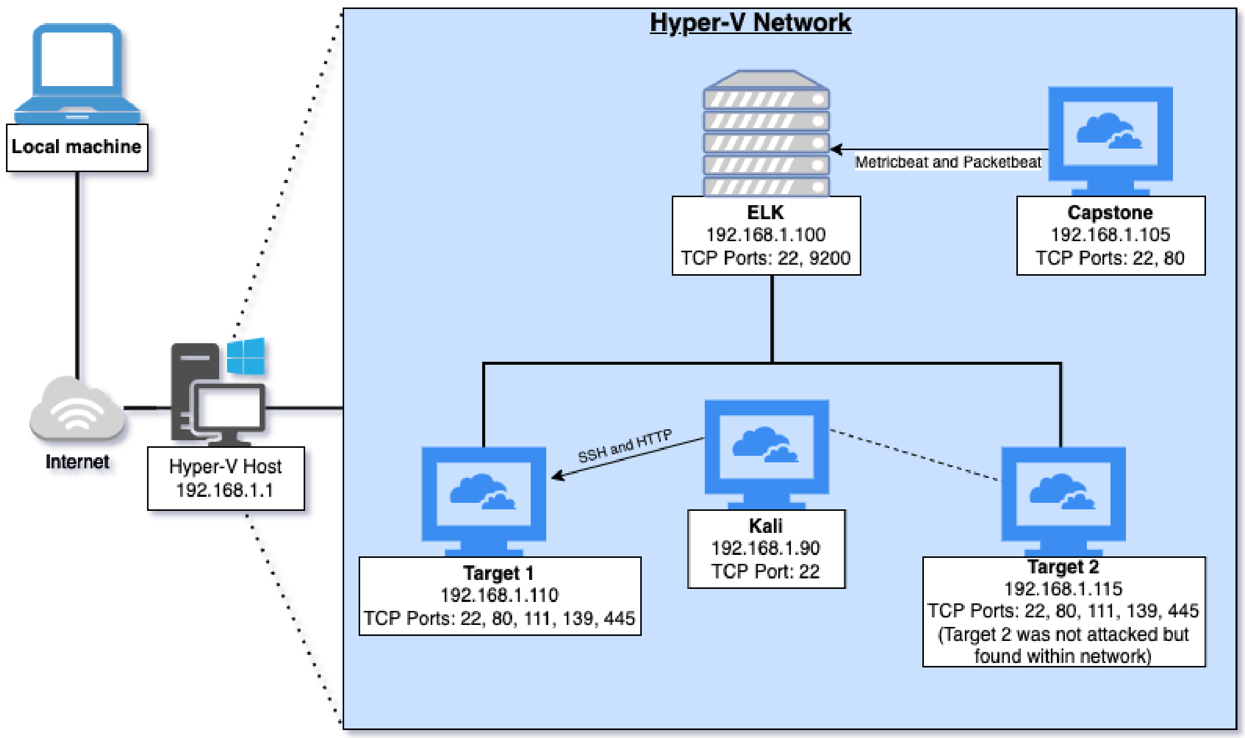
Blue Team: Summary of Operations

Table of Contents

Network Topology



The following machines were identified on the network:

- Hyper-V
  - **Operating System**: Linux
  - **Purpose**: Hosts all virtual machines within network
  - **IP Address**: 192.168.1.1

- ELK
    - **Operating System**: Linux
    - **Purpose**: Access via Web to View Alerts
    - **IP Address**: 192.168.1.100/24
- Capstone
    - **Operating System**: Linux
    - **Purpose**: Alert Testing Attack Target
    - **IP Address**: 192.168.1.105/24
- Kali
    - **Operating System**: Linux
    - **Purpose**: Pen Test machine
    - **IP Address**: 192.168.1.90/24
- Target 1
    - **Operating System**: Linux
    - **Purpose**: Target machine to attack
    - **IP Address**: 192.168.1.110/24
- Target 2
    - **Operating System**: Linux
    - **Purpose**: Target machine to attack
    - **IP Address**: 192.168.1.115/24

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:

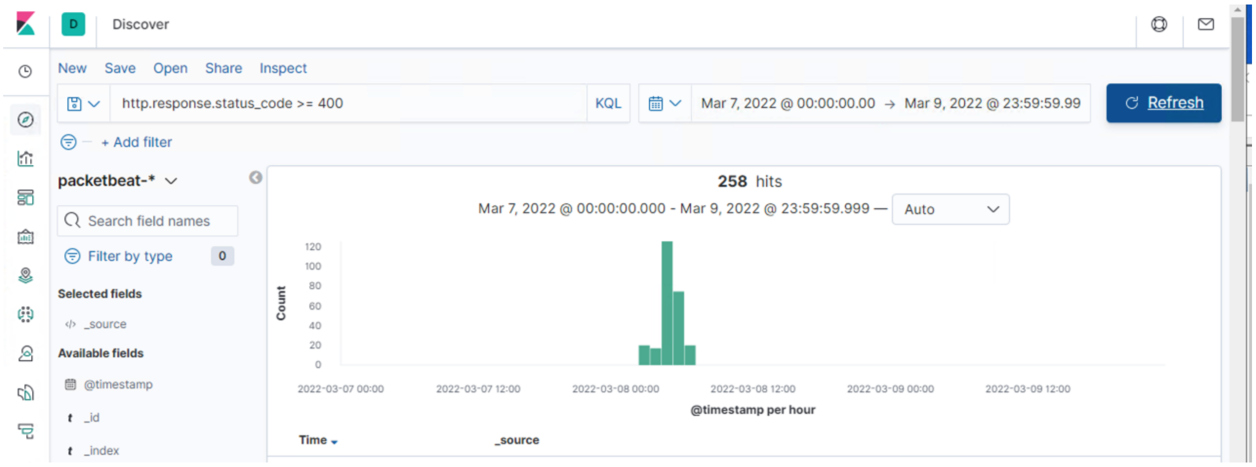
Monitoring the Targets

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

Excessive HTTP Errors

Excessive HTTP Errors is implemented as follows:

- **Metric**: WHEN count() GROUPED OVER top 5 ‘http.response.status.code’ (Packetbeat)
- **Threshold**: IS ABOVE 400 FOR THE LAST 5 minutes
- **Vulnerability Mitigated**: Enumeration
- **Reliability**: High reliability. This alert filters out successful responses. Status code 400+ are server error codes.



http.response.status_code >= 400

Mar 7, 2022 @ 00:00:00.00 → Mar 9, 2022 @ 23:59:59.99

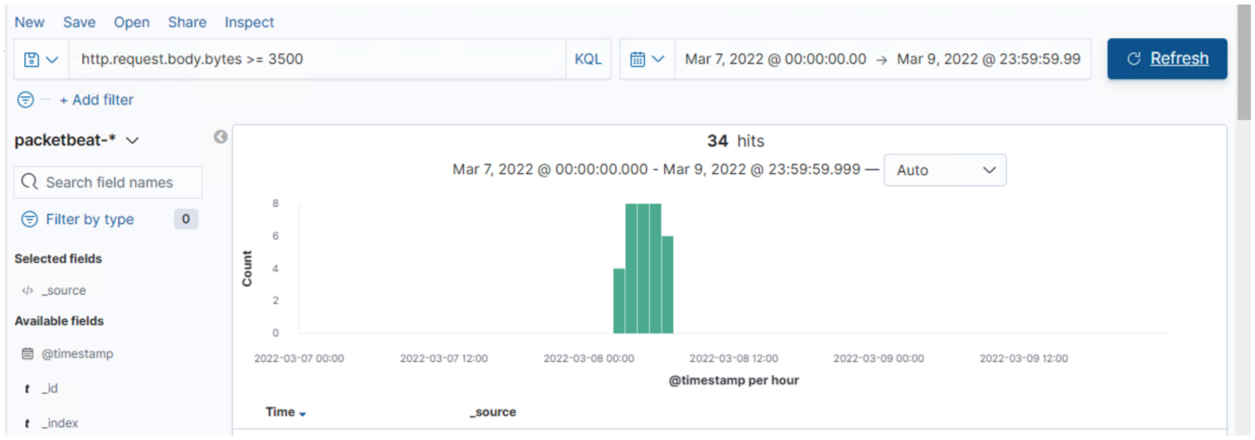
258 hits

Mar 7, 2022 @ 00:00:00.000 - Mar 9, 2022 @ 23:59:59.999

HTTP Request Size Monitor

HTTP Request Size Monitor is implemented as follows:

- **Metric**: WHEN sum() of http.request.bytes OVER all documents (Packetbeat)
- **Threshold**: IS ABOVE 3500 FOR THE LAST 1 minute
- **Vulnerability Mitigated**: The large request bytes can indicate an attack/ suspicious activity.
- **Reliability**: This alert has medium reliability as it can generate false positives indicating that the large traffic turns out to be non-malicious activity.



http.request.body.bytes >= 3500

Mar 7, 2022 @ 00:00:00.00 → Mar 9, 2022 @ 23:59:59.99

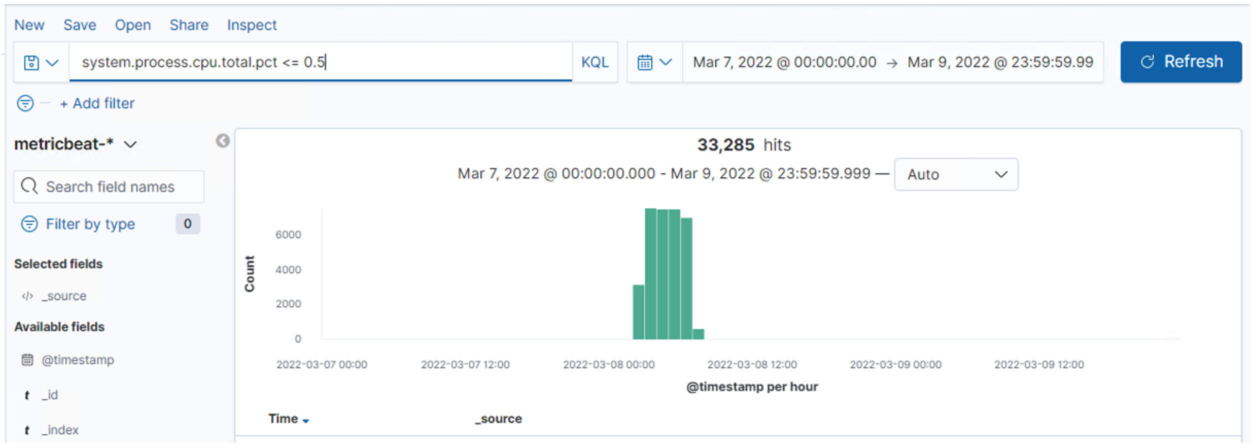
34 hits

Mar 7, 2022 @ 00:00:00.000 - Mar 9, 2022 @ 23:59:59.999

CPU Usage Monitor

CPU Usage Monitor is implemented as follows:

- **Metric**: WHEN max() OF system.process.cpu.total.pct OVER all documents (Metricbeat)
- **Threshold**: IS ABOVE 0.5 FOR THE LAST 5 minutes
- **Vulnerability Mitigated**: Malicious activity
- **Reliability**: This alert has medium to low reliability. It generated false positives that did not indicate the CPU usage was tied to malicious activity.



Suggestions for Going Further

Each alert above pertained to a specific vulnerability/exploit. These alerts only detect malicious behavior, but do not stop it. The following vulnerabilities/exploits were found:

1. Open SSH access
2. WordPress user enumeration access
3. High HTTP traffic

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**: Use TCP wrappers by editing /etc/hosts.deny and /etc/hosts.allow
  - **Why It Works**: The host-based ACL protection will help you filter who can access the OpenSSH server.
  - **Command example**: *vim -w /etc/hosts.deny*
  - **Add line within file:** *ALL : ALL*
    - This line will deny all connections from unknown hosts.

- Vulnerability 2
  - **Patch**: Install 'WP Hardening' plugin via web browser. It is free to download.
    - https://wordpress.org/plugins/wp-security-hardening/
    - After installation, go to the "*Security Fixers*" tab and select "*Stop user enumeration*"
  - **Why It Works**: WP Hardening by Astra Security is a tool that performs a real-time security audit of websites to find missing security best practices.

- Vulnerability 3
  - **Patch**: Redirect HTTP to HTTPS on Apache
    - **Command:** *sudo a2enmod rewrite*
    - *LoadModule rewrite_module modules/mod_rewrite.so*
    - Edit/ create .htaccess file in your domain root directory and add the following:
    - *RewriteEngine On*
    - *RewriteCond %{HTTPS} !=on*
    - *RewriteRule ^/?(.*) https://%{SERVER_NAME}/$1 [R,L]*
  - **Why It Works**: Redirecting HTTP traffic to HTTPS will increase security of the overall website. Port 80 is unsecure therefore redirecting the data from the website will encrypt it, which provide more confidentiality than those without. Only your browser and the website's server can decrypt the information you provide.