Blue Team: Summary of Operations

Table of Contents

Network Topology

The following machines were identified on the network:

- Name of VM 1: ML-RefVm-684427
    - **Operating System**: Windows 10
    - **Purpose**: Host machine, contains Hyper-V Manager for the other VM's
    - **IP Address**: 192.168.1.1
    - Subnet Mask: 255.255.255.0
    - Gateway: 10.0.0.1
- Name of VM 2: Capstone
    - **Operating System**: Linux 4.15.0
    - **Purpose**: Targeting machine / apache server
    - **IP Address**: 192.168.1.105
- Name of VM 3: ELK
    - **Operating System**: Linux 4.15.0
    - **Purpose**: Network monitor / Kibana
    - **IP Address**:192.168.1.100
- Name of VM 4: Kali
    - **Operating System**: Linux 4.15.0
    - **Purpose**: Attacking machine / Penetration testing
    - **IP Address**: 192.168.1.90
- Name of VM 5: Target 1
    - **Operating System**: Linux 4.15.0
    - **Purpose**: Vulnerable server
    - **IP Address**:192.168.1.110
- Name of VM 6: Target 2
    - **Operating System**: Linux 4.15.0
    - **Purpose**: Vulnerable server
    - **IP Address**: 192.168.1.115

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:

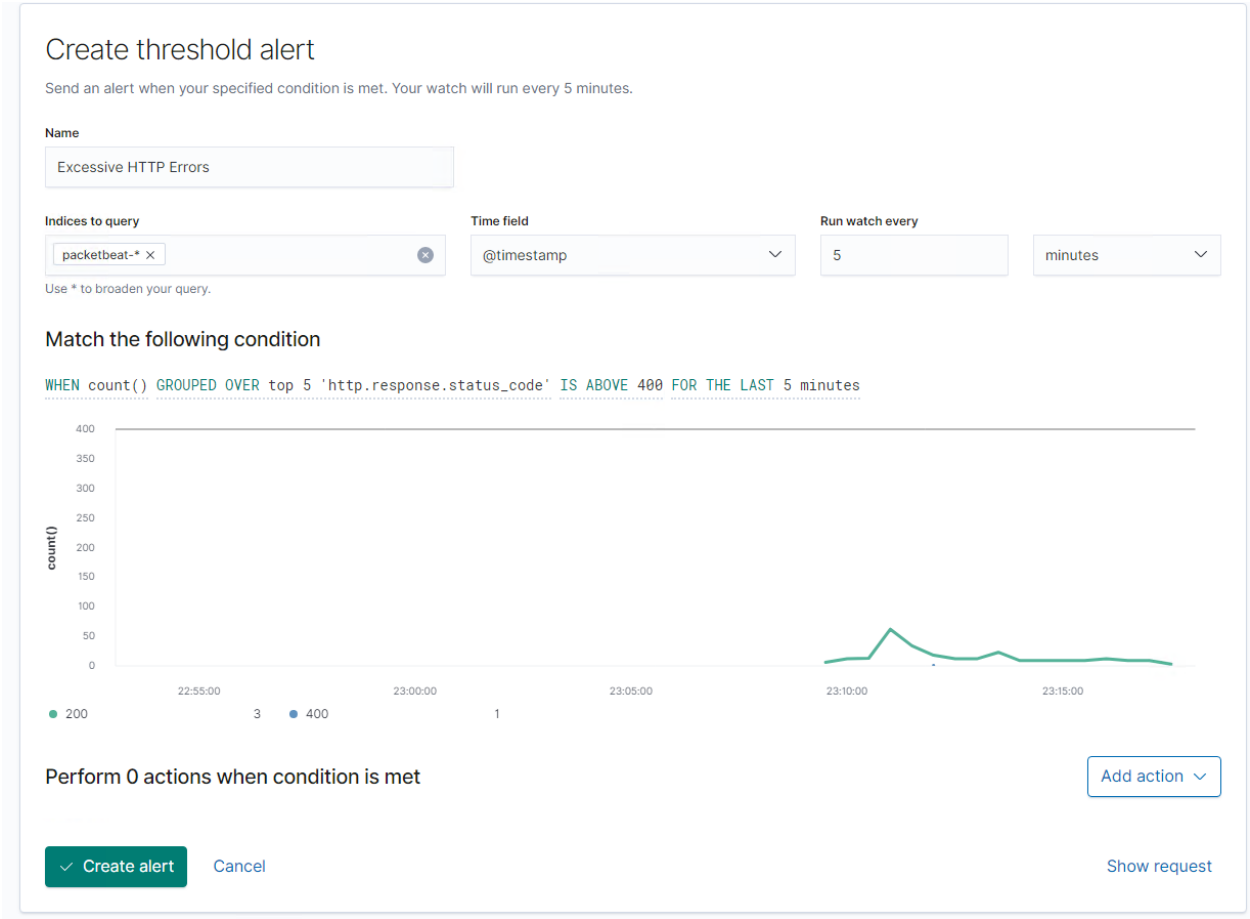
Monitoring the Targets

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

Alert 1: Excessive HTTP Errors

Excessive HTTP Errors is implemented as follows:

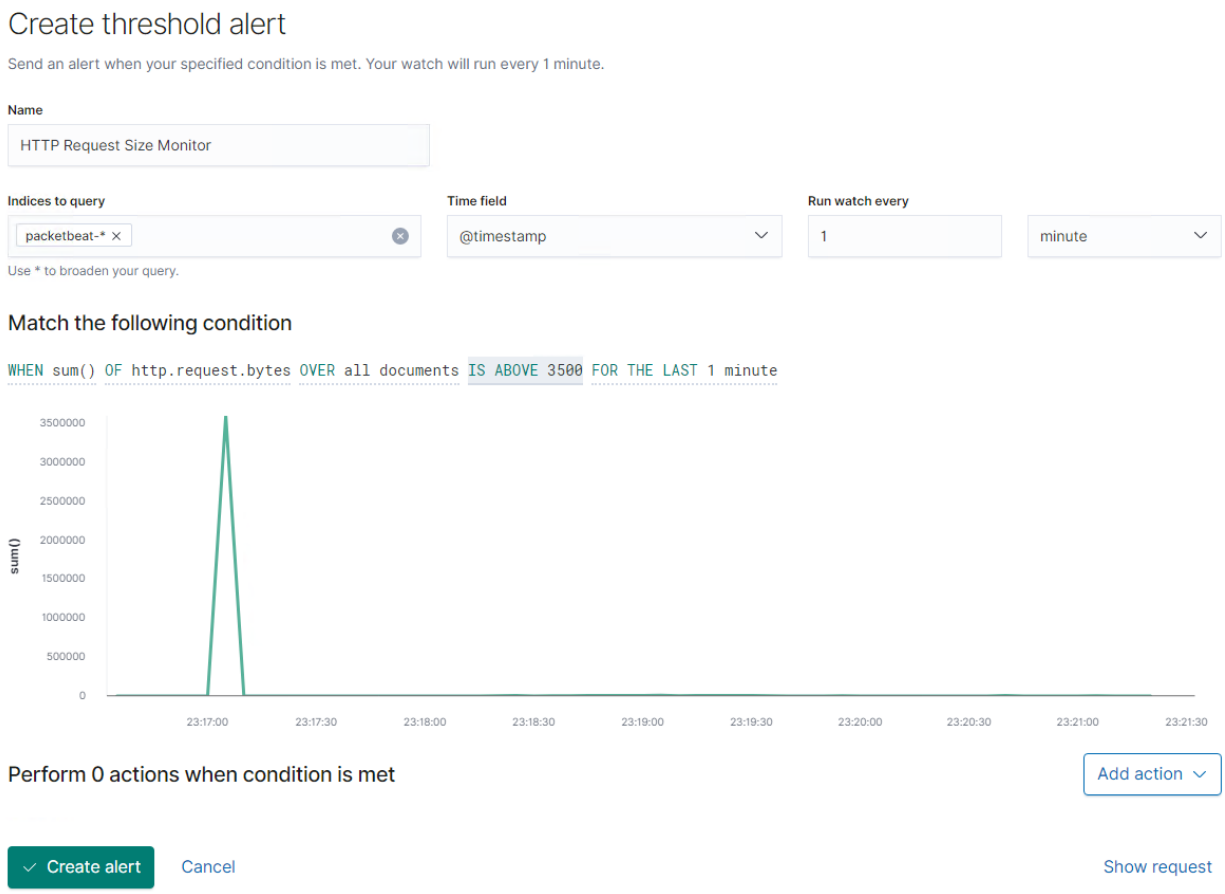
- **Metric**: Packetbeat, http.response.status_code
- **Threshold**: WHEN count() GROUPED OVER top 5 'http.response.status_code' IS ABOVE 400 FOR THE LAST 5 minutes
- **Vulnerability Mitigated**: Brute Force Attack
- **Reliability**: High reliability. This alert measures the error code of above 400 HTTP codes which detects client and server errors.



Alert 2: HTTP Request Size Monitor

HTTP Request Size Monitor is implemented as follows:

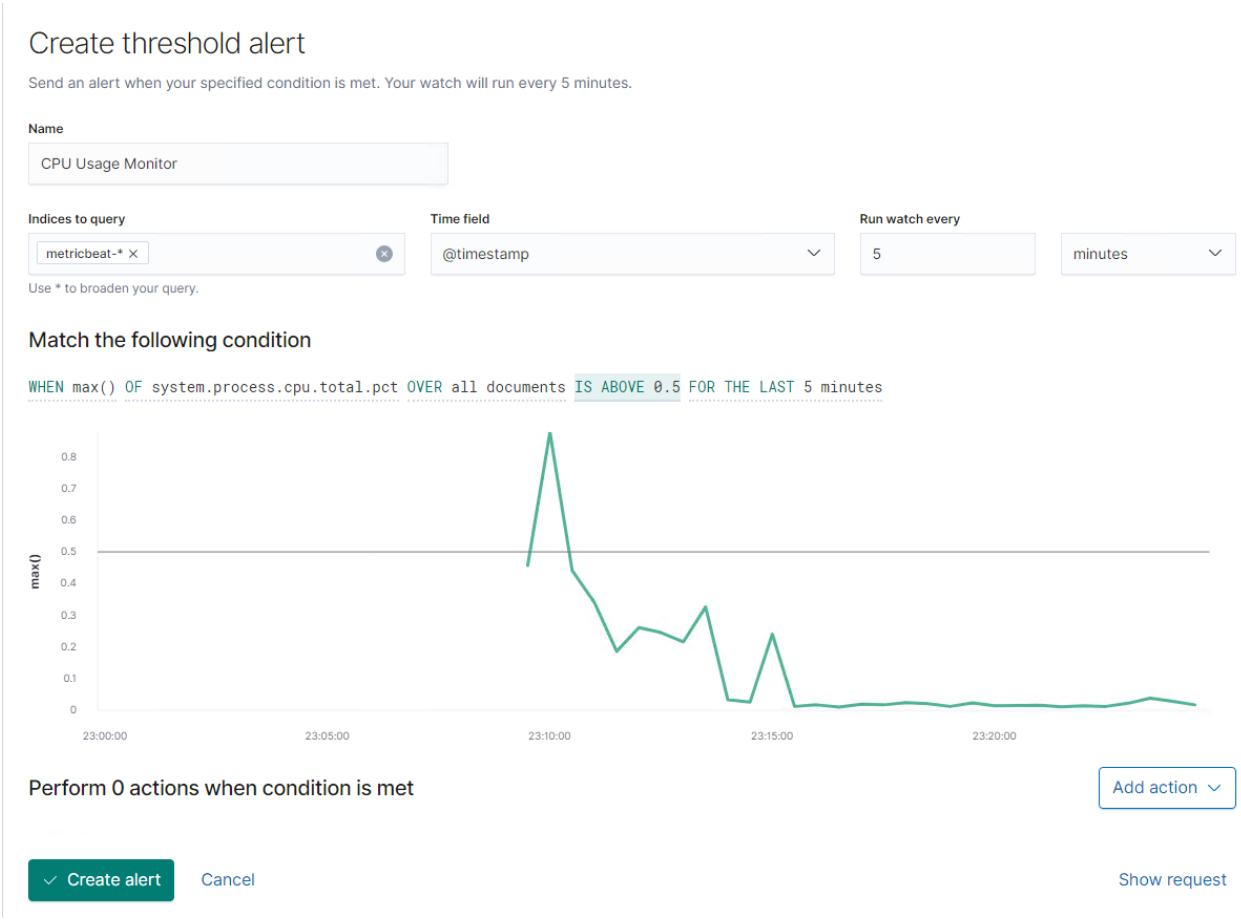
- **Metric**: Packetbeat, http.request.bytes
- **Threshold**: WHEN sum() of http.request.bytes OVER all documents IS ABOVE 3500 FOR THE LAST 1 minute
- **Vulnerability Mitigated**: HTTP request smuggling, denial of service attacks
- **Reliability**: Medium reliability. This alert does not generate excessive amount of false positives due to denial of service attacks that occurs seconds.



Alert 3: CPU Usage Monitor

CPU Usage Monitor is implemented as follows:

- **Metric**: Packetbeat, system.process.cpu.total.pct
- **Threshold**: WHEN max() OF system.process.cpu.total.pct OVER all documents IS ABOVE 0.5 FOR THE LAST 5 minutes
- **Vulnerability Mitigated**: Malware programs that take up a lot of resources and CPU usage
- **Reliability**: High reliability. Effective tool that will detect if any malicious activity is happening on your CPU. Good to maintain appropriate 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:

- Vulnerability 1: Excessive HTTP Errors
    - **Patch**: Install SSHGuard with apt-get install sshguard
    - **Why It Works**: SSHGuard is a fast and lightweight monitoring open source tool that helps monitor and protect web servers from brute force attacks using log activities. SSHGuard will block by inputting IP addresses in iptables.
- Vulnerability 2: HTTP Request Size Monitor
    - **Patch**: Install NGINX with apt-get install nginx

    - **Why It Works**: NGINX is an open source tool with HTTP and reverse proxy server, mail proxy server and generic TCP/UDP proxy server. Known for its high performance, stability and simple configuration with low resource consumption to help prevent DDoS attacks. It will limit the rate of requests by configuring to allow whichever client IP address you want to access.
- Vulnerability 3: CPU Usage Monitor
    - **Patch**: Install SNORT with
        - wget https://www.snort.org/downloads/snort/snort-2.9.20.tar.gz
        - tar xvzf snort-2.9.20.tar.gz
        - cd snort-2.9.20
        - ./configure --enable-sourcefire && make && sudo make install
    - **Why It Works**: Having an Intrusion Prevention System such as Snort is equipped with rules to detect malicious activities so you can stop going inside your computer by setting predefined rules. Snort contains packet sniffer, logger, and a system-wide full-time network IPS Tool.

References

Atienza, J. (n.d.). *Prevent Brute Force Attacks Using These Tools*. Unixmen. Retrieved August 24, 2022, from https://www.unixmen.com/prevent-brute-force-attacks-using-these-tools/

Home. (n.d.). YouTube. Retrieved August 24, 2022, from https://snort-org-site.s3.amazonaws.com/production/document_files/files/000/012/147/original/Snort_3.1.8.0_on_Ubuntu_18_and_20.pdf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAU7AK5ITMJQBJPARJ%2F20220824%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=

Installing NGINX Open Source | *NGINX Plus*. (n.d.). NGINX Docs. Retrieved August 24, 2022, from https://docs.nginx.com/nginx/admin-guide/installing-nginx/installing-nginx-open-source/