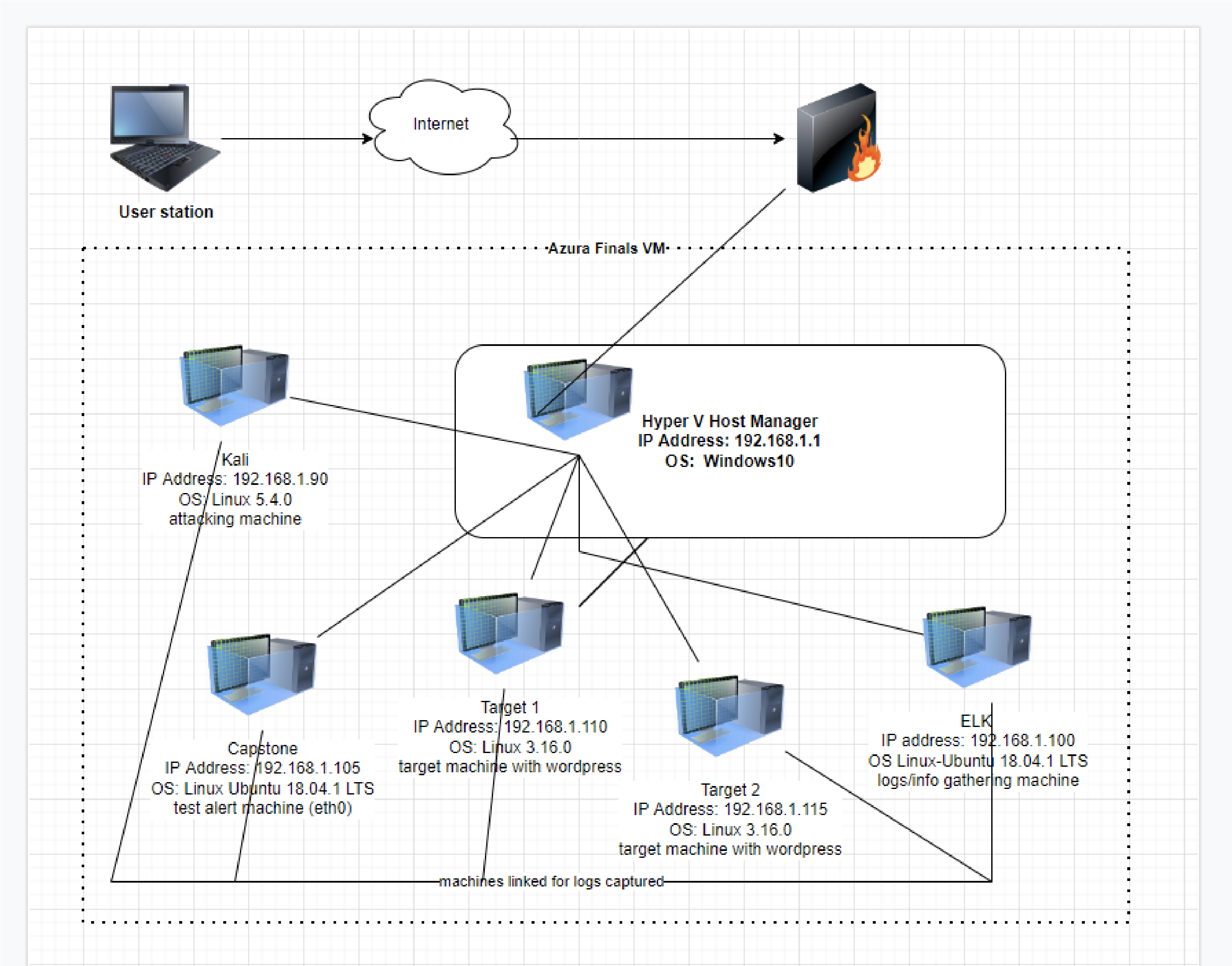
Blue Team: Summary of Operations

Table of Contents

Network Topology


User station
Internet
Azura Finals VM
Hyper V Host Manager
IP Address: 192.168.1.1
OS: Windows10
Kali
IP Address: 192.168.1.90
OS: Linux 5.4.0
attacking machine
Capstone
IP Address: 192.168.1.105
OS: Linux Ubuntu 18.04.1 LTS
test alert machine (eth0)
Target 1
IP Address: 192.168.1.110
OS: Linux 3.16.0
target machine with wordpress
Target 2
IP Address: 192.168.1.115
OS: Linux 3.16.0
target machine with wordpress
ELK
IP address: 192.168.1.100
OS Linux-Ubuntu 18.04.1 LTS
logs/info gathering machine
machines linked for logs captured

Description of Targets

- Name of VM 1: Hyper V Host Manager
  Operating System: Windows 10
  Purpose: contain all VMs below, including target and attacking machine
  IP Address: 192.168.1.1
- Name of VM 2: Kali
  Operating system: Linux 5.4.0
  Purpose: use as attacking machine
  IP Address: 192.168.1.90
- Name of VM 3: Capstone
  Operating System: Linux-Ubuntu 18.04.1 LTS
  Purpose: use for test system for alerts (eth0)
  IP Address: 192.168.1.105
- Name of VM 4: ELK
  Operating System: Linux-Ubuntu 18.04.1 LTS
  Purpose: use for information gathering from target machine using, metricbeat, packetbeat and filebeat
  IP Address: 192.168.1.100
- Name of VM 5: Target 1
  Operating System: Linux 3.16.0
  Purpose: target machine with wordpress as vulnerable server
  IP Address: 192.168.1.110
- Name of VM 6: Target 2
  Operating System:Linux 3.16.0
  Purpose: target machine with wordpress as vulnerable server
  IP Address:192.168.1.115

The target of this attack was: `Target 1` 192.168.1.110

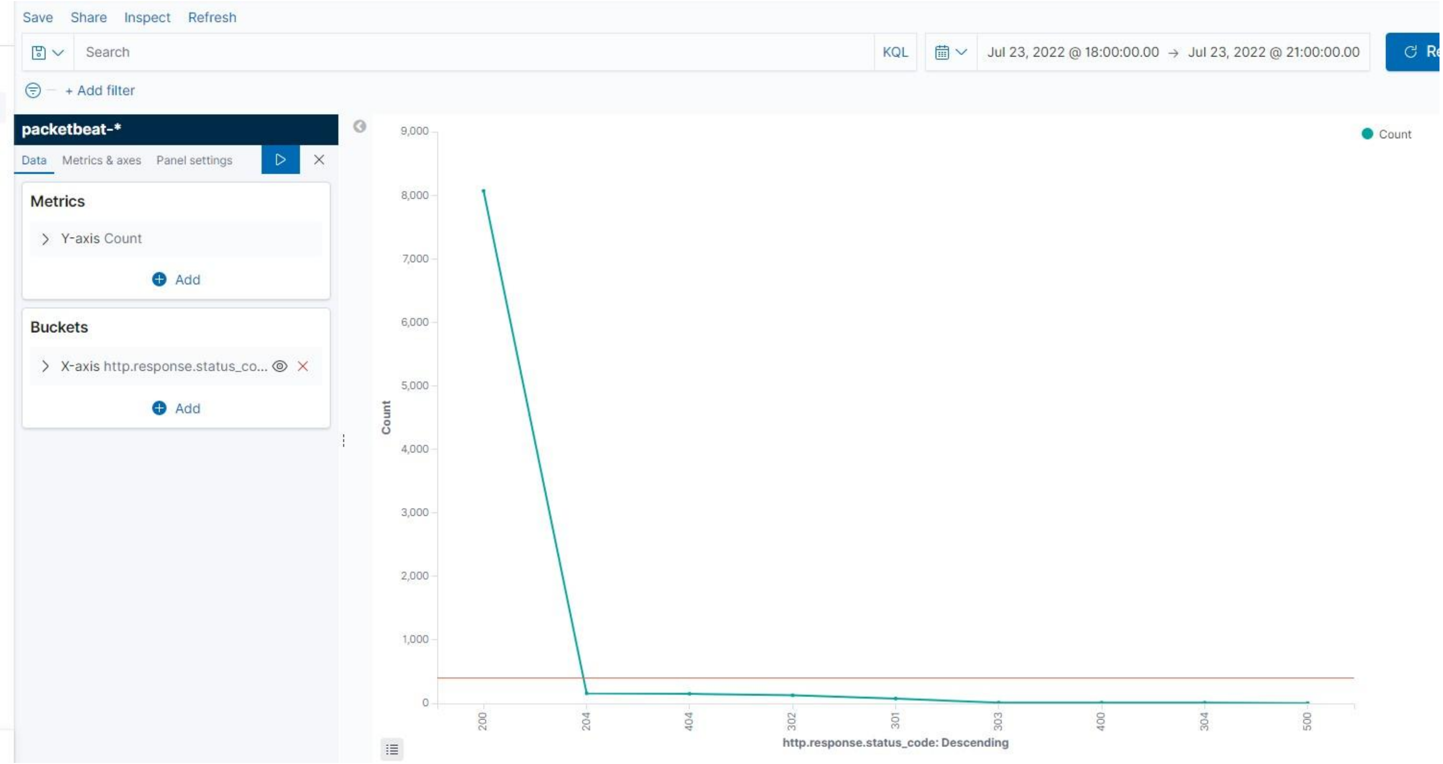
Target 1 is an Apache web server and has SSH enabled, so ports 80 and 22 are possible ports of entry for attackers. As such, the following alerts have been implemented:

Monitoring the Targets

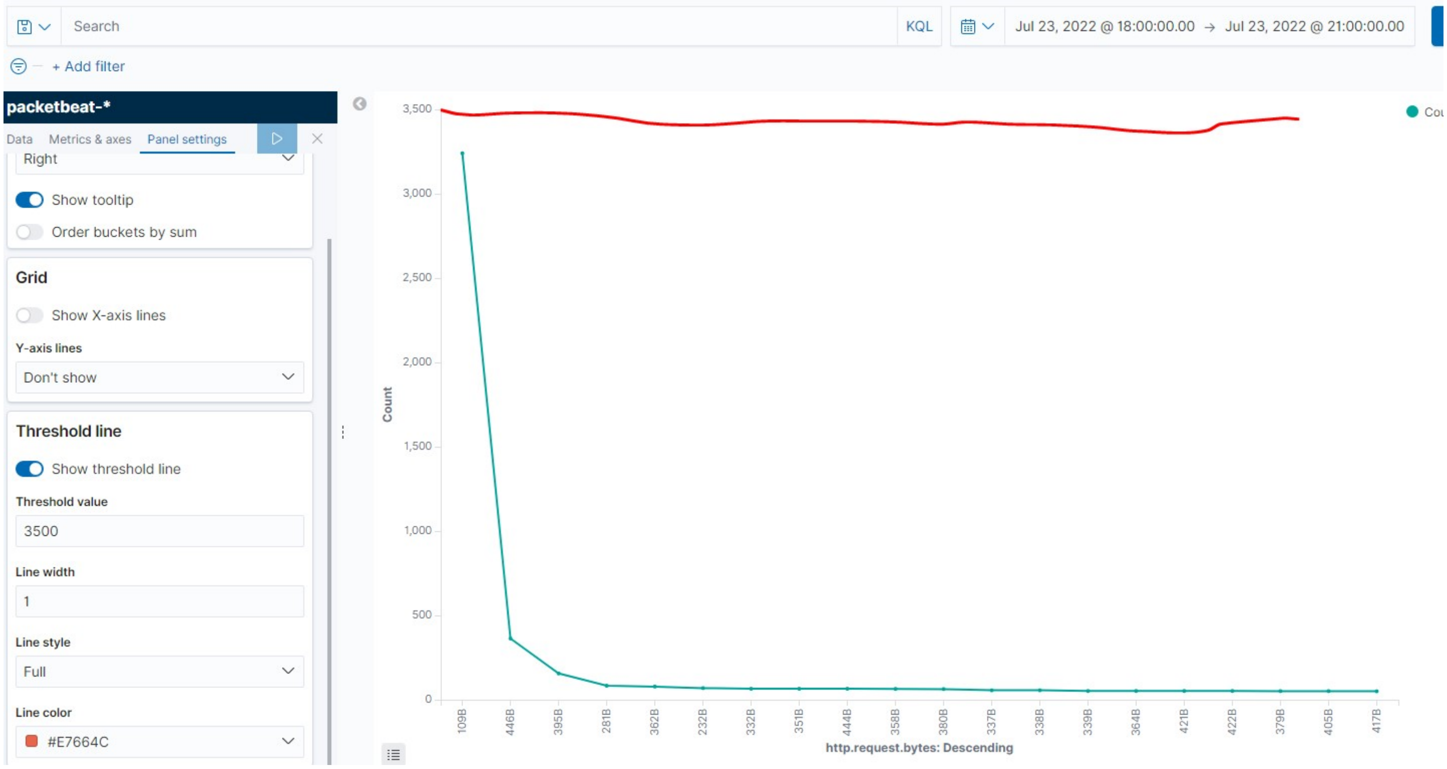
Traffic to these services should be carefully monitored. To this end, we have implemented the alerts below:

Excessive HTTP Errors

Excessive HTTP Errors is implemented as follows:
  - **Metric**: packetbeat - 'http.response.status_code' >400
  - **Threshold**: WHEN count() GROUPED OVER top 5 IS ABOVE 400 FOR THE LAST 5 minutes
  - **Vulnerability Mitigated**:
    Use IPS to detect/prevent suspicious IP access
    Use public/private keys with SSH
    Disable/close port 22 SSH ports
    Lock user accounts when x amount of attempts are triggered within x minutes
  - **Reliability**:No, this alert will not generate a high amount of false positive for brute force attacks based on the threshold it's set. Medium reliability is where I think the alert is as it detected some, but not enough to trigger the alert.



HTTP Request Size Monitor
Alert 2 is implemented as follows:
  - **Metric**: packetbeat - ' http.request.bytes' > 3500
  - **Threshold**: WHEN sum() of OVER all documents IS ABOVE 3500 FOR THE LAST 1 minute
  - **Vulnerability Mitigated**:with more precise control over the request bytes (lower threshold) and timing of the report set at higher frequency (10 second), this will give a better indication from sudden spikes in traffic, thus potentially triggering the alert earlier.
  - **Reliability**: No, this alerts generates information by the minute when attacks are usually by the seconds; also there are excessive false position, again due to threshold size and timing of the alert. Low reliability for this alert as the perimeter of the alert is too big to detect attacks in a timely manner.



Jul 23, 2022 @ 18:00:00.00 → Jul 23, 2022 @ 21:00:00.00

packetbeat-*

Right

● Show tooltip

○ Order buckets by sum

Grid

○ Show X-axis lines

Y-axis lines: Don't show

Threshold line

● Show threshold line

Threshold value: 3500

Line width: 1

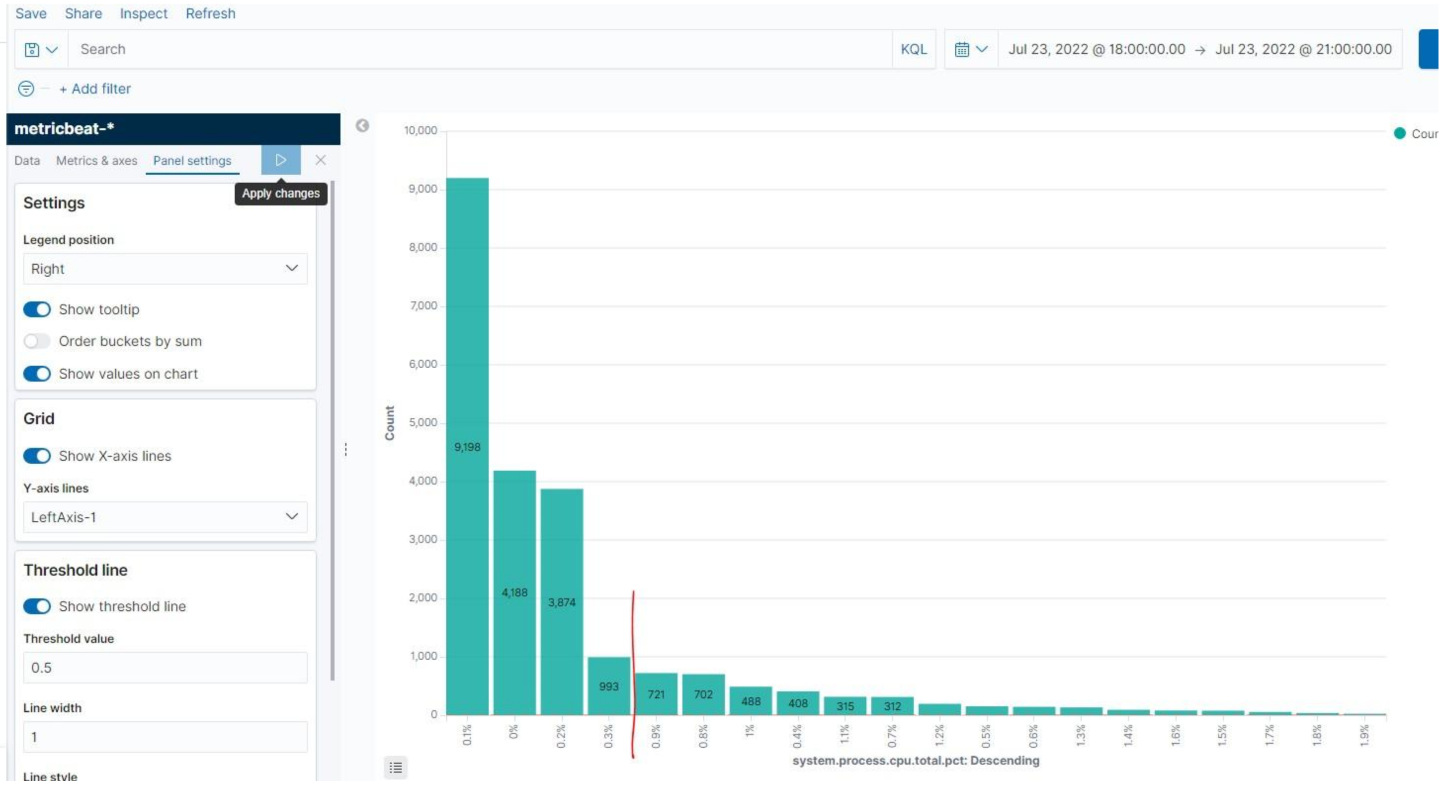
Line style: Full

Line color: 🟥 #E7664C

CPU Usage Monitor

Alert 3 is implemented as follows:

- **Metric**: metricbeat - 'system.process.cpu.total.pct' > 0.5
- **Threshold**: WHEN max() OF OVER all documents IS ABOVE 0.5 FOR THE LAST 5 minutes
- **Vulnerability Mitigated**:This alert does indeed shows CPU usage but threshold needs to be set higher (30% or higher) to avoid massive false positive. it also can extend the time threshold to 10 mins to avoid the trigger being set off by high demand processing programs
- **Reliability**: No, this alert generates massive false positive as starting up applications or general usgae will cause a spike, making it very difficult to pin point if system is under attack or not . High reliability.



Settings

Legend position: Right

Show tooltip: on

Order buckets by sum: off

Show values on chart: on

Grid

Show X-axis lines: on

Y-axis lines: LeftAxis-1

Threshold line

Show threshold line: on

Threshold value: 0.5

Line width: 1

Line style

TODO Note: Explain at least 3 alerts. Add more if time allows.

Suggestions for Going Further (Optional)

- Wordpress Enumeration and Brute Force Attacks
  - **Patch**: Suggest user to change password every 60 days
    System user lockout after 5 fail attempts with 3 minutes
    Use SSH public/private keys for encryption access
    Stronger, complex passwords combine with multi-factor authenication
  - **Why It Works**: with password changes, it will help to eliminate previous known access and a cost effective solution. System user lockout is a basic counter measure to prevent brute force attack from trigging; stronger, complex password provides additional challenge for brute attacks and also helps to provide opportunities for pre-set alerts to trigger. using public/private SSH will ensure secured connection from the remote host and limits to a single machine access
- Code injection in HTTP and MySQL
  - **Patch**:Setup input validation
    create a pre-approved list of possible inputs
    Disable any non-preauthorized file type uploads
    Sanitize all inputs
  - **Why It Works**: Sanitize inputs will help to weed out any HTM codes fro m being entered; combine with pre-approved list and disable non-preauthorized file uploads will increase the changes of system security and prevent malicious attempts. Finally, input validation will prevent improper formatted data to be entered into system
- Antivirus software
  - **Patch**: install antivirus, use window defender
  - **Why It Works**: besides firewalls, antivirus software daily scans can help to discover loopholes or malicious files/programs running in the background. it'a an added tool on top of network security to help cover and detect places overlooked through initial setup or user errors (USB hacking, phishing, social engineering, etc)