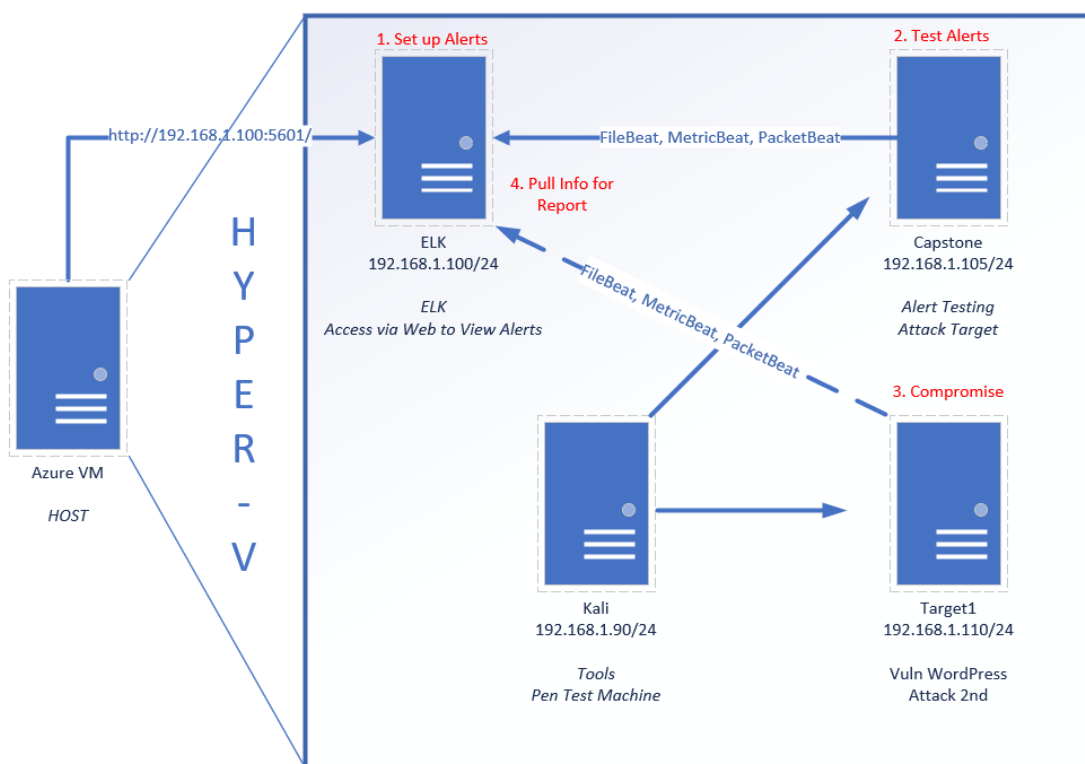


Defensive: Summary of Operations

Table of Contents

- Network Topology
- Description of Targets
- Monitoring the Targets
- Patterns of Traffic & Behavior
- Suggestions for Going Further

Network Topology



The following mach

```
File  Actions  Edit  View  Help

root@Kali:~# nmap -sV 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2022-02-26 10:43 PST
Nmap scan report for 192.168.1.110
Host is up (0.0024s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
80/tcp    open  http         Apache httpd 2.4.10 ((Debian))
111/tcp   open  rpcbind      2-4 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 00:15:5D:00:04:10 (Microsoft)
Service Info: Host: TARGET1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://
/nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.13 seconds
root@Kali:~#
```

lines

were identified on the network:

- Name of VM 1: **Target 1**
 - **Operating System:** **Linux**
 - **Purpose:** **Word press server**
 - **IP Address:** **192.168.1.110**
- Name of VM 2
 - **Operating System:**
 - **Purpose:**
 - **IP Address:**
- Etc.

Description of Targets

TODO: Answer the questions below.

The target of this attack was: Target 1 **ip. 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:

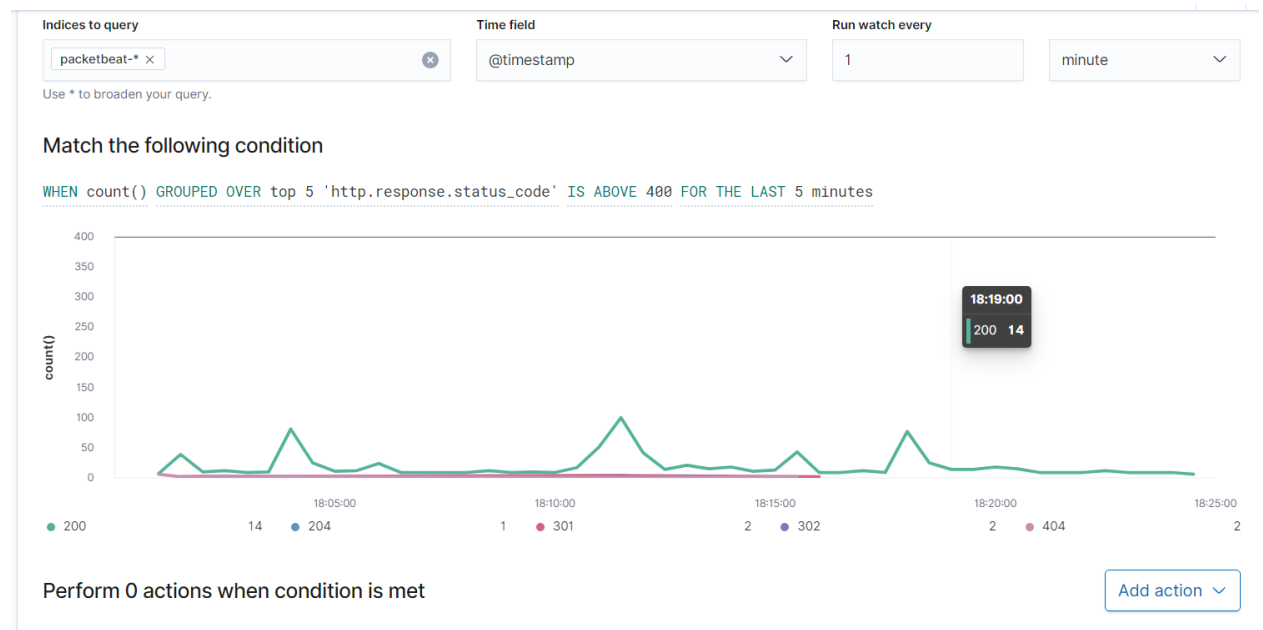
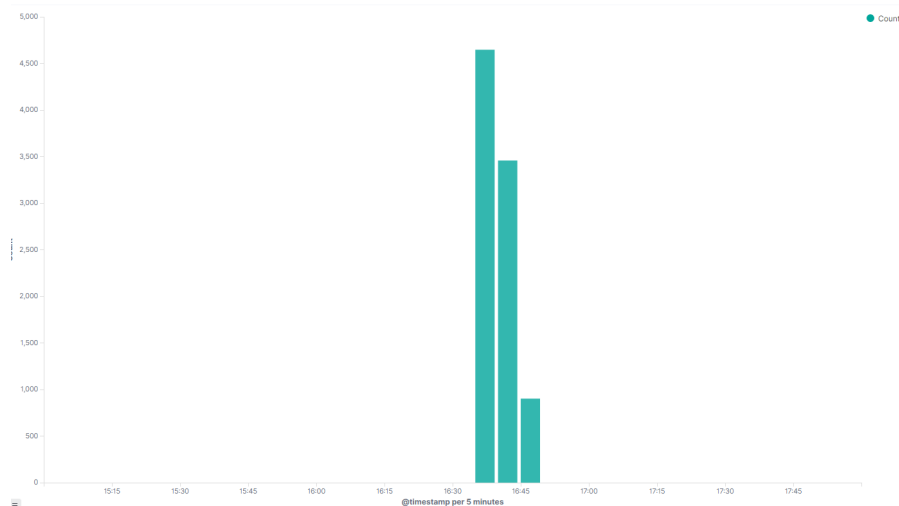
Monitoring the Targets

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

Name of Alert 1

Excessive HTTP Errors is implemented as follows:

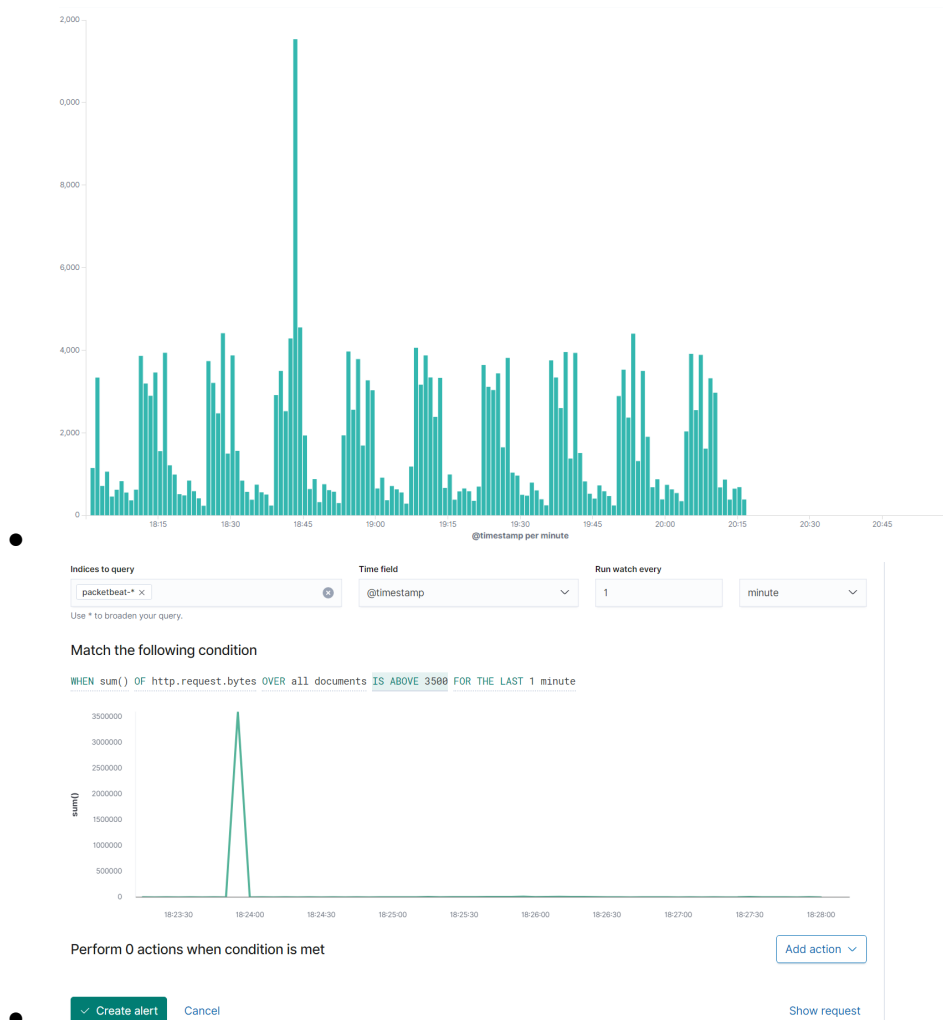
- **Metric:** packetbeat
- **Threshold:** `http.response.status_code > 400`
- **Vulnerability Mitigated:** `http.response.status_code`
- **Reliability:** This alert does not generate false positives. I feel that it is a highly reliable alert for monitoring a brute force attack.
-



Name of Alert 2

HTTP Request Size Monitor is implemented as follows:

- **Metric:** Packetbeat
- **Threshold:** 3500 hits in 1 min
- **Vulnerability Mitigated:** http.request.bytes
- **Reliability:** No false positives. I feel the reliability is medium due to the number of hits over 3500 but not much higher than 5000.

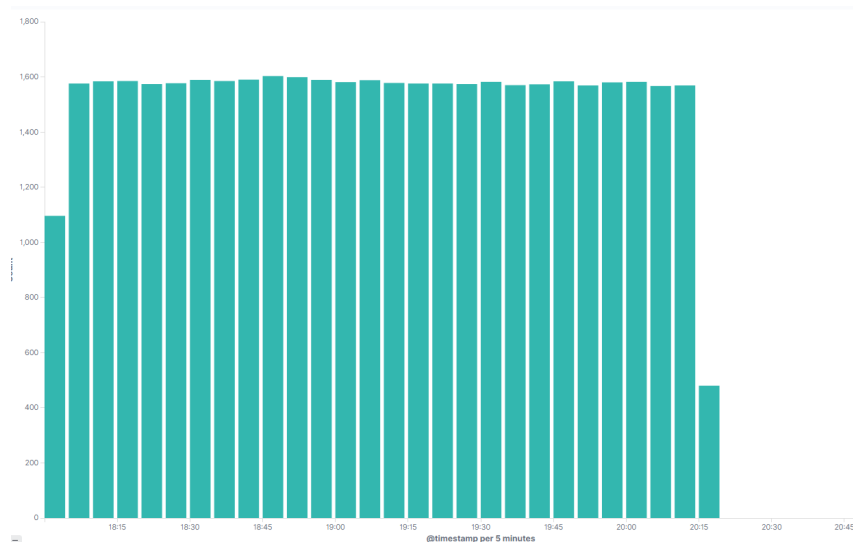


Name of Alert 3:

CPU Usage Monitor is implemented as follows:

- **Metric:** metricbeat
- **Threshold:** 0.5 usage every 5 minutes
- **Vulnerability Mitigated:** system.process.cpu.total.pct

- **Reliability:** TODO: This alert will generate a lot of false positives. I would rate this alert low.



Indices to query: Time field: Run watch every:

Match the following condition

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

Perform 0 actions when condition is met

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

Suggestions for Going Further (Optional)

TODO:

- 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
 - **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*
- Vulnerability 2
 - **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*
- Vulnerability 3
 - **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*