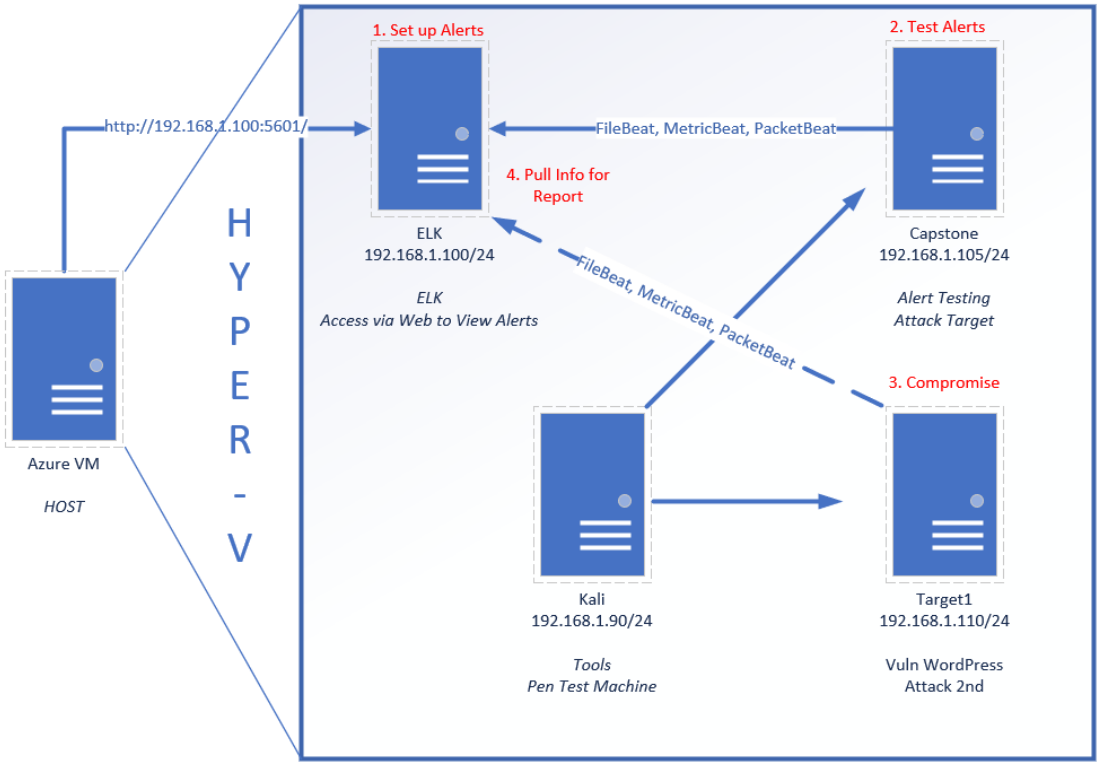
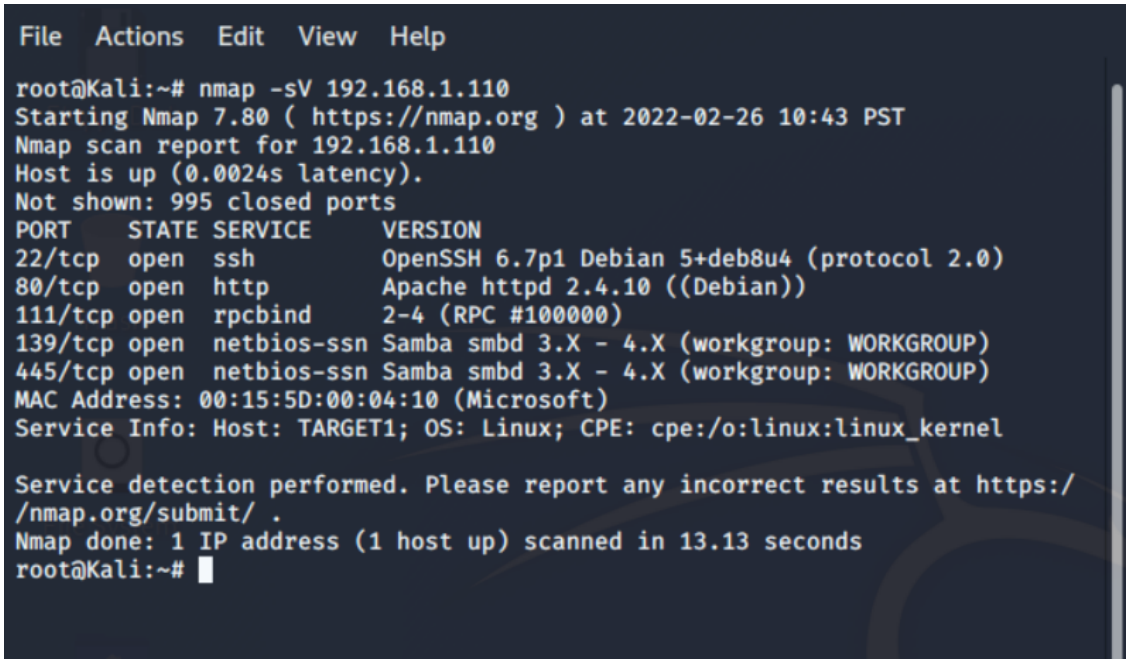
Defensive: Summary of Operations

Table of Contents

Network Topology



The following mach



ines 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:

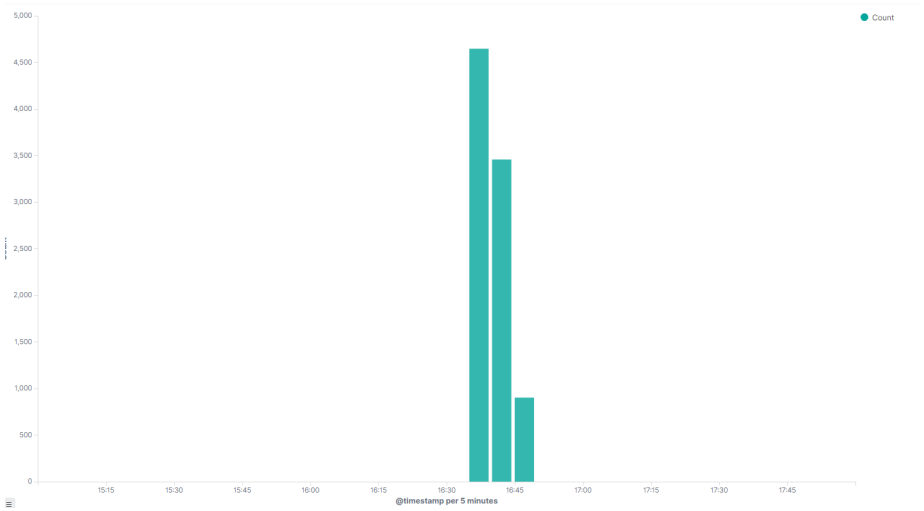
Monitoring the Targets

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.respnose.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.
-



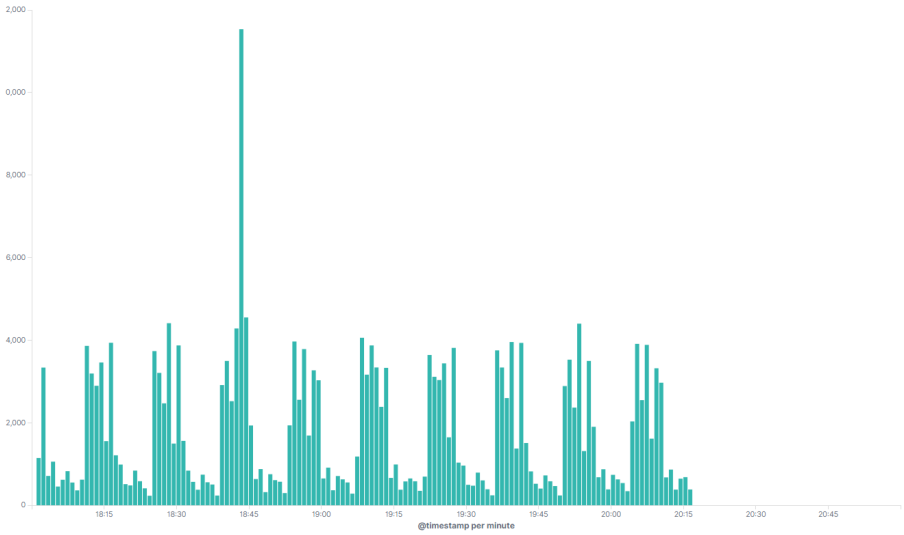
-

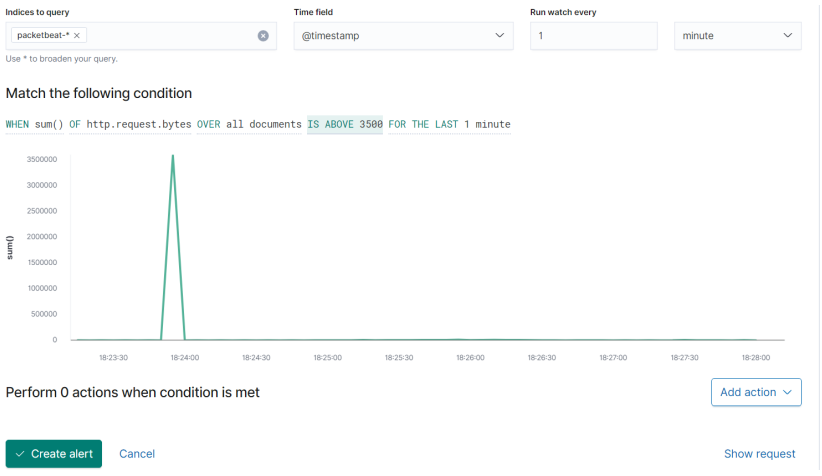
-

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.

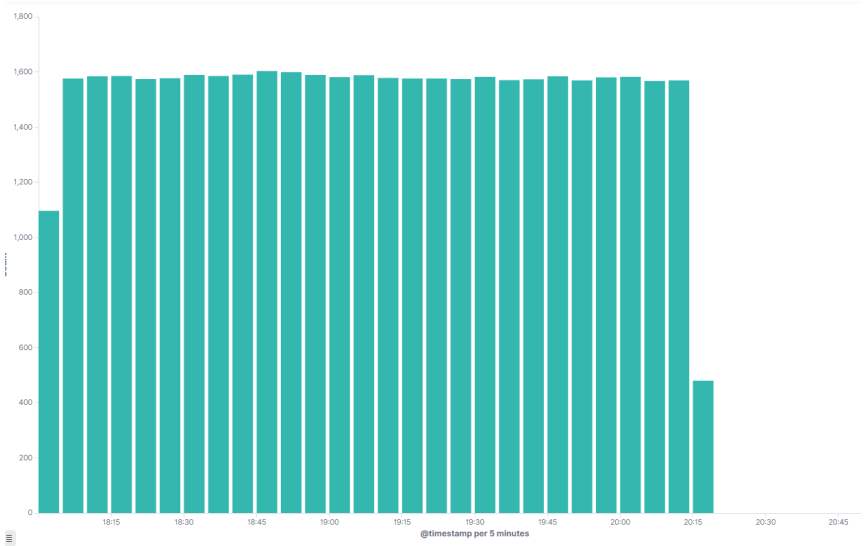


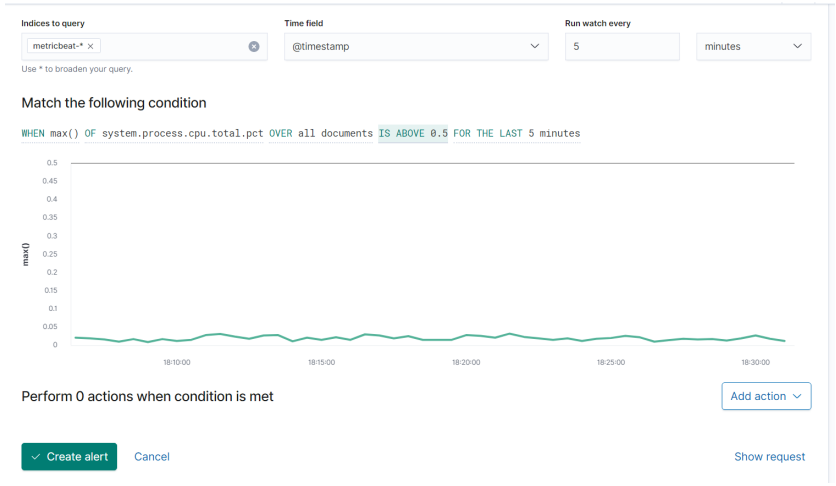


Name of Alert 3:

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.
- 

- 

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*