**Blue Team: Summary of Operations Henry Bartechko**

**Table of Contents**

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

**Network Topology**

The following machines were identified on the network:

* Name of VM 1 **Azure Hypervisor**
  + **Operating System**: Windows
  + **Purpose**: NAT Switch
  + **IP Address**: 192.168.1.1
* Name of VM 2 **ELK Stack**
  + **Operating System**: Linux
  + **Purpose**: Network Monitoring
  + **IP Address**: 192.168.1.100
* Name of VM 3: **Capstone**
  + **Operating System**: Linux
  + **Purpose**: Apache Webserver
  + **IP Address**: 192.168.1.105
* Name of VM 4: **Target1**
  + **Operating System**: Linux
  + **Purpose**: Target VM
  + **IP Address**: 192.168.1.100
* Name of VM 5: **Target2**
  + **Operating System**: Linux
  + **Purpose**: Target VM
  + **IP Address**: 192.168.1.115
* Name of VM 6: **Kali**
  + **Operating System**: Linux
  + **Purpose**: Pen Testing Machine
  + **IP Address**: 192.168.1.90

**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:

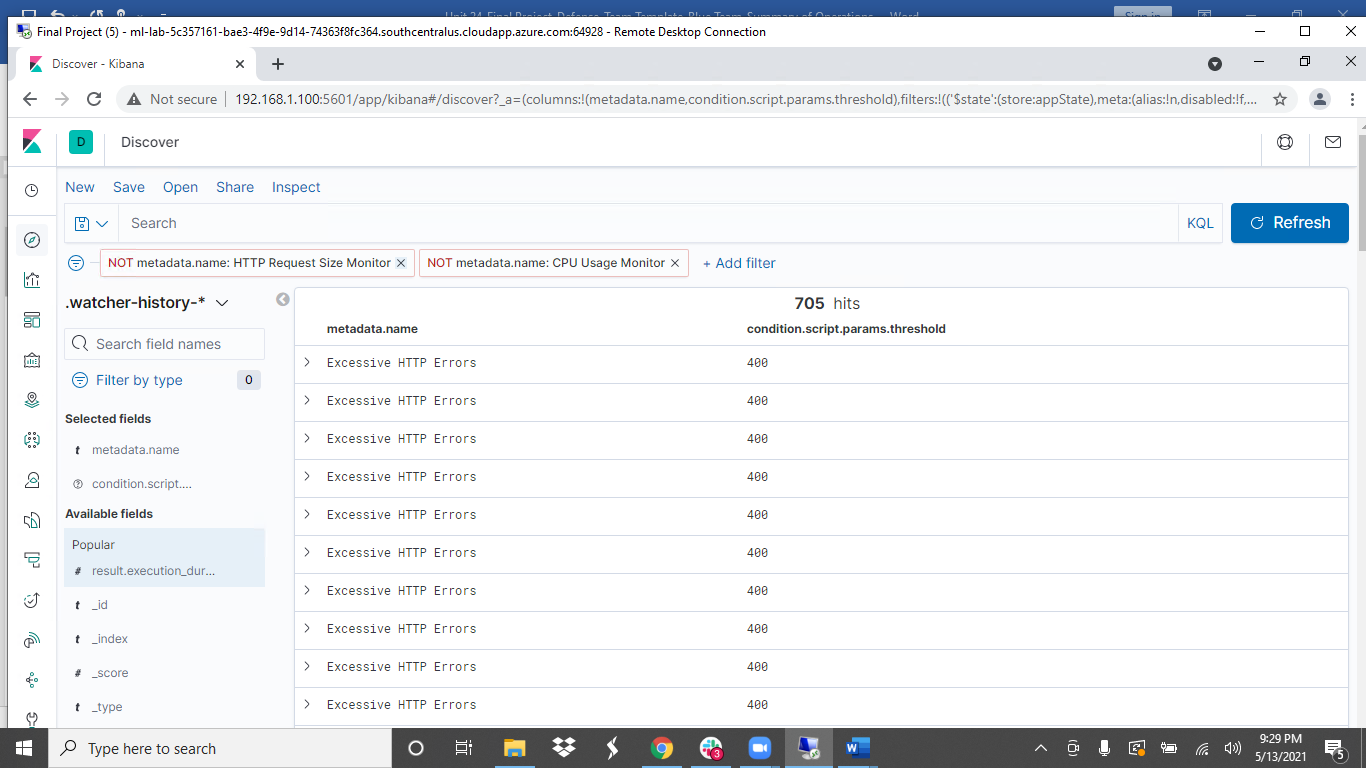
**Monitoring the Targets**

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

**Name of Alert 1:** **Excessive HTTP Errors**

Alert 1 is implemented as follows:

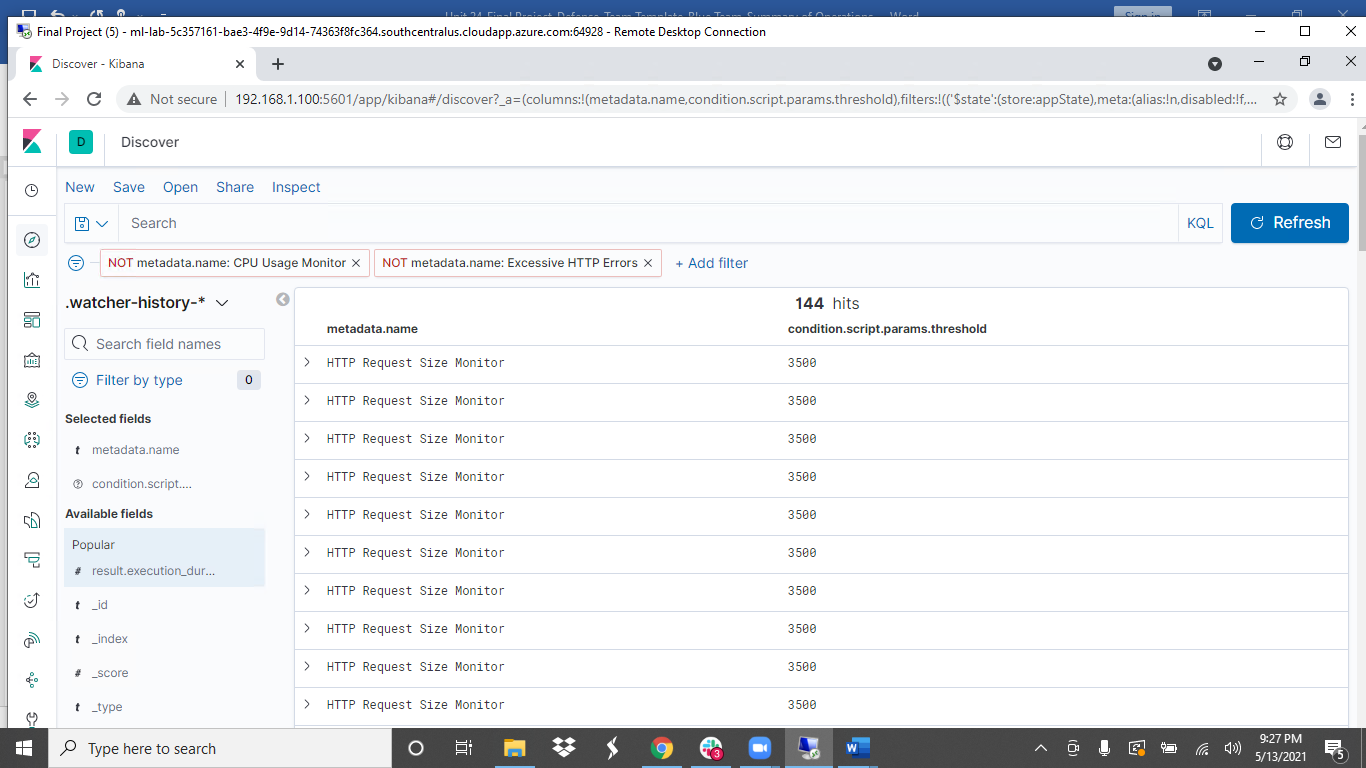
* **Metric**: WHEN count() GROUPED OVER top 5 'http.response.status\_code'
* **Threshold**: IS ABOVE 400 FOR THE LAST 5 minutes
* **Vulnerability Mitigated**: CWE-521: Weak Password Requirements/Brute Force Attack
* **Reliability**: May create some false positives from user error. High reliability



**Name of Alert 2: HTTP Request Size Monitor**

Alert 2 is implemented as follows:

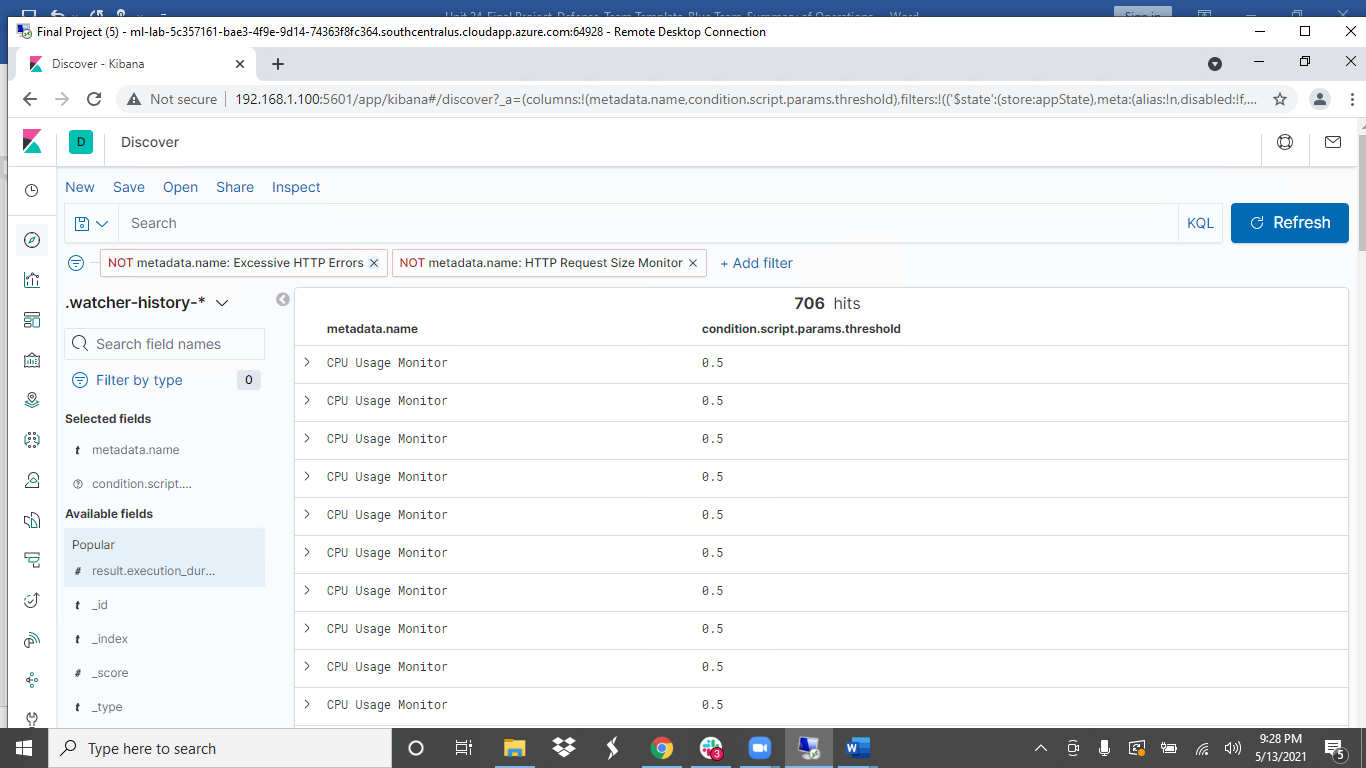
* **Metric**: WHEN sum() of http.request.bytes
* **Threshold**: OVER all documents IS ABOVE 3500 FOR THE LAST 1 minute
* **Vulnerability Mitigated**: When an attacker POSTs or GETs files to the web server
* **Reliability**: May create some false positives if the webserver has frequent uploads and/or downloads. Medium reliability



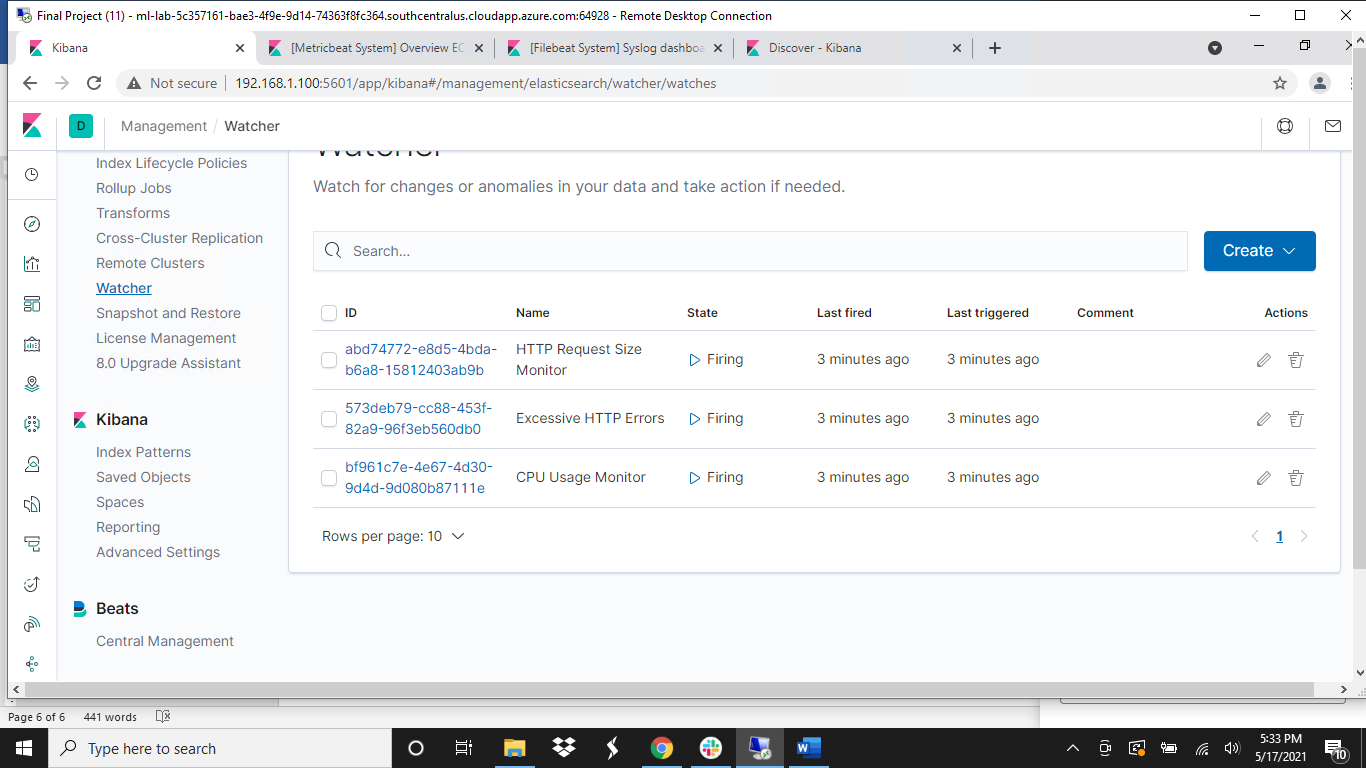
**Name of Alert 3: CPU Usage Monitor**

Alert 3 is implemented as follows:

* **Metric**: WHEN max() OF system.process.cpu.total.pct
* **Threshold**: OVER all documents IS ABOVE 0.5 FOR THE LAST 5 minutes
* **Vulnerability Mitigated**: Metasploit attack, this attack may spike the CPU usage
* **Reliability**: May create more than average false positives/false negatives. CPU usage can spike for many different reasons. Low reliability.



**Watcher : Alerts firing**



**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 **CWE-540: Inclusion of Sensitive Information in Source Code**
  + **Patch**: Recommendations include removing this script from the web server and moving it to a location not accessible from the Internet.
  + **Why It Works**: Removes sensitive data from source code and moves directories to a more secure location away from access on the Internet
* Vulnerability 2 **CWE-521: Weak Password Requirements**
  + **Patch**: Strong Password Policy: Complexity, length, and Password expiration.
  + **Why It Works**: A strong password policy makes it harder to Brute force attack a machine. Can alert Security administrator before the Brute Force attack is successful
* Vulnerability 3 **CVE-2015-6565: OpenSSH 6.8 < 6.9 - 'PTY' Local Privilege Escalation**
  + **Patch**: Least Privilege: Update sudoers file to ensure that sudo privileges match users’ needs/roles and that ALL sudo privileges require a password.
  + **Why It Works**: Prevents attacker’s ability to run a simple python script to escalate a compromised user’s privileges.