Blue Team: Summary of Operations

Table of Contents

Network Topology

TODO: Fill out the information below.

The following machines were identified on the network:

- HOST
  - **Operating System**:microsoft windows 2008 XP server
  - **Purpose**: Host / Jump box
  - **IP Address**:192.168.1.1
  - **Open ports:** 135,139,445,2179,3389
  - **MAC Address:00:15:5D:00:04:OD**
- ELK SERVER
  - **Operating System**:Linux
  - **Purpose**:ELK Stack set up alert
  - **IP Address**:192.168.1.100
  - **Open ports:**22,9200
  - **MAC Address:4C:EB:42:D2:D5:D7**
- CAPSTONE
  - **Operating System**:Linux
  - **Purpose**: Test Alert
  - **IP Address**:192.168.1.105
  - **Open ports:**22 , 80
  - **MAC Address: 00:15:5D:00:04:0F**
- TARGET 1
  - **Operating System**:Linux 3.2 - 4.9
  - **Purpose**:compromised system
  - **IP Address**:192.168.1.110
  - **Open ports:22, 80 , 111,139,445**
  - **MAC Address:00:15:5D:00:04:10**

- TARGET 2
    - **Operating System**:Linux
    - **Purpose**:compromised system
    - **IP Address**:192.168.1.115
    - **Open ports:22, 80 , 111,139,445**
    - **MAC Address:00:15:5D:00:04:11**

- ATTACKING MACHINE
    - **Operating System**:Linux 2.6.32
    - **Purpose**:Attacking/penetration testing machine
    - **IP Address**:192.168.1.90
    - **Open ports:22**
    - **MAC Address:**

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:

Excessive HTTP Errors Alert

Excessive HTTP Errors Alert is implemented as follows:

- **Metric**: Packetbeat, HTTP Response Status Code 400 or above.
- **Threshold**: Above 400 for the last 5 minutes.
- **Vulnerability Mitigated**: Client-side and Server-side authentication errors can serve as an indicator of attack, including for brute force attacks or privilege escalation attempts.
- **Reliability**: High reliability. It detected WordPress Scans (wpscan)

HTTP Request Size Monitor Alert

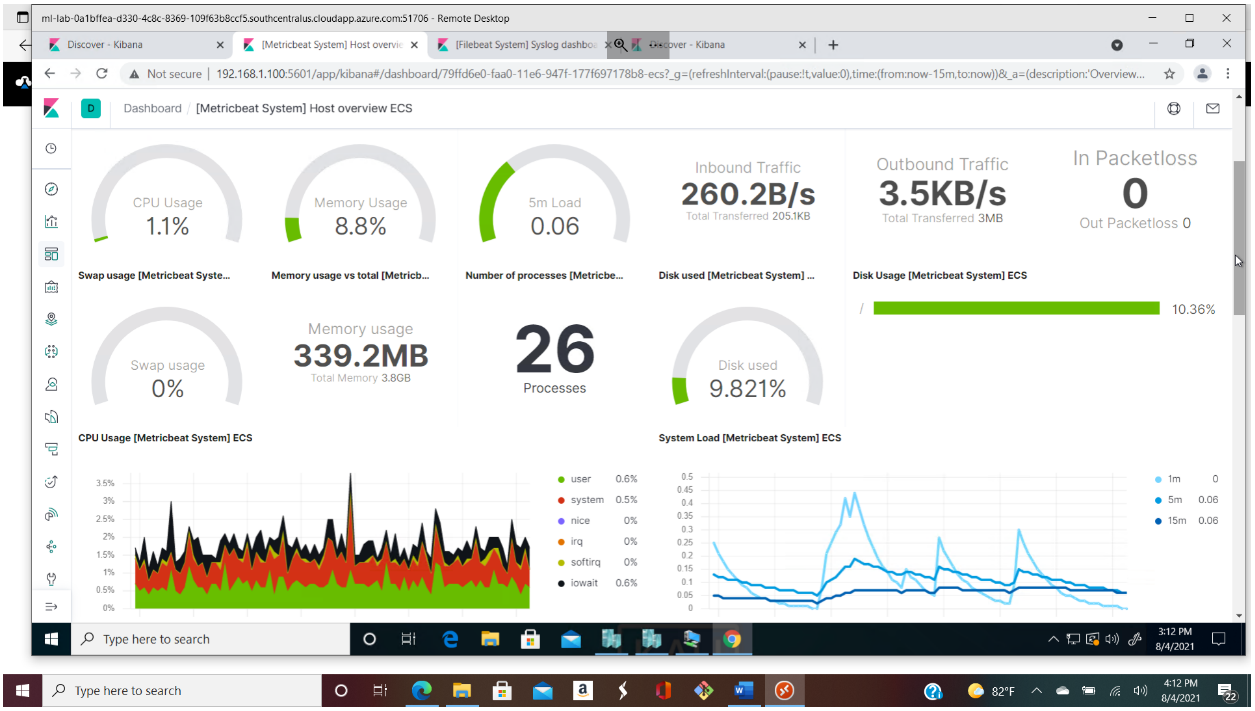
HTTP Request Size Monitor Alert is implemented as follows:

- **Metric**: Packetbeat, HTTP Request Size
- **Threshold**: When requested byte size is above 3500 for 1 minute.
- **Vulnerability Mitigated**: Indicative of high traffic events, which could be an indicator of attack, such as DOS or DDOS.
- **Reliability**: TODO: Does this alert generate lots of false positives/false negatives? Rate as low, medium, or high reliability.

CPU Usage Monitor Alert

CPU Usage Monitor Alert is implemented as follows:

- **Metric**:Metricbeat, System Process CPU usage
- **Threshold**: When 50% of CPU is used by system processes.
- **Vulnerability Mitigated**: Activity didnt cause a spike in the CPU usage but in the case of a DoS, DDoS attack, a crypto hijacking or the presence of a malware in a machine which causes a spike in CPU usage then an alert can be sent to an administrator when the utilization is => 50%. Use of host based IPS can be employed to mitigate against this figures.
- **Reliability**:High reliability. This alert did not fire during the engagement because none of the Red Team activity caused a CPU spike looking at the CPU usage which is about 1.1%.

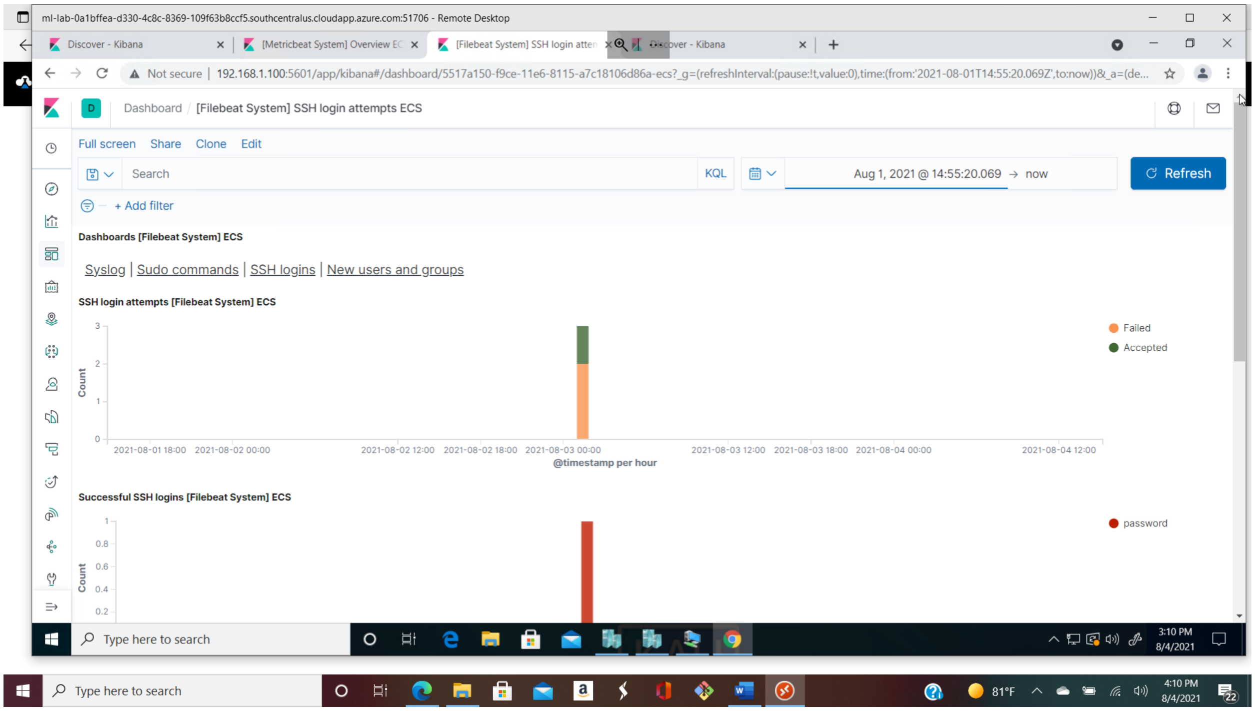

ml-lab-0a1bffea-d330-4c8c-8369-109f63b8ccf5.southcentralus.cloudapp.azure.com:51706 - Remote Desktop
Discover - Kibana
[Metricbeat System] Host overvie
[Filebeat System] Syslog dashbo
Discover - Kibana
Not secure | 192.168.1.100:5601/app/kibana#/dashboard/79ffd6e0-faa0-11e6-947f-177f697178b8-ecs?_g=(refreshInterval:(pause:!t,value:0),time:(from:now-15m,to:now))&_a=(description:'Overview...
Dashboard / [Metricbeat System] Host overview ECS
CPU Usage
1.1%
Memory Usage
8.8%
5m Load
0.06
Inbound Traffic
260.2B/s
Total Transferred 205.1KB
Outbound Traffic
3.5KB/s
Total Transferred 3MB
In Packetloss
0
Out Packetloss 0
Swap usage [Metricbeat Syste...
Memory usage vs total [Metricb...
Number of processes [Metricbe...
Disk used [Metricbeat System] ...
Disk Usage [Metricbeat System] ECS
/
10.36%
Swap usage
0%
Memory usage
339.2MB
Total Memory 3.8GB
26
Processes
Disk used
9.821%
CPU Usage [Metricbeat System] ECS
3.5%
3%
2.5%
2%
1.5%
1%
0.5%
0%
● user 0.6%
● system 0.5%
● nice 0%
● irq 0%
● softirq 0%
● iowait 0.6%
System Load [Metricbeat System] ECS
0.5
0.45
0.4
0.35
0.3
0.25
0.2
0.15
0.1
0.05
0
● 1m 0
● 5m 0.06
● 15m 0.06
Type here to search
3:12 PM
8/4/2021
Type here to search
82°F
4:12 PM
8/4/2021

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

SSH Traffic Alert

SSH Traffic is implemented as follows:

- Metric: Packetbeat, Destination Port 22
- Threshold: Any Traffic in last minute
- Vulnerability Mitigated: Unauthorized access via SSH on port 22.
- Reliability: Medium reliability. If SSH is used for legitimate purposes, then this alert will generate false positives.



ml-lab-0a1bffea-d330-4c8c-8369-109f63b8ccf5.southcentralus.cloudapp.azure.com:51706 - Remote Desktop

Not secure | 192.168.1.100:5601/app/kibana#/dashboard/5517a150-f9ce-11e6-8115-a7c18106d86a-ecs?_g=(refreshInterval:(pause:!t,value:0),time:(from:'2021-08-01T14:55:20.069Z',to:now))&_a=(de...

Dashboard / [Filebeat System] SSH login attempts ECS

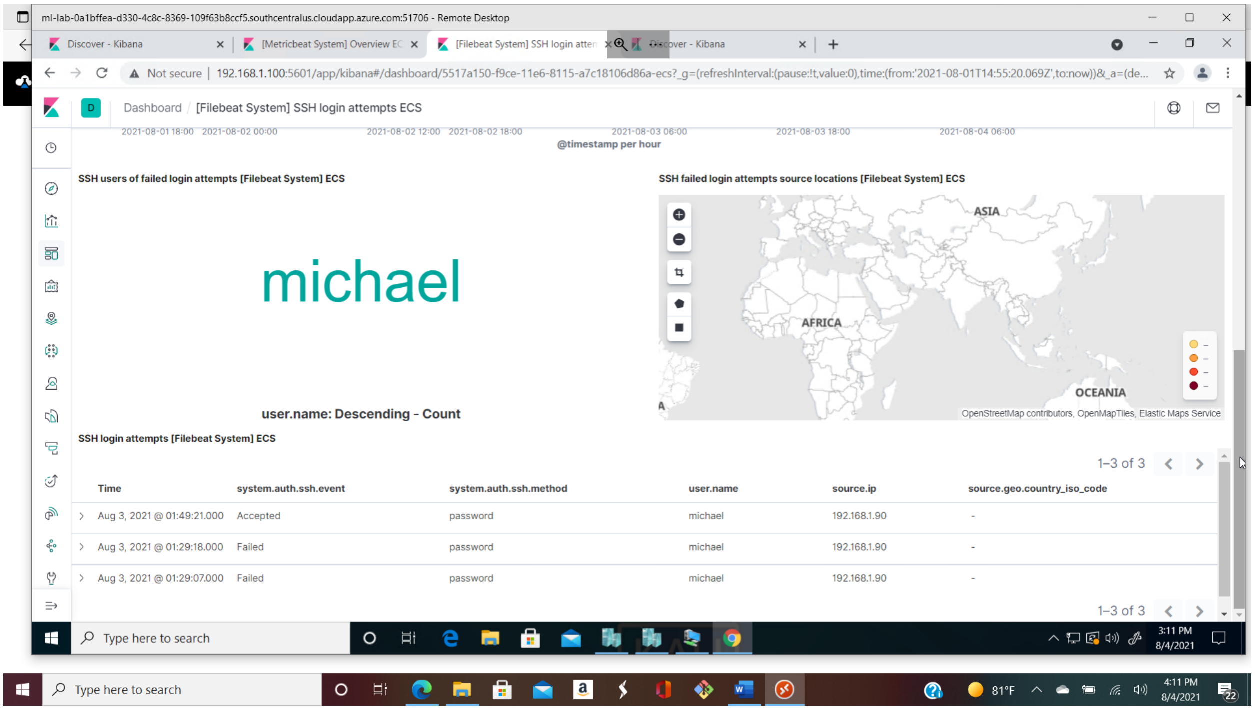
Aug 1, 2021 @ 14:55:20.069 → now

Dashboards [Filebeat System] ECS

Syslog | Sudo commands | SSH logins | New users and groups

SSH login attempts [Filebeat System] ECS

Successful SSH logins [Filebeat System] ECS


ml-lab-0a1bffea-d330-4c8c-8369-109f63b8ccf5.southcentralus.cloudapp.azure.com:51706 - Remote Desktop
Discover - Kibana
[Metricbeat System] Overview EC
[Filebeat System] SSH login atten
Discover - Kibana
Not secure
192.168.1.100:5601/app/kibana#/dashboard/5517a150-f9ce-11e6-8115-a7c18106d86a-ecs?_g=(refreshInterval:(pause:!t,value:0),time:(from:'2021-08-01T14:55:20.069Z',to:now))&_a=(de...
Dashboard / [Filebeat System] SSH login attempts ECS
2021-08-01 18:00
2021-08-02 00:00
2021-08-02 12:00
2021-08-02 18:00
2021-08-03 06:00
2021-08-03 18:00
2021-08-04 06:00
@timestamp per hour
SSH users of failed login attempts [Filebeat System] ECS
michael
user.name: Descending - Count
SSH failed login attempts source locations [Filebeat System] ECS
ASIA
AFRICA
OCEANIA
OpenStreetMap contributors, OpenMapTiles, Elastic Maps Service
Type here to search
3:11 PM
8/4/2021
81°F
4:11 PM
8/4/2021

SSH login attempts [Filebeat System] ECS

1–3 of 3

Time	system.auth.ssh.event	system.auth.ssh.method	user.name	source.ip	source.geo.country_iso_code
Aug 3, 2021 @ 01:49:21.000	Accepted	password	michael	192.168.1.90	-
Aug 3, 2021 @ 01:29:18.000	Failed	password	michael	192.168.1.90	-
Aug 3, 2021 @ 01:29:07.000	Failed	password	michael	192.168.1.90	-

1–3 of 3

Listener Alert

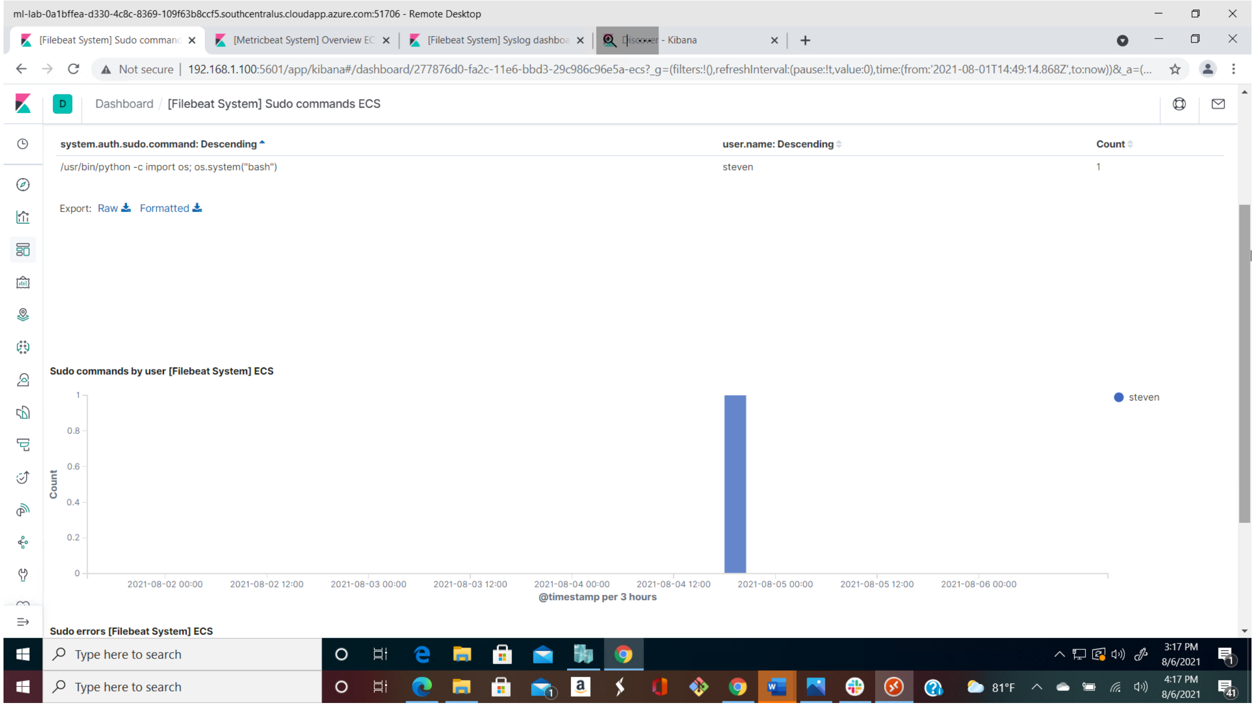
Listener Alert is implemented as follows:

- Metric: Packetbeat, Destination Port between 4000-5000
- Threshold: When destination port values fall between 4000 and 5000.
- Vulnerability Mitigated: Reverse Shells and other unusual traffic that could indicate the system has been compromised.
- Full Rule: packetbeat-* WHEN count () OF destination.port OVER all documents IS BETWEEN 4000 and 5000 FOR THE LAST 1 minute
- Reliability: High reliability. This alert fired during all Red Team activity utilizing a Reverse Shell with the targeted system directing traffic to 192.168.1.90:4444. However, if the attack set the listener outside this port range, the alert would not activate.

Suggestions for Going Further (Optional)

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:

- Python Privilege Escalation User has sudo access for python, allowing privilege escalation via spawning a bash shell through a python command.
    - **Patch**: *Removing sudo access for python users and regularly doing software patching.*
    - *Recommendation:*
        - *sudo access for python for the users should be removed.*
        - *If the user requires this access, then craft an alert or report that will watch for “bash” within a sudo command (system.auth.sudo.command: “bash”)*
    - *Why It Works: If this access is removed, the method of privilege escalation is closed. If the access is required and has legitimate use, such as the user routinely needing to access python, then monitoring for suspicious commands is needed [4].*



ml-lab-0a1bffea-d330-4c8c-8369-109f63b8ccf5.southcentralus.cloudapp.azure.com:51706 - Remote Desktop

Not secure | 192.168.1.100:5601/app/kibana#/dashboard/277876d0-fa2c-11e6-bbd3-29c986c96e5a-ecs?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:'2021-08-01T14:49:14.868Z',to:now))&_a=(...

Dashboard / [Filebeat System] Sudo commands ECS

system.auth.sudo.command: Descending	user.name: Descending	Count
/usr/bin/python -c import os; os.system("bash")	steven	1

Export: Raw Formatted

Sudo commands by user [Filebeat System] ECS

Sudo errors [Filebeat System] ECS

- Broken Authentication with Weak and Exposed Passwords / SSH Login Users on the system was relatively not meeting the complexity requirement . In addition, passwords were exposed within files in both plaintext and hashed form in files that were accessible by users with weak passwords.
    - **Patch**: *installing Pam (Pluggable Authentication Module) [3]*
    - *Recommendations:*
        - *Require SSH keys to login via SSH and disable passwords. Logging in via keys is generally a more secure way to access the*

        SSH service, especially if best practices are followed regarding securing private keys.
        - *Update password policy, including password change requirements, size and complexity. Installing PAM allows the administrator to set password requirements for types of characters, etc [3].*
    -
    - *Why It Works:*
        - *Strong passwords are critical to keeping systems secure. In addition, requiring periodic changes mean that if any passwords have been compromised, administrators can cut off that access with the reset.*
        - *SSH keys are also a better method for logging into SSH for security purposes, since they are much more difficult to brute force.*
        - *Using SSH keys also prevents the Metasploit exploit for SSH Login because it would not be able to brute force the password. If the private key is also properly protected, this exploit would not be possible [1], [2].*
- 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*

Install the Linux-PAM (oracle.com) …..1

1. https://www.offensive-security.com/metasploit-unleashed/scanner-ssh-auxiliary-modules/
2. https://nest.parrot.sh/packages/tools/metasploit-
3. Install the Linux-PAM (oracle.com)
4. Linux Privilege Escalation using Sudo Rights
5.