Ardavan Moghaddam

Final Project

Blue Team: Summary of Operations (Defensive)

Name of VM : ELK
Operating System: Ubuntu 18.04
Purpose: The ELK Stack
IP Address: 192.168.1.100

Name of VM : Kali
Operating System: Debian Kali 5.4.0
Purpose: The Penetration Tester
IP Address: 192.168.1.90

Name of VM : Target 1
Operating System: Debian GNU/Linux 8
Purpose: The WordPress Host
IP Address: 192.168.1.10

Description of Targets

Target 1 (192.168.1.110) .

Target 2 (192.168.1.115) optional.

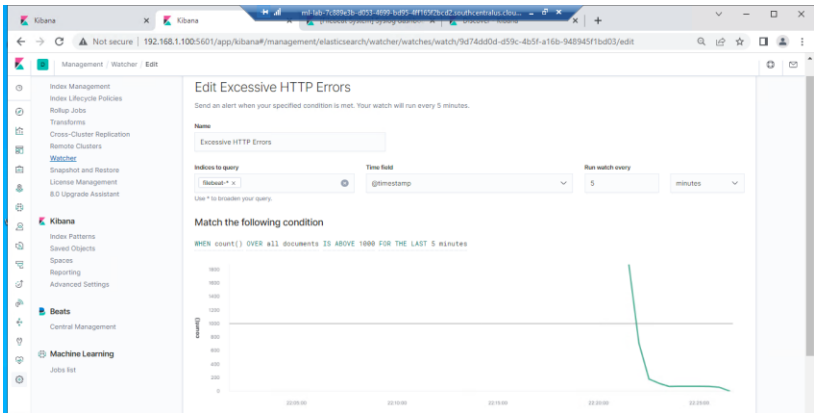
Ports 80 and 22 are possible ports of entry for attackers.

Monitoring the Targets

Configuring Alerts

Alert 1:

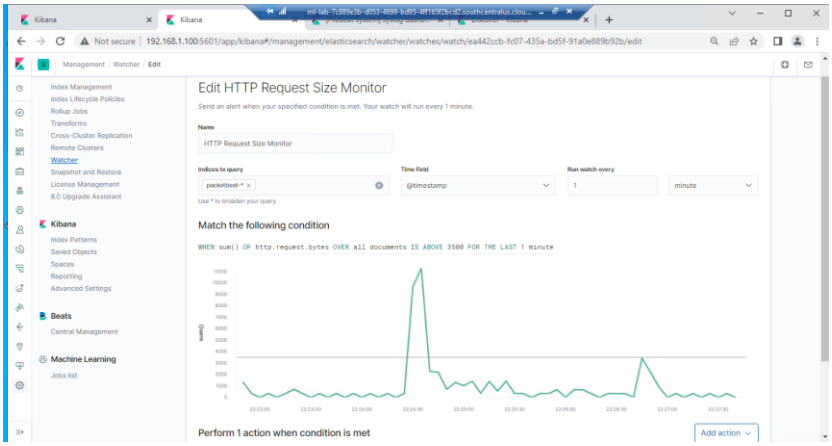
Excessive HTTP Errors
WHEN count() GROUPED OVER top 5 'http.response.status_code' IS ABOVE 400 FOR THE LAST 5 minutes
Selected the packetbeat indice
Metric: WHEN count() GROUPED OVER top 5 ‘http.response.status_code’
Threshold: IS ABOVE 400
Vulnerability Mitigated: Enumeration/Brute Force



Alert 2:

HTTP Request Size Monitor

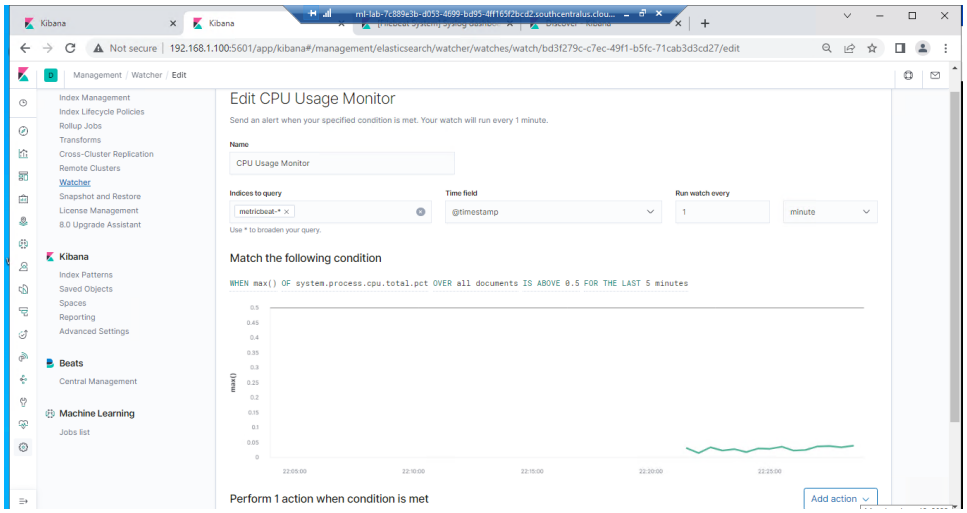
Selected the **packetbeat** indice
Metric:
WHEN sum() of http.request.bytes OVER all documents IS ABOVE 3500 FOR THE LAST 1 minute
Threshold: ABOVE 3500
Vulnerability Mitigated: Code injection in HTTP requests (XSS and CRLF) or DDOS
Reliability: Alert could create false positives. There is a possibility for a large non malicious HTTP request or legitimate HTTP traffic.



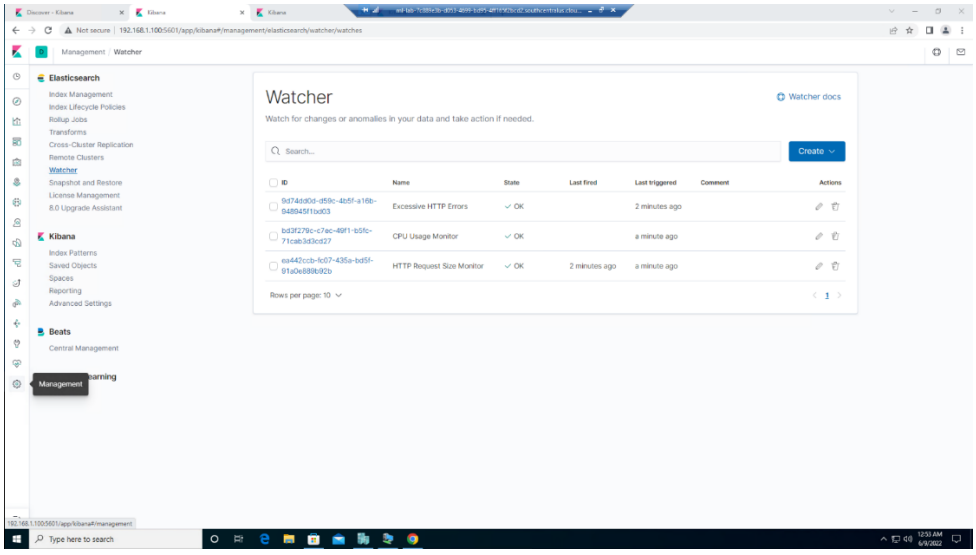
Alert 3:

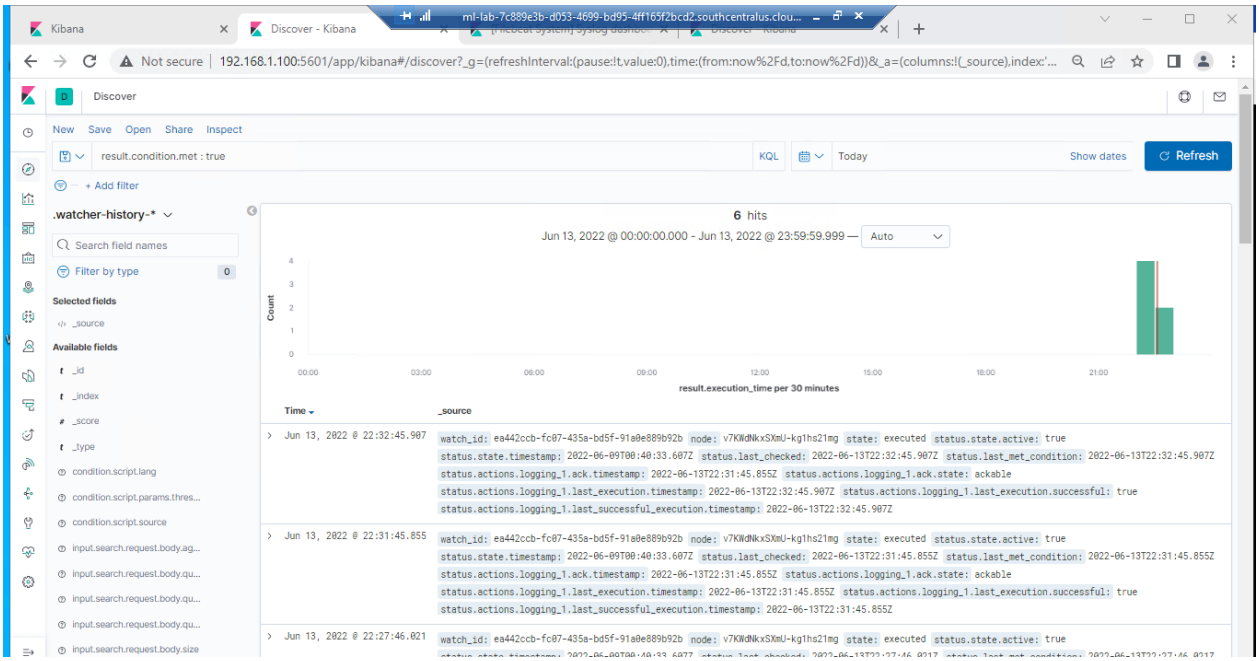
CPU Usage Monitor

Selected the **metricbeat** indice
Metric: WHEN max() OF system.process.cpu.total.pct OVER all documents
Threshold: ABOVE 0.5
Vulnerability Mitigated: Malicious software, programs (malware or viruses) running taking up resources.
Reliability: The alert is highly reliable. Even if there isn't a malicious program running this can still help.



After created 3 Alerts:




Kibana
Discover - Kibana
Not secure | 192.168.1.100:5601/app/kibana#/discover?_g=(refreshInterval:(pause:!t,value:0),time:(from:now%2Fd,to:now%2Fd))&_a=(columns:!(_source),index:'...
Discover
New Save Open Share Inspect
result.condition.met : true
KQL
Today
Show dates
Refresh
+ Add filter
.watcher-history-*
Search field names
Filter by type
0
Selected fields
_source
Available fields
_id
_index
_score
_type
condition.script.lang
condition.script.params.thres...
condition.script.source
input.search.request.body.ag...
input.search.request.body.qu...
input.search.request.body.qu...
input.search.request.body.qu...
input.search.request.body.size
6 hits
Jun 13, 2022 @ 00:00:00.000 - Jun 13, 2022 @ 23:59:59.999 —
Auto
Count
result.execution_time per 30 minutes
Time
_source
Jun 13, 2022 @ 22:32:45.907
watch_id: ea442ccb-fc07-435a-bd5f-91a0e889b92b node: v7KWdNkxSXmU-kg1hs21mg state: executed status.state.active: true
status.state.timestamp: 2022-06-09T00:40:33.607Z status.last_checked: 2022-06-13T22:32:45.907Z status.last_met_condition: 2022-06-13T22:32:45.907Z
status.actions.logging_1.ack.timestamp: 2022-06-13T22:31:45.855Z status.actions.logging_1.ack.state: ackable
status.actions.logging_1.last_execution.timestamp: 2022-06-13T22:32:45.907Z status.actions.logging_1.last_execution.successful: true
status.actions.logging_1.last_successful_execution.timestamp: 2022-06-13T22:32:45.907Z
Jun 13, 2022 @ 22:31:45.855
watch_id: ea442ccb-fc07-435a-bd5f-91a0e889b92b node: v7KWdNkxSXmU-kg1hs21mg state: executed status.state.active: true
status.state.timestamp: 2022-06-09T00:40:33.607Z status.last_checked: 2022-06-13T22:31:45.855Z status.last_met_condition: 2022-06-13T22:31:45.855Z
status.actions.logging_1.ack.timestamp: 2022-06-13T22:31:45.855Z status.actions.logging_1.ack.state: ackable
status.actions.logging_1.last_execution.timestamp: 2022-06-13T22:31:45.855Z status.actions.logging_1.last_execution.successful: true
status.actions.logging_1.last_successful_execution.timestamp: 2022-06-13T22:31:45.855Z
Jun 13, 2022 @ 22:27:46.021
watch_id: ea442ccb-fc07-435a-bd5f-91a0e889b92b node: v7KWdNkxSXmU-kg1hs21mg state: executed status.state.active: true