SPLUNK: RECONNAISSANCE PHASE Report 2025/12/10

Scenario

A Big corporate organization **Wayne Enterprises** has recently faced a cyber-attack where the attackers broke into their network, found their way to their web server, and have successfully defaced their website **http://www.imreallynotbatman.com**. Their website is now showing the trademark of the attackers with the message **YOUR SITE HAS BEEN DEFACED** as shown below:

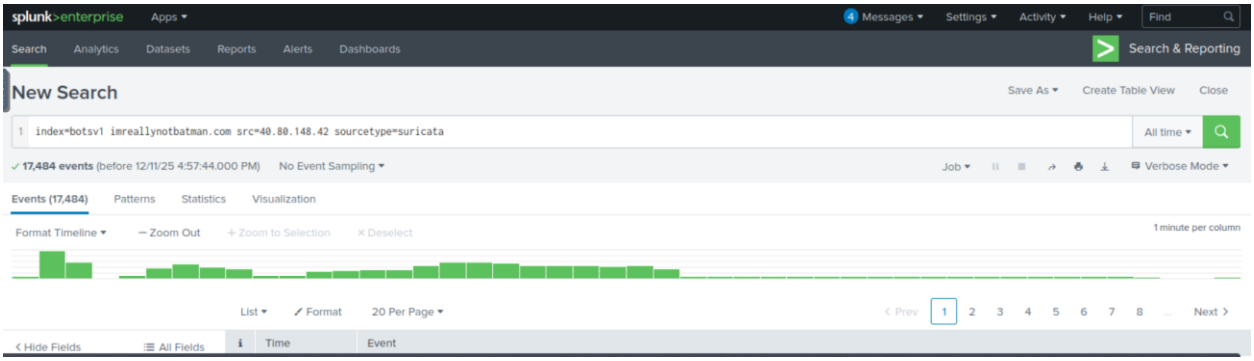
They have requested "**US**" to join them as a **Security Analyst** and help them investigate this cyberattack and find the root cause and all the attackers' activities within their network.

The good thing is, that they have Splunk already in place, so we have got all the event logs related to the attacker's activities captured. We need to explore the records and find how the attack got into their network and what actions they performed.

This Investigation comes under the **Detection and Analysis** phase.

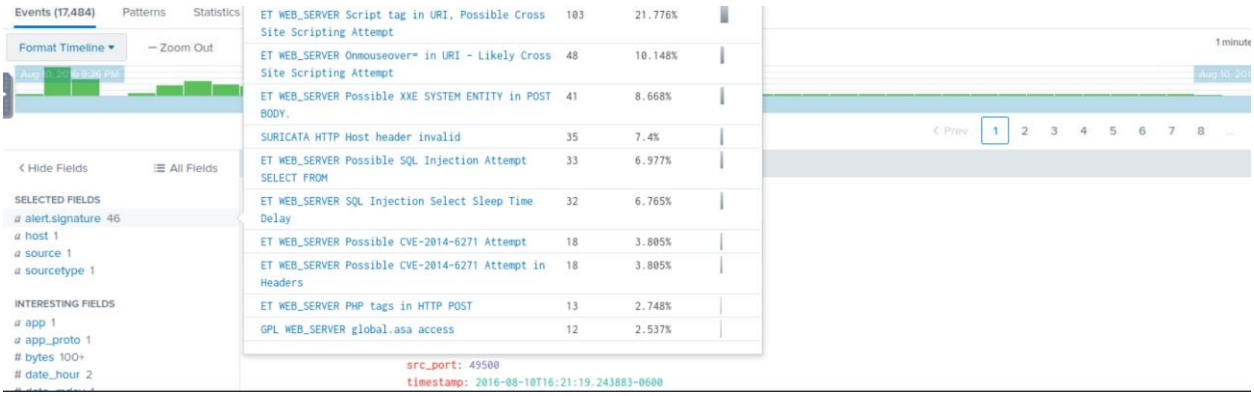
After launching splunk, and selecting 'All Time' in the Time Range Picker. I provided input in the search query - **index=botsv1 imreallynotbatman.com** where We are going to look for the event logs in the index "botsv1" which contains the term imreallynotbatman.com and clicked search.

STEP 1: One suricata alert highlighted the CVE value associated with the attack attempt. What is the CVE value?



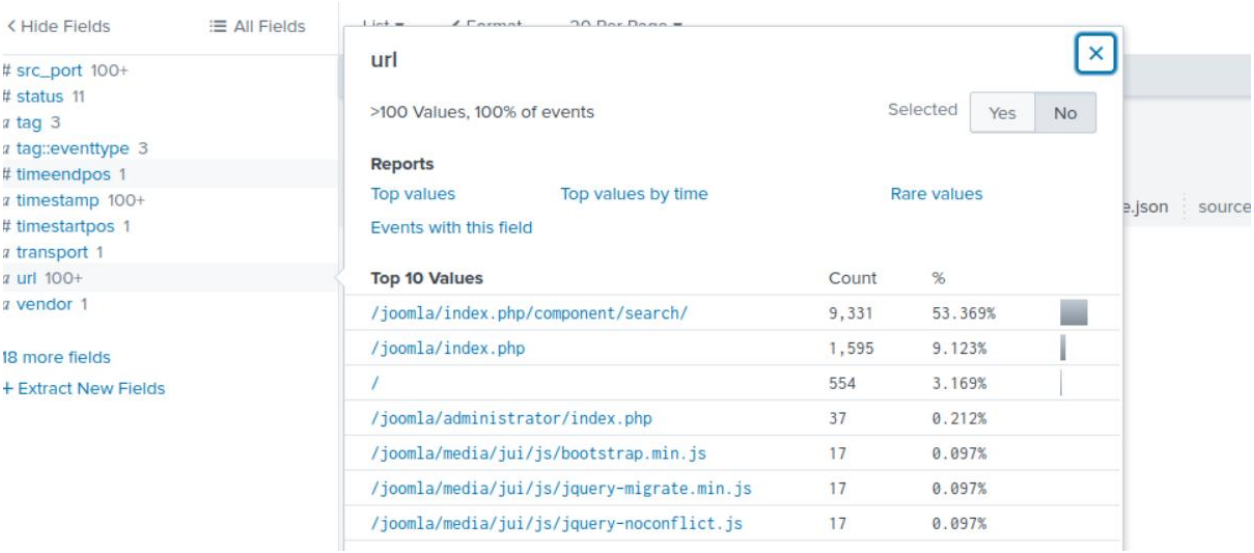
Index=botsv1 imreallynotbatman.com src=40.80.148.42 sourcetype=suricata

This query will show the logs from the suricata log source that are detected/generated from the source IP **40.80.248.42**, and we have narrowed our search on the src IP and looked at the source type suricata to see what Suricata triggered alerts.



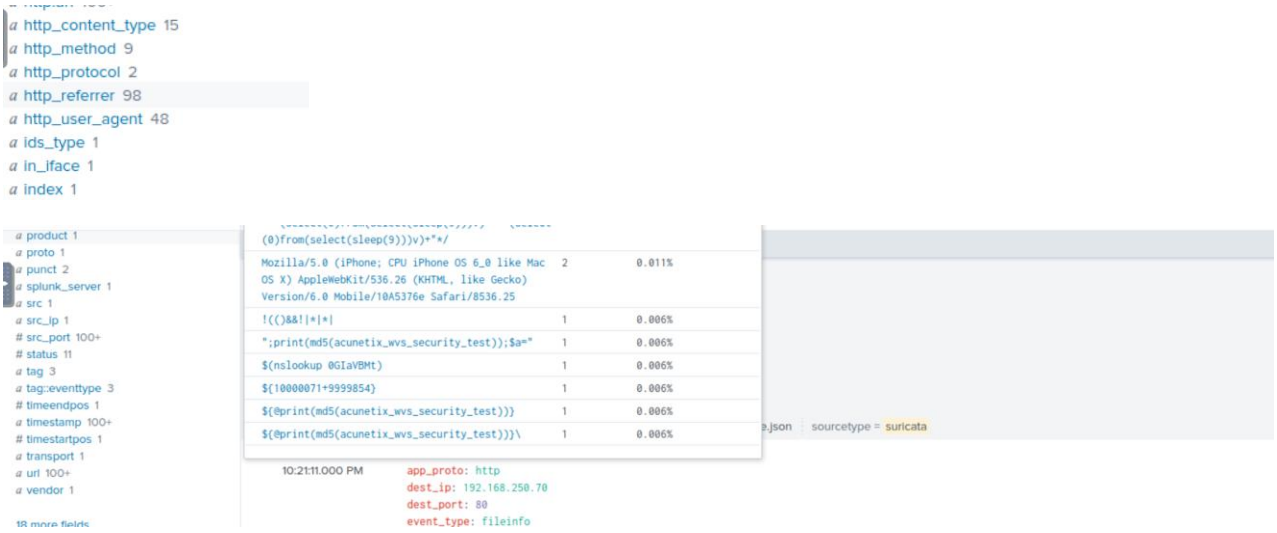
I then looked on the left side and clicked 'Select Fields' and looked at '**alert_signature**' and clicked on it which is where we'd find our CVE value and voila! Our CVE value – (**CVE-2014-6271**) found in the listed signatures.

STEP 2: What is the CMS our web server is using?



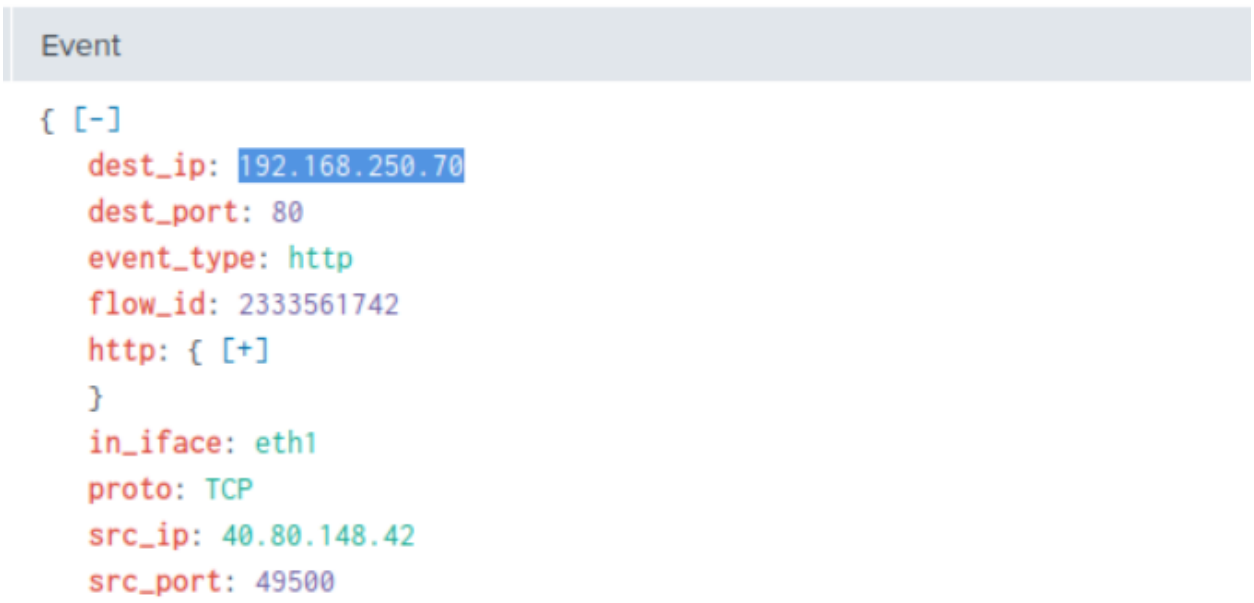
I looked through our filters on the left and came across the '**uri**'(the *path or location* of a resource being accessed on a website or server) and clicked on it. I then found the CMS(a tool that lets you create and manage a website like you're editing a document) which was **joomla**.

STEP 3: What is the web scanner, the attacker used to perform the scanning attempts?



This task was a bit tricky, I skimmed through the filters on the left again and tried to find something I could link to the attacker and found '**http_user_agent**' and clicked on it. I looked through the filters once again and found the web scanner - **acunetix**.

STEP 4: What is the IP address of the server imreallynotbatman.com?



I clicked open on one event and looked at the '**dest_ip**' filter and found the IP – **192.168.250.70**.

Conclusion Summary

This Splunk investigation focused on analysing reconnaissance activity that led to the defacement of *imreallynotbatman.com*. By querying the **botsv1 index**, filtering relevant sources, and examining Suricata alerts, I identified the CVE linked to the attack (**CVE-2014-6271**). Further analysis of URL fields revealed that the compromised web server was running **Joomla** as its CMS. Reviewing the **http_user_agent** field exposed the attacker's scanning tool, **Acunetix**, and inspection of event details confirmed the server's destination IP (**192.168.250.70**). This phase successfully uncovered key indicators outlining how the attacker probed and targeted the environment, laying the groundwork for deeper investigation into the intrusion path and subsequent exploitation.