

Splunk — Boss of the SOC v1

11 Mayıs 2024 tarihinde BTK'nın Siber Tehdit İstihbaratı ve Olay Müdahale Atölyesi'nde öğrendiğim Splunk Bots çözümlerini sizlerle paylaşmak istiyorum. İyi okumalar dilerim.

Önce Splunk'ın ne olduğundan başlayalım.

Splunk, büyük veri analizi ve izleme için kullanılan bir platformdur. Çeşitli kaynaklardan gelen verileri toplar, depolar, analiz eder ve görselleştirir. İşletmelere BT altyapısının performansını artırmak, sorun giderme yapmak ve güvenlik sağlamak için yardımcı olur.

Splunk bots ise, Splunk platformunun otomasyon yeteneklerini genişletmek için kullanılan önceden yapılandırılmış ve programlanmış botlardır. Bu botlar, belirli görevleri gerçekleştirmek için yapılandırılmıştır ve Splunk Enterprise veya Splunk Cloud gibi Splunk ürünleriyle entegre çalışabilirler. Splunk botları, kullanıcıların manuel olarak yapması gereken tekrarlayan görevleri otomatikleştirmelerine ve Splunk platformunun kullanımını daha verimli hale getirmelerine yardımcı olabilir.



Şimdi Google'a splunk bots yazarak başlayabiliriz. İlk çıkan siteye tıklayıp üyelik oluşturarak kaydımızı tamamlıyoruz.

Play Now'dan Boss of the SOC Version 1'e tıklayıp 1. senaryo olan Web Site Defacement'i seçiyoruz.

SCENARIOS

BACK TO HOME CREDITS

Web site defacement

Today is Alice's first day at the Wayne Enterprises' Security Operations Center. Lucius sits Alice down and gives her first assignment: A memo from Gotham City Police Department (GCPD). Apparently GCPD has found evidence online (<https://www.imreallnotbatman.com/vuln/1>) that the website [www.imreallnotbatman.com](https://www.imreallnotbatman.com/vuln/1) hosted on Wayne Enterprises' IP address space has been compromised. The group has multiple objectives... but a key aspect of their modus operandi is to deface websites in order to embarrass their victim. Lucius has asked Alice to determine if [www.imreallnotbatman.com](https://www.imreallnotbatman.com/vuln/1). (the personal blog of Wayne Corporations CEO) was really compromised.

Status

Resources

Total Questions: 17

? Unanswered: 17

✓ Correct: 0

✗ Incorrect: 0

Splunk server: <https://gettingstarted.splunk.com>

Credentials: [user001-splk](#) / [Splunk.5](#)

Bots v1 sourcetype sum https://botscontent.netlify.app/v1/bots_sourcetypes.html

Splunk quick reference <https://www.splunk.com/pdfs/solution-guides/splunk-quick-reference-guide.pdf>

Gcpd poison ivy memo: <https://botscontent.netlify.app/v1/gcpd-poisonivy-memo.html>

Alices journal: <https://botscontent.netlify.app/v1/alice-journal.html>

Mission document: https://botscontent.netlify.app/v1/mission_document.html

Finishing in:
03:45:02
Your score: 0
2 minutes ago

Splunk server'a tıklayarak verilen username ile password'u giriyoruz. Daha sonra soruları açıyoruz.

Bu arada bu senaryoda toplam 17 soru var. Bugün ben sadece 101, 102, 104 ve 109. soruları çözdüm. Ayrıca her sorunun puanı olup yanlış girilen cevaplar da -10 puan olarak hesaplanıyor.

#101

Question:

What is the likely IPv4 address of someone from the Po1s0n1vy group scanning imreallnotbatman.com for web application vulnerabilities?

Öncelikle,

`index="botsv1" sourcetype="stream:http" | top dest_ip`

sorgusunu yazıyorum.

Bu SPL yani Splunk Processing Language sorgusu, "botsv1" dizinindeki ve "stream:http" kaynak türündeki verileri filtreler. Sonra bu verileri "dest_ip" alanına göre gruplar ve her bir IP adresinin ne kadar sık kullanıldığını sayar. Sonuç olarak, en çok hit alan IP adresini bulur.

Ve bu sorgudan 192.168.250.70 IP'yi öğreniyoruz.

splunk>enterprise Apps user001-splk Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

New Search Save As Create Table View Close

index="botsv1" sourcetype="stream:http" | top dest_ip All time

✓ 39,010 events (01/08/2016 00:00:00.000 to 11/05/2024 19:46:50.000) No Event Sampling Job

Events (39,010) Patterns Statistics (10) Visualization

100 Per Page Format Preview

dest_ip	count	percent
192.168.250.70	22643	58.668221
134.170.104.154	4766	12.348750
134.170.111.154	3392	8.788703
207.46.7.252	1800	4.663817
207.46.101.29	1228	3.181759
69.192.167.227	966	2.502915
108.161.187.134	374	0.969037
192.168.250.20	340	0.880943
23.63.227.128	222	0.575204
104.89.246.147	211	0.546703

Daha sonra;

index="botsv1" sourcetype="stream:http" dest_ip="192.168.250.70"
| top src_ip

komutunu yazıyorum.

Bu sorgu, "botsv1" dizinindeki ve "stream:http" kaynak türündeki verileri filtreler. Bu filtreleme, belirli bir "dest_ip" (hedef IP adresi) değerine sahip olan kayıtları içerir, yani 192.168.250.70. Daha sonra, bu filtrelenmiş veriler "src_ip" (kaynak IP adresi) alanına göre gruplanır ve her bir kaynak IP adresinin kaç kez kullanıldığını sayar. Sonuç olarak, en çok hit alan kaynak IP adresini bulur.

New Search Save As Create Table View Close

index="botsv1" sourcetype="stream:http" dest_ip="192.168.250.70" | top src_ip All time

✓ 22,643 events (01/08/2016 00:00:00.000 to 11/05/2024 19:53:17.000) No Event Sampling Job

Events (22,643) Patterns Statistics (3) Visualization

100 Per Page Format Preview

src_ip	count	percent
40.80.148.42	20996	92.738516
23.22.63.114	1430	6.316254
192.168.2.50	214	0.945230

Cevap 40.80.148.42

#102

Question:

What company created the web vulnerability scanner used by Po1s0n1vy? Type the company name.

Answer guidance: For example “Microsoft” or “Oracle”

İlk önce;

```
index="botstv1" sourcetype="stream:http" dest_ip="192.168.250.70"
src_ip="40.80.148.42"
```

sorgusunu yazıyorum.

Bu sorgu, belirli bir hedef IP adresine (192.168.250.70) yapılan isteklerin kaynak IP adresi (40.80.148.42) ile ilişkili olanlarını belirlemek için kullanılır. Yani, 40.80.148.42 IP adresinden gelen isteklerin, 192.168.250.70 IP adresine yönlendirildiği kayıtları bulmak için bu sorgu kullanılır.

Ya da ilk soru için de kullanabileceğimiz index="botstv1" "imrealllynotbatman.com" sorgusunu şu an da tekrar yazarak aratıyorum. Biraz göz gezdirdikten sonra kullanılan web güvenlik açığı tarayıcısını oluşturan şirketin Acunetix olduğu anlaşılıyor .

Time	Event
	<pre>missing_packets_out: 0 network_interface: eth1 packets_in: 3 packets_out: 4 reply_time: 1070126 request: POST /joomla/index.php/component/search/ HTTP/1.1 request_ack_time: 44229 request_time: 0 response_ack_time: 77527 response_time: 0 sc_date: Wed, 10 Aug 2016 22:22:27 GMT server: Microsoft-IIS/8.5 server_rtt: 44229 server_rtt_packets: 1 server_rtt_sum: 44229 site: imrealllynotbatman.com src_content: areas%5b%5d%3f%22ordering=alpha&searchphrase=all&searchword=&task=search src_headers: POST /joomla/index.php/component/search/ HTTP/1.1 Content-Length: 78 Content-Type: application/x-www-form-urlencoded Referer: http://imrealllynotbatman.com:80/ Cookie: ae72c62a4936b238523950a4f26f67d0=v7ikb3m59romokmbiet3vphv3 Host: imrealllynotbatman.com Connection: Keep-alive Accept-Encoding: gzip,deflate User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21 Acunetix-Product: WVS/10.0 (Acunetix Web Vulnerability Scanner - Free Edition) Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm Accept: */*</pre>

Cevap: Acunetix

#104

Question:

What is the name of the file that defaced the imrealllynotbatman.com website? Please submit only the name of the file with extension?

Sunucumuzun kaynak IP adresinin kötü amaçlı bir dosyayı indirdiğini varsayarsak ve bu indirme işlemlerinin HTTP GET yöntemini kullandığını biliyorsak, bu bilgilerle birlikte ilgili verileri analiz edebiliriz. Aşağıdaki sorgu, sunucumuzun belirli bir zaman aralığında belirli bir dosyayı indirip indirmediğini kontrol etmek için kullanılabilir. Bu sorguyu çalıştırarak sunucumuzun faaliyetlerini inceleyebilir ve herhangi bir şüpheli veya ilginç etkinlik bulabiliriz.

index="botsv1" sourcetype="stream:http" src_ip="192.168.250.70"

yazıp sonuna da http_method=GET ekleyebiliriz.

i	Time	Event
		<pre>data_packets_in: 2 data_packets_out: 0 dest_ip: 23.22.63.114 dest_mac: 08:5B:0E:93:92:AF dest_port: 1337 duplicate_packets_in: 2 duplicate_packets_out: 0 endtime: 2016-08-10T22:13:46.915172Z http_method: GET missing_packets_in: 0 missing_packets_out: 0 network_interface: eth1 packets_in: 6 packets_out: 5 reply_time: 0 request: GET /poisonivy-is-coming-for-you-batman.jpeg HTTP/1.0 request_ack_time: 3246 request_time: 61714 response_ack_time: 0 response_time: 0 server_rtt: 32357 server_rtt_packets: 2 server_rtt_sum: 64714 site: prankglassinebracket.jumpingcrab.com:1337 src_headers: GET /poisonivy-is-coming-for-you-batman.jpeg HTTP/1.0 Host: prankglassinebracket.jumpingcrab.com:1337</pre>

Sonuçlara göz attığımızda, “poisonivy-is-coming-for-you-batman.jpeg” adlı dosya için kullanılan HTTP GET yöntemine atıfta bulunan bir istek alanı içerdiğini görüyoruz.

Cevap: poisonivy-is-coming-for-you-batman.jpeg

#109

Question:

Cevap: 3791.exe