



نادي الأمن السيبراني
جامعة جدة

Cyber Kill Chain in Blue Team Perspective

نموذج الـ Cyber Kill chain من منظور الفريق الدفاعي

مقدمة:

النموذج هو مجموعة من الخطوات التي تتصل فيما بينها لتشكل سلسلة من الاحداث التي ينفذها المهاجم لاختراق النظام وكل مرحلة تحتوي على العديد من الأساليب والأدوات التي يمكن استخدامها.

أهمية النموذج:

يمثل هذا النموذج لاي باحث في مجال الامن السيبراني خطوات منظمه لكيفية حدوث الهجمة وبالأخص الفريق الدفاعي، حيث إن الباحث يستطيع من خلاله إعادة تركيب كيفية حدوث الهجمة مما يجعل الاستجابة لها أسرع وذا كفاءة عالية.

خطوات النموذج:

1- الاستطلاع والاستقصاء

في هذه المرحلة يتم جمع معلومات عن الضحية بطريقه مباشره مثل فحص منافذ الشبكة او بطريقه غير مباشره مثل برامج التواصل الاجتماعي او البحث في أي من محركات البحث

2- التسليح

في هذه المرحلة يتم انشاء البرنامج الخبيث اما ان يكون ransomware او virus او worm او أي من أنواع البرامج الخبيثة الذي يستغل ثغره معينه

3- التسليم

في هذه المرحلة يتم توصيل البرنامج الخبيث الى جهاز الضحية وهناك أكثر من طريقه منها ارسال البرنامج عن طريق بريد الكتروني احتيالي او عن طريق رابط وهمي، ويمكن دمج هذه العملية مع الهندسة الاجتماعية لتكون أكثر كفاءه

4- الاستغلال

في هذه المرحلة يتم تشغيل البرنامج الخبيث في جهاز الضحية

5- التثبيت

في هذه المرحلة يتم تثبيت الباب الخلفي وتنزيل برامج تساعد المهاجم على فحص اجهزه الشبكة او غيرها

6- الاوامر والتحكم

في هذه المرحلة يتصل المهاجم بجهاز الضحية وينشئ قناة تواصل مخفية لينفذ أوامر اضافية

7- الاجراءات على الهدف

في هذه المرحلة يقوم المهاجم بتنفيذ مبتغاه من عملية الاختراق وتتنوع اهداف المهاجمين بحسب الدافع، تشتمل على تسريب البيانات، تشفير الملفات، وطلب فدية.

مثال عملي:

في هذا المثال المحلل يقوم بالاستجابة الى الحوادث السيبرانية من مركز العمليات السيبرانية والذي يستخدم برنامج splunk لجمع ومراقبة بيانات المنظمة في نظام مركزي واحد

السيناريو:

تعرض موقع Wayne Enterprises لهجمة مما تبين لاحقا ان كل من يزور الموقع يرى صفحة الويب التالية:

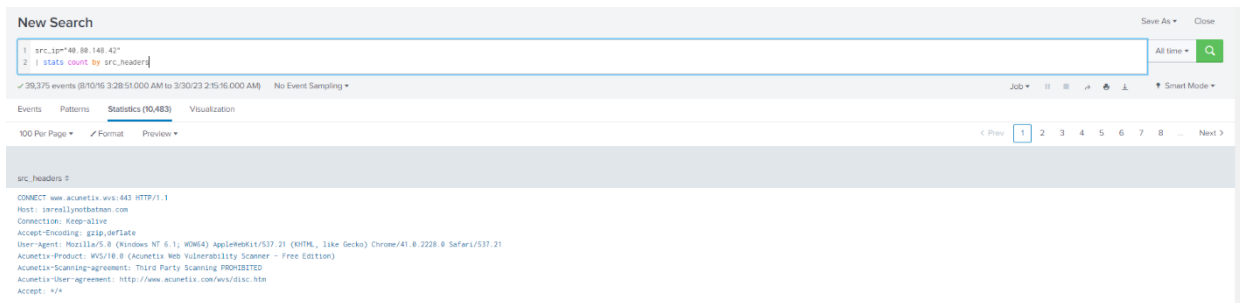


وهدفنا هو تحليل كيف وقع هذا الهجوم من خلال نموذج: cyber kill chain

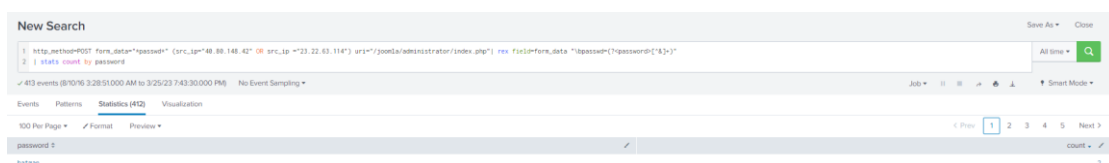
الخطوات:

1- الاستطلاع والاستقصاء

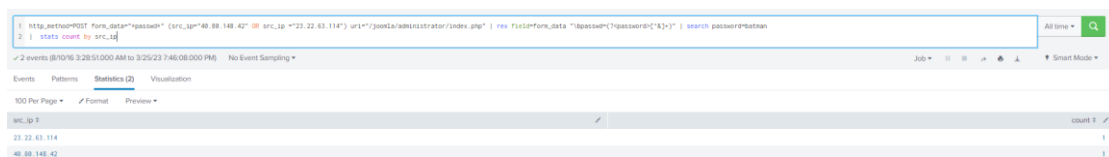
New Search		Save As	Close
1 index="botsv1" sseal1ymobtan sourcetype="stream:http"		All time	Q
2 stats count by src_ip			
✓ 22,200 events (8/10/16 3:28:51.000 AM to 3/30/23 2:12:34.000 AM) No Event Sampling			
Job			
Smart Mode			
Events Patterns Statistics (2) Visualization			
100 Per Page			
Format Preview			
src_ip		count	
21 22 63 114		1236	
48 88 148 42		28932	



بناءً على المعطيات موقع الويب تواصل مع عنوانين IP و عند البحث في العنوان صاحب أعلى عدد من البيانات نجد في متغير src_headers معلومات تشير أن الموقع يتعرض لعملية فحص ثغرات من خلال تطبيق Acunetix ونجد أن أحد العمليات هي brute force والتي تحاول اختراق حساب مشرف الموقع والذي لديه صلاحيات عالية نجح البرنامج في إيجاد كلمة المرور الصحيحة والتي هي "batman"



والتي استعملها المهاجم فيما بعد لتسجيل الدخول من جهاز آخر



2- التسليح

في هذه الخطوة المهاجم انشئ الملف الخبيث والذي تم رفعه للموقع فيما بعد باسم 3791.exe

3- التسليم

بعدما حصل المهاجم على كلمة المرور الصحيحة تمكن من رفع الملف المذكور في الخطوة رقم اثنان الى الخادم الذي يعمل عليه الموقع

4- الاستغلال

5- التثبيت

poisonivy-is-coming-for-you-batman.jpeg نلاحظ هنا انه طلب صورته باسم

```
8/10/16      { [-]
10:13:46.915 PM
ack_packets_in: 2
ack_packets_out: 5
bytes: 106
bytes_in: 106
bytes_out: 0
c_ip: 192.168.250.70
canceled: 1
capture_hostname: demo-01
client_rtt: 1
client_rtt_packets: 1
client_rtt_sum: 1
cs_version: 1.0
data_center_time: 0
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: pranglassinebracket.jumpingcrab.com:1337
src_headers: GET /poisonivy-is-coming-for-you-batman.jpeg HTTP/1.0
Host: pranglassinebracket.jumpingcrab.com:1337

src_ip: 192.168.250.70
src_mac: 00:0C:29:C4:02:7E
src_port: 63139
time_taken: 61715
```

6- الاورامر والتحكم

في هذا المثال لم يتم المهاجم بعمل أي اتصال ب جهاز الضحية

7- الاجراءات على الهدف

في هذه المرحلة نفذ المهاجم مبتغاه من الهجمة وهو تغيير محتوى صفحة الويب وأبدلها بالصورة المرفقة في وصف السيناريو

المصادر:

<https://www.crowdstrike.com/cybersecurity-101/cyber-kill-chain/>
<https://cyberdefenders.org/blueteam-ctf-challenges/15#nav-overview>