CCNA Cybersecurity Operations v1.0
Skills Assessment

Introduction

Working as the security analyst for ACME Inc., you notice a number of events on the SGUIL dashboard. Your task is to analyze these events, learn more about them, and decide if they indicate malicious activity.

You will have access to Google to learn more about the events. Security Onion is the only VM with Internet access in the Cybersecurity Operations virtual environment.

The tasks below are designed to provide some guidance through the analysis process.

You will practice and be assessed on the following skills:

- Evaluating Snort/SGUIL events.
- Using SGUIL as a pivot to launch ELSA, Bro and Wireshark for further event inspection.
- Using Google search as a tool to obtain intelligence on a potential exploit.

Content for this assessment was obtained from http://www.malware-traffic-analysis.net/ and is used with permission. We are grateful for the use of this material.

Addressing Table

The following addresses are preconfigured on the network devices. Addresses are provided for reference purposes.

Device	Interface	Network/Address	Description
Security Onion VM	eth0	192.168.0.1/24	Interface connected to the Internal Network
	eth2	209.165.201.21/24	Interface connected to the External Networks/Internet

Part 1: Gathering Basic Information

a. Log into Security Onion VM using with the username **analyst** and password **cyberops**.

b. Open a terminal window. Enter the **sudo service nsm status** command to verify that all the services and sensors are ready.

c. When the nsm service is ready, log into SGUIL with the username **analyst** and password **cyberops**. Click **Select All** to monitor all the networks. Click **Start SQUIL** to continue.

d. In the SGUIL window, identify the group of events that are associated with exploit(s). This group of events are related to a single multi-part exploit.

How many events were generated by the entire exploit?

11 unique evets related to the exploid

e. According to SGUIL, when did the exploit begin? When did it end? Approximately how long did it take?

Start: 2017/09/07 15:31:12

End: 2017/09/07 15:31:34

Duration: 21 seconds

f. What is the IP address of the internal computer involved in the events?

192.168.0.12

g. What is the MAC address of the internal computer involved in the events? How did you find it?

MAC address 00:1b:21:ca:f:d7 using wireshark

h. What are some of the Source IDs of the rules that fire when the exploit occurs? Where are the Source IDs from?

multiple source IDs and in Emerging threats website:

93.114.64.118, 173.201.198.128, 192.99.198.158, 208.113.226.171, 209.126.97.209 (209.165.200.235

i. Do the events look suspicious to you? Does it seem like the internal computer was infected or compromised? Explain.

Ya, event tersebut terlihat mencurigakan dan faktanya terjadi pada internal yang telah terkompromi. Peringatan Flash plugin yang telah kedaluwarsa dan peringatan Angler EK adalah bukti kuat kemungkinan tereksploitasi atau terkompromi.

j. What is the operating system running on the internal computer in question?

Window-based OS

Part 2: Learn About the Exploit

a. According to Snort, what is the exploit kit (EK) in use?

Angler EK

b. What is an exploit kit?

Exploit kit adalah alat pemrograman yang memungkinkan seseorang yang tidak memiliki pengalaman menulis kode perangkat lunak untuk membuat, menyesuaikan, dan mendistribusikan malware. Kit eksploit dikenal dengan sejumlah nama lain, termasuk kit infeksi, kit crimeware, kit serangan DIY, dan toolkit malware.

Exploit kit memiliki antarmuka program aplikasi grafis (API) yang memungkinkan pengguna non-teknis untuk mengelola serangan canggih yang mampu mencuri data perusahaan dan pribadi, mengatur eksploitasi denial of service (DoS)) atau membangun botnet

c. Do a quick Google search on ‘Angler EK’ to learn a little about the fundamentals the exploit kit. Summarize your findings and record them here.

1.Penyerang kompromi sejumlah situs lalu lintas tinggi dan menyuntikkan kode berbahaya

2. Pengguna mengunjungi situs yang disusupi dan browser mereka menjalankan kode yang disuntikkan berbahaya

3. Kode berbahaya memungkinkan pemindaian sistem korban, yang pada akhirnya mencari kemungkinan kerentanan

4. Informasi seperti plugin yang diinstal dan versinya, OS, nama dan versi browser web kemudian disaring ke server jahat, sering melalui HTTP POST yang disandikan.

5. Berdasarkan data exfiltrated, server jahat menyiapkan paket eksploit yang disesuaikan dan mengirimkannya ke browser korban

6. Paket exploit sering berisi exploit yang disesuaikan dan payload; exploit digunakan untuk mendapatkan hak eksekusi kode dalam sistem korban. Payload terdiri dari kode berbahaya tambahan yang hanya dapat dieksekusi setelah eksploit melakukan tugasnya.

d. How does this exploit fit the definition on an exploit kit? Give examples from the events you see in SGUIL.

eksploit menggunakan situs web yang disusupi untuk memindai host untuk mengetahui kerentanan dan kemudian mengunduh perangkat lunak berbahaya

e. What are the major stages in exploit kits?

1.Penyerang mencopy sejumlah situs yang pengunjung website yang tinggi dan menyuntikkan kode berbahaya

2. pengguna mengunjungi situs yang disusupi dan browser mereka menjalankan kode yang disuntikkan berbahaya

3. kode jahat memindai sistem korban, mencari kerentanan dan mengekstrak hasilnya ke server jahat lain melalui POST

4. berdasarkan pada data yang disaring, server jahat menyiapkan eksploit yang disesuaikan dan mengirimkannya ke browser korban

Part 3: Determining the Source of the Malware

a. In the context of the events displayed by SGUIL for this exploit, record below the IP addresses involved.

192.168.0.12, 93.114.64.118, 173.201.198.128, 192.99.198.158, 208.113.226.171, 192.168.0.1, 209.126.97.209

b. The first new event displayed by SGUIL contains the message “ET Policy Outdated Flash Version M1”. The event refers to which host? What does that event imply?

192.168.0.12; host menggunakan versi lama dari plugin Flash

c. According to SGUIL, what is the IP address of the host that appears to have delivered the exploit?

192.99.198.158

d. Pivoting from SGUIL, open the transcript of the transaction. What is the domain name associated with the IP address of the host that appears to have delivered the exploit?

qwe.mvdunalterableairreport.net

e. This exploit kit typically targets vulnerabilities in which three software applications?

adobe flash player, java runtime environmt, Microsoft Silverlight

f. Based on the SGUIL events, what vulnerability seems to have been used by the exploit kit?

outdated flash plugin

g. What is the most common file type that is related to that vulnerable software?

- adobe flash authoring file FLA
- action script file AS
- flash XML file XML
- compiled flash file SWF

h. Use ELSA to gather more evidence to support the hypothesis that the host you identified above delivered the malware. Launch ELSA and list all hosts that downloaded the type of file listed above. Remember to adjust the timeframe accordingly.
Were you able to find more evidence? If so, record your findings here.

Yes.
1510604611.228059|CYCGVz4HyAXsgGuNV2|209.165.201.17|47144|209.165.200.235|80|1|GET|209.165.200.235|/mutillidae/index.php?page=user-info.php&username='+union+select+ccid,ccnumber,ccv,expiration,null+from+credit_cards+--+&password=&user-info-php-submit-button=View+Account+Details|http://209.165.200.235/mutillidae/index.php?page=user-info.php&username=%27+union+select+ccid%2Cccnumber%2Cccv%2Cexpiration%2Cnull+from+credit_cards+--+&password=&user-info-php-submit-button=View+Account+Details|1.1|Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0|0|960|200|OK|-|-|HTTP::URI_SQLI|-|-|-|-|-|-|FvFBhF1tikxaHjaG1|-|text/html

host=127.0.0.1 program=bro_http class=BRO_HTTP srcip=209.165.201.17 srcport=47144 dstip=209.165.200.235 dstport=80 status_code=200 content_length=960 method=GET site=209.165.200.235 uri=/mutillidae/index.php?page=user-info.php&username='+union+select+ccid,ccnumber,ccv,expiration,null+from+credit_cards+--+&password=&user-info-php-submit-button=View+Account+Details referer=http://209.165.200.235/mutillidae/index.php?page=user-info.php&username=%27+union+select+ccid%2Cccnumber%2Cccv%2Cexpiration%2Cnull+from+credit_cards+--+&password=&user-info-php-submit-button=View+Account+Details user_agent=Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 mime_type=text/html

i. At this point you should know, with quite some level of certainty, whether the site listed in **Part 3b** and **Part 3c** delivered the malware. Record your conclusions below.

192.168.0.12, the internal host, was likely infected. It has an aotdated version of the flash plugin which was noticed by the exploit kit. 192.168.0.12 was then led to download a malicious SWF (Flash file) from qwe.mvdunalterableairreport.net

Part 4: Analyze Details of the Exploit

a. Exploit kits often rely on a landing page used to scan the victim's system for vulnerabilities and exfiltrate a list of them. Use ELSA to determine if the exploit kit in question used a landing page. If so, what is the URL and IP address of it? What is the evidence?

Hint: The first two SGUIL events contain many clues.

173.201.198.128

Landing page : lifeinsidetroit.com (173.201.198.128)

server script name: 02024870e4644b68814aadfbb58a75bc.php

extfiltrated data : e8bd3799338799332593b0b9caa1f426

full POST URI : POST/02024870e4644b68814aadfdbb58a75bc.php?q=e8bd3799ee8799332593b0b9caa1f426

The second new event in SGUIL implies that the compromised site allowed for a malicious Flash-based ad to be loaded from an ads site. This Flash-based ad is designed to scan the victim's computer and exfiltrate data to the EK's landing page.

After the vulnerability information has been collected, the Flash-based advertisement submits it via POST to a PHP script hosted on lifeinsidedetroit.com, the landing page. The landing page processes the collected info and chooses the exploit according to the vulnerability that has been discovered.

The exploit is then delivered to the client's web browser. As seen earlier in this documents, the victim's computer has an outdated version of Fkash. The exploit, hosted at qwe.mvdunalterableairreport.net, is then sent to the victim's computer. Notice that exploit is designed to allow code execution only. The exploit also contains further malware, known by EK terminology as the payload. The execution of the payload is the end game of the EK

b. What is the domain name that delivered the exploit kit and malware payload?

   qwe.mvdunalterableairreport.net

c. What is the IP address that delivered the exploit kit and malware payload?

   192.99.198.158

d. Pivoting from events in SGUIL, launch Wireshark and export the files from the captured packets as was done in a previous lab. What files or programs are you able to successfully export?

   3xdz3bcxc8