CCNA Cybersecurity Operations v1.0

Skills Assessment

Андрусів Соломія

1. 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.

1. 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 |

1. Gathering Basic Information
   * + 1. Log into Security Onion VM using with the username **analyst** and password **cyberops**.
       2. Open a terminal window. Enter the **sudo service nsm status** command to verify that all the services and sensors are ready.
       3. 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.
       4. 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\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + - 1. According to SGUIL, when did the exploit begin? When did it end? Approximately how long did it take?

\_\_\_\_\_07.09.2017 15.31.12-15.31.34 22 seconds \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + - 1. What is the IP address of the internal computer involved in the events?

\_\_\_\_192.168.0.12\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + - 1. What is the MAC address of the internal computer involved in the events? How did you find it?

\_\_\_\_00:1b:21:ca:fe:d7 right click the alertID, open Wireshark and there find the mac address \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + - 1. What are some of the Source IDs of the rules that fire when the exploit occurs? Where are the Source IDs from?

\_\_\_\_\_3.788, 3.787, 3,785 …\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + - 1. Do the events look suspicious to you? Does it seem like the internal computer was infected or compromised? Explain.

Комп’ютер був заражений трояном,(ET TROJAN), за дуже короткий проміжок часу (22 секунди) сталось аж 11 подій, тобто одна подія на дві секунди. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_What is the operating system running on the internal computer in question?

\_\_\_Windows XP 2000\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Learn About the Exploit
   * + 1. According to Snort, what is the exploit kit (EK) in use?

\_\_\_\_Angler\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + - 1. What is an exploit kit?

Це автоматизовані загрози, які використовують компрометовані веб-сайти для переадресації веб-трафіку, пошуку вразливих програм на базі браузера та запуску шкідливих програм. Були розроблені як спосіб автоматичного та безшумного використання вразливих версій на машинах жертв під час перегляду веб-сторінок.

* + - 1. 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.

Angler EK був виявлений вперше в 2013 році. Angler був одним з провідних ЕК, що використовувався кіберзлочинцями для розповсюдження зловмисних програм, починаючи від викупу та банківських троянів до рекламного шахрайства. Як і більшість інших ЕК, він зосереджувався на вразливостях веб-браузерів та їх плагінів. Angler був одним із небагатьох EK, який пропонував безпілотні інфекції, де зловмисне програмне забезпечення ніколи не торкалося диска і залишалося лише в пам'яті, щоб уникнути виявлення. Angler став неактивним у червні 2016 року. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + - 1. How does this exploit fit the definition on an exploit kit? Give examples from the events you see in SGUIL.

Англер пропонував безпілотні інфекції, які не зберігались на диску зараженого пристрою, а також здіснював зараження через переадресацію з веб-сторінки, що прямо відповідає визначенню EK.

Традиційні антивірусні продукти сканують файли, щоб виявити зараження зловмисними програмами. Але якщо файлів для сканування немає, то робиться висновок, що зараження також немає.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + - 1. What are the major stages in exploit kits?

4 основні стадії

1.Establish contact (встановлення контакту із середовищем хоста через цільову сторінку.)

2.Redirect (перенаправлення на альтернативну цільову сторінку та виявлення вразливих місць на хості, які можна використовувати.)

3.Exploit (запуск шкідливої програми та поширення вірусу)

4.Infect (Зараження хоста) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Determining the Source of the Malware
   * + 1. In the context of the events displayed by SGUIL for this exploit, record below the IP addresses involved.

192.168.0.1

192.168.0.12

192.99.198.158

173.201.198.128

208.113.226.171

209.126.97.209

93.114.64.118

* + - 1. 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?

Хост з ір адресою 192.168.0.12

Повідомлення вказує на те, що версія М1 флешу є застарілою\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + - 1. According to SGUIL, what is the IP address of the host that appears to have delivered the exploit?

\_\_\_\_192.199.198.158\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + - 1. 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?

\_\_\_\_\_\_\_\_\_\_\_\_\_ https://qwe.mvdunalterbleairreport.net\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + - 1. This exploit kit typically targets vulnerabilities in which three software applications?

\_\_\_\_\_\_\_Flash player, Internet Explorer та Silverlight\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + - 1. Based on the SGUIL events, what vulnerability seems to have been used by the exploit kit?

\_\_\_\_\_Flash \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + - 1. What is the most common file type that is related to that vulnerable software?

\_\_\_\_\_ SWE(Shockwave Flash file)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + - 1. 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.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + - 1. 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.

Так, сайт з 3с постачав шкідливе ПЗ, а хост з 3б мав застарілу, а отже, вразливу версію Flash\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Analyze Details of the Exploit
   * + 1. 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.

\_\_\_\_\_\_\_\_\_\_ IP address: 173.201.198.128 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

URL: http://adstirs.ro/544b29bcd035b2dfd055f5deda91d648.swf \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + - 1. What is the domain name that delivered the exploit kit and malware payload?

\_\_\_\_\_\_ https://qwe.mvdunalterbleairreport.net\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + - 1. What is the IP address that delivered the exploit kit and malware payload?

\_\_\_\_\_\_192.99.198.158\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + - 1. 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?

\_\_\_\_filename 3xdz3bcxc8 hostname qwe.mvdunalterbleairreport.net packet nums [13,16,18,20,21,27,47,48,51,62]\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_