Lab 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. Located here: http://194.47.149.5/incidents/Lab_1.ova

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.

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_____

_____

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

____Початок: 2017-09-07 15:31:12_____

____Кінець: 2017-09-07 15:31:34_____

____Тривалість: 22 секунди_____

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?

____00:1b:21:CA:FE:D7 _____

____Щоб дізнатись цільову MAC-адресу необхідно було переглянути у Wireshark відповідне поле Ethernet II фрейму для повідомлення, яке сповіщало про активність цього внутрішнього комп'ютера___

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

____2018316, 2018954, 2019645, 2020491, 2021120 _____

____/nsm/server_data/securityonion/rules/seconion-eth0-1/downloaded.rules_____

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

____Дійсно, ці всі події, які пов'язані з експлойтом виглядають підозрілими, так як схоже, що для атаки було використано знайомий зразок ШПЗ – TROJAN Zeus GameOver. Проте SGUIL не може вказувати на те, що якийсь там внутрішній комп'ютер був заражений або зламаний, адже цей застосунок призначений лише для сповіщення про потенційні інциденти безпеки. А от уже відповідні фахівці проводять додаткові дослідження, щоб визначити, чи були комп'ютери у мережі інфіковані або скомпрометовані. Із точки зору управління інцидентами, цей експлойт, справді, міг нашкодити комп'ютеру, тому спеціалісти з аналізу шкідливого програмного забезпечення повинні взяти до уваги цей випадок і провести власне дослідження___

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

____Windows _____

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 – це набір програмних засобів, розроблений для автоматизації процесу доставки зловмисного програмного забезпечення на вразливі комп'ютери за допомогою веб-атак. До того ж, ці набори, як правило, розроблені таким чином, щоб бути простими у використанні та доступними навіть для нетехнічних зловмисників, що робить їх популярним вибором для широкого кола кіберзлочинців_____

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.

____Angler EK був хорошим витонченим інструментом, який використовувався для доставки шкідливого програмного забезпечення через скомпрометовані веб-сайти або рекламні кампанії. Він був відомий своєю здатністю виявляти низку вразливостей програмного забезпечення, параметрами налаштування, передовою автоматизацією та використанням методів ухилення, що ускладнювало виявлення антивірусами та IDS/IPS. Набір міг доставляти різноманітне шкідливе програмне забезпечення та становив серйозну загрозу для користувачів та організацій. Хоча Angler EK більше не доступний, його методи й тактики продовжують використовуватися іншими наборами експлойтів і кампаніями зловмисного програмного забезпечення. Тому залишатися завжди пильним і оновлювати програмне забезпечення є надзвичайно важливим для захисту від таких типів атак _____

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

____Angler EK абсолютно точно відповідає визначенню терміну "exploit kit", оскільки він, дійсно, є тим самим комплексним інструментом, що використовується для автоматизації використання вразливостей програмного забезпечення на стороні клієнта, які зазвичай являють собою ненадійні веб-браузери та застарілі веб-плагіни_____

____Для наглядності продемонструємо усі повідомлення про події, які були залоговані під час активізації експлойту. Додатково також опишемо, яких зміст вони за собою несуть ▼▼▼_____

- "ET POLICY Outdated Flash Version M1" – вказує на те, що на хості використовується застаріла версія Flash Player, яка потенційно може бути вразливою для використання.
- "ET CURRENT_EVENTS 32-byte by 32-byte PHP EK Gate with HTTP POST" – відноситься до 32-byte by 32-byte шлюзу набору експлойтів PHP, який використовує запити HTTP POST для зв'язку зі своїм сервером command and control (C&C).
- "ET CURRENT_EVENTS DRIVEBY Angler EK Apr 01 2014" – посилається на екземпляр набору експлойтів Angler, який використовувався в атаці завантажень Drive-by 1 квітня 2014 р.
- "ET CURRENT_EVENTS Angler EK Oct 22 2014" – посилається на екземпляр набору експлойтів Angler, який використовувався в атаці 22 жовтня 2014 р.
- "ET CURRENT_EVENTS Angler EK Feb 04 2015 M2" – посилається на екземпляр набору експлойтів Angler, який використовувався в атаці 4 лютого 2015 року.
- "ET CURRENT_EVENTS EK Encoded Shellcode IE" – посилається на закодований шеллкод, який використовується в атаці набору експлойтів, націленої на Internet Explorer.
- "ET POLICY External Timezone Check (earthtools.org)" – вказує на те, що хост виконує зовнішню перевірку часового поясу за допомогою веб-сайту earthtools.org, який потенційно може бути використаний для визначення місцезнаходження жертви.
- "ET TROJAN Possible Bedep Connectivity Check (2)" – вказує на те, що хост може намагатися встановити з'єднання з трояном Bedep, який може бути використаний для зловмисних цілей.
- "ET TROJAN Zeus GameOver Possible DGA NXDOMAIN Responses" – посилається на можливий алгоритм генерації домену (DGA), який використовується трояном Zeus GameOver для уникнення виявлення.
- "ET TROJAN Bedep SSL Cert" – вказує на те, що троян Bedep використовує сертифікат SSL, який можна використовувати для підвищення безпеки зв'язку з його сервером C&C.
- "ET CURRENT_EVENTS Angler EK Flash Exploit URI Struct" – посилається на екземпляр набору експлойтів Angler, який використовується для використання вразливості в Adobe Flash Player через структуру URI.

e. What are the major stages in exploit kits?

____Exploit kits зазвичай складаються з кількох етапів, кожен із яких відіграє певну роль у атаці. Ці стадії включають Delivery of the exploit kit, Exploitation, Payload delivery, Command and Control та Persistence. Трохи детальніше про кожен етап ▼▼▼ _____

* Етап **доставки експлойтного набору** передбачає доставку набору експлойтів до системи жертви. Це часто робиться за допомогою фішингових електронних листів або рекламних кампаній.

* Етап **експлуатації** передбачає використання відомих вразливостей програмного забезпечення для отримання доступу до системи жертви.
* Етап **доставки корисного навантаження** передбачає доставку шкідливого файлу в систему жертви. Цей файл може бути трояном або програмою-вимагачем і може бути зашифрованим або обфускованим, щоб уникнути виявлення.
* Стадія **команд-контролю** передбачає встановлення з'єднання між системою жертви та віддаленим сервером, контрольованим зловмисником. Це дозволяє зловмиснику видавати команди корисному навантаженню та вилучати дані з системи жертви.
* І нарешті, стадія **продовження існування** включає в себе встановлення бекдору або іншого механізму, який дозволяє зловмиснику підтримувати доступ до системи жертви протягом тривалого часу.

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, 192.168.0.1_____

____93.114.64.118, 173.201.198.128 _____

____192.99.198.158, 208.113.226.171, 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?

____IP: 93.114.64.118 та Hostname: adstairs.ro_____

____Подія з повідомленням "ET Policy Outdated Flash Version M1" зазвичай означає, що в системі мережі працює застаріла версія Adobe Flash Player, що може становити загрозу безпеці, оскільки зловмисники можуть використати відомі вразливості програмного забезпечення. Отож, у даному випадку рекомендується вжити заходів для оновлення програмного забезпечення до останньої версії або повністю вимкнути його, якщо воно більше не потрібне, щоб зменшити ризик успішної атаки_____

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 Environment, Microsoft Silverlight _____

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

____У наданому SGUIL-звіті такі події, які, для прикладу, містять повідомлення "ET CURRENT_EVENTS Angler EK Flash Exploit URI Struct" та "ET CURRENT_EVENTS EK Encoded Shellcode IE" свідчать про те, що Angler EK використовував уразливості в **Adobe Flash Player** і **Internet Explorer** для доставки зловмисного корисного навантаження на комп'ютер жертви_____

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

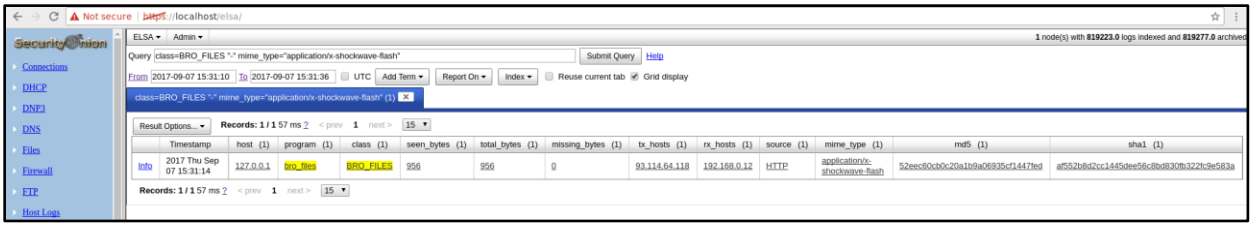
____.swf (Shockwave Flash) – це формат файлів, який використовується для мультимедійного та інтерактивного вмісту, наприклад анімації, ігор і відео, який часто відтворюється у веб-браузері чи іншій програмі за допомогою плагіна Adobe Flash Player. Файли SWF можуть містити код ActionScript, який використовується для додавання інтерактивності та функціональності вмісту. Однак уразливості в плагіні

Flash Player дозволяють зловмисникам використовувати недоліки в коді ActionScript або в самому форматі файлу SWF, потенційно надаючи їм змогу виконувати шкідливий код або контролювати систему жертви____

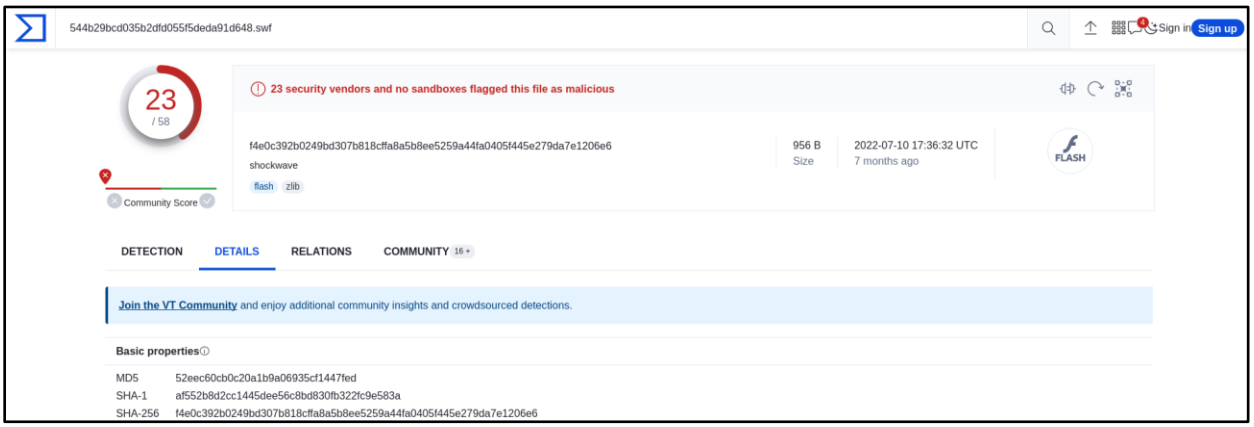
h. Use ELSA to gather more evidence to support the hypothesis that the host you identified above delivered the malware. Launch ELSA and list all hosts that downloaded the type of file listed above. Remember to adjust the timeframe accordingly.

Were you able to find more evidence? If so, record your findings here.

___Так, схоже, що веб-застосунок `ELSA` дозволив підтвердити той факт, що було використано `.swf` файл для активізації шкідливого програмного забезпечення. Для наглядності наведемо відповідний знімок екрану↓___



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.



_____↑Судячи із вищенаведеного зображення, ми можемо стверджувати, що із великою долею ймовірності на цільовий комп'ютер було, дійсно, доставлено зловмисне програмне забезпечення. Звідси маємо, що відповідні веб-сторінки були залучені до процесу доставки та експлуатації вразливостей внутрішнього хоста__

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?

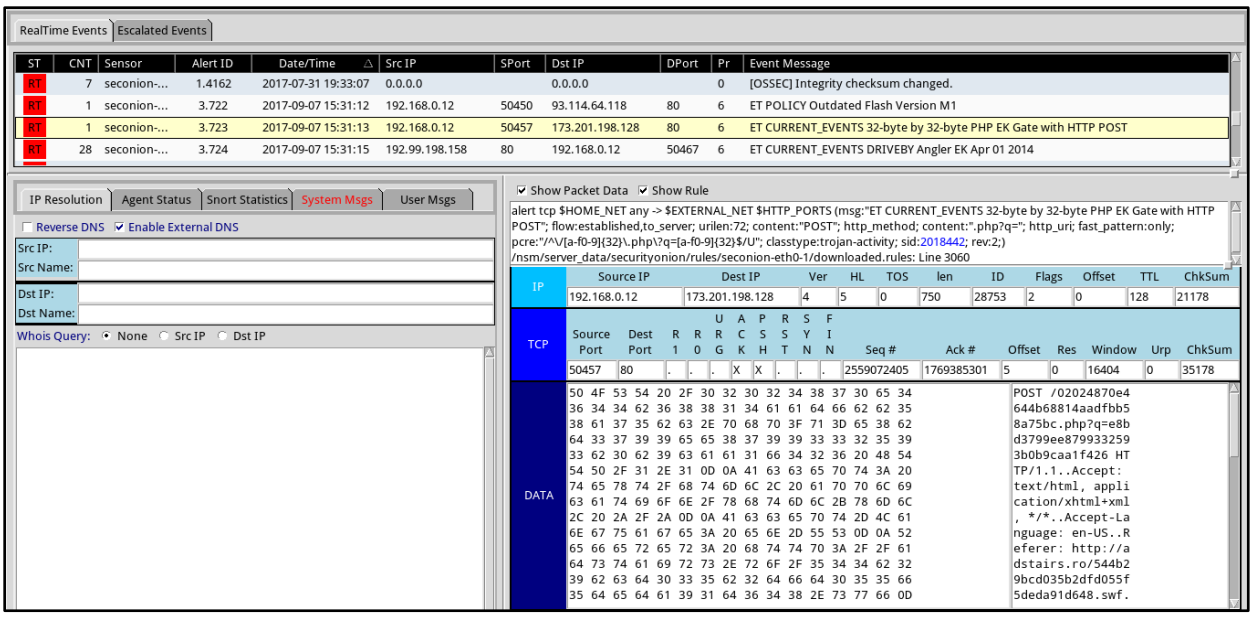
Hint: The first two SGUIL events contain many clues.

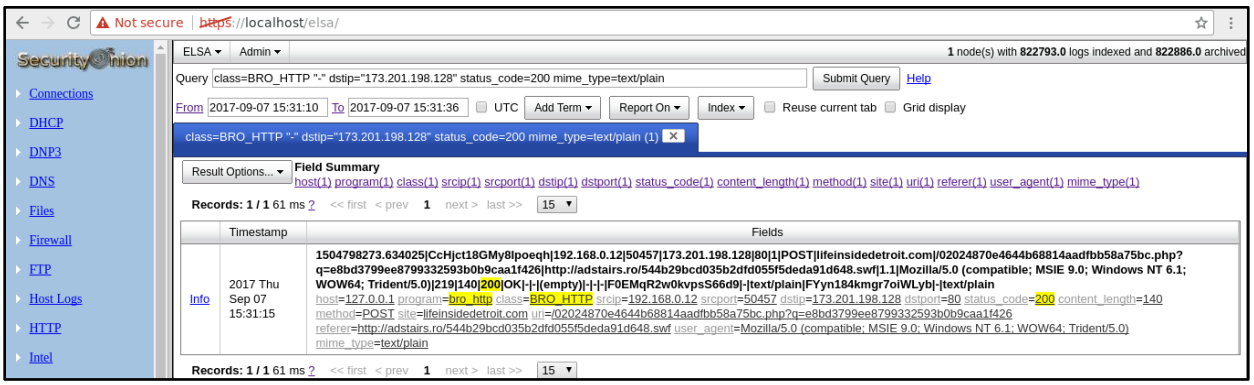
____IP: 173.194.116.121 _____

____site: lifeinsidedetroit.com_____

____URI: /02024870e4644b68814aadfbb58a75bc.php?q=e8bd3799ee8799332593b0b9caa1f426 _____

____referer: http://adstairs.ro/544b29bcd035b2dfd055f5deda91d648.swf_____





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?

____Щоби не виписувати довгу та в деяких випадках беззмістовну назву кожного файлу, то запишемо лише тип змісту цих даних, які можна експортувати із перехоплених пакетів у застосунку Wireshark▼▼▼_____

- application/x-shockwave-flash
- application/x-www-form-urlencoded
- text/html
- data
- application/xml