

# 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](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

- Log into Security Onion VM using with the username: **analyst** and password: **cyberops**.
- Open a terminal window. Enter the **sudo service nsm status** command to verify that all the services and sensors are ready.
- 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.
- 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\_\_\_\_\_

- 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 експлоїту. 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 експлоїтів 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 експлоїтів Angler, який використовувався в атаці завантажень Drive-by 1 квітня 2014 р.
- “ET CURRENT\_EVENTS Angler EK Oct 22 2014” – посилається на екземпляр набору експлоїтів Angler, який використовувався в атаці 22 жовтня 2014 р.
- “ET CURRENT\_EVENTS Angler EK Feb 04 2015 M2” – посилається на екземпляр набору експлоїтів 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 експлоїтів, 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 експлоїтів 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 експлоїтного набору** передбачає доставку набору експлоїтів 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

- 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\_\_\_\_\_
- 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\_\_\_\_\_
- According to SGUIL, what is the IP address of the host that appears to have delivered the exploit?  
 \_\_\_\_192.99.198.158\_\_\_\_\_
- 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?  
 \_\_\_\_gwe.mvdunalterableairreport.net\_\_\_\_\_
- This exploit kit typically targets vulnerabilities in which three software applications?  
 \_\_\_\_Adobe Flash Player, Java Runtime Environment, Microsoft Silverlight\_\_\_\_\_
- 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\_\_\_\_\_
- 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↓\_\_\_\_

Query: class=BRO\_FILES "mime\_type=application/x-shockwave-flash"

From: 2017-09-07 15:31:10 To: 2017-09-07 15:31:36 UTC Add Term Report On Index Reuse current tab Grid display

Timestamp	host (1)	program (1)	class (1)	seen_bytes (1)	total_bytes (1)	missing_bytes (1)	tx_hosts (1)	rx_hosts (1)	source (1)	mime_type (1)	md5 (1)	sha1 (1)
2017 Thu Sep 07 15:31:14	127.0.0.1	ms_exe	BRO_FILES	956	956	0	93.114.64.118	192.168.0.12	HTTP	application/x-shockwave-flash	52eec50c0c20a1b9a06935c1447fed	a1552b8d2cc1445dee56c8bd830b322fc9e583a

Records: 1 / 1 57 ms 2 < prev 1 next > 15 >

- 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.

544b29bcd035b2dfd055f5deda91d648.swf

23 / 58 security vendors and no sandboxes flagged this file as malicious

4e0c392b0249bd307b818cfa8a5b8ee5259a44fa0405445e279da7e1206e6

shockwave 956 B 2022-07-10 17:36:32 UTC 7 months ago

Flash ZIP

DETECTION DETAILS RELATIONS COMMUNITY 18

Join the VT Community and enjoy additional community insights and crowdsourced detections.

Basic properties

MD5	52eec50c0c20a1b9a06935c1447fed
SHA-1	a1552b8d2cc1445dee56c8bd830b322fc9e583a
SHA-256	4e0c392b0249bd307b818cfa8a5b8ee5259a44fa0405445e279da7e1206e6

\_\_\_\_↑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: /02024870e4644b68814aadfb58a75bc.php?q=e8bd3799ee8799332593b0b9caa1f426\_\_\_\_

\_\_\_\_referer: <http://adstairs.ro/544b29bcd035b2dfd055f5deda91d648.swf>\_\_\_\_

RealTime Events

Escalated Events

ST	CNT	Sensor	Alert ID	Date/Time	Δ	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	7	seconion-...	1.4162	2017-07-31 19:33:07	0.0.0.0	0.0.0.0		0.0.0.0		0	[OSSEC] Integrity checksum changed.
RT	1	seconion-...	3.722	2017-09-07 15:31:12	192.168.0.12	50450	93.114.64.118	80	6	6	ET POLICY Outdated Flash Version M1
RT	1	seconion-...	3.723	2017-09-07 15:31:13	192.168.0.12	50457	173.201.198.128	80	6	6	ET CURRENT_EVENTS 32-byte by 32-byte PHP EK Gate with HTTP POST
RT	28	seconion-...	3.724	2017-09-07 15:31:15	192.99.198.158	80	192.168.0.12	50467	6	6	ET CURRENT_EVENTS DRIVEBY Angler EK Apr 01 2014

IP Resolution

Agent Status

Snort Statistics

System Msgs

User Msgs

Reverse DNS

Enable External DNS

Src IP:

Src Name:

Dst IP:

Dst Name:

Whois Query:

None

Src IP

Dst IP

Show Packet Data

Show Rule

alert tcp \$HOME\_NET any -> \$EXTERNAL\_NET \$HTTP\_PORTS (msg:"ET CURRENT\_EVENTS 32-byte by 32-byte PHP EK Gate with HTTP POST"; flow:established,to\_server; urilen:72; content:"POST"; http\_method; content:".php?q="; http\_uri; fast\_pattern:only; pcre:"/^(a-f0-9){32}.php?q=(a-f0-9){32}\$/U"; classtype:trojan-activity; sid:2018442; rev:2; /nsm/server\_data/securityonion/rules/seconion-eth0-1/downloaded.rules: Line 3060

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum					
TCP	192.168.0.12	173.201.198.128	4	5	0	750	28753	2	0	128	21178					
	Source Port	Dest Port	R	R	C	S	S	Y	I	Seq #	Ack #	Offset	Res	Window	Urp	ChkSum
	50457	80	.	.	.	X	X	.	.	2559072405	1769385301	5	0	16404	0	35178
DATA	50 4F 53 54 20 2F 30 32 30 32 34 38 37 30 65 34 POST /02024870e4644b68814aadfb58a75bc.php?q=e8bd3799ee8799332593b0b9caa1426 HTTP/1.1..Accept: text/html, application/xhtml+xml, /*..Accept-Language: en-US..Referer: http://a dstairs.ro/544b29bcd035b2dfd055f5deda91d648.swf.															

→ ↶ ↷

⚠ Not secure | https://localhost/elsa/

☆

Security Onion

Connections

DHCP

DNP3

DNS

Files

Firewall

FTP

Host Logs

HTTP

Intel

ELSA Admin 1 node(s) with 822793.0 logs indexed and 822886.0 archived

Query class=BRO\_HTTP "-" dstip="173.201.198.128" status\_code=200 mime\_type=text/plain Submit Query Help

From 2017-09-07 15:31:10 To 2017-09-07 15:31:36 UTC Add Term Report On Index Reuse current tab Grid display

class=BRO\_HTTP "-" dstip="173.201.198.128" status\_code=200 mime\_type=text/plain (1) X

Result Options... Field Summary

host(1) program(1) class(1) srcip(1) srcport(1) dstip(1) dstport(1) status\_code(1) content\_length(1) method(1) site(1) uri(1) referer(1) user\_agent(1) mime\_type(1)

Records: 1 / 1 61 ms 2 << first < prev 1 next > last >> 15

Timestamp Fields

Info

2017 Thu Sep 07 15:31:15

1504798273.634025[CcHjct18GMy8lpoeqh]192.168.0.12[50457]173.201.198.128[80][1]POST[lifeinsidedetroit.com]/02024870e4644b68814aadfb58a75bc.php?q=e8bd3799ee8799332593b0b9caa1426/http://adstairs.ro/544b29bcd035b2dfd055f5dada91d648.swf[1.1]Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)[219][140][200]OK[-][-]F0EMqR2w0kvpsS66d9[-]text/plain[FYn184kmgr7oiWLYb[-]text/plain

host=127.0.0.1 program=bro\_http class=BRO\_HTTP srcip=192.168.0.12 srcport=50457 dstip=173.201.198.128 dstport=80 status\_code=200 content\_length=140 method=POST site=lifeinsidedetroit.com uri=/02024870e4644b68814aadfb58a75bc.php?q=e8bd3799ee8799332593b0b9caa1426 referer=http://adstairs.ro/544b29bcd035b2dfd055f5dada91d648.swf user\_agent=Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0) mime\_type=text/plain

Records: 1 / 1 61 ms 2 << first < prev 1 next > last >> 15

- b. What is the domain name that delivered the exploit kit and malware payload?  
 \_\_\_\_gwe.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 беззмстовну 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