CCNA Cybersecurity Operations v1.1 – Skills Assessment Answers

itexamanswers.net/ccna-cybersecurity-operations-v1-1-skills-assessment-answers.html

July 12, 2020

CCNA Cybersecurity Operations v1.1
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:

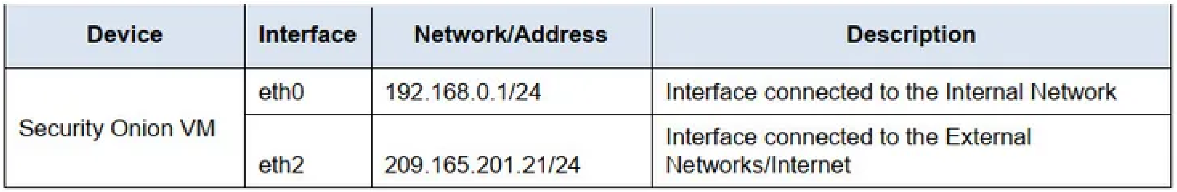
- Evaluating Snort/SGUIL events.
- Using SGUIL as a pivot to launch ELSA, Bro and Wireshark for further event inspection.

- 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?

Events that will be exploited are 15 events out of 25 group

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

Exploits begin 2017-09-07 15:31:12 and end 2017-09-07 15:31:34. so the time interval only lasts for 22 seconds.

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

Internal IP addresses involved in the event is 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:fe: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.

Yes, the event looks suspicious and the fact is that internal compromises have been made. The Flash plugin warning has expired and the Angler EK warning is strong evidence of possible exploitation or compromise

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?

(https://en.wikipedia.org/wiki/Exploit_kit)

An exploit kit is a software kit designed to run on web servers, with the purpose of identifying software vulnerabilities in client machines communicating with it, and discovering and exploiting vulnerabilities to upload and execute malicious code on the client. One of the earlier kits was MPack, in 2006. Exploit kits are often designed to be modular and easy to use, enabling the addition of new vulnerabilities and the removal of existing ones. Exploit kits also provide a user interface for the person who controls them, which typically includes information on success rates and other types of statistics, as well as the ability to control their settings. A typical kit is a collection of PHP scripts that target security holes in commonly used programs such as Apple Quicktime or Mozilla Firefox. Widely used software such as Oracle Java and Adobe Systems products are targeted particularly often.

The exploit kit gathers information on the victim machine, finds vulnerabilities and determines the appropriate exploit, and delivers the exploit, which typically silently drive-by downloads and executes malware. Kits are becoming ever more sophisticated. They tend to be neatly packaged, and do not require any understanding of exploits, and very little computer proficiency. Kits may have a Web interface showing active victims and statistics. They may have a support period and updates like commercial software.

Exploit kit is a programming tool that allows someone who has no experience writing software code to create, customize, and distribute malware. Exploiting kits are known by a number of other names, including infection kits, crimeware kits, DIY attack kits, and malware toolkits.

Exploit kit has a graphical application program interface (API) that allows non-technical users to manage sophisticated attacks capable of stealing corporate and personal data, manage denial of service exploits (DoS)) or build botnets.

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. Attackers compromise a number of high-traffic sites and inject malicious code
2. Users visit compromised sites and their browsers run maliciously injected code
3. The malicious code allows scanning of the victim's system, which in turn looks for possible vulnerabilities
4. Information such as the installed plugin and version, OS, name and version of the web browser are then filtered to the malicious server, often via encrypted HTTP POST.
5. Based on exfiltrated data, the malicious server prepares a customized exploit package and sends it to the victim's browser
6. Exploit packages often contain customized exploits and payloads; exploit is used to get code execution rights in the victim system. The payload consists of additional malicious code that can only be executed after the exploiter has done its job

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

Exploits use compromised websites to scan hosts to find out vulnerabilities and then download malicious software

e. What are the major stages in exploit kits?

1. The attacker copies a number of sites that have high website visitors and injects malicious code.
2. users visit compromised sites and their browsers run dangerous injected code
3. The malicious code scans the victim's system, looks for vulnerabilities and extracts the results to other malicious servers via POST
4. Based on filtered data, the malicious server prepares a customized exploit and sends it to the victim's browser

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; The host uses an old version of the Flash plugin

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?

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=userinfo.php&username='+union+select+ccid,ccnumber,ccv,expiration,null+from+credit_cards+–+&password=&user-info-php-
submitbutton=View+Account+Details|http://209.165.200.235/mutillidae/index.php?
page=userinfo.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; Linuxx86_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=47144dstip=209.165.200.235 dstport=80
status_code=200 content_length=960 method=GETsite=209.165.200.235 uri=/mutillidae/ndex.php?
page=userinfo.php&username='+union+select+ccid,ccnumber,ccv,expiration,null+from+credit_cards+–+&password=&user-info-php-
submit-button=View+Account+Detailsreferer=http://209.165.200.235/mutillidae/index.php?
page=userinfo.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 E

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