Lab 5
Puppetnets: Simple Forensics Investigation

Student 1 – FULL NAME: Mohammad Musaab Student 1 – Student/Banner ID: 100828060

Student 2 – FULL NAME: Sreejon Chowdhury Student 2 – Student/Banner ID: 100828598

Tools: `Wireshark`

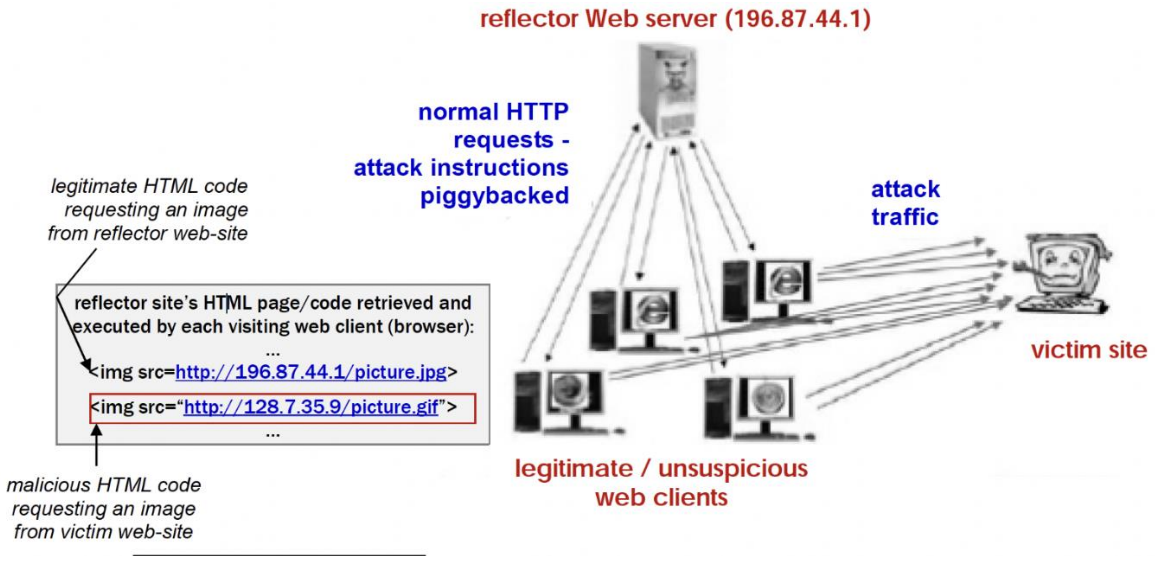
Submission expectations: In this lab, you must write your answers in the provided regions on the lab manual, save, and submit the saved copy online (DO NOT CREATE A SEPARATE PDF DOCUMENT).

1 Puppetnets [30 points]

Application-layer Distributed Denial of Service (DDoS) attacks can be conducted using either botnets or puppetnets.1 Recall, the main difference between the two is that:

1) Botnet approach requires that a large number of 3rd party machines be infected and put under the control of the DDoS attacker/hacker – thus forming a network of bots/agents.

2) Puppetnet approach is much simpler. Instead of infecting many machines and creating a network of bots, a puppetnet requires that a 'malicious HTML code' be injected (only) into one or a few popular websites, i.e. their respective web/HTML pages. We will refer to these as reflector web-sites. An example of a malicious puppetnet code could be something as simple as a request for a large image from the machine/server that is the ultimate target of the DDoS attack (i.e., the victim machine). Clearly, if such a command is injected into the HTML code of the reflector web-site, then every time the reflector web-site gets visited by a legitimate/unsuspicious user, an HTTP/image request will be sent towards the victim machine. For popular reflector web-sites that get visited hundreds of thousands of times a day, this would imply an equally large number of requests directed towards the victim web-site – i.e., a pretty powerful application-layer DDoS attack. (For an illustration, see below.)


reflector Web server (196.87.44.1)
normal HTTP requests - attack instructions piggybacked
attack traffic
victim site
legitimate / unsuspicious web clients
legitimate HTML code requesting an image from reflector web-site
malicious HTML code requesting an image from victim web-site

reflector site's HTML page/code retrieved and executed by each visiting web client (browser):

```
...
<img src=http://196.87.44.1/picture.jpg>
<img src="http://128.7.35.9/picture.gif">
...
```

We have learned that one of our course web-pages have been altered by an unauthorized user and utilized for the purposes of puppetnet-based DDoS attack on a third party (victim) website.

Your task is to inspect the given page, and find the answers to the following:

1. What is the identity of the victim web-site? http://192.197.183.149/test.png______

2. What is the actual malicious code injected by the unauthorized user?
<img src="http://192.197.183.149/test.png" height="1" width="1" />____________

3. Is the malicious code clearly visible, i.e. could it be spotted through 'visual inspection' of the infected web-page? no___________________________

The suggested tools to be used are:

a) Wireshark. It is recommended that you launch/run Wireshark prior to the loading of the infected web-page, in order to capture all the relevant communication/packets. Retrieval of packets from sites other than `pmadani.ca` domain is a good indication of a malicious activity.

b) View "Page Source" by right clicking on the website and find the appropriate option for source viewing.

c) nslookup. This ms-dos command2 can help you reveal the DNS (i.e., symbolic-name) identity of various IP addresses appearing in Wireshark capture.

d) Just visit the IP address you have found, it is the easit way to find out the identity of the victim: by visting their website!

The infected web-page is: http://pmadani.ca/resources/dos.html