Homework 4
CS 468: Network Security

April 3, 2022

Getting Started

The homework assignment is due date is **April 13, 2022 at 11:59pm local time**. For this assignment, you are required to write your solution in Python programming language, version 3.5 or later. The goal of this assignment is to write a proxy program that intercepts connections and does certain actions on them. To complete this assignment, you are allowed to use standard Python libraries as well as packet related modules. Kindly read through the handout before starting. If you have any questions, please ask on Piazza.

Malicious Proxy (20 Points)

Proxies on the network intercept and forward traffic on the Internet. In a normal scenario (without a proxy) all the traffic is sent to the destination. When there is a proxy present, clients relay their traffic to the proxy, which forwards the traffic to the destination, awaits the response, and then sends the response back to the client.

Your task in this assignment is to write a malicious proxy. Your proxy will operate in either active or passive mode, which we will talk about in a bit. In the passive mode the proxy will only observe all cleartext traffic and will extract certain sensitive information. In the active mode, your proxy will inject malicious javascript into the packets. For this assignment you can assume no traffic sent through the proxy is encrypted using application layer mechanisms (ssh, ssl) etc. You should write your program in a single file and name it as `proxy.py`. Your proxy should execute using the following command and take in the following inline arguments:

```
>> python3 proxy.py [-m [active/passive] listening_ip listening_port domain
```

- `-m`: The mode you want your proxy to operate, which will either be active or passive.
- `listening_ip`: The IP address your proxy will listen on connections on.
- `listening_port`: The port your proxy will listen for connections on.
- `domain` : The target domain that your proxy will serve a phishing page (only available under the active mode).

Below are the requirements you need to implement in your proxy for each of the respective modes.

Passive Mode: In this mode your proxy, in addition to forwarding packets, should continuously look for the presence of the following information in packets and log them to to a file named `info_1.txt`. Note that your code will be tested against a variety of inputs so be comprehensive as possible.

- Usernames/emails and passwords sent as query parameters, or submitted through a form.
- Anything resembling a credit card number or a social security number.
- Common North American names, US addresses and US based phone numbers.
- Cookies present along with the HTTP request

Hint: Make use of regular expressions to capture nuances in different format types, ensure you look at both request and response packets. Remember, information can be passed in the URL and headers too.

Active Mode: In this mode your proxy will actively inject JavaScript in the response pages. Your injected code should extract the client's user agent, screen resolution, and language and should send this information back to the proxy server IP address as a GET request with the details encoded as the query parameters, stated in the example below. On receiving the request, your proxy should parse it, and save the relevant information into a file named `info_2.txt`.

```
http://proxy_ip_address/?user-agent=USER_AGENT&screen=SCREEN_RES&lang=LANGUAGE
```

Hint: To get the user-agent and language, look into the JS navigator module. The screen resolution can be extracted from the JS window module. To send strings as a query parameter, make sure you encode them accordingly.

Phishing Attack. Additionally, your system should deploy a phishing attack when the user tries to connect to a predefined domain (e.g., `example.com`). Your proxy should return a bogus page with a login form in those cases. Your goal is **NOT** to create a realistic phishing page (do not use actual copyrighted logos etc.), so feel free to design the page's aesthetic however way you want.

Testing Your Proxy

To test your proxy, you can go into your browser settings and configure a HTTP proxy with the IP and port your proxy is running on. This configuration will cause your browser to send all HTTP traffic to your proxy which should process and forward it accordingly.

In addition, to facilitate testing we have created the following sample URLs that you can load in your browser to test if your proxy is able to extract relevant information from the responses.

- http://cs468.cs.uic.edu/test_page.html

For the phishing attack task, you should be able to detect the HTTP request on the target domain and serve the phishing page through the crafted response. Since this is a separate task from the injected JS code, you can test it on the course's test website or any website you choose.

Submission

For this assignment you are required to upload the following files in an archive named as `hw4.zip` to Gradescope.

1. `proxy.py:` Your main proxy program.
2. `phishing_page.html` : Your crafted phishing page.
3. `explanation.txt:` Describe in a paragraph about your general approach for this homework, the tested domain(s) for the phishing attack and details of your implementation and the list of online resources that you referred to.

Good Luck!