Networks and Systems Security II - Winter 2022

Sambuddho Chakravarty

April 29, 2022

Exercise 4 (total points: 140)

Due date: May 15. Time: 23:59 Hrs. (Hard deadline, no extensions)

1 Running Tor Client (total points: 50)

The first exercise is to familiarize you with Tor. You need to download the Tor source code and compile and install it on your local machine (laptop/desktop) and configure your browser manually, by changing the proxy settings to point to the Tor program. This should relay the web traffic via the Tor program.

Thereafter, you need to be able to create arbitrary length Tor circuits using the `TorCtl/stem` library.

What you need to submit/grading rubric:

1. Screenshots of the steps, and commands used, along with description of these commands and their options (20 points).
2. A python script that automates the above Tor circuit creation process. It should take inputs as the number of relays required, and also their RSA fingerprints and creates a custom circuit through the chosen relays. The circuit can be of arbitrary length. (30 points).

2 Private Tor Network Using VMs (total points: 50)

The second exercise is for you to set-up your own private Tor network with various VMs. You need 5 VMs, each one for the client, guard node, middleman, exit node and the server. You need to configure three of these VMs as relays – guard, middle and exit node. The relays are configured to operate as private Tor relays, via the configuration changes.

The client uses a web request client like `wget` or `curl` and uses that to communicate to the server to download a particular file. The server should be running a web server like `apache` or `lighttpd`. The client should use the `TorCtl/stem` library to create a Tor circuit via the private Tor setup so as to communicate to the server. Further, some of the relays (guard, middle or exit) should be running directory services on them so as to advertise relay fingerprints and statistics, which the client may use when building circuits.

What you need to submit/grading rubric:

1. Screenshots showing the setting up of the relays(s) and the private Tor network, particularly showing the steps, and commands used, along with description of these commands and their options (20 points).
2. Screenshot showing where the client uses the `TorCtl/stem` library to establish a circuit via the relays and communicates to the server (20 points).
3. Screenshot / packet capture showing that the traffic from the client to the entry node and the exit to the server (10 points).

3 SQL Injection (total points: 40)

The second part of the exercise is related to SQL injection. For this you need to first install `docker` on your system. Thereafter, you need to install the `docker` image for a vulnerable application server, *i.e.* `juiceshop` (https://github.com/bkimminich/juice-shop). It would be listening on port 3000 on the localhost. If you access it via a browser (URL localhost:3000), you would see a webpage that looks like an e-commerce site.

You also need to install `burpsuite` (https://wiki.archlinux.org/title/Burp_suite). It works as a HTTP/HTTPS proxy on a certain port number. You need to configure your browser to use `burpsuite` as a proxy. It should show you all the web interactions between the client (*i.e* browser) and the web server (`juiceshop`'s docker image).

You need to use your knowledge of SQL injection to achieve the following:

1. Get admin access on the web portal (not same as `root` user access).
2. Get the credentials of all the users who are registered in the portal.

What you need to submit/grading rubric:

1. For acquiring admin access, describe the inputs you gave to the portal that led to getting admin access without password. Describe the logic used for the said inputs. Also show the screenshots of the same, that should show the input and the outcomes. (20 points)
2. Similarly, also describe the inputs you gave to the portal that led to revealing the user credentials for all users who are registered. Describe the logic used for the said inputs. Also show the screenshots of the same, that should show the input and the outcomes. (20 points)