COMP6224: An Introduction to Tor

In this lab, we will be exploring Tor. We will use the Tails environment which is preconfigured and set up with Tor and can be run inside a virtual machine. We will examine how Tor forms links and communicates with other nodes, compare how Tor traffic differs, browse and search the "dark web" and connect to different types of hidden services.

Getting Started

We will be using Tor through Tails, a Debian-based live environment pre-configured for Tor usage. It is easy to set up and run, with limited persistence and configuration and based around the idea of amnesia, leaving no trace behind after a session. While Tails can be booted from directly, we will be using it within a virtual environment for this lab.

1. Download the Tails ISO from https://tails.boum.org/install/download/openpgp/index.en.html
2. Run VirtualBox (or install it from https://www.virtualbox.org/wiki/Downloads if you are on your own machine)
3. Create a new Virtual Machine in VirtualBox: Other Linux (32-bit), with at least 2GB of RAM and load the Tails ISO image you downloaded into the optical drive
4. Start the virtual machine, and when Tails starts, choose to enter the options and ensure you specify an administrative password
5. You should now have a Tails environment ready to go

How does Tor work?

1. Open the Tor Browser and begin browsing the internet as you would do normally and observe what you notice when proxying through Tor
    a. While browsing the web with Tor, what do you notice compared to a normal browsing experience?
2. Visit the web browser fingerprinting services at https://panopticlick.eff.org/ at https://ip-check.info/ using a normal web browser on your computer and using the Tor Browser on your VM and note the differences.
    a. What differences do you note in the ability of websites to fingerprint your browser normally, compared to the Tor Browser? How does the Tor Browser protect you?
3. Now, install Wireshark onto Tails and start recording traffic by opening a terminal and running '**sudo apt-get update && sudo apt-get install wireshark && sudo wireshark**'. Using both the Unsafe Browser and the Tor Browser, compare accessing a site, such as www.southampton.ac.uk over HTTP, HTTPS and using Tor.
    a. What differences can you find between HTTP, HTTPS (using the Unsafe Browser) and using Tor (using the Tor browser) in the traffic. What identifiable information can you find?

Exploring Tor Web Services

We are now going to dive deeper into the Dark Web, beyond proxying to normal websites. **Please don't do anything illegal!**

1. Using the Tor Browser, starting at the Hidden Wiki, found at http://wikitjerrta4qgz4.onion/ explore some popular Tor sites.
2. Attempt to find any additional hidden service websites on Tor. Try out the search engine and directories and attempt to find other websites that aren't listed anywhere else.
    a. You may also want to visit the List of Tor Hidden Services on Wikipedia at https://en.wikipedia.org/wiki/List_of_Tor_hidden_services, or some of the Tor search engines, such as Torch at http://xmh57jrzrnw6insl.onion or Not Evil at http://hss3uro2hsxfogfq.onion
3. How can you find additional services on Tor? See if you can find any additional catalogues, search engines, directories and other techniques that you find which help you discover Tor websites

Alternative Services

Tor can also be used for other non-web based services. Some of these applications are already available in Tails, some are set up for usage over Tor already, and you can also use the Tor SOCKS server for other connections, such as SSH.

1. Explore the other programs available in Tails and investigate how they operate over the Tor network
2. Locate a hidden service of another type other than a website to connect to over Tor, for example an IRC server.
3. Experiment with the torsocks command on the commandline to connect to other types of services

Other Ways of Accessing Tor

1. In addition to Tails, there are other ways of accessing Tor
2. Have a play with using the Tor Browser Bundle, a special version of Firefox which connects through Tor, on a normal machine, outside of Tails.
    a. How does this differ to using Tails?
3. Explore the use of Tor Gateways, such as Tor2Web – just change a .onion url to a .onion.to URL and you can access it over the normal web
    a. How does this differ to going through Tor?
    b. How does the traffic differ when analysed through Wireshark?