Week 11 - Supplementary Materials

Markdown | PDF | MS Word DOCX | Libre ODT | HTML

Tor Browser

Tor Browser will allow us to proxy ordinary HTTP/HTTPS traffic through the Tor network to browse Websites. It is a heavily locked-down version of Mozilla Firefox.

Download Tor Browser

We will save the .xz file for the Tor Browser application to `~/Desktop/`:

- https://www.torproject.org/dist/torbrowser/12.0/tor-browser-linux64-12.0_ALL.tar.xz

We want to download the Linux version for Kali Linux but you can also try the Windows or Mac versions at home.

Checksum of the Tor Browser Installer

We can check the SHA256 hash value of the file we downloaded via the command:

```
sha256sum ~/Desktop/tor-browser-linux64-12.0_ALL.tar.xz
```

This hash is a checksum that can be used to verify the integrity of the file. For example, it can be compared against the checksum listed at the origin of the download (in this case, the https://torproject.org website).

However, we can go one step further by verifying the authorship (e.g. the authenticity) of the file and know with cryptographic certainty that we downloaded the exact file created by the Tor Project Developers. This can guard against attacks such as attacker-in-the-middle (AiTM or MiTM).

Tor Project Developer Signature

We will save this signature .asc file to `~/Desktop/`.

- `https://www.torproject.org/dist/torbrowser/12.0/tor-browser-linux64-12.0_ALL.tar.xz.asc](https://www.torproject.org/dist/torbrowser/12.0/tor-browser-linux64-12.0_ALL.tar.xz.asc)

We will verify this signature using the commands below. It's easiest to use the following commands if we navigate into the Desktop directory:

```
cd ~/Desktop
```

NOTE: In Windows and MacOS operating systems, you will need to follow instructions here to check the signature of the file you download and ignore the commands below:

- https://support.torproject.org/tbb/how-to-verify-signature/

Install the Tor Project Developer PGP/GPG Keyring

```
gpg --auto-key-locate nodefault,wkd --locate-keys torbrowser@torproject.org
```

Output the Tor Project Developer Key to File

```
gpg --output ./tor.keyring --export
0xEF6E286DDA85EA2A4BA7DE684E2C6E8793298290
```

Check the Signature for the Tor Browser Installer against the Tor Project Developer key

```
gpgv --keyring ./tor.keyring tor-browser-linux64-12.0_ALL.tar.xz.asc tor-browser-linux64-12.0_ALL.tar.xz
```

Websites on the "Dark Web"

The Tor network is often referred to as the "Dark Web". However, that term can be used to refer to any network that hosts data that is not available on the ordinary Internet experienced by most users, for example on an overlay network or "darknet".

Tor is able to to host hidden services ("onion services") via the special-use TLD `.onion`. To browse safe .onion sites, refer to this directory:

- Real World Onion Sites

These .onion URLs will only work in Tor Browser or another Tor-enabled browser (like Brave Tor Tabs.

IMPORTANT: The so-called "Dark Web" does contain content that is objectionable, illegal, or offensive. If you stray off the path of the Real World Onion Sites directory above, **we are not responsible**.

OnionShare

We can deploy a hidden service in Kali Linux by installing OnionShare.

Install OnionShare in Kali Linux:

```
sudo apt-get install onionshare
```

Now launch it either through the Kali top menu in the GUI or via the CLI:

```
onionshare
```

Persistent Hidden Services

In Kali Linux, follow these instructions for a persistent .onion address / hidden service.

- Tor Hidden Service in Ubuntu/Debian