Deakin University

Real World Practices for Cyber Security

OnTrack Submission

Task T9.3D

Submitted By:
Jack Perry
s217298346
2022/09/17 04:41

Tutor:
Jack Li

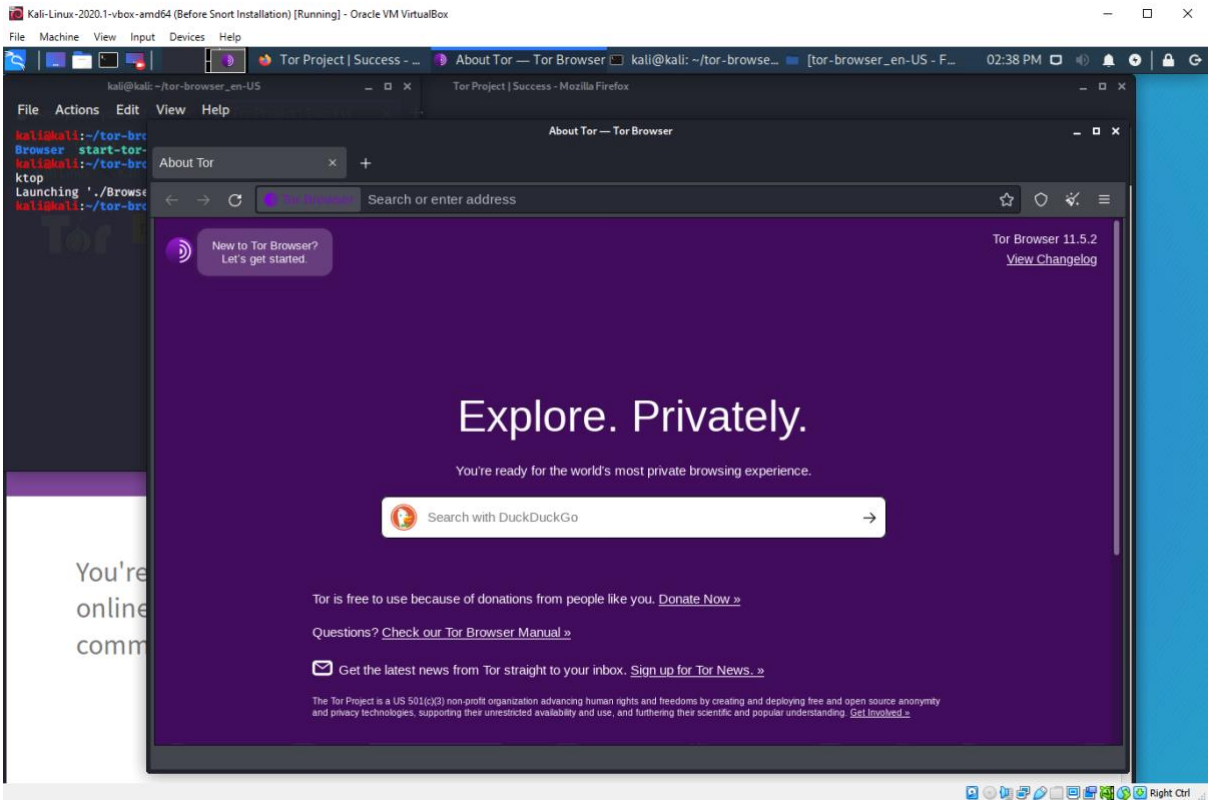
September 17, 2022

Cyber 9.3 D

1. **What is Tor? Why would someone want to use Tor?**
   Tor is an alternative web browser which uses the Tor network, filtering your web traffic through proxy servers and consequently protecting your online identity. Tor browsers are especially useful for maintaining anonymity online. An individual may use a tor browser to exercise free speech. As web traffic can be more simply monitored on the surface internet, many users may not feel comfortable using these services to voice unpopular opinions which may potentially face repercussions. Tor browsers can be used to voice opinions or communicate with like-minded people without fear of punishment by authoritarian figures. Alternatively, tor browsers could be used to carry out illegal activities which would otherwise be monitored on the surface web. Tor browsers have a history of facilitating illegal websites such as SilkRoad where users can act anonymously, without free of law enforcement.

2. **Install Tor Browser from https://www.torproject.org/ on Kali VM. An easy way of installing Tor is using APT package manager. For this, run sudo apt-get install torbrowser-launcher in the Terminal and follow the prompts.**

3. **Include a screenshot of Tor browser running successfully on your Kali VM. The screenshot should cover the browser window entirely.**



4. **What are ".onion" sites?**
   ".onion" sites are websites which are accessed through the use of a Tor network. The word "tor" stands for "the onion routing". Onion routing refers to path your web traffic takes when you operate a web browser. Instead of making a direct connection with the server you intend on accessing, the tor browser routes your web traffic through three proxy servers, encrypting the data at each stepping, intending to hide the identity of the person accessing

it. Onion sites refer to webpages which can only be accessed through onion routing, preventing the identity of any users who access the website to be revealed.

5. **Is HTTPS important for accessing websites via Tor? Is HTTPS important for accessing ".onion" sites?**
   Yes, HTTPS is still an important security measure when operating .onion sites or operating the Tor browser. Although onion routing aims to hide to the identity and location of the person accessing it, it doesn't explicitly protect the data which is being transmitted. When simply accessing a page which requires no user input, onion routing will accurately protect the user's identity. However, when accessing a webpage which requires user input such as log in credentials or other sensitive information, onion routing doesn't encrypt the information that you enter. While HTTPS is not necessary to enter .onion websites, it is encouraged as data packets can still be sniffed, consequently revealing data which you have entered. HTTPS provides an extra layer of protection useful for encrypting users data.

6. **What does Jacob Appelbaum mean by "privacy by design" in his TED talk video?**
   Privacy by design refers to the implementation of something which ensures privacy, as opposed to relying on a third party to ensure privacy. Privacy by policy relates to an assurance by a third party to uphold a privacy agreement. In this instance your privacy is reliant on both your trust and the party's willingness to uphold their claims. Privacy by design aims to eliminate this by ensuring privacy through design features. In the instance of Tor, users' data are not stored on a server possessed/owned by any individual, the design features of Tor ensure privacy which cannot be overcome.

7. **What is the difference between Tor and a VPN? Would you need to use both?**
   Tor browsers are used for complete anonymity. Both Tor browsers and VPNs encrypt your internet connection and route it through a number of servers before granting access to a site. However, Tor browsers are decentralized meaning they route traffic through servers which are public domain meaning they cannot be tracked/accessed by any company which might otherwise own them. Alternatively, VPN is a centralized service, meaning the servers are owned by private companies. This means there is a potential for data trafficked through a VPN to be exposed by the owner of the servers. While tor browsers accurately mask the identity of the user, they do not hide the web traffic as well as a VPN. Tor browsers make it difficult to find out who is committing actions but not so much what those actions are. VPN's do a better job of hiding a user's activities from anyone that might be interested such as Internet Service Providers (ISP's). Both a VPN and a Tor can be used at the same time, for added security measures. One benefit of using both a VPN and a Tor browser is to hide the fact that a Tor browser is being used. As there are many instances where a Tor is seen as either illegal or immoral (by either ISPs or government), using it in conjunction with a VPN can hide the fact that a user is using a Tor.

8. **When using Tor, does your Internet Service Provider (ISP) know you are using Tor?**
   Yes. A tor browser only encrypts its data after a connection with the browser has been made. This means an ISP would be able to see that a user has made a connection with a Tor browser but will not be able to identify any traffic after the connection with the browser has been established.

9. **Can Tor be blocked by network administrators? If so, would it be possible to bypass that blocking? (if answer is yes, list the approaches that could be used for this).**
   Tor can be blocked by network administrators; however, bridges can be used to bypass the block. Bridges can be described as alternative access points which are not listed in the public

Tor directory. Network administrators may block known access points to Tor browsers, however, cannot block all bridges as they are potential unknown and therefore unable to be blocked. Much like rogue access points, it is difficult to block access to something if you aren't aware it exists.

References:

1. Youtube.com. 2022. *What is the Tor project? How onion routing works*. [online] Available at: <https://www.youtube.com/watch?v=potUvSM4u3c> [Accessed 15 September 2022].
2. Bischoff, P., 2022. *Tor vs VPN: What's the difference and which is safer?*. [online] Comparitech. Available at: <https://www.comparitech.com/blog/vpn-privacy/tor-vs-vpn/> [Accessed 15 September 2022].
3. Anon, D., 2022. *What is the Tor Network and Browser and how can you use it safely?*. [online] Privacy.net. Available at: <https://privacy.net/what-is-tor/#:~:text=Tor%20is%20often%20blocked%20by,Pluggable%20Transports%20(see%20below).> [Accessed 15 September 2022].
4. Torproject.org. 2022. *The Tor Project | Privacy & Freedom Online*. [online] Available at: <https://www.torproject.org/> [Accessed 15 September 2022].
5.