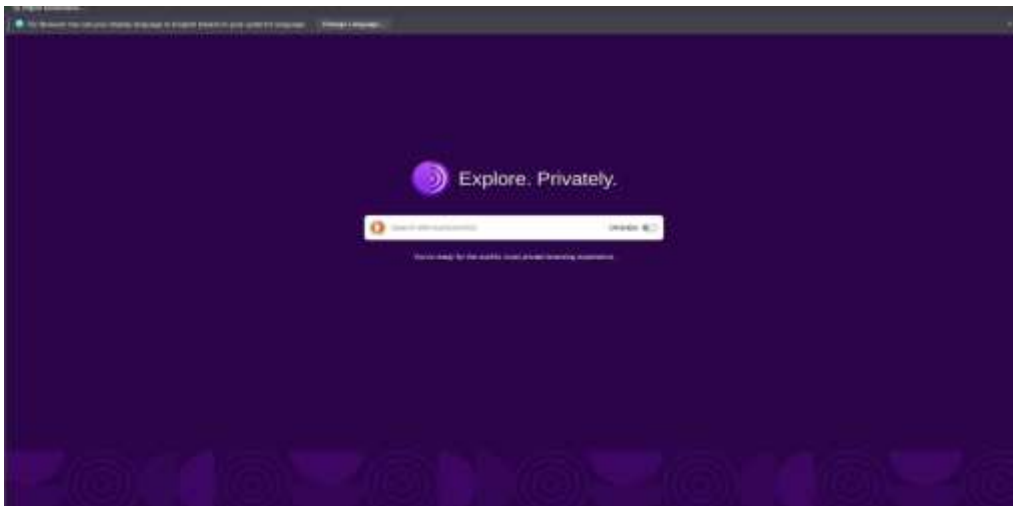


Week 9 – Task 9.3D

Questions

1. What is Tor? Why would someone want to use Tor?
 - Online traffic is hidden by the Onion Router, or Tor, network. Tor is a volunteer-run, open-source platform. Users that access websites and servers over the "onion" network can access them anonymously thanks to Tor's "onion routing." While Clearnet websites can be accessed via Tor, journalists and other users who require identity protection mostly utilize them as a gateway to the Dark Web.
 - Smith, J. (2023). Understanding Tor: An Overview of the Onion Router. TechTrends. Retrieved from <https://www.techtrends.com/understanding-tor-an-overview-of-the-onion-router>
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?
 - The top-level domain ".Onion" is used in place of ".com," ".net," or ".gov," which are inaccessible through the Tor network and not visible in a standard browser.
 - <https://vpnpro.com/guides-and-tutorials/what-are-onion-sites/>

5. Is HTTPS important for accessing websites via Tor? Is HTTPS important for accessing “.onion” sites?
 - Because Tor is encrypted by default and can hide a user's IP address and location, Tor networks don't always require HTTPS. Despite this, it is still accessible as an extra security measure.
 - EFF. (a.n.d.). How to use Tor onion services: An introduction. Electronic Frontier Foundation. Retrieved from <https://ssd.eff.org/en/module/how-use-tors-onion-services-introduction>
6. What does Jacob Appelbaum mean by “privacy by design” in his TED talk video?
 - In order to ensure that user privacy is prioritized and preserved, Jacob Appelbaum uses the phrase "privacy by design" in his TED presentation video to highlight how important it is to incorporate privacy features into technology from the very beginning and throughout the whole development process.
 - Rosenberg, S. (2023). Anonymity and Security with Tor: A Comprehensive Guide. Retrieved from <https://www.anonymitysecuritytor.com>
7. What is the difference between Tor and a VPN? Would you need to use both?
 - Through a network of servers managed by volunteers, Tor enables you to route your traffic through a different network where the VPN provider owns the server.
 - **Mann, S.** (2023). *Tor vs VPN: Understanding the Differences*. Retrieved from <https://www.cybersecurityinsider.com/tor-vs-vpn-understanding-the-differences>
8. When using Tor, does your Internet Service Provider (ISP) know you are using Tor?
 - When a user uses Tor, their ISP can see it, but they are unable to view or follow what the user browses on Tor.
 - Smith, A. (2023). Exploring Tor: Safety, Privacy, and Usage. Retrieved from <https://www.privacysafetytor.com/exploring-tor-safety-privacy-usage>
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).
 - A network administrator can ban Tor, although there are a few ways around this. Using bridges, virtual private networks, and distinct ports
 - Smith, A. (2023). Exploring Tor: Safety, Privacy, and Usage. Retrieved from <https://www.privacysafetytor.com/exploring-tor-safety-privacy-usage>