Tutorial No. 5

Title: Tutorial no 5 Report on Encrypted network TOR and Dark Web browsing

Roll No.: 16010420075 **Tutorial No.: 5**

Aim: Make a report on Encrypted network TOR and Dark Web browsing

\

Resources: virtual box, Tor Browser, Firefox

Theory

Tor (short for "The Onion Router") is an open-source browser that allows you to surf the web anonymously. With each session, it immediately clears your browsing history and encrypts all of your traffic.

It also gives you access to the dark web, which is comprised of unindexed and hidden websites on the internet. Some countries block Tor totally because of its capacity to allow unrestricted access to the internet.

The Tor network was created by the US Navy to allow military organizations to communicate anonymously online. The military abandoned the project in 2006, and it has now been taken over by a non-profit.

These days, the Tor Project is primarily concerned with the development of its browser and a few other privacy tools.

Tor strives to increase our online privacy and security up to a point. To mask our IP and safeguard our connection, the browser makes use of the Tor network's massive, global server network.

When we use Tor, your data is routed through many Tor servers (or "nodes"). At the different nodes, the traffic is extensively encrypted — and then painstakingly decrypted — one layer at a time.

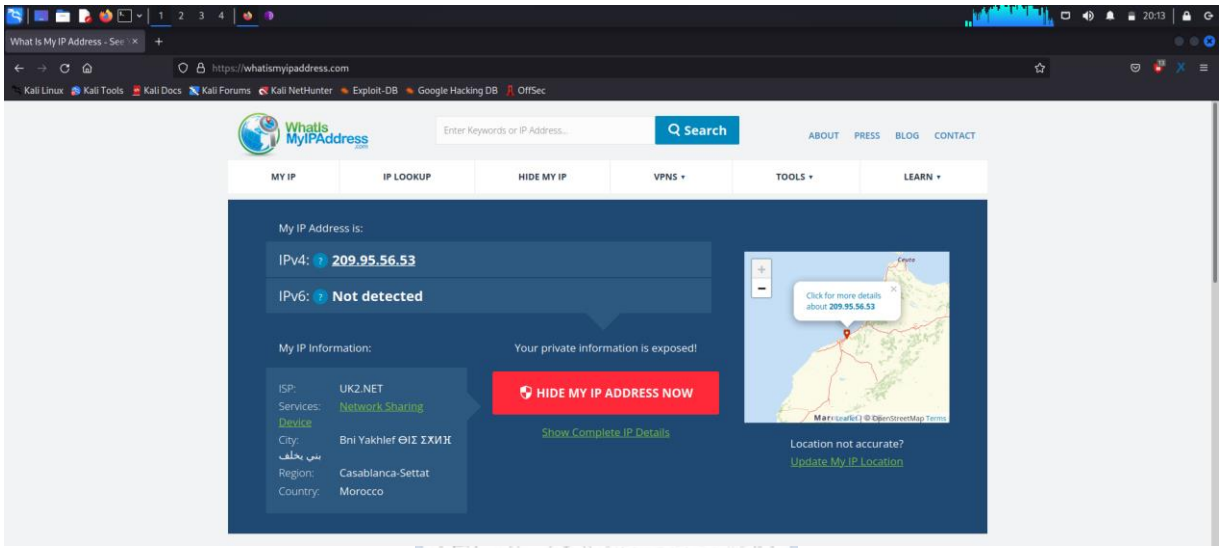
This implies that anyone attempting to identify us based on our online traffic will only come across the last server your data traffic travelled through (a.k.a. the 'Tor exit node,') making it extremely impossible to identify Tor users. The Tor browser is better than a regular web browser for accessing the web anonymously.

The only browser that allows us to access the black web is Tor. The dark web is made up of websites that aren't easily located using a search engine and can't be accessed using a standard web browser. To view a dark website, we also need to know the specific web URL.

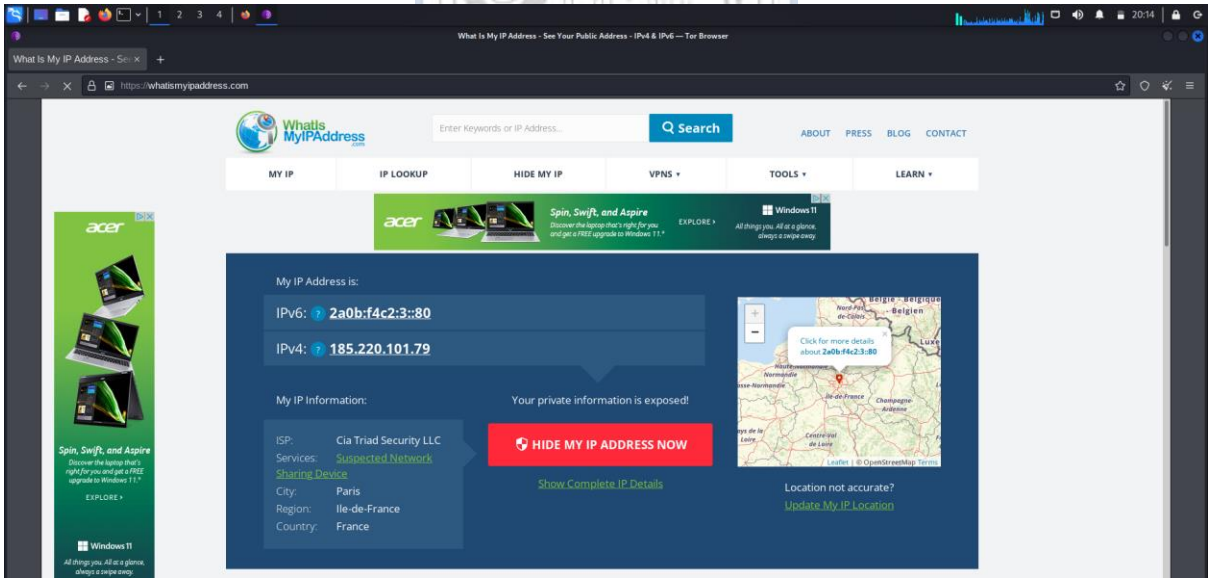
Unregulated websites make up the dark web, which means we can find anything there, from pirated movies to black marketplaces, illegal substances, and weaponry.

IMPLEMENTATION AND RESULTS:

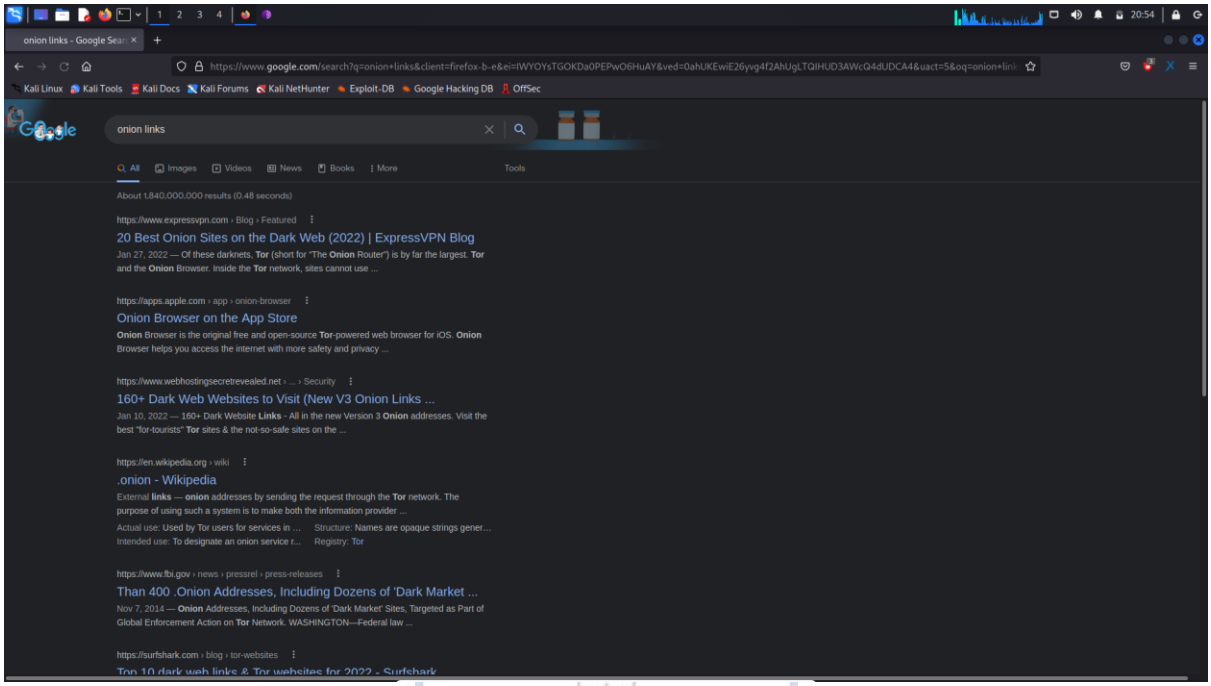
Initial IP address in another browser:



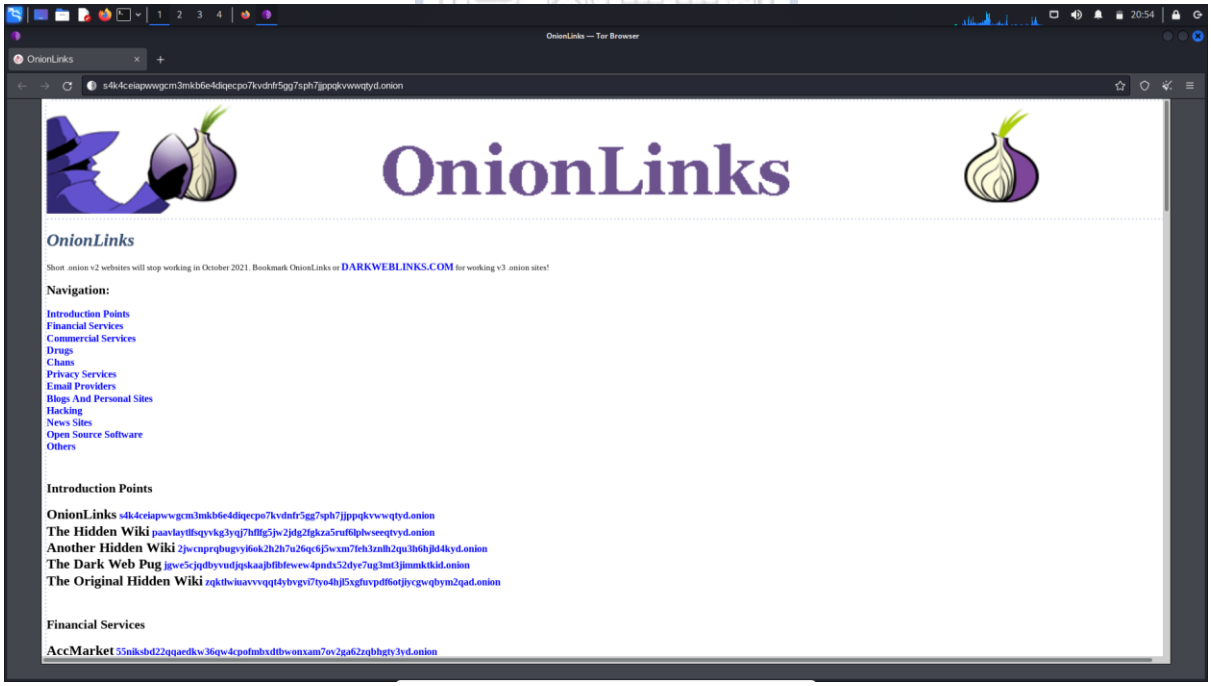
IP address in Tor Browser:



Searching for onion links in another browser:



Accessing onion links in Tor browser:



From the results above, we get that Tor browser has successfully encrypted our network so that we get access to the dark web websites including the onion links that we can travel through safely while maintaining anonymity. This action cannot be done on any other browser and it would risk us being exposed to dark web attackers.

Outcomes:

CO-1: Realize that premise of vulnerability analysis and penetration testing (VAPT).

Conclusion: (Conclusion to be based on the objectives and outcomes achieved)

Report on Tor browser was successfully made and its implications and concepts were understood.

Grade: AA / AB / BB / BC / CC / CD /DD

Signature of faculty in-charge with date

REFERENCES:

www.torproject.com