Lab – Ensuring Anonymity Using the CSI Linux Gateway

Overview

In this short lab, you will learn how to use the CSI Linux Gateway to provide an additional layer of anonymity while surfing the Internet. The CSI Linux Gateway sends all CSI Linux Analyst traffic through Tor to hide any source IP addresses. This keeps the anonymity of users and minimizes potential back tracing of the pentester, hacker, or investigator.

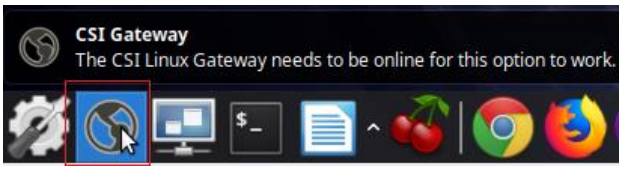
Start the lab

From your VirtualBox management console, launch CSI Linux Analyst.

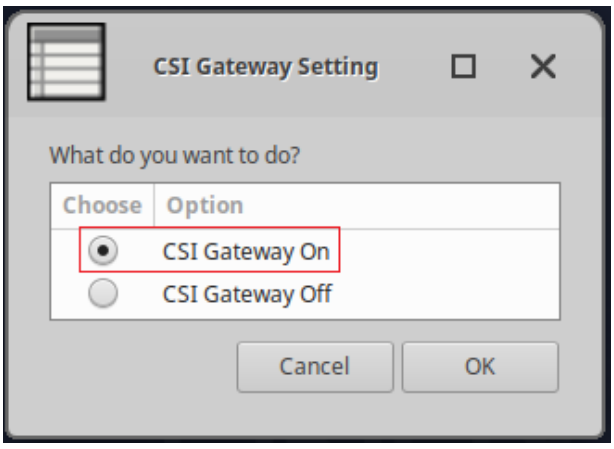
Once the CSI Analyst has finished booting, login to the desktop using the password of csi, all lower case.

Using the CIS Gateway for improved anonymity

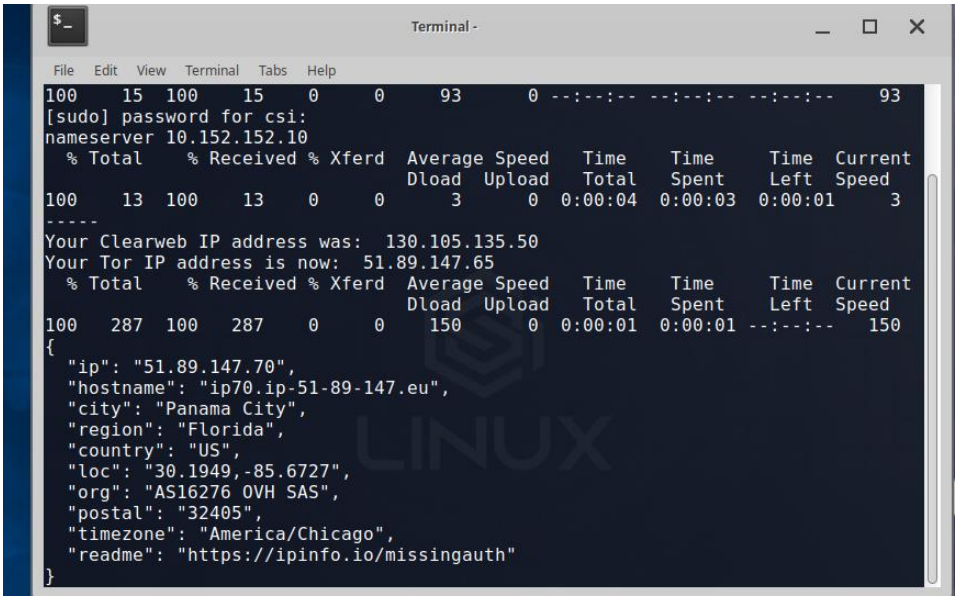
From the bottom taskbar of your CSI Linux desktop, click on the CSI Gateway icon.



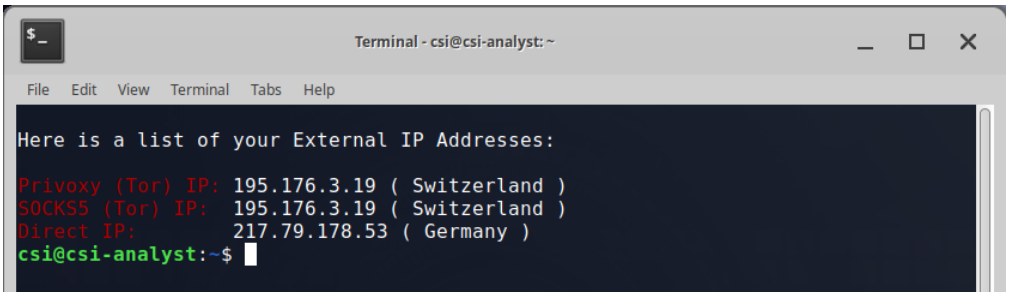
This launches a terminal with the GUI Gateway management control. Except the default to turn on CSI Gateway and click, OK.



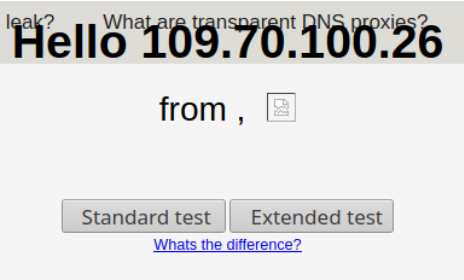
When prompted for the sudo password, type in csi all lower case.



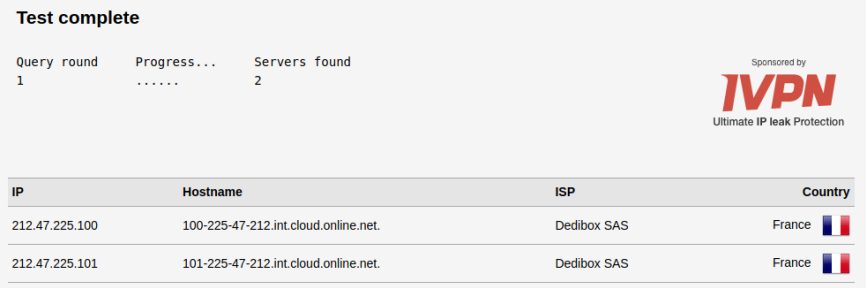
If we check our current adapter settings, you notice we have all new IP addresses and that my direct IP address shows me as being in Germany.



Notice my actual Gateway IP address has now been changed, hiding my exact location. We can confirm this is the case by once again running the DNS leak test at https://www.dnsleaktest.com/ using your Firefox browser inside of the CSI Linux Analyst desktop.



Notice by IP address has changed, showing somewhere where I am not. When I run the standard test, my new location shows me as being in France.



You can turn the Gateway off by just launching the CIS Linux Gateway and disconnecting from the Gateway.

Summary –

The technology and the means to hide in plain sight is the same idea behind the WHOIX gateway. The only difference is the way each Gateway is started and launched. With the additional layer of the CSI Linux Gateway comes slower response times and web pages can take longer to load. TOR has me in Germany; the Gateway has me France. As hard as it would be to find my actual IP address, I would never say it couldn't happen, but this is as difficult as we can make for someone to locate our real IP address. An interesting note; I did have to disable the VPN running on my Windows 10 host machine for this to work.

End of the lab!