

Lab – Ensuring Anonymity Using the CSI Linux Gateway

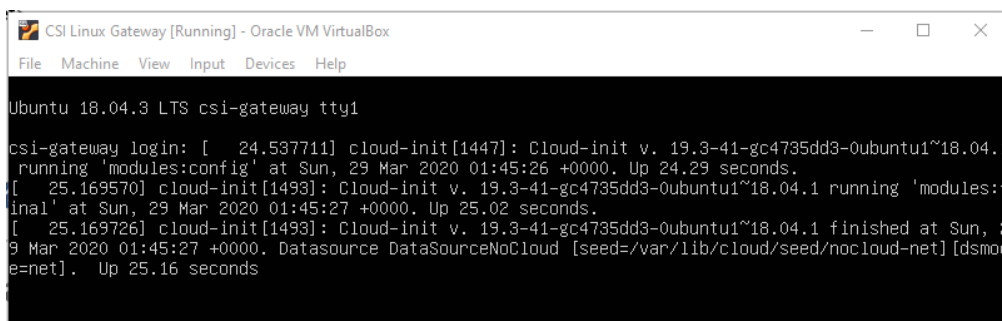
Overview

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 both the CSI Linux Gateway and the CSI Linux Analyst.

The CSI Linux Gateway is a non-GUI platform, and once it completes booting, you will see a CLI screen.



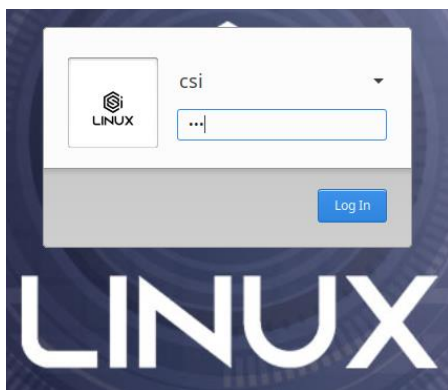
```
CSI Linux Gateway [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Ubuntu 18.04.3 LTS csi-gateway tty1

csi-gateway login: [ 24.537711] cloud-init[1447]: Cloud-init v. 19.3-41-gc4735dd3-0ubuntu1~18.04.1
running 'modules:config' at Sun, 29 Mar 2020 01:45:26 +0000. Up 24.29 seconds.
[ 25.169570] cloud-init[1493]: Cloud-init v. 19.3-41-gc4735dd3-0ubuntu1~18.04.1 running 'modules:f
inal' at Sun, 29 Mar 2020 01:45:27 +0000. Up 25.02 seconds.
[ 25.169726] cloud-init[1493]: Cloud-init v. 19.3-41-gc4735dd3-0ubuntu1~18.04.1 finished at Sun, 2
9 Mar 2020 01:45:27 +0000. Datasource DataSourceNoCloud [seed=/var/lib/cloud/seed/nocloud-net] [dsmod
e=net]. Up 25.16 seconds
```

Minimize the Gateway and leave it running.

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



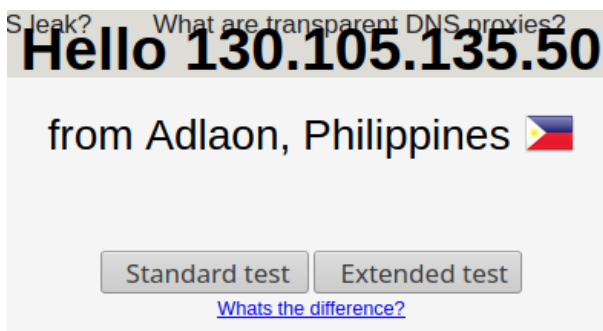
Check the configuration of your network adapters

From the far right of the taskbar, click on the icon that has a question mark over a wireless network icon.








Note that even though we are using the TOR service and the onion network, my real IP address showing my actual location is exposed. In the past, the TOR network has been compromised by law enforcement who were able to find the real IP address of the machine leading them to the individual's location.

Open your Firefox browser is open, browse on over to <https://www.dnsleaktest.com/> Perform the standard test. Notice my actual IP address is exposed.



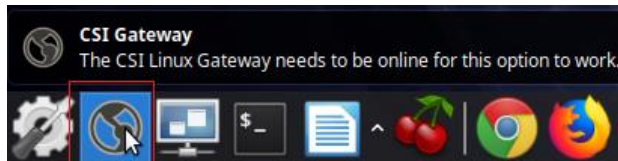
Results of the standard test.

I'm being routed through the U.S and Singapore. You can perform the extended test, and you will see you are being routed through a vast number of servers courtesy of the Onion network. Still, if the TOR service becomes compromised, my actual location could be discovered.

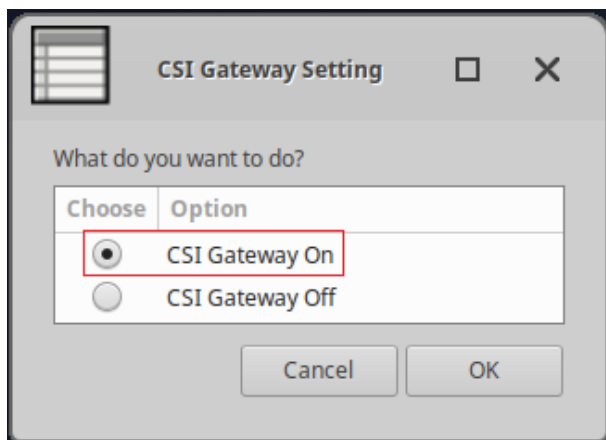
IP	Hostname	ISP	Country
172.253.211.14	None	Google	United States 
172.253.211.73	None	Google	United States 
172.253.211.76	None	Google	United States 
74.125.190.11	None	Google	Singapore, Singapore 
74.125.190.15	None	Google	Singapore, Singapore 

Using the CIS Gateway for improved anonymity

From the bottom taskbar of your CSI Analyst 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.

```

$ _
File Edit View Terminal Tabs Help
100 15 100 15 0 0 93 0 -:-:-:- -:-:-:- -:-:-:- 93
[sudo] password for csi:
nameserver 10.152.152.10
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 13 100 13 0 0 3 0 0:00:04 0:00:03 0:00:01 3
-----
Your Clearweb IP address was: 130.105.135.50
Your Tor IP address is now: 51.89.147.65
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 287 100 287 0 0 150 0 0:00:01 0:00:01 -:-:-:- 150
{
  "ip": "51.89.147.70",
  "hostname": "ip70.ip-51-89-147.eu",
  "city": "Panama City",
  "region": "Florida",
  "country": "US",
  "loc": "30.1949,-85.6727",
  "org": "AS16276 OVH SAS",
  "postal": "32405",
  "timezone": "America/Chicago",
  "readme": "https://ipinfo.io/missingauth"
}

```

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.

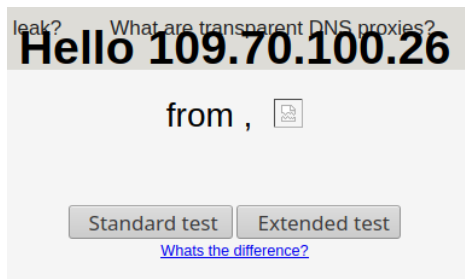
```

Terminal - csi@csi-analyst: ~
File Edit View Terminal Tabs Help

Here is a list of your External IP Addresses:
Privoxy (Tor) IP: 195.176.3.19 ( Switzerland )
SOCKS5 (Tor) IP: 195.176.3.19 ( Switzerland )
Direct IP: 217.79.178.53 ( Germany )
csi@csi-analyst:~$

```

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.

Test complete

Query round	Progress...	Servers found
1	2

Sponsored by
IVPN
Ultimate IP leak Protection

IP	Hostname	ISP	Country
212.47.225.100	100-225-47-212.int.cloud.online.net.	Dedibox SAS	France 
212.47.225.101	101-225-47-212.int.cloud.online.net.	Dedibox SAS	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!