

Lab – Preparing CSI Investigator to Use Shodan

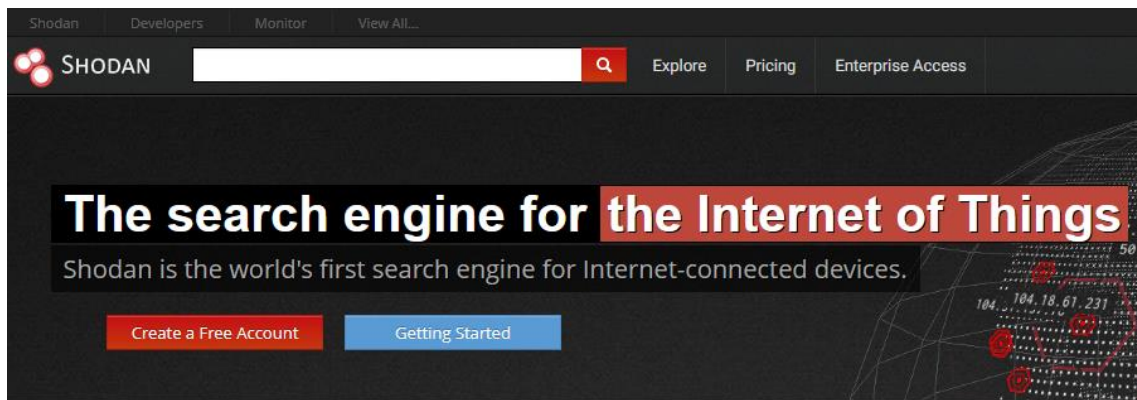
Disclaimer: Please use this lab responsibly. Attempting to access any system you do not own or have permission to access is illegal. This lab is meant to be used for educational and research purposes only.

Overview

Shodan is a search engine that lets the user find specific types of devices (webcams, routers, servers, etc.) connected to the Internet using a variety of search filters.

Unlike traditional search engines such as Google, which help you find websites, Shodan enables you to find information about desktops, servers, IoT devices, and more by grabbing service banners, which are metadata that the server sends back to the client.

Typical uses of Shodan include network security, market research, cyber risk, scanning IoT devices, and tracking ransomware. Shodan was created by John C. Matherly in 2009.



<https://www.shodan.io/>

Lab Requirements

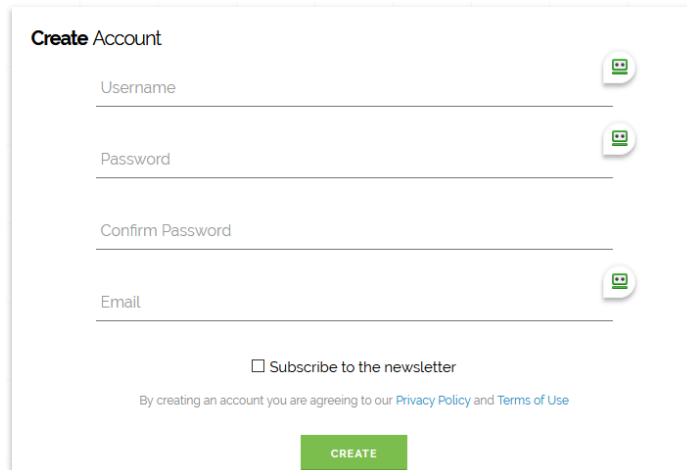
1. One virtual install of CSI Linux Analyst (preferred)
2. One virtual install of CSI Linux Gateway (preferred)
3. One virtual install of Kali Linux running behind a VPN
4. Optional – Windows 10, Linux, MAC, or Apple machine running behind a VPN.
5. Internet Access

Caveat

Regardless if you're using Shodan for a forensics investigation or as a pentester looking for vulnerable devices on the web, best practices would be to ensure you use a virtual machine running behind a secured gateway or VPN so as not to expose your real IP address and location. You've been warned!

Create a free user account at <https://www.shodan.io/> Use the Create a Free Account button provided. Without a free account, most of the search filters will be disabled. To get access to all the search filters, register your account using an EDU address.

Use an email address you have access to as you will need to verify your account information. Use an EDU address, if at all possible, for a free full server account upgrade.

A screenshot of the 'Create Account' form on the Shodan website. The form is titled 'Create Account' in bold. It contains four input fields: 'Username', 'Password', 'Confirm Password', and 'Email'. Each field has a small icon to its right. Below the fields is a checkbox labeled 'Subscribe to the newsletter'. At the bottom, there is a line of text: 'By creating an account you are agreeing to our [Privacy Policy](#) and [Terms of Use](#)'. Below this is a green button labeled 'CREATE'.

Does Shodan offer student/ professor/ university discounts?

Yes, Shodan will provide free upgrades to students, professors, or IT staff at universities. If you create a Shodan account with your academic email address, you will automatically receive the free upgrade to a full paid account. If you don't receive the upgrade, please email academic@shodan.io from the same EDU email address you used to sign-up. Using a default free account is fine for this lab.

Benefits of registering with an EDU email address:

- All add-ons (HTTPS, Telnet, view up to 10,000 search results)
- 100 Export Credits
- Improved API plan (access to up to 20 million results/ month)
- Shodan Maps (<https://maps.shodan.io>)
- Shodan Images (<https://images.shodan.io>)
- Free access to the Complete Guide to Shodan book

Once I registered with an EDU email address, I used the academic@shodan.io support link, and had my free account upgraded to a full account at no charge.

Hi,

We've applied the free upgrade to your Shodan account, which is linked to your academic email. A separate welcome email has been sent with several links to get started (including a copy of the official Shodan book).

The free academic account includes:

- *Download up to 10,000 results per month*
- *Scan up to 100 IPs per month*

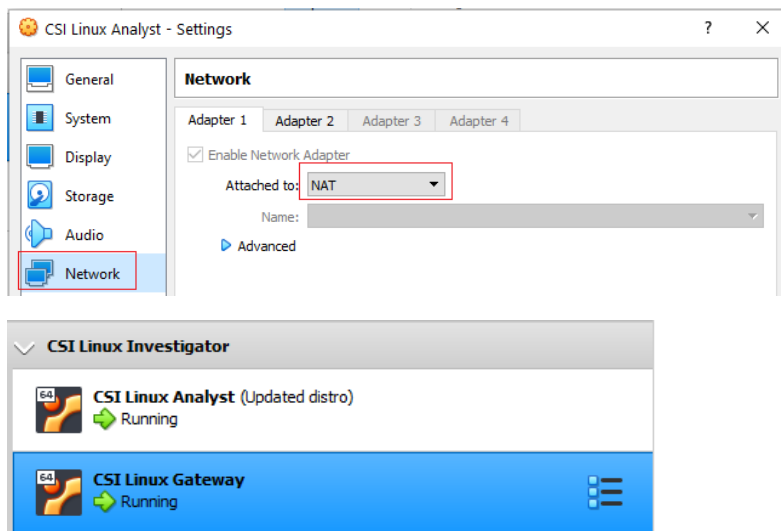
- Network monitoring for 16 IPs
- The ability to use the “vuln” search filter on the website

Sincerely,

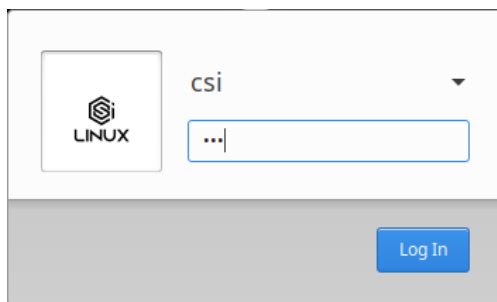
Configuring the lab

For this lab, we will be using a virtual install of CSI Investigator Analyst working behind the CSI Gateway. Students are also free to use Kali Linux, Windows 10, or a MAC working behind a VPN.

1. From within VirtualBox, launch the CSI Linux Analyst and then the CSI Gateway. **Make sure both network adapters for both virtual machines are set to NAT networking.**



2. Log onto the CSI Analyst using the password, **csi** all lower case.



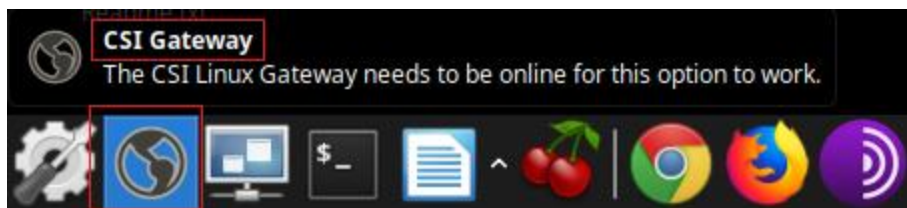
3. Minimize your virtual machine of running the CSI Gateway. No need to log on.

```

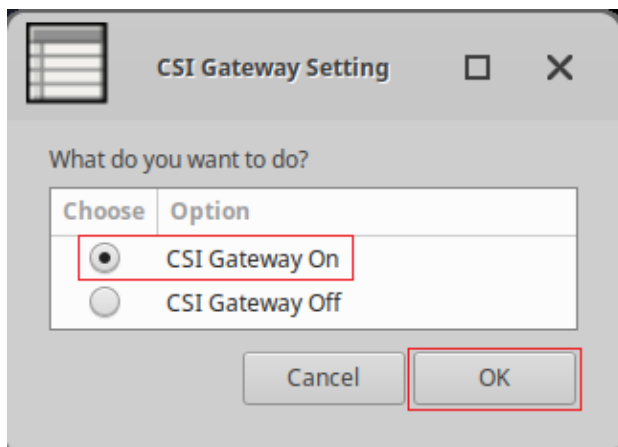
Ubuntu 18.04.3 LTS csi-gateway tty1
csi-gateway login: _

```

4. Once you have a CSI Analyst desktop, from the lower left toolbar of the screen, find the icon for your CSI Gateway, and launch.



5. Once you launch the CSI Gateway, you need to choose the option to turn the 'CSI Gateway On.'



Once launched, you will be asked for your CSI Analyst password within the terminal. **You will not see the password as it is being typed in the terminal.** Type **csi** using all lower-case letters at the terminal, read what is being echoed onto the terminal screen.

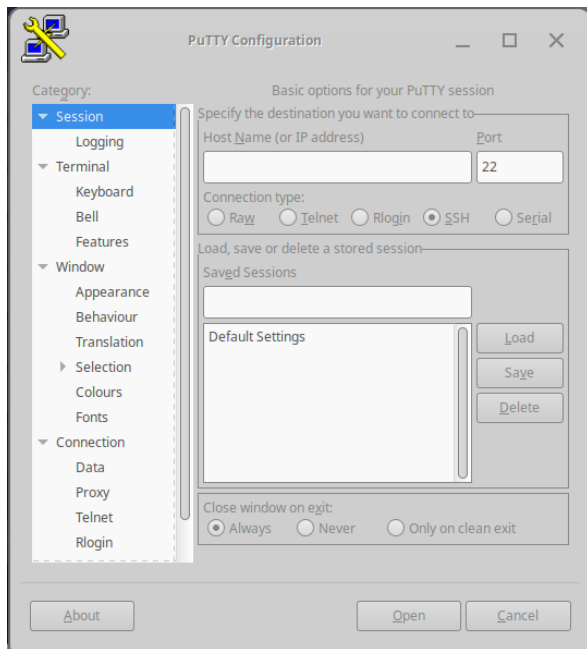
Since you will be using Putty in this lab, quickly install the free program using the following command from your CSI Analyst terminal.

```
sudo apt-get install -y putty
```

```
csi@csi-analyst:~$ sudo apt-get install -y putty
[sudo] password for csi:
Reading package lists... Done
Building dependency tree
Reading state information... Done
```

When you're ready to launch PuTTY, you can do by just typing **putty** at the terminal prompt.

```
csi@csi-analyst:~$ putty
```



Summary –

In this first lab, we configured our CSI Linux Analyst and CSI Getaway in preparation for using the Shodan search engine. In our next lab, we will see how we can use the Shodan search engine to help find devices connected to the Internet that are vulnerable and why they are vulnerable.