



eLearnSecurity
Forging security professionals

HERA LAB

User Manual



1. TABLE OF CONTENTS

1. Windows users.....	4
1.1. Download OpenVPN Client.....	4
1.2. Create user and password.....	4
1.3. Start the OpenVPN GUI.....	5
1.4. Start the lab.....	5
1.5. Download configuration file.....	6
1.6. Connect.....	6
1.7. Test the tunnel.....	8
1.8. Enjoy the Lab.....	8
1.9. Stop the LAB	8
2. Linux users.....	10
2.1. Download OpenVPN Client	10
2.2. Create user and password.....	10
2.3. Start the lab.....	11
2.4. Download configuration file.....	11
2.5. Connect.....	12
2.6. Test the tunnel.....	13
2.7. Enjoy the Lab.....	14
2.8. Stop the LAB	14
3. Mac Users.....	15
3.1. Download OpenVPN Client	15
3.2. Create Resolver File	16
3.3. Start the OpenVPN GUI.....	16
3.4. Start the lab.....	16
3.5. Download configuration file.....	17
3.6. Connect.....	17
3.7. Test the tunnel.....	19



3.8. Enjoy the Lab.....	19
3.9. Stop the LAB	19
4. Firewall Configuration	21
5. Lab information	21
5.1. How long is the lab running for?.....	21
5.2. How can I verify how much time I have left in my account?	22
5.3. How is my total time calculated with On-demand model?.....	22
5.4. Lab Expiration and Automatic Stop.....	23



1. WINDOWS USERS

1.1. DOWNLOAD OPENVPN CLIENT

Before starting your Lab, download and install OpenVPN Client from here:

<https://openvpn.net/index.php/open-source/downloads.html>

Run the installer with the default options. Make sure the following components are selected:

TAP Virtual Ethernet Adapter
Add OpenVPN to PATH

1.2. CREATE USER AND PASSWORD

In order to connect through the VPN, you first need to create a Username and a Password. To do that open the “Lab VPN Credentials” menu item in the upper-right corner of the site.

Home / Virtual Labs / Lab VPN credentials

VPN Credentials

Before accessing virtual labs, you must create a username and password to connect to the VPN tunnels.

Username

Password

Repeat Password

Note: Username and password work for all your VPN tunnels. The new credentials **apply from the next tunnel creation.**



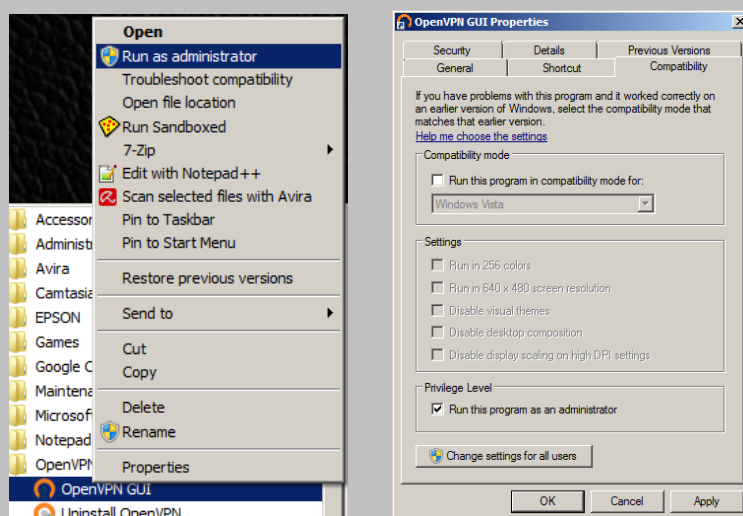
1.3.START THE OPENVPN GUI

From the start menu, launch **OpenVPN GUI**. Once the application starts, you will see an icon with a display and a lock in the system tray. That is the OpenVPN GUI icon.



IMPORTANT



*On some systems the VPN connection might not work due to insufficient privileges. Therefore, it might be necessary to start OpenVPN GUI as Administrator:
Right click on **OpenVPN GUI** icon, then click on **Run as Administrator***



1.4.START THE LAB



You can start the Lab by clicking the 'Start' button.



Labs catalog						
Lab	Manual	Actions	Status	Runtime	VPN File	Completed
HTTP(S) Traffic Sniffing			Off	00:00:00	--	<input type="checkbox"/>
Find the Secret Server			Off	00:00:00	--	<input type="checkbox"/>

Note: The lab could take up to a few minutes to start.

Once the lab is deployed, the VPN tunnel file will become visible.

Labs catalog						
Lab	Manual	Actions	Status	Runtime	VPN File	Completed
HTTP(S) Traffic Sniffing			Running	00:00:07		<input type="checkbox"/>

1.5.DOWNLOAD CONFIGURATION FILE

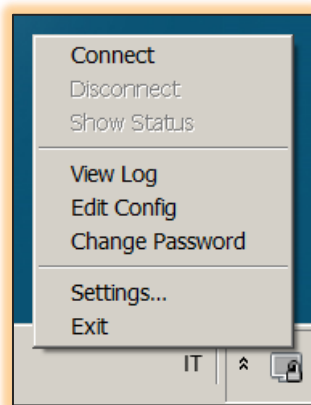
After you start a lab, you will need to click the key icon to download a VPN file to connect to the lab network. Save the OpenVPN file to the following folder:

C:\Program Files\OpenVPN\config

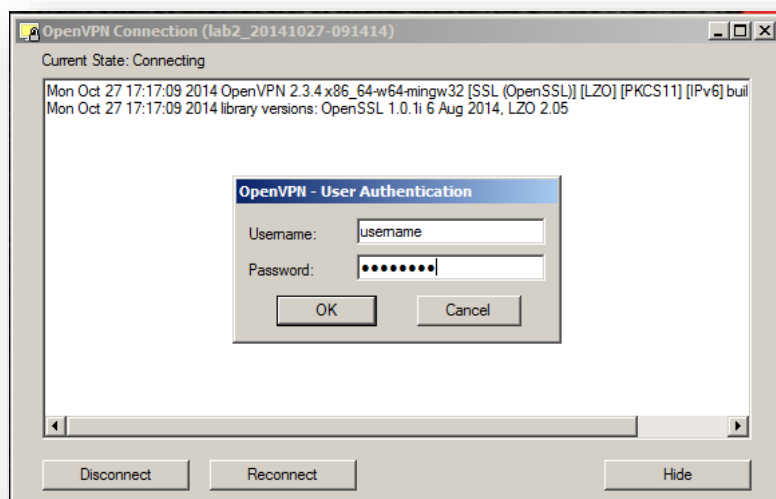
1.6.CONNECT

Once a lab scenario is started and you have downloaded the configuration file, it's time to connect to the VPN tunnel. From the System Tray you should see the list of tunnels downloaded and for each of them connect to the respective tunnel by clicking on the **Connect** option:

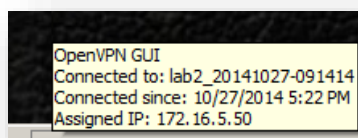




If the connection is successful, you will be notified that the connection was established. At this point you will need to authenticate to the VPN server using the credentials you set during the first use wizard (you can configure them again in the VPN credentials menu item in your Members area):

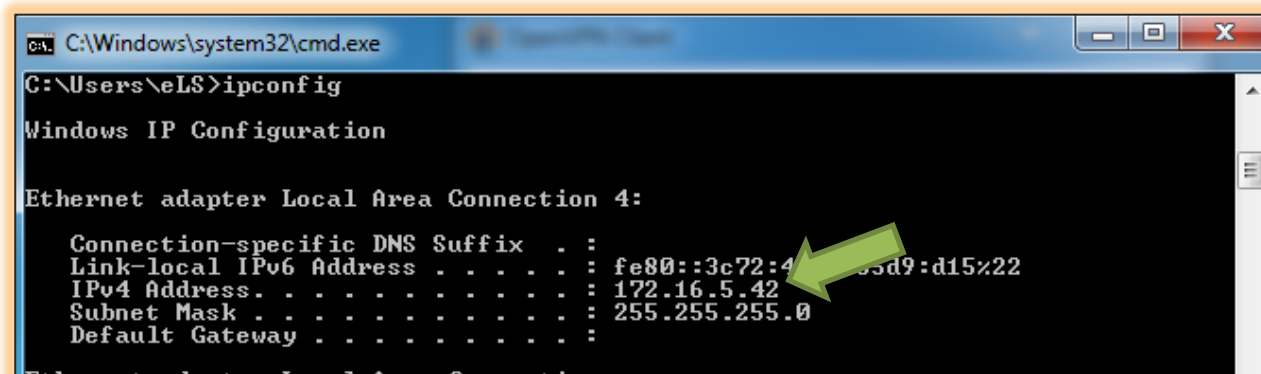


If authentication is successful, you will see this message in the System Tray:



1.7. TEST THE TUNNEL

If the tunnel works, you should have a new network interface with the same IP address displayed in the OpenVPN client.



```
C:\Windows\system32\cmd.exe
C:\Users\eLS>ipconfig



Windows IP Configuration

Ethernet adapter Local Area Connection 4:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::3c72:4...:d15:22
    IPv4 Address. . . . . : 172.16.5.42
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :
```

1.8. ENJOY THE LAB





Each Lab comes with a manual that explains the scenario, the goals and a list of tasks that will guide you through the steps necessary to reach the goals. At the end of the manual you will find detailed Solutions for the lab. You can download the Lab Manual by clicking on the PDF icon:

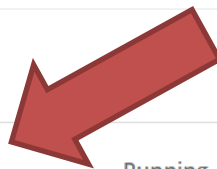
Lab	Manual	Actions	Status	Runtime	VPN File	Completed
HTTP(S) Traffic Sniffing		Start	Off	00:00:00	--	<input type="checkbox"/>
Find the Secret Server		Start	Off	00:00:00	--	<input type="checkbox"/>

1.9. STOP THE LAB

Once you have finished to use the Lab, remember to **stop it by clicking on the 'Stop' button** in the Members area.



Labs catalog						
Lab	Manual	Actions	Runtime	VPN File	Completed	
 HTTP(S) Traffic Sniffing			Running	00:00:07		<input type="checkbox"/>



Please consider that if you are using the On-Demand plan, you should stop the Lab as soon as you are done with your exercises.

This ensures that no account time is wasted.



2. LINUX USERS

2.1. DOWNLOAD OPENVPN CLIENT

Before starting your Lab, download and install OpenVPN Client from here:

<https://openvpn.net/index.php/open-source/downloads.html>

Once the client is installed, reboot your system (you actually have to reboot to avoid later issues).

2.2. CREATE USER AND PASSWORD

In order to connect through the VPN, you first need to create a Username and a Password. To do that open the “Lab VPN Credentials” menu item in the upper-right corner of the site.

Home / Virtual Labs / Lab VPN credentials

VPN Credentials

Before accessing virtual labs, you must create a username and password to connect to the VPN tunnels.

Username

Password

Repeat Password







Note: Username and password works for all your VPN tunnels.

The new credentials apply from the next tunnel creation.







2.3. START THE LAB

You can start the Lab by clicking the 'Start' button.

Labs catalog						
Lab	Manual	Actions	Status	Runtime	VPN File	Completed
 HTTP(S) Traffic Sniffing			Off	00:00:00	--	<input type="checkbox"/>
 Find the Secret Server			Off	00:00:00	--	<input type="checkbox"/>

Note: The lab could take few minutes to start.

Once the lab is deployed, the VPN file icon will become visible:

Labs catalog						
Lab	Manual	Actions	Status	Runtime	VPN File	Completed
 HTTP(S) Traffic Sniffing			Running	00:00:07		<input type="checkbox"/>

2.4. DOWNLOAD CONFIGURATION FILE

After you start a lab, you will need to click the key icon to download a VPN file to connect to the lab network. Save the OpenVPN file to your local machine.



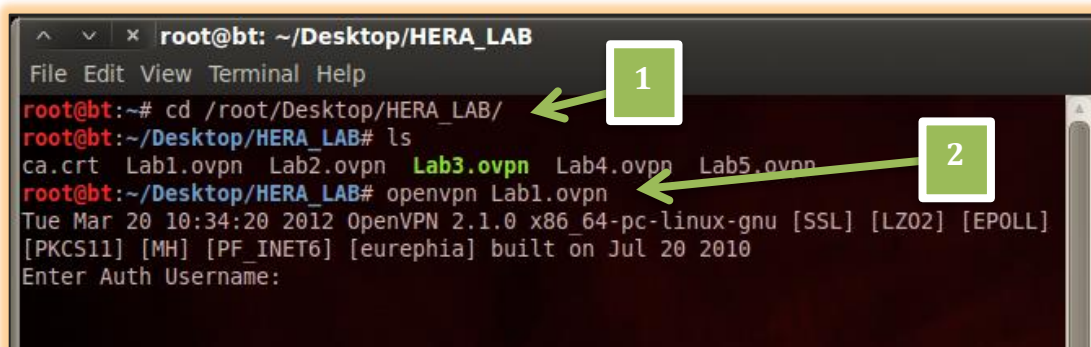
2.5. CONNECT

Once the lab is ready, run a new terminal,

1) move into the folder where the configuration file resides, then

2) run the following command:

```
>> openvpn lab_configuration_file.ovpn
```

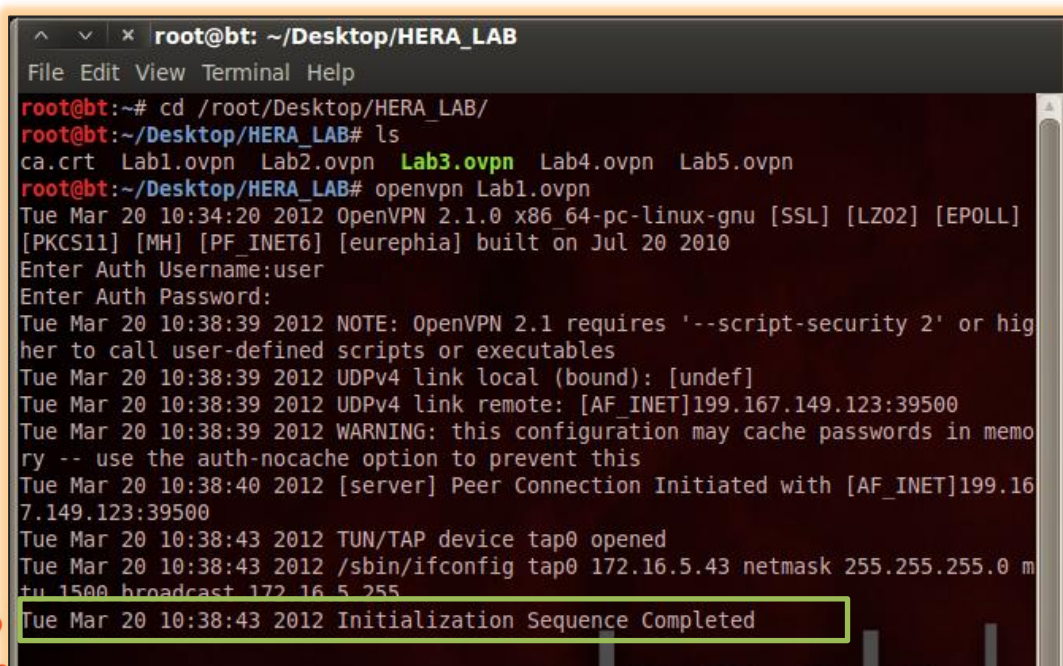


```
root@bt: ~/Desktop/HERA_LAB
File Edit View Terminal Help
root@bt:~# cd /root/Desktop/HERA_LAB/
root@bt:~/Desktop/HERA_LAB# ls
ca.crt Lab1.ovpn Lab2.ovpn Lab3.ovpn Lab4.ovpn Lab5.ovpn
root@bt:~/Desktop/HERA_LAB# openvpn Lab1.ovpn
Tue Mar 20 10:34:20 2012 OpenVPN 2.1.0 x86_64-pc-linux-gnu [SSL] [LZ02] [EPOLL]
[PKCS11] [MH] [PF_INET6] [eurephia] built on Jul 20 2010
Enter Auth Username:
```

If you are not using the root user, you should run the openvpn using sudo with the following command:

```
sudo openvpn lab_configuration_file.ovpn
```

If the connection works, you have to insert your credentials (see step b.) and then confirm. Once the connection is established, you should see something like this:



```
root@bt: ~/Desktop/HERA_LAB
File Edit View Terminal Help
root@bt:~# cd /root/Desktop/HERA_LAB/
root@bt:~/Desktop/HERA_LAB# ls
ca.crt Lab1.ovpn Lab2.ovpn Lab3.ovpn Lab4.ovpn Lab5.ovpn
root@bt:~/Desktop/HERA_LAB# openvpn Lab1.ovpn
Tue Mar 20 10:34:20 2012 OpenVPN 2.1.0 x86_64-pc-linux-gnu [SSL] [LZ02] [EPOLL]
[PKCS11] [MH] [PF_INET6] [eurephia] built on Jul 20 2010
Enter Auth Username:user
Enter Auth Password:
Tue Mar 20 10:38:39 2012 NOTE: OpenVPN 2.1 requires '--script-security 2' or hig
her to call user-defined scripts or executables
Tue Mar 20 10:38:39 2012 UDPv4 link local (bound): [undef]
Tue Mar 20 10:38:39 2012 UDPv4 link remote: [AF_INET]199.167.149.123:39500
Tue Mar 20 10:38:39 2012 WARNING: this configuration may cache passwords in memo
ry -- use the auth-nocache option to prevent this
Tue Mar 20 10:38:40 2012 [server] Peer Connection Initiated with [AF_INET]199.16
7.149.123:39500
Tue Mar 20 10:38:43 2012 TUN/TAP device tap0 opened
Tue Mar 20 10:38:43 2012 /sbin/ifconfig tap0 172.16.5.43 netmask 255.255.255.0 m
tu 1500 broadcast 172.16.5.255
Tue Mar 20 10:38:43 2012 Initialization Sequence Completed
```

2.6. TEST THE TUNNEL

You can test the tunnel by running ifconfig:

```
tap0      Link encap:Ethernet  HWaddr 22:52:04:17:da:e0
          inet addr:172.16.5.43  Bcast:172.16.5.255  Mask:255.255.255.0
          inet6 addr: fe80::2052:4ff:fe17:dae0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:0 (0.0 B)  TX bytes:468 (468.0 B)





root@bt:~#
```

If you see a new network interface (tap0), the tunnel works fine.







2.7. ENJOY THE LAB

Each Lab comes with a manual that explains the scenario, the goals and a list of tasks that will guide you through the steps necessary to reach the goals. At the end of the manual you will find detailed Solutions for the lab. You can download the Lab Manual by clicking on the PDF icon:

Lab	Manual	Actions	Status	Runtime	VPN File	Completed
 HTTP(S) Traffic Sniffing		Start	Off	00:00:00	--	<input type="checkbox"/>
 Find the Secret Server		Start	Off	00:00:00	--	<input type="checkbox"/>

2.8. STOP THE LAB

Once you have finished to use the Lab, remember to **stop it by clicking on the 'Stop' button** in the Members area.

Labs catalog						
Lab	Manual	Actions		Runtime	VPN File	Completed
 HTTP(S) Traffic Sniffing		<div>Stop</div>		Running	00:00:07	 <input type="checkbox"/>

Please consider that if you are using the On-Demand plan, you should stop the Lab as soon as you are done with your exercises.

This ensures that no account time is wasted.



3. MAC USERS

3.1. DOWNLOAD OPENVPN CLIENT

Before starting your Lab, download and install an OpenVPN Client for MacOSX such as Tunnelblick: <https://tunnelblick.net/downloads.html>

- Run the installer with the default options.
- Create user and password

In order to connect through the VPN, you first need to create a Username and a Password. To do that open the “Lab VPN Credentials” menu item in the upper-right corner of the site.

Home / Virtual Labs / Lab VPN credentials

VPN Credentials

Before accessing virtual labs, you must create a username and password to connect to the VPN tunnels.

Username

Password

Repeat Password

Save Credentials

Note: Username and password work for all your VPN tunnels. The new credentials **apply from the next tunnel creation.**



3.2. CREATE RESOLVER FILE

Note: This step is only necessary for connecting to Hera Labs in the following two courses:

- **Web Application Penetration Testing**
- **Web Application Penetration Testing Extreme**

Create the directory `/etc/resolver` if it does not exist with the command:

```
sudo mkdir /etc/resolver
```

Then create the resolver file for the domain you need to resolve, containing the row:

```
nameserver 10.100.13.37
```

Example: you can create it with the command (for the `xss.labs` domain):

```
echo nameserver 10.100.13.37 | sudo tee /etc/resolver/xss.labs
```

Note: Both commands will require your password to gain supervisor privileges



3.3. START THE OPENVPN GUI

From the Applications folder, launch **Tunnelblick**. Once Tunnelblick has been launched, you control it from the Tunnelblick icon in the Status Bar at the top of your screen. The Tunnelblick icon is usually placed between the time and the Spotlight icon. When no VPN connection is active, the icon is dim.

3.4. START THE LAB



You can start the Lab by clicking the 'Start' button.



Labs catalog						
Lab	Manual	Actions	Status	Runtime	VPN File	Completed
HTTP(S) Traffic Sniffing			Off	00:00:00	--	<input type="checkbox"/>
Find the Secret Server			Off	00:00:00	--	<input type="checkbox"/>

Note: The lab could take up to a few minutes to start.

Once the lab is deployed, the VPN file icon will become visible.

Labs catalog						
Lab	Manual	Actions	Status	Runtime	VPN File	Completed
HTTP(S) Traffic Sniffing			Running	00:00:07		<input type="checkbox"/>

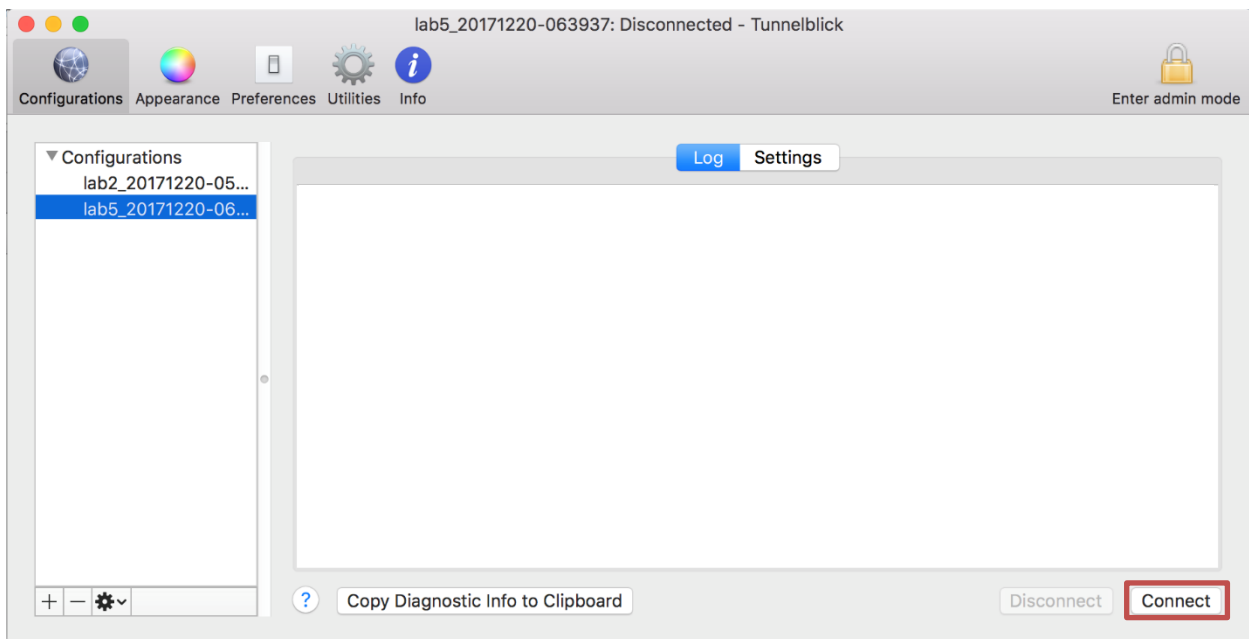
3.5. DOWNLOAD CONFIGURATION FILE

After you start a lab, you will need to click the key icon to download a VPN file to connect to the lab network. Save the OpenVPN file to your local machine.

3.6. CONNECT

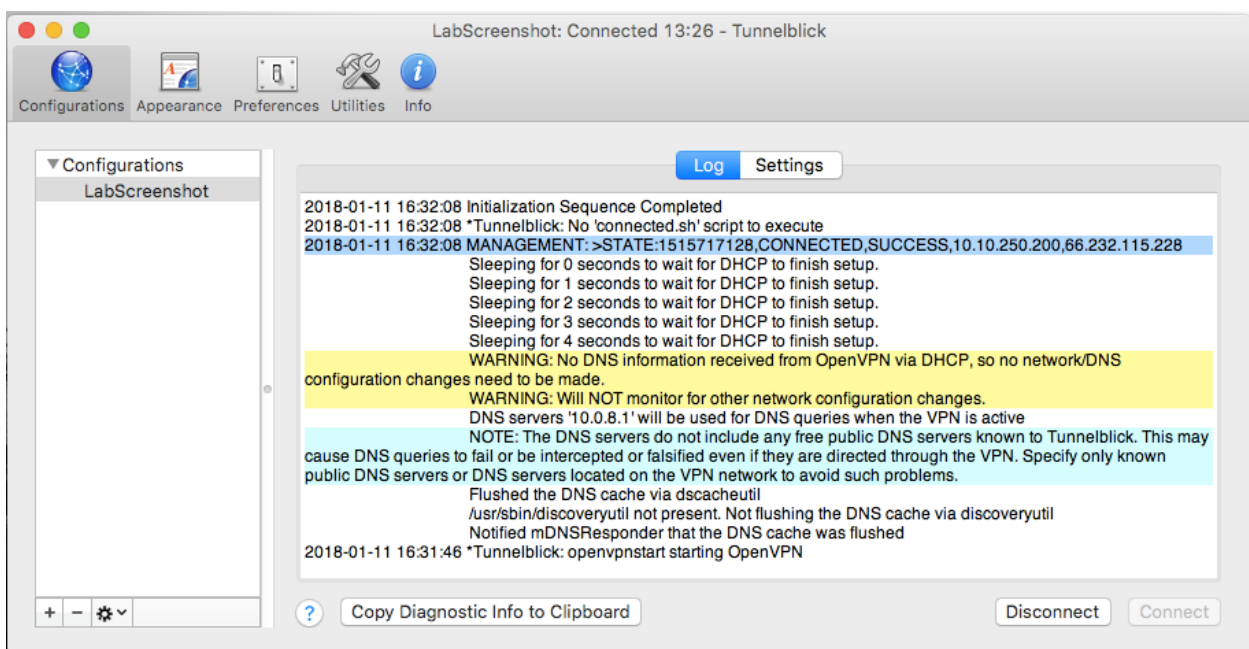
Once a lab scenario is started and you have downloaded the configuration files, it's time to connect to the VPN tunnel. Accessing Tunnelblick from the status bar, you should see the list of tunnels downloaded and for each of them connect to the respective tunnel by clicking on the **Connect** option:





If the connection is successful, you will be notified that the connection was established. At this point you will need to authenticate to the VPN server using the credentials you set during the first use wizard (you can configure them again in the Lab VPN Credentials menu item in the members area)

If authentication is successful, you will see this message:



Note: If Tunnelblick displays a message warning that the computer's apparent public IP address was not different after connecting to the VPN, this can be safely ignored.







3.7. TEST THE TUNNEL

If the tunnel works, you should have a new network interface with the same IP address displayed in the OpenVPN client.

```
tap0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
  ether f6:4b:61:32:95:55
  inet 10.10.250.200 netmask 0xfffff000 broadcast 10.10.250.255
  inet 169.254.185.88 netmask 0xffff0000 broadcast 169.254.255.255
  media: autoselect
  status: active
  open (pid 37871)
```

3.8. ENJOY THE LAB





Each Lab comes with a manual that explains the scenario, the goals and a list of tasks that will guide you through the steps necessary to reach the goals. At the end of the manual you will find detailed Solutions for the lab. You can download the Lab Manual by clicking on the PDF icon:

Lab	Manual	Actions	Status	Runtime	VPN File	Completed
 HTTP(S) Traffic Sniffing			Off	00:00:00	--	<input type="checkbox"/>
 Find the Secret Server			Off	00:00:00	--	<input type="checkbox"/>

3.9. STOP THE LAB

Once you have finished to use the Lab, remember to **stop it by clicking on the 'Stop' button** in the Members area.



Labs catalog						
Lab	Manual	Actions	Status	Runtime	VPN File	Completed
 HTTP(S) Traffic Sniffing			Running	00:00:07		<input type="checkbox"/>

Please consider that if you are using the On-Demand plan, you should stop the Lab as soon as you are done with your exercises.



4. FIREWALL CONFIGURATION

To have fully-isolated environments, Hera Lab makes use of dedicated ports selected (randomly during the first fresh start) from a wide port range. It's not possible to reserve a static port to a customer.





We suggest you to talk with your sys admins in order to add a firewall exception. They should allow outgoing connections (to our Hera OpenVPN servers) with these parameters:

- protocol: udp
- destination port range: [33000 - 43000]
- destination ip addresses:
 - 209.133.193.243
 - 162.220.60.104
 - 69.46.22.139

5. LAB INFORMATION

5.1. HOW LONG IS THE LAB RUNNING FOR?

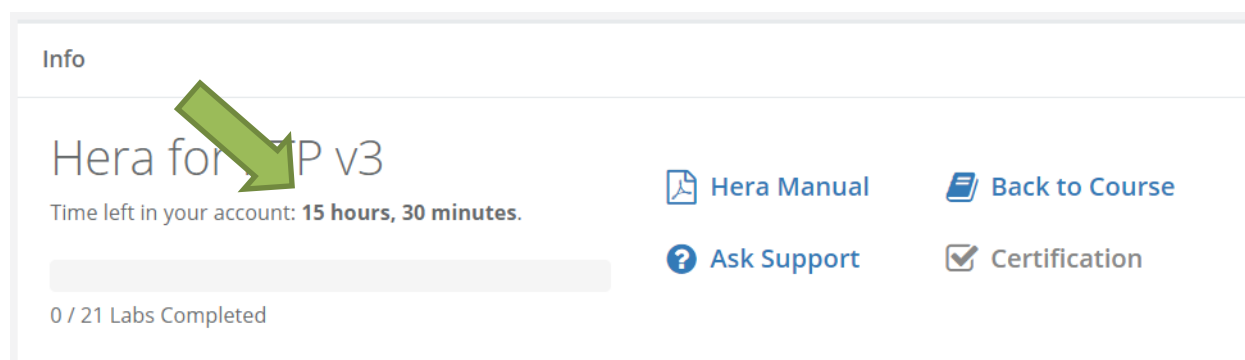
In order to check how long a specific lab is running for, you can monitor the "Runtime" column for the lab scenario.

Labs catalog						
Lab	Manual	Actions	Status	Runtime	VPN File	Completed
 HTTP(S) Traffic Sniffing			Running	00:00:07		<input type="checkbox"/>



5.2. How can I verify how much time I have left in my account?

Please Log in to the Members area, click the “Virtual Labs” tab, and select the lab catalog that you want to view. Your remaining lab hours are visible on the top section of the lab catalog.



5.3. How is my total time calculated with On-demand model?

You purchase an amount of hours to use on Hera Lab.

This amount of time is decreased when you use Hera Lab for exactly the number of minutes of each of your session.

E.g.

You purchase 30 hours and you use the lab for 26 minutes you will have 29 hours and 34 minutes left. After that you then use the lab for exactly 72 minutes: you will have 27 hours and 22 minutes left.

Note: the time required for the Tunnel to be created/destroyed is not counted towards your remaining minutes.



5.4. LAB EXPIRATION AND AUTOMATIC STOP

Please note that:

- When you first start a lab, it will reset to a clean slate after 3 days. Additionally, this deadline of resetting every 3 days will be postponed every time you start the lab during this timeframe. When the lab automatically resets, you will lose all changes you did to the environment.
- Once started, the lab will automatically stop after 3 hours to save resources. Before the times run out, you will be presented with the following pop-up to extend the running time of the lab:

