



eLearnSecurity
Forging security professionals

PWD LAB

USER MANUAL

v. 1.2 - January 7, 2019

- 1) WINDOWS USERS
- 2) LINUX USERS

1. WINDOWS USERS

A. ENTER THE LAB

Once the connection to the lab has been established, you can interact with the webserver in different ways: SSH, VNC or your web browser.

For reviewing or editing the code we suggest you to use SSH. This will give you a fast connection to the code; while you can use your web browser to navigate through the web application. The VNC access, is an extra way you could use, for example, if you want to have GUI access to the webserver.

The web server address, is always **10.143.87.50**

i. SSH CONNECTION

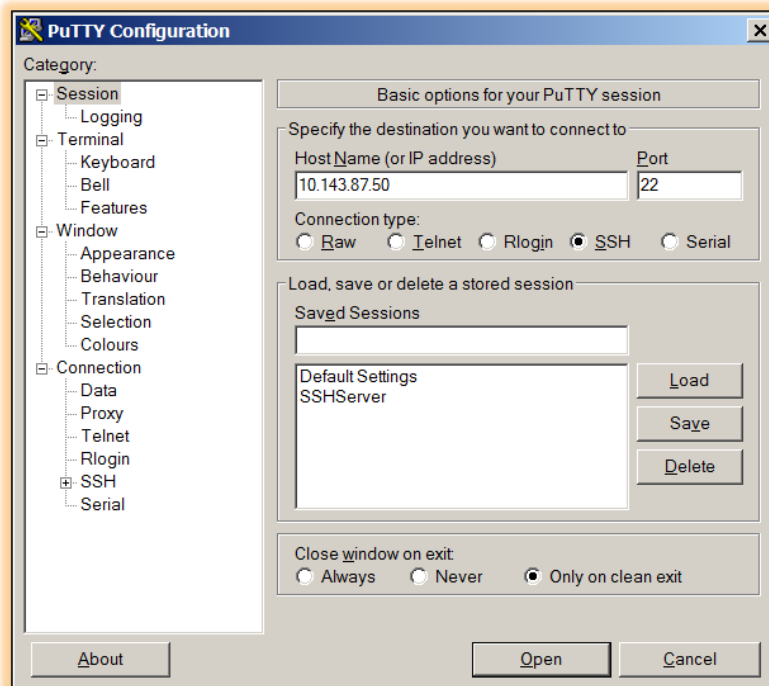
To start SSH you can use [PuTTY](#) with the following settings:

Remote IP Address:	10.143.87.50
Remote port:	22
Username:	root
Password:	toor

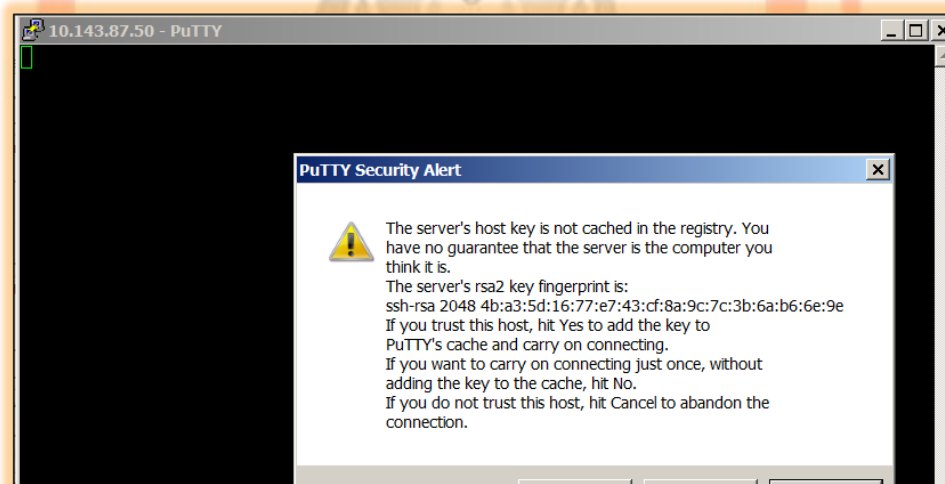
Note: this configuration is valid for all the labs related to this course

The following screenshots show how to configure putty:





If it's your first connection you will receive a certificate warning. Click yes to continue.



When the shell prompts the "Login as:" insert the username *root* and confirm. After few seconds it will ask to insert the password (which is *toor*).



```
root@kali: ~
login as: root
root@10.143.87.50's password:
Linux kali 3.7-trunk-amd64 #1 SMP Debian 3.7.2-0+kali8 x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Nov 12 07:46:27 2013 from 10.10.80.50
root@kali:~#
```

ii. YOUR WEB BROWSER

In order to access the web application easily through your web browser, add the following entries inside the **hosts** file located at:

```
C:\Windows\System32\drivers\etc\hosts
```

This is a **non-complete** list of entries you could add to the hosts file:

```
# PWD Labs
10.143.87.50 example.com
10.143.87.50 hospital.com
10.143.87.50 powerplant.com
10.143.87.50 monitoring.com
10.143.87.50 hr-portal.com
10.143.87.50 sales-portal.com
```

Finally, test your connection to the lab by opening the following URLs:

- <http://example.com>

YOU SHOULD SEE DIRECTORY INDEXING IN THESE URLS!



Note: the binding with some sites may be already cached in your web browser. To apply these changes you should delete the DNS cache of the browser.

If you use **Chrome** or **Firefox**, please refer to the following link, on how to delete the DNS cache of your browser: <https://techwiser.com/clear-dns-cache-on-browser>

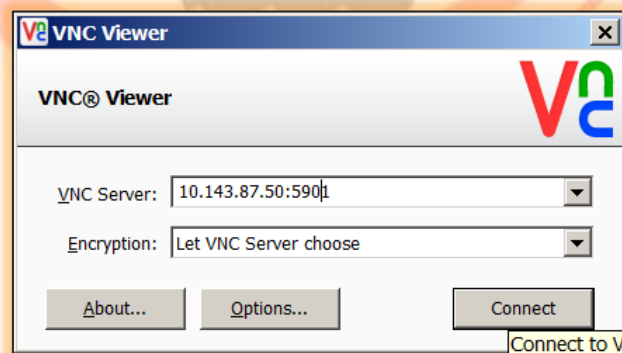
iii. VNC CONNECTION

To start a VNC connection download and install [VNC Viewer](#) (or any other VNC client) and use the following settings:

Remote IP Address: 10.143.87.50
Remote port: 5901
Username:
Password: passwd

Note: this configuration is valid for all the labs related to this course

The following screenshots show how to configure VNC Viewer

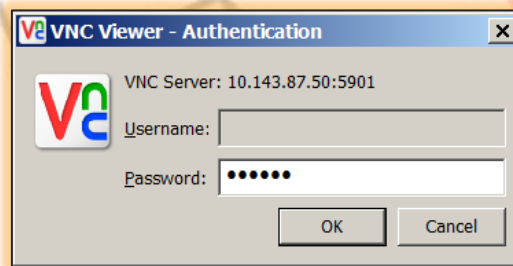


Once you hit “Connect”, the following warning appears on the screen. Check the box “Do not warn me...” and click continue.

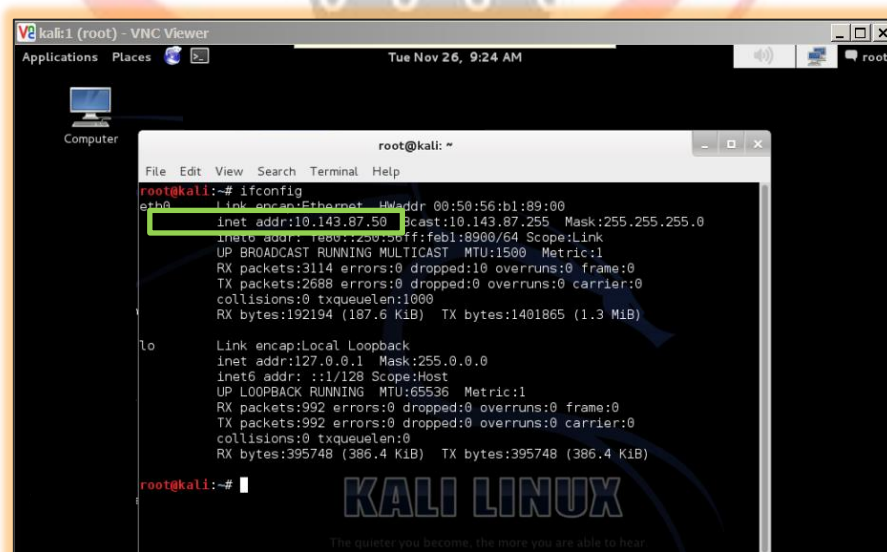




Once you hit "Continue" VNC Viewer will ask the password. Insert "passwd".



After few seconds the screen of the remote machine appears:



2. LINUX USERS

A. ENTER THE LAB

Once the connection to the lab has been established, you can interact with the webserver in different ways: SSH, VNC or your web browser.

For reviewing or editing the code we suggest you to use SSH. This will give you a fast connection to the code; while you can use your web browser to navigate through the web application. The VNC access, is an extra way you could use, for example, if you want to have GUI access to the webserver.

The web server address, is always **10.143.87.50**

i. SSH CONNECTION

The following table summarizes the SSH settings

Remote IP Address: 10.143.87.50
Remote port: 22
Username: root
Password: toor

Note: *this configuration is valid for all the labs related to this course*

You can start an SSH connection with the following command:



```
root@litsnarf: ~  
File Edit View Search Terminal Help  
root@litsnarf:~# ssh root@10.143.87.50  
The authenticity of host '10.143.87.50 (10.143.87.50)' can't be established.  
ECDSA key fingerprint is 9b:1a:49:8f:6e:18:b7:c1:a5:e1:ab:d3:e2:80:18:46.  
Are you sure you want to continue connecting (yes/no)?
```

Then write yes to continue and insert the password (*toor*):

```
root@kali: ~  
File Edit View Search Terminal Help  
root@litsnarf:~# ssh root@10.143.87.50  
The authenticity of host '10.143.87.50 (10.143.87.50)' can't be established.  
ECDSA key fingerprint is 9b:1a:49:8f:6e:18:b7:c1:a5:e1:ab:d3:e2:80:18:46.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added '10.143.87.50' (ECDSA) to the list of known hosts.  
root@10.143.87.50's password:  
Linux kali 3.7-trunk-amd64 #1 SMP Debian 3.7.2-0+kali8 x86_64  
  
The programs included with the Kali GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
Last login: Tue Nov 26 09:10:59 2013 from 10.10.80.53  
root@kali:~#
```

ii. YOUR WEB BROWSER

In order to access the web application easily through your web browser, add the following entries inside the **hosts** file located at:

```
/etc/hosts
```

This is a **non-complete** list of entries you could add to the hosts file:

```
# PWD Labs  
10.143.87.50 example.com  
10.143.87.50 hospital.com
```



```
10.143.87.50 powerplant.com
10.143.87.50 monitoring.com
10.143.87.50 hr-portal.com
10.143.87.50 sales-portal.com
```

Finally, test your connection to the lab by opening the following URLs:

- <http://example.com>

YOU SHOULD SEE DIRECTORY INDEXING IN THESE URLS!

Note: the binding with some sites may be already cached in your web browser. To apply these changes you should delete the DNS cache of the browser.

If you use **Chrome** or **Firefox**, please refer to the following link, on how to delete the DNS cache of your browser: <https://techwiser.com/clear-dns-cache-on-browser>

iii. VNC CONNECTION

The following table summarizes the VNC settings:

Remote IP Address: 10.143.87.50
Remote port: 5901
Username:
Password: passwd

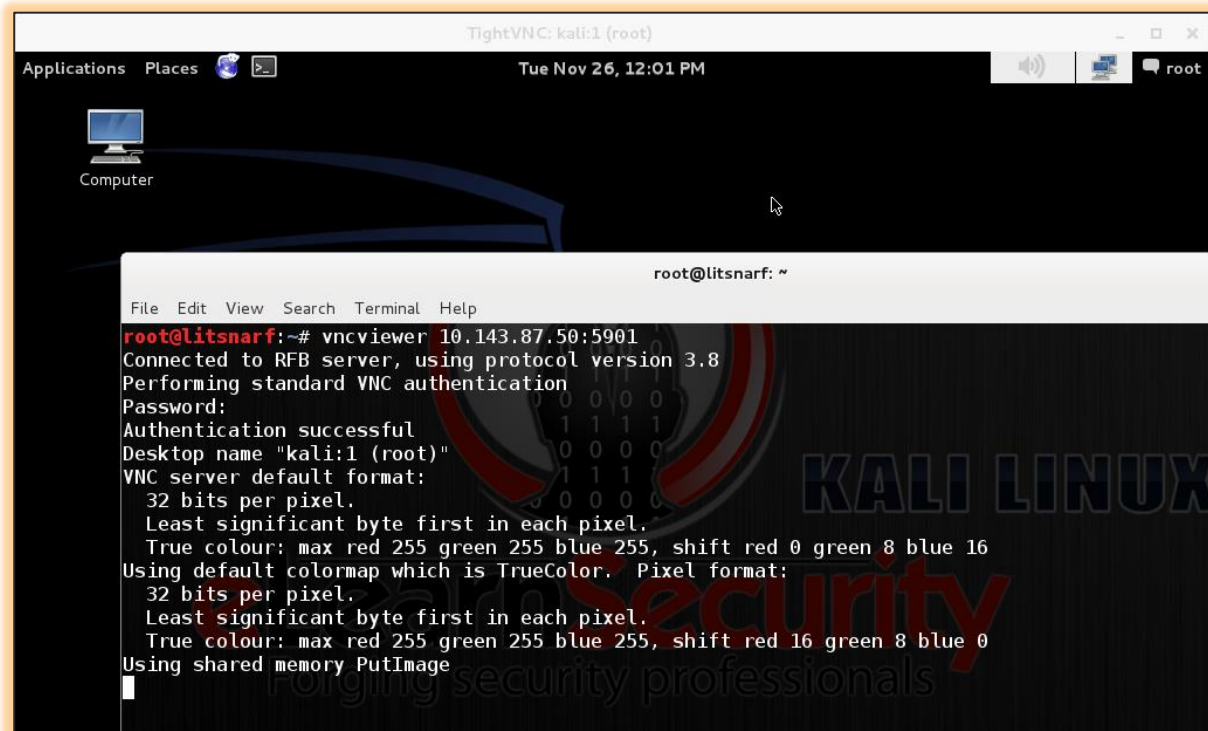
Note: this configuration is valid for all the labs related to this course

In order to start a VNC session you can use the following command:



```
vncviewer 10.143.87.50:5901
```

and then, insert the password “passwd”:

The image shows a screenshot of a Kali Linux desktop environment. At the top, there is a window title bar for 'TightVNC: kali:1 (root)'. Below it, a panel shows 'Applications', 'Places', and system icons for volume, network, and power. The desktop background is dark with a 'KALI LINUX' watermark and a stylized logo. A terminal window is open in the foreground, titled 'root@litsnarf: ~'. The terminal output shows the execution of 'vncviewer 10.143.87.50:5901', which connects to an RFB server and performs VNC authentication. The password 'passwd' is entered, and the connection is successful. The terminal also displays VNC server default format and colormap information.

```
TightVNC: kali:1 (root)
Applications Places [Icons] [Terminal] [System Icons]
Tue Nov 26, 12:01 PM root

Computer

root@litsnarf: ~
File Edit View Search Terminal Help
root@litsnarf:~# vncviewer 10.143.87.50:5901
Connected to RFB server, using protocol version 3.8
Performing standard VNC authentication
Password:
Authentication successful
Desktop name "kali:1 (root)"
VNC server default format:
 32 bits per pixel.
Least significant byte first in each pixel.
True colour: max red 255 green 255 blue 255, shift red 0 green 8 blue 16
Using default colormap which is TrueColor. Pixel format:
 32 bits per pixel.
Least significant byte first in each pixel.
True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using shared memory PutImage
```