

EX 11 Explore Tor network for anonymous communication

AIM:

To learn about TOR and its implementation.

PROBLEMS:

The screenshot shows a web browser window with the address bar displaying `tryhackme.com/room/torforbeginners`. A blue progress bar at the top indicates "Room progress (91%)". The main content area contains text about the Tor network, its purpose, and its use in penetration testing. Below the text, there is a section titled "Answer the questions below" with four quiz questions. Each question has a text input field and a green "Correct Answer" button.

Room progress (91%)

Tor is free and open source software for enabling anonymous communication. It uses a worldwide, volunteer, relays network consisting of more than seven thousand relays to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis. Using Tor makes it more difficult to trace Internet activity to the user: this includes "visits to Web sites, online posts, instant messages, and other communication forms". Tor's intended use is to protect the personal privacy of its users, as well as their freedom and ability to conduct confidential communication by keeping their Internet activities unmonitored.

In penetration testing, there might be a need to conduct a full-fledged black-box test. This is a form of testing in which security professionals have to deal with such things as firewalls and other mechanisms of restriction on the customer's side. In this case, the Tor network can be used in order to constantly change IP and DNS addresses and therefore successfully overcome any restrictions.

In this unit, we are going to install the Tor service and learn basic commands.

Answer the questions below

Run `apt-get install tor` to install/update your Tor packages.

No answer needed ✓ Correct Answer

Run `service tor start` to start the Tor service.

No answer needed ✓ Correct Answer

Run `service tor status` to check Tor's availability.

No answer needed ✓ Correct Answer

Run `service tor stop` to stop the Tor service.

No answer needed ✓ Correct Answer

koorn progress (91%)

Proxychains is widely used by pentesters during the reconnaissance stage (For example with `nmap`).

Answer the questions below

Let's start with running `apt install proxychains` to install/update proxychains tool.

No answer needed

✓ Correct Answer

Now it's time to configure proxychains to work properly.

Run `nano /etc/proxychains.conf` to edit the settings. (Note: You can use any text editing tool instead of nano.)

No answer needed

✓ Correct Answer

We can now see, that most of the methods are under comment mark. You can read their description and decide on using one of them in the future. For this lesson let's uncomment `dynamic_chain` and comment others (simply put `#` to the left). Additionally, it is useful to uncomment `proxy_dns` in order to prevent DNS leak. Scroll through the document and see whenever you want to add some additional proxies at the bottom of the page (which is not required at this point).

Apply all the settings.

No answer needed

✓ Correct Answer

Now let's check our settings.

Start the TOR service and run `proxychains firefox`. Usually, you are required to put `proxychains` command before anything in order to force it to transfer data through Tor.

No answer needed

✓ Correct Answer

After the Firefox has loaded, check if your IP address has changed with any website that provides such information. Also, try running a test on `dnsleaktest.com` and see if your DNS address changed too.

NOTE: All commands, browser configurations should be stored before installing Firefox then the browser itself.

RESULT: hence the experiment was done successfully.