

Forum:[Hack Forums](#)

Thread: [Terminal over TOR for security?](#)

insta164 - July 15, 2019, 12:38 pm

Hey all.

I browsed HF for some hours and ended up at Blackhat Training It was a thread talking about security doing Blackhat and security over TOR.

I saw something that i didn't understand, running a terminal over TOR for security. what does it mean? What is a Terminal and if you are using a Terminal, don't you need a VPN then?

Take care y'all ?

ItsJigSaw - July 15, 2019, 12:47 pm

Im a beginner aswell but afaik by that they mean that u install and use Tor network as a proxy. I think that nmap or some other tool i used had that option for anonymity.

Salon0503 - July 15, 2019, 6:35 pm

I don't know what that means, but it is safe to just run your traffic through Tor. (as a proxy or just the browser)

Faith Connors - July 15, 2019, 8:22 pm

link the thread i want to call out the skid

Asdethprime - July 15, 2019, 9:32 pm

Terminal = a console for command line.

If you are using Windows your terminal would be Powershell or simple command prompt.

For Linux Bash is normally the most popular.

Terminal over Tor ; is referring to routing all internet packets through tor.

Let's try and give u a more practical example. First few assumptions

- 1) operating system being used here is Linux (Ubuntu)
- 2) Terminal being used is Bash

What happens is there is this beautiful command line tool call nmap. This allows you to scan either a single IP address or a network.

One option you can use is called -A (Aggressive Scan).

On Ubuntu I would do as follows:

```
$ nmap -A google.com
```

This will cause nmap is aggressively scan IP address returned for google.com

To do this scanning your computer is actually sending bits of information , called packets , to google.com and checking the response to find out what it's running.

One problem with this is these so called packets have information about your network (normally the IP address of your wifi box) . Google.com server can see that.

As a hacker , specially when u are doing anything offensive u don't want that to happen.

One available option is TOR (The Onion Router) . This is a special network you can connect to before sending these packets to google.com

Doing so makes sure that your IP address is NOT included in the packets u send.

Forcefully getting your communication packet to send through tor from a command line is what people are talking about when they say things like terminal over tor.

The way I would do this (people have their own way of doing things) is used a tool called proxychains.

So remember my original command from the command line was:

```
$ nmap -A google.com
```

If I want the terminal connection to go through tor I would do

```
$ proxychains nmap -A google.com
```

My scanning is going to be super slow but sadly that's the price you pay for anonymity.

You can use VPN if you like ; tor is another method and generally one that is HUGELY recommended over using VPN.

Does that make sense to u ?

insta164 - July 16, 2019, 3:14 am

(Jul 15, 2019 09:32 PM)Asdethprime Wrote: [\[CITE\]](#) Terminal = a console for command line.

If you are using Windows your terminal would be Powershell or simple command prompt.

For Linux Bash is normally the most popular.

Terminal over Tor ; is referring to routing all internet packets through tor.

Let's try and give u a more practical example. First few assumptions

- 1) operating system being used here is Linux (Ubuntu)
- 2) Terminal being used is Bash

What happens is there is this beautiful command line tool call nmap. This allows you to scan either a single IP address or a network.

One option you can use is called -A (Aggressive Scan).

On Ubuntu I would do as follows:

```
$ nmap -A google.com
```

This will cause nmap is aggressively scan IP address returned for google.com

To do this scanning your computer is actually sending bits of information , called packets , to google.com and checking the response to find out what it's running.

One problem with this is these so called packets have information about your network (normally the IP address of your wifi box) . Google.com server can see that.

As a hacker , specially when u are doing anything offensive u don't want that to happen.

One available option is TOR (The Onion Router) . This is a special network you can connect to before sending these packets to google.com

Doing so makes sure that your IP address is NOT included in the packets u send.

Forcefully getting your communication packet to send through tor from a command line is what people are talking about when they say things like terminal over tor.

The way I would do this (people have their own way of doing things) is used a tool called proxychains.

So remember my original command from the command line was:

```
$ nmap -A google.com
```

If I want the terminal connection to go through tor I would do

```
$ proxychains nmap -A google.com
```

My scanning is going to be super slow but sadly that's the price you pay for anonymity.

You can use VPN if you like ; tor is another method and generally one that is HUGELY recommended over using VPN.

Does that make sense to u ?Shit, that was some heavy shit for a beginner but I understand. So using a VPN is way more risky than doing this terminal over TOR thing?
Appreciate your answer and thanks for the perfect explanation. ?

ririki - July 16, 2019, 3:18 am

(Jul 16, 2019 03:14 AM)insta164 Wrote: [\[CITE\]](#) Shit, that was some heavy shit for a beginner but I understand. So using a VPN is way more risky than doing this terminal over TOR thing?

Appreciate your answer and thanks for the perfect explanation. ?

Tor is overall better, a lot of people uses it and the way of tracing something is almost impossible. VPN is maybe faster, many people uses it but the way of tracing can be simple as you never know whether your provider keep logs or not.

Asdethprime - July 16, 2019, 3:55 am

(Jul 16, 2019 03:14 AM)insta164 Wrote: [\[CITE\]](#) Shit, that was some heavy shit for a beginner but I understand. So using a VPN is way more risky than doing this terminal over TOR thing?

Appreciate your answer and thanks for the perfect explanation. ?

It does not have to be terminal over tor, you can just use Tor. There is a Tor browser.

<https://www.torproject.org/download/>

Try that if you want

Advantage of Tor

- 1) More secured, really FAR MORE SECURED from anonymity perspective
- 2) FREE

Disadvantage:

- 1) Very slow and hence can't be used for day to day task (for example, try watching a youtube video over tor)
- 2) A lot of security sensitive machines (for example bank server) simply wont let you use tor to connect. Why, coz they can't track who you are :p

daymon - July 16, 2019, 4:28 am

(Jul 16, 2019 03:55 AM)Asdethprime Wrote: [\[CITE\]](#) It does not have to be terminal over tor, you can just use Tor. There is a Tor browser.

<https://www.torproject.org/download/>

Try that if you want

Advantage of Tor

- 1) More secured, really FAR MORE SECURED from anonymity perspective
- 2) FREE

Disadvantage:

- 1) Very slow and hence can't be used for day to day task (for example, try watching a youtube video over tor)
- 2) A lot of security sensitive machines (for example bank server) simply wont let you use tor to connect. Why, coz they can't track who you are :p
browsing via tor != utilizing shell functions via tor

(Jul 15, 2019 08:22 PM)Faith Connors Wrote: [\[CITE\]](#) link the thread i want to call out the skid
LOL i love ur new sig bby

kayla_90 - July 16, 2019, 4:44 am

I always use Tor+ vpn in that order

Asdethprime - July 16, 2019, 5:03 am

(Jul 16, 2019 04:28 AM)daymon Wrote: [\[CITE\]](#) browsing via tor != utilizing shell functions via tor

LOL i love ur new sig bby

That would be the post before the one you quoted.

insta164 - July 16, 2019, 11:58 am

(Jul 16, 2019 03:55 AM)Asdethprime Wrote: [\[CITE\]](#) It does not have to be terminal over tor, you can just use Tor. There is a Tor browser.

[Tor Project | Download](#)

Try that if you want

Advantage of Tor

- 1) More secured, really FAR MORE SECURED from anonymity perspective
- 2) FREE

Disadvantage:

- 1) Very slow and hence can't be used for day to day task (for example, try watching a youtube video over tor)

2) A lot of security sensitive machines (for example bank server) simply wont let you use tor to connect. Why, coz they can't track who you are :p
Appreciate your answers, thanks!