REPORT S7/L4

TOR

Traccia

Da Kali, scaricare e provare Tor Browser (senza modificare alcuna impostazione predefinita). Effettuare qualche navigazione sulla rete tor ed effettuare screenshot per il report

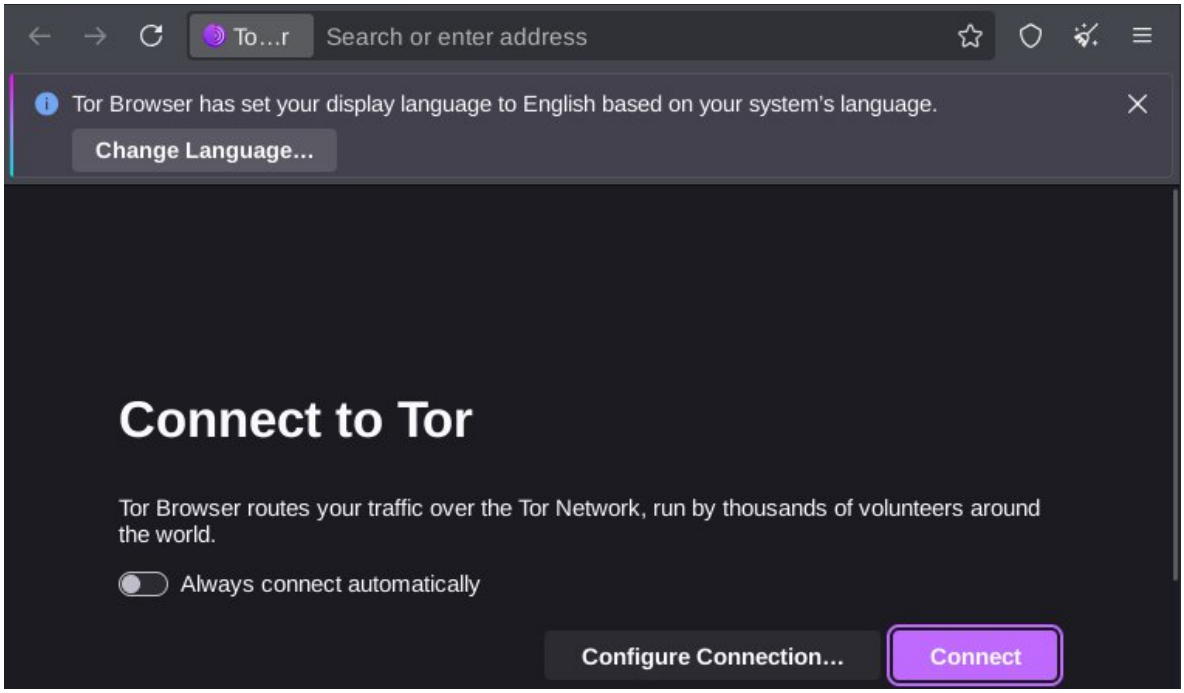
Svolgimento

Come descritto dalla traccia andiamo ad installare Tor browser tramite il comando

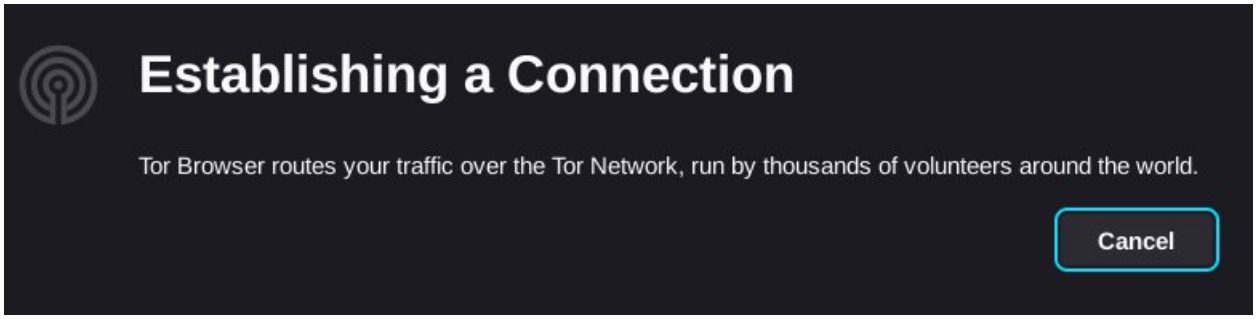
sudo apt install -y tor torbrowser-launcher

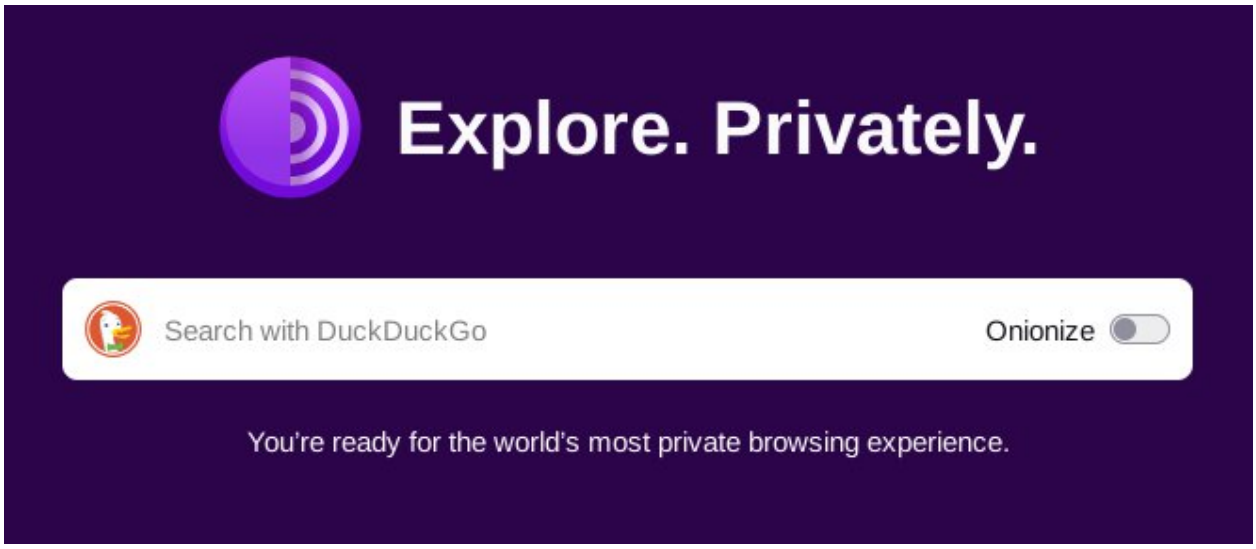
```
┌──(kali㉿kali)-[~]
└─$ sudo apt install -y tor torbrowser-launcher
[sudo] password for kali:
Installing:
  tor  torbrowser-launcher

Installing dependencies:
  tor-geoipdb  torsocks

Suggested packages:
  mixmaster  apparmor-utils  nyx  obfs4proxy

Summary:
  Upgrading: 0, Installing: 4, Removing: 0, Not Upgrading: 1884
  Download size: 4,596 kB
  Space needed: 26.6 MB / 53.3 GB available

Get:1 http://kali.download/kali kali-rolling/main amd64 tor amd64 0.4.8.13-2 [2,053 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 tor-geoipdb all 0.4.8.13-2 [2,414 kB]
Get:3 http://kali.download/kali kali-rolling/contrib amd64 torbrowser-launcher amd64 0.3.7-2 [54.7 kB]
Get:4 http://kali.download/kali kali-rolling/main amd64 torsocks amd64 2.4.0-2 [74.4 kB]
Fetched 4,596 kB in 10s (481 kB/s)
```

Dopo possiamo avviarlo con il comando *torbrowser-launcher*

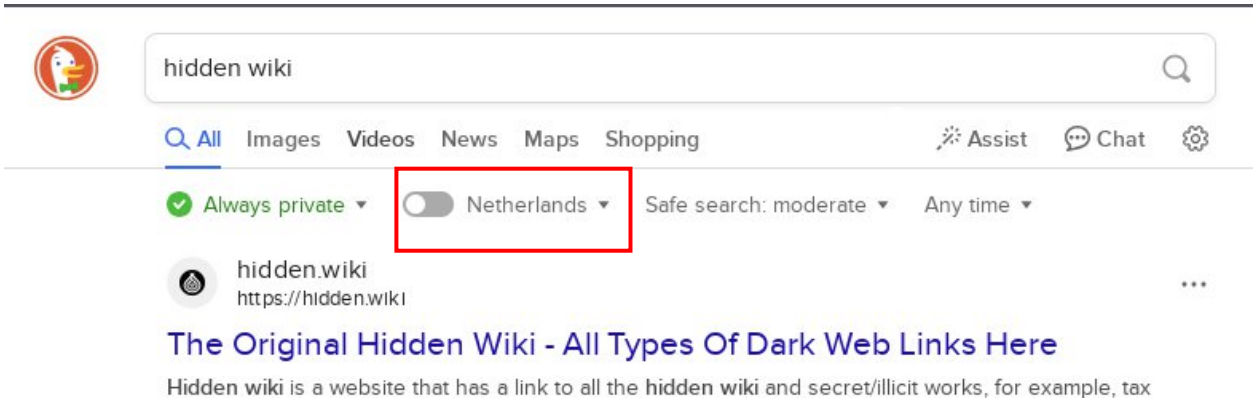


Come possiamo vedere, all'avvio non siamo ancora collegati alla rete tor, perciò clicchiamo su connect



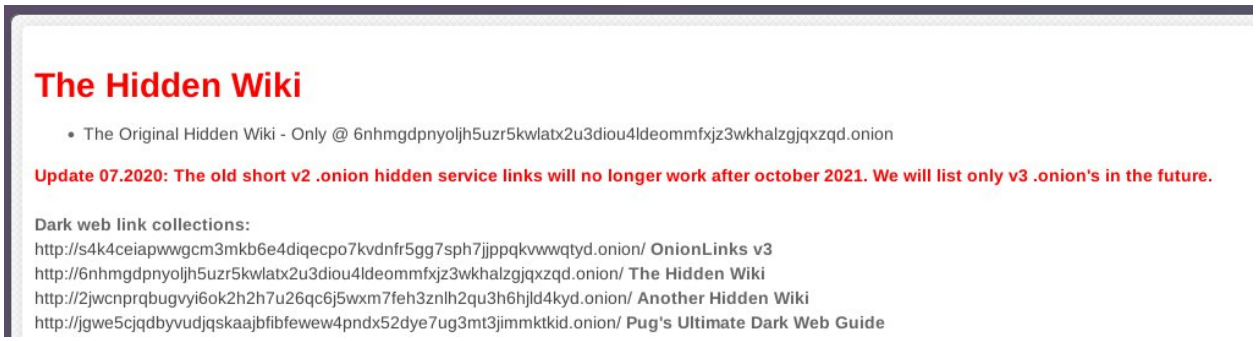


La prima ricerca che possiamo effettuare è cercando hidden wiki e già notiamo una cosa particolare, ovvero che il motore di ricerca DuckDuckGo ci localizza in Olanda



Scegliamo la Hidden Wiki come prima ricerca perchè HW è una web directory di altri siti .onion. Come servizio nascosto, The Hidden Wiki opera esclusivamente attraverso lo pseudo-dominio di primo livello .onion, che può essere raggiunto solamente attraverso Tor. Il sito fornisce una serie di link in formato wiki ad altri servizi nascosti e siti.

Possiamo anche usare direttamente il link http://6nhmgdpnyoljh5uzr5kwlatx2u3diou4ldeommfxjz3wkhalzgjqxzqd.onion/ che è pubblico sulla pagina wikipedia della HW.

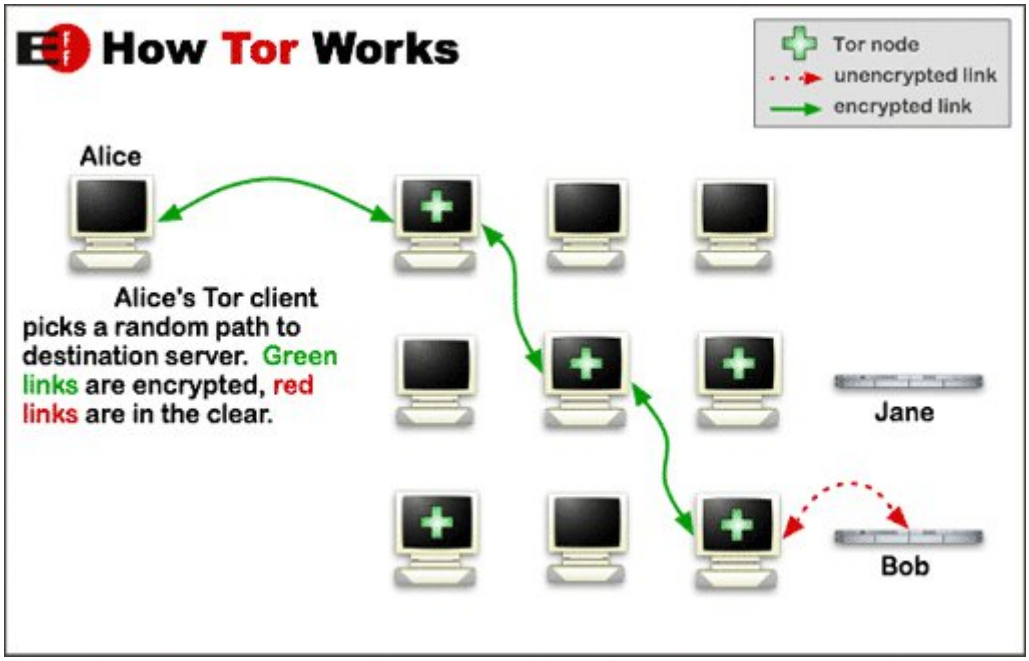


Dall'elenco presente nella pagina possiamo cominciare la nostra navigazione verso i vari siti disponibili, che come abbiamo detto a lezione sono perlopiù fake, scam oppure gestiti dalle forza dell'ordine che li utilizzano per attirare ignari utenti del dark web con intenzioni illecite.

Difatti ricordiamo che la navigazione nel dark web non è illegale, ma lo è l'acquisto o il download di materiale illegale. Oltre a questo la navigazione, anche se sotto rete Tor, ci espone ad alcuni rischi come la possibilità di essere hackerati, o che ci vengano rubati i nostri dati. Lo capiamo meglio spiegando in breve cos'è Tor.

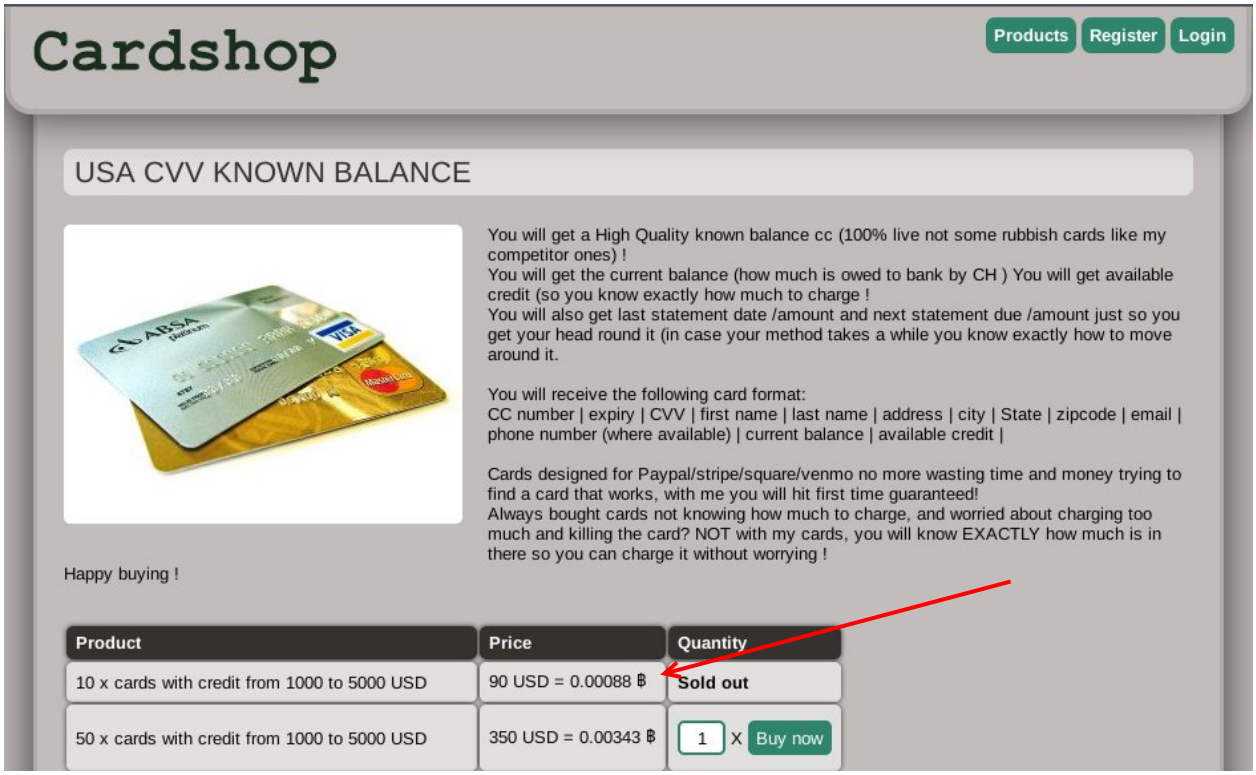
Tor (**The Onion Router**) è un software libero che permette una navigazione anonima sul Web: tramite il suo utilizzo è molto più difficile tracciare o intercettare l'attività che l'utente compie su Internet, sia da parte di società commerciali che da parte di soggetti potenzialmente ostili.

Il funzionamento "a cipolla" di Tor fa in modo che il nostro indirizzo IP originale venga nascosto sotto diversi strati in modo che non sia visibile, ma non tutta la comunicazione avviene in maniera criptata, come mostra l'immagine sotto:



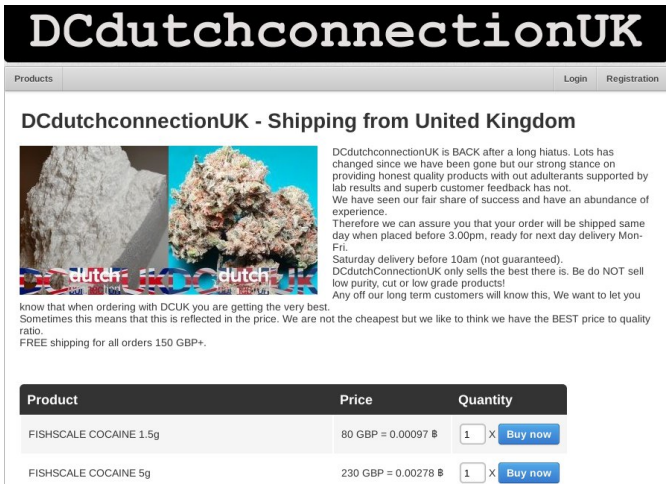
Da questo possiamo capire che l'ultimo salto verso il pc/sito gestito da Bob avviene in chiaro e per questo è rintracciabile. Se al posto di Bob ci mettiamo un sito gestito dalle forze dell'ordine allora tutta la nostra navigazione potrebbe essere rintracciata, a maggior ragione se compiamo attività illegali.

A scopo illustrativo inseriamo alcuni screen di pagine che visitiamo

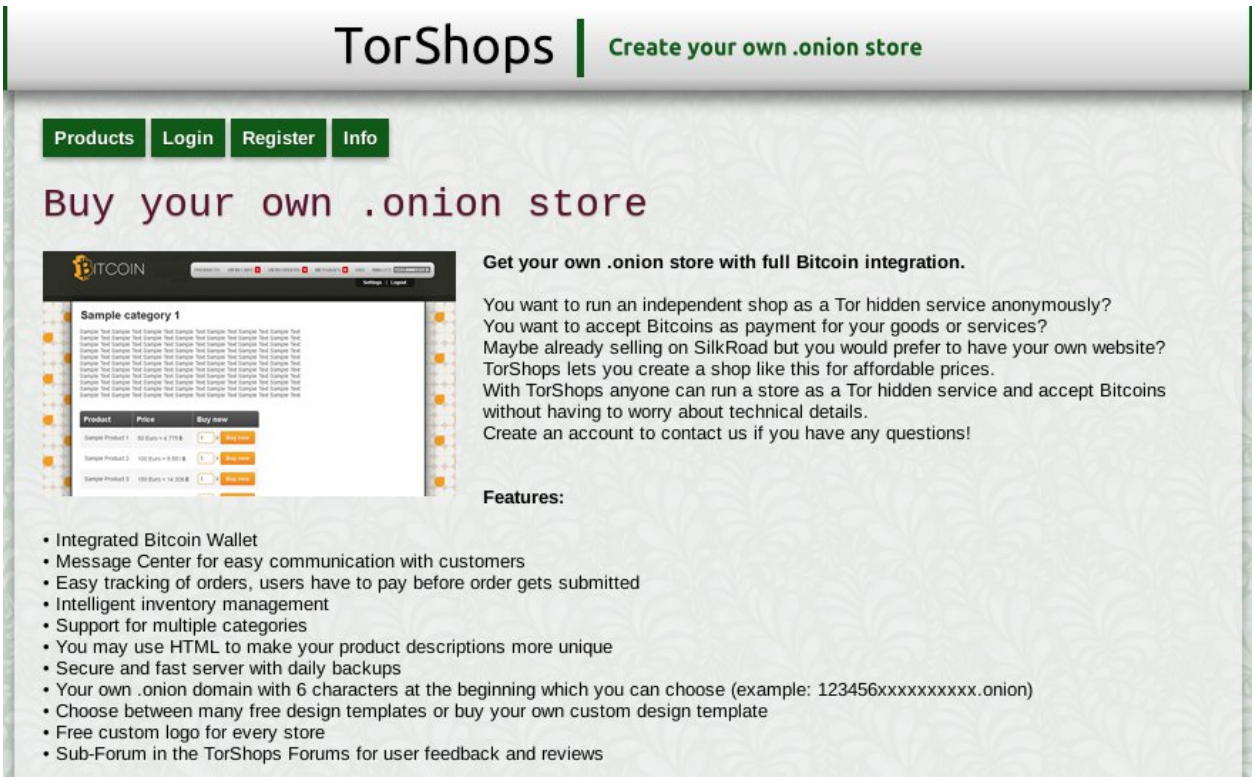


Da questo primo sito visitato vediamo il modo più scontato e diffuso in cui viene usata la rete Tor, ovvero compravendita di servizi o materiale illegale. Notiamo che tutte queste attività avvengono con l'utilizzo di cripto valute perchè rendono gli acquirenti e i venditori anonimi.

Come detto prima, questo sito, come tanti altri, sono solo dei siti truffa, creati apposta per rubare sia i dati che i soldi di chi va a comprare.



Esempio di sito per vendita di sostanze stupefacenti.



Da questo sito si può comprare tutto il necessario per aprire il proprio negozio online su rete Tor.

Ricordiamo infine che Tor non è l'unica rete anonima esistente, altri due esempi sono iRC e Freenet. L'esistenza di queste reti non è dovuta soltanto per scopi illeciti o illegali, ma inizialmente nacquero per permettere a persone, che vivevano in situazioni di difficoltà socio-politica, di poter comunicare senza la paura di essere rintracciati. Tuttora questo è lo scopo principale della loro esistenza e utilizzo.

REPORT S7/L4 - BONUS

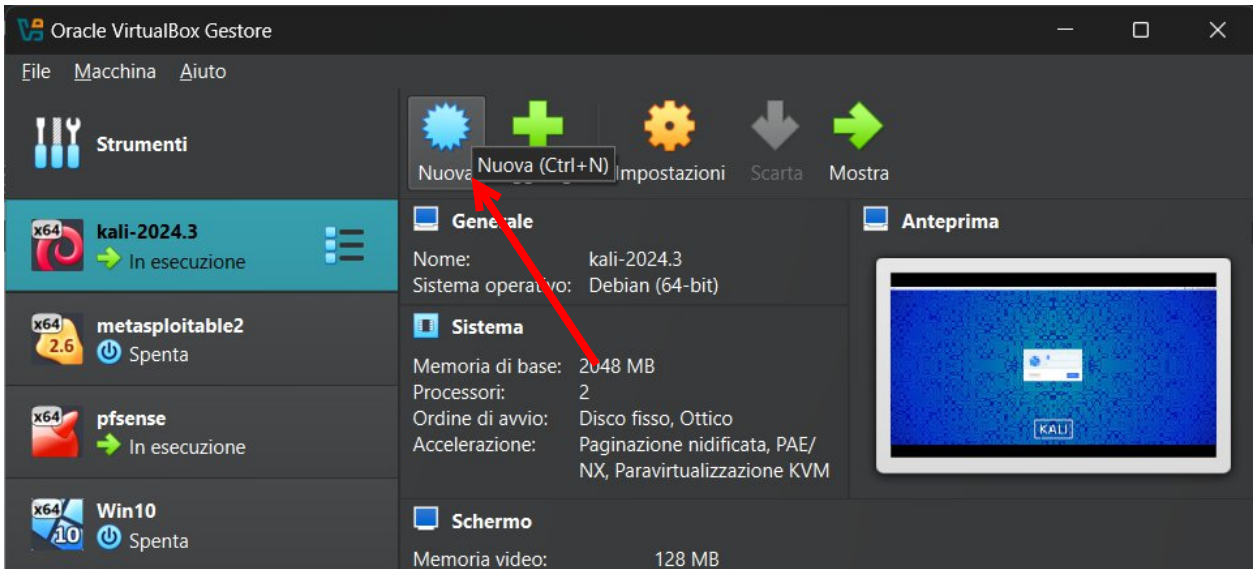
Installare Tails su macchina virtuale

Svolgimento

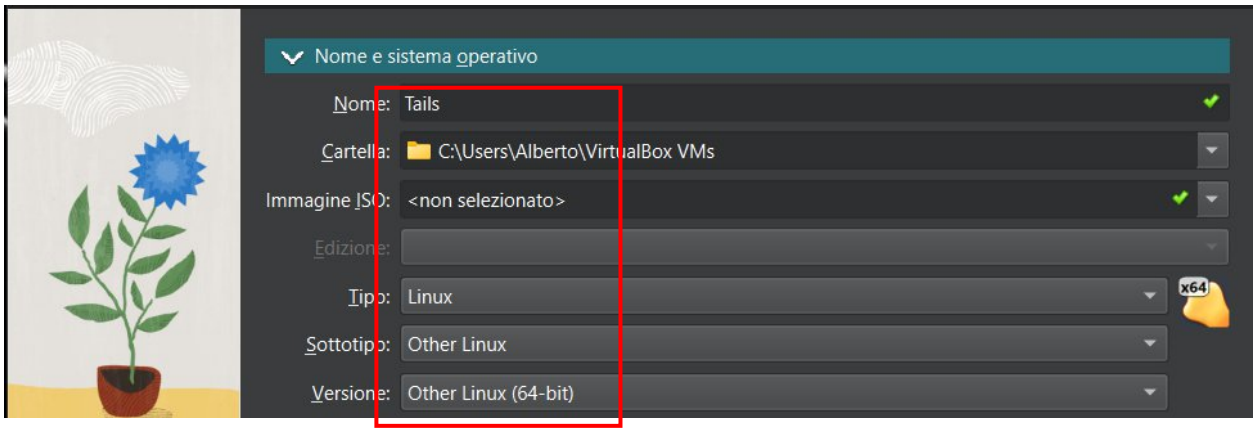
Cominciamo con il download dell'immagine iso di Tails, che ricordiamo è un sistema operativo su base debian incentrato sull'anonimato dell'utilizzatore, molto più di Kali.

Possiamo trovare la iso all'indirizzo *https://tails.net/install/download-iso/index.en.html*

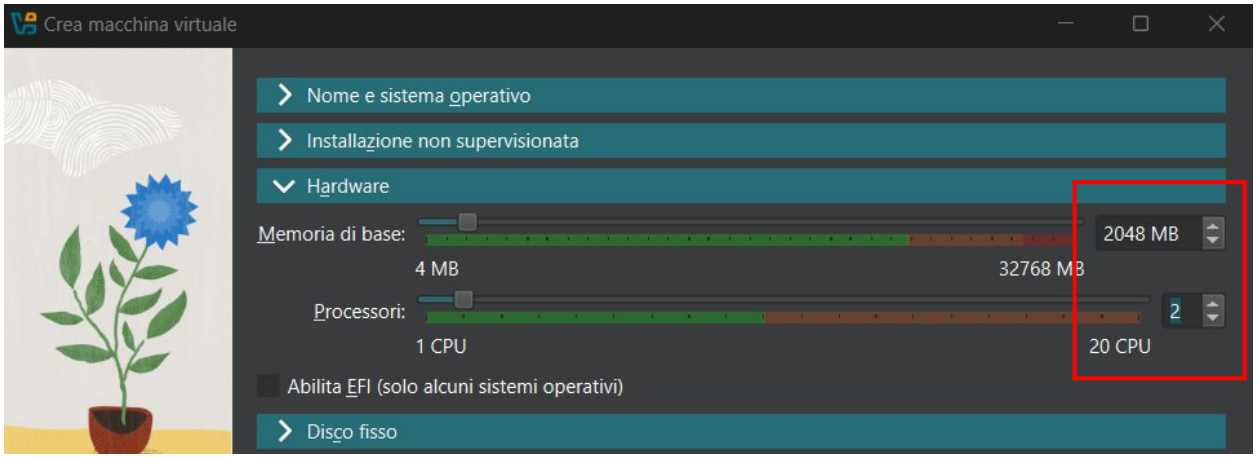
Il nostro scopo non è però installarlo o creare una disco live su chiavetta o DVD, ma piuttosto farne una VM su VBox. A questo scopo avviamo VBox, e clicchiamo su *Nuova*



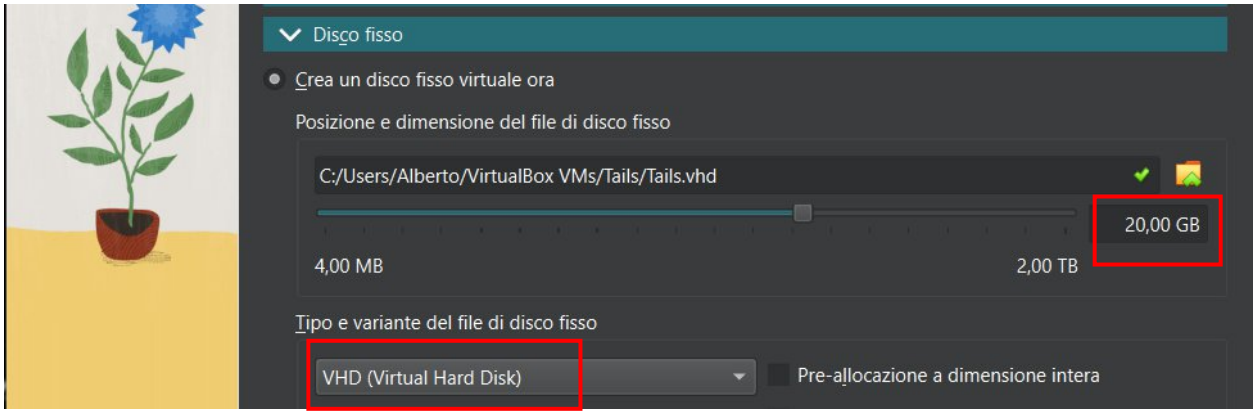
Negli screen successivi mostriamo le impostazioni da inserire per l'installazione del SO.



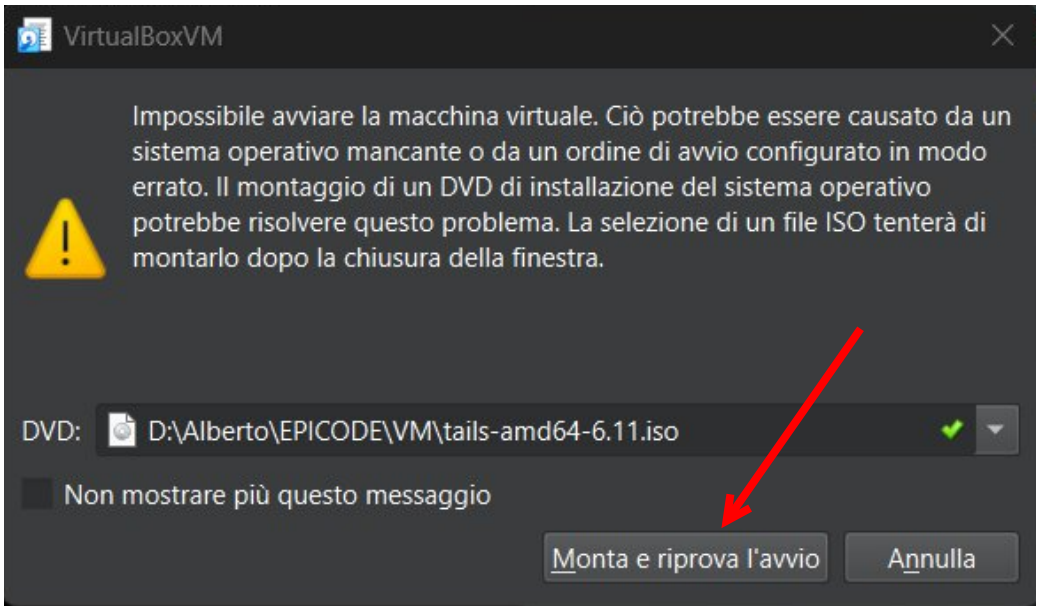
Scegliamo di usare 2GB di RAM e 2 processori, così da rendere l'utilizzo più fluido.



Configuriamo la creazione di un disco virtuale lasciando la dimensione consigliata di 20GB e scegliendo VHD come tipologia, dato che dopo la creazione della macchina dobbiamo provvedere all'installazione del SO.



Creata così la VM la facciamo partire e ci viene subito chiesto un disco dal quale avviare il SO. Selezioniamo l'immagine scaricata dal sito ufficiale e confermiamo.

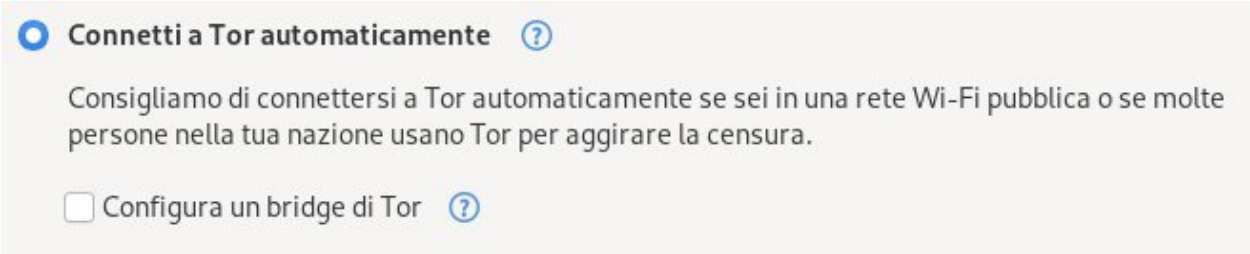


Lasciando poi caricare entreremo nella procedura di installazione che andiamo a completare.

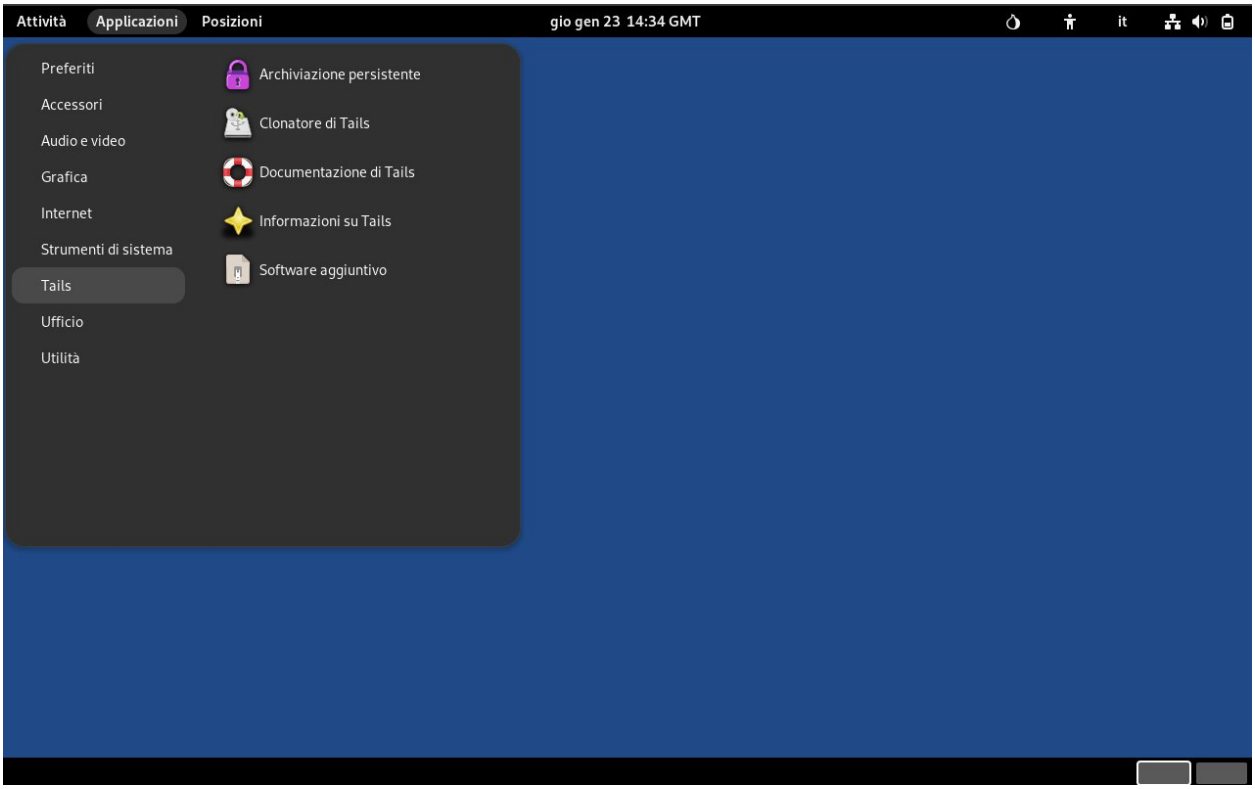
Ci viene chiesta la lingua e selezioniamo italiano, poi va configurata la connessione a Tor di cui abbiamo due scelte:

1. Connessione automatica
2. Connessione nascosta

La prima ci connette automaticamente alla rete Tor, la seconda fa in modo che, se la rete a cui siamo collegati è monitorata, la nostra connessione a Tor venga nascosta. Scegliamo la prima opzione senza configurare alcun bridge.

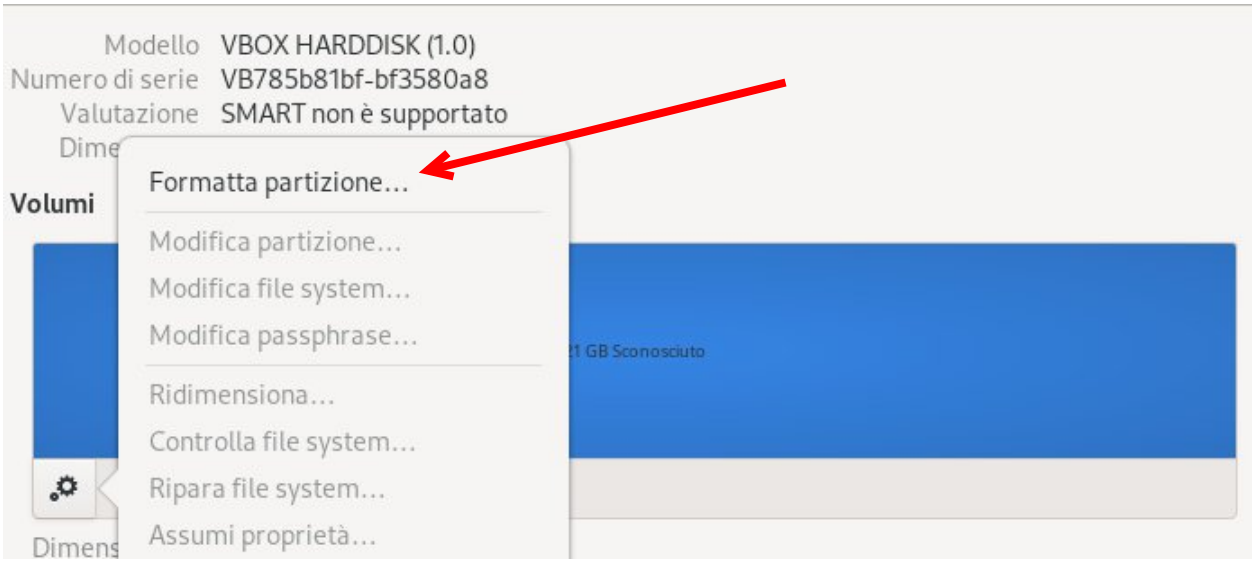


Fatto ciò possiamo usare Tails e navigare in anonimato con Tor.

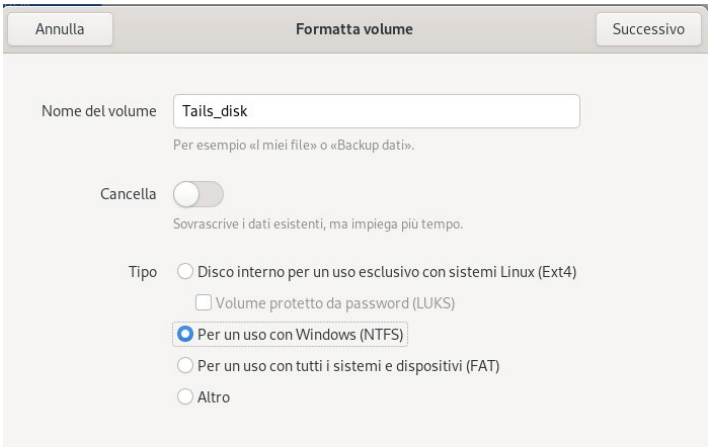


Tuttavia possiamo accedere al disco virtuale creato solo dopo averlo formattato e montato, per questo andiamo su **Applicazioni -> Utilità -> Dischi**

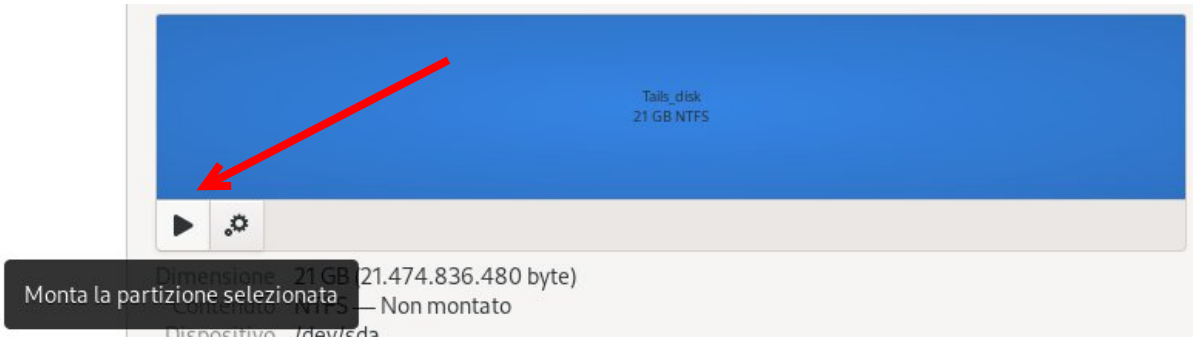
Scegliamo **Formatta partizione**



Scegliamo l'etichetta del disco, e il filesystem, nel nostro caso NTFS così da renderlo accessibile anche da Windows.



Dopo premiamo sul play per montare la partizione



A questo punto possiamo vedere la partizione appena montata