Hidden Service Cookbook

by Krang from Dimension X

v0.2

12.09.2016

Spis treści

Wstęp

Poradnik, krop po kroku jak skonfigurować bezpieczny serwer www dla hidden service w sieci TOR. Poradnik będzie rozwijany i udoskonalany. Krang jest otwarty na wszystkie uwagi, sugestie oraz wykryte błędy.

Bezpieczeństwo Twojego serwera to bezpieczeństwo wszystkich jego użytkowników.

Wymagania

Serwer dedykowany lub VPS z zainstalowaną minimalną wersją systemu Debian >=8. Optymalne parametry dla komfortowej pracy to procesor 1 GHz, pamięć RAM 512 MB dysk 6 GB. Sugerowane parametry to dwurdzeniowy procesor >=2 GHz, pamięć RAM >=1024, dysk SSD 10 GB. Różnego rodzaju serwery w atrakcyjnych cenach znajdziesz na LowEndBox.

Wskazówki

Ten poradnik ma na celu pomóc w konfiguracji serwera w sieci TOR tak aby jego użytkownicy mieli zapewnioną podstawową ochronę oraz aby usługa nie była narażona na atak/wyłączenie/wykradzenie danych. Bezpieczeństwo serwera to nie wszystko, bardzo ważne jest zachowanie anonimowości administratora oraz lokalizacji serwera. Anonimowość oraz dobra konfiguracja zapewni nam odpowiedni poziom prywatności a co za tym idzie podniesie poziom bezpieczeństwa.

Przy wyborze serwera poza jego parametrami kieruj się jego lokalizacją oraz możliwością wykonania płatności w walucie Bitcoin. Bitcoin'y zakup na dowolnej giełdzie a następnie je wypierz za pomocą pralni np. Helix. Do strony i panelu swojego serwera łącz się za pomocą przeglądarki TorBrowser a najlepiej poprzez rozwiązanie jakie oferuje system Whonix lub Tails.

Na lokalizację serwera najlepiej nadaje się kraj spoza UE lub jeśli brak an to środków, taki w którym kładzie się duży nacisk na bezpieczeństwo informacji oraz utrudniony stopień na szybki dostęp niechcianych służb do danych na serwerze np. Austria, Niemcy, Szwecja. Inne fajne lokalizacje to również Holandia, Rosja czy Francja.

Do swojego serwera będziesz łączył się za pomocą protokołu SSH stąd najlepsze rozwiązanie to Whonix Workstation + Whonix Gateway.

Nigdy nie ujawniaj swojej tożsamości podczas łączenia się z serwerem/panelem administracyjnym. Do zakupu nie podawaj prawdziwych danych.

Logowanie i podstawowa konfiguracja

Parametry takie jak porty, nazwa użytkownika, bazy danych, hasła są podane jako przykłady, wskazane jest aby do swojej konfiguracji wprowadzić swoje parametry i trzymać się ich przez całą konfigurację aby w każdym miejscu odpowiadały tym skonfigurowanym.

Ustawienia wstępne

Pierwsze logowanie

```
ssh root@adres_ip
```

Zmiana hasła root

```
passwd
```

Aktualizacja systemu

```
apt-get update && apt-get dist-upgrade
```

Instalacja podstawowych pakietów

```
apt-get install aptitude nano mc htop iftop sudo fail2ban portsentry
```

Konfiguracja języka

```
dpkg-reconfigure locales
```

wybierz:

```
en_US.UTF-8 UTF-8
```

Konfiguracja strefy czasowej

```
dpkg-reconfigure tzdata
```

wybierz:

```
None of the above->UTC
```

Odinstalowanie zbędnych domyślnych aplikacji

```
apt-get purge exim4 exim4-base exim4-config mutt procmail
```

Edycja repozytoriów

```
nano /etc/apt/sources.list
```

Lista powinna wyglądać mniej więcej tak:

```
deb http://httpredir.debian.org/debian jessie main
deb-src http://httpredir.debian.org/debian jessie main
deb http://httpredir.debian.org/debian jessie-updates main
deb-src http://httpredir.debian.org/debian jessie-updates main
deb http://security.debian.org/ jessie/updates main
deb-src http://security.debian.org/ jessie/updates main
```

Tworzenie użytkownika

```
adduser nazwa_użytkownika
```

Dodawanie użytkownika do sudo

```
usermod -g sudo nazwa_użytkownika
```

Poniższe polecenie edytuje listę użytkowników i ich możliwości.

```
visudo
```

Znajdź wpis:

```
root ALL=(ALL:ALL) ALL
```

Dodaj pod nim wpis:

```
nazwa_użytkownika ALL=(ALL:ALL) ALL
```

Zmiana hosta (Opcjonalnie)

```
nano /etc/hosts
```

Motd (Opcjonalnie)

```
nano /etc/motd
```

Przykład:

Issue.net (Opcjonalnie)

```
nano /etc/issue.net
nano /etc/ssh/sshd_config
```

Przykład:

```
**********************************************************************
*                                                                    *
* This system is for the use of authorized users only.  Usage of     *
* this system may be monitored and recorded by system personnel.     *
*                                                                    *
* Anyone using this system expressly consents to such monitoring     *
* and is advised that if such monitoring reveals possible            *
* evidence of criminal activity, system personnel may provide the    *
* evidence from such monitoring to law enforcement officials.        *
*                                                                    *
**********************************************************************
```

Zarówno Issue.net jak MOTD nie powinny zawierać szczegółowych informacji o użytkowniku czy sesji, powyższe obrazki przedstawiają jedynie możliwości obydwu plików.

Usuń # przed linią:

```
Banner /etc/issue.net
```

Wyłączanie logowania root

```
nano /etc/ssh/sshd_config
```

Usuń # przed linią i ustaw „no”:

```
PermitRootLogin no
```

Zmiana portu SSH

```
nano /etc/ssh/sshd_config
```

Zmień port z 22 na 2282

```
Port 2282
```

Restart SSH

```
service sshd restart
```

Przelogowanie

```
ssh nazwa_użytkownika@adres_ip -p 2282
```

Podstawowe zabezpieczenia serwera

Portsentry

```
sudo nano /etc/portsentry/portsentry.conf
```

Domyślnie:

```
# Use these if you just want to be aware:
TCP_PORTS="1,11,15,79,111,119,143,540,635,1080,1524,2000,5742,6667,12345,12346,20034,27665,31337,32771,32772,32773,32774,40421,49724,54320"
UDP_PORTS="1,7,9,69,161,162,513,635,640,641,700,37444,34555,31335,32770,32771,32772,32773,32774,31337,54321"
```

Dodaj # przed powyższą linie i usuń # przed linią:

```
# Un-comment these if you are really anal:
TCP_PORTS="1,7,9,11,15,70,79,80,109,110,111,119,138,139,143,512,513,514,515,540,635,1080,1524,2000,2001,4000,4001,5742,6000,6001,6667,12345,12346,20034,27665,30303,32771,32772,32773,32774,31337,40421,40425,49724,54320"
UDP_PORTS="1,7,9,66,67,68,69,111,137,138,161,162,474,513,517,518,635,640,641,666,700,2049,31335,27444,34555,32770,32771,32772,32773,32774,31337,54321"
```

Ustaw w tym samym pliku pozostałe opcje:

```
BLOCK_UDP="1"
BLOCK_TCP="1"
```

Usuń # przed linią:

```
KILL_HOSTS_DENY="ALL: $TARGET$"
```

Usuń # przed linią:

```
PORT_BANNER="..."
```

Sprawdź kto już próbował się logować:

```
sudo cat /var/log/auth.log | grep 'sshd.*Invalid'
```

Nieźle nie? Pakują się hakerzy na świeżo postawiony VPS. Już po kilku minutach od uruchomienia boty atakują otwarte porty i próbują przeprowadzić atak bruteforce lub atak słownikowy.

Fail2ban

```
cd /etc/fail2ban
cp -v jail.conf jail.local
sudo nano /etc/fail2ban/jail.local
```

Ignorowane IP wpisuj po spacji:

```
ignoreip = 127.0.0.1 twój_adres_ip
```

Czas banowania (przykładowo godzina):

```
bantime = 3600
```

Sekcja [SSH]

Zmień:

```
port = ssh
```

na

```
port = 2282
```

Restart fail2ban:

```
sudo /etc/init.d/fail2ban restart
```

Tor i Hidden Service

Instalacja i konfiguracja

Dodajemy repozytoria Tor:

```
sudo nano /etc/apt/sources.list
```

Dodaj:

```
deb http://deb.torproject.org/torproject.org jessie main
deb-src http://deb.torproject.org/torproject.org jessie main
```

Jeszcze klucze:

```
gpg --keyserver keys.gnupg.net --recv 886DDD89
```

i

```
gpg --export A3C4F0F979CAA22CDBA8F512EE8CBC9E886DDD89 | sudo apt-key add -
```

Instalacja Tor:

```
sudo apt-get update && sudo apt-get install tor tor-arm
```

Konfiguracja Tor:

```
sudo nano /etc/tor/torrc
```

Ustawiamy:

```
SOCKSPort 0
```

Usuń # przed liniami:

```
RunAsDaemon 1
HiddenServiceDir /var/lib/tor/hidden_service/
HiddenServicePort 80 127.0.0.1:8123
```

Nie zapomnijmy o ustawieniu własnego portu np. 8123

Domena onion

Konfigurując Tor zgodnie z powyższą instrukcją adres w domenie .onion zostanie automatycznie wygenerowany dla naszej usługi.

W katalogu:

```
/var/lib/tor/hidden_service/
```

znajdziesz dwa pliki, *hostname* i *private_key*. Pierwszy zawiera przydzielony adres onion dla ukrytej usługi, drugi to klucz prywatny potwierdzający to, że jesteś właścicielem tego adresu.

Nie udostępniaj tych plików nikomu oraz utwórz ich kopię w bezpiecznym miejscu. W przypadku zmiany serwera będziesz mógł publikować z powrotem pod tym samym adresem.

Instalacja serwera WWW + PHP + MySQL

MySQL

Instalacja i konfiguracja bazy danych

Instalacja bazy danych:

```
apt-get install mysql-server mysql-client
```

Podczas instalacji podajemy hasło użytkownika root.

```
New password for the MySQL "root" user: tu_podajemy_hasło_dla_root
Repeat password for the MySQL "root" user: tu_powtarzamy_hasło_dla_root
```

Jeśli nie zostaniemy poproszeni trzeba ustawić samemu:

```
sudo mysqladmin -u root -h localhost -p
```

Tworzenie bazy

```
sudo mysqladmin create nazwa_bazy_danych -u root -p
```

Tworzenie użytkownika bazy danych i nadanie mu uprawnień do bazy:

```
sudo mysql -u root -p
Enter password: hasło_root
```

```
mysql> USE mysql;
mysql> INSERT INTO user set Host='localhost', User='nazwa_użytkownika',
Password=PASSWORD('hasło_użytkownika');
mysql> FLUSH PRIVILEGES;
mysql> GRANT Select,Insert,Update,Delete,Create,Drop ON nazwa_bazy_danych.* TO
nazwa_użytkownika@localhost;
mysql> FLUSH PRIVILEGES;
```

Pozostałe przydatne komendy dla MySQL

Logowanie do konkretnej bazy danych:

```
mysql -u root -p NAZWA_BAZY_DANYCH
```

Usuwanie bazy danych:

```
mysql> drop database NAZWA_BAZY_DANYCH;
```

Wyświetlanie istniejących baz danych:

```
mysql> show databases;
```

Sprawdzanie bazy danych:

```
mysql> check table przykładowa.tabela;
```

Naprawa bazy danych:

```
mysql> repair table przykładowa.tabela;
```

Sprawdzanie bazy danych:

```
mysqlcheck -u nazwa_użytkownika -p hasło
```

Usuwanie błędów i naprawa:

```
mysqlcheck -u nazwa_użytkownika -p --auto-repair
```

Wyjście z konsoli:

```
mysql> quit
```

Archiwizacja bazy

```
sudo mysqldump -u root -p BAZA_DANYCH > BAZA_DANYCH.sql
```

Przywracanie:

```
sudo mysql -u root -p BAZA_DANYCH < BAZA_DANYCH.sql
```

WWW

Serwer Lighttpd

```
sudo apt-get install lighttpd
```

Domyślna lokalizacja plików strony:

```
/var/www
```

Edycja pliku konfiguracyjnego:

```
sudo nano /etc/lighttpd/lighttpd.conf
```

Sugerowana konfiguracja:

```
server.modules = (
"mod_expire",
"mod_auth",
```

```
"mod_evasive",
"mod_status",
"mod_access",
"mod_alias",
"mod_compress",

"mod_redirect",

 "mod_rewrite",
)
server.document-root        = "/var/www"
server.upload-dirs          = ( "/var/cache/lighttpd/uploads" )
server.errorlog             = "/var/log/lighttpd/error.log"
server.pid-file             = "/var/run/lighttpd.pid"
server.username             = "www-data"
server.groupname            = "www-data"
server.port                 = 8123
server.tag
    = "serverwww”
index-file.names            = ( "index.php", "index.html", "index.lighttpd.html" )
url.access-deny             = ( "~", ".inc" )
static-file.exclude-extensions = ( ".php", ".pl", ".fcgi" )
compress.cache-dir          = "/var/cache/lighttpd/compress/"
compress.filetype           = ( "application/javascript", "text/css", "text/html", "text/plain" )
# default listening port for IPv6 falls back to the IPv4 port
include_shell "/usr/share/lighttpd/use-ipv6.pl " + server.port
include_shell "/usr/share/lighttpd/create-mime.assign.pl"
include_shell "/usr/share/lighttpd/include-conf-enabled.pl"
$HTTP["remoteip"] !~ "127.0.0.1" {
url.access-deny = ( "" )
}
# disable auto index directory listings
server.dir-listing
= "disable"
# performance options (aggressive timeouts)
server.max-keep-alive-requests = 0
server.max-keep-alive-idle = 15
server.max-read-idle     = 15
server.max-write-idle    = 15
# number of file descriptors (leave off for lighty loaded sites)
server.max-fds          = 512
# maximum concurrent connections the server will accept (1/2 of server.max-fds)
server.max-connections = 256
# single client connection bandwidth limit in kilobytes (0=unlimited)
connection.kbytes-per-second = 0
# global server bandwidth limit in kilobytes (0=unlimited)
server.kbytes-per-second = 0
# chroot() to directory (default: no chroot() )
server.chroot            = "/"
# disable ssl if not needed
ssl.engine               = "disable"
# mod_evasive
evasive.max-conns-per-ip = 250
# limit request method "POST" size in kilobytes (KB)
#server.max-request-size  = 1
```

```
# disable multi range requests
server.range-requests    = "disable"
# disable symlinks
server.follow-symlink    = "disable"
```

PHP

Instalacja i konfiguracja PHP7

Jeśli jesteś zainteresowany wersją 5 to we wszystkich komendach poniżej zmień 7 na 5.

```
sudo apt-get install php7.0-fpm php7.0
```

Obsługa PHP dla Lighttpd:

```
sudo nano /etc/php/7.0/fpm/php.ini
```

Zmień:

```
cgi.fix_pathinfo=0
```

na:

```
cgi.fix_pathinfo=1
```

Aktywowanie PHP-FPM:

```
cd /etc/lighttpd/conf-available/
sudo cp 15-fastcgi-php.conf 15-fastcgi-php.conf.bak
sudo nano 15-fastcgi-php.conf
```

Zmień część konfiguracji tak aby wyglądała jak poniżej:

```
# /usr/share/doc/lighttpd-doc/fastcgi.txt.gz
# http://redmine.lighttpd.net/projects/lighttpd/wiki/Docs:ConfigurationOptions#mod_fastcgi-fastcgi

## Start an FastCGI server for php (needs the php7.0-cgi package)
fastcgi.server += ( ".php" =>
        ((
                "socket" => "/var/run/php/php7.0-fpm.sock",
                "broken-scriptfilename" => "enable"
        ))
)
```

Włącz konfigurację fastcgi:

```
sudo lighttpd-enable-mod fastcgi
sudo lighttpd-enable-mod fastcgi-php
```

```
sudo ls -l /etc/lighttpd/conf-enabled
```

Restart serwera lighttpd:

```
sudo service lighhtpd restart
```

Konfiguracje PHP możesz sprawdzić tworząc plik:

```
sudo nano /var/www/info.php
```

Zawartość pliku:

```
<?php
phpinfo();
?>
```

Przejdź na swoją stronę do tego pliku w przeglądarce i zobacz sprawdź swoją konfigurację. Po sprawdzeniu nie zapomnij usunąć plik z serwera.

Warto doinstalować potrzebne moduły jak np. wsparcie MySQL dla PHP.

```
sudo apt-get -y install php7.0-mysql
```

Lub wyszukać tego którego potrzebujesz:

```
sudo apt-cache search php7.0
```

Przykładowa instalacja modułów:

```
sudo apt-get -y install php7.0-mysql php7.0-curl php7.0-gd php7.0-intl php-pear php-imagick php7.0-imap
php7.0-mcrypt php-memcache  php7.0-pspell php7.0-recode php7.0-sqlite3 php7.0-tidy php7.0-xmlrpc
php7.0-xsl php7.0-mbstring php-gettext
```

Jeszcze jeden moduł warto zainstalować:

```
sudo apt-get -y install php-apcu
```

Przeładuj FPM i serwer Lighttpd:

```
sudo service php7.0-fpm reload
sudo service lighttpd reload
```

Obsługa formularzy kontaktowych

W sieci Tor po domyślnej konfiguracji serwera www funkcja PHP mail() nie działa, stąd też każdy formularz kontaktowy czy inne powiadomienia z witryny nie będą działały. Sam serwer też nie będzie miał możliwości przesyłać nam informację i różnego rodzaju raportów o błędach czy naruszeniach zasad bezpieczeństwa. Jeśli domyślnie wysyłałby wiadomości można by było w prosty sposób uzyskać informację na temat jego lokalizacji. Wyciągając szczegółowe informacje z nagłówka wiadomości. Tu z pomocą przychodzi SSMTP. Pamiętaj aby wybrać bezpiecznego usługodawcę poczty np. Riseup.

Instalacja:

```
sudo apt-get install ssmtp
```

Konfiguracja:

```
sudo nano /etc/ssmtp/ssmtp.conf
```

Plik konfiguracyjny dla adresu twojadres@email.net:

```
#
# Config file for sSMTP sendmail
#
# The person who gets all mail for userids < 1000
# Make this empty to disable rewriting.
root=twojadres@email.net
# The place where the mail goes. The actual machine name is required no
# MX records are consulted. Commonly mailhosts are named mail.domain.com
mailhub=mail.email.net:25
# Where will the mail seem to come from?
rewriteDomain=email.net
# The full hostname
hostname=twojadres@email.net
UseTLS=Yes
UseSTARTTLS=Yes
# Are users allowed to set their own From: address?
# YES - Allow the user to specify their own From: address
# NO - Use the system generated From: address
FromLineOverride=YES
AuthUser=nazwa_użytkownika
AuthPass=hasło_do_poczty
```

Główny mail dla serwera:

```
sudo nano /etc/ssmtp/revaliases
```

```
# sSMTP aliases
#
# Format:
local_account:outgoing_address:mailhub
#
```

```
# Example: root:your_login@your.domain:mailhub.your.domain[:port]
# where [:port] is an optional port number that defaults to 25.
www-data:twojadres@email.net:mail.email.net:25
```

Wysyłanie testowego maila:

```
echo test | sudo ssmtp -s "test" test@host.tld
```

Konfiguracja php.ini:

```
sudo nano /etc/php7/cgi/php.ini
```

Zmień linijkę aby wyglądała tak:

```
sendmail_path = /usr/sbin/ssmtp -t
```

Firewall

Odpowiednie wpisy w konfiguracji Lighttpd wprowadzone we wcześniejszych rozdziałach oraz prosta konfiguracja firewalla UFW pozwoli na odparcie standardowych ataków DoS/DDoS oraz podniesie poziom bezpieczeństwa naszego serwera.

Instalacja i konfiguracja UFW

Instalacja:

```
sudo apt-get install ufw
```

Sprawdzanie statusu:

```
sudo ufw status
```

Wynik:

```
Status: active
To             Action      From
--             ------      ----
22             ALLOW       Anywhere
```

Wprowadzanie ustawień domyślnych dla połączeń przychodzących, blokada wszystkiego:

```
sudo ufw default deny incoming
```

dla połączeń wychodzących, zezwolenie na wszystko:

```
sudo ufw default allow outgoing
```

Pozwolenie na łączenie z SSH na wcześniej skonfigurowanym porcie:

```
sudo ufw allow 2282/tcp
```

Jeszcze dostęp dla serwera www na wcześniej skonfigurowanym porcie:

```
sudo ufw allow 8123/tcp
```

Wprowadzanie ochrony przed otwarciem wszystkich możliwych portów:

```
sudo nano /etc/ufw/before.rules
```

po linijkach:

```
# Don't delete these required lines, otherwise there will be errors
*filter
:ufw-before-input - [0:0]
:ufw-before-output - [0:0]
:ufw-before-forward - [0:0]
```

```
:ufw-not-local - [0:0]
# End required lines
```

dodaj:

```
# Limit to 10 concurrent connections on port 80 per IP
-A ufw-before-input -p tcp --syn --dport 80 -m connlimit --connlimit-above 10 -j DROP
```

oraz:

```
# Limit to 20 connections on port 80 per 2 seconds per IP
-A ufw-before-input -p tcp --dport 80 -i eth0 -m state --state NEW -m recent --set
-A ufw-before-input -p tcp --dport 80 -i eth0 -m state --state NEW -m recent --update --seconds 2 --hitcount 20 -j DROP
```

Uruchamianie firewalla:

```
sudo ufw enable
```

Sprawdzanie działania firewalla i skonfigurowanych usług:

```
sudo ufw status
```

Przykłady dodatkowych komend

Dla zrozumienia zasady działania i składni UFW, dodatkowe przykłady.

Blokowanie portu:

```
sudo ufw deny 80/tcp
```

Usuwanie reguły:

```
sudo ufw delete allow ssh
```

Zezwolenie na połączenie UDP:

```
sudo ufw allow 1000/udp
```

Zezwolenie na wszystkie połączenia ze zdefiniowanego adresu IP:

```
sudo ufw allow from 192.168.255.255
```

Reset do ustawień domyślnych:

```
sudo ufw reset
```

Wyłączanie firewalla gdyby coś poszło nie tak:

```
sudo ufw disable
```

Dodatkowe informacje

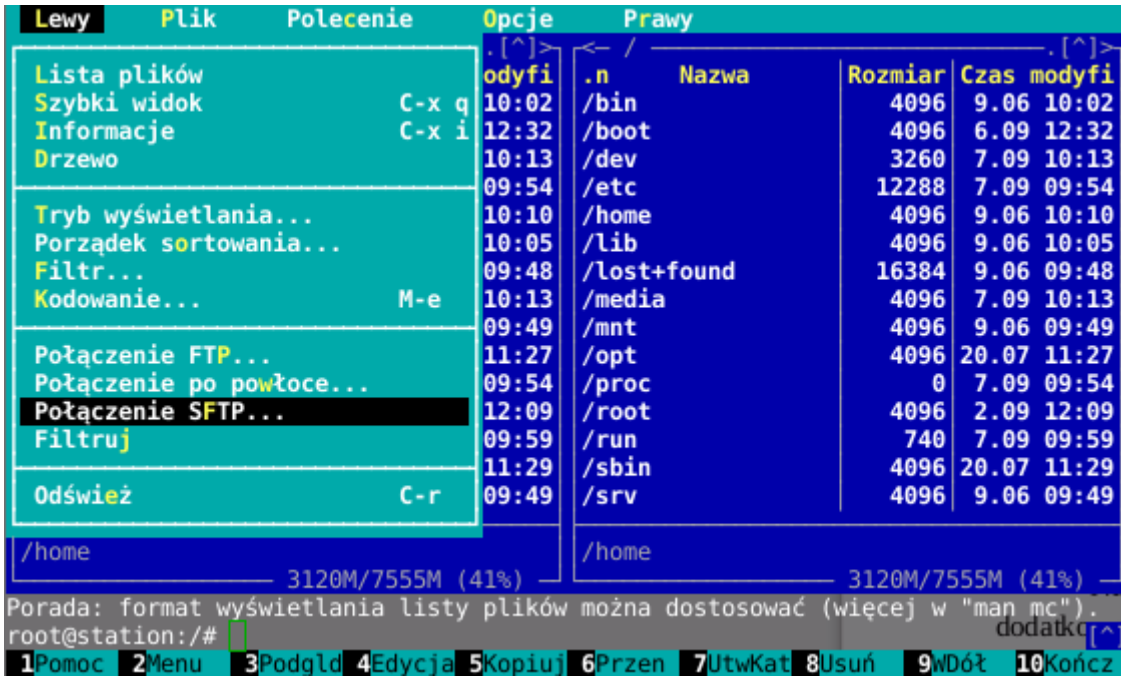
Zarządzanie bazą danych

Nie instaluj ani nie korzystaj z phpMyAdmin, to tylko zbędne narażanie serwera na atak, każda dodatkowa usługa na serwerze w sieci Tor to dodatkowa możliwość złamania jego zabezpieczeń. Najkorzystniej i najbezpieczniej do zarządzania bazą danych na serwerze będzie wykorzystać aplikacje DBeaver. Jest to uniwersalne narzędzie do zarządzania wieloma popularnymi bazami danych. Konfiguracja jest prosta i pozwala również na łączenie się poprzez SSH. Po instalacji na Whonix Workstation i skonfigurowaniu połączenia do serwera SSH oraz danych logowania bazy danych mamy ładny i przejrzysty wgląd do naszych danych.

Wgrywanie plików na serwer

Do wgrywania plików na serwer wykorzystuj połączenie po powłoce/sftp za pomocą programu Midnight Commander. Stawianie serwera FTP w sieci Tor to jak w przypadku phpMyAdmin kolejna podatność na atak. Dla chcącego nic trudnego i zarówno bezpieczny serwer FTP oraz phpMyAdmin mogą spokojnie działać. Jednak po co kusić los.

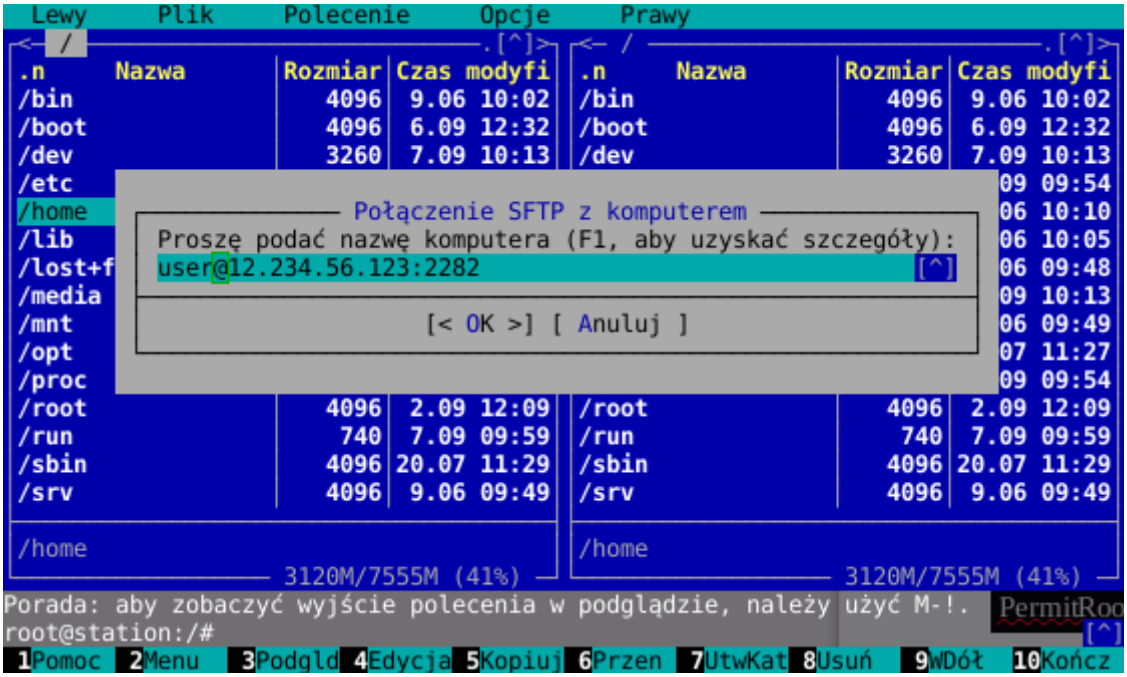
Wybierz w MC Lewy>Połączenie SFTP... lub Połączenie po powłoce...



Podaj dane logowania, połącz podaj hasło i przerzucaj pliki między komputerem lokalnym a serwerem.

Powinieneś użyć składni:

```
nazwa_użytkownika@adres_ip_serwera:port_ssh
```



Skrypty na serwerze

Bez względu na to jak zabezpieczysz serwer, jeśli będziesz korzystał z niezałatanego/dziurawego/źle napisanego skryptu bloga/forum czy jakiegokolwiek innego, to włamanie na serwer osobie zainteresowanej nie zajmie dłużej niż przeczytanie artykułu o dziurze w danej wersji skryptu i wykonaniu odrobiny magicznych komend. Zawsze aktualizuj swój skrypt do najnowszej wersji. Analizuj jakie dodatki instalujesz. Moderuj treści. Używaj systemów antyspamowych. Sieć Tor do demonów szybkości nie należy więc nie twórz pięknych kolorowych stron z milionem ozdobników. Zapewniam Cię, że ludzie odwiedzający ukryte strony nastawieni są na treści a nie ozdobniki. Aktualizuj i analizuj!

Dotacje

Administratorzy serwisów w sieci Tor jeśli nie prowadzą jakiegoś sklepu lub usługi za Bitcoiny to nie zarabiają nic na swoich stronach. Systemy reklamowe, odkąd zlikwidowany został TorAds nie przynoszą, żadnych zysków (oto pole do popisu dla Ciebie młody adepcie stawiania ukrytych usług). Spowodowane jest to tym, że większość systemów reklamowych nastawiona jest na clearnet, większość z nich po prostu nie działa lub działa ale nie do końca tak jak ma.

Jeśli lubisz jakąś stronę czy usługę, odwiedzasz ją często, czerpiesz z niej odpowiednią wiedzę, korzyści, przyjemność to przekaż dotacje dla jej właściciela. Większość z nas posiadaczy ukrytych usług tworzy je za darmo w wolnym czasie, dbamy o to aby użytkownicy usługi mieli zapewnioną choć odrobinę prywatności/anonimowości w dzisiejszym permanentnie inwigilowanym świecie. Inwigilacja jest dobra w przypadku gdy nie jest nadużywana przez władze.

Każde kilka dolców cieszy i motywuje do dalszej pracy. Gdy postawisz swoją pierwsza ukryta usługę sam zrozumiesz o czym piszę. Nie chodzi tu o miliony i ogromne zyski, a jedynie o wsparcie/pokrycie opłat za serwer/kawę na nieprzespane noce. Największym zyskiem w sieci Tor jest Twoja anonimowość i prywatność.

Jeśli zaczniesz przygodę z dotacjami rób to nie tylko w Torze ale również dla każdego projektu Open Source.

Adres BTC: 1L4AYUxUW653tqwFpeVMz7FCr7EXntDgXU

Więcej informacji oraz aktualne wydanie znajdziesz na DimensionX.

Clearnet: http://technodrome.heliohost.org/

Tor: http://54ogum7gwxhtgiya.onion/