



Jakiś czas temu pisałem o ataku typu MITM (Man In The Middle). Dziś zajmiemy się jednym z sposobów zapobiegania takim atakom. Co prawda nie będziemy zapobiegać na poziomie sieci ale na poziomie naszego komputera. Czym jest to rozwiązanie? To VPN (Virtual Private Network).

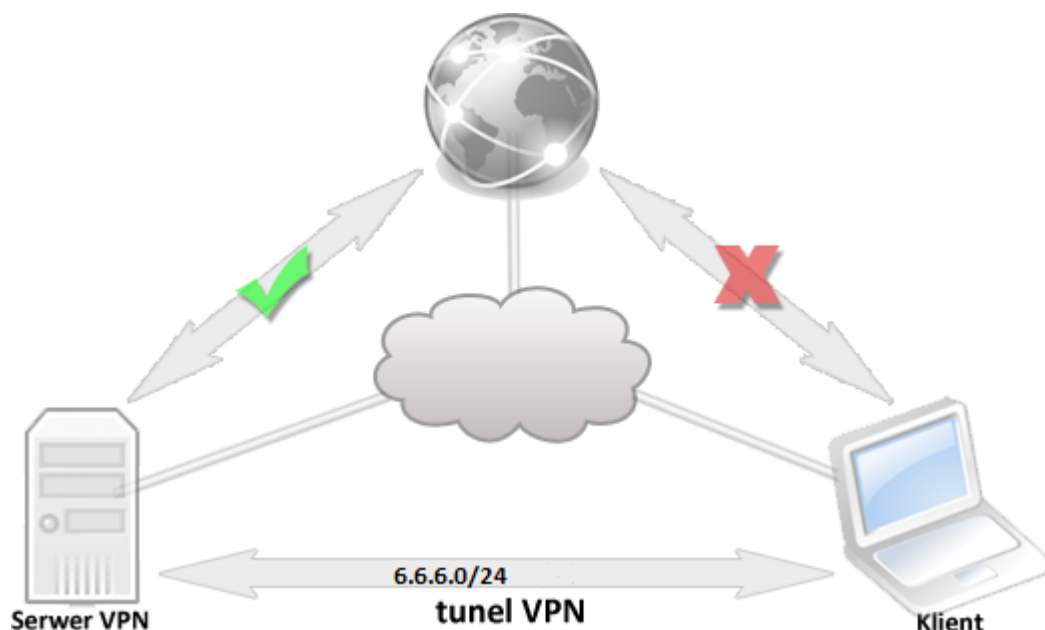
Tradycyjnie zajrzyjmy do wikipedii:

VPN (ang. Virtual Private Network, Wirtualna Sieć Prywatna) – tunel, przez który płynie ruch w ramach sieci prywatnej pomiędzy klientami końcowymi za pośrednictwem publicznej sieci (takiej jak Internet) w taki sposób, że węzły tej sieci są przezroczyste dla przesyłanych w ten sposób pakietów. Można opcjonalnie kompresować lub szyfrować przesyłane dane w celu zapewnienia lepszej jakości lub większego poziomu bezpieczeństwa.

Tłumacząc to na język prostych ludzi:

VPN - tunel łączący nasz komputer z serwerem VPN. Ruch w tunelu dla przełączników sieciowych jak i wszelakich intruzów chcących nas podsłuchiwać jest niewidoczny. Rozwiązanie to, często jest wykorzystywane w dużych firmach, gdzie pracownicy pracują zdalnie, dużo podróżują i zmuszeni są używać niezaufanego łącza.

A jak wygląda to w następujący sposób:



Co będzie nam potrzebne? Na początek potrzebujemy serwera który będzie naszym serwerem VPN. Ja do tego celu wykorzystuje serwer hostowany w rootbox.pl. Już opcja „Small” pozwala nam na wygodne korzystanie z własnego vpn’a. Będziemy też potrzebować dwóch maszyn wirtualnych. Dlaczego dwóch? Już tłumacze. Dziś nie tylko skonfiguruję połączenie VPN’a, ale też i przeprowadzę ponownie atak MITM na maszynę podłączoną tunelem, aby wykazać, brak możliwości podsłuchania.

Pierwszym krokiem jest stworzenie naszego serwera. Ja osobiście wybieram zawsze Debiana 64, jest to wersja, z którą najlepiej mi się pracuje. Po chwili od kliknięcie „utwórz” w panelu rootbox w swoim mailu można znaleźć wiadomość z danymi dostępowymi. Czas więc zacząć instalację.

Spis treści

- [Konfiguracja serwera.](#)
- [Kilka praktycznych uwag dotyczących połączeń VPN.](#)
- [Konfiguracja klienta - Windows](#)
- [Konfiguracja klienta - Linux \(Debian, gnome\)](#)
- [Pro-tip na zwiększenie bezpieczeństwa.](#)
- [Atak MITM.](#)



Konfiguracja serwera.

Logujemy się do naszego vps'a i zaczynamy od aktualizacji. Jest to dobra praktyka, nigdy nie wiemy kiedy serwerownia pre konfigurowała nasz obraz.

```
root@vpn-blog:~# apt-get update && apt-get upgrade
```

Teraz instalujemy Openvpn.

```
root@vpn-blog:~# apt-get install openvpn
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  liblzo2-2 libpkcs11-helper1
Suggested packages:
  openssl resolvconf
The following NEW packages will be installed:
  liblzo2-2 libpkcs11-helper1 openvpn
0 upgraded, 3 newly installed, 0 to remove and 0 not upgraded.
Need to get 621 kB of archives.
After this operation, 1,489 kB of additional disk space will be used.
Do you want to continue [Y/n]?
```

Klikamy „Y” i instalujemy nie tylko Openvpn ale i wymagane dodatkowo pakiety.

Teraz gdy mamy już zainstalowany openvpn, zajmiemy się generowaniem kluczy. Przedtem, jeżeli nie mamy zainstalowanego instalujemy openssl.

```
root@vpn-blog:~/easy-rsa# apt-get install openssl
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  ca-certificates
The following NEW packages will be installed:
  openssl
```



```
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 701 kB of archives.
After this operation, 1,108 kB of additional disk space will be used.
Get:1 http://debian.wdc.pl/security/wheezy/updates/main openssl amd64
1.0.1e-2+deb7u14 [701 kB]
Fetched 701 kB in 0s (9,615 kB/s)
Selecting previously unselected package openssl.
(Reading database ... 20844 files and directories currently
installed.)
Unpacking openssl (from .../openssl_1.0.1e-2+deb7u14_amd64.deb) ...
Processing triggers for man-db ...
Setting up openssl (1.0.1e-2+deb7u14) ...
```

Następnym krokiem będzie:

```
root@vpn-blog:~# pwd
/root
root@vpn-blog:~# cp -r /usr/share/doc/openvpn/examples/easy-rsa/2.0/
./easy-rsa
root@vpn-blog:~# cd easy-rsa/
```

Dla bezpieczeństwa narzędzia do generowania kluczy warto trzymać w katalogu /root. Dlaczego? Bo tylko root będzie miał do niego dostęp.

Następnie edytujemy plik vars

```
# Increase this to 2048 if you
# are paranoid. This will slow
# down TLS negotiation performance
# as well as the one-time DH parms
# generation process.
export KEY_SIZE=2048

# In how many days should the root CA key expire?
export CA_EXPIRE=3650

# In how many days should certificates expire?
export KEY_EXPIRE=3650
```



```
# These are the default values for fields
# which will be placed in the certificate.
# Don't leave any of these fields blank.
export KEY_COUNTRY="PL"
export KEY_PROVINCE="MAZOWIECKIE"
export KEY_CITY="Warszawa"
export KEY_ORG="S.M.S Security"
export KEY_EMAIL="pht@s-m-s.org.pl"
export KEY_EMAIL=pht@s-m-s.org.pl
export KEY_CN=VPN-Blog
export KEY_NAME=VPN-Blog
export KEY_OU=VPN-Blog
export PKCS11_MODULE_PATH=changeme
export PKCS11_PIN=1234
```

Ustawiamy długość klucza na 2048, bo jesteśmy paranoikami oraz edytujemy ostatnie linie, po to by nie musieć uzupełniać ich za każdym razem jak będziemy generować kolejne klucze dla klientów.

Teraz należy wczytać zmiany, które wprowadziliśmy.

```
root@vpn-blog:~/easy-rsa# source ./vars
NOTE: If you run ./clean-all, I will be doing a rm -rf on /root/easy-
rsa/keys
```

Dla pewności używamy ./clean-all by upewnić się, że nie mamy jakiś przypadkowo wygenerowanych kluczy.

Tworzymy tzw. klucz urzędu certyfikacji CA oraz generujemy klucz Diffiego-Hellmana:

```
root@vpn-blog:~/easy-rsa# ./build-ca
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'ca.key'
-----
You are about to be asked to enter information that will
be incorporated
into your certificate request.
```



What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

```
-----  
Country Name (2 letter code) [PL]:PL  
State or Province Name (full name) [MAZOWIECKIE]:  
Locality Name (eg, city) [Warszawa]:  
Organization Name (eg, company) [S.M.S Security]:  
Organizational Unit Name (eg, section) [VPN-Blog]:  
Common Name (eg, your name or your server's hostname) [VPN-Blog]:  
Name [VPN-Blog]:  
Email Address [pht@s-m-s.org.pl]:  
root@vpn-blog:~/easy-rsa# ./build-dh  
Generating DH parameters, 2048 bit long safe prime, generator 2  
This is going to take a long time  
.....+.....+.....+.....  
[...]  
.....+.....++*++*
```

Generowanie kluczy serwera:

```
root@vpn-blog:~/easy-rsa# ./build-key-server klucz-serwera  
Generating a 2048 bit RSA private key  
.....+++  
.....+++  
writing new private key to 'klucz-serwera.key'
```

You are about to be asked to enter information that will be incorporated into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.



Country Name (2 letter code) [PL]:
State or Province Name (full name) [MAZOWIECKIE]:
Locality Name (eg, city) [Warszawa]:
Organization Name (eg, company) [S.M.S Security]:
Organizational Unit Name (eg, section) [VPN-Blog]:
Common Name (eg, your name or your server's hostname) [klucz-serwera]:
Name [VPN-Blog]:
Email Address [pht@s-m-s.org.pl]:

Please enter the following 'extra' attributes
to be sent with your certificate request

A challenge password []:
An optional company name []:
Using configuration from /root/easy-rsa/openssl-1.0.0.cnf
Check that the request matches the signature
Signature ok

The Subject's Distinguished Name is as follows

```
countryName :PRINTABLE:'PL'  
stateOrProvinceName :PRINTABLE:'MAZOWIECKIE'  
localityName :PRINTABLE:'Warszawa'  
organizationName :PRINTABLE:'S.M.S Security'  
organizationalUnitName:PRINTABLE:'VPN-Blog'  
commonName :PRINTABLE:'klucz-serwera'  
name :PRINTABLE:'VPN-Blog'  
emailAddress :IA5STRING:'pht@s-m-s.org.pl'  
Certificate is to be certified until Jan 14 21:05:35 2025 GMT (3650  
days)  
Sign the certificate? [y/n]:y
```

```
1 out of 1 certificate requests certified, commit? [y/n]y  
Write out database with 1 new entries  
Data Base Updated
```

Następnie generujemy klucze dla naszego klienta.

```
root@vpn-blog:~/easy-rsa# ./build-key client  
Generating a 2048 bit RSA private key  
.....+++
```



```
.....+++  
writing new private key to 'client.key'  
-----  
You are about to be asked to enter information that will  
be incorporated  
into your certificate request.  
What you are about to enter is what is called a Distinguished Name  
or a DN.  
There are quite a few fields but you can leave some blank  
For some fields there will be a default value,  
If you enter '.', the field will be left blank.
```

```
-----  
Country Name (2 letter code) [PL]:  
State or Province Name (full name) [MAZOWIECKIE]:  
Locality Name (eg, city) [Warszawa]:  
Organization Name (eg, company) [S.M.S Security]:  
Organizational Unit Name (eg, section) [VPN-Blog]:  
Common Name (eg, your name or your server's hostname) [client]:  
Name [VPN-Blog]:  
Email Address [pht@s-m-s.org.pl]:
```

```
Please enter the following 'extra' attributes  
to be sent with your certificate request  
A challenge password []:  
An optional company name []:  
Using configuration from /root/easy-rsa/openssl-1.0.0.cnf  
Check that the request matches the signature  
Signature ok
```

```
The Subject's Distinguished Name is as follows  
countryName          :PRINTABLE:'PL'  
stateOrProvinceName  :PRINTABLE:'MAZOWIECKIE'  
localityName         :PRINTABLE:'Warszawa'  
organizationName     :PRINTABLE:'S.M.S Security'  
organizationalUnitName:PRINTABLE:'VPN-Blog'  
commonName           :PRINTABLE:'client'  
name                 :PRINTABLE:'VPN-Blog'  
emailAddress         :IA5STRING:'pht@s-m-s.org.pl'  
Certificate is to be certified until Jan 14 21:20:16 2025 GMT (3650
```




days)

Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y

Write out database with 1 new entries

Data Base Updated

root@vpn-blog:~/

Kiedy już wygenerowaliśmy na tą chwilę potrzebne nam klucze. Warto dać upust swojej paranoicznej naturze i zwiększyć stopień bezpieczeństwa. Utworzymy dodatkowy klucz dla mechanizmu *tls-auth*, którego głównym zadaniem jest odrzucanie na wczesnym etapie połączeń od nieautoryzowanych klientów. Dzięki niemu uzyskamy również dodatkową ochronę przed podatnościami typu przepełnienie bufora, występującymi w implementacji protokołu SSL/TLS.

```
root@vpn-blog:~/easy-rsa# openssl genrsa -out ta.key
```

```
root@vpn-blog:~/easy-rsa# mv ta.key keys/
```

Teraz czas na skopiowanie kluczy w odpowiednie miejsca.

```
cp keys/ca.crt /etc/openvpn/
```

```
cp keys/klucz-serwera.crt /etc/openvpn/
```

```
cp keys/klucz-serwera.key /etc/openvpn/
```

```
cp keys/dh2048.pem /etc/openvpn/dh.pem
```

```
cp keys/ta.key /etc/openvpn/
```

Teraz należy stworzyć plik konfiguracyjny.

```
root@vpn-blog:~/easy-rsa# cd /etc/openvpn/
```

```
root@vpn-blog:/etc/openvpn# nano openvpn.conf
```

Może on wyglądać tak:

```
port 1194
```

```
proto udp
```

```
dev tun
```

```
ca ca.crt
```

```
cert klucz-serwera.crt
```

```
key klucz-serwera.key
```



```
dh dh.pem
server 6.6.6.0 255.255.255.0
keepalive 10 120
tls-auth ta.key 0
comp-lzo
user nobody
cipher AES-256-CBC
group nogroup
persist-key
persist-tun
log-append openvpn.log
verb 3
mute 10
```

Następująco uruchamiamy translacje adresów, aby nasz serwer był bramką do internetu.

```
root@vpn-blog:/etc/openvpn# sed -i "/exit 0/d" /etc/rc.local
root@vpn-blog:/etc/openvpn# echo "/sbin/iptables -t nat -A POSTROUTING
-o eth0 -j MASQUERADE" >> /etc/rc.local
root@vpn-blog:/etc/openvpn# echo "exit 0" >> /etc/rc.local
root@vpn-blog:/etc/openvpn# /etc/rc.local
root@vpn-blog:/etc/openvpn# echo "net.ipv4.conf.all.forwarding = 1" >>
/etc/sysctl.conf
root@vpn-blog:/etc/openvpn# sysctl -p
net.ipv4.conf.all.forwarding = 1
```

Dodajemy do pliku konfiguracyjnego

```
push "redirect-gateway def1"
push "dhcp-option DNS 8.8.8.8" #serwery dns google
push "dhcp-option DNS 8.8.4.4"
```

I uruchamiamy usługę.

```
/etc/init.d/openvpn start
```



Kilka praktycznych uwag dotyczących połączeń VPN.

Jak już pisałem, z VPN'a można korzystać z różnych powodów. W domu, pracy, miejscach publicznych. Powyższa konfiguracja jest dobra gdy korzystamy w domu do łączenia się firmą, do łączenia komputera w firmie do naszej domowej sieci czy też do logowania do banku w publicznych sieciach. Można też wykorzystać tego typu połączenie do zestawiania bezpiecznych połączeń z serwerami backupów, bazodanowymi czy deweloperskimi, które nie mają wyjścia na świat innego niż vpn. Oczywiście przede wszystkim VPN pozwoli nam omijać wszelaką cenzurę. Gdy mówimy o cenzurze w firmie, np na facebooka, należy skonfigurować nasz VPN na port 443, ponieważ pozostałe mogą być wycięte na firewallu. Natomiast jeżeli nasza siedziba firmy jest chroniona poprzez Next Generation Firewall taki jak PaloAlto... Cóż wiele nie zdziałamy, ale o tym w osobnym artykule.

Jeżeli, ktoś chce anonimizować swoją tożsamość a nie ją chronić przed kradzieżą, polecam mu sieć TOR. Można też korzystać z sieci vpn'ów [SecurityKiss](#). Ale jaki sens ma posiadanie vpn'a wspólnego z ludźmi, których nawet nie znamy.

Konfiguracja klienta - Windows

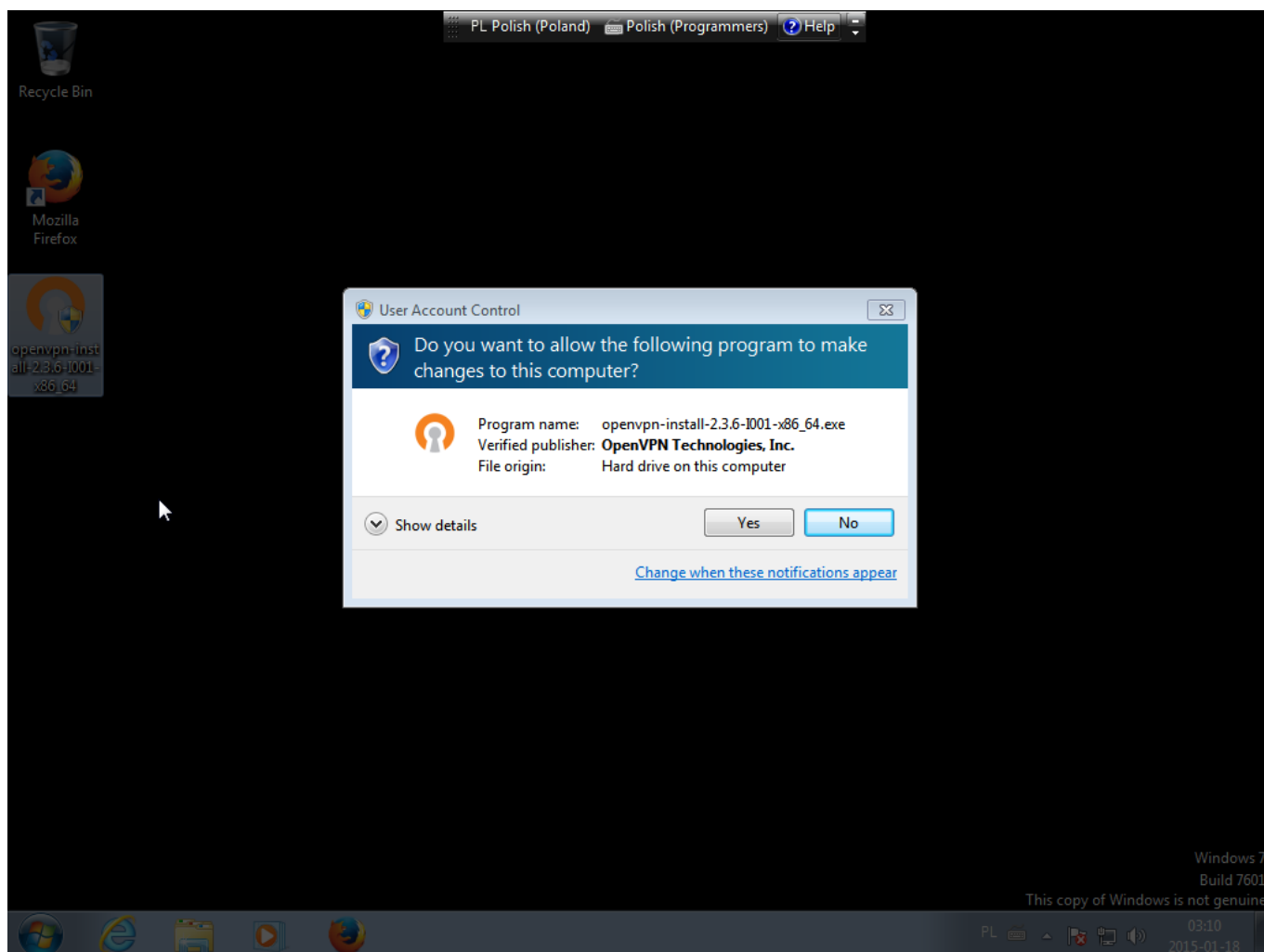
Przyszedł czas na konfigurację klienta. Zaczniemy od pobrania [klienta](#) openvpna z gui, ułatwi to nam prace.

Po pobraniu, zajmijmy się instalacją.

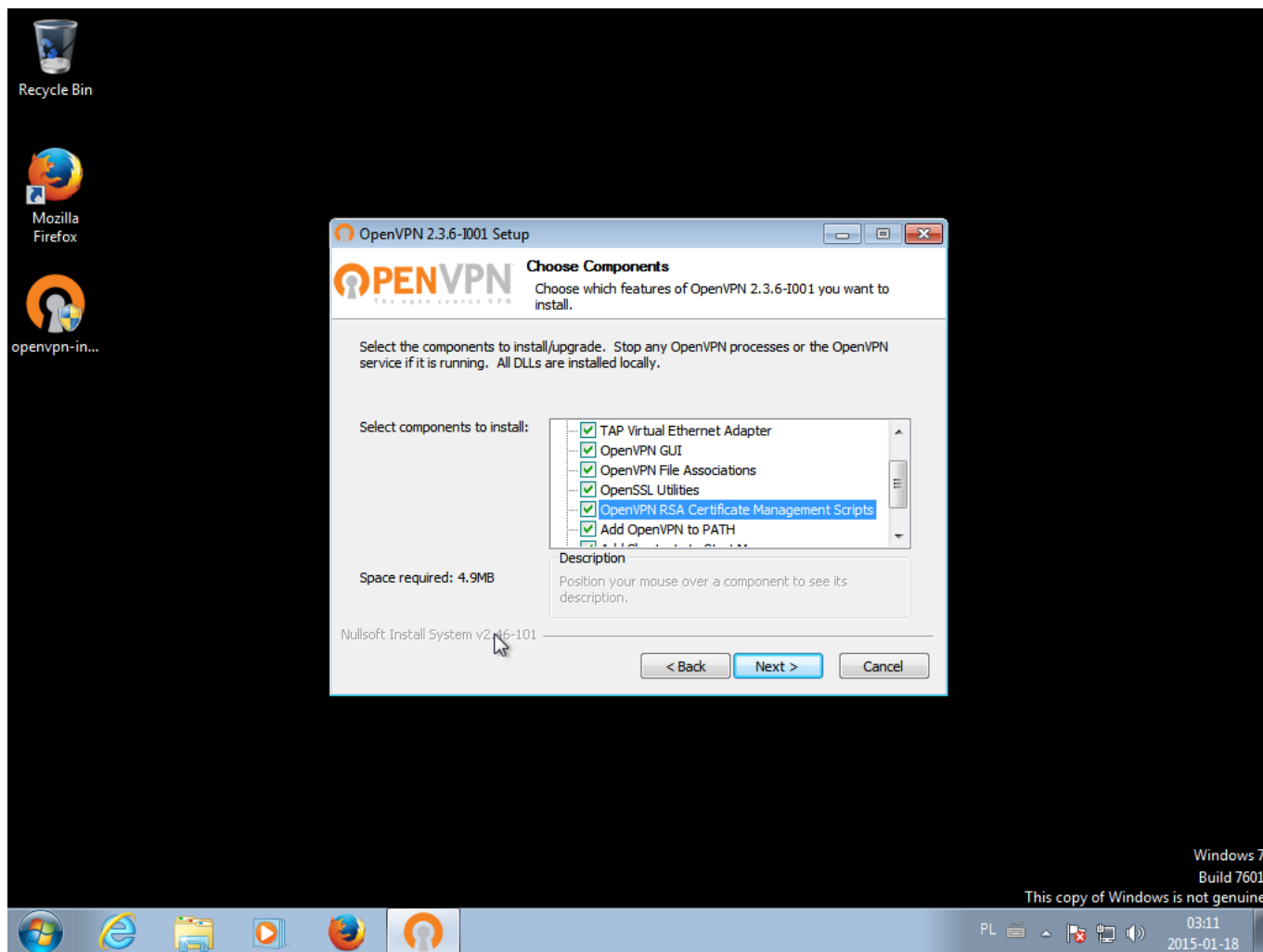
Uwaga, w przypadku windows 7 i wyżej należy instalacje oraz program uruchamiać z prawami administratora.



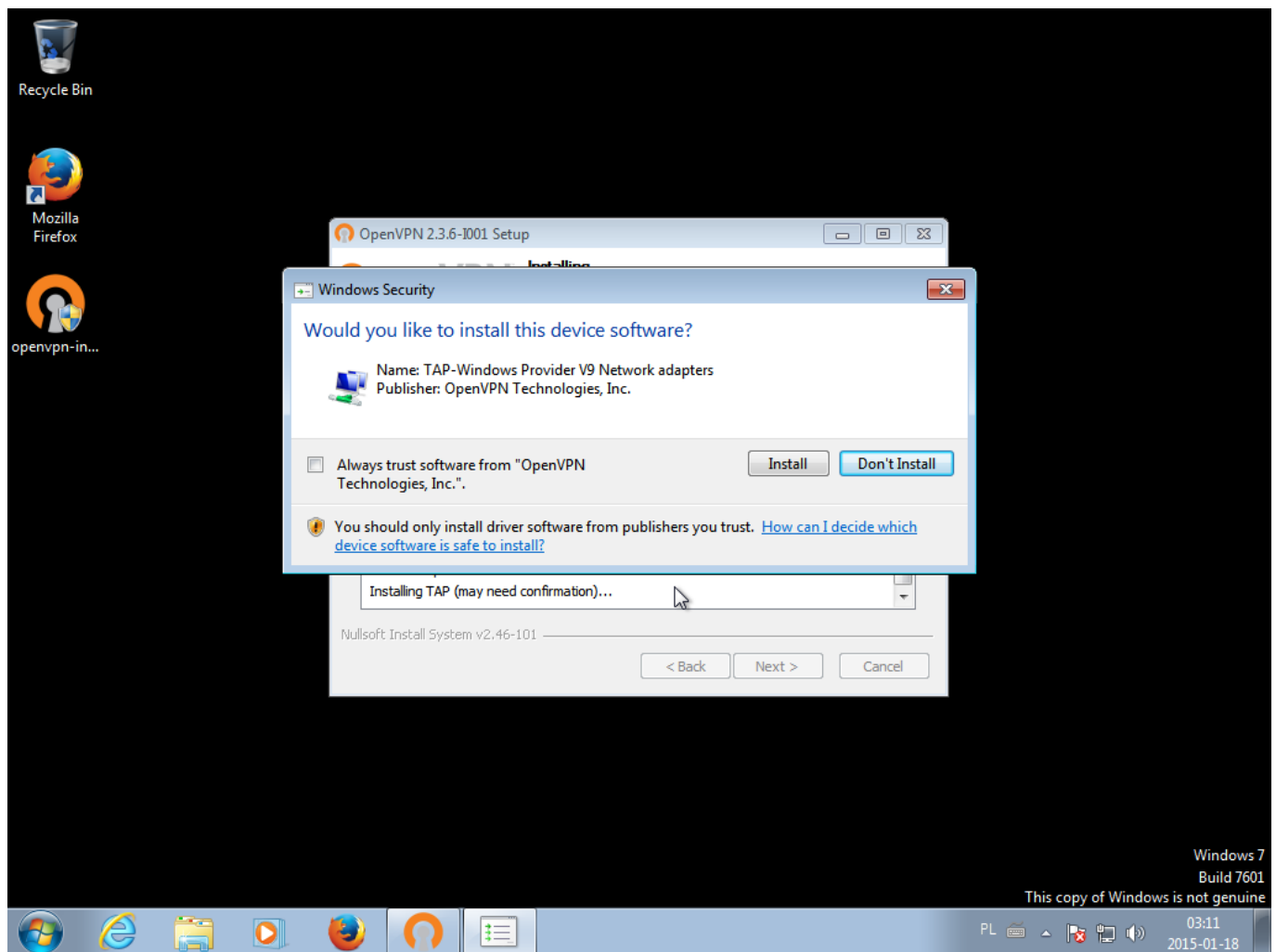
Sposób na MITM? - VPN!



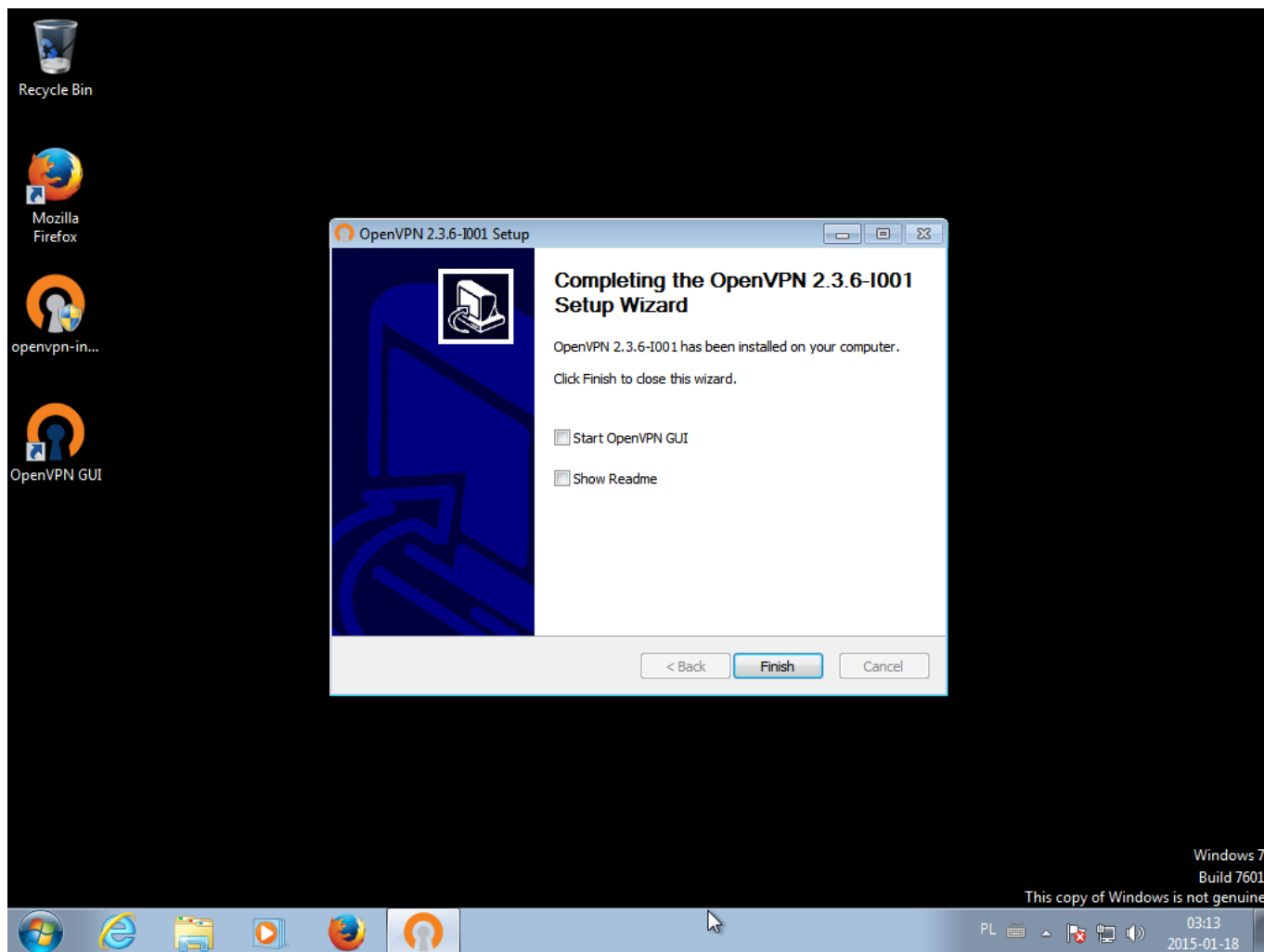
Zaznaczamy wszystkie okienka przy instalacji.



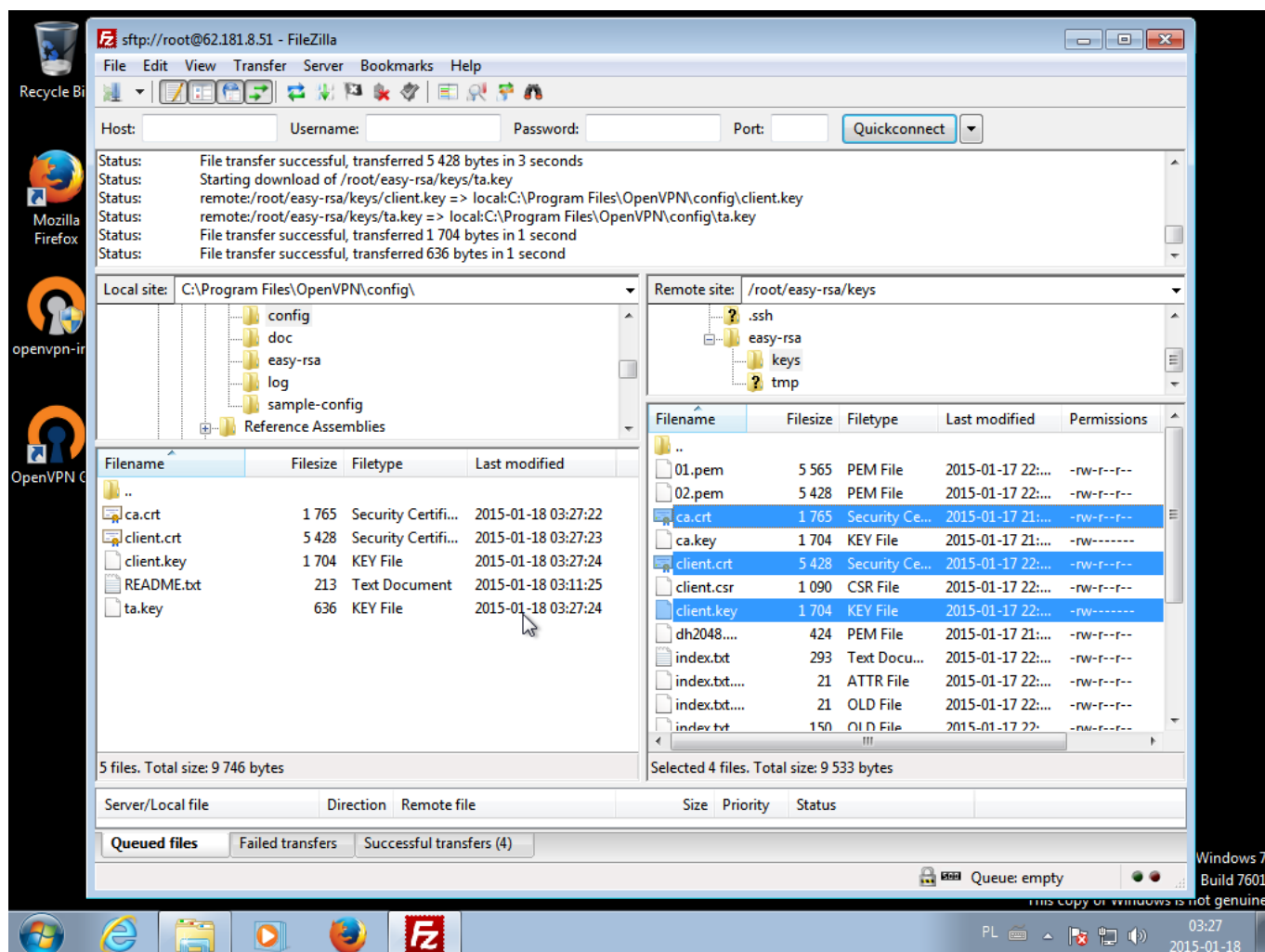
Instalujemy interfejs sieciowy, który będzie interfejsem tunelu.



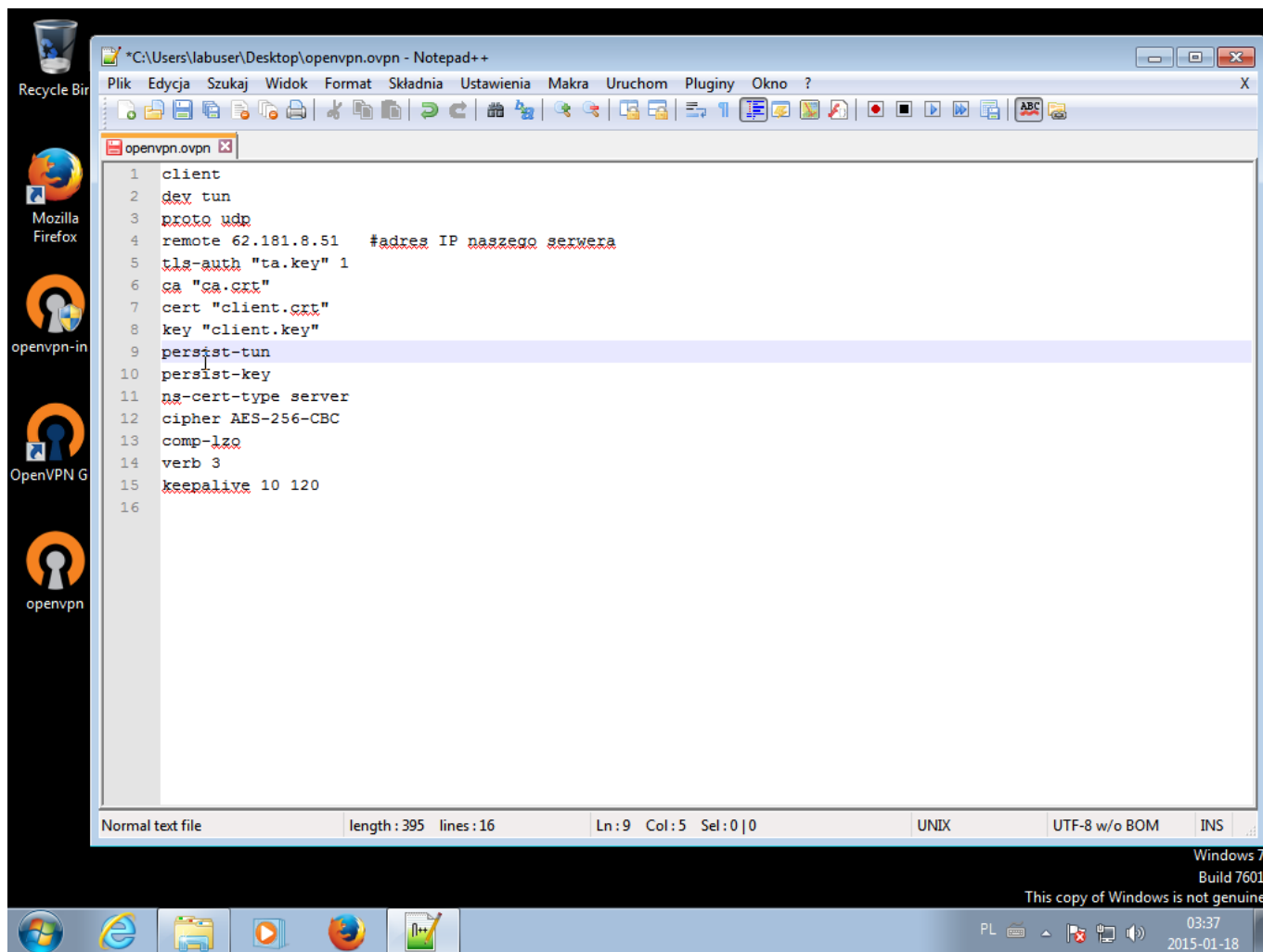
Po instalacji nie uruchamiamy naszego klienta.



Do katalogu w którym zainstalowaliśmy Openvpn w folderze config wrzucamy ca.crt, client.crt, client.key oraz ta.key.



Przygotowujemy plik konfiguracyjny openvpn.



The screenshot shows a Windows 7 desktop environment. A Notepad++ window is open, displaying the configuration for an OpenVPN client. The configuration file is named 'openvpn.ovpn' and is located at 'C:\Users\labuser\Desktop\openvpn.ovpn'. The configuration includes settings for the client mode, protocol (UDP), remote server IP (62.181.8.51), authentication key, certificates, and various security and performance options like cipher, compression, and keepalive.

```
1 client
2 dev tun
3 proto udp
4 remote 62.181.8.51 #adres IP naszego serwera
5 tls-auth "ta.key" 1
6 ca "ca.crt"
7 cert "client.crt"
8 key "client.key"
9 persist-tun
10 persist-key
11 ns-cert-type server
12 cipher AES-256-CBC
13 comp-lzo
14 verb 3
15 keepalive 10 120
16
```

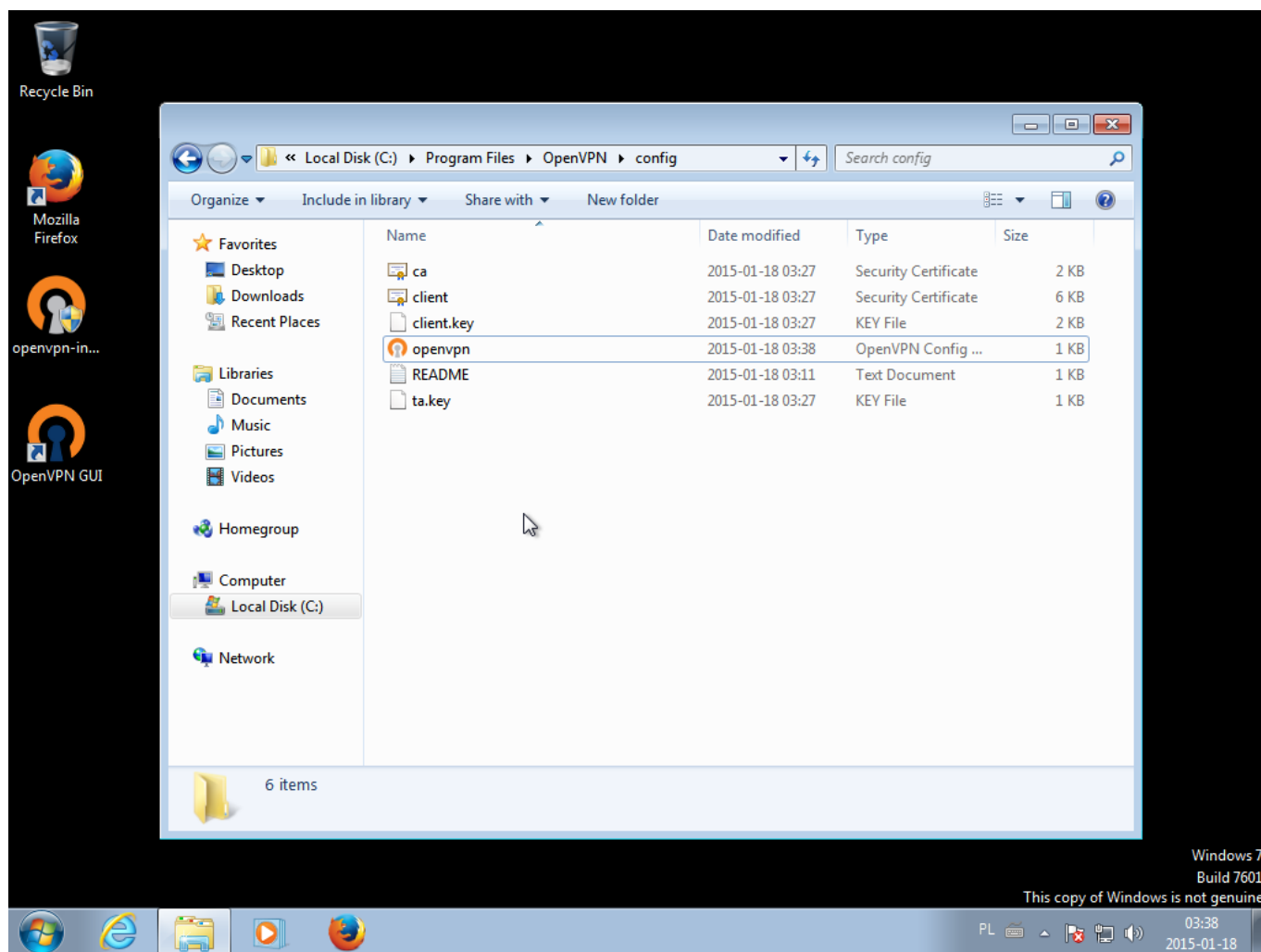
The status bar at the bottom of the Notepad++ window indicates: Normal text file, length: 395, lines: 16, Ln: 9, Col: 5, Sel: 0 | 0, UNIX, UTF-8 w/o BOM, INS.

The Windows taskbar at the bottom shows the system tray with the date 2015-01-18 and time 03:37. A watermark at the bottom right reads: "This copy of Windows is not genuine".

Plik z konfiguracją umieszczamy w katalogu config.



Sposób na MITM? - VPN!

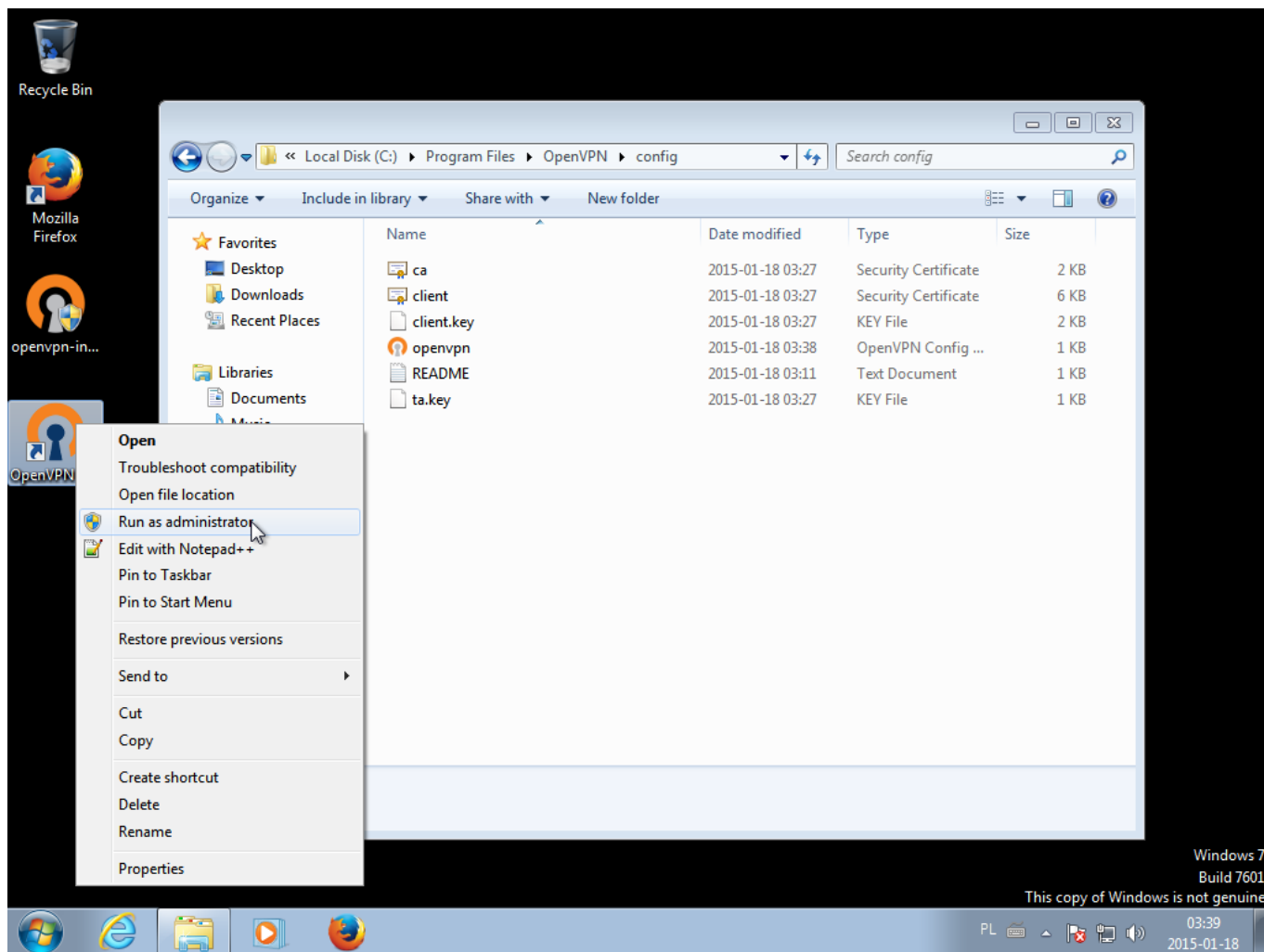


Sprawdźmy teraz nasze ip.

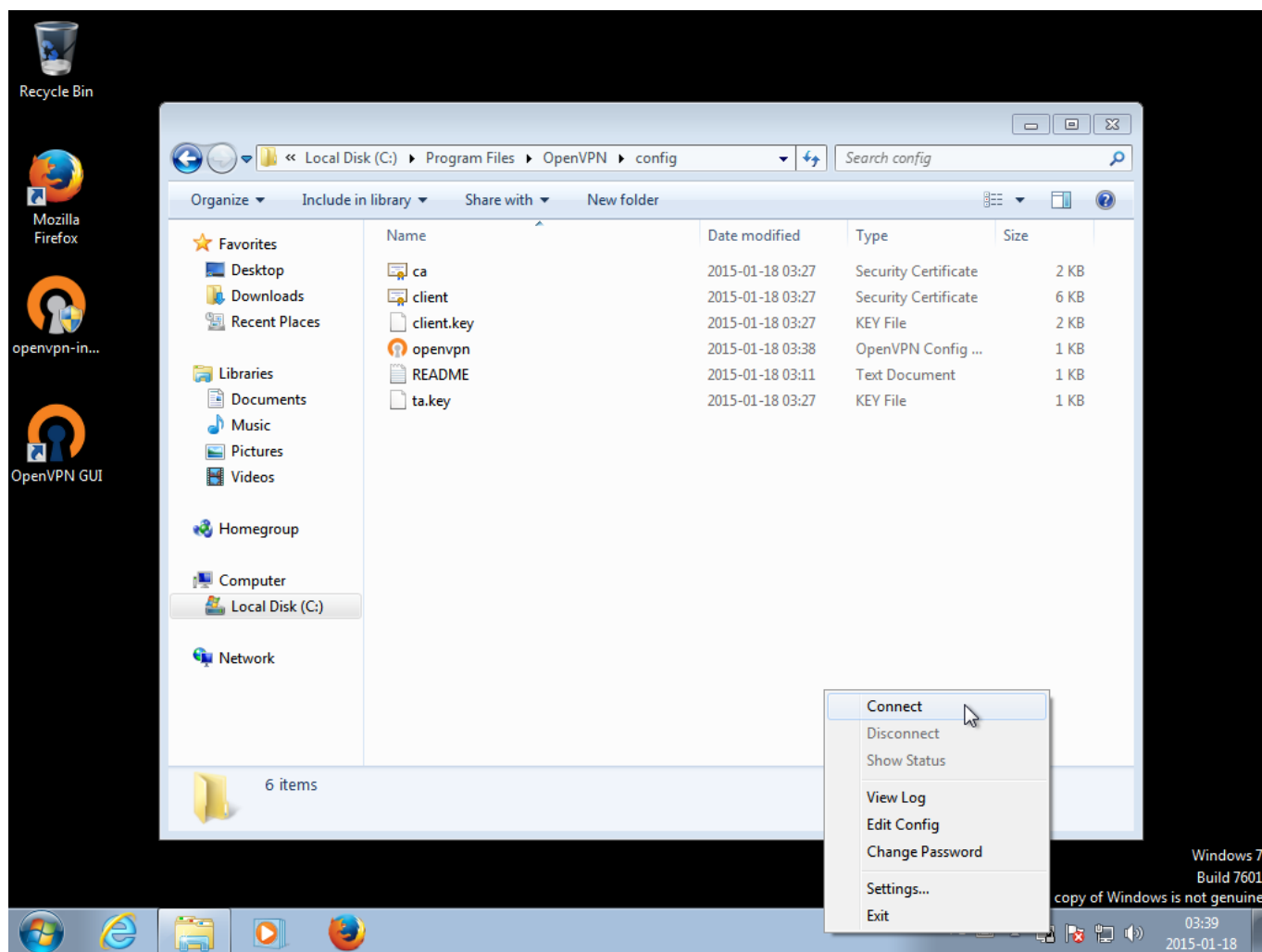


The screenshot shows a web browser window displaying the website www.pokapoka.pl. The page title is "Moje IP na POKAPOKA.PL" and the main heading is "Sprawdź swoje IP". The browser's address bar shows the URL and the search engine is set to Google. The website content includes a navigation menu with links like "Moje ip", "Szczegółowe info IP", "Rodzaj IP", "Co to jest IP", "IP na mojej stronie", "Sprawdzanie Hostów", and "Kontakt". The main content area displays the user's IPv4 address: **94.254.129.58**. Below the IP address, there are links for "Informacja", "Moje ip", "Zmiana ip", "Ip adres", and "Test my ip". A green text box asks "[Moje IP jest Zewnętrzne czy Wewnętrzne?] Kliknij aby sprawdzić". A section titled "Moje IP: Podstawowe informacje:" lists system details: Host: user-94-254-129-58.play-internet.pl, System: Windows 7, Przeglądarka: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:34.0) Gecko/20100101 Firefox/34.0, Referer: (empty), and Proxy: Nie wykryto PROXY bądź Twoje PROXY jest całkowicie anonimowe. A sidebar on the left contains promotional text: "Teraz wszystko co kochasz jest w UPC!", "TV + INTERNET + ponad 1000 filmów i seriali", and "50% taniej przez 3 m-cie". A bottom banner for "Microsoft Cloud OS" is also visible. The Windows taskbar at the bottom shows the system tray with the date 2015-01-18 and time 03:44.

Uruchamiamy klienta openvpn jako administrator.



Na pasku pojawiła się nam ikonka połączenia vpn. Klikamy prawym na „Connect”.



W pojawiającym się oknie ujrzymy logi połączenia i ewentualne informacje o błędach.



Sposób na MITM? - VPN!

```
OpenVPN Connection (openvpn)
Current State: Connecting
Sun Jan 18 05:00:19 2015 OpenVPN 2.3.6 x86_64-w64-mingw32 [SSL (OpenSSL)] [LZO] [PKCS11] [IPv6] built on Dec 1 2014
Sun Jan 18 05:00:19 2015 library versions: OpenSSL 1.0.1j 15 Oct 2014, LZO 2.08
Sun Jan 18 05:00:19 2015 MANAGEMENT: TCP Socket listening on [AF_INET]127.0.0.1:25340
Sun Jan 18 05:00:19 2015 Need hold release from management interface, waiting...
Sun Jan 18 05:00:20 2015 MANAGEMENT: Client connected from [AF_INET]127.0.0.1:25340
Sun Jan 18 05:00:20 2015 MANAGEMENT: CMD 'state on'
Sun Jan 18 05:00:20 2015 MANAGEMENT: CMD 'log all on'
Sun Jan 18 05:00:20 2015 MANAGEMENT: CMD 'hold off'
Sun Jan 18 05:00:20 2015 MANAGEMENT: CMD 'hold release'
Sun Jan 18 05:00:20 2015 Control Channel Authentication: using 'ta.key' as a OpenVPN static key file
Sun Jan 18 05:00:20 2015 Outgoing Control Channel Authentication: Using 160 bit message hash 'SHA1' for HMAC authentication
Sun Jan 18 05:00:20 2015 Incoming Control Channel Authentication: Using 160 bit message hash 'SHA1' for HMAC authentication
Sun Jan 18 05:00:20 2015 Socket Buffers: R=[8192->8192] S=[8192->8192]
Sun Jan 18 05:00:20 2015 UDPv4 link local (bound): [undef]
Sun Jan 18 05:00:20 2015 UDPv4 link remote: [AF_INET]62.181.8.51:1194
Sun Jan 18 05:00:20 2015 MANAGEMENT: >STATE:1421553620,WAIT,...
Sun Jan 18 05:00:20 2015 MANAGEMENT: >STATE:1421553620,AUTH,...
Sun Jan 18 05:00:20 2015 TLS: Initial packet from [AF_INET]62.181.8.51:1194, sid=00d783ef 1cf32183
Sun Jan 18 05:00:22 2015 VERIFY OK: depth=1, C=PL, ST=MAZOWIECKIE, L=Warszawa, O=S.M.S Security, OU=VPN-Blog, CN=VPN-Blog, name=VPN-Blog, emailAddress=pht@s-m-s.org.pl
Sun Jan 18 05:00:22 2015 VERIFY OK: nsCertType=SERVER
Sun Jan 18 05:00:22 2015 VERIFY OK: depth=0, C=PL, ST=MAZOWIECKIE, L=Warszawa, O=S.M.S Security, OU=VPN-Blog, CN=kucz-serwera, name=VPN-Blog, emailAddress=pht@s-m-s.org.pl
Sun Jan 18 05:00:25 2015 Data Channel Encrypt: Cipher 'AES-256-CBC' initialized with 256 bit key
Sun Jan 18 05:00:25 2015 Data Channel Encrypt: Using 160 bit message hash 'SHA1' for HMAC authentication
Sun Jan 18 05:00:25 2015 Data Channel Decrypt: Cipher 'AES-256-CBC' initialized with 256 bit key
Sun Jan 18 05:00:25 2015 Data Channel Decrypt: Using 160 bit message hash 'SHA1' for HMAC authentication
Sun Jan 18 05:00:25 2015 Control Channel: TLSv1, cipher TLSv1/SSLv3 DHE-RSA-AES256-SHA, 2048 bit RSA
Sun Jan 18 05:00:25 2015 [kucz-serwera] Peer Connection Initiated with [AF_INET]62.181.8.51:1194
Sun Jan 18 05:00:26 2015 MANAGEMENT: >STATE:1421553626,GET_CONFIG,...
Sun Jan 18 05:00:27 2015 SENT CONTROL [kucz-serwera]: 'PUSH_REQUEST' (status=1)
Sun Jan 18 05:00:27 2015 PUSH: Received control message: 'PUSH_REPLY,redirect-gateway def1,dhcp-option DNS 8.8.8.8,dhcp-option DNS 8.8.4.4,route 6.6.6.1,topology net30,ping 10,ping-restart 120,fc
Sun Jan 18 05:00:27 2015 OPTIONS IMPORT: timers and/or timeouts modified
Sun Jan 18 05:00:27 2015 OPTIONS IMPORT: -ifconfig/up options modified
Sun Jan 18 05:00:27 2015 OPTIONS IMPORT: route options modified
Sun Jan 18 05:00:27 2015 OPTIONS IMPORT: -ip-win32 and/or -dhcp-option options modified
Sun Jan 18 05:00:27 2015 do_ifconfig, tt->ipv6=0, tt->did_ifconfig_ipv6_setup=0
Sun Jan 18 05:00:27 2015 MANAGEMENT: >STATE:1421553627,ASSIGN_IP,,6.6.6.6,
Sun Jan 18 05:00:27 2015 open_tun, tt->ipv6=0
Sun Jan 18 05:00:27 2015 TAP-WIN32 device [Local Area Connection 2] opened: \\.\Global\{69854EEA-D4A8-4048-BD3A-3FEC1F60BBFC}.tap
Sun Jan 18 05:00:27 2015 TAP-Windows Driver Version 9.9
Sun Jan 18 05:00:27 2015 Notified TAP-Windows driver to set a DHCP IP/netmask of 6.6.6.6/255.255.255.252 on interface {69854EEA-D4A8-4048-BD3A-3FEC1F60BBFC} [DHCP-serv: 6.6.6.5, lease-time: 3
Sun Jan 18 05:00:27 2015 Successful ARP Flush on interface [16] {69854EEA-D4A8-4048-BD3A-3FEC1F60BBFC}
```

Disconnect Reconnect Hide

05:00 2015-01-18

Po udanym połączeniu, sprawdzamy nasze ip. Udało się, teraz nasz ruch jest kierowany przez vpn.

The screenshot shows a web browser window at the URL www.pokapoka.pl. The page title is "Moje Ip na POKAPOKA.PL". The main content area displays the user's IPv4 address as **62.181.8.51**. Below the IP address, there are navigation links: "Informacja", "Moje ip", "Zmiana ip", "Ip adres", and "Test my ip". A green text prompt asks "[Moje IP jest Zewnętrzne czy Wewnętrzne?] Kliknij aby sprawdzić".

Below the IP information, there is a section titled "Moje IP: Podstawowe informacje:" with the following details:

Host:	vpn-blog.srv.rootbox.com
System:	Windows 7
Przeglądarka:	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:34.0) Gecko/20100101 Firefox/34.0
Referer:	
Proxy:	Nie wykryto PROXY bądź Twoje PROXY jest całkowicie anonimowe

There is also a "Pokaż Dodatkowe Informacje" button and a note: "(wysyłane nagłówki HTTP, dane usługodawcy internetowego, lokalizację itd...)" and "Pobieranie informacji może zająć kilka chwil!".

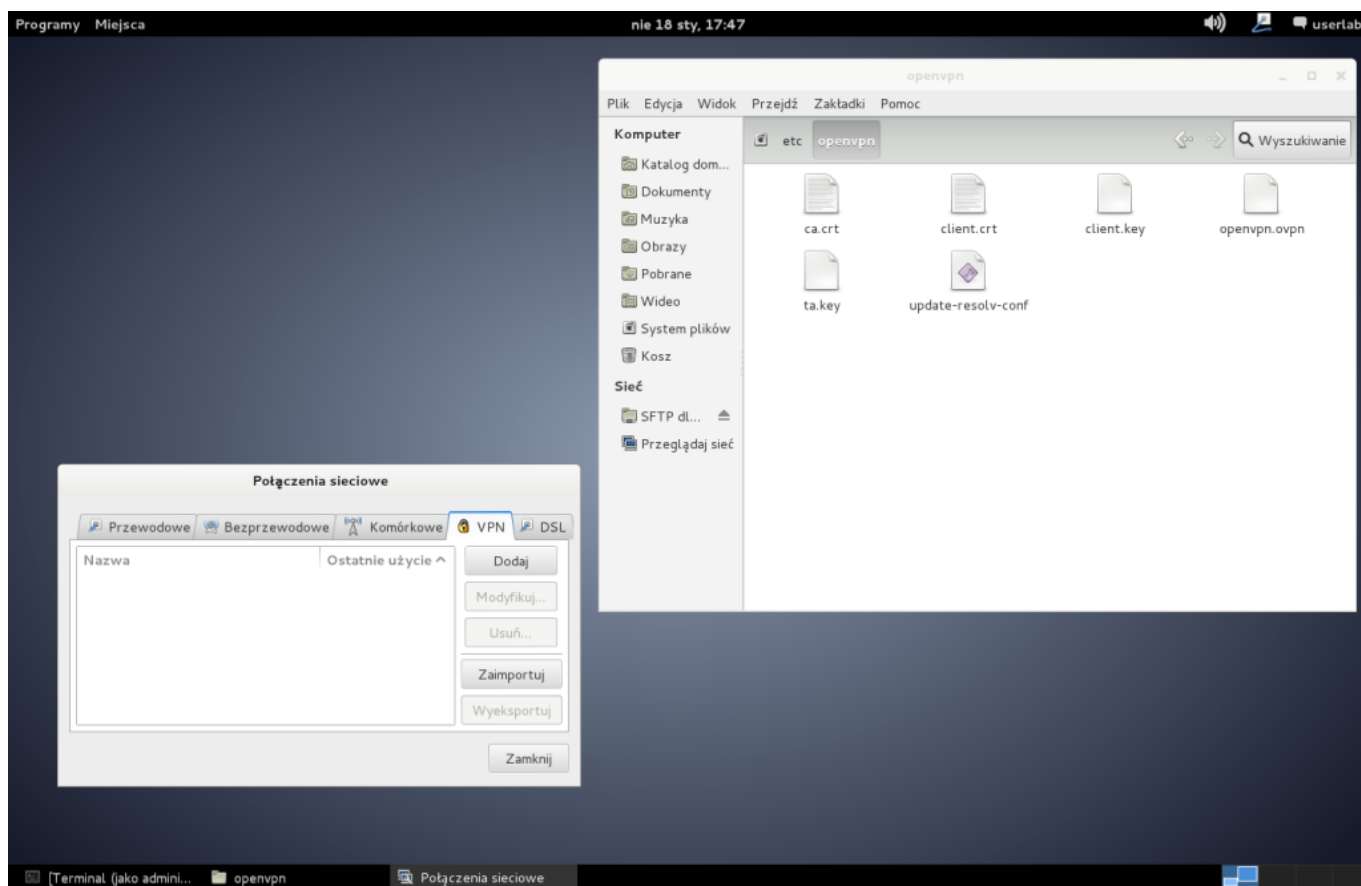
On the left side of the page, there is a "TRADING 212" advertisement with buttons for FOREX, ZŁOTO, ROPA, and AKCJE, and a "KONTO DEMO z 50 000 zł" offer. On the right side, there are advertisements for MITSUBISHI MOTORS and ASX I OUTLAND LIMITOWA EDYCJA FISCHE.

Konfiguracja klienta - Linux (Debian, gnome)

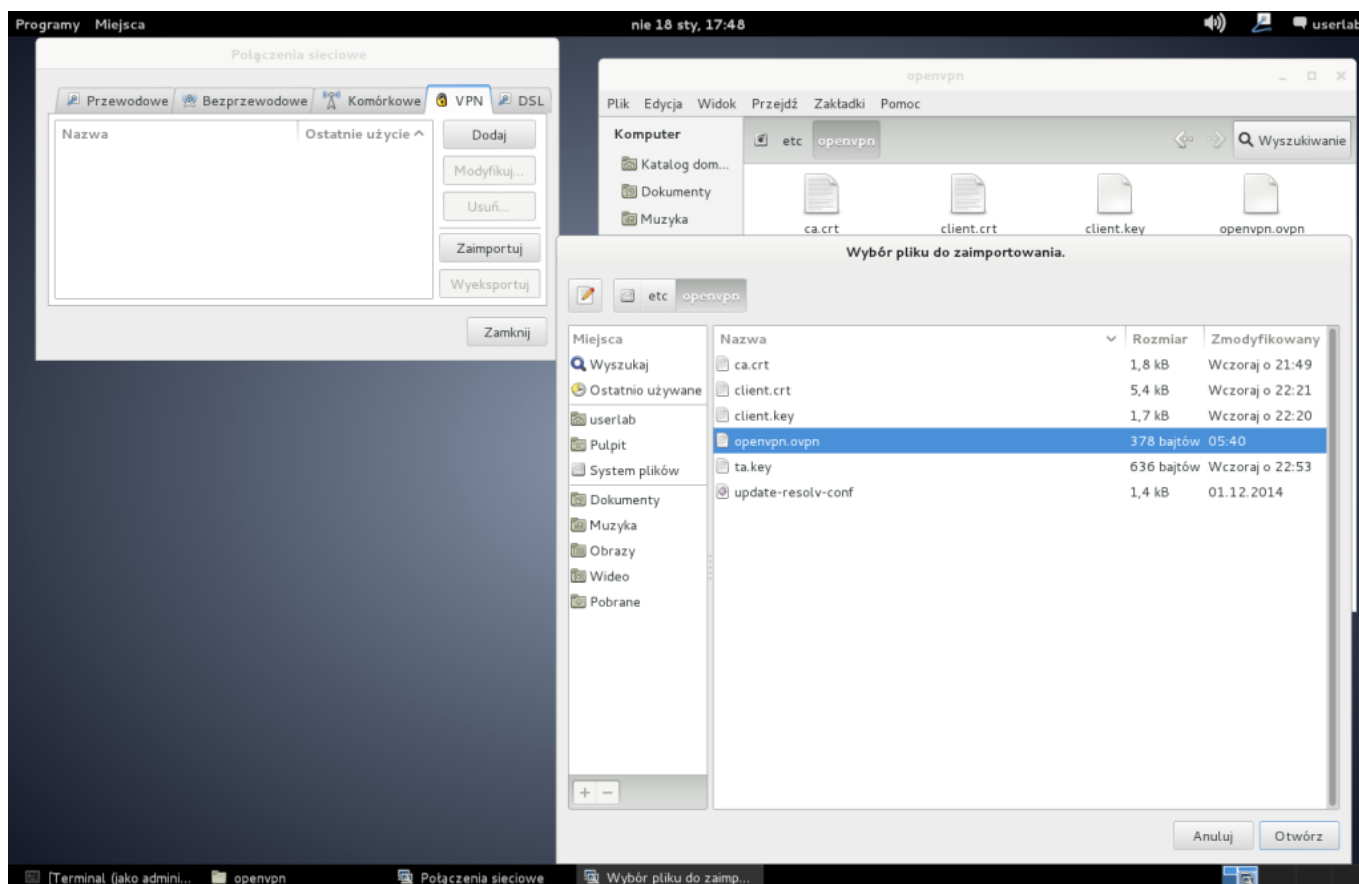
Zaczynamy od instalacji pakietów o ile już ich nie mamy. Oczywiście

```
apt-get install openvpn network-manager-openvpn-gnome
```

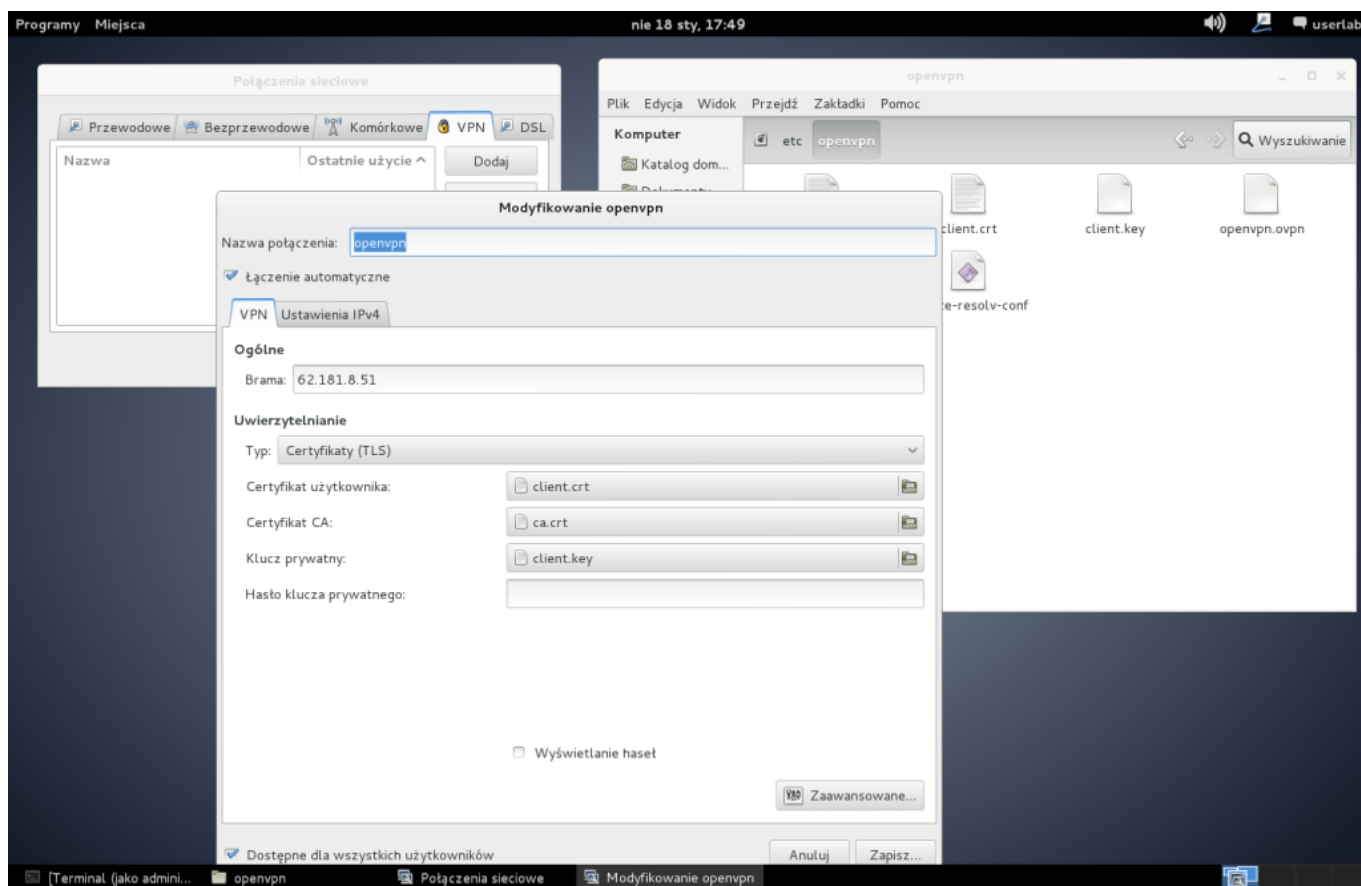
Otwieramy networkmanager'a -> zakładka VPN -> zaimportuj.



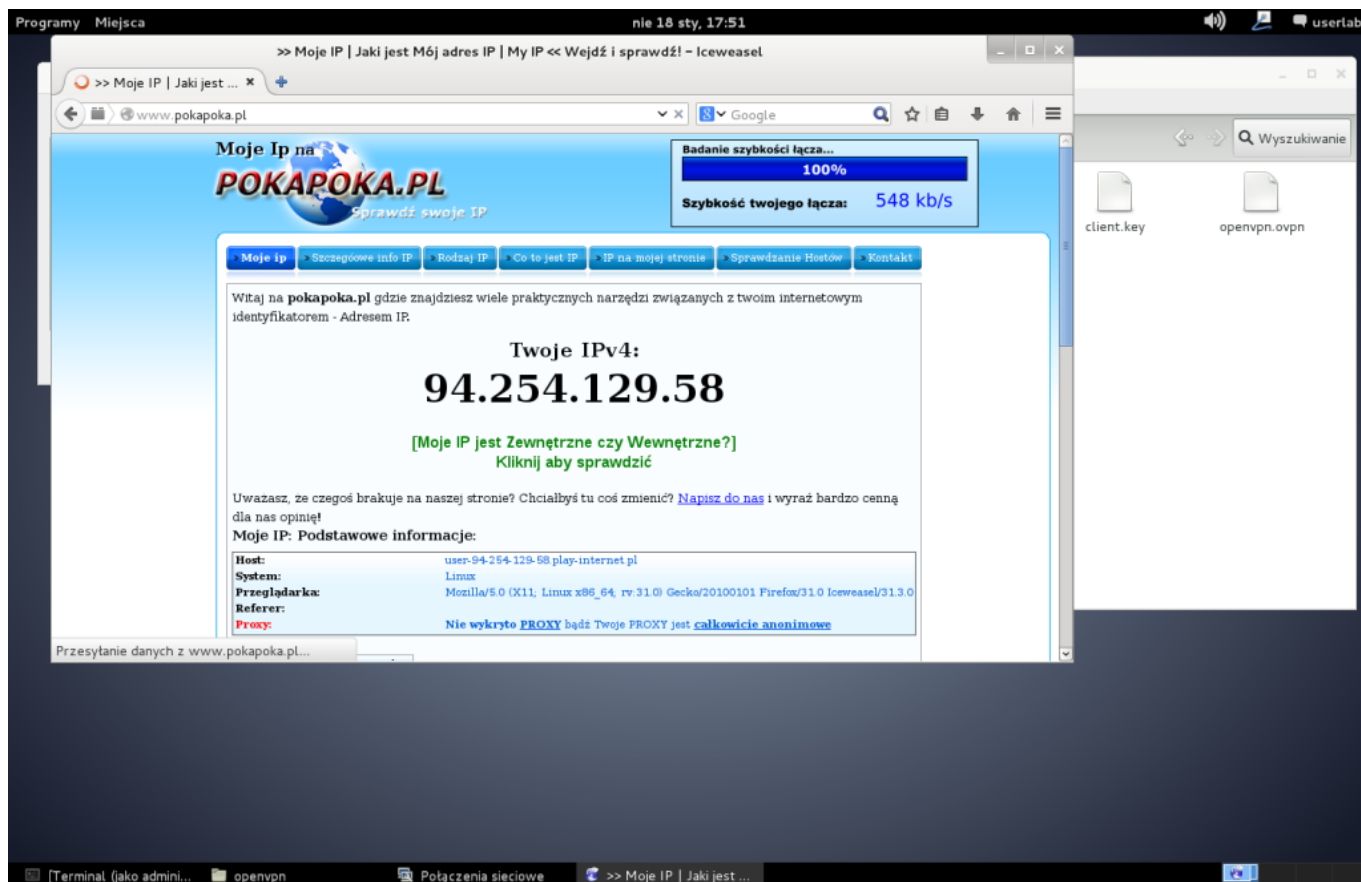
Znajdujemy ca.crt, client.crt, client.key oraz ta.key, które pobraliśmy z serwera vpn.
Wybieramy plik konfiguracji .ovpn



Klikamy zapisz.



Sprawdźmy teraz nasze IP przed połączeniem się do vpn'a.



Uruchamiamy połączenie VPN i czekamy na efekty



Sposób na MITM? - VPN!

The screenshot shows a Linux desktop environment. In the top right corner, a network menu is open, showing options for 'Sieć przewodowa' (Wired connection 1) and 'Połączenia VPN' (VPN connections). The 'Połączenia VPN' submenu is expanded, showing 'openvpn', 'Skonfiguruj VPN...', and 'Rozłącz VPN'. In the center, a web browser window is open to 'www.pokapoka.pl'. The page displays the user's IPv4 address as '94.254.129.58' and a connection speed of '548 kb/s'. Below the IP address, there is a table of system information:

Moje IP: Podstawowe informacje:	
Host:	user-94-254-129-58 play-internet.pl
System:	Linux
Przeglądarka:	Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.3.0
Referer:	
Proxy:	Nie wykryto PROXY bądź Twoje PROXY jest całkowicie anonimowe

Po chwili ukazuje się naszym oczom komunikat o tym, że połączenie zostało nawiązane.



Sposób na MITM? - VPN!

The screenshot shows a Linux desktop environment. In the top right corner, a notification bubble reads: "Wiadomość logowania VPN" and "VPN connection has been successfully established." Below the notification, it says "Nie wyświetlaj tego komunikatu ponownie".

The main window is a web browser displaying the website "Moje IP na POKAPOKA.PL". The browser's address bar shows "www.pokapoka.pl". The website's header includes a navigation menu with items like "Moje ip", "Szczegółowe info IP", "Rodzaj IP", "Co to jest IP", "IP na mojej stronie", "Sprawdzenie Hostów", and "Kontakt".

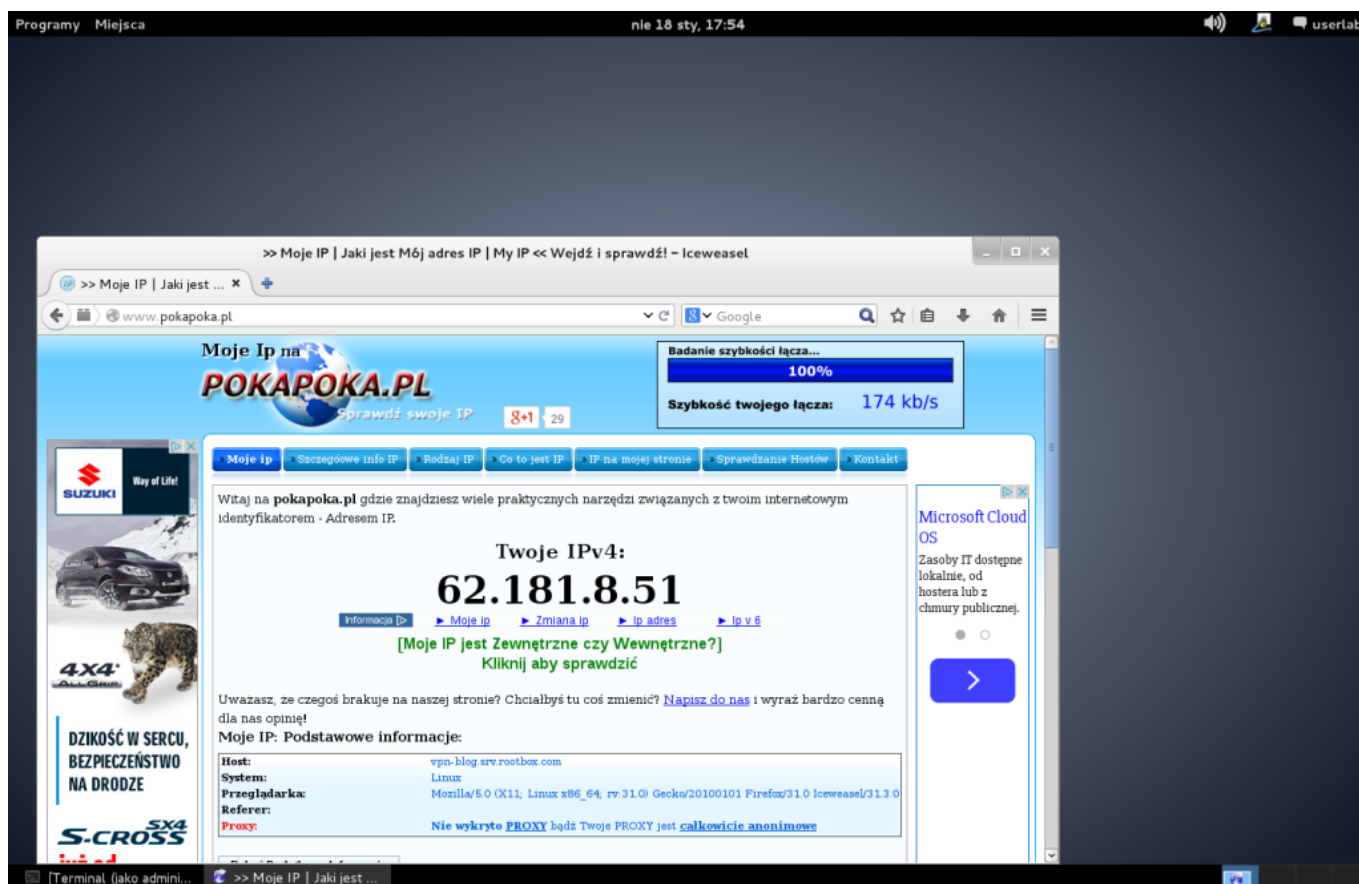
The main content of the website displays the user's IPv4 address: **94.254.129.58**. Below the address, it says "[Moje IP jest Zewnętrzne czy Wewnętrzne?]" and "Kliknij aby sprawdzić".

Below the IP address, there is a section titled "Moje IP: Podstawowe informacje:" with the following details:

Host:	user-94-254-129-58.play-internet.pl
System:	Linux
Przeładowarka:	Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.3.0
Referer:	
Proxy:	Nie wykryto PROXY bądź Twoje PROXY jest całkowicie anonimowe

On the left side of the website, there is a Suzuki advertisement for the S-CROSS SX4, with the text "już od 59 900 zł". On the right side, there is an advertisement for "Napięcie rośnie w pakiecie Multimedia" and "6 miesięcy bez opłat! WPAKIECIE Z PRADEM".

Ponownie sprawdzamy ip i widzimy, że identyfikujemy się za pomocą ip VPN'a, więc udało się nam.



Pro-tip na zwiększenie bezpieczeństwa.

Domyślcie się, że tak naprawdę najsłabszym ogniwem naszego vpn'a jest port 22 wystawiony na public. Zmienimy więc trochę ustawienia ssh.

```
echo "ListenAddress 6.6.6.1" >> /etc/ssh/sshd_config  
netstat -tlnp
```

Teraz do ssh mamy dostęp jedynie podczas połączenia vpn i tylko wtedy.

Atak MITM.

O [MITM](#) już pisałem w jednym z poprzednich artykułów. Dziś ten sam atak przeprowadzimy na ofiarę, która jest połączona do VPN'a. Jak ustaliliśmy w poprzednim artykule o MITM,

w sytuacji gdy intruz i ofiara są w tej samej sieci atak ten jest łatwy do wykonania.

Kilka danych na początek.

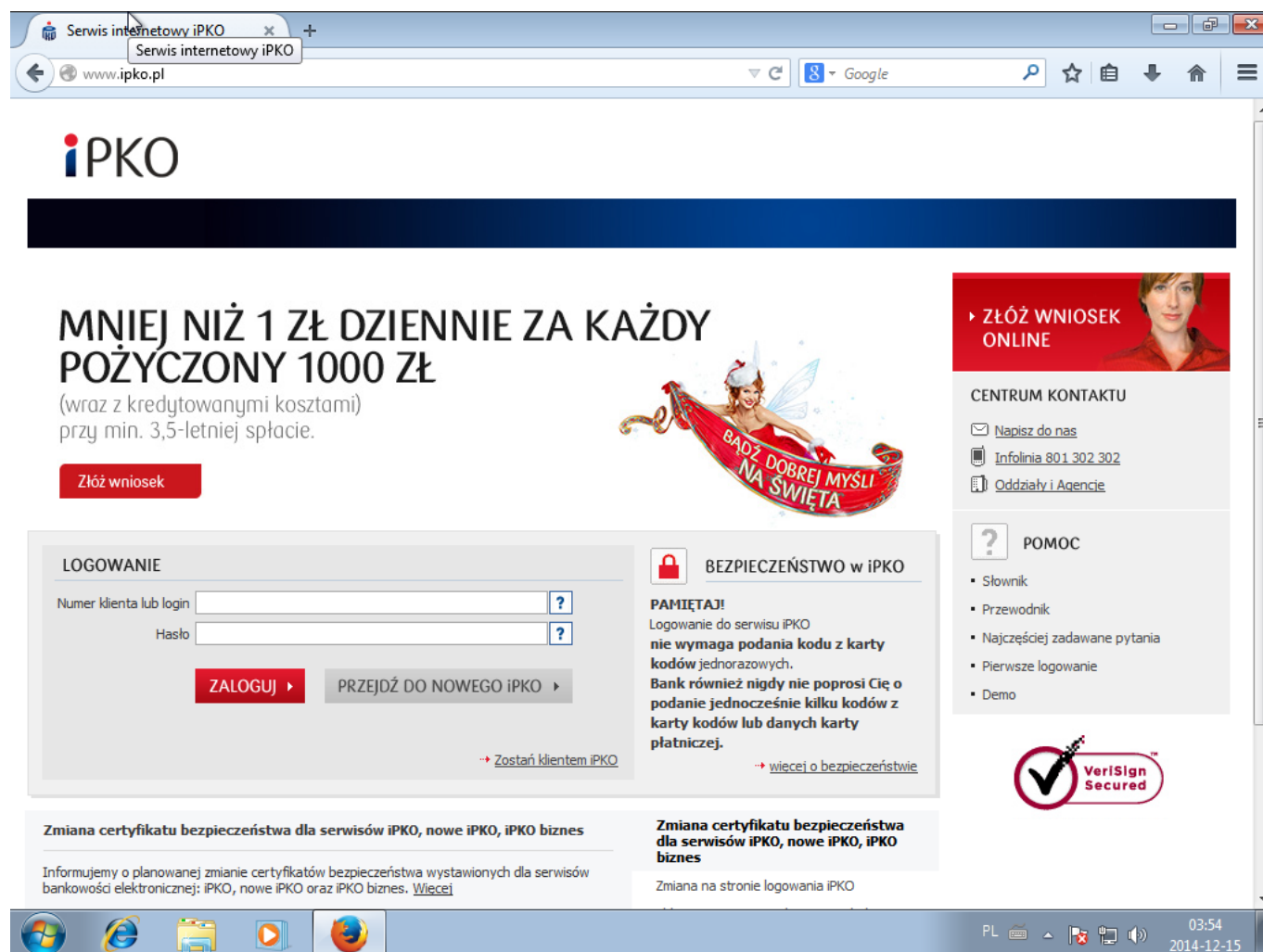
IP Routera: 10.0.2.1

IP Ofiary: 10.0.2.6

IP Intruza: 10.0.2.8

Pozwolę sobie pominąć opis samego ataku, przedstawię rezultaty. Dla porównania:

Gdy ofiara próbuje się zalogować na stronę banku gdy jest połączona bez vpn'a a intruz atakuje metodą MITM.



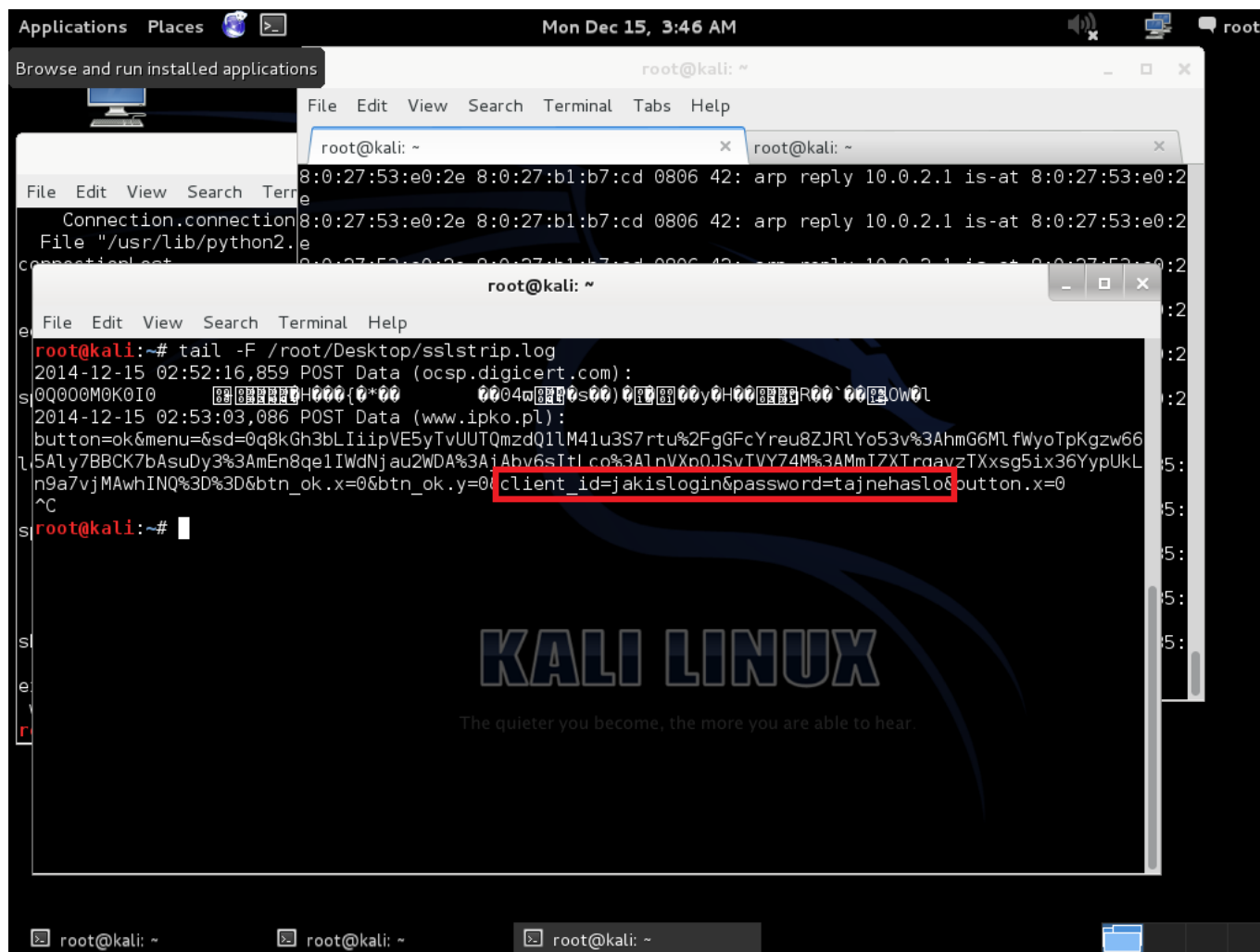
The screenshot shows the iPKO website interface. At the top, there is a navigation bar with the iPKO logo. Below it, a large promotional banner reads "MNIEJ NIŻ 1 ZŁ DZIENNIE ZA KAŻDY POŻYCZONY 1000 ZŁ" (Less than 1 PLN daily for every 1000 PLN borrowed), with a subtext "(wraz z kredytowanymi kosztami) przy min. 3,5-letniej spłacie." (including credit costs) at a minimum 3.5-year repayment. A red button "Złóż wniosek" (Apply) is visible. To the right, there is a "CENTRUM KONTAKTU" (Contact Center) section with options like "Napisz do nas" (Write to us), "infolinia 801 302 302", and "Oddziały i Agencje". Below that is a "POMOC" (Help) section with links to "Słownik", "Przewodnik", "Najczęściej zadawane pytania", "Pierwsze logowanie", and "Demo". A "VeriSign Secured" logo is also present. At the bottom, there are two news items: "Zmiana certyfikatu bezpieczeństwa dla serwisów iPKO, nowe iPKO, iPKO biznes" and "Zmiana certyfikatu bezpieczeństwa dla serwisów iPKO, nowe iPKO, iPKO biznes". The bottom of the screenshot shows the Windows taskbar with the time 03:54 and date 2014-12-15.



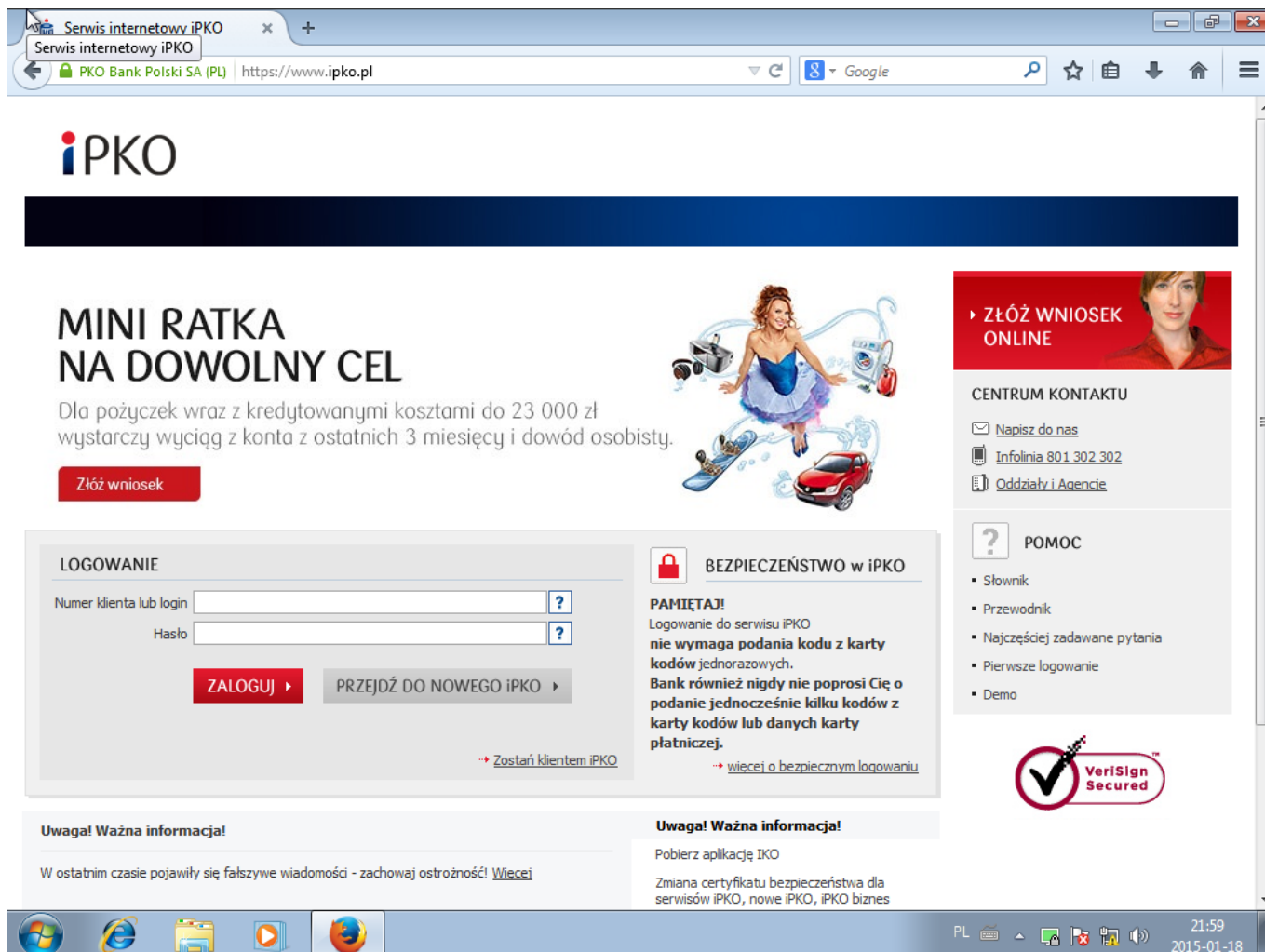
Sposób na MITM? – VPN!

Wyraźnie widać, że połączenie nie jest zabezpieczone za pomocą protokołu SSL (brak zielonego paska.)

Oraz widok maszyny atakującego podczas próby zalogowania do banku.



Teraz ta sama sytuacja tylko, że ofiara używa VPN'a.



MINI RATKA NA DOWOLNY CEL

Dla pożyczek wraz z kredytowanymi kosztami do 23 000 zł wystarczy wyciąg z konta z ostatnich 3 miesięcy i dowód osobisty.

Złóż wniosek

LOGOWANIE

Numer klienta lub login

Hasło

ZALOGUJ ▶ PRZEJDŹ DO NOWEGO iPKO ▶

→ Zostań klientem iPKO

BEZPIECZEŃSTWO w iPKO

PAMIĘTAJ!
Logowanie do serwisu iPKO nie wymaga podania kodu z karty kodów jednorazowych. Bank również nigdy nie poprosi Cię o podanie jednocześnie kilku kodów z karty kodów lub danych karty płatniczej.

→ [więcej o bezpiecznym logowaniu](#)

Uwaga! Ważna informacja!

W ostatnim czasie pojawiły się fałszywe wiadomości - zachowaj ostrożność! [Więcej](#)

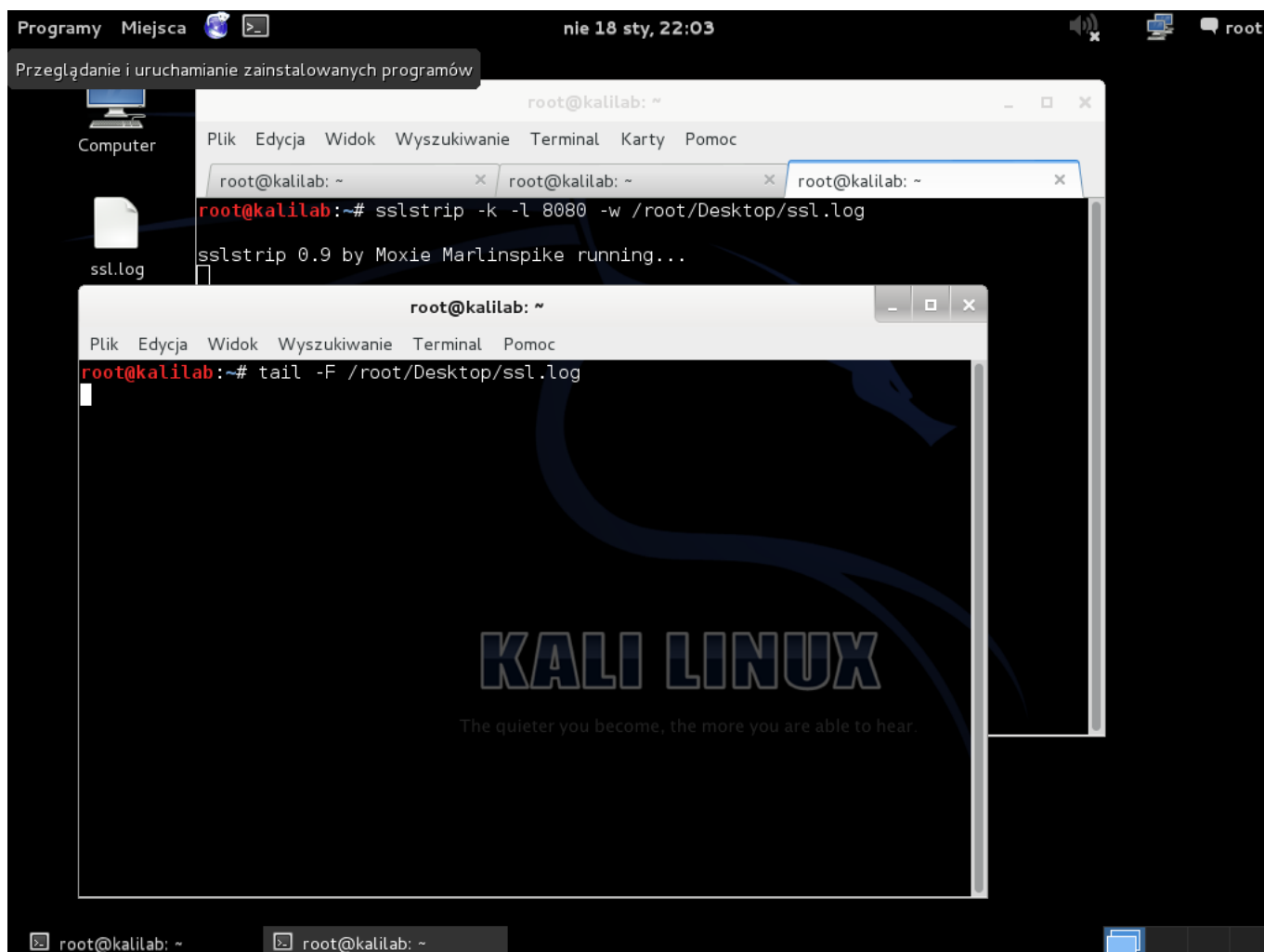
Uwaga! Ważna informacja!

Pobierz aplikację iKO

Zmiana certyfikatu bezpieczeństwa dla serwisów iPKO, nowe iPKO, iPKO biznes

VeriSign Secured

Już na pierwszy rzut oka widzimy zielony pasek świadczący o tym, że nasze połączenie jest kierowane prosto do banku.



Jak widzimy logi intruza są puste. Pomimo iż atakuje ofiarę, cały ruch odbywa się za pomocą tunelu VPN.

Oczywiście, VPN nie jest 100% sposobem na bezpieczeństwo. Bezpieczna jest tylko komunikacja pomiędzy klientem a serwerem.

Myślę, że ten artykuł pokazał Wam, jak skonfigurować własny VPN, oraz, że warto go mieć.