



Czasami sieć lokalna to za mało. Nie mówię o przypadku w którym mamy zamiar naruszać integralność obcych serwerów, a o przypadku gdy wykonujemy sprawdzenie zabezpieczeń naszego VPS'a lub na zlecenie klienta. Wtedy też najczęściej, celem jest host zlokalizowany gdzieś w internecie. Dzisiaj opiszę procedurę jak przygotować sobie narzędzia do pracy z serwerami umiejscowionymi na zewnątrz naszej lokalnej sieci.

Na początek warto nakreślić sytuację w której się znajdujemy. Czasy w jakich żyjemy, to czasy posiadania wielu urządzeń podłączonych do internetu na jednym łączu komunikacyjnym. każdy z nas ma w swoim mieszkaniu podłączony do internetu przynajmniej jeden laptop i telefon. Dzisiejsze routery korzystają z technologii NAT, aby przybliżyć trochę sytuację, czas na [wikisekcje](#).

NAT (skr. od ang. *Network Address Translation*, translacja adresów sieciowych; czasem *Native Address Translation*, translacja adresów rodzimych), znane również jako *maskarada sieci* lub *maskarada IP* (od ang. *network/IP masquerading*) - technika przesyłania ruchu sieciowego poprzez router, która wiąże się ze zmianą źródłowych lub docelowych adresów IP, zwykle również numerów portów TCP/UDP pakietów IP podczas ich przepływu. Zmieniane są także sumy kontrolne (zarówno w pakiecie IP jak i w segmencie TCP/UDP), aby potwierdzić wprowadzone zmiany.

Większość systemów korzystających z NAT ma na celu umożliwienie dostępu wielu hostom w sieci prywatnej do Internetu przy wykorzystaniu pojedynczego publicznego adresu IP. Niemniej NAT może spowodować komplikacje w komunikacji między hostami i może mieć pewien wpływ na osiągi.

Zanim wprowadzono technologię NAT modemy zapewniały możliwość podłączenia wyłącznie jednego komputera. Jego interfejs sieciowy był podłączony bezpośrednio do internetu. Już samo to, rodziło dużo zagrożeń związanych między innymi z bezpośrednim stykiem komputera z internetem. Pomimo, iż komputery posiadały wbudowane firewalle, jak wszyscy wiemy nie były one wystarczające.

W dzisiejszych czasach, aby udostępnić w internecie nasz domowy serwer www, musimy



VPS a KaliLinux - Czyli jak mieć publiczny IP podczas używania kaliego.

posiadać zewnętrzny adres IP (UPC, Vectra, Orange - stacjonarny dawniej neostrada TP) oraz ustawić w odpowiedni sposób translacje adresów (forwardowanie portów) na naszym routerze. Nie wspominam o kwestii stałego adresu IP, ponieważ brak takiego adresu jest rozwiązywalny w dość prosty sposób, a na przykład UPC ma tak skonfigurowane ustawienia sieciowe, że adres IP sprawia wrażenia stałego i bardzo rzadko się zmienia. Jeśli posiadamy internet mobilny, nie jest możliwym posiadanie swojego adresu IP o ile za to dodatkowo nie płacimy.

Rozwiązaniem jest serwer VPS. VPS to najprościej mówiąc wynajęta maszyna na które mamy roota i mamy do nie dostęp za pomocą konsoli po ssh lub za pomocą czegoś podobnego do rdp. Jak już wcześniej pisałem, kaliego na zewnętrznym adresie potrzebujemy do zamówionych pentestów więc wykorzystamy hosting rootbox.pl.

The screenshot shows the rootbox.pl website with a navigation bar in English and Polish, and a 'Log in' button. The main heading is 'SERWER DEDYKOWANY w chmurze dla profesjonalistów i deweloperów'. Below this are three key features: 'SUPER SZYBKI' (Dysk SSD - 100 x szybszy niż zwykły), 'DOBRA CENA' (od 20 zł / miesiąc za serwer), and 'OS DO WYBORU' (Linux lub MS Windows Server). The main content area displays six server plans: Developer, Small, Medium, Large, X Large, and XX Large. Each plan lists its hourly price, vCPU count, RAM, SSD, and transfer limits, along with a 'Założ konto' button.

Developer	Small	Medium	Large	X Large	XX Large
0.028 zł godzina	0.056 zł godzina	0.112 zł godzina	0.223 zł godzina	0.445 zł godzina	0.834 zł godzina
1 vCPU	1 vCPU	2 vCPU	4 vCPU	8 vCPU	16 vCPU
1GB RAM	2GB RAM	4GB RAM	8GB RAM	15GB RAM	30GB RAM
10GB SSD	20GB SSD	40GB SSD	60GB SSD	80GB SSD	100GB SSD
1TB transfer	transfer bez limitu	transfer bez limitu	transfer bez limitu	transfer bez limitu	transfer bez limitu
Założ konto	Założ konto	Założ konto	Założ konto	Założ konto	Założ konto



VPS a KaliLinux - Czyli jak mieć publiczny IP podczas używania kaliego.

Po zalogowaniu się i wpłacenia środków na nasze wirtualne konto (nie wspominałem, że rootbox nalicza opłaty od godziny, przez co jest świetnym rozwiązaniem do tego typu sytuacji - wystawiając rachunek klientowi, wliczamy koszty vps) ujrzymy taki oto widok:

The screenshot shows the Rootbox Admin Panel interface. On the left, there is a navigation menu with options: Serwery, Klucze SSH, Dns, Płatności, Wsparcie, and Ustawienia. Below the menu is a green button labeled 'Nowy serwer'. The main content area is titled 'Rozpocznij korzystanie z rootbox' and contains three steps: 1. 'Doładuj konto' (Add funds) with a 'Gotowe!' status, 2. 'Uruchom serwer' (Start server) with a 'Nowy serwer' button, and 3. 'Zaloguj się' (Log in) with a note that access details will be emailed. On the left side of the main area, there is a user profile section showing a balance of 39.79 PLN and a 'Doładuj' button. Below the profile, user details are listed: 'użytkownik: jasiek.piotr@gmail.com', 'klient: Piotr Jasiek', and a 'Wyloguj' button. At the bottom, there is a system status bar showing 'Serwery 0 | vCPU 0 | RAM 0GB | SSD 0GB' and a taskbar with system icons and the date '2015-09-26'.

Jak widać następnym krokiem jest utworzenie nowego serwera. Ten krok jest dosyć ważny z względu, na dobranie odpowiedniej wersji systemu operacyjnego na naszym VPS.



VPS a KaliLinux - Czyli jak mieć publiczny IP podczas używania kaliego.

The screenshot shows the Rootbox Admin Panel interface. The main heading is "Nowy serwer" (New server). Below it, there is a section "Wybierz nazwę serwera" (Choose server name) with an input field containing "kali". The next section is "Wybierz konfigurację" (Choose configuration), which displays five server configuration options: Developer, Small, Medium, Large, and X Large. Each option shows hourly and monthly prices and hardware specifications. The "Small" configuration is highlighted. Below the configurations is a section "Wybierz system operacyjny lub aplikację" (Choose operating system or application) with three icons representing different OS options. On the left sidebar, there is a "Nowy serwer" button and a user account summary showing a balance of 39.79 PLN and user details for Piotr Jasiek. The footer contains copyright information for Rootbox and Warsaw Data Center, along with server resource usage statistics.

Configuration	Hourly Price	Monthly Price	Specifications
Developer	0.0344	24.80	1 vCPU / 1GB RAM, 10GB SSD, 1 TB transferu
Small	0.0689	49.59	1 vCPU / 2GB RAM, 20GB SSD, transfer bez limitu
Medium	0.1378	99.19	2 vCPU / 4GB RAM, 40GB SSD, transfer bez limitu
Large	0.2743	197.49	4 vCPU / 8GB RAM, 60GB SSD, transfer bez limitu
X Large	0.5474	394.09	8 vCPU / 16GB RAM, 80GB SSD, transfer bez limitu

W polu nazwa wpisujemy nazwę naszego serwera. Będzie ona zarazem jego hostname. Wybieramy również konfigurację serwera. Ja do tego typu zadań wybieram pakiet „Small”.



VPS a KaliLinux - Czyli jak mieć publiczny IP podczas używania kaliego.

The screenshot shows the Rootbox Admin Panel interface. On the left, there's a user profile for 'Piotr Jasiek' with a balance of 39.79 PLN. The main area displays server plans, with 'XX Large' selected, showing 16 vCPU, 32GB RAM, and 100GB SSD. Below this, there's a section 'Wybierz system operacyjny lub aplikację' with icons for Debian, Ubuntu, CentOS, Wordpress, LAMP, and Ruby on Rails. The 'Debian 7 amd64' option is highlighted. A large green 'Uruchom' button is at the bottom. The footer contains copyright information for rootbox and server specifications: 0 vCPU, 0GB RAM, 0GB SSD.

System operacyjny jakie powinniśmy wybrać to debian 7 amd64. Obecna wersja kaliego (2.0) jest redystrybucją debiana. Następnie klikamy „Uruchom”



VPS a KaliLinux - Czyli jak mieć publiczny IP podczas używania kaliego.

Rootbox Admin Panel | roo... x +

https://panel.rootbox.com/vm/560679e0b90c5765a3b65c70

rootbox™

Senwery **kali**

Klucze SSH

Dns

Płatności

Wsparcie

Ustawienia

Nowy serwer

stan konta: **39.79** PLN
+ Doładuj

użytkownik:
jasiek.piotr@gmail.com
klient:
Piotr Jasiek

Wyloguj

Odśwież **Usuń**

Nazwa	kali
ID	Nieznane
Status	Trwają prace
System operacyjny	Debian 7 amd64
Pakiet	Small
Uptime	Nieznane
Uruchomiony	2015-09-26 12:56:36

Konfiguracja serwera

vCPU	1
RAM	2 GB
SSD	20 GB

Konfiguracja sieciowa

Adres IPv4	62.181.8.108
Maska podsieci	255.255.255.0
Adres MAC	00:50:f2:00:03:fd
Brama domyślna	62.181.8.1

Backupy

Historia

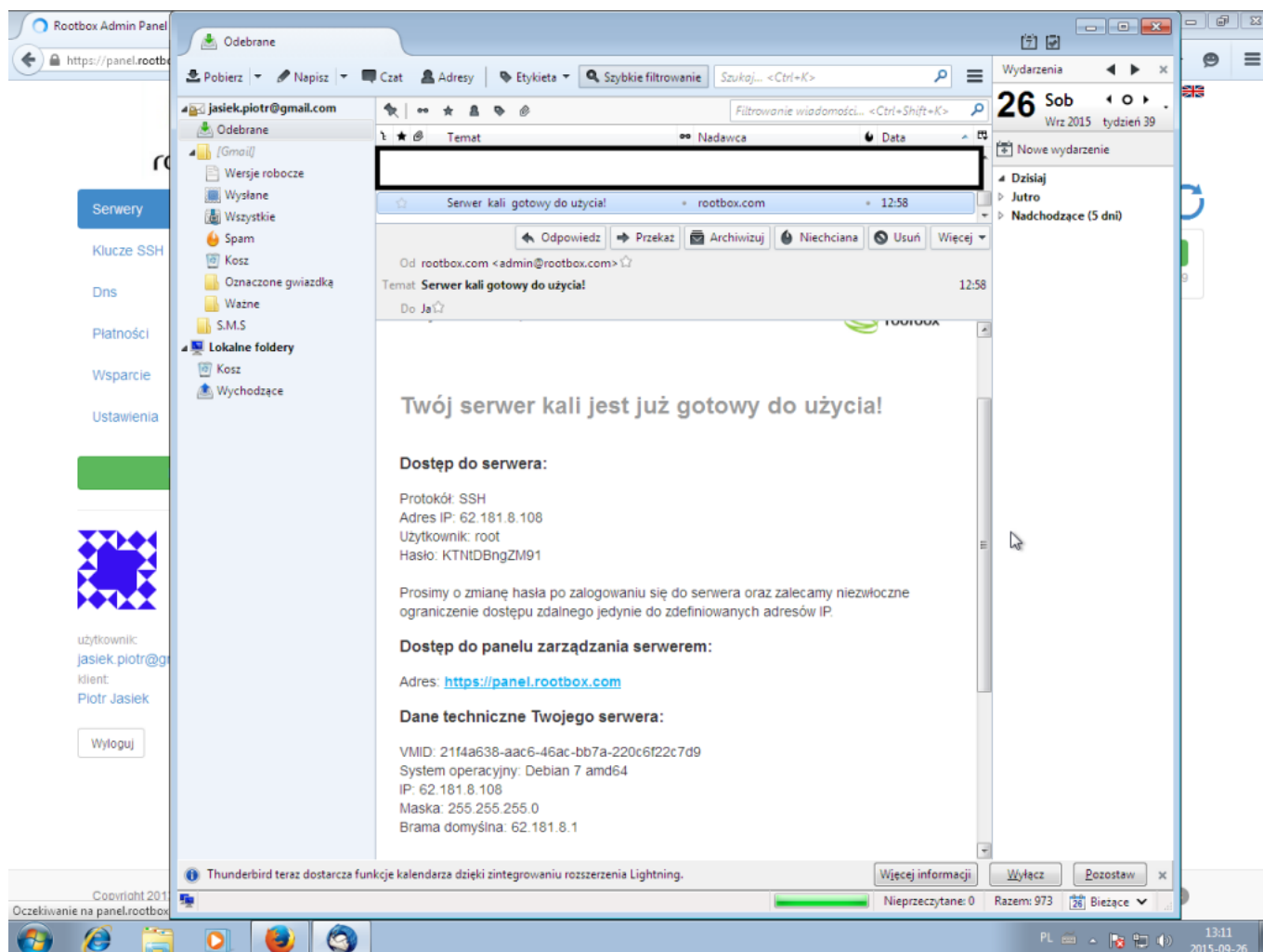
Copyright 2013 rootbox jest zarejestrowanym znakiem handlowym i marką Warsaw Data Center

Senwery 1 | vCPU 1 | RAM 2GB | SSD 20GB

Oczekiwanie na www.google-analytics.com...

PL 12:56 2015-09-26

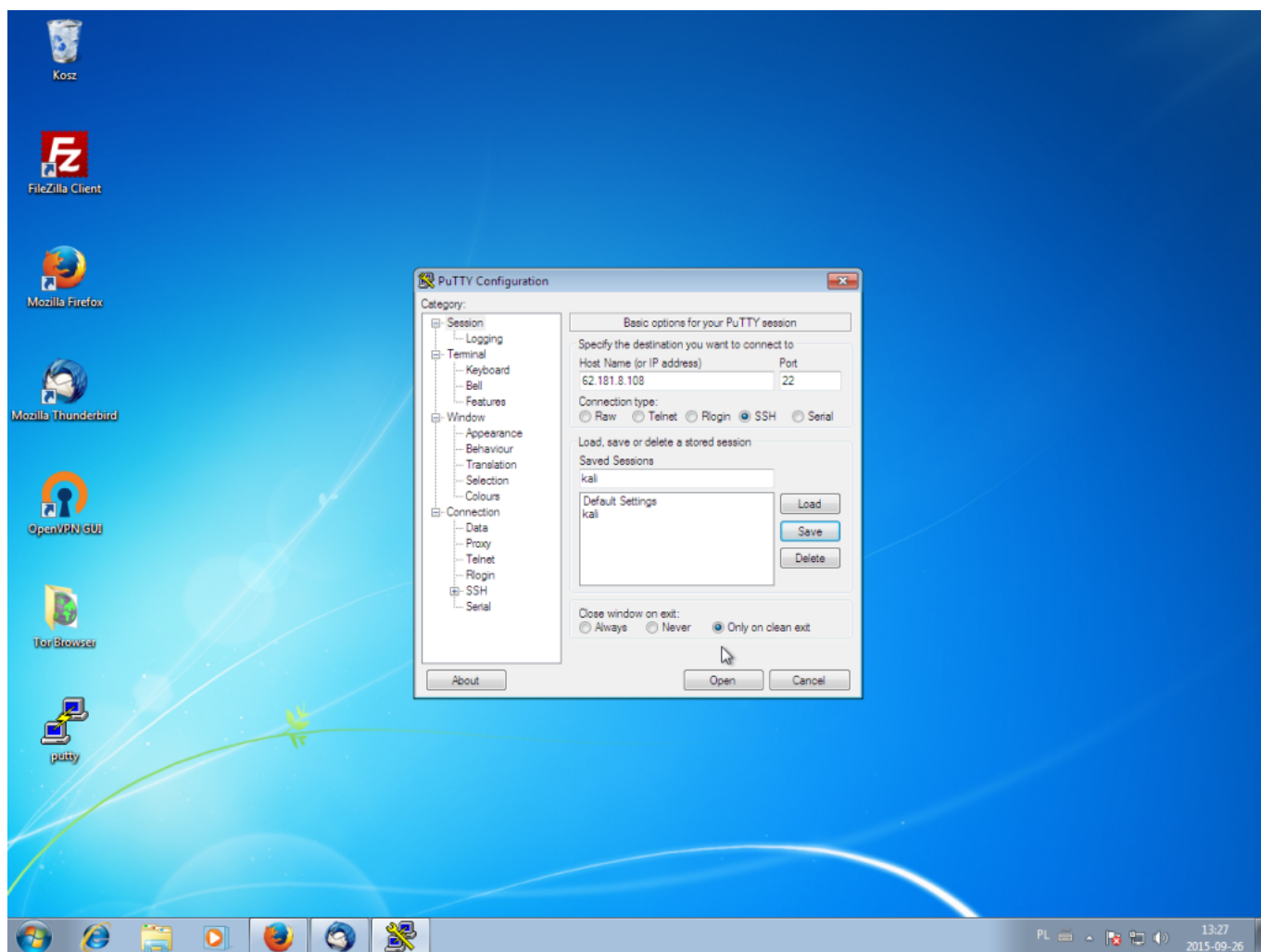
Naszym oczom ukazują się obraz informujący o tym, że nasz serwer jest w przygotowaniu. Po chwili sprawdzamy naszą skrzynkę mailową na którą przyjdzie powiadomienie o tym, że serwer jest gotowy do użycia.



W mailu znajdziemy wszystkie potrzebne dane takie jak hasło oraz adres naszego nowego VPS. Przejdźmy do właściwej części. Czas zalogować się do naszego serwera.

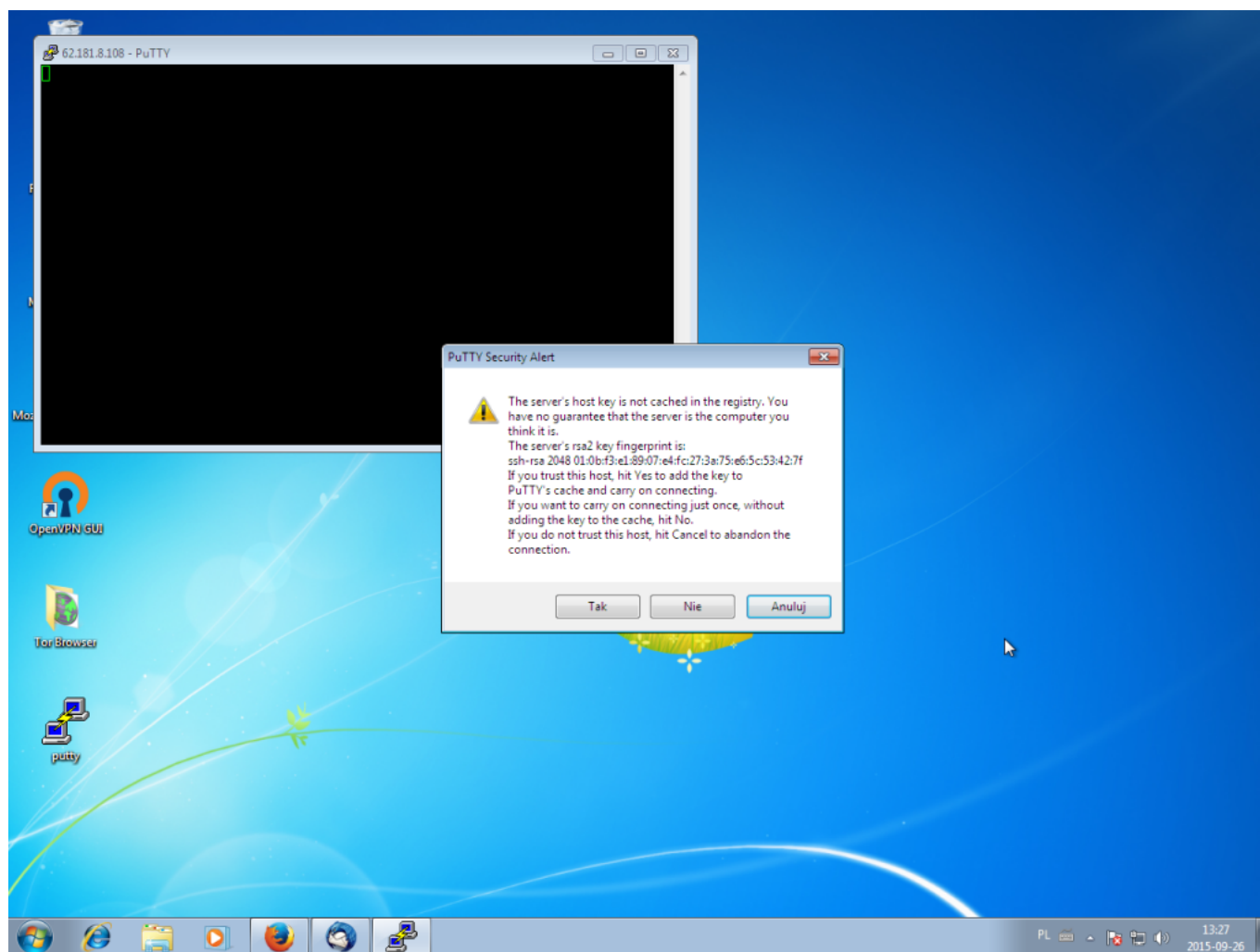


VPS a KaliLinux - Czyli jak mieć publiczny IP podczas używania kaliego.





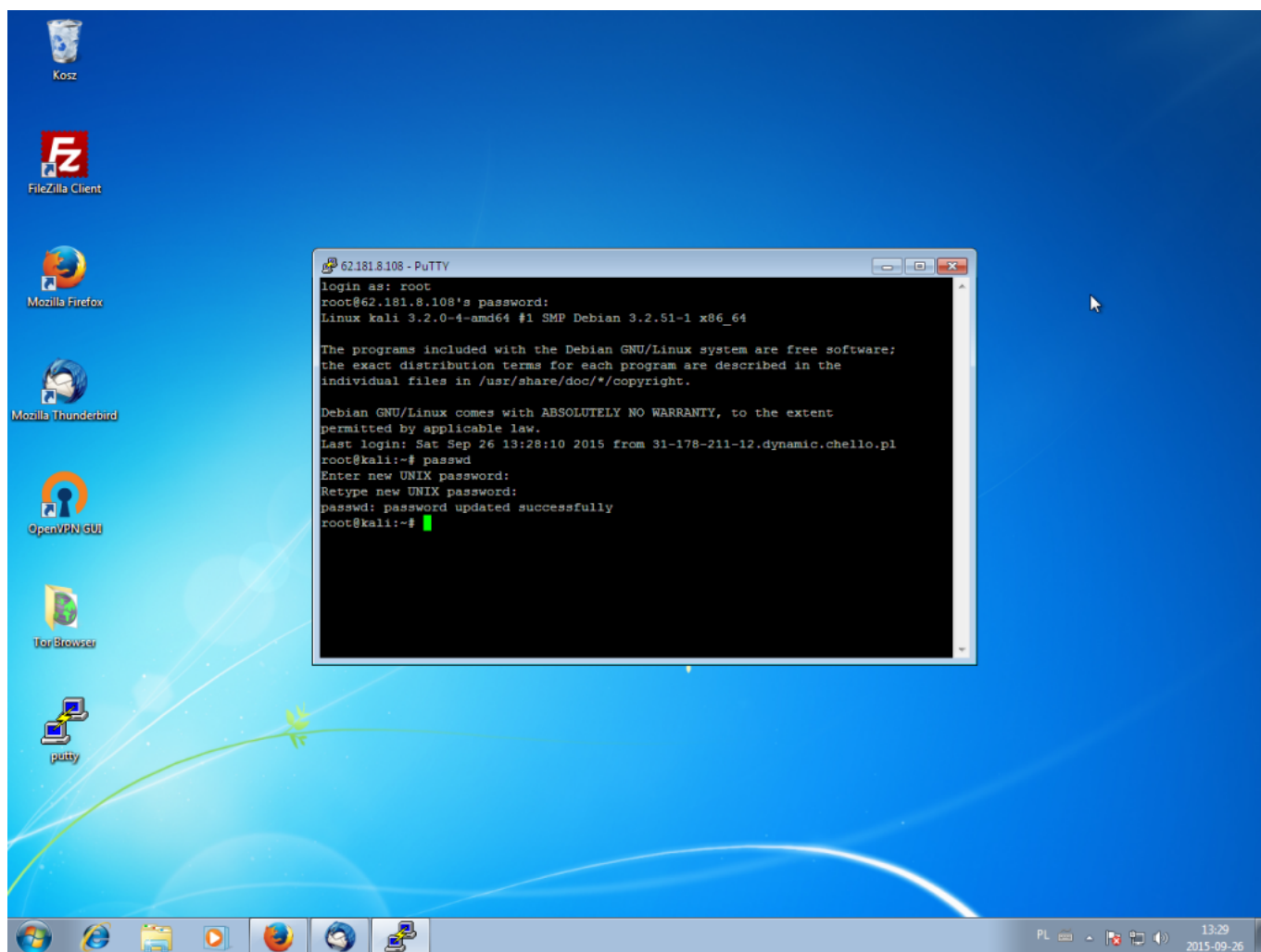
VPS a KaliLinux - Czyli jak mieć publiczny IP podczas używania kaliego.



Po zalogowaniu się warto zmienić hasło na trochę bardziej przyjazne użytkownikowi, czyli nam.



VPS a KaliLinux - Czyli jak mieć publiczny IP podczas używania kaliego.



Na chwilę obecną mamy do dyspozycji „czystego” debiana. następnym krokiem który będzie to odnalezienie odpowiednich wpisów do `/etc/apt/sources.list` i dodanie ich do naszego debiana.



VPS a KaliLinux - Czyli jak mieć publiczny IP podczas używania kaliego.

```
deb http://http.kali.org/kali sana main non-free contrib
deb http://security.kali.org/kali-security sana/updates main contrib non-free
```

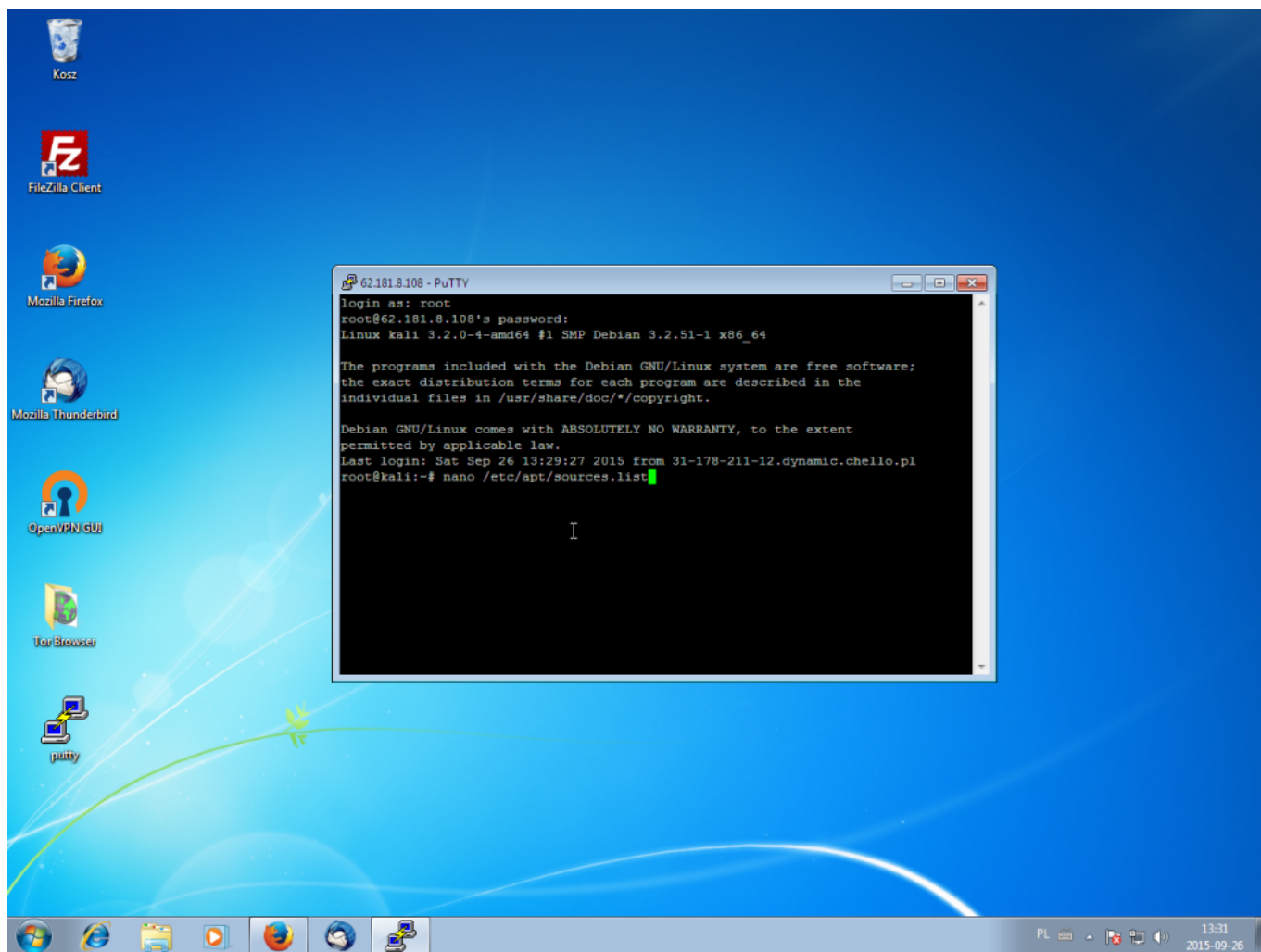
EDIT: Ponieważ dynamika kaliego jest tak duża, że z wersji na wersje zmieniają się linki do repozytoriów, postanowiliśmy przygotować własne repozytorium z pakietami narzędzi z kalilinuxa oraz najnowszymi dostępnymi pakietami na debiana. Zapewni to wygodniejszą i pewniejszą pracę z prezentowanymi przez nas labami.

```
deb http://repo.s-m-s.pl/debian all all
```



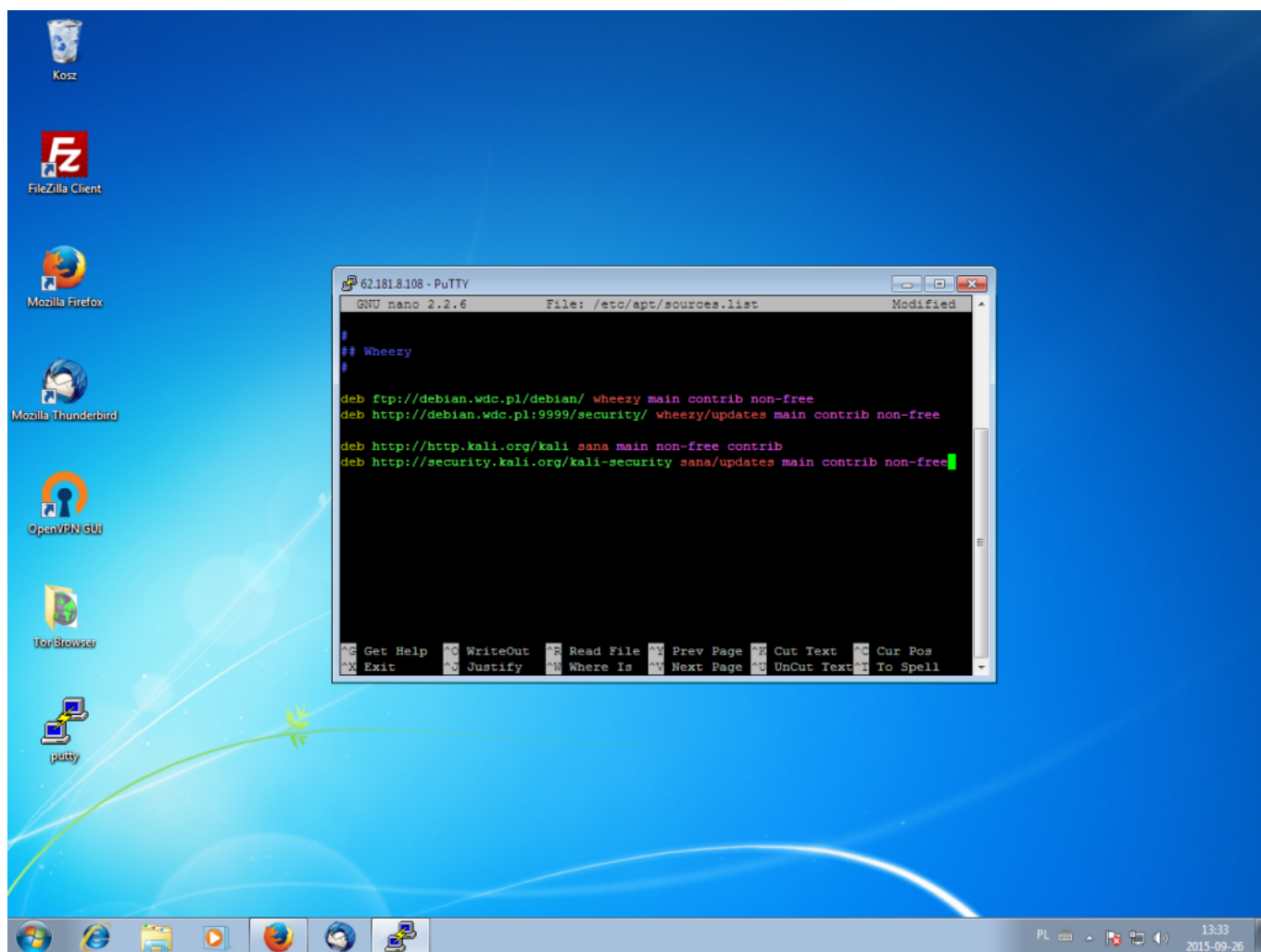
VPS a KaliLinux - Czyli jak mieć publiczny IP podczas używania kaliego.

```
deb-src http://repo.s-m-s.pl/debian all all
```



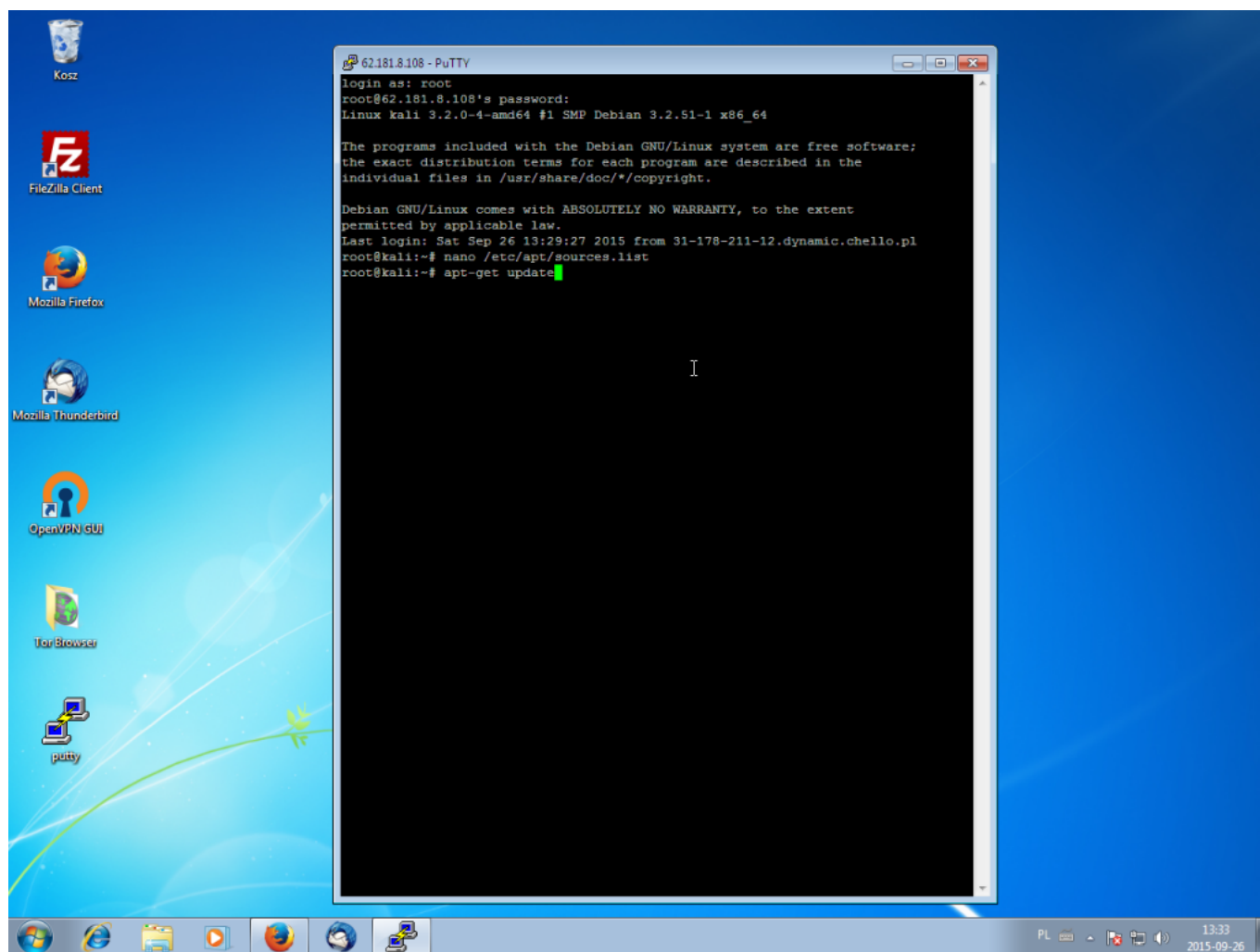


VPS a KaliLinux - Czyli jak mieć publiczny IP podczas używania kaliego.





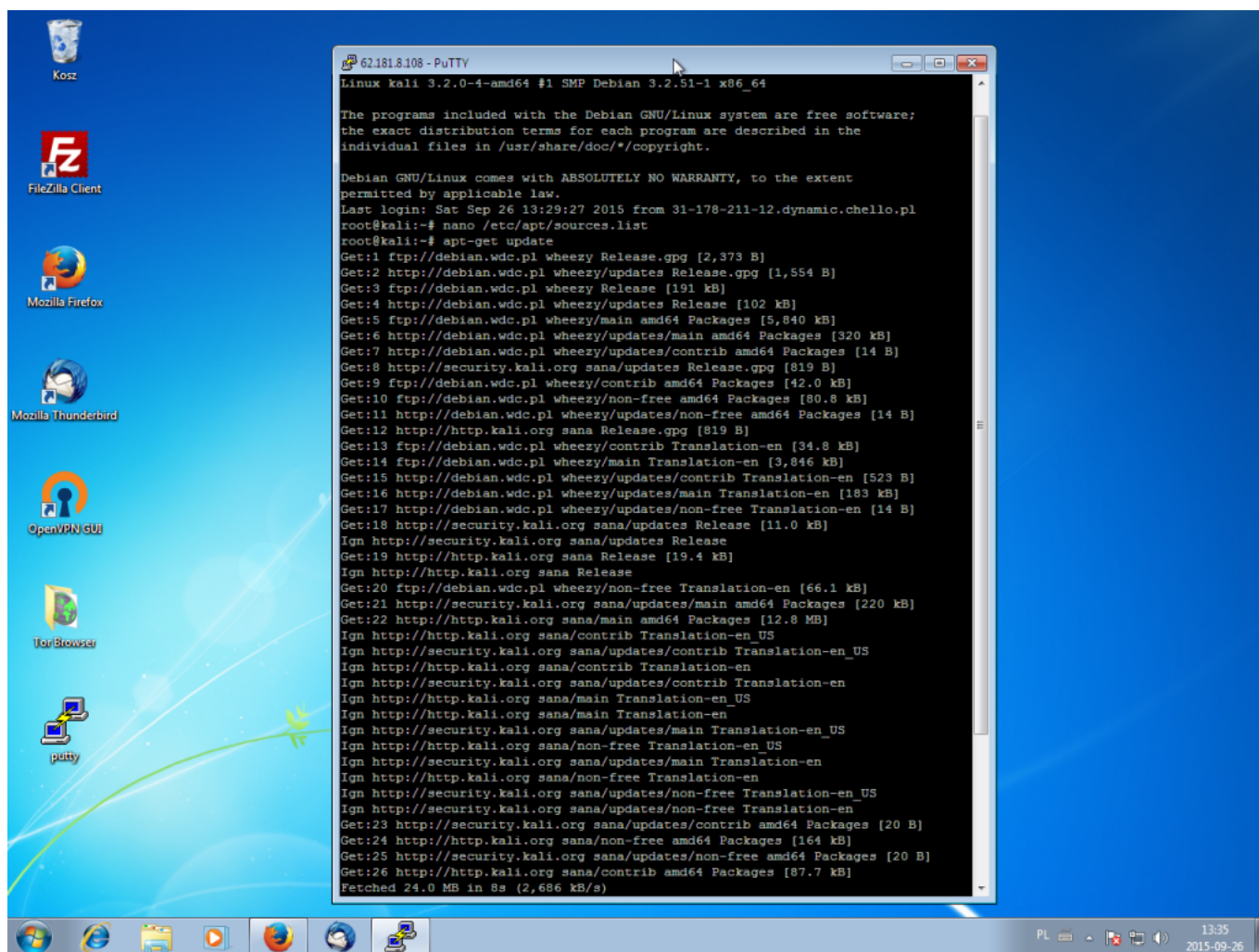
VPS a KaliLinux - Czyli jak mieć publiczny IP podczas używania kaliego.



Następnym krokiem jest wykonanie aktualizacji listy pakietów.

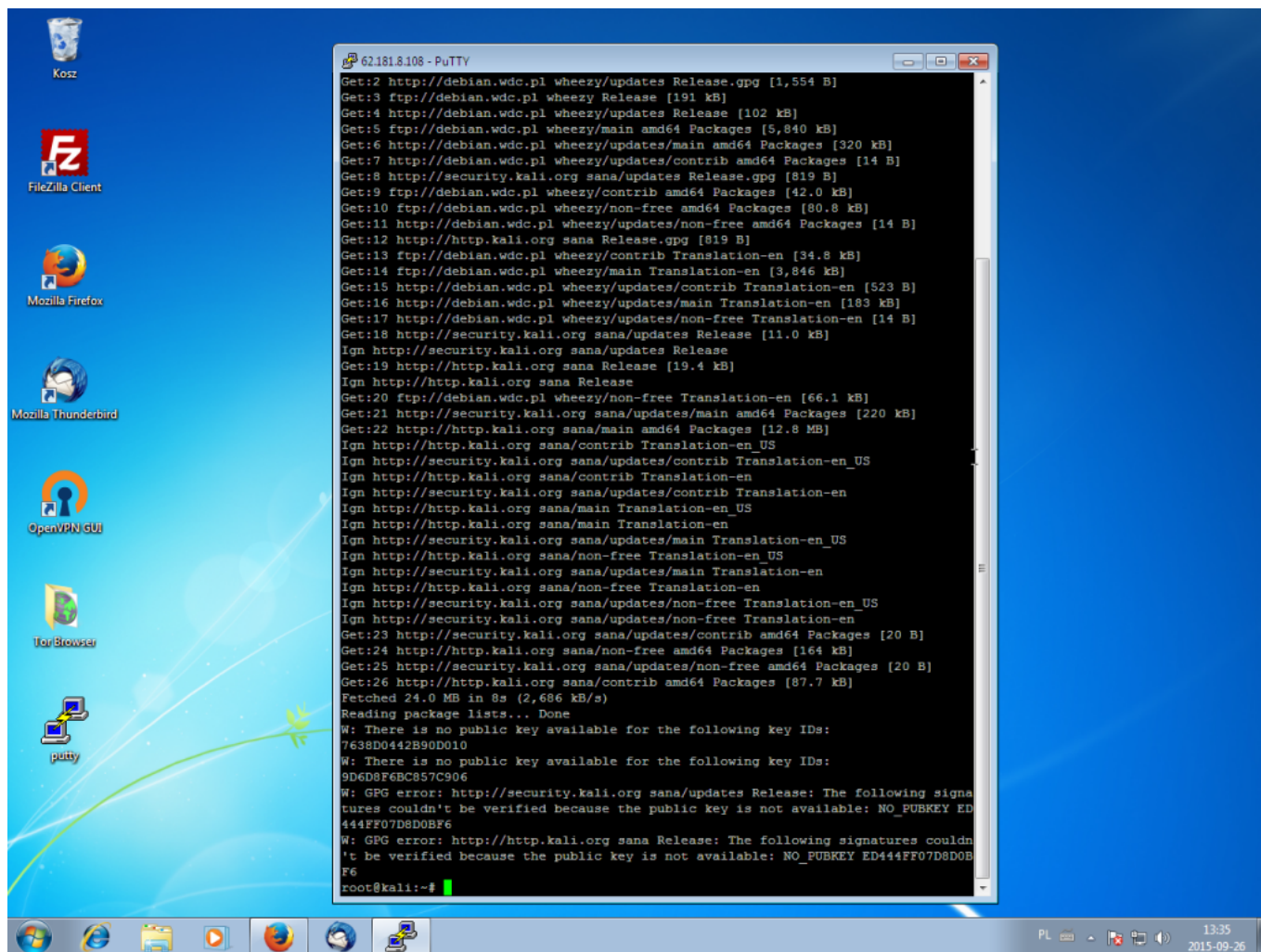


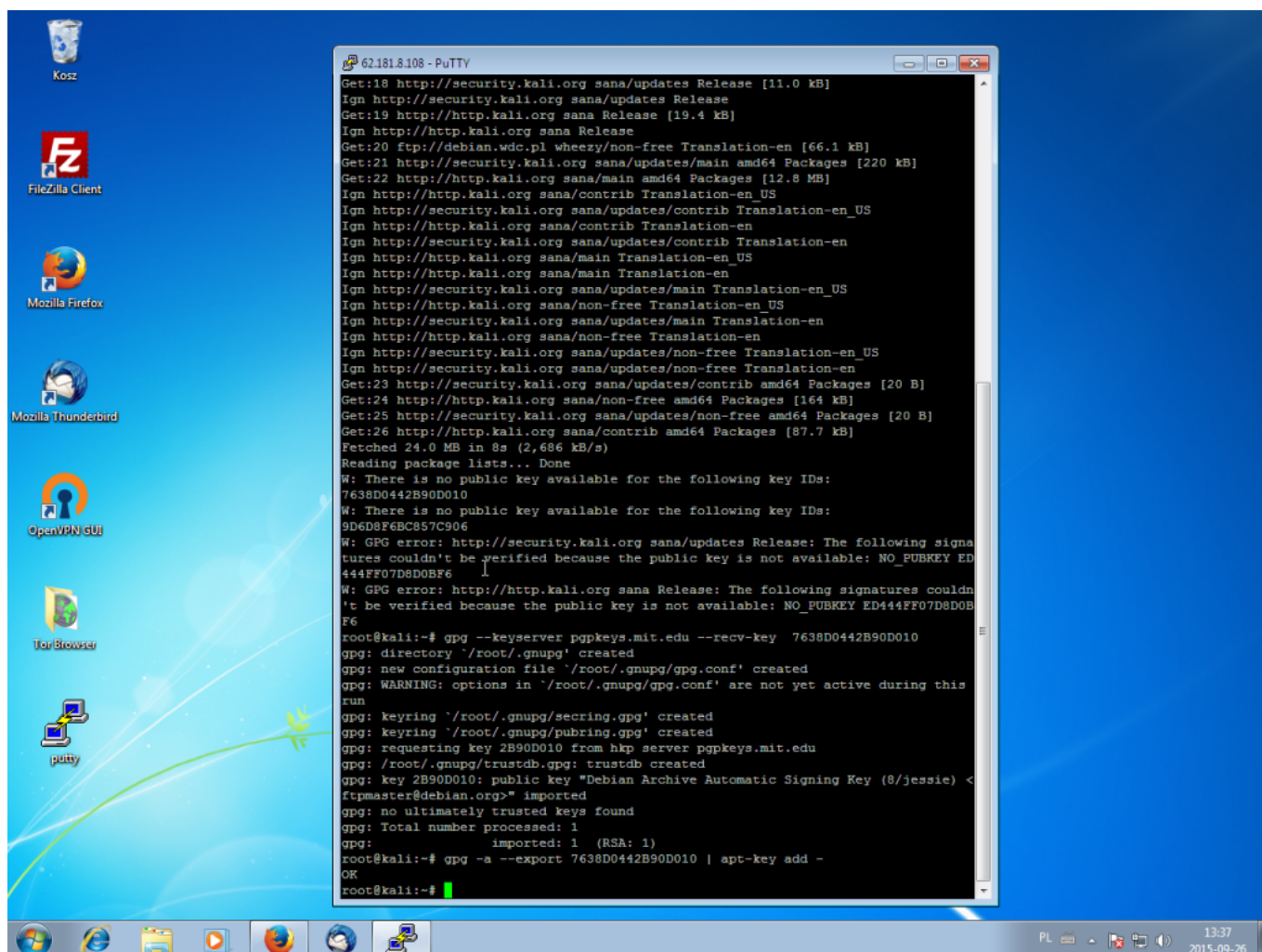
VPS a KaliLinux - Czyli jak mieć publiczny IP podczas używania kaliego.





VPS a KaliLinux - Czyli jak mieć publiczny IP podczas używania kaliego.





Może pojawić się problem z kluczami PGP. Wynika to z kwestii, iż nasze repozytoria kaliego nie są dla debiana domyślnie zaufane. Problem możemy rozwiązać za pomocą dwóch poleceń.

```

gpg --keyserver pgp.mit.edu --recv-keys <klucz>
gpg --armor --export <klucz> | apt-key add -

```

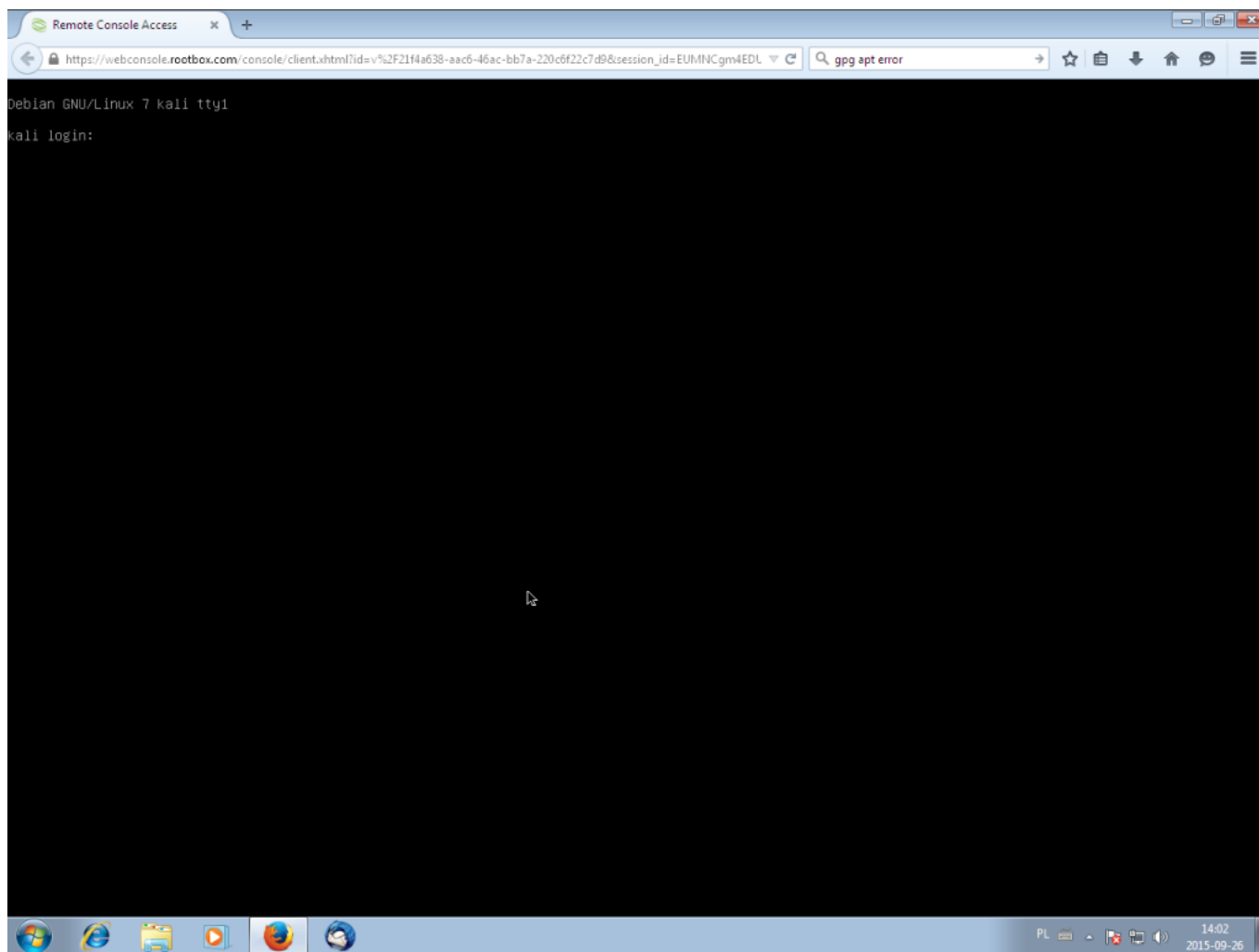
***EDIT

Nasz aktualny klucz publiczny można znaleźć na keybase.io/sms. Zapraszamy serdecznie osoby posiadające konto na keybase.io do śledzenia naszego profilu



VPS a KaliLinux - Czyli jak mieć publiczny IP podczas używania kaliego.

W tym momencie skorzystamy z dodatkowego udogodnienia, którego nie widziałem u innych dostawców, lub po prostu nie działało. Wracamy zatem do naszej przeglądarki, logujemy się do rootbox i przechodzimy do zakładki naszego serwera. Tam wybieramy opcję „Konsola”





VPS a KaliLinux - Czyli jak mieć publiczny IP podczas używania kaliego.

The screenshot shows a web browser window titled "Remote Console Access" with the URL `https://webconsole.rootbox.com/console/client.html?id=v%2F21f4a638-aac6-46ac-bb7a-220c6f22c7d9&session_id=EUMNCGm4EDL`. The search bar contains "gpg apt error". The terminal output is as follows:

```
Debian GNU/Linux 7 kali tty1
kali login: root
Password:
Last login: Sat Sep 26 13:54:42 CEST 2015 on tty1
Linux kali 3.2.0-4-amd64 #1 SMP Debian 3.2.51-1 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@kali:~# _
```

The bottom of the window shows a taskbar with icons for Firefox, LibreOffice, and other applications. The system tray on the right indicates the time is 14:14 on 2015-09-26.



VPS a KaliLinux - Czyli jak mieć publiczny IP podczas używania kaliego.

```
Hit http://security.kali.org sana/updates/main amd64 Packages
Hit http://http.kali.org sana/non-free amd64 Packages
Hit http://security.kali.org sana/updates/contrib amd64 Packages
Get:4 http://debian.wdc.pl wheezy/updates/contrib amd64 Packages [14 B]
Hit http://http.kali.org sana/contrib amd64 Packages
Hit http://security.kali.org sana/updates/non-free amd64 Packages
Get:5 http://debian.wdc.pl wheezy/updates/non-free amd64 Packages [14 B]
Get:6 http://debian.wdc.pl wheezy/updates/contrib Translation-en [523 B]
Get:7 http://debian.wdc.pl wheezy/updates/main Translation-en [183 kB]
Get:8 http://debian.wdc.pl wheezy/updates/non-free Translation-en [14 B]
Ign http://http.kali.org sana/contrib Translation-en_US
Ign http://security.kali.org sana/updates/contrib Translation-en_US
Ign http://http.kali.org sana/contrib Translation-en
Ign http://security.kali.org sana/updates/contrib Translation-en
Ign http://http.kali.org sana/main Translation-en_US
Ign http://security.kali.org sana/updates/main Translation-en_US
Ign http://http.kali.org sana/main Translation-en
Ign http://security.kali.org sana/updates/main Translation-en
Ign http://http.kali.org sana/non-free Translation-en_US
Ign http://security.kali.org sana/updates/non-free Translation-en_US
Ign http://http.kali.org sana/non-free Translation-en
Ign http://security.kali.org sana/updates/non-free Translation-en
Fetched 607 kB in 5s (115 kB/s)
Reading package lists... Done
root@kali:~# _
```

Jak widać, problemy z listą kluczy repozytoriów zniknęły. Czas na aktualizację oprogramowania tak by zgadzały się zależności oraz instalację dodatkowych pakietów.



VPS a KaliLinux - Czyli jak mieć publiczny IP podczas używania kaliego.

```
libmount1 libncurses5 libncursesw5 libnewt0.52 libnfnftlink0 libp11-kit0
libpam-modules libpam-modules-bin libpam0g libpci3 libpipeline1 libpopt0
libreadline6 libselinux1 libsemanage-common libsemanage1 libsepoll1 libslang2
libsqlite3-0 libss2 libssl1.0.0 libstdc++6 libtext-charwidth-perl
libtext-iconv-perl libtinfo5 libusb-0.1-4 libustr-1.0-1 libuuid-perl
liburip0 libx11-6 libxaplan2 libxcb1 libxext6 linux-image-amd64 locales
login logrotate man-db module-init-tools mount nano ncurses-bin net-tools
netcat-traditional openssh-client openssh-server passwd pciutils perl-base
procps python python-minimal python2.7 python2.7-minimal rsyslog sed ssh
sysv-rc sysvinit sysvinit-utils tar traceroute udev util-linux vim
vim-common vim-runtime vim-tiny wget whiptail xauth xz-utils zlib1g
The following packages will be upgraded:
acpi acpi-support-base base-files console-setup console-setup-linux debconf
debconf-i18n debian-archive-keyring discover discover-data dmidecode eject
hostname initramfs-tools installation-report keyboard-configuration
klibc-utils krb5-locales libattr1 libbz2-1.0 libdiscover2 libgcrpt11
libgnutls26 libklibc libpam-runtime libsigc++-2.0-0c2a libtasn1-3 libuuid1
libx11-data libxau6 libxdmcp6 libxmu1 linux-image-3.2.0-4-amd64 lsb-base
lsb-release manpages mime-support multiarch-support ncurses-base
ncurses-term netbase os-prober readline-common sensible-utils tasksel
tasksel-data tcpd tzdata ucf xkb-data
50 upgraded, 0 newly installed, 0 to remove and 147 not upgraded.
Need to get 34.4 MB of archives.
After this operation, 3,150 kB of additional disk space will be used.
Do you want to continue [Y/n]? _
```



VPS a KaliLinux - Czyli jak mieć publiczny IP podczas używania kaliego.

```
Setting up debconf-118n (1.5.56) ...
Setting up krb5-locales (1.12.1+dfsg-19) ...
Setting up mime-support (3.58) ...
Installing new version of config file /etc/mime.types ...
Setting up ncurses-term (5.9+20140913-1) ...
Setting up ucf (3.0030) ...
Setting up acpi (1.7-1) ...
Setting up acpi-support-base (0.142-6) ...
Installing new version of config file /etc/acpi/powerbtn-acpi-support.sh ...
Setting up discover-data (2.2013.01.11) ...
Setting up libdiscover2 (2.1.2-7) ...
Setting up discover (2.1.2-7) ...
Setting up eject (2.1.5+deb1+cvs20081104-13.1) ...
Setting up installation-report (2.58) ...
Setting up libx11-data (2:1.6.2-3) ...
Setting up lsb-release (4.1+Debian13+nmu1) ...
Setting up tcpd (7.6.q-25) ...
Setting up os-prober (1.65) ...
Setting up taskel-data (3.31+kali1) ...
Setting up taskel (3.31+kali1) ...
Processing triggers for initramfs-tools ...
update-initramfs: Generating /boot/initrd.img-3.2.0-4-amd64
root@kali:~# uname -a
Linux kali 3.2.0-4-amd64 #1 SMP Debian 3.2.51-1 x86_64 GNU/Linux
root@kali:~#
```

Jak widzimy, nadal mamy Debiana z repozytoriami i częścią pakietów od kaliego. To bardzo wygodne jeśli ktoś później chce instalować typowo debianowe pakiety, których nie ma w kalim. Natomiast jeśli chcemy mieć kaliego z uzupełnieniem o pakiety debianowe (tutaj zazwyczaj zaczyna się sypać, ale nie zawsze) wystarczy w `/etc/apt/sources.list` wpisać repozytoria kaliego jako pierwsze. Oczywiście nie jest to jedyny sposób w którym możemy posiadać Kaliego na zewnętrznym serwerze, ale ten jest najpewniejszy i najwygodniejszy.

EDIT: Repozytorium o którym wspomnieliśmy wcześniej (<http://repo.s-m-s.pl/debian>) zawiera pakiety stricte debianowe i te odpowiednie dla Kali Linuxa, co za tym idzie nadal mamy dostęp do paczek oryginalnego debiana a więc możemy instalować normalne oprogramowanie. Nie potrzebujemy



VPS a KaliLinux - Czyli jak mieć publiczny IP podczas używania kaliego.

więc dodatkowych wpisów debiana.

PS.

Gdzieś między ostatnim screenem a podsumowaniem wpadłem na genialny pomysł, aby sflashować sobie telefon. Nie był to dobry pomysł! Ale! O moich przygodach z androidem może następnym razem)