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.

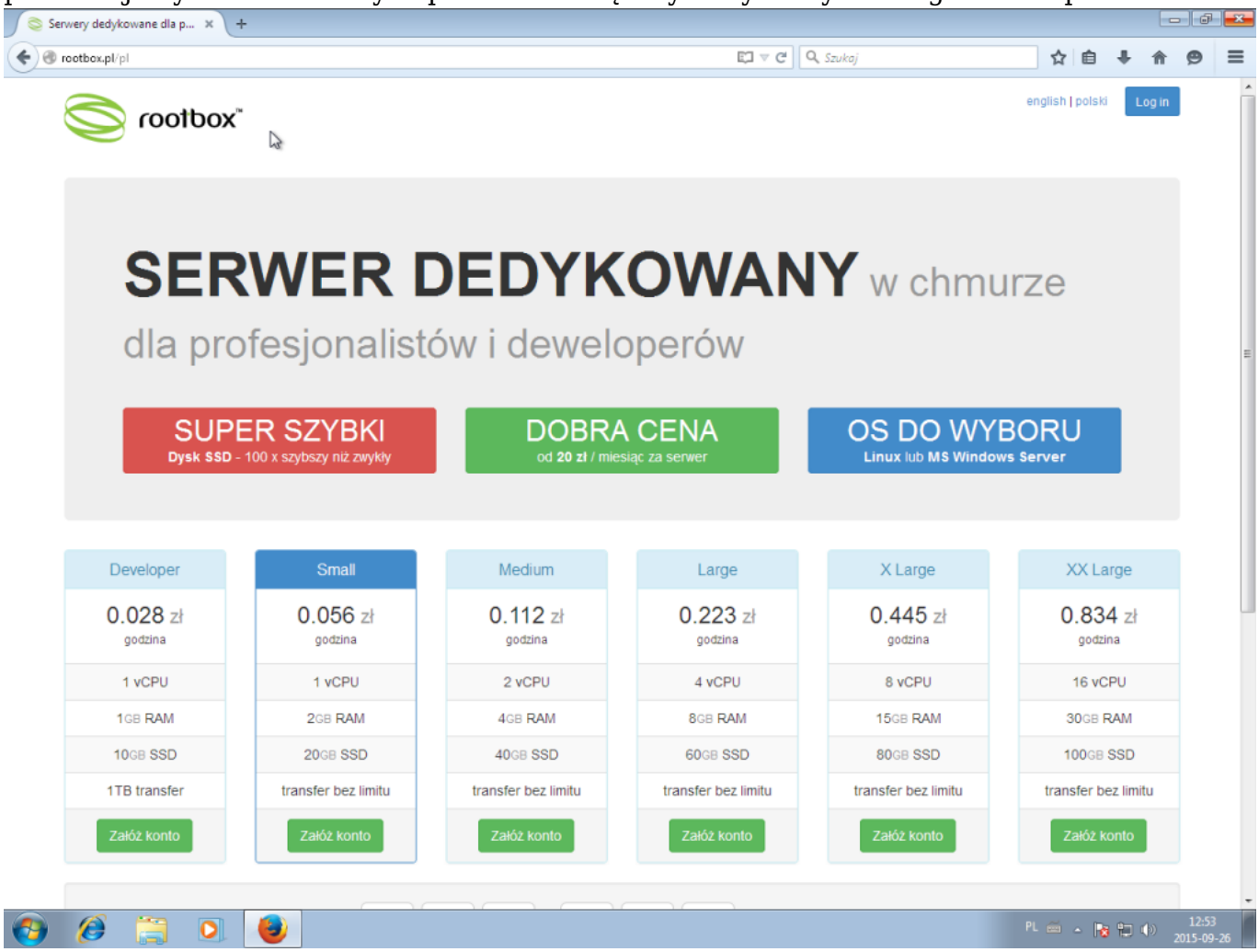
> **NAT** (skr. od ang. *Network Address Translation*, translacja adresów sieciowych; czasem *Native Address Translation*, translacja adresów rodzimych), znane również jako *maskarada sieci* lub *maskarada IP* (od ang. *network/IP masquerading*) – technika przesyłania ruchu sieciowego poprzez router, 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.

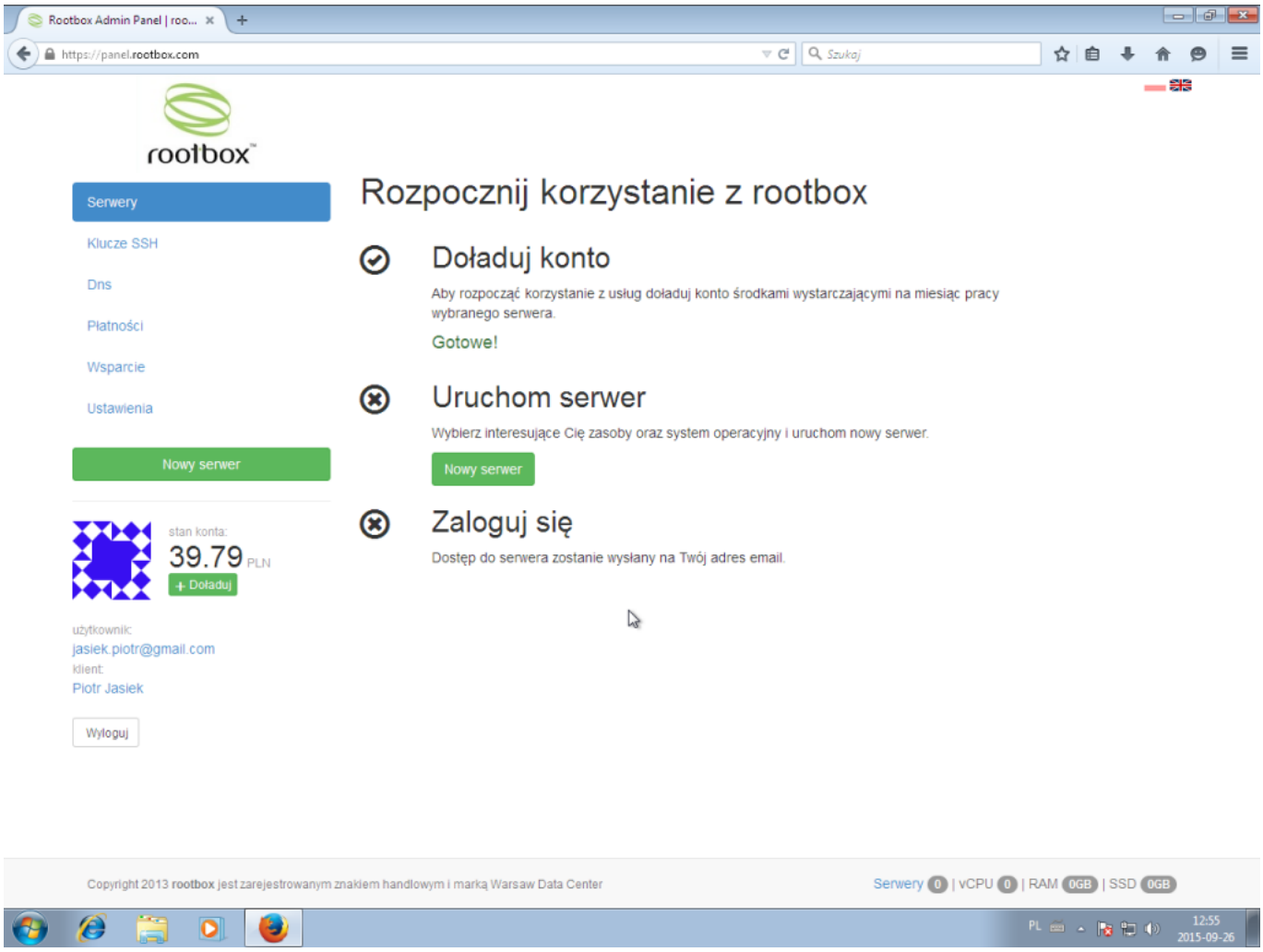
W dzisiejszych czasach, aby udostępnić w internecie nasz domowy serwer www, musimy

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.

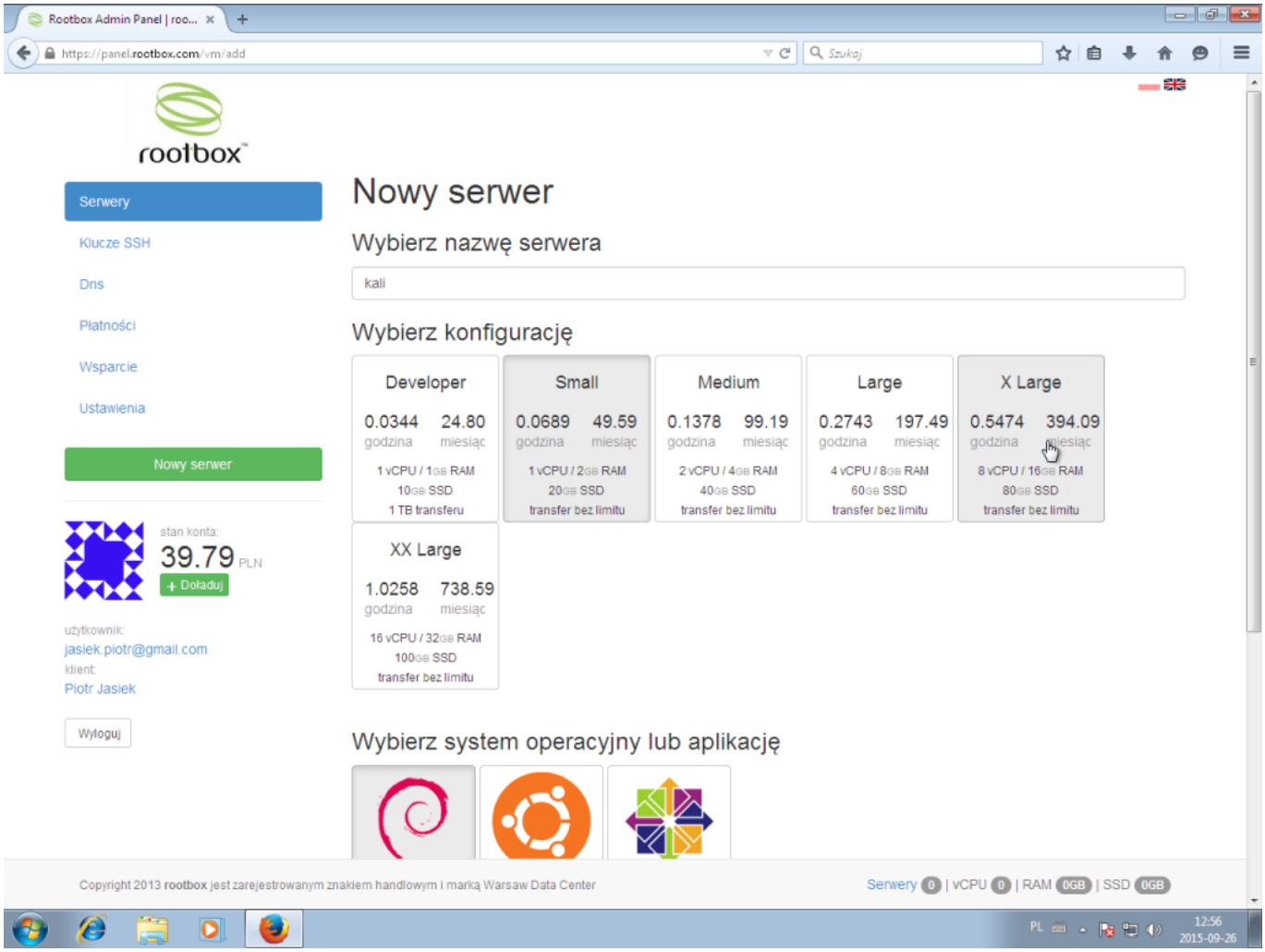
Rozwiązaniem jest serwer VPS. VPS to najprościej mówiąc wynajęta maszynę na które mamy roota i mamy do nie dostęp za pomocą konsoli po ssh lub za pomocą czegoś podobnego do rdp. Jak już wcześniej pisałem, kaliego na zewnętrznym adresie potrzebujemy do zamówionych pentestów więc wykorzystamy hosting rootbox.pl.



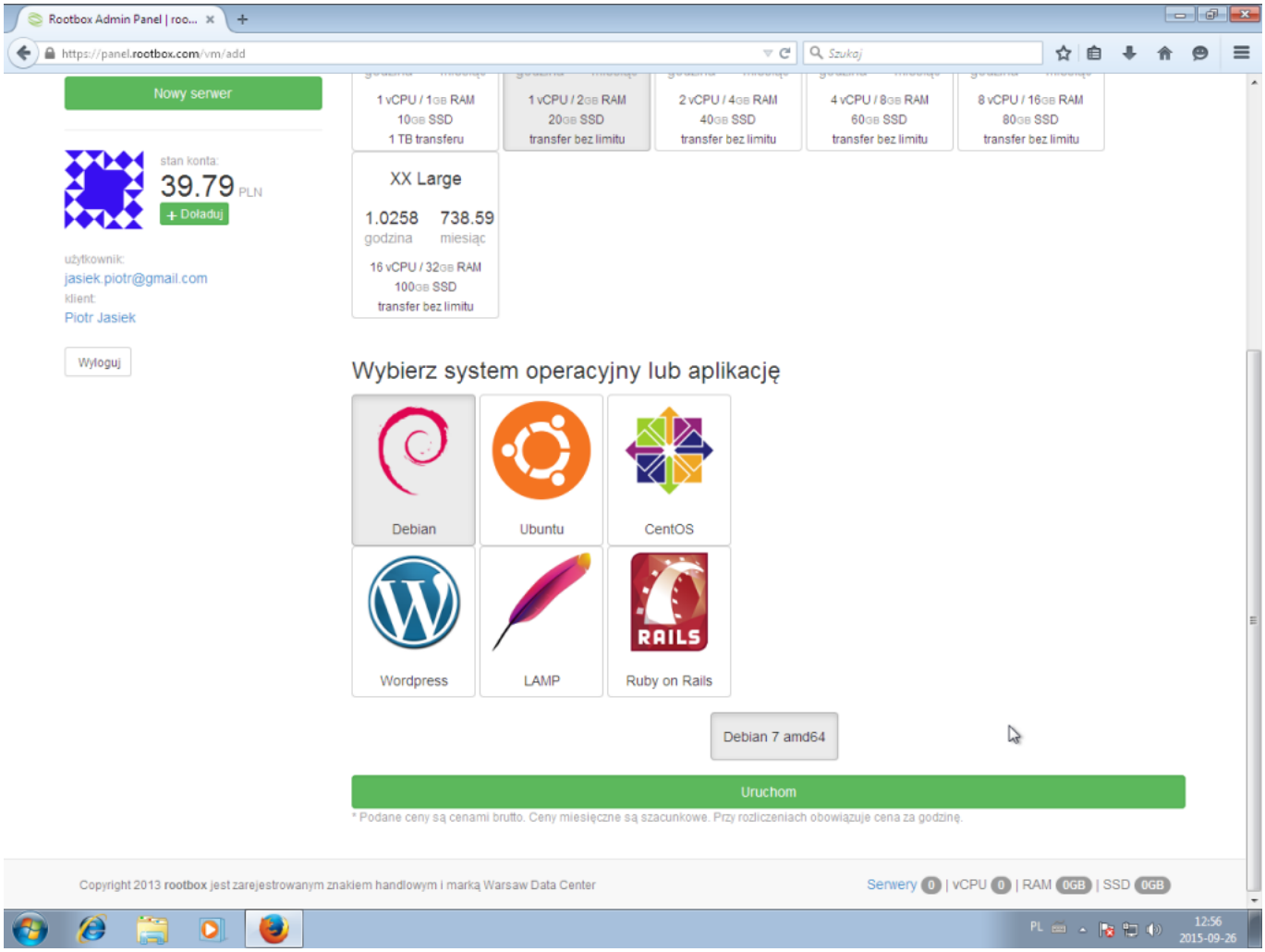
Po zalogowaniu się i wpłacenia środków na nasze wirtualne konto (nie wspomniałem, że rootbox nalicza opłaty od godziny, przez co jest świetnym rozwiązaniem do tego typu sytuacji – wystawiając rachunek klientowi, wliczamy koszty vps) ujrzymy taki oto widok:



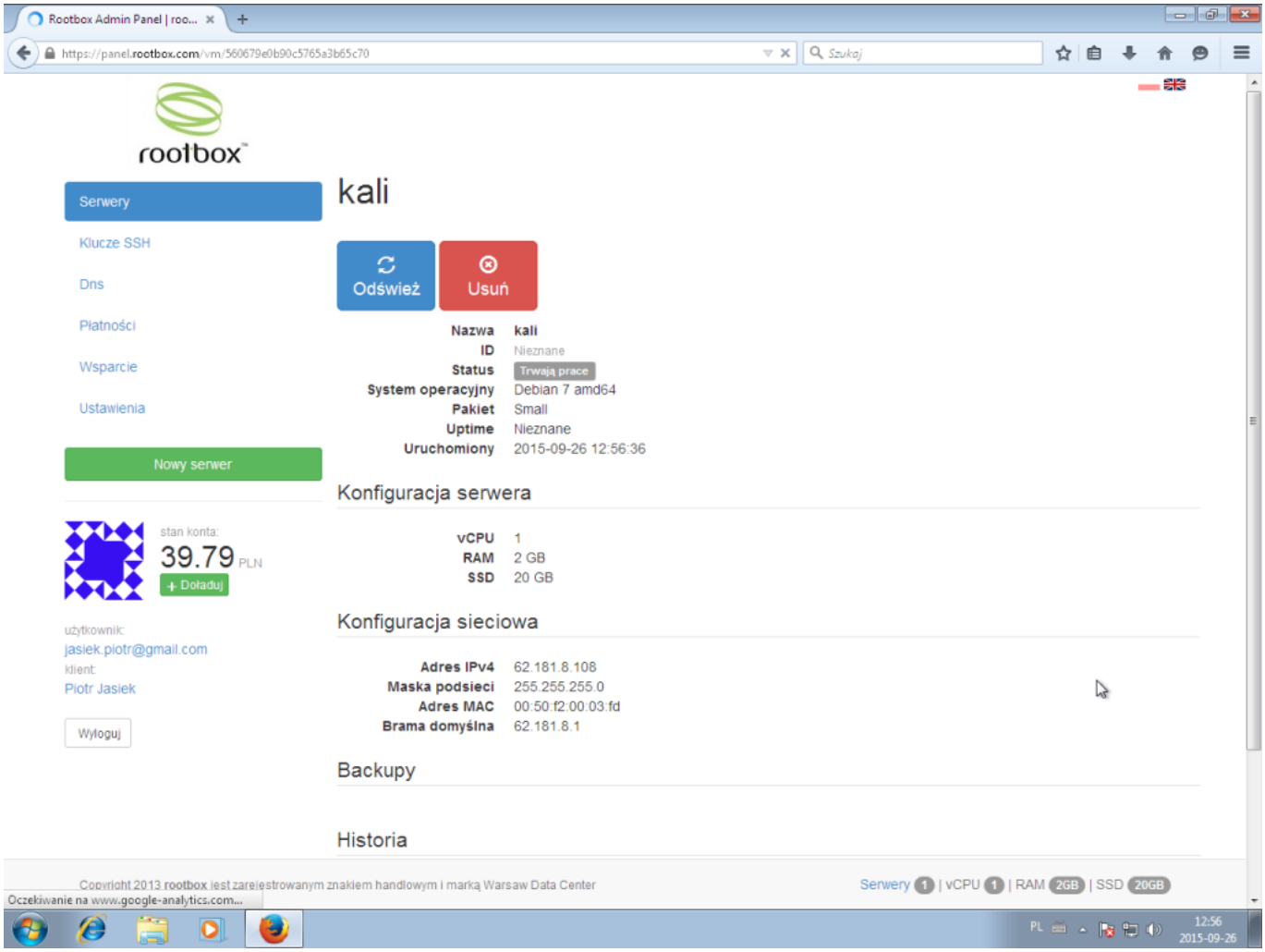
Jak widać następnym krokiem jest utworzenie nowego serwera. Ten krok jest dosyć ważny z względu, na dobranie odpowiedniej wersji systemu operacyjnego na naszym VPS.



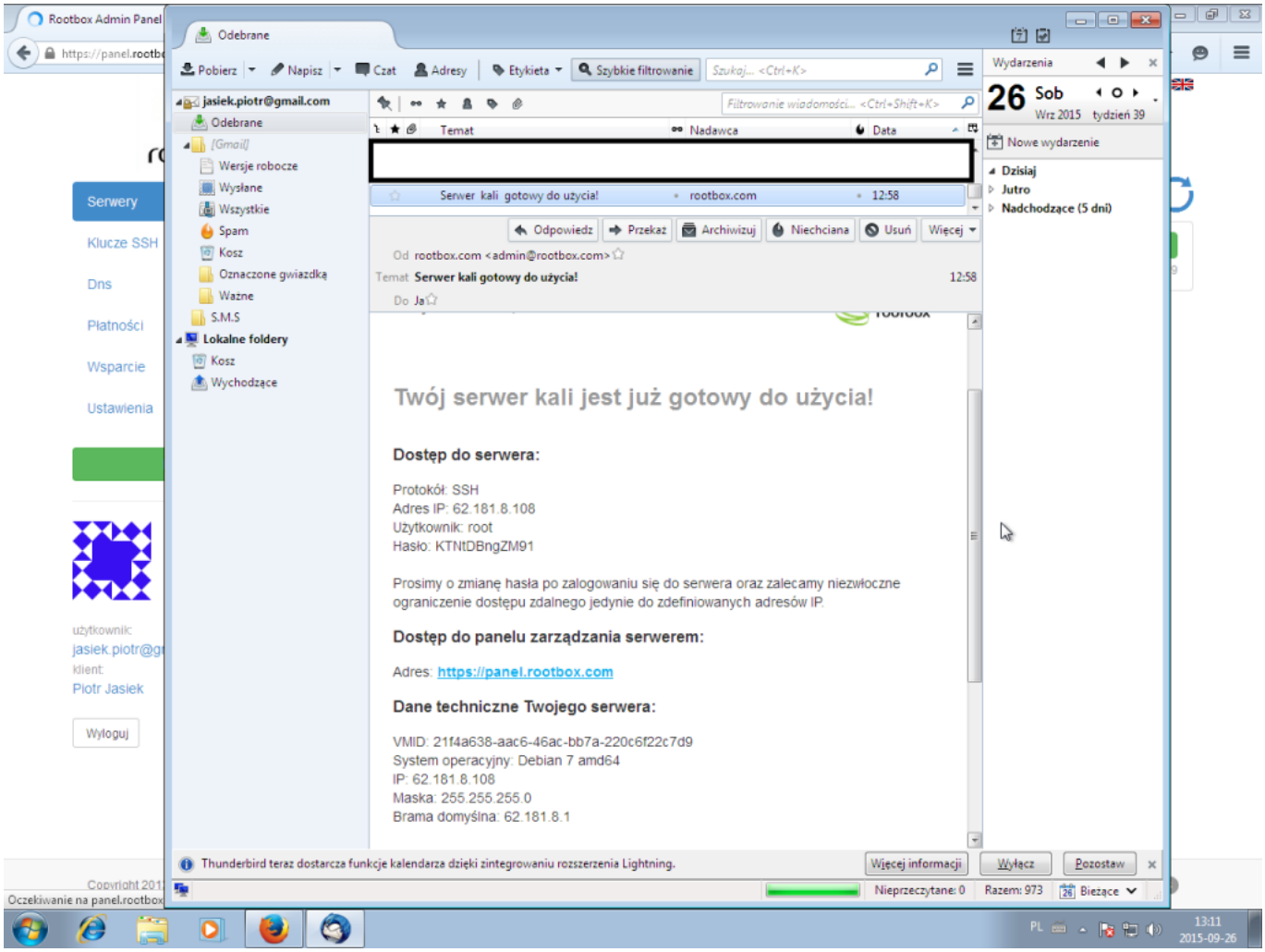
W polu nazwa wpisujemy nazwę naszego serwera. Będzie ona zarazem jego hostname. Wybieramy również konfiguracje serwera. Ja do tego typu zadań wybieram pakiet „Small”.



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



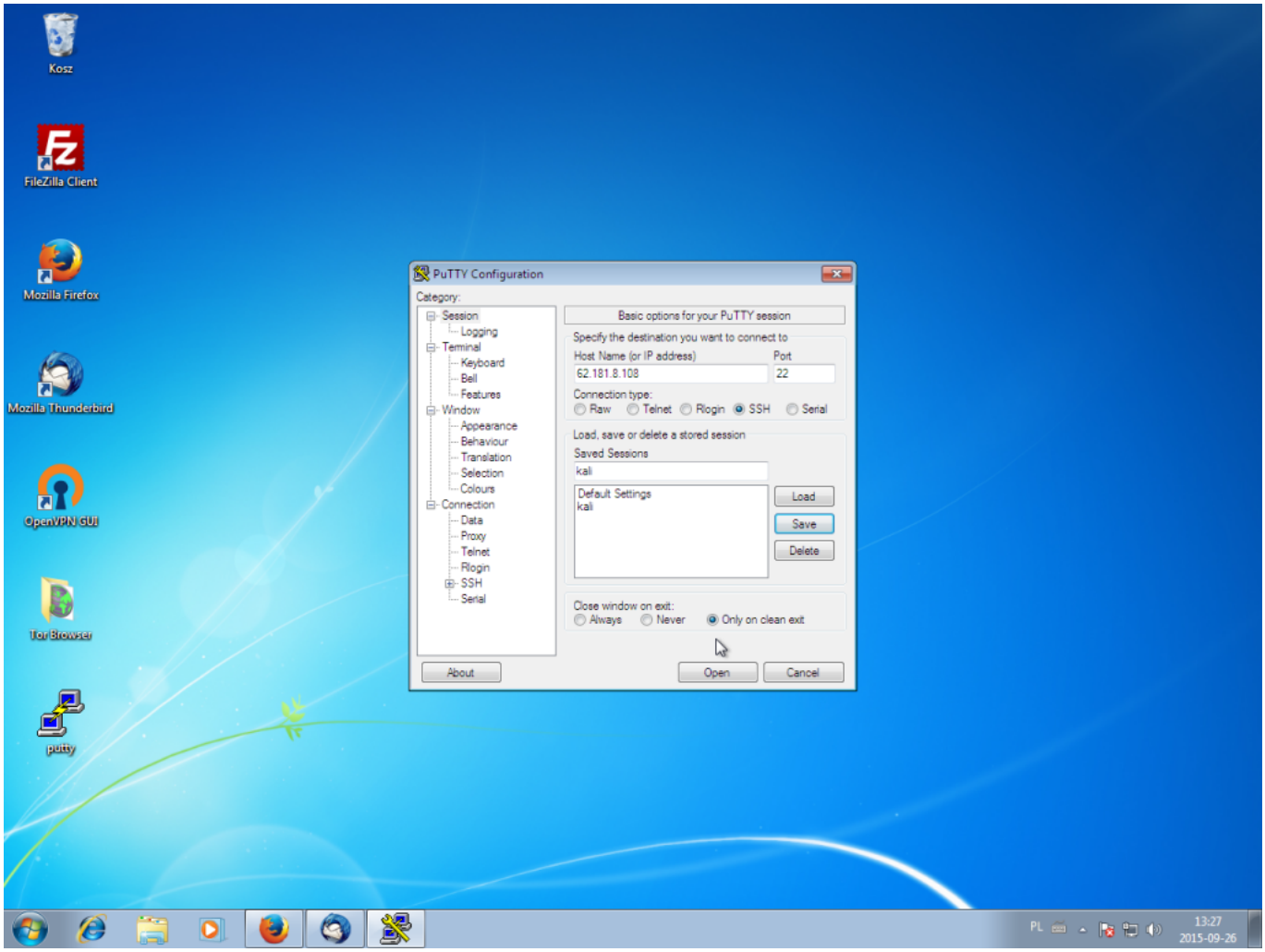
Naszym oczom ukazuje sie obraz informujący o tym, że nasz serwer jest w przygotowaniu. Po chwili sprawdzamy naszą skrzynkę mailową na którą przyjdzie powiadomienie o tym, że serwer jest gotowy do użycia.

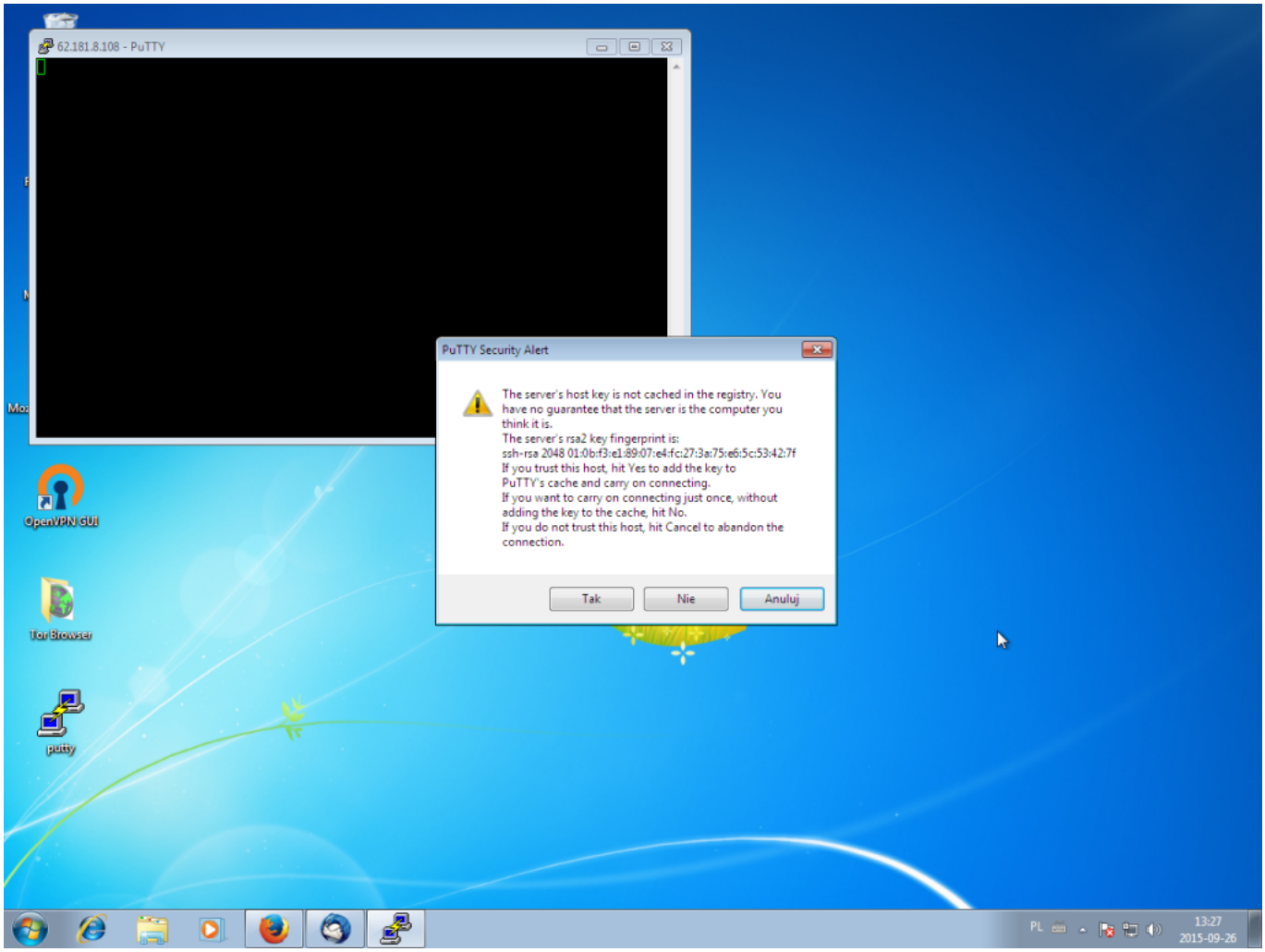


W mailu znajdziemy wszystkie potrzebne dane takie jak hasło oraz adres naszego nowego VPS. Przejdzmy do właściwej części. Czas zalogować się do naszego serwera.

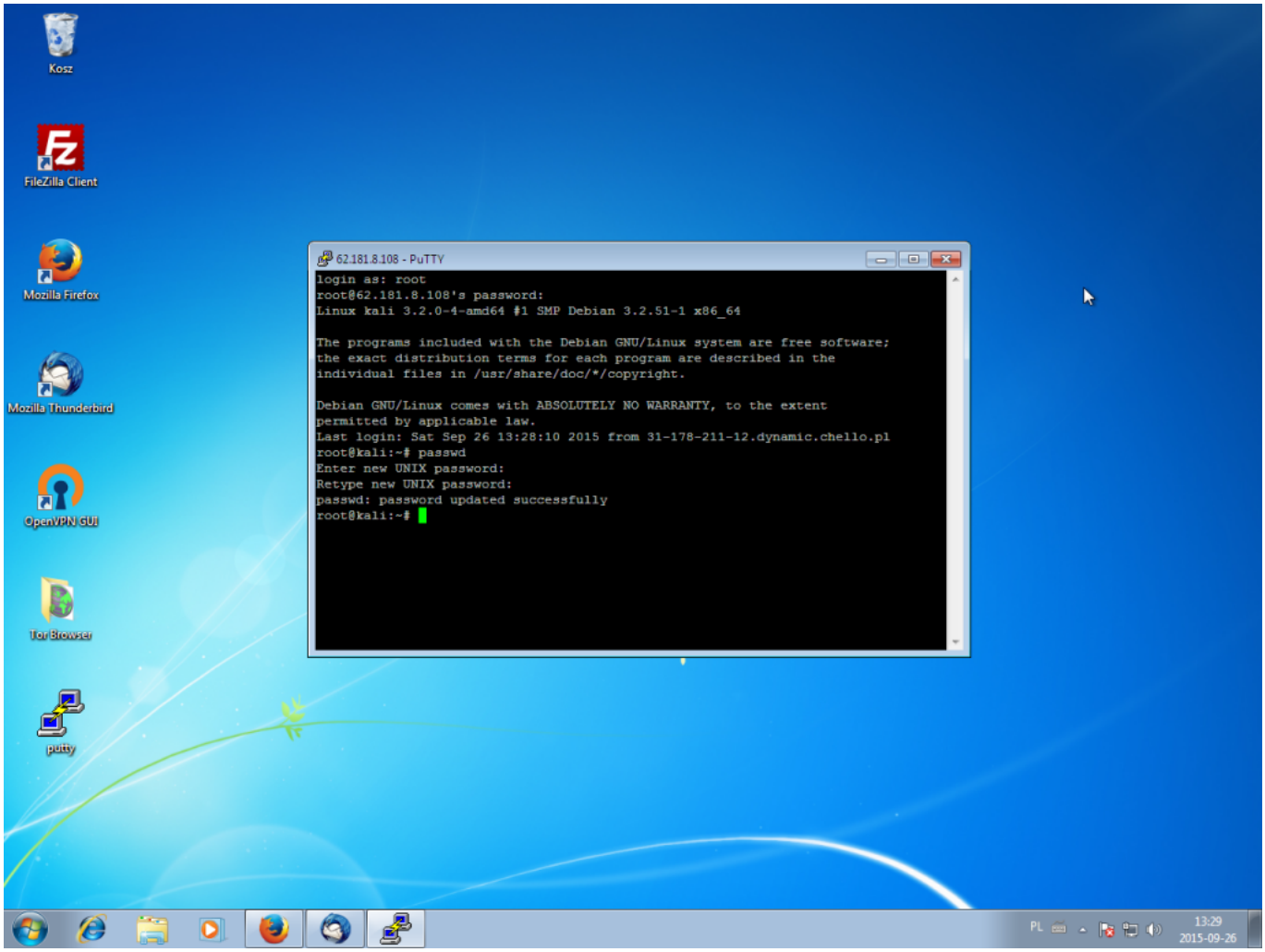
NO SYSTEM IS SAFE

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

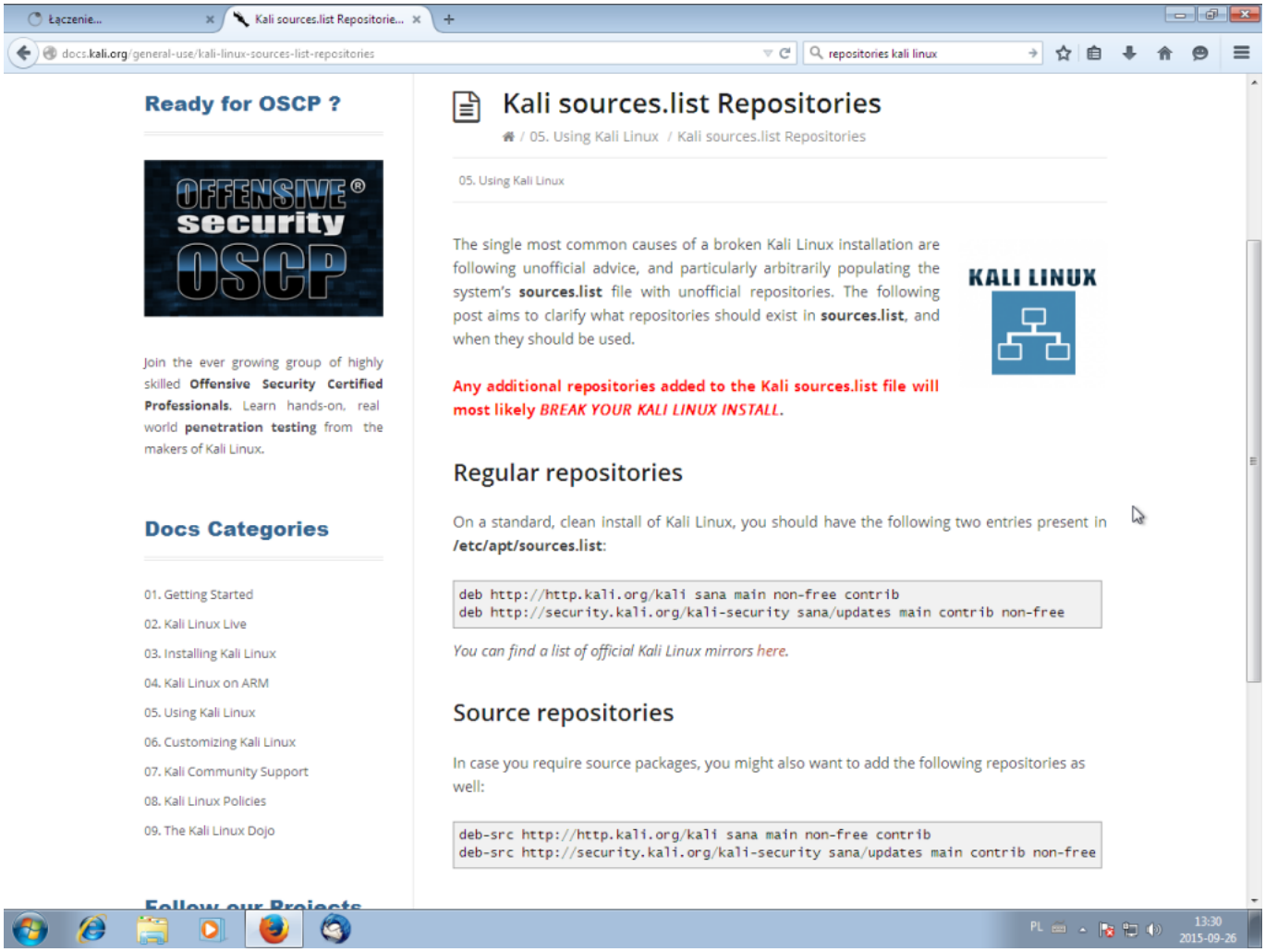




Po zalogowaniu się warto zmienić hasło na trochę bardziej przyjazne użytkownikowi, czyli nam.



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.

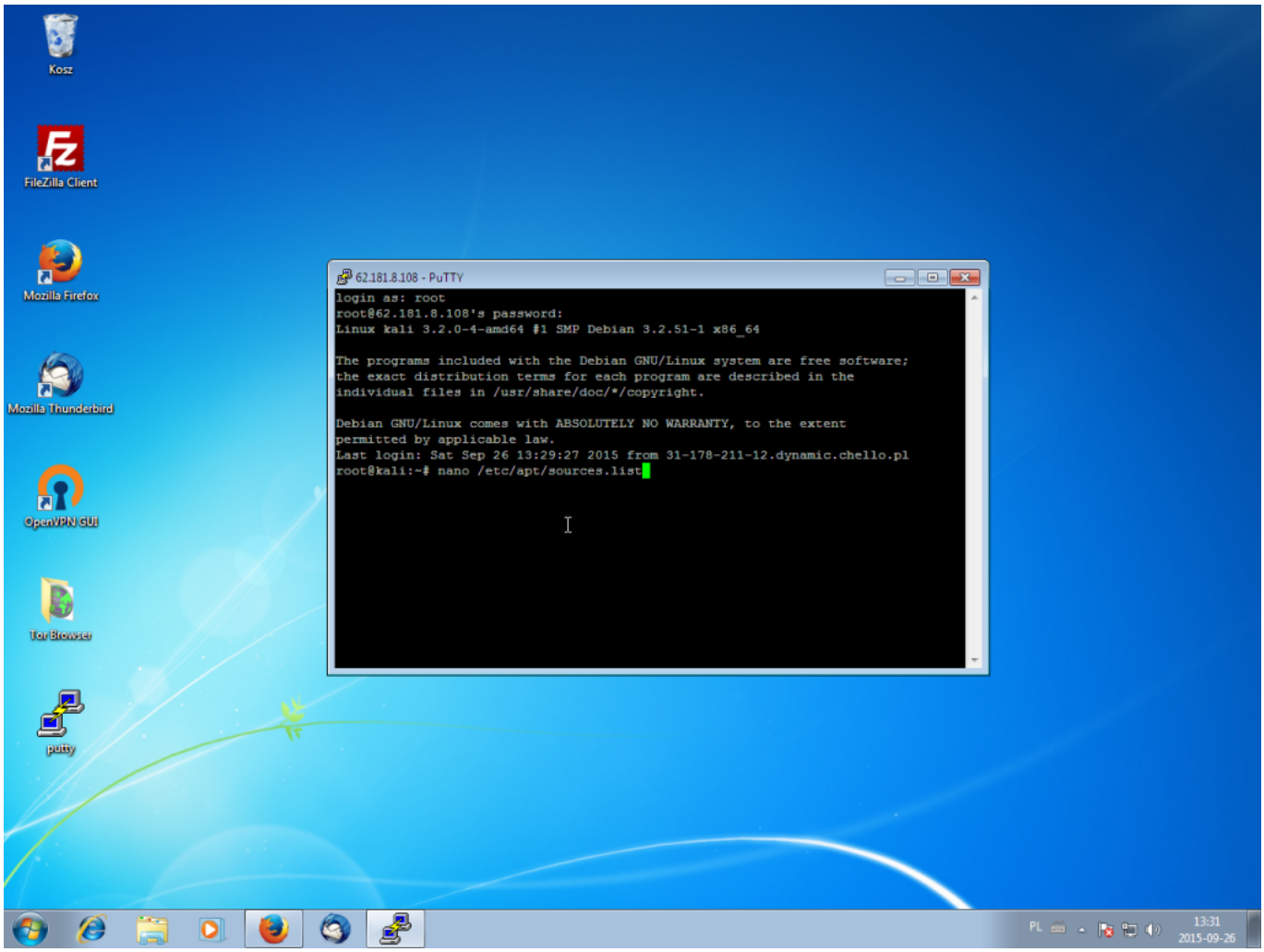


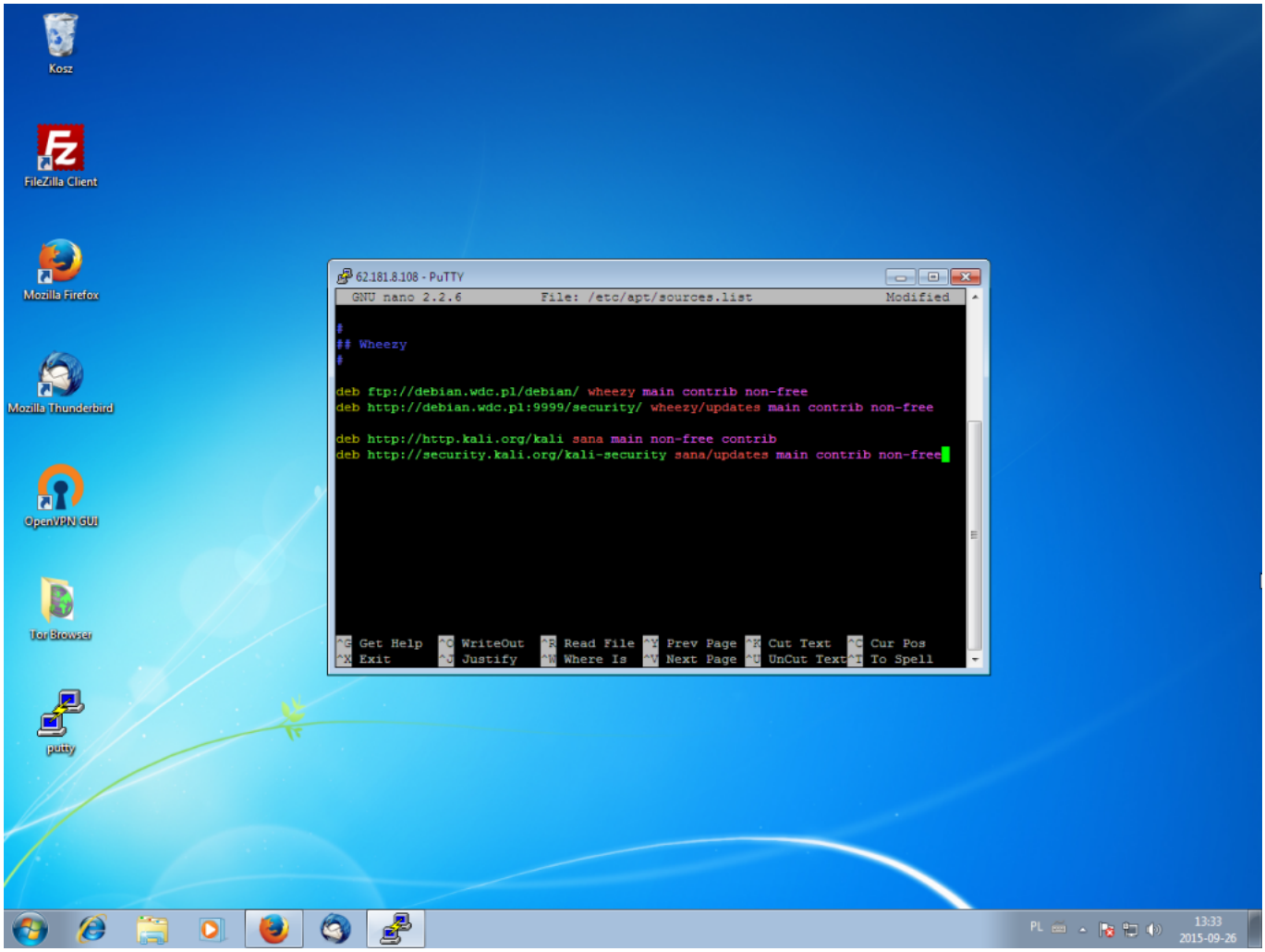
~~deb http://http.kali.org/kali sana main non-free contrib~~
~~deb http://security.kali.org/kali-security sana/updates main contrib non-free~~

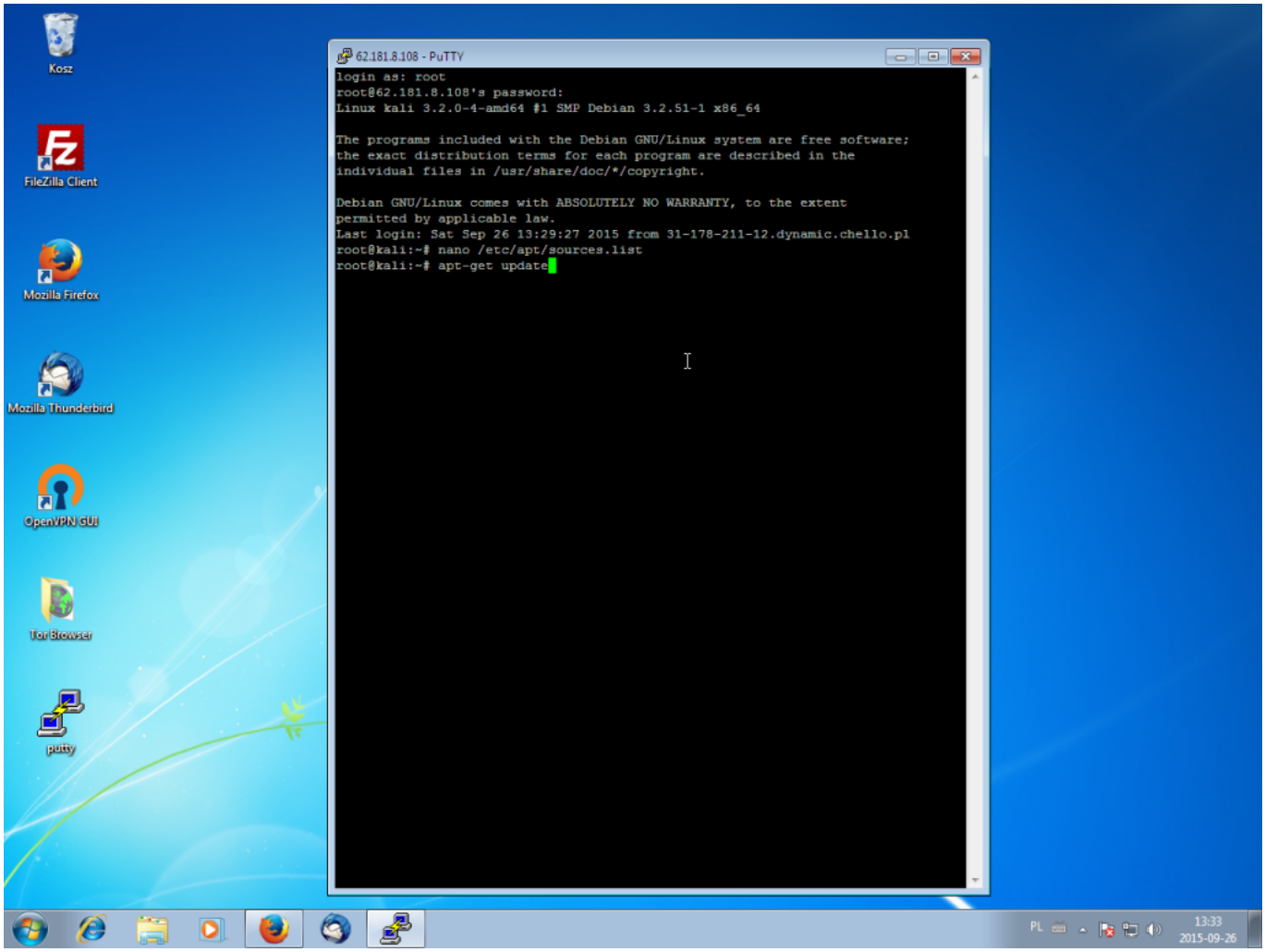
EDIT: Ponieważ dynamika kaliego jest tak duża, że z wersji na wersje zmieniają się linki do repozytoriów, postanowiliśmy przygotować własne repozytorium z pakietami narzędzi z kalilinuxa oraz najnowszymi dostępnymi pakietami na debiana. Zapewni to wygodniejszą i pewniejszą prace z prezentowanymi przez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

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

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



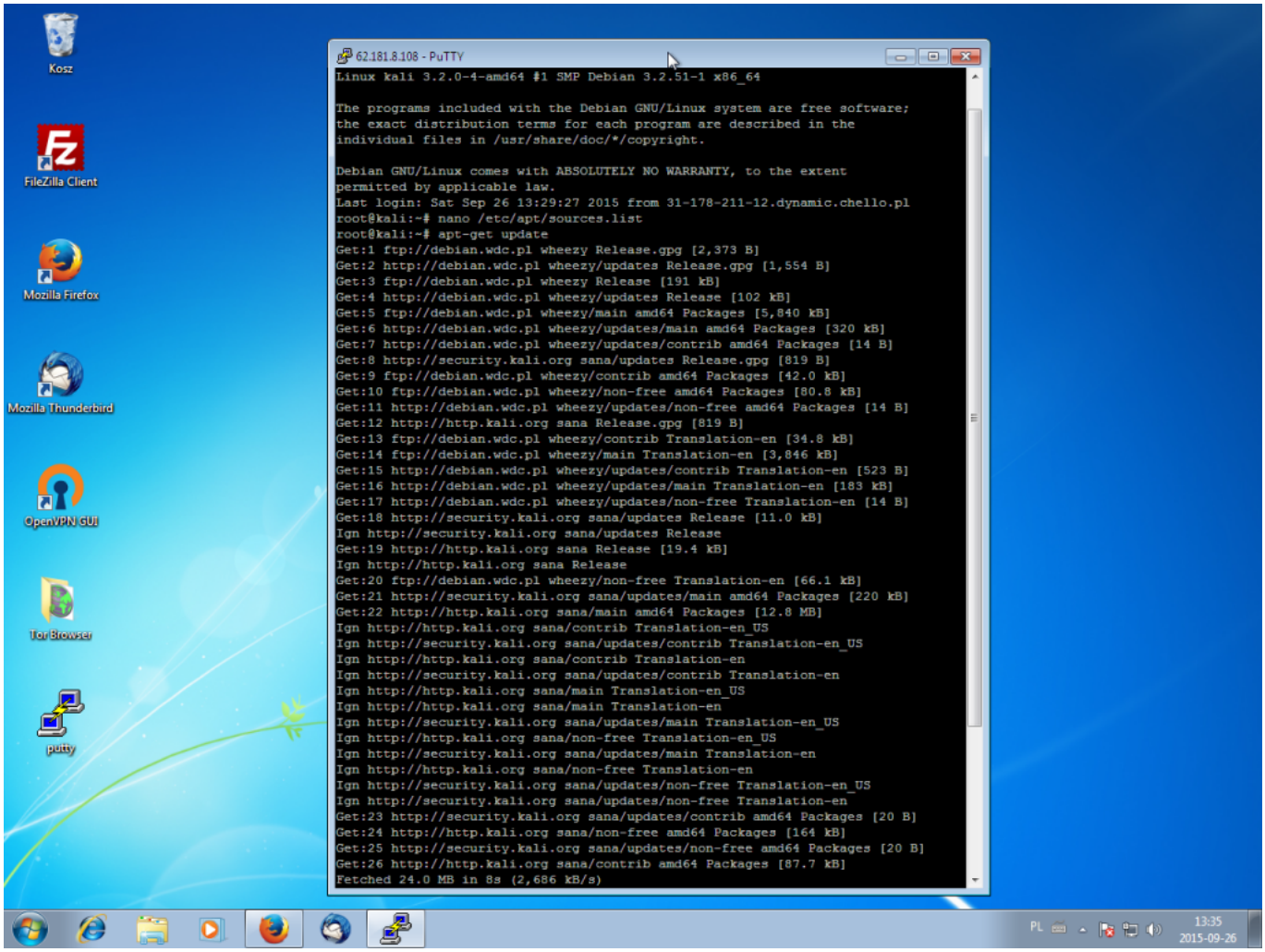

Kosz
FileZilla Client
Mozilla Firefox
Mozilla Thunderbird
OpenVPN GUI
Tor Browser
putty
62.181.8.108 - PuTTY
GNU nano 2.2.6 File: /etc/apt/sources.list Modified
#
Wheezy
#
deb ftp://debian.wdc.pl/debian/ wheezy main contrib non-free
deb http://debian.wdc.pl:9999/security/ wheezy/updates main contrib non-free
deb http://http.kali.org/kali sana main non-free contrib
deb http://security.kali.org/kali-security sana/updates main contrib non-free
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell
PL
13:33
2015-09-26



Następnym krokiem jest wykonanie aktualizacji listy pakietów.

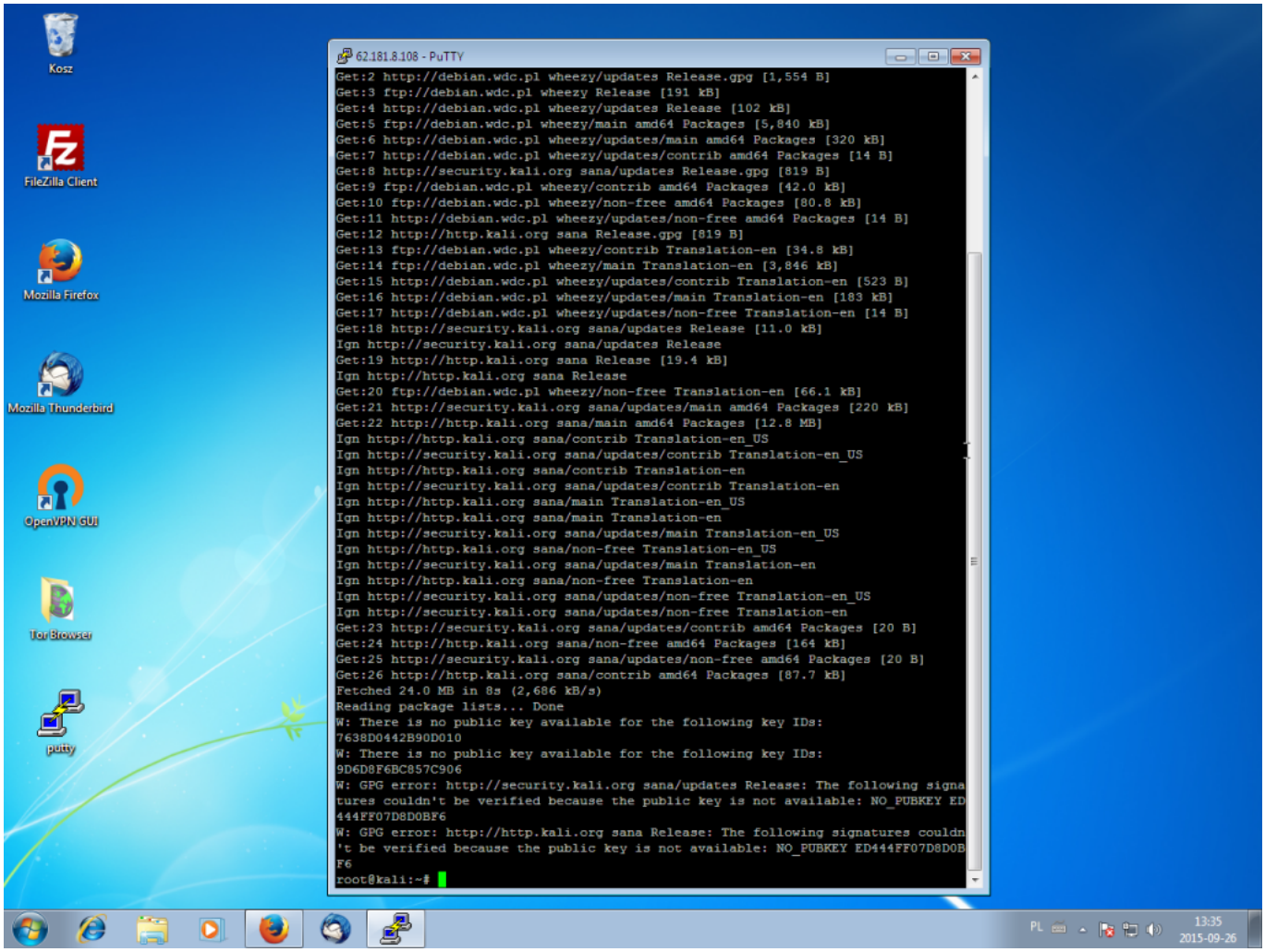
NO SYSTEM IS SAFE

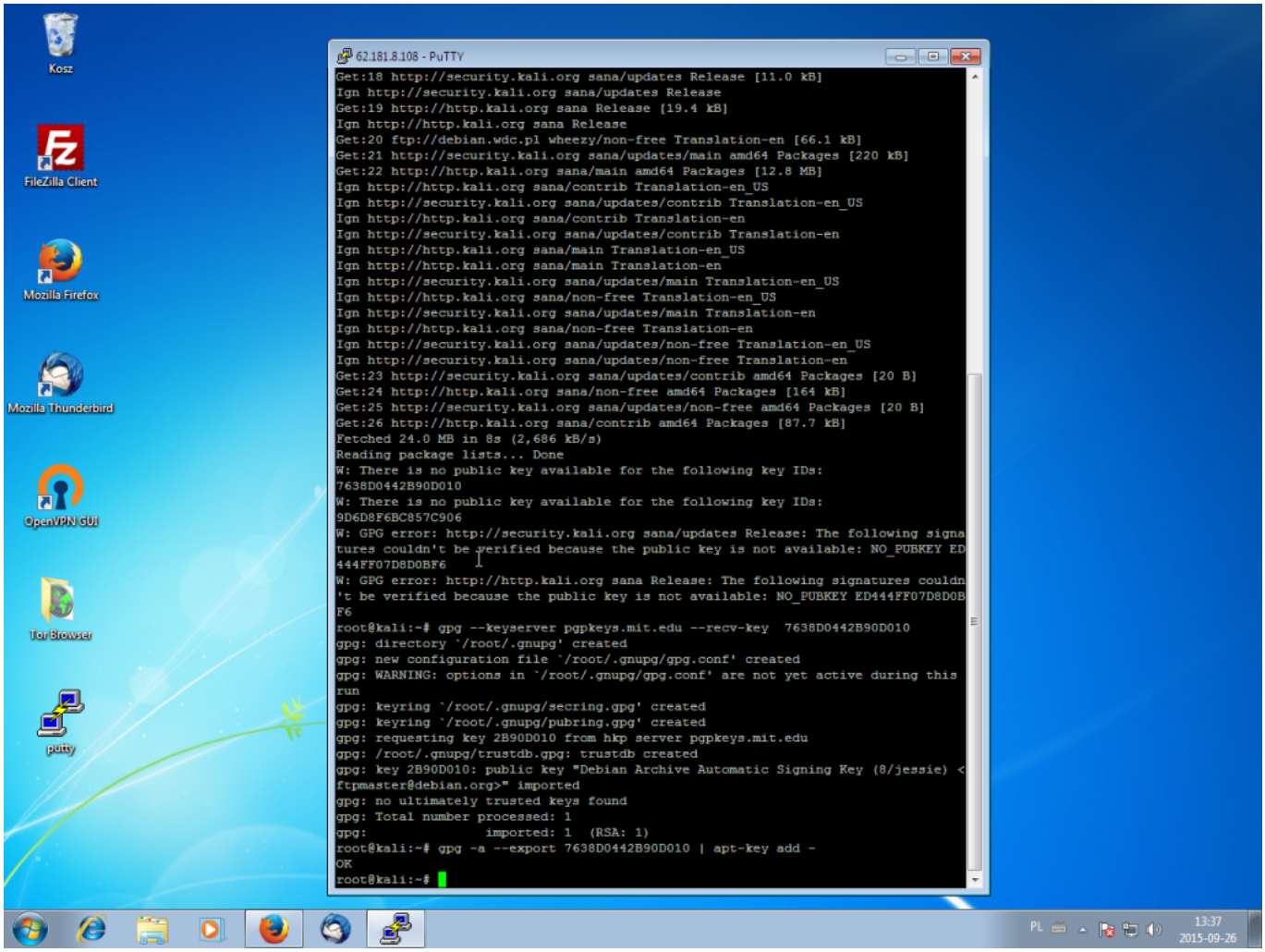
VPS a KaliLinux – Czyli jak mieć publiczny IP podczas używania kaliego.



NO SYSTEM IS SAFE

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.

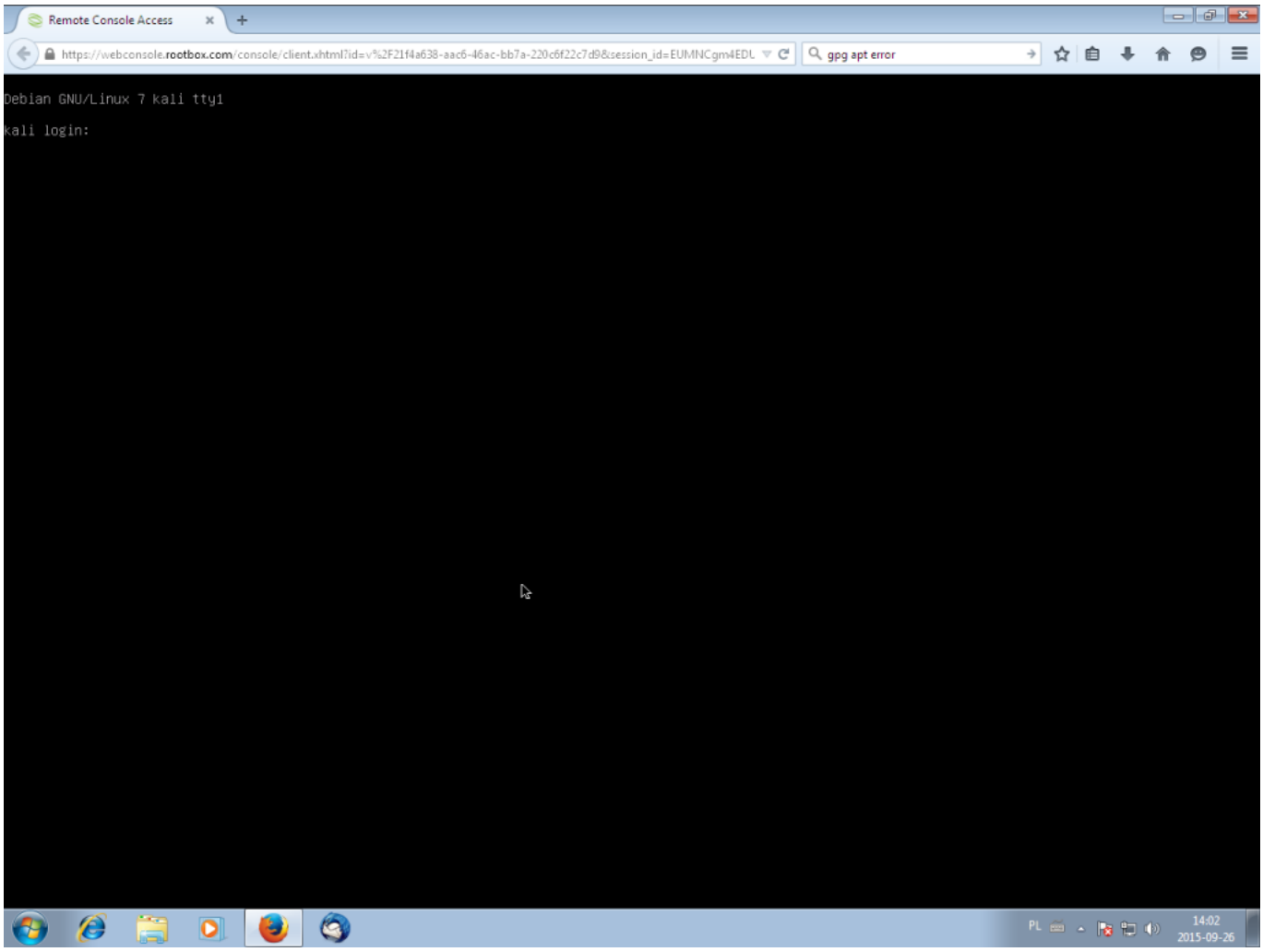
```
gpg --keyserver pgp.mit.edu --recv-keys <klucz>
gpg --armor --export <klucz> | apt-key add -
```

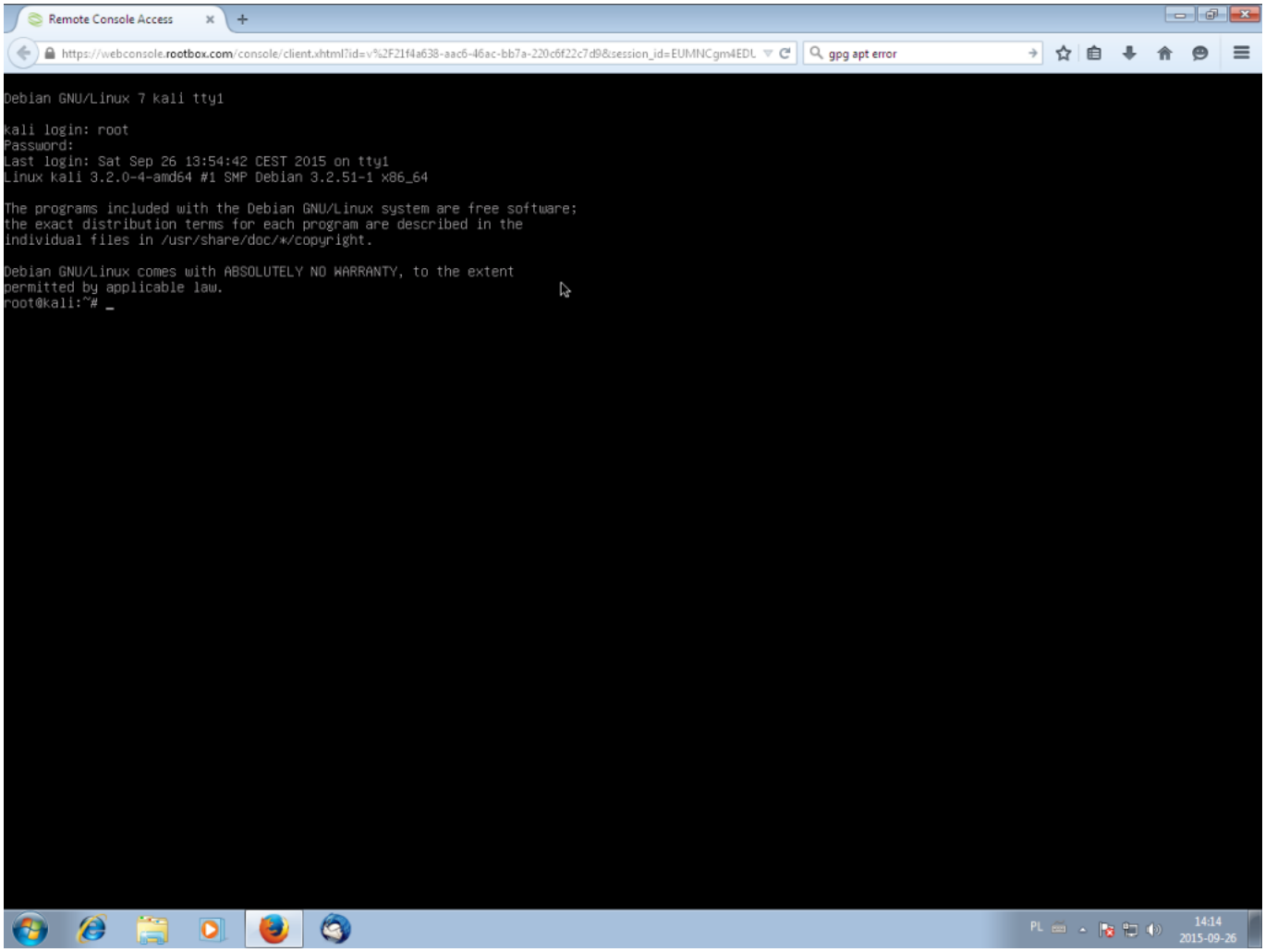
*****EDIT**

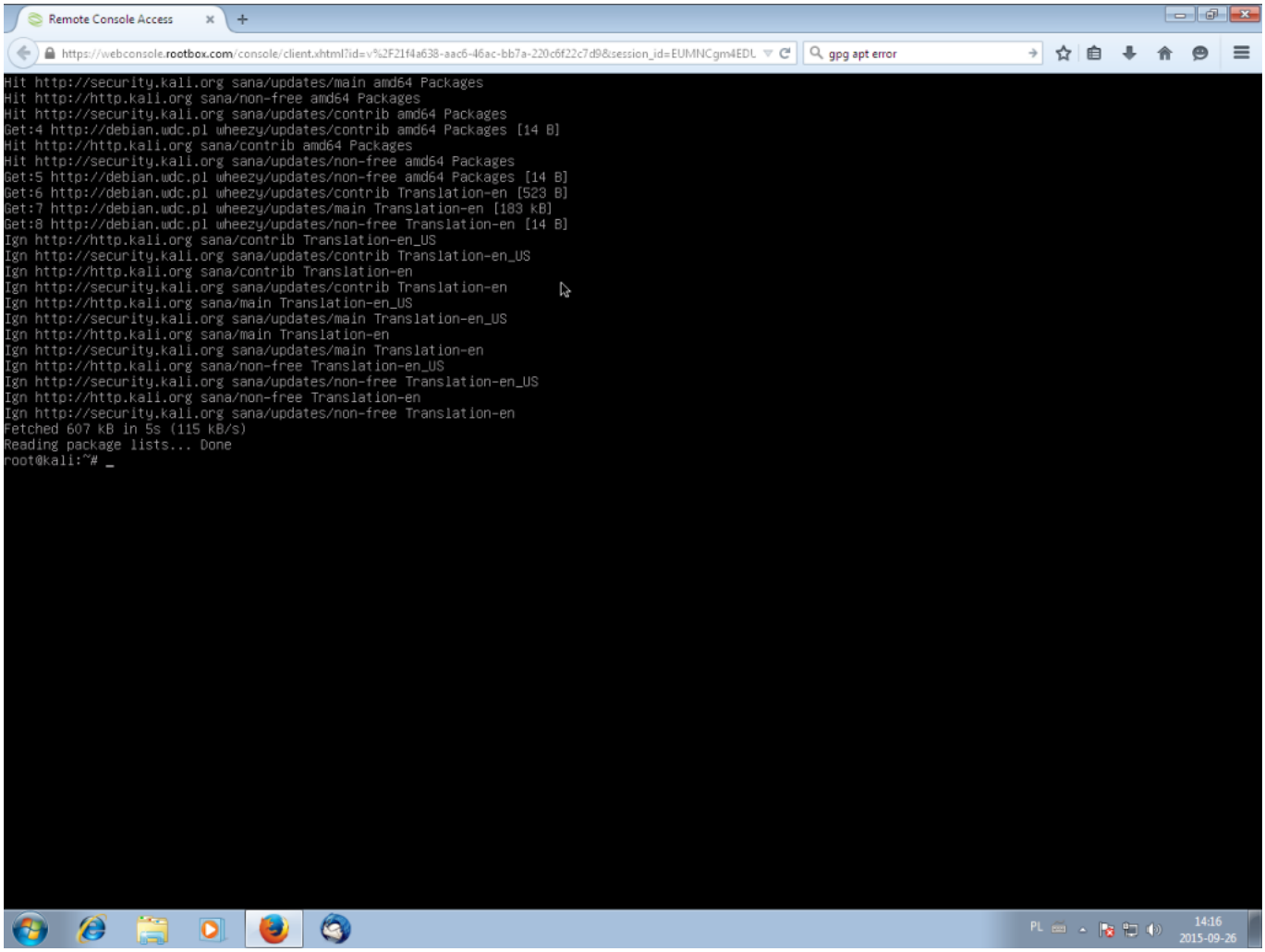
Nasz aktualny klucz publiczny można znaleźć na keybase.io/sms. Zapraszamy serdecznie osoby posiadające konto na kaybase.io do śledzenia naszego profilu

***

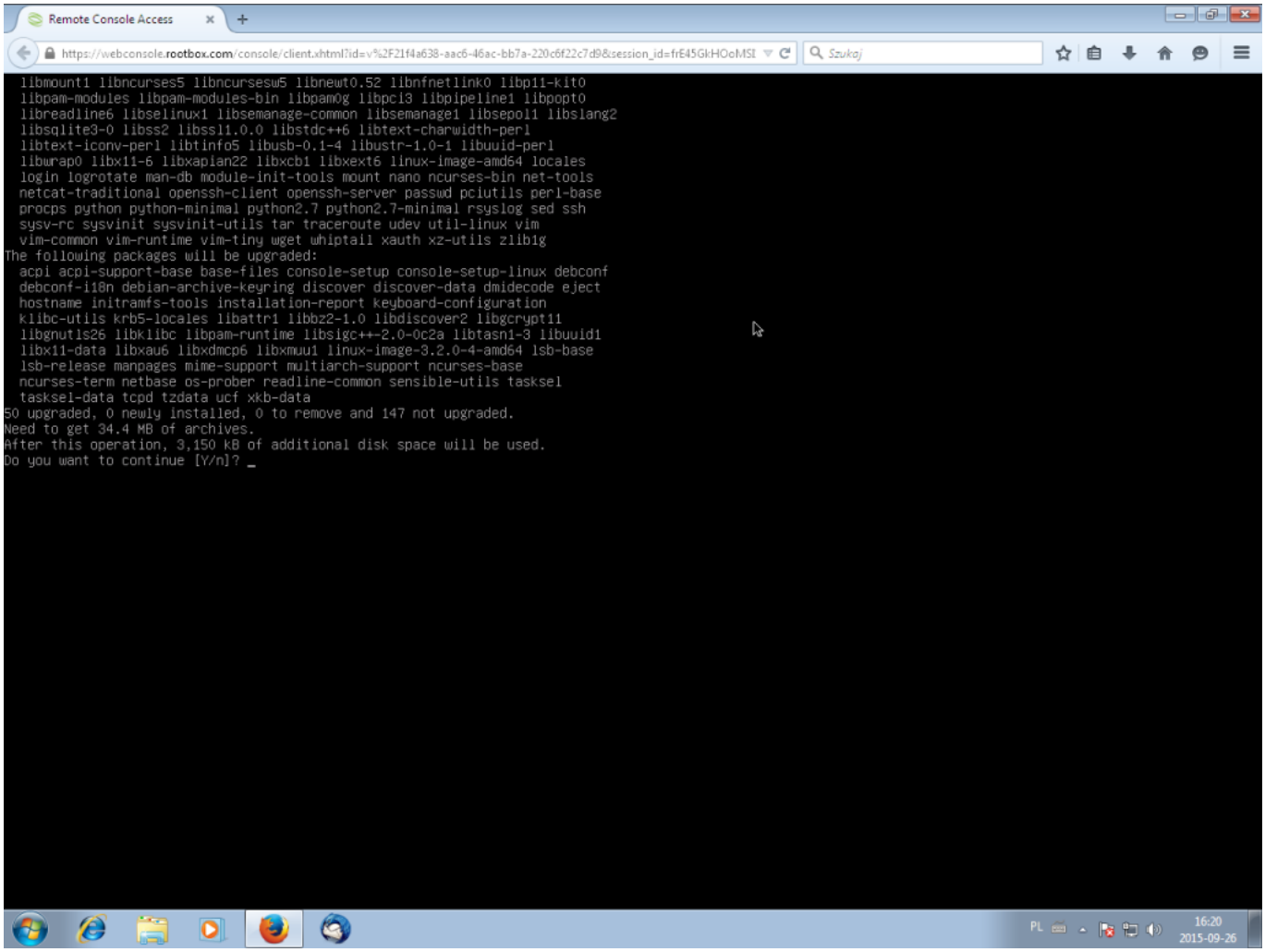
W tym momencie skorzystamy z dodatkowego udogodnienia, którego nie widziałem u innych dostawców, lub po prost on nie działało. Wracamy zatem do naszej przeglądarki, logujemy się do rootbox i przechodzimy do zakładki naszego serwera. Tam wybieramy opcję „Konsola”

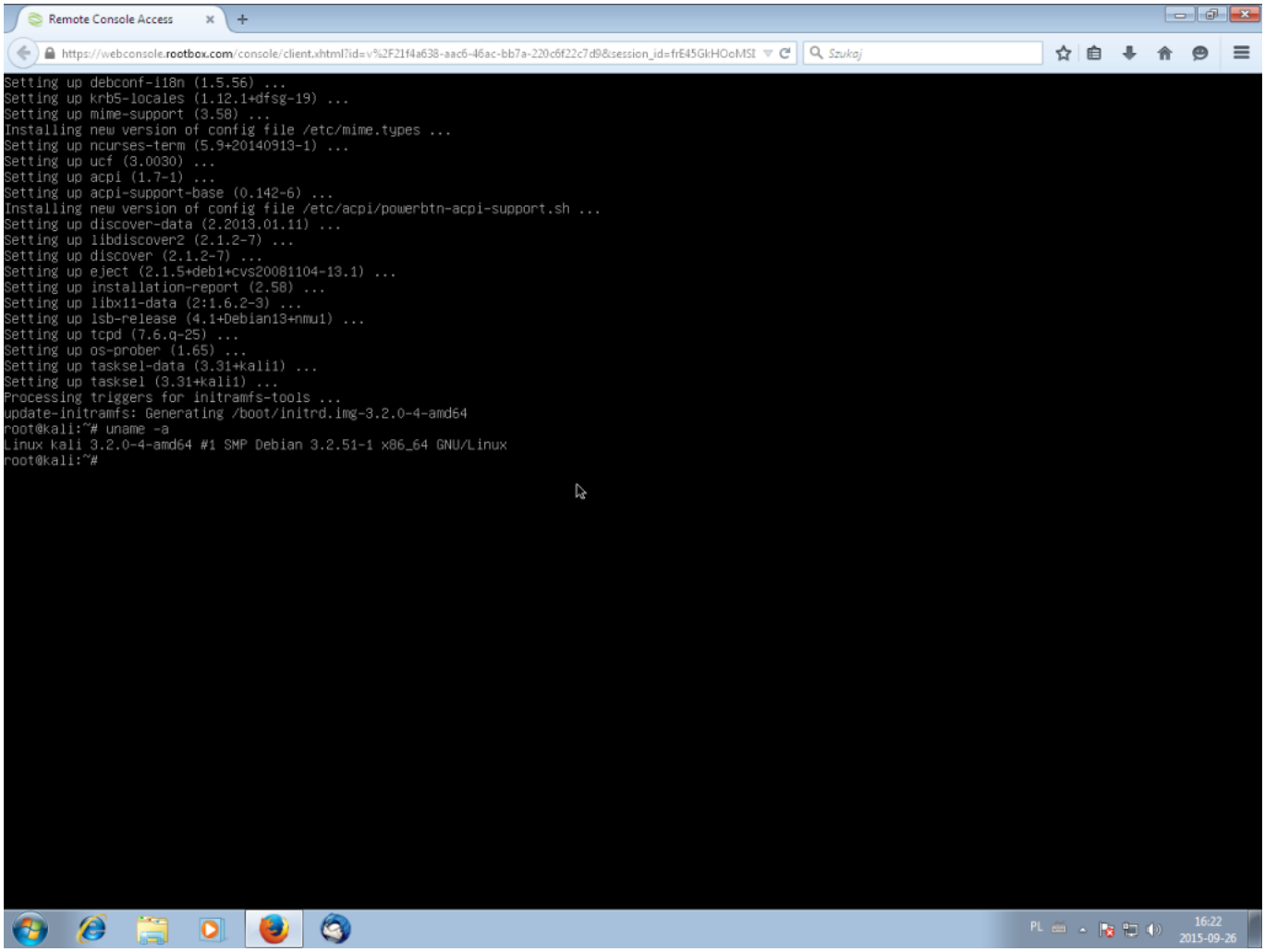



Remote Console Access
https://webconsole.rootbox.com/console/client.xhtml?id=v%2F21f4a638-aac6-46ac-bb7a-220c6f22c7d9&session_id=EUMNCgm4EDL
gpg apt error
Debian GNU/Linux 7 kali tty1
kali login: root
Password:
Last login: Sat Sep 26 13:54:42 CEST 2015 on tty1
Linux kali 3.2.0-4-amd64 #1 SMP Debian 3.2.51-1 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:~# _
PL
14:14
2015-09-26



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


Remote Console Access
https://webconsole.rootbox.com/console/client.xhtml?id=v%2F21f4a638-aac6-46ac-bb7a-220c6f22c7d9&session_id=frE45GkHOoMSI
Szukaj
libmount1 libncurses5 libncursesw5 libnewt0.52 libnfnetlink0 libp11-kit0
libpam-modules libpam-modules-bin libpam0g libpci3 libpipeline1 libpopt0
libreadline6 libselinux1 libsemanage-common libsemanage1 libsepol1 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
libwrap0 libx11-6 libxapian22 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 libgcrypt11
libgnutls26 libklibc libpam-runtime libsigc++-2.0-0c2a libtasn1-3 libuuid1
libx11-data libxau6 libxdmcp6 libxmuu1 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]? _
PL
16:20
2015-09-26



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

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)