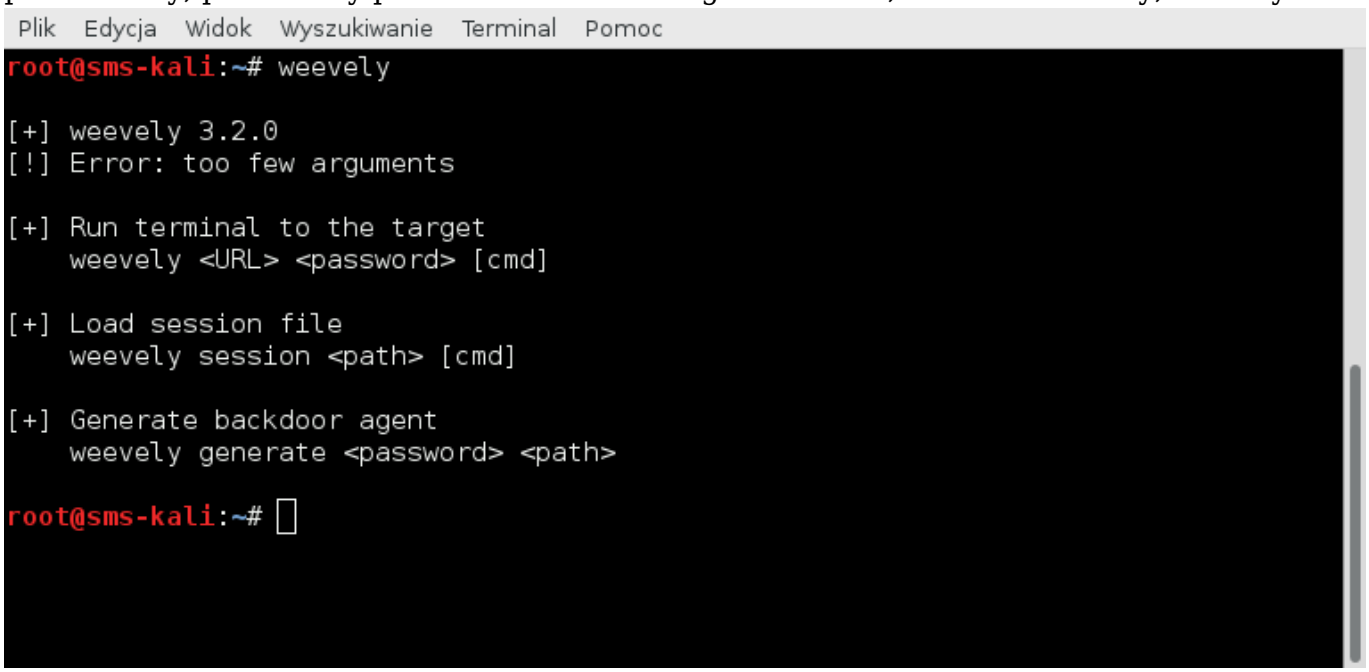
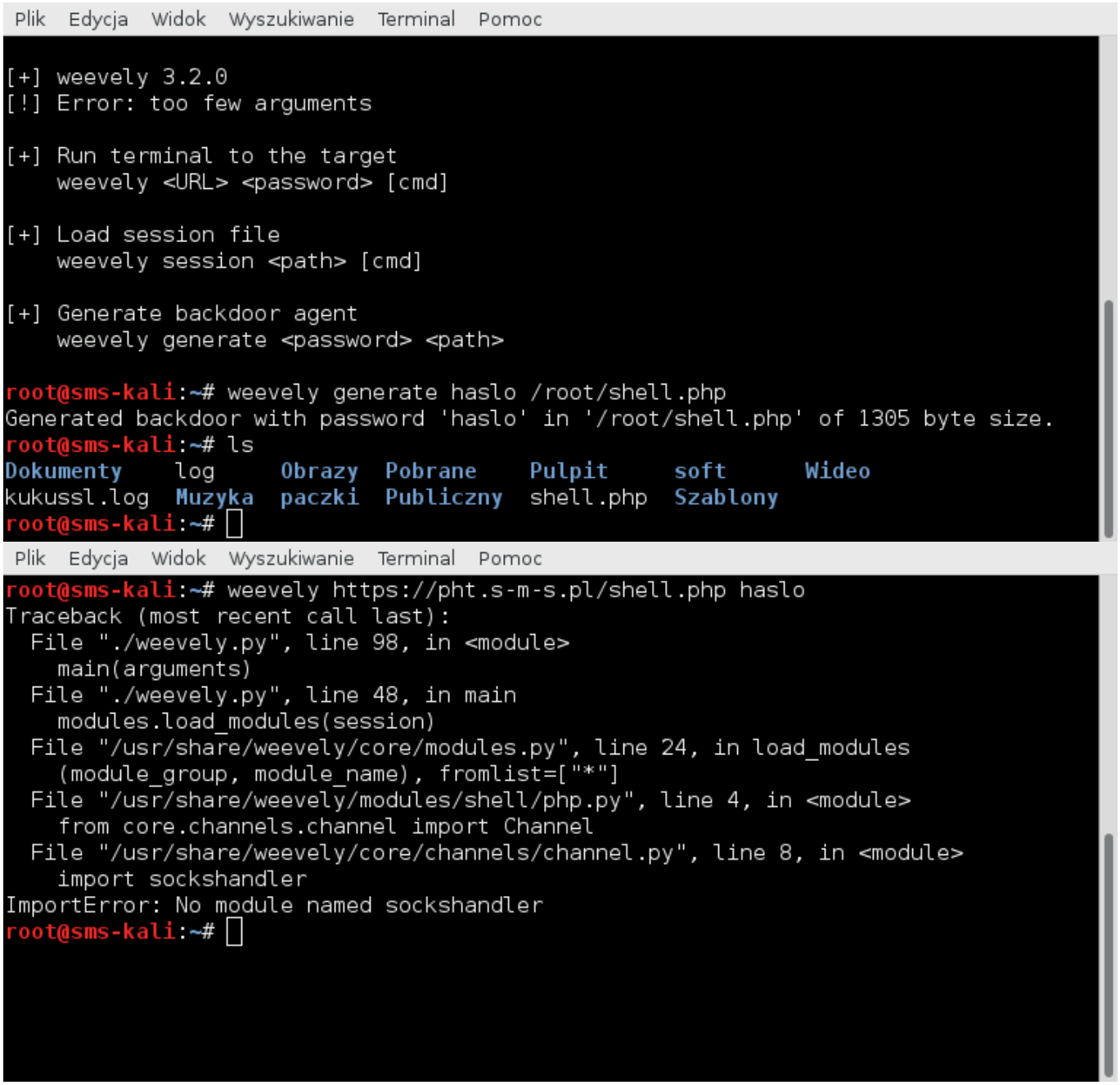
Ostatnio, podczas wykonywania jednego ze zleceń, zauważyliśmy poważny – dla początkujących – błąd w dystrybucji Kali Linux 2.0. Jak się okazało błąd występuje również wtedy, gdy instalujemy program ręcznie, na innych dystrybucjach linuxowych. W dzisiejszym artykule pokażemy jak samodzielnie w kilku krokach naprawić ten błąd.

Weevely jest narzędziem do generowania webshelli oraz zarządzania sesjami za pomocą webshell, którego użycie opisywaliśmy już wcześniej. Postanowiliśmy sprawdzić czy błąd jest powtarzalny, pobraliśmy prosto z serwera Kaliego obraz .iso, zainstalowaliśmy, i oto wynik.





Jak możecie zauważyć, błąd wystapił nawet w oryginalnej, w pełni zaktualizowanej wersji. Oto kilka sposobów jak naprawić ten problem:

1. Manualnie – postepując zgodnie z instrukcjami
2. Używając przygotowanego przez nas skryptu

1. Manualnie

1. Pobierz najnowsze PySocks z https://pypi.python.org/pypi/PySocks/
2. Rozpakuj pakiet w katalogu /tmp
3. Nadaj prawa wykonywalności „chmod 755 /tmp/PySocks/setup.py”
4. Zbuduj pakiet za pomocą „/tmp/PySocks/setup.py build”
5. Zainstaluj „/tmp/PySocks/setup.py install”

2.Używając przygotowanego przez nas skryptu

Source code

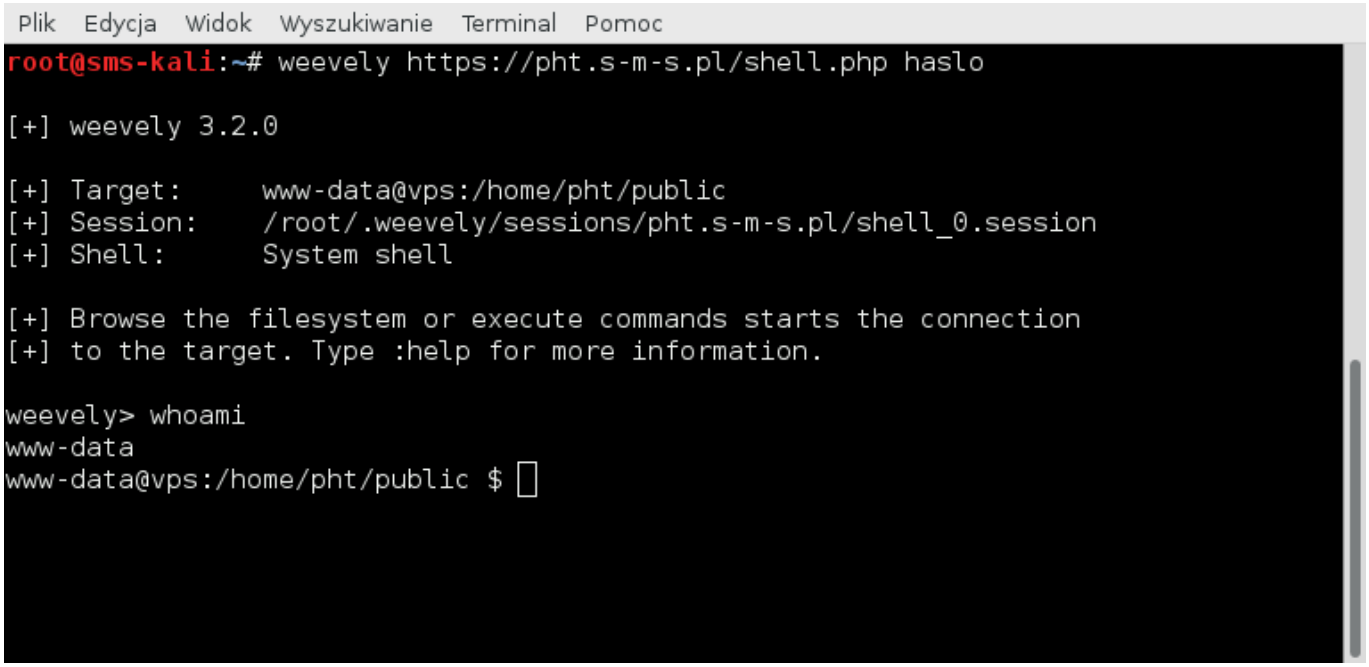
```
#/bin/bash

cd /tmp/

wget
https://pypi.python.org/packages/source/P/PySocks/PySocks-1.5.6.tar.gz
#md5=c825c7c52b2c79dde73cac8d04bd25cb

tar -zxvf PySocks*
cd PySocks*
chmod +x ./setup.py
./setup.py build
./setup.py install
```

Jaki uzyskujemy efekt? W pełni działający backdoor.



Błąd ten występuje także wtedy, kiedy pobieramy Weevely z gita czy z poziomu repo.s-m-s.pl. Instalując program należy pamiętać o naprawieniu tego błędu. Kod skryptu znajduje się w naszym gicie.

Tych kilka prostych kroków naprawi dosyć poważny błąd. Znacie inne błędy tego typu? Dajcie nam znać, chętnie je opiszemy!