**Analiza Wybranych Podatności**

**CVE-2018-10933**

**Autor:** Szymon Litwicki

**Nr albumu:** 264036

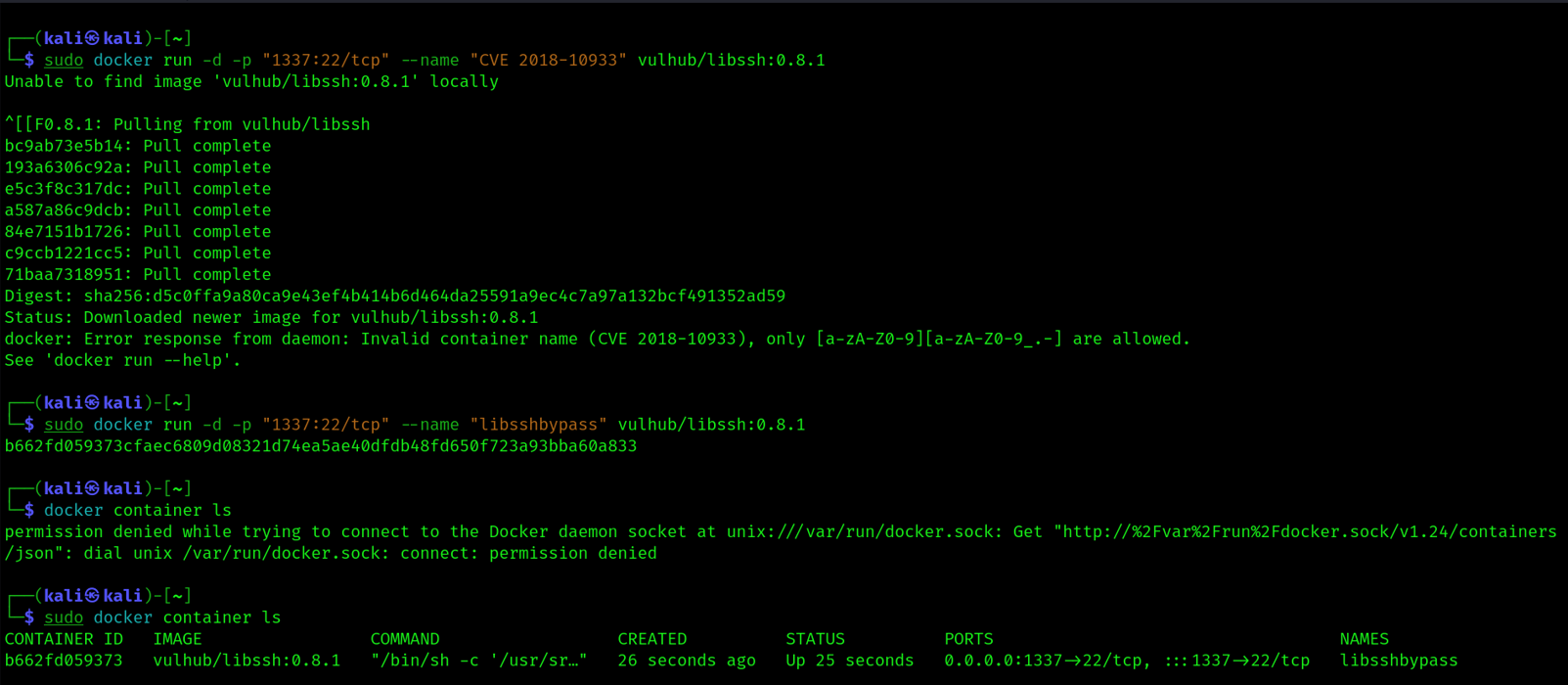
**Nr zespołu:** 2

**CVE-2018-10933**

**Wstęp**

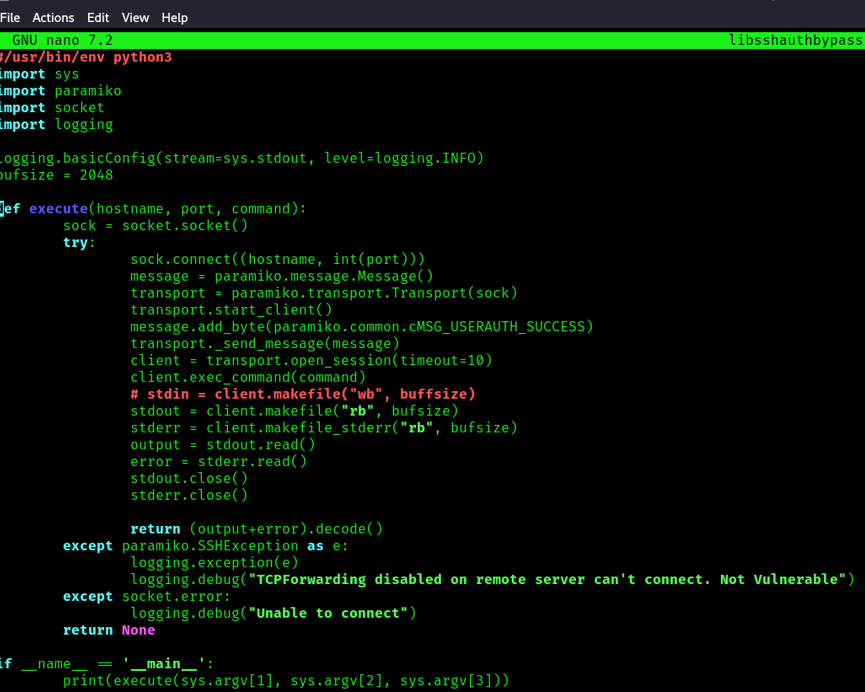
Podatność CVE-2018-10933 została odkryta w oprogramowaniu **libssh**. Znana jest ona również pod nazwą **"LibSSH Authentication Bypass"** Została ujawniona publicznie we wrześniu **2018 roku**. **LibSSH** to biblioteka używana do implementacji protokołu SSH w różnych aplikacjach i narzędziach. Podatność CVE-2018-10933 pozwala uzyskać atakującemu nieautoryzowany dostęp do systemu za pomocą protokołu SSH, wykorzystując błąd w procesie uwierzytelniania w bibliotece LibSSH. Owy błąd występował w kodzie odpowiedzialnym za autentykację klienta SSH, który nieprawidłowo obsługiwał sytuację, gdy klient przekazywał komunikat **SSH2\_MSG\_USERAUTH\_SUCCESS** jako odpowiedź na próbę uwierzytelnienia, podczas gdy faktycznie nie była ona prawidłowo zakończona. Skutkowało to możliwością uzyskania dostępu do systemu bez znajomości prawidłowego hasła lub klucza prywatnego. Podatność CVE-2018-10933 dotyczyła wersji biblioteki **LibSSH** od wersji **0.6** do wersji **0.7.6**.

**Przygotowanie do analizy**

Największym wyzwaniem w analizie tej podatności było skonfigurowanie środowiska, ponieważ nie udało mi się znaleźć obrazu ISO systemu z podatną na ten atak wersją biblioteki libssh. Próby instalacji podatnych wersji tej biblioteki również się nie udały, w dużej mierze ze względu na brak takich zasobów. Udało mi się jednak znaleźć podatny, przygotowany do tego testu kontener Dockera i to na nim przeprowadziłem analizę. Kontener uruchomiłem lokalnie na maszynie Kali Linux, użytej przy testowaniu poprzedniej podatności (CVE-2016-5195).

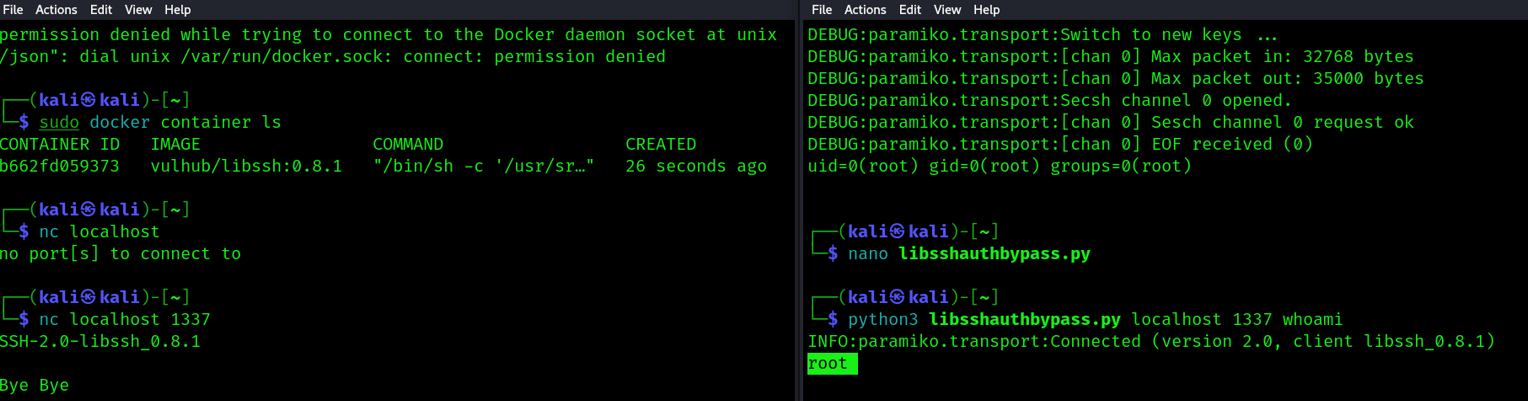
Rysunek 1 Utworzenie kontenera z podatnym na atak oprogramowaniem

Na tym etapie konieczne również było przygotowanie odpowiedniego skryptu wykorzystującego badaną podatność. Stosowny skrypt w języku Python jest standardowo dostępny w systemie Kali Linux. W argumentach wywołania wymaga on podania adresu hosta do którego się łączymy, portu i komendy jaka ma być wykonana w systemie ofiary.



Rysunek 2 Kod exploitu

**Wykorzystanie podatności**

Wykonanie tego ataku polega na wykonaniu skryptu z pożądaną komendą – w tym przypadku **whoami**, na potwierdzenie zdobytych uprawnień w atakowanym systemie

Rysunek 3 Wykonanie exploitu z poleceniem whoami

**Podsumowanie**

Analizowana podatność CVE-2018-10933 okazała się być krytyczna. Była ona spowodowana przez błędy w oprogramowaniu i w celu ochrony przed jej wykorzystaniem należy dbać o aktualność używanych rozwiązań i instalowanie poprawek bezpieczeństwa.