# Zasady

* Należy napisać skrypt (eksploit/solver), który po uruchomieniu przeprowadza atak i uruchamia program “/bin/sh” (dokładniejszy opis poniżej).
* Skrypt rozwiązujący powinien być możliwie niewielki, łatwy do uruchomienia.
* Preferowane rozwiązania to skrypt w pythonie, korzystający z biblioteki pwntools (nie jest to wymagane, ale zalecane, gdyż to bardzo ułatwia życie).
* Eksploit oraz krótki opis rozwiązania należy wysyłać mailem z tytułem **[CTFUW2017] Duże zadanie PWN**
* Adresatami powinni być:
  + [borys.poplawski@codilime.com](mailto:borys.poplawski@codilime.com)
  + [psrok1@gmail.com](mailto:psrok1@gmail.com)
  + W CC: [kdr@mimuw.edu.pl](mailto:kdr@mimuw.edu.pl)
* Rozwiązania należy przesyłać do **północy z ~~1 na 2 lipca~~ 6 na 7 lipca**.

# Założenia

* Zadanie składa się z dwóch części:
  + należy odpalić program “/bin/sh” z głównego wątku eksploitowanego programu
  + wyeksploitować (odpalić shella) drugi wątek obecny w programie po uprzednim odpaleniu skryptu załączonego w folderze z zadaniem:  
    sudo ./prepare\_chall.sh  
    (więcej informacji w środku skryptu)
* Można zrobić tylko jeden z powyższych punktów. Prawdopodobna punktacja: 7-8 za pierwszy, 15 za drugi.
* ASLR włączony.
* Rozwiązanie ma działać na obrazie maszyny, na którym pracowaliśmy (w domyślnej tj. startowej jej konfiguracji).
* Wzorcowe rozwiązanie nie wymaga żadnego brutowania.
* Można zasymulować zdalną eksploitację, przez odpalenie:

socat TCP-LISTEN:31337,fork EXEC:'./chall "/dev/null" '

i podłączenie się lokalnie na porcie 31337 - nie powinno to zmieniać sposobu, skuteczności oraz czasu działania rozwiązania (implikuje to, że nie kontrolujemy argumentów programu, limitów itp.)

# Przydatne rzeczy

* handle SIGALRM ignore - w gdb, ignoruje sygnały SIGALRM
* https://sourceware.org/gdb/onlinedocs/gdb/Threads.html

# Uwagi:

* 23.06: program “/bin/sh” (dash, bash też tak robi) ustawia effective uid na real uid, ale istnieje funkcja setresuid, której można (należy) użyć...