Bezpieczeństwo

Laboratorium 7

Działanie programu

Program sprawdza czy został podany jeden parametr.

Wyświetla komunikat aby wprowadzić kod długości 12 .

Program zawsze w porównaniu zwraca liczbę większą od zera co przekłada się na wypisanie zawsze informacji że nam się nie udało.

Rozwiązanie

Pierwszym rozwiązaniem było dopisanie do wpisanego kodu funkcji powrotu w inne miejsce.
Aby wykonać taką operację należało policzyć miejsca za pomocą GDB wyświetlając miejsca na stosie. Z obliczeń wyszło że miejsc na kod jest 25. Aby nadpisać adres powrotu należy wpisać 4 bajtowy adres do którego funkcja ma powrócić. Na przykład funkcje destroy world. W kolejnym rozwiązaniu wywołaliśmy basha do które ścieżka przypadkiem znalazła się w pliku. Aby tego dokonać do stosu dodaliśmy kolejno:

- 25 znaków x adres powrotu
- Adres powrotu (funkcja wywołująca basha)
- Adres powrotu – funkcja System exit
- Argument /bin/bash
- Parametr funkcji exit -3

Rozwiązanie : gdb --args exploitme_pn `perl -e'print "x"x25 ."\x54\x84\x04\x08" ."\xd4\x84\x04\x08" ."\xd0\x87\x04\x08" ."\x03\x00\x00\x00"'`