Learning UNИX binutils for fun and profit

Fedor Sakharov

Noone at REDSecure.ru
mailto:sakharov@lvk.cs.msu.su

22 ноября 2010 г.

Что в меню?

Исполняемые файлы в Linux

- scripts
- Немного о ELF
- ld
- Переменные окружения
- Процесс связывания

A fistful of swiss army knives

- objdump
- readelf
- ldd
- etc., wtf

Что можно исполнять?

- plaintext #!/bin/bash
- a.out (a very old format)
- *COFF (deprecated)
- ELF

Всю подробную информацию о файлах (в т.ч. и исполняемых) вы можете узнать с помощью утилиты file.

ELF (1/2)

Executable Linkable Format

Может содержать код в любом виде

- Исполняемые файлы
- Динамически загружаемые библиотеки (*.so)
- Объектный код

Разница между исполняемым файлом и динамически загружаемой библиотекой лишь в том, что библиотеки нет точки входа (main)

ELF (2/2)

Содержит данные в различых секциях:

- .bss
- .data
- .dynamic
- .interp
- .text
- .... man page: ELF

Name mangling

ELF создавался для приложений на C (и Fortran).

Внезапно C++

```
class bar {
    void main(int);
    void main(int, char);
};

int main( int argc, char ** argv ) {
    return 0;
}
```

Как всем этим main функциям жить в одном исполняемом файле?

Name mangling

В C++ было предложено обойтись хаком, позволяющим использовать код, написанный на C++ в ELF.

- void main(int, char) -> void _Z1mainic(char, int)
- Для того, чтобы не спутать замангленные имена с уже использованными в программе, перед именем используются одно или два подчеркивания.

Binary interpreter

- Dynamic linker обычно жил в /lib/ld.so
- Для GNU/Linux это /lib/ld.so.* для файлов формата a.out. /lib/ld-linux.so.* (currently .2) для ELF.
- В системе может быть более одного бинарного интерпретатора.
- Consider the .interp section of the ELF file.

dlopen

Иногда, имя внешней функции или библиотеки неизвестно во время компиляции.
Линкер предоставляет механизм dlopen()

```
handle = dlopen( "/usr/local/lib/libbar.so",
                                        RTLD_LOCAL );
*(void **)(&fptr) = dlsym(handle, "my_function" );

(*fptr)(32);
```

More at dlopen(3)

Environment variables

/lib/ld*so* использует переменные окружения для поиска динамических библиотек при загрузке приложения.

По умолчанию, поиск производится в

- /lib и /usr/lib
- /etc/ld.so.cache и /etc/ld.so.preload

Часто используемые переменные:
LD_LIBRARY_PATH
LD_PRELOAD
LD_TRACE_LOADED_OBJECTS

GNU toolchain

- make
- gcc
- autotools
- binutils

binutils

- as
- ld
- gprof
- c++filt
- objdump
- readelf
- strings

c++filt

Позволяет демангли́ть имена из бинарного кода, написанного на C++.
Автоматически определяет тип манглинга имен.

objdump

Swiss army knife of disassembling.
Useful options:

- −−demangle
- −−disassemble-all

readelf

Предназначено только для ELF файлов. Useful options:

- −−dynamic
- −−symbols
- −−all

Questions?

Questions?