Return oriented programming

Игорь Черватюк

Александр Трифанов

Андрей Басарыгин

Москва, 2018

Используемые инструменты

Unix-like:

ldd

strace

readelf

objdump

ropper\ropgadget

gdb\edb

Windows:

mona.py

ropper

Отладчик по вкусу

Инструменты: strace

Утилита, отслеживающая системные вызовы. С помощью strace можно посмотреть, какие системные вызовы происходят при взаимодействии между процессом и ядром операционной системы.

https://habrahabr.ru/post/215577/

Инструменты: readelf и objdump

Обе утилиты используются для извлечения информации из ELF-файлов.

readelf – не зависит от используемой архитектуры;

objdump – нужен разный в зависимости от того, какой объект обрабатывается.

https://stackoverflow.com/questions/8979664/readelf-vs-objdump-why-are-both-needed

https://jvns.ca/blog/2014/09/06/how-to-read-an-executable/

Инструменты: ropper\ropgadget

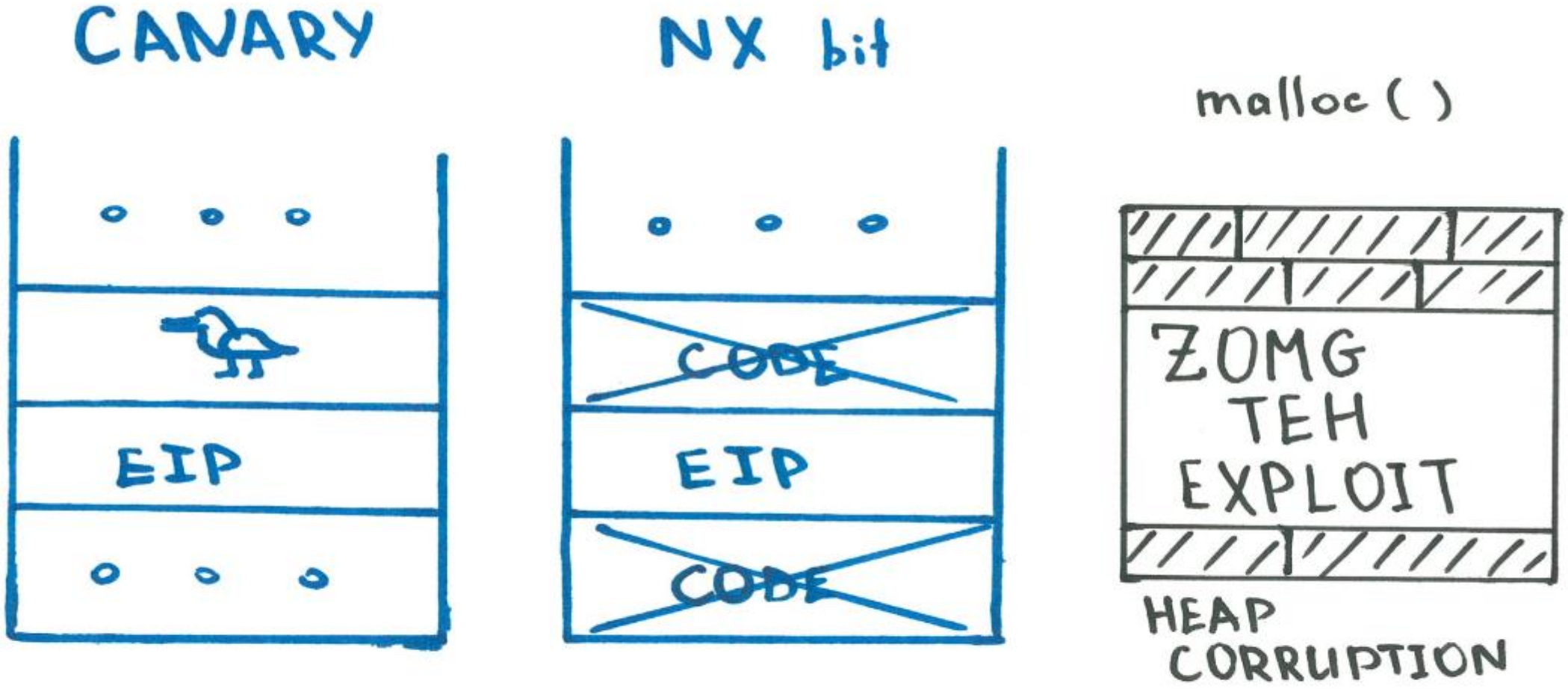
Ropper\ropgadget – используется для поиска гаджетов и для автоматического составления из них ROP-цепочек.

Return oriented programming

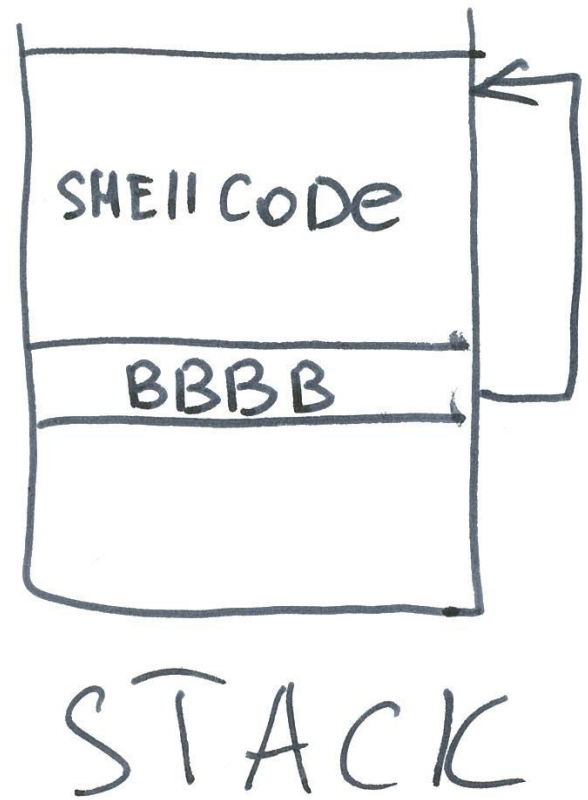
Или возвратно-ориентированное программирование – техника эксплуатации при которой атакующий обладает контролем за стеком программы и использует функциональность самой программы или сопутствующих ей библиотек для проведения атаки.

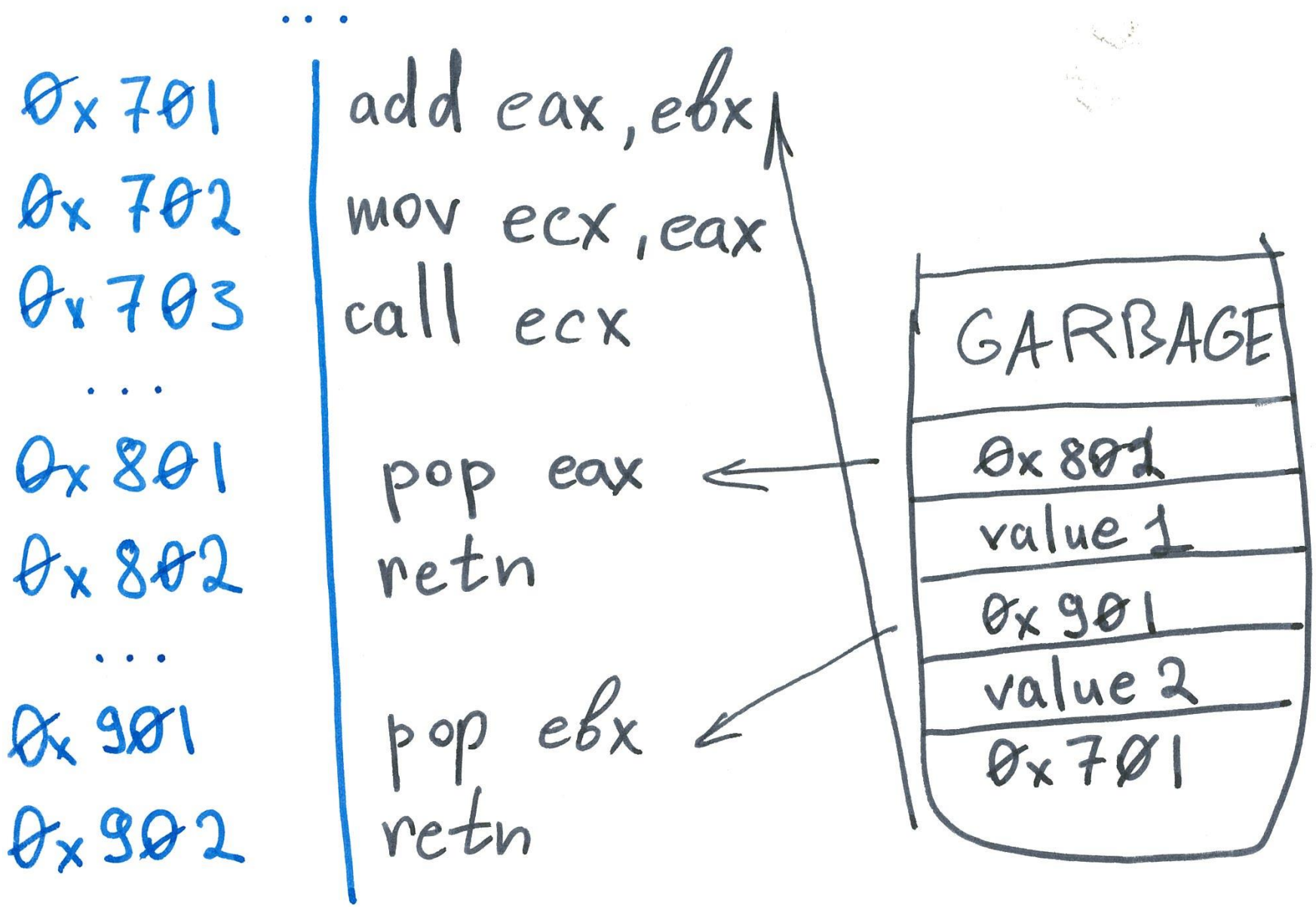
Первая академическая статья на эту тему:

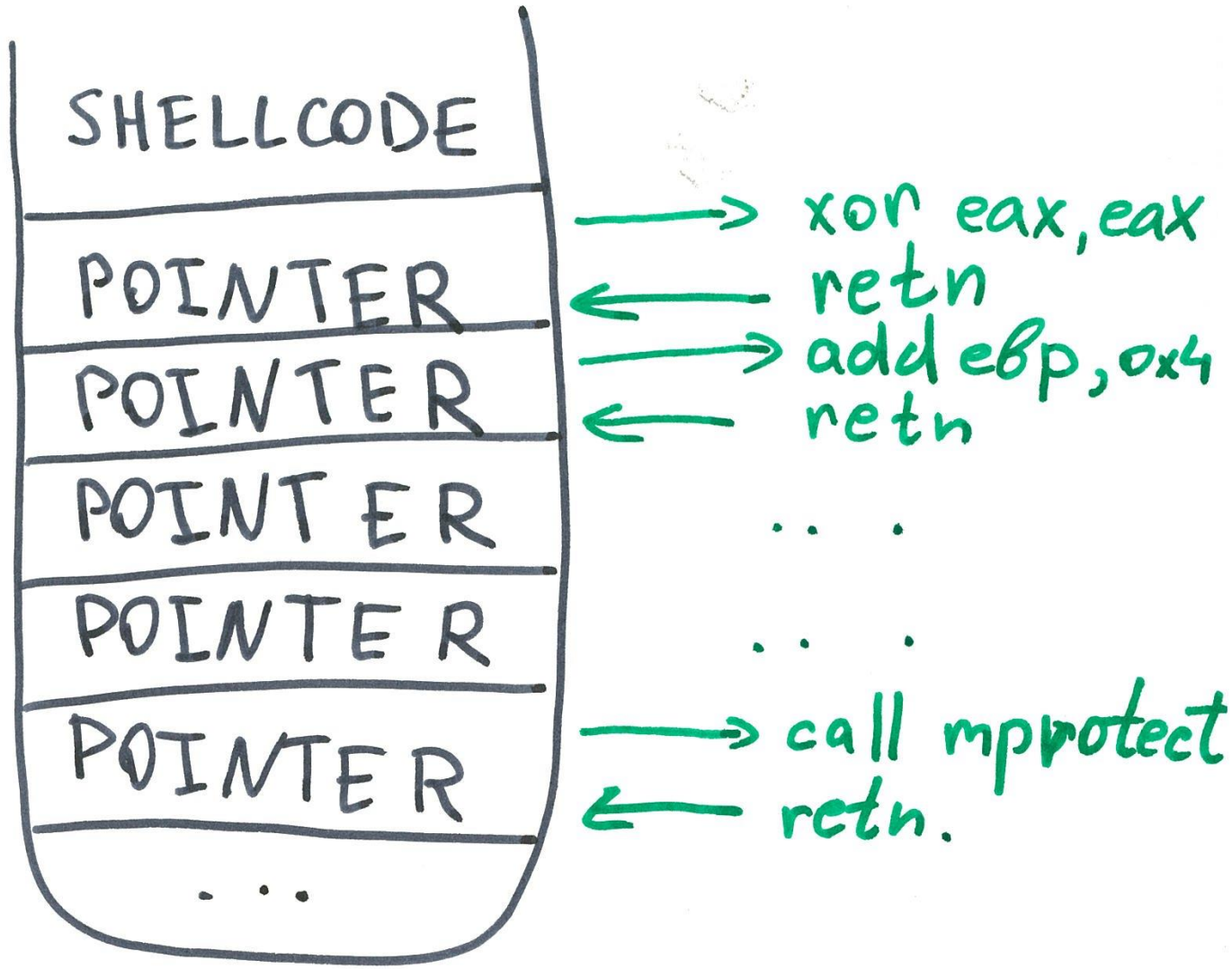
http://cseweb.ucsd.edu/~hovav/dist/geometry.pdf


CANARY
NX bit
malloc ( )
EIP
CODE
EIP
CODE
ZOMG
TEH
EXPLOIT
HEAP
CORRUPTION
SEH
ROP
SafeSEH
ASLR

```
...
0x701   add  eax, ebx
0x702   mov  ecx, eax
0x703   call ecx
...
0x801   pop  eax
0x802   retn
...
0x901   pop  ebx
0x902   retn
```




...
0x701
add eax, ebx
0x702
mov ecx, eax
0x703
call ecx
...
0x801
pop eax
0x802
retn
...
0x901
pop ebx
0x902
retn
GARBAGE
0x802
value 1
0x901
value 2
0x701


SHELLCODE
POINTER
POINTER
POINTER
POINTER
POINTER
...
xor eax,eax
retn
add ebp,0x4
retn
...
...
call mprotect
retn.

Windows	Linux
VirtualAlloc	mprotect
HeapCreate	
SetProcessDEPPolicy	
...	
system()	system()
syscalls() ???	syscalls()
NtSetInformationProc.	

That’s demo time

На дом

- Попробовать либо

https://www.corelan.be/index.php/2010/06/16/exploit-writing-tutorial-part-10-chaining-dep-with-rop-the-rubikstm-cube/#ropversion

- Либо

https://www.vulnhub.com/entry/rop-primer-02,114

- Return-Oriented-Programming (ROP FTW) By Saif El-Sherei

https://www.exploit-db.com/docs/english/28479-return-oriented-programming-(rop-ftw).pdf