Cybersecurity: Buffer Overflow

Lezione 4: Protezioni Moderne e Bypass

Le Protezioni

- Stack Canaries (SSP)
- ASLR
- DEP / NX
- RELRO
- PIE

Stack Canaries

- GCC: `-fstack-protector`
- Valore casuale prima di RET
- Controllato prima del `ret`
- Se modificato → `__stack_chk_fail` → abort

Bypass:

- Overflow parziale senza canary
- Indovinare canary (rare)
- Usare buffer senza canary

ASLR

- Randomizza indirizzi di:
  - Stack
  - Heap
  - Librerie (PIE per eseguibili)
- `/proc/sys/kernel/randomize_va_space`
  - 0 = off
  - 1 = conservativo
  - 2 = completo

ASLR Bypass

- Info leak → rivelare indirizzi
- Brute force (se piccolo spazio)
- Usare indirizzi relativi (se PIE disabilitato)
- DLL senza ASLR (Windows XP/old)

DEP / NX

- No eXecute su stack/heap
- Pagina contrassegnata non eseguibile
- Shellcode in memoria → bloccato

Bypass:

- Return-to-libc
- ROP (Return-Oriented Programming)
- JIT Spraying

Return-to-libc

- Non serve shellcode
- Riutilizza codice esistente (librerie)
- Esempio: `system("/bin/sh")`

```
payload = A*offset + p32(system) + p32(exit) + p32(binsh_addr)
```

ROP (Return-Oriented Programming)

- Catena di "gadgets": piccoli frammenti di codice terminati da `ret`
- Presenti in librerie o binario
- Permettono di fare calcoli arbitrari

Esempio ROP

```
# pop rdi; ret → mette argomento in rdi
# system@plt → chiama system
pop_rdi = 0x401234
system = 0x401050
binsh = 0x4020a0
payload = b"A"*offset + p32(pop_rdi) + p32(binsh) + p32(system)
```

Protezioni Windows

- SafeSEH
- DEP (da Vista)
- ASLR (da Vista SP1)
- Stack Guard (/GS)

Bypass Windows Tipico

1. Info leak per superare ASLR
2. Use `VirtualProtect` per rendere stack eseguibile
3. ROP chain per chiamare `WinExec`

Strumenti

- `checksec` – vedere protezioni binario
- `ROPgadget` – trovare gadget
- `pwntools` – exploit automation
- `GDB` + `pwndbg` / `peda`

Summary

- Canary → stack integrity check
- ASLR → randomizza indirizzi
- DEP → stack non eseguibile
- Bypass: return-to-libc, ROP

Esercizio

Disabilitare ASLR:

```
echo 0 > /proc/sys/kernel/randomize_va_space
```

Scrivere exploit return-to-libc per `vuln` (senza canary).

Cybersecurity: Buffer Overflow – Pinolallo.com