Address Sanitizer

American Fuzzy Lop → sirve para probar el parser

En otro disco ejecutar

1 - afl-clang -01 `find -name ‘\*.c’`

2- afl-fuzz -i examples/ findings -- ./a.out → examples (semillas)

entrar al directorio findings → crashes

clang scan build → analisis estatico

CC=clang scan-build -disable-checker deadcode.DeadStores -o /tmp/out <comando de construcción>

<comando de construccion> = make

tirar el output al navegador → ex: /tmp/out/...

complexity --histogram --score `find -name ‘\*.c’` 2> /dev/null

strace <\*.out>

strace -p pid

CFLAGS=-g make → para debuggear

importante de socks5

REQUEST

CMD → 1 Connect

2 Bind

3 Upd Associate

ATYPE → Address type (1 → IPv4, 3→ name, 4→ IPv6)

Si es 3 → DST address termina en \0

Despues autenticacion

1,2,3,80, 255

**Parse**

Autenticacion

Request

Reply

**Estados del protocolo**

Invalid Version

Recv hello → 5 1 0

Send Hello response -> 5 0

Recv Request

Connecting | Resolve DNS

Error | Reply

Copy

HELLO parser

enum {

hello\_version,

hello\_Nmethods,

hello\_methods,

hello done,

hello\_error\_unsupported}

struct hello\_parser{

void(\*on\_authentication\_method)(struct \* hello\_parser, cont uint8 method);

void \* data;

enum hello\_state hello;

uint8 remaining;

}

**CLAVE MIRAR EL PARCHE NRO 3 DE PARSERS**