Programování síťové služby

Reverse-engineering neznámeho protokolu

Daniel Paulovič <xpaulo04>

Contents

[Zachytenie protokolovej komunikácie 2](#_Toc87358910)

[Formát protokolu 2](#_Toc87358911)

[Implementovanie Wireshark dissectoru 3](#_Toc87358912)

[Implementovanie kompatibilného klienta 4](#_Toc87358913)

# Zachytenie protokolovej komunikácie

## Formát protokolu

### Všeobecný popis protokolu

Protokol ISA je nadstavbou nad TCP protokolom. Po nadviazaní komunikácie medzi socketmi klienta a servera cez TCP, klient pošle request a v prípade dodržania formátu protokolu, naň server pošle naspäť response. Request aj response sa začína znakom “(“ a končí znakom “)”.

Request môže vyzerať nasledovne:

### Requesty a response

#### Command register

Format request pre register vyzera nasledovne: (register “<username>” “<epwd>”)  
kde sa <username> nahradi usernamom vyplneným v argumentoch program a <epwd> je heslo z argumentov programu, ktoré bolo encodované pomocou base64.  
Server naň odpovedá responsum vo formate: (ok “registered user <username>”) alebo   
(err “

#### Command login

#### Command list

#### Command send

#### Command fetch

#### Command logout

# Implementovanie Wireshark dissectoru

# Implementovanie kompatibilného klienta