Počítačové komunikace a sítě

2020/2021

Dokumentace projektu

Varianta ZETA: Sniffer paketů

Autor: Vasil Poposki

Fakulta informačních technologií

Duben 2021

• Úvod

V projektu byla vytvořena komunikující aplikace, která je schopná zachytávat a filtrovat pakety dle zadaných parametrů. Na vstupu aplikace dostane název síťového rozhraní, počet paketů pro tzv. “sniffing” a parametry filtru. Podle toho se výstup vypíše obsah paketu, včetně metadat.

• Implementační detaily

Projekt je implementován v jazyce C. K projektu jsem použil knihovnu *libpcap* a hlavičky *netinet* pro práci s pakety. Implementaci jsem rozložil do několika funkcí, kde každá reprezentuje jednotlivou část implementace.

- pcap_t *session_start(char *dev, char *filter_exp)

Funkce vrací deskriptor socketu který slouží pro další analýzu paketů. Jako parametry funkce dostává název rozhraní, na kterém se budou zachytávat pakety. Druhý parametr reprezentuje výraz, na zakladě kterého se budou pakety filtrovat. Pro filtrování se nejspíš daný výraz přeloží do filtrovacího programu a poté se filtrovací program vytvoří.

- void print_pkt(const u_char *packet, int caplen)

Funkce pro tisk jednotlivých paketů. Jako parametry dostane ukazatel na první bajt a délku paketu. Funkce na každém řádku vytiskne obsah paketu v hexadecimální a ascii podobě a počet vytisknutých bajtů.

- void handle(u_char *args,const struct pcap_pkthdr *pkthdr,const u_char *packet)

Funkce slouží pro zpracování paketu. Funkce *pcap_loop()* volá tuto funkci při každém zachycení paketu. Nejspíš se vytvoří struktura pro zpracování IP hlavičky, poté se určí offset hlavičky na základě délky Ethernet hlavičky. Funkce rozlišuje dva typy protokolu: TCP a UDP. Vypíše na výstup aktuální čas, source a destination adresy a delku paketu. Poté se zavolá funkce *print_pkt()* která obsah paketu vypíše.

- get_devices()

Funkce vypisuje seznam všech dostupných rozhraní.

- Main funkce

Ve funkci main se zpracovávají vstupní argumenty, na základě kterých se volá funkce *session_start()* a potom i *pcap_loop()* pro zpracování paketu.