IMPLEMENTACIJA PREPROSTEGA PAKETNEGA ANALIZATORJA

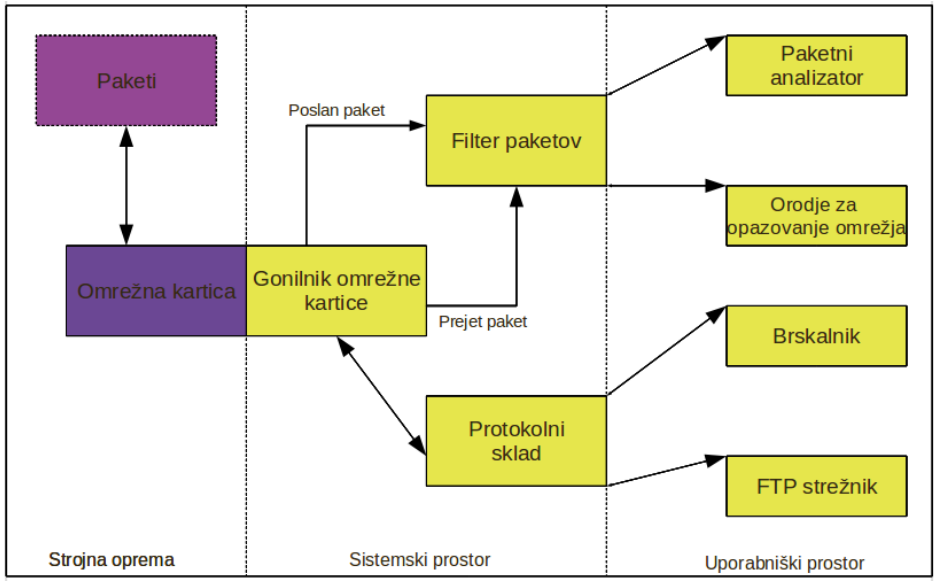
Sniffit

Seminarska naloga
Osnove operacijskih sistemov

Marinka Žitnik
IŠRM
12.01.2011

Analiza in zajem okvirov

- **Uporaba**
  - zaščita omrežij
  - napadi na omrežja
  - odpravljanje napak
  - optimizacija aplikacij



- **Dostop do zaglavij PDU – goli vtičniki (*raw sockets*)**
- **Pasivno prestrezanje**
  - preklop NIC v promiskuitetni način
- **Aktivno prestrezanje**
  - zastrupljanje ARP (*ARP poisoning*)
  - zrcaljenje prometa (port mirroring)
  - Cisco funkcija SPAN

FUNKCIONALNE ZAHTEVE

- Implementacija: C, *libpcap*, tekstovni UI
- Filtriranje zajema omrežnega prometa s filtri BPF
- Zajem podatkovnih okvirov prometa na izbranem vmesniku v datoteko v formatu *.pcap* za poznejšo analizo
- Analiza zajetega omrežnega prometa iz datoteke v formatu *.pcap*
- Preprosta statistika o številu zajetih in filtriranih paketov
- Zajem izbranega števila podatkovnih enot
- Analiza podatkovnih enot v realnem času: IEEE 802.3 Ethernet z enkapsuliranimi PDU protokolov: IPv4, ARP, RARP, IPv6, TCP, UDP, ICMP, IGMP itd. in koristna vsebina (*payload)*

ZS1: Osnovni zagon

```
marinka@marinka-PC:~/workspace/sniffit/Sniffit$ sudo ./Sniffit
DEV: usb0
NET: 178.58.76.96
MASK: 255.255.255.248


        1.
Grabbed packet of length: 118
Received at Sun Jan  9 18:37:01 2011
Ethernet address length: 6
Ethernet type hex: 800 dec: 2048 is an IP v4 packet.
        Destination address:  2:80:37:ec:2:0
        Source address:   2:80:37:ec:2:81
IP:     Source: 74.125.77.83
        Destination: 178.58.76.100
        Header length: 5
        Version: 4
        Packet length: 104
        Fragment offset: 0
        Protocol: TCP
        Src port: 443
        Dst port: 37225

        Payload (52 bytes):
00000   17 03 01 00 2f 3c c9 7b 28 c9 df f5 b3 f5 c4 76         ..../<.{(......v
00016   24 e4 7c a9 1b c2 6e 4b e1 c6 24 37 d2 4a 6f d4         $.|...nK..$7.Jo.
00032   08 9b fe c4 e6 5b ba 71 28 ad b6 e2 69 24 64 09         .....[.q(...i$d.
00048   91 37 a6 94                                             .7..
```

ZS2: Število zajetih okvirov

```
marinka@marinka-PC:~/workspace/sniffit/Sniffit$ sudo ./Sniffit -n 2
DEV: usb0
NET: 178.58.76.96
MASK: 255.255.255.248


        1.
Grabbed packet of length: 118
Received at Sun Jan  9 18:39:23 2011
Ethernet address length: 6
Ethernet type hex: 800 dec: 2048 is an IP v4 packet.
        Destination address:  2:80:37:ec:2:0
        Source address:   2:80:37:ec:2:81
IP:     Source: 74.125.77.83
        Destination: 178.58.76.100
        Header length: 5
        Version: 4
        Packet length: 104
        Fragment offset: 0
        Protocol: TCP
        Src port: 443
        Dst port: 37224

        Payload (52 bytes):
00000   17 03 01 00 2f 56 cb 38 98 d9 85 86 f6 b2 49 1f         ..../V.8......I.
00016   c8 cf e4 72 0d 5a 86 10 18 a0 e4 c3 17 c0 4b 9d         ...r.Z........K.
00032   61 04 ed 1d 42 4d 47 55 6a 51 3e 63 00 b0 c4 ff         a...BMGUjQ>c....
00048   ce 13 df ef                                             ....


        2.
Grabbed packet of length: 66
Received at Sun Jan  9 18:39:23 2011
Ethernet address length: 6
Ethernet type hex: 800 dec: 2048 is an IP v4 packet.
        Destination address:  2:80:37:ec:2:81
        Source address:   2:80:37:ec:2:0
IP:     Source: 178.58.76.100
        Destination: 74.125.77.83
        Header length: 5
        Version: 4
        Packet length: 52
        Fragment offset: 16384
        Protocol: TCP
        Src port: 37224
        Dst port: 443

Packet Capture Statistics:
2 packets received by filter.
0 packets dropped by kernel.

Done processing packets ...
```

Uporaba filtrov BPF (ang. *Berkeley Packet Filter*)

- **Prednosti**
  - ↓ obremenjenost CPE
  - ↓ verjetnost pojava izpuščanja paketov (*dropping packets)*
  - ↓ prenešenih okvirov iz sistemskega v uporabniški prostor
- **Kvalifikatorji**
  - *type* – pomen identifikatorja
  - *dir* – smer prenosa identifikatorja
  - *proto* – ujemanje protokola

Primitiv
< *kvalifikator identifikator* >

```
ip src host 10.1.1.1

src host 10.7.2.12 and not dst net 10.200.0.0/16

(src host 10.4.1.12 or src net 10.6.0.0/16) and tcp dst portrange 200-10000
and dst net 10.0.0.0/8
```

ZS3: Filter BPF

```
marinka@marinka-PC:~/workspace/sniffit/Sniffit$ sudo ./Sniffit -d usb0 -n 1 -f "host www.google.com"
DEV: usb0
NET: 178.58.76.96
MASK: 255.255.255.248


        1.
Grabbed packet of length: 1060
Received at Sun Jan  9 18:42:34 2011
Ethernet address length: 6
Ethernet type hex: 800 dec: 2048 is an IP v4 packet.
        Destination address:  2:80:37:ec:2:81
        Source address:   2:80:37:ec:2:0
IP:     Source: 178.58.76.100
        Destination: 74.125.77.99
        Header length: 5
        Version: 4
        Packet length: 1046
        Fragment offset: 16384
        Protocol: TCP
        Src port: 50749
        Dst port: 80

        Payload (994 bytes):
00000   47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31 0d 0a         GET / HTTP/1.1..
00016   48 6f 73 74 3a 20 77 77 77 2e 67 6f 6f 67 6c 65         Host: www.google
00032   2e 63 6f 6d 0d 0a 55 73 65 72 2d 41 67 65 6e 74         .com..User-Agent
00048   3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 58         : Mozilla/5.0 (X
00064   31 31 3b 20 55 3b 20 4c 69 6e 75 78 20 69 36 38         11; U; Linux i68
00080   36 3b 20 65 6e 2d 55 53 3b 20 72 76 3a 31 2e 39         6; en-US; rv:1.9
00096   2e 32 2e 31 33 29 20 47 65 63 6b 6f 2f 32 30 31         .2.13) Gecko/201
00112   30 31 32 30 36 20 55 62 75 6e 74 75 2f 31 30 2e         01206 Ubuntu/10.
00128   30 34 20 28 6c 75 63 69 64 29 20 46 69 72 65 66         04 (lucid) Firef
00144   6f 78 2f 33 2e 36 2e 31 33 0d 0a 41 63 63 65 70         ox/3.6.13..Accep
00160   74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61 70 70         t: text/html,app
00176   6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78         lication/xhtml+x
00192   6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78         ml,application/x
```

ZS4: Poznejša analiza *.pcap*

```
marinka@marinka-PC:~/workspace/sniffit/Sniffit$ sudo ./Sniffit -d usb0 -cs savefile -n 9 -f "host www.google.com"
DEV: usb0
NET: 178.58.76.96
MASK: 255.255.255.248

Packet Capture Statistics:
13 packets received by filter.
0 packets dropped by kernel.

Done processing packets ...
```

ZS5: Analiza zajetega prometa iz *.pcap datoteke*

```
marinka@marinka-PC:~/workspace/sniffit/Sniffit$ ./Sniffit -cr savefile


        1.
Grabbed packet of length: 98
Received at Sun Jan  9 18:45:05 2011
Ethernet address length: 6
Ethernet type hex: 800 dec: 2048 is an IP v4 packet.
        Destination address:  2:80:37:ec:2:81
        Source address:   2:80:37:ec:2:0
IP:     Source: 178.58.76.100
        Destination: 74.125.77.99
        Header length: 5
        Version: 4
        Packet length: 84
        Fragment offset: 16384
        Protocol: ICMP
```

ZS6: Filtracija prometa ARP

```
marinka@marinka-PC:~/workspace/sniffit/Sniffit$ sudo ./Sniffit -f arp
DEV: usb0
NET: 178.58.76.96
MASK: 255.255.255.248


        1.
Grabbed packet of length: 42
Received at Sun Jan  9 18:52:34 2011
Ethernet address length: 6
Ethernet type hex: 806 dec: 2054 is an ARP packet.
        Destination address:  ff:ff:ff:ff:ff:ff
        Source address:   2:80:37:ec:2:0

Hardware type: Ethernet
Protocol type: IPv4
Operation: ARP Request
Sender MAC: 02:80:37:EC:02:00:
Sender IP: 178.58.76.100.
Target MAC: 00:00:00:00:00:00:
Target IP: 178.58.76.98.



        2.
Grabbed packet of length: 60
Received at Sun Jan  9 18:52:34 2011
Ethernet address length: 6
Ethernet type hex: 806 dec: 2054 is an ARP packet.
        Destination address:  2:80:37:ec:2:0
        Source address:   2:80:37:ec:2:81

Hardware type: Ethernet
Protocol type: IPv4
Operation: ARP Reply
Sender MAC: 02:80:37:EC:02:81:
Sender IP: 178.58.76.98.
Target MAC: 02:80:37:EC:02:00:
Target IP: 178.58.76.100.
```

Hvala za pozornost.

***Op.: Predstavitev objavljena na http://www.helikoid.si.**