

Verkkoliikenteen seuraaminen ja tulkitseminen

Lasse Pesonen

Verkkoliikenteen seuraaminen

- Mitä se on
- Kuinka ja missä mahdollista
- Voidaanko se havaita
- tcpdump
 - esimerkkejä (ARP, TCP)
- Yhteenveto

Verkkoliikenteen seuraaminen

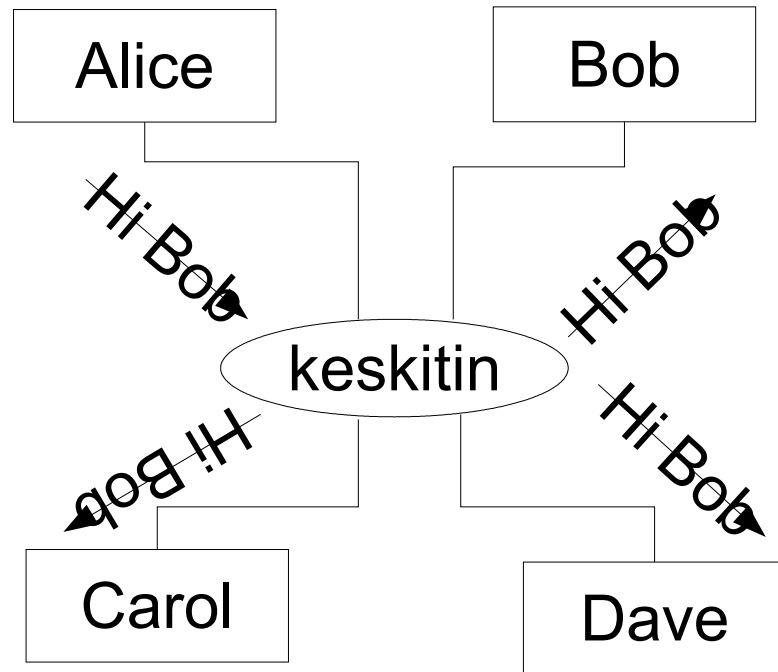
- Seurataan kaikkea liikennettä
- Lainsäädäntö rajoittaa
 - itse lähetettyä tai itselle tarkoitettua saa seurata
 - teleoperaattoreilla erilaisia oikeuksia ja velvollisuuksia

Protokollia

- ARP (Address Resolution Protocol)
 - selvitetään MAC-osoite (Media Access Control)
- IP (Internet Protocol)
 - pakettien kuljetus ja osioiminen
- TCP (Transmission Control Protocol)
 - luotettava siirtoyhteys laitteiden välillä

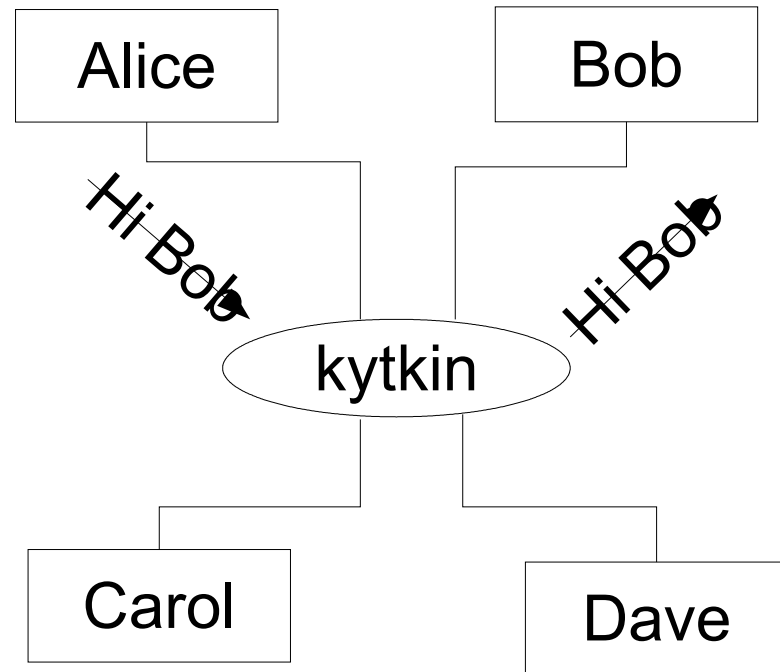
Verkkojen rakenne - keskitin

- Kaikki liikenne kuuluu kaikille
- Helppo kaapata muille kuuluvat paketit



Verkkojen rakenne - keskitin

- Liikenne ohjataan oikeaan porttiin



Hyökkäys kytkintä vastaan

- Täytetään MAC-välimuisti
 - voi toimia kuten keskitin
- Ohjataan liikennettä ARP-paketeilla
 - ARP tilaton ja yhteydetön
 - lähetetään väärennetty ARP-vastaus osapuolille, MAC-osoite oma kone

Miksi verkkoliikennettä seurataan

- Tarkastellaan
 - Protokollan toimintaa
 - Verkon kuormaa
 - Vierailtuja sivustoja
 - Epänormaalia verkkoliikennettä, madot, virukset
- Lokien pito
- Selvitetään verkon vikatilanteita

Miksi verkkoliikennettä seurataan

- Etsitään käyttäjätunnuksia ja salasanoja
- Päätellään laitteen käyttöjärjestelmä

Kuinka verkkoliikennettä seurataan

- Promiscuous-tila
- Sopiva verkkorakenne
 - keskitin
 - hyökkäys
 - yhdyskäytävä
 - omalla koneella tapahtuva liikenne

Voidaanko seuranta havaita

- Muokattu ICMP echo
 - oikea IP-osoite, väärä MAC
- Muokattu ARP
 - muokattu MAC, lähes broadcast-osoite
- DNS-liikenteen seuranta
 - seurantaohjelma yrittää selvittää laitteen nimen

tcpdump

- ohjelma verkkoliikenteen seurantaan
- UNIX-varianteille
- Windump Windowseille
- Tekstipohjainen
- Tulostus ruudulle tai tiedostoon
- Yleinen lokitiedostomuoto

tcpdump, käynnistys ja lopetus

```
# tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes

0 packets captured
0 packets received by filter
0 packets dropped by kernel
```

tcpdump, ARP

```
# tcpdump -n
05:19:50.835495 arp who-has 192.168.1.1 tell 192.168.1.2
05:19:50.835650 arp reply 192.168.1.1 is-at 00:e0:7d:83:c1:f8

# tcpdump -ne
05:19:50.835495 00:0c:6e:41:1a:e4 > ff:ff:ff:ff:ff:ff, ethertype
    ARP (0x0806), length 42: arp who-has 192.168.1.1 tell
    192.168.1.2
05:19:50.835650 00:e0:7d:83:c1:f8 > 00:0c:6e:41:1a:e4, ethertype
    ARP (0x0806), length 60: arp reply 192.168.1.1 is-at
    00:e0:7d:83:c1:f8
```

TCP-yhteyden avaus

- kolme vaihetta, SYN, SYN-ACK, ACK

```
# tcpdump -Snt
IP 192.168.1.2.43362 > 192.168.1.1.22: S 3002001894:3002001894(0)
    win 5840 <mss 1460,sackOK,timestamp 531839274 0,nop,wscale 2>
IP 192.168.1.1.22 > 192.168.1.2.43362: S 46543316:46543316(0)
    ack 3002001895 win 16384 <mss 1460,nop,nop,sackOK,nop,wscale
    0,nop,nop,timestamp 965509041 531839274>
IP 192.168.1.2.43362 > 192.168.1.1.22: . ack 46543317 win 1460
    <nop,nop,timestamp 531839282 965509041>
```

TCP-yhteyden sulkeminen

- FIN, ei täältä enää dataa

```
# tcpdump -Snt
IP 192.168.1.2.43362 > 192.168.1.1.22: F 3002003621:3002003621(0)
    ack 46545635 win 2372 <nop,nop,timestamp 531852329 965509067>
IP 192.168.1.1.22 > 192.168.1.2.43362: . ack 3002003622 win 17344
    <nop,nop,timestamp 965509067 531852329>
IP 192.168.1.1.22 > 192.168.1.2.43362: F 46545635:46545635(0)
    ack 3002003622 win 17344 <nop,nop,timestamp 965509067 531852329>
IP 192.168.1.2.43362 > 192.168.1.1.22: . ack 46545636 win 2372
    <nop,nop,timestamp 531852330 965509067>
```

- kaappaus voidaan tehdä otsikon bittien perusteella
- SYN+FIN ei sallittu

<i>0</i>		<i>8</i>				<i>16</i>				<i>24</i>	
Lähdeportti						Kohdeportti					
Järjestysnumero											
Kuittausnumero											
Pituus	Varattu	C	E	U	A	P	R	S	F	Ikkunan koko	
TCP tarkistussumma						Kiireellinen					

$$3 (0*2^7+0*2^6+0*2^5+0*2^4+0*2^3+0*2^2+1*2^1+1*2^0=3)$$

```

0 0 0 1 0 1 1 1 = 23      # tcpdump 'tcp[13] & 3=3'
0 0 0 0 0 0 1 1 = 3
-----
0 0 0 0 0 0 1 1 = 3

```

tcpdump, esimerkkikäskyjä

- valmiita vakioita, tcp, ip, arp, rarp, ether, icmp, icmptype...
- tcp-fin, tcp-rst, tcp-ack, icmp-echoreply, icmp-unreach...

```
# tcpdump 'host feonar and (port ftp or ftp-data)'
```

```
# tcpdump host helios and \( hot or ace \)
```

```
# tcpdump 'dst host 192.168.1.1 and dst port 22 and tcp  
[tcpflags] & tcp-syn !=0'
```

tulostus heksoina

- 2 merkkiä = tavu

```
# tcpdump -ntv -x 'tcp[13] & (tcp-syn|tcp-fin) !=0'
IP (tos 0x0, ttl 64, id 11486, offset 0, flags [DF], length: 60)
 192.168.1.2.44310 > 192.168.1.1.22: S [tcp sum ok] 576240571:576240571(0) win
 5840 <mss 1460,sackOK,timestamp 617584485 0,nop,wscale 2>
    0x0000:  4500 003c 2cde 4000 4006 8a8a c0a8 0102  E..<,.@.@.....
    0x0010:  c0a8 0101 ad16 0016 2258 bbbb 0000 0000  ..... "X.....
    0x0020:  a002 16d0 666c 0000 0204 05b4 0402 080a  ....fl.....
    0x0030:  24cf 9765 0000 0000 0103 0302                $.e.....
```

0		8				16				24			
Lähdeportti						Kohdeportti							
Järjestysnumero													
Kuittausnumero													
Pituus	Varattu	C	E	U	A	P	R	S	F	Ikkunan koko			
TCP tarkistussumma						Kiireellinen							

```
# tcpdump -ntv -x 'tcp[13] & (tcp-syn|tcp-fin) !=0'
IP (tos 0x0, ttl 64, id 11486, offset 0, flags [DF], length: 60)
192.168.1.2.44310 > 192.168.1.1.22: S [tcp sum ok] 576240571:576240571(0) win
5840 <mss 1460,sackOK,timestamp 617584485 0,nop,wscale 2>
```

0x0000:	4500 003c 2cde 4000 4006 8a8a c0a8 0102	E..<,.@. @.....
0x0010:	c0a8 0101 ad16 0016 2258 bbbb 0000 0000"X.....
0x0020:	a002 16d0 666c 0000 0204 05b4 0402 080afl.....
0x0030:	24cf 9765 0000 0000 0103 0302	\$.e.....

02, kind=maximum segment size
04, length, 4 tavua yhteensä
05b4 1460
0402, selective ACKs käytössä
080a, timestamp

24cf 9675 = 617584485
0000 0000 = 0
01, nop
03, window scale
02, 2

Muita ohjelmia

- ettercap
 - man-in-the-middle
 - kerää käyttäjätunnuksia ja salasanoja
 - pluginit
- snort
 - IDS (Intrusion Detection System)

ethereal

The screenshot displays the Ethereal network protocol analyzer interface. The main window shows a list of captured packets. Packet 14 is selected, and its details are expanded in the lower pane.

No.	Time	Source	Destination	Protocol	Info
6	0.010712	192.168.1.2	192.168.1.1	SSH	Client: Protocol: ssh=2.0-openssh_3.5p1
7	0.025442	192.168.1.1	192.168.1.2	SSHv2	Server: Key Exchange Init[Short Frame]
8	0.025473	192.168.1.2	192.168.1.1	SSHv2	Client: Key Exchange Init[Short Frame]
9	0.225269	192.168.1.1	192.168.1.2	TCP	ssh > 39428 [ACK] Seq=631 Ack=663 Win=17376 Len=0 TSV=96485966
10	0.225304	192.168.1.2	192.168.1.1	SSHv2	Client: Diffie-Hellman GEX Request
11	0.267126	192.168.1.1	192.168.1.2	SSHv2	Server: Diffie-Hellman Key Exchange Reply
12	0.270859	192.168.1.2	192.168.1.1	SSHv2	Client: Diffie-Hellman GEX Init
13	0.370266	192.168.1.1	192.168.1.2	SSHv2	Server: Diffie-Hellman GEX Reply
14	0.374482	192.168.1.2	192.168.1.1	SSHv2	Client: New Keys
15	0.565246	192.168.1.1	192.168.1.2	TCP	ssh > 39428 [ACK] Seq=1247 Ack=847 Win=17376 Len=0 TSV=96485966
16	0.565279	192.168.1.2	192.168.1.1	SSHv2	Encrypted request packet len=48
17	0.569946	192.168.1.1	192.168.1.2	SSHv2	Encrypted response packet len=48
18	0.570231	192.168.1.2	192.168.1.1	SSHv2	Encrypted request packet len=64
19	0.575746	192.168.1.1	192.168.1.2	SSHv2	Encrypted response packet len=80
20	0.575847	192.168.1.2	192.168.1.1	SSHv2	Encrypted request packet len=96
21	0.594956	192.168.1.1	192.168.1.2	SSHv2	Encrypted response packet len=80

WINDOW SIZE: 8272
Checksum: 0x90b6 (correct)

- Options: (12 bytes)
 - NOP
 - NOP
 - Time stamp: tsvval 207111688, tsecr 964859665
- [SEQ/ACK analysis]
 - [This is an ACK to the segment in frame: 13]
 - [The RTT to ACK the segment was: 0.004216000 seconds]
- SSH Protocol
 - SSH Version 2
 - Packet Length: 12
 - Padding Length: 10
 - Key Exchange

0020 01 01 9a 04 00 16 d0 42 20 d3 68 b0 39 91 80 18B...h.9...
0030 08 14 90 b6 00 00 01 01 08 0a 0c 58 46 08 39 82XF.9.
0040 97 11 00 00 00 0c 0a 15 00 00 00 00 00 00 00
0050 00 00 ..

Checksum (tcp.checksum), 2 b; P: 51 D: 51 M: 0

Yhteenveto

- Tehokkaat työkalut Internetistä
- Usea protokolla selväkielinen
 - ftp, telnet, http, icq, irc...
- Lainsäädäntö, ISP:n säännöt
- Protokollien tunteminen tärkeää