

Guida all'uso di TCPDUMP

Tcpdump è uno strumento per l'analisi del traffico che avviene nella rete fisica a cui si è collegati.

Capiamo bene che l'analisi del traffico della rete, sia per mezzo dell'intercettazione di tutti i pacchetti che attraversano una rete fisica, sia per mezzo del controllo di ciò che riguarda esclusivamente una singola interfaccia di rete del nodo locale, è molto importante per comprendere i problemi legati alla sicurezza e per scoprire inconvenienti di vario genere.

Per poter interpretare il contenuto dei pacchetti, è necessario conoscere la loro struttura, in base ai relativi protocolli.

tcpdump [opzioni] [espressioni]

Opzioni principali:

- a Permette di convertire indirizzi broadcast e ip in nomi
- c Esce dopo aver ricevuto un tot di pacchetti (es. c100)
- C Setta la grandezza del file salvato con il flag -w
- e Stampa il mac address in ogni pacchetto catturato
- F Permette di fornire i filtri da un file
- i Definisce l'interfaccia di rete. (es. -i eth0 o -i lo)
- n Non converte l'indirizzo ip in nome
- p L'interfaccia locale non viene settata in modalità promiscua
- q Visualizza il minor numero di informazioni possibili
- r Utilizza il file specificato come input per i dati da filtrare
- s Indica la quantità in bytes di un pacchetto catturato (di default usando linux Slackware è 92 bytes)
- t Non stampa il contrassegno temporale per ogni pacchetto catturato
- tt Stampa il contrassegno temporale (timestamp) non formattato su ogni linea
- v Verbose (incrementa il numero di informazioni)
- w scrive su file il risultato dello sniffing (es. -w file)
- x Visualizza in hex
- X stampa i pacchetti in formato HEX e ASCII

Espressioni:

Le espressioni di Tcpdump sono composte da primitive che possono essere raggruppate per mezzo delle parentesi tonde (in modo da evitare ambiguità nell'ordine di risoluzione) e connesse attraverso operatori booleani: (solo i pacchetti che soddisfano la condizione espressa vengono presi in considerazione). Se l'espressione manca, vengono catturati tutti i pacchetti.

Operatori booleani

! o not

Il punto esclamativo o la parola chiave not indica la negazione logica

&& o and

La doppia && o la parola chiave and rappresenta il concatenamento, ovvero and logico

|| o or

La doppia barra verticale o la parola chiave or rappresenta l'alternanza, ovvero un OR logico

Tcpdump accetta anche operatori come:

<

Significa minore di (es. < 40)

>

Significa maggiore di (es. > 50)

All'interno delle primitive possono apparire riferimenti a diversi tipi di entità:

type

Dicono a che tipo di cose l'ID (numerico o nome) si riferisce. Possibili tipi sono host, net o port

dir

entità che specifica una particolare direzione di trasferimento per e/oppure da un id. Possibili direzioni sono src, dst, src or dst e src and dst (es. 'src foo', 'dst net 128.3', 'src or dst port ftp-data'). Il comportamento di default è src or dst

proto

entità che restringe la cattura ad un particolare protocollo. Possibili protocolli sono: ether, fddi, ip, arp, rarp, decnet, lat, moprc, mopdl, tcp e udp (es. 'ether src foo', 'arp net 128.3', 'tcp port 21'). Se il protocollo non è selezionato, vengono considerati tutti i protocolli (es. 'src foo' significa '(ip o arp o rarp) src foo').

Altre primitive possono essere gateway, broadcast, less, greater

Primitive ammissibili

Primitiva	Descrizione
dst host <i>host</i> src host <i>host</i> host <i>host</i>	Se viene usata la parola chiave dst, si avvera se il campo della destinazione IP corrisponde al nodo indicato; se viene usata la parola chiave src, si avvera se il campo dell'origine IP corrisponde al nodo indicato; altrimenti, in mancanza di tali parole chiave, si avvera se il nodo corrisponde indifferentemente all'origine o alla destinazione.
ether dst <i>host_ethernet</i> ether src <i>host_ethernet</i> ether host <i>host_ethernet</i>	Definisce un indirizzo Ethernet numerico o derivato dal contenuto del file /etc/ethers. Come si può intuire, nel primo caso si fa riferimento a una destinazione, nel secondo a un'origine, nel terzo non si fa differenza.
gateway <i>host</i>	Si avvera nel caso i pacchetti utilizzino il nodo indicato come gateway, ovvero, quando l'indirizzo Ethernet dell'origine o della destinazione non appartiene né all'indirizzo IP dell'origine, né a quello della destinazione.
dst net <i>rete</i> src net <i>rete</i> net <i>rete</i>	Se viene usata la parola chiave dst, si avvera se il campo della destinazione IP appartiene alla rete indicata; se viene usata la parola chiave src, si avvera se il campo dell'origine IP appartiene alla rete indicata; altrimenti, in mancanza di tali parole chiave, si avvera se la rete corrisponde indifferentemente all'origine o alla destinazione. La rete può essere indicata con un numero IP incompleto, oppure attraverso l'aggiunta di una maschera di rete. Per cui, la sintassi potrebbe essere estesa nel modo seguente:
dst net { <i>rete</i> <. '-> <i>indirizzo_ip</i> mask <i>maschera_ip</i> <. '-> <i>indirizzo_ip</i> / <i>lunghezza_maschera</i> }	In tal caso, la maschera di rete può essere indicata attraverso un numero IP corrispondente, oppure attraverso la quantità di bit a uno nella parte iniziale di tale maschera.
src net { <i>rete</i> <. '-> <i>indirizzo_ip</i> mask <i>maschera_ip</i> <. '-> <i>indirizzo_ip</i> / <i>lunghezza_maschera</i> }	
net { <i>rete</i> <. '-> <i>indirizzo_ip</i> mask <i>maschera_ip</i> <. '-> <i>indirizzo_ip</i> / <i>lunghezza_maschera</i> }	
dst port <i>porta</i> src port <i>porta</i> port <i>porta</i>	Definisce una porta TCP o UDP, trattandosi rispettivamente di un'origine, di una destinazione, o di entrambe le cose indifferentemente.

Primitiva	Descrizione
less <i>lunghezza</i> <'`> len <= <i>lunghezza</i> greater <i>lunghezza</i> <'`> len >= <i>lunghezza</i>	Si avvera se la dimensione del pacchetto è inferiore o uguale, oppure maggiore o uguale alla quantità di byte indicata.
ether proto <i>protocollo</i>	Definisce la selezione di un protocollo Ethernet attraverso un numero oppure un nome: ip, arp, rarp. Dal momento che questi nomi sono anche parole chiave per Tcpdump, vanno indicati facendoli precedere da una barra obliqua inversa (\) (ciò tenendo conto anche del tipo di shell utilizzato; nel caso della shell Bash e di altre, occorre raddoppiare la barra obliqua inversa).
ip proto <i>protocollo</i>	Definisce la selezione di un protocollo IP attraverso un numero, oppure un nome: icmp, igrp, udp, nd, tcp. Tuttavia, i nomi icmp, tcp e udp vanno preceduti da una barra obliqua inversa (\) per evitare che vengano interpretati in modo speciale da Tcpdump.
[ether] broadcast	Si avvera se il pacchetto è di tipo Ethernet broadcast.
ip broadcast	Si avvera per un pacchetto IP broadcast.
[ether] multicast	Si avvera se il pacchetto è di tipo Ethernet multicast.
ip multicast	Si avvera per un pacchetto IP multicast.

Significato delle espressioni

=====
[x:y] inizia dall'offset x dall'inizio del pacchetto e legge y bytes
[x] abbreviazione per [x:1]
proto[x:y] inizio dall'offset x nel proto header e legge y bytes (es. tcp[13:1])

p[x:y] & z = 0 p[x:y] non ha bit "selezionati" z
p[x:y] & z != 0 p[x:y] ha qualcuno dei bit "selezionati" z
p[x:y] & z = z p[x:y] ha tutti i bit "selezionati" da z
p[x:y] = z p[x:y] ha solo i bit "selezionati" da z

Tcpdump può processare solamente 1, 2 o 4 bytes (riferito al valore y)

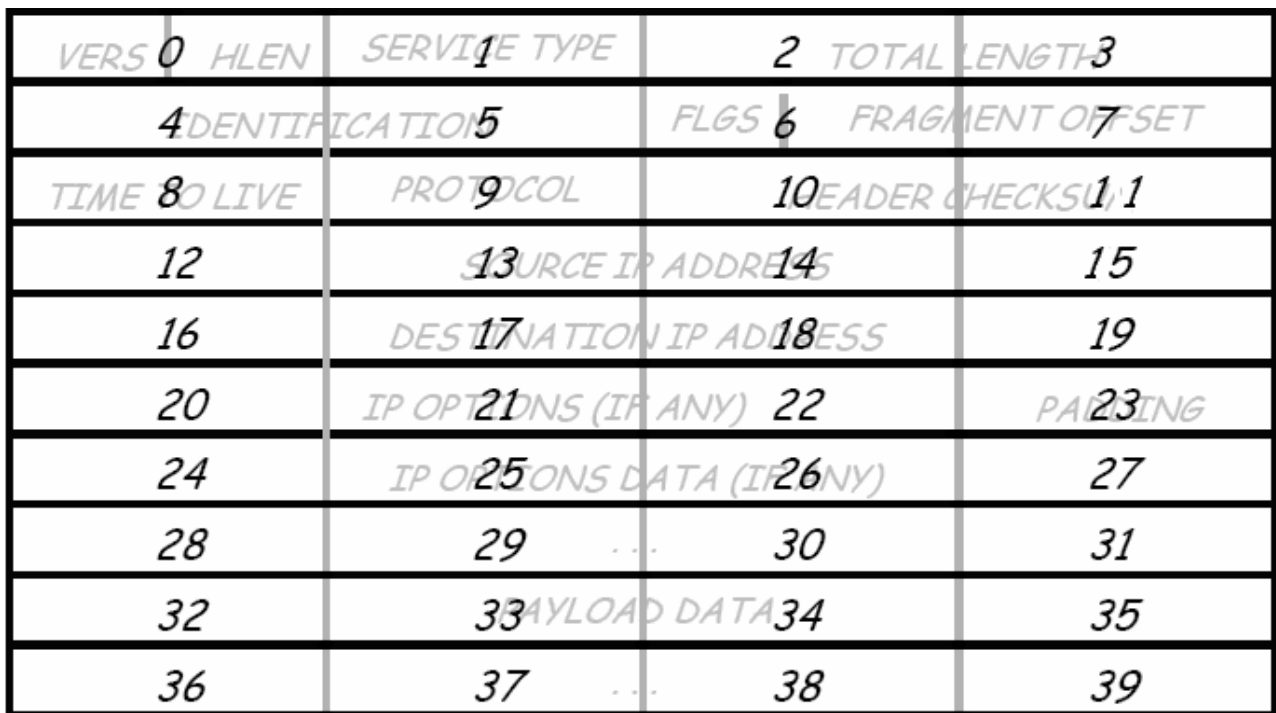
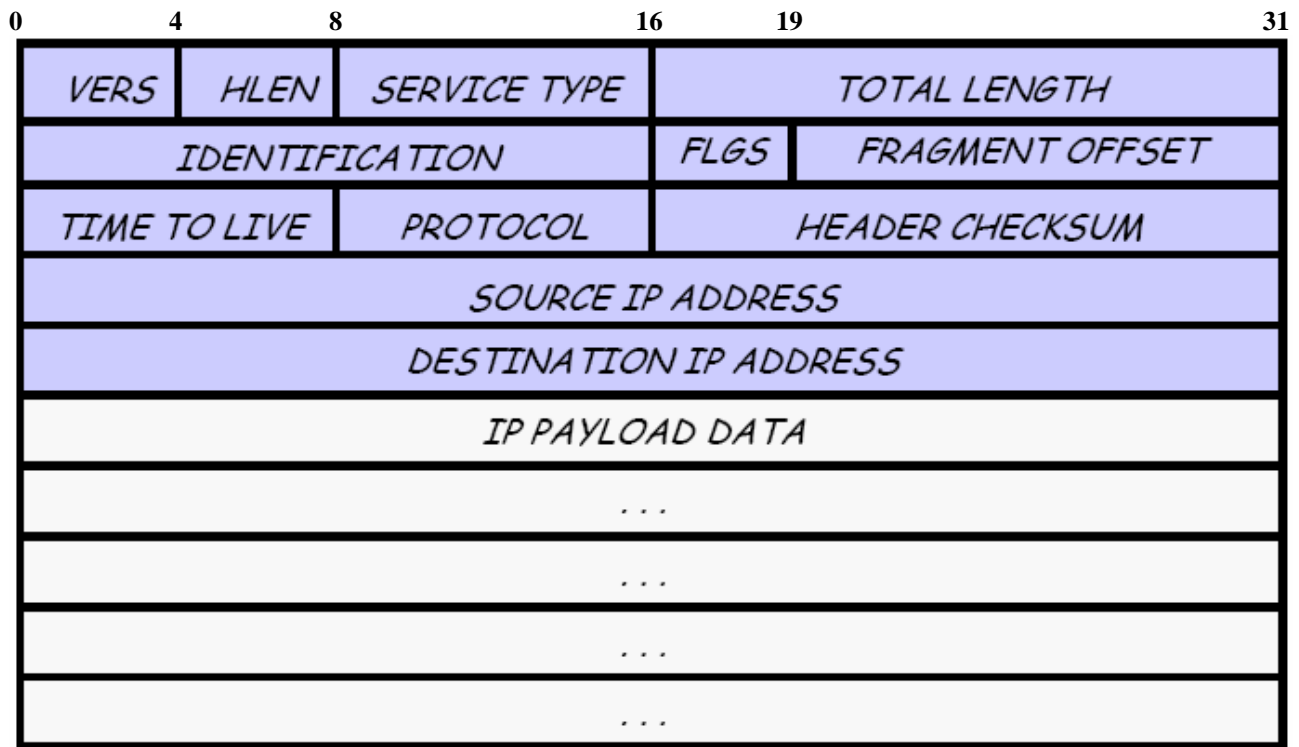
Solitamente una buona metodologia per scrivere regole è inserirle all'interno di parentesi o all'interno di file. Se la regola è scritta in maniera corretta ma l'output non è quello che ci si aspettava si può provare a mettere delle apici singole o doppie all'inizio e alla fine di ogni filtro.

Es.
tcp[13] \& 0x12 !=0
'tcp[13] & 0x12 !=0'
(tcp[13] & 0x12 !=0)

Formato di un messaggio IP (datagramma)

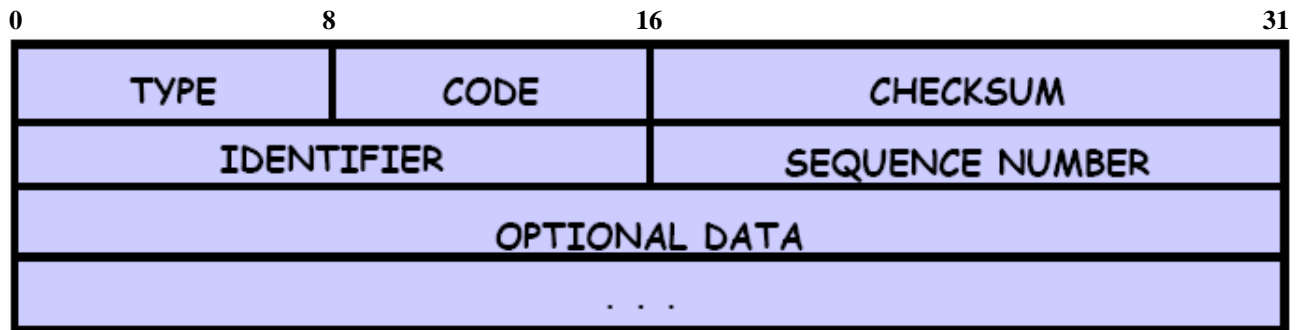
=====
ip[0] & 0xf0 versione IP, (4 per le reti, 6 per le reti v6)
ip[0] & 0x0f Lunghezza d'intestazione, (solitamente 5)
ip[1] Tipo di Servizio /QoS/DiffServ

ip[2:2] Lunghezza totale del datagramma in ottetti
 ip[4:2] IP ID (contiene un numero intero che identifica univocamente il datagramma)
 ip[6] & 0x80 reserved bit (usato per ECN)
 ip[6] & 0x40 DF bit (flag)
 ip[6] & 0x20 MF bit (flag)
 ip[6:2] & 0x1fff Offset del frammento (misurato in unità di 5 ottetti, iniziando dall'offset zero)
 ip[8] Tempo di Vita
 ip[9] Protocollo
 ip[10:2] Header Checksum
 ip[12:4] Indirizzo IP di provenienza
 ip[16:4] Indirizzo IP di destinazione
 ip[20..60] Opzione IP



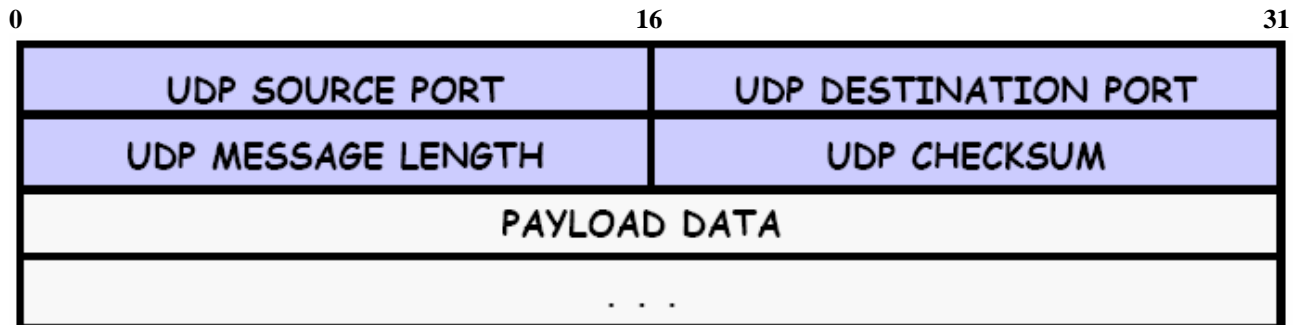
Formato di un messaggio ICMP

=====
icmp[0] Tipo
icmp[1] Codice
icmp[2:2] Checksum
icmp[4...] Dati Opzionali



Formato di un messaggio UDP (datagrammi)

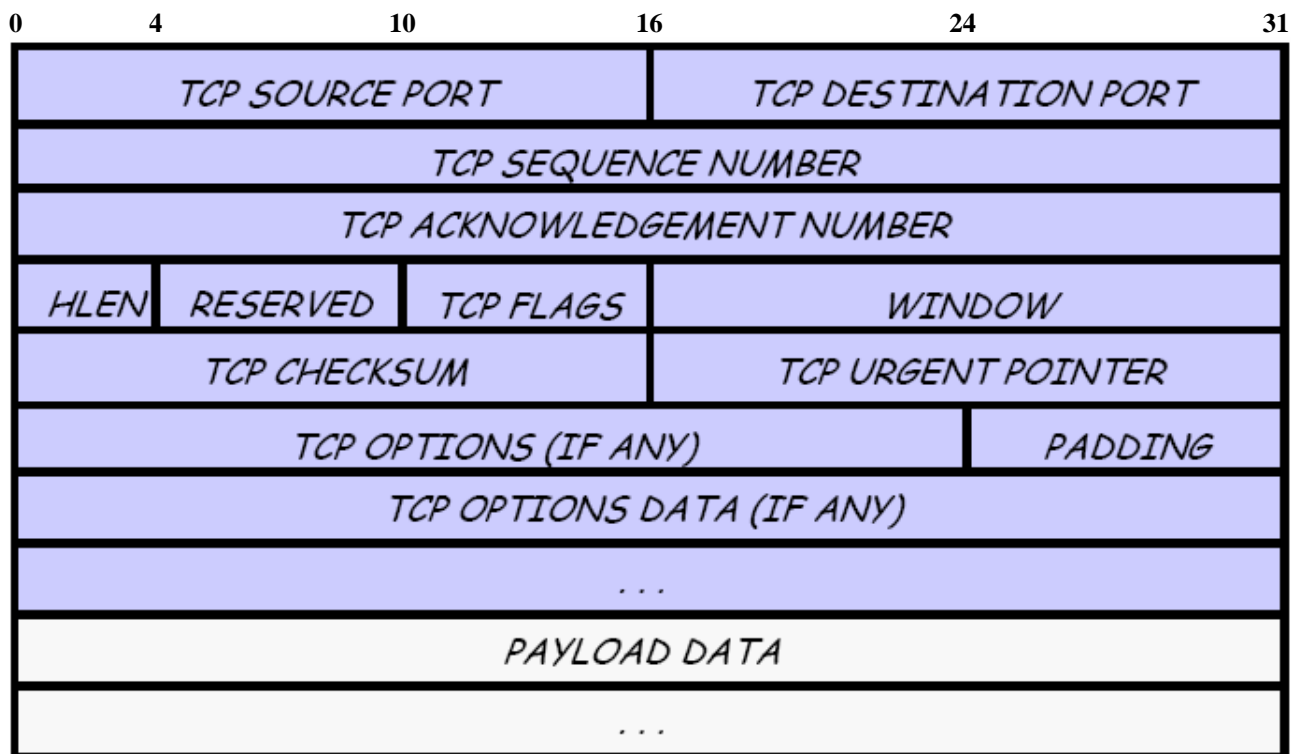
=====
udp[0:2] Porta di provenienza UDP
udp[2:2] Porta di destinazione UDP
udp[4:2] Lunghezza del messaggio UDP
udp[6:2] Checksum UDP



Formato di un messaggio TCP (header)

```

=====
tcp[0:2]      Porta di provenienza
tcp[2:2]      Porta di destinazione
tcp[4:4]      Numero sequenziale
tcp[8:4]      Numero riscontro
tcp[12]       Lunghezza del segmento misurata in multipli di 32 bit (HLEN)
tcp[13]       Flag TCP (URG, ACK, PSH, RST, SYN, FIN)
tcp[14:2]    Window Size (dimensione del buffer in invio e di ricezione)
tcp[16:2]    Checksum
tcp[18:2]    Urgent pointer (usato per contrassegnare i dati urgenti)
tcp[20..94]  Opzioni o Data
    
```



<i>Flags</i>	<i>Numerico</i>	<i>Significato</i>
---- --S-	0000 0010 = 0x02	SYN
---A ----	0001 0000 = 0x10	ACK (conferma di ricezione)
---A --S-	0001 0010 = 0x12	SYN-ACK (quando una connessione si dice ESTABLISHED)
---A -R--	0001 0100 = 0x14	RST-ACK (reset brutale della connessione tcp)
---A -R-F	0001 0101 = 0x15	FIN-RST-ACK
---A P---	0001 1000 = 0x18	PSH-ACK
---A P---F	0001 1001 = 0x19	FIN-PSH-ACK
--UA P---	0011 1000 = 0x38	PSH-URG-ACK
-Y-- ----	0100 0000 = 0x40	>= 0x40 set di bit riservati
XY-- ----	1100 0000 = 0xC0	entrambi sono bit di set riservati
XYUA PRSF	1111 1111 = 0xFF	FULL_XMAS (scan con nmap con il flag impostato a -sX)

Codice e Tipo di un pacchetto ICMP

```
=====
```

0	Risposta di eco
3	Destinazione Irraggiungibile
3:0	Net
3:1	Host
3:2	Protocollo
3:3	Port
3:4	NEEDFRAG
3:5	SRC_ROUTE_FAILED
3:6	NET_UNKNOWN
3:7	HOST_UNKNOWN
3:8	SRC_HOST_ISOLATED
3:9	NET_PROHIB
3:10	HOST_PROHIB
3:11	BAD_TOS_FOR_NET
3:12	BAD_TOS_FOR_HOST
3:13	FILTER_PROHIB
3:14	HOST_PRECEDENCE_VIOLATION
3:15	PRECEDENCE_CUTOFF
4	Blocco della sorgente
5	Rinvio (cambio di un percorso)
5:0	NET
5:1	HOST
5:2	TOSNET
5:3	TOSHOST
8	Richiesta di eco
9	Annuncio dei router
10	Sollecitazione dei router
11	Tempo scaduto per un datagramma
11:0	IN_TRANSIT
11:1	DURING_FRAG_REASSEMBLY
12	Problema di parametro del datagramma
12:1	MISSING_OPT_FOR_REQUEST
13	Richiesta di contrassegno temporale
14	Risposta di contrassegno temporale
15	Richiesta di informazione (obsoleto)
16	Risposta di informazione (obsoleto)
17	Richiesta della maschera degli indirizzi
18	Risposta della maschera degli indirizzi

Visualizzazione dell' Header Ethernet con tcpdump

Destination Addr (MAC)	Source Addr (MAC)	Type	Packet length
00:90:6f:45:00:20	01:00:5e:20:0c:a6	800	1494

13:51:08.402826 00:90:6f:45:00:20 > 01:00:5e:20:0c:a6, ethertype IPv4 (0x0800), length 1494: IP (output di tcpdump)

Visualizzazione dell'Header Ip (datagramma) con tcpdump

4	VERS	5	HLEN	00	SERVICE TYPE	00d2	TOTAL LENGTH	
4294	IDENTIFICATION				0f	FLGS	b9	FRAGMENT OFFSET
1f	TIME TO LIVE	11	PROTOCOL		37f3	HEADER CHECKSUM		
0a0a 200b				SOURCE IP ADDRESS				
e920 0c06				DESTINATION IP ADDRESS				
IP PAYLOAD DATA								
...								
...								
...								
...								

```

0x0000:  4500 00d2 4294 00b9 1f11 37f3 0a0a 200b
0x0010:  e920 0ca6 0f4e 0c50 05b4 fe6e a89b 4200
0x0020:  bc86 ac05 8231 4941 5da4 059f 9829 1420
0x0030:  0083 02ff cf0a 0000 0a91 0c00 0005 ac29
0x0040:  1450 00c2 01a2 013f cd1b 69dc 6793 cde2
0x0050:  c211                (output di tcpdump)
  
```

Visualizzazione dell'Header TCP con tcpdump

027c	TCP SOURCE PORT			0476	TCP DESTINATION PORT		
5691	23ca	TCP SEQUENCE NUMBER					
96b9	965f	TCP ACKNOWLEDGEMENT NUMBER					
50	HLEN	RESERVED	11	TCP FLAGS	8000	WINDOW	
633d	TCP CHECKSUM				TCP URGENT POINTER		
TCP OPTIONS (IF ANY)						PADDING	
TCP OPTIONS DATA (IF ANY)							
...							
PAYLOAD DATA							
...							

```

0x0010:  0004 231f d1c6 0090 6f44 f820 0800 4500
0x0020:  0028 d496 4000 3806 500a 0af9 844b 0a0a
0x0030:  84e1 027c 0476 5691 23ca 96b9 965f 5011
0x0040:  8000 633d 0000 0000 0000 0000 0000 0000
  
```

(output di tcpdump)

Visualizzazione dell'Header ICMP con tcpdump

08	TYPE	00	CODE	fd5c	CHECKSUM
0200	IDENTIFIER		5001	SEQUENCE NUMBER	
OPTIONAL DATA					
...					

0x0030: 1654 0800 fd5c 0200 5001 4142 4344 4445
(output di tcpdump)

Visualizzazione dell'Header UDP con tcpdump

04fe	UDP SOURCE PORT	0c50	UDP DESTINATION PORT
05b4	UDP MESSAGE LENGTH	3db5	UDP CHECKSUM
PAYLOAD DATA			
...			

0x0020: 0ca6 04fe 0c50 05b4 3db5 1c44 4300 bc86
(output di tcpdump)

Sintassi di un filtro

protocollo[*bytecount:offset*] & 0x mask esadecimale operatore valore da comparare

Esempi:

tcpdump -n "tcp[13:1] = 0x02"

contiene SYN e non risolve gli host in ip

tcpdump "ip[12:4] = ip [16:4] "

ip sorgente è uguale all'ip di destinazione

tcpdump "ip[13] & 0x03 != 0"

contiene i pacchetti con il SYN e il FIN flag

tcpdump "icmp and icmp[0] !=8 and icmp[0] != 0"

contiene tutti i pacchetti icmp che non sono ping

Altri ESEMPI di tcpdump:

tcpdump -vvv -X -n -i lo "tcp[13:1] = 0x02 and port 80"

-vvv indica verbose (più informazioni)

-X visualizza in esadecimale e in ascii

-n non risolve l'indirizzo

-i lo indica il loopback

il filtro "tcp[13:1] indica il 13° byte - si mette in ascolto sulla porta 80

tcpdump -vvv -X -n "ip[8:1] = 31"

-vvv indica verbose (più informazioni)
-X visualizza in esadecimale e in ascii
-n non risolve l'indirizzo

Maggiori approfondimenti

TCP/IP Illustrated, Volume I. Richard Stevens.

Internetworking with TCP/IP, Volume I. Douglas E. Comer.

Guida all'uso di TCPDUMP - Copyright © 2004 Demetrio Milea

Copyright (c) 2004 Demetrio Milea

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".

Guida all'uso di TCPDUMP - Copyright © 2004 Demetrio Milea