

## **Domande:**

- Qual è il numero di porta TCP di origine?

### 35016

Come classificheresti la porta di origine?

Porta effimera (dynamically assigned dal client)

Qual è il numero di porta TCP di destinazione?

#### 80

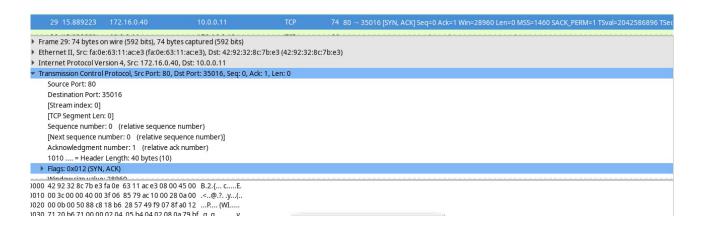
Come classificheresti la porta di destinazione?

## **HTTP Server**

Quale flag è impostato?

### **SYN**

A quale valore è impostato il numero di sequenza relativo?



29 15.889223 172.16.0.40		TCP	74 80 → 35016 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=2042586896 TSec
[TCP Segment Len: 0]			
Sequence number: 0 (relative sequence	number)		
[Next sequence number: 0 (relative sequence number)]			
Acknowledgment number: 1 (relative ack number)			
1010 = Header Length: 40 bytes (10)			
Flags: 0x012 (SYN, ACK)			
Window size value: 28960			
[Calculated window size: 28960]			
Checksum: 0xb671 [unverified]			
[Checksum Status: Unverified]			
Urgent pointer: 0			
<ul><li>Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale</li></ul>			
▶ [SEQ/ACK analysis]			
▶ [Timestamps]			

# Domande:

Quali sono i valori delle porte di origine e destinazione?

Porta di origine: 80 (HTTP)

Porta di destinazione 35016 → porta effimera (client)

- Quali flag sono impostati?

SYN + ACK

- A quali valori sono impostati i numeri relativi di sequenza e acknowledgment?

Relative Sequence Number: 0

Relative Acknowledgment Number: 1

```
30 15.889238 10.0.0.11 172.16.0.40 TCP 66 35016 → 80 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=1843568393 TSecr=2042586896

▶ ttnernet Ir, Src 4z/92/32/85C/70:e3 (4z/92/32/85C/70:e3), DSt Tacue:03:11/acce3 (Tatue:03:11/acce3)

▶ Internet Protocol Version 4, Src: 10.0.0.11, Dst: 172.16.0.40

▼ Transmission Control Protocol, Src Port: 35016, Dst Port: 80, Seq: 1, Ack: 1, Len: 0

Source Port: 35016

Destination Port: 80

[Stream index: 0]

[TCP Segment Len: 0]

Sequence number: 1 (relative sequence number)

[Next sequence number: 1 (relative sequence number)]

Acknowledgment number: 1 (relative ack number)

1000 .... = Header Length: 32 bytes (8)

▶ Flags: 0x010 (Ack)

Window size value: 58
```

# - Quale flag è impostato?

### **ACK**

```
file ] [ -V file ] [ -s snaplen ] [ -T type ] [ -w file ]
                  -W filecount ]
                 -E <u>spi@ipaddr</u> <u>algo:secret,...</u>
                  -y <u>datalinktype</u> ] [ -z <u>postrotate-command</u> ] [ -Z <u>user</u> ]
                   -time-stamp-precision=tstamp_precision ]
                  --immediate-mode ] [ --version ]
                 expression ]
DESCRIPTION
       Topdump prints out a description of the contents of packets on a net-
       work interface that match the boolean expression;
                                                            the
                                                                 description
       preceded by a time stamp, printed, by default, as hours, minutes, sec-
       onds, and fractions of a second since midnight. It
                                                              can
                                                                    also
       with the -w flag, which causes it to save the packet data to a file for
       later analysis, and/or with the -r flag, which causes it to read from a
       saved packet file rather than to read packets from a network interface.
       It can also be run with the -V flag, which causes it
                                                              to read a list
```

## - Cosa fa l'opzione -r?

L'opzione -r <file> in tcpdump serve a leggere i pacchetti da un file pcap invece che in tempo reale da un'interfaccia di rete.

- Elencare tre filtri Wireshark che potrebbero essere utili a un amministratore di rete
- ip.addr==indirizzo\_ip, si possono visualizzare tutti i pacchetti che riguardano quel determinato indirizzo IP (sia come sorgente che come destinazione).
- tcp.port==numero\_porta o udp.port==numero\_porta, si possono visualizzare le comunicazioni che utilizzano una porta specifica.
- arp per isolare il traffico ARP e diagnosticare problemi di indirizzamento MAC/IP

## - In quali altri modi Wiresharl potrebbe essere utilizzato in una rete di produzione?

- o Debug di applicazioni: Analizzare la comunicazione tra applicazioni e sistemi per risolvere problemi di performance o di funzionamento.
- Rilevamento di attività sospette: Identificare traffico non autorizzato, attacchi di tipo DDoS o malware.
- o Identificazione di bottleneck: Individuare i punti critici della rete che causano rallentamenti o interruzioni.
- o Integrato in ambienti di controllo (usando dump su file o interfacce virtuali) per avere alert automatici su pattern di traffico anomalo.
- o Rilevare attività sospette (es. scanning di porte, attacchi ARP spoofing, tentativi di exploit), estrarre file trasferiti, o ricostruire sessioni dopo un incidente.