Strumenti di Rete

Corso Architettura degli Elaboratori 2

Lezione E6-2 – 15 marzo 2006

Oggi vedremo

NETSTAT : Analizzatore di Protocollo

TCPDUMP : Sniffer per Linux

ETHEREAL : Sniffer per Windows

NETSTAT

Mostra le connessioni TCP, e informazioni relative

- Porte sulle quali il computer sta ascoltando
- Statistiche Ethernet
- Tabella di Routing IP (simile a "route PRINT")
- Statistiche IPv4 (IP,ICMP,TCP e UDP)
- Statistiche IPv6 (IPv6,ICMPv6,TCP over IPv6, e UDP over IPv6)

SNIFFERS

TCPDUMP : http://www.tcpdump.org/

ETHEREAL : http://www.ethereal.com/

TCPDUMP

Mostra gli header di pacchetti su una interfaccia di rete che soddisfano una data espressione booleana

tcpdump [**-adefInNOpqRStuvxX**] [**-c** *count*]
[**-C** *file_size*] [**-F** *file*] [**-i** *interface*]
[**-m** *module*] [**-r** *file*] [**-s** *snaplen*]
[**-T** *type*] [**-w** *file*] [**-E** *algo:secret*]
[*expression*]

Opzioni TCPDUMP

OPZIONE	DESCRIZIONE
-w file	Salva i dati in un file per l'analisi successiva
-r file	Legge da file i dati sui pacchetti
-D	Visualizza l'elenco delle interfacce di rete disponibili
-c count	Esci dopo aver letto count pacchetti
-e	Riporta gli header data-link
-F file	Specifica un file con l'espressione booleana
-i iface	Specifica l'interfaccia di rete dove ascoltareq
-p	Non mette l'interfaccia in modo promiscuo
-x -X	Visualizza solo (risp. anche) la versione ASCII

TCP HEADER

- Source Port
- Destination Port
- Sequence Number
- Acknowledge Number
- Header Lenght
- UrgAckPshRstSynFin
- Window Size
- TCP CheckSum
- Urgent Pointer

DATAGRAM HEADER

- Version
- IHL
- Type Of Service
- Total length
- Identification
- Flags
- Fragmentation Offset
- Time To Live
- Protocol
- Header Checksum
- Source Address
- Destination Address

ETHERNET HEADER

- Preamble

- Destination MAC Address
- Source MAC Address
- Type/Length
- User Data
- Frame Check Sequence (FCS)