Sicurezza delle reti[1]

Mattia Monga

Dip. di Informatica e Comunicazione
Università degli Studi di Milano, Italia
mattia.monga@unimi.it

a.a. 2010/11

Lezione V: Analisi del traffico

tcpdump

- analizzatore di pacchetti (non solo TCP) http://www.tcpdump.org
- basato su librerie pcap (degli stessi autori)
- Command line, ma esistono anche GUI (p.es. Wireshark, a.k.a Ethereal)
- La scheda di rete che intercetta il traffico lavora in modalità promiscua: non scarta i pacchetti che non la contengono come destinatario
- Viene attraversato tutto lo stack:
  - I dati sono affidabili quanto è affidabile il sistema operativo su cui gira
  - Se il traffico di rete è troppo elevato, alcuni pacchetti potrebbero essere scartati

Sintassi di base

es: `tcpdump src 192.168.1.100 and dst 192.168.1.2 and port ftp`

protocollo	direzione	soggetto	valore	conn. logico	altro
tcp	dst	host	10.1.1.1	and	port ftp

protocollo ether, fddi, ip, arp, rarp, decnet, lat, sca, moprc, mopdl, tcp, udp (tutti)

direzione src, dst, src and dst, src or dst (src or dst)

soggetto net, port, host, portrange (host)

conn. logici not, and, or

Altri dettagli utili

man tcpdump!!!

- È possibile anche usare operatori come `less`, `greater` per la dimensione dei pacchetti e operatori bit a bit (`& | << >>`) per i flag
- `-A` pacchetti in ASCII
- `-i` scegliere l'interfaccia su cui catturare pacchetti
- `-n` non convertire i nomi simbolici
- `-S` numeri di sequenza assoluti (e non relativi)
- `-v` livello di verbosità `-vvv`
- `-w` salva in un file (leggibile con `-r`)
- `'tcp[tcpflags] & (tcp-syn|tcp-fin) != 0 and not src and dst net 127.0.0.1'`
- `'icmp[icmptype] != icmp-echo and icmp[icmptype] != icmp-echoreply'`

Usare `'` per evitare di interferire con la shell