Università Degli Studi Di Salerno

Facoltà Di Scienze Matematiche Fisiche Naturali

Sistemi di elaborazione : Sicurezza su reti

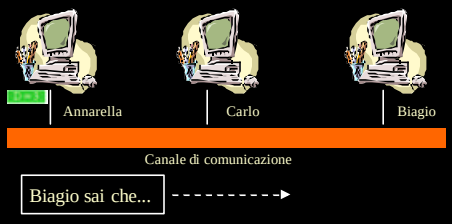
SNIFFING

Anno accademico 2002/2003

A cura di : Catena Gerardo Esposito Mario
Stefanelli Carlo Manna Fortunato

SCENARIO

Annarella Invia Un Messaggio a Biagio



SNIFFER

Strumento software o hardware che permette di:

- Catturare pacchetti dalla rete
- Interpretarli
- Memorizzarli per un' analisi successiva

SNIFFER

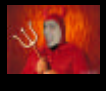
- **Uso lecito**

- Monitorare il traffico all' interno della rete al fine di individuare e risolvere problemi legati alla comunicazione
- Per un amministratore di rete: valutare la sicurezza delle password

SNIFFER

- **Uso illicito**

- Violazione della privacy nelle comunicazioni (e-mail, carta di credito…….)
- Cattura di informazioni preziose (login e password)



SNIFFER

Esempio di cattura di un pacchetto

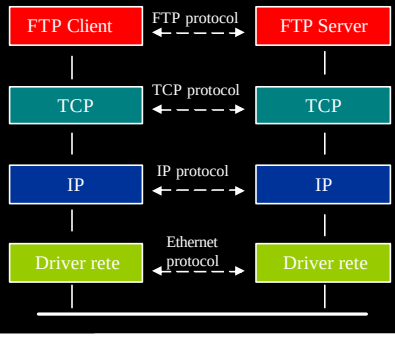
SOMMARIO

- Protocollo TCP/IP
- Rete Ethernet
- Storia Sniffer
- Sniffer in azione
- Creazione di uno sniffer (librerie Pcap)
- Come individuare uno sniffer

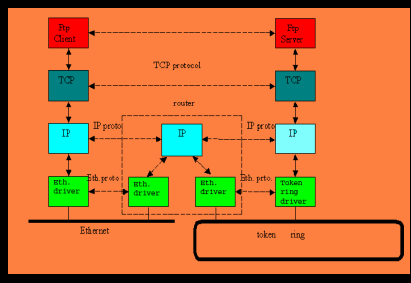
Protocollo TCP/IP

APPLICAZIONE	Ftp, E-mail, Telnet…
TRASPORTO	TCP, UDP
RETE	IP, ICMP, IGMP
LINK	Driver dell'interfaccia di rete

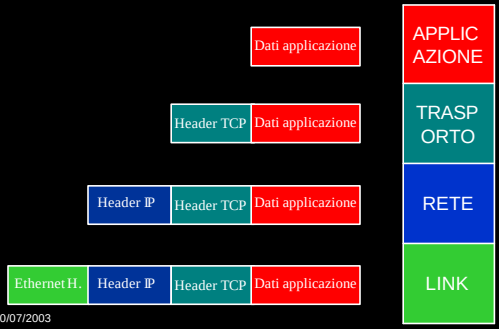
Comunicazione su LAN



Comunicazione su Internet



Struttura Del Pacchetto



Porte TCP/IP

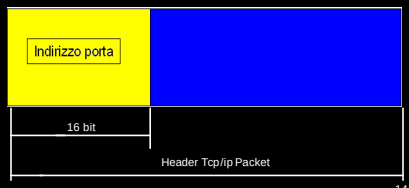
- **Più processi (servizi) sono in esecuzione contemporaneamente sulla stessa macchina**
- **E' necessario un meccanismo per identificare ciascun processo**
- **Per risolvere il problema TCP/IP implementa il concetto di PORTA**

Porte TCP/IP

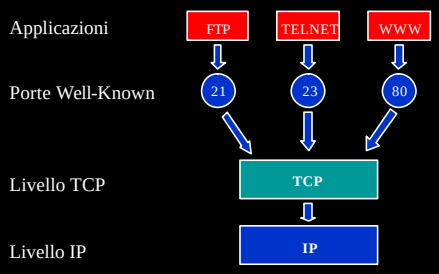
- I primi 1024 numeri di porta sono riservati (well-known port)
- Applicazioni standard utilizzano porte standard (Well-Known):
  - FTP Porta 21
  - TELNET Porta 23
  - WWW Porta 80

Porte TCP/IP

- Nell'header del pacchetto TCP un campo di 16 bit indica l' indirizzo di porta



Esempio

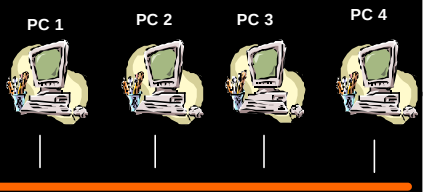


SOMMARIO

- Protocollo TCP/IP
- Rete Ethernet
- Storia Sniffer
- Sniffer in azione
- Creazione di uno sniffer (librerie Pcap)
- Come individuare uno sniffer

Reti Ethernet

- Nate nel 1976
- Basato sul concetto di condivisione: tutte le macchine utilizzano lo stesso canale



Reti Ethernet

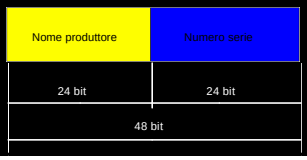
- Identificazione tramite indirizzo MAC
- Un pacchetto viene ricevuto solo se l'indirizzo MAC di destinazione corrisponde al proprio

Controllo Accesso al Mezzo: MAC

- Indirizzo che Identifica univocamente una macchina sulla rete
- Memorizzato al momento della costruzione dell'ethernet adapter

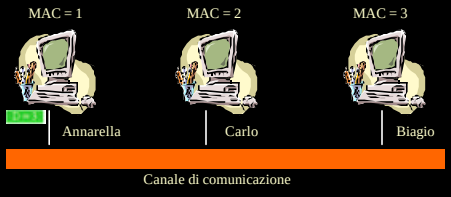
Controllo Accesso al Mezzo: MAC

- Composto da 48 bit
  - 24 bit nome del produttore dell'ethernet adapter
  - 24 bit numero di serie



ESEMPIO

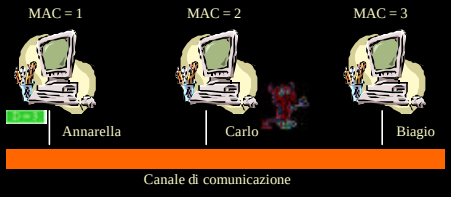
- Annarella invia un messagio a Biagio
- Indirizzo di destinazione del pacchetto: D = 3



- Carlo non influisce nella comunicazione

Promiscuous mode

- Modalità di configurazione dell' Ethernet Adapter



- Carlo sniffa tutti i pacchetti che viaggiano nella rete

SOMMARIO

- Protocollo TCP/IP
- Rete Ethernet
- Storia Sniffer
- Sniffer in azione
- Creazione di uno sniffer (librerie Pcap)
- Come individuare uno sniffer

SNIFFER : un po' di storia

- Il Packet capturing nasce con l'avvento di Ethernet
- Sun implementò NIT(Network Interface Tap) per catturare pacchetti e *etherfind* per stampare gli header dei pachetti
- A partire da *etherfind* Van Jacobs ha sviluppato *tcpdump*
- *Tcpdump* è il più popolare sniffer nella comunità UNIX

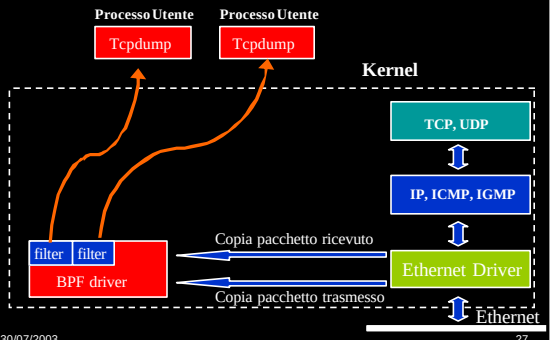
tcpdump

- Primo Sniffer della storia
- raccoglie da un'interfaccia di rete i pacchetti che soddisfano un criterio booleano e ne stampa l'header
- puo` salvare i pacchetti in un file
- puo` leggere l'input da un file invece che dall'interfaccia di rete

BPF

- **Tcpdump utilizza BSD Packet Filtering.**
- **Problema:**
  - **Normalmente accade che i pacchetti vengono passati dal driver di rete agli strati superiori del protocollo.**
  - **Il processo utente non può accedere direttamente ai dati contenuti nei pacchetti**
- **BPF risolve questo problema**

Es: BPF Ethernet



Parametri tcpdump

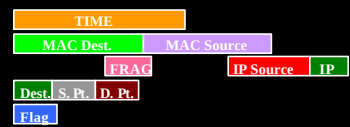
- **-i "interfaccia": Specifica Interfaccia da utilizzare**
- **-w "file": Scrive nel file l'output di tcpdump**
- **-r "file": effettua lo sniffing dal file**
- **-c "numero": specifica il massimo numero di pacchetti da rilevare**
- **-C "byte": max dimensione in byte del file di output.Quando viene superata un nuovo file è creato automaticamente**

Es: tcpdump

- **E' possibile selezionare il traffico da filtrare.**
- **Tcp dump converte le espressioni specificate dall' utente nella corrispondente sequenza di istruzioni per il BPF.**
- ES: **tcpdump -i eth0 -w *file_out* tcp port 23**
- **Cattura pacchetti dull'interfaccia eth0 Destinati alla porta 23 e scrive l'output nel file *file_out***

Un Pacchetto Filtrato

0003 009e b405 0402 0000 5173 0080
0270 0000 0000 009e 9459 1700 800a
16b8 9e86 988f 54c0 fde9 063c 0040
18c6 3000 1045 0008 a4e8 02f8 0000
60a8 b734 e000 0000 003e 0000 003e
000d 041a 3889 f060



SOMMARIO

- **Protocollo TCP/IP**
- **Rete Ethernet**
- **Storia Sniffer**
- **Sniffer in azione**
- **Creazione di uno sniffer (librerie Pcap)**
- **Come individuare uno sniffer**

Uno sniffer: Ethereal

- Analizza I protocolli di rete
- Funziona in ambienti Unix e Windows
- Ambiente grafico per visualizzare dati e informazioni su ogni pacchetto
- E' disponibile anche il source code (www.ethereal.com)

Uno sniffer: Ethereal

- Da linea di comando:

```
Ethereal –i eth0 –k
```

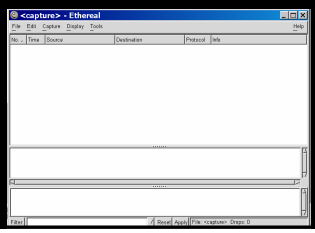
- -i <interfaccia>: seleziona l'interfaccia da cui sniffare
- -k: specifica che la cattura dei pacchetti deve avvenire immediatamente

Parametri Ethereal

- -c <count>: specifica il numero di pacchetti da catturare
- -f <capture filter>: setta l'espressione
- -n: specifica la visualizzazione di indirizzi ip o nomi
- -w <savefile>: scrive l'output nel file

Ethereal Interfaccia grafica

- Appena lanciamo lo sniffer appare la seguente interfaccia
- Clicchiamo su Capture per accedere alle opzioni



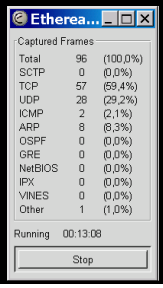
Ethereal Interfaccia grafica

Le opzioni di cattura

- **Una volta settate clicchiamo su ok**

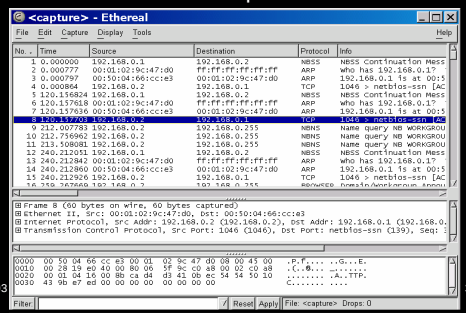
Ethereal Interfaccia grafica

- **Ethereal in azione**



Ethereal Interfaccia grafica

- Visualizzazione dei pacchetti sniffati



Ethereal Interfaccia grafica

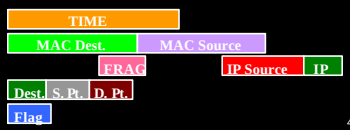
- Interpretazaione dell'output

1. Visualizza un sommario di ogni pacchetto catturato
2. Visualizza informazioni dettagliate su ogni pacchetto
3. Visualizza il campo dati di ogni pacchetto

A. Pulsante "Filter": permette la costruzione del filtro
B. Permette di inserire ed editare la stringa del filtro
C. Pulsante "Reset": cancella il filtro corrente
D. Informazioni generali

Un Pacchetto Filtrato

0003 009e b405 0402 0000 5173 0080
0270 0000 0000 009e 9459 1700 800a
16b8 9e86 988f 54c0 fde9 063c 0040
18c6 3000 1045 0008 a4e8 02f8 0000
60a8 b734 e000 0000 003e 0000 003e
000d 041a 3889 f060



Gli sniffer piu` diffusi

UNIX

- Sniffit di Brecht Claerhout
  reptile.rug.ac.be/~coder/sniffit/sniffit.html
- Tcpdump 3.x
  www-nrg.ee.lbl.gov
- Solsniff di Michael R. Widner
  www.rootshell.com
- dsniff
  www.monkey.org/~dugsong

Gli sniffer piu` diffusi

WINDOWS

- BUTTsniffer di DillDog
  Packetstorm-securify.org/sniffers/buttsniffer
- Dsniff
  Naughty.monkey.org/~dugsong/dsiff

SOMMARIO

- **Protocollo TCP/IP**
- **Rete Ethernet**
- **Storia Sniffer**
- **Sniffer in azione**
- **Creazione di uno sniffer (librerie Pcap)**
- **Come individuare uno sniffer**

Le libreria PCAP: un po' di storia

- Van Jacobs, Craig Leres e Steven McCanne svilupparono PCAP (Paket capturing)
- PCAP fu scritta per evitare che ci fossero tracce di codice proprietario in *tcpdump*
- In essa sono implementate le le potenzialità per la cattura e il filtro di pacchetti

Le libreria PCAP

- Gli sniffer creati con le librerie PCAP devono essere eseguiti con privilegi di superuser
- Le librerie PCAP hanno una licenza BSD e non sono sottoposte a copyright. Le applicazioni che utilizzano le librerie PCAP possono essere modificate e distribuite utilizzando una qualsiasi licenza

SNIFFER E LIBRERIE PCAP

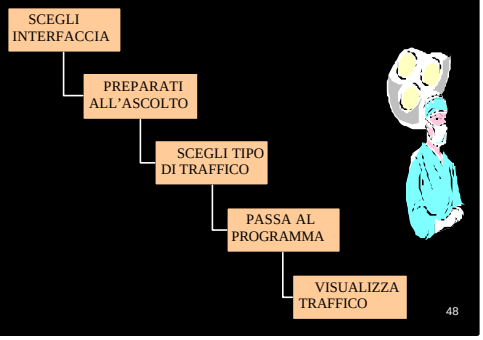
- Quale interfaccia porre in modalità promiscua?
- Quanti byte del pacchetto devo catturare (solo header o anche dati)?
- Che tipo di traffico devo catturare?
- Come passare i dati dalla rete all'applicazione?

Uno Sniffer:cominciamo ad operare

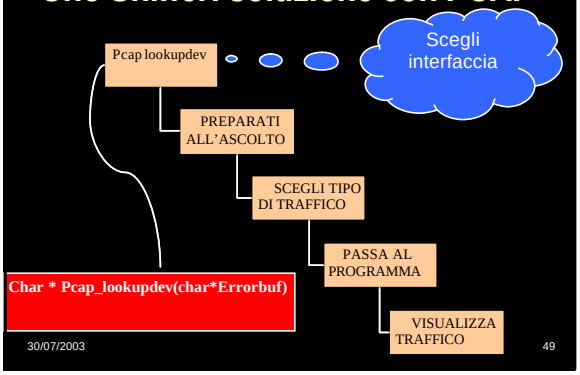
Sniffer()

1. **Scegli interfaccia da porre in modalità promiscua**
2. **Preparati all'ascolto**
3. **Scegli il tipo di traffico**
4. **Passa il traffico all'applicazione**
5. **Visualizza il traffico ascoltato**

Uno Sniffer: cominciamo ad operare



Uno Sniffer: soluzione con PCAP

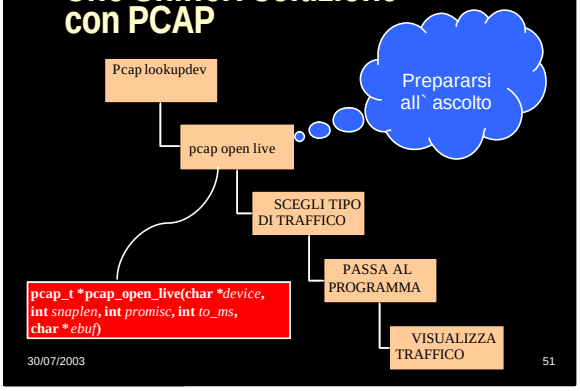


Specifiche delle funzioni di libreria PCAP

- **pcaplookdev()**

  Resituisce il nome della prima interfaccia di rete nell`elenco di sistema.
  Esiste anche la funzione
  pcap_findalldevs()
  la quale restituisce una lista delle interfacce presenti nel sistema.

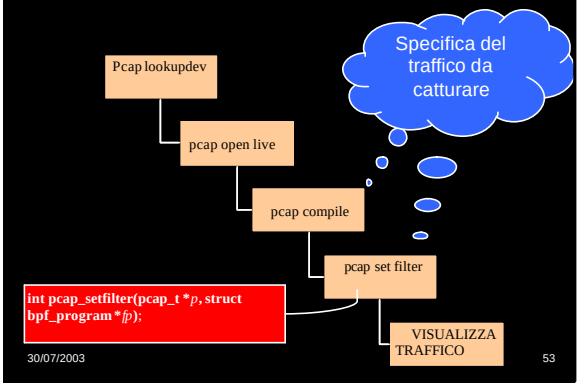
Uno Sniffer: soluzione con PCAP



Specifiche delle funzioni di libreria PCAP

- **Pcap_open_live()**
  - Setta l` interfaccia selezionata in modalita` promiscua
  - Specifica la dimensione massima dei pacchetti da catturare

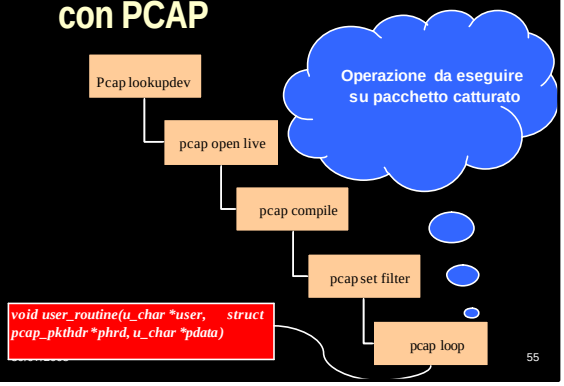
Uno Sniffer: soluzione con PCAP



Specifiche delle funzioni di libreria PCAP

- **Pcap_compile**
  - Utilizzata per creare il filtro BPF (BSD packet filter)
- **Pcap_setfilter**
  - Applica il filtro creato con pcap_compile

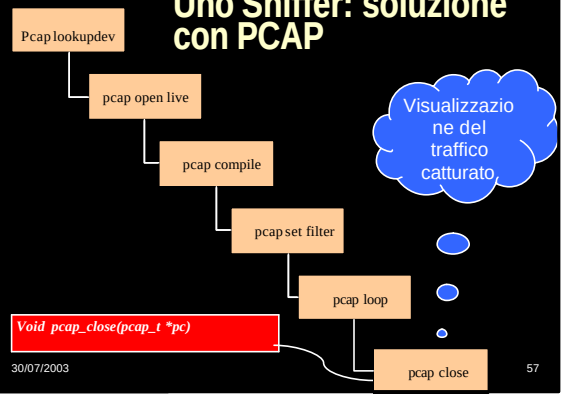
Uno Sniffer: soluzione con PCAP



Specifiche delle funzioni di libreria PCAP

- **Pcap_loop**
  - Specifica quanti pacchetti bisogna catturare e quale routine eseguire su ogni pacchetto catturato. (DNS-reverse-lookup)
- **Pcap_next**
  - Cattura solo il prossimo pacchetto sniffato

Uno Sniffer: soluzione con PCAP



Specifiche delle funzioni di libreria PCAP

- **Pcap_close ()**
  - Termina la cattura dei pacchetti
- **Pcap_dump_open()**
  - Crea un file in cui memorizzare I pacchetti catturati al fine di analizzarli in un secondo momento

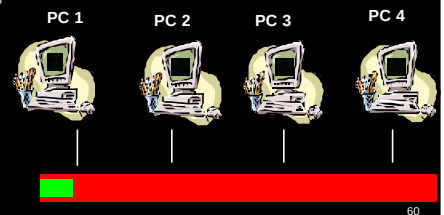
SOMMARIO

- **Protocollo TCP/IP**
- **Rete Ethernet**
- **Storia Sniffer**
- **Sniffer in azione**
- **Creazione di uno sniffer (librerie Pcap)**
- **Come individuare uno sniffer**

Come individuare uno sniffer

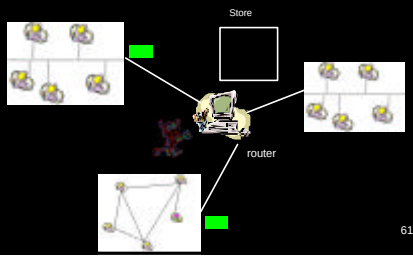
= pacchetto

- **Su reti LAN ogni macchina è un potenziale sniffer**



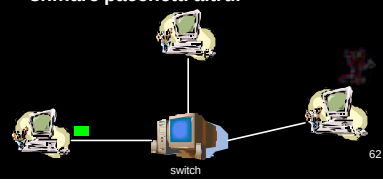
Come individuare uno sniffer

- Su Internet ogni router è un potenziale sniffer



Come evitare di essere sniffati

- Uno dei metodi migliori è adottare gli switch nelle reti LAN, oppure utilizzare la crittografia nelle comunicazioni.
- Lo switch dirige il traffico e un utente maliziose non è in grado di sniffare pacchetti altrui



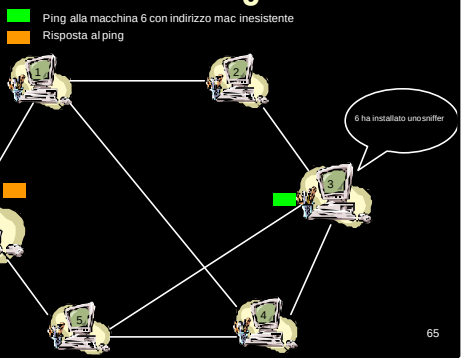
Come individuare uno sniffer

- Sniffer stand-alone.
  Non genera traffico in rete(sniffing passivo) non è perciò individuabile.
- Tutti gli altri sniffer(non stand–alone).
  Generano traffico ben distinguibile sulla base di dei dati e delle richieste (ad es DNS reverse lookup) inviate ed e' possibile localizzarli.

Tecniche di localizzazione: metodo '*ping*'

- ping dell' idirizzo IP ad una macchina sospetta con MAC inesistente. Se arriva una risposta allora su quella macchina sta girando uno sniffer.
- esistono degli exploit per windows che permettono di generare falsi positivi che vanificano la ricerca

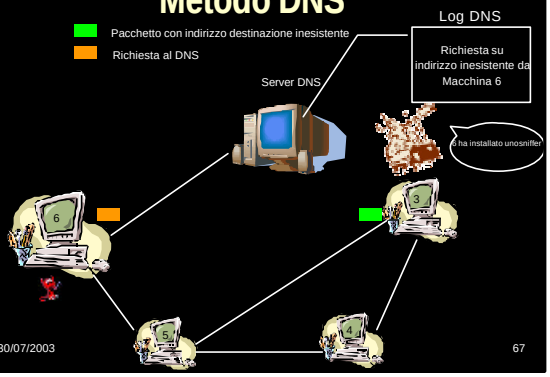
Metodo Ping



Tecniche di localizzazione: metodo DNS

- Molti sniffer eseguono automaticamente il DNS Reverse look-up,al fine di risalire al nome associato all'indirizzo sniffato.
  Trasmettendo pacchetti ad indirizzi inesistenti è possibile rilevare una macchina sospetta, osservando il traffico DNS.
  Se qualcuno cerca di risolvere l' indirizzo inesistente c'è uno sniffer.
- Dai log del server DNS è possibile ricavare l'IP della macchina che sniffa.

Metodo DNS



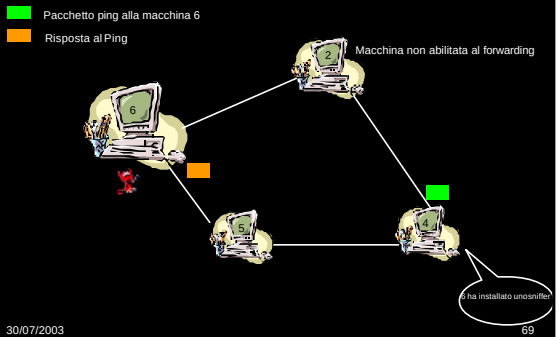
Tecniche di localizzazione: metodo source route

- Forzare l'instradamento di un pacchetto ping, verso una macchina sospetta, tramite una macchina non abilitata al forwarding dei pacchetti.

Se la destinazione risponde lo stesso al ping allora è settata in modo promiscuo ed effettua lo sniffing.

Per essere certi che il pacchetto sia stato sniffato basta confrontare il campo TTL del pacchetto inviato con quello del pacchetto ricevuto.

Metodo Source route

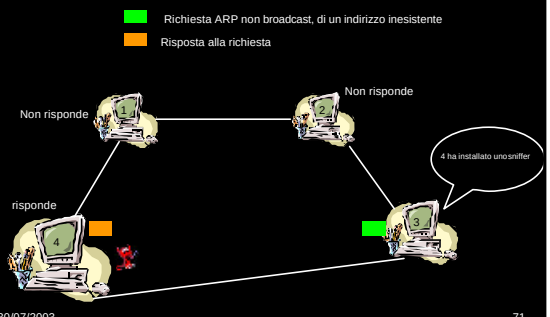


Tecniche di localizzazione: metodo ARP

- Quando si manda una richiesta ARP ad un indirizzo non broadcast, tutte le macchine scartano il pacchetto tranne quelle con schede di rete in modo promiscuo,che inviano una risposta.

Di conseguenza Inviando una richiesta ARP non broadcast alla macchina sospetta, se essa risponde vuol dire che sta sniffando i pacchetti dalla rete.

Maetodo ARP

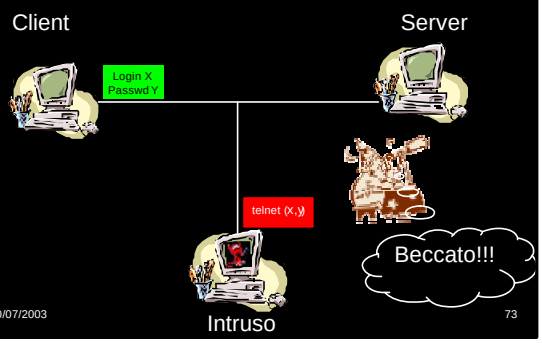


Tecniche di localizzazione: metodo Decoy

- Un client ed un server sono posti ai capi della rete.Il client si logga al server utilizzando username e password fittizzi, trasmessi in chiaro.

L'utente che sniffa tali informazioni tenterà di loggarsi utilizzandole……basta attendere!

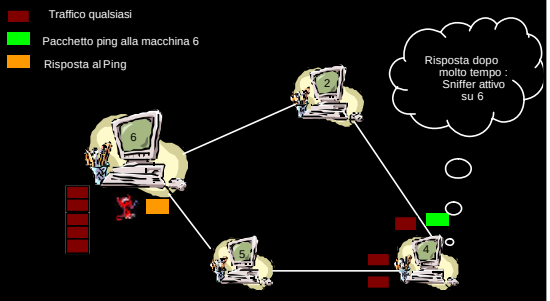
Metodo Decoy



Tecniche di localizzazione: metodo latency

- **Sovraccaricare la rete con pacchetti qualsiasi ed inviare ping alla macchina sospetta. Se il tempo di risposta al ping è elevato, vuol dire che il buffer della macchina sospetta è saturo e che quindi ha sniffato l'intero traffico generato.**

Metodo Latency



Tecniche di localizzazione: metodo host

- **Molte volte un'hacker effettua un attacco utilizzando macchine che non sono le sue.**

Per verificare se qualcuno ha installato uno sniffer sulla vostra macchina basta interrogare la propria schede di rete per verificare se è settata in modo promiscuo utilizzando il comando "ifconfig –a".

Conviene comunque prima reinstallare tale comando poiché l'hacker potrebbe averlo compromesso per evitare che venga rilevato lo sniffer.

- Ma aldilà di tutto :

"NON SI E' MAI SICURI DI ESSERE AL SICURO!"