UNIVERSITA' DEGLI STUDI DI SALERNO

Facoltà di Scienze Matematiche
Fisiche e Naturali

Anno Accademico 2000/2001

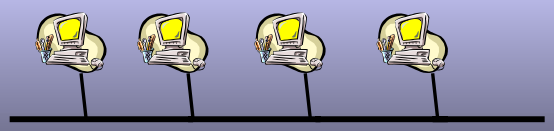
SISTEMI DI ELABORAZIONE: SICUREZZA SU RETI

PACKET SNIFFING

DEFINIZIONI

LAN (Local Area Network):insieme di computer interllacciati entro uno spazio fortemente delimitato

Il protocollo Ethernet: Sviluppato nel 1976 da Bob Metcalfe e David Boggs.
Basato sul concetto di ***condivisione***: tutte le macchine condividono lo stesso cavo.



DEFINIZIONI

Ogni messaggio viene diviso in **PACCHETTI**; ad ogni pacchetto viene assegnato un indirizzo IP e/o MAC.

MAC Address ed Indirizzi IP: Ad ogni macchina deve essere assegnato un identificativo:

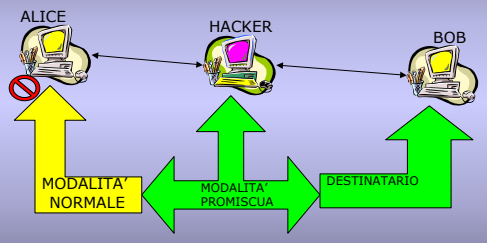
Internet Service Provider: IP dinamico

MAC address di 48 bit, di cui:

-24 bit identificano il produttore della Ethernet card;
-24 bit identificano il numero di serie UNICO assegnato alla scheda;

DEFINIZIONI

PROMISCUOUS MODE:modalità di configurazione dell'*ethernet adapter* in cui è permesso a tutte le macchine l'ascolto di tutto il traffico di rete.



SNIFFER

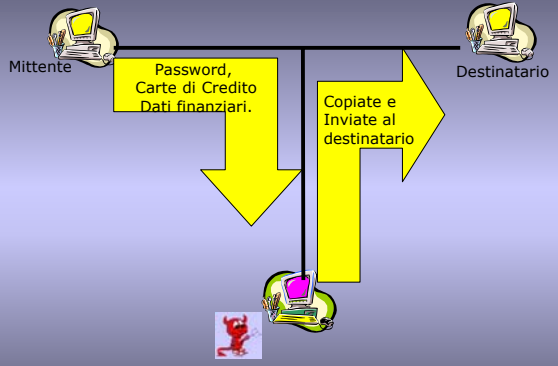
Qualsiasi strumento, software o hardware, che raccoglie le informazioni che viaggiano lungo una rete (network).

Primo sniffer, sviluppato dalla Network Associates, Inc. e protetto da trademark, è: "**The Sniffer Network Analyzer**".

Alcuni degli obiettivi più nefasti:

- Acquisizione di password;
- Acquisizione di numeri di Carte di Credito;
- Raccolta di dati sensibili (codici segreti, dati finanziari, ecc.)

ESEMPIO



FUNZIONI DI UNO SNIFFER

Le funzioni tipiche sono:

- Conversione e filtraggio dei dati e dei pacchetti
- Analisi dei difetti di rete
- Performance Analisys (qualità e portata della rete)
- Setacciamento di Password e Nomi di Utenti
- Creazione di LOG (elenchi del traffico della rete)
- Scoperta di intrusioni attraverso l'analisi dei LOG

COMPONENTI DI UN PACKET SNIFFER

Hardware:
•Standard network adapters;
•con hardware speciale analizzano errori di CRC, problemi della tensione,del cavo, "dribbles" , errori della negoziazione.

Capture driver:
•Cattura il traffico della rete;
•Filtraggio;
•Memorizzazione dei dati in un buffer.

Buffer
Pacchetti catturati dalla rete e immagazzinati in un buffer:

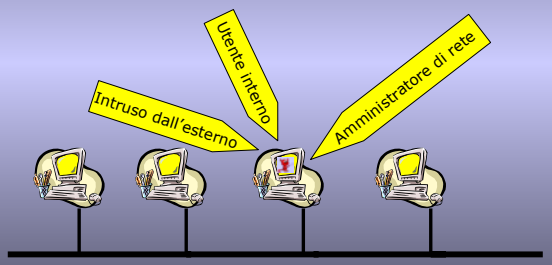
a) cattura finchè il buffer non si riempie;

b) usa il buffer come un "round robin" dove il dati nuovi sostituiscono i vecchi.

LIVELLI DI RISCHIO

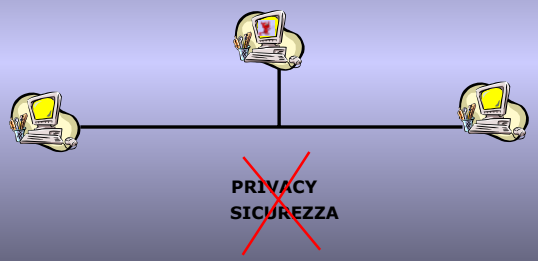
L'esistenza di uno sniffer in rete rappresenta una minaccia alla sicurezza e alla riservatezza delle comunicazioni.

Se la LAN è sottoposta al "controllo" di uno sniffer allora:

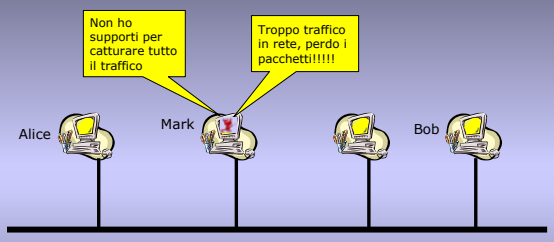


LIVELLI DI RISCHIO

In ogni caso la privacy e la sicurezza stessa di tutte le comunicazioni è compromessa.



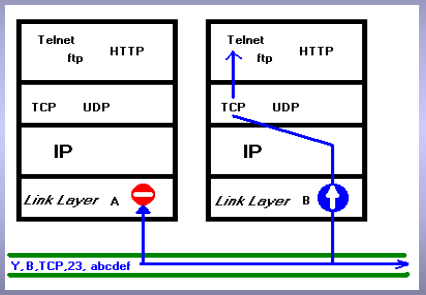
LIVELLI DI RISCHIO



Lo sniffing è un attacco di secondo livello! L'intruso si è già introdotto nella rete e ora cerca di compromettere maggiormente la sicurezza del sistema.

SNIFFER E TCP/IP

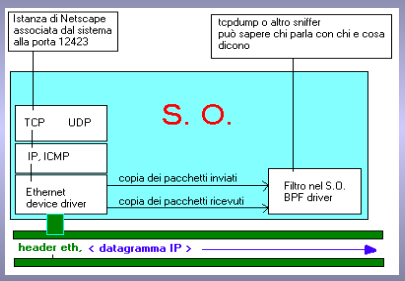
Normalmente solo l'interfaccia del destinatario passa i dati allo strato superiore.



B è il destinatario, solo il suo *link layer* lascerà passare il pacchetto

SNIFFER E TCP/IP

Le API del sistema operativo permettono di leggere tutto ciò che passa sul canale ponendo l'interfaccia di rete in modalità promiscua.



Resta a carico dello sniffer effettuare un'interpretazione dei pacchetti e assemblare i dati.

SNIFFER E TCP/IP

Nei sistemi UNIX il programmatore:

- Ha un controllo più o meno elevato della comunicazione in rete;
- deve gestire molti dettagli implementativi.

La libreria PCAP (Packet Capture):

- rende relativamente semplice la cattura dei pacchetti:
- offre un'interfaccia di programmazione per la cattura dei pacchetti di facile utilizzo;
- indipendente dal tipo di dispositivo di rete.

Molti sistemi hanno già installate le PCAP; esse sono comunque disponibili gratuitamente su Internet.

SNIFFER E TCP/IP

TCP/IP agevola gli sniffer:

- non offre nessun meccanismo di verifica o protezione dei dati;
- I dati viaggiano in chiaro;
- non è fornito nessun modo per garantire l'autenticità degli interlocutori (esistono applicazione per poterlo fare);
- Ciascuna macchina su cui viaggiano i dati potrebbe visualizzarli o anche modificarli;
- non vengono adottati strumenti per garantire l'autenticità e la privacy dei dati.

TCP/IP si ***fida*** semplicemente dell'indirizzo specificato dal mittente.

PROTOCOLLI VULNERABILI

Telnet e rlogin:
Uno sniffing può catturare le pressioni dei tasti, incluso il nome dell'utente e la password.

HTTP
La versione di default di HTTP ha numerose falle:

- L'autenticazione "BASIC" che spedisce password in plain-text.
- richiesta all'utente di UserID e password (spedite in plain-text).
- I Dati vengono spediti in chiaro.

PROTOCOLLI VULNERABILI

SNMP
Le password di SNMP vengono spedite in chiaro attraverso il cavo.

NNTP, POP, FTP, IMAP
Password e dati spediti in chiaro.

COME REPERIRE UNO SNIFFER

WINDOWS:

- **ETHEREAL**
  Esso è un programma basato su UNIX ed eseguito su Windows. E' la migliore soluzione freeware disponibile per sniffare su Windows.
- **WinDump**
  Una versione di tcpdump per Windows.
- **Network Associates Sniffer**
- **WinNT server**
  Comprende un Monitor di Rete. Si può eseguirlo dal menu sotto la voce "Attrezzi Amministrativi."

COME REPERIRE UNO SNIFFER

- **BlackICE Pro**
  Scopre le intrusioni. Più utile quando usato in un ambiente di sicurezza.
- **CiAll**
  Questo è un programma che può solo decodificare.
- **Analyzer**:
  Opera un'analisi del traffico della rete;
- **SpyNet/PeepNet**
  Non decodificha frames, ma riassembla sessioni.

COME REPERIRE UNO SNIFFER

UNIX:

Le soluzioni per UNIX generalmente sono basate sulla libreria libpcap BPF (Berkeley Packet Filters). Si usano:

- **SuperSniffer v1.3**

E' una versione migliorata di *libcap*:

a) encryption di DES di archivio;
b) collegamenti di FTP sono tagliati su una linea;
c) inutili negoziazioni di *telnet* scartati;
d) collegamenti duplici scartati.

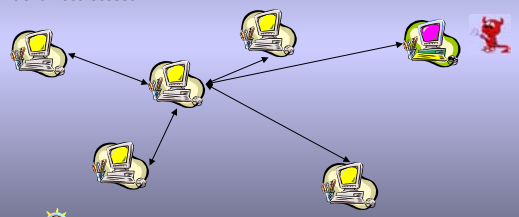
COME REPERIRE UNO SNIFFER

- **trinux**
  Contiene tcpdump e sniffit
- **esniff**
  Un packet sniffer che aiuta a setacciare le password e usernames.
- **Exdump**
- **Tcpdump**
- **Ethereal**
- **Sniffit**
- **Snort**
- **Karpski**

POSSIBILE COLLOCAZIONE DI UNO SNIFFER

Uno sniffer potrebbe essere installato ovunque sulla rete.
Esistono dei punti strategici che sono favoriti rispetto ad altri:

- punto adiacente ad una macchina in cui si può presumere passino notevoli quantità di password;
- un gateway di rete;
- un nodo che ospita traffico in entrata e in uscita verso l'esterno della rete stessa.



Sono favoriti perché passano particolari informazioni

POSSIBILE COLLOCAZIONE DI UNO SNIFFER

Se la LAN è connessa con l'esterno lo sniffer cercherà delle procedure di accesso (login e password) con le altre reti.

Esistono numerose eccezioni per cui è difficile capire i punti esatti in cui cercare uno sniffer.

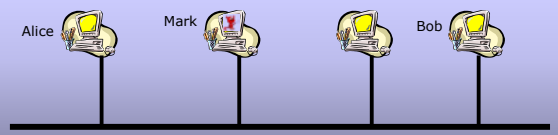
La locazione più probabile di uno Sniffer, in una LAN, è sui server che la gestiscono per intero o nei nodi intermedi.

Sicuramente rappresentano un pericolo per la nostra privacy; possono portare agli stessi risultati di intercettazioni telefoniche e ambientali.

COME SPIARE IL TRAFFICO DELLA RETE

Ethernet fu costruito in base al seguente principio di condivisione:

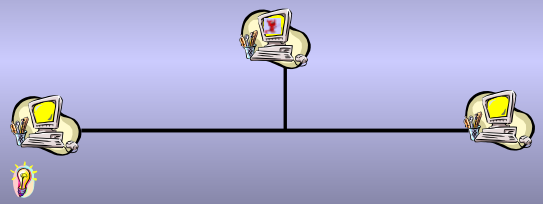
- tutte le macchine della rete locale condividono lo stesso cavo;
- tutte le macchine possono vedere tutto il traffico sullo stesso cavo;
- l' hardware di Ethernet è costruito con un "filtro" che ignora tutto il traffico che non appartiene ad esso semplicemente ignorando tutti i frames il cui indirizzo di MAC non fa matching.



Mark può vedere tutto il traffico tra Alice e Bob, finché loro sono sullo stesso filo di Ethernet.

MONITORAGGIO SU INTERNET

Esempio:
Due macchine in un ufficio che comunicano:
- entrambi sono su Internet;
- prendono una strada diretta di comunicazione;
- il traffico non viaggia mai attraverso la porzione pubblica;
- il traffico e' esterno ad Internet.



Qualsiasi comunicazione segue ovunque nella rete il principio "percorso – minimo - costo".

SNIFFING CON MODEM

Un cavo-modem si divide in due canali asimmetrici:
- Upstream: "ricevere-solo" su uno canale ad alta velocità (tra i 30-mbs e i 50-mbps);
- Downstream: "trasmettere-solo" su un canale a bassa-velocità (circa 1-mbps).

UNSTREAM

DOWNSTREAM

I cavi-modem separano gli indirizzi MAC dagli indirizzi IP; settare il proprio adattatore di Ethernet in "modalità promiscua" non ha effetto.

Se un cavo-modem lavora su un segmento non può lavorare su un'altro diverso.

SNIFFING CON MODEM

Non è possibile sniffare su cavo-modem.

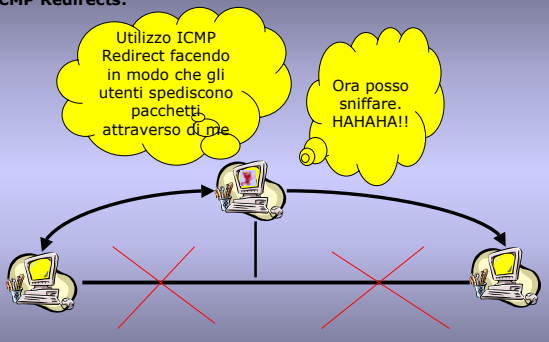
SNIFFING CON MODEM

Comunque ci sono modi per farlo:

- **ARP:**

SNIFFING CON MODEM

- **ICMP Redirects:**

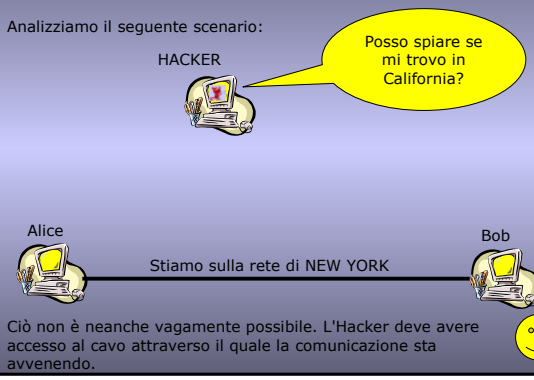


SNIFFING CON MODEM

ICMP Router Advertisements:

SNIFFING SENZA ACCESSO AL CAVO

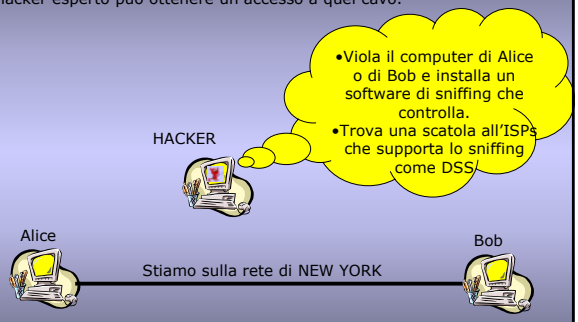
Analizziamo il seguente scenario:



Ciò non è neanche vagamente possibile. L'Hacker deve avere accesso al cavo attraverso il quale la comunicazione sta avvenendo.

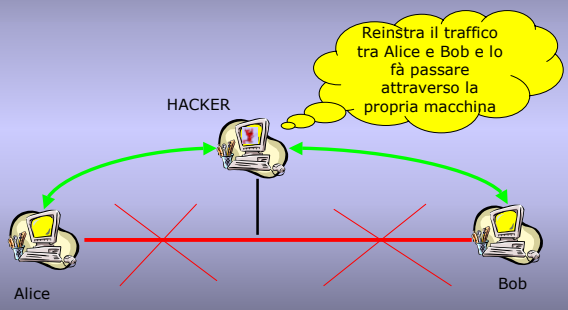
SNIFFING SENZA ACCESSO AL CAVO

Accesso remoto al cavo:
Un hacker esperto può ottenere un accesso a quel cavo.



SNIFFING SENZA ACCESSO AL CAVO

Chiusura del cavo:



SNIFFING SENZA ACCESSO AL CAVO

Rootkits e Admin Trojans Remoto
Su UNIX, programmi di sniffing sono parte di più "rootkits". Su Windows, lo sniffing è parte di alcuni RAT, (Admin Trojans Remoto, e.g. BackOrifice).

Questi programmi possono essere usati per sniffare traffico in generale e solitamente sono configurati per sniffare semplicemente e-mail e password.

COME INDIVIDUARE UNO SNIFFER

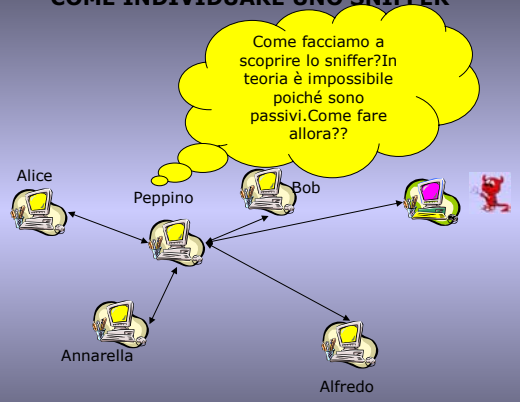
•Gli sniffer catturano solamente pacchetti, e non emettono niente.

La situazione può essere paragonata alla quella di scoprire ricevitori radio/TV.

Gli sniffer si distinguono in:

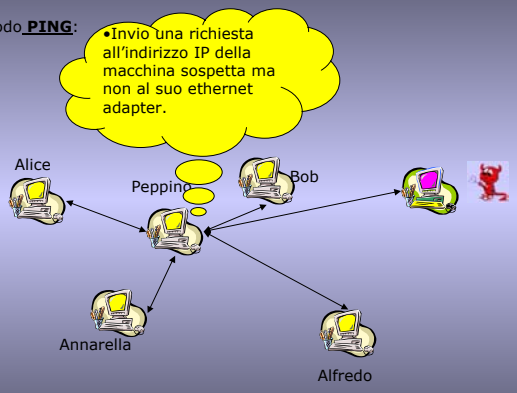
- "*stand-alone*" non trasmettono nulla, e' teoricamente impossibile da individuare;
- "*non-stand-alone*": generano del traffico ben identificabile ed è possibile localizzarli.

COME INDIVIDUARE UNO SNIFFER

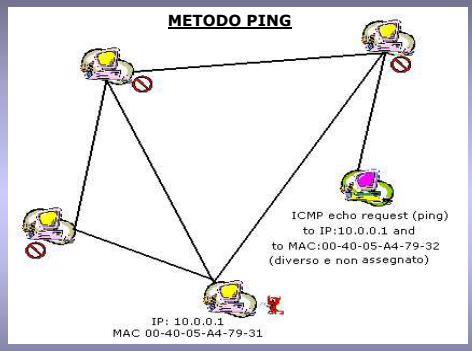


COME INDIVIDUARE UNO SNIFFER

Metodo **PING**:



COME INDIVIDUARE UNO SNIFFER



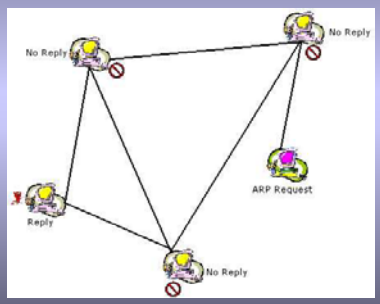
Inconveniente: Gli sniffer adottano un filtro MAC che vanificano la ricerca

COME INDIVIDUARE UNO SNIFFER

metodo ping, parte seconda:si usa il metodo ping su ogni servizio attivo in rete che generi risposte conosciute, oppure si utilizza ogni protocollo che possa generare un errore sulla macchina bersaglio.

COME INDIVIDUARE UNO SNIFFER

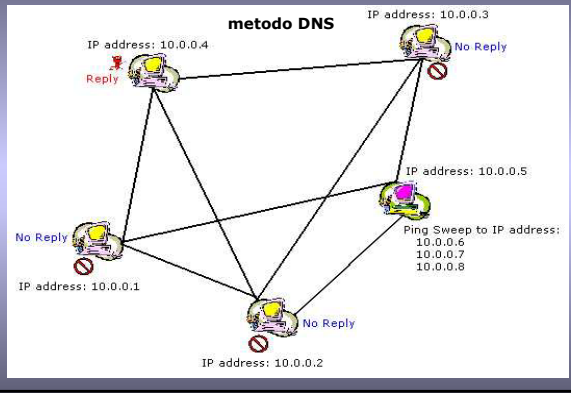
metodo ARP: si usa il protocollo ARP (Address Resolution Protocol); il metodo più semplice è inviare un ARP request a un indirizzo non broadcast sospetto: se risponde è in promiscuos mode.



COME INDIVIDUARE UNO SNIFFER

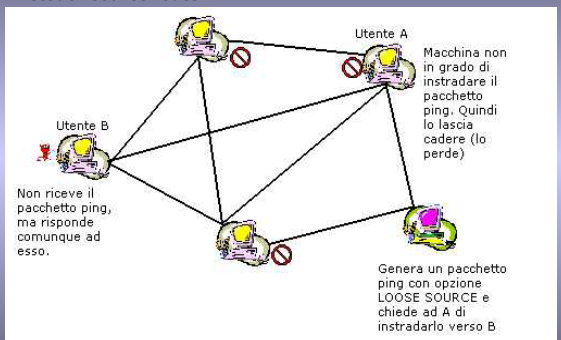
Variante del Metodo ARP
Si avvantaggia della *cache* ARP di ogni macchina, ossia l'archivio in cui vengono immagazzinati, per alcuni minuti o per un tempo più lungo, le informazioni relative sia al mittente che al destinatario del traffico generato da una determinata interfaccia.

COME INDIVIDUARE UNO SNIFFER



COME INDIVIDUARE UNO SNIFFER

metodo *"source route"*:



Poichè B risponde comunque al pacchetto ping vuol dire che il suo dispositivo di rete è settato in modalità promiscua e quindi sta operando uno sniffing.

COME INDIVIDUARE UNO SNIFFER

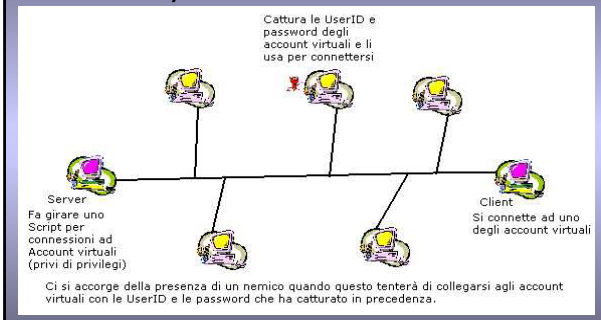
DETTAGLI METODO **SOURCE ROUTE**

1.Viene aggiunta una opzione alla testata di IP.
2.I Routers ignorano gli indirizzi di destinazione IP e invece considerano il prossimo indirizzo IP.

Questo vuole dire che , quando un utente spedisce il pacchetto, può dire "per favore spedisca un pacchetto a Bob, ma instradalo attraverso Anna

COME INDIVIDUARE UNO SNIFFER

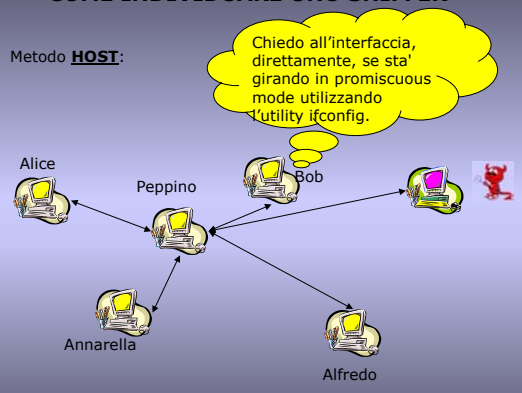
metodo "decoy":



Ci si accorge della presenza di un nemico quando questo tenterà di collegarsi agli account virtuali con le UserID e le password che ha catturato in precedenza.

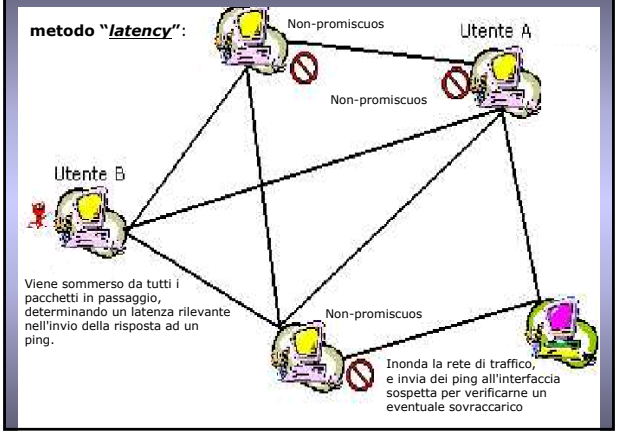
COME INDIVIDUARE UNO SNIFFER

Metodo **HOST**:



COME INDIVIDUARE UNO SNIFFER

metodo "*latency*":



COME INDIVIDUARE UNO SNIFFER

metodo "*latency*":

•Degrada sensibilmente le performance della rete locale

• Genera molti "false positive".

• Lo sniffer può fare in modo di rispondere al ping in "KERNEL-MODE", restando cosi indipendente dal carico sulla CPU determinato dalla raccolta di tutto il traffico

COME INDIVIDUARE UNO SNIFFER

TDR (Time-Domain Reflectometers): Cavo Radar che spedisce impulsi sul cavo, e riflette dei grafici.
TDR fu usato da Ethernet per scoprire i cosiddetti "vampiri", ma molto raramente vengono utilizzati oggi per le topologie a stella

Hub lights:Si può manualmente controllare l'HUB per vedere se c'è qualche collegamento inaspettato. Aiuta ad identificare cavi per dedurre dove (fisicamente) un sniffer del pacchetto è localizzato

SNMP monitoring: Piccoli HAB intelligenti con gestione SNMP che possono provvedere a monitorare le HUB Ethernet (e altro).

COME INDIVIDUARE UNO SNIFFER

TOOLS per scoprire sniffers:

-AntiSniff

-CPM (Controlli Maniera Promiscua)

-neped

-sentinel

-cpm (Controlli Maniera Promiscua)

-ifstatus

MIGLIORARE LA PROTEZIONE

Per avere una difesa migliore contro uno sniffer bisogna:

1- Sostituire l'HUB con uno switch.
Vantaggi:Migliore protezione
Svantaggi:L'hacker può intercettare paccetti ARP.

2- Metodo "router redirection":
Vantaggi: Si nascondono gli IP-to-MAC dei mittenti. L'Hacker non può instradare attraverso la propria macchina.

3- Configurazione manualmente degli indirizzi MAC.

MIGLIORARE LA PROTEZIONE

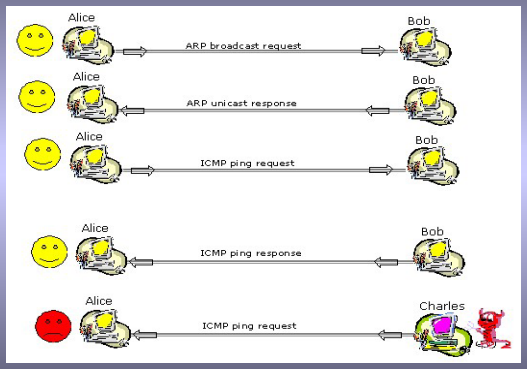
ESEMPIO

Alice vuole trovare l'indirizzo Ethernet MAC di Bob.
Bob ha come indirizzo IP "192.0.2.1". Alice manda una richiesta ARP con le informazioni seguenti.

Operazione: Request
Alice: 192.0.2.173 00-40-05-A4-79-32
Bob: 192.0.2.1 ?? ?? ?? ?? ?? ??

Alice ha un pacchetto IP da spedire a Bob per ottenere l'indirizzo MAC di Bob.
Bob risponde ad Alice,dicendole il suo indirizzo MAC.
Alice spedisce il suo pacchetto all'indirizzo MAC di Bob.

MIGLIORARE LA PROTEZIONE



CONFIGURAZIONE DELLA LAN

Le trasmissioni sono spedite ad ognuno su un Ethernet switch. Per cui un utente può:

1-Sovvertire lo switch mandando l'ARP e dicendo di essere qualcun'altro come indirizzo sorgente.

2-Spedire un ARP all'indirizzo MAC del router dicendo di essere la vittima.

Soluzione:La maggior parte degli switch permettono una configurazione statica prevenendo cosi la situazione descritta.

ADATTATORI CHE NON SUPPORTANO LO SNIFFING

- IBM TOKEN RING

- Ad alcuni adattatori manca la funzionalità nel driver di settare la modalità promiscua e ciò significa che tutti i programmi che tentano di metterli in modalità promiscua falliranno.

PROTEZIONE DEI DATI

SSL
"Secure Sockets Layer". Permette di codificare e quasi sempre è usato quando utenti registrano le loro informazioni relative alle carte di credito.

PGP e S/MIME:
Il migliore modo per proteggere dagli hacker le e-mail consiste nel codificarle. I due modi comuni per fare questo sono: PGP (Pretty Good Privacy) e S/MIME (Secure Mime). PGP. S/MIME è incorporato in programmi di e-mail.

PROTEZIONE DEI DATI

SSH "Secure Shell":
E' lo standard di UNIX e fu sviluppato originalmente dalla Finish Company ed esistono molte realizzazioni freeware.

VPN (Virtual Private Networks)
VPN effettua la codifica del traffico su Internet. Comunque, se un hacker compromette gli end-nodes di una connessione VPN, può sniffare il traffico.

PROTEZIONE DEI DATI

SMB/CIFS
Nell'ambiente di Windows/SAMBA, garantisce che la più vecchia autenticazione di LanManager sia inutilizzabile. Questo richiede SAMBA v2 o successive, WinNT SP3 o successive, e così via.

Kerberos v5
Windows 2000 e UNIX, supportano l'autenticazione per Kerberos. Questo è uno dei meccanismi disponibili più sicuro.

SMART CARDS
Ci sono realizzazioni di "schede intelligenti" che prevedono password one-time. Questi spesso si usano in connessioni remote, sia dial-in che VPN.

Stanford SRP (Secure Remote Password)
Miglioramenti a Telnet e FTP per UNIX e Windows.

TCPDUMP

TCPdump è la versione di UNIX di un decodificatore di pacchetto scritto da Van Jacobsen per analizzare problemi di performance di TCP.

TCPdump deve potere mettere l'interfaccia (tipicamente un Ethernet) in maniera promiscua per leggere tutto il traffico della rete.
Esso darà delle informazioni riassuntive per ogni pacchetto ricevuto o trasmesso sull'interfaccia.

TCPDUMP

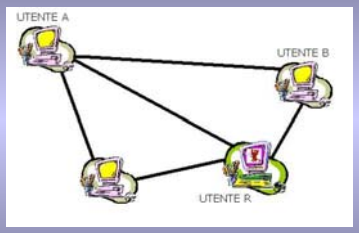
Problemi che si possono riscontrare:

a)Nessun output.

b)Pacchetti lasciati cadere.

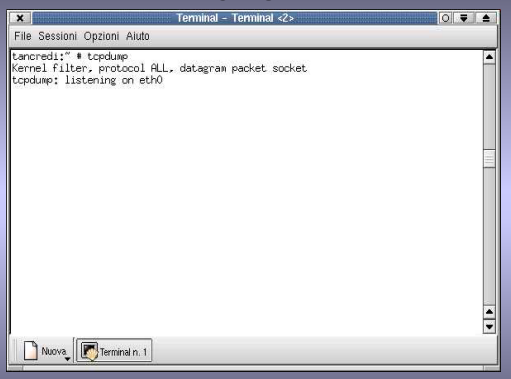
TCPDUMP

Vediamo un tipico esempio di cattura:



L'Utente A e l'Utente B vogliono comunicare e l'Utente R, che ha accesso di root, vuole sniffare il traffico. Per fare ciò avvia TCPDUMP.

TCPDUMP



A questo punto TCPDUMP è in attesa

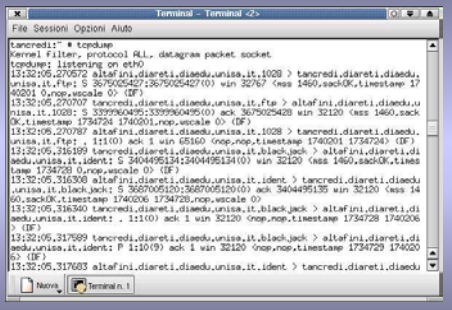
TCPDUMP

L'utente A si *connette* all'utente B attraverso un operazione di FTP:

Da questo momento in poi tutti i pacchetti sono catturati dall'utente R.

TCPDUMP

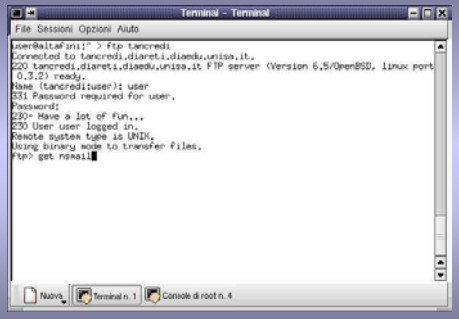
Poiché vi è un sistema di identificazione con UserID e password, esse saranno catturate:



Dalla figura si vede la cattura dei pacchetti contenenti la UserID e la password dell'Utente A.

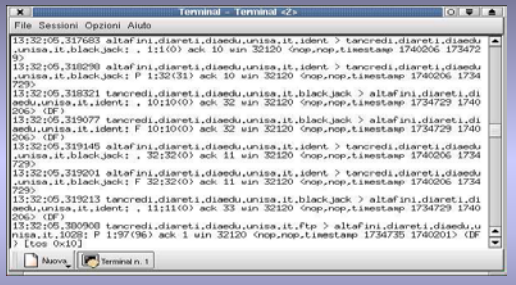
TCPDUMP

Ora l'Utente A trasferisce un file contenente e-mail dalla macchina dell'Utente B:



Anche questi pacchetti vengono catturati dall'utente R:

TCPDUMP



Quando l'Utente R interromperà l'esecuzione di TCPdump gli saranno fornite informazioni sui pacchetti catturati, ad esempio la quantità dei pacchetti catturati; a questo punto potrà analizzare quanto ***sniffato!***