# Linux day @ Egloo
# Wireless 802.11b
# Sicurezza, pregi, difetti, hacking


http://www.cmlug.org

Alfredo Morresi --> legolas.info@gmx.net

Marco Pagnanini --> tmp@cmlug.org

Ancona, 26 Novembre 2005

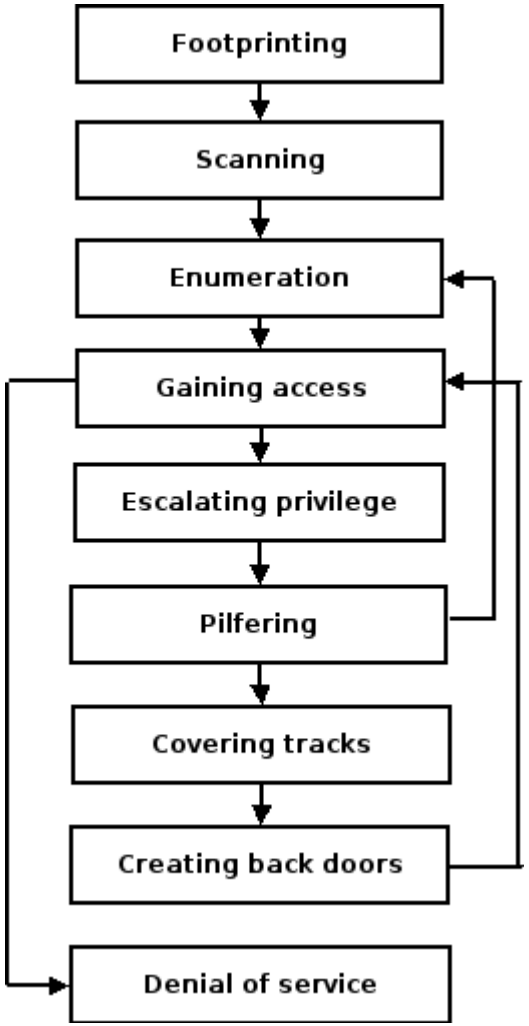
# *Scopo di questo talk*

- Comprendere come si effettua un attacco informatico, come agisce un criminale informatico, per imparare a difendersi, per prendere le giuste contromisure
- Mostrare nella pratica alcune tra le tecniche utilizzate per il cosiddetto “sniffing” delle reti wireless ed ethernet

# *Perchè attaccare?*

- I crackers (malicious hackers) attaccano per diversi motivi
- Obiettivo principale: ottenere i privilegi di root
- In modo che possano:
  - usare la tua banda
  - usare i tuoi dati
  - usare la tua CPU
  - usare il tuo spazio disco
  - fare attività di vandalismo

# Diagramma di flusso dell'anatomia di un attacco

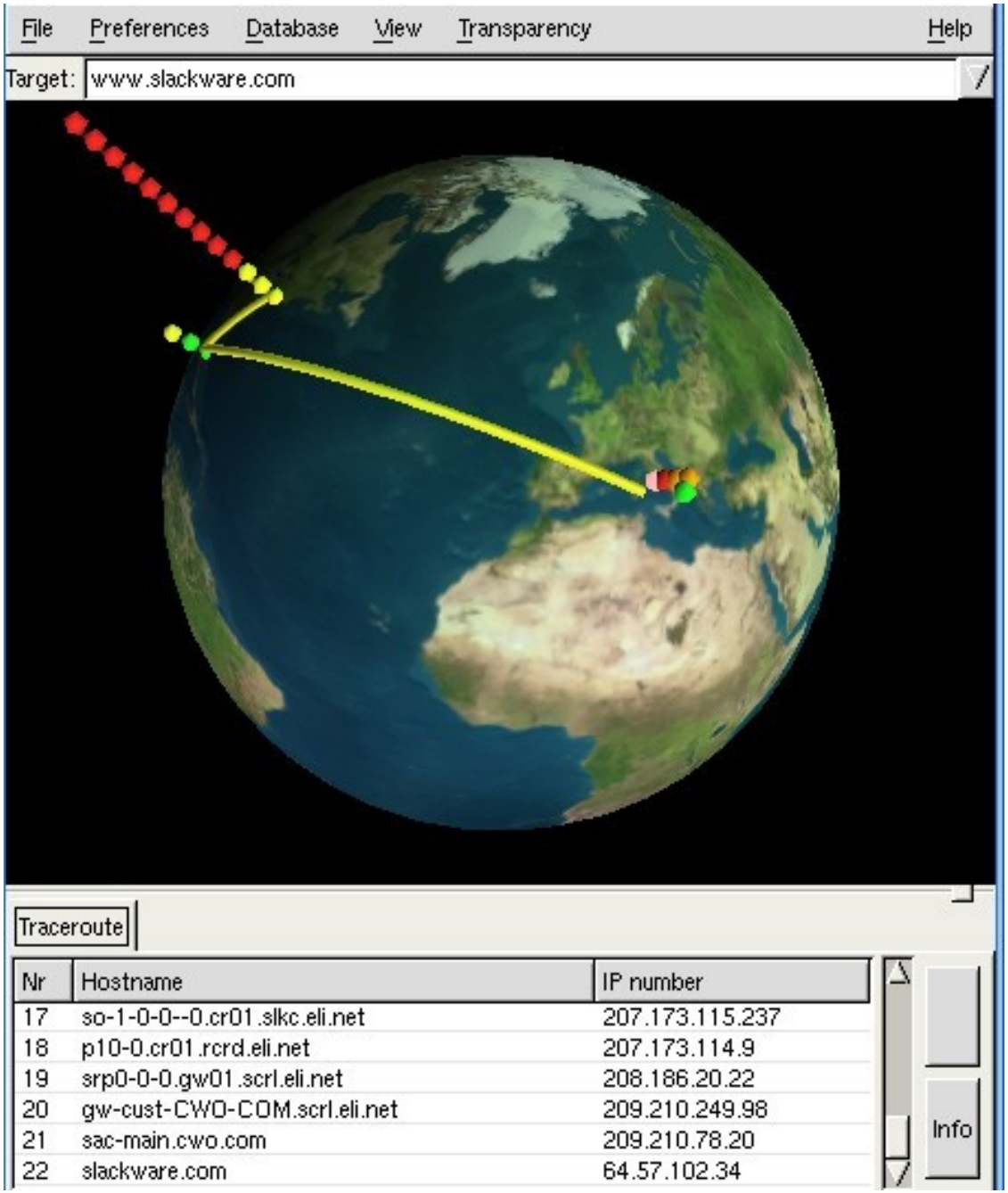



Dal testo “Hacking Exposed”

# *Anatomia di un attacco [1]*

- OGGETTO: acquisizione range di indirizzi, informazioni sul namespace, altre informazioni
- METODOLOGIA: **footprinting**
- TECNICA (STRUMENTI): whois database (whois), DNS (dig), p2p (p2p sw), Edgar (browser: sec.gov), USEnet (browser: google), varie (browser: samspade.org, online tools), routing (traceroute)

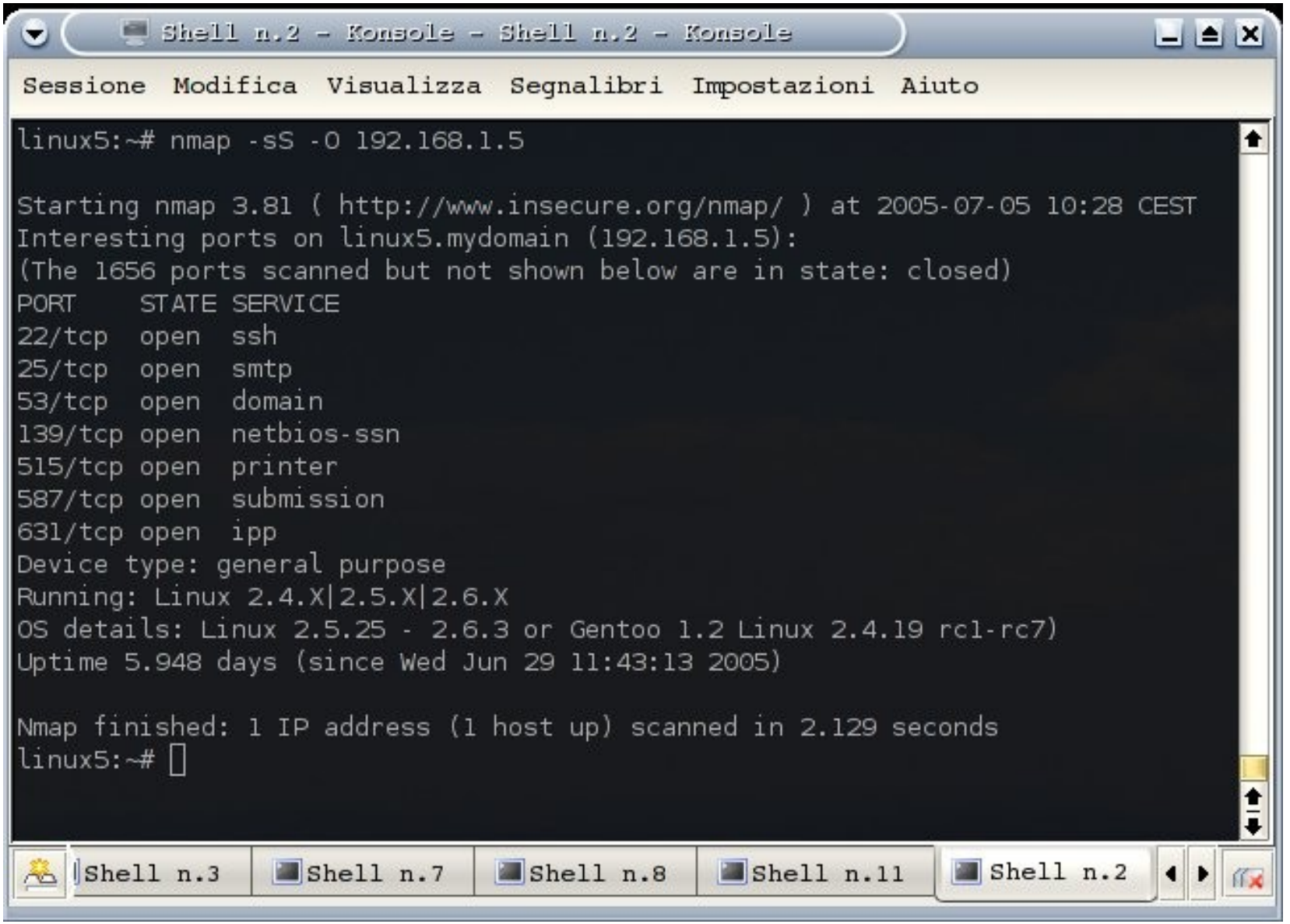
# Anatomia di un attacco [1.1]



# *Anatomia di un attacco [2]*

- OGGETTO: analisi del sistema obiettivo, identificazione dei servizi attivi alla ricerca delle migliori vie di accesso
- METODOLOGIA: **scanning**
- TECNICA (STRUMENTI): ping sweep (fping), TCP/UDP portscan (nmap), OS detection (nmap), firewalking (hping)

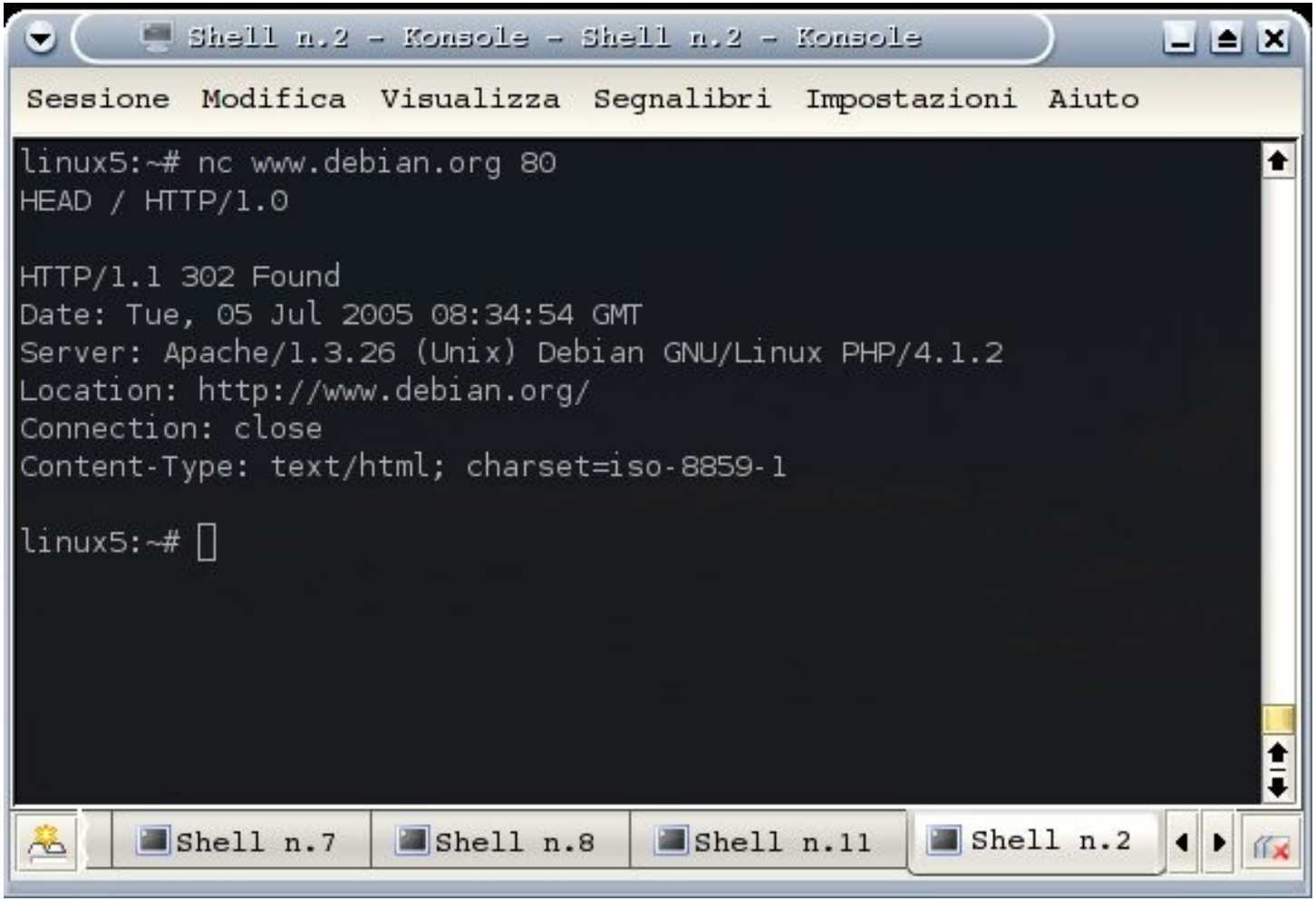
# Anatomia di un attacco [2.1]



# *Anatomia di un attacco [3]*

- OGGETTO: indagini più approfondite e maggiormente intrusive al fine di identificare servizi vulnerabili, account utente validi o risorse condivise scarsamente protette
- METODOLOGIA: **enumeration**
- TECNICA (STRUMENTI): elenco account utente (windows null sessions), elenco file condivisi (showmount), identificazione applicazioni (banner brabbing con telnet o netcat, rpcinfo)

# Anatomia di un attacco [3.1]



# *Anatomia di un attacco [4]*

- OGGETTO: i dati raccolti sono a questo punto sufficienti per tentare un accesso furtivo al sistema target ed eventualmente per acquisire nuove informazioni sensibili
- METODOLOGIA: **gaining access**
- TECNICA (STRUMENTI): sniffing password (ettercap, tcpdump, ethereal, kismet), acquisizione file delle password (dipende...), buffer overflows (dipende...)

# *Anatomia di un attacco [5]*

- OGGETTO: se al passo precedente si è riusciti ad ottenere un accesso a livello utente, in questa fase l'attacker cercherà di ottenere il completo controllo del sistema (root)
- METODOLOGIA: **escalating privilege**
- TECNICA (STRUMENTI): password cracking (john), exploits noti (dipende...)

# *Anatomia di un attacco [6]*

- OGGETTO: si reitera il processo di recupero delle informazioni (in particolare le due fasi precedenti) per guadagnare l'accesso ad altri sistemi fidati
- METODOLOGIA: **pilfering**
- TECNICA (STRUMENTI): sistemi o utenti remoti fidati (~/.rhosts, hosts.equiv), ricerca password in chiaro (dati utente, file di configurazione)

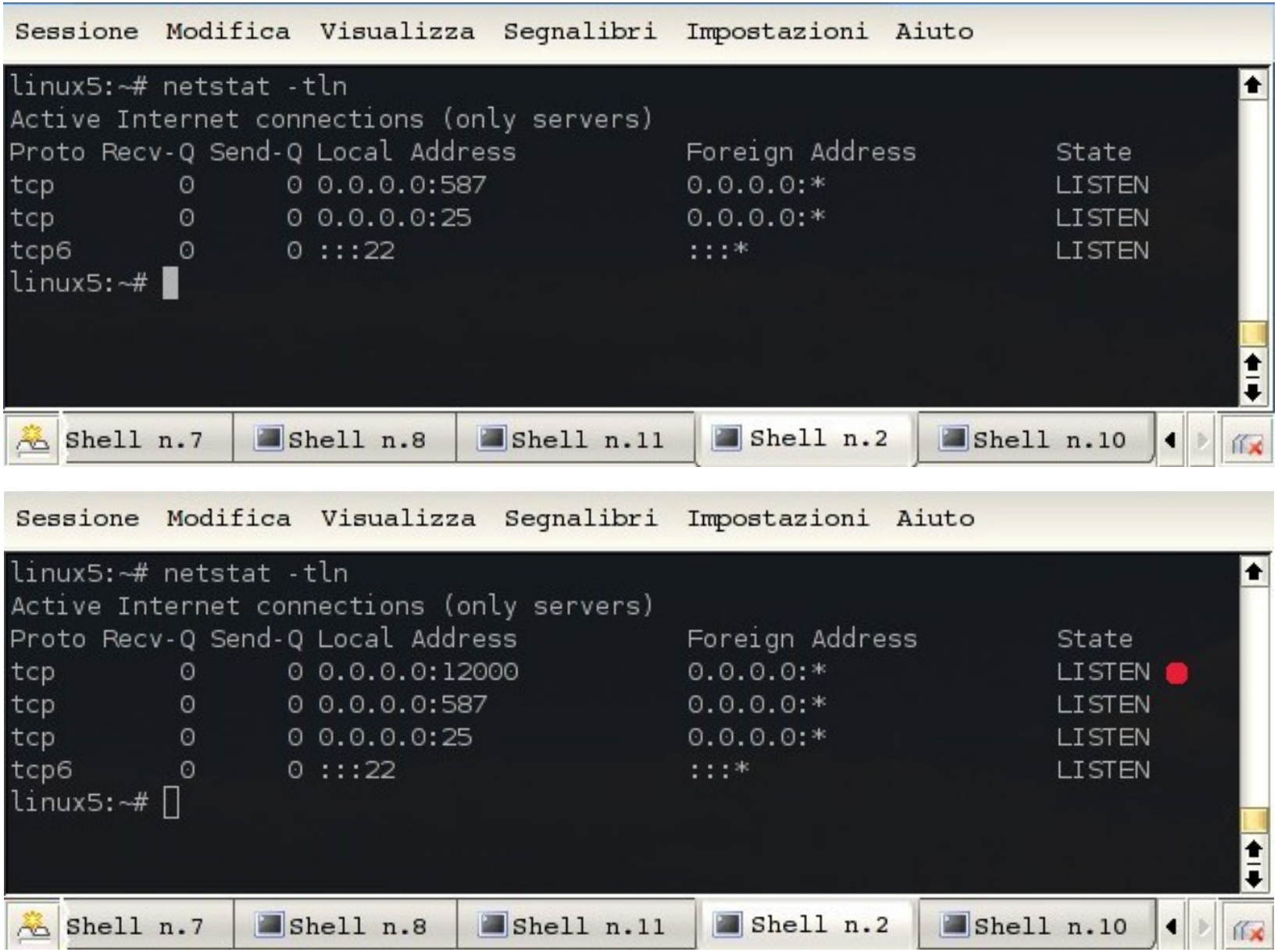
# *Anatomia di un attacco [7]*

- OGGETTO: quando la totale padronanza del sistema è ormai garantita, è necessario eliminare le tracce
- METODOLOGIA: **covering tracks**
- TECNICA (STRUMENTI): eliminazione log (dipende…)

# *Anatomia di un attacco [8]*

- OGGETTO: vengono lasciate aperte delle porte nel sistema per fare in modo che i privilegi di accesso siano facilmente riguadagnati
- METODOLOGIA: **creating backdoors**
- TECNICA (STRUMENTI): creazione falsi account utente appartenenti a gruppi come *wheel* (dipende...), schedulazione processi di rete con cron o at per il controllo remoto (netcat, vnc), modifica file startup  (rc*/, init.d/), installazione di meccanismi di monitoraggio, rilevazione combinazione tasti (keylogger), sostituzione processi principali con trojan (login, ps, ...), occultamento strumenti (rootkit)

# Anatomia di un attacco [8.1]



# *Anatomia di un attacco [9]*

- OGGETTO: se l'attacco non va a buon fine come ultimo tentativo colui che attacca può cercare di mettere fuori uso il sistema obiettivo
- METODOLOGIA: **denial of service**
- TECNICA (STRUMENTI): tecniche ICMP come ping of death, SYN flood (hping, ...), overlapping fragment (teardrop), pacchetti con identico src/dst con flag SYN attivo (hping, ...), DDos (dipende...)

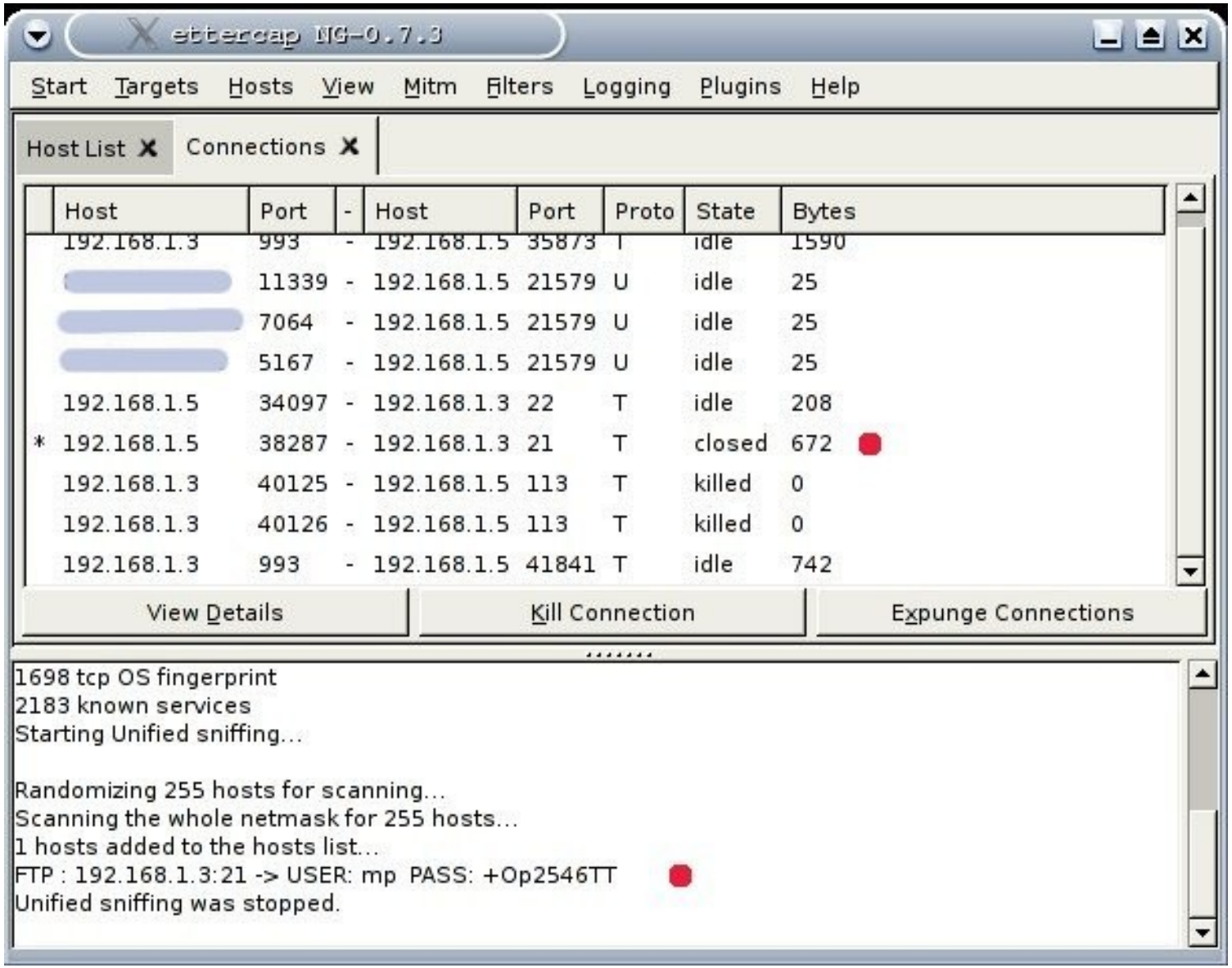
# *Conseguenze falle nei protocolli TCP/IP*

- Come è possibile sfruttare le falle e le vulnerabilità del TCP/IP?
  - Mediante **sniffing**:
    - Individuazione pacchetti alla ricerca di password in chiaro
    - Ricerca di altre informazioni sensibili (Es: chiavi WEP da decifrare)
  - Mediante **session hijacking**:
    - Dirottamento connessioni mediante attacco **Man In The Middle (MITM)**.

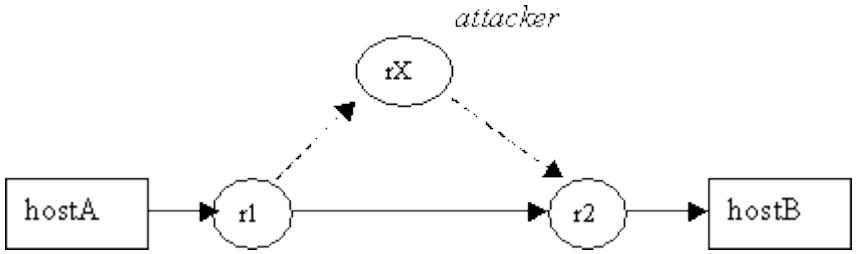
# *Tool più utilizzati*

- I due strumenti più utilizzati sono:
  - **Ettercap** (jack-of-all-trades!)
  - **Hunt**
  - **Dsniff** (Dsniff + altri tool)
- Ettercap è un completo analizzatore di rete
- Hunt permette il dirottamento delle connessioni, il cosiddetto session hijacking, (anche ettercap lo permette) grazie alla tecnica dell'**ARP spoofing**
- Tutti e tre gli strumenti permettono di “sniffare” i pachetti anche in reti dotate di switch sempre grazie alla tecnica dell'**ARP spoofing**

# Ettercap (Made in Italy)



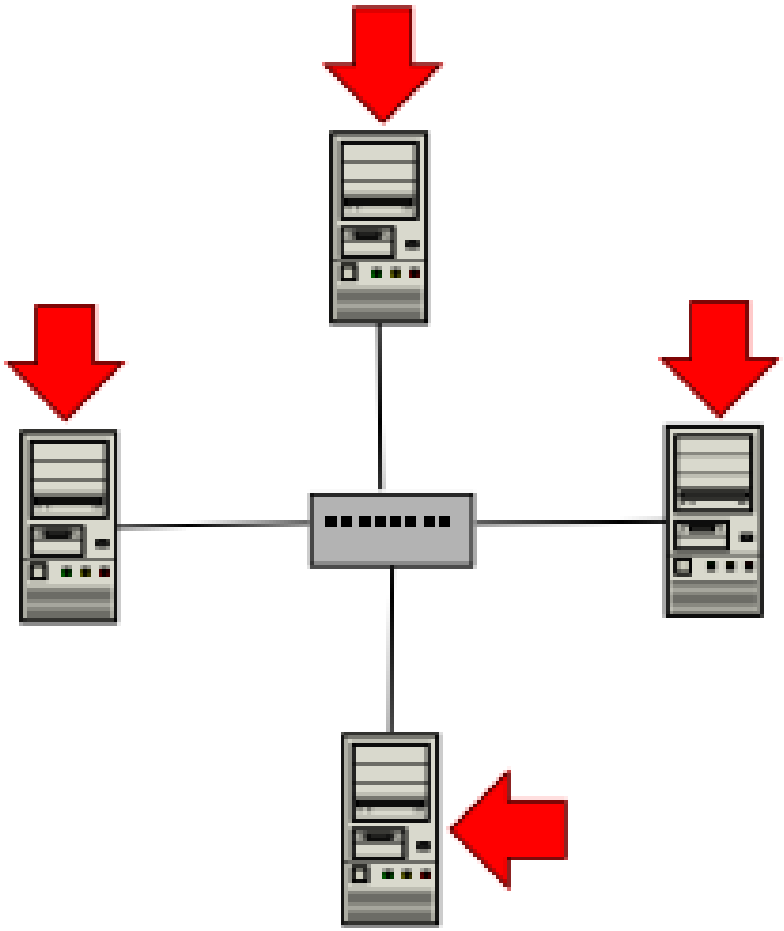
# ARP spoofing (ARP poisoning)




- Si tratta di una tecnica utilizzata dai cracker per sniffare i pacchetti su reti con switch, per effettuare attacchi DOS in reti LAN, per il dirottamento delle sessioni, ...
- Come funziona?
  - Viene modificato il frame ethernet: in particolare si va ad inserire un indirizzo MAC falso per ingannare i dispositivi collegati a quella specifica sottorete. Il frame falsificato contiene un indirizzo MAC diverso dall'indirizzo di colui che invia il frame, in particolare contiene l'indirizzo MAC dell'attacker. L'attacker una volta spiato il contenuto del frame inoltrerà lo stesso al giusto destinatario. Il tutto avviene in maniera trasparente! (In realtà c'è un calo di prestazioni della rete).

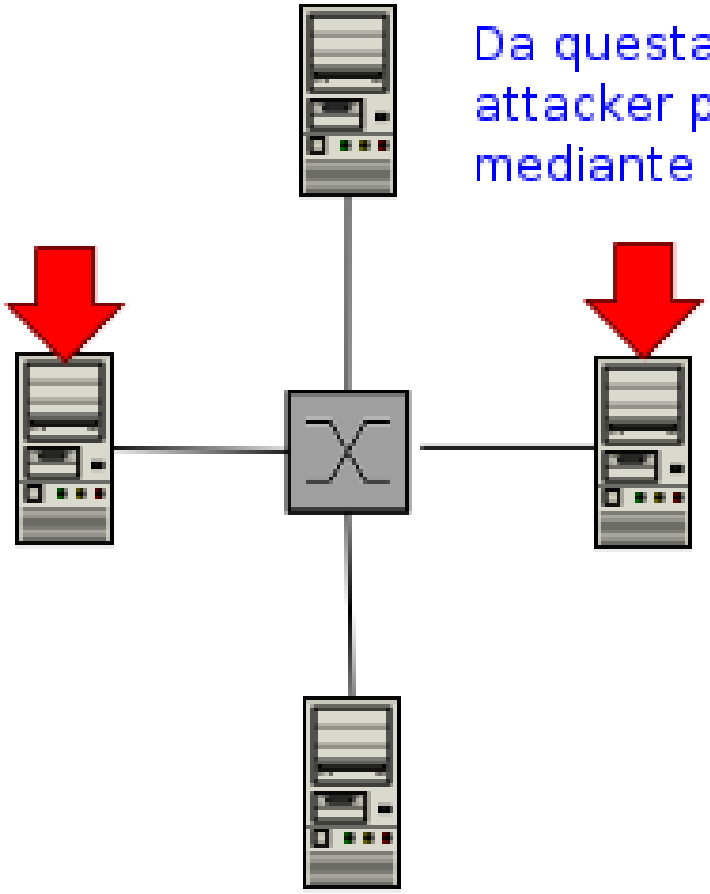
# Perchè è necessario l'ARP spoofing

**Rete con hub**



L'attacker riesce a sniffare i pacchetti da qualsiasi postazione.

**Rete con switch o "switchata"**



Da questa postazione un attacker puo' sniffare solo mediante ARP spoofing.


802.11b

Ovvero: perdete ogni speranza *(di sicurezza)* o voi che entrate!

# Introduzione al wi-fi

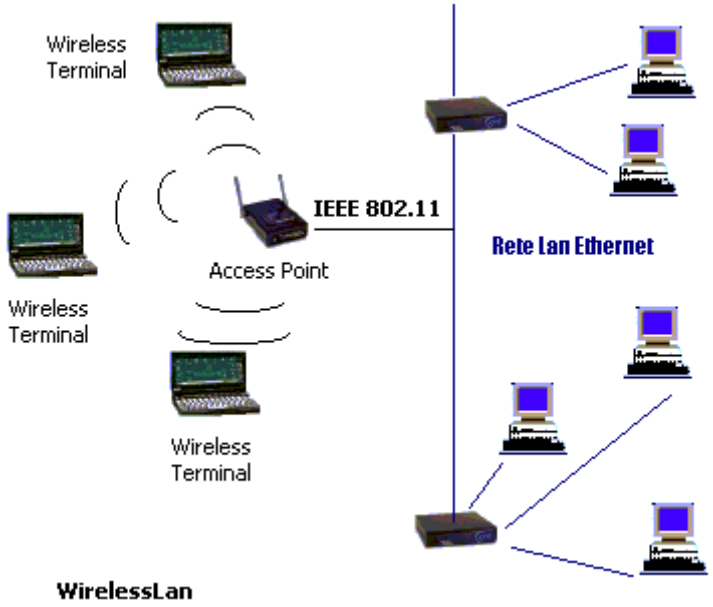
- Wi-Fi: cos'e'?
  - Wi-Fi significa "Wireless Fidelity", e consiste in una serie di standard per reti locali wireless (WLANs) basate sulle specifiche 802.11... Gli scopi iniziali di questa tecnologia furono quelli di abilitare connessioni senza fili tra vari device di una LAN, ma oggi il wi-fi e' anche usato per connettersi ad Internet ecc...
- Alcuni dei vantaggi del Wi-Fi
  - liberta' dai fili
  - facilita' di implementazione - interconnessione tra diversi dispositivi
  - mobilita'
- Alcuni svantaggi del Wi-Fi
  - degrado delle performance
  - range limitato
  - SICUREZZA

# Introduzione al wi-fi - standard

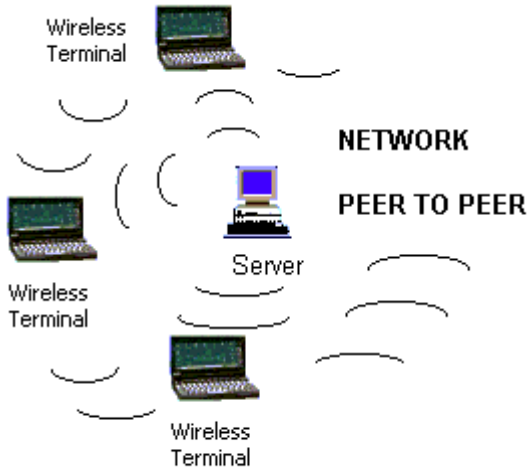
- Standard attuali
  - Promossi dall'WECA (Wireless Ethernet Compatibility Alliance)
  - La famiglia 802.11 include 3 protocolli separati: a, b, g
  - Ci sono ulteriori specifiche (c-f, h-j, n) con diverse estenzioni e miglioramenti
  - Il primo standard largamente accettato fu l'802.11b, seguito dall'802.11a e poi 802.11g
  - Operando a 2.4 ghz, in una banda di frequenze non licenziata, le reti wireless 802.11b e g possono venir disturbate da forni a microonde, telefoni cordless e altri device che usano lo stesso range di frequenza
- WiMAX
  - Nuovo standard, piu' veloce e con piu' copertura del WiFi. Implementa anche diverse politiche di protezione

# Introduzione al wi-fi - topologie

## Topologia infrastructured




## Topologia ad-hoc



# Introduzione al wi-fi - problemi

- L'assenza di controllo fisico all'accesso alla rete rende piu' difficoltoso localizzare eventuali intrusi
- Molti segnali di controllo/gestione della rete (beacon) vengono mandati in broadcast, quindi e' banale intercettarli
- In genere gli access point non hanno bisogno di configurazioni per poter funzionare correttamente. Queste configurazioni sono pero' insicure “out-of-the-box”
- Molti amministratori (?) di reti wireless non hanno il giusto know-how necessario per gestire una rete wireless, quindi lasciano le impostazioni di default degli apparati, non abilitando la crittografia e non cambiando le password di default
- Nonostante tutto, anche se foste dei bravi amministratori... gli schemi di criptatura dei pacchetti sono stati gia' provati insicuri! Evviva!!!!
- Ci sono delle estenzioni proprietarie per aumentare velocita' e sicurezza, ma essendo proprietarie, non sono interoperabili

# *Introduzione al wi-fi – perche' bucare?*

- accesso gratuito a Internet... Puo' sempre far comodo :)
- lanciare attacchi da un ip non riconducibile al cracker
- spamming di vario vario genere
- furto di dati critici / personali / riservati
- sniffing di password
- usare la rete wireless bucata come proxy per attivita' illegali (distribuzione materiale sotto copyright, pedo-porno-pedofilia, minacce e intimidazioni)
- tante altre cose che a me non vengono in mente, ma che ad altri sicuramente avranno gia' solleticato qualche idea

Ovviamente tutte queste attivita' sono illegali

# *Wi-Fi - Tecniche di intrusione*

- Scacco in 3 mosse:
  - scoprire la rete
  - sniffarne il traffico per raccogliere alcuni dati
  - configurare la propria scheda di rete e... entrare!

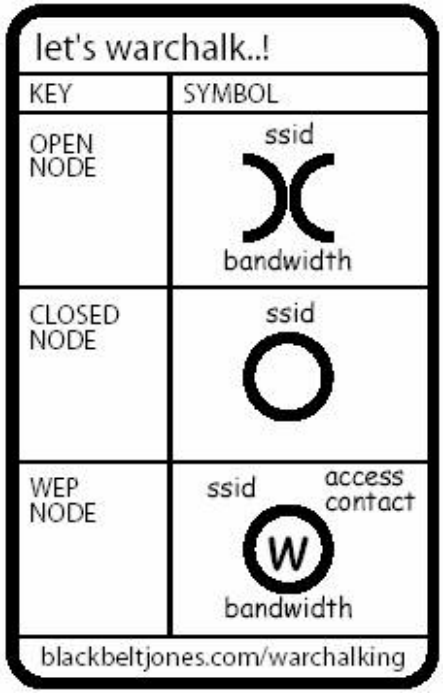
- I pezzi da usare
  - portatile con scheda wi-fi, palmare, antenna omni o direzionale
  - kismet, wepcrack, airsnort
  - macchanger, iwconfig, ifconfig

# Wi-Fi - Tecniche di intrusione: scoprire

- Wardriving
  - Attività che consiste nell'intercettare reti Wi-Fi, in automobile o a piedi con un laptop, solitamente abbinato ad un ricevitore GPS per individuare l'esatta locazione della rete trovata ed eventualmente pubblicarne le coordinate geografiche su un sito web. Per una miglior ricezione vengono usate antenne omnidirezionali. È necessario utilizzare un software specifico, quasi sempre disponibile gratuitamente e per diverse piattaforme: *NetStumbler* (Winzozz), *KisMac* (Mac), *Kismet* (Linux) e *WiFiFoFum* (PocketPC)

# Wi-Fi - Tecniche di intrusione: scoprire

- Warchalking
  - Usanza che consiste nel disegnare simboli in luoghi pubblici per segnalare una rete senza fili Wi-Fi aperta. I simboli warchalking sono stati concepiti da un gruppo di amici nel Giugno 2002 e pubblicati da Matt Jones. Quando una rete Wi-Fi viene intercettata, il warchalker disegna un simbolo speciale su qualunque oggetto vicino all'intercettazione come un muro o sulla pavimentazione della strada




# Wi-Fi - Tecniche di intrusione: sniffare

- Fattori di sicurezza in una rete wi-fi stand-alone
  - SSID
  - Access list su mac address
  - Indirizzo ip da usare
  - Autenticazione OSA (Open Systems Authentication) e SKA (Shared Key Authentication, rappresentata dalla crittografia WEP / WAP)
- Cosa c'e' di debole in questi fattori
  - l'SSID viene mandato in broadcast di default
  - Il mac address si puo' cambiare senza problemi
  - In genere l'access point fa anche da server DHCP
  - Il WEP e WAP hanno delle debolezze intrinseche con dei proof-of-concept gia' disponibili
  - non e' possibile stabilire l'identita' dell'access point o del client

# Wi-Fi - Tecniche di intrusione: sniffare

- Protocollo WEP
  - Il protocollo 802.11b include un metodo di crittografia standard chiamato WEP (Wired Equivalent Privacy). Basato sull'algoritmo di cifratura RC4, prevede l'uso di una chiave segreta "pre-condivisa" a 40 o 104 bit, a cui e' aggiunto un IV (Initialization Vector) a 24 bit, trasmesso in chiaro
  - Nell'Agosto 2001 Scott Fluhrer, Itsik Mantin and Adi Shamir pubblicarono un white-paper intitolato "Weakness in the Key Scheduling Algorithm of RC4". Il primi proof-of-concept (*AirSnort*, *WEPcrack*) potevano decifrare la chiave WEP usata raccogliendo e analizzando pacchetti contenenti IV “interessanti” o “deboli”. In genere, erano necessari dai **5 ai 10 milioni** di pacchetti crittografati (qualche ora)
  - Nell'Agosto 2004 un hacker chiamato KoreK ha reso disponibile un white-paper che tramite cripto-analisi statistica, descriveva come trovare la chiave WEP con appena **centinai di migliaia** di pacchetti. I proof-of-concept di nuova generazione quindi (*WepLab*, *AirCrack*), possono trovare in qualche minuto la chiave WEP.
    Aiutati da generatori di traffico quali *aireplay*, scavalcano anche l'impostazione di ri-codificare l'IV ogni 10 minuti

# Wi-Fi - Tecniche di intrusione: sniffare

- Protocollo WAP
  - Il WAP (WiFi Protected Access) nasce per colmare le lacune del WEP. E' parte integrante dello standard 802.11i, ma puo' essere anche implementato in altri standard precedenti. Sfortunatamente anche il WAP presenta delle vulnerabilita' ad un attacco di tipo passive dictionary. L'efficacia di questo exploit e' proporzionale all'entropia della password scelta, ma dato che molti amministratori (?) scelgono password appartenenti alla lingua e non casuali, ecco che questa vulnerabilita' potrebbe rivelarsi molto efficace
- Brute force attack
  - Entrambi i protocolli sono soggetti, comunque, ad attacchi di tipo brute-force, anche se difficilmente praticabili in certe condizioni

# *Wi-Fi – la paranoia serve davvero?*

- Alcune statistiche
  - Un'indagine di RSA security nel maggio 2005, attraversando un’ampia zona nevralgica della città di Milano, includendo piazza Duomo e tutte le principali vie del centro, un’area compresa tra la Stazione Centrale e la Stazione Garibaldi e diverse strade intorno alla Fiera ha rilevato 148 access point di cui:
    - il 72% (ben 106) non era configurato per poter utilizzare lo standard di crittografia WEP (Wired Equivalent Privacy)
    - e di questi 106, solo 2 utilizzavano le più sicure VPN (Virtual Private Network) come mezzo di protezione alternativo
  - Fonti attendibili ci dicono che a Civitanova, facendo una bella *vasca* lungo il corso, possiamo controllare la nosta posta senza problemi da un palmare, e magari farci una bella navigata mentre siamo seduti a mangiarci una pizza da quelle parti, senza dare neanche nell'occhio...

# *Wi-Fi: Tecniche di protezione*

- Si puo' solo aumentare il livello di complessita' e sicurezza della propria rete
  - Disabilitare il broadcast dell'SSID e usare SSID incomprensibili
  - Cambiare le password e le imposazioni di default degli AP
  - Impostare un'access list basata sui MAC address se possibile
  - Disabilitare il server DHCP se possibile
  - Abilitare la crittografia WEP a 128 bit
  - Usare, se possibile, una crittografia sui singoli dati che transitano in rete (navigazione SSL, posta crittografata, password dei vari servizi come posta, ftp e altro non in chiaro, fino alla VPN)
  - Posizionare gli access point lontani da finestre – muri perimetrali, in modo da evitare la dispersione del segnale
  - Implementare protocolli di autenticazione come il RADIUS
  - Implementare degli IDS per la rete Wi-Fi (anche *Kismet* o *Snort* lo fanno)

# Fine

Domande ?