



**GNU/LINUX WORLD "SOFTWARE LIBERO PER
TUTTI"**

SICUREZZA DELLE RETI WI-FI

Salve a tutti da crusher!!!

WI-FI "Wireless Fidelity"

- Il wi-fi è la tecnologia mediante la quale possiamo collegare innumerevoli computers, senza avere il fastidioso igombro di fili.

- Domanda:

- Le reti senza fili sono sicure quanto le reti cablate?

La risposta è sì, MA se adeguatamente configurate.

Protocolli di sicurezza

- WEP "Wired Equivalent Privacy"

Il suo scopo era quello di rendere le reti wi-fi sicure quanto le reti cablate (wired).

- WPA "Wi-Fi Protected Access"

Successore del protocollo wep, introduce novità sostanziali tra cui il protocollo TKIP che cambia la chiave dinamicamente.

WEP

- Nel protocollo wep può essere a 64 o 128 bit
- Il protocollo wep a 64 bit usa una chiave di 40 bit
- Il protocollo wep a 128 bit usa una chiave a 104 bit
- I restanti 24 bit del protocollo vengono utilizzati dai Vettori di Inizializzazione (VI).

WEP

Protocollo WEP a 64 bit



Protocollo WEP a 128 bit



Vettori di inizializzazione "IV"

- Sono dei numeri casuali, sempre diversi che vengono aggiunti alla chiave per aumentarne la sicurezza.

Debolezze del protocollo WEP

- Come detto la chiave utilizzata da questo protocollo è formata da 40 o 104 bit e 24 bit di IV.
- In 24 bit, la probabilità che un singolo IV venga ripetuto è piuttosto alta
- La presenza di ripetizioni negli IV (collisioni) consente di ridurre notevolmente i tempi richiesti per l'analisi e la decifrazione della chiave

WEP

- Per decifrare una chiave WEP è necessario catturare un numero abbastanza grande di IV, e poi effettuare un attacco statistico.
- **ATTACCO STATISTICO:** attacco che utilizza l'analisi statistica dei dati raccolti per ricavare la chiave di cifratura.
- Dato che nel normale traffico dati vengono trasmessi pochi IV, grazie ad una tecnica chiamata **PACKET INJECTION** è possibile generare un traffico maggiore, così da ridurre il tempo richiesto per raccogliere gli IV necessari.

WPA

- Chiave di cifratura dinamica grazie al protocollo TKIP
- Chiave di cifratura a 128 bit
- IV a 48 bit.

Debolezze del protocollo WPA

- Non è possibile individuare la chiave WPA effettuando un attacco statistico (dimensione IV)
- Per individuare una chiave WPA bisogna effettuare un attacco a FORZA BRUTA (Brute Force), catturando le informazioni sulla chiave dall'handshake tra l'access point (AP) e il client wireless.
- Per catturare l'handshake è necessario che un client si autentichi all'AP, quindi dobbiamo fare in modo che un client si disconnetta e poi riautentichi per catturare l'handshake velocemente

TERMINOLOGIA

- **ATTACCO A FORZA BRUTA**
 - Tecnica di decifrazione delle password che analizza in sequenza tutte le possibili chiavi finchè non individua quella esatta.
- **HANDSHAKE**
 - Scambio di pacchetti tra AP e client all'atto della connessione.

WPA

- Una volta ottenuto l'handshake per effettuare un attacco è necessaria una wordlist.
- **WORDLIST**: lista di parole, una wordlist è un file che contiene una lista di parole.

Limiti di un attacco

- Una volta ottenuto l'handshake per effettuare un attacco è necessaria una wordlist.
- Se una wordlist è una lista di parole potremmo fare in modo che la nostra chiave non entri tra la lista di parole

Esempi di chiave WPA

■ VULNERABILE

- ciao
- casa
- home
- hello
- fabio

■ SICURA

- ciaocasa
- cioa
- iedcafi
- fa17bi12o
- 1789presabastiglia

WPA

- Abbiamo detto che una wordlist è una lista di parole, che potrebbe essere un dizionario della lingua italiana
- La chiave casa è insicura perchè un attacco a forza bruta la individuerrebbe in pochi secondi.
- La chiave iedcafi è una chiave sicura perchè un dizionario è poco probabile che contenga tale parola

Wordlist

- Si potrebbe creare un dizionario che contenga tutte le combinazioni di lettere e numeri?
- Sì, MA per effettuare un attacco a forza bruta con un dizionario di questo genere si dovrebbero usare computer con una velocità di calcolo grandissima, e con tutto ciò si potrebbero impiegare anni.
- Esempio:
 - Per una password di 128bit composta da lettere (26) e numeri (10)

Esempio

- Password di 128bit
- La nostra chiave può essere composta da:
 - Lettere (26)
 - Numeri (10)
- Quindi una password di 128 bit combinazione di 36 elementi, può essere scelta tra 36^{128} chiavi

cioè $161 * 10^{197}$.

Che è il numero di tentativi che dovrebbe effettuare il nostro attacco a forza bruta.

Abbiamo scoperto che...

- Il protocollo da usare per proteggere le nostre reti è il protocollo WPA
- La chiave da utilizzare non deve essere semplice da trovarsi in un dizionario,
- Non necessariamente si deve mettere una chiave senza senso si può utilizzare una concatenazione di parole o concatenazione di parole e numeri

Altri tipi di sicurezza

- SSID NASCOSTO

rintracciabili tramite una scansione delle rete dopo la cattura di alcuni pacchetti

- MAC FILTER

Viene aggirato cambiando l'indirizzo mac della nostra scheda di rete.

- DISABILITAZIONE DHCP

TERMINOLOGIA

- SSID

Id della nostra rete wireless (nome)

- MAC ADDRESS

Codice che identifica, in modo univoco un dispositivo hardware.

- DHCP (Dynamic Host Configuration Protocol)

è un protocollo che permette ai dispositivi di rete di ricevere automaticamente la configurazione necessaria per poter operare su una rete.

Conclusione

- Tipo di protezione
- Password
- Filtri Mac
- Disabilitazione DHCP