Nozioni di base sulla rete wireless

Wireless local-area networks are based on IEEE 802.11

+- IEEE 802.11 is a set of media access control (MAC) and physical layer (PHY) specifications for implementing wireless local area network (WLAN) computer communication in the 900 MHz and 2.4, 3.6, 5, and 60 GHz frequency bands.

+- Un set di servizi di base è costituito da un punto di accesso e diversi client wireless.

+- I punti di accesso trasmettono regolarmente un segnale per far conoscere la rete ai clienti. Trasmettono il traffico da un client wireless a un altro. I punti di accesso possono determinare quali client possono connettersi e quando. Per collegarsi ad un punto di accesso, sono necessari sia il BSSID che il SSID.

Wireless Network frames

Le reti 802.11 utilizzano frame di dati, frame di gestione e frame di controllo.

+- I frame di dati trasmettono i dati reali e sono simili a quelli di Ethernet.

+- I frame di gestione mantengono sia la configurazione di rete che la connettività.

+- I frame di controllo gestiscono l'accesso all'etere e impediscono ai punti di accesso e ai client di interferire l'uno con l'altro nell'etere. Alcune informazioni sui frame di gestione saranno utili per capire meglio i programmi di ricognizione.

Wireless Network frames

+- I Beacon frames sono usati principalmente in ricognizione. Pubblicizzano l'esistenza e la configurazione di base della rete. Ogni frame contiene il BSSID, il SSID e alcune informazioni sull'autenticazione di base e sulla crittografia. I client utilizzano il flusso di frame beacon per monitorare la potenza del segnale del loro punto di accesso.

+- I Probe Request frames sono quasi gli stessi dei beacon frames. Un frame di richiesta viene inviato da un client quando vuole connettersi a una rete wireless. Contiene informazioni sulla rete richiesta.

+- I Probe Response frames vengono inviati ai client per rispondere ai probe request frame. Un frame di risposta risponde a ciascun frame di richiesta e contiene informazioni sulle funzionalità e configurazioni della rete. Utile per le ricognizioni.

+- I Authentication request frame vengono inviati dai client quando vogliono connettersi a una rete. L'autenticazione precede l'associazione nelle reti di infrastruttura. È possibile l'autenticazione aperta o l'autenticazione con chiave condivisa. Dopo aver riscontrato gravi errori nell'autenticazione della chiave condivisa, la maggior parte delle reti è passata all'apertura dell'autenticazione, combinata con un metodo di autenticazione più forte applicato dopo la fase di associazione.

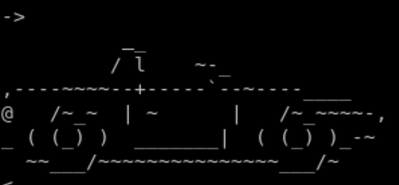
+- I Authentication response frames vengono inviati ai client per rispondere ai frame di richiesta di autenticazione. C'è una risposta a ciascuna richiesta e contiene informazioni sullo stato o una sfida relativa all'autenticazione della chiave condivisa.

+- I Association request frames vengono inviati dai client per l'associazione alla rete. Un frame di richiesta di associazione contiene molte delle stesse informazioni contenute nella richiesta di probe e deve avere il SSID. Questo può essere usato per ottenere l'SSID quando una rete è configurata per nascondere l'SSID nei frame beacon.

+- I Association response frames vengono inviati ai client per rispondere a un frame di richiesta dell'associazione. Contengono un po 'di informazioni sulla rete e indicano se l'associazione ha avuto successo.

+- Deauthentication and disassociation frames inviati a un nodo per notificare che un'autenticazione o un'associazione non sono riusciti e devono essere nuovamente stabiliti.

Wardriving ... giusto citarlo



Il wardriving è nato dal termine wardialing, il quale è un metodo diffuso da un personaggio interpretato da Matthew Broderick nel film WarGames dal quale prende, inoltre, il nome.
Il wardialing consiste nel comporre ogni numero telefonico di una specifica sequenza alla ricerca di modem per poter instaurare una comunicazione.
Questa tecnica è stata molto utilizzata prima dello sviluppo di Internet per l'attacco ad un computer.

da Wikipedia

WEP

WEP was the encryption standard firstly available for wireless networks. It can be deployed in 64 and 128 bit strength. 64 bit WEP has a secret key of 40 bits and an initialisation vector of 24 bits, and is often called 40 bit WEP. 128 bit WEP has a secret key of 104 bits and an initialisation vector of 24 bits, and is called 104 bit WEP.

Association is possible using a password, an ASCII key, or a hexadecimal key.

There are two methods for cracking WEP: the FMS attack and the chopping attack.

WEP

+- The FMS attack – named after Fluhrer, Mantin, and Shamir – is based on a weakness of the RC4 encryption algorithm . The researchers found that 9000 of the possible 16 million initialisation vectors can be considered weak, and collecting enough of them allows the determination of the encryption key. To crack the WEP key in most cases, 5 million encrypted packets must be captured to collect about 3000 weak initialisation vectors. (In some cases 1500 vectors will do, in some other cases more than 5000 are needed for success.) The weak initialisation vectors are supplied to the Key Scheduling Algorithm (KSA) and the Pseudo Random Generator (PRNG) to determine the first byte of the WEP key. This procedure is then repeated for the remaining bytes of the key.

+- The chopping attack chops the last byte off from the captured encrypted packets. This breaks the Cyclic Redundancy Check/Integrity Check Value (CRC/ICV). When all 8 bits of the removed byte were zero, the CRC of the shortened packet is made valid again by manipulation of the last four bytes. This manipulation is: result = original XOR certain value. The manipulated packet can then be retransmitted. This method enables the determination of the key by collecting unique initialisation vectors.

+- The main problem with both the FMS attack and the chopping attack is that capturing enough packets can take weeks or sometimes months. Fortunately, the speed of capturing packets can be increased by injecting packets into the network. One or more Address Resolution Protocol (ARP) packets are usually collected to this end, and then transmitted to the access point repeatedly until enough response packets have been captured. ARP packets are a good choice because they have a recognizable size of 28 bytes. Waiting for a legitimate ARP packet can take awhile. ARP packets are most commonly transmitted during an authentication process. Rather than waiting for that, sending a deauthentication frame that pushes a client off the network will require that client to reauthenticate. This often creates an ARP packet.

WPA WPA2 WPA-PSK

+- WPA was developed because of the vulnerabilities of WEP.

+- WPA uses either a pre-shared key (WPA-PSK) or is used in combination with a RADIUS server (WPA-RADIUS).

+- For its encryption algorithm, WPA uses either the Temporal Key Integrity Protocol (TKIP) or the Advanced Encryption Standard (AES).

+- WPA2 was developed because of some vulnerabilities of WPA-PSK and to strengthen the encryption further. WPA2 uses both TKIP and AES, and requires not only an encryption piece but also an authentication piece.

+- WPA-RADIUS cannot be cracked. However, if the RADIUS authentication server itself can be cracked, then the whole network is compromised

WPS

+- Wi-Fi Protected Setup (WPS, originariamente, Wi-Fi Simple Config) è uno standard di sicurezza di rete per creare una rete domestica wireless sicura.

+- Creato da Wi-Fi Alliance e introdotto nel 2006, l'obiettivo del protocollo è quello di consentire agli utenti domestici che sanno poco della sicurezza wireless e possono essere intimiditi dalle opzioni di sicurezza disponibili per configurare l'accesso protetto Wi-Fi, oltre a rendere è facile aggiungere nuovi dispositivi a una rete esistente senza immettere passphrase lunghi

Cracking_of_wireless_networks

Attacchi che vedremo...

+- WPS: The Offline Pixie-Dust attack

+- WPS: The Online Brute-Force PIN attack

+- WPA: The WPA Handshake Capture + offline crack.

+- WPA: The PMKID Hash Capture + offline crack.

+- WEP: Various known attacks against WEP, including fragmentation, chop-chop, aireplay, etc.

WPS: The Offline Pixie-Dust

Nell'estate del 2014, Dominique Bongard ha scoperto quello che ha definito l'attacco Pixie Dust. Questo attacco funziona solo per l'implementazione WPS predefinita di diversi produttori di chip wireless, tra cui Ralink, MediaTek, Realtek e Broadcom. L'attacco si concentra su una mancanza di randomizzazione quando si generano i punti "segreti" di E-S1 ed E-S2. Conoscendo questi due punti, il PIN può essere ripristinato entro un paio di minuti.

WPS: The Online Brute-Force PIN attack

Poiché sia il punto di accesso che il client devono dimostrare di conoscere il PIN per assicurarsi che il client non si connetta a un AP non autorizzato, l'utente malintenzionato ha già due hash che contengono ciascuna metà del PIN e tutto quello di cui ha bisogno e di forzare il PIN attuale. Il punto di accesso invia due hash, E-Hash1 ed E-Hash2, al client, dimostrando che conosce anche il PIN. La funzione di hashing è HMAC-SHA-256 e utilizza "authkey" che è la chiave utilizzata per creare l'hash dei dati.

* WPA: The WPA Handshake Capture + offline crack.

Ora il primo passo è concettualmente facile. Quello di cui hai bisogno sei tu, l'attaccante, un client che si connetterà alla rete wireless e il punto di accesso wireless. Quello che succede è quando il client e il punto di accesso comunicano per autenticare il client, hanno un handshake a 4 vie che possiamo catturare. Questa "stretta di mano" ha l'hash della password. Ora non esiste un modo diretto per estrarre la password dall'hash, e quindi l'hashing è un metodo di protezione affidabile. Ma c'è una cosa che possiamo fare. Possiamo prendere tutte le password possibili che possono esistere e convertirle in hash. Quindi abbineremo l'hash creato con quello che c'è nella "stretta di mano". Ora, se gli hash corrispondono, sappiamo quale password di testo in chiaro ha dato origine all'hash, quindi conosciamo la password. Se il processo ti sembra davvero dispendioso in termini di tempo, è perché è così. L'hacking WPA (e l'hash cracking in generale) è piuttosto impegnativo e richiede molto tempo.

* WPA: The PMKID Hash Capture + offline crack.

This attack was discovered accidentally while looking for new ways to attack the new WPA3 security standard. WPA3 will be much harder to attack because of its modern key establishment protocol called "Simultaneous Authentication of Equals" (SAE).

The main difference from existing attacks is that in this attack, capture of a full EAPOL 4-way handshake is not required. The new attack is performed on the RSN IE (Robust Security Network Information Element) of a single EAPOL frame.

At this time, we do not know for which vendors or for how many routers this technique will work, but we think it will work against all 802.11i/p/q/r networks with roaming functions enabled (most modern routers).

The main advantages of this attack are as follow:

 +- No more regular users required - because the attacker directly communicates with the AP (aka "client-less" attack)
 +- No more waiting for a complete 4-way handshake between the regular user and the AP
 +- No more eventual retransmissions of EAPOL frames (which can lead to uncrackable results)
 +- No more eventual invalid passwords sent by the regular user
 +- No more lost EAPOL frames when the regular user or the AP is too far away from the attacker
 +- No more fixing of nonce and replaycounter values required (resulting in slightly higher speeds)
 +- No more special output format (pcap, hccapx, etc.) - final data will appear as regular hex encoded string

* WPA: The PMKID Hash Capture + offline crack.

Attack details:

+- The RSN IE is an optional field that can be found in 802.11 management frames. One of the RSN capabilities is the PMKID.

+- The PMKID is computed by using HMAC-SHA1 where the key is the PMK and the data part is the concatenation of a fixed string label "PMK Name", the access point's MAC address and the station's MAC address. (Pairwise Master Key Identifier)

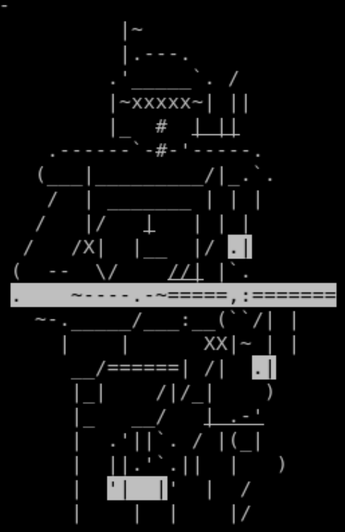
Code:
PMKID = HMAC-SHA1-128(PMK, "PMK Name" | MAC_AP | MAC_STA)

+- Since the PMK is the same as in a regular EAPOL 4-way handshake this is an ideal attacking vector.

+- we receive all the data we need in the first EAPOL frame from the AP.

EXTRA: Evil Twin Attack ->

<-



->

Quando effettuiamo un attacco Evil Twin ci stiamo fingendo un Access point già esistente.

Forzando la disconnessione dei dispositivi dall'Access point vittima essi si collegheranno ad una copia esatta di esso, dove noi abbiamo il pieno controllo, previa cattura dell'hash (come visto in attacchi precedenti)

NOTE

+- Alcuni di questi testi sono tratti da

+- http://www.wikipedia.org

+- https://www.kali.org/

+- https://hashcat.net