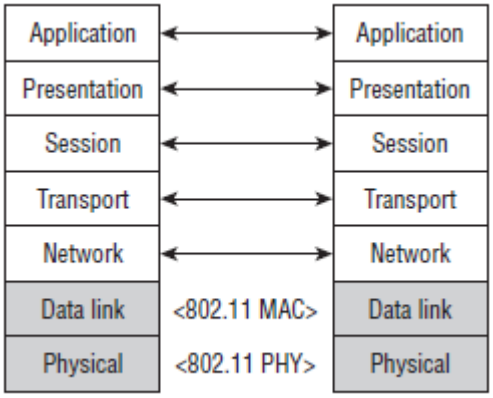
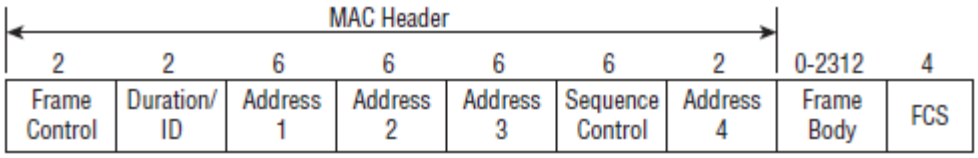
Sieci bezprzewodowe dodają kolejny punkt wejścia do sieci dla hakerów. Wiele już napisano o bezpieczeństwie sieci bezprzewodowej i hakowaniu, ponieważ sieć bezprzewodowa jest stosunkowo nową technologią i zawiera luki w zabezpieczeniach. Od zwiększenia liczby hotspotów Wi-Fi do rosnącej liczby telefonów komórkowych, urządzeń PDA i laptopów wyposażonych w Wi-Fi, bezpieczeństwo bezprzewodowe jest coraz większym problemem dla wielu organizacji. Ze względu na nadawany charakter bezprzewodowych sieci radiowych (RF) oraz zastosowanie szybkich technologii bezprzewodowych w sieciach domowych i firmowych istnieje wiele możliwości włamań do sieci bezprzewodowych. Nawet w przypadku organizacji z zakazem łączności bezprzewodowej - co oznacza, że nie obsługują one żadnej łączności Wi-Fi - nieuczciwe punkty dostępu bezprzewodowego umieszczone w sieci LAN stanowią rosnące zagrożenie. Koszt sprzętu Wi-Fi spada, a wiele organizacji naciska pracowników IT, aby zainstalować sieci bezprzewodowe w celu uzupełnienia lub zastąpienia istniejących sieci przewodowych.

Wi-Fi i Ethernet

Należy pamiętać, że sieci Wi-Fi różnią się zasadniczo od sieci Ethernet. Podczas gdy w sieci Ethernet dane są przenoszone w ramkach na kablach miedzianych lub światłowodowych, w sieci Wi-Fi dane przemieszczają się na otwartym powietrzu. Ponadto każde szyfrowanie stosowane w sieciach bezprzewodowych szyfruje tylko dane, pozostawiając miksturę nagłówka ramki bezprzewodowej otwartą na wiele rodzajów ataków. Szczegóły ataków bezprzewodowych i środków zaradczych zostaną omówione w dalszej części, ale najpierw musisz zrozumieć podstawy standardów i protokołów 802.11. Bezprzewodowe sieci LAN 802.11 działają na poziomie 1 i 2 modelu OSI. Oznacza to, że protokoły używane w sieci WLAN są takie same z warstwy 3 (zwykle IP) na poziomie do warstwy 7 (warstwa aplikacji). Zobacz rysunek 10.1.



Wiele osób nazywa 802.11 sieci WLAN "bezprzewodową siecią Ethernet", co jest dużym błędem. 802.11 ma zupełnie inny format ramki niż Layer 2 niż 802.3 (Ethernet). Na przykład, ramki Ethernet Layer 2 zawierają tylko dwa adresy MAC, podczas gdy ramki 802.11 mają pola dla czterech adresów MAC. Ethernet określa adresy źródłowe i docelowe, a ramka 802.11 może określać źródło, miejsce docelowe, nadajnik i odbiornik. Ramki 802.11 przenoszą również pole kontroli ramki w nagłówku MAC, używane do wskazania informacji o ramce, na przykład, gdy ramka jest zaszyfrowana. Zobacz rysunek 10.2.



Istnieją trzy typy ramek 802.11:

* Zarządzania - używane do powiadamiania, łączenia, rozłączania i informacji.

* Kontroli - służy do kontrolowania, która stacja ma dostęp do bezprzewodowego nośnika sieciowego.

* Dane - używane do przenoszenia danych warstwy wyższej.

Większość bezprzewodowych sieci LAN (WLAN) opiera się na standardach IEEE 802.11 i poprawkach, takich jak 802.11a, 802.11b, 802.11g i 802.11n. Poprawione napisy zostały zrolowane do ostatecznego standardu 802.11 i są teraz określane przez klauzulę lub numer sekcji w standardzie 802.11. Ponieważ jednak poprawki pisane są nadal często używane podczas rozróżniania sekcji standardu 802.11, będą również używane w tym rozdziale. Tabela poniższa przedstawia porównanie standardowych poprawek 802.11.

Stanard IEEE	**Częstotliwość**	**Prędkość**	**Rozpiętość**	**Widmo**
802.11	2,4 GHz	Do 2 Mbps	Zależy od typu widma rozproszonego	DSSS i FHSS
802.11a	5 GHz	Do 54 Mbs	od 25 do 75 stóp w pomieszczeniach; zasięg może zależeć od materiałów budowlanych	OFDM
802.11b	2,4 GHz	Do 11 Mb / s	Do 150 stóp w pomieszczeniach; zakres może zależeć od materiałów budowlanych	DSSS
802.11g	2.4 GHz	Do 54 Mb / s	Do 150 stóp w pomieszczeniach; zakres może zależeć od materiałów budowlanych	DSSS
802.11n	2.4 i 5 GHz	Do 600 Mb / s	Co najmniej tak daleko jak b, g, i-i prawdopodobnie znacznie dalej	OFDM

Początkowy standard 802.11 zawierał jedynie podstawowe funkcje zabezpieczeń i był pełen luk. Poprawka 802.11i to najnowsze rozwiązanie bezpieczeństwa, które usuwa słabości 802.11. Sojusz Wi-Fi utworzył dodatkowe certyfikaty bezpieczeństwa, znane jako Wi-Fi Protected Access (WPA) i WPA2, aby wypełnić lukę między oryginalnym standardem 802.11 a najnowszą poprawką 802.11i. Luki w zabezpieczeniach i rozwiązania bezpieczeństwa omówione w tym rozdziale są oparte na tych normach **IEEE i Wi-Fi Alliance.**

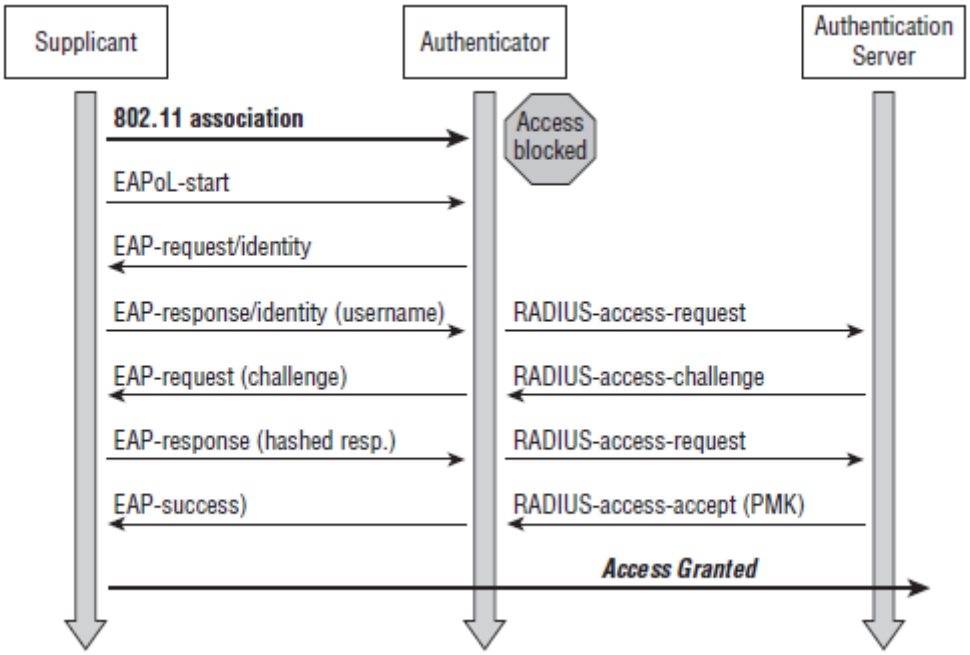
Techniki uwierzytelniania i łamania

W standardzie 802.11 istnieją dwie metody uwierzytelniania klientów bezprzewodowej sieci LAN w punkcie dostępu: uwierzytelnianie za pomocą systemu otwartego lub klucza wspólnego. System otwarty nie zapewnia żadnych mechanizmów bezpieczeństwa, ale jest po prostu żądaniem nawiązania

połączenia z siecią. Uwierzytelnianie za pomocą klucza prywatnego powoduje, że klient sieci bezprzewodowej generuje ciąg tekstowy wyzwania z kluczem WEP (Wired Equivalent Privacy), który uwierzytelnia klienta w sieci. Tabela porównuje typ uwierzytelniania i szyfrowania typu Wi-Fi security.

Wi-Fi Security	Uwierzytelnienie	Szyfr	Szyfrowanie
WPA-Personal	Preshared Key	TKIP	RC4
WPA-Enterprise	802.1X / EAP	TKIP	RC4
WPMP2 Personal	Preshared Key	CCMP(domyślnie)	AES(domyślnie)
		TKIP(opcjonalnie)	RC4(opcjonalnie)
WPA2-Enterprise	802.1X/EAP	CCMP (domyślnie)	AES (domyślnie),
		TKIP (opcjonalnie)	RC4 (opcjonalnie)

WEP była pierwszą opcją bezpieczeństwa dla sieci 802.11 WLAN. Protokół WEP służy do szyfrowania danych w sieci WLAN i opcjonalnie może być powiązany z uwierzytelnianiem za pomocą klucza wspólnego w celu uwierzytelnienia klientów WLAN. WEP używa 64-bitowego lub 128-bitowego klucza szyfrowania RC4 do szyfrowania ładunku danych warstwy 2. Ten klucz WEP zawiera 40-bitowy lub 104-bitowy klucz zdefiniowany przez użytkownika w połączeniu z 24-bitowym wektorem inicjującym (IV), co powoduje, że klucz WEP jest 64-bitowy lub 128-bitowy. Proces, w którym RC4 używa IV, jest prawdziwą słabością WEP: daje hakerowi możliwość złamania klucza WEP. Metoda ta, znana jako atak Fluhrera, Mantina i Shamira (FMS), używa zaszyfrowanych bajtów wyjściowych w celu określenia najbardziej prawdopodobnych bajtów klucza. Możliwość wykorzystania luki WEP została włączona do produktów takich jak AirSnort, WEPCrack i Aircrack. Chociaż haker może próbować złamać WEP za pomocą brutalnej siły, najczęstszą techniką jest atak FMS. WPA stosuje protokół Temporal Key Integrity Protocol (TKIP) - który jest bezpieczniejszą implementacją RC4 - do szyfrowania danych oraz do uwierzytelniania WPA Personal lub WPA Enterprise. WPA Personal używa hasła ASCII do uwierzytelniania, podczas gdy WPA Enterprise używa serwera RADIUS do uwierzytelniania użytkowników. WPA Enterprise jest bezpieczniejszą, solidną opcją bezpieczeństwa, ale opiera się na tworzeniu i bardziej złożonej konfiguracji serwera RADIUS . TKIP obraca klucz szyfrowania danych, aby zapobiec lukom w zabezpieczeniach WEP i, w konsekwencji, atakom cracków. Protokół WPA2 jest podobny do standardu 802.11i i wykorzystuje szyfrowanie AES (Advanced Encryption Standard) do szyfrowania ładunku danych. AES jest uważany za nieskładalny algorytm szyfrowania. WPA2 pozwala również na korzystanie z TKIP w okresie przejściowym zwanym bezpieczeństwem w trybie mieszanym. Ten tryb przejściowy oznacza, że zarówno TKIP, jak i AES mogą być używane do szyfrowania danych. AES wymaga szybszego procesora, co oznacza, że urządzenia low-end, takie jak PDA, mogą obsługiwać tylko TKIP. WPA Personal i WPA2 Personal używają hasła do uwierzytelniania klientów WLAN. WPA Enterprise i WPA2 Enterprise uwierzytelniają użytkowników sieci WLAN za pośrednictwem serwera RADIUS przy użyciu standardów protokołu 802.1X / Extensible Authentication Protocol (EAP). Ilustracja 10.3 pokazuje proces 802.1x / EAP i proces komunikacji używany do uwierzytelniania klienta przy użyciu protokołu 802.1x / EAP.



802.11i i WPA korzystają z tych samych mechanizmów szyfrowania i uwierzytelniania co WPA2. Jednak WPA2 nie wymaga od dostawców implementacji preautoryzacji. Preautoryzacja umożliwia szybki i bezpieczny roaming, który jest niezbędny w bardzo mobilnych środowiskach dzięki czułym aplikacjom, takim jak bezprzewodowy VoIP. Poniższej zawarto podsumowanie opcji uwierzytelniania i szyfrowania dla sieci WLAN oraz związanych z nimi słabości.

Oryginalny standard IEEE 802.11
Szyfrowanie : WEP
Uwierzytelnianie : WEP
Słabość : Słabość IV pozwala złamać klucz WEP. Ten sam klucz jest używany do szyfrowania i uwierzytelnianie wszystkich klientów do sieci WLAN

WPA
Szyfrowanie : TKPI
Uwierzytelnianie : Hasło lub RADIUS (803.1X/EAP)
Słabość : Hasło jest podatne na atak słownikowy

WPA2
Szyfrowanie : AES (może używać TKIP w trybie mieszanym)
Uwierzytelnianie : Hasło lub RADIUS (802.1x / EAP)
Słabość : Hasło jest podatne na atak słownikowy.

IEEE 802.11i
Szyfrowanie : AES (może używać TKIP w trybie mieszanym)
Uwierzytelnianie : Hasło lub RADIUS (802.1x / EAP)
Słabość : Hasło jest podatne na atak słownikowy.

Narzędzia hakerskie

Aircrack to narzędzie do łamania WEP. Nie przechwytuje pakietów; służy do wykonywania pęknięć po przechwyceniu zaszyfrowanych pakietów przez inne narzędzie. Aircrack działa w systemie Windows lub Linux.
WEPCrack i AirSnort to oparte na systemie Linux narzędzia łamania WEP.
NetStumbler i Kismet to narzędzia do wykrywania WLAN. Oboje odkrywają Media
Adres kontroli dostępu (MAC), identyfikator zestawu usług (SSID), tryb bezpieczeństwa i kanał sieci WLAN. Ponadto Kismet może wykrywać sieci WLAN, których identyfikatory SSID są ukryte, zbierać pakiety i zapewniać funkcjonalność IDS.

Bądź ostrożny
W 2003 r. Hakerzy korzystali z sieci bezprzewodowej w domowym sklepie Lowe's dla próby kradzieży numerów kart kredytowych. Trzej hakerzy odkryli podatną na ataki sieć WLAN w sklepie Lowe's w Southfield w stanie Michigan, podczas skanowania w poszukiwaniu otwartych połączeń lub "prowadzenia wojny" w okolicy. Następnie hakerzy wykorzystali otwarty punkt dostępu, aby narazić całą sieć korporacyjną firmy zajmującej się remontami domów w Północnej Karolinie, włamując się do sklepów w Kalifornii, Kansas, Południowej Dakocie i innych stanach w ciągu kilku tygodni. Uzyskali dostęp do programu przetwarzania kredytowego o nazwie tcpcredit, który pobierał informacje o koncie kredytowym dla każdej transakcji przetwarzanej w danym sklepie Lowe. Plan hakerów polegał na pozbyciu się milionów numerów kart kredytowych za pośrednictwem backdoora zainstalowanego w autorskim programie Lowe. Jeden z mężczyzn zaangażowanych w próbę włamania przyznał się do czterech podejrzeń oszustwa i nieautoryzowanego dostępu do komputera po tym, jak on i dwóch wspólników włamali się do sieci Lowe'a. W 2004 r. został skazany i odbył karę dziewięciu lato więzienia, mimo że nie ma dowodów na to, że zebrał wszystkie numery kart kredytowych. Podczas dochodzenia znaleziono tylko sześć numerów kart kredytowych w pliku utworzonym ze zmodyfikowanego programu tcpcredit. Ta historia pokazuje, że nawet nieszkodliwa praca może przyciągnąć niepożądaną uwagę, dlatego należy uważać na sieć WLAN, z którą się łączysz.

Używanie bezprzewodowych snifferów do lokalizowania identyfikatorów SSID
Typowy atak na sieć WLAN obejmuje podsłuchiwanie lub sniffowanie. Jest to łatwy atak do wykonania i zwykle występuje w punktach dostępowych lub z dowolnym domyślnym punktem dostępu do instalacji (AP), ponieważ pakiety są zwykle wysyłane niezaszyfrowane przez sieć WLAN. Hasła do protokołów dostępu do sieci, takich jak FTP, POP3 i SMTP, mogą być przechwytywane w postaci zwykłego tekstu (niezaszyfrowane) przez hakera w niezaszyfrowanej sieci WLAN. Identyfikator zestawu usług (SSID) to nazwa sieci WLAN i może znajdować się w sygnale nawigacyjnym ramki i ramki odpowiedzi na sondę. Jeśli dwie sieci bezprzewodowe są fizycznie blisko, to Identyfikatory SSID służą do identyfikacji i rozróżnienia odpowiednich sieci. Identyfikator SSID jest zwykle wysyłany w klarownej ramce sygnału nawigacyjnego, jak również w innych ramkach, takich jak ramki odpowiedzi sond. Większość punktów dostępu pozwala administratorowi sieci WLAN ukryć identyfikator SSID. Jednak nie jest to solidny mechanizm bezpieczeństwa, ponieważ niektóre narzędzia mogą odczytać identyfikator SSID z innych pakietów, takich jak żądania sond i inne pakiety po stronie klienta. W ćwiczeniu 10.1 omówiono instalację i korzystanie z narzędzia do snifferów WLAN o nazwie Omnipeek.
Ćwiczenie 10.1
Instalowanie i używanie narzędzia Sniffer WLAN
1. Pobierz próbną wersję Omnipeek ze strony www.wildpackets.com. Będziesz musiał mieć adapter sieci bezprzewodowej obsługiwany przez Omnipeek w trybie swobodnym aby Omnipeek mógł poprawnie przechwytywać cały ruch w bezprzewodowej sieci LAN. Sprawdź obsługiwane adaptery bezprzewodowej sieci LAN i sterowniki obsługujące z www.wildpackets.com.

2. Rozpocznij nowe przechwytywanie, klikając przycisk Nowe przechwytywanie na ekranie startowym Omnipeek.
3. Wybierz kartę sieci bezprzewodowej z dostępnych opcji przechwytywania. Uwaga: na karcie Adapter, interfejs API WildPackets musi zawierać opis Tak lub adapter nie będzie działał poprawnie w Omnipeek
4. Kliknij kartę 802.11 i wybierz początkowo, aby skanować wszystkie kanały. Później, kiedy już to zrobisz zidentyfikowaliśmy konkretną sieć WLAN do monitorowania, możesz wybrać tylko przechwytywanie ruchu na tym jednym kanale.
5. Kliknij OK, aby rozpocząć przechwytywanie. Okno przechwytywania pokaże klatki przechwycone. Kliknij dwukrotnie ramkę, aby wyświetlić więcej szczegółów.
6. Kliknij przycisk zatrzymaj przechwytywanie, aby zatrzymać przechwytywanie. Wybierz rozwijany filtr Wyświetl (wygląda jak lejek) z paska narzędzi tuż nad ramkami. Wybierz POP z lista rozwijana filtra. Wyświetlane będą tylko ramki e-mail POP. Możesz użyć filtru wyświetlania, aby pokazać tylko określone typy ramek. Wszystkie klatki POP, SMTP, FTP, TELNET i HTTP zawierają wyraźne dane tekstowe. Hasła i inne informacje można uzyskać z tych ramek.
7. Aby znaleźć Punkty Dostępowe (AP) i Stacje, które są podłączone, kliknij menu WLAN po lewej stronie ekranu. APS BSSID, STA MAC, Channel i SSID mogą znajdować się na ekranie WLAN Omnipeek. Punkty AP nie nadające identyfikatora SSID będą wyświetlać 0x00 dla identyfikatora SSID, dopóki stacja się nie połączy, a Omnipeek może określić identyfikator SSID z ramek sondy. Gdy Omnipeek będzie mógł określić identyfikator SSID, zostanie wyświetlony na ekranie WLAN.

Filtry MAC i fałszowanie adresów MAC

Wczesne rozwiązanie bezpieczeństwa w technologii WLAN wykorzystywało filtry adresów MAC: administrator sieci wprowadził listę poprawnych adresów MAC dla systemów dopuszczonych do skojarzenia z AP. Filtry MAC są kłopotliwe w konfiguracji i nie są skalowalne dla sieci przedsiębiorstwa, ponieważ muszą być skonfigurowane w każdym punkcie dostępowym. Spoofing MAC jest łatwy do wykonania i neguje wysiłek wymagany do wdrożenia filtrów MAC. Haker może zidentyfikować poprawny adres MAC, ponieważ nagłówki MAC nie są nigdy szyfrowane.

<u>Ćwiczenie 10. 2</u>

Fałszowanie adresów MAC

1. Pobierz i zainstaluj TMAC ze strony www.technitium.com.
2. Wybierz kartę bezprzewodową z listy połączeń sieciowych w TMAC. Kliknij Zmień przycisk MAC.
3. Wpisz 00: 11: 22: 33: 44: 55 jako adres MAC; kliknij przycisk Zmień teraz i potwierdź zmiany, które należy wprowadzić w adresie MAC.
4. Otwórz wiersz polecenia i wpisz IPCONFIG / ALL, aby potwierdzić adres MAC karta sieci bezprzewodowej została zmieniona na 00: 11: 22: 33: 44: 55.
5. Aby przywrócić pierwotny adres MAC karty sieciowej, wybierz adapter w TMAC, kliknij przycisk Zmień MAC i kliknij przycisk Oryginalny MAC.
6. Skonfiguruj punkt dostępu, aby umożliwić tylko adres MAC 00: 11: 22: 33: 44: 55, aby połączyć się z siecią WLAN. (Ten krok będzie się różnić w zależności od rodzaju punktu dostępu - zapoznaj się z podręcznikiem użytkownika punktu dostępowego, aby skonfigurować filtrowanie adresów MAC).
7. Przetestuj połączenie klienta bezprzewodowego przy użyciu oryginalnego adresu MAC. Klient nie powinien łączyć się z AP z zastosowanym filtrowaniem MAC. Zmień MAC na 00: 11: 22: 33: 44: 55 używając TMAC i spróbuj połączyć się ponownie z AP. Powinien móc połączyć się z AP, używając adresu Spoofed MAC

Narzędzie hakerskie

SMAC to narzędzie do podszywania się pod MAC, które haker może wykorzystać do sfałszowania prawidłowego adresu użytkownika i uzyskania dostępu do sieci.

Nieuczciwe punkty dostępu

Nieuczciwe punkty dostępu to punkty dostępu WLAN, które nie są autoryzowane do łączenia się z siecią. Nieuczciwe punkty dostępowe otwierają bezprzewodową dziurę w sieci. Haker może stworzyć nieuczciwy punkt dostępu, lub pracownik może nieświadomie utworzyć lukę bezpieczeństwa przez podłączenie punktu dostępu do sieci. Wynikowy fałszywy AP może być używany przez każdego, kto może połączyć się z AP, w tym haker, dając mu dostęp do przewodowej sieci LAN. Dlatego tak ważne jest, aby organizacje skanowały fałszywe punkty dostępu. Nawet organizacje, które mają zasadę "brak łączności bezprzewodowej", muszą przeprowadzić skanowanie bezprzewodowe, aby upewnić się, że żadne nieuczciwe punkty dostępowe nie są podłączone do sieci. Fałszywe AP są prawdopodobnie najbardziej niebezpiecznym zagrożeniem, które istnieje, ponieważ dają potencjalnemu hakerowi bezpośredni dostęp do przewodowej sieci LAN. Klienci łączący się z fałszywymi punktami dostępowymi zwykle otrzymują adres IP bezpośrednio z sieci lub z AP, a następnie ruch jest mostkowany bezpośrednio w przewodowej sieci LAN. Stamtąd haker może wykonywać skanowanie, wyliczanie i hakowanie systemu przeciwko celom w przewodowej sieci LAN. Środki zaradcze do wykrywania i usuwania nieuczciwych punktów dostępu istnieją i powinny być wdrażane przez wszystkie organizacje. Wiele rozwiązań do zarządzania opartych na kontrolerach firmowych WLAN ma możliwość wykrycia nieuczciwych punktów dostępu. Te oparte na regulatorze rozwiązania obejmują możliwość monitorowania powietrza za pomocą punktów dostępowych lub czujników / monitorów lub obu tych elementów. Punkty dostępu z natury muszą pozostać na kanale, gdy klienci są podłączeni w celu obsługi tych klientów, podczas gdy czujniki i monitory są w stanie nieustannie skanować powietrze na wszystkich kanałach w paśmie częstotliwości, aby uchwycić możliwe bezprzewodowe transmisje punktu dostępu. Te bezprzewodowe adresy MAC są porównywane z adresami odebranymi na kablu w celu ustalenia, czy AP jest podłączony do tej samej sieci LAN, co bezprzewodowy system wykrywania wtargnięcia (WIDS) lub bezprzewodowy system zapobiegania włamaniom (WIPS). Niektóre WIPSy mogą również uniemożliwić klientom łączenie się z fałszywymi punktami dostępu przez wysyłanie sfałszowanych ram deauthentication do dowolnego klienta próbującego połączyć się z fałszywym AP- w ten sposób uniemożliwiając klientom przesyłanie danych przez nieuczciwe AP. Nakładane systemy WIDS / WIPS mogą być również pomocne w wykrywaniu nieuczciwych punktów dostępu przez triangulację pozycji nieuczciwego AP. Enterprise WLAN WIPS i nakładka WIPS to tylko tymczasowe opcje wykrywania i ograniczania. Podstawowym celem powinno być zlokalizowanie fałszywego AP i usunięcie go z sieci.

Evil Twin lub AP Masquerading

Hakerzy mogą używać AP opartego na oprogramowaniu do tworzenia AP, który wygląda jak prawdziwy Punkt Dostępowy. Jest to tzw. atak evil twin lub maskowanie AP.

Techniki atakowania sieci bezprzewodowej

Większość bezprzewodowych ataków hakerskich można podzielić na następujące kategorie:

Łamanie szyfrowania i mechanizmów uwierzytelniania: Mechanizmy te obejmują łamanie WEP, hasła uwierzytelniania klucza wstępnego WPA oraz uwierzytelnianie CAPA Lightweight EAP (LEAP). Hakerzy mogą wykorzystywać te mechanizmy do łączenia się z siecią WLAN za pomocą skradzionych danych uwierzytelniających lub mogą przechwytywać dane innych użytkowników i odszyfrowywać je lub szyfrować. Ochroną przed tym atakiem jest wdrożenie silniejszego szyfrowania, takiego jak AES.

Podsłuch lub sniffing Ten rodzaj ataku obejmuje przechwytywanie haseł lub innych poufnych informacji z niezaszyfrowanej sieci WLAN lub hotspotu. Ochrona przed tym atakiem polega na użyciu szyfrowania warstwy aplikacji SSL lub sieci VPN w celu zabezpieczenia danych użytkownika.

Denial of Service : DoS można wykonać w warstwie fizycznej, tworząc głośniejszą sygnaturę RF niż AP z nadajnikiem RF, powodując niepowodzenie zatwierdzonego AP, aby użytkownicy mogli połączyć się z fałszywym AP. DoS można wykonać w warstwie Logical Link Control (LLC), generując ramki deauthentication (deauth attacks), ciągle generując fałszywe ramki lub mając bezprzewodowy NIC wysyłający stały strumień surowego RF (atak Queensland). Przeciwdziałaniem jest egzekwowanie obwodu bezpieczeństwa wokół sieci WLAN oraz wykrywanie i usuwanie źródeł ataków DoS za pomocą IDS.

Maskarada AP lub Spoofing Fałszywe AP udają legalne punkty dostępowe za pomocą tych samych ustawień SSID konfiguracji lub nazwy sieci. Przeciwwskazaniem do maskowania AP jest użycie WIDS do wykrycia i zlokalizowania sfałszowanych AP.

MAC Spoofing Hacker udaje legalnego klienta WLAN i pomija filtry MAC przez podszywanie się pod adres MAC innego użytkownika. WIDS mogą wykrywać podszywanie się pod MAC, a nie używanie filtrowania MAC jest sposobem na uniknięcie ataków polegających na podszywaniu się pod MAC.

Sadzenie nieuczciwych punktów dostępu Najbardziej niebezpieczny atak to nieuczciwy punkt dostępowy, który został obsadzony, aby umożliwić hakerom dostęp do docelowej sieci LAN. Przeciwdziałaniem jest użycie WIPS do wykrywania i lokalizowania nieuczciwych punktów AP.

Sieci bezprzewodowe dają hakerom łatwy dostęp do sieci, jeśli punkt dostępowy nie jest zabezpieczony prawidłowo. Istnieje wiele sposobów na zhackowanie lub wykorzystanie luk w sieci WLAN. Istnieją również skuteczne środki zaradcze dla wielu z tych ataków. W następnej sekcji szczegółowo opisano najlepsze metody zabezpieczenia sieci bezprzewodowej.

Zabezpieczanie sieci bezprzewodowych

Ponieważ sieci bezprzewodowe to stosunkowo nowa technologia w porównaniu do technologii sieci przewodowych, dostępnych jest mniej opcji zabezpieczeń. Metody zabezpieczeń można kategoryzować według odpowiedniej warstwy modelu OSI.

Warstwa 2 lub warstwa MAC opcje zabezpieczeń są następujące:

* Statyczne WEP (nie zalecane)
* WPA
* WPA2 / 802.11i

Warstwa 3 lub warstwa sieciowa ,opcje zabezpieczeń są następujące:

* IPSec
* SSL VPN

Warstwa 7 lub warstwa aplikacji, opcje zabezpieczeń są następujące:

* Aplikacje bezpieczeństwa, takie jak Secure Shell (SSH), HTTP przez SSL (HTTPS) i FTP / SSL (FTPS)

Ze względu na liczne słabości WEP nie powinno być jedynym mechanizmem bezpieczeństwa dla sieci WLAN.

Zabezpieczanie domowych sieci bezprzewodowych

Wiele osób konfigurujących bezprzewodowe sieci domowe przyspiesza pracę, aby ich łączność internetowa działała tak szybko, jak to możliwe. Produkty dla małych biur, biura domowego (SOHO) dostępne na rynku sprawiają, że konfiguracja jest szybka i łatwa, ale niekoniecznie bezpieczna.

Konfiguracja dodatkowych funkcji bezpieczeństwa może być czasochłonna i nieintuicyjna dla niektórych użytkowników domowych, dlatego nie mogą w ogóle implementować żadnego mechanizmu bezpieczeństwa. Obecnie produkty sieci bezprzewodowych są tak wszechobecne i niedrogie, że prawie każdy może skonfigurować WLAN w ciągu kilku minut przy użyciu sprzętu o wartości poniżej 100 USD. Takie powszechne korzystanie z sieci bezprzewodowych oznacza, że może istnieć dziesiątki potencjalnych intruzów sieciowych w zasięgu domowej lub biurowej sieci WLAN. Większość sprzętu WLAN jest dość łatwa do skonfigurowania, aby wielu użytkowników po prostu podłączało się i zaczęło korzystać z sieci bez zastanowienia się nad bezpieczeństwem. Niemniej jednak, poświęcenie kilku dodatkowych minut na skonfigurowanie funkcji bezpieczeństwa routera bezprzewodowego lub punktu dostępu to czas dobrze spędzony. Poniższe zalecenia poprawią bezpieczeństwo domowej sieci bezprzewodowej:

Zmień domyślne hasła administratora i nazwy użytkownika. Podczas konfigurowania domowego punktu dostępowego zwykle uzyskuje się dostęp do interfejsu konfiguracyjnego za pomocą przeglądarki internetowej. Prawie wszystkie routery i punkty dostępu mają hasło administratora potrzebne do zalogowania się do urządzenia i modyfikacji dowolnych ustawień konfiguracyjnych. Aby skonfigurować te urządzenia, producenci dostarczają domyślną nazwę użytkownika i hasło. Wiele domyślnych loginów jest prostych (takich jak username = admin i password = admin) i bardzo dobrze znanych hakerom w Internecie. Większość urządzeń używa słabych domyślnych haseł, takich jak "hasło" lub nazwa producenta, a niektóre w ogóle nie mają domyślnego hasła. Powinieneś zmienić domyślne hasło na swoim domowym AP tak szybko jak to możliwe.

Użyj szyfrowania WEP / WPA. Większość urządzeń Wi-Fi obsługuje pewną formę szyfrowania. Technologia szyfrowania miesza wiadomości wysyłane przez sieci bezprzewodowe, aby hakerzy nie mogli ich łatwo odczytać. Powinieneś skonfigurować najsilniejszą formę szyfrowania, która działa z klientami bezprzewodowymi. Szyfrowanie WEP (Wired Equivalency Privacy) w standardzie 802.11 ma znane słabości, które powodują, że zdeterminowany użytkownik posiadający odpowiedni sprzęt może stosunkowo łatwo złamać szyfrowanie i uzyskać dostęp do sieci bezprzewodowej. Lepszym sposobem ochrony sieci WLAN jest WPA (Wi-Fi Protected Access). WPA zapewnia znacznie lepszą ochronę i jest również łatwiejszy w użyciu, ponieważ twoje znaki hasła nie są ograniczone do 0-9 i A-F, ponieważ są z WEP. (Uwaga: WEP może również używać kluczy ASCII.)

Zmień domyślny identyfikator SSID. Punkty dostępu używają nazwy sieci o nazwie SSID, aby reklamować sieć użytkownikom bezprzewodowym. Producenci zwykle wysyłają swoje produkty z tym samym zestawem SSID. Na przykład identyfikator SSID dla urządzeń Linksys jest zwykle "Linksys". Samo rozpoznanie SSID nie pozwala na to, aby twoi sąsiedzi włamali się do twojej sieci, ale to jest początek. Co ważniejsze, gdy ktoś znajdzie domyślny identyfikator SSID, zwykle wskazuje to na źle skonfigurowaną sieć. Należy zmienić domyślny identyfikator SSID natychmiast po skonfigurowaniu zabezpieczeń sieci bezprzewodowej.

Nie łącz się automatycznie z otwartymi sieciami Wi-Fi. Łączenie się z otwartą siecią Wi-Fi, taką jak bezpłatny hotspot bezprzewodowy lub nieznana sieć WLAN, naraża komputer na zagrożenia bezpieczeństwa. Większość komputerów ma dostępne ustawienie, umożliwiające automatyczne nawiązywanie połączeń bez powiadamiania użytkownika. Większość wersji systemu Windows połączy się ponownie z wcześniej podłączonym identyfikatorem SSID. To ustawienie nie powinno być włączone, z wyjątkiem sytuacji tymczasowych.

Włącz ustawienia zapory na swoim laptopie i punkcie dostępu do domu. Większość routerów sieciowych ma wbudowaną funkcję zapory ogniowej, ale istnieje również opcja ich wyłączenia. Upewnij się, że firewall routera jest włączony. Zawsze należy zainstalować i skonfigurować osobiste oprogramowanie zapory sieciowej na każdym komputerze podłączonym do routera.

Zmniejsz moc nadajnika WLAN. Ta funkcja nie jest dostępna we wszystkich routerach bezprzewodowych i punktach dostępowych, ale niektóre z nich pozwalają obniżyć moc nadajnika

WLAN, a tym samym zmniejszyć zasięg sygnału. (Zwykle ta funkcja jest dostępna tylko w przypadku punktów dostępu klasy enterpriseclass). Chociaż zwykle nie jest możliwe precyzyjne dostrojenie sygnału, który nie wycieknie poza domem lub firmą, przy pewnej próbie i błędzie często można ograniczyć odległość poza zasięgiem pomieszczenia, do których dociera sygnał, minimalizując możliwość kontaktu z siecią WLAN przez osoby postronne. Poprawi to także przepustowość twojego punktu dostępowego, ograniczając komórkę bezprzewodową tylko do twojej przesłanki.

Wyłącz zdalną administrację. Większość routerów WLAN może być zdalnie

administrowane przez Internet. W idealnej sytuacji należy używać tej funkcji tylko wtedy, gdy pozwala zdefiniować określony adres IP lub ograniczony zakres adresów, które będą mogły uzyskać dostęp do routera. W przeciwnym razie prawie każdy użytkownik może znaleźć i uzyskać dostęp do routera. Z reguły, chyba że absolutnie potrzebujesz tej możliwości, najlepiej jest wyłączyć zdalną administrację.

Podsumowanie

Rozwój sieci bezprzewodowych napędzany jest wygodą i coraz większą liczbą pracowników mobilnych. Więcej pracowników pracuje w domu lub w podróży, a organizacje budują większe sieci WLAN, aby zapewnić większą mobilność siły roboczej. W przeszłości wiele organizacji unikało sieci WLAN z powodu nieodłącznego braku bezpieczeństwa i niedojrzałych technologii. Ratyfikacja 802.11n zapewnia większe prędkości w bezprzewodowych sieciach LAN, dzięki czemu są one porównywalne z istniejącymi sieciami Ethernet. Ta zwiększona prędkość zwiększy tylko liczbę organizacji korzystających z sieci bezprzewodowych dla aplikacji biznesowych, a w konsekwencji zwiększy zagrożenia bezpieczeństwa.
Niedawno mechanizmy bezpieczeństwa WLAN dojrzewają do tego stopnia, że firmy i urzędy państwowe zaczynają stosować technologię WLAN. Dzięki odpowiednim mechanizmom bezpieczeństwa i implementacji sieci WLAN można zabezpieczyć na wysokim poziomie. Starannie przestrzegając zaleceń bezpieczeństwa i środków zaradczych, możesz zabezpieczyć sieć WLAN przed atakiem.

Do Zapamiętania!

* Zapoznałeś się z nieodłącznymi słabościami bezpieczeństwa korzystania z sieci WLAN. RF jest medium transmisyjnym, takim jak środowisko centralne, dlatego cały ruch może zostać przechwycony przez hakera.
* Zapoznałeś się z rozwiązaniami bezpieczeństwa zaimplementowanymi w standardzie IEEE 802.11. WEP, klucz udostępniony i filtry MAC to rozwiązania bezpieczeństwa oferowane w oryginalnym standardzie IEEE 802.11.
* Poznałeś rozwiązania bezpieczeństwa oferowane przez Wi-Fi Alliance. WPA i WPA2 są certyfikatami bezpieczeństwa urządzeń Wi-Fi Alliance.
* Dowiedziałeś się, do czego służy SSID w sieci WLAN. Identyfikator SSID identyfikuje nazwę sieci i nie powinien być używany jako mechanizm bezpieczeństwa.
* Wiesz, jakie mechanizmy bezpieczeństwa nie powinny być wykorzystywane do ochrony sieci WLAN. Filtry WEP i MAC nie powinny być używane jako jedyny sposób zabezpieczenia sieci WLAN.