HACKOWANIE SIECI BEZPRZEWODOWYCH

Termin „bezprzewodowy” ogólnie opisuje sprzęt i technologie działające w spektrum częstotliwości radiowych (RF) pomiędzy 3 Hz i 300 GHz. Przykłady sprzętu bezprzewodowego obejmują telefony komórkowe, smartfony, radia AM/FM, urządzenia sieciowe bezprzewodowe i systemy radarowe. Większość sprzętu sieciowego bezprzewodowego działa w mniejszej części spektrum RF, pomiędzy 2,4 GHz i 66 GHz. Technologia bezprzewodowa, szczególnie w Internecie rzeczy (IoT), nadal zyskuje na popularności, co sprawiło, że zabezpieczenie sieci bezprzewodowych przed atakującymi stało się głównym problemem. Ten moduł daje przegląd technologii i standardów sieci bezprzewodowych, wyjaśnia proces uwierzytelniania, opisuje wardriving i obejmuje niektóre narzędzia, których atakujący używają w sieciach bezprzewodowych.

ZROZUMIENIE TECHNOLOGII BEZPRZEWODOWEJ

Aby sieć bezprzewodowa działała, musisz mieć odpowiedni sprzęt i oprogramowanie oraz używać technologii, która wysyła i odbiera fale radiowe. Kiedyś, gdy ludzie widzieli postać komiksową Dicka Tracy'ego rozmawiającego ze swoim zegarkiem nareczynym, zastanawiali się, czy to kiedykolwiek będzie możliwe. Pomysł, że telefon może działać bez podłączonego do niego przewodu, wydawał się zdumiewający, mimo że Alfred J. Gross wynalazł krótkofalówkę w 1938 roku. W rzeczywistości twórca Dicka Tracy'ego poprosił Grossa o pozwolenie przed użyciem bezprzewodowego zegarka naręcznego w swoich komiksach. (Aby dowiedzieć się więcej o Alu Grossie, odwiedź stronę www.retrocom.com.) W 1973 roku, 35 lat po wynalezieniu krótkofalówki, Martin Cooper wynalazł pierwszy telefon komórkowy, który ważył blisko 2 funty. Technologia bezprzewodowa jest częścią Twojego codziennego życia. Oto kilka urządzeń bezprzewodowych, z których wiele osób korzysta codziennie:

• Monitory dziecięce

• Systemy bezkluczykowe

• Telefony komórkowe

• Smartfony

• Urządzenia GPS (Global Positioning System)

• Piloty zdalnego sterowania

• Otwieracze drzwi garażowych

• Radia dwukierunkowe

• Urządzenia zgodne z technologią Bluetooth, takie jak inteligentne zegarki, głośniki i słuchawki

• Telewizory Smart TV

• Inteligentne samochody

Składniki sieci bezprzewodowej

Każda sieć potrzebuje pewnych składników do działania: urządzeń komunikacyjnych do przesyłania i odbierania sygnałów, protokołów i medium do przesyłania danych. W typowej sieci LAN składnikami tymi są karty interfejsu sieciowego (NIC), TCP/IP i kabel Ethernet (przewód służący jako medium połączenia). Choć sieci bezprzewodowe mogą wydawać się skomplikowane, one również mają tylko kilka podstawowych składników:

• Karty interfejsu sieci bezprzewodowej (WNIC), które przesyłają i odbierają sygnały bezprzewodowe, oraz punkty dostępu (AP), które są mostami między sieciami przewodowymi i bezprzewodowymi

• Protokoły sieci bezprzewodowych, takie jak Wi-Fi Protected Access (WPA)

• Część widma RF, która zastępuje przewód jako medium połączenia Poniższe sekcje wyjaśniają, jak AP i WNIC działają w sieci bezprzewodowej.

Punkty dostępu

Punkt dostępu (AP) to radiowy transceiver, który łączy się z siecią za pomocą kabla Ethernet i łączy bezprzewodową sieć LAN (WLAN) z siecią przewodową. Niektóre sieci bezprzewodowe nie łączą się z siecią przewodową, taką jak sieci peer-to-peer, ale ta topologia nie jest objęta, ponieważ testerzy bezpieczeństwa rzadko są zatrudniani do zabezpieczania sieci bezprzewodowej peer-to-peer. Większość firm przeprowadzających testy bezpieczeństwa korzysta z sieci WLAN, która łączy się z topologią sieci przewodowej firmy. Kanały RF są konfigurowane w punkcie dostępowym. Hakerzy szukają punktów dostępowych, jeżdżąc z anteną i laptopem skanującym w poszukiwaniu dostępu. Kanały są wyjaśnione bardziej szczegółowo później w „Standard 802.11". Na razie pomyśl o kanale jako o zakresie lub częstotliwości, przez którą przesyłane są dane, tak jak o kanale w radiu. AP umożliwia użytkownikom łączenie się z siecią LAN za pomocą technologii bezprzewodowej. AP można skonfigurować tak, aby transmitował i odbierał tylko w określonym obszarze lub metrażu, w zależności od technologii. Jeśli znajdujesz się 20 mil od AP, prawdopodobnie jesteś poza zasięgiem.

Identyfikatory zestawu usług

Identyfikator zestawu usług (SSID) to nazwa używana do identyfikacji sieci WLAN, podobnie jak identyfikator VLAN jest używany do identyfikacji sieci VLAN. SSID jest skonfigurowany w AP jako unikalna, alfanumeryczna nazwa o długości od 1 do 32 znaków, rozróżniająca wielkość liter. Aby uzyskać dostęp do sieci WLAN, z którą łączy się AP, komputery z włączoną łącznością bezprzewodową muszą być skonfigurowane z tym samym SSID co AP. Nazwa SSID lub „kod" jest dołączana do każdego pakietu, aby zidentyfikować go jako należący do tej sieci bezprzewodowej. AP zwykle nadaje (rozgłasza) SSID kilka razy na sekundę, aby użytkownicy posiadający karty WNIC mogli zobaczyć wyświetlacz wszystkich sieci WLAN w zasięgu sygnału AP. SSID jest nadawany w postaci zwykłego tekstu (niezaszyfrowany tekst), co może stanowić problem bezpieczeństwa. Każdy, kto wykryje SSID punktu dostępowego, może spróbować się z nim połączyć, w tym hakerzy. Aby lepiej zabezpieczyć punkt dostępowy, możesz wyłączyć nadawanie SSID, tak aby mogły się z nim połączyć tylko osoby, które znają (lub odgadną) SSID. Niektóre karty sieciowe WNIC są wyposażone we wbudowane oprogramowanie do połączeń bezprzewodowych, które wygląda inaczej niż narzędzie systemu Windows. Wielu dostawców ma ustawione SSID na wartość domyślną. Na przykład punkty dostępowe Cisco wcześniej używały domyślnego SSID „tsunami". Typowe domyślne SSID to pojedyncze słowa, takie jak Wireless, Netgear, Linksys, Admin i Default, chociaż domyślne SSID mogą się często zmieniać. Jako specjalista ds. bezpieczeństwa musisz stale badać i zbierać informacje, aby być na bieżąco ze zmianami w tej branży. Jeśli punkt dostępowy jest skonfigurowany tak, aby po uwierzytelnieniu podawać swój SSID, hakerzy sieci bezprzewodowej mogą próbować odgadnąć SSID, używając dobrze znanego domyślnego SSID. Upewnij się, że Twój klient nie używa domyślnego SSID. Czasami domyślny SSID może powiedzieć atakującemu, że docelowy AP jest stary lub nieaktualny. Jeśli bezprzewodowy AP używa domyślnego SSID, może również używać innych domyślnych ustawień, takich jak domyślna nazwa użytkownika i hasło do logowania administracyjnego. Jeśli hakerzy chcący uzyskać dostęp do AP znajdą domyślny SSID, najpierw wypróbują domyślne dane logowania administracyjnego.

Znajdowanie luk w zabezpieczeniach za pomocą domyślnych identyfikatorów SSID

Czas trwania: 30 minut

Cel: Dowiedz się, w jaki sposób rozpoznanie domyślnego identyfikatora SSID może otworzyć drzwi do odkrywania luk w zabezpieczeniach.

Opis: Jak dowiedziałeś się wcześniej, rozpoznanie, z którego systemu operacyjnego korzysta klient, jest niezbędne, aby móc wykryć luki w zabezpieczeniach systemu lub sieci. Dotyczy to również prób wykrywania luk w zabezpieczeniach punktu dostępowego. Podczas przeprowadzania testu bezpieczeństwa w sieci WLAN zaczynasz od wyszukania identyfikatorów SSID reklamowanych bezprzewodowo, aby określić typ punktu dostępowego używanego przez firmę.

1. W razie potrzeby uruchom komputer w systemie Windows lub uruchom system Kali Linux i uruchom przeglądarkę internetową. Przejdź do witryny https://nvd.nist.gov.

2. W lewym panelu kliknij opcję Szukaj, aby przejść do strony wyszukiwania.

3. Na stronie wyszukiwania kliknij przycisk Luki w zabezpieczeniach – CVE, aby przejść do strony bazy danych luk w zabezpieczeniach.

4. Wpisz dlink wireless w polu tekstowym Wyszukiwanie słów kluczowych, a następnie kliknij przycisk Szukaj. Przejrzyj niektóre ostatnie luki w zabezpieczeniach z wynikiem 9 lub wyższym według Common Vulnerability Scoring System (CVSS).

5. Kliknij łącze CVE i przeczytaj podsumowanie informacji o lukach w zabezpieczeniach, aby dowiedzieć się więcej o każdej krytycznej luce w zabezpieczeniach. Czy dostępna jest demonstracja wykorzystania luki lub ataku?

6. Czy router używa typowego domyślnego identyfikatora SSID? Ponieważ modele routerów (i adresy URL) zmieniają się nieustannie, wykorzystaj swoje umiejętności wyszukiwania, aby znaleźć domyślny identyfikator SSID dla wybranej marki i modelu routera.

7. Jakie rozwiązanie zaproponowałbyś klientowi korzystającemu z routera wybranego w kroku 3?

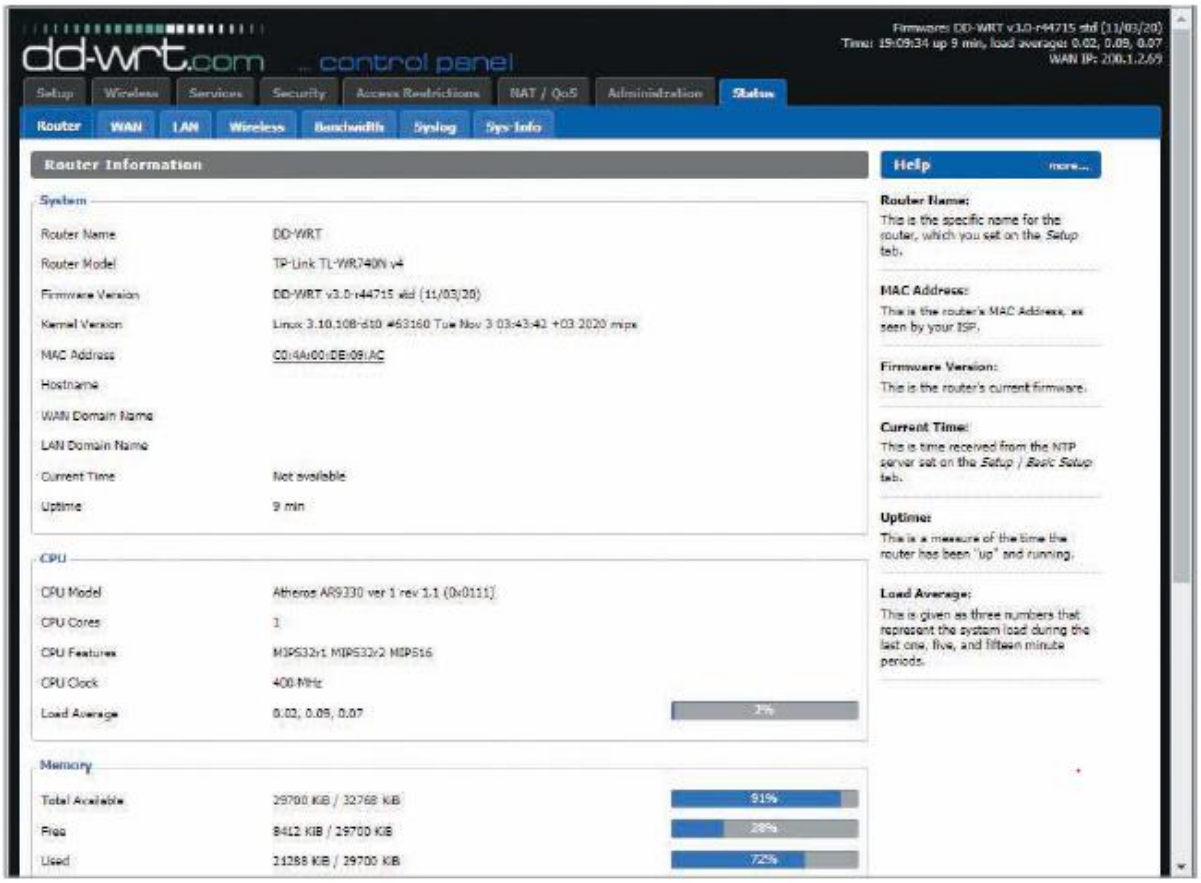
8. Pozostaw przeglądarkę internetową otwartą na czas następnej czynności.

Konfigurowanie punktu dostępowego

Konfigurowanie punktu dostępowego różni się w zależności od wbudowanego systemu operacyjnego dostarczonego przez producenta. W przypadku większości punktów dostępowych użytkownicy mogą uzyskać dostęp do oprogramowania za pośrednictwem przeglądarki internetowej, ponieważ punkt dostępowy ma wbudowany system operacyjny obsługujący serwer internetowy. Poniższy przykład przedstawia opcje dla dd-wrt, wbudowanego systemu operacyjnego Linux, który zastępuje wbudowany system operacyjny używany w setkach routerów firm Linksys, D-Link, Netgear, Belkin, Microsoft, U.S. Robotics, Dell, Buffalo i wielu innych. Zobaczysz, jak administrator punktu dostępowego może określić SSID i kanał oraz skonfigurować zabezpieczenia. Poniższy przykład przedstawia kroki, jakie podejmuje specjalista ds. bezpieczeństwa, aby uzyskać dostęp i ponownie skonfigurować router bezprzewodowy z systemem dd-wrt o adresie IP 192.168.1.1. Przeczytaj, ale nie wykonuj następujących kroków.

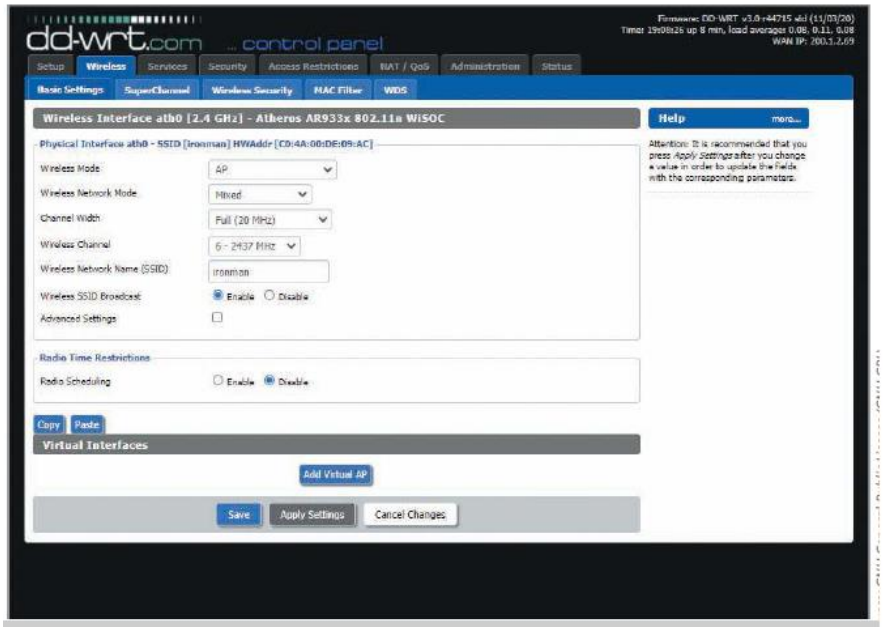
1. Po wpisaniu adresu IP w przeglądarce internetowej użytkownik jest proszony o podanie nazwy logowania i hasła. W dd-wrt domyślna nazwa użytkownika to „root”, a domyślne hasło to „admin”. Ze względów bezpieczeństwa zmiana tych danych uwierzytelniających jest niezbędna.

2. Po pomyślnym zalogowaniu kliknij kartę Status u góry, aby wyświetlić okno pokazane na rysunku.



Zwróć uwagę na model routera i model procesora wymienione w sekcji Informacje o routerze.

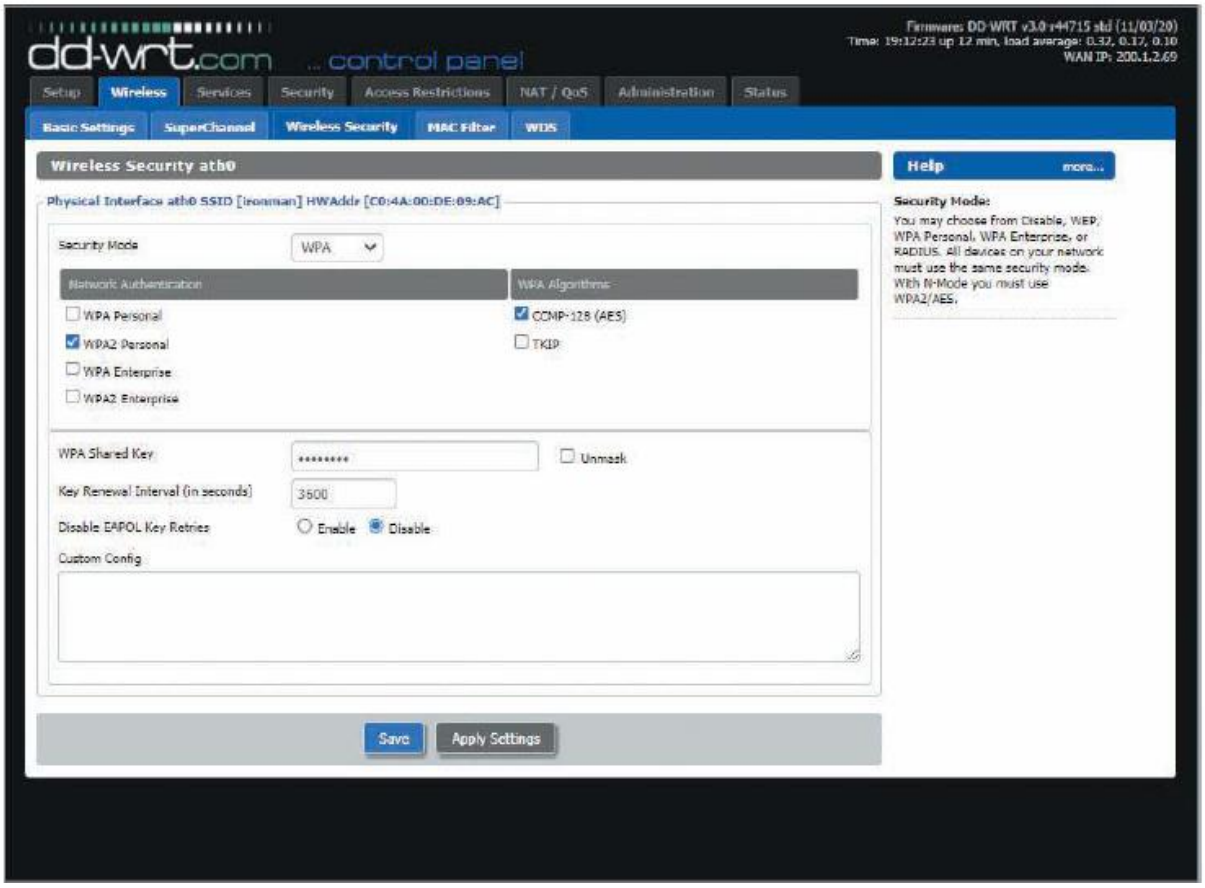
3. Kliknij kartę Wireless, aby wyświetlić okno pokazane na rysunku.



Użytkownik wprowadził „ironman” jako SSID. (Uwaga: domyślny SSID dla routerów bezprzewodowych z systemem dd-wrt to „dd-wrt”). Użytkownik mógł zmienić domyślną nazwę na „Cisco”, aby spróbować

oszukać atakujących i sprawić, by uwierzyli, że router jest produktem Cisco; jednak wybranie nazwy, która nie jest powiązana z producentem ani systemem operacyjnym, może być skuteczniejsze w zniechęcaniu do ataków. Zwróć uwagę, że wybrano kanał 6, domyślny kanał dla wielu systemów operacyjnych routerów bezprzewodowych. Aby poprawić bezpieczeństwo, możesz chcieć wyłączyć rozgłaszanie SSID, ponieważ reklamowanie swojej tożsamości i tego, czy używasz szyfrowania, zwiększa ryzyko ataku. W systemie dd-wrt wyłączasz rozgłaszanie SSID, klikając przycisk opcji Wyłącz.

4. Aby skonfigurować zabezpieczenia, kliknij kartę Wireless Security (Zabezpieczenia sieci bezprzewodowej). Na rysunku użytkownik wprowadził hasło (nazywane „kluczem współdzielonym WPA" w dd-wrt), które musi zostać dostarczone przez komputer bezprzewodowy.



UWAGA

Producenci kart WNIC zwykle dostarczają oprogramowanie do zarządzania połączeniami, którego można używać zamiast wbudowanego narzędzia systemu Windows.

Jeśli firma nie zmieni domyślnego SSID, ale zdecyduje się wyłączyć rozgłaszanie SSID, zdeterminowany intruz może użyć pasywnego sniffera bezprzewodowego, takiego jak Kismet. Kismet może wykrywać SSID w ruchu klienta WLAN. Jeśli użytkownik nie przypisał klucza WLAN ani nie zmienił domyślnego hasła administratora do punktu dostępowego, możesz zobaczyć, jak łatwo atakujący mógłby uzyskać dostęp do WLAN. Jako tester bezpieczeństwa musisz sprawdzić, czy sieć WLAN jest wolna od tych luk. Jeśli sieć WLAN je ma, powinieneś zalecić firmie jak najszybsze zamknięcie luk.

Karty sieciowe bezprzewodowe

Aby przesyłać informacje przez dowolne medium, urządzenie komputerowe musi przestrzegać reguł dla medium, przez które przechodzi, dlatego należy zainstalować odpowiednie oprogramowanie i sterowniki dla karty sieciowej. Na przykład dane przesyłane przez przewód miedziany muszą przestrzegać reguł dotyczących sposobu przesyłania sygnałów Ethernet przez to medium. Aby technologia bezprzewodowa działała, każdy węzeł lub komputer musi mieć kartę sieciową WNIC, która zamienia odbierane fale radiowe na sygnały cyfrowe zrozumiałe dla komputera. Na rynku dostępnych jest wiele kart WNIC, ale ostrożnie podejmij decyzję, którą kupić, jeśli rozważasz użycie konkretnych narzędzi do wykrywania punktów dostępowych i odszyfrowywania kluczy WEP lub użycie anten, które mogą pokryć duży dystans. Na przykład AirCrack-ng, program do łamania szyfrowania WEP w sieci WLAN, wymaga użycia konkretnego chipsetu w karcie WNIC, więc można używać tylko niektórych marek kart WNIC.

ZROZUMIENIE STANDARDÓW SIECI BEZPRZEWODOWYCH

Standard to zbiór reguł sformułowanych przez organizację. Wszystkie branże mają standardy, a sieć WLAN nie jest wyjątkiem. Podobnie jak Instytut Inżynierów Elektryków i Elektroników (IEEE) ma standardy określające maksymalną długość kabla w sieci Ethernet, ustala zasady, których należy przestrzegać w przypadku sieci bezprzewodowych. Grupy robocze (WG) IEEE są tworzone w celu opracowywania nowych standardów. Po osiągnięciu przez WG konsensusu w sprawie propozycji standardu, Sponsor Executive Committee musi zatwierdzić propozycję. Na koniec, po zaleceniu propozycji przez Standards Review Committee i zatwierdzeniu jej przez IEEE Standards Board, masz nowy standard. Projekt IEEE 802 został opracowany w celu tworzenia standardów LAN i WAN. (Pierwsze spotkanie odbyło się w lutym 1980 r., więc projektowi nadano numer 802, przy czym „80” oznaczało rok, a „2” miesiąc.) Nazwy WG otrzymują również numery, takie jak 11 dla grupy Wireless LAN, oraz litery oznaczające zatwierdzone projekty, takie jak 802.11a lub 802.11b. W tym module poznasz standardy 802 dotyczące sieci bezprzewodowych.

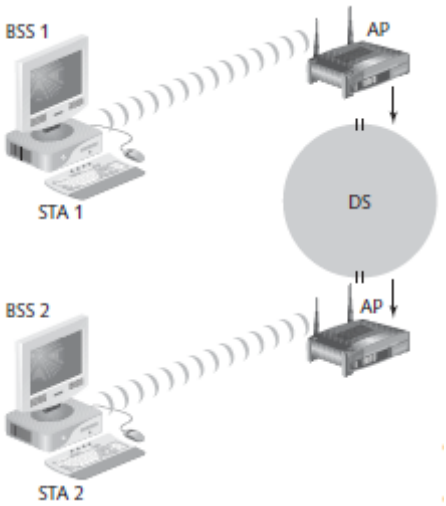
Standard 802.11

Pierwszy standard technologii bezprzewodowej, 802.11, zdefiniował specyfikacje łączności bezprzewodowej jako 1 Mb/s i 2 Mb/s w sieci LAN. Ten standard dotyczył warstwy fizycznej modelu OSI, która zajmuje się problemami łączności bezprzewodowej stacji stacjonarnych, przenośnych i ruchomych w obszarze lokalnym, oraz podwarstwy Media Access Control (MAC) warstwy łącza danych. Często w pobliżu znajduje się wiele nadajników, więc sygnały radiowe mogą się mieszać i potencjalnie zakłócać się nawzajem (jako kolizja sygnału). Z tego powodu zamiast metody CSMA/CD (wykrywanie kolizji, stosowanej w sieci Ethernet) stosuje się wielodostęp/unikanie kolizji z wykrywaniem nośnika (CSMA/CA). Wiele definicji terminów zawarto na ponad 500 stronach standardu 802.11. Jedną z ważnych różnic jest to, że bezprzewodowe sieci LAN nie mają adresu powiązanego z lokalizacją fizyczną, jak ma to miejsce w przypadku sieci LAN przewodowych. W 802.11 adresowalna jednostka nazywana jest stacją (STA). Stacja jest definiowana jako miejsce docelowe wiadomości i może nie być stałą lokalizacją. Inne rozróżnienie dotyczy stacji mobilnych i przenośnych. Stacja mobilna to taka, która uzyskuje dostęp do sieci LAN podczas przemieszczania się; stacja przenośna to taka, która może przemieszczać się z miejsca na miejsce, ale jest używana tylko w stałej lokalizacji.

Podstawowa architektura 802.11

802.11 używa podstawowego zestawu usług (BSS) jako swojego bloku konstrukcyjnego. BSS to zbiór urządzeń (AP i stacji lub tylko stacji), które tworzą sieć WLAN. Podstawowy obszar usług (BSA) to obszar zasięgu zapewniany przez AP. Sieć WLAN działająca w trybie infrastruktury zawsze ma jeden lub więcej AP. Niezależna sieć WLAN bez AP jest nazywana siecią ad-hoc; niezależne stacje łączą się w sposób zdecentralizowany. Dopóki stacja znajduje się w obrębie swojej BSA, może komunikować się z innymi

stacjami w BSS. Prawdopodobnie doświadczyłeś utraty łączności z telefonem komórkowym, gdy byłeś poza zasięgiem swojego obszaru usług. Podobnie możesz utracić łączność sieciową, jeśli nie znajdujesz się w obszarze zasięgu sieci WLAN. Aby połączyć dwa BSS-y, 802.11 wymaga systemu dystrybucyjnego (DS) jako warstwy pośredniej. Zasadniczo BSS 1 łączy się z DS, który z kolei łączy się z BSS 2. Jednak w jaki sposób stacja zwana STA 1 w BSS 1 łączy się ze STA 2 w BSS 2? 802.11 definiuje AP jako stację zapewniającą dostęp do DS. Dane przemieszczają się między BSS i DS przez AP. Ten proces wydaje się skomplikowany, ale rysunek powinien rozwiać wszelkie wątpliwości.



Specyfikacje IEEE definiują również zakres częstotliwości roboczych 802.11. W Stanach Zjednoczonych zakres ten wynosi od 2,4 do 2,4835 GHz. Wyobraź sobie częstotliwość jako superautostradę na niebie, po której przemieszczają się dane, a ta superautostrada obejmuje wiele autostrad (pasm częstotliwości). Każde pasmo częstotliwości zawiera kanały, które dzielą pasmo na mniejsze zakresy częstotliwości. Na przykład kanał 1 pasma częstotliwości od 2,4 GHz do 2,4835 GHz może używać częstotliwości 2,401 GHz, a kanał 2 tego pasma częstotliwości może używać częstotliwości 2,406 GHz. Standard 802.11 definiuje 11 kanałów w zakresie od 2,4 do 2,462 GHz. Jeśli kanały się nakładają, mogą wystąpić zakłócenia. Dźwięk przemieszcza się przez powietrze w postaci fal i podobnie jak fale oceaniczne, długość fali dźwiękowej jest mierzona od szczytu jednej fali do następnej. Amplituda (wysokość) i częstotliwość (szybkość, z jaką powtarza się fala dźwiękowa) fali dźwiękowej określają jej głośność i wysokość. Surferzy czekający na kolejny zestaw fal mogą dokładnie określić częstotliwość (czas potrzebny do powtórzenia się zestawu fal). Ukończenie powtarzającego się wzoru fal dźwiękowych nazywa się cyklem. Dla surferów cykl może trwać minuty. Fale dźwiękowe powtarzają się jednak ze znacznie szybszą częstotliwością. Na przykład kamerton drga z częstotliwością 440 Hz, czyli cykli na sekundę. To 440 fal na sekundę — za szybko dla surfera. Różne technologie wykorzystują różne częstotliwości, zwane pasmami, do przesyłania dźwięku. Tabela zawiera listę pasm częstotliwości.

Częstotliwość: Zakres: Długość fali

Bardzo niska częstotliwość (ELF): 3–30 Hz: 100 000 km–10 000 km

Bardzo niska częstotliwość (SLF): 30–300 Hz: 10 000 km–1000 km

Częstotliwość głosu (VF) lub ultraniska częstotliwość (ULF): 300 Hz–3 KHz: 1000 km–100 km

Bardzo niska częstotliwość (VLF): 3–30 KHz: 100 km–10 km

Niska częstotliwość (LF): 30–300 KHz: 10 km–1 km

Średnia częstotliwość (MF): 300 KHz–3 MHz: 1 km–100 m

Wysoka częstotliwość (HF): 3–30 MHz: 100 m–10 m

Bardzo wysoka częstotliwość (VHF) : 30–300 MHz : 10 m–1 m

Ultra wysoka częstotliwość (UHF): 300 MHz–3 GHz : 1 m–10 cm

Super wysoka częstotliwość (SHF): 3–30 GHz : 10 cm–1 cm

Ekstremalnie wysoka częstotliwość (EHF): 30–300 GHz : 1 cm–1 mm

Na przykład stacje radiowe AM wykorzystują pasmo średniej częstotliwości (MF); stacje radiowe FM i stacje poszukiwawczo-ratownicze wykorzystują pasmo bardzo wysokiej częstotliwości (VHF). Odległość, jaką muszą pokonać fale dźwiękowe, również determinuje, którego pasma częstotliwości użyć.

Przegląd technologii bezprzewodowych

Teraz, gdy rozumiesz częstotliwości, na których mogą przemieszczać się fale radiowe, przyjrzyj się trzem technologiom wykorzystywanym przez sieci WLAN:

• Podczerwień — ludzkie oko nie widzi światła podczerwonego. Technologia podczerwieni (IR) jest ograniczona do jednego pomieszczenia lub linii wzroku, ponieważ światło podczerwone nie może przenikać przez ściany, sufity ani podłogi.

• Wąskopasmowa — technologia wąskopasmowa wykorzystuje częstotliwości pasma radiowego mikrofal do przesyłania danych. Najczęstszymi zastosowaniami tej technologii są telefony bezprzewodowe i otwieracze drzwi garażowych.

• Widmo rozproszone — aby przemieszczać się przez fale radiowe, dane muszą być modulowane w sygnale nośnym lub kanale. Modulacja definiuje sposób umieszczania danych w sygnale nośnym. Na przykład modulacja widma rozproszonego oznacza, że dane są rozproszone w paśmie o dużej częstotliwości, zamiast przemieszczać się tylko przez jedno pasmo częstotliwości. Innymi słowy, wybierana jest grupa częstotliwości radiowych, a dane są „rozproszone” w tej grupie. Rozproszone widmo, najszerzej stosowana technologia WLAN, wykorzystuje następujące metody:

❍ Rozproszone widmo z przeskokiem częstotliwości (FHSS): Dane przeskakują na inne częstotliwości, aby uniknąć zakłóceń, które mogą wystąpić w paśmie częstotliwości. Przeskakiwanie z jednej częstotliwości na drugą odbywa się w odstępach ułamka sekundy i utrudnia intruzowi lub atakującemu zakłócenie kanału komunikacyjnego.

❍ Rozproszone widmo z sekwencją bezpośrednią (DSSS): W przeciwieństwie do FHSS, DSSS rozprzestrzenia pakiety danych jednocześnie na wielu częstotliwościach zamiast przeskakiwać na inne częstotliwości. Podbity są dodawane do pakietu podczas jego przemieszczania się przez pasmo częstotliwości i są używane do odzyskiwania, w taki sam sposób, w jaki RAID-5 wykorzystuje bity parzystości do odbudowy dysku twardego, który uległ awarii. Podbity są nazywane „chipami”, a każdy bit oryginalnej wiadomości jest reprezentowany przez wiele bitów, zwanych kodem chipowania.

❍ Ortogonalne multipleksowanie z podziałem częstotliwości (OFDM): Szerokość pasma jest dzielona na szereg częstotliwości zwanych tonami, co pozwala na większą przepustowość (szybkość transferu danych) niż FHSS i DSSS.

❍ Ortogonalne multipleksowanie z podziałem częstotliwości Access (OFDMA): OFDMA to wielodostępne rozszerzenie jednoużytkownikowego OFDM. ODFMA ma przepustowość trzy razy większą niż OFDM w przypadku krótkich pakietów danych lub wielu punktów końcowych. OFDMA łączy transmisje i wysyła ramki do wielu punktów końcowych jednocześnie. Jest bardziej wydajny przy transmisji o mniejszym opóźnieniu. Dzięki temu OFDMA idealnie nadaje się do urządzeń IoT, wideo, gier online i aplikacji automatyzacyjnych.

Dodatkowe projekty IEEE 802.11

Grupa robocza IEEE opracowała dodatkowe projekty 802.11, wydając standardy 802.11a i 802.11b w październiku 1999 r. 802.11b szybko stał się powszechniej stosowanym standardem, prawdopodobnie dlatego, że jego sprzęt był tańszy. Znany również jako Wi-Fi, 802.11b działa w paśmie 2,4 GHz i zwiększył przepustowość do 11 Mb/s z 1 lub 2 Mb/s oryginalnego 802.11. Umożliwia łącznie 11 oddzielnych kanałów, aby zapobiec nakładaniu się sygnałów. Jednak ze względu na wymagania dotyczące przepustowości każdego kanału, skutecznie tylko trzy kanały (1, 6 i 11) można łączyć bez nakładania się i tworzenia zakłóceń. Ten standard wprowadził również Wired Equivalent Privacy (WEP), co dało wielu użytkownikom fałszywe poczucie bezpieczeństwa, że dane przesyłane przez sieć WLAN są chronione. WEP jest omówiony później w „Understanding Authentication". Standard 802.11a ma inny zakres częstotliwości roboczych niż 802.11 i 802.11b; działa w trzech odrębnych pasmach w paśmie 5 GHz. Ponadto przepustowość wzrasta do 54 Mb/s, znacznie szybciej niż 802.11b. Standard 802.11g, wydany w 2003 r., działa również w paśmie 2,4 GHz. Jednak ze względu na inną modulację, wykorzystuje metodę OFDM, która zwiększa przepustowość do 54 Mb/s. Standard 802.11i wprowadził Wi-Fi Protected Access (WPA) w 2004 r., co zostało omówione w „Understanding Authentication". Na razie należy zauważyć, że 802.11i naprawiło wiele luk w zabezpieczeniach w 802.11b. Dla profesjonalistów ds. bezpieczeństwa standard 802.11i jest prawdopodobnie najważniejszy. Standard 802.11e, wydany w 2005 r., zawiera ulepszenia, które rozwiązują problem zakłóceń. Gdy wykryte zostaną zakłócenia, sygnał może szybciej przeskoczyć na inną częstotliwość, zapewniając lepszą jakość usługi niż 802.11b. Standard 802.11n, sfinalizowany w 2009 r., działa na tej samej częstotliwości (pasmo 2,4 lub 5 GHz) i wykorzystuje to samo kodowanie co 802.11g. Jednak dzięki wykorzystaniu wielu anten i kanałów o szerszym paśmie zwiększa przepustowość do 600 Mb/s. Standard 802.11ac, wydany w 2014 r., wykorzystuje pasmo 5 GHz. Standard ten umożliwia wyższą przepustowość (do 1 gigabita na sekundę) poprzez pomnożenie liczby łączy MIMO i wykorzystanie modulacji o wysokiej gęstości. Standard 802.11ad, nazywany „WiGig", umożliwia transfer danych z szybkością do 7 gigabitów na sekundę w pasmach 2,4 GHz, 5 GHz i 60 GHz. W styczniu 2016 r. firma TP-Link zaprezentowała pierwszy router bezprzewodowy obsługujący specyfikację 802.11ad. Standard 802.11ah, zatwierdzony w maju 2017 r., ma na celu zmniejszenie zużycia energii i tworzy sieci Wi-Fi o rozszerzonym zasięgu, które mogą wykraczać poza typowe sieci 2,4 GHz lub 5 GHz. Oczekuje się, że będzie konkurował z Bluetooth ze względu na niższe zapotrzebowanie na energię. Standard 802.11aj, znany jako China Millimeter Wave, jest używany w Chinach i jest zasadniczo rebrandingiem 802.11ad do użytku w niektórych obszarach świata. Celem jest zachowanie wstecznej kompatybilności z 802.11ad. Technologia ta wykorzystuje pasma 45 GHz i 60 GHz, które są dostępne wyłącznie w Chinach. Standard 802.11x, oznaczony jako Wi-Fi 6, został uruchomiony w 2019 r. i zastąpił 802.11ac jako de facto standard bezprzewodowy. Wi-Fi 6 osiąga maks. 10 Gb/s, zużywa mniej energii, jest bardziej niezawodny w zatłoczonych środowiskach i obsługuje lepsze zabezpieczenia.

Dodatkowe standardy IEEE 802

Standard 802.15 dotyczy urządzeń sieciowych w przestrzeni roboczej jednej osoby, co nazywa się bezprzewodową siecią osobistą (WPAN). Maksymalna odległość między urządzeniami wynosi zwykle 10 metrów. Dzięki specyfikacji telekomunikacyjnej Bluetooth, podstawowej części standardu WPAN, można łączyć urządzenia przenośne, takie jak telefony komórkowe i komputery, bez przewodów. Wersja Bluetooth 2.0 wykorzystuje pasmo 2,4 GHz i może przesyłać dane z prędkością do 12 Mb/s. Nie jest zgodna ze standardami 802.11. Wersja Bluetooth, 4.0, została wydana w 2010 r. i przeszła na pasmo 802.11, aby obsługiwać prędkości do 24 Mb/s. W 2005 r. IEEE rozpoczęło prace nad wykorzystaniem różnych technologii dla standardu WPAN. ZigBee, obecny przykład, jest używany w systemach automatyki, takich jak inteligentne systemy oświetleniowe, sterowanie temperaturą i urządzenia. Standard 802.16 obejmuje bezprzewodowe sieci metropolitalne (MAN). Ten standard definiuje interfejs Wireless MAN Air Interface dla bezprzewodowych sieci MAN i odnosi się do ograniczonej odległości dostępnej dla sieci WLAN 802.11b. Najbardziej rozpowszechnioną implementacją technologii bezprzewodowej MAN jest Worldwide Interoperability for Microwave Access (WiMAX). WiMAX został wprowadzony na rynek jako realna alternatywa dla tak zwanego dostępu do Internetu ostatniej mili, który jest zwykle dostarczany przez kabel i DSL. Istnieją mobilne (802.16e) i stacjonarne (802.16d) wersje WiMAX. Typowa rzeczywista prędkość WiMAX wynosi około 10 Mb/s, mniej niż teoretyczne 120 Mb/s maksymalnego standardu 802.16. WiMAX był przedsięwzięciem nieudanym, a wysiłki zakończyły się w 2015 roku. Inny standard MAN, 802.20, z celem podobnym do mobilnego WiMAX, nazywa się Mobile Broadband Wireless Access (MBWA). Dotyczy bezprzewodowych MAN-ów dla użytkowników mobilnych w pociągach, metrze lub samochodach poruszających się z prędkością do 150 mil na godzinę. Najczęstsza implementacja MBWA, iBurst, jest szeroko stosowana w Azji i Afryce.

Odwiedzanie witryny IEEE 802.11

Czas trwania: 30 minut

Cel: Dowiedz się więcej o standardach bezprzewodowych IEEE.

Opis: Możesz znaleźć mnóstwo informacji na stronie internetowej IEEE, która udostępnia standardy do pobrania. W tej aktywności odwiedzasz stronę internetową IEEE i badasz nowy i ekscytujący projekt w IEEE.

1. Uruchom przeglądarkę internetową, jeśli to konieczne, i przejdź do http://www.ieee802.org/11/Reports/tgay_update.htm.

2. Przejrzyj cele projektu specyfikacji IEEE 802.11ay.

3. Jaka jest teoretyczna przepustowość 802.11ay? Patrząc na Tabelę 11-2, jaka jest przepustowość powszechnie używanych protokołów 802.11a, b, g i n?

4. Odwiedź wpis w Wikipedii dotyczący 802.11 pod adresem https://en.wikipedia.org/wiki/IEEE_802.1

5. Przejrzyj sekcję Bezpieczeństwo w artykule w Wikipedii.

6. Wyjaśnij, dlaczego specjalista ds. bezpieczeństwa może zasugerować wyłączenie funkcji Wi-Fi Protected Setup (WPS) na routerze.

7. Zamknij przeglądarkę internetową.

ZROZUMIENIE UWIERZYTELNIANIA

Problem nieautoryzowanych użytkowników uzyskujących dostęp do zasobów w sieci jest głównym zmartwieniem specjalistów ds. bezpieczeństwa. Organizacja, która wprowadza do sieci technologię bezprzewodową, zwiększa prawdopodobieństwo wystąpienia problemów z bezpieczeństwem. Standard 802.1X, omówiony w poniższej sekcji, zajmuje się kwestią uwierzytelniania. Niektóre routery domyślnie nie wymagają uwierzytelniania, co może narazić sieć korporacyjną na ryzyko.

Standard 802.1X

Ponieważ musi istnieć metoda zapewniająca, że inni użytkownicy z bezprzewodowymi kartami sieciowymi nie będą mogli uzyskać dostępu do zasobów w Twojej sieci bezprzewodowej, standard 802.1X definiuje proces uwierzytelniania i autoryzacji użytkowników w sieci. Ten standard jest szczególnie przydatny w przypadku bezpieczeństwa sieci WLAN, gdy kontrola dostępu fizycznego jest trudniejsza do wyegzekwowania niż w przypadku przewodowych sieci LAN. Aby zrozumieć, jak odbywa się uwierzytelnianie w sieci bezprzewodowej, zapoznaj się z podstawowymi koncepcjami uwierzytelniania w poniższych sekcjach.

Protokół Point-to-Point

Wielu dostawców usług internetowych używa protokołu Point-to-Point (PPP) do łączenia użytkowników dial-up lub DSL. PPP obsługuje uwierzytelnianie, wymagając od użytkownika podania prawidłowej nazwy użytkownika i hasła. PPP weryfikuje, czy użytkownicy próbujący użyć łącza są rzeczywiście tymi, za których się podają.

Protokół Extensible Authentication Protocol

Protokół Extensible Authentication Protocol (EAP), rozszerzenie protokołu PPP, został zaprojektowany, aby umożliwić firmie wybór metody uwierzytelniania. Na przykład firma może użyć certyfikatów lub uwierzytelniania Kerberos do uwierzytelnienia użytkownika łączącego się z punktem dostępowym. Certyfikat to rekord uwierzytelniający jednostki sieciowe, takie jak serwer lub klient. Zawiera informacje X.509, które identyfikują właściciela, urząd certyfikacji (CA) i klucz publiczny właściciela. Certyfikat X.509 można sprawdzić, przechodząc na stronę www.amazon.ca. Ta strona internetowa przekierowuje do bezpiecznego adresu URL (HTTPS), gdzie należy kliknąć ikonę kłódki po lewej stronie paska adresu w przeglądarce Chrome, a następnie kliknąć Certyfikat, aby wyświetlić informacje o certyfikacie pokazane na rysunku .

Następujące metody EAP można wykorzystać w celu zwiększenia bezpieczeństwa w sieci bezprzewodowej:

• Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) — ta metoda wymaga przypisania klientowi i serwerowi cyfrowego certyfikatu podpisanego przez urząd certyfikacji, któremu ufają obie strony. Urząd certyfikacji może być firmą komercyjną pobierającą opłatę lub serwerem skonfigurowanym przez administratora sieci w celu wydawania certyfikatów. W ten sposób zarówno serwer, jak i klient uwierzytelniają się wzajemnie. Oprócz serwerów wymagających od klientów udowodnienia, że są tym, za kogo się podają, klienci chcą również, aby serwery zweryfikowały ich tożsamość.

• Protected EAP — Protected EAP (PEAP) używa TLS do uwierzytelniania serwera względem klienta, ale nie klienta względem serwera. W przypadku PEAP tylko serwer musi mieć certyfikat cyfrowy.

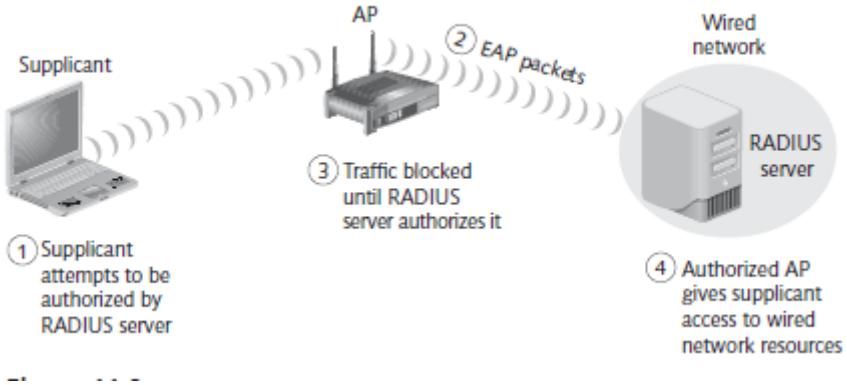
• Microsoft PEAP — w implementacji PEAP firmy Microsoft bezpieczny kanał jest tworzony przy użyciu TLS jako ochrony przed podsłuchem. 802.1X wykorzystuje następujące komponenty do działania:

• Suplikant — Suplikant to użytkownik sieci bezprzewodowej próbujący uzyskać dostęp do sieci WLAN.

• Authenticator — AP działa jako podmiot zezwalający lub odmawiający dostępu suplikantowi.

• Serwer uwierzytelniania — Ten serwer, który może być serwerem Remote Access Dial-In User Service (RADIUS), jest używany jako scentralizowany komponent, który uwierzytelnia użytkownika i wykonuje funkcje rozliczeniowe. Na przykład dostawca usług internetowych używający RADIUS może sprawdzić, kto zalogował się do usługi dostawcy usług internetowych i jak długo użytkownik był połączony. Większość serwerów RADIUS jest oparta na *nix, ale implementacja RADIUS firmy Microsoft nazywa się Internet Authentication Service (IAS) w systemach Windows Server 2000 i Windows Server 2003, a po systemie Windows Server 2008 nazywa się Network Policy Server.

Rysunek przedstawia proces 802.1X opisany w następujących krokach:



1. Nieuwierzytelniony klient (suplikant) próbuje połączyć się z AP działającym jako uwierzytelniacz.

2. AP odpowiada, włączając port, który przekazuje tylko pakiety EAP od suplikanta do serwera RADIUS w sieci przewodowej.

3. AP blokuje cały inny ruch, dopóki serwer RADIUS nie uwierzytelni suplikanta.

4. Po uwierzytelnieniu suplikanta przez serwer RADIUS, udziela on suplikantowi dostępu do zasobów sieciowych za pośrednictwem AP.

Dopóki EAP i 802.1X nie były używane w sieciach LAN bezprzewodowych, w sieci WLAN uwierzytelniane było urządzenie, a nie użytkownik. Dlatego jeśli komputer został skradziony z firmy, złodziej mógł połączyć się z zasobami w sieci WLAN, używając komputera do uwierzytelniania. W poniższych sekcjach opisano funkcje bezpieczeństwa wprowadzone w 802.11b i 802.11i.

Wired Equivalent Privacy

Wired Equivalent Privacy (WEP), część standardu 802.11b, została opracowana w celu szyfrowania danych przesyłanych przez sieć bezprzewodową. Przez pewien czas dawała wielu specjalistom ds. bezpieczeństwa fałszywe poczucie bezpieczeństwa, że technologia bezprzewodowa może być równie bezpieczna jak sieci przewodowe. Niestety, WEP został rozdarty na strzępy przez specjalistów ds. bezpieczeństwa, profesorów z dużych uniwersytetów i hakerów, którzy publikują sposoby łamania szyfrowania WEP. Szyfrowanie WEP jest łatwe do złamania ze względu na wadę algorytmu szyfrowania RC4. Kluczem szyfrującym używanym przez algorytm jest 24-bitowy wektor inicjalizacji (IV) w połączeniu z kluczem domyślnym. 24-bitowy IV jest zbyt krótki i łatwy do złamania. Niektórzy twierdzą, że WEP jest nadal lepszy niż brak zabezpieczeń, a gdy jest połączony z zabezpieczeniami wirtualnej sieci prywatnej (VPN), twierdzą, że WEP dobrze sprawdza się w przypadku użytkowników domowych lub małych firm. Mimo to wielu dostrzegało potrzebę lepszego sposobu ochrony sieci WLAN.

Wi-Fi Protected Access

Wi-Fi Protected Access (WPA, WPA2 i WPA3), określony w standardzie 802.11i, zastępuje WEP, o którym wiadomo, że ma słabości kryptograficzne. WPA poprawia szyfrowanie, wykorzystując Temporal Key Integrity Protocol (TKIP). TKIP ma cztery ulepszenia, które rozwiązują luki w zabezpieczeniach szyfrowania w WEP:

• Message Integrity Check (MIC) — MIC, wymawiane M-I-C, nazywane również Michael, to kryptograficzny kod integralności wiadomości. Jego głównym celem jest zapobieganie fałszerstwom, czyli pakietom tworzonym przez atakujących tak, aby wyglądały jak legalne pakiety. Na przykład MIC używa tajnego klucza uwierzytelniającego, który znają tylko nadawca i odbiorca, i tworzy tag (kod

integralności wiadomości) generowany z klucza i wiadomości wysłanej do odbiorcy. Nadawca wysyła wiadomość i tag do odbiorcy, który musi wprowadzić klucz, tag i wiadomość w programie, który weryfikuje, czy tag utworzony za pomocą trzech pól wejściowych jest równy tagowi, który program powinien utworzyć. Nie musisz zapamiętywać tego procesu, ale powinieneś zrozumieć, że MIC koryguje znaną lukę w zabezpieczeniach protokołu WEP.

• Rozszerzony wektor inicjalizacji (IV) z regułami sekwencjonowania — to ulepszenie zostało opracowane w celu zapobiegania powtórzeniom. W powtórzeniu atakujący rejestruje lub przechwytuje pakiet, zapisuje go i ponownie przesyła wiadomość później. Aby zapobiec wystąpieniu powtórzenia, do pola WEP IV stosuje się numer sekwencyjny. Jeśli pakiet zostanie odebrany z IV równym lub mniejszym od numeru sekwencyjnego odebranego wcześniej, pakiet zostanie odrzucony.

• Mieszanie kluczy dla każdego pakietu — to ulepszenie pomaga pokonać ataki słabymi kluczami, które miały miejsce w protokole WEP. Adresy MAC są używane do tworzenia klucza pośredniego, co zapobiega używaniu tego samego klucza przez wszystkie łącza.

• Mechanizm ponownego kodowania — to ulepszenie zapewnia nowe klucze, aby pomóc zapobiegać atakom polegającym na ponownym używaniu starych kluczy. Oznacza to, że jeśli ten sam klucz jest używany wielokrotnie, ktoś uruchamiający program do jego odszyfrowania prawdopodobnie mógłby to zrobić po zebraniu dużej liczby pakietów. Wielokrotne używanie tego samego klucza stanowiło duży problem w WEP.

WPA dodało również mechanizm uwierzytelniania wykorzystujący 802.1X i EAP, które nie były dostępne w WEP. Od czasu wydania WPA odkryto słabości w TKIP, które wymagały bardziej zaawansowanego WPA2. WPA2 zastąpiło WPA w oficjalnym standardzie Wi-Fi. Główną różnicą między WPA i WPA2 jest wymóg w WPA2 używania szyfrowania AES zamiast TKIP. WPA3 zostało wydane w styczniu 2018 r. WPA3 oficjalnie zastępuje WPA2 i zapewnia ulepszone funkcje bezpieczeństwa. Do szyfrowania WPA3 używa AES-256 i SHA-384 w trybie WPA3-Enterprise i nadal nakazuje używanie CCMP-128 (AES-128 w trybie CCM) jako minimalnego algorytmu szyfrowania w trybie WPA3-Personal. WPA3 zastępuje wymianę kluczy wstępnych (PSK) wymianą równoczesnego uwierzytelniania (SAE), co skutkuje bezpieczniejszą początkową wymianą kluczy. WPA3 utrudnia hakerom dostęp do sieci za pomocą ataków polegających na odgadywaniu haseł w trybie offline. WPA2 umożliwiłoby hakerom przechwytywanie danych z routera i wykorzystywanie ich do wielokrotnych prób odgadnięcia hasła, ale w przypadku WPA3 jedna nieprawidłowa próba włamania sprawia, że dane te stają się bezużyteczne. WPA3 poprawia również bezpieczeństwo w publicznych sieciach Wi-Fi, uniemożliwiając hakerom odzyskanie danych, nawet jeśli przechwycą i złamią zaszyfrowaną transmisję. WPA3 jest bezpieczne, ale nie niezniszczalne. W szczególności jest podatne na ataki czasowe podczas procesu uzgadniania. Informacje zebrane z WPA3 z ataku czasowego mogą być również wykorzystane do przeprowadzenia ataku partycjonowania haseł, który jest podobny do ataku słownikowego. Atak słownikowy to zautomatyzowany atak polegający na odgadywaniu haseł.

Wi-Fi Protected Setup (WPS)

Wi-Fi Protected Setup (WPS) to bezprzewodowy standard uwierzytelniania stworzony, aby umożliwić użytkownikom łatwe i bezpieczne dodawanie urządzeń do sieci bezprzewodowej. WPS ułatwia ten proces, eliminując potrzebę wprowadzania przez użytkownika hasła. Zamiast tego użytkownik po prostu naciska przycisk na routerze, a urządzenie z włączonym WPS łączy się z routerem. Jeśli masz w domu nowoczesny router, prawdopodobnie obsługuje on WPS. WPS może wydawać się świetnym rozwiązaniem, ale pod koniec 2011 roku odkryto poważną lukę w zabezpieczeniach. Ta luka umożliwia atakującemu uzyskanie dostępu do sieci zdalnie, bez znajomości hasła WPA2.

ZROZUMIENIE WARDRIVINGU

Prawdopodobnie nie jest tajemnicą, że hakerzy używają wardrivingu — jeżdżąc z niedrogim sprzętem i oprogramowaniem, które umożliwia im wykrywanie punktów dostępu, które nie zostały zabezpieczone. Co zaskakujące, niektóre punkty dostępowe nie mają haseł ani środków bezpieczeństwa, więc wardriving może być bardzo opłacalny dla hakerów. W chwili pisania tego tekstu wardriving nie jest nielegalny; korzystanie z zasobów sieci odkrytych za pomocą wardrivingu to oczywiście inna historia. Wardriving został teraz rozszerzony o warflying, który obejmuje drony z anteną i tym samym oprogramowaniem, które jest używane w wardrivingu. Testerzy użyli Kismet, omówionego później w tej sekcji, który identyfikuje punkty dostępowe, które próbują „maskować" lub ukrywać swoje SSID-y

Jak to działa

Aby przeprowadzić wardriving, atakujący lub tester bezpieczeństwa po prostu jeździ z obsługującym Wi-Fi smartfonem lub laptopem i oprogramowaniem, które skanuje obszar w poszukiwaniu SSID. Nie wszystkie karty WNIC są kompatybilne z oprogramowaniem skanującym, dlatego przed zakupem sprzętu należy zapoznać się z wymaganiami oprogramowania. Ceny anten różnią się w zależności od ich jakości i zasięgu, jaki mogą pokryć. Niektóre są tak małe jak antena telefonu komórkowego, a niektóre tak duże jak bazooka. Większe mogą czasami zwracać wyniki w sieciach oddalonych o wiele kilometrów od atakującego. Mniejsze mogą wymagać bliskiej odległości od punktu dostępowego. Większość oprogramowania skanującego wykrywa SSID firmy, rodzaj włączonych zabezpieczeń i siłę sygnału, wskazując, jak blisko atakującego znajduje się punkt dostępowy. Ponieważ ataki na WEP są proste, a ataki na WPA są możliwe, każde połączenie 802.11 nieużywające WPA2 lub WPA3 należy uznać za niewystarczająco zabezpieczone. W poniższych sekcjach przedstawiono niektóre narzędzia, z których korzysta wielu hakerów sieci bezprzewodowych i specjalistów ds. bezpieczeństwa.

BAJTY BEZPIECZEŃSTWA

Etyczny haker z Houston, wcześniej zatrudniony w Departamencie Technologii hrabstwa, został oskarżony o włamanie się do sieci bezprzewodowej sądu w Teksasie. Podczas skanowania w ramach swojej pracy zauważył lukę w zabezpieczeniach sieci bezprzewodowej sądu i był zaniepokojony. Pokazał urzędnikowi hrabstwa i lokalnemu reporterowi, jak łatwo może uzyskać dostęp do sieci bezprzewodowej, mając tylko laptopa i kartę WNIC. Później został oskarżony o dwa przypadki nieautoryzowanego dostępu do chronionego systemu komputerowego i nieautoryzowany dostęp do systemu komputerowego używanego w administracji wymiaru sprawiedliwości. Po trzydniowym procesie i 15 minutach narady ławy przysięgłych został uniewinniony. Gdyby uznano go za winnego wszystkich zarzutów, groziłoby mu 10 lat więzienia i grzywna w wysokości 500 000 dolarów.

Vistumbler

Vistumbler (www.vistumbler.net) to darmowe narzędzie napisane dla systemu Windows, które umożliwia wykrywanie sieci WLAN korzystających z punktów dostępowych 802.11a, 802.11b, 802.11g, 802.11n i 802.11ac. Narzędzie jest łatwe w instalacji, jednak nie wszystkie urządzenia bezprzewodowe współpracują z oprogramowaniem, dlatego należy uważnie przestrzegać instrukcji i sprawdzić, czy sprzęt jest zgodny. Vistumbler został zaprojektowany, aby pomóc testerom bezpieczeństwa w następujących czynnościach:

- Weryfikacja konfiguracji sieci WLAN
- Wykrywanie innych sieci bezprzewodowych, które mogą zakłócać działanie sieci WLAN

• Wykrywanie nieautoryzowanych punktów dostępowych, które mogły zostać umieszczone w sieci WLAN

UWAGA

Vistumbler jest również używany w wardrivingu, ale należy pamiętać, że w większości części świata korzystanie z czyjejś sieci bez pozwolenia jest nielegalne. Prawo to obejmuje korzystanie z czyjegoś połączenia internetowego bez jego wiedzy lub pozwolenia.

Inną cechą Vistumblera jest to, że może połączyć się z GPS-em, umożliwiając testerowi bezpieczeństwa lub hakerowi mapowanie lokalizacji wszystkich sieci WLAN wykrytych przez oprogramowanie. Gdy Vistumbler identyfikuje sygnał AP, rejestruje SSID, adres MAC i producenta AP, kanał, na którym sygnał został usłyszany, siłę sygnału i to, czy szyfrowanie jest włączone (ale nie konkretny typ szyfrowania). Atakujący mogą wykryć AP w promieniu 350 stóp, chociaż przy dobrej antenie mogą zlokalizować AP oddalone o kilka mil. Dla osób z umiejętnościami mechanicznymi liczne strony internetowe zawierają instrukcje dotyczące budowy własnej anteny z pustych puszek po fasoli, puszkach po chipsach ziemniaczanych i tym podobnych. Można również kupić przyzwoitą antenę za około 50 USD.

Odkrywanie punktów dostępowych za pomocą Wifite

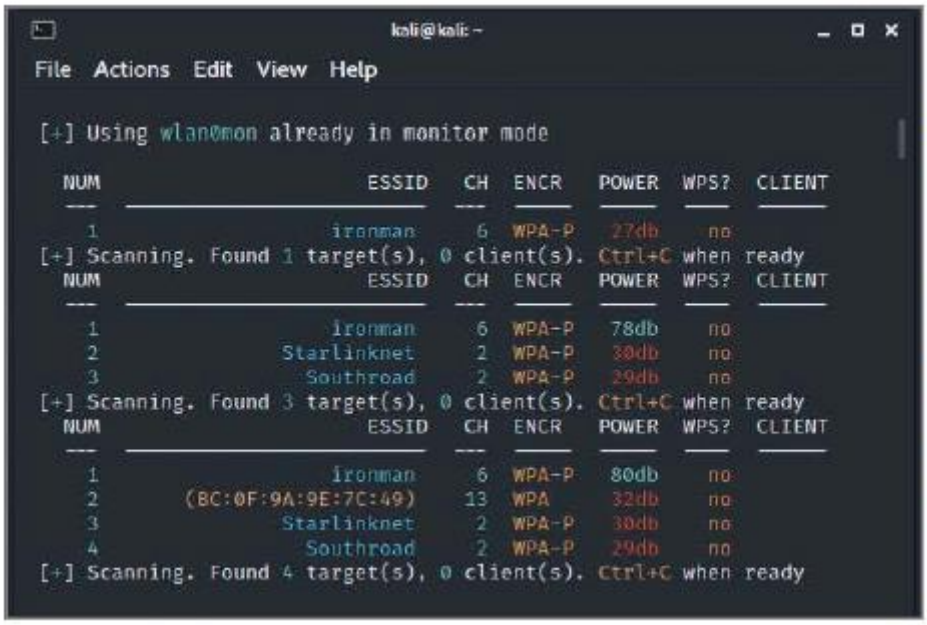
Czas trwania: 15 minut

Cel: Zobacz, jakie informacje może zebrać skaner bezprzewodowy, taki jak Wifite.

Opis: Podczas testowania sieci pod kątem luk w zabezpieczeniach nie zaniedbuj sprawdzania luk w zabezpieczeniach żadnych sieci WLAN skonfigurowanych przez firmę. Wifite to darmowy skaner Wi-Fi, podobny do Vistumbler. Wifite oferuje również funkcje ataku, których możesz użyć do złamania niezabezpieczonych sieci bezprzewodowych. W ramach tej aktywności sprawdzisz funkcjonalność skanera Wifite. Możesz zweryfikować dostępne punkty dostępowe i ich identyfikatory SSID. Jeśli Twoja klasa nie ma bezprzewodowych kart sieciowych ani punktu dostępowego, możesz wykonać tę aktywność później, jeśli sprzęt jest dostępny, na przykład w domu lub biurze.

1. W razie potrzeby uruchom system Kali Linux.

2. Otwórz powłokę terminala i wpisz wifite, a następnie naciśnij Enter, aby uruchomić Wifite. Jeśli znajdujesz się w obszarze z kilkoma punktami dostępowymi, okno terminala Wifite może wyglądać jak na rysunku.



3. Jeśli na ekranie pojawią się SSID-y, sprawdź kolumnę CH. Wyświetla ona informacje o kanale dla każdego punktu dostępowego. Wiele systemów na rysunku używa kanału 6 lub kanału 2, co może wskazywać na przeciążenie. Jeśli odkryłeś te informacje podczas testu bezpieczeństwa, możesz zasugerować klientowi skonfigurowanie niektórych punktów dostępowych na różnych kanałach.

4. Naciśnij Ctrl1C dwa razy, aby wyjść z Wifite. Zamknij wszystkie otwarte okna

Kismet

Innym popularnym produktem do przeprowadzania ataków wardriving jest Kismet (www.kismetwireless.net), napisany przez Mike'a Kershawa. Ten produkt jest darmowy i działa na systemach Linux, BSD UNIX, macOS, a nawet na komputerach PDA z systemem Linux. Oprogramowanie jest reklamowane jako coś więcej niż detektor sieci bezprzewodowej. Kismet to także sniffer i system wykrywania włamań (IDS), który może wykrywać ruch 802.11b, 802.11a, 802.11g, 802.11n, 802.11ac i 802.11ax. Oferuje następujące funkcje:

• Rejestrowanie danych zgodne z Wireshark i Tcpdump

• Zgodność z AirSnort i AirCrack

• Wykrywanie zakresu IP sieci

• Wykrywanie ukrytych identyfikatorów SSID sieci

• Graficzne mapowanie sieci

• Architektura klient/serwer umożliwiająca wielu klientom jednoczesne oglądanie jednego serwera Kismet

• Identyfikacja producenta i modelu punktów dostępowych i klientów

• Wykrywanie znanych domyślnych konfiguracji punktów dostępowych

• Dane wyjściowe XML

• Obsługa dziesiątek typów kart (prawie każdej karty obsługującej tryb monitorowania)

Kismet to pasywny skaner, dzięki czemu może wykrywać nawet ukryte identyfikatory SSID sieci. Kismet może być używany do przeprowadzania wardrivingu i wykrywania nieuczciwych punktów dostępowych w sieci firmy. Nieuczciwy punkt dostępowy to bezprzewodowy punkt dostępowy zainstalowany w organizacji bez autoryzacji. Nieuczciwy punkt dostępowy często ma taki sam identyfikator SSID jak legalny punkt dostępowy. Złoczyńca, który wdrożył nieuczciwego punktu dostępowego, ma nadzieję, że użytkownicy połączą się z nim, zakładając, że jest to legalny punkt dostępowy. Jeśli użytkownicy połączą się z nieuczciwym AP, hakerzy mogą go użyć do przechwycenia ich danych. Ten typ nieuczciwego AP jest często nazywany złym bliźniakiem. Jeśli potrzebujesz obsługi GPS, z Kismet współpracuje kilka narzędzi, takich jak demon GPS (GPSD), GISKismet i Kisgearth, które mogą się przydać do dokładnego APlokalizacji. Gdy Kismet jest skonfigurowany do korzystania z GPSD, wyjście wyświetla współrzędne, wskazując lokalizację skanowanego AP. Te dane współrzędnych można wprowadzić do Google Earth w celu tworzenia map.

ZROZUMIENIE HACKOWANIA BEZPRZEWODOWEGO

Hakowanie sieci bezprzewodowej jest podobne do hakowania przewodowej sieci LAN. Wiele z poznanych narzędzi do skanowania i enumeracji portów można zastosować w sieciach bezprzewodowych. W poniższych sekcjach opisano dodatkowe narzędzia, których używają atakujący, a których można użyć do przeprowadzania testów bezpieczeństwa.

Narzędzia pracy

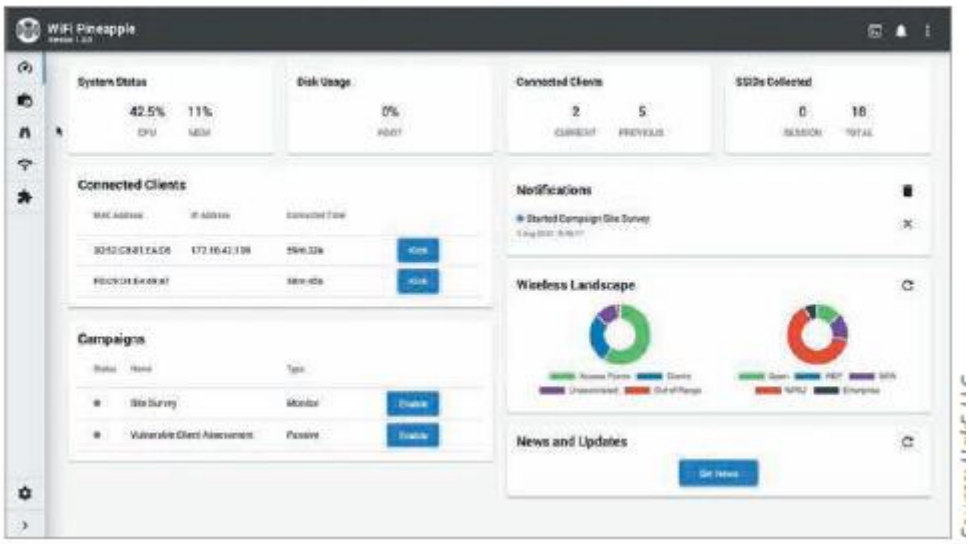
Haker sieci bezprzewodowej zwykle ma laptopa, kartę sieciową WNIC, antenę, sniffery (na przykład Tcpdump lub Wireshark), narzędzia takie jak Vistumbler lub Kismet i mnóstwo cierpliwości. Po użyciu Vistumbler lub Kismet do określenia nazwy sieci, SSID, adresu MAC punktu dostępowego, kanału, siły sygnału, rodzaju włączonego szyfrowania i tego, czy włączony jest WPS, tester bezpieczeństwa jest gotowy do kontynuowania testów. Co robią atakujący lub testerzy bezpieczeństwa, jeśli w punkcie dostępowym włączony jest WEP lub WPA? Kilka narzędzi rozwiązuje ten problem. Aircrack-ng, omówiony w poniższych sekcjach, skłonił organizacje do zastąpienia WEP bezpieczniejszym WPA jako metody uwierzytelniania. Jednak niektóre firmy nadal używają 802.11b z włączonym WEP, a niektóre nawet pozostawiają swoją sieć całkowicie niezabezpieczoną.

Aircrack-ng

Jako specjalisty ds. bezpieczeństwa Twoim zadaniem jest ochrona sieci i utrudnienie atakującym włamania się. Możesz chcieć wierzyć, że możesz całkowicie uniemożliwić atakującym włamanie się, ale niestety, ten cel jest niemożliwy do osiągnięcia. Aircrack-ng (dołączony do Kali Linux lub dostępny bezpłatnie na www.aircrack-ng.org) to narzędzie, którego większość hakerów używa do uzyskiwania dostępu do sieci WLAN obsługujących WEP. Aircrack-ng zastąpił AirSnort, produkt stworzony przez badaczy bezpieczeństwa sieci bezprzewodowych Jeremy'ego Bruestle'a i Blake'a Hegerle'a, którzy postanowili udowodnić, że szyfrowanie WEP jest wadliwe i łatwe do złamania. AirSnort był pierwszym szeroko stosowanym programem do łamania WEP i obudził niedowiarków, którzy uważali, że WEP jest wystarczającą ochroną dla sieci WLAN. Aircrack-ng kontynuował tam, gdzie skończył AirSnort (i nieco starszy WEPCrack). Ma kilka przydatnych dodatków, takich jak interfejs użytkownika GUI o nazwie Fern WIFI Cracker, pokazany na rysunku (również dołączony do Kali Linux).

WiFi Pineapple

Miłośnicy hakowania Wi-Fi Darren Kitchen i Sebastian Kinne stworzyli scyzoryk szwajcarski do hakowania sieci bezprzewodowych o nazwie WiFi Pineapple. Może on skanować punkty dostępu bezprzewodowego i konfigurować fałszywe punkty dostępowe, aby przeprowadzać ataki socjotechniczne u użytkowników lub dezorientować atakujących za pomocą airbase-ng. WiFi Pineapple ma inną niebezpieczną funkcję, która pozwala atakującemu emulować dowolną sieć, o którą prosi klient. Aby to zrozumieć, pamiętaj, że urządzenia bezprzewodowe stale sondują sieci, z którymi wcześniej się łączyły. Funkcja WiFi Pineapple nasłuchuje tych sond i odpowiada na nie tak, jakby były punktem dostępowym, o który prosił klient. Po przywróceniu odpowiedzi z WiFi Pineapple klient łączy się z fałszywą siecią, narażając cały ruch klienta na ryzyko podsłuchu. Możesz przeczytać więcej na ten temat na stronie internetowej WiFi Pineapple (www.wifipineapple.com/). Strona główna narzędzia jest pokazana na rysunku.



UWAGA

Kali Linux zawiera szeroką gamę narzędzi analitycznych do testowania sieci bezprzewodowych

Środki zaradcze na ataki bezprzewodowe

Ochrona sieci bezprzewodowej stanowi wyzwanie dla specjalistów ds. bezpieczeństwa ze względu na wady konstrukcyjne technologii bezprzewodowej oraz dlatego, że w pewnym stopniu inżynierowie próbują zakleić plaster na otwartą ranę klatki piersiowej. Niektóre techniki zaradcze omówione w tej sekcji, takie jak stosowanie certyfikatów na wszystkich urządzeniach bezprzewodowych, są czasochłonne i kosztowne. Jeśli podejdziesz do zabezpieczania sieci bezprzewodowej LAN tak, jak do sieci przewodowej, masz większe szanse na ochronę danych korporacyjnych i zasobów sieciowych. Czy zezwoliłbyś użytkownikom na dostęp do zasobów sieciowych tylko dlatego, że podłączyli swoje karty sieciowe do przełącznika lub koncentratora firmy? Oczywiście, że nie. Dlaczego więc miałbyś zezwolić użytkownikom na dostęp do sieci bezprzewodowej LAN tylko dlatego, że mają karty sieciowe WNIC i znają identyfikator SSID firmy? Jeśli firma musi korzystać z technologii bezprzewodowej, Twoim zadaniem jest zapewnienie jej jak największego bezpieczeństwa. Upewnij się, że użytkownicy sieci bezprzewodowej są uwierzytelnieni, zanim uzyskają dostęp do zasobów sieciowych. Oto kilka dodatkowych wskazówek, które pomogą zabezpieczyć sieć bezprzewodową:

• Rozważ użycie oprogramowania antywardrivingowego, aby utrudnić atakującym odkrycie Twojej sieci WLAN. Później w tym kursie dowiesz się o honeypotach, czyli hostach lub sieciach dostępnych publicznie, które kuszą hakerów do atakowania ich zamiast prawdziwej sieci firmy. Personel IT może zbadać, w jaki sposób przeprowadzany jest atak na honeypot, co może być przydatne w zabezpieczeniu rzeczywistej sieci firmy. Aby utrudnić wardriverom odkrycie Twojej sieci WLAN, możesz użyć airbase-ng. Jak sama nazwa wskazuje, ten program tworzy fałszywe punkty dostępowe, co sprawia, że wardriverzy są tak zajęci próbami połączenia się z nieistniejącymi sieciami bezprzewodowymi, że nie mają czasu na odkrycie Twojego legalnego punktu dostępowego.

• Istnieją środki zapobiegające wydostawaniu się fal radiowych z budynku lub wchodzeniu do niego, dzięki czemu z technologii bezprzewodowej mogą korzystać tylko osoby w obiekcie. Jednym z nich jest użycie określonego rodzaju farby na ścianach, ale ta metoda nie jest niezawodna, ponieważ niektóre fale radiowe mogą wyciekać, jeśli farba nie zostanie prawidłowo nałożona.

• Użyj routera, aby zezwolić tylko zatwierdzonym adresom MAC na dostęp do Twojej sieci. Niestety, niektóre exploity umożliwiają atakującym podszywanie się pod autoryzowane adresy, ale ten środek utrudnia typowym atakującym wykorzystanie exploitów.

• Rozważ użycie serwera uwierzytelniania zamiast polegać na urządzeniu bezprzewodowym do uwierzytelniania użytkowników. Serwer RADIUS, który może odsyłać wszystkich użytkowników do serwera z systemem Windows Server z usługą Active Directory, może być używany do uwierzytelniania użytkowników bezprzewodowych próbujących uzyskać dostęp do zasobów sieciowych. Ta metoda może również uniemożliwić intruzowi wysyłanie lub odbieranie pakietów HTTP, HTTPS, DHCP, SMTP lub innych pakietów sieciowych przez sieć przed uwierzytelnieniem.

• Rozważ użycie protokołu EAP, który umożliwia korzystanie z różnych protokołów zwiększających bezpieczeństwo. Na przykład protokół EAP umożliwia korzystanie z certyfikatów do uwierzytelniania, a dostawcy urządzeń bezprzewodowych mogą wdrażać uwierzytelnianie oparte na haśle, korzystając ze standardu EAP. Protokół EAP oferuje więcej opcji zwiększających bezpieczeństwo.

• Rozważ umieszczenie punktu dostępowego w strefie zdemilitaryzowanej (DMZ) i użycie zapory sieciowej przed wewnętrzną siecią firmy, która filtruje ruch z nieautoryzowanych adresów IP.

• WEP z szyfrowaniem 104-bitowym jest tylko nieznacznie lepsze od WEP z szyfrowaniem 40-bitowym. Jeśli to możliwe, zastąp WEP WPA2 lub WPA3 dla lepszego bezpieczeństwa i wymień sprzęt, którego nie można uaktualnić do obsługi WPA2 lub WPA3. Szyfrowanie WEP można łatwo złamać za pomocą samych narzędzi w Kali Linux, a złamanie WPA zajmuje po prostu więcej czasu.

• Przypisz statyczne adresy IP klientom bezprzewodowym zamiast używać DHCP.

• Wyłącz WPS, co usunie znane wektory ataku WPS.

• Zmień domyślny SSID i wyłącz rozgłaszanie SSID, jeśli to możliwe. Jeśli nie możesz wyłączyć rozgłaszania SSID, zmień nazwę domyślnego SSID, aby utrudnić atakującym ustalenie producenta routera. Na przykład pozostawienie domyślnego SSID firmy Netgear ułatwia atakującemu ustalenie, jaki router jest używany. Zmiana jego SSID na domyślny SSID innego producenta lub na taki, który nie jest powiązany z żadnym dostawcą, może odstraszyć atakującego.

Te metody nie są niezawodne. W rzeczywistości, kiedy czytasz tę książkę, mogą istnieć nowe sposoby na złamanie WPA3 i innych metod zabezpieczeń chroniących bezprzewodowe sieci LAN. To właśnie sprawia, że dziedzina bezpieczeństwa jest zabawna i dynamiczna. Nie ma łatwych rozwiązań. Gdyby były, te rozwiązania nie trwałyby długo, niestety.

PODSUMOWANIE MODUŁU

• Technologia bezprzewodowa definiuje, w jaki sposób i na jakiej częstotliwości dane przemieszczają się przez widmo częstotliwości radiowych (RF). Termin „bezprzewodowy” ogólnie opisuje urządzenia działające w widmie RF między 3 Hz a 300 GHz, chociaż większość urządzeń sieciowych bezprzewodowych działa w zakresie od 2,4 GHz do 66 GHz.

• Podstawowymi komponentami sieci bezprzewodowych są karty WNIC, które przesyłają i odbierają sygnały bezprzewodowe; punkty dostępowe (AP), które są mostami między sieciami przewodowymi i bezprzewodowymi; protokoły sieciowe bezprzewodowe; oraz część widma RF, która działa jako medium do przenoszenia sygnału.

• Identyfikator zestawu usług (SSID) jest konfigurowany w AP i służy do identyfikacji sieci WLAN. Jest to unikalna, 1- do 32-znakowa, alfanumeryczna nazwa rozróżniająca wielkość liter.

• Głównym celem IEEE jest tworzenie standardów dla sieci LAN i WAN. 802.11 to standard IEEE dla sieci bezprzewodowych i obejmuje wiele dodatkowych standardów, które dotyczą bezpieczeństwa i uwierzytelniania.

• BSS to zbiór wszystkich urządzeń (punktów dostępowych i stacji), które tworzą sieć WLAN. BSA to obszar zasięgu sieci bezprzewodowej, który punkt dostępowy zapewnia stacjom w sieci WLAN działającej w trybie infrastruktury. Chociaż tryb infrastruktury jest najczęstszy w sieciach WLAN, niezależne stacje mogą również ustanowić zdecentralizowaną sieć ad-hoc, która nie wymaga punktu dostępowego.

• Sieci WLAN wykorzystują trzy technologie: podczerwień, wąskopasmowe i rozproszone widmo. Aby dane mogły być przesyłane przez fale radiowe, muszą być modulowane w sygnale nośnym lub kanale. Najpopularniejszymi metodami modulacji dla rozproszonego widma są DSSS i OFDM.

• Bluetooth to najpopularniejsza forma technologii WPAN (standard 802.15), która zwykle ma bardziej ograniczony zasięg niż typowa sieć WLAN. Na drugim końcu widma znajduje się MAN (standard 802.16), który ma znacznie większy obszar zasięgu niż sieć WLAN. LTE to najczęstsza implementacja bezprzewodowej sieci MAN.

• WEP, WPA, WPA2 i WPA3 to standardy szyfrowania sieci bezprzewodowych stosowane w celu ochrony sieci WLAN przed nieautoryzowanym dostępem i podsłuchem. WEP jest łatwy do złamania, WPA i WPA2 są trudniejsze do złamania, a WPA3 jest najbezpieczniejszy z tych trzech.

• Uwierzytelnianie jest zwykle stosowane ze standardami szyfrowania sieci bezprzewodowych w celu zapewnienia autoryzacji dostępu do sieci WLAN. 802.1X jest przykładem uwierzytelniania sieci WLAN i składa się z trzech komponentów: petenta, użytkownika sieci bezprzewodowej próbującego uzyskać dostęp do sieci WLAN; uwierzytelniacza, punktu dostępowego, który zezwala lub odmawia dostępu petentowi; oraz serwera uwierzytelniającego, takiego jak serwer RADIUS.

• Wardriving i warflying obejmują jazdę samochodem lub pilotowanie drona z urządzeniem komputerowym, kartą sieciową WNIC, anteną i oprogramowaniem, które skanuje dostępne punkty dostępowe.

• Sieci WLAN można atakować wieloma z tych samych narzędzi, które są używane do hakowania przewodowych sieci LAN. Na przykład sniffer, taki jak Wireshark, może skanować sieci WLAN w poszukiwaniu informacji o logowaniu i haśle. Specjalistyczne narzędzia bezprzewodowe obejmują Vistumbler, który może badać punkty dostępowe jako część skanowania wardriving, oraz Kismet, zaawansowane wielofunkcyjne narzędzie bezprzewodowe, które może wykrywać ukryte identyfikatory SSID sieci.

• Niektóre metody ochrony sieci bezprzewodowej to wyłączanie rozgłaszania SSID, zmiana nazw domyślnych identyfikatorów SSID, korzystanie z serwera uwierzytelniania, umieszczanie punktu dostępowego w strefie DMZ, korzystanie z protokołu EAP, uaktualnianie do protokołu WPA3, przypisywanie statycznych adresów IP klientom bezprzewodowym i korzystanie z routera w celu zezwalania na dostęp do sieci tylko zatwierdzonym adresom MAC.