Hakowanie sieci bezprzewodowych

Cele kształcenia

Sieci bezprzewodowe są tańsze i łatwiejsze w utrzymaniu niż sieci przewodowe. Osoba atakująca może łatwo naruszyć sieć bezprzewodową bez odpowiednich środków bezpieczeństwa lub odpowiedniej konfiguracji sieci. Ponieważ mechanizmy wysokiego bezpieczeństwa dla sieci bezprzewodowych mogą być kosztowne, wskazane jest określenie krytycznych źródeł, zagrożeń lub słabych punktów związanych z siecią, a następnie sprawdzenie, czy obecny mechanizm bezpieczeństwa może chronić sieć bezprzewodową przed wszystkimi możliwymi atakami. Jeśli nie, należy zaktualizować mechanizmy bezpieczeństwa. W tym module opisano typy sieci bezprzewodowych, ich mechanizmy bezpieczeństwa, zagrożenia i środki zwalczania zagrożeń w celu zapewnienia bezpieczeństwa sieci. Analizowane są różne algorytmy szyfrowania bezprzewodowego wraz z ich mocnymi i słabymi stronami. Moduł analizuje również techniki ataków na sieci bezprzewodowe i omawia środki zaradcze w celu ochrony systemów informatycznych.

Koncepcje bezprzewodowe

Technologia sieciowa zmierza w kierunku nowej ery ewolucji technologicznej poprzez technologie bezprzewodowe. Sieci bezprzewodowe rewolucjonizują sposób, w jaki ludzie pracują i bawią się. Usuwając fizyczne połączenia lub kable, użytkownicy mogą korzystać z sieci na nowe sposoby, aby dane były przenośne, mobilne i dostępne. Sieć bezprzewodowa to nieograniczony system transmisji danych, który wykorzystuje technologię częstotliwości radiowej do komunikowania się z urządzeniami i uzyskiwania danych. Ta sieć uwalnia użytkownika od skomplikowanych i wielokrotnych połączeń przewodowych wykorzystujących fale elektromagnetyczne (EM) do łączenia dwóch pojedynczych punktów bez ustanawiania jakiegokolwiek połączenia fizycznego. W tej sekcji opisano podstawowe pojęcia dotyczące sieci bezprzewodowych.

Terminologia bezprzewodowa

W sieci bezprzewodowej dane są przesyłane za pomocą fal elektromagnetycznych, które przenoszą sygnały na ścieżce komunikacyjnej. Terminy związane z sieciami bezprzewodowymi obejmują:

Global System for Mobile Communications (GSM): Jest to uniwersalny system służący do mobilnej transmisji danych w sieciach bezprzewodowych na całym świecie.

Przepustowość: opisuje ilość informacji, które mogą być transmitowane przez połączenie. Zwykle przepustowość odnosi się do szybkości przesyłania danych i jest mierzona w bitach (ilość danych) na sekundę (bps).

Punkt dostępowy (AP): Punkt dostępowy służy do łączenia urządzeń bezprzewodowych z siecią bezprzewodową/przewodową. Umożliwia bezprzewodowym urządzeniom komunikacyjnym łączenie się z siecią bezprzewodową za pośrednictwem standardów bezprzewodowych, takich jak Bluetooth i Wi-Fi. Służy jako przełącznik lub koncentrator między przewodową siecią LAN a siecią bezprzewodową.

Identyfikator podstawowego zestawu usług (BSSID): Jest to adres kontroli dostępu do mediów (MAC) punktu dostępowego (AP) lub stacji bazowej, która skonfigurowała podstawowy zestaw usług (BSS). Na ogół użytkownicy nie są świadomi BSS, do którego należą. Kiedy użytkownik przenosi urządzenie, BSS używany przez urządzenie może się zmienić z powodu zmiany zasięgu objętego przez AP, ale ta zmiana może nie wpłynąć na łączność urządzenia bezprzewodowego.

Pasmo przemysłowe, naukowe i medyczne (ISM): To pasmo to zestaw częstotliwości używanych przez międzynarodowe społeczności przemysłowe, naukowe i medyczne.

Hotspot: Są to miejsca, w których sieci bezprzewodowe są dostępne do użytku publicznego. Hotspoty to obszary z dostępem do Wi-Fi, w których użytkownicy mogą włączyć Wi-Fi na swoich urządzeniach i połączyć się z Internetem.

• Powiązanie: odnosi się do procesu łączenia urządzenia bezprzewodowego z punktem dostępowym.

• Identyfikator zestawu usług (SSID): Identyfikator SSID to unikalny identyfikator składający się z 32 znaków alfanumerycznych nadawany bezprzewodowej sieci lokalnej (WLAN), który działa jako bezprzewodowy identyfikator sieci. Identyfikator SSID umożliwia połączenia z wybraną siecią wśród dostępnych niezależnych sieci. Urządzenia łączące się z tą samą siecią WLAN powinny używać tego samego identyfikatora SSID do nawiązywania połączeń.

Multipleksowanie z ortogonalnym podziałem częstotliwości (OFDM): OFDM to metoda cyfrowej modulacji danych, w której sygnał o wybranej częstotliwości jest dzielony na wiele częstotliwości nośnych, które są ortogonalne (występują pod kątem prostym) względem siebie. OFDM odwzorowuje informacje o zmianach fazy nośnej, częstotliwości, amplitudy lub ich kombinacji i dzieli szerokość pasma z innymi niezależnymi kanałami. Tworzy schemat transmisji, który obsługuje wyższe przepływności niż praca w kanale równoległym. Jest to również metoda kodowania danych cyfrowych na wielu częstotliwościach nośnych.

Wiele wejść, wiele wyjść - multipleksowanie z ortogonalnym podziałem częstotliwości (MIMOOFDM):

MIMO-OFDM wpływa na wydajność widmową usług komunikacji bezprzewodowej 4G i 5G. Przyjęcie techniki MIMO-OFDM zmniejsza zakłócenia i zwiększa odporność kanału.

Widmo rozproszone z sekwencją bezpośrednią (DSSS): DSSS to technika widma rozproszonego, która mnoży oryginalny sygnał danych za pomocą pseudolosowego kodu rozpraszającego szum. Nazywana również schematem transmisji danych lub schematem modulacji, technika ta chroni sygnały przed zakłóceniami lub zagłuszaniem.

Rozproszone widmo z przeskakiwaniem częstotliwości (FHSS): FHSS, znane również jako wielodostęp z podziałem kodowym z przeskakiwaniem częstotliwości (FH-CDMA), to metoda transmisji sygnałów radiowych poprzez szybkie przełączanie nośnej między wieloma kanałami częstotliwości. Zmniejsza to skuteczność nieautoryzowanego przechwytywania lub zakłócania łączności telekomunikacyjnej. W FFISS nadajnik przeskakuje między dostępnymi częstotliwościami przy użyciu określonego algorytmu w pseudolosowej sekwencji znanej zarówno nadawcy, jak i odbiorcy.

Sieci bezprzewodowe

Sieci bezprzewodowe wykorzystują transmisję fal radiowych, która zwykle występuje w warstwie fizycznej struktury sieci. Wraz z globalną rewolucją w komunikacji bezprzewodowej fundamentalne zmiany zachodzą w sieciach danych i telekomunikacji. Wi-Fi odnosi się do sieci WLAN opartej na standardzie IEEE 802.11 i umożliwia urządzeniu dostęp do sieci z dowolnego miejsca w zasięgu punktu dostępowego. Wi-Fi to szeroko stosowana technologia w komunikacji bezprzewodowej w kanale radiowym. Wi-Fi wykorzystuje liczne techniki, takie jak DSSS, FHSS, podczerwień (IR) i OFDM, aby ustanowić połączenie między nadajnikiem a odbiornikiem. Urządzenia, takie jak komputery osobiste, konsole do gier wideo i smartfony, wykorzystują Wi-Fi do łączenia się z zasobami sieciowymi, takimi jak Internet, za pośrednictwem punktu dostępu sieci bezprzewodowej. Oto niektóre zalety i wady sieci bezprzewodowych:

Zalety

o Instalacja jest szybka i łatwa bez konieczności prowadzenia okablowania przez ściany i sufity

o Łatwo zapewnia łączność w obszarach, w których trudno jest położyć kable

o Dostęp do sieci można uzyskać z dowolnego miejsca w zasięgu punktu dostępowego

o Przestrzenie publiczne, takie jak lotniska, biblioteki, szkoły, a nawet kawiarnie oferują stałe połączenia z Internetem za pośrednictwem sieci WLAN

Wady

o Bezpieczeństwo może nie spełniać oczekiwań

o Przepustowość spada wraz ze wzrostem liczby urządzeń w sieci

o Aktualizacje Wi-Fi mogą wymagać nowych kart bezprzewodowych i/lub punktów dostępowych

o Niektóre urządzenia elektroniczne mogą zakłócać działanie sieci Wi-Fi

Rodzaje sieci bezprzewodowych

Poniżej opisano różne typy sieci bezprzewodowych.

Rozszerzenie do sieci przewodowej

Użytkownik może rozszerzyć sieć przewodową, umieszczając punkty dostępowe między siecią przewodową a urządzeniami bezprzewodowymi. Sieć bezprzewodową można również utworzyć za pomocą punktu dostępowego. Typy punktów dostępowych obejmują:

o Oprogramowanie AP (SAP): SAP można podłączyć do sieci przewodowej i uruchomić na komputerze wyposażonym w bezprzewodową kartę sieciową (NIC).

o Sprzętowe punkty dostępowe (HAP): punkty dostępowe obsługują większość funkcji bezprzewodowych.

W tego typu sieciach punkt dostępowy działa jak przełącznik, zapewniając łączność komputerowi korzystającemu z bezprzewodowej karty sieciowej. Punkt dostępowy może łączyć klientów bezprzewodowych z przewodową siecią LAN, co umożliwia bezprzewodowy dostęp do zasobów sieci LAN, takich jak serwery plików i połączenia internetowe.

Wiele punktów dostępu

Ten typ sieci łączy komputery bezprzewodowo przy użyciu wielu punktów dostępowych. Jeśli pojedynczy punkt dostępowy nie może pokryć obszaru, można ustanowić wiele punktów dostępowych lub punktów rozszerzeń. Obszar bezprzewodowy każdego punktu dostępowego musi pokrywać się z obszarem sąsiada. Zapewnia to użytkownikom możliwość płynnego poruszania się za pomocą funkcji zwanej roamingiem. Niektórzy producenci opracowują punkty rozszerzeń, które działają jak przekaźniki bezprzewodowe, zwiększając zasięg pojedynczego punktu dostępowego. Wiele punktów rozszerzeń można połączyć ze sobą, aby zapewnić bezprzewodowy dostęp do lokalizacji oddalonych od centralnego punktu dostępowego.

Sieć bezprzewodowa LAN-to-LAN

Punkty dostępowe zapewniają łączność bezprzewodową z komputerami lokalnymi, a komputery lokalne w różnych sieciach mogą być ze sobą połączone. Wszystkie sprzętowe punkty dostępowe mają możliwość łączenia się z innymi sprzętowymi punktami dostępowymi. Jednak łączenie sieci LAN za pośrednictwem połączeń bezprzewodowych jest złożonym zadaniem.

Hotspot 3G/4G

Hotspot 3G/4G to rodzaj sieci bezprzewodowej, która zapewnia dostęp Wi-Fi do urządzeń Wi-Fienabled, w tym odtwarzaczy MP3, notebooków, tabletów, aparatów fotograficznych, palmtopów, netbooków i innych.

Standardy bezprzewodowe

Standard IEEE 802.11 ewoluował od standardu podstawowego rozszerzenia bezprzewodowego do przewodowej sieci LAN do dojrzałego protokołu obsługującego uwierzytelnianie korporacyjne, silne szyfrowanie i jakość usług. Wprowadzony w 1997 r. standard WLAN określał działanie z szybkością 1 i 2 Mb/s w zakresie podczerwieni, jak również w nielicencjonowanym paśmie częstotliwości ISM (przemysłowym, naukowym i medycznym) 2,4 GHz. Na początku sieć 802.11 składała się z kilku komputerów PC z funkcją łączności bezprzewodowej podłączonych do sieci LAN Ethernet (IEEE 802.3) za pośrednictwem jednego sieciowego punktu dostępowego. Obecnie sieci 802.11 działają ze znacznie wyższymi prędkościami iw dodatkowych pasmach. Pojawiły się nowe problemy, takie jak bezpieczeństwo, roaming między wieloma punktami dostępowymi i jakość usług. Zmiany w standardzie są oznaczone literami alfabetu pochodzącymi od grup zadaniowych 802.11, które stworzyły ten chem.

802.11: Standard 802.11 (Wi-Fi) dotyczy sieci WLAN i wykorzystuje FHSS lub DSSS jako widmo z przeskokiem częstotliwości. Pozwala urządzeniu elektronicznemu nawiązać połączenie bezprzewodowe w dowolnej sieci.

802.11a: Jest to pierwsza poprawka do pierwotnego standardu 802.11. Standard 802.11 działa w paśmie częstotliwości 5 GHz i obsługuje przepustowości do 54 Mb/s przy użyciu multipleksowania z ortogonalnym podziałem częstotliwości (OFDM). Ma wysoką prędkość maksymalną, ale jest stosunkowo bardziej wrażliwy na ściany i inne przeszkody.

802.11b: IEEE rozszerzyło standard 802.11, tworząc w 1999 r. specyfikację 802.11b. Ten standard działa w paśmie ISM 2,4 GHz i obsługuje przepustowości do 11 Mb/s przy użyciu modulacji DSSS (Direct-Sequence Spread Spectrum).

802.lid: Standard 802.lid to udoskonalona wersja 802.11a i 802.11b obsługująca domeny regulacyjne. Specyfikacje tego standardu można ustawić w warstwie kontroli dostępu do mediów (MAC).

IEEE 802.11e: jest używany w aplikacjach czasu rzeczywistego, takich jak głos, VoIP i wideo. Aby zapewnić tym wrażliwym czasowo aplikacjom zasoby sieciowe, których potrzebują, 802.lie definiuje mechanizmy zapewniające jakość usług (QoS) w warstwie 2 modelu referencyjnego, czyli warstwie MAC.

802.11g: Jest to rozszerzenie standardu 802.11 i obsługuje maksymalną przepustowość 54 Mb/s przy użyciu technologii OFDM. Wykorzystuje to samo pasmo 2,4 GHz co standard 802.11b. Standard IEEE 802.llg definiuje szybkie rozszerzenia 802.11b i jest zgodny ze standardem 802.11b, co oznacza, że urządzenia 802.11b mogą współpracować bezpośrednio z punktem dostępowym 802.11g.

802.11i: Standard IEEE 802.lli zwiększa bezpieczeństwo sieci WLAN poprzez wdrożenie nowych protokołów szyfrowania, takich jak Temporal Key Integrity Protocol (TKIP) i Advanced Encryption Standard (AES).

802.11n: IEEE 802.lln to wersja rozszerzająca standard 802.11g o wielowejściowe anteny wielowyjściowe (MIMO). Działa zarówno w paśmie 2,4 GHz, jak i 5 GHz. Ponadto jest to branżowy standard IEEE dla transportu bezprzewodowej sieci lokalnej Wi-Fi. Digital Audio Broadcasting (DAB) i

WLAN wykorzystują OFDM, obsługuje komunikację Internet of Things (loT) z wyższymi szybkościami transmisji danych i szerszym zasięgiem niż poprzednie standardy.

802.11ac: Zapewnia sieć o wysokiej przepustowości na częstotliwości 5 GHz. Jest szybszy i bardziej niezawodny niż standard 802.lln. Ponadto obejmuje sieć Gigabit, która zapewnia natychmiastowe przesyłanie danych.

802.11ad: Standard 802.llad zawiera nową warstwę fizyczną dla sieci 802.11 i działa w paśmie 60 GHz. Szybkość propagacji danych w tym standardzie jest znacznie większa niż w standardach działających w paśmie 2,4 GHz i 5 GHz, takich jak 802.11n.

802.12: Wykorzystanie mediów jest zdominowane przez ten standard, ponieważ działa na protokole priorytetu żądania. Szybkość Ethernetu w tym standardzie wynosi 100 Mb/s. Ponadto jest kompatybilny ze standardami 802.3 i 802.5. Użytkownicy korzystający obecnie z tych standardów mogą bezpośrednio przejść na standard 802.12.

802.15: Określa standardy bezprzewodowej sieci osobistej (WPAN) i opisuje specyfikacje łączności bezprzewodowej z urządzeniami stacjonarnymi lub przenośnymi.

802.15.1 (Bluetooth): Bluetooth jest używany głównie do wymiany danych na krótkie odległości na urządzeniach stacjonarnych lub mobilnych. Ten standard działa w paśmie 2,4 GHz.

802.15.4 (ZigBee): Standard 802.15.4 charakteryzuje się niską szybkością transmisji danych i złożonością. Specyfikacją używaną w tym standardzie jest ZigBee, przesyłanie danych na duże odległości przez sieć kratową. Specyfikacja obsługuje aplikacje o niskiej przepustowości 250 Kb/s, ale jej użycie zwiększa żywotność baterii.

802.15.5: Ten standard jest wdrażany w topologii pełnej lub połowicznej siatki. Obejmuje inicjalizację sieci, adresowanie i emisję pojedynczą.

802.16: Standard IEEE 802.16 to standard komunikacji bezprzewodowej zaprojektowany w celu zapewnienia wielu opcji warstwy fizycznej (PHY) i MAC, jest również znany jako WiMax. Ten standard jest specyfikacją dla stacjonarnych szerokopasmowych bezprzewodowych sieci dostępu metropolitalnego (MAN), które wykorzystują architekturę punkt-wielopunkt.

Identyfikator zestawu usług (SSID)

Identyfikator zestawu usług (SSID) jest rozróżnianym wielkością liter, czytelnym dla człowieka unikalnym identyfikatorem sieci WLAN o długości 32 znaków alfanumerycznych. SSID to token używany do identyfikowania i lokalizowania sieci 802.11 (Wi-Fi). Domyślnie jest to część nagłówka ramki pakietów wysyłanych przez sieć WLAN. Działa jako pojedynczy wspólny identyfikator między punktami dostępowymi a klientami. Pomaga to użytkownikom zlokalizować punkt dostępowy, z którym mogą podjąć kolejną próbę uwierzytelnienia i połączenia ASSOC. Wątpliwości dotyczące bezpieczeństwa pojawiają się, gdy użytkownik nie zmienia wartości domyślnych, ponieważ jednostki te można łatwo złamać. Punkty dostępowe SSID odpowiadają na żądania sondy odpowiedziami sondy, które obejmują również sam identyfikator SSID, jeśli nie jest on ukryty. Ponieważ identyfikator SSID jest unikalnym identyfikatorem sieci WLAN, wszystkie urządzenia i punkty dostępowe w sieci WLAN muszą używać tego samego identyfikatora SSID. Każde urządzenie, które próbuje dołączyć do sieci WLAN, musi podać identyfikator SSID. Ponieważ każdy użytkownik w sieci musi skonfigurować identyfikator SSID w ustawieniach sieci swojego systemu, w przypadku zmiany identyfikatora SSID sieci administrator sieci musi ponownie skonfigurować identyfikator SSID na każdym kliencie. Tryb dostępu niezabezpieczonego umożliwia klientom łączenie się z punktem dostępowym przy użyciu

skonfigurowanego identyfikatora SSID, pustego identyfikatora SSID lub identyfikatora SSID skonfigurowanego jako „dowolny”. Niestety SSID nie zapewnia bezpieczeństwa sieci WLAN, ponieważ łatwo jest uzyskać SSID jako zwykły tekst z pakietów. W przypadku wielu produktów komercyjnych domyślnym identyfikatorem SSID jest nazwa dostawcy. SSID można zachować w tajemnicy tylko w zamkniętych sieciach bez aktywności, co jest niewygodne dla legalnych użytkowników.

Tryby uwierzytelniania Wi-Fi

Tryby, które przeprowadzają uwierzytelnianie Wi-Fi, obejmują uwierzytelnianie otwartego systemu i uwierzytelnianie za pomocą klucza współdzielonego.

Proces uwierzytelniania systemu otwartego: w tym procesie każdy klient bezprzewodowy, który próbuje uzyskać dostęp do sieci Wi-Fi, wysyła żądanie uwierzytelnienia do bezprzewodowego punktu dostępowego. W tym procesie stacja wysyła ramkę zarządzania uwierzytelnianiem zawierającą tożsamość stacji wysyłającej w celu uwierzytelnienia i połączenia z inną stacją bezprzewodową, którą jest bezprzewodowy punkt dostępowy. Następnie punkt AP zwraca ramkę uwierzytelnienia, aby potwierdzić dostęp do żądanej stacji, kończąc w ten sposób proces uwierzytelniania.

802.11ah: Nazywany również Wi-Fi HaLow, wykorzystuje pasma 900 MHz dla sieci Wi-Fi o rozszerzonym zasięgu i proces uwierzytelniania za pomocą klucza współdzielonego: w tym procesie każda stacja bezprzewodowa otrzymuje wspólny tajny klucz przez bezpieczny kanał, który różni się od standardu 802.11 kanały komunikacji sieci bezprzewodowej. Poniższe kroki ilustrują ustanowienie połączenia w procesie uwierzytelniania za pomocą klucza współdzielonego:

Stacja wysyła do AP ramkę uwierzytelniającą.

Punkt dostępowy wysyła tekst wyzwania do stacji.

Stacja szyfruje tekst wyzwania przy użyciu skonfigurowanego klucza 64-bitowego lub 128-bitowego i wysyła zaszyfrowany tekst do punktu dostępowego.

Punkt dostępowy używa skonfigurowanego na przykład klucza Wired Equivalent Privacy (WEP) do odszyfrowania zaszyfrowanego tekstu. AP porównuje odszyfrowany tekst z oryginalnym tekstem wyzwania. Jeśli pasują, AP uwierzytelnia stację.

Stacja łączy się z siecią.

AP może odrzucić stację, jeśli odszyfrowany tekst nie pasuje do oryginalnego tekstu wezwania; wówczas stacja nie będzie mogła komunikować się ani z siecią Ethernet, ani z sieciami 802.11.

Proces uwierzytelniania Wi-Fi przy użyciu scentralizowanego serwera uwierzytelniania

Standard 802.IX zapewnia scentralizowane uwierzytelnianie. Aby uwierzytelnianie 802.IX działało w sieci bezprzewodowej, punkt dostępowy musi być w stanie bezpiecznie identyfikować ruch generowany przez określonego klienta bezprzewodowego. W tym procesie uwierzytelniania Wi-Fi scentralizowany serwer uwierzytelniania znany jako Usługa RADIUS (Remote Authentication Dial-in User Service) wysyła klucze uwierzytelniające zarówno do punktu dostępowego, jak i klientów, którzy próbują uwierzytelnić się w punkcie dostępowym. Ten klucz umożliwia punktowi dostępowemu identyfikację określonego klienta bezprzewodowego.

Rodzaje anten bezprzewodowych

Anteny są integralną częścią sieci Wi-Fi. Oprócz wysyłania i odbierania sygnałów radiowych przetwarzają impulsy elektryczne na sygnały radiowe i odwrotnie. Rodzaje anten bezprzewodowych obejmują:

Antena kierunkowa

Antena kierunkowa może nadawać i odbierać fale radiowe z jednego kierunku. Aby poprawić transmisję i odbiór, konstrukcja anteny kierunkowej umożliwia jej efektywną pracę tylko w kilku kierunkach. Pomaga to również w zmniejszeniu zakłóceń.

Antena dookólna

Anteny dookólne emitują energię elektromagnetyczną (EM) we wszystkich kierunkach. Zapewnia poziomą charakterystykę promieniowania 360°. Wypromieniowują silne fale równomiernie w dwóch wymiarach, ale fale zwykle nie są tak silne w trzecim wymiarze. Anteny te są wydajne w obszarach, w których stacje bezprzewodowe wykorzystują technologię wielodostępu z podziałem czasu. Dobrym przykładem anteny dookólnej jest antena używana przez stacje radiowe. Anteny te są skuteczne w transmisji sygnału radiowego, ponieważ odbiornik nie może być nieruchomy. Dlatego radioodbiornik może odbierać sygnał niezależnie od jego lokalizacji.

Antena siatkowa paraboliczna

Paraboliczna antena siatkowa działa na tej samej zasadzie, co antena satelitarna, ale nie ma solidnej anteny. Składa się z półtalerza w formie siatki składającej się z aluminiowych drutów. Paraboliczne anteny siatkowe mogą osiągać transmisje Wi-Fi na bardzo duże odległości dzięki wysoce skupionym wiązkom radiowym. Ten typ anteny jest przydatny do przesyłania słabych sygnałów radiowych na bardzo duże odległości rzędu 10 mil. Umożliwia to atakującym uzyskanie lepszej jakości sygnału, co skutkuje większą ilością danych do podsłuchania, większą przepustowością do nadużyć i wyższą mocą wyjściową, co jest niezbędne w przypadku odmowy usługi warstwy 1 (DoS) i man-in-the -środkowe (MITM) ataki. Konstrukcja tej anteny oszczędza wagę i miejsce oraz może odbierać sygnały Wi-Fi spolaryzowane poziomo lub pionowo.

Antena Yagi

Antena Yagi, zwana także anteną Yagi-Uda, jest anteną jednokierunkową powszechnie używaną w komunikacji w paśmie częstotliwości 10 MHz do VHF i UHF. Ta antena ma wysoki zysk i niski stosunek sygnału do szumu (SNR) dla sygnałów radiowych. Co więcej, nie tylko ma jednokierunkowy wzór promieniowania i odpowiedzi, ale także koncentruje promieniowanie i odpowiedź. Składa się z reflektora, dipola i wielu direktorów. Ta antena rozwija wzór promieniowania końcowego ognia.

Antena dipolowa

Antena dipolowa jest prostym przewodnikiem elektrycznym o długości połowy długości fali od końca do końca i jest podłączona w środku linii zasilającej o częstotliwości radiowej (RF). Antena, zwana także dubletem, jest dwustronnie symetryczna; dlatego jest to z natury antena zbalansowana. Ten rodzaj anteny zasila zbalansowaną linię transmisyjną RF o równoległym przewodzie.

Anteny odblaskowe

Anteny reflektorowe służą do skupiania energii EM, która jest emitowana lub odbierana w punkcie centralnym. Reflektory te są na ogół paraboliczne. Jeśli powierzchnia anteny parabolicznej mieści się w granicach tolerancji, może być używana jako zwierciadło główne dla wszystkich częstotliwości. Może to zapobiec zakłóceniom podczas komunikacji z innymi satelitami. Większy reflektor anteny pod

względem wielokrotności długości fali skutkuje większym zyskiem. Anteny reflektorowe odbijają sygnały radiowe i mają wysoki koszt produkcji.

Szyfrowanie bezprzewodowe

Szyfrowanie sieci bezprzewodowej to proces ochrony sieci bezprzewodowej przed atakującymi, którzy próbują zebrać poufne informacje poprzez naruszenie ruchu radiowego. Ta sekcja zawiera wgląd w różne standardy szyfrowania sieci bezprzewodowych, takie jak Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), WPA2 i WPA3, a także problemy z WEP, WPA i WPA2.

Rodzaje szyfrowania bezprzewodowego

Ataki na sieci bezprzewodowe rosną z dnia na dzień wraz ze wzrostem wykorzystania sieci bezprzewodowych. Szyfrowanie informacji przed ich przesłaniem w sieci bezprzewodowej jest najpopularniejszą metodą zabezpieczania sieci bezprzewodowych przed atakami. Istnieje kilka rodzajów algorytmów szyfrowania sieci bezprzewodowej, które mogą zabezpieczyć sieć bezprzewodową. Każdy algorytm szyfrowania sieci bezprzewodowej ma zalety i wady.

802.Hi: Jest to poprawka IEEE określająca mechanizmy bezpieczeństwa dla sieci bezprzewodowych 802.11.

WEP: WEP to algorytm szyfrowania dla sieci bezprzewodowych IEEE 802.11. Jest to stary standard bezpieczeństwa sieci bezprzewodowej i można go łatwo złamać.

EAP: Protokół Extensible Authentication Protocol (EAP) obsługuje wiele metod uwierzytelniania, takich jak karty tokenowe, protokół Kerberos i certyfikaty.

LEAP: Lightweight EAP (LEAP) to zastrzeżona wersja protokołu EAP opracowana przez firmę Cisco.

WPA: Jest to zaawansowany bezprzewodowy protokół szyfrowania wykorzystujący TKIP i Message Integrity Check (MIC) w celu zapewnienia silnego szyfrowania i uwierzytelniania. Wykorzystuje 48-bitowy wektor inicjalizacji (IV), 32-bitową cykliczną kontrolę redundancji (CRC) i szyfrowanie TKIP dla bezpieczeństwa sieci bezprzewodowej.

TKIP: Jest to protokół bezpieczeństwa używany w WPA jako zamiennik dla WEP.

WPA2: Jest to uaktualnienie do WPA przy użyciu AES i protokołu CCMP (Cipher Mode Cipher Block Chaining Message Authentication Code Authentication) w trybie licznika do bezprzewodowego szyfrowania danych.

AES: Jest to szyfrowanie z kluczem symetrycznym używane w WPA2 jako zamiennik dla TKIP.

CCMP: Jest to protokół szyfrowania używany w WPA2 do silnego szyfrowania i uwierzytelniania.

WPA2 Enterprise: integruje standardy EAP z szyfrowaniem WPA2.

RADIUS: Jest to scentralizowany system uwierzytelniania i zarządzania autoryzacjami.

PEAP: Jest to protokół, który hermetyzuje EAP w zaszyfrowanym i uwierzytelnionym tunelu Transport Layer Security (TLS).

WPA3: Jest to protokół bezpieczeństwa Wi-Fi trzeciej generacji, który zapewnia nowe funkcje do użytku osobistego i korporacyjnego. Wykorzystuje Galois/Counter Mode-256 (GCMP-256) do szyfrowania i 384-bitowy kod uwierzytelniania wiadomości hash z algorytmem Secure Hash Algorithm (HMAC-SHA-384) do uwierzytelniania.

Szyfrowanie równoważne prywatności przewodowej (WEP).

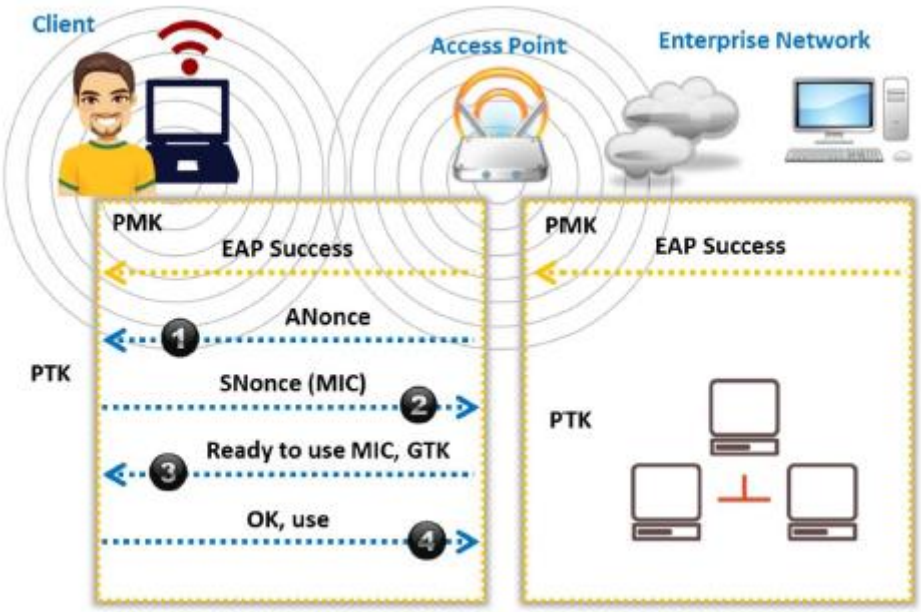
WEP był wczesną próbą ochrony sieci bezprzewodowych przed naruszeniami bezpieczeństwa, ale wraz z rozwojem technologii stało się oczywiste, że informacje zaszyfrowane przy użyciu WEP są podatne na ataki. Szczegółowo omawiamy tutaj WEP.

Co to jest szyfrowanie WEP?

WEP jest składnikiem standardów IEEE 802.11 WLAN. Jego podstawowym celem jest zapewnienie poufności danych w sieciach bezprzewodowych na poziomie równoważnym z przewodowymi sieciami LAN, z których można korzystać z zabezpieczenia fizycznego zapobiegającego nieautoryzowanemu dostępowi do sieci. W sieci WLAN użytkownik lub osoba atakująca może uzyskać dostęp do sieci bez fizycznego łączenia się z siecią LAN. Dlatego WEP wykorzystuje mechanizm szyfrowania w warstwie łącza danych w celu zminimalizowania nieautoryzowanego dostępu do sieci WLAN. Osiąga się to poprzez szyfrowanie danych za pomocą symetrycznego algorytmu szyfrowania Rivest Cipher 4 (RC4), który jest mechanizmem kryptograficznym używanym do obrony przed zagrożeniami.

TKIP: Jest używany w kluczu szyfrowania emisji pojedynczej, który zmienia się dla każdego pakietu, zwiększając w ten sposób bezpieczeństwo. Ta zmiana klucza dla każdego pakietu jest automatycznie koordynowana między klientem bezprzewodowym a punktem dostępowym. TKIP używa algorytmu Michael Integrity Check z kluczem MIC do generowania wartości MIC. Wykorzystuje szyfrowanie strumieniowe RC4 z 128-bitowymi kluczami i 64-bitową kontrolę integralności MIC. Zmniejsza podatność na zagrożenia, zwiększając rozmiar IV i używając funkcji mieszania. W TKIP klient zaczyna od 128-bitowego klucza czasowego (TK), który jest następnie łączony z adresem MAC klienta i IV w celu utworzenia strumienia klucza, który jest używany do szyfrowania danych przez RC4. Implementuje licznik sekwencji w celu ochrony przed atakami powtórek. TKIP ulepsza WEP, dodając mechanizm zmiany klucza, aby zapewnić świeże klucze szyfrowania i integralności. TK są zmieniane co 10 000 pakietów, co sprawia, że sieci chronione TKIP są bardziej odporne na ataki kryptoanalityczne polegające na ponownym użyciu klucza.

TK: Wszystkie nowo wdrożone urządzenia Wi-Fi używają szyfrowania TKIP (dla WPA) lub AES (dla WPA2), aby zapewnić bezpieczeństwo sieci WLAN. W mechanizmie szyfrowania WEP protokół uzyskuje klucze szyfrujące (TK) z pary kluczy głównych (PMK), który jest tworzony podczas sesji uwierzytelniania EAP, natomiast w mechanizmach szyfrowania WPA i WPA2 protokół uzyskuje klucze szyfrujące w ciągu czterech - sposób uścisk dłoni. W komunikacie o sukcesie EAP PMK jest wysyłany do punktu dostępowego, ale nie jest kierowany do klienta Wi-Fi, ponieważ uzyskał on własną kopię PMK. Poniższy rysunek przedstawia procedurę instalacji TK.



o AP wysyła ANonce do klienta, który używa go do skonstruowania parami klucza przejściowego (PTK).

o Klient odpowiada z własną wartością Nonce (SNonce) do AP wraz z MIC.

o AP wysyła grupowy klucz czasowy (GTK) i numer sekwencyjny wraz z innym MIC, który jest używany w następnych ramkach rozgłoszeniowych.

o Klient potwierdza, że klucze tymczasowe są zainstalowane.

Jak działa WPA

TK, adres transmisji i licznik sekwencji TKIP (TSC) są używane jako dane wejściowe algorytmu RC4 do generowania strumienia klucza.

Sekwencja IV lub TK, adres transmisji lub docelowy adres MAC oraz TK są łączone z funkcją mieszania lub funkcją mieszania w celu wygenerowania 128-bitowego i 104-bitowego klucza.

Ten klucz jest następnie łączony z RC4 w celu utworzenia strumienia klucza, który powinien mieć taką samą długość jak oryginalna wiadomość.

Jednostka danych usługi MAC (MSDU) i kontrola integralności wiadomości (MIC) są połączone przy użyciu algorytmu Michaela.

Kombinacja MSDU i MIC jest pofragmentowana w celu wygenerowania jednostki danych protokołu MAC (MPDU).

32-bitowe ICV jest obliczane dla MPDU.

Kombinacja MPDU i ICV jest bitowo XORowana ze strumieniem klucza w celu wytworzenia zaszyfrowanych danych.

IV jest dodawany do zaszyfrowanych danych w celu wygenerowania ramki MAC.

Szyfrowanie WPA2

Wi-Fi Protected Access 2 (WPA2) to protokół bezpieczeństwa używany do zabezpieczania sieci bezprzewodowych. WPA2 zastąpił WPA w 2006 roku. Jest zgodny ze standardem 802.Hi i obsługuje wiele funkcji bezpieczeństwa, których nie obsługuje WPA. WPA2 wprowadza użycie algorytmu szyfrowania AES zgodnego ze standardem FIPS 140-2 Narodowego Instytutu Standardów i Technologii (NIST), który jest silnym algorytmem szyfrowania bezprzewodowego, oraz protokołu CCMP (Counter Mode Cipher Block Chaining Message Authentication Code). Zapewnia lepszą ochronę danych i kontrolę dostępu do sieci niż WPA. Ponadto zapewnia wysoki poziom bezpieczeństwa połączeń Wi-Fi, dzięki czemu dostęp do sieci mają tylko upoważnieni użytkownicy.

Tryby działania

WPA2 oferuje dwa tryby działania:

WPA2-Personal: WPA2-Personal używa ustawionego wcześniej hasła, zwanego kluczem wstępnym (PSK), w celu ochrony nieautoryzowanego dostępu do sieci. Każde urządzenie bezprzewodowe używa tego samego 256-bitowego klucza wygenerowanego na podstawie hasła do uwierzytelnienia w punkcie dostępowym. W trybie PSK każde urządzenie sieci bezprzewodowej szyfruje ruch sieciowy za pomocą 128-bitowego klucza pochodzącego z hasła o długości od 8 do 63 znaków ASCII. Router wykorzystuje kombinację hasła, identyfikatora SSID sieci i TKIP do wygenerowania unikalnego klucza szyfrowania dla każdego klienta bezprzewodowego. Te klucze szyfrowania zmieniają się w sposób ciągły.

WPA2-Enterprise: WPA2-Enterprise używa EAP lub RADIUS do scentralizowanego uwierzytelniania klientów przy użyciu wielu metod uwierzytelniania, takich jak karty tokenowe, Kerberos i certyfikaty. WPA-Enterprise przypisuje unikalny zaszyfrowany klucz do każdego systemu i ukrywa go przed użytkownikiem, aby zapewnić dodatkowe bezpieczeństwo i zapobiec udostępnianiu

Jak działa WPA2

Podczas implementacji CCMP dodatkowe dane uwierzytelniające (AAD) są generowane przy użyciu nagłówka MAC i są uwzględniane w procesie szyfrowania, który wykorzystuje zarówno szyfrowanie AES, jak i CCMP. W rezultacie niezaszyfrowana część ramki jest chroniona przed wszelkimi zmianami lub zniekształceniami. Protokół wykorzystuje sekwencyjny numer pakietu (PN) i część nagłówka MAC do wygenerowania wartości jednorazowej, której używa w procesie szyfrowania. Protokół zapewnia dane w postaci zwykłego tekstu, a klucze czasowe, AAD i Nonce są używane jako dane wejściowe w procesie szyfrowania danych, który wykorzystuje zarówno algorytmy AES, jak i CCMP. PN jest zawarty w nagłówku CCMP w celu ochrony przed atakami powtórkowymi. Wynikowe dane z algorytmów AES i CCMP tworzą zaszyfrowany tekst i zaszyfrowaną wartość MIC. Wreszcie złożony nagłówek MAC, nagłówek CCMP, zaszyfrowane dane i zaszyfrowany MIC tworzą ramkę WPA2 MAC. Poniższy rysunek przedstawia przepływ operacyjny WPA2.

Szyfrowanie WPA3

Wi-Fi Protected Access 3 (WPA3) został ogłoszony przez Wi-Fi Alliance w styczniu 2018 roku jako zaawansowana implementacja WPA2, która zapewnia pionierskie protokoły. Podobnie jak WPA2, protokół WPA3 ma dwa warianty: WPA3-Personal i WPA3-Enterprise. WPA3 zapewnia najnowocześniejsze funkcje upraszczające bezpieczeństwo Wi-Fi i zapewnia możliwości niezbędne do obsługi różnych wdrożeń sieci, od sieci korporacyjnych po sieci domowe. Zapewnia również spójność kryptograficzną przy użyciu algorytmów szyfrowania, takich jak AES i TKIP, w celu obrony przed atakami sieciowymi. Ponadto zapewnia odporność sieci dzięki chronionym ramkom zarządzania (PMF), które

zapewniają wysoki poziom ochrony przed podsłuchiwaniem i atakami fałszerstwa. WPA3 nie zezwala również na przestarzałe starsze protokoły.

Tryby działania

WPA3 oferuje dwa tryby działania:

WPA3-Personal: Ten tryb jest używany głównie do uwierzytelniania opartego na haśle. WPA3 jest bardziej odporny na ataki niż WPA2, ponieważ wykorzystuje nowoczesny protokół ustanawiania klucza o nazwie Simultaneous Authentication of Equals (SAE), znany również jako Dragonfly Key Exchange, który zastępuje koncepcję PSK stosowaną w WPA2-Personal. Poniżej opisano niektóre funkcje WPA3-Personal.

Odporność na ataki słownikowe w trybie offline: Zapobiega pasywnym atakom na hasła, takim jak brute-force.

Odporność na odzyskanie klucza: nawet po ustaleniu hasła nie jest możliwe przechwycenie i ustalenie kluczy sesyjnych przy jednoczesnym zachowaniu poufności ruchu sieciowego.

Naturalny wybór hasła: Pozwala użytkownikom wybrać słabe lub popularne frazy jako hasła, które są łatwe do zapamiętania.

Łatwa dostępność: Może zapewnić lepszą ochronę niż WPA2 bez zmiany poprzednich metod używanych przez użytkowników do łączenia się z siecią.

WPA3-Enterprise: Ten tryb jest oparty na WPA2. Zapewnia lepsze bezpieczeństwo niż WPA2 w całej sieci i chroni poufne dane przy użyciu wielu koncepcji i narzędzi kryptograficznych. Poniżej opisano niektóre protokoły bezpieczeństwa używane przez WPA3-Enterprise.

Uwierzytelnione szyfrowanie: Pomaga w utrzymaniu autentyczności i poufności danych. W tym celu WPA3 wykorzystuje 256-bitowy protokół Galois/Counter Mode Protocol (GCMP-256).

Pochodzenie i walidacja klucza: Pomaga w generowaniu klucza kryptograficznego z hasła lub klucza głównego. Wykorzystuje 384-bitowy tryb uwierzytelniania zaszyfrowanych wiadomości (FIMAC) z algorytmem Secure Flash, określanym jako FIMAC-SFIA-384.

Ustanowienie i weryfikacja klucza: Pomaga w wymianie kluczy kryptograficznych między dwiema stronami. W tym celu WPA3 wykorzystuje wymianę Elliptic Curve Diffie-Heilman (ECDH) i Elliptic Curve Digital Signature Algorithm (ECDSA) przy użyciu 384-bitowej krzywej eliptycznej.

Ochrona ramek i niezawodna administracja: WPA3 wykorzystuje do tego celu 256-bitowy Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIPGMAC-256).

Ulepszenia w WPA3 w odniesieniu do WPA2

WPA3 można wykorzystać do wdrożenia wielowarstwowej strategii bezpieczeństwa, która może chronić wszystkie aspekty sieci Wi-Fi. WPA3 ma program certyfikacji, który określa obowiązujące standardy, które produkt musi obsługiwać. Protokół Dragonfly Handshake/SAE jest obowiązkowy dla certyfikacji WPA3.

Ważne cechy WPA3 są następujące.

1. Bezpieczne uzgadnianie: Protokół SAE (Simultaneous Authentication of Equals), znany również jako uzgadnianie Dragonfly, może być użyty do uczynienia hasła odpornym na ataki słownikowe i siłowe, uniemożliwiając odszyfrowanie danych w trybie offline.

2. Wi-Fi Easy Connect: Ta funkcja upraszcza proces konfiguracji zabezpieczeń, zarządzając różnymi połączeniami interfejsów w sieci za pomocą jednego interfejsu przy użyciu protokołu Wi-Fi Device Provisioning Protocol (DPP). Może to bezpiecznie umożliwić wielu inteligentnym urządzeniom w sieci łączenie się z jednym urządzeniem za pomocą kodu szybkiej odpowiedzi (QR) lub hasła. Pomaga także skonfigurować połączenie między różnymi urządzeniami IoT.

3. Nieuwierzytelnione szyfrowanie: wykorzystuje nową funkcję o nazwie Opportunistic Wireless Encryption (OWE), która zastępuje „otwarte" uwierzytelnianie 802.11, zapewniając lepszą ochronę podczas korzystania z publicznych hotspotów i sieci publicznych.

4. Większe klucze sesyjne: Proces bezpieczeństwa kryptograficznego WPA3-Enterprise obsługuje klucze o długości 192 bitów lub większej, które są trudne do złamania, zapewniając sztywną ochronę.

Porównanie WEP, WPA, WPA2 i WPA3

WEP zapewnia poufność danych w sieciach bezprzewodowych, ale jest słaby i nie spełnia żadnego z celów bezpieczeństwa. Podczas gdy WPA rozwiązuje większość problemów WEP, WPA2 sprawia, że sieci bezprzewodowe są prawie tak samo bezpieczne, jak sieci przewodowe. Ponieważ WPA2 obsługuje uwierzytelnianie, dostęp do sieci mają tylko autoryzowani użytkownicy. WEP należy zastąpić WPA lub WPA2, aby zabezpieczyć sieć Wi-Fi. Chociaż WPA i WPA2 zawierają zabezpieczenia przed fałszowaniem i atakami powtórkowymi, WPA3 może zapewnić bardziej udoskonalony mechanizm ochrony hasłem i bezpieczne połączenia IoT; ponadto wykorzystuje silniejsze techniki szyfrowania. Poniższa tabela porównuje WEP, WPA, WPA2 i WPA3 pod względem używanego algorytmu szyfrowania, rozmiaru klucza szyfrującego, generowanego wektora inicjalizacji (IV), zarządzania kluczami i integralności danych.

Encryption	Attributes				
	Encryption Algorithm	IV Size	Encryption Key Length	Key Management	Integrity Check Mechanism
WEP	RC4	24-bits	40/104-bits	None	CRC-32
WPA	RC4, TKIP	48-bits	128-bits	4-way handshake	Michael algorithm and CRC-32
WPA2	AES-CCMP	48-bits	128-bits	4-way handshake	CBC-MAC
WPA3	AES-GCMP 256	Arbitrary length 1 - 2^{64}	192-bits	ECDH and ECDSA	BIP-GMAC-256

Problemy z WEP, WPA i WPA2

Problemy z WEP

Szyfrowanie WEP jest niewystarczające do zabezpieczenia sieci bezprzewodowych z powodu pewnych problemów i anomalii, które obejmują następujące.

CRC32 nie wystarcza do zapewnienia pełnej integralności kryptograficznej pakietu: przechwytując dwa pakiety, osoba atakująca może niezawodnie odwrócić bit w zaszyfrowanym strumieniu i zmodyfikować sumę kontrolną, aby pakiet został zaakceptowany.

IV mają 24 bity: IV to 24-bitowe pole, które jest zbyt małe, aby mogło być bezpieczne, i jest wysyłane w części wiadomości zawierającej zwykły tekst. Punkt dostępowy emitujący 1500-bajtowe pakiety z szybkością 11 Mb/s wyczerpałby całą przestrzeń IV w ciągu pięciu godzin.

WEP jest podatny na ataki ze znanym tekstem jawnym: gdy wystąpi kolizja IV, możliwa staje się rekonstrukcja strumienia klucza RC4 w oparciu o IV i odszyfrowany ładunek pakietu.

WEP jest podatny na ataki słownikowe: ponieważ WEP jest oparty na haśle, jest podatny na ataki polegające na łamaniu hasła. Mała przestrzeń IV umożliwia atakującemu utworzenie tabeli deszyfrowania, co jest atakiem słownikowym.

WEP jest podatny na ataki DoS: Dzieje się tak dlatego, że komunikaty dotyczące kojarzenia i rozłączania nie są uwierzytelniane.

Osoba atakująca może ostatecznie utworzyć tabelę deszyfrowania zrekonstruowanych strumieni kluczy: mając około 24 GB miejsca, osoba atakująca może użyć tej tabeli do odszyfrowania pakietów WEP w czasie rzeczywistym.

Brak scentralizowanego zarządzania kluczami utrudnia regularną zmianę kluczy WEP.

IV jest wartością używaną do losowania wartości strumienia klucza, a każdy pakiet ma wartość IV: standard IV dopuszcza tylko pole 24-bitowe, które jest zbyt małe, aby mogło być bezpieczne, i jest wysyłane w części wiadomości zawierającej zwykły tekst. Wszystkie dostępne wartości IV mogą zostać wykorzystane w ciągu kilku godzin przy zajętym punkcie dostępowym. IV jest częścią klucza szyfrującego RC4 i jest podatny na atak analityczny, który odzyskuje klucz po przechwyceniu i przeanalizowaniu stosunkowo niewielkiej ilości ruchu. Identyczne strumienie klucza są tworzone przy ponownym wykorzystaniu IV do ochrony danych, ponieważ krótkie strumienie klucza IV są powtarzane w krótkim czasie. Ponadto karty bezprzewodowe tego samego dostawcy mogą generować tę samą sekwencję IV. Umożliwia to atakującym określenie strumienia klucza i odszyfrowanie tekstu zaszyfrowanego. Standard nie wymaga, aby każdy pakiet miał unikalny IV: Dostawcy wykorzystują tylko niewielką część dostępnych możliwości 24-bitowych. W rezultacie mechanizm oparty na losowości wcale nie jest przypadkowy, a osoby atakujące mogą łatwo określić strumień klucza i odszyfrować inne wiadomości. Użycie RC4 zostało zaprojektowane jako szyfr jednorazowy i nie jest przeznaczone do użytku z wielu wiadomości.

Ponieważ większość organizacji skonfigurowała swoich klientów sieciowych i punkty dostępowe tak, aby używały tego samego klucza współdzielonego lub czterech kluczy domyślnych, losowość strumienia klucza zależy od unikalności wartości IV. Użycie IV i klucza zapewnia, że strumień klucza dla każdego pakietu jest inny, ale w większości przypadków IV zmienia się, podczas gdy klucz pozostaje stały. Ponieważ ten proces szyfrowania składa się tylko z dwóch głównych składników, a jeden pozostaje stały, proces ma niedopuszczalny poziom randomizacji. Zajęty punkt dostępowy może wykorzystać wszystkie 224 dostępne wartości IV w ciągu kilku godzin, co wymaga ponownego wykorzystania wartości IV. Taka powtarzalność w procesie polegającym na przypadkowości prowadzi do niepowodzenia. Kwestię IV pogarsza fakt, że standard 802.11 nie wymaga, aby każdy pakiet miał inną wartość IV, co jest analogiczne do żądania rygorystycznych zabezpieczeń przy jednoczesnym stosowaniu słabych środków. W wielu implementacjach wartość IV zmienia się tylko wtedy, gdy bezprzewodowa karta sieciowa jest ponownie inicjowana, zwykle podczas ponownego uruchamiania. Chociaż 24 bity zapewniają wystarczające możliwe kombinacje wartości IV, większość implementacji wykorzystuje tylko kilka bitów; w związku z tym te implementacje nawet nie wykorzystują dostępnych im środków bezpieczeństwa. Przyczyny generowania słabych IV w WEP obejmują:

Aby wygenerować różne pakiety w WEP, algorytm RC4 używa algorytmu planowania klucza (KSA) w celu utworzenia IV i dodania go do klucza podstawowego, co sprawia, że kilka pierwszych bajtów tekstu jawnego jest łatwo przewidywalnych.

Wartość IV nie jest jawna dla sieci. Dlatego ten sam IV może być używany z tym samym tajnym kluczem na wielu urządzeniach bezprzewodowych.

Metoda dołączania IV na początku klucza bezpieczeństwa sprawia, że sieć jest podatna na ataki Fluhrer-Mantin-Shamir (FMS), które umożliwiają atakującym wykonanie narzędzi skryptowych w celu złamania tajnego klucza poprzez sprawdzenie łącza.

Większość słabych IV zależy od klucza WEP i ujawnia dokładne informacje o bajtach klucza z pierwszego bajtu wyjściowego RC4, a także mniejsze wskazówki z innych bajtów.

Dzięki dodatkowemu przetwarzaniu odzyskanych bajtów, części algorytmu generowania pseudolosowego (PRGA) mogą być emulowane w celu wyodrębnienia kluczowych informacji z bajtu IV.

Nie można skutecznie wykryć manipulowania wiadomością. Chociaż metody takie jak suma kontrolna i ICV mogą sprawdzać integralność wiadomości, mają one pewne wady. Niektóre bezpieczne metody obliczania MIC mają wysoki koszt obliczeniowy, gdy są wprowadzane w TKIP.

WEP korzysta bezpośrednio z klucza głównego i nie ma wbudowanej możliwości aktualizacji kluczy.

Luka w zabezpieczeniach implementacji WEP RC4 powoduje generowanie słabych IV, które atakujący mogą łatwo wykorzystać do wydedukowania podstawowego klucza WEP. Atakujący może użyć narzędzi do podsłuchiwania sieci WLAN do przechwytywania pakietów zaszyfrowanych tym samym kluczem oraz narzędzi takich jak aircrack-ng i WEPCrack do odszyfrowania słabych IV, ujawniając w ten sposób podstawowy klucz WEP.

Problemy z WPA

WPA jest pod wieloma względami ulepszeniem w stosunku do WEP, ponieważ wykorzystuje TKIP do szyfrowania danych i pomaga w bezpiecznym przesyłaniu danych. Jednak WPA ma również wiele problemów związanych z bezpieczeństwem. Poniżej opisano niektóre problemy związane z bezpieczeństwem WPA.

Słabe hasła: jeśli użytkownicy polegają na słabych hasłach, WPA PSK jest narażony na różne ataki polegające na łamaniu haseł.

Brak tajemnicy przekazywania: jeśli atakujący przechwyci PSK, może odszyfrować wszystkie pakiety zaszyfrowane tym kluczem (tj. Wszystkie przesyłane lub przesyłane pakiety mogą zostać odszyfrowane).

Podatność na fałszowanie i deszyfrowanie pakietów: Klienci korzystający z WPA-TKIP są narażeni na ataki polegające na wstrzykiwaniu pakietów i ataki deszyfrujące, co dodatkowo umożliwia atakującym przejmowanie połączeń protokołu TCP (Transmission Control Protocol).

Przewidywalność grupowego klucza czasowego (GTK): Niepewny generator liczb losowych (RNG) w WPA umożliwia atakującym wykrycie GTK wygenerowanego przez punkt dostępowy. To dodatkowo umożliwia atakującym wprowadzanie szkodliwego ruchu do sieci i odszyfrowywanie wszystkich transmisji w toku przez Internet.

Zgadywanie adresów IP: Luki w zabezpieczeniach TKIP umożliwiają atakującym odgadnięcie adresu IP podsieci i wstrzyknięcie do sieci małych pakietów w celu obniżenia wydajności sieci.

Problemy z WPA2

Chociaż WPA2 jest bezpieczniejszy niż WPA, ma również pewne problemy z bezpieczeństwem, które omówiono poniżej.

Słabe hasła: jeśli użytkownicy polegają na słabych hasłach, WPA2 PSK jest narażony na różne ataki, takie jak podsłuchiwanie, ataki słownikowe i łamanie haseł.

Brak tajemnicy przekazywania: jeśli atakujący przechwyci PSK, może odszyfrować wszystkie pakiety zaszyfrowane tym kluczem (tj. Wszystkie przesyłane lub przesyłane pakiety można odszyfrować).

Podatność na ataki man-in-the-middle (MITM) i ataki typu „odmowa usługi" (DoS): Luka Hole96 w WPA2 umożliwia atakującym wykorzystanie wspólnego klucza czasowego grupy (GTK) do przeprowadzania ataków MITM i DoS.

Przewidywalność GTK: Niepewny generator liczb losowych (RING) w WPA2 umożliwia atakującym wykrycie GTK generowanego przez punkt dostępowy. To dodatkowo umożliwia atakującym wprowadzanie szkodliwego ruchu do sieci i odszyfrowywanie wszystkich transmisji w toku przez Internet.

Luki w zabezpieczeniach KRACK: WPA2 ma znaczną podatność na exploit znany jako atak polegający na ponownej instalacji klucza (KRACK). Ten exploit może pozwolić atakującym na wąchanie pakietów, przejmowanie połączeń, wprowadzanie złośliwego oprogramowania i odszyfrowywanie pakietów.

Podatność na bezprzewodowe ataki DoS: osoby atakujące mogą wykorzystać funkcję wykrywania ataków typu replay WPA2 do wysyłania sfałszowanych ramek danych adresowanych do grupy z dużym numerem PN w celu przeprowadzenia ataku DoS.

Niepewne odzyskiwanie kodu PIN WPS: W niektórych przypadkach wyłączenie WPA2 i WPS może być czasochłonnym procesem, w którym osoba atakująca musi kontrolować WPA2 PSK używane przez klientów. Gdy WPA2 i WPS są włączone, osoba atakująca może ujawnić klucz WPA2, określając osobisty numer identyfikacyjny (PIN) WPS, wykonując proste czynności.

Zagrożenia bezprzewodowe

W poprzednich sekcjach omówiono podstawowe koncepcje sieci bezprzewodowych i mechanizmy zabezpieczeń sieci bezprzewodowych, takie jak algorytmy szyfrowania, które zabezpieczają komunikację w sieci bezprzewodowej. Aby zabezpieczyć sieci bezprzewodowe, administrator sieci musi zrozumieć różne możliwe słabości algorytmów szyfrowania, które mogą zwabić atakujących. Sieć bezprzewodowa może być narażona na różne rodzaje ataków, w tym ataki kontroli dostępu, ataki na integralność, ataki na poufność, ataki na dostępność i ataki na uwierzytelnianie. W tej sekcji omówiono różne rodzaje zagrożeń bezpieczeństwa, zagrożeń i ataków związanych z sieciami bezprzewodowymi.

Ataki kontroli dostępu

Ataki kontroli dostępu bezprzewodowego mają na celu penetrację sieci poprzez obejście środków kontroli dostępu WLAN, takich jak filtry AP MAC i kontrola dostępu do portów Wi-Fi. Istnieje kilka rodzajów ataków kontroli dostępu, w tym następujące.

WarDriving: W ataku WarDriving sieci WLAN są wykrywane albo przez wysyłanie zapytań sondujących przez połączenie, albo przez nasłuchiwanie sygnałów nawigacyjnych. Osoba atakująca, która wykryje punkt penetracji, może przeprowadzić dalsze ataki na sieć LAN. Niektóre z narzędzi, których atakujący może użyć do przeprowadzenia ataków Wardrivingu, to KisMAC i NetStumbler.

Fałszywe punkty dostępowe: w celu stworzenia backdoora do zaufanej sieci osoba atakująca może zainstalować niezabezpieczony lub fałszywy punkt dostępowy w zaporze sieciowej. Atakujący może

również użyć programowych lub sprzętowych punktów dostępowych do przeprowadzenia tego rodzaju ataku. Bezprzewodowy punkt dostępowy jest określany jako nieuczciwy punkt dostępowy, gdy jest zainstalowany w zaufanej sieci bez autoryzacji. Wewnętrzny lub zewnętrzny atakujący może zainstalować nieuczciwe punkty dostępowe w zaufanej sieci ze złośliwymi intencjami.

Fałszowanie adresu MAC: Za pomocą techniki fałszowania adresu MAC osoba atakująca może ponownie skonfigurować adres MAC, aby był widoczny dla hosta w zaufanej sieci jako autoryzowany punkt dostępowy. Atakujący może użyć narzędzi takich jak SMAC do przeprowadzenia tego rodzaju ataku.

Błędna konfiguracja punktu dostępowego: jeśli użytkownik niewłaściwie skonfiguruje którekolwiek z krytycznych ustawień zabezpieczeń w dowolnym punkcie dostępowym, cała sieć może być narażona na luki w zabezpieczeniach i ataki. Punkt dostępowy nie może wyzwalać alertów w większości systemów wykrywania włamań, ponieważ systemy te rozpoznają je jako legalne urządzenie.

Skojarzenia ad hoc: osoba atakująca może przeprowadzić tego rodzaju atak przy użyciu dowolnego adaptera uniwersalnej magistrali szeregowej (USB) lub karty bezprzewodowej. Atakujący łączy hosta z niezabezpieczonym klientem, aby zaatakować określonego klienta lub uniknąć zabezpieczeń punktu dostępowego.

Rozwiązły klient: korzystając z rozwiązłego klienta, osoba atakująca wykorzystuje zachowanie kart bezprzewodowych 802.11: zawsze próbuje znaleźć silniejszy sygnał do połączenia. Atakujący umieszcza punkt dostępowy w pobliżu docelowej sieci Wi-Fi i nadaje mu wspólny identyfikator SSID, oferując nieodparcie silniejszy sygnał i wyższą prędkość niż docelowa sieć Wi-Fi. Celem jest zwabienie klienta do połączenia z punktem dostępowym atakującego, a nie z legalną siecią Wi-Fi. Rozwiązliwi klienci umożliwiają atakującemu przesyłanie docelowego ruchu sieciowego przez fałszywy punkt dostępowy. Jest to bardzo podobne do zagrożenia złego bliźniaka w sieciach bezprzewodowych, w którym atakujący uruchamia punkt dostępowy udający autoryzowany punkt dostępowy, wyświetlając identyfikator SSID sieci WLAN.

Błędne skojarzenie klienta: Klient może celowo lub przypadkowo połączyć się lub skojarzyć z punktem dostępowym poza legalną siecią, ponieważ sygnały WLAN przechodzą przez powietrze, ściany i inne przeszkody. Ten rodzaj błędnego skojarzenia klienta może prowadzić do ataków kontroli dostępu.

Nieautoryzowane powiązanie: Nieautoryzowane powiązanie jest głównym zagrożeniem dla sieci bezprzewodowych. Zapobieganie tego rodzaju atakom zależy od metody lub techniki, której używa atakujący, aby połączyć się z siecią.

Ataki na integralność

Atak na integralność obejmuje zmianę lub modyfikację danych podczas transmisji. W przypadku ataków na integralność sieci bezprzewodowej osoby atakujące wysyłają sfałszowane ramki kontrolne, zarządzające lub danych przez sieć bezprzewodową w celu niewłaściwego skierowania urządzeń bezprzewodowych i przeprowadzenia innego rodzaju ataku, takiego jak atak DoS. Poniższa tabela podsumowuje różne rodzaje ataków na integralność.

Rodzaj ataku : Opis : Metoda i narzędzia

Wstrzykiwanie ramek danych : Konstruowanie i wysyłanie sfałszowanych ramek 802.11 : Airpwn, File2air, Wperf, voidll, WEPWedgie, w sieci dinject

Iniekcja WEP : Konstruowanie i wysyłanie sfałszowanego klucza WEP : Klucze szyfrujące WEP Injection. Łamanie WEP + narzędzia do wstrzykiwania

Ataki polegające na odwracaniu bitów : Przechwytywanie ramki i odwracanie losowych bitów w ładunku danych, modyfikowanie ICV i wysyłanie go do użytkownika

Rozszerzalna powtórka AP: Przechwytywanie protokołów uwierzytelniania rozszerzonego 802.IX (np. EAP Identity, Success i Failure) do późniejszego odtworzenia. : Bezprzewodowe przechwytywanie + narzędzia do wstrzykiwania między klientem a punktem dostępowym

Odtwarzanie danych: przechwytywanie ramek danych 802.11 do późniejszego (zmodyfikowanego) odtwarzania. : Przechwytywanie + narzędzia do wstrzykiwania

Ataki z powtórzeniem wektora inicjalizacji: Wyprowadzenie strumienia klucza przez wysłanie wiadomości w postaci zwykłego tekstu.

RADIUS Replay: przechwytywanie komunikatów RADIUS Access-Accept lub Reject do późniejszego odtworzenia: przechwytywanie Ethernet + narzędzia do wstrzykiwania między punktem dostępowym a serwerem uwierzytelniającym

Wirusy sieci bezprzewodowych: Wirusy mają ogromny wpływ na sieci bezprzewodowe. Mogą zapewnić atakującemu prostą metodę na złamanie zabezpieczeń punktów dostępowych.

Ataki na poufność

Ataki te mają na celu przechwycenie poufnych informacji przesyłanych przez sieć bezprzewodową, niezależnie od tego, czy system przesyła dane w postaci zwykłego tekstu, czy w formacie zaszyfrowanym. Jeśli system przesyła dane w zaszyfrowanym formacie (takim jak WEP lub WPA), osoba atakująca może próbować złamać szyfrowanie. Poniższa tabela podsumowuje różne rodzaje ataków na poufność w sieciach bezprzewodowych.

Podsłuchiwanie: przechwytywanie i dekodowanie ruchu niezabezpieczonych aplikacji w celu uzyskania potencjalnie wrażliwych informacji: Wireshark, Ettercap, Kismet, analizatory komercyjne

Analiza ruchu: wnioskowanie o informacjach z obserwacji zewnętrznych cech ruchu

Łamanie klucza WEP: Przechwytywanie danych w celu odzyskania klucza WEP przy użyciu brutalnej siły lub kryptoanalizy Fluhrer-Mantin-Shamir (FMS): Aircrack-ng, AirSnort, chopchop, WepAttack, WepDecrypt

Punkt dostępowy Evil Twin: Udawanie autoryzowanego punktu dostępowego poprzez sygnalizowanie identyfikatora SSID sieci WLAN w celu zwabienia użytkowników: HostAP, EvilTwinFramework, Wifiphisher

Honeypot AP: Ustawianie SSID punktu dostępowego tak, aby był taki sam, jak legalnego punktu dostępowego: Manipulowanie SSID

Przejęcie sesji: Manipulowanie siecią w taki sposób, aby host atakującego wydawał się być pożądanym miejscem docelowym. : Manipulacja

Maskarada : Udawanie autoryzowanego użytkownika w celu uzyskania dostępu do systemu : Kradzież identyfikatorów logowania i haseł, omijanie mechanizmów uwierzytelniania

Atak MITM: Uruchamianie konwencjonalnych narzędzi ataku MITM na punkcie dostępowym typu „zły bliźniak” w celu przechwycenia sesji TCP lub tuneli Secure Sockets Layer (SSL)/Secure Shell (SSH): dsniff, Ettercap, alter

Ataki na dostępność

Ataki na dostępność mają na celu utrudnianie dostarczania usług bezprzewodowych uprawnionym użytkownikom poprzez paraliżowanie zasobów sieci WLAN lub odmowę im dostępu do tych zasobów. Ten atak powoduje, że usługi sieci bezprzewodowej są niedostępne dla uprawnionych użytkowników. Atakujący mogą przeprowadzać ataki dostępności na różne sposoby, utrudniając dostępność sieci bezprzewodowych. Poniższa tabela podsumowuje różne rodzaje ataków dostępności na sieci bezprzewodowe.

Rodzaj ataku : Opis : Metoda i narzędzia

Kradzież punktu dostępowego: Fizyczne usunięcie punktu dostępowego z miejsca jego instalacji. : Ukrycie i/lub szybkość

Ataki powodujące odłączenie: niszczenie łączności między

AP i klienta, aby cel był niedostępny dla innych urządzeń bezprzewodowych. : Zniszczenie łączności

EAP-Failure: Obserwacja prawidłowej wymiany 802.IX EAP, a następnie wysłanie do klienta sfałszowanego komunikatu EAP-Failure: File2air i Airtool Pi

Beacon Flood: Generowanie tysięcy fałszywych beaconów 02.11, aby utrudnić klientom znalezienie legalnego AP. : Fałszywy AP

Denial-of-Service : Wykorzystanie mechanizmu oceny czystego kanału (CCA) z wykrywaniem operatora przez wykrywanie operatora z unikaniem kolizji (CSMA/CA), aby kanał wyglądał na zajęty.: Adapter obsługujący tryb CWTx z narzędziem niskiego poziomu wywołać ciągłe transmisje

De-authenticate Flood : Zalewanie klienta (klientów) sfałszowanymi anulowania uwierzytelnienia

lub odłącza, aby odłączyć użytkowników od punktu dostępowego. : AirJack, pustka

Ataki routingowe: Dystrybucja informacji o routingu w sieci.: protokół RIP, wykorzystanie wektora odległości Ad-Floc na żądanie

(AODV) i protokoły Dynamic Source Routing (DSR) wykorzystujące ataki tuneli czasoprzestrzennych i leje krasowe

Authenticate Flood: Wysyłanie sfałszowanych uwierzytelnień lub powiązań z losowych adresów MAC w celu wypełnienia tabeli asocjacji docelowego punktu dostępowego: AirJack, File2air, voidll

Address Resolution Protocol (ARP) Ataki zatruwające pamięć podręczną: tworzenie wielu wektorów ataku.

Ataki oszczędzające energię: przesyłanie sfałszowanej mapy wskazania ruchu (TIM) lub dostarczanie TIM (DTIM) do klienta w trybie oszczędzania energii, narażając klienta na atak DoS.

Exploit TKIP MIC: Generowanie nieprawidłowych danych TKIP w celu przekroczenia progu błędu MIC docelowego punktu dostępowego, zawieszanie usługi WLAN.:File2air, wnet dinject

Ataki uwierzytelniające

Celem ataków uwierzytelniających jest kradzież tożsamości klientów Wi-Fi, ich danych osobowych, danych logowania itp. w celu uzyskania nieautoryzowanego dostępu do zasobów sieciowych. Poniższa tabela podsumowuje różne rodzaje ataków uwierzytelniających na sieci bezprzewodowe.

Rodzaj ataku : Opis : Metoda i narzędzia

Łamanie PSK: Odzyskiwanie PSK WPA z przechwyconych klatek uzgadniania klucza za pomocą narzędzia do ataku słownikowego. : Cowpatty, KisMAC, Fern Wifi Cracker

LEAP Cracking : Odzyskiwanie poświadczeń użytkownika z przechwyconych pakietów 802.IX Lightweight EAP (LEAP) za pomocą narzędzia do ataku słownikowego w celu złamania skrótu hasła NT: Asleap, THCLEAPcracker

Łamanie logowania VPN: zdobywanie poświadczeń użytkownika (np. hasła protokołu PPTP lub współdzielonego tajnego klucza zabezpieczeń protokołu internetowego (IPsec)) za pomocą ataków brute-force na protokoły uwierzytelniania wirtualnej sieci prywatnej (VPN). : ike_scan i IKECrack (IPsec), Anger i TFHCpptpbruter (PPTP)

Łamanie logowania do domeny: Odzyskiwanie poświadczeń użytkownika (np. loginu i hasła do systemu Windows) poprzez łamanie skrótów haseł NetBIOS za pomocą narzędzia do ataku siłowego lub słownikowego. : John the Ripper, LOphtCrack, TFIC-Hydra

Atak polegający na ponownej instalacji klucza: wykorzystanie czterokierunkowego uzgadniania protokołu WPA2. : Jednorazowa technika ponownego użycia

Kradzież tożsamości: Przechwytywanie tożsamości użytkowników z czystego tekstu 802.IX Identity Response Packages: Narzędzia do przechwytywania pakietów

Zgadywanie klucza współdzielonego: Próba uwierzytelnienia klucza współdzielonego 802.11 przy użyciu domyślnych lub złamanych kluczy WEP dostawcy. : Narzędzia do łamania WEP, Wifite

Spekulacja hasła: Wielokrotne próby uwierzytelnienia 802.IX przy użyciu przechwyconej tożsamości w celu odgadnięcia hasła użytkownika. : Słownik haseł

Kradzież logowania do aplikacji: przechwytywanie poświadczeń użytkownika (np. adresu e-mail i hasła) z protokołów aplikacji w postaci zwykłego tekstu. : Ace Password Sniffer, dsniff, Wi-Jacking Attack

Nieuczciwy atak AP

Punkty dostępowe łączą się z kartami sieciowymi klienta, uwierzytelniając się za pomocą identyfikatorów SSID. Nieautoryzowane (lub nieuczciwe) punkty dostępowe mogą pozwolić każdemu, kto ma urządzenie wyposażone w standard 802.11, na połączenie się z siecią korporacyjną. Nieautoryzowany punkt dostępowy może dać atakującemu dostęp do sieci. Za pomocą bezprzewodowych narzędzi do sniffingu na podstawie punktów dostępowych można określić: autoryzowane adresy MAC, nazwę dostawcy i konfiguracje zabezpieczeń. Atakujący może następnie utworzyć listę adresów MAC autoryzowanych punktów dostępowych w docelowej sieci LAN i sprawdzić tę listę z listą adresów MAC znalezionych przez wąchanie. Następnie osoba atakująca może utworzyć fałszywy punkt dostępowy i umieścić go w pobliżu docelowej sieci korporacyjnej. Atakujący używają nieuczciwych punktów dostępowych umieszczonych w sieci 802.11 w celu przejęcia połączeń legalnych użytkowników sieci. Gdy użytkownik włączy komputer, nieuczciwy punkt dostępowy zaoferuje połączenie z kartą sieciową użytkownika sieciowego. Atakujący nakłania użytkownika do połączenia się z fałszywym punktem dostępowym, wysyłając identyfikator SSID. Jeśli użytkownik łączy się z nieuczciwym punktem dostępowym, mając wrażenie, że jest to legalny punkt dostępowy, cały ruch od użytkownika przechodzi przez nieuczciwy punkt dostępowy, umożliwiając pewną formę wąchania pakietów bezprzewodowych. Przeszukane pakiety mogą nawet zawierać nazwy użytkowników i hasła.

Błędne skojarzenie klienta

Błędne powiązanie to luka w zabezpieczeniach, która może wystąpić, gdy klient sieci łączy się z sąsiednim punktem dostępowym. Błędne skojarzenia klientów mogą wystąpić z różnych powodów, takich jak źle skonfigurowani klienci, niewystarczający zasięg korporacyjnej sieci Wi-Fi, brak polityki Wi-Fi, ograniczenia w korzystaniu z Internetu w biurze, połączenia ad-hoc, którymi administratorzy nie zarządzają regularnie i atrakcyjne identyfikatory SSID. Mogą one wystąpić z lub bez wiedzy klienta bezprzewodowego i nielegalnego punktu dostępowego. Aby przeprowadzić atak polegający na błędnym powiązaniu klienta, atakujący ustawia nieuczciwy punkt dostępowy poza granicami korporacji. Atakujący najpierw poznaje identyfikator SSID docelowej sieci bezprzewodowej. Wykorzystując sfałszowany identyfikator SSID, atakujący może wysyłać sygnały nawigacyjne reklamujące nieuczciwy punkt dostępowy, aby zwabić klientów do połączenia. Atakujący może wykorzystać nieuczciwy punkt dostępowy jako kanał do obejścia zasad bezpieczeństwa przedsiębiorstwa. Gdy klient połączy się z nieuczciwym punktem dostępowym, osoba atakująca może odzyskać poufne informacje, takie jak nazwy użytkowników i hasła, uruchamiając ataki MITM, słownikowe EAP lub Metasploit w celu wykorzystania błędnego powiązania klienta.

Źle skonfigurowany atak AP

Większość organizacji poświęca znaczną ilość czasu na definiowanie i wdrażanie zasad bezpieczeństwa sieci Wi-Fi, ale klient sieci bezprzewodowej może przypadkowo zmienić ustawienia zabezpieczeń punktu dostępowego. To z kolei może prowadzić do błędnej konfiguracji punktów dostępowych. Źle skonfigurowany punkt dostępowy może narazić dobrze zabezpieczoną sieć na ataki. Trudno jest wykryć źle skonfigurowany punkt dostępowy, ponieważ jest to autoryzowane, legalne urządzenie w sieci. Atakujący mogą łatwo połączyć się z zabezpieczoną siecią za pośrednictwem źle skonfigurowanych punktów dostępowych, które nadal działają normalnie po nawiązaniu połączenia przez atakującego, ponieważ żadne alerty nie zostaną uruchomione, nawet jeśli atakujący użyje połączenia do naruszenia bezpieczeństwa. Wiele organizacji nie utrzymuje zasad bezpieczeństwa Wi-Fi i nie podejmuje odpowiednich działań w celu wyeliminowania tej luki w konfiguracjach zabezpieczeń. Ponieważ sieci Wi-Fi organizacji rozszerzają się na coraz więcej lokalizacji i urządzeń, źle skonfigurowane punkty dostępowe stają się coraz bardziej niebezpieczne. Do kluczowych elementów, które odgrywają ważną rolę w tego rodzaju ataku, należą:

Rozgłaszanie identyfikatorów SSID: osoba atakująca konfiguruje punkty dostępowe w celu rozgłaszania identyfikatorów SSID autoryzowanym użytkownikom. Wszystkie modele punktów dostępowych mają własny domyślny identyfikator SSID, a punkty dostępowe z domyślną konfiguracją wykorzystującą domyślne identyfikatory SSID są podatne na ataki słownikowe typu brute-force. Nawet jeśli użytkownicy włączą WEP, niezaszyfrowany identyfikator SSID rozgłasza hasło w postaci zwykłego tekstu.

Słabe hasło: niektórzy administratorzy sieci błędnie używają identyfikatorów SSID jako podstawowych haseł do weryfikacji autoryzowanych użytkowników. Identyfikatory SSID działają jak podstawowe hasła i pomagają administratorom sieci rozpoznawać autoryzowane urządzenia bezprzewodowe w sieci.

Błąd konfiguracji: Błędy konfiguracji obejmują błędy popełnione podczas instalacji, zasady konfiguracji punktu dostępowego, błędy ludzkie popełnione podczas rozwiązywania problemów z siecią WLAN oraz zmiany zabezpieczeń niejednolicie zaimplementowane w całej architekturze. Rozgłaszanie SSID to błąd konfiguracji, który pomaga atakującym w kradzieży SSID, co sprawia, że punkt dostępowy zakłada, że atakujący próbuje nawiązać legalne połączenie

Nieautoryzowane stowarzyszenie

Nieautoryzowane skojarzenie jest głównym zagrożeniem dla sieci bezprzewodowych. Ma dwie formy: skojarzenie przypadkowe i skojarzenie złośliwe. Atakujący wykonuje złośliwe powiązanie za pomocą miękkich punktów dostępowych zamiast korporacyjnych punktów dostępowych. Atakujący tworzy miękki punkt dostępowy, zwykle na laptopie, uruchamiając narzędzie, które sprawia, że karta sieciowa laptopa wygląda jak legalny punkt dostępowy. Następnie atakujący używa miękkiego punktu dostępowego, aby uzyskać dostęp do docelowej sieci bezprzewodowej. Programowe punkty dostępowe są dostępne na kartach klienckich lub wbudowanych radiach WLAN w niektórych urządzeniach PDA i laptopach; osoba atakująca może je uruchomić bezpośrednio lub za pośrednictwem programu antywirusowego. Atakujący infekuje maszynę ofiary i aktywuje miękkie punkty dostępowe, umożliwiając nieautoryzowane połączenie z siecią firmową. Osoba atakująca, która uzyskuje dostęp do sieci za pomocą nieautoryzowanego powiązania, może ukraść hasła, przeprowadzić atak na sieć przewodową lub umieścić trojany. Z drugiej strony przypadkowe skojarzenie polega na połączeniu się z punktem dostępowym sieci docelowej z nakładającej się sieci sąsiedniej organizacji bez wiedzy ofiary.

Atak połączenia ad-hoc

Klienci Wi-Fi mogą komunikować się bezpośrednio w trybie ad-hoc, który nie wymaga AP do przekazywania pakietów. Dane można wygodnie udostępniać klientom w sieciach ad-hoc, które są dość popularne wśród użytkowników Wi-Fi. Zagrożenia bezpieczeństwa pojawiają się, gdy atakujący wymusza na sieci włączenie trybu ad-hoc. Niektóre zasoby sieciowe są dostępne tylko w trybie ad-hoc, ale ten tryb jest z natury niepewny i nie zapewnia silnego uwierzytelniania ani szyfrowania. W ten sposób osoba atakująca może łatwo połączyć się z klientem działającym w trybie ad-hoc i skompromitować go. Osoba atakująca, która penetruje sieć bezprzewodową, może również użyć połączenia ad-hoc, aby zagrozić bezpieczeństwu przewodowej sieci LAN organizacji.

Atak AP Honeypot

Jeśli na tym samym obszarze współistnieje wiele sieci WLAN, użytkownik może połączyć się z dowolną dostępną siecią. Takie obszary są podatne na ataki. Zwykle po włączeniu klienta bezprzewodowego sonduje pobliską sieć bezprzewodową w poszukiwaniu określonego identyfikatora SSID. Osoba atakująca wykorzystuje takie zachowanie klientów bezprzewodowych, konfigurując nieautoryzowaną sieć bezprzewodową przy użyciu nieuczciwego punktu dostępowego. Ten punkt dostępowy ma anteny o dużej mocy (o dużym wzmocnieniu) i używa tego samego identyfikatora SSID co sieć docelowa. Użytkownicy, którzy regularnie łączą się z wieloma sieciami WLAN, mogą łączyć się z fałszywym punktem dostępowym. Takie punkty AP zamontowane przez atakujących nazywane są punktami dostępowymi typu „honeypot”. Wysyłają silniejszy sygnał nawigacyjny niż legalne punkty dostępowe, dzięki czemu karty sieciowe szukające najsilniejszego dostępnego sygnału mogą łączyć się z fałszywym punktem dostępowym. Jeśli autoryzowany użytkownik połączy się z punktem dostępowym typu honeypot, powstaje luka w zabezpieczeniach, a poufne informacje użytkownika, takie jak tożsamość, nazwa użytkownika i hasło, mogą zostać ujawnione atakującemu.

Fałszowanie adresu MAC AP

W sieciach bezprzewodowych sondy nadawcze punktów dostępowych odpowiadają za pomocą sygnałów nawigacyjnych, informując o obecności i dostępności. Odpowiedzi sondy zawierają informacje o tożsamości AP (adres MAC) oraz o tożsamości sieci, którą obsługuje (SSID). Klienci w pobliżu łączą się z siecią za pośrednictwem tych sygnałów nawigacyjnych na podstawie adresu MAC i zawartego w nim identyfikatora SSID. Wiele narzędzi programowych i punktów dostępowych umożliwia ustawianie zdefiniowanych przez użytkownika wartości adresów MAC i identyfikatorów SSID urządzeń AP. Osoba atakująca może sfałszować adres MAC punktu dostępowego, programując

nieuczciwy punkt dostępowy, aby rozgłaszał te same informacje o tożsamości, co legalny punkt dostępowy. Atakujący podłączony do AP jako autoryzowany klient może mieć pełny dostęp do sieci. Ten typ ataku jest skuteczny, gdy docelowa sieć bezprzewodowa używa filtrowania adresów MAC do uwierzytelniania klientów (użytkowników).

Atak typu „odmowa usługi".

Sieci bezprzewodowe są podatne na ataki DoS. Sieci te działają w pasmach nielicencjonowanych z transmisją danych w postaci sygnałów radiowych. Projektanci protokołu MAC dążyli do prostoty, ale jest on podatny na ataki DoS. Sieci WLAN zwykle obsługują aplikacje o znaczeniu krytycznym, takie jak VoIP, dostęp do baz danych, pliki danych projektów i dostęp do Internetu. Zakłócenie tych aplikacji w sieciach WLAN za pomocą ataku DoS jest łatwe i może spowodować utratę produktywności lub przestoje w sieci. Przykładami ataków MAC DoS są ataki typu de-authentication flood, wirtualne zagłuszanie i ataki typu Association flood. Bezprzewodowe ataki DoS zakłócają połączenia sieci bezprzewodowej, emitując polecenia cofnięcia uwierzytelnienia. Przesłana de-uwierzytelnianie zmusza klientów do odłączenia się od punktu dostępowego.

Atak polegający na ponownej instalacji klucza (KRACK)

Atak polegający na ponownej instalacji klucza (KRACK) wykorzystuje luki w implementacji procesu czterokierunkowego uzgadniania w protokole uwierzytelniania WPA2, który służy do nawiązywania połączenia między urządzeniem a punktem dostępowym. Wszystkie bezpieczne sieci Wi-Fi wykorzystują proces czterokierunkowego uzgadniania do nawiązywania połączeń i generowania nowego klucza szyfrowania, który będzie używany do szyfrowania ruchu sieciowego. Atakujący wykorzystuje czterokierunkowe uzgadnianie protokołu WPA2, wymuszając ponowne użycie Nonce. W

W tym ataku atakujący przechwytuje klucz AOnce ofiary, który jest już używany do manipulowania i odtwarzania wiadomości kryptograficznych uzgadniania. Ten atak działa na wszystkie nowoczesne chronione sieci Wi-Fi (zarówno WPA, jak i WPA2); sieci osobiste i firmowe; oraz szyfry WPA-TKIP, AES-CCMP i GCMP. Pozwala atakującemu na kradzież poufnych informacji, takich jak numery kart kredytowych, hasła, wiadomości na czacie, e-maile i zdjęcia. Każde urządzenie z systemem Android, Linux, Windows, Apple, OpenBSD lub MediaTek jest podatne na niektóre warianty ataku KRACK.

Zagłuszający atak sygnału

Zagłuszanie to atak przeprowadzany na sieć bezprzewodową w celu jej skompromitowania. W przypadku tego rodzaju wykorzystania, przytłaczająca ilość złośliwego ruchu powoduje atak DoS na autoryzowanych użytkowników, blokując legalny ruch. Wszystkie sieci bezprzewodowe są podatne na zagłuszanie, a ataki polegające na zagłuszaniu widma zwykle całkowicie blokują całą komunikację. Osoba atakująca używa specjalistycznego sprzętu do przeprowadzenia tego rodzaju ataku. Sygnały generowane przez urządzenia zakłócające wydają się być szumem dla urządzeń w sieci bezprzewodowej, co powoduje, że wstrzymują one transmisje do momentu ustania sygnału, co skutkuje atakiem typu DoS. Ponadto, zagłuszające ataki sygnału nie są łatwo zauważalne. Procedura ataku sygnału zagłuszającego jest podsumowana w następujący sposób.

* Atakujący wytycza obszar docelowy z pobliskiej lokalizacji za pomocą wzmacniacza o dużym wzmocnieniu, który zagłusza legalny punkt dostępowy.

* Użytkownicy nie mogą się zalogować lub są rozłączani przez zbyt silny sygnał w pobliżu.

* Sygnał zagłuszający powoduje DoS, ponieważ 802.11 jest protokołem CSMA/CA, którego algorytmy unikania kolizji wymagają okresu ciszy, zanim radio będzie mogło nadawać.

Urządzenia zakłócające Wi-Fi

Atakujący może zablokować sieć bezprzewodową za pomocą zakłócacza Wi-Fi. To urządzenie korzysta z tego samego pasma częstotliwości, co zaufana sieć. Powoduje zakłócenia w legalnych sygnałach i tymczasowo zakłóca działanie usługi sieciowej. Poniżej przedstawiono przykłady urządzeń zakłócających Wi-Fi:

Zagłuszacz CPB-3016N-5G

Zasięg: 50-150 m

6 anten

Zablokowane 6 pasm częstotliwości (CDMA, 3G UMTS, Wi-Fi i Buletooth)

Możliwość montażu na ścianie

Zagłuszacz PCB-2040

Zasięg: 20-50 m

4 anteny

Zablokowane 4 pasma częstotliwości (2G, 3G, 4G, GPS, Wi-Fi)

Czas pracy: 40 min

Zagłuszacz CPB-2060B

Zasięg: 10-40 m

6 anten

Zablokowane 6 pasm częstotliwości (GPS, 4G, Wi-Fi)

Żywotność baterii wewnętrznej: 2,5-3,0 godz

Zagłuszacz CPB-2660H

o Zasięg: 20-60 m

6 anten

o 6 zagłuszonych pasm częstotliwości (CDMA, DCS, 3G, 4G, UMTS, Wi-Fi)

o Możliwość montażu na ścianie

Zagłuszacz CPB-2061

o Zasięg: 10-40 m

6 anten

o Zablokowane 6 pasm częstotliwości (mobile, Wi-Fi, GPS)

o Montaż naścienny iRysunek 16.30: Zagłuszacz CPB-2061

Zagłuszacz CPB-2680H-AGP

Zasięg: 20-60 m

8 anten

Zablokowane 8 pasm częstotliwości (CDMA, GPS, DCS, 3G, 4G, UMTS, Wi-Fi)

Możliwość montażu na ścianie

Atak aLTEr

Long-Term Evolution (LTE) lub 4G to bezprzewodowy standard komunikacji szerokopasmowej opracowany jako następca 3G w celu poprawy szybkości i bezpieczeństwa bezprzewodowych sieci komórkowych. Oferuje skalowalność przepustowości i obsługuje wcześniejsze technologie, takie jak Global System for Mobile Communications (GSM; 2G) i Universal Mobile Telecommunications System (UMTS; 3G). Chociaż technologia ta została zaprojektowana tak, aby przezwyciężyć wszystkie wady sieci bezprzewodowych, jest podatna na ataki polegające na przejmowaniu danych. Atak aLTEr jest zwykle wykonywany na urządzeniach LTE, które szyfrują dane użytkownika w liczniku AES (AES-CTR), który nie zapewnia ochrony integralności. Aby przeprowadzić ten atak, atakujący instaluje wirtualną (fałszywą) wieżę komunikacyjną między dwoma autentycznymi punktami końcowymi, aby wprowadzić ofiarę w błąd. Atakujący wykorzystuje tę wirtualną wieżę do przerwania transmisji danych między użytkownikiem a prawdziwą wieżą, próbując przejąć aktywną sesję. Po otrzymaniu żądania użytkownika atakujący manipuluje ruchem za pomocą wirtualnej wieży i przekierowuje ofiarę na złośliwe strony internetowe. Atak ten jest przeprowadzany na „warstwie 2", znanej jako warstwa łącza danych, która odpowiada za udostępnianie informacji za pośrednictwem sieci bezprzewodowych ze standardowymi technologiami szyfrowania danych. Umożliwia także wielu użytkownikom dostęp do zasobów sieciowych i określa sposób przesyłania danych między dwoma węzłami bez żadnych przeszkód. Wykorzystując luki w zabezpieczeniach lub wady projektowe w tej warstwie, osoba atakująca próbuje przejąć kontrolę nad danymi przeglądania i modyfikuje dane wprowadzane przez użytkownika za pomocą sfałszowanego serwera DNS, przekierowując użytkownika do niezamierzonych lub szkodliwych stron internetowych.

Kroki związane z atakiem aLTEr podsumowano w następujący sposób.

Atakujący instaluje złośliwą wieżę udającą prawdziwą wieżę.

Atakujący określa pozycję użytkownika i wysyła pakiet, który wygląda na ważny

prośba do prawdziwej wieży.

Prawdziwa wieża odpowiada żądanym linkiem internetowym.

Atakujący łączy użytkownika z niechcianymi lub szkodliwymi witrynami internetowymi.

Atak tunelu czasoprzestrzennego

Atak tunelem czasoprzestrzennym wykorzystuje dynamiczne protokoły routingu, takie jak Dynamic Source Routing (DSR) i Ad-Hoc On-Demand Distance Vector (AODV). W tym ataku atakujący lokalizuje się strategicznie w sieci docelowej, aby wąchać i rejestrować trwające transmisje bezprzewodowe. Z tej lokalizacji atakujący ogłasza, że złośliwy węzeł ma najkrótszą trasę do przesyłania danych do innych węzłów w sieci. Aby przeprowadzić podsłuchiwanie i zarejestrować trwającą komunikację, atakujący tworzy tunel do przekazywania danych między węzłem źródłowym a docelowym. W bezprzewodowych sieciach czujników protokoły, takie jak AODV i DSR, wykorzystują komunikaty żądania trasy (RREQ) i odpowiedzi na trasę (RREP) do wykrywania dynamicznej trasy między węzłami źródłowymi i docelowymi. Na przykład węzeł źródłowy (S) wysyła pakiet RREQ, który jest komunikatem rozgłoszeniowym do węzła docelowego (D), a węzeł D odpowiada wysyłając pakiet RREP, który jest

komunikatem emisji pojedynczej. RREP zawiera informacje o trasie do osiągnięcia D. Kiedy S odbiera ten komunikat, przechowuje te informacje w swojej pamięci podręcznej tras i przesyła wszystkie dane aplikacji do D przy użyciu tej trasy. W ataku tunelem czasoprzestrzennym atakujący próbuje zbudować tunel między S i D za pomocą złośliwego węzła (M) w zasięgu transmisji S i D. Atakujący nasłuchuje ruchu sieciowego oczekującego na komunikaty RREQ. Kiedy S próbuje przesłać jakieś dane aplikacji do D, najpierw wysyła wiadomość RREQ, aby odkryć trasę do D. Atakujący wyszukuje tę wiadomość RREQ od S i przekazuje wiadomość RREQ bezpośrednio do D, zanim oryginalna wiadomość RREQ dotrze do D. Podobnie, atakujący wyszukuje wiadomość RREP z D i przekazuje ją do S, zanim oryginalna wiadomość RREP dotrze do S, tworząc w ten sposób fałszywe bezpośrednie łącze między S i D przez M. Po ustanowieniu udanego tunelu między S i D, atakujący zaczyna kontrolować dane przepływ między dwoma węzłami i może rozpocząć wykonywanie innych typów ataków. Ataki tunelami czasoprzestrzennymi stanowią poważne zagrożenie dla bezprzewodowych sieci czujników, ponieważ osoby atakujące wykorzystujące ten atak mogą manipulować danymi dotyczącymi tras i aplikacji w czasie rzeczywistym, poważnie wpływając na poufność, integralność i dostępność danych sieciowych.

Atak na dziurę

Atak typu sinkhole to odmiana ataku z przekierowaniem selektywnym, w którym atakujący reklamuje zainfekowany lub złośliwy węzeł jako najkrótszą możliwą trasę do stacji bazowej. Atakujący umieszcza złośliwy węzeł w pobliżu stacji bazowej i przyciąga wszystkie sąsiednie węzły fałszywymi informacjami o ścieżce trasowania, a następnie przeprowadza atak fałszowania danych. Atakujący używają zainfekowanego węzła do wąchania i manipulowania wszystkimi trwającymi transmisjami sieciowymi. Atak typu sinkhole może być również przeprowadzony jednocześnie z atakiem tunelem czasoprzestrzennym, w którym złośliwy węzeł może zająć cały ruch sieciowy i wykorzystać technikę tunelowania, aby dotrzeć do stacji bazowej szybciej niż inne węzły. Atak typu sinkhole jest trudny do wykrycia i może niekorzystnie wpłynąć na aplikacje wyższych warstw w modelu Open Systems Interconnection (OSI).

Eskalacja uprawnień międzyukładowych/bezprzewodowy atak koegzystencji

Atak polegający na eskalacji uprawnień między chipami wykorzystuje luki w zabezpieczeniach układów bezprzewodowych obsługujących komunikację bezprzewodową, takich jak Bluetooth i Wi-Fi. Producenci często projektują osobne chipy dla Bluetooth i Wi-Fi. Alternatywnie, projektują układ typu combo dla obu rodzajów komunikacji bezprzewodowej. Atakujący wykorzystują kombinowane chipy, aby wykorzystać jeden chip do kradzieży danych z innego chipa i wykonać boczne ruchy w celu wykorzystania innych chipów. Na przykład podczas udostępniania zasobów układ Bluetooth może bezpośrednio przechwytywać dane uwierzytelniające lub inne poufne dane z układu Wi-Fi lub manipulować ruchem przechodzącym przez układ Wi-Fi. Może to spowodować atak dotyczący współistnienia sieci bezprzewodowych, który może prowadzić do eskalacji uprawnień na granicach chipów.

Fałszowanie GNSS

Globalny system nawigacji satelitarnej (GNSS) to konstelacja satelitów, która przesyła sygnały do odbiorników GNSS. Odbiorniki GNSS są instalowane w wielu systemach elektronicznych, takich jak telefony komórkowe i pojazdy. Komunikacja w systemie GNSS odbywa się pomiędzy satelitami a odbiornikami GNSS za pośrednictwem kontrolera. Fałszowanie GNSS to procedura, w której atakujący modyfikuje prawidłowe pomiary sygnału GNSS docelowego użytkownika — pozycję, nawigację i czas (PNT) — za pomocą szkodliwych sygnałów i nadaje te same sygnały do odbiornika GNSS docelowego użytkownika. Odbierając szkodliwy sygnał, odbiornik GNSS użytkownika uważa go za autentyczny. W związku z tym atakujący może zmusić ofiary do fałszywego pozycjonowania i synchronizacji. Podobnie

jak w przypadku ataku zagłuszającego, spoofing powoduje inną formę zakłóceń, która zmusza użytkowników do uwierzenia, że znajdują się w fałszywej pozycji.

Techniki fałszowania GNSS

Atakujący wykonują fałszowanie GNSS przy użyciu następujących technik.

Przerwanie mechanizmu blokującego

Celem atakujących jest odkrycie nowego zamka odbiornika GNSS za pomocą wadliwego sygnału. Atakujący inicjują ten proces emitując sygnał zagłuszający wewnątrz odbiornika GNSS, gdzie otrzymują żądania kolejnej akwizycji. Następnie symulator sygnału jest używany do generowania fałszywego sygnału, przesyłania go do docelowego odbiornika GNSS i uzyskiwania nowych danych blokady odbiornika.

Strategia przeciągania

Atakujący śledzą pozycję odbiornika i identyfikują odchylenie od pierwotnej lokalizacji do fałszywej. Atakujący inicjują tę technikę, odzwierciedlając oryginalne sygnały nawigacyjne, wprowadzając stopniową niewspółosiowość między tymi sygnałami i przesyłając je do odbiornika GNSS. Strategia drag-off to skuteczny atak, który chroni atakujących przed wykryciem przez systemy radarowe.

Metodologia anulowania

Atakujący używają podwójnej transmisji sygnału, aby wyeliminować pojedyncze sfałszowane sygnały, wprowadzając fałszywe dane satelitarne. Sygnały docelowe są początkowo sfałszowane, a ten ostatni jest dodawany z fałszywym komponentem, który oszukuje docelowy odbiornik GNSS. Ta metoda jest korzystna dla atakującego pod względem wyodrębnienia danych fazy kodu, ale ograniczona pod względem uzyskania dopasowania amplitudy i fazy nośnej.

Metoda Meaconinga

Atakujący mają na celu zablokowanie i ponowne nadanie oryginalnych sygnałów w celu zamaskowania rzeczywistego sygnału w kierunku docelowego odbiornika. Ten atak jest skuteczny w przypadku meaconów jedno- i wieloantenowych, które kontrolują wiele satelitów i umożliwiają atakującym manipulowanie oryginalnym sygnałem za pomocą fałszywych danych pozycjonowania i czasów opóźnienia. Atakujący preferują tę metodę, gdy fałszerz nie jest w stanie wygenerować sekwencji rozprzestrzeniania.

Metodologia hakowania bezprzewodowego

Aby zhakować sieci bezprzewodowe, osoba atakująca postępuje zgodnie z metodologią hakerską obejmującą systematyczne kroki w celu przeprowadzenia skutecznego ataku na docelową sieć bezprzewodową. Ta sekcja wyjaśnia kroki metodologii hakowania bezprzewodowego. Metodologia hakowania bezprzewodowego pomaga atakującemu osiągnąć cel, jakim jest zhakowanie docelowej sieci bezprzewodowej. Osoba atakująca zwykle stosuje metodologię hakowania, aby mieć pewność, że znajdzie każdy pojedynczy punkt wejścia, aby włamać się do sieci docelowej. Celem metodologii hakowania bezprzewodowego jest złamanie zabezpieczeń sieci Wi-Fi w celu uzyskania nieautoryzowanego dostępu do zasobów sieciowych. Atakujący wykonują następujące kroki, aby przeprowadzić bezprzewodowe hakowanie:

Odkrycie Wi-Fi

Mapowanie GPS

Analiza ruchu bezprzewodowego

Rozpoczęcie ataków bezprzewodowych

Łamanie szyfrowania Wi-Fi

Kompromitacja sieci Wi-Fi

Wykrywanie Wi-Fi

Pierwszym krokiem jest znalezienie sieci lub urządzenia Wi-Fi. Atakujący przeprowadza wykrywanie Wi-Fi w celu zlokalizowania docelowej sieci bezprzewodowej za pomocą narzędzi, takich jak inSSIDer, NetSurveyor itp. Procedury wykrywania Wi-Fi obejmują śledzenie sieci bezprzewodowych i znajdowanie odpowiedniej sieci docelowej, która znajduje się w zasięgu, aby przeprowadzić atak.

Obciążenie sieci bezprzewodowej

Atak na sieć bezprzewodową rozpoczyna się od jej wykrycia i śledzenia. Footprinting obejmuje lokalizację i analizę (lub zrozumienie) sieci. Aby określić ślad sieci bezprzewodowej, osoba atakująca musi zidentyfikować BSS zapewniane przez punkt dostępowy. Atakujący może zidentyfikować BSS lub niezależny BSS (IBSS) za pomocą identyfikatora SSID sieci bezprzewodowej. Dlatego atakujący musi określić identyfikator SSID docelowej sieci bezprzewodowej, który może zostać wykorzystany do ustanowienia powiązania z punktem dostępowym w celu naruszenia jego bezpieczeństwa. Osoba atakująca może użyć następujących dwóch metod śledzenia, aby wykryć identyfikator SSID sieci bezprzewodowej:

Metoda pasywnego śladu

Wykorzystując metodę pasywną, atakujący wykrywa istnienie punktu dostępowego poprzez wąchanie pakietów z fal radiowych. Ujawnia to urządzenia bezprzewodowe, punkty dostępowe i identyfikator SSID. W metodzie pasywnego śledzenia atakujący nie próbuje łączyć się z żadnymi punktami dostępowymi ani klientami bezprzewodowymi, ani nie wprowadza żadnych pakietów danych do ruchu bezprzewodowego.

Metoda Active Footprinting

W tej metodzie urządzenie bezprzewodowe atakującego wysyła żądanie sondy z identyfikatorem SSID do punktu dostępowego i czeka na odpowiedź. Jeśli urządzenie bezprzewodowe nie ma wcześniej identyfikatora SSID, może wysłać żądanie sondy z pustym identyfikatorem SSID. W przypadku żądania sondy z pustym identyfikatorem SSID większość punktów dostępowych odpowiada własnym identyfikatorem SSID w pakiecie odpowiedzi sondy. W związku z tym puste identyfikatory SSID są przydatne do uczenia się identyfikatorów SSID punktów dostępowych. W tej metodzie atakujący zna właściwy BSS, z którym ma się powiązać i może skonfigurować punkt dostępowy, aby ignorował żądanie sondy z pustym identyfikatorem SSID. Atakujący może skanować w poszukiwaniu sieci Wi-Fi za pomocą narzędzi do skanowania sieci bezprzewodowych, takich jak NetSurveyor i Wi-Fi Scanner. Identyfikator SSID jest obecny w sygnałach nawigacyjnych, żądaniach sondy i odpowiedziach, a także żądaniach skojarzenia i ponownego skojarzenia. Napastnik może uzyskać identyfikator SSID sieci poprzez skanowanie pasywne. Atakujący, któremu nie uda się uzyskać identyfikatora SSID poprzez skanowanie pasywne, może go wykryć poprzez skanowanie aktywne. Następnie atakujący może połączyć się z siecią bezprzewodową i przeprowadzić atak. Skanowanie sieci bezprzewodowej umożliwia wąchanie poprzez dostrajanie się do różnych kanałów radiowych urządzeń.

Wyszukiwanie sieci Wi-Fi w zasięgu ataku

Pierwszym zadaniem atakującego szukającego celów Wi-Fi jest sprawdzenie potencjalnych sieci znajdujących się w zasięgu, aby znaleźć najlepszą do zaatakowania. Atakujący używają różnych technik kredowania Wi-Fi, takich jak WarWalking, WarChalking, WarFlying i WarDriving, aby znaleźć docelową sieć Wi-Fi.

Techniki kredowania Wi-Fi

o WarWalking: Atakujący chodzą z laptopami obsługującymi Wi-Fi z zainstalowanym narzędziem do wykrywania sieci bezprzewodowych w celu mapowania otwartych sieci bezprzewodowych.

o WarChalking: Symbole są rysowane w miejscach publicznych w celu reklamowania otwartych sieci Wi-Fi.

o Warflying: Atakujący wykorzystują drony do wykrywania otwartych sieci bezprzewodowych.

o WarDriving: Atakujący poruszają się po okolicy z laptopami obsługującymi Wi-Fi, na których zainstalowano narzędzie do wykrywania sieci bezprzewodowych w celu mapowania otwartych sieci bezprzewodowych.

Atakujący używają następujących narzędzi do wykrywania sieci Wi-Fi w celu przeprowadzania ataków:

* Laptop z kartą Wi-Fi

* Zewnętrzna antena Wi-Fi

* Oprogramowanie do wykrywania sieci

Niektóre z narzędzi używanych do wykrywania sieci Wi-Fi w zasięgu ataku to inSSIDer, NetSurveyor, Skaner Wi-Fi i Acrylic Wi-Fi Home.

Wyszukiwanie punktów dostępowych obsługujących WPS

Atakujący używają narzędzia wiersza poleceń Wash do identyfikowania punktów dostępowych obsługujących WPS w docelowej sieci bezprzewodowej. To narzędzie pomaga również atakującym sprawdzić, czy punkt dostępowy jest zablokowany. Większość routerów z obsługą WPS jest blokowana automatycznie, gdy nieprawidłowe dane uwierzytelniające zostaną wprowadzone więcej niż 5 razy pod rząd, i można je odblokować tylko ręcznie w interfejsie administratora routera. Polecenie Wash obsługuje kanał 5 GHz i może być używane po zainstalowaniu pakietu Reaver. Poniżej przedstawiono niektóre z ważnych argumentów polecenia Wash używanych przez osoby atakujące:

-i, --interface=<iface> (określa interfejs do przechwytywania pakietów)

-a, --all (wyświetla wszystkie punkty dostępu, w tym te z wyłączonym WPS)

-f, --file [PLIKI PLIK2 PLIK3 ...] (odczytuje pakiety z przechwyconych plików)

-c, --channei=<liczba> (określa kanał do słuchania [auto])

-o, --out-fiie=<fiie> (zapisuje dane do pliku)

-n,--probes=<liczba> (określa maksymalną liczbę sond do wysłania do każdego punktu dostępowego w trybie skanowania)

-D, --daemonize (polecenie Wash)

-5, --5ghz (polecenie użycia kanałów 5 GHz 802.11)

-s, --scan (polecenie do uruchomienia w trybie skanowania)

- u, --survey (polecenie, aby użyć trybu ankiety [domyślnie])

Atakujący używają następującego polecenia, aby wykryć punkt dostępu, identyfikator zestawu usług rozszerzonych (ESSID) i identyfikator BSSID urządzenia lub routera:

sudo wash -i wlan0

Narzędzia do wykrywania Wi-Fi

inSSIDer

inSSIDer to narzędzie do optymalizacji Wi-Fi i rozwiązywania problemów, które skanuje w poszukiwaniu sieci bezprzewodowych z adapterem Wi-Fi użytkownika, dzięki czemu użytkownik może wizualizować siłę sygnału i kanały, z których korzysta. Zawiera również przydatne informacje o każdej sieci. Atakujący używają inSSIDer do wykrywania punktów dostępowych Wi-Fi i urządzeń w ich pobliżu.

Cechy:

o Inspekcja sieci WLAN i otaczających sieci w celu rozwiązania problemów z konkurencyjnymi punktami dostępowymi

o Śledzi siłę odbieranego sygnału w dBm w czasie i filtruje punkty dostępowe

o Wyróżnia punkty dostępowe dla obszarów o wysokim stężeniu Wi-Fi

o Eksportuje dane Wi-Fi i GPS do pliku KML, aby wyświetlić je w Google Earth

o Pokazuje nakładające się kanały sieci Wi-Fi

NetSurveyor

NetSurveyor to narzędzie do wykrywania sieci 802.11, które gromadzi informacje o pobliskich bezprzewodowych punktach dostępowych w czasie rzeczywistym i wyświetla je w różnych widokach diagnostycznych i wykresach. Dane mogą być zapisywane przez dłuższy czas i odtwarzane później. NetSurveyor generuje również raporty w formacie Adobe PDF. Atakujący używają NetSurveyor do wykrywania sieci Wi-Fi, lokalnych punktów dostępowych i siły sygnału ich beaconów.

Oprócz powyższego istnieje wiele narzędzi, których atakujący mogą użyć do wykrycia docelowych sieci Wi-Fi. Te narzędzia do wykrywania sieci Wi-Fi pomagają atakującemu w wykrywaniu sieci (BSS/IBSS) oraz sieci rozgłaszających lub nierozgłaszających ESSID, ich możliwości WEP oraz producentów sprzętu. Te narzędzia umożliwiają karcie Wi-Fi znalezienie zabezpieczonych i niezabezpieczonych połączeń bezprzewodowych. Oto niektóre z dodatkowych narzędzi do wykrywania sieci Wi-Fi:

Skaner Wi-Fi (https://lizordsystems.com)

Acrylic Wi-Fi Home (https://www.ocrylicwifi.com)

WirelessMon (https://www.possmork.com)

Ekahau Wi-Fi Heatmaps (https://www.ekohou.com)

Mobilne narzędzia do wykrywania Wi-Fi

Analizator Wi-Fi

WiFi Analyzer to narzędzie do optymalizacji sieci Wi-Fi, które służy do badania otaczających sieci Wi-Fi, mierzenia siły ich sygnału i identyfikowania zatłoczonych kanałów. Atakujący używają WiFi Analyzer do wykrywania pobliskich punktów dostępowych, tworzenia wykresów siły sygnału kanałów, szacowania odległości do punktów dostępowych itp.

Oto niektóre z dodatkowych mobilnych narzędzi do wykrywania sieci Wi-Fi:

OpenSignal (https://opensignal.com)

Network Signal Info Pro (https://www.kaibits-software.com)

Menedżer Wi-Fi (https://kmansoft.com)

Network Refresher: Network Signal Refresher (https://play.google.com)

Skaner Wi-Fi (https://play.google.com)

Mapowanie GPS

Drugim krokiem w metodologii bezprzewodowego hakowania jest mapowanie GPS. Osoba atakująca, która wykryje docelową sieć bezprzewodową, może przystąpić do hakowania bezprzewodowego, rysując mapę sieci. Na tym etapie atakujący może użyć różnych zautomatyzowanych narzędzi do mapowania docelowej sieci bezprzewodowej. Globalny system pozycjonowania (GPS) to kosmiczny system nawigacji satelitarnej, który zapewnia lokalizację fizycznych obiektów na Ziemi wraz z czasem ich obecności w tym miejscu. Korzystając z narzędzia GPS, każdy może znaleźć określoną lokalizację na Ziemi i jej cechy geograficzne. Osoba atakująca używa tego narzędzia GPS do zlokalizowania i zmapowania docelowej sieci bezprzewodowej na określonym obszarze geograficznym. Odbiornik GPS oblicza pozycję, czas i prędkość, przetwarzając specjalnie zakodowane sygnały satelitarne. Atakujący wiedzą, że obecność bezpłatnych sieci Wi-Fi na danym obszarze może wskazywać na istnienie niezabezpieczonej sieci. Atakujący zwykle tworzą mapy wykrytych sieci Wi-Fi oraz bazę danych ze statystykami zebranymi za pomocą narzędzi do wykrywania Wi-Fi, takich jak inSSIDer Office i NetSurveyor. GPS jest przydatny w śledzeniu lokalizacji wykrytych sieci Wi-Fi i współrzędnych przesłanych do witryn takich jak WiGFE. Atakujący mogą udostępniać takie informacje społeczności hakerów lub sprzedawać je z zyskiem.

WiGL

WiGFE konsoliduje informacje o sieciach bezprzewodowych na całym świecie, w tym ich lokalizacji, w centralnej bazie danych i udostępnia przyjazne dla użytkownika aplikacje Java, Windows i sieciowe, które mogą mapować, wyszukiwać i aktualizować bazę danych przez Internet. Sieć bezprzewodową można dodać do WiGLE z pliku potknięcia lub ręcznie, a uwagi można dodać do istniejących sieci. Lokalizację wykrytych sieci Wi-Fi można śledzić za pomocą WiGLE, wykonując następujące czynności.

o Przejdź do https://wigle.net i kliknij Przesłane.

o Na stronie przesyłania kliknij PRZEŚLIJ PLIK, aby przesłać plik dziennika.

Uwaga: WiGLE obsługuje obecnie formaty DStumbler, G-Mon, inSSIDer, KisMAC, Kismet, MacStumbler, NetStumbler, Pocket Warrior, Wardrive-Android, WiFiFoFum, WiFi-Where, WiGLE WiFi Wardriving i skonsolidowana baza danych firmy Apple.

o Pojawi się wyskakujące okienko, pokazujące typy plików obsługiwanych do przesłania. Kliknij Wybierz plik. W wyskakującym okienku, które pojawi się w celu wybrania pliku, wybierz narzędzia wykrywania Wi-Fi, a następnie plik dziennika do przesłania. Na koniec kliknij Wyślij.

o WiGLE pokazuje następnie pełne informacje o lokalizacji sieci Wi-Fi.

Narzędzia do mapowania GPS

Oprogramowanie do mapowania Maptitude

Dzięki oprogramowaniu mapującemu Maptitude i odbiornikowi GPS osoby atakujące mogą śledzić lokalizację ofiary za pomocą komputera przenośnego, zbierać dane terenowe i tworzyć nowe lub aktualizowane pliki geograficzne oznaczające obiekty na mapie. Mówiąc szczegółowo, oprogramowanie Maptitude Mapping Software umożliwia atakującym wykonanie następujących czynności:

o Śledź lokalizację odbiornika GPS na mapie

o Rejestruj dane GPS

o Importuj dane odtwarzania GPS z ręcznego odbiornika GPS

o Lokalizowanie punktów według współrzędnych lub długości/szerokości geograficznej

o Wybierz znaczniki, pinezki i niestandardowe ikony dla lokalizacji

Oto kilka dodatkowych narzędzi mapowania GPS:

Skyhook (https://www.skyhook.com)

ExpertGPS (https://www.expertgps.com)

GPS Visualizer (https://www.gpsvisuolizer.com)

Mapwel (https://www.mopwel.net)

TrackMaker (https://www.trockmoker.com)

Narzędzia do wyszukiwania hotspotów Wi-Fi

Wyszukiwarka Wi-Fi

Wi-Fi Finder to aplikacja mobilna na Androida, której można używać do wyszukiwania bezpłatnych lub płatnych publicznych hotspotów Wi-Fi online lub offline. Atakujący używają Wi-Fi Finder do wyszukiwania hotspotów Wi-Fi w pobliżu i uzyskują dostęp do swoich danych. Jego funkcje obejmują:

o Wyszukaj pobliskie hotspoty Wi-Fi

o Wyszukiwanie publicznych sieci Wi-Fi w dowolnym miejscu na świecie

o Zobacz szczegóły hotspotu Wi-Fi, lokalizacje połączeń, uzyskaj wskazówki lub udostępnij hotspot

o Filtruj wyniki według lokalizacji (kawiarnia, hotel itp.) lub typu dostawcy

Oto kilka dodatkowych narzędzi do wyszukiwania hotspotów Wi-Fi:

Homedale::Wi-Fi/WLAN Monitor (https://www.the-sz.com)

Fing - narzędzia sieciowe (https://play.google.com)

WiFi Finder - Free WiFi Map (https://play.google.com)

Wi-Fi Map (https://play.google.com)

Find Wifi & Connect to Wi-Fi (https://play.google.com)

Wykrywanie sieci Wi-Fi poprzez WarDriving

WarDriving można wykorzystać do wykrywania sieci Wi-Fi za pomocą następującej procedury.

Zarejestruj się w WiGLE (https://wigle.net) i pobierz pakiety map obszaru docelowego, aby wyświetlić naniesione punkty dostępowe na mapie.

Podłącz laptopa do anteny i urządzenia GPS za pomocą adaptera szeregowego USB i wsiądź do samochodu.

Zainstaluj i uruchom oprogramowanie klienckie NetStumbler i WiGLE oraz włącz urządzenie GPS.

Prowadź samochód z prędkością 35 mil na godzinę lub niższą (przy wyższych prędkościach antena Wi-Fi nie będzie w stanie wykryć sieci Wi-Fi).

Przechwyć i zapisz pliki dziennika NetStumbler, które zawierają współrzędne GPS punktów dostępowych.

Prześlij ten plik dziennika do WiGLE, który automatycznie naniesie punkty na mapę.

Analiza ruchu bezprzewodowego

Trzecim krokiem w metodologii hakowania bezprzewodowego jest analiza ruchu w wykrytej sieci bezprzewodowej. Osoba atakująca przeprowadza analizę ruchu sieci bezprzewodowej przed rozpoczęciem rzeczywistych ataków na sieć bezprzewodową. Ta analiza pomaga atakującemu określić słabe punkty i podatne ofiary w docelowej sieci, a także odpowiednią strategię skutecznego ataku. Atakujący wykorzystuje różne narzędzia i techniki do analizy ruchu docelowej sieci bezprzewodowej. Protokoły Wi-Fi są unikalne dla warstwy 2, a ruch w powietrzu nie jest serializowany, co ułatwia wąchanie i analizowanie pakietów bezprzewodowych. Atakujący analizują sieć bezprzewodową w celu określenia rozgłaszanego identyfikatora SSID, obecności wielu punktów dostępowych, możliwości odzyskania identyfikatorów SSID, zastosowanej metody uwierzytelniania, algorytmów szyfrowania WLAN itp. Atakujący wykorzystują narzędzia do podsłuchiwania pakietów Wi-Fi, takie jak AirMagnet WiFi Analyzer PRO, Wireshark, SteelCentral Packet Analyzer, OmniPeek Network Protocol Analyzer i CommView dla Wi-Fi do przechwytywania i analizowania ruchu w docelowej sieci bezprzewodowej.

Wybór optymalnej karty Wi-Fi

Wybór optymalnej karty Wi-Fi jest bardzo ważny dla atakującego, ponieważ narzędzia takie jak aircrack-ng i KisMAC działają tylko z wybranymi chipsetami bezprzewodowymi. Przy wyborze optymalnej karty Wi-Fi osoba atakująca bierze pod uwagę następujące kwestie.

Określ wymagania Wi-Fi: osoba atakująca może chcieć nasłuchiwać ruchu w sieci bezprzewodowej lub zarówno nasłuchiwać, jak i wprowadzać pakiety. Systemy Windows mogą nasłuchiwać ruchu sieciowego, ale nie mają możliwości wstrzykiwania pakietów danych, podczas gdy Linux ma możliwość zarówno nasłuchiwania, jak i wstrzykiwania

Poznaj możliwości karty bezprzewodowej: Karty bezprzewodowe mają dwóch producentów. Jedna to marka karty, a druga to producent chipsetu. Znajomość producenta i modelu karty nie wystarczy, aby wybrać kartę Wi-Fi. Atakujący musi również wiedzieć o chipsecie karty. Większość producentów kart niechętnie ujawnia chipset używany w ich kartach, ale te informacje są krytyczne dla atakującego, ponieważ pozwalają mu określić obsługiwany system operacyjny, wymagane sterowniki oprogramowania i ograniczenia.

Określenie chipsetu karty Wi-Fi: Osoba atakująca może określić chipset karty Wi-Fi za pomocą następujących technik.

o Przeszukaj Internet.

o Zobacz nazwy plików sterowników Windows, które często ujawniają nazwę chipsetu,

o Sprawdź stronę producenta.

o Bezprzewodowy układ scalony można bezpośrednio przeglądać w przypadku niektórych kart. Często można również zaobserwować numer chipsetu.

o Wyszukiwanie identyfikatorów Federalnej Komisji Łączności (FCC) może służyć do wyszukiwania szczegółowych informacji o urządzeniu, jeśli numer identyfikacyjny FCC jest wydrukowany na płycie. To wyszukiwanie zwróci informacje o producencie, modelu i chipsecie.

Producenci kart czasami zmieniają chipset karty, zachowując numer modelu. Producenci mogą nazywać to „wersją karty" lub „wersją karty". Dlatego wyszukiwanie przeprowadzane przez osobę atakującą musi obejmować wersję lub poprawkę. Metoda określania tego może się różnić w zależności od systemu operacyjnego. Witryna https://wireless.wiki.kernel.org/en/users/Drivers może zawierać informacje o zgodności.

Sprawdź możliwości chipsetu: Przed wyborem karty Wi-Fi osoba atakująca musi sprawdzić, czy chipset jest zgodny z systemem operacyjnym i spełnia wszystkie wymagania.

Określ wymagane sterowniki i poprawki: osoby atakujące muszą określić sterowniki wymagane dla chipsetu oraz wszelkie poprawki wymagane dla systemu operacyjnego.

Po rozważeniu wszystkich tych aspektów w celu wybrania chipsetu atakujący wybiera kartę, która korzysta z tego konkretnego chipsetu, korzystając z listy zgodnych kart.

Sniffowanie ruchu bezprzewodowego

Sniffing to rodzaj podsłuchiwania, w którym atakujący przechwytują całą trwającą komunikację bezprzewodową. Atakujący wykonują bezprzewodowe podsłuchiwanie, po prostu dostrajając odbiornik do docelowej częstotliwości transmisji i identyfikując używany docelowy protokół komunikacyjny. Atakujący analizują przechwycony ruch w celu przeprowadzenia dalszych ataków na sieć docelową. Aby wykryć ruch bezprzewodowy, osoba atakująca musi włączyć tryb monitorowania na swojej karcie Wi-Fi. Wszystkie karty Wi-Fi nie obsługują trybu monitora w systemie Windows. Poniższy link może być użyty do sprawdzenia, czy https://secwiki.Org/w/Npcap/WiFi_adapters

Atakujący używają narzędzi takich jak Wireshark z Npcap, SteelCentral Packet Analyzer, OmniPeek Network Protocol Analyzer, CommView dla Wi-Fi i Kismet do sniffowania sieci bezprzewodowych.

Wireshark z Npcapem

Wireshark to sniffer i analizator protokołów sieciowych. Pozwala użytkownikom przechwytywać i interaktywnie przeglądać ruch w sieci docelowej. Wireshark może odczytywać bieżące dane z sieci Ethernet, sieci Token Ring, sieci FDDI, sieci protokołu Point-to-Point (PPP) i protokołu Serial Line Internet Protocol (SLIP), bezprzewodowej sieci LAN 802.11, połączeń z bankomatami (jeśli bankomat OS pozwala na to Wireshark) i dowolne urządzenie obsługiwane w systemie Linux przez najnowsze wersje libpcap. Npcap jest zintegrowany z Wireshark w celu pełnej analizy ruchu WLAN, wizualizacji, drążenia i raportowania. Atakujący przechwytują ruch bezprzewodowy, włączając tryb monitorowania w programie Wireshark. Wireshark umożliwia atakującym przechwytywanie ogromnej liczby ramek

zarządzania, ramek kontrolnych, ramek danych itp., a ponadto pomaga im analizować pola nagłówka Radiotap w celu zebrania krytycznych informacji, takich jak używane protokoły, stosowane techniki szyfrowania, długości ramek i adresy MAC.

Wykonaj analizę widma

Osoba atakująca może użyć analizatorów widma, aby wykryć obecność sieci bezprzewodowych. Analiza widma sieci bezprzewodowych umożliwia atakującemu aktywne monitorowanie wykorzystania widma na określonym obszarze i wykrywanie widma sygnału sieci docelowej. Pomaga również atakującemu zmierzyć moc widmową znanych i nieznanych sygnałów. Analizatory widma wykorzystują analizę statystyczną do wykreślania wykorzystania widma, ilościowego określania „jakości powietrza" i izolowania źródeł transmisji. Technicy RF używają analizatorów widma RF do instalowania i utrzymywania sieci bezprzewodowych oraz identyfikowania źródeł zakłóceń. Analiza widma Wi-Fi pomaga również w wykrywaniu ataków bezprzewodowych, w tym ataków DoS, ataków uwierzytelniających/szyfrujących oraz ataków penetrujących sieć.

Poniżej przedstawiono niektóre zautomatyzowane narzędzia wykorzystywane przez osoby atakujące do analizy widma docelowej sieci bezprzewodowej.

RF Explorer

RF Explorer to narzędzie do analizy widma RF. Może działać jako samodzielny, ręczny analizator widma RF lub jako interfejs z komputerem PC z bardziej zaawansowanym oprogramowaniem do analizy danych. Analizator widma RF jest instrumentem z wyboru do wstępnego wykrywania i identyfikacji źródeł zakłóceń RF oraz późniejszego monitorowania stanu systemu bezprzewodowego. RF Explorer jest podstawowym narzędziem służącym do obserwacji transmitowanych sygnałów RF i pomaga użytkownikowi, zapewniając widok lokalnego środowiska RF. Ten widok RF może być wykorzystany do wykrywania obecności transmisji RF, które są źródłem zakłóceń.

Rozpoczęcie ataków bezprzewodowych

Po zakończeniu wykrywania sieci bezprzewodowej, mapowania i analizy docelowej sieci bezprzewodowej atakujący będzie mógł przeprowadzić atak na docelową sieć bezprzewodową. Atakujący może przeprowadzać różne rodzaje ataków, takie jak ataki fragmentacyjne, ataki polegające na fałszowaniu adresów MAC, ataki DoS i ataki z użyciem protokołu ARP (Address Resolution Protocol). W tej sekcji opisano ataki bezprzewodowe i sposób ich przeprowadzania.

Aircrack-ng Suite

Aircrack-ng to pakiet oprogramowania sieciowego składający się z detektora, sniffera pakietów, crackera WEP i WPA/WPA2 PSK oraz narzędzia do analizy sieci bezprzewodowych 802.11. Ten program działa pod Linuksem i Windowsem.

Airbase-ng: przechwytuje uzgadnianie WPA/WPA2 i może działać jako punkt dostępowy ad-hoc.

Aircrack-ng: Ten program jest de facto narzędziem do łamania WEP i WPA/WPA2 PSK.

Airdecap-ng: Odszyfrowuje WEP/WPA/WPA2 i może być używany do usuwania nagłówków bezprzewodowych z pakietów Wi-Fi.

Airdecloak-ng: Usuwa maskowanie WEP z pliku pcap.

Airdrop-ng: ten program służy do ukierunkowanego, opartego na regułach cofnięcia uwierzytelnienia użytkowników.

Aireplay-ng: Służy do generowania ruchu, fałszywego uwierzytelniania, odtwarzania pakietów i wstrzykiwania żądań ARP.

Airgraph-ng: Ten program tworzy relację klient-AP i wspólny wykres sondy z pliku airodump.

Airmon-ng: Służy do przełączania z trybu zarządzanego do trybu monitorowania na interfejsach bezprzewodowych i odwrotnie.

Airodump-ng: Ten program służy do przechwytywania pakietów nieprzetworzonych ramek 802.11 i zbierania danych WEP IV.

Airolib-ng: Ten program przechowuje i zarządza listami ESSID i haseł używanymi do łamania WPA/WPA2.

Airserv-ng: Pozwala wielu programom na niezależne korzystanie z karty Wi-Fi za pośrednictwem połączenia TCP klienta i serwera.

Airtun-ng: Tworzy interfejs wirtualnego tunelu do monitorowania zaszyfrowanego ruchu i wprowadzania dowolnego ruchu do sieci.

Easside-ng: Ten program umożliwia użytkownikowi komunikację za pośrednictwem punktu dostępowego z szyfrowaniem WEP bez znajomości klucza WEP.

Packetforge-ng: Atakujący mogą używać tego programu do tworzenia zaszyfrowanych pakietów, które następnie można wykorzystać do wstrzyknięcia.

Tkiptun-ng: wstrzykuje ramki do sieci WPA TKIP z QoS i może odzyskiwać klucze MIC i strumienie kluczy z ruchu Wi-Fi.

Wesside-ng: Ten program zawiera różne techniki bezproblemowego uzyskiwania klucza WEP w ciągu kilku minut.

WZCook: Służy do odzyskiwania kluczy WEP z narzędzia konfiguracji zerowej sieci bezprzewodowej systemu Windows XP.

Wykrywanie ukrytych identyfikatorów SSID

W oparciu o zasadę bezpieczeństwa przez zaciemnienie wiele organizacji ukrywa identyfikator SSID swojej sieci bezprzewodowej, nie rozgłaszając go. Jest to część polityki bezpieczeństwa wielu organizacji, ponieważ osoba atakująca może wykorzystać identyfikator SSID do naruszenia bezpieczeństwa ich sieci bezprzewodowych. Jednak ukrywanie identyfikatorów SSID nie zwiększa bezpieczeństwa. Osoba atakująca może ujawnić ukryty identyfikator SSID za pomocą pakietu aircrack-ng, wykonując następujące czynności.

Uruchom airmon-ng w trybie monitora

Uruchom airodump-ng, aby wykryć identyfikatory SSID w interfejsie

Usuń uwierzytelnienie (deauth -> -0) klienta, aby ujawnić ukryty identyfikator SSID za pomocą Aireplay-ng

Przełącz się na airodump, aby wyświetlić ujawniony identyfikator SSID

Atak fragmentacyjny

Udany atak fragmentacyjny może uzyskać 1500 bajtów algorytmu generowania pseudolosowego (PRGA). Jednak ten atak nie powoduje bezpośredniego odzyskania klucza WEP. Aby zainicjować ten atak, od docelowego punktu dostępowego musi zostać odebrany co najmniej jeden pakiet danych. Pakiet aircrack-ng pomaga atakującemu uzyskać niewielką ilość materiału klucza z pakietu, po czym próbuje wysłać pakiety ARP i/lub logicznego sterowania łączem (LLC) ze znaną zawartością do punktu dostępowego. Atakujący może zebrać większą ilość informacji o kluczach z pakietu powtórki, jeśli punkt dostępowy powtórzy ten pakiet. Atakujący powtarza ten cykl kilka razy, aby uzyskać PRTG. Atakujący może użyć PRGA z packageforge-ng do generowania pakietów do ataków iniekcyjnych.

Atak fałszowania adresu MAC

Adres MAC to unikalny identyfikator zakodowany na stałe w obwodzie karty sieciowej przez jej producenta. Niektóre sieci stosują filtrowanie adresów MAC jako środek bezpieczeństwa. Podczas fałszowania adresów MAC osoby atakujące zmieniają swój adres MAC na adres uwierzytelnionego użytkownika, aby ominąć filtrowanie adresów MAC skonfigurowane w punkcie dostępowym. Aby sfałszować adres MAC, atakujący musi po prostu ustawić wartość zwracaną przez ifconfig na inną wartość szesnastkową w formacie aa:bb:cc:dd:ee:ff. Ta zmiana jest dokonywana za pomocą polecenia sudo, które wymaga hasła roota. Atakujący używają narzędzi do fałszowania adresów MAC, takich jak Technitium MAC Address Changer i MAC Address Changer, aby zmienić adres MAC.

Narzędzia do fałszowania adresów MAC

Zmieniacz adresów MAC Technitium

Technitium MAC Address Changer umożliwia użytkownikowi natychmiastową zmianę (sfałszowanie) adresu MAC karty sieciowej. Ma prosty interfejs użytkownika i dostarcza informacji dotyczących każdej karty sieciowej w urządzeniu. Adres MAC jest używany przez sterowniki systemu Windows do uzyskiwania dostępu do sieci Ethernet LAN.

Odmowa usługi: ataki powodujące odłączenie i usunięcie uwierzytelnienia

Sieci bezprzewodowe są podatne na ataki DoS ze względu na relacje między warstwami fizyczną, łącza danych i sieci. Bezprzewodowe ataki DoS obejmują ataki powodujące odłączenie i ataki polegające na de-uwierzytelnieniu.

Atak dysocjacyjny

W przypadku ataku polegającego na odłączeniu połączenia atakujący powoduje, że ofiara jest niedostępna dla innych urządzeń bezprzewodowych, niszcząc łączność między punktem dostępowym a klientem.

Atak de-uwierzytelniający

W ataku polegającym na de-uwierzytelnieniu atakujący zalewa stacje sfałszowanymi de-uwierzytelnieniem lub odłącza się, aby odłączyć użytkowników od punktu dostępowego.

Atak typu Man-in-the-Middle

Atak man-in-the-middle (MITM) to aktywny atak internetowy, w którym osoba atakująca próbuje przechwycić, odczytać lub zmienić informacje przesyłane między dwoma komputerami. Ataki MITM są związane z sieciami WLAN 802.11 oraz systemami komunikacji przewodowej.

Podsłuchiwanie

Podsłuchiwanie jest łatwe w sieci bezprzewodowej, ponieważ do komunikacji nie jest używany żaden fizyczny nośnik. Osoba atakująca znajdująca się w pobliżu sieci bezprzewodowej może odbierać fale radiowe w sieci bezprzewodowej bez większego wysiłku i sprzętu. Ponadto osoba atakująca może zbadać całą ramkę danych przesłaną przez sieć lub zapisać ją do późniejszej oceny. Należy zaimplementować kilka warstw szyfrowania, aby uniemożliwić atakującym uzyskanie poufnych informacji. W tych warstwach można zastosować szyfrowanie WEP lub łącza danych. Ponadto należy zastosować mechanizm bezpieczeństwa, taki jak IPsec, SSFI lub SSL, w przeciwnym razie przesłane dane mogą być dostępne dla atakujących. Jednak, jak pokazano w poprzedniej sekcji, osoba atakująca może złamać zabezpieczenia WEP za pomocą narzędzi dostępnych bezpłatnie w Internecie. Dostęp do poczty za pomocą protokołu POP (Post Office Protocol) lub IMAP (Internet Message Access Protocol) jest ryzykowny, ponieważ te protokoły umożliwiają wysyłanie wiadomości e-mail przez sieć bezprzewodową bez dodatkowej formy szyfrowania. Wykwalifikowany haker może potencjalnie rejestrować gigabajty ruchu chronionego za pomocą WEP, przetwarzać dane i łamać szyfrowanie.

Manipulacja

Manipulacja to poziom wykraczający poza podsłuchiwanie. Występuje, gdy atakujący otrzymuje zaszyfrowane dane ofiary, manipuluje nimi i ponownie przesyła zmanipulowane dane ofierze. Ponadto osoba atakująca może przechwycić pakiety z zaszyfrowanymi danymi i zmienić adres docelowy, aby przesłać te pakiety przez Internet.

Osoba atakująca przeprowadza atak MUM, wykonując następujące kroki.

Atakujący sniffuje parametry sieci bezprzewodowej ofiary (adres MAC, ESSID/BSSID i liczbę kanałów).

Atakujący wysyła żądanie DEAUTH do ofiary ze sfałszowanym adresem źródłowym AP ofiary.

Po otrzymaniu żądania komputer ofiary jest usuwany z uwierzytelnienia i zaczyna przeszukiwać wszystkie kanały w poszukiwaniu nowego ważnego punktu dostępowego.

Atakujący ustawia sfałszowany punkt dostępowy na nowym kanale z oryginalnym adresem MAC (BSSID) i ESSID punktu dostępowego ofiary, łącząc w ten sposób ofiarę ze sfałszowanym punktem dostępowym.

Po udanym powiązaniu ofiary ze sfałszowanym punktem dostępowym atakujący podszywa się pod ofiarę, aby połączyć się z oryginalnym punktem dostępowym.

Atakujący ustawia się między punktem dostępowym a ofiarą, nasłuchując całego ruchu.

Atak MITM przy użyciu Aircrack-ng

Atakujący może przeprowadzić atak MITM przy użyciu aircrack-ng, wykonując następujące kroki.

Uruchom airmon-ng w trybie monitora. Uruchom airodump, aby wykryć identyfikatory SSID w interfejsie.

De-uwierzytelnij (deauth) klienta za pomocą aireplay-ng.

Skojarz kartę bezprzewodową (fałszywe skojarzenie) z punktem dostępowym, aby uzyskać do niej dostęp za pomocą funkcji aireplayng-

Bezprzewodowy atak zatruwający ARP

ARP określa adres MAC punktu dostępowego, jeśli zna on już jego adres IP. Zwykle ARP nie posiada żadnej funkcji sprawdzania, czy odpowiedzi pochodzą od prawidłowych hostów. Zatruwanie ARP to

technika ataku wykorzystująca ten brak weryfikacji. W tej technice pamięć podręczna ARP utrzymywana przez system operacyjny jest uszkodzona z powodu nieprawidłowych adresów MAC. Atakujący osiąga to, wysyłając pakiet powtórki ARP skonstruowany z nieprawidłowym adresem MAC. Atak zatruwania ARP wpływa na wszystkie hosty w podsieci. Wszystkie stacje powiązane z podsiecią dotkniętą atakiem zatruwającym ARP są podatne na atak, ponieważ większość punktów dostępowych działa jak przezroczyste mosty MAClayer. Wszystkie hosty podłączone do przełącznika lub koncentratora są podatne na ataki ARP poisoning, jeśli punkt dostępowy jest podłączony bezpośrednio do tego przełącznika lub koncentratora bez routera/zapory między nimi. Poniższy rysunek ilustruje proces ataku zatruwającego ARP. W bezprzewodowym ataku fałszowania ARP pokazanym na powyższym rysunku atakujący najpierw fałszuje adres MAC systemu ofiary i próbuje uwierzytelnić się w punkcie dostępowym 1 (API) za pomocą narzędzia do zatruwania ARP, takiego jak arpspoof. Interfejs API wysyła zaktualizowane informacje o adresie MAC do routerów i przełączników sieciowych, które z kolei aktualizują swoje tablice routingu i przełączania. W rezultacie ruch ze szkieletu sieci do systemu ofiary jest kierowany do API, a nie do punktu dostępowego 2 (AP2).

Atak zatruwający ARP przy użyciu Ettercap

Atakujący używają Ettercap do identyfikowania adresów MAC klientów i routerów w celu przeprowadzania różnych ataków, takich jak zatruwanie ARP, wąchanie i ataki MITM. Za pomocą tego narzędzia atakujący może uzyskać wszystkie informacje o ruchu sieciowym ofiary. Atakujący przeprowadza atak zatruwania ARP przy użyciu Ettercap, wykonując następujące kroki.

* Uruchom interfejs graficzny Ettercap i włącz opcję ujednoliconego wąchania, wybierając opcję Sniff -> Unified Sniffing z paska menu. Pozwala to atakującemu na mostkowanie połączenia i wąchanie ruchu przechodzącego przez interfejsy.

* W wyskakującym oknie konfiguracji Ettercap ustaw interfejs podstawowy na wąchanie i kliknij OK. Spowoduje to wyświetlenie zaawansowanych opcji menu, takich jak cele, hosty, MITM i wtyczki.

* Zidentyfikuj docelowego hosta w sieci, wybierając opcję Hosty -> Skanuj w poszukiwaniu hostów. Ettercap przeprowadza skanowanie wszystkich aktywnych hostów w sieci i wyświetla listę hostów. Następnie wybierz Hosty -> Lista hostów, aby wyświetlić wszystkie hosty wykryte w sieci lokalnej.

* Wybierz Widok -> Połączenia, aby rozpocząć podglądanie zidentyfikowanych połączeń. Połączenia można filtrować w widoku Połączenia na podstawie adresu IP, typu połączenia i stanu połączenia (otwarte/zamknięte/aktywne/zabite).

*Wybierz hosty do przeprowadzenia ataku polegającego na spoofingu ARP. Przejdź do okna Hosty i wybierz docelowy adres IP. Wybierz Cele -> Bieżące cele, aby dodać listę hostów docelowych, które mają być używane do spoofingu ARP.

* Wybierz MITM -> Zatrucie ARP. W wyskakującym oknie, które się pojawi, wybierz Sniff Remote Connections i kliknij OK, aby przeprowadzić atak zatruwania ARP na cel.

Po rozpoczęciu ataku dane logowania docelowego hosta mogą również zostać podsłuchane, jeśli ruch sieciowy nie jest szyfrowany za pomocą Hypertext Transfer Protocol Secure (HTTPS).

Nieuczciwe AP

Nieuczciwe punkty dostępowe to bezprzewodowe punkty dostępowe, które osoba atakująca instaluje w sieci bez autoryzacji i którymi nie zarządza administrator sieci. Te nieuczciwe punkty dostępowe nie są skonfigurowane pod kątem bezpieczeństwa, w przeciwieństwie do autoryzowanych punktów dostępowych w docelowej sieci bezprzewodowej. W ten sposób ten nieuczciwy punkt dostępowy

może zapewnić dostęp tylnym wejściem do docelowej sieci bezprzewodowej. Poniżej przedstawiono interesujące scenariusze instalacji i konfiguracji nieuczciwych punktów dostępowych.

Kompaktowy, kieszonkowy nieuczciwy punkt dostępowy podłączony do portu Ethernet sieci docelowej:

Atakujący może użyć kompaktowych, kieszonkowych punktów dostępowych, ponieważ są one łatwo dostępne, można je potajemnie przenieść na miejsce i zużywają bardzo mało energii.

Nieuczciwy punkt dostępowy połączony z sieciami firmowymi za pośrednictwem łącza Wi-Fi: osoba atakująca łączy nieuczciwy punkt dostępowy z łączem Wi-Fi docelowej sieci. Ponieważ nieuczciwy punkt dostępowy łączy się bezprzewodowo z autoryzowaną siecią, można go łatwo ukryć. Jednak do połączenia wymagane są poświadczenia sieci docelowej.

Nieuczciwy punkt dostępowy USB podłączony do maszyny sieciowej: osoba atakująca może łatwo podłączyć nieuczciwy punkt dostępowy USB do dowolnego komputera z systemem Windows w docelowej sieci, który jest połączony przewodowo lub bezprzewodowo. Oprogramowanie punktu dostępowego USB współdzieli dostęp sieciowy urządzenia z nieuczciwym punktem dostępowym. Eliminuje to potrzebę zarówno nieużywanego portu Ethernet, jak i poświadczeń docelowej sieci Wi-Fi, które są wymagane w powyższych dwóch scenariuszach do skonfigurowania nieuczciwego punktu dostępowego.

Oparty na oprogramowaniu nieuczciwy punkt dostępowy działający na sieciowym komputerze z systemem Windows: osoba atakująca może skonfigurować programowy nieuczciwy punkt dostępowy na wbudowanej/podłączonej karcie Wi-Fi sieci docelowej zamiast na osobnym urządzeniu sprzętowym.

Nieuczciwy AP jest wdrażany w następujących krokach.

Wybierz odpowiednią lokalizację do podłączenia nieuczciwego punktu dostępowego, aby uzyskać maksymalny zasięg z punktu połączenia

Wyłącz rozgłaszanie SSID (tryb cichy) i wszelkie funkcje zarządzania, aby uniknąć wykrycia.

Jeśli to możliwe, umieść punkt dostępowy za zaporą ogniową, aby uniknąć skanerów sieciowych.

Wdróż nieuczciwy AP na krótki okres.

Tworzenie nieuczciwego punktu dostępowego za pomocą narzędzia MANA Toolkit

MANA Toolkit zawiera zestaw narzędzi wykorzystywanych przez atakujących do tworzenia nieuczciwych punktów dostępowych oraz przeprowadzania ataków sniffingowych i MUM. Jest również używany do omijania HTTPS i HTTP Strict Transport Security (HSTS). Atakujący używają MANA Toolkit do stworzenia nieuczciwego punktu dostępowego, wykonując następujące kroki.

* Zmodyfikuj plik konfiguracyjny MANA hostapd-mana.conf za pomocą dowolnego edytora tekstu, aby skonfigurować fałszywy punkt dostępu. Ustaw interfejs bezprzewodowy (tutaj używany jest wlanO) oraz adres MAC (BSSID) lub SSID (tutaj używany jest SSID Free Internet).

* Zmodyfikuj plik skryptu start-nat-simple.sh używany do uruchamiania fałszywego punktu dostępowego. Ustaw parametr karty bezprzewodowej phy (tutaj używany jest wlanO) i parametr upstream (tutaj używany jest ethO), które określają, że karta ma połączenie z Internetem.

* Uruchom plik skryptu start-nat-simple.sh za pomocą polecenia bash # bash <ścieżka do MANA>/mana-toolkit/run-mana/start-nat-simple.sh. Wykonanie tego polecenia powoduje uruchomienie nieuczciwego punktu dostępowego.

* Gdy fałszywy punkt dostępowy zacznie działać, użyj komputera z systemem Windows lub urządzenia mobilnego z inną kartą bezprzewodową, aby połączyć się z fałszywym punktem dostępowym.

* W urządzeniu obsługującym Wi-Fi wyszukaj połączenie internetowe, które nie jest chronione hasłem (w tym przypadku używany jest bezpłatny Internet) i połącz się z nim.

* Po podłączeniu do Internetu przez nieuczciwy punkt dostępowy wszystkie pakiety danych z urządzenia przepływają przez nieuczciwy punkt dostępowy. Teraz narzędzia takie jak tcpdump i Wireshark mogą być używane do przechwytywania i analizowania pakietów.

Zły bliźniak

Zły bliźniak to bezprzewodowy punkt dostępowy, który udaje legalny punkt dostępowy, naśladując jego identyfikator SSID. Stanowi wyraźne i aktualne zagrożenie dla użytkowników bezprzewodowych w prywatnych i publicznych sieciach WLAN. Atakujący konfiguruje nieuczciwy punkt dostępowy poza granicami sieci i zachęca użytkowników do zalogowania się do tego punktu dostępowego. Atakujący wykorzystuje narzędzia takie jak KARMA, które monitorują sondy stacji w celu stworzenia złego bliźniaka. Narzędzie KARMA pasywnie nasłuchuje bezprzewodowych ramek żądania sondy i może przyjąć dowolny powszechnie używany identyfikator SSID jako własny identyfikator SSID, aby zwabić użytkowników. Atakujący może skonfigurować złego bliźniaka ze wspólnym identyfikatorem SSID dla użytkowników domowych, identyfikatorem SSID punktu dostępu lub identyfikatorem SSID sieci WLAN organizacji. Osoba atakująca, która może monitorować legalnych użytkowników, może atakować punkty dostępowe, które nie wysyłają identyfikatorów SSID w żądaniach sondujących. Stacje WLAN zwykle łączą się z określonymi punktami dostępowymi na podstawie ich identyfikatorów SSID i siły sygnału, a stacje automatycznie ponownie łączą się z dowolnym identyfikatorem SSID używanym w przeszłości. Problemy te pozwalają atakującym oszukać legalnych użytkowników poprzez umieszczenie złego bliźniaka w pobliżu docelowej sieci. Po skojarzeniu, atakujący może ominąć zasady bezpieczeństwa przedsiębiorstwa i uzyskać dostęp do danych sieciowych. Ponieważ pracownicy firmy mogą zabierać firmowe laptopy do placówek z publicznymi sieciami Wi-Fi, zapewnienie bezpieczeństwa danych firmowych jest wyzwaniem.

Konfiguracja fałszywego hotspotu (Evil Twin)

Hotspoty na danym obszarze mogą nie zawsze być legalne, ponieważ zły bliźniak dosiadany przez atakującego może udawać legalny hotspot. Trudno jest odróżnić legalny hotspot od złego bliźniaka. Na przykład użytkownik, który próbuje się zalogować, może znaleźć dwa AP, z których jeden jest legalny. Jeśli użytkownik łączy się z siecią za pośrednictwem złego bliźniaka, atakujący może uzyskać dane logowania i uzyskać dostęp do komputera ofiary. Każda próba zalogowania się użytkownika zakończy się niepowodzeniem i prawdopodobnie założy on, że próba losowo się nie powiodła. Fałszywy hotspot można skonfigurować za pomocą laptopa z połączeniem internetowym (3G lub połączenie przewodowe) i mini AP, wykonując następujące czynności.

1. Włącz Udostępnianie połączenia internetowego w systemie Windows lub Udostępnianie Internetu w systemie macOS.

2. Rozgłaszaj połączenie Wi-Fi i uruchom program sniffer w celu przechwycenia haseł.

Atak aLTEr

Atak ALTER składa się z dwóch faz.

Faza zbierania informacji: osoby atakujące biernie zbierają informacje potrzebne do przeprowadzenia ataku ALTEr przy użyciu technik takich jak mapowanie tożsamości i pobieranie odcisków palców witryn internetowych. Faza ataku: atakujący wykorzystują zebrane informacje do przeprowadzenia aktywnego ataku przy użyciu technik takich jak fałszowanie DNS.

Faza zbierania informacji

Atakujący szpiegują strony internetowe, do których użytkownicy próbują uzyskać dostęp, i rejestrują, jak często je odwiedzają. Atakujący tylko szpiegują lub monitorują transmisję między stacją bazową a użytkownikiem końcowym i nie modyfikują żadnych danych uwierzytelniających ani informacji w tym ataku. Atakujący wykorzystują następujące techniki do pasywnego zbierania informacji.

Mapowanie tożsamości: osoba atakująca początkowo mapuje tożsamość, aby zlokalizować urządzenie docelowe. Po określeniu celu atakujący opracowuje strategię realizacji dwóch kolejnych ataków.

Pobieranie odcisków palców witryn internetowych: osoba atakująca rejestruje natężenie ruchu, do którego uzyskuje dostęp klient, i śledzi działania użytkownika online oraz inne metadane.

Faza ataku

Po podglądaniu lub zebraniu informacji o docelowych użytkownikach atakujący przeprowadza atak MITM przy użyciu fałszywej wieży, utrudniając i manipulując danymi użytkownika, które mają być udostępniane prawdziwej wieży. Atakujący wykorzystuje spoofing DNS w celu przekierowania ofiary na złośliwą lub wybraną przez siebie witrynę internetową, na której zapisuje wszystkie poufne informacje wprowadzone przez ofiarę, takie jak nazwy użytkowników i hasła.

Wi-Jacking Atak

Atakujący wykorzystują atak Wi-Jacking w celu uzyskania dostępu do ogromnej liczby sieci bezprzewodowych. W tym ataku informacje Wi-Fi najbliższych ofiar można odzyskać bez użycia jakichkolwiek mechanizmów łamania zabezpieczeń. Atak ten może zostać wykorzystany, gdy dane uwierzytelniające są zapisywane w przeglądarce ofiary, gdy ofiara wielokrotnie uzyskuje dostęp do tej samej witryny internetowej oraz gdy router używa niezaszyfrowanego połączenia HTTP w celu uzyskania dostępu do interfejsu konfiguracyjnego routera w przeglądarce. Atakujący mogą wykorzystać te luki do złamania sieci WPA/WPA2 bez konieczności przechodzenia przez pojedynczy proces uzgadniania. Aby przeprowadzić atak Wi-Jacking, muszą być spełnione następujące warunki.

* Co najmniej jedno aktywne urządzenie klienckie musi być podłączone do sieci docelowej.

* Urządzenie klienckie musi być już podłączone do dowolnej otwartej sieci i umożliwiać automatyczne ponowne połączenie z tą siecią.

* Urządzenie klienckie musi korzystać z przeglądarki internetowej opartej na chromie.

* Przeglądarka urządzenia klienckiego musi przechowywać poświadczenia interfejsu administratora routera.

* Router sieci docelowej musi używać nieszyfrowanego połączenia HTTP dla interfejsu konfiguracyjnego routera.

Atakujący przeprowadzają atak Wi-Jacking, wykonując następujące kroki.

* Wysyłaj żądania cofnięcia uwierzytelnienia do urządzenia ofiary za pomocą aireplay-ng, aby odłączyć ofiarę od legalnej sieci Wi-Fi.

* Wykonaj atak KARMA za pomocą „hostapd-wpe", wabiąc ofiarę do połączenia się ze złośliwą siecią Wi-Fi.

* Po udanym cofnięciu uwierzytelnienia użyj narzędzi, takich jak „dnsmasq" i skrypty Pythona, aby wstrzyknąć złośliwy adres URL i zmusić przeglądarkę ofiary do załadowania tego złośliwego adresu URL. Na podstawie BSSID i ESSID można wykryć parę URL/strona, która ma zostać wysłana.

* Poczekaj, aż ofiara uzyska dostęp do strony HTTP. W tym momencie router ofiary jest aktualizowany i automatycznie restartowany.

* Gdy ofiara otworzy złośliwą stronę, przeglądarka sprawdzi następujące dwa warunki, aby automatycznie załadować stronę z zapisanymi danymi uwierzytelniającymi:

* Czy złośliwy adres URL i interfejs administratora routera mają to samo pochodzenie?

* Czy pola wprowadzania na stronie i interfejsie administratora routera są zgodne?

* Po otrzymaniu danych uwierzytelniających ofiara ma dostęp do strony jeszcze przez jakiś czas. Następnie zatrzymaj atak KARMA i pozwól ofierze połączyć się z legalną siecią. Gdy urządzenie ofiary zostanie podłączone do legalnej sieci, szkodliwa strona pozostaje w interfejsie administratora routera wraz z poświadczeniami administratora załadowanymi do kodu JavaScript.

* Użyj XMLHttpRequest, aby zalogować się do routera w celu wyodrębnienia WPA2 PSK ofiary i dalszych złośliwych zmian, jeśli to konieczne. Korzystając z tego PSK i innych danych uwierzytelniających, można zhakować prywatną sieć ofiary, a także uzyskać dostęp do krytycznych danych i zmodyfikować je za pomocą techniki Wi-Jacking.

Atak klonowania RFID

Klonowanie RFID polega na przechwytywaniu danych z legalnego znacznika RFID, a następnie tworzeniu jego klonu przy użyciu nowego chipa. Innymi słowy, dane z jednego znacznika RFID są kopiowane do innego znacznika poprzez zmianę identyfikatora znacznika (TID), ale współczynnik kształtu i dane mogą pozostać takie same. Sklonowana kopia różni się od oryginalnego znacznika RFID i może być łatwo wykryta. Atakujący używają iCopy-X, RFIDIer itp. do klonowania tagów RFID.

iCopy-X

iCopy-X to przenośne urządzenie do klonowania RFID, które może być używane przez atakujących do klonowania tagów RFID. Jest to całkowicie samodzielne urządzenie ze zintegrowanym ekranem i przyciskami, które zapewnia funkcjonalność Proxmarka, ale nie wymaga zewnętrznego komputera.

Oto kilka dodatkowych narzędzi do klonowania RFID:

RFIDIer (https://github.com)

RFID Mifare Cloner (https://github.com)

Proxmark3 (https://proxmark.com)

Boscloner Pro (https://www.boscloner.com)

Łamanie szyfrowania Wi-Fi

Po tym, jak atakującemu uda się uzyskać nieautoryzowany dostęp do sieci docelowej za pomocą takich metod, jak ataki bezprzewodowe, nieuczciwe punkty dostępowe i złe bliźniaki, atakujący musi złamać zabezpieczenia narzucone przez docelową sieć bezprzewodową. Ogólnie rzecz biorąc, do zabezpieczenia komunikacji bezprzewodowej sieci Wi-Fi używają szyfrowania WEP lub WPA/WPA2, które atakujący musi złamać. W tej sekcji zbadamy, w jaki sposób osoba atakująca może złamać te systemy szyfrowania, aby naruszyć bezpieczeństwo sieci bezprzewodowej.

Łamanie szyfrowania WEP

Zebranie dużej liczby IV jest niezbędne do złamania klucza szyfrującego WEP. Atakujący może zebrać wystarczającą liczbę IV, po prostu nasłuchując ruchu sieciowego. Wstrzykiwanie pakietów WEP przyspiesza proces zbierania IV i umożliwia przechwytywanie dużej liczby IV w krótkim czasie. Osoba atakująca może złamać szyfrowanie WEP, wykonując następujące czynności.

Uruchom interfejs bezprzewodowy w trybie monitorowania na określonym kanale AP: W tym kroku atakujący ustawia interfejs bezprzewodowy w trybie monitorowania. Interfejs może nasłuchiwać każdego pakietu w powietrzu, a atakujący może wybrać kilka pakietów do wstrzyknięcia, nasłuchując każdego pakietu dostępnego w powietrzu.

Testowanie możliwości wstrzykiwania z urządzenia bezprzewodowego do punktu dostępowego: Atakujący sprawdza, czy interfejs bezprzewodowy znajduje się w zasięgu określonego punktu dostępowego i czy jest w stanie wstrzykiwać do niego pakiety.

Użyj narzędzia takiego jak aireplay-ng do fałszywego uwierzytelnienia z punktem dostępowym: atakujący upewnia się, że źródłowy adres MAC jest już powiązany, aby punkt dostępowy zaakceptował wstrzyknięte pakiety. Wstrzyknięcie nie powiedzie się przy braku powiązania z AP.

Uruchom narzędzie do podsłuchiwania sieci Wi-Fi: osoba atakująca przechwytuje wygenerowane IV za pomocą narzędzi takich jak airodump-ng z filtrem BSSID w celu zebrania unikalnych IV.

Uruchom narzędzie do szyfrowania pakietów Wi-Fi, takie jak aireplay-ng w trybie odtwarzania żądania ARP, aby wprowadzić pakiety: Aby uzyskać dużą liczbę IV w krótkim czasie, atakujący uruchamia aireplay-ng w trybie odtwarzania żądania ARP, co nasłuchuje żądań ARP, a następnie ponownie wprowadza je do sieci. Punkt dostępowy zwykle ponownie rozgłasza pakiety, generując nowy IV. Dlatego, aby uzyskać dużą liczbę IV, atakujący wybiera tryb żądania ARP.

Uruchom narzędzie do łamania zabezpieczeń, takie jak aircrack-ng: Za pomocą narzędzi do łamania zabezpieczeń, takich jak aircrack-ng, osoba atakująca może wyodrębnić klucze szyfrujące WEP z IV.

Łamanie WEP za pomocą Aircrack-ng

Szyfrowanie WEP można złamać za pomocą Aircrack-ng, wykonując następujące czynności.

* Uruchom airmon-ng w trybie monitora.

* Uruchom airodump, aby wykryć identyfikatory SSID w interfejsie i utrzymać go w ruchu. Plik przechwytywania powinien zawierać ponad 50 000 IV, aby pomyślnie złamać klucz WEP.

*Powiąż kartę bezprzewodową systemu z docelowym punktem dostępowym.

* Wstrzykiwanie pakietów za pomocą aireplay-ng do generowania ruchu w docelowym punkcie dostępowym.

* Poczekaj, aż airodump-ng przechwyci ponad 50 000 IV. Złam klucz WEP za pomocą aircrack-ng.

Łamanie szyfrowania WPA/WPA2

Szyfrowanie WPA jest mniej podatne na wykorzystanie niż szyfrowanie WEP. Jednak osoba atakująca nadal może złamać szyfrowanie WPA/WPA2, przechwytując niezbędny typ pakietów. Atakujący może to zrobić w trybie offline, ale musi znajdować się w pobliżu punktu dostępowego przez kilka chwil. Poniżej przedstawiono niektóre rodzaje technik używanych do łamania szyfrowania WPA.

WPA PSK: WPA PSK używa hasła zdefiniowanego przez użytkownika do zainicjowania czterokierunkowego uzgadniania. Osoba atakująca nie może złamać tego hasła, ponieważ jest to klucz na pakiet, ale klucze można wymusić metodą brute-force za pomocą ataków słownikowych. Atak słownikowy może naruszyć większość haseł konsumenckich.

Atak offline: aby przeprowadzić atak offline, osoba atakująca musi znajdować się w pobliżu punktu dostępowego przez kilka sekund, aby przechwycić uścisk dłoni uwierzytelniania WPA/WPA2. Przechwytując niezbędny typ pakietów, klucze szyfrowania WPA można złamać w trybie offline. W uzgadnianiu WPA protokół nie wysyła hasła przez sieć, ponieważ uzgadnianie WPA zwykle odbywa się w niezabezpieczonych kanałach iw postaci zwykłego tekstu. Przechwycenie pełnego uzgadniania uwierzytelnienia od klienta i punktu dostępowego pomaga w złamaniu szyfrowania WPA/WPA2 bez wstrzykiwania pakietów.

Atak de-uwierzytelniający: aby przeprowadzić atak de-uwierzytelniający w celu złamania szyfrowania WPA, osoba atakująca musi znaleźć aktywnie połączonego klienta. Atakujący zmusza klienta do odłączenia się od punktu dostępowego, po czym używa narzędzi takich jak aireplay do przechwycenia pakietu uwierzytelniającego, gdy klient próbuje ponownie się połączyć. Klient powinien być w stanie ponownie uwierzytelnić się w punkcie dostępowym w ciągu kilku sekund. Pakiet uwierzytelniający zawiera parami klucz główny (PMK), który atakujący może złamać za pomocą ataków słownikowych lub siłowych w celu odzyskania klucza WPA.

Brutalne wymuszanie kluczy WPA: Techniki brutalnej siły są przydatne do łamania kluczy szyfrowania WPA/WPA2. Osoba atakująca może przeprowadzić atak siłowy na klucze szyfrowania WPA przy użyciu słownika lub narzędzi, takich jak aircrack, aireplay lub KisMAC. Technika brute-force ma znaczący wpływ na szyfrowanie WPA ze względu na jej intensywny obliczeniowo charakter. Łamanie kluczy WPA techniką brutalnej siły może zająć godziny, dni, a nawet tygodnie.

Łamanie WPA-PSK za pomocą Aircrack-ng

WPA-PSK to mechanizm uwierzytelniania, w którym użytkownicy podają pewne dane uwierzytelniające w celu uwierzytelnienia w sieci. WPA i WPA-PSK używają tego samego mechanizmu szyfrowania, a jedyną różnicą między nimi jest mechanizm uwierzytelniania. Uwierzytelnianie w WPAPSK obejmuje proste wspólne hasło. Tryb PSK WPA jest narażony na takie same zagrożenia, jak każdy inny system współdzielonych haseł. Atakujący może złamać WPA-PSK, ponieważ zaszyfrowane hasło jest udostępniane w czterokierunkowym uścisku dłoni. W schemacie WPA-PSK, gdy klienci próbują uzyskać dostęp do punktu dostępowego, przechodzą czteroetapowy proces uwierzytelniania. Ten proces obejmuje udostępnianie między nimi zaszyfrowanego hasła. Atakujący przechwytuje hasło, a następnie próbuje złamać schemat WPA-PSK. Można to również uznać za atak KRACK. Oto kroki, aby złamać WPA-PSK:

Monitoruj ruch bezprzewodowy za pomocą airmon-ng, używając następującego polecenia:

C:\>airmon-ng start ethl

Zbierz dane o ruchu bezprzewodowym za pomocą airodump-ng, używając następującego polecenia:

C:\>airodump-ng --write przechwytywania eth1

De-uwierzytelnij (usuń) klienta za pomocą Aireplay-ng. Klient spróbuje uwierzytelnić się w punkcie dostępowym, co prowadzi do przechwycenia przez airodump pakietu uwierzytelniającego (Uścisk dłoni WPA).

Uruchom plik przechwytywania za pomocą aircrack-ng.

Łamanie WPA/WPA2 za pomocą Wifiphisher

Wifiphisher to nieuczciwa platforma AP do przeprowadzania zadań Red Team lub testowania bezpieczeństwa Wi-Fi. Korzystając z Wifiphisher, testerzy penetracji mogą z łatwością osiągnąć pozycję MUM w stosunku do klientów bezprzewodowych, przeprowadzając ukierunkowane ataki na skojarzenia Wi-Fi. Wifiphisher może być dalej wykorzystywany do przeprowadzania dostosowanych do ofiary ataków phishingowych na podłączonych klientów w celu przechwycenia ich danych uwierzytelniających (np. Poniżej przedstawiono niektóre z ważnych opcji konfiguracyjnych Wifiphisher.

-iI INTERNET INTERFEJS - Wybierz interfejs podłączony do Internetu.

- ji JAMMINGINTERFACE - Ręcznie wybierz interfejs obsługujący tryb monitora de-uwierzytelniania ofiar.

-aI APINTERFACE - Ręcznie wybierz interfejs obsługujący tryb AP.

-nJ — Pomiń fazę de-uwierzytelniania.

-e ESSID - Wprowadź ESSID nieuczciwego AP.

-p PHISHINGSCENARIO — wybierz scenariusz phishingu do wykonania.

-pK PRESHAREDKEY - Dodaj ochronę WPA/WPA2 na nieuczciwym AP.

WEP/WPA/WPA2 można złamać za pomocą Wifiphisher, wykonując następujące kroki.

* Uruchom Wifiphisher za pomocą polecenia wifiphisher .

* Wyświetlane są wszystkie dostępne sieci. Wybierz sieć docelową, jak pokazano na rysunku.

* Gdy ofiara połączy się z nieuczciwą siecią bezprzewodową, strona Network Manager otwiera się automatycznie na urządzeniu ofiary, zachęcając ofiarę do podania hasła Wi-Fi w celu połączenia się z punktem dostępowym.

* Gdy ofiara wprowadzi hasło, na ekranie Wifiphisher pojawi się powiadomienie. Wifiphisher przechwytuje hasło WEP/WPA/WPA2 przez nieuczciwą sieć Wi-Fi.

* Ofiarę można również oszukać, wyświetlając fałszywy ekran ładowania, powodując, że sieć wydaje się wolniejsza.

Łamanie WPS za pomocą Reavera

Reaver został zaprojektowany jako solidne i praktyczne narzędzie do ataku na kody PIN rejestratora Wi-Fi Protected Setup (WPS) w celu odzyskania haseł WPA/WPA2 i został przetestowany pod kątem szerokiej gamy AP i implementacji WPS. PIN WPS można złamać za pomocą Reavera, wykonując następujące czynności. Skonfiguruj interfejs bezprzewodowy w trybie monitorowania za pomocą Airmon-ng za pomocą następującego polecenia:

airmon-ng <start|stop> <interfejs>

Na przykład,

airmon-ng start wlan0

* Użyj narzędzia Wash do wykrywania urządzeń obsługujących WPS za pomocą następującego polecenia:

wash -i <interfejs>

Na przykład,

wash -i mon0

Jeśli urządzeń obsługujących WPS nie można wykryć za pomocą narzędzia Wash, użyj Airodump-ng do wykrycia urządzeń za pomocą WPS za pomocą następującego polecenia:

airodump-ng <interfejs>

Na przykład, jeśli w poprzednim kroku konfiguracja urządzenia w trybie monitorowania została zaobserwowana jako wlanOmon, polecenie powinno brzmieć airodump-ng wlan0mon

To polecenie wyświetla wszystkie dostępne identyfikatory BSSID (adresy MAC punktów dostępowych).

Po zidentyfikowaniu identyfikatora BSSID urządzenia docelowego rozpocznij łamanie kodu PIN WPS za pomocą narzędzia Reaver za pomocą następującego polecenia:

reaver -i < Name of the monitor-mode interface to use> -b < BSSID of the target AP> -w <Display non-critical warnings>

Na przykład,

reaver -i wlanOmon -b B4:75:OE:89:00:60 -w

Powyższe polecenie skanuje wszystkie dostępne kody PIN WPS, dopóki nie znajdzie pasującego kodu PIN. Po wykryciu kodu PIN WPS rozpoczyna się eksploatacja.

Łamanie szyfrowania WPA3

Standard bezpieczeństwa Wi-Fi WPA3 zastępuje czterokierunkową metodę uzgadniania WPA2 (PSK) funkcją uzgadniania Dragonfly (znaną również jako SAE), aby zapewnić jak dotąd najsilniejsze uwierzytelnianie oparte na haśle. Jednak nadal jest podatny na ataki polegające na łamaniu haseł. Dragonblood to zestaw luk w standardzie bezpieczeństwa WPA3, który umożliwia atakującym odzyskanie kluczy, obniżenie poziomu mechanizmów bezpieczeństwa i przeprowadzanie różnych ataków mających na celu kradzież informacji. Atakujący mogą używać różnych narzędzi, takich jak Dragonslayer, Dragonforce, Dragondrain i Dragontime, aby wykorzystać te luki i przeprowadzać ataki na sieci obsługujące WPA3. Poniżej przedstawiono niektóre techniki stosowane do łamania szyfrowania WPA3.

Ataki bezpieczeństwa na niższą wersję

Aby przeprowadzić ten atak, klient i punkt dostępowy powinny obsługiwać mechanizmy szyfrowania WPA3 i WPA2. W tym przypadku atakujący zmusza użytkownika do zastosowania starszej metody szyfrowania, WPA2, w celu połączenia z siecią. Atak na obniżenie wersji może zostać zaimplementowany na dwa sposoby.

o Wykorzystanie kompatybilności wstecznej: jeśli użytkownik i punkt dostępowy są zgodni zarówno z mechanizmami szyfrowania WPA2, jak i WPA3, atakujący instaluje w pobliżu nieuczciwy punkt dostępowy zgodny tylko z WPA2 i zmusza klienta do przejścia przez czterokierunkowe uzgadnianie (WPA2) w celu Połącz się. Po nawiązaniu połączenia atakujący wykorzystuje wszystkie dostępne narzędzia ataku, aby wykorzystać lub złamać szyfrowanie WPA2.

o Wykorzystanie uścisku dłoni Dragonfly: W tej metodzie atakujący udaje autentycznego AP. Gdy użytkownik próbuje wymienić klucze dostępu do Internetu za pomocą mechanizmu uwierzytelniania WPA3, atakujący informuje użytkownika, że nie obsługuje metody WPA3. Następnie atakujący sugeruje użycie słabszego mechanizmu szyfrowania, takiego jak WPA2, w celu uzyskania dostępu do Internetu.

Następnie osoba atakująca może użyć różnych technik w celu wykorzystania lub złamania szyfrowania WPA2.

Ataki kanałami bocznymi (atak polegający na wycieku informacji)

Atakujący atakują protokoły lub mechanizmy szyfrowania używane przez urządzenia próbujące połączyć się z siecią. Podczas procesu wymiany klucza osoba atakująca przeprowadza ten atak w celu przechwycenia ujawnionych informacji. Informacje te są następnie wykorzystywane przez atakującego do przeprowadzania ataków siłowych lub słownikowych w celu uzyskania wszystkich danych docelowego użytkownika. Atak kanałem bocznym można przeprowadzić na dwa sposoby.

o Atak oparty na czasie: w tym ataku atakujący analizuje czas potrzebny na uzgadnianie Dragonfly do zakodowania określonego procesu uwierzytelniania hasła. W analizie atakujący obserwuje iteracje procesu kodowania i tworzy krótką listę możliwych haseł. Po uzyskaniu listy haseł atakujący próbuje uzyskać dostęp do urządzenia docelowego użytkownika za pomocą różnych technik.

o Atak oparty na pamięci podręcznej: w tym ataku atakujący wprowadza złośliwy kod JavaScript lub aplikację internetową do przeglądarki docelowego użytkownika. Pozwala to atakującemu przejąć kontrolę nad przeglądarką internetową użytkownika i dalej obserwować wzorce dostępu do pamięci w celu odzyskania informacji o haśle.

Łamanie WEP i brutalne wymuszanie WPA za pomocą Wesside-ng i Fern Wifi Cracker

Łamanie WEP

Wesside-ng to narzędzie do łamania zabezpieczeń WEP, które obejmuje kilka technik umożliwiających bezproblemowe uzyskanie klucza WEP w ciągu kilku minut. Najpierw identyfikuje sieć, a następnie łączy się z nią, uzyskuje dane XOR algorytmu generowania pseudolosowego (PRGA), określa schemat IP sieci, ponownie wstrzykuje żądania ARP i ostatecznie określa klucz WEP. Wesside-ng jest wykonywany za pomocą następującego polecenia:

wesside-ng <opcje> -i <nazwa interfejsu bezprzewodowego>

o -h Wyświetla listę opcji

o -i-> Nazwa interfejsu bezprzewodowego

o -n Network IP -> Domyślnie źródłowy adres IP żądania ARP, które jest przechwytywane i odszyfrowywane

o -m MY IP Domyślnie network.123 na przechwyconym żądaniu ARP (opcjonalnie)

o -a -> Źródłowy adres MAC

o -c -> Nie uruchamiaj aircrack-ng i po prostu przechwytuj pakiety, dopóki nie zostanie naciśnięty control + C, aby zatrzymać program

o - f -> Umożliwia zdefiniowanie najwyższego kanału do skanowania; domyślnie kanał 11

o -k -> Ignoruje ACK, ponieważ niektóre karty/sterowniki ich nie zgłaszają

o -p -> Określa minimalną liczbę gromadzonych bajtów PRGA; domyślnie 128 bajtów

o -t -> Uruchom ponownie silnik airecrack-ng PTW dla każdej określonej liczby IV

o –v Adres MAC bezprzewodowego punktu dostępowego

Brutalne wymuszanie WPA/WPA2

Fern Wifi Cracker to oprogramowanie do audytu i ataków bezpieczeństwa sieci bezprzewodowej, napisane przy użyciu języka programowania Python i biblioteki graficznego interfejsu użytkownika (GUI) Python Qt. Program może łamać i odzyskiwać klucze WEP/WPA/WPS, a także przeprowadzać inne ataki sieciowe na sieci bezprzewodowe lub oparte na sieci Ethernet. Fern Wifi Cracker obsługuje obecnie następujące funkcje:

• Łamanie WEP z fragmentacją, Chop-Chop, Caffe-Latte, Hirte, powtarzaniem żądań ARP lub atakami WPS

• Łamanie WPA/WPA2 za pomocą ataków słownikowych lub opartych na WPS

• Automatyczne zapisywanie klucza w bazie danych po pomyślnym złamaniu

• Przejęcie sesji (tryb pasywny i Ethernet)

• Śledzenie geolokalizacji adresu MAC punktu dostępowego

Bezprzewodowe narzędzia hakerskie

W poprzednich sekcjach omówiono metodologię hakowania i zautomatyzowane narzędzia wykorzystywane przez osoby atakujące w sieciach bezprzewodowych. Ta sekcja opisuje więcej bezprzewodowych narzędzi hakerskich.

Narzędzia do łamania zabezpieczeń WEP/WPA/WPA2

Narzędzia do łamania WEP/WPA/WPA2 są przydatne do łamania tajnych kluczy WEP/WPA/WPA2. Te narzędzia mogą odzyskać 40-bitowy, 104-bitowy, 256-bitowy lub 512-bitowy klucz WEP po przechwyceniu wystarczającej liczby pakietów danych. Kilka narzędzi odgaduje klucze WEP na podstawie aktywnego ataku słownikowego, generatora kluczy, ataku sieci rozproszonej itp. Poniżej przedstawiono kilka narzędzi do łamania zabezpieczeń WEP/WPA/WPA2, których może użyć atakujący:

Audytor bezpieczeństwa sieci bezprzewodowej Elcomsoft

Elcomsoft Wireless Security Auditor umożliwia atakującym włamanie się do zabezpieczonej sieci Wi-Fi poprzez wąchanie ruchu bezprzewodowego i rozpoczęcie ataku na hasło WPA/WPA2 PSK sieci. Pierwotnie został opracowany, aby pomóc administratorom sprawdzić, jak bezpieczna jest firmowa sieć bezprzewodowa. Sprawdza bezpieczeństwo sieci bezprzewodowej, próbując włamać się do sieci z zewnątrz lub od wewnątrz. Może pracować jako bezprzewodowy sniffer lub działać w trybie offline,

analizując zrzut komunikacji sieciowej. Narzędzie próbuje odzyskać oryginalne hasła WPA/WPA2 PSK w postaci zwykłego tekstu.

Oto niektóre z dodatkowych narzędzi do łamania zabezpieczeń WEP/WPA/WPA2:

Wifi (https://github.com)

EAPHammer (https://github.com)

Portable Penetrator (https://www.secpoint.com)

WepCrackGui (https://sourceforge.net)

Pyryt (https://github.com)

Narzędzia do łamania WEP/WPA/WPA2 dla urządzeń mobilnych

WlBR+- Wi-Fi BRuteforce

WIBR+ to aplikacja do testowania bezpieczeństwa sieci Wi-Fi WPA/WPA2 PSK. Odkrywa słabe hasła. WIBR+ obsługuje kolejkowanie, niestandardowe słowniki, generator brutalnej siły i zaawansowane monitorowanie. Za pomocą WIBR+ można przeprowadzić następujące dwa rodzaje ataków.

Atak słownikowy: WIBR+ sekwencyjnie próbuje wprowadzić hasła z predefiniowanej listy. WIBR+ obsługuje import niestandardowych list haseł.

Atak brutalny: WIBR+ obsługuje niestandardowe alfabety i niestandardowe maski. Jeśli wiadomo, że hasło to „hacker", po którym następują dwie cyfry, maskę można ustawić na hacker[x][x] z wybranym alfabetem cyfr. Aplikacja spróbuje wszystkich kombinacji haseł od hackerOO, hackerOl, do hacker99!

Oto kilka dodatkowych mobilnych narzędzi do łamania zabezpieczeń WEP/WPA/WPA2:

WIFI WPS WPA TESTER (https://ploy.google.com)

WPS WPA WiFi Tester (https://ploy.google.com)

WiFi Password Hacker (https://ploy.google.com)

Wifi password show (https://ploy.google.com)

WIFI Hacker WPS WPA TESTER (https://ploy.google.com)

Sniffery pakietów Wi-Fi

Analizator pakietów SteelCentral

SteelCentral Packet Analyzer to analizator sieci przewodowych i bezprzewodowych, który przechwytuje terabajty danych pakietowych. Przemierzanie ich to pierwszy krok w kierunku pełnej analizy w czasie rzeczywistym i wstecz w czasie. Po zintegrowaniu z Wireshark ulepsza Wireshark, zwiększając jego skuteczność w identyfikowaniu i diagnozowaniu problemów sieciowych. SteelCentral Packet Analyzer mierzy wykorzystanie kanałów bezprzewodowych i pomaga w identyfikacji nieuczciwych sieci i stacji bezprzewodowych.

Analizator protokołów sieciowych Omnipeek

Analizator protokołów sieciowych OmniPeek oferuje widoczność i analizę ruchu sieciowego w czasie rzeczywistym oraz zapewnia kompleksowy widok całej aktywności sieci bezprzewodowej, pokazując każdą sieć bezprzewodową, punkty dostępowe wchodzące w skład tej sieci oraz użytkowników

podłączonych do każdego punktu dostępowego. Oferuje wgląd w czasie rzeczywistym i analizę każdej części sieci z jednego interfejsu, w tym Ethernet, Gigabit, 10 Gigabit, 802.11a/b/g/n wireless, VoIP i wideo do zdalnych biur.

CommView dla Wi-Fi

CommView dla Wi-Fi to monitor i analizator sieci bezprzewodowych dla sieci 802.11 a/b/g/n. Przechwytuje pakiety i wyświetla ważne informacje, takie jak lista punktów dostępowych i stacji, statystyki poszczególnych węzłów i kanałów, siła sygnału, lista pakietów i połączeń sieciowych oraz wykresy dystrybucji protokołów. Użytkownik może odszyfrować pakiety za pomocą zdefiniowanych przez użytkownika kluczy WEP lub WPA-PSK i zdekodować je do najniższej warstwy. Ten analizator sieci ujawnia każdy szczegół przechwyconego pakietu za pomocą wygodnej struktury drzewiastej do wyświetlania warstw protokołów i nagłówków pakietów.

Kismet

Kismet to detektor sieci bezprzewodowej 802.11 Layer-2, sniffer i system wykrywania włamań. Identyfikuje sieci poprzez pasywne zbieranie pakietów i wykrywanie sieci o standardowych nazwach. Wykrywa sieci ukryte i obecność sieci bez sygnalizacji nawigacyjnej za pośrednictwem ruchu danych.

Narzędzia analizatora ruchu Wi-Fi

Narzędzia analizatora ruchu Wi-Fi analizują, debugują, konserwują i monitorują sieci lokalne i połączenia internetowe pod kątem wydajności, wykorzystania przepustowości i problemów z bezpieczeństwem. Przechwytują dane przechodzące przez połączenie telefoniczne lub kartę sieciową Ethernet, analizują te dane i przedstawiają je w czytelnej formie. To narzędzie zapewnia kompleksowy obraz ruchu przechodzącego przez połączenie sieciowe lub segment WLAN. Narzędzia te analizują ruch sieciowy w celu śledzenia określonych transakcji lub wykrywania naruszeń bezpieczeństwa. Jednak osoby atakujące wykorzystują je do złośliwych celów. Poniżej przedstawiono niektóre narzędzia używane do analizowania ruchu w docelowych sieciach bezprzewodowych.

Analizator Wi-Fi AirMagnet PRO

AirMagnet WiFi Analyzer PRO to narzędzie do audytu ruchu w sieci Wi-Fi i rozwiązywania problemów, które zapewnia dokładną, niezależną i niezawodną analizę Wi-Fi w sieciach bezprzewodowych 802.11a/b/g/n/ax, w których brakuje ruchu. Atakujący używają AirMagnet WiFi Analyzer PRO do zbierania szczegółowych informacji, takich jak łączność sieci bezprzewodowej, zasięg Wi-Fi, wydajność, roaming, zakłócenia i problemy z bezpieczeństwem sieci.

Oto kilka dodatkowych narzędzi do analizowania ruchu Wi-Fi:

SteelCentral Packet Analyzer (https://www.riverbed.com)

Omnipeek Network Protocol Analyzer (https://www.liveoction.com)

CommView for Wi-Fi (https://www.tomos.com)

Capsa Portable Network Analyzer (https://www.colosoft.com)

PRTG Network Monitor (https://www.poessler.com)

Narzędzia do prowadzenia wojny

Narzędzia WarDriving umożliwiają użytkownikom wyświetlanie listy wszystkich punktów dostępowych emitujących sygnały nawigacyjne w ich lokalizacji. Pomaga użytkownikom konfigurować nowe punkty dostępowe, upewniając się, że nie istnieją żadne zakłócające punkty dostępowe. Narzędzia te weryfikują konfigurację sieci, znajdują lokalizacje o słabym zasięgu w sieci WLAN i wykrywają inne sieci, które mogą powodować zakłócenia. Mogą również wykrywać nieautoryzowane nieuczciwe punkty dostępowe. Poniżej przedstawiono niektóre narzędzia WarDriving.

Airbase-ng (https://oircrock-ng.org)

inSSIDer (https://www.metogeek.com)

NetSpot (https://www.netspotopp.com)

WiGLE WiFi Wardriving (https://ploy.google.com)

AirFart (https://sourceforge.net)

Narzędzia do monitorowania częstotliwości radiowych

Narzędzia do monitorowania częstotliwości radiowych (RF) pomagają w wykrywaniu i monitorowaniu sieci Wi-Fi. Narzędzia te kontrolują i monitorują interfejsy sieciowe, w tym bezprzewodowe. Wyświetlają aktywność sieciową i pomagają kontrolować interfejsy sieciowe. Poniżej przedstawiono niektóre narzędzia do monitorowania RF.

RFXpert (https://www.dektec.com)

Monies 200 (https://www.krotosdefense.com)

Monies satID (https://www.krotosdefense.com)

RF Signal Tracker (https://ploy.google.com)

FieldSENSE60 (https://www.fieldsense.com)

Narzędzia do przechwytywania surowych pakietów

Narzędzia do przechwytywania surowych pakietów przechwytują pakiety sieci bezprzewodowej i monitorują aktywność pakietów WLAN. Narzędzia te przechwytują każdy pakiet, obsługują zarówno Ethernet LAN, jak i 802.11 oraz wyświetlają ruch sieciowy na poziomie MAC. Poniżej przedstawiono niektóre narzędzia do przechwytywania nieprzetworzonych pakietów.

WirelessNetView (https://www.nirsoft.net)

PRTG Network Monitor (https://www.paessler.com)

Tcpdump (https://www.tcpdump.org)

RawCap (https://www.netresec.com)

Airodump-ng (https://www.aircrack-ng.org)

Narzędzia do analizy widma

Narzędzia do analizy widma wykonują analizę widma RF i rozwiązywanie problemów z Wi-Fi. Za pomocą tych narzędzi użytkownicy mogą wykryć każdą aktywność RF w środowisku, a także obszary, w których zakłócenia RF wpływają na wydajność i powodują niezadowolenie użytkownika z powodu wolnych połączeń lub częstych rozłączeń. Poniżej przedstawiono niektóre narzędzia do analizy widma.

Chanalyzer Essential (https://www.metageek.com)

AirMagnet Spectrum XT (https://www.netally.com)

Wi-Fi Cisco Spectrum Expert (https://www.cisco.com)

RSA306B USB Spectrum Analyzer (https://www.tek.com)

AirSleuth-Pro (https://nutsaboutnets.com)

Hakowanie Bluetootha

Bluetooth to technologia bezprzewodowa, która umożliwia urządzeniom udostępnianie danych na niewielkie odległości. Technologia Bluetooth jest podatna na różnego rodzaju ataki. Poprzez hakowanie Bluetooth osoba atakująca może wykonywać różne złośliwe operacje na docelowym urządzeniu mobilnym. W tej sekcji opisano, w jaki sposób osoby atakujące przeprowadzają hakowanie Bluetooth przy użyciu różnych typów narzędzi.

Stos Bluetooth

Bluetooth to technologia komunikacji bezprzewodowej krótkiego zasięgu, która zastępuje kable łączące urządzenia przenośne lub stacjonarne przy zachowaniu wysokiego poziomu bezpieczeństwa. Umożliwia telefonom komórkowym, komputerom i innym urządzeniom wymianę informacji. Dwa urządzenia obsługujące technologię Bluetooth łączą się za pomocą techniki parowania. Stos Bluetooth odnosi się do implementacji stosu protokołów Bluetooth. Pozwala aplikacji dziedziczenie do pracy przez Bluetooth. Użytkownik może przenieść się do dowolnego systemu przy użyciu warstwy abstrakcji systemu operacyjnego firmy Atinav. Poniższy rysunek przedstawia stos Bluetooth.

Stos Bluetooth składa się z dwóch części: ogólnego przeznaczenia i systemu wbudowanego.

Tryby Bluetooth

Użytkownik może ustawić Bluetooth w następujących trybach.

Wykrywalne tryby

Bluetooth działa w następujących trzech wykrywalnych trybach.

o Wykrywalne: Gdy urządzenia Bluetooth są w trybie wykrywalnym, są widoczne dla innych urządzeń obsługujących technologię Bluetooth. Jeśli urządzenie próbuje połączyć się z innym, urządzenie próbujące nawiązać połączenie musi wyszukać urządzenie, które jest w trybie wykrywalnym; w przeciwnym razie urządzenie próbujące zainicjować połączenie nie będzie w stanie wykryć drugiego urządzenia. Tryb wykrywalny jest potrzebny tylko przy pierwszym połączeniu z urządzeniem. Po zapisaniu połączenia urządzenia zapamiętują się nawzajem; dlatego wykrywalny tryb nie jest konieczny do ustanowienia połączenia poprzecznego.

o Ograniczona wykrywalność: W trybie ograniczonej wykrywalności urządzenia Bluetooth są wykrywalne tylko przez ograniczony czas, w przypadku określonego zdarzenia lub w warunkach tymczasowych. Jednak nie ma polecenia interfejsu kontrolera hosta (HCI), aby ustawić urządzenie bezpośrednio w trybie ograniczonej wykrywalności. Użytkownik musi to zrobić pośrednio. Kiedy urządzenie jest ustawione w tryb ograniczonej wykrywalności, odfiltrowuje niedopasowane kontrolery LAC i ujawnia się tylko tym, które pasują.

o Niewykrywalne: Ustawienie urządzenia Bluetooth w trybie niewykrywalnym zapobiega pojawianiu się tego urządzenia na liście podczas procesu wyszukiwania urządzeń obsługujących technologię

Bluetooth. Pozostaje jednak widoczny dla użytkowników i urządzeń, które były z nim wcześniej sparowane lub znają jego adres MAC.

Tryby parowania

Poniżej przedstawiono tryby parowania urządzeń Bluetooth.

o Tryb niemożliwy do sparowania: W trybie niemożliwym do sparowania urządzenie Bluetooth odrzuca żądania parowania wysyłane przez dowolne urządzenie.

o Tryb parowania: W trybie parowania urządzenie Bluetooth może akceptować żądania parowania i nawiązywać połączenie z urządzeniem, które zażądało parowania.

Hakowanie Bluetootha

Hakowanie Bluetooth odnosi się do wykorzystywania luk w implementacji stosu Bluetooth w celu naruszenia poufnych danych w urządzeniach i sieciach obsługujących Bluetooth. Urządzenia obsługujące technologię Bluetooth łączą się i komunikują bezprzewodowo za pośrednictwem sieci ad-hoc, znanych jako pikosieci. Atakujący mogą uzyskać informacje, hakując docelowe urządzenie obsługujące technologię Bluetooth z innego urządzenia obsługującego technologię Bluetooth.

Oto niektóre ataki na urządzenia Bluetooth:

Bluesmacking: Atak Bluesmacking ma miejsce, gdy atakujący wysyła zbyt duży pakiet ping do urządzenia ofiary, powodując przepełnienie bufora. Ten typ ataku jest podobny do ataku ping-of-death przy użyciu protokołu ICMP (Internet Control Message Protocol).

Bluejacking: Bluejacking to wykorzystanie Bluetooth do wysyłania wiadomości do użytkowników bez zgody odbiorcy, podobnie jak w przypadku spamowania e-maili. Przed jakąkolwiek komunikacją Bluetooth urządzenie inicjujące połączenie musi podać nazwę wyświetlaną na ekranie odbiorcy. Ponieważ ta nazwa jest zdefiniowana przez użytkownika, można ją ustawić jako irytującą wiadomość lub reklamę. Ściśle mówiąc, Bluejacking nie powoduje żadnych uszkodzeń urządzenia odbiorczego. Jednak może to być irytujące i uciążliwe dla ofiar.

Bluesnarfing: Bluesnarfing to metoda uzyskiwania dostępu do poufnych danych w urządzeniu obsługującym technologię Bluetooth. Atakujący znajdujący się w zasięgu celu może użyć specjalistycznego oprogramowania w celu uzyskania danych przechowywanych na urządzeniu ofiary. Aby wykonać Bluesnarfing, osoba atakująca wykorzystuje lukę w protokole Object Exchange (OBEX), którego Bluetooth używa do wymiany informacji. Atakujący łączy się z celem i wykonuje operację GET dla plików o poprawnie odgadniętych lub znanych nazwach, takich jak /pb.vcf dla książki telefonicznej urządzenia lub telecom /cal.vcs dla pliku kalendarza urządzenia.

BlueSniff: BlueSniff to kod sprawdzający koncepcję dla narzędzia Wardriving Bluetooth. Jest to przydatne do znajdowania ukrytych i możliwych do wykrycia urządzeń Bluetooth. Działa na Linuksie.

Bluebugging: Bluebugging to atak, w którym osoba atakująca uzyskuje zdalny dostęp do docelowego urządzenia obsługującego technologię Bluetooth bez wiedzy ofiary. W tym ataku osoba atakująca wyszukuje poufne informacje i może wykonywać złośliwe działania, takie jak przechwytywanie połączeń telefonicznych i wiadomości oraz przekazywanie połączeń i wiadomości tekstowych.

Blueprinting: Blueprinting to technika oznaczania śladów wykonywana przez atakującego w celu określenia marki i modelu docelowego urządzenia obsługującego technologię Bluetooth. Atakujący zbierają te informacje w celu stworzenia infografik modelu, producenta itp. i analizują je w celu ustalenia, czy urządzenie ma luki, które można wykorzystać.

Btlejacking: Atak Btlejacking jest szkodliwy dla urządzeń Bluetooth o niskim zużyciu energii (BLE). Atakujący może wąchać, blokować i przejmować kontrolę nad transmisją danych między urządzeniami BLE, przeprowadzając atak MUM. Po udanej próbie atakujący może również ominąć mechanizmy bezpieczeństwa i nasłuchiwać udostępnianych informacji. Aby przeprowadzić ten atak, osoba atakująca musi użyć niedrogiego sprzętu z wbudowanym oprogramowaniem układowym i drobnego kodowania oprogramowania.

Atak KNOB: atak A Key Negotiation of Bluetooth (KNOB) umożliwia atakującemu złamanie mechanizmów bezpieczeństwa Bluetooth i przeprowadzenie ataku am MITM na sparowane urządzenia bez śledzenia. Atakujący wykorzystuje lukę w bezprzewodowym standardzie Bluetooth i podsłuchuje wszystkie dane udostępniane w sieci, takie jak naciśnięcia klawiszy, rozmowy i dokumenty. Atak KNOB jest szczególnie szkodliwy dla dwóch urządzeń obsługujących technologię Bluetooth, które dzielą zaszyfrowane klucze. Atak jest przeprowadzany na protokoły komunikacji krótkiego zasięgu Bluetooth, negocjując klucze szyfrujące wymagane do współdzielenia między węzłami w celu nawiązania połączenia.

Atak polegający na fałszowaniu adresu MAC: Atak polegający na fałszowaniu adresu MAC to atak pasywny, w którym atakujący fałszują adres MAC docelowego urządzenia obsługującego technologię Bluetooth w celu przechwycenia lub manipulowania danymi wysyłanymi do urządzenia docelowego.

Atak Man-in-the-Middle / podszywanie się: W ataku MITM / podszywanie się osoby atakujące manipulują danymi przesyłanymi między urządzeniami komunikującymi się za pośrednictwem połączenia Bluetooth (piconet). Podczas tego ataku urządzenia, które miały się ze sobą sparować, nieświadomie łączą się z urządzeniem atakującego, umożliwiając w ten sposób atakującemu przechwycenie i manipulowanie danymi przesyłanymi w sieci piconet.

Zagrożenia Bluetooth

Podobnie jak sieci bezprzewodowe, urządzenia Bluetooth również mają różne zagrożenia bezpieczeństwa. Atakujący wykorzystują luki w zabezpieczeniach konfiguracji urządzeń Bluetooth, aby uzyskać dostęp do poufnych informacji i sieci, do której są podłączone. Poniżej przedstawiono niektóre zagrożenia bezpieczeństwa Bluetooth.

Wyciek kalendarzy i książek adresowych: osoby atakujące mogą ukraść dane osobowe użytkownika i wykorzystać je do złośliwych celów.

Podsłuchiwanie urządzeń: osoby atakujące mogą nakazać smartfonowi wykonanie połączenia z innymi telefonami bez interakcji użytkownika. Mogą nawet nagrywać rozmowy użytkownika.

Wysyłanie wiadomości SMS: Terroryści mogą wysyłać fałszywe groźby bombowe do linii lotniczych za pomocą smartfonów legalnych użytkowników.

Powodowanie strat finansowych: Hakerzy mogą wysyłać wiele wiadomości MMS za pomocą telefonu międzynarodowego użytkownika, co skutkuje wysokimi rachunkami telefonicznymi.

Zdalne sterowanie: Hakerzy mogą zdalnie sterować smartfonem, aby wykonywać połączenia telefoniczne lub łączyć się z Internetem.

Socjotechnika: atakujący mogą nakłonić użytkowników Bluetooth do obniżenia bezpieczeństwa lub wyłączenia uwierzytelniania połączeń Bluetooth w celu sparowania z nimi i kradzieży ich informacji.

Złośliwy kod: robaki na smartfony mogą wykorzystywać połączenie Bluetooth do replikacji i rozprzestrzeniania się.

Luki w protokole: Atakujący wykorzystują parowanie Bluetooth i protokoły komunikacyjne do kradzieży danych, wykonywania połączeń, wysyłania wiadomości, przeprowadzania ataków DoS na urządzenie, szpiegowania telefonów itp.

Bluejacking

Bluejacking to metoda tymczasowego przejęcia smartfona poprzez wysłanie do niego anonimowej wiadomości tekstowej za pomocą bezprzewodowego systemu sieciowego Bluetooth. Wykorzystuje lukę w zabezpieczeniach w opcjach przesyłania wiadomości w smartfonach. Zasięg działania urządzeń Bluetooth klasy 2 wynosi 10 m. Smartfony z obsługą Bluetooth mogą wyszukiwać inne smartfony z obsługą Bluetooth, wysyłając do nich wiadomości. W bluejackingu anonimowe wiadomości są wysyłane do urządzeń obsługujących technologię Bluetooth za pośrednictwem protokołu OBEX. Bluejacking można wykonać, wykonując następujące kroki.

Wybierz obszar z wieloma użytkownikami mobilnymi, na przykład kawiarnię lub centrum handlowe.

Przejdź do kontaktów w książce adresowej.

Utwórz nowy kontakt (ten kontakt może zostać później usunięty).

Wpisz wiadomość w polu imienia, na przykład „Czy chcesz się ze mną umówić?”

Zapisz nowy kontakt z tekstem nazwy i bez numeru telefonu.

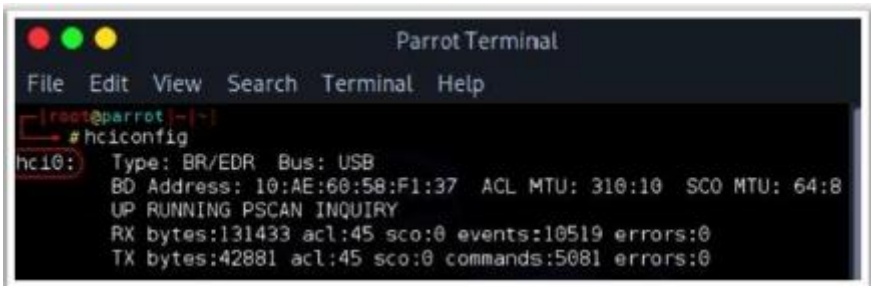
Wybierz „wyślij przez Bluetooth”, co spowoduje wyszukanie dowolnego urządzenia Bluetooth w zasięgu.

Wybierz jeden telefon z listy urządzeń Bluetooth i wyślij kontakt.

Po otrzymaniu komunikatu „karta wysłana” nasłuchuj sygnału SMS telefonu ofiary.

Rekonesans Bluetooth za pomocą BlueZ

Stos protokołów Bluetooth umożliwia użytkownikom łączenie się z innymi urządzeniami i wykonywanie czynności. BlueZ to podobny wbudowany stos protokołów dla systemów opartych na Linuksie, który ma kilka domyślnych narzędzi do rekonesansu Bluetooth. Ponieważ są one dostępne w każdym systemie Linux, osoba atakująca może je wykorzystać przy niewielkich umiejętnościach dowódczych. Atakujący używają narzędzi BlueZ do wykrywania urządzeń Bluetooth, wykonując następujące czynności. Skonfiguruj urządzenie Bluetooth za pomocą „hciconfig”: Użyj domyślnego narzędzia BlueZ hciconfig, aby potwierdzić wykrycie i aktywację urządzenia Bluetooth.



Jak pokazano na powyższym rysunku, urządzenie Bluetooth i jego adres MAC o nazwie hciO zostało wykryte. Teraz użyj następującego polecenia, aby rozpocząć proces:

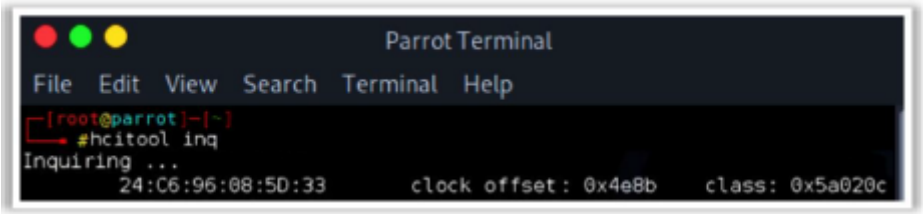
hciconfig hci0 up

Wyszukiwanie urządzeń Bluetooth, które można sparować, za pomocą „hcitool”: osoba atakująca utrzymuje aktywne urządzenie Bluetooth i skanuje w poszukiwaniu innych urządzeń Bluetooth, które przesyłają sygnały parowania. Urządzenia, które można sparować, są wykrywane za pomocą następującego polecenia:

hcitool scan

Po znalezieniu urządzeń, które można sparować, użyj następującego polecenia, aby wyświetlić dalsze informacje o wykrytych urządzeniach:

hcitool inq



Jak pokazano na powyższym rysunku, wyświetlana jest klasa i przesunięcie zegara. Klasa ujawnia

informacje o urządzeniu.

Użyj narzędzia Service Discovery Protocol (SDP), aby przeskanować usługi: sdptool jest wydajnym narzędziem służącym do wyszukiwania usług oferowanych przez urządzenie. Jego składnia to

sdptool browse <MAC Address>

Pinguj wszystkie dostępne urządzenia, aby sprawdzić, czy są osiągalne za pomocą L2ping: atakujący ma teraz adresy MAC dostępnych urządzeń i wysyła polecenie ping do wszystkich z nich, aby sprawdzić, czy są one dostępne lub czy można je wykryć za pomocą narzędzia „I2ping”. Jego składnia to 12ping <MAC ADRESS>

Wykonując powyższe kroki, osoby atakujące mogą zbierać informacje, takie jak adresy MAC i usługi oferowane przez urządzenia. Dzięki tym informacjom mogą przeprowadzać dalsze ataki.

Btlejacking za pomocą Btlejacka

BtleJack to oprogramowanie typu open source, które umożliwia atakującemu wykonanie ataku Btlejacking przy użyciu narzędzia sprzętowego, takiego jak micro:bit (https://microbit.org). Pomaga atakującym wąchać, blokować i przejmować połączenia Bluetooth. Po uzyskaniu dostępu do połączenia osoba atakująca może przejąć kontrolę, odczytać i wyeksportować poufne informacje udostępniane między podłączonymi urządzeniami. Btlejacking jest wykonywany przy użyciu następujących kroków. Wybierz urządzenia docelowe za pomocą następującego polecenia:

btlejack -d /dev/ttyACMO -d /dev/ttyACM2 -s

Za pomocą narzędzia Btlejack zajmij pozycję w promieniu 5 m od urządzeń docelowych.

Przechwytywanie już ustanowione (na żywo), a także nowy Bluetooth o niskim zużyciu energii (BLE) połączenia za pomocą następujących poleceń.

Sniffowanie istniejącego połączenia:

btlejack -s

Wyszukiwanie nowych połączeń:

btlejack -c any

Po przechwyceniu połączenia wykonaj operację zagłuszania w następujący sposób

btlejack -f 0xl29f3244 –j

Rozpocznij przejmowanie połączenia za pomocą następującego polecenia:

btiejack -f 0x9c68fd30 -t -m Oxlfffffffff

Przechwycone dane można przekonwertować do formatu pcap za pomocą następującego polecenia:

btlejack -f 0xac56bcl2 -x nordic -o capture.nordic.pcap

Łamanie szyfrowania BLE za pomocą crackle

Technologia Bluetooth Low Energy (BLE) jest wdrażana w nowoczesnych urządzeniach i gadżetach bezprzewodowych, takich jak czujniki, telefony komórkowe, samochody, beacony i zegarki fitness. Proces wymiany danych i parowania w urządzeniach BLE może przebiegać dwuetapowo. W pierwszej fazie urządzenia wymieniają się informacjami o swoich typach i możliwościach, aby ustalić najlepszy możliwy sposób nawiązania połączenia. Druga faza jest fazą kluczową, która obejmuje ustanowienie i wymianę klucza. Atakujący mogą używać narzędzi takich jak crackle, które są ukierunkowane głównie na drugą fazę, aby włamać się i uzyskać dostęp do urządzenia docelowego.

crackle

Crackle wykorzystuje lukę w procesie parowania BLE, która umożliwia atakującemu odgadnięcie lub bardzo szybkie użycie klucza tymczasowego (TK). Dzięki TK i innym danym zebranym z procesu parowania można zebrać klucz krótkoterminowy (STK), a później klucz długoterminowy (LTK). Dzięki STK i LTK można odszyfrować całą komunikację między urządzeniami nadrzędnymi i podrzędnymi. crackle działa w dwóch trybach.

o Złamać tryb TK

Ten tryb działa podczas fazy parowania BLE, w której narzędzie próbuje brutalnie wymusić TK. W tym celu narzędzie wymaga pliku PCAP zawierającego wszystkie zdarzenia parowania BLE. Uruchom następujące polecenie, aby sprawdzić, czy wszystkie pakiety parowania są obecne w pliku PCAP, używając argumentu -i:

$ crackle -i <file.pcap>

crackle sprawdza aktywne połączenia, a następnie określa połączenia podatne na naruszenie, jak pokazano na zrzucie ekranu.

Zaszyfrowane dane pcap można odszyfrować, dodając opcję -o za pomocą następującego polecenia:

$ crackle -i <plik.pcap> -o <output.pcap>

o Deszyfrowanie za pomocą LTK

W tym trybie, aby odblokować zaszyfrowane dane, crackle wymaga wartości LTK, która jest liczbą szesnastkową 128, oraz pliku PCAP zawierającego pakiety LL_ENC_REQ i LL_ENC_RSP. Uruchom następującą komendę z opcjami -iand -1, które pomagają w weryfikacji danych w pliku:

$ crackle -i <file.pcap> -1 <LTK>

Zrzut ekranu pokazuje dostępność dziewięciu zaszyfrowanych pakietów, z których sześć można odszyfrować.

```
Analyzing connection 0:
  xx:xx:xx:xx:xx:xx (public) -> yy:yy:yy:yy:yy:yy (public)
  Found 9 encrypted packets
  Decrypted 6 packets

Specify an output file with -o to decrypt packets!
```

Uruchom następujące polecenie, aby odszyfrować pakiety i zapisać je w pliku PCAP przy użyciu opcji -o:

$ crackle -i <plik.pcap> -o <out.pcap> -1 <LTK>

Narzędzia hakerskie Bluetooth

BluetoothView

BluetoothView to narzędzie, które monitoruje aktywność urządzeń Bluetooth w pobliżu. Dla każdego wykrytego urządzenia Bluetooth wyświetla informacje, takie jak nazwa urządzenia, adres Bluetooth, główny typ urządzenia, drugorzędny typ urządzenia, czas pierwszego wykrycia i czas ostatniego wykrycia. Może również dostarczyć powiadomienie, gdy zostanie wykryte nowe urządzenie Bluetooth.

Oto kilka dodatkowych narzędzi hakerskich Bluetooth:

• BTCrawler (http://petronius.sourceforge.net)

• BlueScan (http://bluescanner.sourceforge.net)

• Bluetooth Scanner - btCrawler (https://play.google.com)

• Bluedevil (https://github.com)

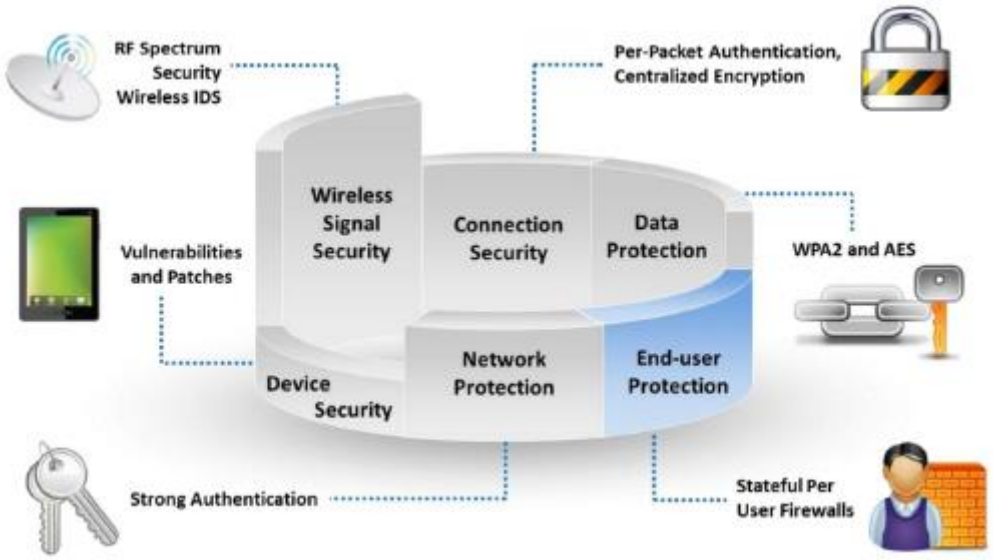
• Blueman (https://github.com)

Środki zaradcze w przypadku ataków bezprzewodowych

W poprzednich sekcjach wyjaśniono, w jaki sposób osoby atakujące włamują się do sieci bezprzewodowych w celu uzyskania poufnych danych. Etyczny haker pracuje nad zwiększeniem bezpieczeństwa sieci bezprzewodowej. Aby zabezpieczyć sieć bezprzewodową, ważne jest wdrożenie i przyjęcie odpowiednich środków zaradczych. W tej sekcji wymieniono środki zaradcze i najlepsze praktyki dotyczące bezpieczeństwa sieci bezprzewodowej.

Warstwy zabezpieczeń sieci bezprzewodowej

Bezprzewodowy mechanizm bezpieczeństwa ma sześć warstw. To warstwowe podejście zwiększa zakres ochrony sieci przed atakiem i zwiększa możliwość złapania atakującego. Poniższy rysunek przedstawia strukturę warstw zabezpieczeń sieci bezprzewodowej.



Bezpieczeństwo sygnału bezprzewodowego: W sieciach bezprzewodowych sieć i widmo RF w środowisku powinny być stale monitorowane i zarządzane w celu identyfikacji zagrożeń i świadomości. Bezprzewodowy system wykrywania włamań (WIDS) analizuje i monitoruje widmo RF. Generowanie alarmów pomaga wykrywać nieautoryzowane urządzenia bezprzewodowe, które naruszają zasady bezpieczeństwa sieci. Działania takie jak zwiększone wykorzystanie przepustowości, zakłócenia RF i nieznane nieuczciwe bezprzewodowe punkty dostępowe mogą wskazywać na złośliwego intruza w sieci. Ciągłe monitorowanie sieci to jedyny środek, który może zapobiec takim atakom i zabezpieczyć sieć.

Bezpieczeństwo połączenia: Uwierzytelnianie poszczególnych ramek/pakietów zapewnia ochronę przed atakami MUM. Uniemożliwia atakującemu podsłuchiwanie danych, gdy dwóch prawdziwych użytkowników komunikuje się ze sobą, zabezpieczając w ten sposób połączenie.

Bezpieczeństwo urządzeń: zarówno zarządzanie lukami w zabezpieczeniach, jak i poprawkami są ważnymi składnikami infrastruktury bezpieczeństwa.

Ochrona danych: Algorytmy szyfrowania, takie jak WPA3, WPA2 i AES, mogą chronić dane.

Ochrona sieci: Silne uwierzytelnianie gwarantuje, że tylko autoryzowani użytkownicy uzyskają dostęp do sieci.

Ochrona użytkowników końcowych: Nawet jeśli atakujący powiązał się z punktami dostępowymi, osobiste zapory zainstalowane w systemach użytkowników końcowych w sieci WLAN uniemożliwiają atakującemu dostęp do plików.

Obrona przed łamaniem WPA/WPA2/WPA3

Hasła

Jedynym sposobem na złamanie WPA jest wąchanie hasła PMK związanego z procesem uwierzytelniania „uzgadniania”. Jeśli to hasło jest wyjątkowo skomplikowane, jego złamanie będzie prawie niemożliwe. W celu zabezpieczenia haseł można zastosować następujące środki.

o Wybierz losowe hasło, które nie składa się ze słów ze słownika.

o Wybierz złożone hasło o długości co najmniej 20 znaków i zmieniaj je w regularnych odstępach czasu.

o Używaj słów Diceware lub menedżera haseł, aby zabezpieczyć hasła.

Ustawienia klienta

o Używaj tylko WPA2 z szyfrowaniem AES/CCMP.

o Ustaw odpowiednie ustawienia klienta (np. zweryfikuj serwer, podaj adres serwera i nie pytaj o nowe serwery).

o Regeneruj klucze dla każdego nowego połączenia.

Dodatkowe elementy sterujące

o Zapewnij okresowe aktualizacje oprogramowania sprzętowego urządzeń bezprzewodowych.

o Korzystaj z technologii wirtualnej sieci prywatnej (VPN), takich jak zdalny dostęp VPN, extranet VPN i intranet VPN.

o Zaimplementuj protokoły, takie jak IPsec i SSL/TLS, aby zapewnić bezpieczną komunikację

o Zaimplementuj rozwiązanie kontroli dostępu do sieci (NAC) lub ochrony dostępu do sieci (NAP), aby uzyskać dodatkową kontrolę nad łącznością użytkowników końcowych

Obrona przed atakami KRACK

Poniżej przedstawiono niektóre środki zaradcze zapobiegające atakom KRACK.

Zaktualizuj wszystkie routery i urządzenia Wi-Fi za pomocą najnowszych poprawek bezpieczeństwa.

Włącz automatyczne aktualizacje dla wszystkich urządzeń bezprzewodowych i zaktualizuj oprogramowanie sprzętowe urządzenia.

Unikaj korzystania z publicznych sieci Wi-Fi.

Przeglądaj tylko zabezpieczone strony internetowe i nie uzyskuj dostępu do wrażliwych zasobów, gdy urządzenie jest podłączone do niezabezpieczonej sieci.

Jeśli istnieją urządzenia loT, skontroluj urządzenia i nie łącz się z niezabezpieczonymi routerami Wi-Fi.

Zawsze włączaj rozszerzenie HTTPS Everywhere.

Włącz uwierzytelnianie dwuskładnikowe.

Użyj VPN, aby zabezpieczyć przesyłane informacje.

W sieciach bezprzewodowych zawsze używaj protokołu zabezpieczeń Wi-Fi Protected Access 3 (WPA3).

Wyłącz szybki roaming i tryb repeatera w urządzeniach bezprzewodowych, aby poprawić łagodzenie ataków KRACK.

Użyj licznika powtórzeń klucza EAPOL, aby upewnić się, że punkt dostępowy rozpoznaje tylko ostatnią wartość przeciwną.

Korzystaj z zapasowego połączenia przewodowego (Ethernet) lub mobilnej transmisji danych natychmiast po wykryciu podatności na ataki KRACK.

Korzystaj z alternatywnych routerów innych firm zamiast routerów dostarczonych przez dostawcę usług internetowych, jeśli nie zapewniają one wystarczających poprawek zabezpieczeń.

Obrona przed atakami alternatywnymi

Najważniejszą zalecaną metodą obrony sieci przed atakami ALTEr jest szyfrowanie zapytań DNS z zachowaniem odpowiednich standardów bezpieczeństwa. Aby wdrożyć ten środek, firma Cisco we współpracy z firmą Apple opracowała aplikację o nazwie „Cisco Security Connectors", która uniemożliwia klientom wchodzenie na niezamierzone strony internetowe. Ta aplikacja szyfruje zapytania DNS i ładuje je do Cisco Umbrella (blok wywiadowczy) w celu dalszej weryfikacji. Chroni sieć przed przejęciem na poziomie IP, jak również na poziomie DNS. W celu obrony przed atakami ALTER można zastosować następujące środki zaradcze.

Szyfruj zapytania DNS i używaj tylko zaufanych programów rozpoznawania nazw DNS.

Rozwiąż zapytania DNS przy użyciu protokołu HTTPS.

Uzyskuj dostęp tylko do stron internetowych z połączeniami HTTPS.

Używaj DNS przez Transport Layer Security (TLS) lub DNS przez datagram TLS (DTLS) do szyfrowania ruchu DNS i ochrony integralności.

Zaimplementuj RFC 7858/RFC 8310, aby zapobiec atakom polegającym na fałszowaniu DNS. Może również zwiększyć szyfrowanie i inteligentne zasady rozpoznawania nazw.

Dodaj kod uwierzytelniania wiadomości (MAC) do pakietów płaszczyzny użytkownika.

Użyj protokołu DNSCrypt do uwierzytelnienia komunikacji między klientem DNS a programem rozpoznawania nazw DNS.

Używaj narzędzi urządzeń mobilnych, takich jak Zimperium, do wykrywania phishingu i innych ataków ze złośliwych witryn.

Używaj prawidłowych parametrów HTTPS, takich jak HSTS, aby uniknąć przekierowania na złośliwą stronę internetową.

Użyj wirtualnego tunelu sieciowego z ochroną integralności i uwierzytelnianiem punktów końcowych.

Korzystaj z połączeń sieciowych 5G, aby zapobiegać atakom ALTEr.

Obrona przed fałszowaniem GNSS

Poniżej przedstawiono środki zaradcze do wykrywania fałszowania GNSS i obrony przed nim:

Wdróż metody obronne podczas przetwarzania sygnałów. Chociaż sygnały w GNSS po stronie odbiornika są przetwarzane w kilku etapach, fałszywe sygnały można monitorować i wykrywać na podstawie ich bezwzględnej mocy sygnału, efektu Dopplera sygnału, wartości szczytowych sygnału i odchylenia zegara.

Wdrożenie metod kryptograficznych GNSS, takich jak szyfrowanie rozproszonego kodu (SCE), uwierzytelnianie/szyfrowanie komunikatów nawigacyjnych (NMA/NME) i TESLA, aby zapobiec odtworzeniu błędnego kodu atakującego.

Skoreluj synchronizację GNSS z innymi źródłami synchronizacji, takimi jak inercyjne jednostki pomiarowe (IMU), które weryfikują dane GNSS.

Wdróż urządzenia obronne, takie jak anteny i widma radiowe, chroniące przed atakami oprogramowania.

Wdróż przetwarzanie przestrzenne z adaptacyjnym przetwarzaniem przestrzenno-czasowym (STAP), które pomaga zapobiegać zakłóceniom i replikom wielościeżkowym.

Wykrywanie i blokowanie nieuczciwych punktów dostępowych

Wykrywanie nieuczciwych punktów dostępowych

Skanowanie RF: Punkty dostępowe o zmienionym przeznaczeniu, które wykonują jedynie przechwytywanie i analizę pakietów (czujniki RF), są podłączane do całej sieci przewodowej w celu wykrywania i ostrzegania administratora sieci WLAN o wszelkich urządzeniach bezprzewodowych działających w okolicy.

Skanowanie punktów dostępowych: punkty dostępowe, które mają funkcję wykrywania sąsiednich punktów dostępowych, udostępniają dane za pośrednictwem MIBS i interfejsu sieciowego.

Wejścia przewodowe: oprogramowanie do zarządzania siecią wykorzystuje tę technikę do wykrywania nieuczciwych punktów dostępowych. To oprogramowanie wykrywa urządzenia podłączone do sieci LAN, w tym Telnet, SNMP i Cisco Discovery Protocol (CDP), przy użyciu wielu protokołów.

Blokowanie nieuczciwych punktów dostępowych

Odmów usługi bezprzewodowej nowym klientom, przeprowadzając atak typu „odmowa usługi" (DoS) na nieuczciwy punkt dostępowy.

Zablokuj port przełącznika, do którego podłączony jest punkt dostępowy lub ręcznie zlokalizuj punkt dostępowy i fizycznie usuń go z sieci LAN.

Obrona przed atakami bezprzewodowymi

Najlepsze praktyki dotyczące konfiguracji

o Zmiana domyślnego SSID po konfiguracji WLAN,

o Ustaw hasło dostępu do routera i włącz ochronę firewall,

o Wyłącz rozgłaszanie SSID.

o Wyłącz zdalne logowanie do routera i administrację bezprzewodową,

o Włącz filtrowanie adresów MAC w punktach dostępowych lub routerach,

o Włącz szyfrowanie w punktach dostępowych i często zmieniaj hasła,

o Zamknij wszystkie nieużywane porty, aby zapobiec atakom na punkty dostępowe.

o Oddziel sieć, aby upewnić się, że goście nie mają dostępu do sieci prywatnej.

o Korzystaj z zamkniętych sieci i podawaj SSID pracownikom, zamiast pozwalać im wybierać go z listy rozgłoszeniowej.

o Wyłącz protokół dynamicznej konfiguracji hosta (DHCP) i polegaj na statycznych adresach IP.

o Wyłącz protokół prostego zarządzania siecią (SNMP). Jeżeli jest to wymagane, skonfiguruj ustawienia na najmniejsze uprawnienia,

o Zmień domyślny adres IP konsoli routera.

Najlepsze praktyki dotyczące ustawień SSID

o Używaj maskowania SSID, aby niektóre domyślne wiadomości bezprzewodowe nie rozgłaszały identyfikatora SSID wszystkim.

o Nie używaj identyfikatora SSID, nazwy firmy, nazwy sieci ani żadnych łatwych do odgadnięcia ciągów w hasłach.

o Umieść zaporę ogniową lub filtr pakietów między punktem dostępowym a firmowym intranetem.

o Ogranicz moc sieci bezprzewodowej, aby nie można jej było wykryć poza granicami organizacji.

o Regularnie sprawdzaj urządzenia bezprzewodowe pod kątem problemów z konfiguracją lub konfiguracją.

o Zaimplementuj dodatkową technikę szyfrowania ruchu, taką jak IPsec przez sieć bezprzewodową.

o Zmodyfikuj identyfikator SSID za pomocą unikalnych znaków i łańcuchów, zamiast używać domyślnego identyfikatora SSID producenta.

o Użyj oddzielnego identyfikatora SSID dla gości, aby odizolować ich od sieci organizacyjnej.

o Podziel sieć organizacyjną na wiele stref z własnymi identyfikatorami SSID, aby zmniejszyć poziom wykorzystania podczas ataków.

o Zawsze utrzymuj rozgłaszanie SSID urządzeń bezprzewodowych organizacji w trybie ukrytym.

Najlepsze praktyki dotyczące uwierzytelniania

o Wybierz WPA2-Enterprise z uwierzytelnianiem 802.lx zamiast WPA lub WEP.

o Implementuj WPA2/WPA3-Enterprise tam, gdzie to możliwe,

o Wyłącz sieć, gdy nie jest wymagana.

o Umieść bezprzewodowe punkty dostępowe w bezpiecznym miejscu.

o Aktualizuj sterowniki wszystkich urządzeń bezprzewodowych.

o Użyj scentralizowanego serwera do uwierzytelniania.

o Aby temu zapobiec, włącz weryfikację serwera po stronie klienta przy użyciu uwierzytelniania 802.IX

Ataki MITM.

Włącz uwierzytelnianie dwuskładnikowe jako dodatkową linię obrony.

Wdrażaj systemy wykrywania nieuczciwych punktów dostępowych lub systemy zapobiegania/wykrywania włamań bezprzewodowych, aby zapobiegać atakom bezprzewodowym.

Obrona przed hakowaniem Bluetooth

Bluetooth działa w jednym z czterech trybów bezpieczeństwa. Urządzenia Bluetooth przyjmujące tryb bezpieczeństwa 1 mają bardzo niski poziom bezpieczeństwa, narażając siebie i sieć na ataki. Stan zabezpieczeń poprawia się wraz ze wzrostem numeru trybu zabezpieczeń. W celu ustanowienia parowania Bluetooth między zgłaszającym (nadawcą) a weryfikatorem (odbiorcą), tryby bezpieczeństwa 2 i 3 implementują technikę parowania osobistego numeru identyfikacyjnego (PIN),

podczas gdy tryb bezpieczeństwa 4 implementuje technikę prostej bezpiecznej analizy składniowej (SSP). Urządzenia Bluetooth, które wykorzystują tryb bezpieczeństwa 4, uniemożliwiają hakerom uzyskanie dostępu do urządzenia lub sieci Bluetooth. Poniżej przedstawiono niektóre środki zaradcze w celu obrony przed hakowaniem Bluetooth.

Używaj nieregularnych wzorów jako kodów PIN podczas parowania urządzenia. Kombinacje klawiszy nie powinny następować po sobie na klawiaturze.

Utrzymuj Bluetooth w stanie wyłączonym i włączaj go tylko wtedy, gdy jest to konieczne. Wyłącz Bluetooth natychmiast po zakończeniu zamierzonego zadania.

Utrzymuj urządzenie w trybie niewykrywalnym (ukrytym).

Nie akceptuj żadnych nieznanych lub nieoczekiwanych próśb o sparowanie.

Regularnie sprawdzaj wszystkie sparowane urządzenia w przeszłości i usuwaj podejrzane sparowane urządzenia.

Zawsze włączaj szyfrowanie podczas nawiązywania połączenia Bluetooth.

Ustaw zasięg sieci urządzenia obsługującego technologię Bluetooth na najniższy i przeprowadzaj parowanie tylko w bezpiecznym obszarze.

Zainstaluj oprogramowanie antywirusowe obsługujące oprogramowanie zabezpieczające oparte na hoście na urządzeniach obsługujących technologię Bluetooth.

Zmień domyślne ustawienia urządzenia obsługującego technologię Bluetooth na najlepszy standard bezpieczeństwa.

Używaj szyfrowania łącza dla wszystkich połączeń Bluetooth.

Jeśli używanych jest wiele połączeń bezprzewodowych, upewnij się, że na każdym łączu w łańcuchu komunikacyjnym włączone jest szyfrowanie.

Unikaj udostępniania poufnych informacji za pośrednictwem urządzeń obsługujących technologię Bluetooth.

Wyłącz automatyczne połączenia z publicznymi sieciami Wi-Fi, aby chronić urządzenia Bluetooth przed niezabezpieczonymi źródłami.

Aktualizuj oprogramowanie i sterowniki urządzeń Bluetooth oraz regularnie zmieniaj hasła.

Użyj VPN do bezpiecznych połączeń między urządzeniami Bluetooth.

Wyłącz uprawnienia dostępu Bluetooth do aplikacji natychmiast po zakończeniu zamierzonego zadania.

Bezprzewodowe narzędzia bezpieczeństwa

W poprzedniej sekcji omówiono najlepsze praktyki i środki zaradcze w celu zabezpieczenia sieci WLAN. Etyczni hakerzy mogą również używać zautomatyzowanych narzędzi bezpieczeństwa sieci bezprzewodowych do utrzymywania bezpieczeństwa w sieciach bezprzewodowych. W tej sekcji przedstawiono różne narzędzia zabezpieczające sieć bezprzewodową.

Bezprzewodowe systemy zapobiegania włamaniom

Bezprzewodowy system zapobiegania włamaniom (WIPS) to urządzenie sieciowe, które monitoruje widmo radiowe w celu wykrywania punktów dostępowych (wykrywanie włamań) bez zgody hosta w pobliskich lokalizacjach. Może również automatycznie wdrażać środki zaradcze. WIPS chronią sieci przed zagrożeniami bezprzewodowymi i zapewniają administratorom możliwość wykrywania różnych ataków sieciowych i zapobiegania im.

Wdrożenie WIPS

WIPS składa się z kilku komponentów, które współpracują ze sobą, tworząc ujednolicone rozwiązanie do monitorowania bezpieczeństwa. Wdrożenie WIPS firmy Cisco obejmuje następujące funkcje komponentów:

Punkty dostępowe w trybie monitorowania: ten tryb zapewnia ciągłe skanowanie kanałów z możliwością wykrywania ataków i przechwytywania pakietów.

Silnik usług mobilności (uruchamiający usługę bezprzewodowego IPS): Jest to centralny punkt agregacji alarmów ze wszystkich kontrolerów i ich odpowiednich bezprzewodowych punktów dostępowych IPS w trybie monitorowania. Informacje o alarmach i pliki śledcze są przechowywane w systemie w celu archiwizacji.

Punkty dostępowe w trybie lokalnym: Ten tryb zapewnia klientom usługi bezprzewodowe oprócz skanowania nieautoryzowanych i lokalizacyjnych z podziałem czasu.

Kontrolery bezprzewodowej sieci LAN: te kontrolery przekazują informacje o ataku z bezprzewodowych punktów dostępowych IPS w trybie monitorowania do MSE i przesyłają parametry konfiguracyjne do punktów dostępowych.

Bezprzewodowy system sterowania: Zapewnia środki do konfigurowania bezprzewodowej usługi IPS w MSE, wysyłania bezprzewodowych konfiguracji IPS do kontrolera i ustawiania punktów dostępowych w trybie monitora bezprzewodowego IPS. Jest również używany do przeglądania bezprzewodowych alarmów IPS, analizy śledczej, raportowania i uzyskiwania dostępu do encyklopedii zagrożeń.

Narzędzia audytu bezpieczeństwa Wi-Fi

Cisco Adaptive Wireless IPS

Cisco Adaptive Wireless Intrusion Prevention System (IPS) oferuje zaawansowane zabezpieczenia sieci do dedykowanego monitorowania i wykrywania anomalii w sieci bezprzewodowej, nieautoryzowanego dostępu i ataków radiowych. Rozwiązanie to, w pełni zintegrowane z Cisco Unified Wireless Network, zapewnia zintegrowany wgląd i kontrolę w całej sieci, bez potrzeby stosowania rozwiązania nakładkowego. Adaptive WIPS zapewnia wykrywanie i łagodzenie zagrożeń w sieci bezprzewodowej przed złośliwymi atakami i lukami w zabezpieczeniach. Zapewnia także specjalistom ds. bezpieczeństwa możliwość wykrywania, analizowania i identyfikowania zagrożenia bezprzewodowego.

Oto kilka dodatkowych narzędzi do audytu bezpieczeństwa Wi-Fi:

AirMagnet WiFi Analyzer PRO (https://www.netolly.com)

RFProtect (https://www.orubonetworks.com)

Fern Wifi Cracker (https://github.com)

OSWA-Assistant (https://securitystortshere.org)

BoopSuite (https://github.com)

Wi-Fi IPS

Wi-Fi IPS blokują zagrożenia bezprzewodowe, automatycznie skanując, wykrywając i klasyfikując nieautoryzowany dostęp bezprzewodowy i nieuczciwy ruch do sieci, zapobiegając w ten sposób sąsiadującym użytkownikom lub wykwalifikowanym hakerom uzyskanie nieautoryzowanego dostępu do zasobów sieci Wi-Fi.

WatchGuard Wi-Fi Cloud WIPS

WatchGuard Wi-Fi Cloud WIPS chroni przed nieautoryzowanymi urządzeniami i nieuczciwymi aplikacjami, zapobiega złym bliźniakom i blokuje złośliwe ataki, takie jak ataki DoS, z niemal zerową liczbą fałszywych alarmów, zapewniając jednocześnie wysoką wydajność łączności bezprzewodowej.

Poniżej przedstawiono kilka dodatkowych narzędzi zapobiegania włamaniom bezprzewodowym:

Extreme AirDefense (https://www.extremenetworks.com)

SonicWall SonicPoint N2 (https://www.sonicwoll.com)

Menedżer sieci bezprzewodowej SonicPoint (https://www.sonicwoll.com)

Network Box IDP (https://www.network-box.com)

Zapory nowej generacji FortiGate (NGFW) (https://www.fortinet.com)

Narzędzia planowania predykcyjnego Wi-Fi

Narzędzia planowania predykcyjnego Wi-Fi służą do planowania, wdrażania, monitorowania, rozwiązywania problemów i tworzenia raportów dotyczących sieci bezprzewodowych z centralnej lokalizacji.

Planer AirMagnet

AirMagnet Planner to narzędzie do planowania sieci bezprzewodowej, które uwzględnia materiały budowlane, przeszkody, konfiguracje punktów dostępowych, układy anten i kilka innych zmiennych, aby zapewnić niezawodną mapę predykcyjną sygnału i wydajności Wi-Fi.

Oto kilka dodatkowych narzędzi do planowania predykcyjnego Wi-Fi:

Cisco Prime Infrastructure (https://www.cisco.com)

Ekahau Pro (https://www.ekohou.com)

TamoGraph Site Survey (https://www.tomos.com)

NetSpot (https://www.netspotopp.com)

Wi-Fi Designer (https://www.combiumnetworks.com)

Narzędzia do skanowania luk w zabezpieczeniach sieci Wi-Fi

Specjaliści ds. bezpieczeństwa używają narzędzi do skanowania pod kątem luk w zabezpieczeniach sieci Wi-Fi w celu określenia słabych punktów w sieciach bezprzewodowych i zabezpieczenia ich przed wystąpieniem ataków.

Zenmapa

Zenmap to wieloplatformowy graficzny interfejs użytkownika dla skanera bezpieczeństwa Nmap, który jest przydatny do skanowania luk w sieciach bezprzewodowych. To narzędzie zapisuje skany w poszukiwaniu luk w zabezpieczeniach jako profile, aby były uruchamiane wielokrotnie. Wyniki ostatnich skanów są przechowywane w bazie danych z możliwością wyszukiwania.

Oto kilka dodatkowych narzędzi do skanowania luk w zabezpieczeniach sieci Wi-Fi:

Nessus Pro (https://www.tenoble.com)

Network Security Toolkit (https://networksecuritytoolkit.org)

Nexpose (https://www.ropid7.com)

Penetrator Vulnerability Scanner (https://www.secpoint.com)

SILICA (http://www.immunityinc.com)

Narzędzia bezpieczeństwa Bluetooth

Zapora sieciowa Bluetooth

FruitMobile Bluetooth Firewall chroni urządzenia z Androidem przed wszystkimi rodzajami ataków Bluetooth. Wyświetla alerty, gdy występują działania Bluetooth. Umożliwia także użytkownikowi skanowanie urządzenia i wykrywanie aplikacji z funkcjami Bluetooth.

Oto kilka dodatkowych narzędzi zabezpieczających Bluetooth:

• BlueMaho (https://github.com)

• Btscanner (https://packages.debian.org)

• SecureTether (https://play.google.com)

• AccessPro Bluetooth (https://play.google.com)

• Bluetooth Inspector (https://apps.appie.com)

Narzędzia bezpieczeństwa Wi-Fi dla urządzeń mobilnych

ARP Guard

ARP Guard zapewnia ochronę przed atakami sieciowymi, takimi jak fałszowanie ARP i zatruwanie ARP. Zapewnia funkcję automatycznego wyłączania Wi-Fi po wykryciu ataku w trybie innym niż root.

Safe Connect VPN: bezpieczne Wi-Fi

Safe Connect VPN: Secure Wi-Fi pozwala użytkownikowi aktywować bezpieczne i bezpieczne połączenie VPN dla wszystkich swoich urządzeń podczas korzystania z publicznych hotspotów Wi-Fi. Maskuje adres IP użytkownika przed cyberprzestępcami korzystającymi z hotspotów VPN, zapewniając, że działania online pozostają zarówno prywatne, jak i bezpieczne.

Wifi Inspector

Wifi Inspector wyszukuje wszystkie urządzenia podłączone do sieci (zarówno przewodowej, jak i Wi-Fi, w tym konsole, telewizory, komputery PC, tablety i telefony), podając odpowiednie dane, takie jak adresy IP, nazwy producentów, nazwy urządzeń i adresy MAC. To narzędzie może obsługiwać urządzenia uzyskujące dostęp do danych. Pozwala także na zapisanie listy znanych urządzeń z niestandardowymi nazwami i szybkie odnajdywanie intruzów.

Oto kilka dodatkowych narzędzi zabezpieczających Wi-Fi dla urządzeń mobilnych:

Secure Wi-Fi (https://play.google.com)

Hotspot Shield (https://play.google.com)

Fing - narzędzia sieciowe (https://play.google.com)

Net Master (https://play.google.com)

WIFI PASSWORD (https://play.google.com)

Podsumowanie modułu

W tym module omówiliśmy koncepcje sieci bezprzewodowych oraz różne typy technologii szyfrowania bezprzewodowego. Omówiliśmy również szczegółowo różne zagrożenia bezprzewodowe i metodologię hakowania bezprzewodowego, obejmującą wykrywanie Wi-Fi, mapowanie GPS, analizę ruchu bezprzewodowego, przeprowadzanie ataków bezprzewodowych i łamanie szyfrowania Wi-Fi. Moduł ten ilustruje również różne narzędzia do hakowania bezprzewodowego. Ponadto omówiliśmy koncepcje hakowania Bluetooth i metody hakowania urządzeń Bluetooth za pomocą różnych narzędzi hakerskich Bluetooth. Ponadto omówiliśmy różne środki zaradcze zapobiegające próbom hakowania sieci bezprzewodowych przez cyberprzestępców. Na koniec w tym module przedstawiono szczegółową dyskusję na temat zabezpieczania sieci bezprzewodowych za pomocą narzędzi bezpieczeństwa bezprzewodowego. W następnym module omówimy szczegółowo, w jaki sposób osoby atakujące, a także etyczni hakerzy i pentesterzy przeprowadzają mobilne hakowanie w celu przejęcia urządzeń mobilnych.