Podsłuchiwanie pakietów w sieciach bezprzewodowych 802.11

Wprowadzenie

Po zapoznaniu się z podsłuchiwaniem pakietów za pomocą programu Wireshark, omówimy podsłuchiwanie pakietów w sieciach bezprzewodowych 802.11 (WLAN). Omówimy podstawy sieci bezprzewodowych, przechwytywanie i analizę ruchu sieciowego w sieci WLAN. Rozpoczyna się krótkim wprowadzeniem do sieci WLAN i niezbędną konfiguracją przechwytywania pakietów. Następnie omawiamy podsłuchiwanie ruchu sieciowego WLAN oraz różnice między trybami monitorowania i promiscuous. Obejmuje również analizę różnych typów ruchu WLAN, w tym WPA/WPA2 z PSK lub EAP, ruchu multicast i uwierzytelniania internetowego. Celem jest kompleksowe zrozumienie podsłuchiwania pakietów WLAN i efektywnej analizy przechwyconego ruchu WLAN.

Cele

Celem jest kompleksowe zrozumienie standardu WLAN 802.11 oraz sposobów efektywnego przechwytywania i analizowania ruchu w sieci WLAN. Omawiamy architekturę sieci bezprzewodowych 802.11, w tym strukturę pakietów i tryby kart bezprzewodowych. Wyjaśnia różnicę między trybem monitorowania a trybem promiscuous oraz konfiguruje niezbędne środowisko do przechwytywania ruchu w sieci WLAN. Koncentruje się na technikach podsłuchiwania ruchu w sieci WLAN za pomocą programu Wireshark i zawiera szczegółowe instrukcje dotyczące używania programu Wireshark do przechwytywania i analizowania ruchu w sieciach WLAN. Omawia analizę przechwyconych danych sniffera 802.11, w tym WPA/WPA2 z PSK lub EAP, multicast i uwierzytelnianie web. Po przeczytaniu czytelnicy będą mieli solidną wiedzę na temat narzędzi i metodologii używanych do przechwytywania i analizowania ruchu w sieciach WLAN, a także na temat zagrożeń bezpieczeństwa związanych z sieciami WLAN i sposobów ich ograniczania. Niniejszy rozdział ma na celu wyposażenie czytelnika w wiedzę i umiejętności niezbędne do przeprowadzania sniffingu sieci WLAN w uzasadnionych i etycznych celach, takich jak analiza sieci i rozwiązywanie problemów.

Sieci bezprzewodowe 802.11

IEEE 802.11 to zestaw standardów dla bezprzewodowych sieci lokalnych (WLAN), które definiują specyfikacje komunikacji bezprzewodowej między urządzeniami w sieci WLAN. Jest to rodzaj sieci lokalnej, która wykorzystuje technologię komunikacji bezprzewodowej do przesyłania i odbierania danych drogą radiową, w przeciwieństwie do komunikacji kablowej. Standardy 802.11 określają warstwę fizyczną, warstwę kontroli dostępu do nośnika (MAC) oraz mechanizmy zarządzania i bezpieczeństwa sieci WLAN. Warstwa fizyczna definiuje specyfikacje bezprzewodowej transmisji danych, w tym pasma częstotliwości, szybkości transmisji danych i techniki modulacji. Warstwa MAC określa, w jaki sposób urządzenia w sieci WLAN uzyskują dostęp do kanału bezprzewodowego i współdzielą go, a także zarządzają transmisją i odbiorem danych. Mechanizmy zarządzania i bezpieczeństwa obejmują specyfikacje dotyczące zarządzania siecią WLAN, takie jak zarządzanie energią, oraz zabezpieczania sieci WLAN, takie jak szyfrowanie i uwierzytelnianie. Sieci WLAN oparte na standardach 802.11 są powszechnie nazywane sieciami Wi-Fi. Sieci Wi-Fi wykorzystują technologię częstotliwości radiowej (RF) do przesyłania i odbierania danych bezprzewodowo i są wykorzystywane w różnych zastosowaniach, w tym w domach, biurach, publicznych hotspotach i sieciach korporacyjnych. Sieci Wi-Fi mogą obsługiwać wiele urządzeń jednocześnie, zapewniając wysoką prędkość transmisji danych i niezawodną komunikację. Standardy 802.11 ewoluowały z czasem, aby zapewnić szybsze prędkości transmisji danych i lepsze bezpieczeństwo, a najnowszym standardem jest 802.11ax (znany również jako Wi-Fi 6). 802.11ax wprowadza kilka nowych technologii, takich jak MU-MIMO i OFDMA, aby poprawić wydajność i przepustowość sieci Wi-Fi oraz obsługiwać wyższe prędkości transmisji danych i większą liczbę podłączonych urządzeń. Podsumowując, sieci WLAN

802.11 to bezprzewodowe sieci lokalne oparte na standardach 802.11 dla komunikacji bezprzewodowej i są powszechnie znane jako sieci Wi-Fi. Sieci WLAN wykorzystują technologię RF do przesyłania i odbierania danych drogą radiową i są szeroko stosowane ze względu na łatwość wdrożenia, wysoką przepustowość i kompatybilność z różnymi urządzeniami. Standardy 802.11 określają mechanizmy fizyczne, adresy MAC, zarządzania i bezpieczeństwa dla sieci WLAN i zostały opracowane w celu zapewnienia większej przepustowości i lepszego bezpieczeństwa.

Architektura sieci bezprzewodowej 802.11

Architektura sieci bezprzewodowej 802.11, znana również jako Wi-Fi, to technologia bezprzewodowej sieci lokalnej (WLAN), która umożliwia urządzeniom komunikację między sobą i dostęp do internetu bez konieczności stosowania kabli. Głównymi elementami sieci bezprzewodowej 802.11 są:

Punkt dostępu bezprzewodowego (AP): Punkt dostępu jest centrum łączności dla wszystkich klientów bezprzewodowych, którzy łączą się z siecią i uzyskują do niej dostęp. Posiada bezprzewodowy nadajnik-odbiornik radiowy i antenę, które służą do transmisji sygnału bezprzewodowego na określonym obszarze. Posiada również przewodowe połączenie z internetem lub siecią lokalną, umożliwiając klientom bezprzewodowym dostęp do internetu lub innych zasobów w sieci lokalnej.

Klienci bezprzewodowi: Są to urządzenia, które łączą się z siecią za pośrednictwem punktu dostępu. Klientami bezprzewodowymi mogą być laptopy, smartfony, tablety, inteligentne urządzenia domowe i inne urządzenia z kartą sieciową bezprzewodową. Klient bezprzewodowy posiada kartę sieciową z nadajnikiem-odbiornikiem radiowym i anteną, która służy do odbierania sygnału z punktu dostępu i komunikacji z nim.

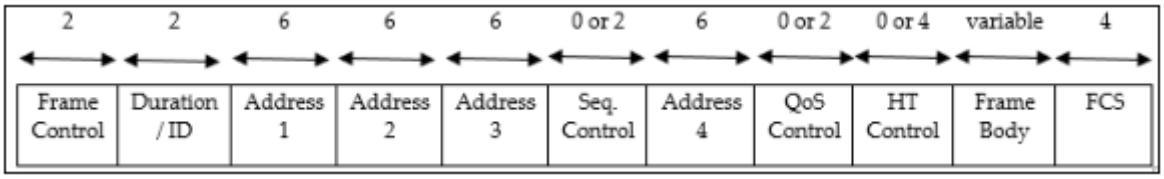
Karta sieciowa (NIC): Jest to element urządzenia, który umożliwia mu połączenie z siecią bezprzewodową. Karta sieciowa to urządzenie sprzętowe zawierające nadajnik-odbiornik radiowy i antenę, a także inne komponenty niezbędne do komunikacji bezprzewodowej. Odpowiada za przesyłanie i odbieranie danych między urządzeniem a punktem dostępu. Router bezprzewodowy: Router bezprzewodowy łączy w sobie funkcjonalność punktu dostępowego i routera, umożliwiając wielu klientom bezprzewodowym połączenie się z jedną siecią i dostęp do internetu. Router posiada przewodowe połączenie z internetem, a także bezprzewodowy nadajnik-odbiornik radiowy i antenę, które służą do transmisji sygnału bezprzewodowego. Router posiada również funkcje routingu, które umożliwiają przekazywanie danych między klientami bezprzewodowymi a internetem.

Karty sieciowe bezprzewodowe: Urządzenia te można dodać do komputera lub innego urządzenia, aby umożliwić mu połączenie z siecią bezprzewodową. Karta sieciowa zawiera bezprzewodowy nadajnik-odbiornik radiowy i antenę, a także inne komponenty niezbędne do komunikacji bezprzewodowej. Karta sieciowa odpowiada za przesyłanie i odbieranie danych między urządzeniem a punktem dostępowym.

W sieci bezprzewodowej 802.11 komunikacja między różnymi komponentami odbywa się bezprzewodowo, wykorzystując fale radiowe do przesyłania danych. Punkt dostępowy i klienci bezprzewodowi używają określonej częstotliwości i protokołu do komunikacji, a dane są szyfrowane w celu zapewnienia ich bezpieczeństwa i poufności. Standard 802.11 definiuje kilka różnych częstotliwości i protokołów, w tym 802.11a, 802.11b, 802.11g, 802.11n i 802.11ac, z których każdy ma swoje własne możliwości i specyfikacje.

Struktura pakietu 802.11

Główną różnicą między pakietami przewodowymi i bezprzewodowymi jest dodanie nagłówka 802.11 w pakietach bezprzewodowych, który zawiera informacje o typie przesyłanej ramki i jej miejscu docelowym. Rysunek przedstawia podział każdego pola w strukturze pakietu 802.11:



Kontrola ramki: To 2-bajtowe pole zawiera informacje o typie przesyłanej ramki, jej podtypie oraz inne informacje sterujące, takie jak zarządzanie energią, szybkość transmisji danych i fragmentacja. Pierwsze 2 bity tego pola wskazują typ ramki, który może być zarządzaniem, sterowaniem lub danymi. Kolejne 4 bity wskazują podtyp ramki, który dodatkowo klasyfikuje typ ramki. Pozostałe bity zawierają informacje sterujące specyficzne dla typu i podtypu ramki.

Czas trwania/ID: To 2-bajtowe pole wskazuje, jak długo medium bezprzewodowe będzie zarezerwowane na transmisję ramki. Może być używane zarówno do określania odstępu między ramkami, jak i metod dostępu opartych na rywalizacji.

Adres 1, 2 i 3: Te 6-bajtowe pola zawierają odpowiednio adresy MAC urządzenia docelowego, urządzenia źródłowego i punktu dostępowego (jeśli dotyczy).

Kontrola sekwencji: To pole o wartości 0 lub 23 bajtów służy do wskazania numeru sekwencyjnego pakietu, a także numeru sekwencyjnego fragmentacji, jeśli pakiet jest pofragmentowany.

Adres 4: To 6-bajtowe pole występuje w niektórych typach ramek, takich jak ramki zarządzania używane do uwierzytelniania i kojarzenia, i służy do wskazania adresu stacji pomocniczej, takiej jak klient lub repeater.

Sterowanie QoS: To 2-bajtowe pole występuje tylko w niektórych typach ramek, takich jak ramki danych z włączoną funkcją Quality of Service (QoS), i służy do wskazania priorytetu ramki oraz liczby zawartych w niej fragmentów.

Sterowanie HT: To 4-bajtowe pole występuje tylko w niektórych typach ramek, takich jak ramki danych korzystające z trybu wysokiej przepustowości (HT), i służy do wskazania indeksu schematu modulacji i kodowania (MCS), strumieni przestrzennych i szerokości kanału.

Treść ramki: To pole zawiera przesyłane dane, takie jak pakiet IP lub sygnał Wi-Fi.

FCS: To 4-bajtowe pole służy do weryfikacji integralności pakietu i wykrywania błędów transmisji. Jest generowane przez nadawcę i weryfikowane przez odbiorcę. Jeżeli FCS nie zgadza się z obliczoną wartością, pakiet jest odrzucany.

Zrozumienie struktury pakietów 802.11 jest istotne dla analizy i rozwiązywania problemów w sieciach Wi-Fi, ponieważ pozwala zrozumieć sposób przesyłania ramek i komunikację urządzeń za pośrednictwem łącza bezprzewodowego.

Jeśli chodzi o trzy główne typy ramek 802.11, to są to:

Ramki zarządzania: Ramki zarządzania służą do zadań zarządzania siecią, takich jak kojarzenie, uwierzytelnianie i rozłączanie. Pomagają one w nawiązywaniu i utrzymywaniu połączeń między urządzeniami w sieci bezprzewodowej. Przykładami ramek zarządzania są: żądanie skojarzenia, odpowiedź skojarzenia i uwierzytelnianie.

Ramki sterujące: Ramki te służą do sterowania przepływem i zarządzania energią. Ramki sterujące regulują przepływ danych w sieci bezprzewodowej i zarządzają zużyciem energii przez urządzenia bezprzewodowe. Przykładami ramek sterujących są: Power Save (PS), Poll (PS), Request to Send (RTS) i Clear to Send (CTS).

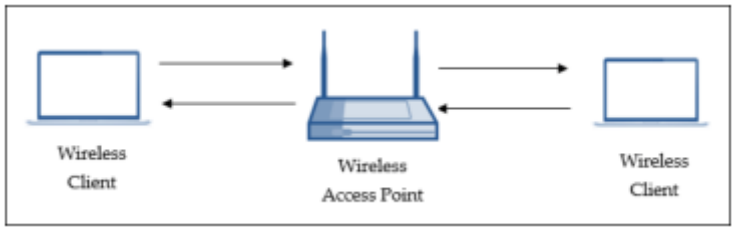
Ramki danych: Ramki te służą do przesyłania danych między urządzeniami sieciowymi. Ramki danych służą do przesyłania rzeczywistych danych wymienianych między urządzeniami w sieci bezprzewodowej. Przykładami ramek danych są: Data (Data) i Null Data (Null Data).

Należy zauważyć, że każdy z tych typów ramek ma odrębną strukturę i służy określonemu celowi w funkcjonowaniu sieci bezprzewodowej.

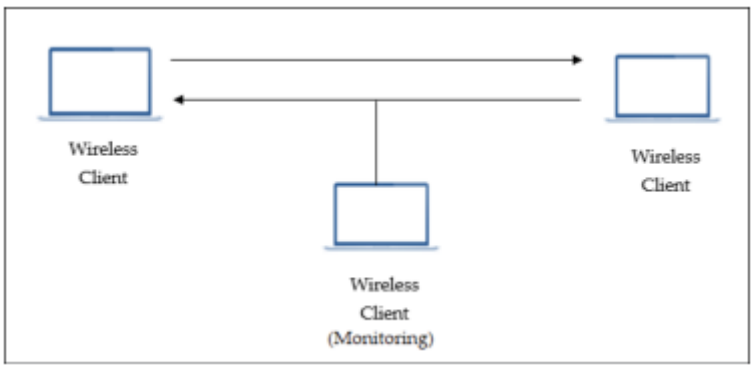
Tryby karty bezprzewodowej

Zanim zaczniemy analizować pakiety bezprzewodowe, musimy zrozumieć różne tryby, w jakich może działać karta bezprzewodowa w kontekście przechwytywania pakietów. Zasadniczo w sieci bezprzewodowej dostępne są cztery tryby pracy karty sieciowej (NIC):

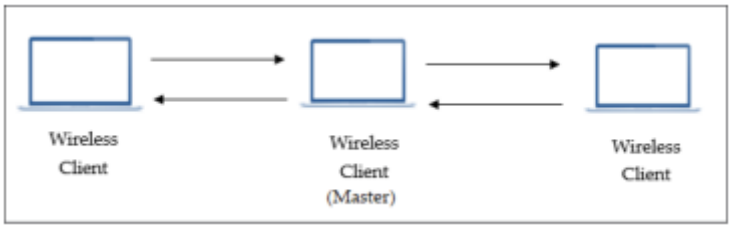
Tryb zarządzany: Jest to standardowy tryb działania bezprzewodowej karty sieciowej, w którym urządzenie jest powiązane z punktem dostępowym i może komunikować się z innymi urządzeniami w sieci. W trybie zarządzanym bezprzewodowa karta sieciowa działa w ramach ograniczeń sieci i ma ograniczone możliwości przechwytywania i przesyłania ruchu bezprzewodowego. Patrz Rysunek 2:



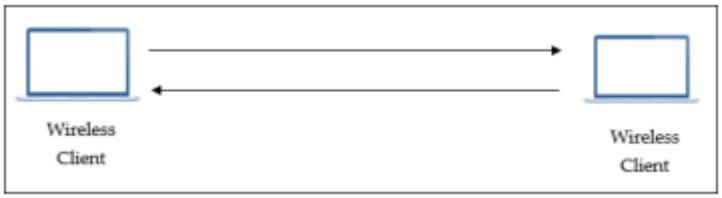
Tryb monitorowania: Ten tryb umożliwia bezprzewodowej karcie sieciowej przechwytywanie całego ruchu bezprzewodowego w swoim zasięgu, niezależnie od tego, czy jest on przeznaczony dla danego urządzenia. W trybie monitorowania bezprzewodowa karta sieciowa działa jako pasywny odbiornik, przechwytując cały ruch bezprzewodowy przesyłany w jej zasięgu. Jest on często używany do podsłuchiwania i analizy pakietów bezprzewodowych, ponieważ zapewnia dostęp do pełnego i niefiltrowanego widoku ruchu bezprzewodowego. Patrz Rysunek 3:



Tryb Master: W tym trybie karta sieciowa sieci bezprzewodowej pełni rolę punktu dostępowego, umożliwiając innym urządzeniom bezprzewodowym łączenie się i komunikację. W trybie Master karta sieciowa sieci bezprzewodowej odpowiada za zarządzanie siecią bezprzewodową i kontrolowanie dostępu do niej. Patrz Rysunek 4:



Tryb ad-hoc: Ten tryb umożliwia urządzeniom bezprzewodowym bezpośrednią komunikację między sobą bez użycia punktu dostępowego. W trybie ad-hoc karty sieciowe sieci bezprzewodowej tworzą sieć peer-to-peer i odpowiadają za bezpośrednią transmisję danych między sobą. Patrz rysunek 5:



Uwaga: Należy pamiętać, że dostępność i implementacja tych trybów może się różnić w zależności od używanego sprzętu i systemu operacyjnego. Niektóre bezprzewodowe karty sieciowe mogą obsługiwać tylko podzbiór tych trybów, podczas gdy inne mogą mieć dodatkowe tryby działania.

Ponadto niektóre karty bezprzewodowe obsługują tryb promiscuous, który pozwala im przechwytywać cały ruch w sieci, a nie tylko ruch przeznaczony dla ich adresu MAC. Tryb ten może być przydatny do monitorowania sieci i podsłuchiwania pakietów, ale może być również wykorzystywany do celów złośliwych. Przyjrzyjmy się różnicy między trybem monitorowania a trybem promiscuous.

Różnica między trybem monitorowania a trybem promiscuous

Tryb monitorowania i tryb promiscuous to dwa różne tryby działania kart sieciowych w komputerze. Tryby te określają sposób, w jaki karta sieciowa przechwytuje i filtruje ruch sieciowy. Tryb monitorowania to tryb specyficzny dla sieci bezprzewodowych, który pozwala karcie sieciowej przechwytywać wszystkie pakiety przesyłane bezprzewodowo, niezależnie od tego, czy są one przeznaczone dla hosta, czy nie. Ten tryb jest również znany jako tryb monitorowania częstotliwości radiowej (RFMON). W trybie monitorowania karta sieciowa przechwytuje wszystkie pakiety przesyłane bezprzewodowo, w tym ramki zarządzania, ramki sterujące i ramki danych. Tryb ten jest przydatny do analizy sieci i rozwiązywania problemów, ponieważ zapewnia pełny obraz ruchu w sieci bezprzewodowej. Aby skonfigurować tryb monitorowania w programie Wireshark, użytkownik musi posiadać kartę sieciową obsługującą ten tryb. Następnie użytkownik musi skonfigurować kartę do pracy w trybie monitorowania za pomocą odpowiednich narzędzi lub sterowników. Gdy karta sieciowa przejdzie w tryb monitorowania, Wireshark może przechwytywać i analizować ruch w sieci bezprzewodowej. Tryb promiscuous to z kolei funkcja powszechnie spotykana w przewodowych kartach sieciowych. W trybie promiscuous karta sieciowa przechwytuje wszystkie pakiety przesyłane w sieci, niezależnie od tego, czy są one przeznaczone dla hosta, czy nie. W przeciwieństwie do trybu monitorowania, tryb promiscuous działa tylko w sieciach przewodowych i nie ma zastosowania w sieciach bezprzewodowych. Aby skonfigurować tryb promiscuous w programie Wireshark, użytkownik musi posiadać przewodową kartę sieciową obsługującą ten tryb. Następnie należy skonfigurować kartę do pracy w trybie promiscuous za pomocą odpowiednich narzędzi lub sterowników. Gdy karta działa w trybie promiscuous, Wireshark może przechwytywać i analizować ruch w sieci przewodowej. Po przełączeniu karty w tryb promiscuous, Wireshark może przechwytywać i analizować ruch w sieci przewodowej. Włączenie trybu monitorowania może zależeć od systemu operacyjnego i karty

sieciowej, ale zazwyczaj wymaga wykonania określonych czynności konfiguracyjnych. Na przykład niektóre platformy, takie jak FreeBSD, umożliwiają przechwytywanie wszystkich typów ruchu 802.11 bez przełączania karty w tryb monitorowania poprzez wybranie typu nagłówka warstwy łącza 802.11 podczas przechwytywania. Jednak ta metoda może nie uwzględniać zarówno ruchu przychodzącego, jak i wychodzącego. Na innych platformach, takich jak Windows, tryb monitorowania włącza się poprzez pobranie i zainstalowanie specjalnych sterowników karty sieciowej, co pozwala karcie przechwytywać wszystkie rodzaje ruchu sieciowego.

Konfiguracja przechwytywania WLAN

Aby przechwycić pakiety WLAN, potrzebujesz:

Komputer i karta sieciowa: Aby przechwycić pakiety WLAN, potrzebujesz komputera lub urządzenia z kartą sieciową obsługującą tryb monitorowania. Tryb ten umożliwia karcie odbieranie wszystkich pakietów przesyłanych bezprzewodowo, a nie tylko tych przeznaczonych dla urządzenia.

Narzędzie do podsłuchiwania pakietów: Po uzyskaniu komputera i karty sieciowej umożliwiającej przechwytywanie pakietów, będziesz potrzebować narzędzia do podsłuchiwania pakietów, takiego jak Wireshark, które umożliwi Ci ich wyświetlanie i analizę. Narzędzie to zapewnia graficzny interfejs użytkownika do przeglądania i analizowania pakietów w czasie rzeczywistym, a także umożliwia zapisywanie przechwyconych pakietów do analizy offline.

Punkt dostępu bezprzewodowego: Aby przechwycić pakiety WLAN, potrzebujesz sieci bezprzewodowej, z której będziesz mógł przechwytywać pakiety. Może to być istniejąca sieć, do której masz dostęp, lub możesz skonfigurować własną sieć za pomocą punktu dostępu bezprzewodowego lub routera. Podczas konfigurowania własnej sieci możesz skonfigurować ustawienia sieciowe zgodnie z własnymi specyfikacjami i upewnić się, że przechwytujesz interesujące Cię pakiety.

Po zainstalowaniu tych komponentów możesz przełączyć kartę sieciową w tryb monitorowania i uruchomić narzędzie do podsłuchiwania pakietów. Zobaczysz wówczas surowe dane przesyłane przez sieć WLAN, w tym informacje takie jak adresy MAC, adresy IP i dane użyteczne. Dzięki tym informacjom możesz analizować ruch sieciowy, rozwiązywać problemy z siecią i poprawiać bezpieczeństwo sieci.

Włączanie trybu monitorowania w systemie Linux

Aby włączyć tryb monitorowania interfejsu bezprzewodowego w systemie Linux, można użyć polecenia iw połączeniu z poleceniem ip. Oto ogólna procedura:

1. Sprawdź nazwę interfejsu bezprzewodowego:

sudo iw dev

Spowoduje to wyświetlenie listy wszystkich dostępnych interfejsów bezprzewodowych.

2. Przełącz interfejs w tryb monitorowania:

Zastąp wlan0 nazwą interfejsu bezprzewodowego uzyskaną w kroku 1.

sudo ip link set wlan0 down

sudo iw wlan0 set monitor control

sudo ip link set wlan0 up

3. Sprawdź, czy interfejs został pomyślnie przełączony w tryb monitorowania:

sudo iw dev

Alternatywnie, jeśli chcesz użyć polecenia iwconfig, proces jest podobny:

1. Sprawdź nazwę interfejsu bezprzewodowego:

iwconfig

2. Przełącz interfejs bezprzewodowy w tryb monitorowania, wprowadzając następujące polecenia:

sudo ifconfig wlan0 down

sudo iwconfig wlan0 mode monitor

sudo ifconfig wlan0 up

Zastąp wlan0 nazwą interfejsu bezprzewodowego

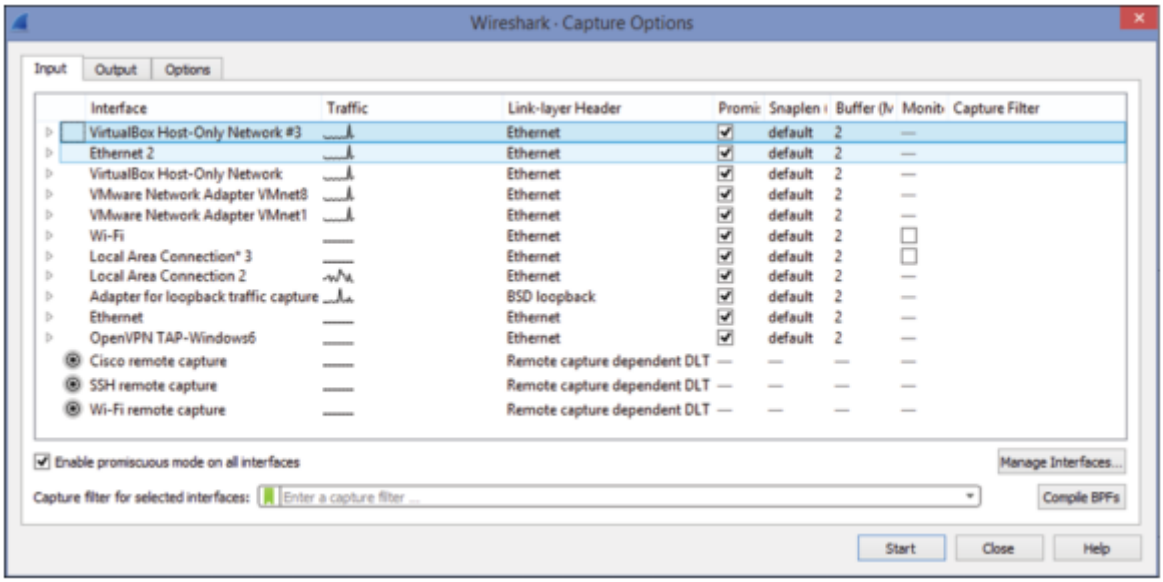
uzyskaną w kroku 1.

3. Sprawdź, czy interfejs bezprzewodowy jest w trybie monitorowania, używając następującego polecenia:

iwconfig

Włączanie trybu monitorowania w systemie Windows

Po uruchomieniu programu Wireshark w oknie dialogowym interfejsu przechwytywania kart Wi-Fi pojawi się pole wyboru „Tryb monitorowania”, jak pokazano na rysunku 6.



Można je otworzyć z menu głównego, wybierając Przechwytywanie | Opcje lub naciskając Ctrl+K. Niestety, nawet po prawidłowym zainstalowaniu programu npcap, kliknięcie go nie działa, ponieważ znacznik wyboru znika po chwili. Wykonaj poniższe kroki, aby włączyć tryb monitorowania interfejsu bezprzewodowego w systemie Windows za pomocą narzędzia „wlanhelper”, które jest częścią instalacji npcap:

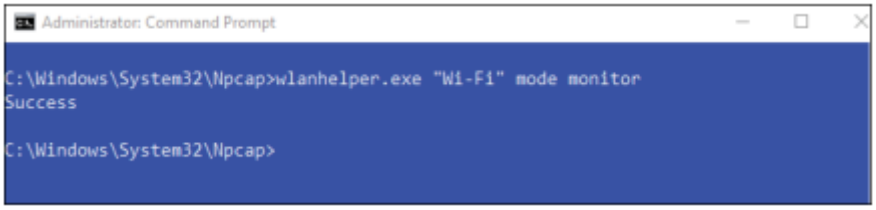
1. Otwórz wiersz poleceń jako administrator i przejdź do katalogu C:\Windows\System32\npcap.

2. Możesz użyć narzędzia wlanhelper.exe, aby sprawdzić, w jakim trybie działa Twoja karta Wi-Fi. Domyślnie powinna być w trybie „Zarządzany”, co oznacza, że jest gotowa do normalnego połączenia Wi-Fi.

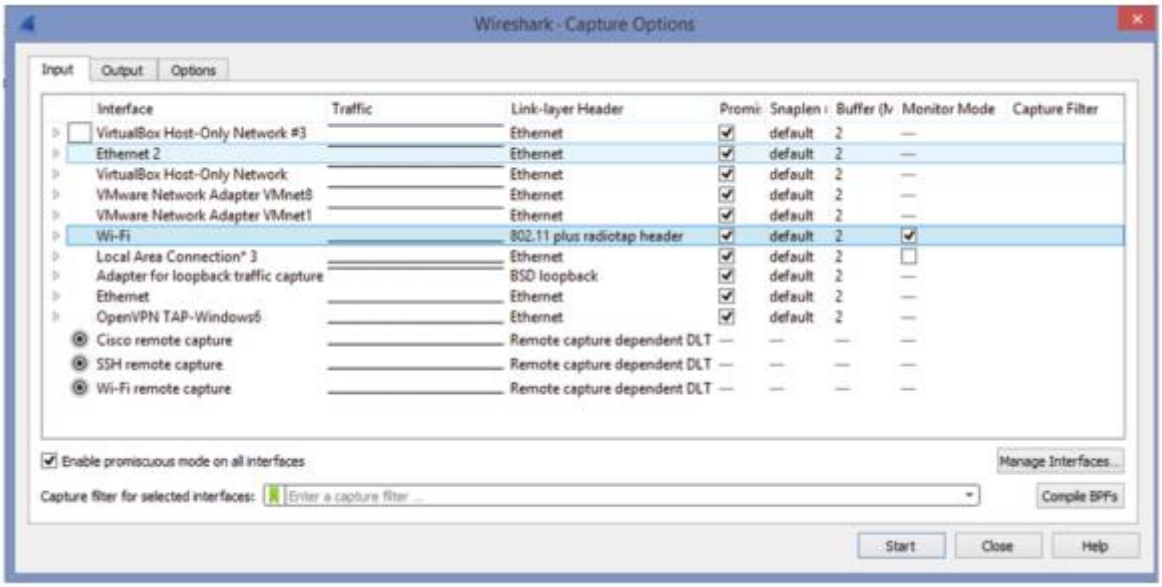
3. Aby przełączyć ją w tryb monitorowania, użyj następującego polecenia:

wlanhelper.exe "Wi-Fi" mode monitor

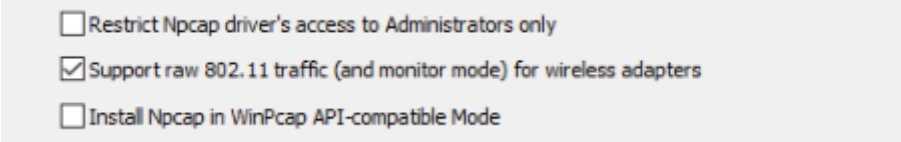
Zastąp „Wi-Fi” nazwą swojej karty sieciowej. Patrz Rysunek 7:



4. Po przełączeniu karty w tryb monitorowania możesz ponownie uruchomić program Wireshark i „włączyć” tryb monitorowania w oknie dialogowym interfejsu przechwytywania, jak pokazano na rysunku 8:



Uwaga: Jeśli nie możesz włączyć trybu monitorowania w programie Wireshark, jednym z rozwiązań jest odinstalowanie zarówno programu Wireshark, jak i Npcap z komputera z systemem Windows, a następnie ponowna instalacja programu Wireshark. Upewnij się, że opcja „Obsługa surowego ruchu 802.11 (i trybu monitorowania) dla kart sieciowych” jest zaznaczona podczas instalacji, jak pokazano na rysunku 9. Dzięki temu instalacja będzie zawierać niezbędne komponenty do obsługi trybu monitorowania.

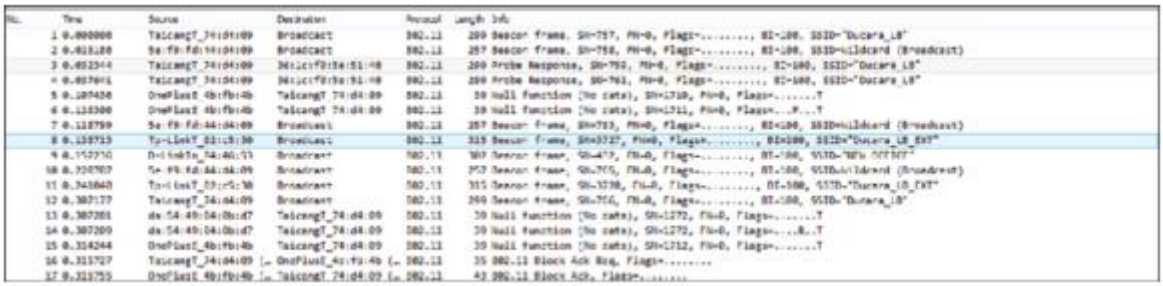


Ponadto ważne jest, aby upewnić się, że karta sieciowa obsługuje tryb monitorowania, ponieważ nie wszystkie karty obsługują ten tryb. Jeśli karta obsługuje tryb monitorowania, może być konieczna

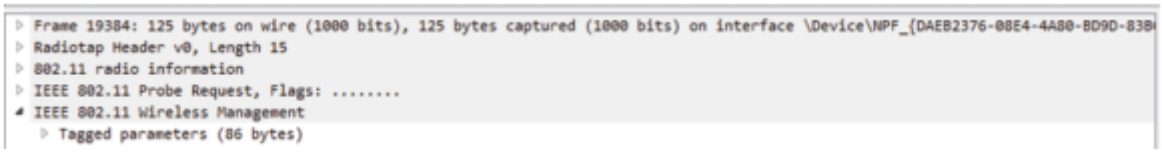
aktualizacja jej sterowników do najnowszej wersji. Jeśli nadal nie możesz włączyć trybu monitorowania, spróbuj użyć innej karty lub skontaktuj się z producentem, aby uzyskać informacje o znanych problemach lub zgodności.

Sniffing ruchu sieciowego WLAN

Po włączeniu trybu monitorowania na karcie sieciowej w systemie Windows lub Linux możesz rozpocząć sniffing ruchu sieciowego WLAN. Poczekaj, aż pakiety zaczną pojawiać się na liście pakietów Wireshark, jak pokazano na rysunku 10. Następnie możesz rozpocząć analizę ruchu sieciowego.



Podczas podsłuchiwania ruchu sieciowego WLAN w trybie monitorowania, w panelu szczegółów pakietu programu Wireshark wyświetlane są różne informacje, patrz Rysunek 11.



Sekcja protokołu zazwyczaj wyświetla protokół 802.11, standard IEEE dla komunikacji bezprzewodowej WLAN. Ta sekcjapokazuje typ przesyłanej ramki, taki jak ramka nawigacyjna, ramka żądania sondy lub ramka odpowiedzi sondy. Zawiera ona informacje o adresach MAC nadawcy i odbiorcy, a także wszelkie dodatkowe informacje zawarte w ramce.

W sekcji „Informacje” ramki można zobaczyć informacje takie jak „Beacon”, „Żądanie sondy” lub „Odpowiedź sondy”. Odnoszą się one do typów przesyłanych ramek zarządzania i mogą zawierać informacje o sieci bezprzewodowej, takie jak identyfikator SSID sieci, kanał i ustawienia zabezpieczeń. Można również zobaczyć „Nagłówek Radiotap”, który zawiera informacje o warstwie radiowej komunikacji WLAN. Nagłówek ten zawiera informacje takie jak częstotliwość kanału, siła sygnału i szybkość transmisji danych, które mogą być przydatne do zrozumienia wydajności i charakterystyki sieci bezprzewodowej.

Gdy karta sieci bezprzewodowej znajduje się w trybie monitorowania, jest ustawiona na „tryb tylko odbioru”, co oznacza, że może jedynie odbierać pakiety i nie może wysyłać żadnych żądań do internetu. Pozwala to na przechwytywanie wszystkich pakietów bezprzewodowych przesyłanych w zasięgu karty. Jeśli chcesz nadal korzystać z internetu podczas podsłuchiwania ruchu sieciowego WLAN, możesz użyć dwóch kart Wi-Fi – jednej w trybie monitorowania do przechwytywania pakietów, a drugiej w trybie zarządzania do dostępu do internetu.

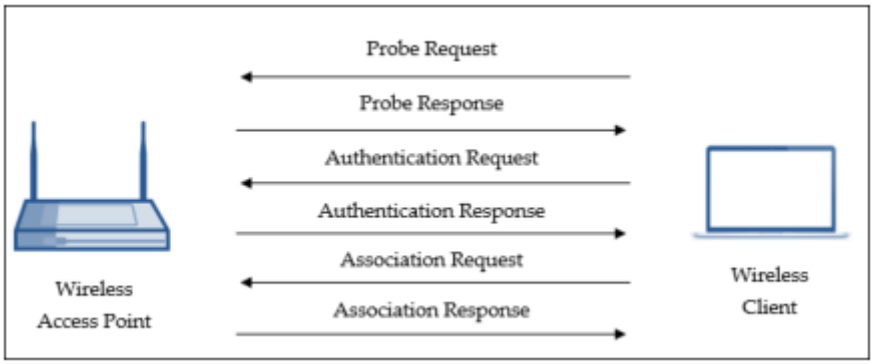
Uwaga: Należy również pamiętać, że po ponownym uruchomieniu interfejs bezprzewodowy powróci do trybu zarządzanego, dlatego konieczne będzie ponowne włączenie trybu monitorowania, aby kontynuować przechwytywanie pakietów bezprzewodowych.

Sniffer Wi-Fi: WPA/WPA2

Analiza PSK lub EAP W przypadku WPA/WPA2 z PSK lub EAP, analiza przechwytywania sniffera 802.11 może być użyta do analizy ruchu sieciowego podczas uwierzytelniania i szyfrowania. Wi-Fi Protected Access (WPA) i WPA2 to standardy bezpieczeństwa sieci bezprzewodowych. Protokoły WPA i WPA2 obsługują dwie metody uwierzytelniania: Pre-Shared Key (PSK) i Extensible Authentication Protocol (EAP). Przechwycone dane mogą posłużyć do weryfikacji prawidłowego działania procesu uwierzytelniania i szyfrowania oraz identyfikacji potencjalnych problemów bezpieczeństwa, takich jak ataki typu man-in-the-middle lub próby nieautoryzowanego dostępu. Na przykład, przechwycone dane mogą posłużyć do analizy metody szyfrowania użytej w procesie uwierzytelniania, formatu żądania i odpowiedzi uwierzytelniania oraz poprawności używanych poświadczeń. W przypadku PSK, przechwycone dane mogą posłużyć do weryfikacji, czy do połączenia używany jest prawidłowy klucz PSK. W przypadku EAP, przechwycone dane mogą posłużyć do weryfikacji autentyczności serwera uwierzytelniania i poprawności używanych poświadczeń. Analizując dane przechwycone przez sniffer, można uzyskać wgląd w proces uwierzytelniania klienta 802.11 i obserwować kroki nawiązywania bezpiecznego połączenia między urządzeniem klienckim a bezprzewodowym punktem dostępu. Może to być przydatne w diagnozowaniu problemów z procesem uwierzytelniania lub weryfikowaniu, czy proces uwierzytelniania przebiega zgodnie z oczekiwaniami.

Proces uwierzytelniania klienta 802.11

Proces uwierzytelniania klienta 802.11 to kluczowy krok w nawiązywaniu bezpiecznego połączenia między urządzeniem klienckim a punktem dostępu bezprzewodowego. Proces ten obejmuje kilka kroków, które zapewniają kompatybilność urządzenia klienckiego i punktu dostępu oraz autoryzację klienta do dostępu do sieci. Patrz rysunek 12:



Oto szczegółowe wyjaśnienie procesu uwierzytelniania klienta 802.11:

1. Ramki nawigacyjne: Punkty dostępowe stale wysyłają ramki nawigacyjne, które ogłaszają ich obecność oraz identyfikator SSID sieci bezprzewodowej, przepustowość i inne informacje. Ramki te są odbierane przez pobliskie urządzenia klienckie, które wyszukują dostępne sieci.

2. Ramki żądania sondy: Oprócz informacji zawartych w ramce nawigacyjnej, klienci bezprzewodowi używają również innych ramek zarządzania, takich jak ramki żądania sondy i ramki odpowiedzi sondy, aby zebrać więcej informacji o sieci przed nawiązaniem połączenia. Urządzenie klienckie rozgłasza ramki żądania sondy na każdym kanale, ogłaszając obsługiwane przez siebie przepustowości i możliwości standardu 802.11, takie jak 802.11n. Ramki żądania sondy są rozgłaszane do wszystkich punktów dostępowych w zasięgu.

3. Ramki odpowiedzi sondy: Punkty dostępowe w zasięgu odpowiadają ramkami odpowiedzi sondy, które dostarczają informacji o sieci bezprzewodowej, w tym identyfikator SSID, przepustowość, typy szyfrowania (jeśli są wymagane) i inne możliwości standardu 802.11 punktu dostępowego.

4. Żądanie uwierzytelnienia: Na podstawie informacji otrzymanych z ramek odpowiedzi sondy, urządzenie klienckie decyduje, który punkt dostępowy jest najlepszy dla dostępu i wysyła do niego żądanie uwierzytelnienia. Jeśli punkt dostępowy zaakceptuje żądanie uwierzytelnienia, klient i punkt dostępowy rozpoczynają proces asocjacji, podczas którego klient nawiązuje połączenie z punktem dostępowym i może rozpocząć komunikację w sieci.

5. Odpowiedź uwierzytelnienia: Punkt dostępowy wysyła odpowiedź uwierzytelnienia, zapraszając klienta do uwierzytelnienia się w SSID. Odpowiedź ta zawiera informacje o metodach zabezpieczeń używanych przez sieć, takich jak WPA lub WPA2 z kluczem PSK lub EAP.

6. Żądanie asocjacji: Po pomyślnym uwierzytelnieniu klient wysyła ramkę żądania asocjacji do punktu dostępowego. Żądanie asocjacji zawiera informacje o ustawieniach sieciowych urządzenia klienckiego, takich jak obsługiwane prędkości transmisji danych i możliwości standardu 802.11.

7. Odpowiedź asocjacji: Punkt dostępowy odpowiada odpowiedzią asocjacji, przyznając klientowi dostęp do sieci. Odpowiedź asocjacji zawiera komunikat o powodzeniu, wskazujący, że urządzenie klienckie uzyskało autoryzację do dostępu do sieci.

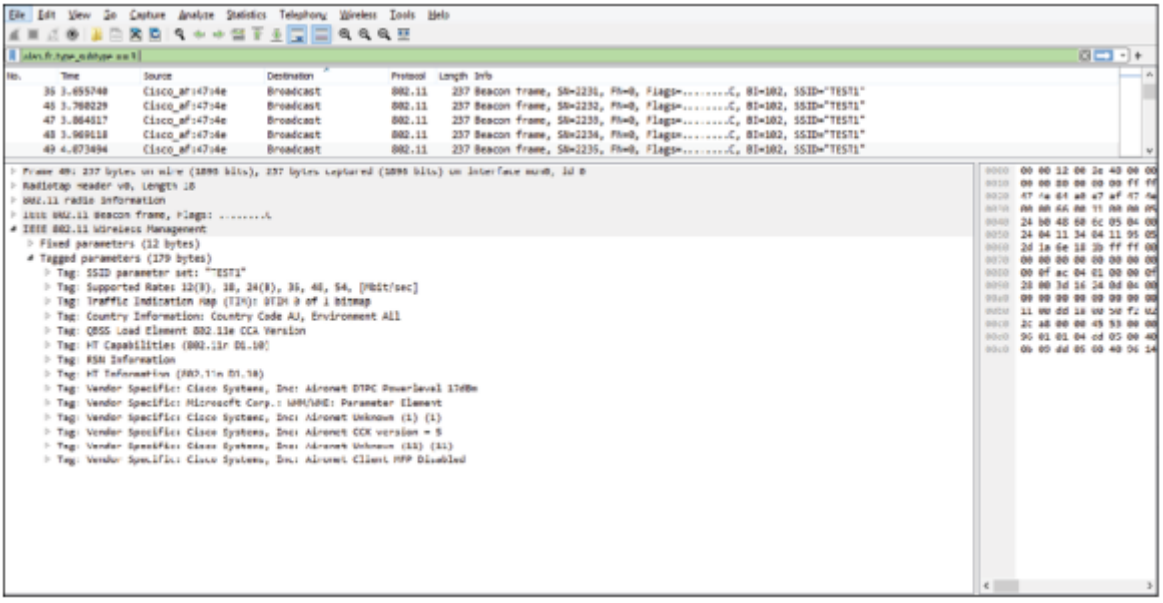
8. Dostęp do sieci: Urządzenie klienckie może teraz komunikować się z punktem dostępowym i przesyłać ruch przez sieć bezprzewodową.

Uwaga: Należy pamiętać, że proces uwierzytelniania klienta 802.11 może się różnić w zależności od konkretnej implementacji i zastosowanych środków bezpieczeństwa. Na przykład, w przypadku WPA i WPA2, proces uwierzytelniania może obejmować użycie serwera uwierzytelniającego, takiego jak serwer RADIUS, lub użycie klucza PSK.

Jak omówiono w sekcji poświęconej strukturze pakietów 802.11, w komunikacji warstwy MAC 802.11, która odbywa się drogą radiową w celu zarządzania i regulacji sieci bezprzewodowej, używane są trzy typy ramek (zarządzania, sterowania i danych). W kolejnych sekcjach przyjrzymy się tym ramkom, wykorzystując wspomnianą powyżej funkcję przechwytywania pakietów.

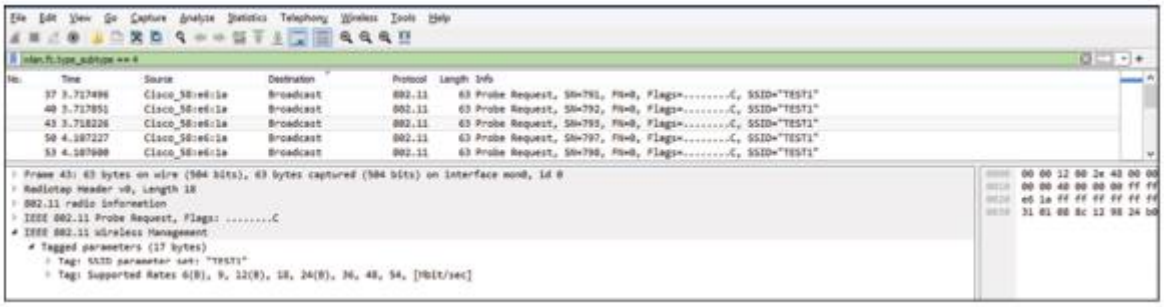
Poniżej przedstawiono przykład procesu uwierzytelniania klienta, który pochodzi z poprzedniego przechwycenia pakietów.

1. Ramka Beacon to ramka zarządzania w protokole sieci bezprzewodowej 802.11. Jest ona regularnie przesyłana przez punkt dostępowy w celu ogłoszenia swojej obecności i dostarczenia informacji o sieci pobliskim klientom bezprzewodowym. Ramka Beacon zawiera informacje takie jak nazwa sieci (SSID), obsługiwane szybkości transmisji danych, metody zabezpieczeń sieci (takie jak WEP, WPA lub WPA2), numer kanału oraz identyfikator BSSID punktu dostępowego. Aby filtrować ramki Beacon w programie Wireshark, należy użyć wyrażenia filtrującego wlan.fc.type_subtype==8. Spowoduje to wyświetlenie tylko ramek Beacon w przechwyconych pakietach, jak pokazano na rysunku 13:

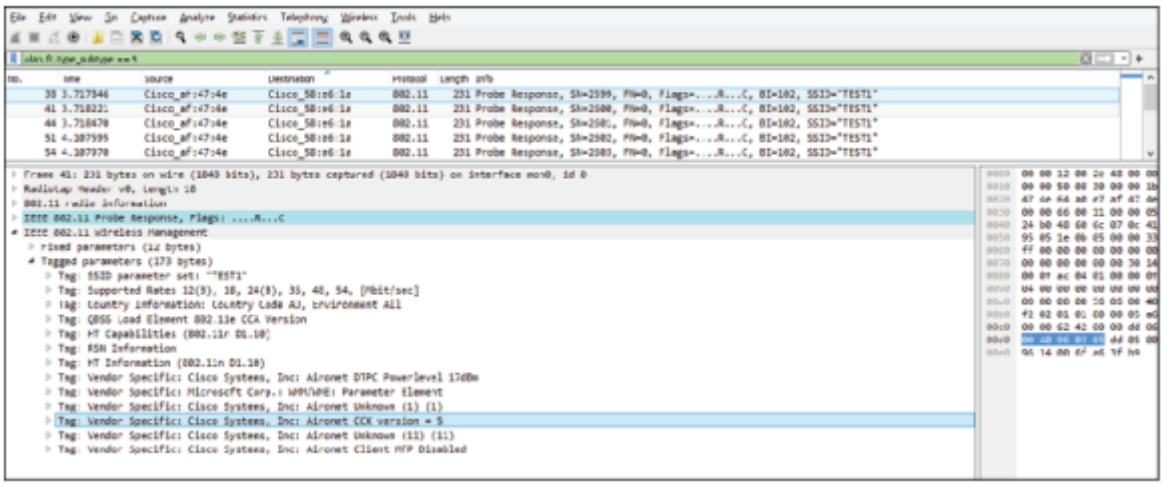


2. STA (stacja) wysyła żądanie sondy do AP w celu uzyskania informacji (punktu dostępowego). Aby filtrować ramki żądania sondy w Wireshark, należy użyć wyrażenia filtrującego wlan.fc.type_subtype==4.

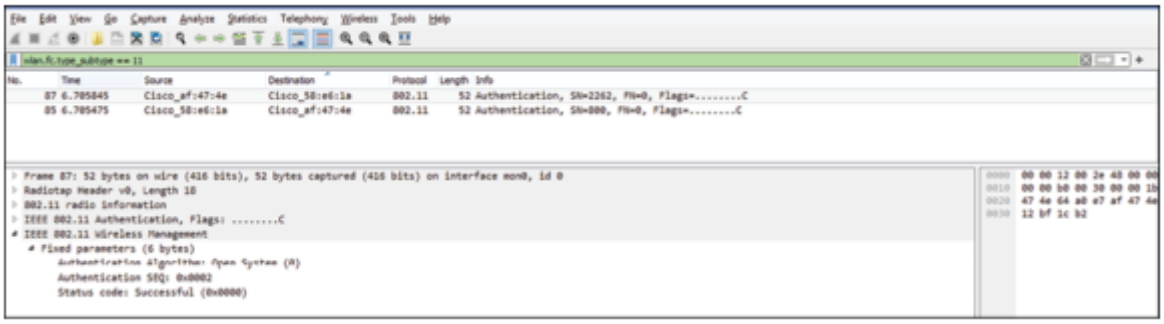
Spowoduje to wyświetlenie tylko ramek żądania sondy w przechwyconych pakietach, jak pokazano na rysunku 14:



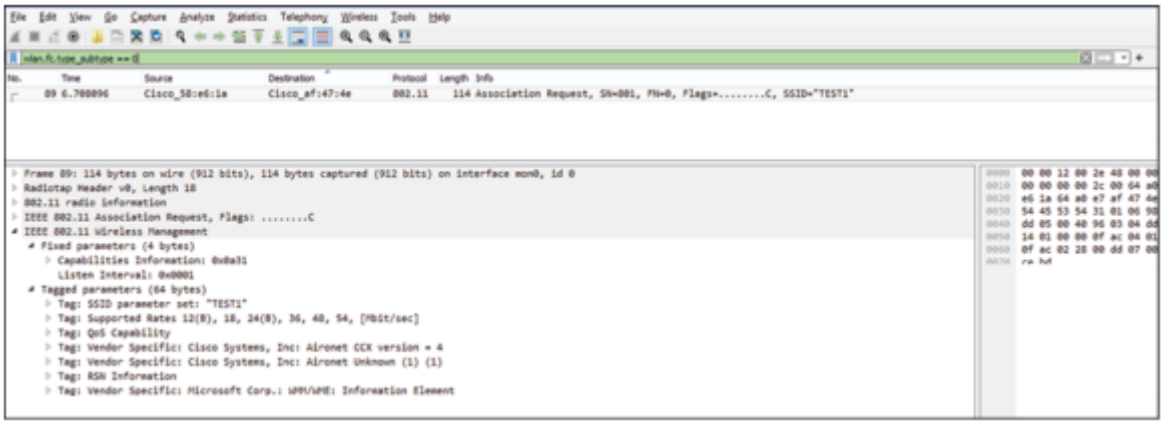
3. Gdy punkt dostępowy odbierze ramkę żądania sondy, odpowiada ramką odpowiedzi sondy. Odpowiedź sondy zawiera informacje o punkcie dostępowym, takie jak jego identyfikator SSID, obsługiwane szybkości transmisji danych i ustawienia zabezpieczeń. Aby filtrować ramki odpowiedzi sondy w programie Wireshark, należy użyć wyrażenia filtrującego wlan.fc.type_subtype==5. Spowoduje to wyświetlenie w przechwyconych pakietach tylko ramek odpowiedzi sondy. Patrz rysunek 15:



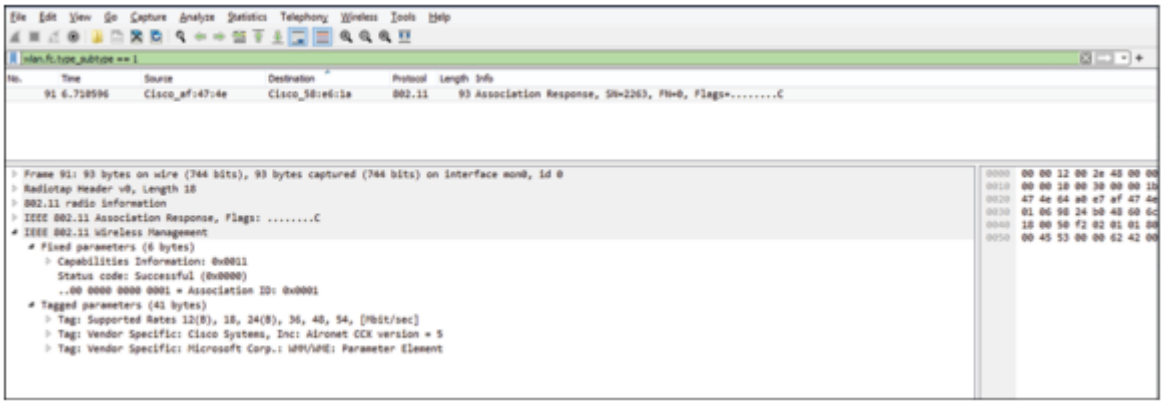
4. Uwierzytelnianie 802.11 to proces, w którym punkt dostępowy akceptuje lub odrzuca identyfikację radiowej karty sieciowej. Karta sieciowa rozpoczyna procedurę, dostarczając do punktu dostępowego ramkę uwierzytelniającą zawierającą jej identyfikację. Radiowa karta sieciowa wysyła tylko jedną ramkę uwierzytelniającą z uwierzytelnianiem w systemie otwartym (domyślnie), a punkt dostępowy odpowiada ramką uwierzytelniającą jako odpowiedzią potwierdzającą akceptację (lub odrzucenie). Aby filtrować ramki uwierzytelniające w programie Wireshark, należy użyć wyrażenia filtrującego wlan.fc.type_subtype==11. Spowoduje to wyświetlenie tylko ramek uwierzytelniających w przechwyconych pakietach. Patrz Rysunek 16:



5. Powiązanie punktu dostępowego 802.11 umożliwia mu przypisywanie zasobów do radiowej karty sieciowej i synchronizację z nią. Procedura powiązania jest inicjowana przez kartę sieciową wysyłającą żądanie powiązania do punktu dostępowego. Żądanie powiązania zawiera informacje o kliencie, takie jak jego przepustowość i identyfikator SSID sieci, z którą chce się połączyć. Aby filtrować ramki żądania powiązania w programie Wireshark, należy użyć wyrażenia filtrującego wlan.fc.type_subtype==0. Spowoduje to wyświetlenie w przechwytywaniu pakietów tylko ramek żądania powiązania. Patrz Rysunek 17:



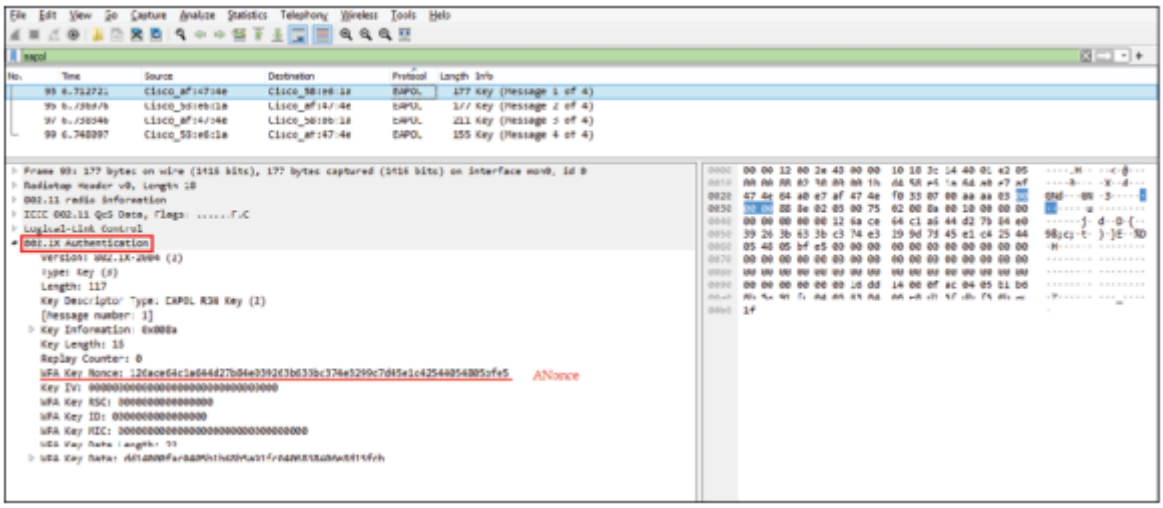
6. Gdy punkt dostępowy odbierze ramkę żądania skojarzenia, wysyła ramkę odpowiedzi skojarzenia, aby potwierdzić lub odrzucić skojarzenie. Ramka odpowiedzi skojarzenia zawiera informacje o punkcie dostępowym, takie jak obsługiwane szybkości transmisji danych i identyfikator skojarzenia. Aby filtrować ramki odpowiedzi skojarzenia w programie Wireshark, należy użyć wyrażenia filtrującego wlan.fc.type_subtype==1. Spowoduje to wyświetlenie w przechwyconych pakietach tylko ramek odpowiedzi skojarzenia. Patrz Rysunek 18:



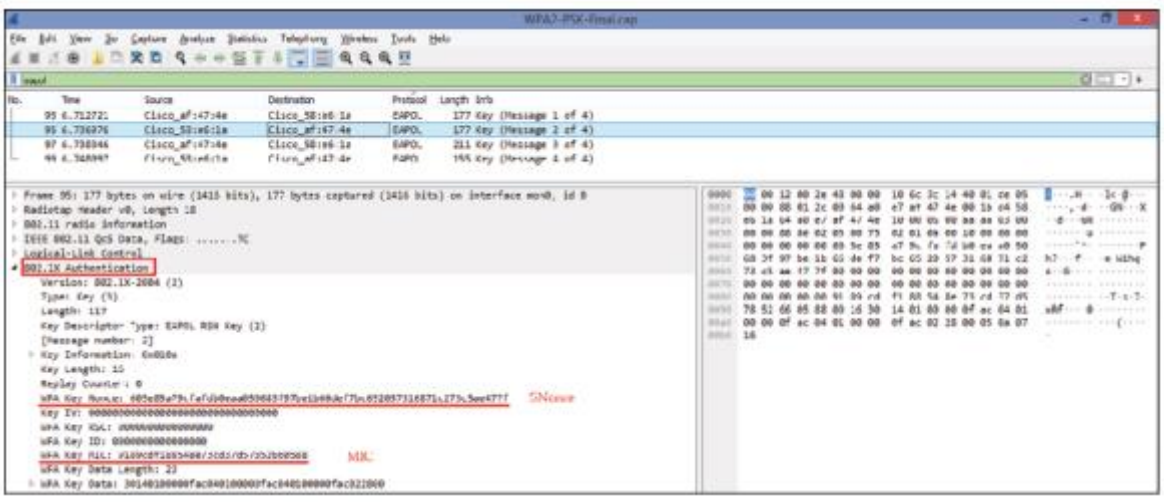
Czteroetapowe uzgadnianie jest używane zarówno w identyfikatorach SSID skonfigurowanych w PSK (WPA-Personal), jak i 802.1x (WPA2-Enterprise), aby nawiązać bezpieczne połączenie między punktem dostępowym a klientem bezprzewodowym. Jest to proces wymiany czterech pakietów, który generuje klucze szyfrujące używane do szyfrowania danych w medium bezprzewodowym. Proces wymiany kluczy następuje po uwierzytelnieniu klienta bezprzewodowego i powiązaniu go z punktem dostępowym. Po zakończeniu wymiany kluczy ramki sterujące służą do bezpiecznego przesyłania danych w sieci bezprzewodowej. Ramki sterujące wykorzystują klucze szyfrujące wygenerowane podczas czteroetapowego uzgadniania, aby zapewnić poufność i ochronę integralności ruchu w sieci bezprzewodowej. Podczas czteroetapowego uzgadniania, punkt dostępowy i stacja bazowa wymieniają ramki uwierzytelniające zawierające wartości jednorazowe (nonces) i wykorzystują PSK jako klucz główny parowy (PMK) do generowania klucza przejściowego parowego (PTK), który następnie jest używany do szyfrowania danych między punktem dostępowym a stacją bazową (STA). Punkt dostępowy wysyła również klucz grupowy (GTK) z numerem sekwencyjnym do wykorzystania w przyszłości w ramkach rozgłoszeniowych/multicastowych. Po potwierdzeniu odbioru GTK przez STA, dane są wysyłane w postaci zaszyfrowanej za pomocą klucza PTK.

Oto opis krok po kroku 4-etapowego uzgadniania:

1. Punkt dostępowy wysyła ramkę uwierzytelniania 802.1x z ANonce (Authenticator Nonce): ANonce (AP Nonce) to losowa wartość generowana przez punkt dostępowy lub uwierzytelniacz. Jest to 32-bajtowa (256-bitowa) liczba losowa używana w procesie uzgadniania 4-etapowego. Punkt dostępowy wysyła ramkę EAPOL-Start, aby zainicjować proces uwierzytelniania. STA odpowiada ramką EAPOL-Identity zawierającą jego tożsamość. Następnie punkt dostępowy wysyła ramkę EAPOL-Challenge zawierającą losowo wygenerowany ANonce do punktu dostępowego, jak pokazano na rysunku 19. W polu filtru wpisz „eapol". Spowoduje to odfiltrowanie przechwyconych ramek i wyświetlenie tylko tych, które zawierają pakiety EAPOL.

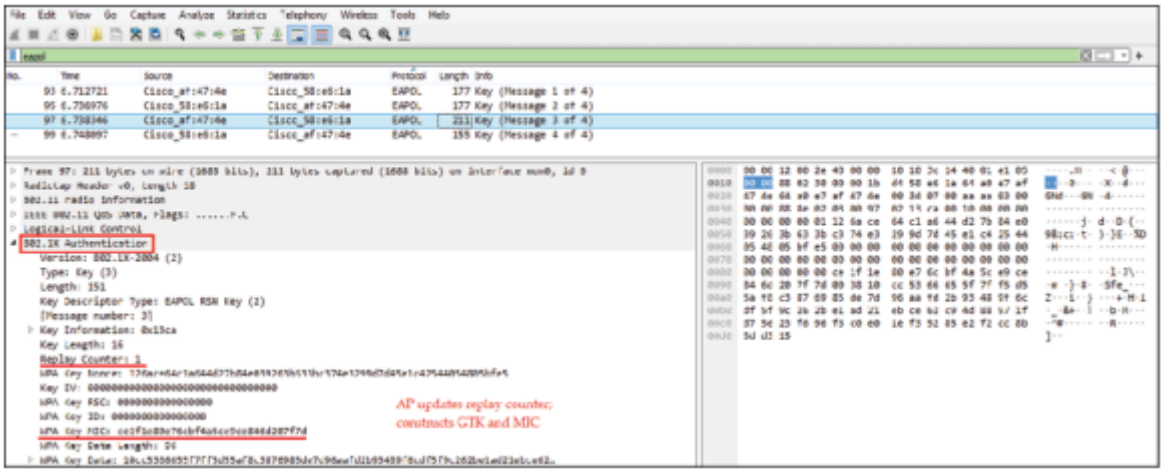


2. STA odpowiada ramką uwierzytelniania 802.1x z identyfikatorem suplikanta (SNonce) i kodem MIC: SNonce to losowa wartość generowana przez suplikanta (klienta). Podobnie jak ANonce, jest to 32-bajtowa (256-bitowa) liczba losowa. STA generuje swój identyfikator nonce (SNonce) i łączy go z kodem ANonce otrzymanym od punktu dostępowego, aby utworzyć klucz PMK. Następnie STA wysyła ramkę odpowiedzi EAPOL zawierającą identyfikator SNonce i kod integralności wiadomości (MIC) generowany za pomocą klucza PMK, jak pokazano na rysunku 20. W ten sposób weryfikowana jest tożsamość STA w punkcie dostępowym.

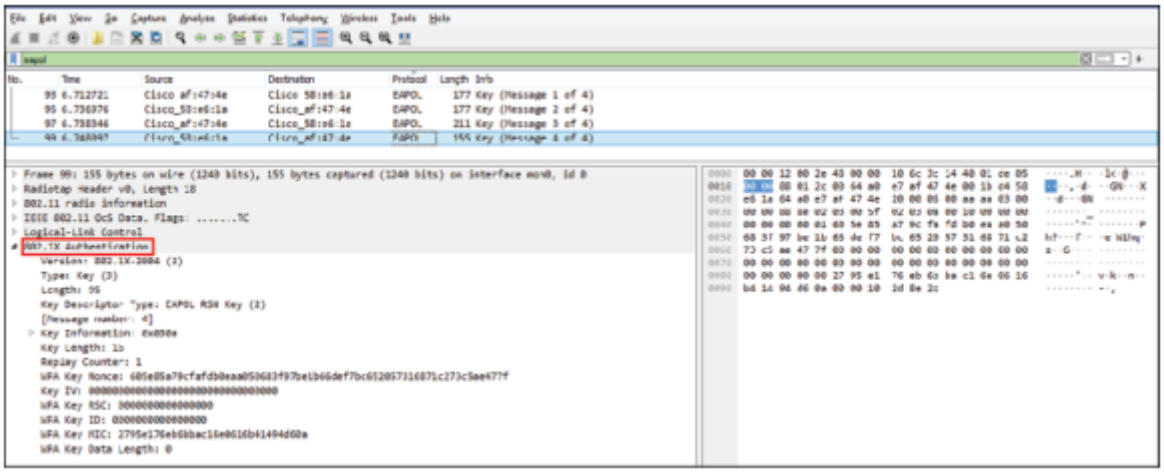


3. Punkt dostępowy konstruuje ramkę 802.1x z nowym kodem MIC i kluczem GTK z numerem sekwencyjnym: AP generuje również klucz PMK za pomocą wartości ANonce i SNonce, a następnie oblicza nowy klucz MIC w celu weryfikacji tożsamości punktu dostępowego do stacji bazowej (STA). Następnie punkt dostępowy wysyła ramkę odpowiedzi EAPOL zawierającą nowy kod MIC i klucz

czasowy grupy (GTK) wraz z numerem sekwencyjnym, patrz rysunek 21. Klucz GTK służy do szyfrowania ramek rozgłoszeniowych i multicastowych.



4. STA wysyła ACK: STA weryfikuje nowy MIC wysłany przez punkt dostępowy i wysyła ramkę odpowiedzi EAPOL z potwierdzeniem (ACK), aby potwierdzić zakończenie uzgadniania. Patrz rysunek 22:



Po zakończeniu uzgadniania 4-etapowego, punkt dostępowy (AP) i stacja bazowa (STA) otrzymują klucz PMK i mogą wyprowadzić klucz PTK, który służy do szyfrowania danych między nimi. Klucz PTK jest generowany z klucza PMK, parametru ANonce, parametru SNonce, adresów MAC punktu dostępowego i stacji bazowej (STA) oraz innych parametrów. Klucz PTK służy do szyfrowania wszystkich ramek danych wymienianych między punktem dostępowym a stacją bazową (STA).

Analiza przechwytywania sniffera 802.11: Multicast

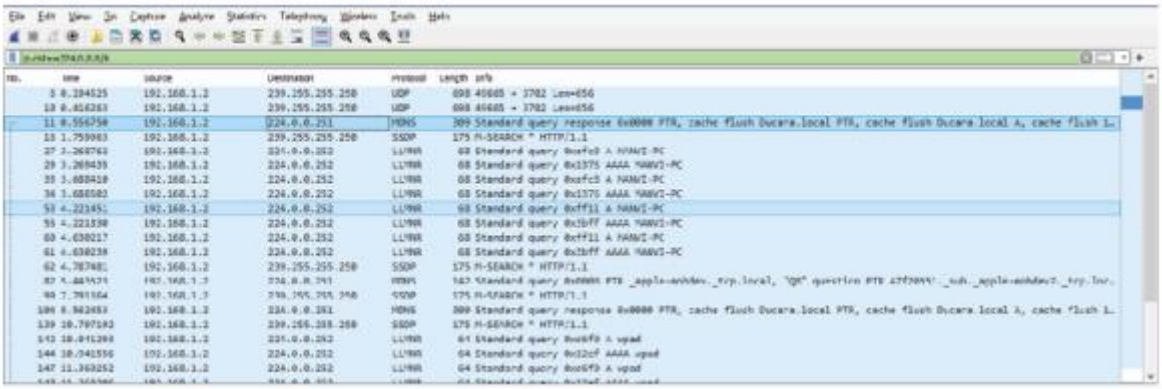
W przypadku multicastu, analiza przechwytywania sniffera 802.11 może być użyta do analizy ruchu sieciowego podczas transmisji multicast. Multicast to metoda komunikacji, która pozwala nadawcy wysłać pojedynczą wiadomość do grupy odbiorców w jednej transmisji. Jest to przeciwieństwo do unicastu, gdzie wiadomość jest wysyłana od jednego nadawcy do jednego odbiorcy, oraz rozgłoszeniowego, gdzie wiadomość jest wysyłana do wszystkich urządzeń w sieci. Przechwycone dane mogą posłużyć do weryfikacji prawidłowego działania transmisji multicast oraz identyfikacji potencjalnych problemów, takich jak przeciążenie sieci lub utracone pakiety. Na przykład, przechwycone dane mogą posłużyć do analizy formatu transmisji multicast, rozmiaru grupy multicast

oraz szybkości transmisji. Dodatkowo, analiza przechwytywania 802.11 Sniffer Capture Analysis może posłużyć do monitorowania zachowania transmisji multicast i identyfikacji wszelkich problemów z bezpieczeństwem, takich jak nieautoryzowane próby dostępu lub podsłuchy. Multicast jest szczególnie przydatny w sytuacjach, w których wielu odbiorców musi otrzymywać te same informacje, na przykład w wideokonferencjach online, grach online i aplikacjach telewizji internetowej (IPTV). Korzystając z multicast, nadawca może zmniejszyć natężenie ruchu sieciowego i uniknąć narzutu związanego z wysyłaniem oddzielnych wiadomości do każdego odbiorcy. Aby przechwycić ruch multicast, wykonaj poniższe kroki:

1. Otwórz program Wireshark i wybierz kartę sieciową podłączoną do przełącznika sieciowego. Po wybraniu odpowiedniej karty sieciowej możesz rozpocząć przechwytywanie pakietów, klikając przycisk Start w programie Wireshark.

2. Powinieneś zauważyć aktywność w sieci.

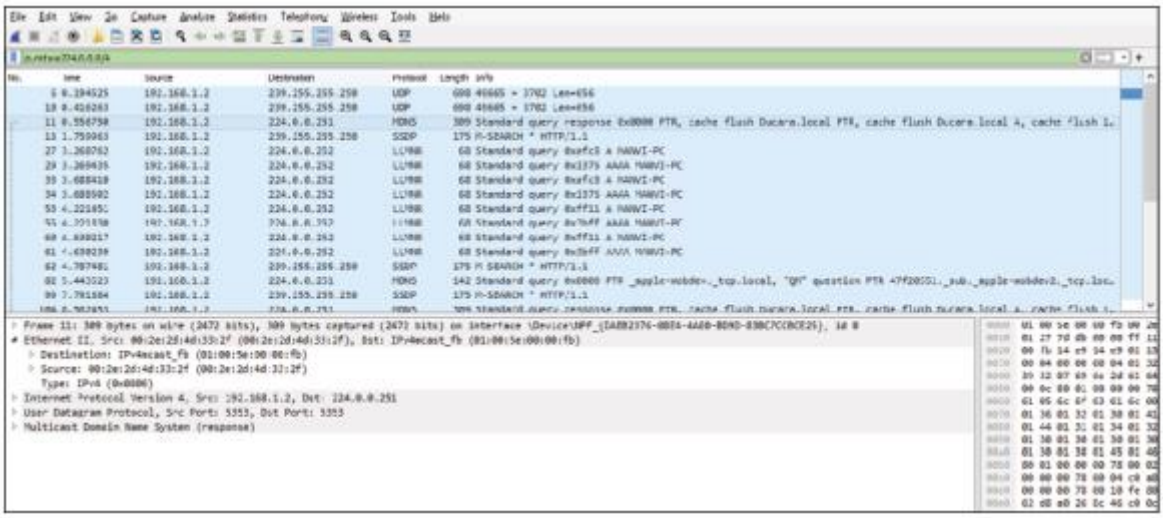
3. Przefiltruj przechwytywany ruch sieciowy, aby wyświetlać tylko pakiety multicast, jak pokazano na rysunku 4.23. Aby to zrobić, wpisz „ip.dst==224.0.0.0/4” w polu filtru programu Wireshark i naciśnij „Enter”. Ten filtr będzie wyświetlał tylko pakiety wysłane na adres multicast.



4. Obserwuj przechwycony ruch sieciowy. Po zastosowaniu filtra powinieneś zauważyć pewną aktywność sieciową w przechwyconym ruchu. Zobaczysz ramki wysłane na adres multicast.

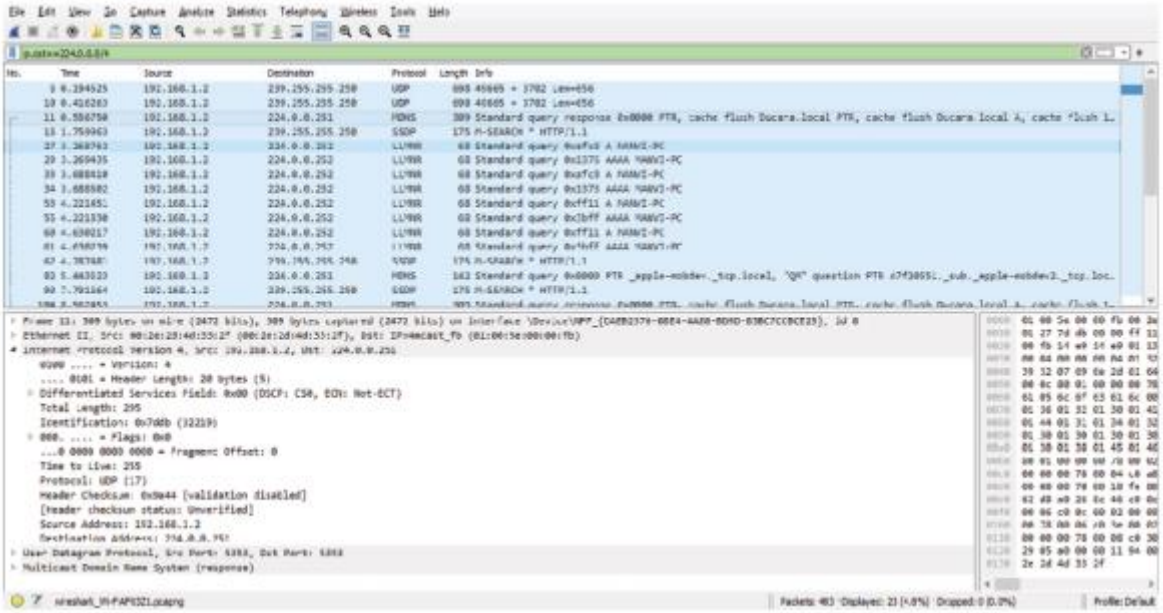
5. Wybierz pierwszą ramkę i przyjrzyj się szczegółom jej pakietu. Aby to zrobić, wystarczy kliknąć pierwszą ramkę w oknie przechwytywania. Szczegóły pakietu powinny być widoczne w środkowym panelu okna Wireshark.

6. Rozwiń szczegóły Ethernetu, aby wyświetlić ramkę Ethernetu. W panelu szczegółów pakietu powinny być widoczne szczegóły Ethernetu. Klikając strzałkę obok pola Ethernet II, możesz rozwinąć te szczegóły, aby wyświetlić więcej informacji o ramce Ethernetu, jak pokazano na rysunku 24:



7. Zwróć uwagę na adres docelowy ramki Ethernet. Adres docelowy ramki Ethernet będzie zaczynał się od „01:00:5e”, czyli adresu multicast Ethernet dla IPv4. Ten adres oznacza, że ramka została wysłana do grupy multicast.

8. Rozwiń szczegóły IPv4, aby wyświetlić pakiet IP, jak pokazano na rysunku 25.



W panelu szczegółów pakietu powinny być widoczne szczegóły IPv4. Klikając strzałkę obok pola Protokół internetowy w wersji 4, możesz rozwinąć te szczegóły, aby wyświetlić więcej informacji o pakiecie IP.

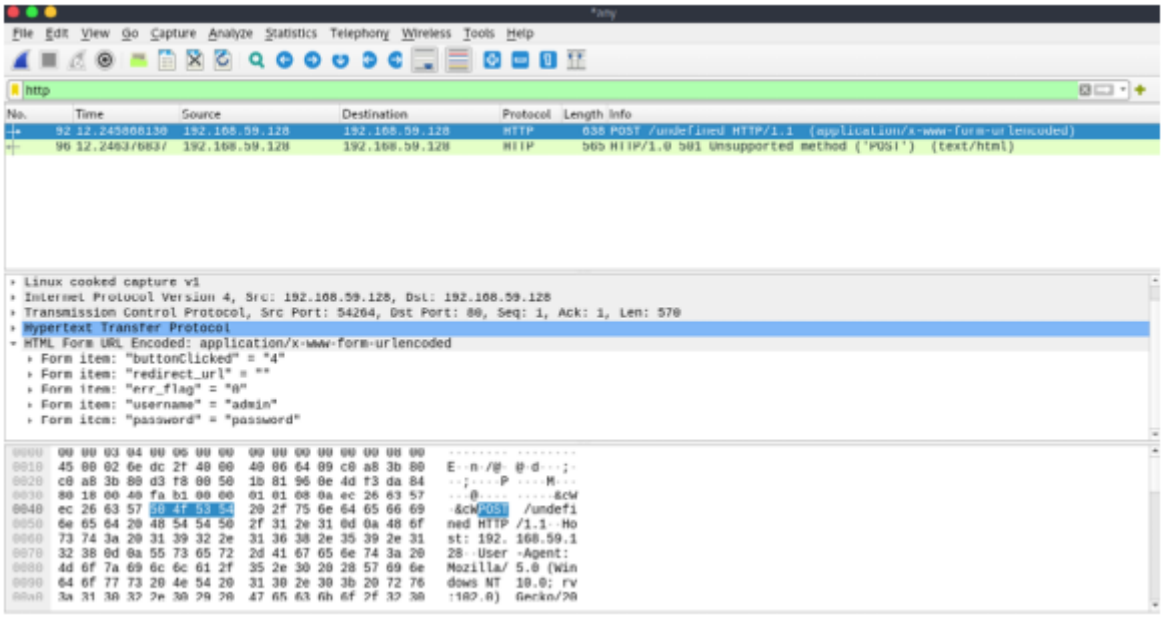
Zwróć uwagę na adres docelowy pakietu IP. Adres docelowy pakietu IP będzie mieścił się w zakresie od 224.0.0.0 do 239.255.255.255, który jest zakresem adresów multicast IPv4. Jeśli ruch to ruch SSDP lub WS-Discovery, najprawdopodobniej będzie on adresowany na adres 239.255.255.250. Wybierz dodatkowe ramki i zwróć uwagę na szczegóły dotyczące sieci Ethernet i IPv4. Wybierając dodatkowe ramki w oknie przechwytywania, możesz obserwować szczegóły dotyczące sieci Ethernet i IPv4 dla innych pakietów wysyłanych na adres multicast. Może to pomóc w lepszym zrozumieniu charakterystyki i zachowania ruchu multicast w sieci.

Analiza przechwytywania sniffera 802.11: Uwierzytelnianie sieciowe

W przypadku uwierzytelniania sieciowego, analiza przechwytywania sniffera 802.11 może służyć do analizy ruchu sieciowego podczas uwierzytelniania sieciowego, czyli procesu weryfikacji tożsamości użytkownika uzyskującego dostęp do aplikacji lub usługi sieciowej. Przechwytywanie za pomocą sniffera można wykorzystać do monitorowania wymiany informacji między urządzeniem klienckim a serwerem podczas procesu uwierzytelniania.

Przechwycone dane można analizować w celu ustalenia, czy proces uwierzytelniania działa prawidłowo i zidentyfikowania potencjalnych problemów bezpieczeństwa, takich jak ataki typu man-in-the-middle lub próby nieautoryzowanego dostępu. Przechwycone dane można na przykład wykorzystać do analizy metody szyfrowania używanej w procesie uwierzytelniania, formatu żądania i odpowiedzi uwierzytelniającej oraz ważności używanych danych uwierzytelniających. W tej sekcji wyjaśnimy uwierzytelnianie sieciowe za pomocą protokołu HTTP i sposób jego przechwytywania w programie Wireshark.

Protokół HTTP (Hypertext Transfer Protocol) jest protokołem bezstanowym i nie zapewnia żadnego mechanizmu utrzymywania stanu uwierzytelnionego użytkownika. Aby ominąć to ograniczenie, powszechnie stosowaną techniką jest użycie pliku cookie sesji do przechowywania informacji uwierzytelniających użytkownika po stronie klienta. Gdy użytkownik loguje się do aplikacji internetowej, serwer zwraca plik cookie sesji zawierający unikalny identyfikator, używany do identyfikacji użytkownika w kolejnych żądaniach. Ten plik cookie jest zazwyczaj przechowywany w pamięci przeglądarki i wysyłany do serwera w kolejnych żądaniach. Przechwytywanie danych uwierzytelniających sieciowych w programie Wireshark polega na przechwytywaniu ruchu sieciowego i jego analizie. Pierwszym krokiem jest skonfigurowanie programu Wireshark do przechwytywania ruchu sieciowego na interfejsie, którego przeglądarka używa do łączenia się z serwerem WWW. Po przechwyceniu ruchu przez Wireshark, zaloguj się do aplikacji WWW i wykonaj wszelkie czynności, które wygenerują ruch sieciowy związany z procesem uwierzytelniania. Po zakończeniu procesu uwierzytelniania zatrzymaj przechwytywanie w programie Wireshark i przefiltruj przechwycony ruch, aby wyświetlić tylko ruch HTTP, używając filtra „http” na pasku filtrów wyświetlania. W ruchu HTTP poszukaj żądań i odpowiedzi zawierających plik cookie sesji, jak pokazano na rysunku 26. Plik cookie zostanie zapisany w nagłówku „Cookie” w żądaniu HTTP, a serwer zwróci nowy plik cookie w nagłówku „Set-Cookie” w odpowiedzi HTTP.



Ponieważ protokół HTTP nie zapewnia szyfrowania danych przesyłanych między klientem a serwerem, jest on podatny na podsłuch i manipulację przez osoby niepowołane, które mają dostęp do ruchu sieciowego. Jednym z powszechnych rozwiązań tego problemu jest użycie protokołu HTTPS zamiast HTTP. Protokół HTTPS zapewnia szyfrowanie przesyłanych danych i pomaga chronić poufne informacje przed przechwyceniem i niewłaściwym wykorzystaniem. W następnym rozdziale zobaczymy, jak Wireshark może analizować ruch HTTPS, przechwytując pakiety wymieniane między klientem a serwerem podczas sesji HTTPS.

Wyzwania związane z podsłuchiwaniem sieci bezprzewodowych 802.11

Podsłuchiwanie sieci bezprzewodowych 802.11 (WLAN) nie jest tak proste, jak podsłuchiwanie sieci przewodowych, ze względu na szereg ograniczeń i wyzwań, takich jak:

Szyfrowanie: Większość nowoczesnych sieci WLAN korzysta z protokołów szyfrowania (np. WPA2/WPA3) w celu ochrony danych przed nieautoryzowanym dostępem i modyfikacją. Szyfrowanie utrudnia przechwytywanie i deszyfrowanie ruchu sieciowego bez klucza szyfrującego, który zazwyczaj jest współdzielony tylko przez autoryzowane urządzenia. Sniffery muszą albo uzyskać klucz szyfrujący, albo złamać algorytm szyfrujący, aby uzyskać dostęp do danych.

Klucze efemeryczne: Urządzenia bezprzewodowe często używają krótkotrwałych kluczy sesji do szyfrowania każdego pakietu danych, które są generowane na podstawie klucza szyfrującego i innych parametrów. Te klucze sesji często się zmieniają i nie są przesyłane bezprzewodowo. Utrudnia to deszyfrowanie ruchu, nawet jeśli sniffer przechwyci pakiety, ponieważ musi również znać klucze sesji.

Skakanie po kanałach: Sieci WLAN działają na wielu kanałach w paśmie częstotliwości, a urządzenia mogą dynamicznie przełączać kanały, aby uniknąć zakłóceń lub przeciążeń. Wymaga to od snifferów ciągłego przeskakiwania między kanałami w celu przechwycenia całego ruchu w sieci WLAN, co może skutkować utratą danych lub niekompletnymi pakietami.

Ukryte identyfikatory SSID: Niektóre punkty dostępowe ukrywają swój identyfikator SSID, czyli nazwę sieci WLAN, aby uniemożliwić nieautoryzowanym urządzeniom dołączenie do sieci. Ukryte identyfikatory SSID utrudniają wykrywanie i łączenie się z sieciami WLAN, ponieważ sniffery muszą korzystać z innych metod (na przykład pasywnego skanowania lub aktywnego sondowania), aby je wykryć.

Zasięg sygnału: Ograniczenia siły i zasięgu sygnału mogą utrudniać przechwytywanie pakietów z dużej odległości, wymagając fizycznej bliskości źródła. Sniffery muszą mieć silne i stabilne połączenie bezprzewodowe, aby niezawodnie przechwytywać pakiety, co może być niemożliwe w niektórych środowiskach lub scenariuszach.

Utrata pakietów: Sieci bezprzewodowe są podatne na utratę pakietów z powodu różnych czynników, takich jak zakłócenia, szumy, kolizje lub niska jakość sygnału. Utrata pakietów utrudnia przechwytywanie całego ruchu w sieci WLAN, szczególnie w obszarach o dużej gęstości, gdzie wiele urządzeń konkuruje o ten sam kanał.

Szum i zakłócenia: Zakłócenia pochodzące z innych urządzeń elektronicznych lub źródeł mogą wpływać na jakość przechwytywanych danych, powodując zniekształcenia, uszkodzenia lub błędy w pakietach. Sniffery muszą odfiltrować szum i zakłócenia z odpowiednich danych, co w niektórych przypadkach może być trudne lub wręcz niemożliwe.

Aspekty prawne i etyczne: Podsłuchiwanie sieci bezprzewodowych bez odpowiedniego upoważnienia może naruszać prywatność i przepisy prawne, ponieważ może ujawnić poufne lub osobiste informacje

innych użytkowników lub urządzeń. Sniffery muszą przestrzegać zasad etycznych i uzyskać zgodę właścicieli lub administratorów sieci przed przechwyceniem jakichkolwiek danych.

Złożoność protokołów: Przechwytywanie, analizowanie i deszyfrowanie ruchu bezprzewodowego 802.11 może być skomplikowane i wymagać dogłębnej znajomości protokołów i standardów bezprzewodowych. Sniffery muszą rozumieć strukturę, format i znaczenie każdego pakietu i jego pól, a także mechanizmy szyfrowania i uwierzytelniania używane przez sieć WLAN.

Urządzenia podejrzane: Obecność urządzeń podejrzane lub nieautoryzowane może dodatkowo komplikować monitorowanie, ponieważ mogą one zakłócać normalne działanie sieci WLAN lub stanowić zagrożenie dla bezpieczeństwa. Sniffery muszą identyfikować i izolować urządzenia podejrzane od legalnych, co może być trudne lub czasochłonne.

Aby pokonać te ograniczenia i wyzwania, snifferzy muszą używać odpowiedniego sprzętu, oprogramowania i najlepszych praktyk podczas podsłuchiwania sieci bezprzewodowych 802.11. Należą do nich między innymi:

Używanie dedykowanych adapterów lub kart sieciowych obsługujących tryb monitorowania i tryb promiscuous, które pozwalają snifferom przechwytywać cały ruch w sieci WLAN, niezależnie od jego miejsca docelowego lub statusu szyfrowania.

Używanie specjalistycznych narzędzi programowych lub aplikacji, które mogą skutecznie i wydajnie przechwytywać, analizować i deszyfrować ruch bezprzewodowy, takich jak Wireshark.

Używanie anten kierunkowych lub wzmacniaczy, które mogą zwiększyć siłę i zasięg sygnału, umożliwiając snifferom przechwytywanie pakietów z większej odległości lub w obszarach o słabym sygnale.

Używanie filtrów lub masek, które mogą redukować szumy i zakłócenia z nieistotnych źródeł lub kanałów, umożliwiając snifferom skupienie się na istotnych danych.

Stosowanie etycznych technik hakerskich, które mogą uzyskać klucze szyfrujące lub sesyjne z autoryzowanych urządzeń lub punktów dostępu, takich jak ataki de-authentication lub ataki brute-force.

Postępuj zgodnie z zasadami prawnymi i etycznymi, które szanują prywatność i prawa innych użytkowników lub urządzeń w sieci WLAN. Na przykład uzyskaj zgodę właścicieli lub administratorów sieci przed przechwyceniem jakichkolwiek danych.

Podsłuchiwanie sieci bezprzewodowych 802.11 (WLAN) może być użyteczną i skuteczną techniką analizy sieci i rozwiązywania problemów, ale wiąże się również z szeregiem ograniczeń i wyzwań, które należy wziąć pod uwagę i rozwiązać. Dzięki zastosowaniu odpowiedniego sprzętu, oprogramowania i najlepszych praktyk, sniffery mogą pokonać te przeszkody oraz skutecznie i wydajnie przechwytywać i analizować ruch bezprzewodowy.

Wnioski

Omówiliśmy, jak podsłuchiwać sieci bezprzewodowe 802.11 (WLAN) za pomocą programu Wireshark. Omówiliśmy podstawy sieci WLAN, w tym architekturę sieci bezprzewodowych 802.11, strukturę pakietów 802.11 oraz różne tryby działania kart sieciowych. Omówiliśmy również różnicę między trybem monitorowania a trybem promiscuous, które są ważne dla przechwytywania ruchu w sieci WLAN. Pokazaliśmy, jak skonfigurować przechwytywanie WLAN oraz jak przechwytywać i analizować ruch w sieci WLAN za pomocą programu Wireshark. W szczególności omówiliśmy, jak przeprowadzić

analizę przechwytywania sniffera dla WPA/WPA2 z PSK lub EAP, uwierzytelnianiem wielokierunkowym i internetowym. W kolejnym rozdziale będziemy kontynuować naszą przygodę z Wireshark, omawiając, jak przechwytywać poufne informacje, dane uwierzytelniające i pliki w celu etycznego hakowania i analizy sieci. Obejmuje to omówienie różnych scenariuszy i technik ataków, takich jak przechwytywanie haseł, podszywanie się pod ARP i ekstrakcja plików.

Pytania

1. Jaki jest cel czteroetapowego uzgadniania w zabezpieczeniach Wi-Fi WPA/WPA2?

a) Skojarzenie klienta bezprzewodowego z punktem dostępu

b) Wygenerowanie kluczy szyfrujących do transmisji danych

c) Uwierzytelnienie klienta bezprzewodowego na serwerze RADIUS

d) Wszystkie powyższe

2. Jaka jest główna różnica między trybem monitorowania a trybem promiscuous w Wireshark?

a) Tryb monitorowania przechwytuje tylko niezaszyfrowane pakiety, podczas gdy tryb promiscuous przechwytuje zarówno pakiety zaszyfrowane, jak i niezaszyfrowane.

b) Tryb monitorowania przechwytuje tylko pakiety wysyłane do określonego klienta bezprzewodowego, podczas gdy tryb promiscuous przechwytuje wszystkie pakiety w sieci bezprzewodowej.

c) Tryb monitorowania przechwytuje pakiety w czasie rzeczywistym, podczas gdy tryb promiscuous przechwytuje pakiety przechowywane w buforze.

d) Tryb monitorowania przechwytuje tylko niezaszyfrowane pakiety, podczas gdy tryb promiscuous przechwytuje pakiety przechowywane w buforze.

3. Który z poniższych adresów jest przykładem adresu multicast w protokole IPv4?

a) 192.168.0.1

b) 255.255.255.0

c) 224.0.0.1

d) Wszystkie powyższe

4. Jaki jest cel protokołu SSDP?

a) Wykrywanie drukarek sieciowych i komunikacja z nimi

b) Wykrywanie udziałów plików w sieci i komunikacja z nimi

c) Wykrywanie urządzeń UPnP i komunikacja z nimi

d) Żadne z powyższych

5. Który z poniższych trybów karty bezprzewodowej jest używany do ataków typu „pakiet injection” i innych zaawansowanych ataków?

a) Tryb główny

b) Tryb zarządzany

c) Tryb monitora

d) Tryb mieszany

6. Do której warstwy modelu OSI należy struktura pakietów 802.11?

a) Warstwa fizyczna

b) Warstwa łącza danych

c) Warstwa sieciowa

d) Warstwa transportowa

7. Jaki jest cel uwierzytelniania internetowego w sieciach bezprzewodowych 802.11? a) Uwierzytelnianie klientów sieci bezprzewodowej za pomocą serwera RADIUS

b) Szyfrowanie ruchu w sieci bezprzewodowej

c) Umożliwienie klientom sieci bezprzewodowej uwierzytelniania za pośrednictwem portalu uwierzytelniającego

d) Nawiązanie bezpiecznego połączenia VPN

8. Który z poniższych standardów bezpieczeństwa Wi-Fi wykorzystuje uwierzytelnianie 802.1X?

a) WEP

b) WPA-Personal

c) WPA2-Enterprise

d) WPA3-SAE

9. Jaki jest cel ramki Beacon w sieciach bezprzewodowych 802.11?

a) Synchronizacja klientów sieci bezprzewodowej z punktem dostępowym

b) Nadawanie identyfikatora SSID sieci bezprzewodowej

c) Szyfrowanie ruchu w sieci bezprzewodowej

d) Ogłaszanie dostępnej przepustowości sieci

10. Jaka jest różnica między skanowaniem pasywnym a aktywnym w sieci Wi-Fi?

a) Skanowanie pasywne nasłuchuje ramek Beacon od punktów dostępowych, podczas gdy skanowanie aktywne wysyła żądania sondy do punktów dostępowych. b) Skanowanie pasywne wysyła żądania sondy do punktów dostępowych, podczas gdy skanowanie aktywne nasłuchuje ramek beacon z punktów dostępowych.

c) Nie ma różnicy między skanowaniem pasywnym a aktywnym w sieciach Wi-Fi.

d) Skanowanie pasywne działa tylko w sieciach otwartych, podczas gdy skanowanie aktywne działa w sieciach szyfrowanych.

Odpowiedzi

1. b
2. b
3. c
4. c
5. a
6. b
7. c
8. c
9. b
10. a