Konfigurowanie laboratorium

W tej części dowiesz się, jak skonfigurować laboratorium do hakowania. Tak więc, możesz mieć system operacyjny, taki jak Windows, Linux lub Mac OS X, ale do hakowania potrzebujesz systemu operacyjnego, takiego jak Kali lub Backtrack. Te systemy operacyjne są tworzone w celu hakowania i testów penetracjyjnych. Mają wsparcie prawie wszystkich programów hakerskich. Dobra wiadomość, te systemy operacyjne są bezpłatne. My zamierzamy zainstalować i używać Kali. Oba systemy operacyjne to Linux, ale jest kilka różnic. Kiedy zainstalujemy Kali, będą zainstalowane wstępnie zainstalowane programy, które mogą być użyte do hakowania. Być może uważasz, że jest jakiś problem, że musisz zainstalować na komputerze nowy system operacyjny, ale jest kilka programów, które pomagają wirtualizować systemy operacyjne. Istnieją dwa słynne programy o nazwie "VirtualBox" i "VMware Workstation". Będziemy używać VirtualBox, ponieważ jest on bezpłatny i ma prawie takie same funkcje. VirtualBox to darmowy program o otwartym kodzie źródłowym, który umożliwia wirtualizację systemów operacyjnych takich jak Windows, Linux, Mac OS X, a nawet własnych systemów operacyjnych. Obsługuje prawie cały system operacyjny. Nie musisz nawet instalować Kali na swoim komputerze, możesz po prostu zainstalować Kali w VirtualBox, a następnie użyć go jako zwykłego komputera. Przede wszystkim pobierz najnowszą wersję VirtualBox i zainstaluj ją. Oto link dostępny:

https://www.virtualbox.org/wiki/Downloads

jeśli korzystasz z systemu operacyjnego Windows, powinieneś pobrać dla Windows hosta wersję binarną, jeśli używasz Linuksa do pobrania dla systemu operacyjnego Linux i jeśli używasz do tego Mac OS X do pobrania. Potrzebujemy również czegoś, co nazywa się "Pakiet rozszerzania Virtualbox" (można go znaleźć i pobrać z linku do pobierania VirtualBoxa), co pozwala nam na wprowadzanie USB, kart bezprzewodowych i wielu urządzeń przenośnych. Najpierw zainstaluj VirtualBox, a następnie kliknij dwukrotnie pakiet rozszerzający i kliknij instaluj, instalacja jest bardzo łatwa, więc nie zamierzam tego wyjaśniać. Po zainstalowaniu potrzebujemy systemu operacyjnego Kali do zainstalowania na VirtualBox. Ale dlaczego tracić czas, kiedy można po prostu pobrać już zainstalowane Kali? Na stronie Kali znajduje się link do pobrania zdjęć wirtualnych Kali, a następnie możesz po prostu otworzyć te wirtualne obrazy. VirtualBox i musisz pobrać VirtualBox bez względu na posiadany system operacyjny. Po zakończeniu pobierania przejdź do folderu Pobrane i wyszukaj obraz wirtualny Kali, rozszerzenie musi być "ova", następnie kliknij dwukrotnie i poczekaj, aż proces się zakończy. Jeśli obraz został pomyślnie zainstalowany, poszukaj przycisku ustawień i kliknij go. Przede wszystkim przejdź do systemu i poprawnie wpisz użycie pamięci RAM dla maszyny wirtualnej (pamiętaj, twój system operacyjny potrzebuje co najmniej dwóch gigabajtów pamięci RAM), następnie przejdziesz do systemu> procesor i wprowadzisz procesor do użycia, również bardzo ważne jest ustawienie połączenia sieciowego, ponieważ bez tego nie będziesz w stanie zrobić czegoś z Kali. Aby to zrobić, przejdź do sieci i wybierz "Bridged Adapter", co oznacza, że program użyje wbudowanej karty sieci bezprzewodowej. Teraz jesteś gotowy do uruchomienia maszyny wirtualnej. Kliknij "Start" i poczekaj wcześniej nazwa użytkownika promt pojawia się. domyślną nazwą użytkownika jest "root", a domyślne hasło to "toor", ale ze względów bezpieczeństwa zmienimy to później. Ekran powinien wyglądać tak:

Po lewej stronie powinien być program o nazwie "terminal", kliknij go, a zobaczysz, że czarny ekran pojawi się z czerwonym promt "root @ kali #". Możesz mieć pytanie typu "co root oznacza?", A root to rodzaj dostępu, aby zrozumieć, że łatwo jest to dostęp, gdy masz pełny dostęp przez komputer, możesz zrobić wszystko, co twój komputer potrafi. W oknach może się wydawać, że "Administrator" jest dostępem na najwyższym poziomie, ale tak nie jest. Najwyższym poziomem dostępu jest root. Tutaj będziemy uruchamiać nasze polecenia. Z poziomu terminala możesz łatwo uruchamiać programy i robić, co chcesz. Nasz system może być nieaktualny, więc uruchom komendę "apt-get update", aby zaktualizować system i poczekać, aż pojawi się promt. Program apt-get to program, który pozwala nam na łatwą aktualizację systemu i instalowanie programów (użyjemy go często później), dlatego poleceniem "aktualizacja aptget" wywołujemy program apt-get i powiadamiamy go o aktualizacji systemu. masz zaktualizowany system, musimy zmienić hasło, ponieważ jest ono domyślne i każdy może uzyskać do niego dostęp. Aby zmienić hasło, otwórz ponownie terminal i uruchom polecenie "passwd", a następnie poprosi o stare hasło, wpisz "toor" i kliknij enter, a następnie wprowadź nowe hasło (nie zmienia tego, co będzie) i zapamiętaj je. Aby wyłączyć maszynę wirtualną, kliknij przycisk w górę i w prawo, a następnie kliknij znak wyłączania. Teraz już wszystko konfigurujemy i jesteśmy gotowi dowiedzieć się, jak ukryć swoją tożsamość, jak stać się niemożliwe do wykrycia.

Ukryj identyfikację, stań się niemożliwy do wykrycia

W hakowaniu bardzo ważnej rzeczą jest bycie niezauważonym. Znalezienie czegoś jest niczym bez ukrywania swojej tożsamości. Na przykład, wyobraź sobie, że włamałeś się do czyjegoś wifi i nie ukryłeś identyfikacji, za kilka dni policja przetestuje router wifi i będą informacje o twoim komputerze, aż wreszcie znajdą cię i wsadza do więzienia. Tak bardzo ważna część całego hackingu, aby ukryć, zidentyfikować i uczynić hack niemożliwym do wykrycia. W tym rozdziale dowiesz się, jak być anonimowym, ukryj się i jak stać się w pełni niemożliwym do wykrycia.

Co to jest adres MAC?

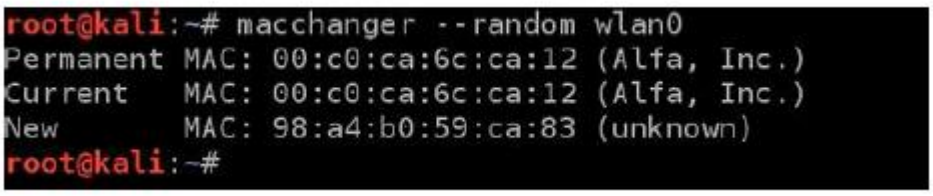
Adres MAC (adres kontroli dostępu do nośnika) jest unikalnym identyfikatorem przypisanym do interfejsów sieciowych do komunikacji w fizycznym segmencie sieci. Każde urządzenie komputerowe ma inny adres MAC. Adres MAC jest wbudowany w każde urządzenie komputerowe podczas jego tworzenia. Po uruchomieniu komputera system operacyjny odczytuje urządzenie sprzętowe. Po nawiązaniu połączenia z siecią bezprzewodową wysyła pakiety do użytkownika, a następnie komputer konwertuje te informacje na witryny internetowe, filmy, obrazy ... Wyobraź sobie, że dwa komputery są połączone z siecią bezprzewodową, pierwszy komputer potrzebuje witryny google.com, a drugi komputer chce amazon.com, sieć wysyła pakiety do tych komputerów, ale w jaki sposób te komputery wiedzą, jakie pakiety są ignorowane i jakie pakiety mają być odbierane? Komputery identyfikują pakiety do odbioru lub zignorowania przez adres MAC, kiedy sieć wysyła pakiet do komputera, zapisuje również w pakiecie adres MAC komputera, który wysyła. tak właśnie łączą się sieci bezprzewodowe i komputery. Jeśli więc nie zmienisz sieci IP i nie zhakujesz sieci bezprzewodowej, pozwolisz im zbadać swoją tożsamość, analizując historię sieci.

Jak ukryć adres MAC?

Możesz pomyśleć, w jaki sposób możesz zmienić adres MAC, jeśli komputer odczytuje go ze sprzętu? Nie zamierzasz modyfikować sprzętu, zmienić RAM. Gdy komputer się uruchomi, adres MAC zostanie załadowany do pamięci RAM, a my zmienimy już załadowany adres MAC. Tak więc po zmianie adresu MAC policja wykryje fałszywy adres MAC i nie będzie w stanie wykryć hakera. Teraz masz podstawowe informacje o tym, jaki jest adres MAC, zagrożenia związane z hakowaniem bez zmiany adresu MAC, jak policja może Cię śledzić, jak możemy to zmienić.

Zmień adres MAC przez Kali

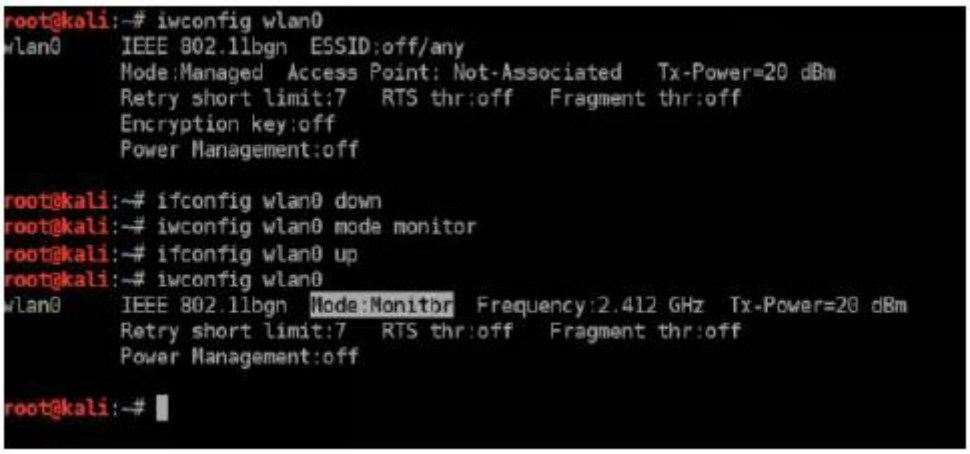
Kali zainstalował już program o nazwie "macchanger", który pozwala nam zmienić adres MAC w pamięci RAM. Otwórz VirtualBox, uruchom maszynę wirtualną kali i otwórz terminal. Musimy zatrzymać naszą kartę bezprzewodową, aby zmienić adres MAC. Wpisz "ifconfig wlan0 down". Ifconfig to program, wlan0 to nasza bezprzewodowa karta, a down to akcja, którą chcemy zrobić. Tak więc to polecenie zatrzyma każdą usługę bezprzewodową i konieczne jest zatrzymanie karty sieciowej przed zmianą adresu MAC. Następnie wpisz następujące polecenie "macchanger --help". Polecenie to każe Kali wywołać polecenie macchanger i wyświetlić pomoc. Istnieją instrukcje użytkowania programu. W moim przypadku wykorzystam losowy adres MAC wpisując "macchanger -random wlan0" .macchanger jest nazwą programu -random jest opcją, a wlan0 jest kartą bezprzewodową. Jeśli wszystko jest poprawne, ekran powinien wyglądać tak:



Pokazuje on, co było trwałym (wbudowanym w kartę sieciową) adresem MAC i jego korporacją w nawiasach, a na dole pokazuje, że istnieje nowy adres MAC, który nie ma korporacji. Teraz zmieniliśmy już adres mac i musimy włamać się do dowolnej sieci. Ale nie jesteś na to gotowy teraz, ponieważ nie wiesz, co to jest tryb monitora i jak z niego korzystać. Zaraz dowiesz się, jaki jest tryb monitora i jak go używać z Kali.

Tryby bezprzewodowe

Kiedy chcesz włamać się do wifi, musisz uchwycić "uścisk dłoni". Uzgadnianie to połączenie komputera osobistego i sieci bezprzewodowej, gdy spotykają się pakiety sieciowe i pakiety komputerów osobistych. Z uściskiem dłoni nie musisz już być w zasięgu Wi-Fi, możesz hakować hasło z handshake i nazwą Wi-Fi (dowiesz się o tym później). Teraz trzeba przechwycić wszystkie pakiety wysyłane przez router Wi-Fi i wszystkie komputery osobiste w sieci. Pojawia się pytanie typu "czy adres MAC jest używany w celu zapewnienia, że każdy pakiet zostanie dostarczony we właściwe miejsce, a następnie w jaki sposób je przechwycimy?", A odpowiedź brzmi: "Tak i nie, służy do wysyłania pakietów po prawej stronie miejsca docelowego, a my jako hakerzy możemy odbierać tylko pakiety wysyłane na nasz adres MAC, ale dotyczy to tylko trybu domyślnego karty sieci bezprzewodowej, który jest trybem "zarządzanym", jednak istnieje tryb, który pozwala nam przechwytywać wszystkie pakiety w naszej ofercie wi-fi, nie tylko te wysyłane do naszego urządzenia, stąd tryb monitorowania nazw. ". Teraz już znasz podstawy i jesteś gotowy, aby złapać uścisk dłoni. Przede wszystkim zmień adres MAC, wejdź w tryb monitorowania, wpisując te polecenia na zdjęciu:



Widać, że w końcu, gdy sprawdziłem tryb wlan0, był to monitor, jak widać na obrazku. Więc jesteś gotowy, aby rzeczywiście uchwycić uścisk dłoni, wtedy bardzo łatwo jest włamać się do sieci bezprzewodowej poprzez uzgadnianie i listę słów.

Łapanie uścisku dłoni

Pakiety handshake są wysyłane za każdym razem, gdy klient łączy się z docelowym AP. Aby go przechwycić, przechwycimy wszystkie wysłane pakiety. W tej sekcji będziemy używać programu o nazwie "airodump-ng". Ten program pozwala nam sniffować i przechwytywać pakiety wysyłane przez sieć. Ten program jest również preinstalowanym programem. Są dwa kroki do przechwycenia uścisku dłoni.

1. Uruchom airodump-ng na docelowym AP (Access Point):

Składnia jest podobna do tej:

>airodump-ng --channel [channel] –bssid [bssid] –write [file-name]

[interface]

Ex: >airodump-ng –channel 6 –bssid 11:22:33:44:55:66 --write out

wlan0mon

2. Poczekaj, aż klient połączy się z punktem dostępu lub anuluje uwierzytelnianie podłączonego klient (jeśli taki jest), aby ich system automatycznie nawiązał połączenie.

Składnia jest podobna do tej:

> aireplay-ng --deauth [liczba pakietów deauth] -a [AP] -c [cel]

[interface]

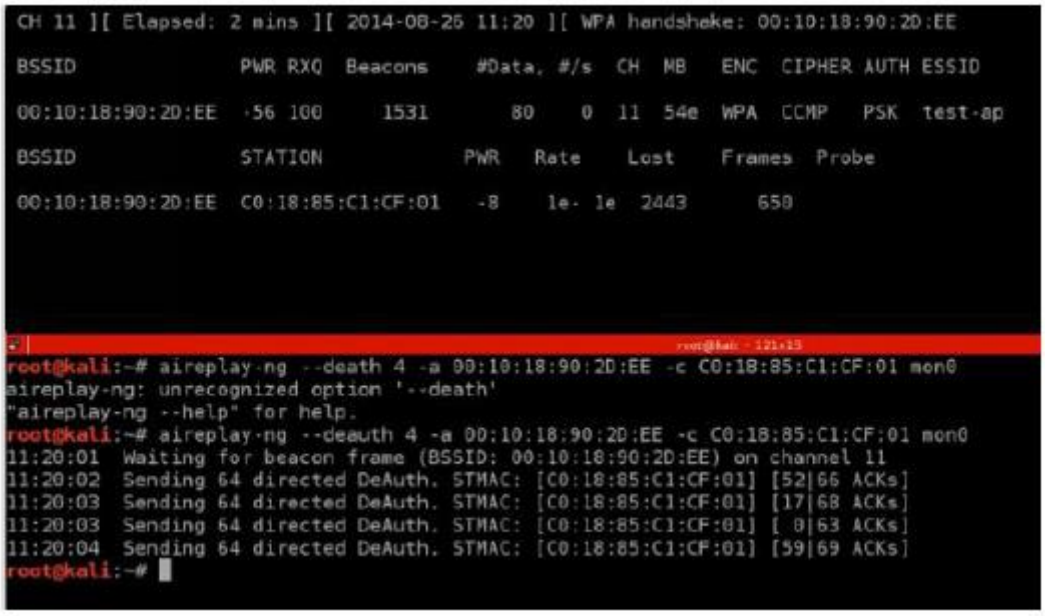
Np .:> aireplay-ng -deauth 1000 -a 11: 22: 33: 44: 55: 66 -c

00: AA: 11: 22: 33 mon0

Jeśli uzgadnia się uścisk dłoni, kali poinformuje cię w prawym górnym rogu

airodump-ng powie "WPA Handshake".

Wykonaj poniższe czynności, a kiedy złapiesz się uścisk dłoni, ekran powinien wyglądać tak:



Po złapaniu uścisku dłoni jesteś gotowy, aby złamać hasło

Łamanie dowolnej sieci bezprzewodowej

Teraz masz uścisk dłoni i musisz pobrać największą na świecie listę słów, aby zmienić hasło hakowania. Możesz pobrać tę listę słów z następującej strony internetowej:

http://www.hackreports.com/2013/05/biggest-password-crackingwordlist-with.html

drugi link:

https://crackstation.net/buy-crackstation-wordlistpassword-cracking-dictionary.htm

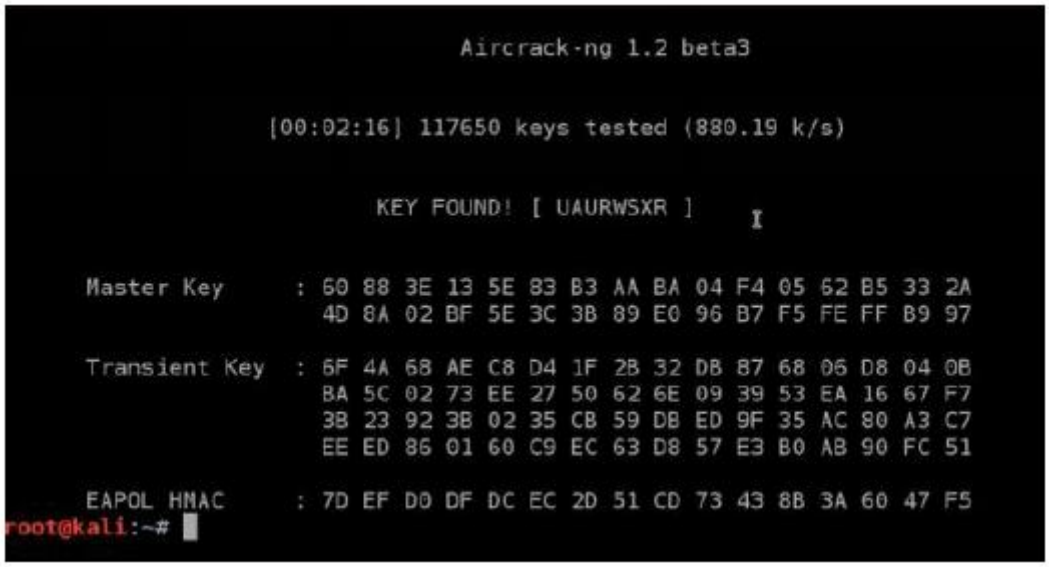
po pobraniu jednego z nich jesteś gotowy do hackowania sieci. Zamierzamy użyć aircrack-ng do złamania klucza. Czyni to, łącząc każde hasło na liście słów z nazwą punktu dostępu (essid), aby obliczyć

pary klucz główny (PMK) za pomocą algorytmu pbkdf2, PMK jest porównywany do pliku uzgadniania. Składnia wygląda następująco:

> aircrack-ng [nazwa handshake] -w [lista słów] [interfejs]

Np:> aircrack-ng is-01.cap -w list wlan0mon

Uruchom tę składnię i poczekaj, zanim aircrack-ng ją złamie . Kiedy hasło zostanie zhackowane, ekran powinien wyglądać tak:



Gratulacje!!! Zhakowałeś zabezpieczoną sieć bezprzewodową WPA !!! Nadszedł czas, aby zabezpieczyć naszą sieć bezprzewodową, ponieważ jak wiesz, bardzo łatwo jest hakować, a jeśli ktoś to zrobi, będzie mógł przechwytywać pakiety wysyłane przez sieć i analizować je. Będzie tam twoje hasło pocztowe, twoje hasło do sieci społecznościowej, pin do karty itd. Bardzo trudno jest nie mieć bezpiecznej sieci bezprzewodowej. W następnym rozdziale dowiesz się, jak zabezpieczyć swoją sieć i stać się prawie nietykalną.

Zabezpieczanie sieci przed powyższymi atakami

Teraz, gdy wiemy, jak przetestować bezpieczeństwo wszystkich znanych szyfrowań bezprzewodowych (WEP / WPA / WPA2), stosunkowo łatwo jest zabezpieczyć nasze sieci przed tymi atakami, ponieważ znamy wszystkie słabości, które mogą zostać wykorzystane przez hakerów do złamania tych szyfrów. Zatem spójrzmy na każde z tych szyfrów jeden po drugim:

1. WEP: WEP to stare szyfrowanie, a jego słabość, jak widzieliśmy w kursie, istnieje wiele metod, które mogą być użyte do złamania tego szyfrowania bez względu na siłę hasła, a nawet jeśli nikt nie jest podłączony do sieć. Ataki te są możliwe ze względu na sposób działania WEP, omawialiśmy słabość WEP i sposób jego złamania, niektóre z tych metod pozwalają nawet na złamanie klucza w kilka minut.

2. WPA / WPA2: WPA i WPA2 są bardzo podobne, jedyną różnicą między nimi jest algorytm używany do szyfrowania informacji, ale oba szyfrowania działają w ten sam sposób. WAP / WPA2 można złamać na dwa sposoby

a. Jeśli funkcja WPS jest włączona, istnieje duża szansa na uzyskanie klucza niezależnie od jego złożoności, można to zrobić wykorzystując słabość funkcji WPS. WPS służy do umożliwienia

użytkownikom łączenia się z siecią bezprzewodową bez wprowadzania klucza, odbywa się to poprzez naciśnięcie przycisku WPS na routerze i urządzeniu, które chcą połączyć, uwierzytelnianie działa za pomocą ośmiocyfrowej pinezki, hakerzy mogą brutalnie zmusić ten trzpień w stosunkowo krótkim czasie (średnio 10 godzin), po uzyskaniu właściwego sworznia mogą użyć narzędzia o nazwie reaver do odwrotnej inżynierii pin i uzyskać klucz, to wszystko jest możliwe ze względu na fakt, że WPS funkcja używa łatwego pinezka (tylko 8 znaków i zawiera tylko cyfry), więc nie jest słabością w WPA / WPA2, jest słabością funkcji, którą można włączyć na routerach, które używają WPA / WPA2, które można wykorzystać do uzyskania rzeczywistego Klucz WPA / WPA2.

b. Jeśli WPS nie jest włączony, jedynym sposobem na złamanie WPA / WPA2 jest użycie ataku słownikowego, w tym ataku lista haseł (słownika) jest porównywana z plikiem (plik uzgadniania), aby sprawdzić, czy którekolwiek z haseł jest rzeczywisty klucz do sieci, więc jeśli hasło nie istnieje na liście słów, napastnik nie będzie mógł znaleźć hasła.

Wniosek:

1. Nie używaj szyfrowania WEP, ponieważ widzieliśmy, jak łatwo jest go złamać, niezależnie od złożoności hasła, a nawet jeśli nikt nie jest podłączony do sieci.

2. Użyj WPA2 ze złożonym hasłem, upewnij się, że hasło zawiera małe litery, wielkie litery, symbole i cyfry oraz;

3. Upewnij się, że funkcja WPS jest wyłączona, ponieważ może zostać wykorzystana do złamania złożonego klucza WPA2 przez brutalne wymuszenie prostego kodu PIN WPS.