Wprowadzenie

Cyberprzestępczość jest największym zagrożeniem, z którym zmaga się każda organizacja na świecie! I nie tylko organizacje są podatne na ataki. Ludzie również są narażeni na ataki hakerów. Dlatego postaramy się pokazać, jak ważne jest, aby pozostać na szczycie tego zagrożenia, ucząc się … hakowania. Chociaż prawdą jest, że hakerzy mieli złą reputację przez lata, głównie z powodu stronniczych doniesień medialnych, nie wszyscy hakerzy mają intencje kryminalne. Tekst ten ma służyć jako przewodnik edukacyjny dla osób zainteresowanych nauką prostych narzędzi hakerskich. , wskazówki i techniki w celu ochrony siebie i sieci komputerowych. Ma być używana do hakowania etycznego, a nie do złośliwych działań. Jeśli kiedykolwiek byłeś ciekawy hackowania i chciałeś nauczyć się sztuki hackowania, to znalazłeś odpowiedni tekst. Żyjemy w świecie, w którym wszystko jest ze sobą powiązane. W dawnych czasach polegaliśmy na rządach i dużych organizacjach, aby zapewnić wystarczające bezpieczeństwo naszych danych osobowych. Nie jest to już możliwe w świecie, w którym same agencje bezpieczeństwa są głównymi celami złośliwych hakerów. W rzeczywistości, w większości przypadków największe zagrożenie cybernetyczne pochodzi od twojego własnego rządu! Więc co robisz? Siedzisz wygodniekrzyżując palce, mając nadzieję, że twój firewall i program antywirusowy wystarczą, aby Cię chronić? Niezależnie od tego, czy ci się to podoba, czy nie, będziesz musiał nauczyć się włamywania, jeśli masz szansę utrzymać swoje własne systemy cyber -bezpieczne. Dzięki zrozumieniu, w jaki sposób złośliwi hakerzy robią to, co robią, będziesz w stanie wykryć i zapobiec potencjalnym zagrożeniom dla systemu komputerowego lub sieci. Ten tekst pomoże ci to zrobić. Zaczynamy od ogólnego przeglądu stanu globalnego bezpieczeństwa cybernetycznego. Nauczysz się, jak rozróżniać różne typy hakerów, ich motywacje i umiejętności potrzebne do natychmiastowego hakowania. Omówimy także metody przeprowadzania testów penetracyjnych, aby sprawdzić potencjalne luki w sieci. Każda sieć, niezależnie od tego, jak bezpieczna, ma jakąś słabość. Dowiesz się, co dzieje się z targetowaniem, skanowaniem i analizowaniem celu oraz jak uzyskać dostęp do systemu. Istnieją różne sposoby włamania do systemu cybernetycznego. Szczegółowo analizujemy niektóre z najlepszych metod stosowanych przez złośliwych hakerów do ataków na ich cele. Wreszcie, co możesz zrobić, aby zachować bezpieczeństwo jako haker? Przeczytaj o tym wszystkim tutaj… jeśli będziesz chciał !!!

Część 1: To świat hakerów!

Dni odpoczynku łatwe, wiedząc, że twoje prywatne informacje są bezpieczne od wścibskich oczu są skończone! Świat, w którym obecnie mieszkamy, nie jest już taki jak dawniej. Cyberprzestępczość jest prawdziwym, niebezpiecznym i trwałym zagrożeniem, które każda organizacja i osoba musi traktować poważnie. Obecnie żyjemy w erze cyfrowej i w globalnej wiosce. Ponieważ wszystko i wszyscy są połączeni na tak masową skalę, można śmiało powiedzieć, że jest to świat hakerów. Nowy prezydent USA, Donald Trump, stwierdził, że kradzież cybernetyczna jest najszybciej rosnącą przestępczością w Ameryce. To nie jest tylko jego osobista opinia. Społeczność bezpieczeństwa cybernetycznego również się zgadza. Nie wierzysz mi? Sprawdźmy niektóre statystyki.

1. Czy wiesz, że szkoda wyrządzona przez cyberprzestępczość w 2016 r. kosztowała będzie 3 tryliony dolarów, a do 2021 r. ma wzrosnąć do 6 trylionów dolarów rocznie?

2. Czy wiesz, że organizacje w całych Stanach Zjednoczonych wydały 80 miliardów dolarów na produkty i usługi, aby chronić się przed cyberprzestępczością? Przewiduje się, że w 2017 r. Liczba ta przekroczy 1 bilion USD.

3. Czy wiesz, że praktycznie nie ma szans na bezrobocie, jeśli pracujesz w branży cyberbezpieczeństwa? Analitycy doszli do wniosku, że istnieje ogromny deficyt talentów cyberbezpieczeństwa na całym świecie, a stopa bezrobocia w cyberprzestrzeni spadła do zera w 2016 roku!

4. Złośliwi hakerzy są teraz „po krwi", nie „krzemie". Według Microsoftu do 2020 roku liczba osób online wyniesie 4 miliardy, a ludzie, a nie komputery, są obecnie głównym celem hakerów.

5. Czy wiesz, że przeciętny haker jest w stanie pozostać uśpiony w Twojej sieci przez średnio 200 dni bez wykrycia?

Te statystyki nie mają na celu cię przestraszyć. Mają one otworzyć oczy na to, co dzieje się na całym świecie. Jeśli oglądasz i czytasz wiadomości, to powinieneś wiedzieć, jak wielki problem pojawi się w przyszłości.

Hakowanie zdefiniowane

Co przychodzi ci na myśl, kiedy słyszysz słowo "hackowanie"? Czy wyobrażasz sobie postać z kapturem skuloną nad komputerem próbującym uzyskać nielegalny dostęp do sieci w celu kradzieży danych? A może jakiś głupek, który nie ma nic do roboty przez cały dzień, ale wysyła zaszyfrowane programy do infekowania sieci i systemów? Niezależnie od tego, jakie obrazy pojawiły się w twojej głowie, faktem jest, że większość ludzi wierzy, że wszyscy hakerzy mają zamiar kraść informacje lub szpiegować ludzi. Większość ludzi uważa, że wszyscy hakerzy są przestępcami, a hakowanie jest złe. Być może tak jest w filmach i programach telewizyjnych, ale po prostu tak nie jest. Hakowanie można zdefiniować jako próbę rozwiązania problemu lub ulepszenia aplikacji poprzez przeprojektowanie sprzętu lub oprogramowania. Innymi słowy, jeśli masz problem z komputerem i nie potrafisz go rozwiązać za pomocą konwencjonalnych technik, możesz być zmuszony do użycia dowolnej technologii, ale w nowy sposób. Jeśli spojrzysz na historię hackingu, wszystko zaczęło się od chęci rozwiązania problemu za pomocą kreatywnych środków. Pierwszymi nagranymi "hakerami" była grupa maniaków z MIT, którzy używali starego sprzętu telefonicznego do sterowania pociągami modelowymi z powrotem w 1950 roku. Ci ludzie byli tak w modelowych pociągach, że wzięli sprzęt telefoniczny, który otrzymali jako darowiznę i opracowali go aby wielu operatorów mogło kontrolować tory pociągu, po prostu wybierając numer telefonu. Niektórzy z nich poszli dalej i zaczęli modyfikować ostatnio wprowadzone programy komputerowe w kampusie. Ich celem było dostosowanie programów do specjalnego użytku i uczynienie ich lepszymi. Po prostu wykorzystali to, co mieli do dyspozycji, aby uzyskać kreatywność, wymyślić nowy sposób robienia czegoś i rozwiązywania problemów. O to właśnie chodzi w hakowaniu. Dziś hakowanie może stanowić naruszenie cyberbezpieczeństwa, szkodliwe systemy i nielegalny dostęp, ale to nie wszystko. Jak więc odróżnić dobrych facetów od przestępców?

Psychologia hakowania

Aby zatrzymać hakera, musisz najpierw zrozumieć, co go napędza. W społeczności hakerów istnieje kilka różnorodnych i skomplikowanych poziomów umiejętności i motywacji. Ważne jest, abyś zrozumiał różne typy hakerów, abyś mógł przewidzieć ich próby i zrozumieć ich mentalność. Nawet jako początkujący, który uczy się hakowania systemu, nie chcesz pozostawiać się podatnym na kontratak.

Kategorie hakerów

Największym błędem, jaki popełniają ludzie, jest umieszczanie wszystkich hakerów w tej samej grupie, tak jakby mieli jeden cel. Często to robią media, a opinia publiczna zakochuje się w tym kłamstwie. Nie możesz próbować kategoryzować hakerów bez uprzedniego dowiedzenia się, dlaczego dokonali

włamania i jakie były ich cele. Społeczność hakerów jest nieco podzielona w kwestii nazwania różnych typów hakerów, ale ogólnie rzecz biorąc, są to kategorie, z którymi większość ludzi się zgadza:

White Hats - znani również jako "hakerzy etyczni", hakerzy działają zgodnie z prawem. Trzymają się etyki hakerskiej, która mówi, że haker powinien "nie robić nic złego". Pracują również jako eksperci od bezpieczeństwa cybernetycznego i są zatrudniani do wykrywania potencjalnych luk w systemie lub sieci i naprawiania ich. Ten typ hakera współpracuje z dostawcami oprogramowania, aby naprawić lukę w ich oprogramowaniu. Białe kapelusze zazwyczaj robią to, co robią służby publiczne. Ich celem jest uświadomienie opinii publicznej o zagrożeniach, aby ludzie wiedzieli, jak wrażliwy jest system. Jednak nigdy publicznie nie publikują takich danych, dopóki sprzedawca oprogramowania sam tego nie zrobił.

Black Hats - Ten typ hakerów jest często przekonany, że wykonują oni służbę publiczną, ale w rzeczywistości ich główną motywacją jest siła i pieniądze. Mają tendencję do penetrowania sieci, aby mogli kraść lub powodować uszkodzenia danych. Kieruje nimi złośliwa nienawiść lub gniew przeciwko organizacji lub krajowi. Warto zauważyć, że wzięli swoją nazwę od faktu, że złoczyńcy w większości kowbojskich zachodnich filmów nosili czarne kapelusze.

Gray Hats - termin ten został pierwotnie wprowadzony przez bardzo znaną grupę hakerów w starej szkole, która nie chciała być kojarzona z Czarnymi Kapeluszami, a jednocześnie nie chciała być oznaczana jako tester bezpieczeństwa korporacyjnego. Szare kapelusze można określić jako hakerów, którzy niegdyś byli Czarnymi Kapeluszami, ale zreformowali się i teraz pracują jako eksperci od bezpieczeństwa cybernetycznego. Czasami określa się je jako hakerów, którzy konsultują się, a także uzyskują nielegalny dostęp do sieci.

Klasy hakerów

Istnieją określone klasy, które wchodzą w zakres wspomnianych wyżej kategorii hakerów Black and White Hat. Obejmują one:

Elite - To są guru świata hakerów. Mają umiejętności i wiedzę, których nikt inny nie posiada. Ale to, co czyni ich niezwykle rzadkimi, to etyka i uczciwość. Często działają jako Białe Kapelusze, które znają infrastrukturę sieciową i mają wiedzę programistyczną do pisania własnych narzędzi. Nie są motywowane intencjami przestępczymi i są bardziej skoncentrowane na wykrywaniu problemów z kodowaniem lub błędami bezpieczeństwa i informowaniu administratorów systemu. Możesz zostać tylko elitarnym hakerem wykonując dobrze znany hack lub exploit lub utrzymując długowieczność jako haker.

Cyberprzestępcy - ta klasa hakerów wykracza poza zwykłe awarie sieci przy użyciu ataku DoS (Denial of Service). Rozwijają się i kochają fakt, że mogą chować się za zasłoną sieci, gdy dzielą się ze sobą informacjami. Są w stanie ukryć zaszyfrowane dane w widoku zwykłym, tak aby mógł je znaleźć tylko inny cyberprzestępca. Rządy na całym świecie często zatrudniają hakerów, którzy zajmują się ich brudnymi sprawami, od prostego szpiegowania po cyberataki.

Script Kiddies - Nikt nie jest tak złośliwy lub wyśmiewany jak script kiddies. Ta klasa hakerów to młodzi, niedoświadczeni i niewykwalifikowani twórcy własnych narzędzi. Używają narzędzi stworzonych przez elitarnych hakerów i mogą hakować tylko te systemy, w których inni wykryli luki. Przeważnie włamują się do zabawy i są tymi, których wyczyny są powszechnie wymieniane w mediach. Ich głównymi osiągnięciami są zazwyczaj ataki DoS i defacement strony internetowej.

Hacktivist - To połączenie hakera i aktywisty. Niosą agendy polityczne, społeczne lub religijne i mogą być bardzo wytrwałe. Atakują strony internetowe i wykonują ataki DoS, aby wywrzeć nacisk na rządy lub organizacje, które ich zdaniem wyrządzają szkodę określonej grupie społecznej.

Gniewni pracownicy - to ludzie, którzy mają wewnętrzną wiedzę na temat organizacji i korzystają z ich dostępu do zbierania informacji dla siebie lub innych. Uważane są za wyjątkowo niebezpieczne, mimo że opinia publiczna rzadko się o nich mówi. Tacy hakerzy są zwykle spokojni i nieśmiali, ale mają narcystyczne osobowości. Zwracają się do swoich pracodawców za każdym razem, gdy uważają, że nie byli uznani za swoją pracę.

Piszący wirusy - to ludzie, którzy korzystają z każdej słabości, które ujawnił haker, i pisać dalej, aby wykorzystać te luki.

Umiejętności wymagane do hakowania

Jako początkujący, masz kilka podstawowych umiejętności, które będziesz musiał rozwinąć, jeśli chcesz awansować w świecie hakerów. Obejmują one:

1. Umiejętności obsługi komputera - Musisz posiadać wiedzę w zakresie obsługi komputera i rozumieć pisemne instrukcje. Przeglądanie internetu bez celu nie ma znaczenia. Czy możesz użyć modułu poleceń Windows? Te podstawowe umiejętności są kluczowe dla każdego hakera wartego swojej soli.

2. Znajomość systemu operacyjnego Linux - Linux pozwala na dostosowanie programów, dlatego hakerzy wolą go na Macu i systemie Windows.

3. Umiejętności baz danych - Nauka korzystania z systemów zarządzania bazami danych, takich jak Oracle i MySQL pomoże ci zrozumieć, jak przeniknąć bazy danych.

4. Umiejętności pracy w sieci - Jako haker, który będzie angażował się w wiele działań online, powinieneś wiedzieć o takich pojęciach jak podsieć, DNS, porty, hasła WPS i tak dalej.

5. Skrypty - Możesz nie wiedzieć jak teraz kodować, ale prędzej czy później będziesz musiał się nauczyć. Każdy haker musi mieć własne narzędzia hakerskie, a nie zależne od tego, co stworzyli inni. Opieranie się na narzędziach tworzonych przez innych hakerów pozostawia system podatny na wykorzystanie. Poświęć trochę czasu, aby nauczyć się języków skryptowych, takich jak Ruby on Rails lub Python.

6. Umiejętności odwrotnej inżynierii - Jednym z najbardziej skutecznych sposobów na opracowanie świetnego narzędzia hakerskiego jest wzięcie istniejącego, rozebrać go na części i znaleźć sposób na jego ulepszenie. Takie umiejętności są nieocenione dla hakera.

7. Używanie oprogramowania do wirtualizacji - Ten rodzaj oprogramowania pozwala bezpiecznie przetestować hakowanie na własnym komputerze, zanim wyzwolisz go na kimś innym. Dobrym przykładem jest VMWare Workstation.

Co motywuje hakera?

Kiedyś było tak, że operacje hakerskie były przeprowadzane przez jakiegoś nastolatka z college'u lub liceum ukrywającego się w piwnicy rodziców. W dzisiejszych czasach ataki cybernetyczne są bardziej wyrafinowane i powszechne. Jednak pomimo tego, że cyberprzestępczość jest zaawansowana w alarmującym tempie z lepszą technologią, motywy dzisiejszego hakera niewiele różnią się od poprzednich pokoleń. Co więc napędza cyberprzestępcę, aby włamać się do sieci lub systemu? Istnieją cztery podstawowe motywy:

1. Pieniądze - zyski finansowe są największą motywacją większości współczesnych cyberataków. Słyszeliście o hakerach wykorzystujących luki systemowe instytucji finansowych i wyłudzających numery kart kredytowych, kont e-mail, haseł, nazw użytkowników itp. Haker sprzedaje wszystko, co może znaleźć za konkretną cenę. Niektóre Czarne Kapelusze nawet szantażują organizacje używające oprogramowania ransomware.

2. Agenda polityczna / ideologiczna - tu hacktywiści są na tapecie. Atakują sieci instytucji rządowych, organizacji i wybitnych osobistości, aby realizować swoje ideologiczne, polityczne, społeczne lub naukowe programy. Jedna grupa znana z takich motywacji to Anonymous.

3. Rozrywka - większość szarych kapeluszy ma tendencję do wykorzystywania sieci dla zabawy lub dumy. Szukają wyzwania i łamią prawa etyczne, by zaspokoić swoją ciekawość. Jednak nie są złośliwi, a nawet poinformują administratora sieci o wykrytych lukach.

4. Cyberbezpieczeństwo - Białe Kapelusze zazwyczaj wykorzystują system do znajdowania słabości, aby mogły zwiększyć bezpieczeństwo. Organizacje często zatrudniają hakerów do pracy dla nich, łatają luki w zabezpieczeniach i tworzą kodeksy postępowania dla pracowników, których należy przestrzegać, aby uniknąć cyberprzestępstw.

Część 2: Testowanie penetracyjne

Testy penetracyjne odnoszą się do testowania systemu cybernetycznego, sieci lub aplikacji w celu wykrycia słabości, które mogą zostać wykorzystane przez złośliwego hakera. Zasadniczo próbujesz uzyskać dostęp do systemu bez żadnych nazw użytkownika ani haseł. Celem jest sprawdzenie, jak łatwo można uzyskać poufne informacje o organizacji, a następnie zwiększyć bezpieczeństwo testowanego systemu. Czym dokładnie jest różnica między testem penetracyjnym a atakiem? Pozwolenie! Haker, który przeprowadzi test penetracyjny, otrzyma autoryzację od właściciela systemu, który następnie będzie oczekiwał szczegółowego raportu na koniec tego wszystkiego. Jako tester możesz uzyskać dostęp na poziomie użytkownika, aby uzyskać dostęp do systemu. Stamtąd należy sprawdzić, czy możliwe jest uzyskanie dostępu do poufnych informacji, których zwykły użytkownik nie powinien nigdy widzieć. Inną opcją jest pójść w ciemno. W ślepej lub ukrytej ocenie, nie podasz wszelkich informacji z wyjątkiem nazwy organizacji klienta. Reszta należy do ciebie, a to jest właśnie to, jak robią to najbardziej złośliwi hakerzy. Jedynym problemem z ukrytą oceną jest to, że zajmie to więcej czasu niż jawna, zwiększając szanse, że stracisz jakąś wadę. Możesz zostać zatrudniony, aby znaleźć tylko jedną słabość, ale w większości wypadków będziesz musiał dalej szukać, aby znaleźć wszystkie potencjalne luki w sieci. Po zidentyfikowaniu, będziesz musiał znaleźć sposoby na naprawienie tych dziur. Dlatego będziesz musiał zapisać szczegółowe uwagi dotyczące procedury i wyników testu. Prowadzenie notatek pozwala klientowi określić efektywność swojej pracy i sprawdzić, czy wykryte problemy są naprawdę naprawione. Jest jednak bardzo mało prawdopodobne, że wykryjesz każdą lukę lub dziurę bezpieczeństwa w systemie.

Wykrywanie słabych punktów

Kroki podjęte przez testera penetrującego i złośliwego hakera są zwykle takie same. W większości przypadków złośliwy haker przenosi się powoli przez system, aby uniknąć wykrycia. Możesz również zastosować tę samą taktykę, aby zobaczyć, jak skuteczny jest system klienta w wykrywaniu takich ataków. Kiedy to nastąpi, te luki powinny być zapieczętowane. Pierwszym krokiem jest zwykle rozpoznanie. Próbujesz zebrać jak najwięcej informacji o swojej sieci docelowej. Zwykle jest to proces pasywny, polegający na wykorzystaniu zasobów dostępnych publicznie. Możesz zidentyfikować serwery WWW organizacji, system operacyjny, wersja oprogramowania, łatki lub moduły, które serwer włączył, adresy IP, a w niektórych przypadkach nawet nazwa wewnętrznego serwera. Po zebraniu informacji, nadszedł czas, aby je zweryfikować. Można to osiągnąć przez porównanie informacji o sieci lub systemie zebranych ze znanymi lukami. Po przetestowaniu luk będziesz wiedzieć na pewno, czy zebrane informacje są dokładne, czy nie

Powody wykonywania testów penetracyjnych

1. Zidentyfikuj słabości, które mogą zostać wykorzystane przez złośliwych hakerów

Nawet teraz, kiedy czytasz ten książke, możliwe jest, że istnieją złośliwi hakerzy uruchamiający narzędzia i ataki sieciowe, aby spróbować przeniknąć do twojego systemu. Ataki te nigdy się nie kończą i nie można przewidzieć, kiedy system zostanie trafiony. W większości przypadków exploity te są dobrze znane, a zatem można im zapobiec. Dział IT organizacji może chcieć wiedzieć, gdzie znajdują się słabe punkty w ich sieci i jak złośliwy haker może z nich skorzystać. Jako tester penetracji będziesz musiał zaatakować system i naprawić dziury, zanim znajdzie się ktoś, kto ma złe intencje. System może być dziś bezpieczny, ale jutro może paść ofiarą naruszenia.

2. Uzasadnij zarządzanie potrzebą zwiększenia zasobów

Zdarzają się sytuacje, gdy wyższe kierownictwo nie widzi potrzeby przeznaczania większej ilości środków finansowych na bezpieczeństwo cybernetyczne. W tym przypadku test penetracji jest najlepszym sposobem dla zespołu bezpieczeństwa firmy, aby uzasadnić roszczenia o więcej środków. Zespół ds. Bezpieczeństwa cybernetycznego może być świadomy luk w zabezpieczeniach, ale zarządzanie jest odporne na zmiany wprowadzane w istniejącym systemie. Dzięki zlecaniu testów zewnętrznemu konsultantowi kierownictwo z większym prawdopodobieństwem będzie szanować otrzymane wyniki.

3. Potwierdź, że zespół bezpieczeństwa wewnętrznego wykonuje swoją pracę

Raport z testu penetracji pokaże, czy dział bezpieczeństwa cybernetycznego jest sprawny w swojej pracy. Może określić, czy istnieje luka między wiedzą o słabych punktach systemu a wdrażaniem środków bezpieczeństwa.

4. Szkolenie sieciowe dla personelu

Wyobraź sobie, że haker miałby uzyskać dostęp do systemu organizacji bez wiedzy personelu. Przeprowadzając test penetracyjny, można odkryć, jak czujne jest twoje bezpieczeństwo i czy personel potrzebuje dodatkowego szkolenia. Podkreśla również skuteczność środków zaradczych zostały wprowadzone w przypadku cyberataku.

5. Testowanie nowej technologii

Przed uruchomieniem nowej technologii, na przykład nowej infrastruktury bezprzewodowej, ważne jest, aby system był testowany pod kątem luk. To z pewnością pozwoli zaoszczędzić więcej pieniędzy niż wykonanie testu, gdy klienci już go używają.

Raport z testu penetracji

Po zakończeniu testu musisz skompilować wszystkie dane we właściwym formacie i przesłać raport. Należy pamiętać, że większość kadry zarządzającej może nie być zorientowana pod względem technicznym, dlatego należy ją podzielić na odpowiednie sekcje, aby ułatwić jej czytanie. Powinieneś mieć Podsumowanie Wykonawcze, Podsumowanie Techniczne zawierające cały specyficzny żargon IT oraz Podsumowanie Zarządzania, które wyjaśnia, co należy zrobić, aby naprawić wykryte wady.

Część 3: Metodologia hakera

Wyobraź sobie żołnierza wchodzącego na pole bitwy w pełni wyposażonego w najnowszą i najbardziej zaawansowaną broń. Są pełni pewności siebie i wiedzą na pewno, że wygrają. Jednakże, gdy rozpoczyna się walka, żołnierz odkrywa, że wszedł w zasadzkę. Może on zestrzelić większość oddziałów wroga, ale ponieważ nigdy nie był przygotowany do bitwy, kończy przegrywając. Ten scenariusz nie jest tak daleko idący, jeśli weźmiemy pod uwagę liczbę tak zwanych "hakerów", którzy nie zadali sobie

trudu, aby przygotować się na ich ataki. W tym momencie przydatna jest metodologia hakerska. Metodą hakerską jest to, czego używa haker, prowadząc ją od pierwszego do ostatniego kroku. Aby skutecznie wykorzystać lukę w systemie, musisz zidentyfikować kluczowe rzeczy, które pomogą ci osiągnąć twoje cele. Bez odpowiedniej metodologii skończy się marnowanie czasu i energii na przegraną bitwę.

Docelowe mapowanie

Znalezienie idealnego celu ataku nie jest tak proste, jak się wydaje. Musisz być strategiczny w sposobie, w jaki prowadzisz badania i wyszukiwać cel o największym potencjale. Musisz przeanalizować swoje przyzwyczajenia, a następnie użyć zgromadzonych informacji, aby opracować najbardziej odpowiednią strategię. Celem mapowania celu jest ustalenie, co i kogo atakujesz przed przeniknięciem do systemu. Hakerzy zwykle atakują jeden lub kilka celów naraz. W zależności od rodzaju informacji, których szukasz, możesz zdecydować się na atakowanie serwerów internetowych przechowujących dane osobowe. Możesz również zdecydować się na duże i włamać się do instytucji finansowej. Twoim celem może być konkretna strona internetowa, którą chcesz usunąć za pomocą ataków DoS, lub możesz zablokować tę stronę. Możesz być zainteresowany konkretną osobą w organizacji. Kiedy szukasz potencjalnych celów do ataku, musisz wziąć pod uwagę poziom bezpieczeństwa, który będziesz próbował pokonać. Większość hakerów atakuje cele, o których wiedzą, że są łatwe do pokonania, więc poziom luki jest często kluczowym czynnikiem w mapowaniu celu. Kolejnym czynnikiem, który należy wziąć pod uwagę, jest to, czy informacja uzyskana z ataku jest tego warta. Pomoże to ustalić, jak długo jesteś gotów podjąć próbę aby uzyskać dostęp do systemu. Jak więc zdobyć informacje na temat zamierzonego celu?

* Przeprowadzanie wyszukiwania w Internecie Możesz sprawdzić nazwę celu i sprawdzić konto na Facebooku lub LinkedIn. Może to wywołać ich dane kontaktowe. Jeśli twoim celem jest organizacja, możesz wyszukać oferty pracy, które reklamowała firma, w szczególności w dziale IT. Możesz być zaskoczony, gdy dowiesz się, ile użytecznych informacji podano w ogłoszeniu o pracę, na przykład oprogramowanie, które potencjalni rekruci muszą znać.Jako haker musisz wiedzieć, które słowa kluczowe wywołają najwięcej informacji. Użyj zaawansowanej funkcji wyszukiwania Google, aby zidentyfikować witryny z linkami zwrotnymi w witrynie celu. Jeśli chcesz uzyskać dostęp do plików znajdujących się na stronie firmy, musisz użyć przełącznika, jak pokazano poniżej:

site: www.abc.com keyword

Inną techniką do użycia jest narzędzie Whois. Whois to świetny sposób na atak socjotechniczny lub skanowanie sieci. Możesz znaleźć serwery DNS domeny docelowej, a także nazwiska i adresy osób, które zarejestrowały domenę docelową. Grupy dyskusyjne Google przechowują wiele wrażliwych danych na temat użytkowników, na przykład nazw użytkowników, nazw domen i adresów IP.

* Web crawling

Zdobądź tzw. "Narzędzia do indeksowania stron internetowych", aby stworzyć lustrzany obraz docelowej strony internetowej. Gdy to zrobisz, każdy plik w witrynie, który jest publicznie dostępny, zostanie pobrany na lokalny dysk twardy. Pozwoli to skanować kopię lustrzaną i znaleźć nazwiska i adresy e-mail pracowników, pliki, katalogi, kod źródłowy do stron internetowych i wiele więcej informacji.

* Strony internetowe

Do tej pory powinieneś wiedzieć, że istnieją pewne strony internetowe, które są skarbnicą kluczowych informacji o osobach i organizacjach. Dobrymi przykładami są www.sec.gov/edgar.shtml, www.zabasearch.com oraz www.finance.yahoo.com.

Skanowanie sieci docelowej

Do tej pory zbierasz informacje, które pozwolą Ci zobaczyć całą sieć docelową jako całość. Nazwy hostów, otwarte porty, adresy IP i uruchomione aplikacje powinny być teraz widoczne. Pamiętaj, że jeśli masz wykonać skuteczny exploit, musisz nauczyć się myśleć jak złośliwy haker. Możesz zacząć korzystać z oprogramowania do skanowania, aby znaleźć i nagrać wszystkie hosty dostępne online. Twój własny system operacyjny powinien mieć własne standardowe narzędzie ping. Istnieją jednak narzędzia innych firm, takie jak SuperScan i NetScan Tools Pro, które mogą jednocześnie pingować nazwę hosta domeny lub wiele adresów IP.

Analizowanie otwartych portów

Dla początkujących istnieją narzędzia, których możesz użyć do sprawdzenia obecności otwartych portów w celu penetracji sieci docelowej. Przykłady niektórych skutecznych narzędzi obejmują SuperScan, Wireshark i OmniPeek.

Narażenie na luki systemowe

Zakładając, że znajdujesz jakąś lukę w systemie celu, możesz zacząć sprawdzać, czy te luki bezpieczeństwa są możliwe do wykorzystania. Możesz przejść do trasy ręcznej lub skorzystać z automatycznego narzędzia oceny. Metoda ręczna będzie wymagać połączenia z dowolnym otwartym portem, który wcześniej odkryłeś. Przetestuj te porty, aż znajdziesz drogę. Zautomatyzowana metoda polega na użyciu takich narzędzi, jak QualysGuard, czyli narzędzie oparte na chmurze, zaprojektowane do skanowania otwartych portów. Innym dostępnym narzędziem jest Nexpose, który może jednocześnie skanować łącznie 32 hosty.

Część 4: Uzyskanie dostępu fizycznego

Wyobraź sobie: wielomilionowa korporacja inwestuje miliony dolarów w środki bezpieczeństwa cybernetycznego zorientowane na technologię, aby chronić swoje dane. Całkowicie zablokowali swoje sieci i system oraz przeprowadzili wiele testów penetracyjnych za pomocą elitarnych hakerów, aby powstrzymać wszystkich złośliwych hakerów, którzy mogli zostać zatrudnieni przez ich konkurentów. Teraz wyobraź sobie, że firma ta wynajmuje firmę ochroniarską, która ma leniwych ochroniarzy. Nigdy nie przeprowadzają żadnych fizycznych kontroli wokół obiektu, a nawet pozostawiają otwarte drzwi. Odwiedzający są rzadko skanowani lub proszeni o zalogowanie. Nawet pokoje komputerowe są zwykle otwarte. Czy uważasz, że jest to sprytna firma, która dba o ochronę swoich danych przed hakerami? Tak, załatali elektroniczne dziury, ale dosłownie zostawili szeroko otwarte drzwi dla hakerów, którzy fizycznie naruszają ich bezpieczeństwo! Nie musisz zdalnie włamywać się do sieci, aby uzyskać dostęp do danych. Możesz uzyskać fizyczny dostęp do obiektu i wykonać swój exploit od wewnątrz. W ciągu ostatnich kilku dekad większość firm uznała, że niezwykle trudne jest utrzymanie bezpieczeństwa fizycznego. Dzięki postępowi technologicznemu istnieje teraz więcej fizycznych luk, które może wykorzystać haker. W dzisiejszym świecie dysków USB, tabletów, smartfonów i laptopów coraz więcej danych jest zapisywanych na mniejszych urządzeniach przenośnych. Nie jest trudno zdobyć takie urządzenia, zwłaszcza biorąc pod uwagę fakt, że większość pracowników zabiera ze sobą dane, gdy wychodzą z pracy pod koniec dnia. Po zidentyfikowaniu celu możesz nie musieć nawet wchodzić do budynku, a one dostarczą ci dane. W tej części dowiesz się, jak wykorzystać niektóre luki w

zabezpieczeniach fizycznych w budynkach, które są twoim celem. Jeśli naruszysz zabezpieczenia na miejscu i uzyskasz fizyczny dostęp, przygotuj się do penetracji systemu z poziomu wewnątrz.

Rodzaje fizycznych słabości

- Nie można ustanowić recepcji do monitorowania gości wchodzących i wychodzących z budynku.
- Niewykonanie obowiązkowego logowania wszystkich pracowników i odwiedzających.
- Zatrudnieni pracownicy i pracownicy ochrony, którzy nie są w pełni zaznajomieni z osobami zajmującymi się naprawą sprzętu IT, dostawcami lub dostawcami.
- Przerzucanie poufnych dokumentów firmowych i osobistych do kosza zamiast ich niszczenie.
- Nie można zablokować drzwi prowadzących do pomieszczeń komputerowych.
- Pozostawiając urządzenia cyfrowe leżące wokół biur.
- Nie można naprawić drzwi, które nie można prawidłowo zamknąć.

Tworzenie twojego planu

Jedną z pierwszych rzeczy, które musisz zrobić, to wymyślić sposób na naruszenie bezpieczeństwa fizycznego. Będzie to wymagało pewnych rozległych zadań rozpoznawczych z Twojej strony. Musisz określić rodzaj środków bezpieczeństwa, które placówka wprowadziła, słabe punkty i słabe punkty obecne oraz sposoby ich wykorzystania. Może się to wydawać proste na papierze, ale nie jest to łatwe, gdy pojawi się na ziemi. Założeniem jest to, że pracujesz bez wewnętrznego człowieka, aby przekazał ci istotne informacje dotyczące bezpieczeństwa. Może to być kilka tygodni wcześniej jak jesteś w stanie zebrać wszystkie informacje potrzebne do rozpoczęcia ataku. Fizyczne naruszenie bezpieczeństwa oznacza, że musisz mieć odpowiednie umiejętności i wiedzę, aby nie tylko wejść do budynku, ale także manewrować w środku, a następnie wyjść bez wykrycia. Jeśli brakuje ci cierpliwości, sprawności fizycznej i sprawności umysłowej koniecznej do wykonania takiego zadania, nie próbuj fizycznego naruszenia. Trzymaj się swoich ataków z odległej lokalizacji. Istnieje wiele czynników bezpieczeństwa fizycznego, które należy uwzględnić przy planowaniu sposobu uzyskania dostępu do celu. Są one podzielone na dwie odrębne klasy: Kontrola fizyczna i Kontrola techniczna.

<u>Kontrola fizyczna</u>

Będziesz musiał rozważyć, w jaki sposób zespół bezpieczeństwa kontroluje, monitoruje i zarządza dostępem do i z obiektu. W niektórych przypadkach budynek można podzielić na sekcje publiczne, prywatne i ograniczone. Będziesz musiał określić najlepszą technikę, aby wejść do sekcji zawierającej cel.

<u>1. Bezpieczeństwo na obrzeżach</u>

Jak planujesz omijać zabezpieczenia na granicy? Będziesz musiał wiedzieć, czy obiekt ma ścianę, ogrodzenie, psy, kamery monitorujące, bramki obrotowe, potzraski i inne rodzaje zabezpieczeń obwodowych. Są to tylko środki odstraszające, z którymi być może trzeba poradzić sobie na zewnątrz. Dobrze strzeżony obiekt będzie miał dodatkowe warstwy bezpieczeństwa, gdy zbliżysz się do budynku. W tym momencie powinieneś wiedzieć, jakie są słabości w projektowaniu obiektu. Jeśli jest wysoki mur, w którym są duże drzewa, możesz wspiąć się na gałęzie i wskoczyć do kompleksu. Oczywiście będziesz musiał być sprawny fizycznie i wystarczająco sprawny, aby to zrobić. Dowiedz się, gdzie znajdują się światła bezpieczeństwa i gdzie spadają ciemne plamy lub cienie. Mogą one zapewnić świetną kryjówkę, jeśli planujesz uzyskać dostęp na noc. Powinieneś również rozważyć nurkowanie na śmietniku, aby uzyskać dostęp do poufnych danych. Sprawdź lokalizację pojemników na śmieci i czy są

one łatwo dostępne. Byłoby dobrze wiedzieć, kiedy zbiera się śmieci, aby można było udawać, że są częścią załogi śmieci.

2. Identyfikatory

Organizacje używają identyfikatorów i identyfikatorów użytkowników do monitorowania i kontrolowania przepływu pracowników. Są również używane do śledzenia plików i katalogów tworzonych lub modyfikowanych przez pracownika. Zdobycie odznaki może wymagać kradzieży jednego od uprawnionego pracownika lub stworzenia fałszywej odznaki. Jeśli nie możesz uzyskać identyfikatora, pozostałe opcje będą następujące:

- Wejdź jako odwiedzający i unikaj eskorty.
- Użyj techniki tailgating, zakładając, że budynek nie ma potrzasków.
- Zaprzyjaźnij się z pracownikiem w strefie palenia i postępuj zgodnie z nim, kontynuując rozmowę.
- Zdobądź fałszywy uniform i podrób się pod wykonawcę, sprzedawcę lub mechanika. Jeśli chcesz zagrać all-in, rozważ zakup ciężarówki serwisowej i sprzętu, aby wyglądać bardziej legalnie.

3. Systemy wykrywania wtargnięcia

Obejmują one na ogół czujniki ruchu i alarmy włamaniowe. Będziesz musiał znać typy detektorów ruchu, z którymi masz do czynienia. Czy są to czujniki ruchu w podczerwieni, oparte na wysokiej temperaturze, falowe, pojemnościowe, fotoelektryczne lub pasywne? Każde z nich działa inaczej, a zrozumienie jego mocnych i słabych stron pomoże ci w misji. Konieczne będzie również poznanie rodzaju alarmów wewnątrz budynku. Obiekt może mieć czujniki na drzwiach i oknach, czujniki zbicia szyby, czujniki wody i tak dalej. Podczas gdy niektóre alarmy mają cicho powiadamiać o bezpieczeństwie potencjalnego naruszenia, inne mają na celu powstrzymanie lub odstraszanie atakującego. Alarm odstraszający zamknie drzwi i uruchomi zamki, aby uszczelnić wszystko i wszystkich. Odstraszający alarm będzie generował głośne dźwięki i emitował jasne światła, by spróbować zmusić napastnika do opuszczenia budynku.

Kontrole techniczne

Zazwyczaj koncentrują się na kontrolowaniu dostępu, ponieważ jest to najbardziej narażony obszar fizycznego bezpieczeństwa. Kontrola techniczna obejmuje karty inteligentne i kamery CCTV.

1. Karty inteligentne

Zawierają one układy scalone które przetwarzają dane i umożliwiają uwierzytelnianie dwuskładnikowe. Karty inteligentne zawierają informacje o pracowniku oraz obszary obiektu, do którego mają uprawnienia / do których nie mają dostępu. Posiadanie samej karty nie zapewni ci dostępu do obiektu. Skaner biometryczny i PIN / Hasło musi być również użyte do uwierzytelnienia. Jednak karty inteligentne mają pewne luki w zabezpieczeniach. Jedną z metod ominięcia kart inteligentnych jest generowanie błędów. To jest tam, gdzie używasz inżynierii odwróconej do szyfrowania, aby znaleźć klucz szyfrujący i uzyskać dostęp do przechowywanych danych. Obejmuje to wprowadzanie błędów obliczeniowych poprzez zmianę częstotliwości taktowania i napięcia wejściowego lub zmianę fluktuacji temperatury. Możesz również użyć ataku z kanału bocznego, aby dowiedzieć się, jak działa karta, nie uszkadzając jej. Obejmuje to wystawienie karty na różne warunki za pomocą analizy elektromagnetycznej, analizy mocy różnicowej i pomiaru czasu. Innym sposobem jest użycie oprogramowania do przeprowadzenia nieinwazyjnego ataku. Wymaga to włamania do oprogramowania i załadowania poleceń, które umożliwiają wyodrębnienie danych konta. Wreszcie

istnieje metoda określana jako mikro-sondowanie. Jest to atak inwazyjny polegający na podłączaniu sond bezpośrednio do chipa. Celem jest wyjęcie układu i zresetowanie go.

2. Kamery CCTV

Standardem nadzoru wideo są kamery CCTV. Znajdują się w strategicznych miejscach i są monitorowane przez ochroniarzy siedzących w sterowni. Zawsze jednak istnieją martwe pola, które należy wykorzystać, więc musisz wiedzieć, gdzie one są. Kamery mogą być bezprzewodowe lub sieciowe, co oznacza, że możesz hakować kanał kamery i manipulować obrazami wyświetlanymi na ekranie lub zacinać sygnał. Bezpieczeństwo fizyczne jest kluczową częścią bezpieczeństwa cybernetycznego. Hakerzy będą zawsze szukać słabości, które mogą znaleźć, zarówno online, jak i offline.

Część 5: Inżynieria społeczna

Czy wiesz, że w 2016 roku trzy największe zagrożenia cybernetyczne dotyczyły inżynierii społecznej, zagrożeń wewnętrznych i zaawansowanych trwałych zagrożeń? To pokazuje, jak nieokiełznane ataki inżynierii społecznej stały się ważne cyberbezpieczeństwie. Dlaczego uważasz, że socjotechnika jest numerem jeden na tej liście? Haker powinien atakować system lub sieć, więc dlaczego mieliby się skupić na innym aspekcie systemu bezpieczeństwa organizacji? Odpowiedź leży w ludziach. Największą słabością każdego elementu bezpieczeństwa są zaangażowani ludzie. W ostatniej części zobaczyliśmy, że najbardziej zaawansowana technologia nie może ochronić cię przed cyberatakami, jeśli ludzie strzegący budynku śpią w pracy. Dzięki inżynierii społecznej możesz hakować ludzi, zdobywając ich zaufanie i wykorzystując je do potrzebnych informacji. Będziesz jednak wymagał pewnego stopnia odwagi i umiejętności, aby skłonić ludzi do zaufania ci, biorąc pod uwagę, że jesteś zupełnie obcy. Jednym z aspektów inżynierii społecznej jest to, że zwykle odbywa się to razem z włamanie bezpieczeństwa fizycznego. Celem jest nawiązanie kontaktu z kimś, kto ma konkretne informacje, które mogą pomóc ci uzyskać dostęp do plików lub zasobów twojego celu. Na przykład:

- Wyślij celowi e-mail zawierający linki. Po kliknięciu łącza, złośliwe oprogramowanie lub wirus jest pobierany na komputer, co pozwala kontrolować system i gromadzić dane.
- Jeśli jesteś pracownikiem firmy i chcesz uzyskać nieautoryzowany dostęp do poufnych danych, możesz poinformować wydział bezpieczeństwa, że zgubiłeś swój klucz dostępu. Dadzą ci klucze do wejścia do pokoju, dzięki czemu możesz dostać się do plików fizycznych i cyfrowych, które chcesz.
- Możesz podszyć się pod prawdziwego sprzedawcę produktów i twierdzić, że Twoja firma musi zaktualizować lub zainstalować łatkę na oprogramowaniu klienta (np. Oprogramowanie księgowe). Możesz wtedy poprosić o podanie hasło administratora. Alternatywnie możesz po prostu poprosić ich o pobranie fałszywego oprogramowania, które umożliwi ci zdalny dostęp do sieci celu.

  Te przykłady mogą wydawać się zbyt proste lub łatwe, ale pamiętaj, że socjotechnika jest najczęściej używaną taktyką hakerów, która narusza bezpieczeństwo cybernetyczne. Ucząc się, jak złośliwi hakerzy popełniają swoje wyczyny, jesteś lepiej przygotowany do tego, aby uniemożliwić włamanie się Twojemu systemowi lub innym osobom.

Strategie inżynierii społecznej

Przyjrzyjmy się dokładniej niektórym strategiom używanym przez hakerów podczas ataku socjotechniki.

1. Zdobywanie zaufania

Jednym z najlepszych sposobów budowania zaufania do hakowania w inżynierii społecznej są słowa i działania. Musisz być elokwentny, ostry i być dobrym rozmówcą. Są przypadki, gdy inżynier socjalny zawodzi w swojej misji, ponieważ byli nieostrożni w swoich rozmowach lub działali nerwowo. Zdarza się to często, gdy haker okazuje następujące znaki:

- Zbyt dużo mówi lub wykazuje zbyt duży entuzjazm
- Działając nerwowo w odpowiedzi na pytania
- Zadaje dziwne pytania
- Wydaje się spieszyć
- Posiada informacje wyłącznie dla osób posiadających informacje poufne
- Mówi o osobach z wyższego kierownictwa w organizacji
- Udaje, że ma autorytet w firmie

Dopóki będziesz ćwiczyć umiejętności i techniki inżynierii społecznej, będziesz w stanie ukryć te znaki. Jedną niezwykle skuteczną taktyką, którą można wykorzystać do zdobycia czyjegoś zaufania jest wyjście z drogi, aby zrobić komuś przysługę, a następnie natychmiast poprosić o nią w zamian. Kolejna taktyka to coś, co prawdopodobnie zobaczyłeś w filmie. Ktoś podniósł kogoś, tworząc dla niego konkretny problem. Kiedy ofiara woła o pomoc, rzuca się na scenę i ratuje. To działa, aby stworzyć więź między tobą a potencjalnym celem. Fałszywy identyfikator i mundur pracy może czasami pomóc podszyć się pod Ciebie pracownika w firmie, dzięki czemu można wejść do obiektu niewykryte. Ludzie będą nawet podawać hasła i inne poufne informacje, o ile wydaje się, że jesteś jednym z nich.

2. Phishing

Hakerzy wykorzystujący ataki z zakresu socjotechniki mogą wykorzystywać swoje cele za pomocą technologii, ponieważ jest to łatwiejsze i bardziej rozrywkowe. Ludzie mogą być bardzo naiwni, szczególnie gdy są online. To po prostu niesamowite, jak bardzo ufni są ludzie w dobie rosnących cyberataków. Phishing polega na wysyłaniu docelowych wiadomości e-mail, które wydają się pochodzić z wiarygodnego lub zaufanego źródła. Celem jest skłonienie ich do dzielenia się wrażliwymi lub osobistymi informacjami poprzez wysyłanie ich bezpośrednio lub klikanie linków. Wiadomość e-mail będzie wyglądać jak prawdziwa transakcja dla zamierzonego celu, ale to dlatego, że podszywasz pod adres IP, aby wyświetlić adres e-mail, który wydaje się oryginalny. Możesz udawać bliskiego przyjaciela, krewnego lub współpracownika i poprosić o przesłanie swoich danych osobowych. Możesz także udawać instytucję finansową i poprosić o kliknięcie linku w celu zaktualizowania informacji o koncie. Kiedy to zrobią, zostaną przekierowani na fałszywą stronę internetową, która odzwierciedla prawdziwą. Po zalogowaniu się możesz uzyskać dostęp do swoich nazw użytkowników, identyfikatorów użytkowników, haseł, numeru konta bankowego lub numeru ubezpieczenia społecznego. Spamowanie to kolejna taktyka, którą możesz wykonać. Po prostu wyślesz im mnóstwo maili i poczekasz, aż staną się ciekawi i otworzą przynajmniej jednego z nich. E-mail będzie zawierał prośbę o pobranie bezpłatnego prezentu (e-book, wideo, kupon itp.) W zamian za podanie niektórych danych osobowych. Jedną z najczęstszych sztuczek jest twierdzenie, że jest to zweryfikowany dostawca oprogramowania. Wszystko, co musisz zrobić, to wysłać łatkę oprogramowania pocztą e-mail i poprosić o pobranie jej za darmo. Nie zdają sobie jednak sprawy z tego, że oprogramowanie jest w rzeczywistości koniem trojańskim lub backdoorem, który pozwala na pełną kontrolę nad swoim

systemem. Oszustwa wyłudzające informacje działają tak dobrze, ponieważ są bardzo trudne do prześledzenia z powrotem do hakera. Narzędzia wykorzystywane przez inżynierów społecznych, na przykład remailery i serwery proxy, zapewniają odpowiednią anonimowość, aby zapobiec ich ujawnieniu.

Jak zapobiec hakowi inżynierii społecznej

Jako początkujący haker prawdopodobnie bardziej interesuje Cię uczenie się wykonywania ataku, niż zapobieganie mu. Jednak, jak powiedzieliśmy na początku, hackowanie może działać zarówno na dobre, jak i na złe. Dlatego ważne jest, abyś rozumiał, w jaki sposób można zapobiec atakowi, abyś mógł odpowiednio poinformuj klienta. Informacje te pomogą także w przeprowadzeniu skuteczniejszych exploitów. W końcu nie ma potrzeby tracić czasu i energii na atakowanie obiektu za pomocą techniki, której już wcześniej chronili. Organizacje będą zazwyczaj używać dwóch technik, aby uniemożliwić inżynierom społecznym wykorzystywanie ich luk:

1. Opracowywanie i egzekwowanie surowych zasad - organizacja może tworzyć hierarchie informacji, w których użytkownicy mają dostęp do niektórych, ale nie wszystkich danych. Należy również bezwzględnie wymuszać noszenie identyfikatorów przez wszystkich pracowników i konsultantów, a każdy gość musi być eskortowany przez ochronę. Kiedy zwolnieni pracownicy, wykonawcy lub dostawcy opuszczają strefę pomieszczenia, należy ich pozbawić identyfikatorów. To samo hasło nie powinno również być używane przez dłużej niż ustawiony czas. Wreszcie, w przypadku wykrycia naruszenia lub podejrzanego zachowania, personel ochrony musi szybko zareagować. Najważniejszy aspekt każdej organizacji jest przestrzegana polityka. Ludzie zaangażowani muszą zrozumieć wymagania i śledzić je przez cały czas.

2. Szkolenie użytkowników w zakresie świadomości bezpieczeństwa - Większość pracowników po prostu nie wie, co zrobić, gdy mają do czynienia z atakiem inżynierii społecznej. Musi istnieć świadomość i szkolenie użytkowników, aby uczyć ludzi, jak rozpoznawać i reagować na hakerów. Szkolenie powinno być raczej ciągłe niż jednorazowe. Program szkolenia powinien być wystarczająco łatwy dla tych, którzy nie są technicznie nastawieni do zrozumienia. Ważne jest również, aby wyżsi menedżerowie dawali przykład i podejmowali szkolenie. Ponieważ ataki inżynierii społecznej nie są skierowane wyłącznie do organizacji, musimy zbadać, w jaki sposób jednostki mogą się chronić. Niektóre sposoby zapobiegania tego typu atakom obejmują:

1. Unikaj rozdawania haseł przypadkowym osobom.

2. Unikaj wysyłania swoich danych osobowych za pośrednictwem poczty e-mail lub mediów społecznościowych bez sprawdzania tożsamości odbiorcy. Upewnij się, że wiesz, kto wysyła Ci przyjaciela lub prośbę o połączenie na Facebooku, LinkedIn lub Twitterze.

3. Unikaj pobierania załączników z niezidentyfikowanych adresów IP lub klikania linków w spamie.

4. Unikaj tendencji do ustawiania kursora nad linkiem e-mail. Hakerzy mogą osadzać złośliwe oprogramowanie w łączu i uruchamiać pobieranie w momencie, gdy mysz się na nim przesunie. Ochrona przed złośliwym oprogramowaniem to dobry sposób na zapobieganie tego typu hackowaniu. Prawda jest taka, że inżynieria społeczna może być nieco skomplikowana, zapobieganie jest również bardzo trudne. Organizacja nie może kontrolować wszystkich osób powiązanych z nią przez cały czas, a jako jednostki, każdy ma swoją unikalną słabość. Twoim zadaniem jest go znaleźć i wykorzystać.

Część 6: Hakowanie haseł

Jednym z najczęstszych sposobów zapewnienia bezpieczeństwa danych jest ochrona hasłem. Tak bardzo przyzwyczailiśmy się do wprowadzania haseł we wszystkich naszych urządzeniach cyfrowych, że uważamy, że ten środek jest wystarczający, aby zapewnić bezpieczeństwo naszym informacjom. Jednak prawda jest zupełnie inna. Hasła wykonują dobrą robotę, uniemożliwiając nieautoryzowanym użytkownikom opuszczenie systemu, ale jak wszyscy wiemy, hakerzy mają łamacze haseł. W większości przypadków użytkownik może nie zdawać sobie nawet sprawy, że ktoś inny zna jego hasło. Hasła mogą sprawiać, że ludzie czują się bezpiecznie, ale istnieje w nich wiele luk, które haker może z łatwością wykorzystać

Typy luk w zabezpieczeniach haseł

Zasadniczo istnieją dwa rodzaje luk w zabezpieczeniach hasłem: użytkownik i pracownik techniczny.

Usterki użytkownika

Luki w zabezpieczeniach to słabe strony wynikające z braku odpowiednich zasad haseł lub słabego egzekwowania takich wytycznych. Na przykład, ile razy widziałeś, że ktoś używa tego samego hasła do swojego laptopa, smartfona, tabletu i wszystkich swoich urządzeń cyfrowych? Wyobraź sobie kogoś używającego tego samego hasła dla kont Yahoo, Gmail, LinkedIn, Facebook i Twitter! Nie ma potrzeby, aby sobie wyobrazić, ponieważ jest to dokładnie to, co robi większość ludzi! Większość ludzi po prostu zbyt trudno zapamiętać każde hasło. Żyjemy w świecie wygody, więc większość ludzi szuka najszybszych i najprostszych sposobów na załatwienie spraw. Zwykle powoduje to, że ludzie powtarzają to samo hasło dla wszystkich swoich kont. Niestety, to po prostu ułatwiło pracę hakerów. Przy wszystkich dostępnych literach i liczbach istnieją potencjalnie trzy trylionowe kombinacje haseł o długości ośmiu znaków. Jednak byłbyś zaskoczony liczbą osób, które wybierają słabe i głupie hasła, aby ułatwić im wkuwanie. Niektórzy nawet nie zawracają sobie głowy hasłami i całkowicie pomijają ten proces!

Jakie są więc luki w zabezpieczeniach, które może wykorzystać haker? Hasła, które nigdy się nie zmieniają. Kiedy ostatnio zmieniałeś swoje hasło na Twitterze lub e-mail? Po co przechodzić przez kłopoty, prawda? To samo hasło jest używane na kilku różnych kontach w różnych sieciach i systemach. Hasła zbyt proste i powiązane z Twoim imieniem i nazwiskiem, lokalizacją, szkołą, pracą i tym podobne. Większość użytkowników rozgląda się po pokoju, gdy zostanie poproszony o utworzenie hasła. Cokolwiek zobaczą, to, tego będą używać. Może to zabrzmieć zabawnie, ale to prawda. Hasła, które są długie i złożone, zazwyczaj są zapisywane na kartkach papieru lub przechowywane w pliku. Dopóki lokalizacja pliku jest niezabezpieczona, może zostać skradziona.

Luki techniczne

Wykorzystywanie luk w zabezpieczeniach użytkowników jest zazwyczaj pierwszym krokiem dla hakera. Następnie próbujesz sprawdzić, czy istnieją jakieś słabości techniczne, które możesz wykorzystać. Najczęstsze z nich to:

- Nieużywanie aplikacji ukrywających hasło podczas pisania na ekranie. Chociaż większość aplikacji natychmiast ukrywa znaki wpisywane na ekranie, niektóre nie. Jeśli użytkownik nie skonfiguruje odpowiednio ustawień, pozostawiają one wrażliwe na surferów (co zostanie wyjaśnione w dalszej części).
- Używanie programów lub baz danych do przechowywania wszystkich haseł, ale niepoprawne zabezpieczenie bazy danych. Niektórzy użytkownicy przechowują wszystkie swoje hasła w jednym pliku MS Word, Access lub Excel, ale nie zabezpieczy samego dokumentu.

- Używanie niezaszyfrowanych baz danych, do których ma dostęp duża liczba nieautoryzowanych osób. Tak jest często w przypadku organizacji.
- Wykorzystanie słabych technik szyfrowania przez producentów oprogramowania i programistów. Większość programistów ma zbyt dużą wiarę w to, że ich kody źródłowe są nieznane. Nie zdają sobie jednak sprawy, że przy odpowiednim czasie i cierpliwości każdy doświadczony haker może złamać kod źródłowy. Haker, który ma wystarczającą moc obliczeniową, może nawet użyć narzędzi zaprojektowanych do łamania słabych szyfrów.

Zrozumienie szyfrowania hasła

Hasło jest szyfrowane, gdy jest przechowywane w systemie przy użyciu algorytmu szyfrowania lub jednokierunkowego skrótu. Po haszowaniu hasła, każdy użytkownik widzi zaszyfrowany ciąg o stałej długości. Podstawowym założeniem jest to, że po haszowaniu hasła nie można go złamać. LINUX idzie jeszcze dalej i dodaje losową wartość (sól) do zaszyfrowanego hasła, tylko po to, by było bezpieczniejsze. Sól umożliwia tym dwóm osobom używanie dokładnie tego samego hasła, ale generuje zupełnie inne wartości mieszania. Istnieje wiele narzędzi, które mogą być wykorzystywane przez hakerów do łamania haseł. Narzędzia te działają, biorąc kilka dobrze znanych haseł, uruchamiając je za pomocą algorytmu mieszania, a następnie generując zaszyfrowane hashe. Po wygenerowaniu zaszyfrowanych skrótów narzędzie porównuje je z hasłem, które należy złamać. Oczywiście proces ten odbywa się z bardzo dużą szybkością, a hasło jest łamane w momencie, gdy oryginalny hash i zaszyfrowany hash są zgodne. Czasami haker może znaleźć hasło, które jest bardzo skomplikowane i silne. Takie hasła są dość trudne do złamania, ale dzięki odpowiednim narzędziom, wystarczającej ilości czasu i odpowiedniej cierpliwości, wszystkie hasła mogą zostać zhackowane. Jeśli chcesz się upewnić, że Twój system jest chroniony przed złośliwymi hakerami, musisz uzyskać te same narzędzia, których używasz, przeszukać system pod kątem luk i naprawić je

Narzędzia do łamania haseł

Na rynku dostępnych jest teraz wiele zaawansowanych narzędzi do łamania haseł. Niektóre są bardziej popularne niż inne ze względu na ich skuteczność w różnych systemach i oprogramowaniu operacyjnym. Na przykład:

Ophcrack - To narzędzie służy do łamania haseł w aplikacjach Windows.

Cain and Abel - To jedno z najbardziej skutecznych narzędzi. Może być używany do łamania hashy, haseł VNC i Windows oraz wielu innych aplikacji.

John the Ripper - Jest to zdecydowanie jeden z najbardziej znanych i lubianych programów do łamania haseł. Łączy on słownikowy styl ataku przed rozpoczęciem pełnego ataku brute force. Służy do łamania LINUX i mieszania haseł do systemu Windows.

Brutus - to narzędzie działa dobrze w łamaniu loginów dla HTTP, FTP i innych

Elcomsoft Distributed Password Recovery - To narzędzie działa bardzo szybko dzięki zastosowaniu programu akceleracji wideo GPU i jednoczesnego korzystania z tysięcy komputerów w sieci. Jest w stanie złamać Windows, Adobe, iTunes i inne aplikacje.

Elcomsoft System Recovery - to narzędzie wykorzystuje bootowalną płytę CD do resetowania uprawnień administracyjnych w systemie Windows.

Istnieje wiele innych narzędzi do hackowania haseł w różnych aplikacjach, systemach i sieciach. Najważniejszą rzeczą jest zrozumienie, jak działa szyfrowanie i jak te narzędzia mogą być użyte do przezwyciężenia szyfrowania.

Techniki łamania haseł

Wszyscy próbowaliśmy w pewnym momencie złamać hasło. To mógł być domowy komputer, laboratorium szkolne, a może urządzenie przyjaciela. Prawdopodobnie użyłeś metody konwencjonalnej zamiast zaawansowanej. Poniższe techniki są połączeniem niektórych podejść ze starej szkoły i niektórych zaawansowanych technologicznie metod.

1. Zgadywanie - jest to prawdopodobnie jedna z najbardziej nadużywanych technik. Jest to również najprostsze podejście, ponieważ większość użytkowników wybiera hasła, które będą łatwo zapamiętywać. Wszystko, co musisz zrobić, to użyć logiki, aby odgadnąć, co mogło być użyte do utworzenia hasła. Ta technika działa najlepiej, gdy znasz cel lub masz łatwy dostęp do swoich danych osobowych. Hasło to często imię, nazwisko, data urodzenia, a nawet ulubione zwierzę użytkownika lub członka rodziny

2. Surfowanie przez ramię - Tutaj podglądasz osobę, która wpisuje hasło. Możesz obserwować znaki na ekranie lub zapamiętywać ich klawisze. Ważne jest, aby mieszać się w celu uniknięcia wykrycia i być dyskretnym w swoich ruchach. Jeśli chcesz uzyskać hasła od osób w miejscach publicznych, takich jak kawiarnia, możesz umieścić kamerę w strategicznym miejscu, aby monitorować ich naciśnięcia klawiszy logowania.

3. Inżynieria społeczna - Co zrobić, jeśli możesz uzyskać hasło, prosząc o to po prostu? Zdecydowana większość ludzi wierzy w to, co im się mówi, zwłaszcza jeśli jest w oficjalnym otoczeniu. Możesz dosłownie uzyskać dostęp do danych pracowników z dowolnego miejsca w tych dniach, dzięki serwisom społecznościowym i stronom internetowym firmy. Haker może podszyć się pod pracownika z działu IT firmy, zadzwonić do użytkownika i poinformować go o pewnych problemach technicznych w systemie e-mail. Haker następnie prosi, aby użytkownik podał im swoje hasło, aby rozwiązać problem.

4. Ataki słownikowe - w tym miejscu program służy do tworzenia listy słów słownika tekstowego, które można porównać z rzeczywistym hasłem. Obejmuje to mieszanie słów w postaci zwykłego tekstu, solenie ich, a następnie porównywanie ich z hasłem użytkownika. Słowo, które pasuje, jest następnie uważane za hasło użytkownika. Programy, które mogą pomóc w uruchomieniu ataku słownikowego, to John the Ripper, LophtCrack, i Cain and Abel

5. Brute force attacks - To nigdy nie powinno być twoim pierwszym wyborem, jeśli chodzi o złamanie hasła. Jest to technika nieefektywna i niezwykle czasochłonna. Jest uważana za opcję awaryjną, która jest używana, gdy wszystkie inne metody zawiodły. Jest używany przede wszystkim do łamania haseł składających się z 6 znaków lub mniej, dlatego zawsze zaleca się, aby hasła składały się z 8 lub więcej znaków. Im więcej bohaterów wprowadza hasło, tym trudniej jest je złamać przy użyciu brutalnego ataku. Jednak atak brutalnej siły jest bardzo wyczerpujący, co oznacza, że prędzej czy później hasło zostanie złamane. Niestety, nikt nie jest w stanie przewidzieć, kiedy to nastąpi. Programy które używają tej techniki to John the Ripper, Rarcrack i Oracle. Powyższe metody są najprostszymi i najczęściej używanymi sposobami łamania haseł. Dostępne są inne podejścia, na przykład macierz prawdopodobieństwa hasła i tabele tęczowe. Jednak dla początkujących byłoby to po prostu zbyt skomplikowane, aby je tutaj opisać. Używanie programu John the Ripper i pwddump3 do złamania hasła Narzędzie pwdump3 to skuteczny sposób wyodrębniania haszowanych haseł z bazy danych Menedżera kont zabezpieczeń. John the Ripper, jak wspomniano wcześniej, może pracować zarówno z hasłami LINUX, jak i Windows. Ta procedura wymaga dostępu administracyjnego. Jeśli próbujesz złamać system Windows, wykonaj poniższą procedurę:

1. Na komputerze przejdź do napędu C. Utwórz katalog i nazwij go "password"

2. Upewnij się, że na komputerze jest zainstalowane narzędzie do dekompresji (takie jak WinZip). Jeśli nie, pobierz i zainstaluj.

3. Pobierz pwdump3 i John the Ripper i zainstaluj je natychmiast. Wyodrębnij je do katalogu, który utworzyłeś powyżej.

4. Wpisz polecenie

c: passwordspwdump3> cracked.txt

Wyjściem tego kroku będzie Menedżer kont zabezpieczeń systemu Windows hashy haseł, które następnie zostaną przechwycone w pliku .txt.

5. Wpisz polecenie

c: passwordsjohn craked.txt

Spowoduje to uruchomienie programu John the Ripper z hashami hasłowymi, a wynikiem będzie złamanie hasła użytkownika. Jednak proces ten może zająć bardzo dużo czasu, w zależności od tego, jak złożone są hasła i od liczby użytkowników w systemie. Jeśli łamiesz system LINUX, wykonaj poniższą procedurę:

1. Pobierz pliki źródłowe dla LINUX.

2. Wpisz polecenie

[root @ local host yourcurrentfilename] #tar - zxf john - 1.7.9.tar.gz

Spowoduje to wyodrębnienie programu i utworzenie katalogu / src.

3. W katalogu / src wpisz polecenie

Make generic

4. W katalogu / uruchom wpisz polecenie

. / unshadow / etc / passwd / etc / shadow> cracked.txt

Program unshadow zostanie użyty do scalenia plików shadow i hasła i wprowadź je do pliku .txt.

5. Wpisz polecenie:

. / john cracked.txt

Spowoduje to uruchomienie procesu pękania, co może również zająć trochę czasu. Dane wyjściowe powinny być takie same, jak w procedurze systemu Windows.

Tworzenie bezpiecznych haseł

Jeśli chodzi o wzmocnienie bezpieczeństwa danych w organizacji, konieczne staje się zatrudnienie Białego Kapelusza, aby pomóc w tworzeniu lepszych zasad haseł. Celem jest nauczenie użytkowników systemu, jak tworzyć bezpieczniejsze hasła, a także skutki słabego zabezpieczenia hasłem. W przypadku osób, które chcą zabezpieczyć swoje dane osobowe, w większości przypadków można zastosować te same techniki. Kryteria, których należy przestrzegać, obejmują:

- Tworzenie haseł, które łączą wielkie i małe litery, cyfry, symbole i znaki specjalne.
- Dodawanie znaków interpunkcyjnych pomiędzy oddzielnymi słowami
- Świadome błędy ortograficzne

- Zmieniając słowa co sześć do 12 miesięcy. W przypadku naruszenia bezpieczeństwa wszystkie hasła mają zostać zmienione.
- Zapewnienie, że hasła mają różną długość, aby utrudnić pękanie.
- Przechowywanie wszystkich haseł w programie do zarządzania hasłami zamiast niezabezpieczonego pliku MS Excel, Access lub Word.
- Unikanie tendencji do recyklingu starych haseł.
- Zapewnienie, że hasła nie są w ogóle udostępniane, nawet z przyjaciółmi lub współpracownikami.
- Blokowanie systemu BIOS za pomocą hasła
- Ustanawianie bardziej zaawansowanych metod uwierzytelniania, na przykład certyfikatów cyfrowych lub kart inteligentnych.

Aby włamać się do hasła, musisz zrozumieć, jak wygląda silne lub słabe hasło. Posiadanie odpowiedniej wiedzy o tworzeniu silnego hasła pomoże ci stać się skuteczniejszym hakerem.

Część 7: Ataki na sieci bezprzewodowe

Sieci bezprzewodowe stały się dziś tak powszechne, ale niestety są również bardzo podatne na hakowanie zagrożeń. Wynika to z faktu, że obejmują one transmisję danych za pośrednictwem częstotliwości radiowych, dzięki czemu informacje są narażone na przechwycenie. W przypadkach, gdy algorytm szyfrowania jest słaby lub przesyłane dane nie są szyfrowane, sytuacja staje się znacznie gorsza.

Ataki WLAN

Istnieje kilka sposobów na uruchomienie ataku na sieci bezprzewodowej. Obejmują one:

1. Niezamierzone skojarzenie

Zdarzają się sytuacje, w których jedna sieć bezprzewodowa pokrywa się z inną, co pozwala użytkownikowi niechcący przeskoczyć z jednej na drugą. Jeśli złośliwy haker skorzysta z tego, może zdobyć informacje zawarte w sieci, w której nigdy nie zamierzali być na pierwszym miejscu.

2. Sieci niekonwencjonalne

Są to sieci, które nie mają odpowiedniego zabezpieczenia, które jest zwykle zarezerwowane dla laptopów i punktów dostępu. Są raczej celami miękkimi dla hakerów. Są to drukarki bezprzewodowe, czytniki kodów kreskowych, urządzenia Bluetooth i podręczne urządzenia PDA.

3. Ataki Denial of Service

Ten rodzaj ataku obejmuje wysyłanie setek lub tysięcy wiadomości, poleceń lub żądań do jednego punktu dostępu. W końcu sieć jest zmuszona do awarii lub użytkownicy nie mają dostępu do sieci.

4. Ataki typu man-in-the - middle

Atak ten polega na tym, że haker używa swojego laptopa do działania jako miękki punkt dostępu, a następnie przyciąga do niego użytkowników. Haker łączy swój miękki punkt dostępu z rzeczywistym punktem dostępu za pomocą innej karty bezprzewodowej. Użytkownicy, którzy próbują dotrzeć do prawdziwego punktu dostępu, muszą przejść przez miękki punkt dostępu. Pozwala to hakerowi na pobieranie wszelkich informacji przesyłanych w sieci. Ataki typu "man-in-the-middle" są zwykle wykonywane w miejscach publicznych z bezprzewodowymi hotspotami.

5. Podszywanie się pod MAC

Najlepiej można to określić jako kradzież tożsamości komputera z uprawnieniami sieciowymi. Haker próbuje ukraść adres MAC (Media Access Control) autoryzowanego komputera, uruchamiając oprogramowanie, które "wyłapuje" go. Gdy haker znajdzie te komputery administracyjne i ich identyfikatory, korzysta z innego oprogramowania, które umożliwia im korzystanie z tych adresów MAC

Weryfikacja sieci bezprzewodowych

Większość sieci bezprzewodowych jest zabezpieczona hasłami, aby kontrolować sposób, w jaki użytkownicy uzyskują dostęp do sieci i jej używać. Dwa sposoby uwierzytelniania sieci bezprzewodowej to Wired Equivalent Privacy (WEP) i Wi-Fi Protected Access (WAP).

Wired Equivalent Privacy (WEP)

WEP oferuje tyle samo prywatności, co sieć przewodowa i szyfruje wszystkie dane przesyłane przez sieć. Jednak ze względu na liczne luki, został w dużej mierze zastąpiony przez WPA. Łamanie sieci WEP może odbywać się aktywnie lub pasywnie. Aktywne łamanie jest bardziej skuteczne, powoduje przeciążenie sieci, a zatem jest łatwiejsze do wykrycia. Z drugiej strony łamanie pasywne nie ma wpływu na obciążenie ruchem, dopóki sieć nie zostanie złamana. Narzędzia, za pomocą których można złamać sieć WEP, obejmują:

WEPCrack - to narzędzie open-source, które możesz pobrać z wepcrack.sourceforge.net.

Aircrack - To narzędzie umożliwia wykrywanie sieci i może być pobrane z aircrack-ng.org

WebDecrypt - To narzędzie wykorzystuje atak słownika do generowania kluczy WEP. Można go pobrać z wepdecrypt.sourceforge.net

Kismet - To narzędzie, które może być używane do wielu różnych celów, takich jak węszenie pakietów sieciowych, wykrywanie widocznych i niewidocznych sieci, a także identyfikowanie intruzów.

Wi-Fi Protected Access (WAP)

To uwierzytelnienie zostało zaprojektowane w celu przezwyciężenia słabości WEP. Zależy to od hasła i szyfrowania pakietów za pomocą kluczy czasowych. Jedną z słabych stron WAP jest to, że jest podatny na ataki słownikowe, jeśli używane są słabe hasła. Narzędzia do łamania zabezpieczeń WPA obejmują:

Cain and Abel - To narzędzie dekoduje pliki wykradane przez inne programy

CowPatty - To narzędzie wykorzystuje brutalną siłę taktyki, aby złamać wstępnie udostępnione klucze

Jak przeprowadzać ataki na podszywanie MAC

Jednym z najpopularniejszych sposobów zapobiegania atakom na podszywanie się pod MAC jest użycie filtrowania MAC. Filtr MAC służy do blokowania nieautoryzowanych adresów MAC przed dołączeniem do sieci bezprzewodowej, nawet jeśli użytkownik ma hasło. Jednak nie jest to skuteczny sposób na zablokowanie określonego hakera. W poniższym przykładzie dowiesz się, jak sfałszować adres MAC użytkownika , który ma uprawnienia do łączenia się z siecią. Upewnij się, że karta Wi-Fi jest w trybie monitorowania. Narzędzia, które będą używane, to Airodump-ng i Macchanger.

1. Gdy adapter jest w trybie monitorowania, wpisz polecenie

Airodump-ng-c [kanał] -bssid [adres MAC routera docelowego] -I wlan0mon

Umożliwi to wykrycie docelowej sieci bezprzewodowej. Wszyscy użytkownicy korzystający z sieci zostaną wyświetleni w wyskakującym okienku, w tym ich autoryzowane adresy MAC.

2. Wybierz jeden z tych adresów MAC, aby użyć go jako własnego adresu. Musisz jednak najpierw wyłączyć interfejs monitorowania. Wpisz polecenie

Airmon-ng zatrzymują walnomon

3. Następnie należy wyłączyć interfejs bezprzewodowy wybranego adresu MAC. Wpisz polecenie

Ifconfig wlano down

4. Teraz czas na uruchomienie oprogramowania Mcchanger. Wpisz polecenie

Macchanger -m [Nowy adres MAC] wlan0

5. Włącz interfejs bezprzewodowy wybranego adresu MAC.

Wpisz polecenie

Ifconfig wlano w górę

Pomyślnie zmieniłeś swój adres MAC na adres autoryzowanego użytkownika. Zaloguj się do sieci bezprzewodowej i sprawdź, czy możesz się z nią połączyć

Jak zabezpieczyć sieć bezprzewodową

Istnieje wiele metod, za pomocą których można zabezpieczyć sieć bezprzewodową. Każdy etyczny haker powinien znać te wskazówki, aby zapobiec atakom złośliwych hakerów na system. Obejmują one:

- Instalacja zapory ogniowej, programu antywirusowego i antyspyware. Upewnij się, że całe oprogramowanie zabezpieczające jest aktualizowane, a zapora jest włączona.
- Szyfruj swoje stacje bazowe, routery i punkty dostępowe poprzez szyfrowanie komunikacji sieciowej. Urządzenia te są produkowane z przełącznikami szyfrującymi, chociaż są one zazwyczaj wyłączane.
- Upewnij się, że włączasz funkcję szyfrowania.
- Zmień domyślne hasło routera bezprzewodowego. Upewnij się, że są długie i złożone.
- Wyłączaj sieć, gdy nie jest używana.
- Wyłącz nadawcę identyfikatora routera, w taki sposób, w jaki urządzenie nadaje swoją obecność. Nie jest to konieczne, ponieważ prawdziwi użytkownicy wiedzą już, że istnieje.

Część 8: Hakowanie smartfona

Ta częśćał omawia procedurę, którą możesz wykonać, aby włamać się do smartfona z systemem Android. Będziesz musiał pobrać specjalistyczne oprogramowanie od legalnych stron trzecich, aby proces był łatwiejszy i szybszy. Ta procedura jest całkowicie anonimowa i będziesz mógł uzyskać dostęp do wszystkich danych w telefonie celu. Jest to zdalna gra wykonywana za pośrednictwem bezpiecznego połączenia internetowego. Kroki do naśladowania:

1. Przejdź na stronę MasterLocate (MasterLocate.com), aby skorzystać z aplikacji online. Nie musisz pobierać oprogramowania na komputer lub telefon, aby z niego korzystać. Narzędzie pozwoli Ci śledzić lokalizację GPS celu w czasie rzeczywistym, monitorować ich wiadomości SMS i WhatsApp, słuchać ich połączeń i śledzić swoje konto na Facebooku.

2. Uruchom aplikację MasterLocate na swoim telefonie lub komputerze.

3. Pojawi się okno dialogowe z polem numeru komórkowego ofiary . Wprowadź tutaj numer celu. Upewnij się, że telefon celu jest w trybie online, gdy robisz ten krok.

4. W tym samym oknie dialogowym, tuż pod polem Numer telefonu ofiary, znajduje się karta Potwierdź. Po kliknięciu na niego program spróbuje nawiązać połączenie. Zaczekaj, aż pojawi się kraj docelowy.

5. Po ustanowieniu połączenia i weryfikacji przejdź do prawej strony okna dialogowego. Przejrzyj sekcję Raporty, aby wyświetlić wiadomości celu, rejestry połączeń i pliki. Jeśli chcesz pobrać coś na swoje urządzenie, kliknij opcję Eksportuj metodę. Przedstawi Ci opcje pobierania formatów, takich jak .zip i .rar. Ta metoda hakowania smartfonów jest prosta . Wszystko, co musisz zrobić, to upewnić się, że zarówno ty, jak i cel jesteście online podczas całego procesu hakerskiego. Każda przerwa w połączeniu internetowym zatrzyma ten proces. Inną sprawą jest to, że musisz znać numer telefonu ofiary, a także numer kierunkowy swojego numeru telefonu komórkowego

Hackowanie smartfona. Środki zaradcze

Dopóki telefon jest podłączony do niezabezpieczonej sieci Wi-Fi lub zawiera złośliwe oprogramowanie, jest narażony na wykorzystywanie przez hakerów. Jakie są więc środki, które można podjąć, aby zabezpieczyć smartfon przed złośliwymi hakerami?

1. Sprawdź, czy na Twoim telefonie działa niezawodny, zaufany i zaktualizowany program antywirusowy.

2. Łącz się tylko z bezpiecznym Wi-Fi podczas przeglądania Internetu, szczególnie w miejscach publicznych. Takie miejsca są najlepszym polowaniem dla hakerów na kradzież danych od niczego nie podejrzewających ofiar. Publicznego połączenia Wi-Fi nie należy używać do działań wymagających podawania danych konta bankowego, na przykład zakupów lub bankowości.

3. Unikaj tendencji do pobierania aplikacji żądających dostępu do twoich danych osobowych.

4. Upewnij się, że wszystkie oprogramowanie układowe jest stale aktualizowane, automatycznie lub ręcznie.

5. Jeśli masz jakiekolwiek wątpliwości co do źródła oprogramowania, zostaw go w spokoju. Kupuj lub pobieraj tylko ze zweryfikowanych sklepów z aplikacjami. Sprawdź, co mówią opinie, aby lepiej zrozumieć, co mówią inni, którzy go używali.

6. Zablokuj telefon za każdym razem, gdy nie jest używany. Upewnij się, że twoje hasło jest silne i zmieniaj je regularnie.

7. Jeśli otrzymujesz wiadomości tekstowe zawierające linki, nie klikaj linku, szczególnie jeśli nie znasz nadawcy. Najlepiej jest usuwać takie wiadomości spamowe, gdy tylko wejdą one do twojego telefonu. Hakerzy wysyłają wiadomości do tysięcy użytkowników telefonów, którzy twierdzą, że pochodzą z legalnych firm lub stron internetowych. Po kliknięciu łącza złośliwe oprogramowanie jest instalowane w telefonie, co umożliwia dostęp do danych.

Na całym świecie jest miliard telefonów komórkowych i jest to jeden z obszarów dla hakerów, który zapewnia najszybszy i najłatwiejszy sposób na zaatakowanie celu. Większość ludzie mają tendencję do bycia ostrożnym, gdy są na swoich komputerach, ale w jakiś sposób rzucają się na siebie, gdy przeglądają telefony. Dlatego niezwykle ważne jest, aby ludzie zachowali czujność przez cały czas.

Część 9: Wskazówki hakerskie dla początkujących

Czytasz ten tekst , ponieważ chciałeś nauczyć się podstawowych umiejętności i technik hakerskich. Czy nie byłby to wstyd, gdybyś został naruszony, albo jeszcze gorzej, zhackowany przez kolegę hakera z większym doświadczeniem? Bardzo ważne jest, abyś upewnił się, że będziesz bardzo ostrożny przy rozpoczynaniu pracy. Tak, jest to świetna zabawa, kiedy po raz pierwszy zobaczysz wyniki swojej pracy, ale musisz zrozumieć, jak manewrować i pozostać niewykrytym. Oto pięć kluczowych wskazówek, które każdy początkujący powinien przestrzegać:

1. Unikaj pułapek kupowania oprogramowania hakerskiego z przypadkowych stron internetowych. Istnieją tysiące oszustów, którzy udają, że mają oprogramowanie i narzędzia, które są "gwarantowane" do działania, ale zazwyczaj są one skonfigurowane tak, aby przyciągnąć hakerów rekrutów. Stracisz pieniądze w zamian za bezużyteczne oprogramowanie. Możesz nawet straciić własne dane osobowe. Upewnij się, że zajmujesz się wyłącznie legalnymi lub zweryfikowanymi witrynami. Wykonuj dobrze swoje badania i dowiedz się, czego używają inni hakerzy i gdzie oni je odbierają.

2. Unikaj pokusy pobierania freeware z Internetu. Dotyczy to głównie keyloggerów i koni trojańskich. Jeśli poważnie myślisz o hakowaniu, musisz być przygotowany na wydanie gotówki, aby uzyskać rzeczy, które działają. Najlepsze i najskuteczniejsze oprogramowanie nie jest bezpłatne. Bycie sknerusem i chodzenie za gratisy narazi cię na złośliwych hakerów, którzy nie zawahają się wykorzystać twojego systemu.

3. Kupując narzędzia hakerskie, spróbuj użyć bitcoinów. Istnieje kilka narzędzi, których nie chcesz śledzić, na przykład wirtualne serwery prywatne, anonimowe VPS i serwery rejestracji domen. Jeśli korzystasz z osobistej karty kredytowej, możesz narazić się na więcej niż jeden sposób, a szybka kontrola konta ujawni twoje działania hakerskie. Najlepszym posunięciem jest zawsze utrzymywanie swojej prawdziwej tożsamości oddzielnie od działań online.

4. Naucz się rozwijać swoje umiejętności. Jeśli masz doświadczenie w tworzeniu stron internetowych, musisz nauczyć się programowania. Jeśli jesteś programistą, naucz się pisania skryptów. Celem jest wiedzieć coś o wszystkim, zamiast czuć się komfortowo będąc w pudełku.

5. Na początku dobrze jest używać oprogramowania innych ludzi do przeprowadzania ataków. Jednak każdy haker, którego wartość wcześniej czy później zdobędzie sól, nauczy się pisać własne kody, programy i skrypty. Jeśli potrafisz tworzyć własne narzędzia hakerskie, przejdziesz na następny poziom, aby stać się elitarnym hakerem.

Wniosek

Zakończyliśmy długą podróż przez świat hakowania. Jeśli nie wiesz nic na ten temat, powinieneś mieć wystarczającą wiedzę, aby zacząć wykonywać małe exploity. Istnieje duży potencjał w hakowaniu i nie jest on złośliwy. Nauka skutecznego hakowania to najlepszy sposób na zachowanie bezpieczeństwa w świecie, w którym sprawdzanie poczty jest niebezpieczne, a rozmowa z tym uroczym nieznajomym może prowadzić do czegoś więcej niż oczekiwałeś (a nie w dobry sposób)! Niezależnie od tego, czy jest to urządzenie mobilne czy komputer stacjonarny, konieczna jest całkowita czujność . Złośliwi hakerzy są zawsze na wolności, więc musisz nauczyć się ich sztuczek i przeciwdziałać im. Jako przewodnik etycznego hakowania, ten tekst pokazał Ci pierwsze kroki do hakowania, a także do ochrony siebie. Kontynuuj naukę i zastosuj to, czego się tutaj nauczyłeś. Pamiętaj, aby być zabezpieczonym przez cały czas i nie przejmuj się.

Powodzenia!