Wykonywanie testów

„Nie ma tajemnic lepiej strzeżonych niż te, które wszyscy odgadują". George Bernard Shaw

Chciałbym otworzyć tą część przykładem tego, jak nie wdrażać bezpieczeństwo. Pracowałem w witrynie klienta, wykonując (niefizyczny) audyt bezpieczeństwa. Pomimo faktu, że zespół został sprawdzony i oczyszczony przed wpuszczeniem go przez drzwi (był to klient rządowy), musieliśmy przejść cztery dodatkowe godziny procedur przesiewowych. Kiedy to się skończyło, nasz sprzęt elektroniczny (w tym laptopy i telefony komórkowe) został skonfiskowany i zamknięto nas w pokoju, w którym będziemy pracować. Zablokowany, to znaczy, że potrzebujesz plakietki zbliżeniowej, aby wejść i wyjść, a my nie mieliśmy między nami. Jeśli w dowolnym momencie chcielibyśmy wyjść z pokoju (na przykład, aby skorzystać z łazienki), musieliśmy zadzwonić do naszego Punktu Kontaktowego (PoC) na telefon stacjonarny. Problem polegał na tym, że nigdy nie odpowiedział. Brzmi bezpiecznie, prawda? Źle. Problem polegał na tym, że stali członkowie otaczającego nas personelu byli przyzwyczajeni do nakładania ograniczeń na kontrahentów i dość mieli dość eskortowania gości, gdy mieli swoją pracę do wykonania. Skutkiem tego było to, że ktoś otworzyłby dla ciebie drzwi, w dowolnym miejscu i czasie, jeśli poprosisz grzecznie. Wątpię, aby klient byłby w stanie funkcjonować skutecznie, gdyby tego nie zrobił. O poranku postanowiłem wybrać się na spacer i zobaczyć, jak daleko mogę się dostać bez odznaki. Powiedzmy, że nie było mnie godzinę i przeszedłem z jednej strony budynku na drugą (pomimo wielu drzwi kodowanych zbliżeniowo). Spędziłem nawet trochę czasu omawiając pogodę ze strażnikiem. Jeśli bezpieczeństwo stanie się niewykonalne, ludzie obejdą go, ponieważ muszą. Jest to bezpośrednio porównywalne z frazesem na temat zapisywania haseł na karteczkach na widoku, ponieważ użytkownicy mają problemy ze złożoną polityką haseł. Dyski USB zostały również zakazane na miejscu, ale bez alternatywnego rozwiązania przenoszenia dużych ilości danych w środowisku niesieciowym, pracownicy i tak ich używali. W końcu nie możesz rutynowo wyszukiwać u ludzi rzeczy tak małych, jak pamięć USB. Skutkiem tego jest to, że duże ilości tajnych danych prawdopodobnie wchodzą i wychodzą z budynku każdego dnia. Bezpieczeństwo jest złożonym i efemerycznym tematem i nic nie jest tym, czym się wydaje. Ta część zaczyna mówić o praktycznych aspektach i zawiera przegląd wykonywania fizycznych testów penetracyjnych. Nie omawia szczegółowo wybierania zamków ani inżynierii społecznej. Są to specjalistyczne tematy, które mają własne części, ale ich dotykam. Nauczysz się jednak praktycznych technik, których możesz używać wielokrotnie. W szczególności mówię o technikach, które są bezpośrednio stosowane i użyteczne dla członków zespołu operacyjnego przeprowadzającego test penetracyjny. Omawiam różne paradygmaty lub podejścia stosowane przez testerów oraz ich znaczenie. Omawiam także konkretne techniki, których testerzy mogą użyć, aby obejść kontrole bezpieczeństwa, środki zaradcze i technologie. To tutaj zaczyna się zabawa. Cieszysz się?

Wspólne paradygmaty przeprowadzania testów

Ogólnie rzecz biorąc, istnieją trzy podejścia do fizycznego testowania penetracyjnego.Przegląd każdego z nich podano w poniższych sekcjach. Podczas planowania testu przydatne jest sporządzenie planu testu po wstępnych badaniach. Ten proces maksymalizuje proces twórczy i pomaga odkryć najbardziej realny plan ataku.

Cechy Jawnego Testera

Jawny tester nie próbuje ukryć swojej obecności. Nie oznacza to, że ogłosi swoje zamiary, ale stara się unikać kontroli bezpieczeństwa lub strażników i będzie działał „w systemie" w jak największym stopniu. Podczas jawnych testów polegasz w jak największym stopniu na inżynierii społecznej i wadach bezpieczeństwa ludzi. Operator kamery raczej nie zauważyłby niczego podejrzanego w stosunku do testera, ponieważ jego intencją jest stać się częścią jego środowiska. Na przykład jawny tester wszedłby

do recepcji, podał fałszywe poświadczenia i otrzymał legalną odznakę. Po naruszeniu bezpieczeństwa granic stajesz się częścią systemu i nie masz się czego obawiać. Zwykle takie testowanie wymaga wyższego stopnia wstępnego planowania i konfiguracji, aby zapewnić testerowi zaufanie. Oto przykład jawnego testu:

1. Nazwiska i funkcje personelu badawczego.

2. Ustal, kto jest na wakacjach.

3. Pojaw się na spotkanie sprzedażowe z menedżerem średniego stopnia, o którym wiesz, że jest nieobecny.

4. Zaloguj się w recepcji, zdobądź odznakę i „zadzwoń do kontaktu", zanim odbiór będzie miał okazję. Zaraz będziesz.

Jeśli strona wymaga eskorty gościa z recepcji, powyższe podejście nie zadziała, chociaż mogą zapomnieć o tobie, jeśli są zajęci, w którym to momencie stajesz się tajnym testerem.

Cechy Ukrytego Testera

Tajne testy są podobne do jawnych, z tym że operatorzy bardziej polegają na podstępach i unikaniu kontaktu z ludźmi na wysokich stanowiskach. Tajny tester nie wejdzie przez drzwi wejściowe bez wiarygodnych, podrobionych danych uwierzytelniających, takich jak przepustka, znaczek lub inne tokeny dostępu. Woli wślizgnąć się przez boczne drzwi lub skorzystać z ataków na tailgating. Ta forma testowania jest najczęściej wdrażana. Innym przykładem jest ubieranie się jako robotnik, aby wędrować bez przeszkód po obwodzie lub uzyskać dostęp do śmietników. Testowanie ukryte jest najczęstszym podejściem, ponieważ jest najbardziej elastyczne i teoretycznie najmniej ryzykowne. (Klasycznym) przykładem użycia go do wejścia na rynek jest dołączenie do grupy palaczy i śledzenie ich.

Cechy Niewidzialnego Testera

Niewidoczny tester nie kontaktuje się z żadną osobą na stronie, ale całkowicie polega na ukryciu. Z tych powodów niewidoczne testy są zwykle używane do testowania zabezpieczeń fizycznych lub automatycznych w nocy. Niewidzialne testy w dużej mierze polegają na tym, że ludzie mogą unikać strażników i kamer, mają silne umiejętności w takich obszarach, jak otwieranie zamków i nerwy ze stali. Niebezpieczeństwo związane z niewidzialnymi testami polega na tym, że jeśli zostanie złapany, tester zostanie potraktowany jako wrogo nastawiony przez personel ochrony i jest mało prawdopodobne, aby miał taką samą szansę na wyjaśnienie siebie jak ktoś ubrany w garnitur w chłodnym świetle dnia. Niewidoczne testy najlepiej sprawdzają się w nocy, gdy atak w godzinach pracy jest niepraktyczny.

Przeprowadzanie eksploracji witryny

Bez względu na to, jak uzyskasz dostęp do obiektu docelowego, pamiętaj, aby nie przekroczyć terminu powitania. Ryzyko przyłapania staje się wykładniczo wyższe, im dłużej przebywasz na miejscu. Nie oznacza to, że powinieneś się spieszyć. Pośpiech jest równie ryzykowny, ale powinieneś mieć przemyślany i elastyczny plan i z góry wiedzieć, czego szukasz. Czasami nie jest to możliwe lub zasady zaangażowania są celowo niejasne i musisz przeprowadzić małą eksplorację. Tester penetracyjny może zainteresować następujące obszary.

Odbiór (nie jest zabezpieczeniem)

Czasami wydaje się, że chodzi o odbiór. Celem odbioru nie jest bezpieczeństwo; to bardzo drugorzędna funkcja. Główną funkcją recepcji jest powitanie gości i pokazanie twarzy w budynku. To, kto zobaczy tę

twarz, zależy całkowicie od charakteru firmy, ale zazwyczaj obejmuje to klientów, sprzedawców, kontrahentów i dostawców. Oczywiste jest, że grupy te są traktowane na bardzo różne sposoby. Z mojego doświadczenia wynika, że nie ma nic bardziej niebezpiecznego dla firmy niż połączenie funkcji spotkania i powitania z bezpieczeństwem. Są to zupełnie różne rzeczy i nie są wzajemnie kompatybilne. Na przykład wielokrotnie widziałem, że protokoły bezpieczeństwa były zaniedbywane, gdy recepcjonista bał się urazić gościa VIP (jak im się wydawało). Nie oznacza to, że recepcja nie powinna rejestrować gości ani wydawać tymczasowych odznak, ale wszyscy odwiedzający firmę powinni zostać wcześniej poinformowani o bezpieczeństwie, a dowód tożsamości (paszport lub prawo jazdy) należy sprawdzić po przyjeździe. Odwiedzający, których nie ma na liście, nie powinni być wpuszczani. Innym niebezpieczeństwem centralizacji bezpieczeństwa wokół recepcji jest to, że stwarza iluzję, że nie ma innych punktów wejścia. Jak już widzieliśmy, po prostu tak nie jest.

Konfigurowanie w salach konferencyjnych

Sale konferencyjne są moim ulubionym miejscem podczas przeprowadzania testów etycznego hakowania, ponieważ na ogół gwarantują, że pozostaniesz sam na kilka godzin. Sale konferencyjne często można rezerwować przez recepcję, ale najlepiej spróbować szczęścia. W większości przypadków najgorsze, co się stanie, to to, że ktoś szturchnie zirytowaną głowę wokół drzwi i twierdzi, że zarezerwował ten pokój na ten czas. Nie kłóć się, po prostu powiedz, że nie widziałeś ile czasu minęło i właśnie kończysz, a następnie przenieś się do innego pokoju.

Odkrywanie wyższych biur sztabowych

Nic nie przywodzi na myśl poważnego bezpieczeństwa fizycznego wyższej kadry kierowniczej, tak jak w przypadku naruszenia biura. Czasami zasób w teście penetracyjnym nie jest czymś fizycznym, ale dostępem do osoby. Tego rodzaju testy są przeprowadzane w celu określenia narażenia kierownictwa na zagrożenia zewnętrzne, które mogą obejmować atak fizyczny niezadowolonych osób, a także podsłuchiwanie ich biur przez dziennikarzy lub szpiegów korporacyjnych. W nocy biura te są zazwyczaj dostępne za pomocą klasycznych technik otwierania zamków. W ciągu dnia jest mało prawdopodobne, że zostaną w ogóle zamknięte; oczywiście, jeśli docelowym zasobem jest osoba fizyczna, nie ma to znaczenia.

Naruszenie serwerowni

Serwerownia jest jednym z najbezpieczniejszych obszarów w każdej organizacji, a jej naruszenie jest celem wielu testów penetracji fizycznej. Duża organizacja prawdopodobnie będzie mieć więcej niż jedną serwerownię i na pewno będzie miała infrastrukturę sieciową, taką jak routery i przełączniki na każdym piętrze. Uzyskanie bezpośredniego fizycznego dostępu do serwerów oznacza, że można ominąć wiele mechanizmów bezpieczeństwa, takich jak zapory ogniowe i systemy wykrywania włamań. Samo pokazanie, że można uzyskać dostęp do serwerowni bez uprawnień, jest niezwykle poważnym problemem bezpieczeństwa. Jest mało prawdopodobne, że jakikolwiek podłączony token zbliżeniowy zapewni ci dostęp do serwerowni. Połączenie tailgating i inżynierii społecznej to twoja najlepsza broń.

Dostęp do przestrzeni magazynowej i magazynu

Magazyn - jeśli taki istnieje - jest najbardziej prawdopodobnym celem dla złodziei, a zatem doskonałym celem do testu penetracyjnego. Magazyny mają więcej niż jedno wejście. Zwykle istnieje pewien stopień bezpieczeństwa regulujący, kto może wejść do nich ze świata zewnętrznego. Jednak wejścia istnieją również z biur i nikogo, kto wejdzie stamtąd, nie można uznać za podejrzane.

Szpiegowanie w posterunkach straży

Stanowiska strażnicze, pokoje lub kabiny mogą być interesującym celem dla nieustraszonego testera. Są doskonałym źródłem tokenów bezpieczeństwa i informacji dla personelu. Zgodnie z polityką bezpieczeństwa pokój warty nigdy nie jest pozostawiony niezajęty, chyba że jest zamknięty, ale będziesz zaskoczony, jak często te zasady nie są przestrzegane. Nawet jeśli drzwi do biura są zamknięte, często można sięgnąć przez okno bezpieczeństwa i chwycić klucze, przepustki itp. Możesz użyć wielu testerów i rozproszyć uwagę, aby zmusić strażnika do opuszczenia kabiny, zapewniając ci kilka chwil nieprzerwany dostęp. Wykazanie praktycznych ataków na rdzeń bezpieczeństwa witryny jest odkrywcze i stanowi doskonały raport.

Przykładowe podejścia taktyczne

Są to specyficzne podejścia, w których uważam, że są bardzo skuteczne w większość okoliczności. Pewność siebie jest potężnym czynnikiem w każdej sytuacji testowej i absolutnie niezbędna do Twojego sukcesu. To banał, ale jeśli wierzysz w siebie i wybraną przez siebie osobę, inni też.

Tailgating, aby uzyskać wejście

Tailgating to atak, którego można użyć w dowolnym środowisku korzystającym z kontroli drzwi zbliżeniowych. Zasadniczo koncepcja jest dość prosta, ale w praktyce wymaga pomyślnego wykonania. Ty (lub intruz) nie jesteś w stanie otworzyć zamków drzwi zbliżeniowych bez aktywowanego tokena. Aby temu zaradzić, zaczekaj, aż legalny posiadacz przepustki otworzy drzwi, a następnie prześlizgnij się za nimi. Ważne jest, aby robić to w sposób, który nie wzbudza podejrzeń. Klasycznym podejściem jest „rozmowa" na telefonie komórkowym przy drzwiach i zakończenie połączenia, gdy ktoś przechodzi przez korytarz i otwiera go. Następnie podążaj za nimi. Sprawiać wrażenie, jakbyś właśnie wyszedł, aby odebrać lub odebrać telefon, który właśnie zakończyłeś i wracasz do środka. Nie nawiązuj kontaktu wzrokowego, jeśli to możliwe, i wydaj się zajęty, sfrustrowany lub ogólnie zirytowany. Są to naturalne emocje w większości środowisk korporacyjnych i twój znak będzie wiedział lepiej niż rzucać ci wyzwanie, chociaż przez większość czasu nawet cię nie zauważy. To kończy spraw,e. Bądź jednak ostrożny. Chociaż jest to świetna technika naruszania bezpieczeństwa granic - szczególnie w drugim punkcie wejścia - powinieneś unikać podążania tą samą osobą przez wiele drzwi, chyba że chcesz sprawić, by poczuł się nieswojo, a tym samym zwrócić na siebie uwagę. Nie angażuj w rozmowę osób, do których chcesz kierować. Możesz przyciągać trudne pytania. W każdym razie jest to technika, której nie będziesz musiał używać więcej niż dwa razy w większości witryn, jeśli wykonasz ją poprawnie. Warto jednak zrobić jeszcze więcej, jeśli chodzi o wiarygodność: zdobądź token zbliżeniowy identyczny z tym używanym na docelową stronę i miej ją w ręku, gdy podążasz za swoim znakiem.

Ubrania Maketh the Man

To fakt, że ludzie będą cię oceniać po twoim wyglądzie. W teście penetracji fizycznej jest to dokładnie to, co chcesz, aby zrobili. Do testu można zaadaptować kilka osób (lub „glamour") - szczególnie jeśli jest on przeprowadzany etapami - ale nigdy nie lekceważ potrzeby zwracania uwagi na szczegóły. Właściwe logo, styl znaczek, posiadacz karty identyfikacyjnej, przepustka itp. zrobią różnicę, dlatego ryzykuję powtórzenie badań. Na przykład, jeśli wszyscy robotnicy na miejscu mają pomarańczowe, dobrze widoczne kurtki, a twój jest zielony z logo innego wykonawcy, pracownicy generalni mogą tego nie zauważyć, ale robotnicy na pewno to zauważą. Zastanów się, gdzie i dlaczego przykłady poniżej mogą być przydatne.

Biznesmen: garnitur w paski, wyrazisty wygląd, skórzana teczka lub torba na laptopa

Chłopiec dostarczający pizzę: Upokarzający strój, motorower, duże kartonowe pudełko

Kurier: Rower i powiązany sprzęt, skrzynia kurierska

Facet dostarczający wodę: niebieski kombinezon, baniak z wodą

Robotnik: Odzież dobrze widoczna, kask ochronny

W jaki sposób można wykorzystać każdą z tych osób, aby uzyskać dostęp do placówki korporacyjnej? Kurier jest jednym z moich ulubionych. Kurierzy są praktycznie niewidoczni; przychodzą i odchodzą cały czas w urzędach miejskich; nikt nie rzuca im drugiego spojrzenia. Ponadto pracownicy są przyzwyczajeni do przepuszczania ich przez drzwi bez zastanowienia. Pod wieloma względami jest to idealne przebranie. Połącz go z garniturem i kutą plakietką ukrytą w skrzynce kuriera i szybką wycieczką do łazienki. To prawie jak klucz główny do dowolnego obiektu korporacyjnego. Wszelkie ubrania potrzebne do udoskonalenia tych strojów można łatwo nabyć online. Logo można wykonać na komputerze, wydrukować na papierze transferowym i wyprasować na dowolnej powierzchni, od tkaniny po plastik.

Odwiedziny nieistniejącego pracownika

Jedną sztuczką, która sprawdza się w dużej firmie, jest „nieistniejący pracownik". Założeniem jest to, że rotacja pracowników jest często dość wysoka, a ludzie poruszają się również w obrębie firmy. W rezultacie bazy danych personelu i listy telefonów nigdy nie są całkowicie aktualne. Jeśli poprosisz o pracownika, który nie istnieje w recepcji lub w biurze ochrony (w zależności od tego, gdzie jesteś), to oczywiście nie będzie go można znaleźć w podanych źródłach. Można by pomyśleć, że wzbudzi to podejrzenia, ale tak naprawdę nie dzieje się tak z powodów już podanych. Ponieważ pracownicy recepcji również przychodzą i odchodzą, nie ma możliwości, aby byli świadomi każdego pracownika w firmie. Po pięciu minutach niecierpliwego oczekiwania po prostu powiedz im, że masz dane kontaktowe w telefonie komórkowym i zadzwonisz do nich. Strażnicy lub pracownicy recepcji będą prawdopodobnie wdzięczni, ponieważ do tego czasu za tobą utworzy się kolejka. Udawaj, że rozmawiasz przez telefon, podnieś kciuki do strażnika, a wszyscy jesteście przygotowani na dobry atak z tailgating, gdy goście za tobą w kolejce są przetwarzani. Prawdopodobnie będziesz musiał zalogować się jako stały gość, ale możesz otrzymać przepustkę, gdy tylko to zrobisz. Większość przyjęć będzie gotowa, zanim zadzwonią do twojego gospodarza. W każdym razie zapomną o tobie, gdy tylko znikniesz z pola widzenia.

Studium przypadku - dostawca

Kris był pracownikiem Fountain Express, małego lokalnego zespołu, który specjalizował się w dostarczaniu wody butelkowanej firmom w mieście. Fakt, że Fountain Express nie istniał poza Photoshopem na jego laptopie, miał charakter akademicki. Spojrzał na tę część swojego niebieskiego kombinezonu i czapki ozdobionych logo swojego nowego „pracodawcy". Wszedł do głównego holu, pchając wózek wypełniony chłodnymi butelkami i skierował się do recepcji. Nie musiał zbyt często sprawdzać swojego otoczenia, ponieważ już wiedział, gdzie są strażnicy i kamery, a w każdym razie zajęty, zajęty, woda do dostarczenia! Kris zastukał kilka razy w recepcji, zarabiając gniew dziewczyny, która nie rozpoznała go natychmiast. „Ach, no cóż", pomyślał, „kiedy jesteś zajęty złością, nie jesteś podejrzliwy." „Dostawa na piętro piąte", powiedział głośno. „Która firma?", Odpowiedziała. „Unicorn Systems", powiedział Kris, sumiennie sprawdzając swój schowek. Dziewczyna (Mandy według jej imienia) wskazała drzwi na końcu korytarza. „Strażnik cię przepuści". „Dzięki!", Odpowiedział i to miał na myśli

Mechanizmy bezpieczeństwa fizycznego

W tej sekcji omówiono technologie powszechnie stosowane w celu powstrzymania intruzów i szczegółowo opisano ich słabości. Omówione tutaj środki bezpieczeństwa obejmują:

• odznaki i tokeny dostępu;

• strażnicy;

• aparaty fotograficzne;

• fizyczna kontrola dostępu.

Po zrozumieniu, o co ci chodzi, o wiele łatwiej jest zademonstrować, jak tę wiedzę można wykorzystać w procesie testowania lub wzmocnić własne praktyki bezpieczeństwa.

Odznaki

Identyfikatory wydawane są pracownikom podczas rejestracji lub wręczane odwiedzającym po zalogowaniu się w recepcji. Celem odznaki jest identyfikacja (i rozróżnienie) personelu i gości oraz teoretycznie natychmiastowe wykrycie intruza. Przyjmują jedną z następujących form:

• Proste identyfikatory - Te identyfikatory zapewniają jedynie podstawowy identyfikator. Wyświetlają zdjęcia i niektóre informacje dla pracowników, takie jak nazwisko, dział i stanowisko. Przepustki te nie zawierają elementów elektronicznych ani układów scalonych.

• Tokeny zbliżeniowe - same tokeny mogą być puste, w takim przypadku pracownicy będą mieli inną formę dowodu tożsamości. Jednak identyfikatory często zawierają token zbliżeniowy. Token zbliżeniowy służy do otwierania drzwi, gdy przepustka jest trzymana blisko czytnika. Są pasywne, to znaczy nie mają własnego źródła zasilania i aktywują się tylko wtedy, gdy znajdują się w pobliżu czytnika (stąd nazwa). Oprócz podstawowych zabezpieczeń urządzenia te mają dwie zalety:

• Różne poziomy dostępu w całym budynku mogą być przyznane różnym pracownikom po prostu poprzez zmianę flag w centralnej bazie danych.

• Personel może być monitorowany, aby można było wiedzieć, gdzie się znajduje (i co ważniejsze) gdzie był. Czasami takie urządzenia są inteligentne: nie pozwalają na szybkie otwarcie tych samych drzwi, aby zapobiec udostępnianiu tokenów, ale w większości przypadków nie dzieje się tak z powodu różnych praktycznych problemów we wdrażaniu.

• Odznaki z kodem kreskowym - jest to bardzo proste rozszerzenie przepustki identyfikacyjnej, do której dodano kod kreskowy w celu kontroli dostępu. Oczywiście są one łatwe do skopiowania. Witryny korzystające z takich przepustek prawdopodobnie będą miały czytniki tylko na granicy bezpieczeństwa ze względu na niedogodności związane z fizycznym przeciągnięciem przepustki przez czytnik optyczny. Jednak wrażliwe obszary w budynku prawdopodobnie będą dalej chronione za pomocą drzwi kodowanych zbliżeniowo. Jedną z zalet tego systemu jest to, że kody kreskowe są szybkie i tanie w drukowaniu, co czyni je idealnym rozwiązaniem, gdy witryna ma wielu odwiedzających, którzy muszą otrzymać jakąś formę kontroli dostępu. Często można je znaleźć we wspólnych pomieszczeniach, gdzie centralna recepcja wydaje plakietkę z kodem kreskowym, aby uzyskać dostęp do wind, a indywidualne przyjęcia wydają wszelkie dalsze niezbędne przepustki.

• Tymczasowe lub wejściówki dla odwiedzających - gdy ktoś odwiedza witrynę, zwykle otrzymuje tymczasowe hasło. Może to należeć do dowolnej z wcześniej omawianych kategorii, chociaż zwykle jest to zwykły kawałek tektury z napisem, nazwą firmy i napisem „V” lub „Gość”. Niektóre firmy przechowują zapas kart zbliżeniowych o z góry określonym poziomie dostępu odpowiednim dla gości. Jest to konieczne w witrynach, które intensywnie korzystają z technologii zbliżeniowej, ponieważ alternatywą jest wszędzie eskortowanie gości. To, która przepustka zostanie wydana, może również zależeć od poziomu zaufania udzielonego przez firmę przyjmującą lub poziomu poświadczenia

bezpieczeństwa posiadanego przez gościa. Podczas sprawdzania przepustek zwracaj szczególną uwagę na szczegóły, takie jak cyfry, litery lub kolory, które mogą określać poziom dostępu przyznany danej osobie. Możesz także zobaczyć oznaczenia, takie jak „Wymagana eskorta" lub „Nieudane".

Ominięcie zabezpieczeń odznak

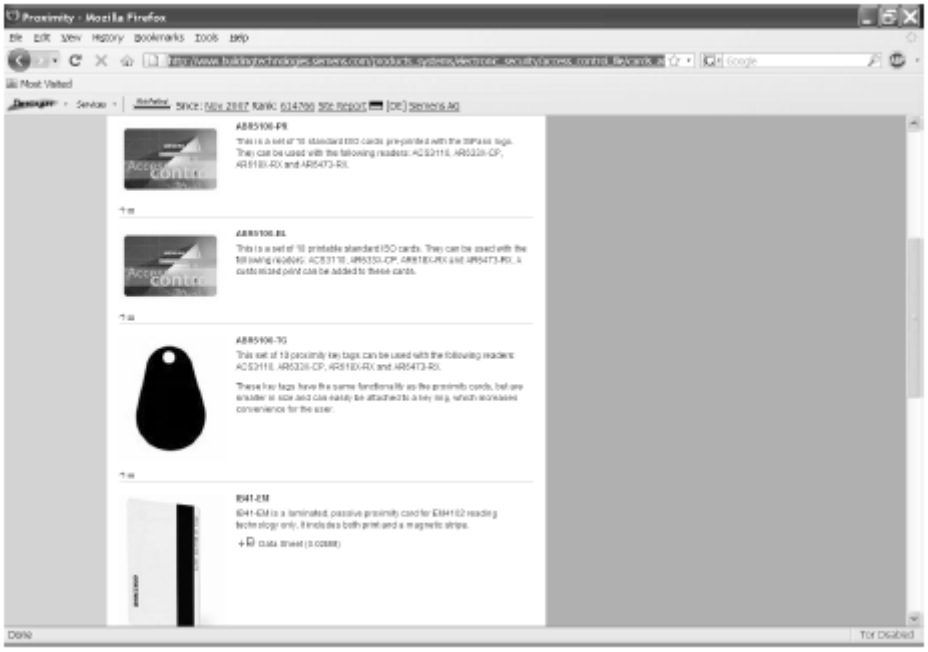
W witrynie, która obsługuje kontrolę odznak w ramach swoich zasad bezpieczeństwa, wszyscy pracownicy, kontrahenci i goście są zobowiązani do otwartego pokazywania swoich odznak przez cały czas. Polityka bezpieczeństwa będzie również stwierdzać, że każdy, kto nie nosi odznaki, powinien zostać zakwestionowany. Z mojego długoletniego doświadczenia w doradztwie w zakresie bezpieczeństwa na wielu różnych stronach, tylko raz zostałem wezwany za to, że nie nosiłem identyfikatora. Kiedy odwiedzam klienta i nie przeprowadzam testów penetracyjnych, tj. kiedy otrzymałem odznakę zgodnie z prawem, staram się nosić ją w kurtce lub na pasku, gdzie jest tylko częściowo widoczna. Niektóre odznaki są wydawane na smyczach do noszenia na szyi i nikt nigdy nie rzucił mi wyzwania, że mam to w niewłaściwy sposób (smycze zawsze wydają się powodować, że odznaka jest skierowana w niewłaściwy sposób), aby szczegóły nie były widoczne. Jest to ciekawe, choć przydatne i istnieją dwa powody, dla których występuje. Personel uzna, że jeśli tam jesteś, to powinieneś tam być. Możliwość, że jesteś intruzem, jest zwykle ostatnią rzeczą, jaka przyjdzie im do głowy. Ludzie są z natury niekonfrontacyjni: większość ludzi zrobi wszystko, aby uniknąć konfrontacji.

Jeśli przedstawisz się jako pełnoprawny pracownik ze wszystkimi niezbędnymi urządzeniami peryferyjnymi (tj. czysty garnitur i laptop lub kombinezon roboczy i kask), to jedynym powodem, dla którego ludzie będą cię podejrzewać, jest to, że robisz wszystko, aby dać im powód. Ludzie zauważą, że nie nosisz znaczka znacznie chętniej, niż zauważą, że nie jest to właściwa odznaka. Jeśli sfałszujesz identyfikator, jeśli możesz wyprodukować coś, co przejdzie pomyślnie, to jesteś w połowie drogi. Ile razy patrzysz uważnie na odznaki, które noszą inni ludzie? Podczas wstępnych badań powinieneś być w stanie określić, co najmniej z grubsza, jak wyglądają docelowe odznaki, a zatem czego potrzebujesz, aby móc się powielić.

Wykonywanie przepustek

Zasadniczo przepustki dla gości to wydrukowana karta lub papier włożone do plastikowej torebki, podczas gdy odznaki personelu są wykonane z plastiku i włożone w twardą plastikową osłonę. Możesz łatwo uzyskać odpowiednie posiadanie przepustek online, choć zazwyczaj tylko luzem. To decyduje o tym, którą trasę wybrać. Przepustki dla gości są łatwiejsze do sfałszowania, ale przepustka dla personelu zapewnia większą swobodę i zachęca do mniejszej liczby pytań. Dzięki nowoczesnemu oprogramowaniu do obróbki zdjęć i drukarkom tworzenie fałszywych identyfikatorów jest dość proste. Bardzo przydatny jest również laminator. Dobrym pomysłem jest posiadanie planu awaryjnego na wypadek, gdybyś został zatrzymany i zakwestionowany. Przygotuj wizytówki pasujące do Twojej przepustki i opatrzone odpowiednią nazwą, firmą i logo. Firmowy numer telefonu na wizytówkach powinien być bezpośrednią linią do inżyniera społecznego, koordynatora lub lidera zespołu z powrotem w centrali. Większość toreb na laptopa ma na zewnątrz uchwyt na wizytówkę, więc używaj go; trzymanie „id" na widoku w ten sposób wzmacnia Twój wizerunek wiarygodności, podobnie jak noszenie innych przedmiotów, takich jak folder biznesowy z wytłoczonym logo firmy. Jeśli kontrola dostępu jest regulowana po prostu za pomocą mechanizmu kodów kreskowych, wówczas należy starać się powielić kod kreskowy lub wypracować kodowanie. Oprogramowanie do kodowania, dekodowania i drukowania kodów kreskowych jest dostępne bezpłatnie online. W ten sposób można z pewnością ominąć bezpieczeństwo. Twoje wstępne badania powinny dostarczyć ci surowca do pracy. Witryny używające kodów kreskowych mają czytniki tylko przed wejściem do strony głównej. Jeśli możesz to ominąć, wtedy stary kod kreskowy zrobi to, co oczywiście, będzie tylko dla wyglądu. Odznaki

zawierające elektroniczne środki kontroli dostępu są najtrudniejsze do odtworzenia. Ponieważ nie wszystkie formy technologii zbliżeniowych są sobie równe, możliwe jest powielanie odznak, ale często jest to zbyt drogie. Twoje wstępne badania, jeśli zostaną dobrze przeprowadzone, dostarczą informacji o tym, z których dostawców firma korzystała. Umożliwia to ustalenie, czy istnieją jakieś znane słabości technologii. Szybkie wyszukiwanie Google w „bliskości kluczy" zwraca stronę pokazaną na rysunku



ze strony internetowej Siemens. Ta strona informuje sprzedawcę i czytelników, którzy pracują z tymi tokenami. Jest to brelok zbliżeniowy Siemens SiPass (numer seryjny ABR5100-TG) i współpracuje z kilkoma czytnikami z zakresu SiPass (ACS3110, AR633X-CP, AR618X-RX i AR6473-RX). Według strony internetowej te breloki do kluczy mają wszystkie funkcje kart zbliżeniowych SiPass.

System działa w ten sposób. Każdy token ma indywidualny numeryczny identyfikator, który jest przechowywany na breloku (jest również wydrukowany na zewnętrznej stronie breloka). Podczas rejestracji numer ten jest przypisywany do osoby, a jej poziom dostępu jest wprowadzany do komputera. Inną przydatną rzeczą, na którą należy zwrócić uwagę, jest to, że jest zdolny do alarmowania, co oznacza, że gdy system SiPass wykryje alarm pożarowy, na przykład, wyłącza system bezpieczeństwa i otwiera drzwi. Bez wchodzenia w skomplikowane techniki klonowania kart masz już dwie możliwości ataku. Pierwszy to atak socjotechniczny przeciwko administratorowi bazy danych kart, aby dodać numer posiadanego tokena, a drugi jest o wiele prostszy - alarm pożarowy. Pamiętaj, że Siemens nie zastąpi zagubionych tokenów. Konieczne jest aktywowanie nowego numeru i wygaśnięcie starego. Posiadanie breloczka lub karty zbliżeniowej identycznych z tymi używanymi na miejscu w twoim posiadaniu (nawet jeśli nie są aktywowane) znacznie poprawią Twój sukces w atakach typu tailgating. Niezależnie od tego, którą drogą wybierzesz z fałszywymi przepustkami , najprawdopodobniej będziesz mieć plakietkę bez elementów elektronicznych, a zatem nie będziesz mógł otworzyć zamków zbliżeniowych. W takim przypadku musisz skorzystać z pewnej formy inżynierii społecznej, aby inni mogli otworzyć dla ciebie drzwi.

Słabości systemu MIFARE

W tej sekcji omówiono jedną formę elektronicznej kontroli dostępu, zwaną MIFARE Classic (lub Standard), wykonaną przez holenderską firmę półprzewodnikową NXP (spin-off firmy Philips). Karta

jest używana do wielu celów, w tym do bezpieczeństwa witryny i przedpłaconego dostępu do systemów tranzytowych na całym świecie, w tym systemu kart Oyster w londyńskim metrze (LU). Niedawno wykazano, że ma znaczące słabości, pozwalające atakującym klonować karty, zwiększać kredyty i omijać zabezpieczenia. MIFARE jest zasadniczo urządzeniem do przechowywania w pamięci, które jest bardzo tanie w produkcji (stąd jego popularność). W 2007 r. dwóch niemieckich badaczy bezpieczeństwa, Henry Plock i Karsten Nohl, wygłosili w Berlinie prezentację, w której zasugerowali, że technologia jest wyjątkowo niepewna w oparciu o własną częściową inżynierię wsteczną. Teorię tę wdrożyła w 2008 r. grupa badawcza z Uniwersytetu Radboud w Nijmegen w Holandii. Wykazali, że można klonować i manipulować zawartością karty. Szczególnie niepokojące było to, że szyfrowanie używane przez karty (nazwane Crypto-1) mogło zostać złamane w około 12 sekund. NXP potraktował to badanie poważnie i próbował (bezskutecznie) zablokować jego publikację. Po opublikowaniu tych badań wyciekły dokumenty z LU, które pokazały, że zostały ostrzeżone w nieokreślony sposób, że MIFARE Classic nie nadaje się do przyjęcia w projekcie Oyster, i wezwały do przyjęcia jednej z innych technologii, ale LU zdecydowała się pójść i tak dalej. W zakresie bezpieczeństwa pycha jest zwykle surowo karana. Sprzęt do klonowania kart MIFARE Classic już zaczyna krążyć w Internecie oraz w podziemnym komputerze.

Obejście prewencyjnych kontroli bezpieczeństwa

Prewencyjne kontrole bezpieczeństwa to takie, które działają raczej jako środek odstraszający niż fizyczna bariera. Słabość polega na tym, że jeśli intruza nie zniechęca, kontrole zapobiegawcze zapewniają niewielkie lub żadne bezpieczeństwo. Podstawa odstraszania w obiekcie korporacyjnym jest dokładnie taka sama, jak na ulicach: umundurowana obecność i kamery. Wady tej kontroli bezpieczeństwa są przedmiotem tej sekcji.

Praca wokół strażników

Można by pomyśleć, że obecność strażników tylko zwiększyłaby ogólne bezpieczeństwo, ale myliłbyś się. Strażnicy wprowadzają element kontroli dostępu, który możesz wykorzystać w sposób, który nie może być wykorzystany w formie elektronicznej. Strażnicy pracują przez wiele godzin za niskie wynagrodzenie i są przyzwyczajeni do tego, że są traktowani z góry. Zwykle mają dość łatwą, choć nieciekawą pracę. Strażnik przy wejściu widzi setki ludzi przychodzących i odchodzących każdego dnia, a jego obecność ma charakter zapobiegawczy, co oznacza, że działa odstraszająco. Jest jednak niewiele więcej niż chwalebnym portierem. Strażnicy rozmieszczeni przy wejściach są tam z kilku powodów:

• w celu sprawdzenia identyfikatorów;

• wpuszczać ludzi;

• dopilnować, aby nikt oczywiście niepożądany nie błąkał się po ulicy;

• zapewnienie pomocy odwiedzającym i personelowi w przypadku awarii czytnika;

• zapewnienie poczucia bezpieczeństwa z korzyścią dla personelu;

• w celu powstrzymania potencjalnych intruzów.

W niektórych witrynach, w których czytniki kart nie są używane, strażnicy są jedynym punktem kontroli dostępu do weryfikacji odznak i przepustek. Chociaż staje się to coraz rzadsze, warto rozważyć: czy jest to coś, za co chciałbyś być odpowiedzialny? Do przepustek, które opierają się wyłącznie na wizualnym potwierdzeniu, czasami dołączane są dodatkowe środki bezpieczeństwa - na przykład naklejka holograficzna - ale dla wszystkich z wyjątkiem najbardziej bezpiecznych witryn można założyć, że przepustki dla odwiedzających tego nie będą. Strażnicy mogą być niezwykle pomocni dla testera. Są

zaznajomieni z układem budynku i zwykle udzielają wskazówek i innej pomocy. Jak zobaczysz później, ludzie reagują pozytywnie, gdy podchodzą do nich w sposób odpowiedni do ich indywidualnego sposobu myślenia. Strażnicy, jak większość ludzi, chcą czuć się ważni, a kiedy są traktowani jako tacy przez profesjonalistów w garniturach, zwykle stają się wyjątkowo przychylni. Strażnicy są również szkoleni i oczekuje się, że będą uprzejmi i pomocni dla gości. Istnieją historie o ochroniarzach pomagających złodziejom w ładowaniu łupów do samochodów dostawczych. Nie wiem, czy to prawda, ale nie zaskoczyłoby mnie to. Mój szczególnie zuchwały kolega wkroczył kiedyś na miejsce docelowe w stroju ochroniarza. Po zbadaniu, która firma zewnętrzna była używana, nabył odpowiedni mundur, a następnie zwolnił strażnika dyżurnego i odesłał go do domu. To jest bardzo stylowe, ale bardzo ryzykowne podejście.

Radzenie sobie z aparatami

Aparaty są często traktowane jako panaceum bezpieczeństwa, ale tak naprawdę przez większość czasu mają charakter odstraszający. Oczywiście są wyjątki. Kamera może zostać użyta do zidentyfikowania kogoś na granicy bezpieczeństwa lub może być zamocowana w miejscu i monitorować bramkę obrotową. Jednak po wejściu do witryny docelowej, szczególnie dużych witryn, większość kamer nie jest monitorowana. Po prostu nagrywają. Analiza dziesiątek różnych kanałów nie jest opłacalna - potrzebowałby dużego personelu zaangażowanego w bieżący nadzór. Nawet jeśli masz personel, spróbuj obserwować transmisje z kamery przez cztery godziny z rzędu, a zobaczysz, co mam na myśli; wystarczy kilka minut nieuwagi, aby umożliwić naruszenie bezpieczeństwa. Oczywiście atakujący nie wie, które kilka minut i na tym polega środek odstraszający, ale pamiętaj, że kanały prawdopodobnie nie będą i tak monitorowane w jakikolwiek znaczący sposób. Kamery bezpieczeństwa są w porządku do celów dowodowych, ale są bardzo nieodpowiednie dla bezpieczeństwa prewencyjnego. Załóżmy jednak, że witryna ma około 50 kamer i że są one monitorowane 24 godziny na dobę przez dedykowany personel banku monitorów, które przełączają się między kamerami co kilka sekund. Jest to z pewnością bezpieczniejsze niż kanały tylko do nagrywania, ale problemy pojawiają się, gdy analizujesz, w jaki sposób szkoleni są pracownicy monitorujący kamery. Zazwyczaj pełne szkolenie w telewizji przemysłowej (monitorowanie CCTV trwa najwyżej tydzień i obejmuje następujące obszary:

• obowiązki operatora telewizji przemysłowej;

• kodeksy postępowania;

• techniczna obsługa urządzeń CCTV;

• komunikacja i bezpieczeństwo w sterowni;

• ustawodawstwo;

• radzenie sobie z incydentami;

• techniki nadzoru CCTV;

• zdrowie i bezpieczeństwo;

• ciągły rozwój umiejętności operatora.

Większość z tych kursów nie istnieje, aby uczyć technik nadzoru jako głównego celu szkolenia, ponieważ większość miejsc wie, że monitoring CCTV jest w najlepszym wypadku odstraszający. Operatorzy kamer spędzają większość czasu na poznawaniu zdrowia i bezpieczeństwa oraz prawa. W ten sposób organizacja dołożyła należytej staranności i jest prawnie ubezpieczona, że personel monitorujący wykracza poza zakres swojej pracy. W rzeczywistości, podczas gdy operator kamery jest

przeszkolony w poszukiwaniu zachowań, które można interpretować jako podejrzane, duży nacisk kładzie się na zachowania, których należy unikać, takie jak stronnicze oglądanie na podstawie rasy lub płci. Czym jest podejrzane zachowanie? Odznaki często mają różne kolory (lub bardzo wyraźne litery lub cyfry) wskazujące na różne poziomy dostępu lub status bezpieczeństwa personelu. Jednym z powodów jest to, że jakość telewizji przemysłowej kanały z kamer zwykle nie są zbyt wysokie, a personel monitorujący czasami musi wybierać szczegóły z odznak. Tak więc niewłaściwy kolor lub litera w niewłaściwym obszarze są podejrzane, podobnie jak ktoś, kto ma eskortowaną odznakę bez eskorty. Ogólnie lista jest bardzo krótka:

• Osoba wygląda „nie na miejscu", na przykład nosząc niewłaściwą odzież lub fryzurę.

• Osoba wydaje się pozbawiona celu, wygląda na zagubioną lub wędruje.

• Osoba fizyczna nie ma lub ma nieprawidłową odznakę.

• Osoba pozostaje w jednym miejscu zbyt długo lub wydaje się, że tak jest 'przyczajony'.

• Osoba wykazuje ogólnie podejrzane zachowanie, zauważone przez personel monitorujący lub zgłoszone. To jest miejsce, w którym coś się trochę zachmurza. Niektóre zachowania są oczywiście podejrzane - na przykład przyłapanie na blokowaniu (chyba że udajesz ślusarza). Ogólnie rzecz biorąc, jest to raczej instynkt, który pracownicy monitorujący powinni podnieść.

Zakładając, że naruszyłeś bezpieczeństwo granic, powinieneś przestrzegać następujących zasad:

• Ubierz się odpowiednio do swojej roli.

• Być w posiadaniu dobrze sfałszowanych przepustek, jeśli to możliwe.

• Wyglądaj, jakbyś należał.

• Nie wędruj po okolicy. Jeśli się zgubiłeś, poproś kogoś o pomoc. Jeśli potrzebujesz przerwy lub opanowania, idź do łazienki.

• Nie daj się przyłapać na robieniu czegoś głupiego.

• Poświęć tyle czasu, ile potrzeba na prawidłowe wykonanie pracy. Pośpiech cię złapie.

Poradzenie sobie z fizyczną kontrolą dostępu

W przeciwieństwie do kontroli polegających na odstraszaniu, fizyczne kontrole dostępu są zaprojektowane tak, aby bezpośrednio utrudniać postęp intruza. Takie mechanizmy obejmują:

• bramy lub bariery;

• mantanty;

• bramki obrotowe;

• zamknięte drzwi;

• czujniki ruchu.

Żadna z tych opcji nie jest niezawodna, a pomysłowy tester zwykle może znaleźć sposób na ich obejście.

Ominięcie bramy lub bariery

W wielu miejscach, w których stosuje się systemy kart zbliżeniowych, brama lub bariera zapewniająca dostęp z holu głównego do reszty budynku nie jest fizyczną kontrolą. Można opłynąć, przeskakując nad nim lub omijając go. Jedynymi rzeczami, które mogą temu zapobiec, są:

• Członkowie personelu - jeśli pracownicy zobaczą, jak przeskakujesz barierę, prawdopodobnie skomentują ją. Nie ma innego wyjścia niż to aby upewnić się, że cię nie widzą. Jeśli jesteś w niefortunnej pozycji biorąc pod uwagę to podejście, upewnij się, że nie dzieje się to w godzinach szczytu - pierwsza rzecz rano, ostatnia po południu lub w porze lunchu.

• Strażnicy lub recepcja - Tacy ludzie mogą być rozproszeni przez innych testerów. Rodzaje rozrywek, które stosujesz, są ograniczone według twojej wyobraźni, ale może obejmować wszystko, od prostych zapytań po udawanie zawału serca. Na praktycznie wszystkich stronach strażnicy dbają o zdrowie i bezpieczeństwo personelu i gości przed pilnowaniem stanowiska.

• Aparaty - większość kamer nie będzie wskazywała na samą barierę, ale na drzwi prowadzące do recepcji, a czasem na obszar poza nią, na przykład wśród wind.

Naruszenie bezpieczeństwa granic poprzez przeskakiwanie barier w miejscach publicznych powinno być absolutną ostatecznością. Prawdopodobnie zostaniesz złapany i naprawdę będziesz wyglądać bardzo głupio. Zawsze istnieje lepsze, bardziej inteligentne podejście; po prostu jeszcze tego nie znalazłeś.

Praca wokół matant

Mantanta jest śluzową formą kontroli dostępu, którą można znaleźć w miejscach o wysokim poziomie bezpieczeństwa i jest prowadzona wyłącznie za pomocą identyfikatorów zbliżeniowych. Kiedy machasz odznaką, otwierają się pierwsze drzwi, wchodzisz i zamyka się za tobą. Dopiero wtedy drugie drzwi się otwierają i umożliwiają wejście. Proces ten powtarza się po wyjściu. Aby jeszcze bardziej skomplikować sytuację, podłoga mantanty jest czujnikiem ciśnienia, który mierzy wagę i rozkład masy w celu wykrycia obecności więcej niż jednej osoby. W niektórych środowiskach masa ciała podczas wychodzenia jest porównywana z tą przy wchodzeniu. Każda znacząca wariancja wywołuje alarm; działa to również jako surowe wykrywanie kradzieży. Oczywiście takie urządzenia uniemożliwiają ataki typu tailgating. Mantanta może być zastraszającą przeszkodą dla testera (i, ogólnie rzecz biorąc, pracowników), ale o to właśnie chodzi. Jest to bardzo widoczny wskaźnik fizycznego bezpieczeństwa i ma na celu wyświetlenie obrazu, że takie rzeczy są tutaj traktowane bardzo poważnie. Jednak, podobnie jak wszystkie obrazy, są w dużej mierze tylko na pokaz. Gdy wchodzisz do recepcji firmy, widzisz to, co firma chce, abyś zobaczył. Mantanta robi wrażenie na odwiedzających i działa odstraszająco na intruza. Jednak ich użycie stwarza pewne problemy. Niewielki obszar wewnątrz mantanty pozwoli na wejście osoby, ale niewiele więcej. Firma (szczególnie duża firma) wymaga do działania znacznie więcej niż tylko ludzi: potrzebuje również biurka, krzeseł, komputerów, wody do lodówek i tak dalej. Te rzeczy nie przechodzą przez mantatnę. Zasadniczo masz dwie opcje omijania takich przeszkód; albo znajdź wejście dla dostawy (które będzie bezpiecznie wolne od mantr) i wniknij tam lub pokaż się w recepcji z dostawą, w którym to momencie przejście pozwoli ci przejść przez alternatywne drzwi (czasami znajdujące się z boku mantanty) lub skierować cię do środka kierunek wejścia dostawy. Kolejna uwaga do zapamiętania: dostęp przez mantanty jest powolny. Przejście przez nią jednej osoby może zająć około 20 sekund, zarówno wejściowych, jak i wyjściowych. W sytuacji awaryjnej jest to całkowicie niedopuszczalne, więc niektóre zdarzenia, takie jak alarm pożarowy, automatycznie powodują otwarcie obu drzwi, umożliwiając szybką ewakuację. Nie daj się zastraszyć krzykliwymi kontrolami granic i pamiętaj, że bezpieczeństwo jest tak silne, jak najsłabsze ogniwo w łańcuchu. Twoim zadaniem jest znaleźć najsłabszy link.

Uzyskiwanie dostępu przez kołowrót

Bramki obrotowe są powszechnym widokiem w obiektach o wysokim poziomie bezpieczeństwa, zwykle na zewnątrz, na granicy terenu. Bramka obrotowa, podobnie jak mantrap, została zaprojektowana w celu umożliwienia dostępu do jednej osoby na raz i nie jest oczywiście łatwa do ominięcia. Zapewniają ci dokładnie te same problemy, co Mantry. Zazwyczaj można uniknąć kołowrotu, wjeżdżając (lub idąc) na parking, na którym pracownicy i goście mogą mieć dostęp do kontroli wewnętrznej. Z pewnością istnieją inne sposoby wejścia. Dlatego przeprowadzasz wstępne badania (patrz rozdział 6).

Naruszenie zamkniętych drzwi

Wiele rzeczy, na których bez wątpienia polegamy w kwestii bezpieczeństwa, można łatwo skompromitować przy odrobinie wiedzy i przemyślenia. Nigdzie to nie jest prawdziwsze niż z zamkami. Przez zamki nie mówię o elektronicznych systemach zbliżeniowych, ale o tradycyjnych urządzeniach, które otwierają się za pomocą przyciętych kluczy. Ponieważ niektóre testy będą nieuchronnie obejmować element wybierania zamków. Blokady, których można się spodziewać, że nie będą (w większości przypadków) wysokie, nie zapewniają wysokiego poziomu bezpieczeństwa. Cele wybierania śluz podczas testu fizycznego obejmują:

• kłódki na śmietnikach lub drzwiach bocznych;

• zamki w szafkach na dokumenty i szufladach biurkowych;

• zamki do drzwi biurowych (w miejscach, w których personel rutynowo je zamyka, w porze lunchu lub w dniu wyjazdu).

W większości przypadków zamki te można ominąć przy niewielkiej wiedzy i praktyce.

Ominięcie czujnika ruchu

Detektory ruchu nie są używane w godzinach pracy biura, z wyjątkiem obszarów o wysokim poziomie bezpieczeństwa, a nawet tylko w miejscach o wysokim poziomie bezpieczeństwa. Takie urządzenia mają zatem znaczenie tylko wtedy, gdy przeprowadzasz w nocy penetrację mniejszego obiektu (większe witryny mają całodobową ochronę). Zazwyczaj są one uruchamiane przez centralny system alarmowy, gdy działania są zakończone. Zaletą wcześniejszej wiedzy o tym, że strona jest alarmowana i wyposażona w czujniki ruchu, jest to, że będziesz tam jedyną osobą. Minusem tego jest ominięcie samych czujników. Można to jednak osiągnąć na następujące sposoby:

• Niektóre czujniki mają przycisk obejścia na dole. Jeśli jesteś w stanie dotrzeć do czujnika bez jego aktywacji, możesz go wyłączyć w ten sposób. Jest to czasami możliwe, gdy lokalizacja czujnika jest niska. Szczególnie kiepska lokalizacja znajduje się na szczycie schodów, gdzie często można je wczołgać pod linią wzroku czujnika. Innym przykładem jest drzwi, w których drzwi wychylają się na zewnątrz. Jeśli przełącznik obejścia jest w pozycji nieobecny, możesz (bardzo powoli) spróbować zasłonić czujnik lepkim klejem lub podobną substancją.

• Czujniki ruchu wykrywają ruch: poruszaj się powoli! Urządzenia te zwykle nie są tak wrażliwe, jak można sobie wyobrazić. Widziałem zmniejszoną wrażliwość z kilku dziwnych powodów. Na przykład czujnik wskazywał okno z drzewem na zewnątrz. Drzewo kołysze się na wietrze i uruchamia alarm. Najwyraźniej problem stanowiło umieszczenie czujnika, biorąc pod uwagę, że kombinacja drzewa i okna okazała się bardzo przydatna.

• Znajomość kodu alarmu z góry jest bardzo przydatna. Liczba osób w firmie, które mają dostęp do tych informacji, bezpośrednio wpływa na twoje szanse w ataku socjotechnicznym, ale to jest najbardziej eleganckie rozwiązanie.

• Jeśli uruchomisz wystarczającą liczbę alarmów w ciągu wieczora, będzie to wyglądać jak awaria sprzętu i ostatecznie system alarmowy zostanie wyłączony na noc. Gdy to nastąpi, odczekaj kilka godzin przed próbą wejścia. Firmy reagujące na te alarmy nie są głupie.

• Możesz wyłączyć niektóre czujniki odcinając zasilanie budynku; niektóre mają podtrzymanie bateryjne. Tak czy inaczej rzadko jest to możliwe.

• Czujniki wykorzystujące światło podczerwone (IR) można wykryć za pomocą odpowiedniego sprzętu, takiego jak kamera kieszonkowa w trybie noktowizyjnym.

• Czujniki wykorzystujące częstotliwość radiową (RF) mają większy zasięg śledzenia i działają w taki sam sposób jak fotoradary (na zasadzie Dopplera lub radaru). Wykrywanie tych czujników nie jest łatwe (musisz wiedzieć, jakie częstotliwości skanować), ale można to zrobić z większej odległości niż czujniki podczerwieni i nie wymagają one pola widzenia.

Podsumowanie

W tej omówiliśmy wiele podstawowych materiałów. Zestawy umiejętności omówione są absolutnie niezbędne dla prawdziwego zrozumienia natury fizycznych testów penetracyjnych i ich wykonywania. Powinieneś teraz zrozumieć, co następuje:

• Praktyczne testy bezpieczeństwa fizycznego - paradygmaty lub podejście zespołu operacyjnego w celu wykonania zadania.

• Eksploracja witryny - aktywa, które możesz potrzebować do nabycia.

• Podejścia taktyczne - techniki, które można zastosować na poziomie taktycznym, aby uzyskać dostęp do obiektu.

• Bezpieczeństwo odznak - środki techniczne i podejścia psychologiczne, które można zastosować w celu ograniczenia bezpieczeństwa odznaki i przekazania.

• Mechanizmy bezpieczeństwa - mogą to być fizyczne kontrole zapobiegawcze lub tylko odstraszający. Powinieneś mieć dobre pojęcie o ich mocnych stronach i słabości.

To ważna część. Po przeczytaniu kolejnej części, który dotyczy teorii i praktyki inżynierii społecznej, możesz wrócić i przeczytać ją ponownie, aby zastosować tam zdobytą wiedzę.