Zbieranie informacji

„Cała wojna, a właściwie cała sprawa życia, polega na próbach odkrycia tego, czego nie wiesz z tego, co robisz” - Arthur Wellesley, 1.książę Wellington - 4 września 1852 r

W tej części omówiono różne sposoby uzyskiwania i analizowania informacji i danych wywiadowczych:

• Gdzie szukać informacji i czego szukać.

• Jak przeprowadzić analizę kryminalistyczną na mediach elektronicznych.

• Jak zrozumieć wartość tego, co ludzie wyrzucają.

• Jak podejść do zbierania informacji fotograficznych.

• Jak przeprowadzić nadzór elektroniczny.

• Jak prowadzić tajny nadzór.

Każdy wymaga innego podejścia i zestawu umiejętności. Nie zawsze jest konieczne stosowanie wszystkich technik opisanych tutaj w każdym przeprowadzanym teście penetracji fizycznej. Powinieneś jednak upewnić się, że jesteś biegły w każdym z nich. Na przykład pierwsze nocne wejście do obiektu docelowego nie jest najlepszym momentem na naukę korzystania z kliszy termowizyjnej, a pierwszy raz, gdy kupujesz wyrzucone nośniki cyfrowe, nie powinien być pierwszym eksperymentem z akwizycją kryminalistyczną. Moim zamiarem jest skłonienie Cię do innego myślenia o bezpieczeństwie - postawienia się w sytuacji napastnika. Tylko w ten sposób możesz naprawdę docenić zakres zagrożeń, które organizacja musi wziąć pod uwagę, zanim zacznie je łagodzić. Informacja to efemeryczny byt, ale obowiązuje jedna dość solidna zasada; więcej informacji jest dobrych, a mniej jest złych. Gromadząc informacje, ich wartość może nie być widoczna, dopóki jej nie potrzebujesz. Dlatego zachęcam do jak największej staranności podczas budowania profilu organizacji docelowych i pracowników.

Nurkowanie w śmietniku

Wiele można się nauczyć o ludziach, po prostu ich obserwując, ale można dowiedzieć się więcej, niż kiedykolwiek chciałeś wiedzieć, przeglądając ich śmieci.

15 września 1993 r. FBI, zbierając dowody w celu oskarżenia podejrzanego podwójnego agenta Aldricha Amesa, znalazło w jego śmieci notatkę - notatkę dotyczącą zbliżającego się spotkania z KGB. Można by pomyśleć, że 31-letni weteran CIA ćwiczyłby lepsze rzemiosło. Jest to jednak ilustracyjne. Jeśli ktoś, kogo specjalnością są tajemnicami i kłamstwami, popełniłby taki błąd debiutanta, jak można oczekiwać, że reszta świata będzie miała się lepiej? Nurkowanie w śmietniku to po prostu przeszukiwanie śmieci celu w poszukiwaniu informacji, dokumentów i mediów elektronicznych, które byłyby pomocne dla napastnika. Dostęp do obiektu w nocy i uzyskanie poufnych informacji z kosza czasami obejmuje całość testu. Jednak ćwiczenie to jest znacznie bardziej przydatne w połączeniu z pełnym testem fizycznym w celu oceny użyteczności uzyskanych informacji. Oczywiście niektóre rodzaje informacji są bardziej przydatne niż inne, więc czego szukają testerzy? Jeśli wdrażasz zabezpieczenia, jakiego rodzaju informacje nie dotrą do Twoich śmietników?

• Informacje o pracowniku: przydatne są wszelkie informacje, które pozwalają napastnikowi udawać insidera. Informacje o pracownikach są szczególnie przydatne w atakach socjotechnicznych, ponieważ sprawiają wrażenie wiedzy wewnętrznej. Nawet pozornie nieszkodliwe dane, takie jak imię i nazwisko, dział i numer pracownika, są wystarczające, aby stworzyć prawdopodobny atak przed wysłaniem wiadomości.

• E-maile: drukowane wiadomości e-mail umożliwiają atakującym określenie struktury adresów e-mail, ale zwykle można to również uzyskać z innych źródeł. Interesujące może być sprawdzenie, kto wysyła e-maile do kogo, a same e-maile mogą zawierać istotne informacje. Na przykład wiadomość e-mail z systemów powiadamiająca firmę o zbliżającym się przestoju sieci zawiera imię i nazwisko oraz adres e-mail administratora systemu. Podobnie, e-mail informujący firmę o nowym pracowniku ma oczywistą wartość. Pracownicy omawiają różne rzeczy za pośrednictwem poczty elektronicznej, a rodzaje e-maili, które są drukowane, zwykle są tymi, które mają wartość odniesienia.

• Mapy sieci: Informacje o strukturze sieci wewnętrznej, a w szczególności mapy i diagramy sieciowe, są nieocenione dla testera penetracji. Atakujący mogą zmniejszyć o połowę ilość pracy, którą muszą wykonać w placówce firmy, jeśli znają już strukturę sieci. Szczególnie przydatne są informacje takie jak adresy i zakresy IP, nazwy serwerów, dystrybucja systemu operacyjnego i nazwy dostawców. To informacje, których nigdy nie należy wyrzucać do kosza.

• Papier firmowy: Firmowy papier firmowy, niezależnie od jego zawartości, jest niezwykle przydatny. Pozwala atakującemu na realistyczne fałszowanie komunikacji firmowej, skierowanej do pracowników lub osób trzecich. Przydatne również dla zespołu testującego penetrację, ponieważ pozwala im robić dokładnie to samo. Tworzenie dobrze podrobionych liter jest istotnym aspektem inżynierii społecznej.

• Dokumenty rozliczeniowe / faktury: takie informacje pokazują, z kim odbiorca prowadzi interesy, co warto wiedzieć. W dalszej części ćwiczenia osoba atakująca może udawać partnera biznesowego lub klienta. Jeśli cel outsourcuje IT (lub inne usługi), wiedza, z kogo korzysta, jest przydatna z tego samego powodu.

• Podpisy: podpisany dokument, taki jak papier firmowy, jest cenny sam w sobie. Znajomość podpisu ułatwia kopiowanie. Listy wysyłane masowo często mają kserokopię podpisu, co czyni go równie łatwym. Szczególnie przydatne są podpisy dyrektorów generalnych, szefów działów, księgowych, kierowników biur i wszystkich osób odpowiedzialnych za fakturowanie lub fakturowanie.

• Nazwy użytkownika / hasła: Znajdowanie nazw użytkowników jest przydatne, ponieważ ujawnia, w jaki sposób tworzone są takie nazwy użytkownika. Zwykle jest to dość proste, tj. John Smith zostaje jsmith lub john.smith. Jednak nie zawsze tak jest, w niektórych wewnętrznych i być może bardziej sklasyfikowanych systemach może nie być sposobu, aby je odgadnąć. Dlatego każdy dokument, który odwołuje się do nazw użytkowników, jest świetnym znaleziskiem. Jeszcze lepsze jest znajdowanie haseł. To naprawdę uderza w płacę. Tak, ludzie cały czas je zapisują, zwykle na małej żółtej karteczce z notatkami, że trzymają się monitora. . . . Jak na ironię, często jest to reakcja na próby wymuszenia przez administratora trudnych do odgadnięcia haseł; trudny do odgadnięcia oznacza trudny do zapamiętania.

• Podręczniki firmowe i procedury operacyjne: Wszystkie zasady, przepisy i codzienne procedury operacyjne firmy są zwykle przekazywane nowym pracownikom podczas procesu wdrażania w formie podręcznika firmowego. Ponieważ te rzeczy są często aktualizowane szybciej, niż można je odczytać, trafiają do kosza z zaskakującą regularnością. To zapłata dla inżyniera społecznego.

• Rozdrobniony papier: Tak, dobrze to przeczytałeś. Chociaż wiele dokumentów ulega zniszczeniu, przeciętna niszczarka biurowa jest całkiem bezużyteczna w utrzymywaniu tego w ten sposób. Papier pocięty na paski można łatwo złożyć ponownie, często bez pomocy zaawansowanych technologii. Gdy papier jest podawany do niszczarki, a strzępy nie są mieszane, paski papieru pozostają blisko siebie. Dodatkowo, jeśli dokumenty są wprowadzane do niszczarki liniami tekstu równolegle, a nie prostopadle do ostrzy niszczarki, to na dokumencie pozostają długie czytelne paski. Odwrotnie, duże ilości pasków papieru z wielu dokumentów są trudniejsze do poskładania (chyba że masz dużo czasu

jeśli to czytasz, prawdopodobnie nie). Wprowadź oprogramowanie do rekonstrukcji dokumentów. FBI, księgowi sądowi i inni śledczy regularnie muszą odzyskiwać zniszczone dane. Sposób, w jaki podchodzą do tego w erze Enron, polega na skanowaniu wszystkich małych fragmentów i używaniu oprogramowania, które automatycznie rekonstruuje dokumenty. Istnieje rozwiązanie komercyjne; Unshredder to narzędzie do rekonstrukcji dokumentów handlowych, które daje dużo frajdy. Jeśli regularnie bawisz się strzępionym papierem, powinieneś to sprawdzić.

• Media elektroniczne: dyskietki, płyty CD-ROM, DVD, stare dyski twarde, pamięci USB. To niesamowite, co ludzie wyrzucają. Widziałem stare dyski twarde wyrzucane z kosza wypełnionego informacjami o pracownikach, danymi recept z apteki (nazwiska, adresy, schorzenia) i wszystkimi innymi dokumentami, arkuszami kalkulacyjnymi i bazami danych. Media elektroniczne to nasz cel numer jeden. Praktycznie nikt bezpiecznie nie usuwa dysków ani nie niszczy płyt CD-ROM, zanim te rzeczy trafią do kosza. Odzyskiwanie danych z mediów elektronicznych zasługuje na swoją część własne i przyjrzysz się temu szczegółowo w dalszej części tego rozdziału.

Nurkowanie

Kiedy twoje śmieci trafiają na ulicę, trafiają do domeny publicznej, każdy może przez nią przejść i nie musi się martwić o złamanie prawa. Dzieje się tak w większości jurysdykcji, a na pewno w Wielkiej Brytanii i USA (chociaż w niektórych miejscach istnieją specjalne regulaminy, które temu zapobiegają). Jednak większość śmietników zawierających śmieci firmowe znajduje się na terenie prywatnym. Zapewniamy jednak, że nie będą mieli mniej niż 24 godziny na uzbrojenie strażnika z kamerami i psami. W rzeczywistości najprawdopodobniej nawet nie zostaną zamknięte. Jeśli są zablokowane, nie będzie to nic poważnego. Jeśli przeprowadzasz test, pamiętaj, że śmietniki będą na terenie prywatnym, więc potraktuj ćwiczenie nurkowania na śmietniku z taką samą powagą, jak każdą inną część zadania. Planuj z wyprzedzeniem i postaraj się jak najszybciej wejść i wyjść. Nie ulegaj pokusie, aby zacząć sortować rzeczy na miejscu, weź to, co możesz zabrać - weź ze sobą kilka dużych płóciennych toreb - i przeprowadź analizę poza miejscem pracy.

Wykonywanie analizy kryminalistycznej na przechwyconych danych

Forensics to termin używany do opisania procesów związanych z pozyskiwaniem i analizowaniem danych z przechwyconych mediów elektronicznych. Mogą to być dyski twarde, pendrive'y, płyty CD-ROM lub cokolwiek innego, co zawiera dane komputerowe. Kryminalistyka jako część dochodzenia prawnego może być niezwykle skomplikowana ze względu na konieczność zachowania ulotnych dowodów i łańcucha dostaw - na szczęście nie musisz się tym martwić, ponieważ Twoim jedynym celem jest odzyskanie danych w kontekście testu penetracyjnego . Istnieje wiele różnych sposobów analizowania przechwyconych mediów elektronicznych. Jednak następujące podejście jest łatwe do naśladowania, daje wyniki i jest powtarzalne. Potrzebne będą:

• Kopię zestawu narzędzi kryminalistycznych Helix, który można pobrać bezpłatnie ze strony www.e-fense.com/helix/

• Zewnętrzny dysk twardy o dużej pojemności z obsługą USB2.0.

Chcesz utworzyć obraz przechwyconego nośnika i zapisać go na dysku twardym. Pozwala to na większą swobodę podczas procesu analizy i ponieważ nie pracujesz na oryginalnych danych, których nie masz, nie musisz martwić się o usunięcie lub uszkodzenie danych. Śledczy kryminalistyczni polegają na tej technice, aby zapewnić legalną integralność danych, chociaż nie jest to problemem dla testerów penetracyjnych. Helix odczytuje dane „bitowo” z nośnika, aby zapewnić doskonałą kopię. Ma to dodatkową zaletę: wszelkie usunięte dane na dysku (które nie zostały nadpisane) są zachowane i

można je analizować tak łatwo, jak zwykłe dane. Helix umożliwia między innymi wykonywanie innych czynności, takich jak wyszukiwanie słów kluczowych, określonych rodzajów danych i odczytywanie haseł do systemu operacyjnego. Podsumowując, jest to elastyczny, łatwy w użyciu pakiet, ale ma wiele zaawansowanych funkcji dla zaawansowanych użytkowników. Jest również bezpłatny.

Pierwsze kroki z Helixem

Byłoby bardzo łatwo napisać całą książkę o Helix i nadal nie opisywać wszystkich jej funkcji. Jednak moim jedynym zamiarem w tej sekcji jest opisanie podstawowych funkcji akwizycji i analizy, ale zachęcam do pracy z Helixem i nauczenia się korzystania z bardziej zaawansowanych funkcji. To jest tego warte.

Akwizycja danych w systemie Windows

Całe gromadzenie danych odnosi się tutaj do mediów, które zostały zabrane z witryny (tj. śmietniki). Pozyskiwanie nośnika jest znacznie łatwiejsze w systemie Windows. Niestety nie ma (dobrych) narzędzi analitycznych dla systemu Windows, więc w tym celu przełączam się na Linuksa. Helix może uruchamiać się bezpośrednio do Linuksa podczas uruchamiania lub działać jako program w systemie Windows. To najłatwiejszy sposób na rozpoczęcie. Możliwe jest użycie Helixa jako bezpiecznego dysku rozruchowego Linuksa, ale nie jest to absolutnie konieczne. Nie próbujesz zachować łańcucha dowodów, tylko moje dane. Wykonaj następujące kroki:

1. Uruchom system Windows.

2. Podłącz nośnik, który chcesz przechwycić, i zewnętrzny dysk twardy, aby zapisać powstałe obrazy Uwaga: Możesz przechowywać te obrazy na dysku twardym, jeśli chcesz, ale jeśli przechwytujesz dużo multimediów, których będziesz używać szybko zajmuje miejsce na dysku.

3. Włóż płytę CD-ROM Helix. Spowoduje to automatyczne załadowanie oprogramowania Helix dla systemu Windows.

4. Teraz musisz skonfigurować ustawienia przechwytywania. Wybierz akwizycję na żywo (ikona kamery po lewej stronie) i ustaw:

• Źródło: to jest nośnik docelowy. Możesz go wybrać z listy rozwijanej.

• Miejsce docelowe: powinien to być dysk zewnętrzny.

• Nazwa obrazu: jeśli tak, zastosuj się do jakiejś konwencji nazewnictwa

Systemy plików FAT mogą tworzyć tylko pliki o rozmiarze do 4 GB. Dlatego dobrze jest kliknąć opcję Podziel obraz. Następnie masz możliwość próbkowania nośnika w kawałkach, które zmieszczą się na systemie plików cdrom, dvd lub FAT32.

5. Teraz kliknij Acquire. Długość tego procesu będzie zależała od rozmiaru nabywanego nośnika.

Analiza danych

W tym momencie będziesz mieć jeden duży plik .dd lub kilka mniejszych plików .dd.xx. Niestety dla systemu Windows Helix nie ma żadnej aplikacji do analizy obrazów. Aby to zrobić, musisz uruchomić system za pomocą Helix (tj. w trybie Linux). Aby to zrobić, włóż dysk Helix i uruchom ponownie komputer. Helix uruchomi się automatycznie. Następnie wykonaj następujące kroki:

1. Po uruchomieniu systemu uruchom Autopsję z menu kryminalistycznego Helix w menu głównym. To jest interfejs przeglądarki internetowej, więc poczekaj, aż przeglądarka się załaduje, a następnie utwórz nowe zgłoszenie u dołu ekranu. Następnie zostaniesz poproszony o dodanie hostów.

2. Kliknij przycisk Dodaj hosta, a pojawi się nowa strona. Będzie prosić o dodanie obrazu do zbadania. Tutaj podaj lokalizację pliku obrazu, który właśnie uzyskałeś. Poniżej pola lokalizacji obrazu znajdują się trzy pola radiowe umożliwiające wybór między kopiowaniem, przenoszeniem lub tworzeniem łącza do rzeczywistego pliku obrazu w katalogu locker. Najlepszą opcją jest skopiowanie całego pliku obrazu do katalogu locker.

3. Na koniec kliknij przycisk Dodaj obraz. Nadszedł czas, aby przeprowadzić testy na właśnie utworzonej sprawie.

4. Z Case Gallery najpierw wybierz przypadek, hosta i obraz, na którym chcesz uruchomić testy. Na przykład, jeśli chcesz poznać wszystkie usunięte pliki w obrazie, kliknij przycisk Analiza plików, a następnie kliknij przycisk Wszystkie usunięte pliki. Spowoduje to wyświetlenie nazw i dat wszystkich usuniętych plików.

Być może szukasz określonej informacji lub słowa kluczowego. Na szczęście autopsja umożliwia wyszukiwanie określonych słów. Być może szukasz określonej informacji lub słowa kluczowego. Na szczęście autopsja umożliwia wyszukiwanie określonych słów. Dostępnych jest ogromna liczba narzędzi kryminalistycznych, wiele z nich można pobrać bezpłatnie, chociaż istnieją drogie rozwiązania komercyjne. Chciałem przedstawić wam świat kryminalistyki za pośrednictwem Helix, ponieważ te narzędzia stanowią podstawę tego, czego potrzebujecie; możliwość pozyskiwania danych i ich analizy w sposób proceduralny. Chociaż jest to kuszące, aby spędzić resztę rozdziału na rozmowie o medycynie sądowej, a w szczególności o Helixie, jest to tylko jeden aspekt procesu zbierania informacji. W każdym razie na dysku Helix znajduje się wiele narzędzi służących do wykonywania wszelkiego rodzaju specjalistycznych zadań, od analizy rejestru systemu Windows po odzyskiwanie hasła. Zdecydowanie zalecamy zapoznanie się z nimi. Są potężną bronią w twoim arsenale.

Zalety niszczenia elektronicznego

Ryzyko wyrzucenia mediów elektronicznych do śmieci powinno być teraz bardzo jasne, ale jakie masz opcje? CDROM'y i DVD powinny zostać rozdrobnione (większość niszczarek akceptuje dyski) lub pocięte na ćwiartki. Dyski twarde należy wyczyścić kryptograficznie przed utylizacją (lub sprzedażą w serwisie eBay…). Istnieje bootowalna dystrybucja Linuksa o nazwie DBAN, która jest bezpłatnie dostępna na www.dban.org. To oprogramowanie pozwala całkowicie wymazać dysk twardy, zastępując go kilka razy z nieprzewidywalnymi losowymi danymi. DBAN zapobiega lub całkowicie utrudnia (w zależności od trybu pracy) wszystkie znane techniki kryminalistyki.

Surfowanie na ramieniu

Nie ma nic technicznego w surfowaniu przez ramię (przynajmniej nie tradycyjnie). Surfowanie przez ramię to czynność bezpośredniej obserwacji (np. patrzenie przez ramię) w celu uzyskania niewielkich fragmentów kluczowych informacji, takich jak nazwy użytkownika lub hasła, kody do bankomatów lub (bardzo popularne w tym czasie) kody połączeń zamiejscowych w automatach telefonicznych. Surfowanie na ramieniu jest najbardziej skuteczne w zatłoczonych miejscach, ponieważ pozwala na większy potencjał zarówno celów, jak i ukrycia. Klasycznym przykładem przestępczym jest surfowanie po kodzie PIN na szafce na siłowni. Ponieważ ludzie mają tendencję do ponownego wykorzystywania swoich czterocyfrowych kodów, możesz być dość pewien, że kody PIN na kartach kredytowych przechowywanych w szafce będą takie same. Innym przykładem jest klasyczne oszustwo związane z

bankomatami. Wiadomo, że przestępcy instalują małe urządzenia w bankomatach, które przechwytują karty. Gdy użytkownik bankomatu stoi tam, próbując dowiedzieć się, co się stało, podszedł do niego oszust, który powiedział mu, że miał ten sam problem poprzedniego dnia i po prostu próbuje ponownie wprowadzić kod, co zostało dyskretnie odnotowane. Oczywiście to nie działa, więc Mark odchodzi, aby zadzwonić do swojego banku. Przestępca również odchodzi, mając teraz zarówno kartę, jak i pin. W tej sekcji omówię dwie bardziej interesujące rzeczy, które można uzyskać dzięki podsłuchiwaniu ramienia: kody dostępu do komputera (nazwy użytkowników, hasła, piny itp.) I kody do drzwi. Surfowanie przez ramię w poszukiwaniu kodów komputerowych może odbywać się zarówno w docelowym lokalu, dyskretnie obserwując personel, jak i na zewnątrz w kafejkach internetowych, pociągach lub wszędzie tam, gdzie personel używa swoich komputerów. Gdy znajdziesz się w docelowej lokalizacji, zdobycie haseł jest łatwiejsze, ponieważ masz możliwość wykorzystania zaufania. Jako przykład rozważ następujące studium przypadku:

Case Sudy: Hasło

Kris uznał, że wejście do biura jest bardzo proste, ale potrzebował haseł. Właściwie potrzebował tylko jednej nazwy użytkownika i hasła. To doprowadziłoby go do lokalnego kontrolera domeny. Potem umieścił laptopa w cichym, małym, niezajętym pokoju z dala od ciekawskich oczu i wykorzystał swoją magię. Siedząca sama w kącie Kris zauważyła pracownika, który najwyraźniej miał problemy ze swoim stanowiskiem pracy. Uśmiechnął się, to będzie łatwe. „Przepraszam panią, jestem Dave z działu pomocy technicznej, jak się masz dzisiaj?" - zapytał. „W porządku, jestem Cindy" - odpowiedziała z roztargnieniem. „Przez cały ranek otrzymywaliśmy skargi dotyczące wydajności sieci. Jak samej to widzisz?" „Ach, wszystko wydaje się być trochę powolne, a Office ciągle się zawiesza" "Doskonale, pomyślał Kris, stary dobry Office. "" Hmm. Tak myślałem, czy nie masz nic przeciwko, jeśli spojrzę? "- zapytał. „„ Oczywiście, proszę! Wszystko, co możesz zrobić, aby pomóc! "- odpowiedziała Cindy, realizując beznadziejne marzenie o bezawaryjnym biurze. „Czy mogłbyś się dla mnie wylogować?" Zapytała Kris, przechylając się przez jej ramię, aby lepiej się przyjrzeć. ''DOBRZE. Dobrze, teraz zaloguj się ponownie. Doskonale, hmmm, jest wolny, prawda? Na koniec przeprowadzę kilka testów "- powiedział, wyciągając laptopa i kierując się do opuszczonego biura. Nazwa użytkownika: Cindyh. Hasło: Bobby1. Idealnie.

Pobieranie kodów do drzwi

Większość kodów drzwi ma tylko czterocyfrowe piny numeryczne. W przypadkach, gdy używane są kody drzwi, wszyscy pracownicy zwykle używają tego samego kodu PIN. W rezultacie często spotyka się piny strzegące drzwi do mniejszych biur. Większe pomieszczenia są częściej chronione przy użyciu zbliżeniowych kart dostępu. Punkty wejściowe do drzwi są zwykle wyraźnie umieszczone na wysokości oczu. Pracownicy na ogół nie ukrywają, co piszą, zwłaszcza z samego rana przed wypiciem kawy. W każdym razie, jeśli jesteś odpowiednio ubrany, nie powinieneś przyciągać zbytniej uwagi i dlatego nie powinieneś mieć większych problemów z odczytaniem kodu dostępu. Jeśli proste surfowanie po ramieniu jest zbyt widoczne, oto mała sztuczka. Kod PIN prawdopodobnie nie będzie miał więcej niż cztery cyfry; jest również mało prawdopodobne, że cyfry zostaną ponownie użyte. Dlatego zakładając, że klawiatura działa od 0-9, istnieje $10 \times 9 \times 8 \times 7$ lub 5040 możliwych kombinacji, czyli o wiele za dużo, by zgadnąć. Gdybyś wiedział, które cyfry są używane, ale nie w kolejności, trudność jest znacznie zmniejszona: $4 \times 3 \times 2 \times 1$ lub 24 możliwe kombinacje. Jak Ty to robisz? To całkiem proste: przetrzyj czystą szmatką klawiaturę, a następnie upewnij się, że jest sucha i wolna od odcisków palców. Następnym razem, gdy ktoś wprowadzi kod drzwi, jego odciski palców będą dość widoczne na przyciskach.

Elektroniczne i zautomatyzowane metody surfowania przez ramię

Być może słyszałeś historie o przestępcach instalujących małe kamery w pobliżu bankomatów w celu przechwytywania kodów PIN. Stało się to z zaskakującym sukcesem, dlatego wiele bankomatów wyświetla teraz ostrzeżenia, że użytkownicy powinni szukać załączników, które wydają się nie na miejscu. Obecnie istnieje możliwość zakupu bardzo małych niezależnych kamer bezprzewodowych, które mają wystarczający zasięg transmisji, rozdzielczość i dyskretny profil, aby sprostać naszym potrzebom. Podłączenie kamery do podkładki drzwiowej, choć nie jest czymś, na czym chcesz się przyłapać, jest możliwe, a zalety są oczywiste. Preferowane jest ukrycie aparatu w jakiś sposób. Pod górną krawędzią można umieścić Małe kamery bezprzewodowe, dostępne w zwykłych sklepach szpiegowskich. (Właściwie przesadzona krawędź używana do ukrycia klawiatury i zapobiegania surfowaniu po ramionach pomaga w tym przypadku.) Możesz także spróbować dołączyć logo firmy i słowa Test diagnostyczny. Taka strategia pozwala urządzeniu działać bez zarzutu wystarczająco długo, aby przechwycić kod dostępu. Oczywiście, gdy twoje urządzenie zostanie znalezione, twój cel szybko zmieni się z nieświadomego na świadomy.

Techniki surfowania na duże odległości

Czasami można obserwować monitory komputerowe, klawiatury i systemy wejściowe z dużej odległości za pomocą lornetki lub aparatu z długim obiektywem. Aparaty Canon G Range Powershot, które omówimy w następnej sekcji (w rzeczywistości większość nowoczesnych aparatów) są w stanie przechwytywać wideo HD. Podczas próby uchwycenia naciśnięć klawiszy, które mogą być niejednoznaczne, bardzo przydatna jest możliwość wielokrotnego przeglądania wpisu. Możesz surfować po ramionach z dużej odległości z ulicy, sąsiednich budynków, korytarzy, a nawet pokoi hotelowych. Najlepsze rezultaty daje ustawienie na podwyższeniu, na przykład patrzenie w dół przez okno biurowca. Obserwuj otoczenie i określ, czy można to zrobić z sąsiedniego budynku publicznego. Dostęp do dachu budynku po drugiej stronie ulicy jest idealny do tego rodzaju prac.

Zbieranie inteligencji fotograficznej

Przed rozpoczęciem testu penetracji fizycznej pożądane jest zbudowanie inteligencji fotograficznej samego budynku docelowego, a także personelu, ogólnego otoczenia i innych interesujących miejsc. Zwykle jest to wykonywane przed samym testem fizycznym z tak długim czasem realizacji, jak to konieczne. Charakter nadzoru fotograficznego będzie różny w zależności od zadania, ale należy dążyć do stworzenia możliwie wyczerpującej dokumentacji informacji. Jako minimum powinieneś przywieźć ze zdjęciami:

• Budynki docelowe: Zrób jak najwięcej zdjęć z jak największej liczby kątów, aby zbudować pełny obraz docelowej lokalizacji.

• Punkty wejścia / wyjścia: upewnij się, że wiesz, gdzie znajdują się wszystkie wejścia i wyjścia oraz jakie środki są dostępne, aby je chronić. Pomyśl poza tym, co oczywiste, w pewnych okolicznościach wyjście przeciwpożarowe może być również wejściem.

• Kontrola dostępu: czy cel używa kart przesuwanych, kodów PIN, identyfikatorów zbliżeniowych lub kodów kreskowych, aby umożliwić wejście? Należy pamiętać, że w niektórych przypadkach stali członkowie personelu mają identyfikatory zbliżeniowe, podczas gdy odwiedzający otrzymują tymczasowe identyfikatory z kodami kreskowymi lub które muszą być okazywane ochronie. Zrób zdjęcia samych czytników kart do późniejszej analizy technologicznej. Wierz lub nie, ale witryny wymagające eskortowania gości są generalnie mniej bezpieczne, ponieważ w praktyce jest to raczej niewykonalne, a personel szybko męczy się eskortowaniem gości do łazienki. W związku z tym ludzie są przyzwyczajeni do wpuszczania nieznanych gości do i poza bezpieczne obszary.

• Karnety / odznaki: jeśli to możliwe, zrób z bliska dyskretne zdjęcia samych przepustek. Zwykle pracownicy wchodzący do budynku wystawiają je na otwartej przestrzeni albo na szyi na smyczy, na zewnętrznych kieszeniach kombinezonu lub na klipsach do paska. Posiadanie dobrego obrazu odznaki umożliwi późniejszą pracę w Photoshopie. Czasami możesz pójść dalej.

• Śmieciarki: Omówiliśmy już nurkowanie w śmietnikach. Jeśli wiesz gdzie się wybierasz przed wejściem na stronę, tym lepiej.

• Pracownicy ochrony: Czy cel zatrudnia dedykowany personel ochrony, jeśli tak, upewnij się, że robisz dobre zdjęcia ich mundurów. Czy personel jest na miejscu, czy (co jest bardziej prawdopodobne) docelowy outsourcing? Jeśli tak, to która firma? Ilu jest strażników? Gdzie oni są? Czy są statyczne czy mobilne? Czy w danym momencie można przewidzieć ich ruchy?

• Bezpieczeństwo obwodowe:

• Jakie fizyczne zabezpieczenia stosuje cel i czy zmienia się to w ciągu dnia? Wykonuj zdjęcia zamków i wszelkiego rodzaju barier fizycznych. Co jest potrzebne, aby wjechać na parking? Na przykład niektóre wymagają plakietki pracownika, inne są po prostu zautomatyzowane.

• Inne mechanizmy bezpieczeństwa: Zrób zdjęcia kamer i ich lokalizacji; pozwoli to określić czarne punkty - obszary bez pokrycia. Umożliwi to również określenie, którzy dostawcy są celem i wszelkie wrodzone luki, które mogą mieć. O której zazwyczaj przyjeżdżają pracownicy? Jak długo trwa, zanim wszyscy wyjdą? Jakie są zasady dotyczące ubioru? Czy masowe wejścia i wyjścia stwarzają lepszy potencjał fizycznego wejścia?

Odznaka

Kris odchylił się na ławce w parku i niedbale oddał kilka kolejnych strzałów. Szerokokątny obiektyw w jego Canonie G10 pozwolił mu skierować aparat na zabytkowy budynek jak zwykły turysta , który pojawił się na całym świecie w okularach przeciwsłonecznych, czapce z daszkiem i luźnych dżinsach. W rzeczywistości fotografował pracowników biura, rozmawiających tuż po jego lewej stronie. Dzięki Bogu za wielopunktowe skupienie, pomyślał. Ich plakietki były dobrze widoczne i sprawdzając ekran aparatu, zrobił kilka bardzo dobrych zdjęć. Bardzo dobrze, jak się okazało, ponieważ kod kreskowy i odpowiadający mu numer były dobrze widoczne. W bazie Kris rozpoczął proces odtwarzania, który był w większości bardzo łatwy. Kod kreskowy był jednak wyzwaniem. Badając sam kod kreskowy, zdał sobie sprawę, że to przepustka tymczasowa, ważna tylko na ten dzień. Liczby odpowiadające dzisiejszej dacie, a także niektóre liczby końcowe potrzebne do uzupełnienia kodu kreskowego. Przyjrzał się obrazowi kolejnej przepustki - to samo, z tym że końcowe liczby były różne, co wskazywało, że mogą być dodatkową warstwą zabezpieczeń, sumą kontrolną lub całkowicie losowo. Kris utworzył nowy kod kreskowy z zakodowaną datą testu penetracji i zaimportował powstały plik .jpg do programu Photoshop, aby wkleić go na swoją odznakę. Musiałby założyć, że końcowe postacie są przypadkowe, jeśli odznaka nie zadziała, musiałby ją po prostu imrpozwizować. Uśmiechnął się; improwizowanie było tym, co robił najlepiej.

Wprowadzenie do fotografii dyskretnej

Ważną umiejętnością, którą należy rozwijać, jest fotografowanie ludzi, często z bliskiej odległości, bez wykrycia. Obserwowanie ludzi przychodzących i wychodzących zawsze było dla mnie źródłem fascynacji. Polecam The Decisive Moment autorstwa Henri Cartier-Bresson. Ten niewielki zbiór fotografii na zawsze zmienił sposób, w jaki patrzyłem na świat. Cartier-Bresson był twórcą gatunku znanego jako fotografia uliczna, rodzaj pseudoreportażu, który stara się uchwycić ludzi w szczerych sytuacjach w miejscach publicznych i ogólnie nieświadomych. Każdy sukces w tej dziedzinie wymaga

od początkującego fotografa ulicznego bardzo szybkiego nauczenia się obsługi aparatu, jednocześnie sprawiając wrażenie, że robi coś innego. Kiedy ktoś zorientuje się, że jest fotografowany, zachowuje się zupełnie inaczej. Wiele umiejętności w fotografii ulicznej można bezpośrednio przenieść na to, co nazwiemy fotografią dyskretną - uzyskiwanie z bliska i osobistych zdjęć, które będą przydatne dla zespołu przeprowadzającego testy penetracyjne. Przykładem może być uchwycenie wysokiej jakości obrazu karty wstępu, jak w powyższym studium przypadku. Przede wszystkim ważne jest, aby skonfigurować kamerę w taki sposób, aby Cię nie zdradziła. Zdecydowanie faworyzuję Canon Powershot Grange do tego rodzaju prac, ale każdy przyzwoity kompaktowy aparat cyfrowy z wyższej półki jest odpowiedni i tę radę można bezpośrednio przenieść do większości aparatów. Aparaty cyfrowe oferują następujące ustawienia:

• Tryb RAW: Jeśli twój aparat obsługuje tryby RAW, DNG lub TIFF, to używaj ich w tej kolejności. Nieprzetworzony obraz i doskonała jakość to więcej niż dodatkowe przetwarzanie końcowe.

• Autofokus: użyj go, chyba że autofokus w aparacie jest szczególnie opóźniony. Jeśli nie, użyj trybu ręcznego i skonfiguruj hiperfokalną odległość odpowiednią do aparatu. Sytuacja wygląda inaczej w przypadku wszystkich aparatów, ale w Internecie dostępnych jest wiele zasobów wyjaśniających powody takiego postępowania.

• Flash: wyłącz to! Wystrzelenie komuś w twarz błyskiem ma tendencję do odchylania się dyskretnego.

• Dźwięki: brak sygnałów dźwiękowych lub kliknięć. Możliwe jest całkowite wyciszenie aparatu kompaktowego, co jest zaletą w stosunku do charakterystycznego odbicia lustrzanego, które można uzyskać dzięki lustrzance jednoobiektywowej (SLR).

• Wspomaganie ostrości: wyłącz tę wiązkę rzutowaną przez kamerę, aby pomóc autofokusowi znaleźć zakres. Nie tylko sama wiązka jest dobrze widoczna, ale jest też oczywiste, że pochodzi z aparatu.

• Automatyczne wspomaganie ISO: ponieważ prawdopodobnie nie będziesz mieć zbyt wielu okazji, aby skomponować ujęcie, a na pewno nie będziesz używać statywu, potrzebujesz wszelkiej możliwej pomocy, aby zachować ostrość zdjęcia. Wspomaganie ISO automatycznie dostosowuje czułość ISO (prędkość ekspozycji) w górę, zmniejszając czas ekspozycji. W skrajnych przypadkach może to wprowadzić szumy do obrazów, ale nie na tyle, aby stanowić problem dla Twoich celów. Zapisz te ustawienia w niestandardowym slocie, a będą one dostępne po naciśnięciu przycisku.

Wtopienie się

Słynny mit dotyczący Henri Cartier-Bressona mówi, że owijał aparat w chusteczkę i robił zdjęcia, udając, że kicha. To właściwie wystarczająco głupie, aby było prawdą. Jednak nowoczesne aparaty kompaktowe są bardzo małe i prawie każdy posiada aparat. Są wszędzie, gdzie spojrzysz, na ulicy. Kiedy będziesz następny w mieście, obserwuj, ile osób ma aparaty na szyi i co fotografują. Większość ludzi, których widzisz, jak się odrywają, to turyści i nikt nie rzuca im drugiego spojrzenia. Jest wiele książek na temat ukrytej fotografii w monitoringu, ale szczerze mówiąc, podczas fotografowania ludzi na ulicy wystarczy jedna prosta zasada, zachowuj się niewinnie i wyglądaj, jakbyś należał do ciebie, i nikt nie spojrzy na ciebie ponownie. Ustawiając się do robienia zdjęć z bliska, cały czas trzymaj dłoń nad spustem migawki, jakbyś tylko trzymał aparat, aby się nie kołysał. Niewielkie ciśnienie zwolni migawkę, a aparat zrobi resztę. Zrób tyle zdjęć, ile możesz. Podczas robienia zdjęć dobrze jest pochłonąć się czymś innym, udawać zainteresowanie czymś w innym kierunku, studiować przewodnik lub cokolwiek innego. Wszystko, co odwraca uwagę od tego, co naprawdę robisz. Jeśli ktoś do Ciebie podejdzie lub zostanie zapytany, to jak zareagujesz, zależy od Ciebie, ale zachowaj swój charakter, aby była to odpowiedź naturalna i mniej podejrzana. Zaprzeczaj wszystkiemu lub twierdz, że jesteś sławnym

fotografem ulicznym - to zależy od Ciebie - ale pamiętaj, że nie robisz niczego nielegalnego. Dostępny jest specjalistyczny sprzęt produkowany przez Leikę, który obejmuje dyskretny obiektyw, który robi zdjęcia pod kątem prostym itd., Ale podobnie jak większość rzeczy wytwarzanych obecnie przez Leikę są one zbyt drogie i niepotrzebne. Trochę nerwów będzie ci służyć znacznie lepiej. Dyskretne zdjęcia nie muszą być szczególnie dobrze skomponowane - nie bierzesz udziału w konkursie, po prostu muszą być wystarczająco jasne, aby dostarczyć Ci potrzebnych informacji.

Korzystanie z kamer dyskretnych

W „sklepach szpiegowskich" można znaleźć dowolną liczbę ukrytych kamer na sprzedaż w Internecie. Waham się, czy polecić którąkolwiek z nich - aby taki aparat był przydatny w teście penetracyjnym, musiałby być całkowicie przenośny, z dobrą żywotnością baterii i mieć wysokiej jakości kanał wideo. Takie kamery istnieją, ale nie za 200 dolarów, które większość tych miejsc pobiera. Jakość obrazu z tych kamer jest słaba i zawiera dużo szumów, co chociaż można wybaczyć w przypadku statycznego nadzoru pomieszczenia, nie jest odpowiednie dla szybko zmieniającego się środowiska, w którym można się znaleźć, potajemnie rejestrując cele w miejscach publicznych. To powiedziawszy, technologia stale się poprawia, kurczy i staje się tańsza, więc te porady mogą być coraz bardziej niedokładne.

Fotografia nocna

Dyskretne fotografowanie nocą to wyjątkowe wyzwanie. Nawet drogie lustrzanki jednoobiektywowe obsługujące ekstremalnie wysokie czułości ISO będą słabo działać w bardzo słabym świetle bez lampy błyskowej. Możliwe jest jednak fotografowanie w całkowitej ciemności przy użyciu aparatów 35 mm wyposażonych w film na podczerwień i lampę błyskową. Jest to dziedzina fotografii, o której w dzisiejszych czasach rzadko się mówi ze względu na powszechność aparatów cyfrowych (słabo radzących sobie w polu podczerwieni) oraz kamer cyfrowych wyposażonych w tryb Night Shot. Piękną rzeczą w lampie błyskowej na podczerwień jest to, że jest ona całkowicie niewidoczna w ciemności nawet kilka stóp od obiektu. Film jest drogi i kosztuje około 20 dolarów za rolkę, a obróbka nie jest tania, ale w przypadku dyskretnej fotografii nocnej naprawdę nie masz wyboru. W niektórych modelach kompaktowych aparatów cyfrowych (takich, które nie filtrują podczerwieni w celu poprawy jakości obrazu) można zbudować filtr obiektywu podczerwieni. Jednak do prawidłowego funkcjonowania wymagany jest zbyt długi czas naświetlania, co nie jest zgodne z naszymi potrzebami.

Wyszukiwanie informacji ze źródeł publicznych i Internetu

Około 90 procent informacji potrzebnych każdemu do złamania zabezpieczeń jest dostępnych bezpłatnie; trudną częścią jest rozpoznanie i przeanalizowanie go. Z pozostałych 10 procent, znacznie ponad połowę można zwykle wywnioskować z tych 90. W przypadku każdego celu istnieje zwykle tylko ograniczona liczba sensownych wniosków. Nigdy nie było to bardziej prawdziwe niż teraz w XXI wieku. Dzięki wszechprzenikającej naturze Internetu gromadzenie informacji nigdy nie było łatwiejsze; Jesteśmy teraz kulturą ekshibicjonistów informacji i wiele osób ma blogi, osobiste strony internetowe i profile w serwisach społecznościowych. W połączeniu z faktem, że praktycznie wszystko, co jest napisane w Internecie, jest indeksowane przez wyszukiwarki i że jest możliwy dostęp do wielu baz danych o firmach i osobach, Internet jest ogromnym zasobem, z którego można czerpać. W tej sekcji omówię zasoby, które okazały się przydatne podczas badania celów. Chociaż w żadnym wypadku nie jest to wyczerpujące, wystarczy zilustrować punkty, które tu przedstawiłem.

Górnicze portale społecznościowe

Serwisy społecznościowe są nieocenione. Pozwalają swoim użytkownikom przesyłać profile, hostować blogi (blogi), udostępniać zdjęcia i inne media, grać w gry z innymi użytkownikami i nawiązywać

znajomości. Facebook, wiodąca witryna, ma ponad 150 milionów użytkowników, podczas gdy MySpace przekroczył 100 milionów, przyciągał 230 000 nowych użytkowników dziennie. Osobiste profile w sieciach społecznościowych mogą być interesujące, choćby dlatego, że ludzie zakładają, że istnieją w próżni i nie będą z nimi powiązani w prawdziwym świecie. W konsekwencji takie profile mogą dostarczyć wielu informacji o docelowym personelu: adresy e-mail są przydatne do śledzenia większej ilości informacji w Internecie, zdjęcia pozwalają zidentyfikować pracowników na miejscu, wszelkie dane osobowe mogą pozwolić ci udawać tę osobę. Jeśli jesteś biznesmenem, bardzo dobrym pomysłem jest uważanie na to, co publikujesz w internecie. Facebook i MySpace, choć bardzo popularne, nie są bynajmniej jedynymi portalami społecznościowymi. Na przykład w Holandii rdzenny Hyves jest znacznie bardziej popularny niż którykolwiek z nich. Pamiętaj o tym podczas badania celów. Znacznie bardziej interesujące dla testera penetracji są portale społecznościowe zorientowane na biznes. Kierując się mniej więcej tymi samymi zasadami określonymi przez wspomniane wcześniej firmy, strony takie jak Linkedin.com ułatwiają profesjonalne nawiązywanie kontaktów. W październiku 2008 roku miał ponad 30 milionów zarejestrowanych użytkowników. W przypadku LinkedIn chodzi o stworzenie internetowego CV i aktywne zapraszanie współpracowników, partnerów biznesowych i klientów do kontaktów. W ten sposób możesz zobaczyć, czy jesteś zainteresowany kontaktując się z kimś o określonym profilu lub zestawie umiejętności i możesz poprosić o skierowanie za pośrednictwem wzajemnej sieci kontaktów. Chociaż niektórzy użytkownicy wyznają filozofię otwartego networkingu, czyli akceptowania połączeń od każdego, kto ich zaprosi, jest to zniechęcane i (do pewnego stopnia) karane. W rezultacie czyjś profil na LinkedIn ujawnia ogromną ilość bardzo istotnych informacji. Zawiera:

• Obecny pracodawca.

• Aktualna pozycja.

• Poprzedni pracodawcy.

• Nazwy połączeń: można je ukryć, choć rzadko jest.

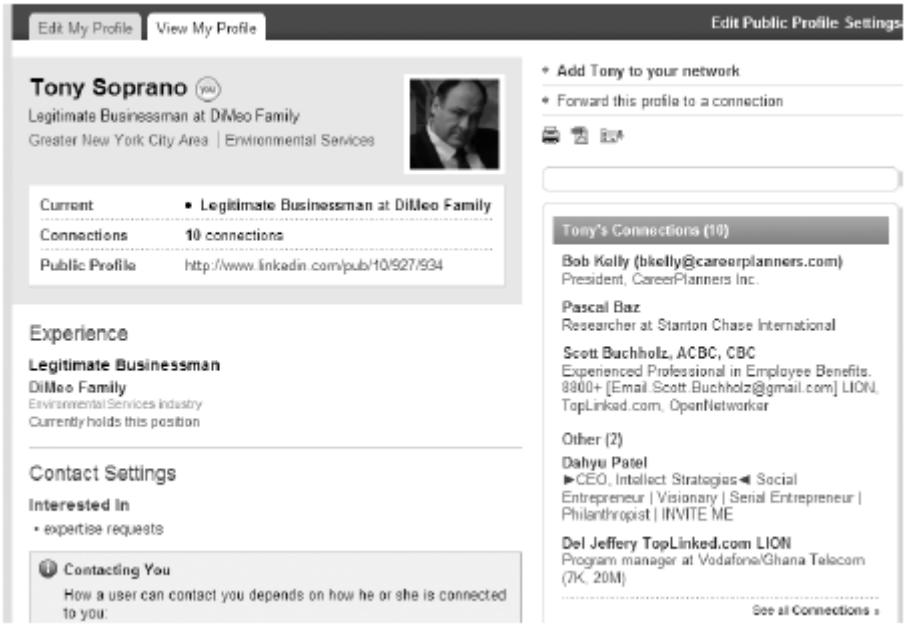
• Zalecenia: Możesz polecić współpracownika lub partnera biznesowego. Zalecenia od klientów są szczególnie przydatne do celów inżynierii społecznej.

• Zestaw umiejętności: jest to bardzo przydatne dla testera penetracji, ponieważ pozwala zebrać informacje o pracownikach dla określonej firmy, określić, do kogo skierować ataki socjotechniczne w celu uzyskania określonych informacji i określić, kto jest odpowiedzialny za kluczowe role, takie jak administracja, bezpieczeństwo, finanse i technologie informacyjne. Co więcej, każdy może utworzyć profil LinkedIn, dzięki czemu będzie to łatwiejsze udawanie dawnego przyjaciela lub kolegę celu. Budowanie wiarygodności za pomocą profilu Linkedin jest niezwykle łatwe. Potrzebujesz dwóch rzeczy:

• Połączenia: Jak wcześniej wspomniano, na LinkedIn istnieje wiele otwartych grup sieciowych. Kiedy dołączysz do jednego z nich, Twój adres e-mail zostanie wysłany do wszystkich uczestników, którzy następnie Cię zaproszą. Pozwala to bardzo szybko uzyskać kilkaset weryfikowalnych połączeń.

• Zalecenia: utwórz fałszywy profil i dodaj kontakty dla wiarygodności, a następnie użyj tego konta, aby polecić swój profil. Ogólnie rzecz biorąc, fałszywe profile powinny być obecnie używane przez bardzo duże firmy, więc fakt, że nikt nie wie o tobie, nie zostanie uznany za niezwykły.

Rozważmy ironiczny przykład pokazany poniżej



Witryny, takie jak pipl.com, gromadzą informacje o Tobie w oparciu o heurystykę wyszukiwarek i Bóg wie, co jeszcze. (Informacje są często potwornie niepoprawne, zwłaszcza jeśli masz wspólną nazwę). To powiedziawszy, takie strony mogą być interesujące i tylko trochę niebezpieczne, ponieważ te profile są tworzone bez Twojej zgody, a często bez Twojej wiedzy. To ciekawe ćwiczenie, które możesz raz na jakiś czas wykonać w Google i zobaczyć, co tam jest. Możesz być zaskoczony. Jeśli martwisz się o bezpieczeństwo w swojej organizacji, warto skorzystać z usług Google, aby sprawdzić, gdzie pojawia się nazwa Twojej firmy. Ponownie możesz być zaskoczony. Jeśli odpowiadasz za bezpieczeństwo informacji w swojej organizacji, powinieneś rozważyć stworzenie polityki sieci społecznościowych do użytku poza biurem. Zakaz używania nazwy firmy w profilach osobistych i w korespondencji elektronicznej, aby utrudnić oszustom podszywanie się pod pracownika innego biura.

Odkrywanie firmowych witryn internetowych

Strony internetowe organizacji docelowych są pod wieloma względami najgorszymi winowajcami, jeśli chodzi o wyciek informacji. Często istnieje możliwość uzyskania dostępu do katalogów pracowników, które zawierają szczegółowe informacje dla inżynierów społecznych. Dane powszechnie dostępne obejmują:

• Imię.

• Identyfikator działu / działu.

• Pracownik numer.

• Biuro fizyczne.

• Numer telefonu stacjonarnego Często numer telefonu komórkowego dla pracowników sprzedaży.

• Zdjęcie.

Dobrą praktyką jest ograniczanie firmowych katalogów do intranetów, ale w dużych firmach zatrudniających wielu pracowników w wielu biurach, do których mogą również potrzebować się klienci lub potencjalni klienci, nie zawsze jest to uważane za wykonalne.

(Bardzo) krótki przewodnik po wykorzystaniu Google

Google może być używany na wiele sposobów do zbierania informacji o celu. Możliwe jest udostępnienie Google różnych filtrów w polu wyszukiwania, aby dokładnie określić wyniki, które chcesz zobaczyć. Na przykład, jeśli ktoś szukał witryn internetowych używanych przez fikcyjną firmę Lithex Corporation, osoba atakująca może użyć następującego wyszukiwanego hasła:

site: lithexcorp.com -www.lithexcorp.com

Spowoduje to zwrócenie wszystkich witryn należących do Lithex (zaindeksowanych przez Google) innych niż witryna publiczna. Jest to przydatne do wyszukiwania witryn, które mają być poza zasięgiem opinii publicznej, takich jak ekstranety, fora i ogłoszenia, katalogi firmowe, witryny testowe (przydatne, ponieważ są zwykle mniej bezpieczne), poczta internetowa, interfejsy zarządzania, kamery sieciowe i wiele innych. Oto kilka innych przykładów:

site: lithexcorp.com filetype: doc

Zwraca wszystkie dokumenty słowne znalezione w dowolnej witrynie Lithex. Może to być przydatne, ponieważ dokumenty pakietu Office zwykle zawierają wiele niezanieczyszczonych informacji osadzonych w szablonie dokumentu, takich jak nazwiska, adres e-mail, a nawet topologia sieci. W tym przypadku .doc można zastąpić .xls. Spróbuj wyszukać .mdb. Są to bazy danych MS Access, a ich hasła można łatwo zhakować (jeśli są nawet chronione). Aby znaleźć strony zawierające słowo „hasło", użyj:

site: lithexcorp.com hasło

Aby znaleźć kamery sieciowe Axis, użyj:

site: lithexcorp.com inurl: indexFrame.shtml Axis

Istnieje wiele, wiele innych przykładów. Zamiast zajmować więcej miejsca, radzę zapoznać się z bazą danych Google Hacking pod adresem http: // johnny. ihackstuff.com/ghdb.php. Powinieneś także pobrać oprogramowanie o nazwie Goolag, które automatyzuje proces wyszukiwania informacji w Google:

http://www.goolag.org.

Innym sposobem korzystania z Google jest sprawdzenie, co inni ludzie mówią o celu. Dobrym tego przykładem są komunikaty prasowe stron trzecich. Aby wzmocnić własny wizerunek firmy, dostawcy często publikują informację prasową, gdy sprzedają technologię klientowi z najwyższej półki. Dotyczy to szczególnie oprogramowania. Innym miejscem wyszukiwania jest Usenet (lub Grupy dyskusyjne Google, jak to się czasem mylnie nazywa). Obecnie nie jest tak powszechnie używany, wraz z pojawieniem się internetowych systemów tablic ogłoszeniowych, ale nadal jest bardzo popularny wśród starszych techników. Mówiłem bardzo krótko o Google, nie dlatego, że ma mniejsze znaczenie. Wręcz przeciwnie, ale ponieważ jest on używany do zbierania informacji, został szczegółowo omówiony w innych miejscach, zarówno w wersji drukowanej, jak i online, i nie chcę wpaść w pułapkę powielania tutaj pracy innych. To wyszukiwarka, której możesz użyć do wyszukiwania. Wystarczająco powiedziane.

Zbieranie informacji z Maltego

Przydatne narzędzie do zbierania informacji, a zwłaszcza wykreślania relacji między poszczególnymi danymi, nazywa się Maltego i można je pobrać ze strony http://www.paterva.com/maltego. Dostępna jest bezpłatna (społecznościowa) wersja do pobrania. Działa dobrze, ale jeśli używasz go regularnie (a po prostu możesz), polecam zakup pełnej wersji, która pozwala na nieskończoną liczbę wyszukiwań.

Maltego to aplikacja wywiadowcza i kryminalistyczna. Umożliwia wyszukiwanie i gromadzenie informacji, a także przedstawianie tych informacji w sposób graficzny. Ponieważ Maltego może zidentyfikować kluczowe relacje między fragmentami informacji, jest niezwykle przydatnym narzędziem podczas przeprowadzania wstępnych badań do wszelkiego rodzaju testów penetracyjnych, a szczególnie w testach z wykorzystaniem inżynierii społecznej. Obraz mówi więcej niż tysiąc słów, więc rysunek przedstawia przykład:

W lewej kolumnie znajduje się kilka elementów, które Maltego nazywa „podmiotami". Podmiotem może być imię i nazwisko osoby, adres e-mail, lokalizacja fizyczna, nazwa domeny internetowej i tak dalej. Przeciągasz elementy do głównego okna i wypełniasz je danymi. Możesz wysyłać zapytania do internetowych baz danych i wyszukiwarek, aby odkrywać relacje. Klikając prawym przyciskiem myszy w ten podmiot proszę Maltego o znalezienie wszystkich stron internetowych i adresów e-mail powiązanych z tą osobą. Zwracana jest ogromna liczba wyników, w tym wiele fałszywych alarmów, z których większość jest oczywista i można je usunąć. Już teraz widać wzajemnie powiązane relacje między adresami e-mail a witrynami internetowymi. Jeśli poprosimy Maltego o zwrot wszystkich blogów znanych z „Wila Allsoppa", pojawi się kolejny obrazek. W tym prostym przykładzie ustaliłem, że Wil Allsopp regularnie publikuje posty na stronach internetowych związanych z bezpieczeństwem, uzyskał wiele adresów e-mail i upewniłem się, że ma profil na LinkedIn. To mniej niż minuta pracy. Mając czas i dobry plan analizy, Maltego pozwala wydobyć dużą ilość danych i nawiązać bardzo złożone relacje.

Korzystanie ze zdjęć satelitarnych

Obecnie istnieje wiele publicznych źródeł zdjęć satelitarnych ale zdecydowanie wyróżnia się Google Earth (http://earth.google.com).

Google Earth to płynna mozaika zdjęć satelitarnych wykonanych z różnych źródeł i regularnie aktualizowanych. Właściwie to o wiele więcej, ale interesują nas zdjęcia. Większość cywilizowanych miejsc (a nawet Walia) jest pokazywana w wysokiej rozdzielczości i dość bezkrytycznie. Są to skrajne

przykłady, ale mam nadzieję, że moja uwaga jest jasna, zdjęcia satelitarne powinny być pierwszym przystankiem podczas analizy celu. Oprócz ogólnego wyczucia otoczenia, niektóre przydatne informacje, które można uzyskać, obejmują lokalizację wejść, wyjść i parkingów (na których można przeprowadzić bezprzewodowe hakowanie), czy lokalizacja nadaje się do fotografii publicznej i gdzie znajdują się wszystkie śmietniki . Kolejną fajną rzeczą w Google Earth jest to, że możesz nakładać ścieżki GPS i współrzędne na mapy i obrazy satelitarne lub odwrotnie wskazywać potencjalne cele i punkty w oprogramowaniu, a następnie przesyłać ich współrzędne do urządzenia GPS.

Krótka uwaga na temat ponownego wykorzystania hasła. . . .

Nie jest to technika, której będziesz używać podczas testu penetracji, ale warto o tym pamiętać, choćby po to, by zwrócić uwagę. Ludzie mają konta w wielu systemach w internecie; blogi, poczta internetowa, fora itp., a poziom bezpieczeństwa wszystkich tych odmiennych usług nie jest równy. Przy odrobinie badań i przy użyciu narzędzi takich jak Maltego i Google można określić, kto z czego korzysta przy minimum badań. Jeśli twoje konto w systemie o niskim poziomie bezpieczeństwa jest zagrożone, a twoje hasło jest takie samo w innych systemach, masz problem. Nie ma innego prostego rozwiązania niż ostrożność, z kim się rejestrujesz i używanie różnych haseł i adresów e-mail w przypadku zwykłych i poważnych kont. Nigdy nie przechowuj poufnych informacji, takich jak hasła, klucze szyfrowania i numery kart kredytowych na kontach poczty internetowej.

Elektroniczny nadzór

Covert Electronic Monitoring (CEM) to jedno z największych zagrożeń dla organizacji narażonych na szpiegostwo komercyjne, dlatego zespoły testujące penetracyjnie są wykorzystywane do symulacji fizycznego wtargnięcia napastnika, którego celem jest zainstalowanie urządzeń podsłuchowych we wrażliwych obszarach. Przez urządzenia podsłuchowe mam na myśli:

• Tradycyjne „pluskwy” w pokoju: Profesjonalne pluskwy (a nie te kupowane tanio w „sklepach szpiegowskich”) są zdolne do wyjątkowo długotrwałego autonomicznego działania. Podczas przeszukiwania przestrzeni sufitu w 2002 roku mój zespół znalazł pluskwę która został umieszczony przez nieznanego napastnika prawdopodobnie kilka lat wcześniej i nadal jest bardzo aktywny. Czasami używa się również kamer dyskretnych, ale w szpiegostwie komercyjnym wideo jest mniej powszechne niż nagrywanie głosu i szpiegowanie danych. Ogólnie rzecz biorąc, pluskwy są zaprojektowane do przesyłania głosu za pośrednictwem sygnału radiowego do odbiornika. Zasięg sygnału zmienia się w zależności od siły transmisji i charakteru otaczającej nadbudowy. Częstotliwości, na których transmitują błędy, również różnią się w zależności od tego, ile zapłaciłeś za takie urządzenie, ale także od regionu, ponieważ rządy mają tendencję do licencjonowania różnych długości fal. Będzie to jednak miało niewielkie znaczenie dla przestępców i szpiegów korporacyjnych.

• Zaczepy telefoniczne: można je umieścić praktycznie w dowolnym miejscu wewnętrznego systemu telefonicznego, ale często celem są określone biura, a urządzenia są podłączone bezpośrednio do słuchawki lub w linii z systemem telefonicznym. Lubię pluskwy pokojowe, są one zwykle przeznaczone do przesyłania sygnałów radiowych.

• Zaczepy sieciowe: mogą to być urządzenia fizyczne, które są podłączone do wrażliwego kabla lub „skrzynki pełzające”, samodzielne autonomiczne komputery dyskretne, które wykonują różnorodne zadania monitorowania. Stuknięcia sieciowe przekazują informacje atakującemu za pośrednictwem własnego połączenia internetowego organizacji lub łącza GSM.

• Monitorowanie oprogramowania: Dostępnych jest wiele różnych programów do zdalnego monitorowania stacji roboczych. Zazwyczaj takie oprogramowanie jest używane do przechwytywania

naciśnięć klawiszy, zapisywania haseł i udzielania zdalnego dostępu do plików i zasobów sieciowych. Zaleca się, aby takie oprogramowanie było tworzone we własnym zakresie, a nie pobierane z Internetu. Oprócz unikania oczywistych nieodłącznych zagrożeń, nie musisz martwić się, że Twój kod zostanie wykryty przez skanery antywirusowe i będziesz mieć możliwość dostosowania na podstawie testu po teście. Niektóre pakiety są dostępne w handlu, ale w większości są zawyżone i źle napisane. Każda organizacja zatrudniająca przyzwoity zespół testów penetracyjnych to zrobi aby mieć talent do tworzenia oprogramowania do zdalnego monitorowania.

• Sprzęt do rejestrowania kluczy: Są to małe urządzenia podłączone między stacją roboczą a klawiaturą. Naciśnięcia klawiszy są rejestrowane, a urządzenia fizycznie odzyskiwane w późniejszym terminie. Fizyczne rejestratory kluczy są ulubioną bronią szpiegów przemysłowych pracujących w docelowym miejscu. Można je łatwo zainstalować i chociaż jest oczywiste, jeśli ktoś ich szuka, ma tę zaletę, że oprogramowanie antywirusowe ich nie wykryje, co jest problemem w przypadku rejestratorów kluczy oprogramowania.

Należy pamiętać, że podczas przeprowadzania testu penetracyjnego nie jest konieczne instalowanie takich urządzeń w celu wykazania podatności na uszkodzenia. Jeden z klientów woli, aby zamiast, na przykład, instalować rejestrator kluczy sprzętowych, owijać małą opaską kablową wokół kabla klawiatury docelowej stacji roboczej. Zwykle jest to wystarczające w większości przypadków. Podczas gdy dyskusja na temat ukrytych błędów i podsłuchów jest fascynująca, jesteśmy dobrymi facetami i dlatego jesteśmy bardziej zainteresowani znajdowaniem i wyłączaniem tych pozostawionych przez złych. Mamy część poświęconą kontrwywiadowi, który obejmuje szereg tematów, w tym potajemne podsłuchiwanie. Creeper box to niewielki komputer PC, który jest potajemnie wdrażany w sieci docelowej. Powinno to być urządzenie typu „odpal i zapomnij", tj. Po uruchomieniu nie powinno wymagać dalszej interwencji, aby mogło działać. To, co robi pudełko, zależy od Ciebie, ale służy głównie do cichego siedzenia w tle i zbierania haseł, e-maili i innych informacji sieciowych, które są posłusznie dostarczane z powrotem w kluczowych odstępach czasu. Podczas budowania własnego pnącza należy wziąć pod uwagę kilka czynników:

• Forma: Oczywiście im mniejsze ogólne pudełko, tym lepiej. Na rynku dostępnych jest wiele małych obudów do komputerów PC. Kup taki, który spełnia Twoje potrzeby.

• Autonomia: Po rozmieszczeniu creeper box musi wykonywać swoje zadania bez udziału człowieka przez cały czas trwania misji. Wymaga to stabilnego oprogramowania i braku przerw w zasilaniu.

• Komunikacja: zebrane informacje muszą zostać przesłane z powrotem w bezpiecznej formie. Jeśli to możliwe, możesz użyć do tego lokalnego połączenia internetowego. Możesz jednak użyć karty mobilnej do przesyłania danych raz dziennie za pośrednictwem połączenia danych (GPRS / 3G).

• Funkcja: budowanie skrzynki wyłącznie do przechwytywania haseł jest stosunkowo proste. Należy jednak wziąć pod uwagę inne możliwości, takie jak przechwytywanie wiadomości e-mail, wykrywanie sieci, analiza podatności, i eksploatacji.

• Ukrywanie się i umiejscowienie: jak wspomniano wcześniej, fizyczny profil urządzenia powinien być jak najmniejszy, ale należy upewnić się, że pudełko nie zostanie wykryte w inny sposób. Creeper Box aktywnie sondujący sieć może wyzwolić wykrycie włamania do systemu i zostać wyśledzonym, ponieważ takie urządzenie wymaga adresu IP, który można wykryć podczas rutynowych audytów sieci.

Fizyczne umiejscowienie powinno być odpowiednie, aby zapewnić dobrą widoczność odpowiednią dla jego misji, będąc poza zasięgiem wzroku. Przynajmniej nie powinno wydawać się nie na miejscu. W misjach krótkoterminowych umieszczenie może być tak proste, jak znalezienie nieużywanego portu

sieciowego w nieużywanym biurze, podczas gdy misja długoterminowa (do której są przeznaczone pnącza) będzie wymagać większej pomysłowości. Takie okoliczności są wysoce specyficzne dla klienta. Rozważ ukrycie urządzenia jako czegoś nieszkodliwego, na przykład drukarki.

• Przechwytywanie „na żywo" sieci: jeśli możesz podłączyć się bezpośrednio do korporacyjnej sieci LAN, istnieje wiele narzędzi, które są przydatne do szybkiego przechwytywania haseł i skrótów haseł do łamania offline i przechwytywania zaszyfrowanych sesji. Najłatwiejszym i najbardziej funkcjonalnym narzędziem dla kogoś, kto podchodzi do tego tematu po raz pierwszy, jest aplikacja Windows o nazwie Cain. Jest dostępny bezpłatnie i można go pobrać ze strony http://www.oxid.it.

Cain koncentruje się na przechwytywaniu haseł w postaci zwykłego tekstu, zaszyfrowanych haseł (z których wiele jest w stanie złamać), ale moim zdaniem najbardziej użyteczną funkcją jest możliwość przekierowywania zaszyfrowanych sesji Secure Sockets Layer (SSL) i Secure Shell (SSH) innych użytkowników za pośrednictwem laptopa. Pozwala to zobaczyć zawartość sesji poprzez wykorzystanie nieodłącznych luk w kryptografii (różnych wersjach) używanych przez te protokoły. Kain nie jest jedynym narzędziem „węszącym" w sieci o milę, ale jeśli masz zamiar zabrać ze sobą tylko jedno, powinno to być to.

Covert Surveillance

Czasami trzeba trochę posunąć się do gromadzenia danych wywiadowczych, aby uzyskać informacje, które umożliwią lub przerwą test penetracyjny. Dzieje się tak zwykle w przypadku, gdy głównym źródłem informacji będą sami ludzie. Przykłady informacji, które możesz chcieć uzyskać, obejmują:

• Dane osobowe pracowników do ataków przed wysłaniem wiadomości. Na przykład adres domowy, którego nie można uzyskać w żaden inny sposób.

• Informacje o pojeździe - identyfikatory parkingowe są dobrym źródłem informacji, tablice rejestracyjne, logo, które można skopiować lub które można zidentyfikować , firmy kontraktowe.

• Lokalizacje miejsc spotkań personelu po pracy, służących do podsłuchiwania rozmów lub uzyskiwania informacji bezpośrednio od celu.

• Aby zrobić zbliżenie zdjęć identyfikatorów dostępu.

• Aby właściwie ocenić odzież lub logo pracownika, które możesz chcieć duplikować.

• Każdy inny cel, w którym musisz obserwować, a nie być obserwowanym.

Jest mało prawdopodobne, aby szczegółowy nadzór docelowego personelu poza godzinami w biurze będą usankcjonowane lub docenione przez klienta. Z tego powodu nie nadaję mu tutaj dużego priorytetu. Podczas negocjowania zasad zaangażowania należy omówić, w jakim stopniu odpowiedni jest jakikolwiek ukryty nadzór. Pamiętaj, że uzyskanie zielonego światła od klienta niekoniecznie oznacza, że dobrze przestrzegasz prawa. Wielu pracodawców słusznie jest ostrożnych w przeprowadzaniu ataków socjotechnicznych i inwigilacji wobec swoich pracowników, które mogą skutkować utratą zaufania między firmami i ich pracownikami oraz procesami sądowymi. W każdym przypadku Twoim obowiązkiem jest zapoznanie się z kwestiami prawnymi związanymi z tego rodzaju pracą w Twojej jurysdykcji. W dodatkach omówimy niektóre istotne przepisy. Przykładowe cele nadzoru obejmują:

• Pojazdy: ludzie zostawiają rzeczy w samochodach. Różnego rodzaju rzeczy. Dokumenty w jawnie oznaczonym NATO SECRET, dokumentację medyczną, a nawet dość kompromitujące fotografie. Chociaż nie polecam włamywania się do samochodów, spacer po firmowym parkingu może być bardzo

odkrywczy. Śledzenie i sprawdzanie pojazdów poza terenem zakładu może umożliwić fotografowanie pozwoleń na parkowanie na parkingach firmowych (w celu późniejszego powielenia). Może to być bardzo przydatne. Dostęp do parkingów często pozwala całkowicie ominąć ochronę.

• Personel: Były kolega, w poprzednim życiu pracował dla agencji rządowej na stanowisku kontrwywiadowvy. Jego zadaniem była ocena podatności personelu pełniącego różne role na elementy wywrotowe, poprzez przekupstwo lub nietrzeźwość. Dowiedział się, gdzie się spotykali, zaprzyjaźnił się z nimi, podał im alkohol i zobaczył, czy mógłby zmusić ich do rozmowy. Moim zdaniem to najlepsza praca na świecie, ale wystarczy. Firmy i departamenty rządowe są często bardzo zainteresowane tym, jakie informacje pracownicy przepuszczą w środowisku społecznym. Coraz popularniejsze stają się testy, których jedynym celem jest ustalenie tych informacji.

Podsumowanie

To była kluczowa część i wiele zostało omówione. W przeciwieństwie do innych części, w których skupiono się na jednym temacie, gromadzenie informacji wymaga zrozumienia wielu odmiennych tematów. W tym rozdziale omówiono następujące kwestie:

• Nurkowanie w śmietniku - to zbieranie informacji poprzez sortowanie rzeczy odrzucanych przez firmy. Powinieneś wiedzieć, czego szukać i co zrobić, gdy to znajdziesz.

• Analiza kryminalistyczna - są to techniki używane do obrazowania przechwyconych mediów i analizowania ich pod kątem poufnych danych lub danych, które byłyby przydatne przy udoskonalaniu testu penetracji fizycznej.

• Surfowanie przez ramię - praktyka gromadzenia haseł i szpilek do drzwi poprzez ścisłą obserwację personelu docelowego.

• Gromadzenie danych fotograficznych - Zarówno techniczne, jak i dyskretne aspekty związane z nadzorem fotograficznym.

• Inteligencja open source - wykorzystywanie Internetu do zbierania informacji o docelowych organizacjach i personelu, a także o niektórych powiązanych technikach inżynierii społecznej.

• Nadzór elektroniczny - obejmował podsłuch, podsłuchy telefonu i wprowadził koncepcję „pnącza".

• Tajny nadzór - krótkie wprowadzenie do potajemnej obserwacji personelu docelowego.

Na początku stwierdziłem, że jednym z jego celów jest pomoc w myśleniu jak napastnik i mam nadzieję, że przyniosło to przynajmniej umiarkowany sukces. Zrozumienie, jak działa umysł intruza, ma kluczowe znaczenie zarówno dla zespołu przeprowadzającego testy penetracyjne, jak i dla osób, których zadaniem jest zapewnienie bezpieczeństwa obiektów.