Gromadzenie odpowiedniego sprzętu

„ Nie ma znaczenia, ile sprzętu używamy; ważne jest, abyśmy byli mistrzami wszystkiego, z czego korzystamy ”. - Sam Abell

Część sprzętu potrzebnego do przeprowadzenia testów penetracyjnych jest oczywista, a część nie. Część jest konieczna, a część po prostu miło jest mieć. Ta część dotyczy zestawu, którego używamy i dlaczego go mamy. Najprawdopodobniej zaczniesz od małego podstawowego zestawu sprzętu, który z czasem będziesz rozbudowywać, gdy wymagania będą dyktować dodanie nowego sprzętu. W każdym razie elektronika szybko się starzeje, więc nie ma sensu wydawać pieniędzy na coś, co stanie się przestarzałe i ostanie w Twojej szafie. Ta część nie jest bynajmniej wyczerpująca; przydatnych jest wiele innych urządzeń, z których część jest omawiana w całym tekście. Należy zauważyć, że omawiamy podstawy; główne kategorie i te decyzje są często ubarwione przez moje własne preferencje.

Karta „Get of Jail Free”

Jeśli masz zamiar zabrać ze sobą tylko jedną rzecz, niech tak będzie. To, co nazywamy kartą „Get of Jail Free” to list lub formularz podpisany przez klienta w sposób formalny i kategoryczny, potwierdzający i upoważniający do wykonania testu. Powinien być podpisany przez co najmniej jednego (a najlepiej dwóch) starszych rangą funkcjonariuszy firmy, a jeśli pozwalają na to zasady zaangażowania, również dyrektor ds. informatyki lub większość starszych pracowników ochrony. Ich dane kontaktowe muszą być obecne i muszą być osiągalne podczas testu! Ponadto zalecane są również informacje o zespole testującym, takie jak nazwiska, firma testująca i określone cele. Jeszcze jeden punkt, nie noś tylko jednego. Możesz go zgubić lub mogą ci go skonfiskować. Przyznaj się do posiadania jednej kopii i pokazuj duplikaty tylko organom ścigania, jeśli masz pecha, że musisz to zrobić. Każdy członek zespołu powinien mieć co najmniej dwie kopie i powinny to być oryginały, a nie kserokopie. Przed przystąpieniem do testu, a najlepiej w momencie kulminacji wymagań dotyczących zakresu, należy przedstawić formularze klientowi i upewnić się, że są one podpisane na miejscu i nigdy, przenigdy nie przesłane (per procurationem) w imieniu innej osoby. Ostatnią rzeczą, jakiej chcesz, jest znalezienie pracy dla oficera firmy, który przekroczył swoje uprawnienia i zaprzecza, że kiedykolwiek cię spotkał. Rozważ to studium przypadku, aby zilustrować przedstawione przeze mnie uwagi.

Gdy testy fizyczne idą źle

Kris stwierdził, że początkowe etapy penetracji Lithex Pharamacuticals w Chicago były bardzo proste. Czekał przed drzwiami dla palaczy w swoim prążkowanym garniturze, z Marlboro w dłoni, czekając na pojawienie się kilku prawdopodobnych celów. Po kilku minutach słuchania ich przekomarzania się, wszedł za nimi z powrotem do środka i po kilku chwilach przeszedł przez marmurowy hol i wjechał windą na 8. piętro i sale konferencyjne. Nie wiedział, że ochrona śledziła go od chwili, gdy postawił stopę na parkingu i teraz go szukała. W chwili, gdy położył dłoń na klamce w pustym miejscu, usłyszeli słowa, które wszyscy w jego pracy modlą się, że nigdy nie usłyszą „Stój! Uzbrojona ochrona! ”. Powoli się odwrócił, a skrajnie zdenerwowany wyraz twarzy strażnika był bardziej niepokojący niż Glock 19 wskazał na niego drżącą ręką. Wkrótce potem Kris został przykuty do ławki w pokoju ochrony. Spokojnie próbował wyjaśnić kim jest, dlaczego tam był i wskazać zapieczętowany podpisany list, który to potwierdził. Strażnik wyjął list z kieszeni i przeczytał go, a potem z uśmiechem podarł i wrzucił do kosza na śmieci. To była jedyna kopia Kris. Pół godziny później przyjechała policja i aresztowała Krisa. Po nieprzyjemnym wieczorze w więzieniu okręgowym udowodniono jego niewinność, ale niestety dla Krisa, mimo że nie został oskarżony, został aresztowany za przestępstwo. To jest coś, co będzie w jego aktach za każdym razem, gdy będzie ubiegał się o ochronę w przyszłości. Mam nadzieję, że lekcja tutaj jest prosta. Chociaż ochroniarz nie powinien był zniszczyć jego listu, to zrobił. Zawsze miej więcej kopii! I nigdy nie kłóć się z ludźmi z wycelowanym w ciebie pistoletem Nie mogę tego wystarczająco

podkreślić. Oto przykładowy formularz autoryzacji bezpieczeństwa. Zapraszam do dostosowania go do swoich potrzeb.

Autoryzacja audytu bezpieczeństwa

Nazwisko testera: Podpis:

Firma testująca:

Data audytu bezpieczeństwa:

Podano cele audytu bezpieczeństwa:

Okaziciel tego dokumentu przeprowadza audyt bezpieczeństwa tych pomieszczeń przy pełnej wiedzy, wsparciu i upoważnieniu seniora

zarządzanie. Poświadczenia okaziciela można potwierdzić, kontaktując się z następującymi członkami kadry zarządzającej:

Imię i nazwisko: Stanowisko: Podpis: Telefon kontaktowy:

Imię i nazwisko: Stanowisko: Podpis: Telefon kontaktowy:

Imię i nazwisko: Stanowisko: Podpis: Telefon kontaktowy:

Noszącego należy traktować profesjonalnie i uprzejmie. Konsekwencje złego traktowania, znęcania się lub agresywnego zachowania będą poważne.

Sprzęt fotograficzny i do nadzoru

W tej sekcji omawiamy sprzęt fotograficzny.

Aparaty

Aparat przydaje się na każdym etapie testowania. Będziesz chciał zrobić zdjęcia obiektu, który będziesz penetrować, a także przedstawić fotograficzne dowody penetracji w swoim raporcie końcowym. Aparat w telefonie komórkowym naprawdę tego nie zrobi. To powiedziawszy, nie musisz wydawać ogromnych pieniędzy, chyba że chcesz mieć lustrzankę jednoobiektywową (SLR) z długim obiektywem, ale tak naprawdę nie jest to szczyt dyskrecji. Osobiście wolę tyle mocy, ile mogę uzyskać w dyskretnej obudowie - kompaktowy szybki aparat cyfrowy z dobrym obiektywem i dużą ilością pamięci. Na wszystkich etapach testów używam aparatów z doskonałej serii Canon Powershot G, zwłaszcza G9 i G10. Kamery te dają wyniki o jakości wirtualnej lustrzanki i są bardzo dyskretne.

Lornetka

Muszę mieć dobre powiększenie i zmieścić się w kieszeni, to ostatnie jest krytyczna. Naprawdę nie chcesz sięgać do plecaka stale lub kusić, aby zostawić ją w samochodzie. Para małych, opancerzonych gumą obiektywów wojskowych, będzie ci dobrze służyć, ale jak mówię, nie mam szczególnych preferencji. Lornetka jest przydatna podczas obserwacji personelu z dystansu i może być przydatna w atakach typu „surfowanie po ramionach” z dużej odległości.

Wyposażenie komputera

W przypadku zadań, które obejmują penetrację komputera, laptop jest krytyczny. Nawet w przypadku zadań, które tego nie robią, jest to pożądane. Jeśli udajesz pracownika, torba na laptopa dodaje wiarygodności. Rozważ zdobycie (i jeśli chcesz, zmodyfikowanie) docelowych wizytówek i włożenie ich

do plastikowej teczki na karty w torbie. Małe akcenty mogą wiele zdziałać. Ponownie, nie mam tutaj żadnych szczególnych preferencji; wystarczy dowolny nowoczesny laptop, ale poszukaj następujących:

• Co najmniej jeden giga pamięci RAM: umożliwia to jednoczesne uruchamianie wielu systemów operacyjnych. Pamięć RAM jest obecnie tania jak barszcz.

• Gniazda PCMCIA: Niektóre nowe laptopy unikają tego na rzecz całkowicie USB. Istnieje kilka doskonałych bezprzewodowych adapterów USB, które obsługują USB i będą one coraz bardziej rozpowszechnione, jednak zalecam wybór laptopa z gniazdem PCMCIA, ponieważ zwiększa to zakres dostępnych kart.

• Łączność bezprzewodowa: przydaje się, gdy jest wbudowana, ale nie jest zbyt przydatna do testowania sieci bezprzewodowej, ponieważ potrzebujesz zewnętrznych kart, do których możesz podłączyć anteny.

• Twarda łączność sieciowa: Jest to absolutna konieczność dla każdego fizycznego testu penetracyjnego, który zawiera element ataku komputerowego. Większość laptopów ma wbudowany port sieciowy, ale niektóre nie są urządzeniami czysto bezprzewodowymi.

• USB 2.0: jeśli chodzi o szybkość przesyłania danych, jest to ważna kwestia, jeśli musisz wykonać kryminalistyczne przechwytywanie. Zdecydowanie radzę laptopy PC w przeciwieństwie do komputerów Mac. Nie mam nic przeciwko Apple, a OSX jest bardzo ładny, ale będziesz pracować najczęściej w systemie Windows i Linux. Pewne oprogramowanie i techniki po prostu nie są dostępne na urządzeniach Apple.

• Możliwości szyfrowania: Twój laptop musi mieć zainstalowane pełne szyfrowanie dysku. W dzisiejszych czasach jest to zwykle wymóg kontraktowy. Jeśli twój laptop zostanie skradziony, naprawdę nie chcesz wyglądać jak rząd brytyjski, który próbuje wyjaśnić wszystkie utracone dane. Używam szyfrowania całego dysku PGP. Szyfrowanie, które pyta o hasło podczas rozruchu, a bez niego dysk twardy pozostaje bezpieczny. Jeśli ktoś wyjmie dysk i podłączy go do innego komputera, nadal nie będzie mógł go odczytać.

• Oprogramowanie do wirtualizacji: jak wspomniano powyżej, posiadanie dużej ilości pamięci RAM umożliwia jednoczesne uruchamianie więcej niż jednego systemu operacyjnego. Oprogramowanie takie jak doskonały VMWare lub Virtual Box pozwoli Ci to zrobić. Podczas wykonywania komputerowych testów penetracyjnych na miejscu może zaistnieć potrzeba jednoczesnego uruchomienia Linuksa i Windowsa na jednym laptopie.

• Dodatkowe baterie: zawsze warto mieć pewność, że są naładowane. Baterie Dell Latitude mogą wytrzymać około 6 godzin ładowania razem z bateriami, z którymi są dostarczane. Thinkpady obsługują baterie o długiej żywotności, które można nabyć osobno

Sprzęt bezprzewodowy

Całą część poświęciłem hakowaniu sieci bezprzewodowych. Tutaj przedstawię tylko zalecenia dotyczące sprzętu.

Podstawy sieci bezprzewodowej 802.11x

W bezprzewodowych kartach sieciowych 802.11x istnieją trzy standardy: a, b, g. Standard a jest praktycznie martwy. Prawie nie jest używany nigdzie poza domami. Standard b jest powolny i nieaktualny, więc najprawdopodobniej zakończysz testowaniem g. Mimo to ważne jest, aby mieć w zestawie karty reprezentujące wszystkie trzy standardy. Większość pracy bezprzewodowej, którą

będziesz wykonywać, będzie odbywać się w systemie Linux, dlatego ważne jest, aby mieć karty, które będą działać z tym systemem operacyjnym. Linux różni się od systemu Windows w tym, że sterowniki nie są specyficzne dla producenta, ale dla chipsetu. Może to być mylące, ponieważ wiele kart ma ten sam chipset, ale są one ponownie oznakowane przez różnych dostawców. I odwrotnie, karty, które mogą mieć podobną specyfikację, wydane przez tego samego producenta, mogą mieć zupełnie inne chipsety. Przy wyborze kart ważne są dwie rzeczy: chipset jest kompatybilny i obsługuje wstrzykiwanie pakietów. Wstrzykiwanie pakietów (i dlaczego jest to ważne) zostało omówione wcześniej - jest to ważna funkcja w bezprzewodowym hakowaniu, ale z prostego punktu widzenia sprzętowego wykonaliśmy za Ciebie ciężką pracę. Wszystko wymienione tutaj nadaje się do bezprzewodowego hakowania. Przy zamawianiu sprawdź specyfikacje, czy kod produktu jest prawidłowy, ponieważ chipsety różnią się znacznie nawet w obrębie producentów i zwykle nadają swoim produktom tę samą podstawową nazwę. W obu wymieniono karty i adaptery bezprzewodowe obsługujące wstrzykiwanie pakietów, o których wiadomo, że współpracują z BackTrack Linux Distribution:

Karty bezprzewodowe

Dostawca: Nazwa: Chipset

3Com: 3CRPAG175B: Atheros AR5212

Airlink: 101 AWLC4130: Atheros

Agere: ORiNOCO GOLD: Atheros

Alfa: AWUS036H: Realtek 8187L

Belkin: F5D6020v3: RTL8180

Belkin: F5D7011: Broadcom 4306

Buffalo: WLI-CB-G54HP: Broadcom BCM4318

Dlink: DWL-G650: Atheros AR5212 a / b / g

Linksys: WPC11v4: rtl8180

Motorola: WN825Gv2: Broadcom 4306

NetGear: WG511T: Atheros

SWEEX: LW051ver: 1.0 Atheros

Bezprzewodowe adaptery USB

Dostawca: Nazwa: Chipset

Airlink: 101 AWLL3026: zydas

Edimax: EW-7317UG: zd1211rw

Linksys: WUSB54gv4: Ralink 2570

Alfa: AWUS036H: Realtek RTL8187L

Dołączyłem tylko te urządzenia, o których wiem, że działają idealnie po wyjęciu z pudełka. Wiele innych również będzie działać.

Jednym z powodów, dla których wolę używać PCMCIA zamiast USB, jest to, że wiele kart PCMCIA ma gniazda do podłączenia anten zewnętrznych, co znacznie zwiększy twój zasięg. Anteny są dostępne w dwóch wersjach: wielokierunkowej, która zwiększa wzmocnienie sygnału przychodzącego we wszystkich kierunkach i kierunkowej, która zwiększa wzmocnienie sygnału przychodzącego i wychodzącego w linii wzroku. Anteny dookólne mogą służyć do zwiększania możliwości znajdowania punktów dostępu. Anteny kierunkowe lub Yagi doskonale nadają się do określenia, gdzie w budynku znajduje się punkt dostępowy i zwiększają zdolność do rozmowy z nim na odległość. Niektóre anteny można podłączyć bezpośrednio do karty; niektóre będą wymagały kabla adaptera (zwanego kablem typu pigtail).

Bluetooth

Bluetooth jest drugorzędny w stosunku do 802.11x×. Jako standard sieci bezprzewodowej jest stosunkowo rzadki i używany głównie jako protokół krótkiego zasięgu do interakcji z urządzeniem. Jednak ściśle ze sprzętowego punktu widzenia uwzględnione kwestie są w większości takie same, jak te dotyczące technologii bezprzewodowych już omówionych. Większość oprogramowania do hakowania Bluetooth jest oparta na systemie Linux i dlatego będziesz chciał użyć klucza sprzętowego Bluetooth, który działa od razu po wyjęciu z pudełka z systemami operacyjnymi Linux. Bluetooth jest protokołem przeważnie krótkiego zasięgu, więc anteny generalnie nie są brane pod uwagę. Fajną rzeczą w Bluetooth jest to, że dzieli widmo radiowe 2,4 GHz z 802.11x, co oznacza, że można (przy odrobinie lutowania) używać anten omówionych wcześniej z zestawem Bluetooth. Klucze poniższe działają po wyjęciu z pudełka z systemem Linux:

Dostawca: nazwa

Broadcom: GBU421

Formosa: Teletek Any

CNet: CBD-120 klasa 1

CNet: CBD-220 klasa 2

Broadcom: GeBL2179

Większość wewnętrznych urządzeń Bluetooth w laptopach działa dobrze z Linuksem, a wstrzykiwanie pakietów nie stanowi problemu, tak jak w przypadku 802.11x. Ponownie, urządzenia wymienione powyej to tylko te, które osobiście przetestowałem; jest wiele innych, które wykonają zadanie.

Globalne systemy pozycjonowania

Dobry odbiornik Global Positioning System (GPS) jest ważnym elementem zestawu. Umożliwia wykonanie następujących czynności:

• Zaznacz interesujące miejsca na mapie lub zdjęciu satelitarnym przed testem i nawiguj do nich z łatwością.

• Zaznacz interesujące miejsca na miejscu, na przykład, aby wskazać klientowi ważną lokalizację (na przykład miejsce, w którym mógł coś zostawić).

• Zwróć uwagę na lokalizację kamer, biur ochrony, aby Twój zespół mógł ich ominąć.

• Zaznacz obecność sieci bezprzewodowych.

• Poinformuj personel pomocniczy o tym, gdzie dokładnie jesteś. Na rynku jest wiele odbiorników GPS i możesz wydać trochę lub tyle, ile chcesz. Osobiście chcę mieć w urządzeniu:

• Zintegrowane mapowanie, dostępne w większości nowoczesnych telefonów, daje możliwość pokazania aktualnej lokalizacji na mapie cyfrowej. Jest to przydatne, ponieważ nie musisz odwoływać się do innych mediów.

• Zgodność z National Marine Electronics Association (NMEA) w zakresie przesyłania współrzędnych do komputera (przydatne do oznaczania lokalizacji bezprzewodowych punktów dostępowych w czasie rzeczywistym).

• Możliwość importu i eksportu tras i punktów. Punkty trasy umożliwiają wykreślenie predefiniowanego zestawu współrzędnych przed testem i śledzenie ich. Eksportowanie umożliwia wykreślenie pokonanej trasy w celu późniejszego uwzględnienia w raportach.

• Zgodność z Google Earth jest przydatna podczas pisania raportu. Lubię wyznaczać trasę za pomocą zdjęć satelitarnych.

Moim ulubionym urządzeniem, które spełnia wszystkie te wymagania, jest Magellan eXplorist XL. Jest niezwykle wytrzymały, szybki i niezawodny i moim zdaniem powinien być standardem dla konsultantów na całym świecie. Kolejny zestaw, który uważam za niezbędny, szczególnie gdy jest to urządzenie podręczne

GPS może być zbyt rzucający się w oczy, jest zamontowany na nadgarstku komputer GPS Suunto X9i. To urządzenie wymienia trasy i punkty z komputerem i chociaż (oczywiście) nie zawiera wbudowanego mapowania, nawiguje bezbłędnie i jest wyposażone w narzędzie do komunikacji z Google Earth. GPS staje się standardem w zaawansowanych smartfonach. To do penetracji celów testowych, jest idealnym rozwiązaniem. Drogi biznesowy smartfon zapewnia własną wiarygodność i jest mało prawdopodobne, abyś się wyróżniał w jakimkolwiek środowisku korporacyjnym, jeśli będziesz się nim bawić.

Narzędzia do otwierania zamków

Nie zamierzam omawiać każdego rodzaju narzędzia do otwierania zamków pod słońcem; Po prostu nie mam miejsca. Zamiast tego omawiam narzędzia potrzebne do pokonania zamków omówionych wcześniej. Są to głównie te o konstrukcji typu pin tumbler, ale obejmuję również zamki rurowe i chronione, a także kłódki.

Tradycyjne zestawy wytrychów - używane do podnoszenia szpilek w zamkach bębnowych - są dostępne w zestawach od trzech lub czterech wytrychów do kilkudziesięciu. Zwykle będziesz używać tylko jednego lub dwóch typów: grabie i klucza skrętnego, więc nie ma sensu wydawać dużo pieniędzy na zestaw over-top. Osobiście uważam, że zestaw 14 picków, który zawiera wszystko, czego potrzebujesz za około 15-20 $, to dobry wybór. Wybierając zestawy wytrychów, należy zwracać uwagę na ścisłe tolerancje produkcyjne i wysokiej jakości materiały. Nie ma nic bardziej żmudnego (i zawstydzającego) niż wytrych w zamku klienta. Szukaj kilofów wykonanych ze stali sprężynowej, która jest trwała i elastyczna. Należy pamiętać, że europejskie i japońskie zamki są często węższe niż ich amerykańskie odpowiedniki. Nie mam pojęcia, dlaczego tak jest; jednak dostępne są zestawy wytrychów, które uwzględniają to i działają dobrze z zamkami amerykańskimi. Istnieją narzędzia do otwierania wszelkiego rodzaju zamków, które obejmują:

• Zamki rurowe: Bardziej odporna wersja zamka z bolcem. Są one najczęściej widoczne na automatach sprzedających. Są tutaj interesujące, ponieważ służą również do zabezpieczania laptopów.

• Kłódki: można je znaleźć wszędzie. Kłódki można zwykle łatwo otworzyć za pomocą odpowiednich narzędzi. Często nie jest nawet konieczne atakowanie mechanizmu blokującego, ponieważ kłódki mają własne unikalne luki.

• Zamki chronione: Zamki chronione są jednymi z najstarszych projektów nadal w powszechnym użyciu. Dzięki odpowiednim narzędziom - często o bardzo prostej konstrukcji - zamki te można łatwo otworzyć. Zamki chronione są nadal powszechnie używane w Wielkiej Brytanii zarówno w domach, jak i firmach.

Na rynku dostępne są różne urządzenia zaprojektowane w celu zmniejszenia trudności i zwiększenia szybkości obejścia zamka. Poniżej wymieniono najpopularniejsze i najbardziej istotne:

• Pistolet do otwierania zamków - zgodnie z mitologią otwierania zamków SnapGun został opracowany dziesiątki lat temu, aby umożliwić funkcjonariuszom policji, którzy nie byli biegli w sztuce otwierania zamków, otwieranie zamków przy minimalnych instrukcjach. Zamiast otwierania zamków tradycyjnymi technikami grabienia, Snap Gun wykorzystuje transfer energii. Podstawowy model „zatrzaskuje się", ponieważ większość szpilek znajduje się w górnej części zamka w Ameryce Północnej. W Europie i poza nią często jest odwrotnie. (Ponownie nie mam pojęcia, dlaczego). Tak więc istnieje model tego urządzenia wykonany wyłącznie dla zamków europejskich, przypuszczalnie dla ludzi niewystarczająco bystrych, aby odwrócić to do góry nogami. Należy zauważyć, że wytrych nie jest panaceum i nadal wymaga pewnych umiejętności (i klucza skrętnego).

• Elektryczny wytrych - Elektryczny lub wibracyjny wytrych umożliwia kopiowanie dokładnego ruchu grabienia wiele razy na sekundę. Pistolet zgrabia cylindry ze sworzniami i bębnami za pomocą szybkiego ruchu uderzającego w górę iw dół, co powoduje rozdzielenie się górnych i dolnych sworzni, osiągając linię ścinania. Te kostki są drogie i osobiście nigdy nie miałem z nimi do czynieia, mimo że wszyscy inni mówią mi, jak łatwe są w użyciu. Przeczytaj w tym, co chcesz.

Sprzęt kryminalistyczny

Proces kryminalistyczny składa się z dwóch etapów: gromadzenia i analizy danych. Do akwizycji danych w laboratorium potrzebny jest następujący sprzęt: dedykowany komputer ze zintegrowaną elektroniką napędu (IDE) i Porty Small Computer Systems Interface (SCSI), do których można podłączać dyski twarde. Jeśli nośnik znajduje się na cdrom, dvd, dyskietce lub usb, to oczywiście będziesz musiał mieć możliwość ich odczytania. Jednak w terenie, w którym dostęp do mediów jest krótkotrwały, musisz polegać na laptopie lub dedykowanym urządzeniu kryminalistycznym, takim jak Talon, co nie jest idealne. Ten drugi scenariusz jest z naszej perspektywy mało prawdopodobny.

Analiza danych jest czymś, co zawsze będziesz przeprowadzać w bazie - scenariusz jest taki, że nośniki zostały nabyte podczas wyrzucania na śmieci i chcesz je przestudiować pod kątem informacji, które będą użyteczne. Jeśli chodzi o oprogramowanie analityczne, bardzo polecam doskonały darmowy zestaw narzędzi Helix firmy e-Fence. Jest to bootowalna płyta CD, która automatyzuje pobieranie danych do komputera. Przechowuj puste dyski twarde o dużej pojemności, aby przechowywać obrazy z akwizycji. Helix posiada również szereg narzędzi, które pozwalają na dogłębną analizę przechwyconych danych, czyli nawet jeśli dane pliki zostały usunięte i / lub dyski lub tokeny zostały po sformatowaniu nadal można odzyskać dane.

Sprzęt komunikacyjny

Członkowie zespołu na miejscu i z powrotem w bazie powinni być w ciągłej komunikacji. Najbardziej oczywistym rozwiązaniem są telefony komórkowe i z reguły działa to dobrze. Każdy telefon komórkowy jest do tego odpowiedni, jednak istnieją pewne zaawansowane kwestie. Na przykład komunikacja

przez telefon komórkowy nie jest szyfrowana jako taka. Czasami może być korzystne wdrożenie dodatkowej warstwy zabezpieczeń. Rozwiązanie, które lubię, działa w następujący sposób: każdy członek zespołu ma nowoczesny telefon komórkowy, który obsługuje nieograniczony szerokopasmowy dostęp do Internetu oraz zestaw słuchawkowy Bluetooth. Darmowy internetowy program Voice over IP (VoIP) Skype jest zainstalowany na każdym telefonie. Skype jest przydatny, ponieważ obsługuje konferencje, umożliwiając wszystkim członkom zespołu stały kontakt, a także domyślnie korzysta z szyfrowania. Jego niewielki wpływ na sygnalizację i protokoły ruchu oznaczają, że jakość głosu jest zaskakująco dobra. Ponadto nie generujesz ogromnych rachunków za telefon komórkowy, co zawsze jest pomocne. Gdziekolwiek mieszkasz, masz do wyboru wiele telefonów i pakietów. Należy unikać krótkofalówek; są uciążliwe i rzucają się w oczy. Jedynym przypadkiem, w którym poleciłbym ich użycie, byłyby okoliczności, w których wzmacniają one twoją osobowość, tj. jeśli jesteś ubrany jak konserwator witryny i tak dalej.

Skanery

Jak widzieliście, na falach radiowych krążą różne dobre rzeczy. Podsumowując, interesują Cię głównie:

• Kamery bezprzewodowe (5,8 GHz i 2,4 GHz) - kamery są interesujące, ponieważ stanowią okazję do obrócenia przeciwko nim własnego bezpieczeństwa firmy. Podsłuchując kamery, robisz dokładnie to.

• Rozmowy przez Walkie Talkie - komunikacja w całej witrynie jest rzadko szyfrowana, a nasłuchiwanie może dać wgląd w lokalizację i ilość pracowników ochrony, a także inne informacje.

Do skanowania kamer potrzebny jest laptop z odpowiednim sprzętem i oprogramowaniem lub dedykowany skaner ręczny z szerokim zasięgiem odbioru i wbudowanym ekranem. Tańsze aparaty, takie jak kamery niania, wykorzystują pasmo 2,4 GHz, które jest nielicencjonowane (w Wielkiej Brytanii i USA), a co za tym idzie, jest mocno zaśmiecone technologiami konsumenckimi. Telefony bezprzewodowe (802.11b/g), Bluetooth i telefony bezprzewodowe używają tego zakresu częstotliwości. Kuchenki mikrofalowe będą współpracować ze wszystkimi tymi urządzeniami, aby było jeszcze przyjemniej. Nowe nielicencjonowane pasmo, 5,8 Ghz, zabiera część tego bałaganu, a wiele nowych kamer bezpieczeństwa, które go używają, jest sprzedawanych. Okazują się popularne ze względu na błędne przekonanie, że ponieważ nie mają częstotliwości 2,4 GHz, są bezpieczniejsze. Nie są. Z notki sprzedażowej:

„Ten kompaktowy odbiornik kamery bezprzewodowej wykorzystuje złącze USB do wysyłania sygnałów z kamery bezprzewodowej bezpośrednio do komputera. Odbiornik automatycznie synchronizuje się z dowolnymi kamerami 2,4 GHz w zasięgu, bez obaw o PAL lub NTSC - bez skomplikowanej konfiguracji, idealne dla nowicjuszy. ”

To urządzenie jest całkiem dobre w dekodowaniu wideo i całkiem przydatne do celów testów penetracyjnych, chociaż nie jestem do końca pewien co do rynku docelowego. . . .

Jeśli używasz tego urządzenia w gęsto zaludnionym obszarze, do którego się wybierasz odbierać zdjęcia z wszelkiego rodzaju ukrytych kamer w łazienkach, sypialniach i Bóg wie, co jeszcze. Powtórzę, to pasmo bezprzewodowe. Jeśli zdecydujesz się na zakup ręcznego skanera specjalnie do szpiegowania kamer, w zasadzie jedyną realną opcją jest obecnie ICOM IC R3. Jest jednak dość drogi i nie odbiera sygnałów z kamer 5,8 GHz. Aby uchwycić rozmowy walkie talkie, potrzebujesz ręcznego skanera radiowego, który może odbierać częstotliwości FRS / GMRS w Stanach Zjednoczonych lub częstotliwości PMR446 w UE. W celach informacyjnych przedstawiono je poniżej:

Częstotliwości PMR446

Kanał: Częstotliwość (MHz)

1: 446,00625

2: 446,01875

3: 446,03125

4: 446,04375

5: 446.05625

6: 446,06875

7: 446,08125

8: 446,09375

Częstotliwości FRS / GMRS

Kanał: Częstotliwość (MHz)

1: 462,5625 FRS

2.: 462,5875 FRS

3: 462,6125 FRS

4: 462,6375 FRS

5: 462,6625 FRS

6: 462,6875 FRS

7: 462,7125 FRS

8: 467,5625 FRS

9: 467,5875 FRS

10.: 467,6125 FRS

11: 467,6375 FRS

12 .: 467,6625 FRS

13 .: 467,6875 FRS

14: 467,7125 FRS

Kanał: Częstotliwość (MHz)

15:. 462.550 FRS / GMRS

16.: 462,575 FRS / GMRS

17 .: 462.600 FRS / GMRS

18 .: 462.625 FRS / GMRS

19.: 462.650 FRS / GMRS

20 .: 462,675 FRS / GMRS

21 .: 462.700 FRS / GMRS

22.: 462,725 FRS / GMRS

Każdy przyzwoity skaner uchwyci wszystkie te zakresy i wiele więcej.

Błąd pancerza

Ostateczną ochroną przed trafieniem jest nie stawianie się w sytuacji, w której ktoś wyceluje w Ciebie broń i nie możesz się stresować jak bardzo polecam takie podejście. Upewnij się, że wiesz, czy uzbrojeni strażnicy będą patrolować teren. Jeśli w grę wchodzą uzbrojeni strażnicy, radzę odrzucić tę pracę. Nawet podczas noszenia kamizelki kuloodpornej a, strzały w głowę są prawie zawsze śmiertelne. W sytuacji bojowej lekarze są szkoleni do radzenia sobie z ranami postrzałowymi kończyn, ale bez natychmiastowej pomocy przez osobę posiadającą przeszkolenie medyczne i sprzęt ratunkowy, takie urazy są często śmiertelne.

Podsumowanie

W tej części omówiłem niektóre urządzenia, które moim zdaniem są niezbędne do przeprowadzenia udanego testu penetracji fizycznej. To, co zabierzesz ze sobą, będzie się różnić w zależności od testu, w zależności od zasad zaangażowania i celów. Dlatego tej części nie należy uważać za wyczerpujący i należy pamiętać, że technologie szybko się dezaktualizują i cały czas pojawiają się lepsze rozwiązania. Omówiono następujące kwestie:

• Karta „Get out of Jail free” - jest to najważniejszy element „wyposażenia”, jaki będziesz nosić i na pewno jedyny obowiązkowy element każdego testu. To jest dokument, który pokazuje, że masz upoważnienie do włączenia testowania witryn. Zawsze noś co najmniej dwie kopie.

• Sprzęt fotograficzny - kamera jest niezbędnym elementem zestawu zarówno do nadzoru, jak i do rejestrowania postępów. Powinien być nowoczesny i mocny, ale dyskretny. Powinieneś także wiedzieć, jak go używać.

• Laptopy - komputery przenośne są niezbędne do wszelkich fizycznych testów penetracyjnych, które obejmują element włamań komputerowych (tj. Prawie wszystkie z nich). Laptopy powinny być nowoczesne i mieć możliwość wirtualizacji.

• Sprzęt bezprzewodowy - nie wszystkie urządzenia bezprzewodowe są sobie równe - zwłaszcza nie z punktu widzenia testu bezpieczeństwa. Upewnij się, że sprzęt, który zabierasz ze sobą, pozwala na wykonywanie ataków opisanych w rozdziale 7.

• Sprzęt GPS - dzięki GPS zawsze wiesz, gdzie jesteś, dokąd zmierzasz i (na potrzeby raportowania), gdzie byłeś.

GPS może sprawić, że planowanie testów koordynacyjnych, szczególnie tych z wieloma operatorami, przebiega znacznie łatwiej.

• Elektroniczna kryminalistyka - omówiono to w rozdziale 6. Nie musisz wydawać dużych pieniędzy, aby zbudować działające laboratorium kryminalistyczne, które zwiększy Twoje możliwości gromadzenia informacji.

• Wytrychy - Niezbędne do pokonywania zamków.

• Komunikacja - testerzy muszą pozostawać w stałym kontakcie między sobą i centralą. Sposób, w jaki to zrobisz, zależy od Ciebie, ale wskazałem tutaj moje preferencje.

• Skanery - skanery radiowe mogą być przydatne do przechwytywania transmisji z bezprzewodowych kamer bezpieczeństwa i krótkofalówek. Twoja torba z zestawem będzie szybko ewoluować w czasie (a przynajmniej powinna) i na pewno będzie rosnąć. To powiedziawszy, nie potrzebujesz całego omawianego tutaj sprzętu, aby wykonać udane zadanie, w wielu przypadkach jedyną rzeczą, którą będziesz nosić, jest karta „Get out of Jail Free” - nie wychodź z domu bez niej.