Podstawy fizycznych testów penetracyjnych

Jeśli znasz wroga i znasz siebie, nie musisz obawiać się wyniku stu bitew. Sun Tzu: Sztuka Wojny

Istnieje stare powiedzenie, że bezpieczeństwo jest tak silne, jak najsłabsze ogniwo łańcucha. To jest erudycyjna i często pomijana prawda. Najsłabszym łączem nigdy nie są klucze kryptograficzne chroniące łącze VPN lub korporacyjne zapory ogniowe chroniące granice sieci, chociaż technologie te z pewnością mają swoje wady. Najsłabszym ogniwem w każdym scenariuszu bezpieczeństwa są ludzie. Niektórzy ludzie są leniwi i wszyscy popełniają błędy i można nimi manipulować. To najważniejsza lekcja bezpieczeństwa, jakiej się nauczysz: bezpieczeństwo w jakiejkolwiek formie zawsze sprowadza się do ludzi i zaufania. Każdy porządny haker poinformuje cię: jeśli chcesz być dobry, naucz się technologii i języków programowania, systemów operacyjnych inżynierii wstecznej i tak dalej. Bycie świetnym hakerem wymaga umiejętności uczenia się, które na ogół nie są utrzymywane przez ludzi o takim sposobie myślenia. Gdy opanujesz manipulowanie ludźmi, możesz włamać się do wszystkiego - każdy system, korporacyjny, elektroniczny lub ludzki, jest podatny na ataki. Ta część obejmuje podstawy testów penetracyjnych, czyli rzeczy, które musisz wiedzieć przed zanurzeniem się w bardziej interesujących częściach praktycznych. Obejmuje to przewodnik po terminologii unikalnej dla testerów penetracyjnych, trochę na temat kwestii prawnych i proceduralnych (ponieważ zrozumienie odpowiedniego ustawodawstwa ma kluczowe znaczenie) i, oczywiście, omówienie, dlaczego testowanie penetracja jest ważne, w tym spojrzenie na to, co organizacje zwykle mają nadzieję osiągnąć, przeprowadzając test penetracyjny. Przeprowadzanie fizycznych testów penetracyjnych jest unikalnym i trudnym sposobem na zarabianie na życie; wymaga pewnego sposobu myślenia, szerokiego zestawu umiejętności i wymaga doświadczenia. Nie pomożemy ci w sposobie myślenia: to coś, co musisz rozwinąć; lub doświadczenie: to jest coś, co musisz zgromadzić; ale zapewnimy Ci odpowiedni zestaw umiejętności, a ta część jest pierwszym krokiem. Jeśli reprezentujesz organizację i chcesz zapewnić najwyższy poziom bezpieczeństwa, testy penetracyjne mogą ci pomóc. Dowiesz się, czego możesz oczekiwać od zespołu testującego penetrację.

Co robią testerzy penetracyjni?

Organizacje wynajmują testerów penetracyjnych w celu naruszenia bezpieczeństwa, w celu wykazania podatności. Robią to codziennie, a ich zdolność do płacenia czynszu zależy od ich sukcesu w przełamywaniu bezpieczeństwa. Aby wykazać wady bezpieczeństwa komputera, testerzy penetracji używają oprogramowania do inżynierii wstecznej. Włamują się do sieci i pokonują protokoły. W odniesieniu do bezpieczeństwa fizycznego wykazują one podatność na ataki poprzez fizyczne wtargnięcie do pomieszczeń klienta. Najczęściej osiąga się to poprzez tajne zbieranie danych wywiadowczych, ogólne oszustwo i inżynierię społeczną, chociaż może to obejmować bardziej bezpośrednie podejście, takie jak wtargnięcie w nocy, pokonanie zamków i czołganie się do ucieczki, w zależności od zasad zaangażowania. Różnice między intruzami komputerowymi i fizycznymi mogą wydawać się ogromne, ale między nimi występuje znaczna krzyżówka i często są wykonywane w tandemie. Widziałem zmieniające się wymagania klientów - zarówno w związku ze zmieniającą się technologią, jak i rosnącą świadomością zagrożeń, przed którymi stoją organizacje chcące zachować poufne dane bezpieczne. Problem w skrócie jest następujący: możesz mieć najlepsze zapory ogniowe i zmieniać procedury kontroli; możesz regularnie przeprowadzać elektroniczne testy penetracyjne sieci i aplikacji; możesz skontrolować kod źródłowy i zablokować serwery. Wszystkie te podejścia są w porządku i, jeśli są dobrze przeprowadzone, są ogólnie warte zachodu. Jeśli jednak osoba atakująca może fizycznie przedostać się do Twojej siedziby i uzyskać bezpośredni dostęp do systemów informatycznych, te strategie nie ochronią Cię. Takie podejście do bezpieczeństwa „twardej skorupy, miękkiego centrum” doprowadziło do jednych z najpoważniejszych naruszeń systemu

informatycznego w pamięci. Jak się dowiesz, bezpieczeństwo to znacznie więcej niż SSL i łatanie przed najnowszymi przepełnieniami bufora.

Testy bezpieczeństwa w realnym świecie

Organizacje wojskowe, szczególnie wojsko amerykańskie, od dziesięcioleci zatrudniają zespoły testerów penetracyjnych (zwane „drużynami tygrysimi" lub „czerwonymi").

Ich zadaniem jest penetrowanie przyjaznych baz, aby ocenić poziom trudności, z jakim wróg uzyskałby taki sam dostęp. Może to obejmować zasadzenie kartonu z napisem „bomba" lub próbę kradzieży książek z kodami. Może to obejmować uzyskanie dostępu do bezpiecznego miejsca i robienie zdjęć lub robienie czegoś o wartości wywiadowczej. Z biegiem czasu termin „zespół tygrysów" coraz bardziej kojarzy się z zespołami penetrującymi komputery; jednak termin ten jest nadal szeroko stosowany w pierwotnym kontekście w wojsku. Wyzwania, przed którymi stoją testerzy w sektorach prywatnym i rządowym, są bardzo różne od tych, które stoją przed zespołami wojskowych tygrysów, między innymi dlatego, że mają znacznie mniejsze szanse na zastrzelenie. Jednak atakujący, przed którymi chce się bronić, są zasadniczo różni (terroryści na przykład w jednym przypadku, a w szpiegostwie przemysłowym w drugim), podejście to nie jest odmienne. Wszyscy testerzy zaczynają od określonego celu, zbierają informacje na temat celu, opracowują plan ataku na podstawie dostępnych informacji i ostatecznie wykonują plan. Każdy z tych kroków jest szczegółowo opisany, ale najpierw, dla zachowania spójności, rozważmy niektóre z terminów, których będę używać w całym tekście:

• Klient docelowy- klient inicjujący test oraz fizyczna lokalizacja, w której znajduje się cel;

• Cel - cel, który należy osiągnąć, aby test penetracyjny mógł zostać uznany za udany, na przykład następujące przykłady:

• Naruszenie bezpieczeństwa granic w miejscu docelowym (najprostsza forma testu, często tak podstawowa, jak penetracja poza zasięgiem odbioru, gdzie kończy się większość procedur bezpieczeństwa fizycznego).

• Uzyskaj fizyczny dostęp do sieci komputerowej z poziomu docelowej lokalizacji.

• Zrobienie zdjęcia z góry określonego zasobu.

• Zdobycie z góry określonego zasobu

• Uzyskanie dostępu do wcześniej określonego personelu.

• Zdobycia z góry określonych danych wywiadowczych dotyczących aktywów lub personelu.

• Osadzenie fizycznych dowodów obecności.

• Dowolna kombinacja powyższych.

• Zasób - lokalizacja w celu, coś namacalnego w działaniu co zespół musi zdobyć (np. serwerownię lub dokument) lub coś niematerialnego, np. z góry określony poziom dostępu;

• Test penetracyjny - metoda oceny bezpieczeństwa systemu komputerowego , sieć lub obiekt fizyczny poprzez symulację ataku intruza;

• Zespół operacyjny - zespół, którego zadaniem jest przeprowadzenie testu penetracyjnego. W kontekście penetracji fizycznej i od momentu rozpoczęcia testu zespół operacyjny prawdopodobnie składa się z:

• planiści;

• operatorzy (osoby faktycznie przeprowadzające badanie fizyczne);

• personel pomocniczy.

Skład zespołu będzie zależeć od charakteru testu. Na przykład test obejmujący dostęp do komputera po udanej penetracji fizycznej musi mieć co najmniej jednego operatora wykwalifikowanego w zakresie włamań do komputera. Osoby wykwalifikowane w dziedzinie inżynierii społecznej prawdopodobnie zostaną rozmieszczone w ramach planowania lub wsparcia.

• Zakres - uzgodnione zasady zaangażowania, zwykle oparte na podejściu czarnej skrzynki (zero wiedzy) lub krystalicznej (informacje o celu są dostarczane przez klienta);

• Przewidywany opór lub postawa bezpieczeństwa - opór napotykany przez zespół operacyjny, w zależności od wielu czynników:

• charakter celu;

• świadomość bezpieczeństwa wśród personelu;

• ilość (i jakość) personelu ochrony;

• ogólna gotowość i świadomość potencjalnych zagrożeń na terenie celu.

Inne czynniki obejmują trudność przypisania i skuteczność mechanizmów bezpieczeństwa w celu ochrony aktywów.

Kwestie prawne i proceduralne

Większość klientów oczekuje - i słusznie - że zespół penetracji będzie ubezpieczony, zanim nawet rozważą ich zatrudnienie. Chociaż nie zamierzam kierować cię w stronę żadnego konkretnego ubezpieczyciela, musisz mieć przynajmniej pokrycie błędów i przeoczeń. Wymagany zakres ochrony różni się w zależności od regionu i podlega przepisom określonym w poszczególnych jurysdykcjach. Zalecane jest ubezpieczenie od odpowiedzialności cywilnej. Firmy ubezpieczeniowe mogą chcieć dowiedzieć się trochę o członkach zespołu przed podpisaniem polisy. Takie informacje mogą obejmować wykształcenie, zdrowie i prawie na pewno będą zawierać szczegóły dotyczące przestępstw (tj. spodziewają się ich nie znaleźć), a także historie zawodowe. Nie powinno to stanowić problemu, ponieważ przeprowadziłeś weryfikację przeszłości w zespole przed ich zatrudnieniem. (Czyż nie?) Zatrudniając zespół testujący penetrację, upewnij się, że jest on ubezpieczony. Pomoże to zapewnić przeprowadzenie niezbędnych testów w tle w zespole, który zatrudniasz, aby uzyskać dostęp do informacji prywatnych.

Poświadczenia bezpieczeństwa

Podczas przeprowadzania jakichkolwiek testów penetracyjnych zarówno dla rządu centralnego, jak i wojska, członkowie zespołu muszą posiadać poświadczenia bezpieczeństwa. Poniższe informacje są specyficzne dla Wielkiej Brytanii, chociaż sedno jest takie samo dla Stanów Zjednoczonych, gdzie procedury odpraw są znacznie bardziej rygorystyczne i wykorzystują w szerokim zakresie poligrafy (testy „wykrywacza kłamstw"). Pomimo przytłaczających dowodów przeciwnych, rząd USA twierdzi, że nie można pokonać poligrafów. Można i regularnie są. Poświadczenia bezpieczeństwa mają różne

smaki, w zależności od charakteru wykonywanej pracy i wrażliwości celu. Wszystkie zezwolenia muszą być sponsorowane przez dział inicjujący test, chyba że są już w posiadaniu zespołu operacyjnego (choć są wyjątki). Zasadniczo od wszystkich członków zespołu testującego oczekuje się przeprowadzenia kontroli bezpieczeństwa (SC)

Prawie każdy, kto nie ma danych kryminalnych i nie jest znany agencjom wywiadowczym, raczej nie zostanie odrzucony . Potencjalni członkowie zespołu są zobowiązani do dostarczenia podstawowych informacji o sobie, w tym o miejscach, w których mieszkali i w przeszłości pracowali. Zazwyczaj zadawane są również pytania dotyczące ich członkostwa w organizacjach. Zezwolenie SC umożliwia dostęp do chronionych (niejawnych) informacji oznaczonych ochronnie według projektu, według zasady (zwykle do TAJNEJ). Chociaż zezwolenie to musi być okresowo odnawiane, nie jest (zwykle) konieczne sprawdzanie członków zespołu na indywidualne testy. Ogólnie rzecz biorąc, prześwit SC jest odpowiedni i najbardziej realistyczny wybór, biorąc pod uwagę czas realizacji potrzebny do ustalenia odstępów. O jeden krok wyżej opracowano zezwolenie na weryfikację (DV). Jest to potrzebne do pracy dla organizacji wywiadowczych, takich jak GCHQ lub MI6, i jest minimalnym wymogiem dla osób regularnie pracujących na najwyższym poziomie tajności. Zezwolenia te wydawane są dla poszczególnych projektów i nie podlegają przeniesieniu. Aby uzyskać zezwolenie DV, potencjalni kandydaci są zobowiązani do wzięcia udziału w rozmowie kwalifikacyjnej (zwykle przeprowadzanej przez Agencję ds. Weryfikacji obrony lub MI5). Proces ten obejmuje dogłębną analizę sytuacji osobistej i finansowej wnioskodawcy. Prawdopodobnie zostaną również przesłuchani rodzina i partnerzy, a ich odpowiedzi zostaną powiązane. Przetwarzanie zezwoleń DV jest kosztownym i czasochłonnym przedsięwzięciem dla rządu i często ludzie sprawdzani na stanowiska rządowe zaczynają pracować na nowych stanowiskach (choć na niższym poziomie bezpieczeństwa) na długo przed tym, zanim zostaną sprawdzeni . Tylko najbardziej wrażliwe testy będą wymagały zezwolenia DV. Najważniejsze jest, aby wiedzieć, kogo zatrudniasz, aby poświadczenia ubezpieczenia i ochrony były zwykłym bólem głowy, a nie poważnym bólem. W Wielkiej Brytanii potencjalny najemca może dostarczyć oświadczenie policji, że nie ma w nich żadnych akt (ustawa o ochronie danych daje prawo do takiego oświadczenia). Jeśli tworzysz zespół zajmujący się testami penetracyjnymi, zalecamy przeprowadzenie kontroli finansowej wszystkich osób, choćby po to, aby pokazać klientom, że dołożyłeś należytej staranności, a nie dlatego, że ma to jakąś istotną wartość.

Trzymać się prawa

Nie trzeba dodawać, że wiele umiejętności opisanych jest przydatnych dla przestępców, a także dla legalnych testerów penetracji. Nie mam żadnych szczególnych obaw w zapisywaniu tych umiejętności na papierze. Źli ludzie są już w nich dobrze zorientowani. Byłbym jednak naiwny, gdybym nie zwrócił uwagi, że Twoim obowiązkiem jest upewnienie się, że zawsze pozostajesz po właściwej stronie prawa. Omawiając różne tematy zawarte w tej książce, staram się przedstawić Ci wszelkie istotne kwestie prawne, na które możesz natknąć się, ale nie jestem prawnikiem. Twoja firma powinna zawsze uzyskać wykwalifikowaną poradę prawną. Następujące akty prawne w Wielkiej Brytanii są ilustrującymi przykładami aspektów prawa, których mogłeś nie wziąć pod uwagę.

Ustawa o prawach człowieka z 1998 r

W 2000 r. Zjednoczone Królestwo włączyło Europejską konwencję praw człowieka do prawa brytyjskiego. Większość Ustawy o prawach człowieka z 1998 r. Nie ma znaczenia dla testów penetracyjnych. Należy jednak pamiętać o jednej lub dwóch rzeczach podczas przeprowadzania jakichkolwiek testów penetracyjnych.

Artykuł 8 - Prawo do poszanowania życia prywatnego i rodzinnego

1. Każdy ma prawo do poszanowania życia prywatnego i rodzinnego domu i jego korespondencja.

2. Władza publiczna nie może ingerować w korzystanie z tego prawa, z wyjątkiem przypadków zgodnych z prawem i koniecznych w społeczeństwie demokratycznym w interesie bezpieczeństwa narodowego, bezpieczeństwa publicznego lub dobrobytu gospodarczego kraj, w celu zapobiegania nieporządkowi lub przestępczości, w celu ochrony zdrowia lub moralności lub w celu ochrony praw i wolności innych osób.

Kluczem do art. 8 jest prywatność, którą można (i trzeba) interpretować w nieoczekiwany sposób. Na przykład, jeśli zespół testujący penetrację podczas wykonywania swoich obowiązków przypadkowo lub umyślnie przechwycił prywatną komunikację docelowego personelu, zostało popełnione przestępstwo na podstawie art. 8. Na przykład docelowy użytkownik sprawdza Yahoo! e-mail na komputerze firmowym za pośrednictwem sieci firmowej. Nikt nie ma prawa przechwytywać tego e-maila. Nie ma znaczenia fakt, że to, co robi, może być kwestią dyscyplinarną w kontekście jego zatrudnienia. Dam ci kolejny (prawdziwy) przykład, abyś mógł docenić zakres tego, o czym mówię. Haker narusza bezpieczeństwo departamentu rządu centralnego, a przynajmniej tak mu się wydaje. W rzeczywistości naruszył „honey pot", który ma badać zachowanie hakerów. Haker kieruje swój ruch przez ten hoey pot i używa go do sprawdzenia swojego adresu e-mail. W ten sposób pozwala na przechwycenie jego komunikacji przez rządowy personel bezpieczeństwa. Ten e-mail jest prywatny; poprzez przechwytywanie, przechowywanie (a nawet czytanie) wiadomości e-mail popełniono przestępstwo. Najważniejsze - niezależnie od tego, czy uważasz to za szalone, czy nie - musisz być świadomy tego, na co patrzysz i potencjalnych konsekwencji prawnych tego, co robisz. Jeśli zatrudniasz zespół testujący penetrację, musisz wiedzieć, co mogą legalnie zrobić.

Ustawa o nadużyciach komputerowych z 1990 r

U podstaw Ustawy o nadużyciach komputerowych z 1990 r. Przestępstwem jest świadomy dostęp do systemu informatycznego bez pozwolenia. Przeczytaj i opracuj zasady zaangażowania: zespół testujący penetrację może mieć pozwolenie na wybranie określonego komputera lub sieci w obrębie celu, ale nie sąsiadujących z nim. Mogą być upoważnieni do atakowania określonego serwera, ale nie działających na nim aplikacji (które mogą podlegać zupełnie innej sferze odpowiedzialności organizacyjnej). W dowolnym momencie, jeśli zespół operacyjny ma wątpliwości co do swojej sytuacji prawnej, powinien niezwłocznie skonsultować się ze swoim personelem pomocniczym.

Poznaj wroga

Rozpocząłem być może najsłynniejszym cytatem z Art of War Sun Tzu: Poznaj wroga i poznaj siebie. Zanim poznasz wroga, musisz wiedzieć, kim jest wróg. Dla wojska jest to proste: są to faceci, którzy strzelają do ciebie i bombardują cię. W świecie komercyjnym wróg nie jest tak prosty do zdefiniowania. Zagrożenia, przed którymi stoją organizacje we współczesnym świecie, są różnorodne i wielostronne. Aby test penetracji fizycznej miał jakąkolwiek istotną wartość, konieczne jest określenie i, do pewnego stopnia, naśladowanie charakteru zagrożenia, przed którym stoi ta organizacja. Zagrożenia mogą się znacznie różnić. Tabela krótko objaśnia cele i ich potencjalne narażenie, na które zespoły operacyjne są najbardziej narażone. Temat ten jest znacznie bardziej szczegółowo traktowany w dalszej części książki. Podane zagrożenie niekoniecznie powinno zmienić twoje podejście, ale z pewnością powinno je pokierować.

Cele: potencjalne zagrożenia

Cele korporacyjne (siedziba główna; większe niezależne obiekty): Naruszenie bezpieczeństwa na granicy: szeroki dostęp

Biura korporacyjne (wspólne pomieszczenia), zwykle zarządzane przez służby budowlane lub centralną recepcję: Przekroczona granica bezpieczeństwa: łatwa do złamania, szpiegostwo korporacyjne

Centra danych (zewnętrzne urządzenia do przechowywania danych): Atrakcyjne cele na całym świecie

Lokalne biura rządowe lub samorządowe: dziennikarze i protestujący

Centralne urzędy: wywiad zagraniczny, protestujący i działacze

Komenda policji: przestępczość zorganizowana, działacze i dziennikarze

Narzędzia: terroryzm

Elektrownie : Terroryzm

Bazy wojskowe: wywiad zagraniczny i protestujący

Istnieje pewien stopień skrzyżowania. Na przykład kontrahent do obrony korporacyjnej można uznać za cel wojskowy. Sposób ujawnienia się tych zagrożeń różni się:

• Szpiegostwo handlowe - może to obejmować zewnętrzne hakowanie, fizyczne wtargnięcie do siedziby firmy, użycie moli lub podkładów do zbierania poufnych informacji itp.

• Sabotaż komercyjny - takie czyny mogą obejmować „etyczny" lub „środowiskowy" terroryzm, tj. atakami na obiekty należące do firm farmaceutycznych, koncernów naftowych, zakładów przeprowadzających testy na zwierzętach lub kliniki aborcyjne (te ostatnie są w dużej mierze zjawiskiem północnoamerykańskim). Akty sabotażu jednego podmiotu handlowego przeciwko drugiemu są rzadkie, ale nie są niespotykane, a ja badałem więcej niż jeden.

• Działa przez obce mocarstwo - pod koniec zimnej wojny redukcja tradycyjnych agencji wywiadowczych była nieunikniona, ponieważ wielu agentów terenowych ucierpiało w wyniku „redukcji mocy" (RIF). Jednak wielu byłych funkcjonariuszy KGB (na przykład) jest obecnie zaangażowanych w szpiegostwo handlowe, a większość z nich jest sankcjonowana przez państwo. Zbieranie informacji wywiadowczych przeciwko narodom USA i Europy Zachodniej jest głównym zadaniem rosyjskiego aparatu gromadzącego dane wywiadowcze, w szczególności Służby Wywiadu Zagranicznego (SVR, następca KGB) oraz, w mniejszym stopniu, wywiadu wojskowego (GRU)). Ulubionymi celami są kontrahenci rządowi.

• Terroryzm - w latach 80. i 90. ministerstwa brytyjskie i ich odpowiedniki w sektorze komercyjnym były atakowane przez różne grupy bez niemałego powodzenia. Gdy jedna grupa zostanie zneutralizowana, pojawiają się nowe zagrożenia. MI5 obecnie monitoruje tysiące potencjalnych terrorystów i wydaje się, że minął tydzień bez aresztowania nowych podejrzanych.

Podsumowując, złożoność i zasięg zagrożenia jest o wiele bardziej zaangażowany niż się początkowo wydaje. Klimat, w którym żyjemy, sprawia, że bezpieczeństwo jest problemem wszystkich i bardzo ważne jest, aby każda organizacja, duża lub mała, rozumiała zagrożenia i była na nie przygotowana.

Zaangażowanie zespołu testującego penetrację

Ta część obejmuje podstawy fizycznej penetracji i jej cele. Być może czytasz to z zamiarem zaangażowania firmy do przeprowadzenia testu fizycznego. Zanim zaczniesz czytać dalej, powinieneś rozważyć koszty, potencjalne korzyści i ograniczenia związane z takim ćwiczeniem. Czy to naprawdę coś, czego potrzebujesz? Czy to naprawdę coś, z czego skorzysta Twoja organizacja? Inne pytania, które powinieneś sobie zadać, to:

• Czy obecnie posiadasz wszechstronną politykę bezpieczeństwa?

• Czy przeprowadzasz audyt w odniesieniu do tej zasady?

• Czego chcesz się nauczyć z ćwiczenia?

• Czy są określone obszary, w których brakuje Ci pewności i które chcesz przetestować?

• Czy test powinien być czarny czy kryształowy?

• Jak spodziewasz się, że Twoja organizacja sobie poradzi?

• Czy przeprowadzasz test, aby uzasadnić dodatkowy budżet bezpieczeństwa?

Jeśli nie masz polityki bezpieczeństwa, powinnaś ją wdrożyć jako twój priorytet. Jeśli nie spodziewasz się, że wyniki testu będą bardzo dobre, zastanów się, dlaczego tak jest, i zastosuj dodatkowe zabezpieczenia w tych obszarach. Jeśli nie uważasz, że masz wystarczający budżet i chcesz go zwiększyć dzięki widocznym słabościom bezpieczeństwa, nie martw się, nie jesteś sam. W rzeczywistości jest to pierwszy powód, dla którego firmy po raz pierwszy przeprowadzają jakąkolwiek formę testu penetracyjnego.

Podsumowanie

Omówiono podstawy tego, co musisz wiedzieć, jeśli chcesz się zmierzyć z nieco zaangażowanym obszarem fizycznych testów penetracyjnych. Jest o wiele więcej do omówienia niż te, które wprowadzono tutaj. Bezpieczeństwo to znacznie więcej niż tylko aspekty techniczne, a bezpieczeństwo techniczne to więcej niż przepełnienie bufora. Przyjrzeliście się trochę temu, co robią testerzy penetracji w obliczu zadań fizycznych, a także historii branży i tego, jak rozwinęła się ona z wojskowego dzieciństwa w sektor komercyjny, gdy pojawiła się taka potrzeba. Co najważniejsze, omówiłem podstawową terminologię, która ma kluczowe znaczenie dla zrozumienia późniejszego materiału. Przyzwyczajenie się do terminologii pozwala również zachować właściwy sposób myślenia. Przedstawiłem też trochę, dlaczego chcesz przeprowadzić tę formę testowanie i zagrożenia, przed którymi stoją różne organizacje. Jeśli czytasz tę książkę z perspektywy kierownika ds. Bezpieczeństwa lub dyrektora IT, powinieneś być nieco bardziej zrozumiały na temat tego, co wiąże się z zatrudnieniem zespołu testującego.