PRZEGLĄD HACKOWANIA ETYCZNEGO

Termin „etyczny haker" może wydawać się oksymoronem — jak etyczny kieszonkowiec lub etyczny defraudant. W tym module dowiesz się, że etyczni hakerzy są zatrudniani lub kontraktowani przez firmy, aby robić to, co robią nielegalni hakerzy: włamywać się. Dlaczego? Firmy muszą wiedzieć, które części ich infrastruktury bezpieczeństwa są podatne na ataki. Aby chronić sieć firmy, wielu specjalistów ds. bezpieczeństwa zdaje sobie sprawę, że wiedza o tym, jakich narzędzi używają cyberprzestępcy i jak myślą, pomaga lepiej chronić (wzmacniać) bezpieczeństwo sieci. Pamiętaj o starym przysłowiu: jesteś tak bezpieczny, jak twoje najsłabsze ogniwo. Cyberprzestępcy poświęcają dużo czasu i energii, próbując znaleźć słabe ogniwa. Ten kurs dostarcza narzędzi potrzebnych do ochrony sieci i dzieli się niektórymi podejściami, których etyczny haker — zwany również „testerem bezpieczeństwa" lub „testerem penetracji" — może użyć, aby odkryć luki w zabezpieczeniach sieci. Kurs ten w żadnym wypadku nie jest ostatecznym studium hakowania etycznego. Zamiast tego daje Ci przegląd roli testera bezpieczeństwa i zawiera działania, które pomogą Ci rozwinąć umiejętności potrzebne do ochrony sieci przed atakami. Ten kurs pomaga Ci zrozumieć, jak chronić sieć, gdy odkryjesz metody, których używają źli aktorzy (hakerzy) lub dobrzy aktorzy (etyczni hakerzy, znani również jako hakerzy white hat), aby włamać się do sieci. Pomaga Ci również wybrać najbardziej odpowiednie narzędzia, aby ułatwić Ci pracę. Jako specjalista ds. bezpieczeństwa musisz zrozumieć, jakie prawa mogą mieć na Ciebie wpływ podczas wykonywania Twojej pracy jako testera bezpieczeństwa, zwłaszcza jeśli używasz metod testowania opisanych w tym kursie. Inny temat poruszony w tekście, zrozumienie znaczenia posiadania umowy kontraktowej z klientem przed wykonaniem jakichkolwiek aspektów testu bezpieczeństwa, może pomóc Ci uniknąć łamania prawa.

WPROWADZENIE DO HACKINGU ETYCZNEGO

Firmy czasami zatrudniają hakerów etycznych do przeprowadzania testów penetracyjnych. W teście penetracyjnym haker etyczny próbuje włamać się do sieci lub aplikacji firmy, aby znaleźć słabe punkty. W ocenie podatności tester próbuje wymienić wszystkie luki znalezione w aplikacji lub systemie. Często ocena podatności jest przeprowadzana najpierw w celu zidentyfikowania celów testów penetracyjnych. W teście bezpieczeństwa testerzy robią więcej niż tylko próbują włamać się; analizują również politykę i procedury bezpieczeństwa firmy oraz zgłaszają wszelkie luki kierownictwu. Innymi słowy, testowanie bezpieczeństwa przenosi testowanie penetracyjne na wyższy poziom. Jak stwierdza Peter Herzog w podręczniku Open Source Security Testing Methodology Manual, „[Testowanie bezpieczeństwa] opiera się na połączeniu kreatywności, rozbudowy [baz] wiedzy na temat najlepszych praktyk, kwestii prawnych i przepisów branżowych klienta, a także znanych zagrożeń i szerokości obecności bezpieczeństwa organizacji docelowej (lub punktu ryzyka)". To tylko niektóre z kwestii, które muszą zbadać testerzy bezpieczeństwa. W ten sposób ostrzegają firmy o obszarach, które należy monitorować lub zabezpieczyć. Jako tester bezpieczeństwa nie możesz sprawić, aby sieć była nieprzenikniona. Jedynym sposobem, aby to zrobić z pewnością, jest odłączenie kabla sieciowego. Kiedy odkryjesz luki w zabezpieczeniach („dziury") w sieci, możesz je naprawić. Ten proces może obejmować zadania takie jak aktualizacja systemu operacyjnego (OS), eliminacja niepotrzebnych aplikacji lub usług lub instalacja najnowszej poprawki zabezpieczeń dostawcy. Jeśli Twoja praca to tester penetracyjny, po prostu zgłaszasz swoje ustalenia firmie. To firma podejmuje ostateczną decyzję, jak wykorzystać dostarczone przez Ciebie informacje. Jednak jako tester bezpieczeństwa możesz być również zobowiązany do oferowania rozwiązań w celu zabezpieczenia lub ochrony sieci. Moduły w tym kursie zostały napisane z założeniem, że pracujesz nad tym, aby zostać profesjonalistą ds. bezpieczeństwa sieci odpowiedzialnym za ochronę sieci korporacyjnej, więc nacisk kładzie się na wykorzystanie umiejętności testera bezpieczeństwa w celu zabezpieczenia lub ochrony sieci. W tym kursie dowiesz się, jak znaleźć luki w sieci i je naprawić. Zadaniem testera bezpieczeństwa jest

dokumentowanie wszystkich luk w zabezpieczeniach oraz zarządzanie alertami i personel technologii informatycznych (IT) w obszarach, które wymagają szczególnej uwagi.

Rola testerów bezpieczeństwa i penetracji

Haker uzyskuje dostęp do systemu komputerowego lub sieci bez upoważnienia właściciela systemu. W ten sposób haker łamie prawo i może trafić do więzienia. Osoby włamujące się do systemów w celu kradzieży lub zniszczenia danych są często określane mianem crackerów; hakerzy mogą chcieć jedynie udowodnić, jak podatny jest system, uzyskując dostęp do komputera lub sieci bez niszczenia danych. Na potrzeby tego kursu nie rozróżnia się terminów „hakerzy" i „crackerzy". Departament Sprawiedliwości Stanów Zjednoczonych określa każdy nielegalny dostęp do systemów komputerowych lub sieciowych jako „hakowanie", a ten kurs podąża za tym określeniem. Etyczny haker to osoba, która wykonuje większość tych samych czynności, co haker, ale za zgodą właściciela lub firmy. To rozróżnienie jest ważne i może oznaczać różnicę między oskarżeniem o przestępstwo a nieoskarżeniem. Etyczni hakerzy są zazwyczaj zatrudniani do przeprowadzania testów penetracyjnych lub testów bezpieczeństwa. Firmy zdają sobie sprawę, że intruzi mogą próbować uzyskać dostęp do zasobów sieciowych i są skłonne zapłacić komuś, kto jako pierwszy odkryje te luki. Firmy wolą zapłacić „dobremu hakerowi", aby odkrył problemy w bieżącej konfiguracji sieci, niż pozwolić „złemu hakerowi" odkryć te luki. Źli hakerzy spędzają wiele godzin na skanowaniu systemów przez Internet, szukając luk lub podatnych systemów. Niektórzy hakerzy to utalentowani eksperci komputerowi, ale inni to młodzi, niedoświadczeni ludzie, których doświadczeni hakerzy nazywają „script kiddies" lub „packet monkeys". Te pejoratywne określenia odnoszą się do osób, które kopiują kod lub używają narzędzi stworzonych przez doświadczonych programistów, nie rozumiejąc, jak one działają. Wielu doświadczonych testerów penetracyjnych potrafi pisać programy lub skrypty w Pythonie, Ruby, Perlu lub C, aby przeprowadzać ataki. (Skrypt to zestaw instrukcji, który jest uruchamiany sekwencyjnie, aby wykonywać zadania w systemie komputerowym). Masz szansę napisać skrypt w jednym z tych języków w późniejszym module. Osoba, która włamuje się do systemów komputerowych z powodów politycznych lub społecznych, nazywana jest hacktivistą. Przez kilka lat grupa hacktivistów znana jako Anonymous siała spustoszenie w systemach komputerowych rządu federalnego, a także w sektorze prywatnym. Grupa groziła kiedyś ujawnieniem nazwisk członków Ku Klux Klanu (KKK) po zhakowaniu konta organizacji na Twitterze. Ten rodzaj hakowania nazywa się „haktywizmem". Państwa narodowe obecnie częściej i bardziej wyrafinowanie angażują się w cyberataki hakerskie. Słynny atak na łańcuch dostaw SolarWinds, który naraził na szwank agencje rządowe, a nawet firmy zajmujące się cyberbezpieczeństwem, był cyberatakiem przeprowadzonym przez Rosję. Wyszukiwanie w Internecie na stronach rekrutacyjnych dla pracowników IT hasła „tester penetracyjny" daje setki ogłoszeń o pracę, wiele z nich pochodzi od firm z listy Fortune 500 poszukujących doświadczonych kandydatów. Typowe ogłoszenie może zawierać następujące wymagania:

• Przeprowadzanie oceny podatności, ataków i penetracji w środowiskach internetowych, intranetowych i bezprzewodowych.

• Przeprowadzanie wykrywania i skanowania otwartych portów i usług.

• Stosowanie odpowiednich exploitów w celu uzyskania dostępu i rozszerzenia dostępu w razie potrzeby.

• Udział w działaniach obejmujących testowanie penetracyjne aplikacji i przegląd kodu źródłowego aplikacji.

• Współpracowanie z klientem w razie potrzeby w trakcie trwania współpracy. • Sporządzaj raporty dokumentujące odkrycia dokonane w trakcie realizacji zlecenia.

• Omówienie z klientem po zakończeniu każdego zlecenia.

• Uczestnicz w badaniach i przedstawiaj zalecenia dotyczące ciągłego doskonalenia.

• Uczestnicz w dzieleniu się wiedzą.

• Wykaż się dobrą znajomością obowiązujących przepisów cybernetycznych obowiązujących w kraju, stanie i mieście.

Testerzy penetracyjni i testerzy bezpieczeństwa zazwyczaj mają laptopy skonfigurowane z wieloma systemami operacyjnymi i narzędziami hakerskimi. Ten kurs wykorzystuje systemy Windows, Kali Linux i inne narzędzia Linux potrzebne do przeprowadzania rzeczywistych ataków na aplikacje sieciowe i internetowe. Nauka instalowania systemu operacyjnego nie jest omówiona, ale możesz łatwo znaleźć zasoby na ten temat. Najnowsze wersje Kali Linux można znaleźć na stronie www.kali.org. Procedura instalowania narzędzi bezpieczeństwa różni się w zależności od narzędzia i systemu operacyjnego.

Określanie zapotrzebowania korporacji na specjalistów ds. bezpieczeństwa IT

Czas trwania: 10 minut

Cel: Zbadanie korporacji, które chcą zatrudnić specjalistów ds. bezpieczeństwa IT.

Opis: Wiele firm chętnie zatrudnia lub zawiera umowy z testerami bezpieczeństwa dla swoich sieci korporacyjnych. W tej aktywności przeszukujesz Internet w poszukiwaniu ofert pracy, używając słów kluczowych „bezpieczeństwo IT” i czytasz opisy stanowisk, aby określić umiejętności informatyczne (oraz wszelkie umiejętności pozainformatyczne), jakie większość firm oczekuje od kandydatów.

1. Uruchom przeglądarkę internetową i przejdź do indeed.com.

2. W polu wyszukiwania Co wpisz Bezpieczeństwo IT. W polu wyszukiwania Gdzie wpisz nazwę dużego miasta w pobliżu, a następnie naciśnij Enter.

3. Zanotuj liczbę ofert pracy. Wybierz od trzech do pięciu ofert pracy i przeczytaj opis stanowiska w każdej z nich.

4. Po zakończeniu wyjdź z przeglądarki internetowej.

SECURITY BYTES

Pilne potrzeby organizacji w zakresie cyberbezpieczeństwa doprowadziły do niedoboru wykwalifikowanych specjalistów ds. bezpieczeństwa. W odpowiedzi firma o nazwie Synack opracowała model „crowdsourcingu”, aby świadczyć usługi etycznego hakowania. Synack stworzył platformę oprogramowania, która oferuje firmom zautomatyzowane sposoby wykrywania luk w zabezpieczeniach; następnie przekazuje te luki testerom penetracyjnym — zasadniczo etycznym hakerom, którzy wykorzystują swoje umiejętności w dobrym celu. Ci etyczni hakerzy to freelancerzy zatrudniani online na zasadzie praca po pracy. Jeśli zdecydujesz się zostać etycznym hakerem, znajdziesz wiele możliwości zatrudnienia i będziesz cieszyć się długoterminowym bezpieczeństwem pracy.

Metodyki testów penetracyjnych

Etyczni hakerzy, którzy wykonują testy penetracyjne, korzystają z jednego z tych modeli:

• Model białej skrzynki

• Model czarnej skrzynki

• Model szarej skrzynki

W modelu białej skrzynki testerowi mówi się, jakiej topologii sieci i technologii używa firma, i otrzymuje pozwolenie na przeprowadzenie wywiadu z personelem IT i pracownikami firmy. Na przykład firma może wydrukować schemat sieci pokazujący wszystkie routery, przełączniki, zapory sieciowe i systemy wykrywania włamań firmy lub przekazać testerowi plan piętra szczegółowo opisujący lokalizację systemów komputerowych i systemów operacyjnych działających w tych systemach. Te informacje ułatwiają pracę testera penetracyjnego niż w przypadku korzystania z modelu czarnej skrzynki. W modelu czarnej skrzynki kierownictwo nie ujawnia pracownikom, że przeprowadzane są testy penetracyjne, ani nie przekazuje testerowi żadnych diagramów ani nie opisuje, jakich technologii używa firma. Ten model nakłada na testera obowiązek znalezienia tych informacji za pomocą technik, których uczysz się w trakcie tego kursu. Ten model pomaga również kierownictwu sprawdzić, czy personel ds. bezpieczeństwa firmy może wykryć atak.

Model szarego pola jest hybrydą modelu białego i czarnego pola. W tym modelu firma przekazuje testerowi tylko częściowe informacje. Na przykład tester może uzyskać informacje o tym, które systemy operacyjne są używane, ale nie otrzymać żadnych schematów sieciowych.

SECURITY BYTES

Szpitale często sprawdzają procedury przyjęć wykonywane przez personel medyczny, prosząc stażystów i pielęgniarki o podawanie się za „potencjalnych pacjentów". W jednym szpitalu psychiatrycznym personelowi przyjmującemu z góry powiedziano, że niektórzy ludzie zgłaszający się jako pacjenci będą w rzeczywistości lekarzami lub pielęgniarkami. Co zaskakujące, liczba pacjentów przyjętych w tym miesiącu była niezwykle niska, mimo że żaden z pacjentów nie był stażystą ani pielęgniarką, co wskazuje, że personel przyjmujący zmienił swoje zachowanie z powodu wcześniejszego powiadomienia. W tym samym duchu, jeśli firma wie, że jest monitorowana w celu oceny bezpieczeństwa swoich systemów, pracownicy mogą zachowywać się bardziej czujnie i przestrzegać istniejących procedur. Wiele firm nie chce tego fałszywego poczucia bezpieczeństwa; chcą zobaczyć, jak personel działa bez wcześniejszego ostrzeżenia, że ktoś może próbować zaatakować ich sieć.

Programy certyfikacji dla personelu ds. bezpieczeństwa sieci

Jak większość specjalistów IT wie, certyfikacja zawodowa jest dostępna w niemal każdym obszarze bezpieczeństwa sieci. Poniższe sekcje obejmują kilka stosownych certyfikacji. Niezależnie od tego, czy jesteś specjalistą ds. bezpieczeństwa, programistą komputerowym, administratorem baz danych czy specjalistą ds. sieci, organizacje zawodowe oferują wystarczającą liczbę certyfikatów i egzaminów, aby zapewnić Ci zajęcie na resztę kariery. Powinieneś już uzyskać co najmniej certyfikat CompTIA Security+ lub mieć równoważną wiedzę, która zakłada kompetencje sieciowe na poziomie wiedzy CompTIA Network+, co jest warunkiem wstępnym do uzyskania certyfikatu Security+. Aby uzyskać więcej informacji, odwiedź stronę internetową CompTIA (www.comptia.org).

CompTIA PenTest+

Certyfikat PenTest+ (www.comptia.org) to zaawansowana certyfikacja, która potwierdza, że pomyślnie zdani kandydaci mają wiedzę i umiejętności wymagane do planowania i określania zakresu oceny, rozumienia wymogów prawnych i zgodności, przeprowadzania skanowania podatności i testów penetracyjnych, analizowania danych oraz skutecznego raportowania i komunikowania wyników. Następujące obszary (obszary tematyczne) są objęte egzaminem certyfikacyjnym:

• Planowanie i zakres

• Gromadzenie informacji

• Identyfikacja luk

• Ataki i exploity

• Narzędzia do testów penetracyjnych

• Raportowanie i komunikacja

Offensive Security Certified Professional

Offensive Security Certified Professional (OSCP; www.offensive-security.com) to zaawansowany certyfikat, który wymaga od studentów wykazania się umiejętnościami praktycznymi, aby uzyskać certyfikaty. Obejmuje on exploity sieciowe i aplikacyjne oraz daje studentom doświadczenie w opracowywaniu podstawowych przepełnień bufora, pisaniu skryptów do zbierania i manipulowania danymi oraz próbowaniu exploitów w podatnych systemach.

Certified Ethical Hacker

Międzynarodowa Rada Konsultantów ds. Handlu Elektronicznego (EC-Council) opracowała oznaczenie certyfikacyjne o nazwie Certified Ethical Hacker (CEH; www.eccouncil.org). Obecnie egzamin CEH z pytaniami wielokrotnego wyboru opiera się na 22 obszarach, z którymi musi być zaznajomiony tester. Wymagania dotyczące wiedzy zmieniają się okresowo, więc jeśli jesteś zainteresowany przystąpieniem do tego egzaminu, odwiedź stronę internetową EC-Council, aby uzyskać najnowsze informacje. 22 domeny sprawdzane w egzaminie CEH to:

• Etyka i kwestie prawne

• Footprinting

• Skanowanie

• Enumeracja

• Hakowanie systemów

• Trojany i tylne furtki

• Sniffery

• Odmowa usługi

• Inżynieria społeczna

• Przejmowanie sesji

• Hakowanie serwerów internetowych

• Luki w zabezpieczeniach aplikacji internetowych

• Techniki łamania haseł oparte na sieci WWW

• Wstrzykiwanie języka zapytań strukturalnych (SQL)

• Hakowanie sieci bezprzewodowych

• Wirusy i robaki

• Bezpieczeństwo fizyczne

• Hakowanie Linuksa

• Systemy IDS, zapory sieciowe i honeypoty

• Przepełnienia bufora

• Kryptografia

• Metodyki testów penetracyjnych

Jak widać, aby zdać ten egzamin, musisz znać ogromną ilość informacji. Chociaż do egzaminu potrzebna jest ogólna wiedza na temat tych 22 domen, w miejscu pracy najprawdopodobniej zostaniesz przydzielony do zespołu, który przeprowadza testy penetracyjne. Ten zespół, nazywany w branży zespołem czerwonym, składa się z osób o różnych umiejętnościach, które wykonują testy. Na przykład zespół czerwony może obejmować eksperta ds. programowania, który może wykonywać wstrzyknięcia SQL lub inne testy podatności programowania. W skład zespołu może również wchodzić ekspert ds. sieci, który zna się na podatnościach portów i podatnościach IDS, routerów lub zapór. Jest mało prawdopodobne, aby jedna osoba wykonała wszystkie testy. Jednak zdanie egzaminu wymaga ogólnej wiedzy na temat wszystkich wymienionych domen.

Open Source Security Testing Methodology Manual Professional Security Tester

Certyfikat OSSTMM Professional Security Tester (OPST) jest przyznawany przez Institute for Security and Open Methodologies (ISECOM; www.isecom.org), organizację non-profit, która zapewnia szkolenia z zakresu bezpieczeństwa i programy certyfikacji dla profesjonalistów ds. bezpieczeństwa. Certyfikacja OPST wykorzystuje Open Source Security Testing Methodology Manual (OSSTMM), napisany przez Petera Herzoga, jako swoją znormalizowaną metodologię. W trakcie kursu będziesz korzystać z wielu jej metodologii. Ponieważ podręcznik jest okresowo aktualizowany, powinieneś regularnie sprawdzać witrynę ISECOM, aby pobrać najnowszą wersję. Egzamin obejmuje niektóre z następujących tematów:

• Zawodowy — zasady zaangażowania (określające Twoje zachowanie jako testera bezpieczeństwa)

• Enumeracja — typy pakietów internetowych, testowanie odmowy usługi

• Oceny — badanie sieci, kontrole, wywiad konkurencyjny

• Zastosowanie — łamanie haseł, środki powstrzymujące

• Weryfikacja — rozwiązywanie problemów, testowanie bezpieczeństwa

Egzamin wymaga od testerów odpowiedzi na pytania wielokrotnego wyboru i pomyślnego przeprowadzenia testów bezpieczeństwa w sieci atakującej. Ta praktyczna część egzaminu zapewnia, że testerzy mogą zastosować swoją wiedzę w rzeczywistych warunkach.

Certified Information Systems Security Professional

Certyfikacja Certified Information Systems Security Professional (CISSP) dla specjalistów ds. bezpieczeństwa jest wydawana przez International Information Systems Security Certification Consortium (ISC2; www.isc2.org). Mimo że certyfikacja CISSP nie jest skierowana do technicznych specjalistów ds. IT, stała się jednym ze standardów dla wielu specjalistów ds. bezpieczeństwa. Egzamin nie wymaga od testerów posiadania wiedzy technicznej z zakresu IT; sprawdza umiejętności

menedżerskie związane z bezpieczeństwem. Osoby CISSP zwykle bardziej interesują się politykami i procedurami niż rzeczywistymi narzędziami do przeprowadzania testów bezpieczeństwa lub testów penetracyjnych, więc nie potrzebują umiejętności technicznych specjalistów ds. IT. ISC2 wymaga od osób przystępujących do egzaminu pięcioletniego doświadczenia przed przystąpieniem do pięciogodzinnego egzaminu, więc nie spiesz się z tą certyfikacją, dopóki nie będziesz w branży przez jakiś czas. Egzamin obejmuje pytania z następujących 10 dziedzin:

• Bezpieczeństwo i zarządzanie ryzykiem

• Bezpieczeństwo aktywów (ochrona bezpieczeństwa aktywów)

• Inżynieria bezpieczeństwa (inżynieria i zarządzanie bezpieczeństwem)

• Komunikacja i bezpieczeństwo sieci (projektowanie i ochrona bezpieczeństwa sieci)

• Zarządzanie tożsamością i dostępem (kontrola dostępu i zarządzanie tożsamością)

• Ocena i testowanie bezpieczeństwa (projektowanie, wykonywanie i analizowanie testów bezpieczeństwa)

• Operacje bezpieczeństwa (podstawowe koncepcje, dochodzenia, zarządzanie incydentami i odzyskiwanie po awarii)

• Bezpieczeństwo rozwoju oprogramowania (rozumienie, stosowanie i egzekwowanie bezpieczeństwa oprogramowania)

SANS Institute

SysAdmin, Audit, Network, Security (SANS) Institute (www.sans.org) oferuje szkolenia i certyfikaty bezpieczeństwa IT za pośrednictwem Global Information Assurance Certification (GIAC, www.giac.org). Dwa powiązane certyfikaty w zakresie etycznego hakowania to GIAC Certified Peneration Tester (GPEN) i GIAC Certified Web Application Tester (GWAPT). Oprócz uznawanego certyfikatu, SANS oferuje kursy szkoleniowe za pośrednictwem akredytowanego uniwersytetu, SANS Technology Institute. Oprócz programów szkoleniowych i stopni naukowych, SANS bezpłatnie rozpowszechnia dokumenty badawcze na temat bezpieczeństwa komputerów i sieci na całym świecie. Jednym z najpopularniejszych dokumentów jest lista 25 najczęstszych błędów oprogramowania, która opisuje najczęstsze ataki sieciowe i sugeruje sposoby korygowania luk w zabezpieczeniach. Ta lista oferuje bogactwo informacji dla testerów penetracyjnych lub specjalistów ds. bezpieczeństwa, a Ty zapoznaj się z nią w Aktywności 1-2.

Aktywność 1-2: Badanie 25 najniebezpieczniejszych luk w oprogramowaniu

Czas trwania: 15 minut

Cel: Zbadanie listy SANS zawierającej najczęstsze luki w zabezpieczeniach sieci.

Opis: Tak szybko, jak specjaliści ds. bezpieczeństwa IT próbują korygować luki w zabezpieczeniach sieci, ktoś tworzy nowe luki w zabezpieczeniach, a specjaliści ds. bezpieczeństwa sieci muszą być na bieżąco z tymi lukami. W tej aktywności zbadasz niektóre bieżące luki w zabezpieczeniach wykorzystywane do atakowania sieci. Nie martw się — nie będziesz musiał zapamiętywać swoich odkryć. Ta aktywność po prostu wprowadza Cię do świata bezpieczeństwa sieci.

1. Uruchom przeglądarkę internetową i przejdź do www.sans.org.

2. W obszarze Zasoby kliknij łącze 25 najczęstszych błędów programowania. (Ponieważ witryny internetowe często się zmieniają, może być konieczne wyszukanie tego łącza.)

3. Przeczytaj zawartość listy 25 najczęstszych błędów. (Ten dokument często ulega zmianom, aby odzwierciedlić wiele nowych exploitów tworzonych codziennie.) Lista Top 25 jest również znana jako Top 25 Most Dangerous Software Errors. Linki na liście wyjaśniają system punktacji i ramy używane do klasyfikowania tych błędów.

4. Zbadaj kilka pierwszych wad, klikając łącze CWE-#. Dla każdej wady zanotuj opis, odpowiednią platformę i konsekwencje.

5. Po zakończeniu zamknij przeglądarkę internetową.

Który certyfikat jest najlepszy?

Decyzja, który egzamin certyfikacyjny zdać, może być trudna. Zarówno testerzy penetracyjni, jak i testerzy bezpieczeństwa potrzebują umiejętności technicznych, aby skutecznie wykonywać swoje obowiązki. Muszą również dobrze rozumieć sieci i rolę zarządzania w organizacji, umiejętności pisania i komunikacji werbalnej oraz chęć dalszej nauki. Warto dążyć do uzyskania każdego certyfikatu, jeśli zachęca Cię do czytania i nauki. Posiadanie certyfikatu daje Ci przewagę nad kimś, kto go nie ma. Jeśli masz certyfikaty w obszarze, którego poszukuje pracodawca, Twoje CV często znajdzie się na szczycie listy potencjalnych kandydatów. Niebezpieczeństwo egzaminów certyfikacyjnych polega na tym, że niektórzy uczestnicy po prostu zapamiętują terminologię i nie mają dobrego zrozumienia tematu lub złożonych pojęć, podobnie jak studenci, którzy zdołali zdać egzamin końcowy, wkuwając, ale potem zapominają większości informacji po przystąpieniu do testu. Wykorzystaj mądrze czas poświęcony na naukę do egzaminu certyfikacyjnego, odkrywając obszary, w których możesz potrzebować poprawy, zamiast zapamiętywać odpowiedzi na pytania. Dzięki poznaniu materiału w tym kursie możesz nabyć umiejętności, których potrzebujesz, aby stać się kompetentnym specjalistą ds. bezpieczeństwa IT i zdać egzaminy obejmujące etyczne hakowanie, metody testów penetracyjnych oraz topologie i technologie sieciowe. Niezależnie od tego, jaki egzamin zdasz, najważniejszą rzeczą, o której należy pamiętać, jest to, że przepisy prawa regulują to, co możesz lub czego nie możesz robić jako etyczny haker, tester bezpieczeństwa lub tester penetracyjny. Przestrzeganie przepisów i etyczne zachowanie są ważniejsze niż zdanie egzaminu. Pamiętaj, aby odwiedzić strony internetowe organizacji przeprowadzających testy certyfikacyjne, ponieważ wymagania egzaminacyjne zmieniają się tak szybko, jak technologia. Na przykład kilka lat temu egzamin CISSP nie zawierał pytań dotyczących Internetu rzeczy (IoT), ale teraz egzamin obejmuje ten temat.

UWAGA

Pamiętaj, że strony internetowe często się zmieniają. Być może będziesz musiał trochę poszperać, aby znaleźć informacje, których szukasz. Pomyśl o tej aktywności jako o ćwiczeniu umiejętności testera bezpieczeństwa.

CO MOŻESZ ZROBIĆ LEGALNIE

Ponieważ przepisy dotyczące technologii komputerowej zmieniają się tak szybko, jak sama technologia, musisz być na bieżąco z tym, co dzieje się w Twojej okolicy na świecie. Na przykład to, co jest legalne w Des Moines, może nie być legalne w Indianapolis. Jednak dowiedzenie się, co jest legalne w Twoim stanie lub kraju, może być równie trudne, jak przeprowadzenie testów penetracyjnych. Wielu urzędników państwowych nie jest świadomych przepisów prawnych dotyczących technologii komputerowej. To zamieszanie utrudnia również ściganie przestępców w przestępstwach komputerowych. Przeciętny obywatel w ławie przysięgłych nie chce wysyłać osoby do więzienia za

zrobienie czegoś, czego prokurator stanowy nie zdefiniował jasno jako nielegalnego. Jako tester bezpieczeństwa musisz być świadomy tego, co masz prawo robić, a czego nie powinieneś lub nie możesz robić. Na przykład niektórzy testerzy bezpieczeństwa wiedzą, jak otworzyć zamek zasuwkowy, więc zamknięte drzwi nie powstrzymałyby ich przed uzyskaniem fizycznego dostępu do serwera. Jednak testerzy muszą znać przepisy dotyczące posiadania wytrychów, zanim wyruszą na teren korporacji z narzędziami w ręku. W rzeczywistości przepisy różnią się w zależności od stanu i kraju. W niektórych stanach samo posiadanie narzędzi do wytrychów stanowi przestępstwo, podczas gdy inne stany zezwalają na posiadanie, o ile przestępstwo nie zostało popełnione. W jednym stanie możesz zostać oskarżony o wykroczenie za posiadanie tych narzędzi; w innym stanie możesz zostać oskarżony o zbrodnię.

WSKAZÓWKA Warto przyjrzeć się Open Organisation of Lockpickers (TOOOL), jeśli rozważasz dodanie tej umiejętności do swojego arsenału. Ich strona internetowa, https://toool.us/laws.html, ułatwia sprawdzenie przepisów w każdym stanie przed spakowaniem walizki z narzędziami do wytrychów

Prawo kraju

Podobnie jak w przypadku narzędzi do otwierania zamków, posiadanie narzędzi hakerskich na komputerze lub urządzeniu mobilnym może być nielegalne. Możesz skontaktować się z lokalnymi organami ścigania lub poszukać w Internecie informacji o przepisach obowiązujących w Twoim stanie lub kraju przed zainstalowaniem narzędzi hakerskich na swoich urządzeniach. Możesz zobaczyć, jak skomplikowana staje się ta kwestia, podróżując ze stanu do stanu lub kraju do kraju. W Nowym Jorku może obowiązywać jedno prawo dotyczące instalowania narzędzi hakerskich, a szybka przejażdżka przez most George'a Washingtona prowadzi Cię do innego prawa w New Jersey. Przepisy są pisane w celu ochrony społeczeństwa, ale często słowa pisane są otwarte na interpretację, dlatego sądy i sędziowie są niezbędni. Na przykład na Hawajach państwo musi udowodnić, że osoba oskarżona o popełnienie przestępstwa na komputerze miała „zamiar popełnienia przestępstwa". Tak więc samo skanowanie sieci nie jest przestępstwem na Hawajach. Ponadto państwo ma jeszcze trudniejsze zadanie udowodnienia, że komputer użyty do popełnienia przestępstwa był używany tylko przez jedną osobę — tę, która rzekomo popełniła przestępstwo. Jeśli osoba oskarżona o popełnienie przestępstwa twierdzi, że więcej niż jedna osoba miała dostęp do komputera użytego do zebrania dowodów popełnienia przestępstwa, państwo nie może użyć tego komputera jako dowodu. Co te prawa mają wspólnego z profesjonalistą ds. bezpieczeństwa sieci używającym narzędzi do testów penetracyjnych? Przepisy dotyczące posiadania narzędzi hakerskich, które umożliwiają przeglądanie infrastruktury sieciowej firmy, nie są tak jasno określone jak przepisy dotyczące posiadania narzędzi do otwierania zamków, ponieważ przepisy nie nadążają za tempem postępu technologicznego. W niektórych stanach uruchomienie programu, który daje atakującemu przegląd i szczegółowy opis infrastruktury sieciowej firmy, nie jest postrzegane jako zagrożenie. Jako kolejny przykład tego, jak mogą się różnić przepisy, czy robienie zdjęć zewnętrznej i wewnętrznej części banku jest legalne? Pracownicy ochrony w banku na Hawajach twierdzą, że poproszono by Cię o zaprzestanie robienia zdjęć i opuszczenie budynku. Rzecznik FBI ujął to w prostych słowach: Możesz zostać poproszony o zaprzestanie robienia zdjęć, jeśli znajdujesz się na terenie prywatnym. Robienie zdjęć po drugiej stronie ulicy od banku za pomocą obiektywu z zoomem jest legalne, ale jeśli w przyszłości wykorzystasz zdjęcia do popełnienia przestępstwa, prawnik powie Ci, że zarzuty przeciwko Tobie mogą być poważniejsze. Ze względu na strach przed terroryzmem w niektórych częściach Stanów Zjednoczonych i wielu częściach Europy robienie zdjęć mostów, stacji kolejowych i innych miejsc publicznych jest nielegalne. Wspominanie o wszystkich tych przepisach i regulacjach ma na celu upewnienie się, że jesteś świadomy zagrożeń związanych z byciem testerem bezpieczeństwa lub studentem uczącym się technik hakerskich. Większość ataków obejmowała coś więcej niż skanowanie firmy, ale przypadki te pokazują, że rząd

poważnie podchodzi do karania za cyberprzestępstwa. Niektóre z najbardziej znanych przypadków to włamania przeprowadzone przez studentów, takie jak niedawny atak na szkoły w Miami-Dade. Wielu hakerów używa oprogramowania do łamania haseł kont online. Ten akt, wykonywany przez wielu specjalistów ds. bezpieczeństwa po uzyskaniu pozwolenia od właściciela sieci, jest przestępstwem federalnym, gdy jest wykonywany bez pozwolenia i może znacznie wydłużyć wyrok hakera

SECURITY BYTES

HackerOne to platforma bezpieczeństwa, która łączy hakerów z organizacjami potrzebującymi oceny luk w zabezpieczeniach. Hakerzy to etyczni hakerzy, którzy wykorzystują swoje podstępne umiejętności w dobrym celu. HackerOne płaci etycznym hakerom tzw. bug bounty w zależności od krytyczności błędów, które znajdą. Garstka hakerów HackerOne stała się milionerami w wyniku wypłat bug bounty.

Czy skanowanie portów jest legalne?

Skanowanie portów to powszechna czynność w testach penetracyjnych. Testerzy używają skanowania portów do wykrywania urządzeń komputerowych w sieci i wyszczególniania oferowanych przez nie usług. Na przykład, jeśli skanowanie wykryje, że komputer o adresie IP 192.168.1.100 ma otwarty port 443 dla połączeń, maszyna jest prawdopodobnie serwerem internetowym i może później zostać wykorzystana do testów penetracyjnych serwera internetowego. Niektóre stany uważają skanowanie portów za nieinwazyjne lub nieniszczące i uznają je za legalne. Jednak nie zawsze tak jest, dlatego należy zachować ostrożność przed rozpoczęciem korzystania z narzędzi do testów penetracyjnych. Niektóre firmy wniosły oskarżenia karne przeciwko hakerom za skanowanie ich systemów, ale sędziowie orzekli, że sieci nie zostały uszkodzone, więc zarzuty zostały oddalone. To tylko kwestia czasu, zanim firma stwierdzi, że jej sieć jest również własnością prywatną i powinna mieć prawo stwierdzić, że skanowanie jest niedozwolone. Ponieważ rząd federalny obecnie nie uważa tych naruszeń za naruszenie Konstytucji Stanów Zjednoczonych, każdy stan może zająć się tymi kwestiami osobno. Jednak firma może wnieść podobne oskarżenia przeciwko Tobie, jeśli zdecydujesz się ćwiczyć przy użyciu narzędzi, których uczysz się na tym kursie. Nawet jeśli zostaniesz uznany za niewinnego w swoim stanie, koszty prawne mogą być szkodliwe dla Twojej firmy lub finansów osobistych. Dlatego musisz zbadać przepisy swojego stanu przed wykorzystaniem tego, czego się uczysz, nawet jeśli używasz narzędzi dla dobra innych, a nie w celu popełnienia przestępstwa.

WSKAZÓWKA Podczas podróży poza Stany Zjednoczone należy zapoznać się z przepisami cybernetycznymi kraju, który się odwiedza. Na przykład prowadzenie samochodu wyposażonego w antenę przeznaczoną do identyfikacji punktów dostępu bezprzewodowego jest przestępstwem w Niemczech

Powinieneś również przeczytać umowę z dostawcą usług internetowych, w szczególności sekcję zatytułowaną „Zasady akceptowalnego użytkowania” lub podobną. Większość osób przegląda i akceptuje warunki swojej umowy.

Zasady akceptowalnego użytkowania

(a) PacInfo Net nie nakłada żadnych ograniczeń na użytkowanie, pod warunkiem że takie użytkowanie jest zgodne z prawem i przepisami stanu Hawaje i Stanów Zjednoczonych Ameryki i nie wpływa negatywnie na klientów PacInfo Net. Klient jest odpowiedzialny za uzyskanie i przestrzeganie Zasad akceptowalnego użytkowania dowolnej sieci, do której uzyskuje się dostęp za pośrednictwem usług PacInfo Net. (b) PacInfo Net zastrzega sobie prawo do odłączenia bez uprzedzenia konta, które jest źródłem spamu, nadużyć lub złośliwych działań. Nie będzie zwrotu pieniędzy, gdy konto zostanie zamknięte z tych powodów. Ponadto, na takie konta będzie naliczana stawka rozliczeniowa w

wysokości 125 USD za godzinę, aby pokryć czas pracy personelu poświęcony na naprawę późniejszych uszkodzeń.

(c) Klientom zabrania się stosowania technik mających na celu uszkodzenie lub uniemożliwienie dostępu prawowitym użytkownikom komputerów lub komponentów sieciowych podłączonych do Internetu. PacInfo Net zastrzega sobie prawo do odłączenia witryny klienta, która jest źródłem takich działań, bez uprzedzenia.

Inny dostawca usług internetowych odpowiedział na wiadomość e-mail dotyczącą korzystania z oprogramowania skanującego następującą wiadomością:

Jakiekolwiek korzystanie z Usługi, które zakłóca normalne korzystanie z systemu przez HOL lub innych klientów HOL lub zużywa nadmierną ilość pamięci lub cykli procesora przez długi czas, może skutkować rozwiązaniem umowy zgodnie z Sekcją 1 niniejszej Umowy. Użytkownikom surowo zabrania się podejmowania jakichkolwiek działań, które narażają bezpieczeństwo obiektów HOL. Użytkownicy nie mogą uruchamiać „botów" IRC ani żadnych innych skryptów lub programów niedostarczonych przez HOL.

Pozdrawiam,

Obsługa klienta

Hawaii Online

Oświadczenie zakazujące używania botów Internet Relay Chat (IRC) lub innych skryptów lub programów niedostarczonych przez dostawcę usług internetowych może być najważniejsze dla testerów penetracyjnych. Bot IRC to program, który wysyła automatyczne odpowiedzi użytkownikom, sprawiając wrażenie osoby po drugiej stronie połączenia. Na przykład bot może powitać nowych użytkowników dołączających do sesji czatu, nawet jeśli osoba ta nie jest obecna, aby ich powitać. Nawet jeśli nie masz zamiaru tworzyć bota, klauzula „jakiekolwiek inne skrypty lub programy" powinna nadal budzić wątpliwości. Innym czynnikiem, który należy wziąć pod uwagę podczas skanowania portów, jest to, czy komputer jest podłączony do sieci firmowej za pomocą wirtualnej sieci prywatnej (VPN). Wiele osób pracuje w domu, używając VPN do łączenia się ze swoją siecią służbową. Jeśli uruchomisz skaner portów, gdy Twoja sieć VPN jest podłączona, możesz skończyć na skanowaniu komputerów służbowych, co może być problematyczne. W Ćwiczeniu 1-3 badasz przepisy swojego stanu lub kraju, korzystając z Tabeli A-1 jako przewodnika.

Aktywność 1-3: Identyfikacja przepisów komputerowych w Twoim stanie lub kraju

Czas trwania: 30 minut

Cel: Dowiedz się, jakie przepisy mogą zabraniać przeprowadzania testu penetracji sieci w Twoim stanie lub kraju.

Opis: W ramach tej aktywności korzystasz z wyszukiwarek internetowych, aby zebrać informacje na temat przestępstw komputerowych w Twoim stanie lub kraju (lub w miejscu wybranym przez instruktora). Zostałeś zatrudniony przez ExecuTech, firmę konsultingową ds. bezpieczeństwa, w celu zebrania informacji na temat wszelkich nowych przepisów lub ustaw, które mogą mieć wpływ na testerów bezpieczeństwa, których zatrudnia. Napisz jednostronicową notatkę do Liang Choi, dyrektora ds. bezpieczeństwa i operacji, wymieniając obowiązujące przepisy lub ustawy i przedstawiając zalecenia kierownictwu. Na przykład możesz odnotować w swojej notatce, że przeprowadzenie ataku typu „odmowa usługi" na sieć firmy jest nielegalne, ponieważ kodeks karny Twojego stanu zabrania tego typu ataków, chyba że właściciel wyrazi na to zgodę.

SECURITY BYTES

Nawet jeśli uważasz, że postępujesz zgodnie z wymaganiami klienta, który zatrudnił Cię do wykonania testu bezpieczeństwa, nie zakładaj, że kierownictwo będzie zadowolone z Twoich wyników. Jeden z testerów został upomniany przez menedżera, który był zdenerwowany, że test bezpieczeństwa ujawnił nazwy logowania i hasła. Menedżer uważał, że tester nie powinien znać tych informacji i rozważał przerwanie testu bezpieczeństwa. Powinna obowiązywać umowa o zachowaniu poufności (NDA), aby zapewnić klientów, że testerzy nie ujawnią ani nie wykorzystają żadnych znalezionych informacji. NDA może wystarczyć, aby rozwiać obawy kierownictwa dotyczące odkrywania haseł. Zasady współpracy powinny również wskazywać, czy odkrywanie i odczytywanie danych logowania jest dozwolone, czy niedozwolone.

Aktywność 1-4: Badanie federalnych i międzynarodowych przepisów dotyczących przestępczości komputerowej

Czas trwania: 30 minut

Cel: Zwiększenie zrozumienia amerykańskich przepisów federalnych i międzynarodowych dotyczących przestępczości komputerowej.

Opis: W ramach tej aktywności użyj wyszukiwarek internetowych, aby zebrać informacje na temat Kodeksu Stanów Zjednoczonych, Tytuł 18, Sekcja 1030, który obejmuje oszustwa i pokrewne działania związane z komputerami. Zapoznaj się również z Konwencją o cyberprzestępczości (Konwencją budapeszteńską). Napisz podsumowanie wyjaśniające, w jaki sposób te przepisy mogą wpływać na etycznych hakerów i testerów bezpieczeństwa

CZEGO NIE MOŻESZ ROBIĆ LEGALNIE

Po zapoznaniu się z prawem stanowym, federalnym i międzynarodowym dotyczącym przestępczości komputerowej, możesz zobaczyć, że dostęp do komputera bez zezwolenia, niszczenie danych i kopiowanie informacji bez zezwolenia właściciela jest nielegalne. Nie trzeba mieć wykształcenia prawniczego, aby zrozumieć, że pewne działania są nielegalne, takie jak instalowanie wirusów w sieci, odmawianie użytkownikom dostępu do zasobów sieciowych. Jako tester bezpieczeństwa musisz uważać, aby Twoje działania nie uniemożliwiały pracownikom klienta wykonywania ich pracy. Jeśli uruchomisz program, który wykorzystuje zasoby sieciowe w takim stopniu, że użytkownikowi odmawia się do nich dostępu, naruszyłeś prawo federalne. Na przykład ataki typu „odmowa usługi" (DoS), omówione w późniejszym module, nie powinny być inicjowane w sieciach Twojego klienta.

Uzyskaj to na piśmie

Jak już wspomniano, możesz przypadkowo spowodować atak DoS, uruchamiając określone programy hakerskie w sieci klienta. Taka możliwość utrudnia Twoją pracę, zwłaszcza jeśli przeprowadzasz testy bezpieczeństwa jako niezależny wykonawca zatrudniony przez firmę, zamiast pracować jako pracownik dużej firmy ochroniarskiej, która ma zespół prawny do sporządzenia umowy z klientem. Pracownicy firmy ochroniarskiej są chronieni na mocy umowy firmy z klientem. Na potrzeby tej dyskusji załóżmy, że jesteś niezależnym wykonawcą, który potrzebuje wskazówek w zakresie tworzenia pisemnej umowy. Niektórzy wykonawcy uważają, że pisemne umowy podważają ich relacje z klientami. Jednak konsultacja z prawnikiem i podpisanie pisemnej umowy to dobry interes. Konsultanci, którzy nie otrzymali zapłaty od klienta, zazwyczaj głosują „tak" w kwestii umowy. Podobnie użytkownicy często nie są przekonani o znaczeniu tworzenia kopii zapasowych ważnych dokumentów, dopóki ich komputery nie ulegną awarii. Nie czekaj, aż staniesz przed sądem, aby żałować, że nie masz czegoś na piśmie. Jeśli chcesz uzyskać dodatkowe informacje, możesz zapoznać

się z książkami na temat pracy jako niezależny wykonawca. Internet jest również pomocnym źródłem bezpłatnych szablonów umów, które można zmodyfikować, aby dopasować je do sytuacji biznesowej. Jednak wprowadzone przez Ciebie modyfikacje mogą stwarzać więcej problemów niż brak umowy, więc zlecenie prawnikowi przeczytania umowy przed jej podpisaniem jest dobrą inwestycją czasu i pieniędzy. Czy jesteś zaniepokojony? Dobrze. Większość książek lub kursów na temat etycznego hakowania pomija ten temat, a przecież jest to najważniejsza część zawodu. Jeśli Twój klient dostarczy Ci umowę sporządzoną przez dział prawny firmy, konsultacja z prawnikiem może zaoszczędzić Ci czasu i pieniędzy. Próba zrozumienia umowy napisanej przez prawników reprezentujących najlepsze interesy firmy wymaga prawnika po Twojej stronie, który będzie dbał o Twoje najlepsze interesy. Złożoność prawa jest zbyt trudna do zrozumienia dla większości osób niebędących prawnikami. Nadążanie za technologią komputerową jest wystarczająco trudne. Obie dziedziny zmieniają się nieustannie, ale prawo jest jeszcze bardziej złożone, ponieważ zmienia się w zależności od stanu.

SECURITY BYTES

Zawód etycznego hakera jest dość nowy, a przepisy dotyczące cyberbezpieczeństwa zmieniają się nieustannie. Nawet jeśli firma zatrudnia Cię do testowania swojej sieci pod kątem luk, uważaj, aby nie łamać żadnych przepisów obowiązujących w Twoim stanie lub kraju. Jeśli obawiasz się, że jeden z Twoich testów może spowolnić sieć z powodu nadmiernego wykorzystania przepustowości, Twoje obawy powinny być sygnałem ostrzegawczym. Firma może rozważyć pozwanie Cię o stracony czas lub pieniądze spowodowane tym opóźnieniem. Dokumentacja określająca zasady zaangażowania i zakres testów powinna obejmować tę sytuację. Nie powinieneś obciążać systemów aktywnie używanych przez klientów, chyba że zostało to zatwierdzone przez klienta i udokumentowane w umowie o testach penetracyjnych.

Etyczne hakowanie w pigułce

Po przeczytaniu wszystkich zasad i zakazów możesz rozważać inny zawód. Zanim jednak zmienisz karierę, zapoznaj się z umiejętnościami, jakie musi posiadać tester bezpieczeństwa, aby ustalić, czy masz kwalifikacje do wykonywania tej pracy:

• Znajomość technologii sieciowych i komputerowych — jako tester bezpieczeństwa musisz dobrze rozumieć koncepcje sieciowe. Powinieneś poświęcić czas na naukę i przeglądanie koncepcji TCP/IP i routingu oraz umieć czytać diagramy sieciowe. Jeśli nie masz doświadczenia w pracy z sieciami, zacznij teraz. Bycie testerem bezpieczeństwa jest niemożliwe bez wysokiego poziomu wiedzy specjalistycznej w tej dziedzinie. Powinieneś również dobrze rozumieć technologie komputerowe i systemy operacyjne. Przeczytaj jak najwięcej o obecnie używanych systemach operacyjnych, zwracając szczególną uwagę na systemy Linux i Windows, ponieważ większość testów bezpieczeństwa jest przeprowadzana na tych popularnych systemach.

• Umiejętność komunikowania się z kadrą zarządzającą i personelem IT — testerzy bezpieczeństwa muszą być dobrymi słuchaczami i muszą umieć komunikować się ustnie i pisemnie z kadrą zarządzającą i personelem IT. Wyjaśnienie ustaleń dyrektorom generalnym może być trudne, zwłaszcza jeśli nie mają oni wykształcenia technicznego. Twoje raporty powinny być jasne i zwięzłe oraz zawierać konstruktywne opinie i zalecenia.

• Zrozumienie przepisów obowiązujących w Twojej lokalizacji — jako tester bezpieczeństwa musisz wiedzieć, co możesz, a czego nie możesz robić zgodnie z prawem. Zebranie tych informacji może być trudne podczas pracy z globalnymi firmami, ponieważ przepisy mogą się znacznie różnić w innych krajach.

• Umiejętność stosowania niezbędnych narzędzi do wykonywania swoich zadań — testerzy bezpieczeństwa muszą dobrze rozumieć narzędzia do przeprowadzania testów bezpieczeństwa. Co ważniejsze, musisz umieć myśleć nieszablonowo, odkrywając, tworząc i modyfikując narzędzia, gdy obecne narzędzia nie spełniają Twoich potrzeb.

SECURITY BYTES

Jeśli zależy ci na tym, aby inni cię lubili, możesz rozważyć inny zawód niż testowanie bezpieczeństwa. Jeśli jesteś dobry w swojej pracy, wielu pracowników IT nie znosi, gdy odkrywasz luki w ich systemach. W rzeczywistości jest to jeden z nielicznych zawodów, w którym im lepiej wykonujesz swoją pracę, tym więcej wrogów sobie narobisz.

PODSUMOWANIE

• Wiele firm zatrudnia etycznych hakerów do przeprowadzania testów penetracyjnych. Celem testu penetracyjnego jest odkrycie luk w sieci. Test bezpieczeństwa jest zazwyczaj przeprowadzany przez zespół osób o różnych umiejętnościach, czasami nazywany „czerwonym zespołem", i idzie dalej, aby polecić rozwiązania w celu usunięcia luk.

• Testy penetracyjne są zazwyczaj przeprowadzane przy użyciu jednego z trzech modeli: modelu białej skrzynki, modelu czarnej skrzynki lub modelu szarej skrzynki. Model używany przez testera opiera się na ilości informacji, które klient jest skłonny dostarczyć. W niektórych testach klient nie chce, aby tester miał dostęp do żadnych informacji firmy. Innymi słowy, klient mówi: „Dowiedz się, co możesz o mojej firmie bez mojej pomocy".

• Testerzy bezpieczeństwa mogą zdobywać certyfikaty z wielu źródeł. Najpopularniejszymi certyfikatami są CEH, CISSP i OCSP. Każdy certyfikat wymaga zdania egzaminu i obejmuje różne obszary, które tester musi opanować. Ponieważ wymagania testowe zmieniają się okresowo, odwiedź stronę internetową firmy certyfikującej, aby sprawdzić wymagania egzaminacyjne.

• Jako tester bezpieczeństwa lub tester penetracyjny musisz wiedzieć, co jest dozwolone, a co nie jest dozwolone zgodnie z prawem. Zacznij od zapoznania się z lokalnymi przepisami przed przeprowadzeniem jakichkolwiek testów bezpieczeństwa.

• Twój dostawca usług internetowych może mieć politykę dozwolonego użytku w podpisanej przez Ciebie umowie. Może to ograniczyć Twoją możliwość korzystania z wielu narzędzi dostępnych dla testerów bezpieczeństwa. Uruchamianie skryptów lub programów nieautoryzowanych przez dostawcę usług internetowych może skutkować zakończeniem świadczenia usług.

• Przed przeprowadzeniem testu bezpieczeństwa należy zapoznać się z przepisami stanowymi i federalnymi dotyczącymi przestępczości komputerowej. Przepisy federalne obowiązują we wszystkich stanach, podczas gdy przepisy stanowe mogą się różnić. Znajomość obowiązujących przepisów jest konieczna.

• Uzyskaj to na piśmie. Jako niezależny wykonawca musisz uzyskać od klienta podpisanie pisemnej umowy zezwalającej na przeprowadzenie testów penetracyjnych przed rozpoczęciem. Powinieneś również poprosić prawnika o przeczytanie umowy, zwłaszcza jeśli Ty lub przedstawiciel firmy wprowadziliście jakiekolwiek zmiany.

• Musisz zrozumieć narzędzia dostępne do przeprowadzania testów bezpieczeństwa. Nauka ich używania powinna być ukierunkowanym i metodycznym procesem