Planowanie testów penetracji fizycznej

„Pierwszą ofiarą wojny jest plan”. -nieznany

Celem tej części jest przekazanie wiedzy na temat zbudowania odpowiedniego zespołu do przeprowadzenia testu penetracji fizycznej. To nie jest małe zadanie; obejmuje zebranie zespołu, wyznaczenie odpowiednich ról, organizację wstępne badania i umiejętność zaplanowania zadania od początku do końca. Należy również wziąć pod uwagę aspekty administracyjne i prawne. Po zakończeniu fazy planowania projektu członkowie zespołu powinni wiedzieć, czego się od nich oczekuje i, co równie ważne, czego oczekiwać od zadania. Praca włożona w fazę planowania zostanie nagrodzona podczas realizacji. Jest taki stary żart, że „w teorii teoria i praktyka są tym samym, ale w praktyce tak nie jest”. Touch´e. Ważną rzeczą do zapamiętania na etapie planowania jest to, że nic nie jest ani nie powinno być osadzone w kamieniu. Twój plan testowania powinien być wystarczająco elastyczny, aby uwzględnić ustalenia awaryjne, w przypadku gdy założenia okażą się niepoprawne lub okoliczności, które wcześniej przyjmowałeś za pewnik, zmieniły się . Opracowując scenariusz zaangażowania, należy wziąć pod uwagę potencjalne ryzyko, na jakie narażony jest klient i jakie korzyści przyniesie mu badanie fizyczne. Jeśli przeprowadzasz ogólne testy lub po prostu wykonujesz ruchy, marnujesz czas i pieniądze wszystkich. Rozważ ten przykład: firma zajmująca się optyką wysokiej klasy chce przeprowadzić test fizyczny w ich europejskiej centrali. Obiekt jest duży i zatrudnia kilkaset osób (głównie przedstawicieli handlowych, średniego kierownictwa i personelu pomocniczego). Na stronie znajduje się również magazyn dystrybucji wszystkich produktów wysyłanych do Europy, na Bliski Wschód i do Afryki. Jakie jest ich główne ryzyko? To nie jest szpiegostwo: w witrynie nie są prowadzone żadne badania i prace rozwojowe, chociaż podobnie jak wszystkie witryny firmy na całym świecie, jest ona połączona w sieć. Ta firma produkuje aparaty fotograficzne, skanery i obiektywy, co samo w sobie nie jest kontrowersyjną działalnością; dlatego ryzyko infiltracji przez dziennikarzy i aktywistów jest minimalne. W tym przypadku największym problemem jest prawdopodobnie prosta kradzież. Ponieważ firma produkuje urządzenia, które kosztują wiele tysięcy dolarów i mieszczą się w plecaku, magazyn byłby kuszącym celem dla złodziei. Nie oznacza to, że biura, personel i sieć komputerowa nie powinny być brane pod uwagę w teście penetracyjnym, ale musisz zidentyfikować ryzyko klienta związane z jego interesem biznesowym. Niezależnie od powyższego, przez większość czasu nie będziesz miał dużego wkładu w określanie docelowych zasobów i będzie mocno skierowany na obszary, które klient chce przetestować. Nie powinieneś jednak nieśmiało mówić, jeśli uważasz, że dany scenariusz ma niewielką wartość w świecie rzeczywistym i sugeruje lepsze alternatywy. W poprzednim przykładzie zespół testujący miałby niewielkie trudności z wejściem do docelowych biur i robieniem zdjęć, ale całkowicie zignorowałby prawdziwe problemy. Ryzyko jest różne w różnych organizacjach, ale rozważ przykłady poniższe:

Obszar działalności: przykładowe ryzyko: przykładowy scenariusz

Rząd centralny lub wojsko: atak terrorystyczny „Przemyt paczki do bezpiecznego obszaru.

Siedziba firmy: Szpiegostwo: Dostęp do plików lub systemów komputerowych.

Sprzedaż samochodów luksusowych: Kradzież: Usuwanie aktywów :Budowanie zespołu operacyjnego

Zespół operacyjny faktycznie dokonuje fizycznej penetracji i członków można podzielić na różne role o różnych obowiązkach i obszarach wiedzy specjalistycznej. Skład zespołu będzie się różnić z każdym testem, ponieważ nie ma dwóch takich samych; w związku z tym nie wystarczy zbudować jeden zespół i mieć nadzieję na najlepsze. Należy to zrobić na etapie planowania każdego testu. Względy finansowe i inne praktyczne względy sprawiają, że role te mogą się nakładać, a członkowie zespołu przyjmą więcej niż jedną rolę, nawet w ramach jednego testu.

Operator

Operator to ogólny termin używany w odniesieniu do podstawowego członka zespołu operacyjnego. Termin ten odnosi się do wszystkich członków zespołu, bez względu na ich specjalizacje lub role. Podstawowa rola operatora polega na tym, że każdy zaczyna przed szkoleniem w specjalistycznej dziedzinie. Chociaż wszyscy członkowie zespołu mogą być dokładnie określani jako operatorzy, zwykle są to ludzie, którzy bezpośrednio uczestniczą w testach, a nie w roli wsparcia. Jak mówię, termin ten jest ogólny i nie oznacza wiedzy specjalistycznej w jakiejkolwiek roli.

Lider zespołu

Ten członek zespołu ponosi ostateczną odpowiedzialność za dostarczenie , przypisanie, zarządzanie projektem i członkami zespołu, współpracę z klientem i tak dalej. Ta rola nie powinna być stała, ale cykliczna. Daje to każdemu doświadczenie przywódcze i zachęca do nowego podejścia. Lider zespołu zwykle prowadzi zespół w terenie, ale czasem trzeba to zrobić z centrali (HQ), gdzie pełni rolę koordynatora. Nie jest niczym niezwykłym przekazanie roli lidera zespołu operatorowi w terenie, przy jednoczesnym zachowaniu koordynatora dowództwa, ponieważ zapewnia to najlepsze z obu światów.

Koordynator lub planista

Koordynator kieruje i pomaga członkom zespołu z centrali lub z innej lokalizacji poza siedzibą, gdy lider zespołu jest rozmieszczany z głównym zespołem operacyjnym. Ten członek zespołu zapewnia, że pomoc zewnętrzna (techniczna, prawna, referencyjna, inżynieria społeczna itp.) Jest zawsze dostępna. Kiedy bezpośrednia koordynacja rozmieszczonych operatorów poza siedzibą jest niepotrzebna, nadal zwykle ktoś ma tę rolę i jest absolutnie krytyczny, jeśli wiele wektorów lub zespołów jest rozmieszczonych jednocześnie przeciwko temu samemu celowi. Typowym przykładem może być test fizyczny przeprowadzany równolegle z intruzją komputerową, szczególnie gdy informacje z każdego zespołu muszą być przekazywane do drugiego; udana ingerencja w komputer może zależeć od informacji zebranych na miejscu, a udana ingerencja fizyczna może wymagać ciągłej zdalnej inteligencji lub innej formy kontroli elektronicznej.

Inżynier społeczny

Inżynieria społeczna to sztuka oszukiwania i manipulacji ludźmi, a umiejętność krytyczna dla powodzenia tego rodzaju zaangażowania. Wiedzy fachowej w tej dziedzinie nie można łatwo nauczyć; jest albo naturalna, albo wyuczona przez doświadczenie. Inżynieria społeczna jest najczęściej wykonywana poza siedzibą i jest atakiem często wykonywanym przed testami fizycznymi. Biorąc to pod uwagę, można oczekiwać, że wszyscy operatorzy wykonają pewien stopień inżynierii społecznej podczas pobytu na miejscu.

Specjalista ds. włamań do komputera

Ta rola jest również określana jako „etyczny haker”, dyscyplina sama w sobie. Specjalista ds. Włamań do komputera jest odpowiedzialny za uzyskanie dostępu do komputerów i sieci. W kontekście fizycznego testu penetracji zwykle (ale nie wyłącznie) przeprowadza się go na miejscu. Kluczowymi celami w fizycznych testach penetracyjnych są zwykle systemy informatyczne, dlatego jest mało prawdopodobne, że odniesiesz długofalowy sukces, chyba że w twoich zasobach znajdą się osoby zdolne do tego rodzaju pracy. Na szczęście przemysł testowania penetracji komputerów kwitnie i ten zestaw umiejętności nie jest trudny do znalezienia.

Specjalista ds. bezpieczeństwa fizycznego

Ten członek zespołu powinien posiadać umiejętność otwierania zamków i profilowania

i ogólnie pokonując środki bezpieczeństwa fizycznego. Zazwyczaj przynajmniej jeden członek zespołu powinien posiadać podstawowe umiejętności w tym zakresie. Zbieranie zamków nie jest trudne, ale wymaga wprawy i odrobiny szczęścia. Omawiam wszystko, czego potrzebujesz, aby zacząć w rozdziale 5 i odnoszę się do różnych części sprzętu, które ułatwią ci życie.

Specjalista ds. nadzoru

Oczekuje się, że ten członek zespołu będzie w stanie robić zdjęcia budynków, personelu, odznak, wysypisk śmieci i ochrony granic. Personel nadzoru powinien oczywiście mieć doświadczenie w posługiwaniu się kamerą, chociaż jest to tylko najbardziej podstawowy warunek. Operator nadzoru jest kluczowym członkiem zespołu i musi być w stanie gromadzić dowody tajnymi środkami pieszo, samochodem lub transportem publicznym.

Przypisywanie ról członkom zespołu

Role w poprzednich sekcjach nie opisują poszczególnych członków zespołu , ale zestawy umiejętności specjalistyczne - role, które może przyjąć każdy członek zespołu podczas wykonywania testu. Tylko największe grupy testowe będą mogły wdrożyć role zespołów operacyjnych na tym poziomie rozdzielczości. Nawet wtedy robienie tego nie jest ani opłacalne, ani operacyjne. Efektywność wymaga, aby poszczególni członkowie zespołu przyjmowali wiele obszarów odpowiedzialności. Na przykład gromadzenie informacji nie jest wymienione jako zestaw umiejętności specjalistycznych. Jest to coś, do czego każdy członek zespołu będzie musiał się przyczynić podczas testu, a biorąc pod uwagę liczne dyscypliny, które obejmuje, nie można tego uważać za „specjalistę" per se. Niektóre urządzenia są standardem we wszystkich zleceniach; niektóre nie są wymagane; wiele jest opcjonalnych. Ogólny charakter testu i role przypisane poszczególnemu członkowi zespołu powinny określać sprzęt przydzielany członkom zespołu. Sama definicja zespołu oznacza, że poszczególni członkowie zespołu będą mieli różne zestawy umiejętności i będą naturalnie predysponowani do określonych ról. Przypisanie etycznego hakera roli inżynierii społecznej to nie tylko marnotrawstwo zasobów, ale pokazuje brak zrozumienia, cechy, które składają się na dobrego inżyniera społecznego. Niekoniecznie są one zgodne z naturą etycznego hakera. Co najmniej w zasadzie każdy może nauczyć się etycznego hakowania, fotografii lub otwierania zamków. Inżynieria społeczna wymaga pewnego rodzaju osobowości: pewności siebie, ekstrawertyka i ogólnie dobrego stosunku do ludzi. To nie jest coś, w czym można się akredytować. Z drugiej strony umiejętności specjalisty ds. włamań do komputera mogą nie być od razu widoczne dla kogoś, kto nie ma doświadczenia w etycznym hakowaniu. Dlatego praktykujący muszą albo wykazać się doświadczeniem w tej dziedzinie, albo posiadać podstawową akredytację (ta pierwsza jest lepsza). Zdecydowanie radzę, aby w składzie zespołu uwzględniać tylko własnych pracowników. Korzystanie z kontrahentów nie jest zalecane ze względów operacyjnych i prawnych. Pomyśl o tym z perspektywy klienta, który może sprzeciwić się sprowadzeniu przez Ciebie stron trzecich, które mogą być dla Ciebie nieznane i których poświadczenia mogą być trudniejsze do zweryfikowania.

Planowanie i przepływ pracy

Podczas planowania projektu utwórz przepływ pracy, aby mieć pewność, że obejmiesz wszystkie aspekty zadania. Przygotowanie do zlecenia obejmuje kilka faz. Niektóre są nieuniknione, a niektóre są otwarte na interpretację. Jednak stosuję następujące podejście, ponieważ jest dokładne i pozostawia jak najmniej szansy:

1. Otrzymanie zlecenia - Na tym etapie podpisano umowy i przestrzegano pewnych formalności prawnych.

2. Negocjowanie zasad zaangażowania - określają one, co możesz i nie możesz zrobić podczas testowania, a ich celem jest zwykle ograniczenie testerów do pewnego zakresu.

3. Przeprowadzanie badań wstępnych - Jesteś teraz gotowy do kontynuowania wstępnej fazy gromadzenia informacji. To przybierze wiele form:

• Określanie ryzyka - ważne jest dokładne oszacowanie ryzyka, jakie projekt stwarza zarówno dla firmy, jak i członków zespołu, którzy ją realizują.

• Pisanie planu testów - formalny (ale elastyczny) plan testów to dobry pomysł zarówno z punktu widzenia zarządzania projektami, jak i z perspektywy prawnej.

• Sprzęt do gromadzenia - ważne jest, aby zespół zabrał sprzęt odpowiedni do testu, bez nadmiernego obciążenia.

4. Dostarczanie dokumentacji i wymogów prawnych - Po zakończeniu etapu planowania będziesz mieć nie mniej znaczącą ilość dokumentacji. Omawiamy, co powinieneś mieć i kto powinien mieć do niego dostęp.

Otrzymanie zlecenia i negocjowanie zasad zaangażowania

Faza planowania zwykle rozpoczyna się po podpisaniu umów i wymany. Nie dotyczy to jednak wyłącznie tego przypadku. Niektórzy klienci chcą negocjować zasady zaangażowania (RoE) i dołączyć je jako część umowy przed podpisaniem. Jest to kwestia preferencji: większe organizacje zwykle chcą jak najwięcej szczegółów umowy. RoE są niezwykle ważne. Są to parametry operacyjne, w ramach których pracują członkowie zespołu testującego penetrację; kierują zespołem i ograniczają go. Istnieją one po to, aby określić nie tylko to, co należy wziąć pod uwagę w trakcie cyklu życia projektu, ale także w celu ochrony testerów i klientów przed nieporozumieniami i konsekwencjami prawnymi, jakie mogą one spowodować. RoE są wzajemnie uzgadniane przez testerów i klienta. Oto lista minimalnych uwag:

• Musisz określić, które obszary bezpieczeństwa są uważane przez klienta za słabe i chcą zostać przetestowane, na przykład bezpieczeństwo granic fizycznych.

• Musisz określić, które obszary testowania klient chce uniknąć ze względów prawnych, takich jak ścisły nadzór personelu. Niektórzy klienci wolą unikać testowania w niektórych obszarach, ponieważ zaufanie do tego obszaru jest wysokie lub zostało niedawno ocenione.

• Musisz uzgodnić, którzy członkowie zespołu przeprowadzą testy. Nie wszyscy członkowie zespołu mogą posiadać niezbędne zezwolenia.

• Musisz uzgodnić czas trwania testu lub maksymalny dozwolony czas .

• Musisz uzgodnić wcześniej podany poziom informacji (jeśli istnieje). Test, w którym zespół operacyjny otrzymuje z wyprzedzeniem istotne informacje (w celu zaoszczędzenia czasu i skupienia się na konkretnym obszarze) nazywa się „testowaniem kryształowej skrzynki”. Jeśli nie podano żadnych informacji, test jest określany jako „testowanie czarnej skrzynki”. Coś pośrodku można nazwać „testem w szarej skrzynce”.

• Musisz uzgodnić docelowe aktywa. Aktywa są składnikami ogólnymi celu. Zwykle zasób to coś, co zespół musi zdobyć, identyfikować, uzyskiwać dostęp lub fotografować. Przykłady obejmują centra operacyjne sieci, hasła lub personel docelowy.

• Musisz uzgodnić okoliczności, które muszą wystąpić, aby test mógł zostać uznany za sukces z punktu widzenia zespołu operacyjnego.

• Powinieneś opisać okoliczności, które muszą wystąpić, aby test mógł zostać uznany za porażkę z punktu widzenia zespołu operacyjnego.

• Powinieneś uwzględnić okoliczności, w których, jeśli wystąpią, test uznaje się za przerwany.

• Musisz zgodzić się na działania, które należy podjąć bezpośrednio po udanych, nieudanych i przerwanych testach.

• Musisz ustalić harmonogram prezentacji i dostawy raportu z posttestingu.

Gdy ty i twój klient uzgodnicie te szczegóły, udokumentuj aby wypełnić RoE w celu dodania do zestawu dokumentów projektu.

Przeprowadzanie wstępnych badań

Techniki przeprowadzania wstępnych badań i analizy informacji można znaleźć w różnych częściach. Tutaj omawiam ten temat wyłącznie z perspektywy zrozumienia i planowania. Wstępne gromadzenie danych wywiadowczych można ogólnie podzielić na obszary z poniższej listy. Biorąc pod uwagę, że twoje cele zwykle (choć niekoniecznie) polegają na uzyskaniu dostępu do obiektów korporacyjnych lub rządowych, gromadzony przez ciebie rodzaj wywiadu musi dalej wspierać i wspierać następujące cele:

• Inteligencja ludzka (HUMINT) - inteligencja zebrana bezpośrednio ze źródła ludzkiego; Zasadniczo HUMINT odnosi się do uprzywilejowanych, choć niekoniecznie tajnych lub formalnie poufnych informacji uzyskanych od osób wewnętrz pod fałszywym pretekstem. Gromadzenie takich informacji nazywa się inżynierią społeczną i jest wystarczająco ważnym tematem, aby traktować je samodzielnie. Umiejętne wykorzystanie gromadzenia ludzkiej inteligencji zapewni zespołowi operacyjnemu znaczną przewagę podczas penetracji dowolnej organizacji.

• Inteligencja sygnałów (SIGINT) - inteligencja gromadzona za pomocą technologii przechwytywania lub słuchania; Naruszenie sieci bezprzewodowych w całej witrynie spoza docelowego rdzenia jest formą SIGINT, którą można rozważyć podczas wstępnej fazy, jednak na ogół może ona być drugorzędna w stosunku do innych form gromadzenia danych wywiadowczych w fazie wstępnej (chyba że cel ma bardzo niepewną lub niejawną komunikację). Po przekroczeniu granic bezpieczeństwa fizycznego (określanych jako przejście z PRIME do CORE) inteligencja sygnałów staje się ważniejsza w miarę udostępniania łączy sieciowych i technologii bezprzewodowych krótkiego zasięgu.

• Inteligencja Open Source (OSINT) - inteligencja oparta na informacjach ze źródeł publicznych; Źródła te najczęściej można znaleźć w Internecie lub za pośrednictwem Internetu. Na przykład informacje o pracownikach są szczególnie przydatne, gdy angażują się w preteksty i inne formy inżynierii społecznej.

• Inteligencja obrazów (IMINT) - inteligencja gromadzona za pomocą zarejestrowanych obrazów, tj. Fotografii. Jeśli to możliwe, zdjęcia miejsca docelowego i ewentualnie personelu powinny zostać pozyskane we wstępnej fazie, w zależności od charakteru zlecenia. Wartości dobrej inteligencji fotograficznej nie można lekceważyć, a jej zalety będą coraz bardziej widoczne w całej książce. Historycznie IMINT odnosi się również do wywiadu satelitarnego; jednak zdjęcia satelitarne są skrzyżowaniem IMINT i OSINT, o ile rozciąga się na Google Earth i jego odpowiedniki.

Określanie ryzyka

Ostatecznie obowiązkiem lidera zespołu jest określenie, co stanowi akceptowalny poziom ryzyka projektu. Jeśli lider zespołu uważa, że poziom ryzyka jest zbyt wysoki, wówczas RoE należy ponownie ocenić lub nie należy przeprowadzać testu. Ryzyko w fizycznych testach penetracyjnych można wyrazić na wiele sposobów, ale można je ogólnie podzielić na następujące obszary, które są powiązane i

pokrywają się - brak ryzyka w próżni - ryzyko umowne, operacyjne, prawne i środowiskowe. Entuzjastyczni menedżerowie projektów zauważą, że zapewnia to wygodny akronim –COLE.

• Ryzyko wynikające z umowy - problemy z kontraktem zwykle występują, gdy firma testująca odgryzła więcej, niż może przeżuć, a zespół ma zdolność do wykonania zadania, nie spełnia zobowiązań umownych. Jest to powszechny, ale możliwy do uniknięcia problem. Innymi słowy, ponieważ źle przygotowany i źle wyszkolony zespół nie był w stanie wykonać zadania, niekoniecznie oznacza, że klient jest bezpieczny. Jest to wspólny wątek we wszystkich obszarach oceny podatności, ale szczególnie w testach penetracji fizycznej, ponieważ awarie wydają się być bardziej widoczne. Nigdy nie podejmuj się zadania, które według ciebie nie jest możliwe do zrealizowania lub którego nie można wykonać.

• Ryzyko operacyjne - są to niezamierzone lub nieprzewidziane problemy podczas wykonywania testu, który w najlepszym wypadku prowadzi do trudności w wykonaniu zadania, aw najgorszym przypadku do przerwanej misji. Ryzyko operacyjne jest zwykle przewidywalne z pewnym wyprzedzeniem i dlatego jest możliwe do uniknięcia. Przykłady obejmują:

• Awaria komunikacji z powodu awarii ludzkiej lub technicznej.

• Niedoświadczeni członkowie zespołu źle interpretują instrukcje lub cele.

• Brak prawidłowej oceny trudności w osiągnięciu początkowego kamienia milowego prowadzącego do późniejszego krachu.

• Ryzyko prawne - Projekt może ponosić bezpośrednie lub pośrednie ryzyko prawne. Członkowie zespołu mogą zostać postawieni w pozycji, która może bezpośrednio doprowadzić do ich aresztowania. Może się to zdarzyć, gdy nadmiernie entuzjastyczny ochroniarz obchodzi procedurę i bezpośrednio obejmuje egzekwowanie prawa; gdy ktoś uważa, że członek zespołu zachowuje się podejrzanie i dzwoni na policję; lub gdy członkowie zespołu są bezpośrednio zatrzymywani przez policję, na przykład podczas nocnych ćwiczeń penetracyjnych. Podczas testu czarnej skrzynki zakres może zostać przekroczony operacyjnie, czasem katastrofalnie. Przykładem tego jest penetracja niewłaściwego obiektu lub firmy. Nie śmiejcie się; dzieje się tak, zwłaszcza we wspólnych pomieszczeniach. Wyobraź sobie zażenowanie włamaniem się do niewłaściwej sieci bezprzewodowej lub słyszeniem, że członek zespołu (być może nie posiadający podstawowej wiedzy matematycznej) wspiął się przez niewłaściwe okno do sali zarządu sąsiedniej firmy. Przynajmniej może to obejmować wyjaśnienie sędziemu, że przypadkowo włamałeś się do niewłaściwego budynku. Takie błędy są niezmiennie drogie.

• Zagrożenia dla środowiska - są to zagrożenia fizyczne, które może spowodować Twój zespół spotkanie podczas testów, które może bezpośrednio wpłynąć na zdrowie i bezpieczeństwo członków zespołu. Ryzyka te różnią się znacznie w zależności od zlecenia, ale uwzględniają co najmniej nieodłączne niebezpieczeństwa związane z:

• pracą w nocy lub w ciemności;

• pracą w pobliżu dużych zbiorników wodnych;

• pracą w obecności maszyn lub wysokiego napięcia;

• wspinanie się i opadanie;

• atakowaniem przez psy stróżujące;

• pracą w ekstremalnych temperaturach lub temperaturach;

• wspinaniem się na drut kolczasty lub żyletkę lub ogrodzenie elektryczne;

• konfrontacja z uzbrojoną ochroną.

Lider zespołu nigdy nie powinien świadomie narażać swoich ludzi na niebezpieczeństwo. Wiele witryn w Ameryce Północnej i innych krajach korzysta z uzbrojonych zabezpieczeń. W takich okolicznościach istnieje nieodłączne ryzyko obrażeń lub śmierci każdego członka przydzielonego do zespołu operacyjnego. Odpowiedzialność za wszystkie strony jest ogromna. Osobiście nie zalecam przyjmowania pracy w okolicznościach, w których broń palna jest rutynowo wydawana pracownikom ochrony; mogą pociągnąć za spust , zanim ludzie będą mieli okazję się wylegitymować. Jednym z problemów nieodłącznie związanych z fizycznymi testami penetracji jest uzyskanie realistycznej oceny narażenia klienta. Zespół operacyjny ma ograniczony czas i zakres; atakujący nie jest. Zagrożenia dla środowiska dodatkowo wpływają na możliwość oceny podatności organizacji na zagrożenia, ponieważ klienci nie będą chcieli podpisywać się na testach, które postrzegają jako potencjalnie szkodliwe dla testera, co z kolei może skutkować pozwem klienta.

Pisanie planu testu

Po wykonaniu poprzednich kroków jesteś teraz w stanie sporządzić plan testu. W przykładzie pokazanym w tej sekcji celowo zachowałem luźny język, aby zapewnić maksymalną zgodność z własnymi metodami zarządzania projektami. Plan testowy jest podzielony na trzy sekcje, które wyszczególniają uzgodniony plan zaangażowania z różnych punktów widzenia lub warstw rozdzielczości:

• Strategiczny - jest to widok projektu na bardzo wysokim poziomie, który szczegółowo opisuje cele, zasoby, członków zespołu, potencjalne ryzyko COLE i niezbędny sprzęt. Można tu również przedstawić zarys tła i historii projektu. Można tu również przedstawić zarys tła i historii projektu.

• Taktyczny - Biorąc pod uwagę cele strategiczne, w tej sekcji tworzona jest lista kamieni milowych lub mini-bramek oraz kolejność, w jakiej według nich powinny zostać one ukończone.

• Operacyjny - w tej sekcji szczegółowo określono, co jest wymagane do ukończenia każdego kamienia milowego i jak jego zakończenie wpłynie na zaangażowanie jako całość.

Na tym etapie jest o wiele bardziej ilustracyjne, aby przyjrzeć się przykładowemu planowi testów i zobaczyć, jak ta teoria jest stosowana. Jak widać, plan testów nie musi być ogromny. W rzeczywistości najlepiej jest trzymać go tak krótko i wyraźnie, jak to możliwe.

Przykładowy plan testów

Kierownik zespołu: Kris Mitchell Data: 7 stycznia 2020

Klient: Lithex Pharmaceuticals

Po dyskusji z Lithex Pharma proponuję przyjęte podejście jak poniżej:

ZARYS STRATEGICZNY

Lithex chce testu penetracji fizycznej swojego obiektu w Thame w Anglii. Dlatego proponuję wykorzystanie lokalnych zasobów JE i TS. Po kilku podejrzewanych incydentach szpiegostwa przemysłowego (których szczegółów Lithex postanowił nie udostępniać nam), istnieją obawy, że bezpieczeństwo granic, zarówno fizyczne, jak i elektroniczne, jest niewystarczające i potencjalnie zagrożone. Klient prowadzi wewnętrzne dochodzenie w sprawie możliwości występowania pieprzyki na miejscu. Zadanie polegało na wszystkich aspektach testowania dostępu. Elementem etycznego

włamania do hakowania zajmuje się LS w biurze w Waszyngtonie i dla naszych celów należy go traktować jako osobny projekt. Jeśli chodzi o zaangażowanie fizyczne, klient jest zainteresowany tym, jak łatwo możemy:

• Zdobyć poświadczenia domeny wewnętrznej sieci, szczególnie poświadczeń administratorów domeny.

• Potajemnie zainstalować fałszywe urządzenia podsłuchowe w sali konferencyjnej. Rzeczywiste urządzenia odsłuchowe NIE powinny być używane.

ROE

Mamy pięć dni roboczych (od pon. 14 stycznia 2020 r.) Na zakończenie prac na miejscu. Przeprowadzono już wstępne badania. Zadanie będzie czarne, a cel nie będzie świadomy (tj. CIO i lokalni oficerowie nie zostali poinformowani o testach). Wszelka późniejsza komunikacja będzie przeze mnie. Biuro CEO będzie oficjalnym punktem kontaktowym po rozpoczęciu testów; załatwiła, aby ktoś był dostępny w godzinach pracy w biurze Lithex w Chicago.

Ponieważ bezpieczeństwo poza biurem jest (uważane przez klienta za wysokie), a kampus jest zamknięty, testy są ograniczone tylko do godzin pracy. Nie należy podejmować nurkowania w kontenerach ze względu na fakt, że toksyczne produkty uboczne farmaceutyczne najwyraźniej docierają do głównych kontenerów. Myślę, że zatrzymamy to dla siebie. Biorąc pod uwagę, że nie wolno nam przeprowadzać nocnych testów i widocznej pozycji śmietników, nie jestem pewien, czy i tak byłoby to wykonalne. Na miejscu jest kilka sieci bezprzewodowych, postępuj według własnego uznania dotyczące tego.

RYZYKO COLE

Obiekt znajduje się na wsi i stanowi odrębny kampus; wszystkie budynki są własnością Lithex, a wszyscy pracownicy są pracownikami lub kontrahentami Lithex. Według wstępnych badań, personel ochronny (Tangos) jest lekko obecny, jednak są oni w większości ograniczeni do biura straży z tyłu kampusu. Patroli straży praktycznie nie ma w ciągu dnia; nacisk kładzie się (o ile nam wiadomo) na monitorowanie sygnałów z kamer. Ponieważ jest to obiekt brytyjski, nie ma promieni rentgenowskich.

CZŁONKOWIE ZESPOŁU I SPRZĘT

Koordynuję zespół z biura DC. JE i TS będą w środku pola. JE jest doświadczonym specjalistą od włamań do komputera, choć ma niewielkie doświadczenie w testach fizycznych. TS poradzi sobie z każdą pracą twarzy, blokadą ,zbieraniem i tak dalej. Sprzęt do tego testu będzie prosty; poza standardem sugerowane jest następujące wyposażenie:

• GPS

• Narzędzia do blokowania zamka

• Odpowiednio skonfigurowane laptopy i akcesoria.

Sukienka powinna być elegancka.

ZARYS OPERACYJNY

• Naruszenie bezpieczeństwa granic: Prime- Dotarcie do samego kampusu jest bardzo proste. Pierwszą kontrolą bezpieczeństwa jest odbiór w budynku głównym. Wszystkie inne budynki w kampusie są połączone w sieć.

• Naruszenie bezpieczeństwa granic: Rdzeń - (Będzie to ukryta lub jawna penetracja; będzie to decyzja operacyjna.) Dostęp do sali konferencyjnej będzie wymagał wejścia do głównego budynku, co z kolei będzie konieczne przejście przez recepcję lub znalezienia innego punktu wejścia. Wstępne badania pokazują kilka innych drzwi, ale nic rozstrzygającego. Dostęp do sieci należy uzyskać najpierw za pośrednictwem budynku peryferyjnego.

• Znajdź odpowiedni punkt dostępu do sieci - budynki peryferyjne będą względnie niepewne. Uzyskanie dostępu do sieci wewnętrznej prawdopodobnie nie będzie stąd trudne.

• Zdobądź hasła - tutaj postępuj według własnego uznania. To jest praca J.

• Zlokalizuj salę konferencyjną - Prawdopodobnie nie jest trudna do zlokalizowania, ale ponownie, głównym problemem jest dotarcie do przeszłości. Sugeruję, aby po zakończeniu fazy sieci testerzy zatrzymali się w recepcji, aby zapytać o drogę i ocenić bezpieczeństwo. Można to również zrobić przed rozpoczęciem testów, aby wydłużyć czas realizacji.

• Zakładamy „Podsłuch” - to mówi samo za siebie.

• Wyjdź - podobnie jak to.

Dostarczanie dokumentacji i wymagań prawnych

Do czasu zakończenia fazy planowania projektu będziesz mieć następującą dokumentację, która obejmuje zestaw dokumentacji projektowej (PDS):

• RoE;

• plan testów;

• podpisane umowy;

• kopie kart „wyjdź z więzienia za darmo”;

• skan oficjalnego dowodu tożsamości członków zespołu operacyjnego (paszport, prawo jazdy);

• skan więzi ubezpieczeniowych członków zespołu;

• skan informacji referencyjnych dotyczących poświadczenia bezpieczeństwa (jeśli dotyczy). Powinno to obejmować organizację lub dział sponsorujący. PDS należy złożyć u prawników lub urzędników firmy testującej.

Czy powinieneś powiadomić organy ścigania?

To jest twoja decyzjka. Na jednym teście prawnicy z firmy zachęcili mnie do poinformowania lokalnej policji, że będziemy prowadzić prace w okolicy i podania im pewnych szczegółów. Doprowadziło to do zaparkowania oznakowanego samochodu po drugiej stronie ulicy od miejsca docelowego w noc, w której prowadziliśmy nasz pierwszy nadzór. Około godziny później do naszego zespołu zwrócili się oficerowie, którzy twierdzili, że przeszli, i przesłuchiwali ich, ale wyraźnie wiedzieli o naszej obecności. Albo policja źle zrozumiała powody ich zaangażowania, nie ufała nam lub była po prostu ciekawa, nie jestem pewien. Jednak praca z policją spoglądającą przez ramię jest bardzo rozpraszająca i nie jestem gotów tego powtórzyć.

Kody, znaki wywoławcze i komunikacja

Przed wyruszeniem w teren warto mieć predefiniowaną listę słów i skrótów, niezależnie od wybranej technologii komunikacyjnej. Jest to przydatne dla szybkości komunikacji, bezpieczeństwa oraz eliminacji zamieszania i niejednoznaczności. Niektóre z tych warunków zostały dla nas ustalone na podstawie konwencji historycznej; niektóre dotyczą informacji, które zespół testujący penetrację będzie musiał przekazać, a inne dotyczą konkretnego zespołu operacyjnego. Terminologia nie jest kompletna, aby zachęcić czytelników do opracowania własnych protokołów komunikacyjnych zgodnie z ich potrzebami. Upewnij się, że wszyscy członkowie zespołu biegle przestrzegają przyjętych konwencji komunikacyjnych. W prostym scenariuszu testowym opisanym w ostatniej części konwencje komunikacji nie są konieczne. Jednak gdy testy stają się skomplikowane, gdy wielu członków zespołu znajduje się w różnych lokalizacjach, zdecydowanie powinieneś ustanowić i używać protokołów komunikacyjnych.

Podsumowanie

Przeprowadzenie testu penetracji fizycznej bez odpowiedniego planowania i gromadzenia informacji jest ćwiczeniem skazanym na niepowodzenie. Podczas fazy planowania powinieneś przejrzeć tą część, aby upewnić się, że wszystkie twoje bazy są objęte gwarancją. Powinieneś teraz zapoznać się z następującymi tematami:

• Zbudowanie zespołu operacyjnego - wiąże się to z wyborem odpowiednich ludzi do odpowiedniej roli, która jest silnie uzależniona od charakteru i skali testu. Jest prawdopodobne, że członkowie zespołu będą musieli zdobyć wiele zestawów umiejętności i przejąć wiele ról.

• Planowanie projektu - Różne organizacje preferują różne podejścia do zarządzania projektami, a język użyty w tym rozdziale jest wystarczająco luźny, aby można go było zintegrować z dowolną istniejącą metodologią.

• Zasady zaangażowania - w tym rozdziale przedstawiłem koncepcję RoE i jej wpływ na twoje podejście do testowania. RoE są krytyczne; są zwykle częścią umowy prawnej między firmą testująca a klientem.

• Przeprowadzanie wstępnych badań - w tej części omówiono wstępne badania z perspektywy fazy planowania i tego, jak to pasuje do ogólnego podejścia. Zbadano różne rodzaje gromadzenia danych wywiadowczych.

• Ocena ryzyka - ryzyko występujące podczas testowania ma różne formy i mogą być wyrażane na różne sposoby. Koncepcja COLE został wprowadzona jako środek oceny ryzyka dla zespołu testującego i firmy.

• Plan testu - powinieneś być teraz w stanie napisać plan testu, nawet jeśli nie znasz praktycznych elementów samego testowania.

• Zagadnienia prawne i dokumentacja - Powinieneś być teraz w stanie przedstawić wymaganą dokumentację na poparcie testu penetracji fizycznej i zapoznać się z niektórymi aspektami prawnymi.