Test penetracyjny symuluje metody wykorzystywane przez intruzów do uzyskania nieautoryzowanego dostępu do sieci i systemów organizacji oraz do ich kompromitacji. Celem testu penetracji jest przetestowanie implementacji zabezpieczeń i polityki bezpieczeństwa organizacji. Celem jest sprawdzenie, czy organizacja wdrożyła środki bezpieczeństwa określone w polityce bezpieczeństwa. Haker, którego intencją jest uzyskanie nieautoryzowanego dostępu do sieci organizacji, różni się od profesjonalnego testera penetracji. Profesjonalny tester nie ma złych zamiarów i nie wykorzystuje swoich umiejętności do poprawy bezpieczeństwa sieci organizacji bez powodowania utraty usług lub zakłóceń w działaniu firmy. W tej części przyjrzymy się aspektom testowania penetracji (testowanie penów), które musisz znać jako etyczny haker.

Definiowanie ocen bezpieczeństwa

Tester penetracyjny ocenia postawę bezpieczeństwa organizacji jako całości, aby ujawnić potencjalne konsekwencje realnego ataku na sieć lub aplikację. Oceny bezpieczeństwa można zaklasyfikować jako audyty bezpieczeństwa, oceny wrażliwości lub testy penetracyjne. Każda ocena bezpieczeństwa wymaga, aby osoby przeprowadzające ocenę posiadały różne umiejętności w oparciu o zakres oceny. Audyt bezpieczeństwa i ocena narażenia na atak skanują sieci IP i hosty pod kątem znanych słabości zabezpieczeń za pomocą narzędzi zaprojektowanych do lokalizowania systemów na żywo, wyliczania użytkowników oraz identyfikowania systemów operacyjnych i aplikacji, poszukiwanie wspólnych błędów konfiguracji zabezpieczeń i luk w zabezpieczeniach. Luka w zabezpieczeniach lub ocena bezpieczeństwa identyfikuje tylko potencjalne luki w zabezpieczeniach, podczas gdy test na pióro próbuje uzyskać dostęp do sieci. Przykładem oceny bezpieczeństwa jest patrzenie na drzwi i myślenie, czy te drzwi są odblokowane, może pozwolić komuś uzyskać nieautoryzowany dostęp, podczas gdy test pióra próbuje otworzyć drzwi, aby zobaczyć, dokąd prowadzą. Test penetracyjny jest zwykle lepszym wskaźnikiem słabości sieci lub systemów, ale jest bardziej inwazyjny i dlatego ma większy potencjał do zakłóceń w działaniu sieci.

Testowanie penetracyjne

Istnieją dwa rodzaje ocen bezpieczeństwa: oceny zewnętrzne i wewnętrzne. Zewnętrzna ocena testuje i analizuje publicznie dostępne informacje, przeprowadza skanowanie sieciowe i wyliczanie oraz uruchamia exploity spoza zasięgu sieci, zwykle za pośrednictwem Internetu. Wewnętrzna ocena przeprowadzana jest w sieci od wewnątrz organizacji, a tester działa jako pracownik z dostępem do sieci lub jako czarny kapelusz bez znajomości środowiska. Test penetracji czarnego kapelusza zwykle wiąże się z większym ryzykiem napotkania nieoczekiwanych problemów. Zaleca się zespołowi tworzenie planów awaryjnych w celu efektywnego wykorzystania czasu i zasobów. Możesz przeprowadzić outsourcing testu penetracji, jeśli nie masz wykwalifikowanych lub doświadczonych testerów lub jeśli musisz przeprowadzić specjalną ocenę w celu spełnienia wymagań audytu, takich jak Ustawa o Przenoszalności Ubezpieczeń Zdrowotnych i Odpowiedzialności (HIPAA). Organizacja stosująca termin oceny musi określać zakres oceny, w tym to, co ma być testowane, a czego nie należy testować. Na przykład test penetracyjny może być ukierunkowanym testem ograniczonym do pierwszych 10 systemów w strefie zdemilitaryzowanej (DMZ) lub wyczerpującej oceny, która pozwala odkryć jak najwięcej luk w zabezpieczeniach. W zakresie prac należy określić umowę o poziomie usług (SLA) w celu określenia wszelkich działań, które zostaną podjęte w przypadku poważnego zakłócenia świadczenia usług. Inne warunki angażowania zespołu oceniającego mogą określać pożądany kodeks postępowania, procedury, których należy przestrzegać, a także interakcję lub brak interakcji między organizacją a zespołem testującym. Ocena bezpieczeństwa lub test pióra może być wykonywany ręcznie przy użyciu kilku narzędzi, zazwyczaj freeware lub shareware, chociaż test może również

obejmować zaawansowane oprogramowanie płatne. Innym podejściem jest stosowanie droższych narzędzi automatycznych. Ocena stanu bezpieczeństwa organizacji za pomocą testu ręcznego jest czasem lepszym rozwiązaniem niż użycie automatycznego narzędzia opartego na standardowym szablonie. Firma może skorzystać z wiedzy doświadczonego specjalisty, który analizuje informacje. Chociaż zautomatyzowane podejście może być szybsze i łatwiejsze, w trakcie kontroli może zostać pominięte coś. Jednak podejście manualne wymaga planowania, harmonogramowania i starannej dokumentacji. Jedyną różnicą między prawdziwym "hakowaniem" a testowaniem pióra jest zezwolenie. Ważne jest, aby osoba wykonująca test penetracyjny otrzymała pisemną zgodę na wykonanie testu penetracyjnego.

Upewnij się, że masz pozwolenie przed testowaniem pióra

Około 8 lat temu pracowałem jako administrator sieci dla organizacji liczącej około 500 użytkowników. Mój szef zapytał, czy mógłbym dokonać oceny bezpieczeństwa sieci obwodowej organizacji. Powiedziałem mu, żeby przysłał mi e-mail z opisem tego, czego oczekiwał oceny, i po kilku godzinach zeskanowałem. Po wstępnych recenzjach okazało się, że poprzedni administrator miał kilka wyjątków "Zezwalaj na wszystko" ustawionych w firewallu. Nasza organizacja podzieliła się połączeniem, danymi, serwerami i obiektami z inną organizacją, która wykonała taką samą pracę jak nasza. Raz jeszcze zrobiłem recenzję i naprawiłem szereg problemów, mój szef powiedział innym kierownikom o postępach i zdecydowali, że chcą, żebym przetestował obwód innej organizacji. Najpierw poprosiłem o upewnienie się, że mamy upoważnienie do wykonania tych testów. Po dniu lub dwóch, mój menadżer powiedział mi, że jesteśmy dobrzy, i aby przejść do testów. Kierownictwo było zaniepokojone tym, że ktoś atakuje drugą organizację i przeszukuje naszą dedykowaną linię do naszej sieci. Nie otrzymałem kopii pisemnego upoważnienia do przeprowadzenia testu . Podczas skanowania znalazłem sieć - która nie miała zapory ogniowej i w większości niezłamanych serwerów - z uruchomionymi usługami internetowymi IIS, a jedynie oprogramowanie antywirusowe do ochrony. W sieci działała również baza danych Oracle. Przestałem robić cokolwiek na tym komputerze i sieci, gdy udało mi się zalogować jako administrator na serwerze, ponieważ robienie czegokolwiek dalej było bezcelowe. Napisałem raport i przesłałem to do mojego kierownika. Około miesiąca później ktoś z naszego personelu przeczytał w gazecie, że druga organizacja "została zhakowana". Biuro prokuratora generalnego zrobiło zamieszanie, a moim menedżerom i mnie groziło oskarżenie. Ostatecznie nic mnie nie spotkało ani mojego menedżera.

Testy penetracyjne

Testy penetracyjne obejmują trzy fazy:

* Faza wstępnego ataku

* Faza ataku

* Faza postataku

Faza prenatalna obejmuje rozpoznanie lub zbieranie danych. To pierwszy krok dla testera penetracyjnego. Zbieranie danych z Whois, DNS i skanowania sieciowego może pomóc w mapowaniu sieci docelowej i dostarczaniu cennych informacji dotyczących systemu operacyjnego i aplikacji działających w systemach. Test penetracyjny polega na zlokalizowaniu bloku IP i zastosowaniu wyszukiwania nazw domen Whois w celu znalezienia informacji kontaktowych personelu, a także wyliczenia informacji o hostach. Informacje te można następnie wykorzystać do stworzenia szczegółowego diagramu sieci i identyfikacji celów. Powinieneś także przetestować urządzenia filtrujące sieć, szukając legalnego ruchu, serwerów proxy testujących stres i sprawdzić domyślną

instalację zapór ogniowych, aby upewnić się, że domyślne identyfikatory użytkowników, hasła i hasła gości zostały wyłączone lub zmienione i nie jest dozwolone logowanie zdalne. Następna jest faza ataku, a podczas tej fazy narzędzia mogą obejmować zakres od exploita po responsywność. Są używane przez profesjonalnych hakerów do monitorowania i testowania bezpieczeństwa systemów i sieci. Te działania obejmują, ale nie są ograniczone do następujących:

Penetrowanie obwodu Ta aktywność obejmuje przeglądanie raportów o błędach, sprawdzanie list kontroli dostępu poprzez fałszowanie odpowiedzi za pomocą spreparowanych pakietów i ocenę reguł filtrowania protokołów za pomocą różnych protokołów, takich jak SSH, FTP i telnet. Tester powinien także przetestować przepełnienie bufora, iniekcje SQL, wadliwe sprawdzanie danych wejściowych, odkażanie wyników i ataki DoS. Oprócz wykonywania testów oprogramowania, należy poświęcić czas na przetestowanie wewnętrznych aplikacji internetowych i konfiguracji sieci bezprzewodowej, ponieważ zagrożenie poufne jest obecnie największym zagrożeniem bezpieczeństwa.

Zdobycie celu Ten zestaw działań jest bardziej inwazyjny i stawia większe wyzwanie niż skanowanie luki lub audyt. Możesz skorzystać z automatycznego narzędzia do wykrywania, takiego jak CORE IMPACT lub próbować uzyskać dostęp do systemu za pośrednictwem legalnych informacji uzyskanych inżynierią społeczną. Ta aktywność obejmuje także testowanie egzekwowania zasad bezpieczeństwa lub używanie narzędzi do łamania haseł i uprawnień do eskalacji, aby uzyskać większy dostęp do chronionych zasobów.

Eskalacja uprawnień Po nabyciu konta użytkownika tester może próbować nadać kontu użytkownika więcej uprawnień lub uprawnień systemom w sieci. Wiele narzędzi hakerskich jest w stanie wykorzystać lukę w zabezpieczeniach systemu i utworzyć nowe konto użytkownika z uprawnieniami administratora.

Wykonywanie, wszczepianie i wycofywanie Jest to ostatnia faza testowania. Twoje umiejętności hakerskie są wyzwaniem poprzez eskalowanie uprawnień w systemie lub sieci, nie zakłócając procesów biznesowych. Pozostawienie znaku może pokazać, gdzie udało ci się uzyskać większy dostęp do chronionych zasobów. Wiele firm nie chce, abyś zostawiła ślady lub wykonał dowolny kod, a takie ograniczenia zostały określone i uzgodnione przed rozpoczęciem testu.

Faza po ataku polega na przywróceniu systemu do normalnych konfiguracji próbnych, która obejmuje usuwanie plików, czyszczenie wpisów rejestru, jeśli zostały utworzone luki oraz usuwanie udziałów i połączeń. Na koniec przeanalizujesz wszystkie wyniki i utworzysz dwie kopie raportów oceny bezpieczeństwa, jedną dla twoich zapisów, a drugą dla zarządzania. Raporty te obejmują twoje cele, twoje spostrzeżenia, wszystkie podejmowane działania i wyniki działań testowych, i mogą zalecać poprawki dla luk w zabezpieczeniach. Ćwiczenie 15.1 pokazuje ramy dla wszechstronnego testu penetracji.

Ćwiczenie 15.1

Przeglądanie struktury narzędzi do testowania penetracyjnego

1. Otwórz przeglądarkę internetową na www.vulnerabilityassessment.co.uk.

2. Kliknij łącze Pen Test Framework u góry.

3. Rozwiń sekcję Footprinting sieci i zobacz podpozycje.

4. Kontynuuj w dół główną pozycję, rozwijając każdą z podpozycji dla ramy testu penetracyjnego Możesz użyć tej listy, aby zlokalizować wszystkie narzędzia niezbędne na każdym etapie procesu testowania penetracyjnego

Ramy prawne testu penetracyjnego

Tester penetracyjny musi zdawać sobie sprawę z prawnych konsekwencji włamań do sieci, nawet w sposób etyczny. Badaliśmy prawa mające zastosowanie do hakowania w Części 1. Dokumenty, które haker etyczny wykonujący test penetracyjny musi podpisać z klientem, są następujące:

* Zakres prac, określający, co ma być testowane

* Umowa o nieujawnianiu w przypadku, gdy tester widzi poufne informacje

* Zobowiązanie, zwalniające etycznego hakera z wszelkich działań lub zakłóceń usług spowodowanych testem penetracyjnym

Zautomatyzowane narzędzia do testowania penetracji

Ankieta z 2006 roku na liście dyskusyjnej hakerów stworzyła listę 10 najlepszych narzędzi do skanowania luk w zabezpieczeniach; ponad 3000 osób odpowiedziało. Fiodor (http://insecure.org/fyodor/), który stworzył listę, mówi: "Każdy, kto jest w dziedzinie bezpieczeństwa, powinien przejrzeć listę i zbadać narzędzia, których nie znają." Należy wziąć pod uwagę następujące kwestie: narzędzia do testowania najlepszych pisaków w zestawie narzędzi hakerskich:

Nessus Ten darmowy skaner podatności w sieci ma ponad 11 000 wtyczek. Nessus obejmuje zdalne i lokalne kontrole bezpieczeństwa, architekturę klient / serwer z graficznym interfejsem GTK oraz osadzony język skryptowy do pisania własnych wtyczek lub zrozumienia istniejących.

GFI LANguard Jest to komercyjny skaner bezpieczeństwa sieci dla systemu Windows. GFI LANguard skanuje sieci IP w celu wykrycia, które maszyny są uruchomione. Może określić system operacyjny hosta, jakie aplikacje są uruchomione, jakie pakiety usług systemu Windows są zainstalowane, czy brakuje jakichkolwiek poprawek zabezpieczeń i więcej.

Retina Jest to komercyjny skaner oceny słabości od eEye. Podobnie jak Nessus, Retina skanuje wszystkie hosty w sieci i raportuje o znalezionych lukach.

CORE IMPACT CORE IMPACT to zautomatyzowany produkt do testowania długopisów, uważany powszechnie za najmocniejsze narzędzie do wykorzystania (jest to również bardzo kosztowne). Ma dużą, regularnie aktualizowaną bazę profesjonalnych exploitów. Wśród jego funkcji można wykorzystać jeden komputer, a następnie ustanowić zaszyfrowany tunel za pośrednictwem tego komputera, aby dotrzeć do innych maszyn i wykorzystać je.

ISS Internet Scanner Jest to ocena podatności na poziomie aplikacji. Skaner internetowy może zidentyfikować ponad 1300 typów urządzeń sieciowych w Twojej sieci, w tym komputery stacjonarne, serwery, routery / przełączniki, zapory ogniowe, urządzenia bezpieczeństwa i routery aplikacji.

X-Scan X-Scan to ogólny wielowątkowy skaner podatności na ataki sieciowy z wtyczką. Umożliwia wykrywanie typów usług, zdalnych typów i wersji systemów operacyjnych oraz słabych nazw użytkowników i haseł.

SARA Security Auditor's Assistant Assistant (SARA) to narzędzie do oceny podatności, opracowane na podstawie narzędzia System Administrator Tool for Analysing Networks (SATAN). Aktualizacje są zwykle publikowane dwa razy w miesiącu.

QualysGuard Jest to internetowy skaner podatności. Użytkownicy mogą bezpiecznie uzyskać dostęp do QualysGuard za pomocą łatwego w użyciu interfejsu internetowego. Zawiera ponad 5000 sprawdzeń luk w zabezpieczeniach, a także silnik skanowania oparty na wnioskach.

SAINT Security Administrator's Integrated Network Tool (SAINT) Zintegrowane narzędzie sieciowe Security Administrator (SAINT) jest reklamą narzędzie oceny podatności.

MBSA Microsoft Baseline Security Analyzer (MBSA) jest zbudowany na Windows Update . Infrastruktura agenta i usługi Microsoft Update. Zapewnia spójność z innymi produktami Microsoft i skanuje średnio ponad 3 miliony komputerów tygodniowo.

Oprócz tej listy należy zapoznać się z następującymi narzędziami wykorzystującymi luki w zabezpieczeniach:

Metasploit Framework Jest to oprogramowanie typu open source używane do tworzenia, testowania i używania kodu wykorzystującego exploity.

Canvas Canvas to komercyjne narzędzie do wykorzystania luk w zabezpieczeniach. Obejmuje więcej niż 150 exploitów.

Rezultaty testów penetracyjnych

Głównym rezultatem na końcu testu penetracji jest raport z testu penetracyjnego. Raport powinien zawierać następujące informacje:

* Lista twoich ustaleń, w kolejności największego ryzyka

* Analiza twoich ustaleń

* Wniosek lub wyjaśnienie twoich ustaleń

* Środki zaradcze dla twoich ustaleń

* Pliki dzienników z narzędzi, które dostarczają dowodów potwierdzających twoje odkrycia

* Podsumowanie stanu bezpieczeństwa organizacji

* Nazwa testera i data testowania

* Wszelkie pozytywne wyniki lub dobre wdrożenia zabezpieczeń

Ćwiczenie 15. 2

Przeglądanie przykładowego raportu dotyczącego testowania pióra

1. Otwórz przeglądarkę internetową na www.desktopauditing.com.

2. Kliknij łącze po lewej stronie, aby wyświetlić raport audytu bezpieczeństwa IT i szablon wyników.

3. Przewiń całą drogę na dół strony i kliknij łącze Pobierz.

4. Użyj przykładowego raportu jako szablonu do tworzenia własnych raportów audytu bezpieczeństwa.

Podsumowanie

Audyt bezpieczeństwa lub testowanie pióra jest niezbędną częścią bezpiecznego środowiska sieciowego. Niezwykle ważne jest, aby zaufana i kompetentna osoba, taka jak etyczny haker, mogła zająć się systemami, aplikacjami i komponentami w celu zapewnienia wszystkich ustaleń dotyczących

bezpieczeństwa. Organizacja może wykorzystać raport z badań pióra jako miarę tego, jak skutecznie wdrożyły plan bezpieczeństwa i poprawiły bezpieczeństwo danych.

Do Zapamiętania !

* Zdefiniowałeś ocenę bezpieczeństwa. Ocena bezpieczeństwa to test wykorzystujący narzędzia hakerskie do określenia pozycji bezpieczeństwa organizacji.

* Poznałeś produkty do testowania pióra. Raport z badań pióra dotyczący wyników testu penetracji powinien zawierać sugestie dotyczące poprawy bezpieczeństwa, pozytywne wyniki i pliki dziennika.

* Poznałeś wymagania prawne testu pióra. Tester pióra powinien zlecić klientowi podpisanie umowy o zwolnienie z odpowiedzialności, zakresu prac i umowy o nieujawnianiu.

* Wymieniłeś kroki testowania penetracji. Wstrzymanie ataku, atak i po ataku są trzema fazami testowania penetracyjnego.

* Poznałeś dwa rodzaje ocen bezpieczeństwa. Oceny bezpieczeństwa mogą być wykonywane wewnętrznie lub zewnętrznie.