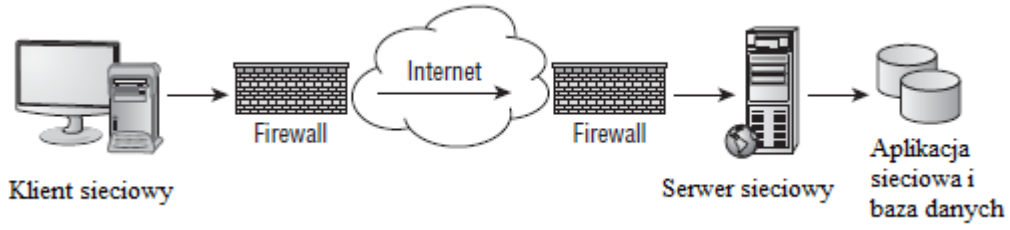
Ta część zawiera podstawowe informacje o hakowaniu serwerów sieciowych i wykorzystywaniu słabych punktów serwera internetowego i aplikacji internetowych. Omówiono także techniki łamania haseł oparte na sieci Web. Serwery WWW i aplikacje internetowe mają bardzo duży potencjał, aby zostać zagrożonym. Głównym powodem jest to, że systemy, które uruchamiają oprogramowanie serwera sieciowego, muszą być publicznie dostępne w Internecie. Serwer internetowy nie może być całkowicie odizolowany i w pewnym stopniu musi być dostępny dla uprawnionych użytkowników. Po zaatakowaniu serwera WWW, system może zapewnić hakerom inne drzwi do sieci. Nie tylko oprogramowanie serwera sieciowego, ale także aplikacje uruchamiane na serwerze sieciowym są otwarte do ataku i można je wykorzystać. Ze względu na swoją funkcję, serwery internetowe są bardziej dostępne niż inne systemy i są mniej chronione, więc są łatwiejsze do wykorzystania. Informacje docelowe na serwerze internetowym zwykle znajdują się w bazie danych na serwerze internetowym; ta baza danych jest dostępna za pośrednictwem aplikacji internetowej. Z tego powodu serwery internetowe i aplikacje internetowe idą w parze. Łamanie serwera sieciowego odbywa się zwykle w celu uzyskania dostępu do podstawowych danych w aplikacji internetowej.

Jak działają serwery sieciowe

Serwery WWW używają protokołu HTTP (Hypertext Transfer Protocol) i protokołu HTTPS (Hypertext Transfer Protocol Secure), aby umożliwić klientom sieciowym łączenie się z nimi oraz przeglądanie i pobieranie plików. HTTP jest protokołem warstwy aplikacji w stosie TCP / IP. HTTP i HTTPS to podstawowe protokoły używane przez klientów sieciowych, którzy uzyskują dostęp do stron internetowych znajdujących się na serwerach internetowych. Hypertext Markup Language (HTML) to język używany do tworzenia stron internetowych i umożliwia renderowanie tych stron w oprogramowaniu przeglądarki internetowej na klientach internetowych. Protokół HTTP działa tak, jak pokazano na rysunku



1. Klient sieci początkowo otwiera połączenie z adresem IP serwera WWW za pomocą portu TCP 80.

2. Serwer WWW czeka na żądanie GET od klienta żądającego strony głównej dla witryny.

3. Serwer WWW odpowiada kodem HTML strony głównej serwera WWW.

4. Klient przetwarza kod HTML, a oprogramowanie przeglądarki klienta WWW renderuje stronę na urządzeniu klienckim.

Zrozumienie, jak serwery internetowe działają - a co za tym idzie, jak są zhackowane - jest ważną częścią twojej pracy jako etycznego hacker. Obejmuje to poznanie ich słabych punktów, a także zrozumienie typów ataków, których może użyć haker. Ponadto należy wiedzieć, kiedy stosować techniki zarządzania poprawkami i zrozumieć metody stosowane w celu wzmocnienia serwerów sieciowych. Przyjrzymy się wszystkim tym tematom w poniższych sekcjach.

Typy luk w zabezpieczeniach serwera WWW

Serwery sieciowe, podobnie jak inne systemy, mogą zostać naruszone przez hakera. Następujące luki są najczęściej wykorzystywane w serwerach internetowych:

Błędna konfiguracja oprogramowania serwera internetowego Częstym problemem związanym z korzystaniem z internetowego serwera informacyjnego Microsoft (IIS) jako serwera WWW jest korzystanie z domyślnej witryny internetowej. Uprawnienia na domyślnej stronie są otwarte, co oznacza, że ustawienia domyślne pozostawiają otwartą stronę do ataku. Na przykład wszyscy użytkownicy w grupie mają pełną kontrolę nad wszystkimi plikami w domyślnym katalogu witryny. Bardzo ważne jest edytowanie i ograniczanie uprawnień po zainstalowaniu usług IIS na serwerze, ponieważ domyślny użytkownik systemu, IUSR_COMPUTERNAME, jest członkiem grupy Wszyscy. W związku z tym każdy, kto uzyska dostęp do domyślnej witryny, będzie miał dostęp do wszystkich plików w domyślnym folderze witryny i będzie miał niebezpieczne uprawnienia, takie jak Execute i Pełna kontrola do plików.

Błędy systemu operacyjnego lub aplikacji lub błędy w kodzie programowania Wszystkie programy, w tym system operacyjny i aplikacje serwera WWW, powinny być regularnie aktualizowane lub aktualizowane. W przypadku systemów Windows obejmuje to poprawki zabezpieczeń, poprawki i aktualizacje systemu Windows. Wszystkie te łatki można zautomatyzować lub ręcznie zastosować w systemach po ich przetestowaniu.

Niewłaściwa instalacja domyślna System operacyjny i ustawienia oprogramowania serwera sieciowego nie powinny być pozostawione domyślnie po zainstalowaniu i powinny być aktualizowane w sposób ciągły. Hakerzy wykorzystują te luki, aby uzyskać dostęp do serwera WWW. Ponieważ serwery internetowe są zwykle zlokalizowane w strefie zdemilitaryzowanej (DMZ), która jest publicznie dostępnym obszarem pomiędzy dwa urządzenia filtrujące pakiety i mogą być łatwo dostępne przez systemy klienckie organizacji - exploit serwera internetowego oferuje hakerom łatwiejszy dostęp do wewnętrznych systemów lub baz danych.

Ćwiczenie 8 .1

Wyłączanie domyślnej witryny w IIS

Aby wyłączyć domyślną witrynę w usługach IIS i dodać nową witrynę, wykonaj następujące kroki:

1. Otwórz IIS na twoim Windows Server lub maszynie wirtualnej (VM).

2. Wybierz witryny sieci Web w lewym okienku.

3. Kliknij prawym przyciskiem myszy domyślną witrynę w prawym panelu i wybierz Zatrzymaj z menu kontekstowego. Domyślna strona internetowa jest teraz wstrzymana.

4. Aby utworzyć nową witrynę, kliknij prawym przyciskiem myszy witryny sieci Web w lewym panelu i wybierz Nowa ➚ Witryna sieci Web.

5. Uruchomi się Kreator tworzenia stron internetowych. W kreatorze pojawi się ekran umożliwiający zmianę uprawnień w katalogu strony.

Maskowanie witryny to zdolność serwera WWW do wyświetlania różnych typów stron internetowych na podstawie adresu IP użytkownika.

W wielu przypadkach warto zebrać wszystkie lub część plików, które tworzą stronę internetową. Jedną z opcji jest kliknięcie prawym przyciskiem myszy dowolnej strony internetowej i wybranie Wyświetl źródło z menu kontekstowego. To polecenie otworzy nowe okno z kodem źródłowym strony. Następnie można zapisać plik tekstowy jako dokument na komputerze lokalnym. To podejście działa,

ale nie jest to praktyczny sposób kopiowania wszystkich plików dla docelowej witryny. Łatwy w użyciu program o nazwie BlackWidow może znacznie ułatwić proces kopiowania plików stron internetowych. Ćwiczenie 8.2 pokazuje, jak używać programu BlackWidow do kopiowania całej witryny lub jej części.

Ćwiczenie 8. 2

Używanie BlackWidow do kopiowania witryny

1. Pobierz i zainstaluj aplikację BlackWidow ze strony www.softbytelabs.com.

2. Otwórz program BlackWidow.

3. Wprowadź docelowy adres witryny na pasku adresu BlackWidow

4. Kliknij przycisk Skanuj na pasku narzędzi BlackWidow.

5. Kliknij kartę Struktura.

Atakowanie serwera internetowego

Serwery WWW zazwyczaj nasłuchują na porcie TCP 80 (HTTP) i porcie TCP 443 (HTTPS). Ponieważ te porty muszą być otwarte i dostępne dla klientów WWW, wszelkie zapory ogniowe lub urządzenia filtrujące pakiety między klientem WWW a serwerem WWW muszą przekazywać ruch przeznaczony dla tych portów. Oprogramowanie aplikacji sieci Web znajduje się na szczycie oprogramowania serwera sieciowego i umożliwia dostęp do dodatkowych portów. Jednym z początkowych etapów zbierania informacji dotyczących serwerów sieciowych jest pozyskiwanie banerów. Pobieranie kart jest próbą zebrania informacji o serwerze sieciowym, takim jak system operacyjny i oprogramowanie serwera WWW oraz wersja. Ćwiczenie 8.3 pokazuje, jak korzystać z pozyskiwania banerów

Ćwiczenie 8 .3

Pozyskiwanie banerów

1. W wierszu polecenia na komputerze z systemem Windows wpisz

telnet <IPaddress> 80

Adres IP jest adresem docelowym serwera WWW. Można również użyć adresu URL zamiast adresu IP.

2. Następnie w oknie telnet wpisz

HEAD / HTTP / 1.0

Następnie naciśnij Enter.

Baner serwera internetowego zostanie zwrócony. Baner będzie wyglądał mniej więcej tak:

Server: Microsoft-IIS/5.0

Date: Fri, 14 Aug 2009 1:14:42 GMT

Content-Length:340

Content-Type: text/html

Wynik przechwytywania banerów zwykle identyfikuje typ i wersję serwera WWW. Te informacje są ważne, ponieważ można zidentyfikować exploity przeciwko temu typowi i wersji serwera WWW. Następnym krokiem po zdobyciu banera będzie zaatakowanie serwera WWW lub zaatakowanie

aplikacji internetowej i uzyskanie dostępu do danych na serwerze. Łagodnym, ale widocznym typem ataku na serwery sieciowe jest zepsucie. Hakerzy niszczy witryny internetowe dla czystej radości i szansy na zwiększenie ich reputacji, zamiast gromadzenia użytecznych danych. Zablokowanie witryny oznacza, że haker wykorzystuje lukę w zabezpieczeniach systemu operacyjnego lub oprogramowania serwera sieciowego, a następnie zmienia pliki witryny, aby pokazać, że witryna została zaatakowana przez hakera. Haker często wyświetla nazwę hakera na stronie głównej witryny. Typowe ataki na witryny, które umożliwiają hakerom stronicowanie witryny, obejmują:

* Przechwytywanie poświadczeń administratora za pomocą ataków man- in-the-middle

* Ujawnienie hasła administratora za pomocą ataku brute-force

* Korzystanie z ataku DNS w celu przekierowania użytkowników do innego serwera WWW

* Naruszenie serwera FTP lub e-mail

* Wykorzystywanie błędów aplikacji sieciowych, które powodują usterkę

* Nieprawidłowe konfigurowanie udziałów sieciowych

* Wykorzystanie słabych uprawnień

* Przekierowywanie klienta po ataku zapory ogniowej lub routera

* Używanie ataków typu SQL injection (jeśli serwer SQL i serwer WWW to ten sam system)

* Korzystanie z włamań telnetu lub Secure Shell (SSH)

* Przeprowadza zatrucia URL, które przekierowuje użytkownika do innego adresu URL

* Korzystanie z rozszerzenia serwera sieciowego lub zdalnej ingerencji w usługę

* Przechwycenie komunikacji między klientem a serwerem i zmiana pliku cookie, aby serwer uwierzył, że istnieje użytkownik z wyższymi uprawnieniami (dotyczy zabezpieczeń plików cookie)

Ćwiczenie 8.4 omawia korzystanie z Metasploit Framework w celu wykorzystania luki w zabezpieczeniach serwera WWW. Ważne jest, aby przed instalacją Metasploit na maszynie lub maszynie wirtualnej zostały całkowicie wyłączone wszystkie programy antywirusowe i zapory ogniowe. W przeciwnym razie oprogramowanie antywirusowe lub zapora sieciowa mogą blokować niektóre składniki Metasploit, powodując ich nieprawidłowe działanie lub otwarcie. Jak wspomnieliśmy w przewodniku konfiguracji laboratorium we Wprowadzeniu do tej książki, nigdy nie należy instalować Metasploit na maszynie produkcyjnej. Do uruchomienia tego oprogramowania można użyć maszyny testowej VM lub laboratorium.

Ćwiczenie 8. 4

Korzystanie z narzędzia Metasploit w celu wyeliminowania luki w zabezpieczeniach serwera WWW

1. Pobierz i zainstaluj Metasploit 3.2 na komputerze z Windows (www.metasploit.com).

2. Wybierz wszystkie domyślne opcje podczas instalacji Metasploit.

3. Wybierz opcję Online Update w folderze Metasploit 3 w menu Programy.

4. Po zakończeniu aktualizacji online otwórz plik GUI Metasploit w folderze Metasploit 3.

5. Rozwiń folder Windows w obszarze Exploits, a następnie rozwiń folder IIS.

6. Kliknij dwukrotnie exploit ms03_007_ntdll_webdav. Kreator Asystenta MSF uruchamia się.

7. Kliknij przycisk Dalej, aby przejść do następnego ekranu kreatora.

8. Wybierz Windows / Exec z listy rozwijanej Ładunek, a następnie kliknij Prześlij dalej.

9. Wpisz adres IP docelowego serwera IIS w polu RHOST. Ten serwer powinna być niezałataną wersją systemu Windows 2000, aby ten konkretny ładunek działał. Jeśli tak nie jest, wybierz inny ładunek, na który serwer jest podatny.

10. Wpisz sol.exe w polu CMD. To jest plik wykonywalny, który będzie uruchamiany na hoście docelowym. sol.exe to gra w pasjansa, która powinna znajdować się we wszystkich systemach operacyjnych Windows. Ładunek jest tym, co zostanie dostarczone do systemu docelowego. W tym przypadku jest to podobne do wpisywania sol.exe w wierszu polecenia serwera IIS. Oczywiście ten plik wykonywalny jest łagodny, ale to ćwiczenie pokazuje, jak niebezpieczny plik wykonywalny, taki jak wirus lub trojan, może być uruchamiany na celu system.

11. Kliknij przycisk Dalej, aby przejść do następnego ekranu kreatora.

12. Kliknij przycisk Zastosuj. Exploit pojawi się w sekcji Jobs, dopóki nie zostanie dostarczony do systemu docelowego.

13. Potwierdź w maszynie Windows IIS VM lub na komputerze IIS, na którym działa program Solitaire. Jeśli program nie działa, sprawdź, czy Pasjans jest zainstalowany na serwerze IIS i spróbuj ponownie użyć exploita Metasploit

Hakowanie internetowego serwera informacyjnego

Windows IIS jest jednym z najpopularniejszych produktów serwerowych. Ze względu na popularność i liczbę serwerów WWW z IIS wiele ataków może zostać uruchomionych na serwerach IIS. Trzy najczęstsze ataki na IIS są następujące:

* Przeniesienie katalogu

* Źródło ujawnienia

* Przepełnienie bufora

Atak typu directory-traversal opiera się na założeniu, że klienci internetowi są ograniczeni do określonych katalogów w systemie plików Windows. Początkowy dostęp do katalogu przez klientów sieciowych jest znany jako katalog główny na serwerze WWW. Ten katalog główny zwykle przechowuje stronę główną zwaną domyślną lub indeksem, a także inne dokumenty HTML dla serwera WWW. Podkatalogi katalogu głównego zawierają inne typy plików; na przykład skrypty mogą zawierać dynamiczne pliki skryptów dla serwera WWW. Serwer internetowy powinien umożliwiać użytkownikom dostęp tylko do tych konkretnych katalogów i podkatalogów root. Jednak atak przemierzający katalog umożliwia dostęp do innych katalogów w systemie plików. Systemy Windows 2000 z IIS są podatne na atak typu directory-traversal, znany również jako exploit Unicode. Luka w zabezpieczeniach usług IIS, która pozwala na przechwytywanie katalogów / Unicode, występuje tylko w niezałatanych systemach Windows 2000 i wpływa na skrypty CGI i rozszerzenia ISAPI (ISAPI), takie jak .asp. Luka istnieje, ponieważ analizator składni IIS nie interpretował poprawnie kodu Unicode, co daje hakerom dostęp do systemu. Zasadniczo Unicode konwertuje znaki dowolnego języka na uniwersalną specyfikację kodu szesnastkowego. Jednak kod Unicode jest interpretowany dwa razy, a analizator składni skanuje wynikowe żądanie tylko raz (po pierwszej interpretacji). Hakerzy mogli więc przekradać się do żądań plików za pośrednictwem IIS. Na przykład użycie% c0% af zamiast ukośnika we

względnej ścieżce wykorzystuje lukę w zabezpieczeniach IIS. W niektórych przypadkach żądanie pozwala hakerowi uzyskać dostęp do plików, których inaczej nie mogliby zobaczyć. Luka w zabezpieczeniach unicode directory traversal pozwala hakerowi dodawać, zmieniać i usuwać pliki oraz przesyłać i uruchamiać kod na serwerze. Możliwość dodawania lub uruchamiania plików w systemie umożliwia hakerowi instalację trojana lub backdoora w systemie. Exploit Unicode IIS to przestarzała luka w zabezpieczeniach, którą przedstawiono w tym tekście jako dowód koncepcji - to znaczy, że luka istnieje i może zostać wykorzystana.

Ataki typu "przepełnienie bufora" nie są unikalne dla serwerów sieci Web i mogą być również uruchamiane przeciwko innym typom systemów. Przepełnienie bufora wiąże się z wysyłaniem większej ilości danych, zwykle w postaci ciągu tekstowego, niż jest w stanie obsłużyć serwer WWW. Podstawowym punktem wejścia dla przepełnienia bufora jest formularz internetowy na serwerze sieciowym. Przepełnienia buforów i środki zaradcze zostaną szczegółowo omówione w następnej części. Ataki ujawnienia źródła występują, gdy można pobrać kod źródłowy aplikacji serwera. Ataki w zakresie ujawniania źródeł mogą prowadzić do tego, że haker będzie identyfikował typ aplikacji, język programowania i inne informacje specyficzne dla aplikacji. Wszystkie te informacje mogą umożliwić potencjalnemu hakerowi zidentyfikowanie luk w zabezpieczeniach i potencjalnych exploitów, które mogą zostać dostarczone na serwer WWW. Ponownie większość czasu haker zbiera informacje o celu, aby zidentyfikować najlepszy punkt wejścia dla exploita.

Łącząc to wszystko za pomocą ataków ujawniania źródeł

Przykładem wykonania ataku na ujawnienie źródła byłoby uruchomienie BlackWidow na serwerze WWW i skopiowanie wszystkich pliki do lokalnego katalogu. Podczas przeglądania źródła pliki z BlackWidow, możesz uzyskać nazwę serwera, adres IP i wersję. Dodatkowe narzędzia do zbierania informacji, takie jak Netcraft, mogą pomóc w odkryciu systemu operacyjnego, typu oprogramowania serwera WWW i wersji. Dodatkowe informacje mogą być gromadzone w odniesieniu do JavaScript (pliki .js) lub Active Server Pages (pliki .asp), które znajdują się na serwerze. W oparciu o aplikacje serwera WWW i luki w zabezpieczeniach, Metasploit może być wykorzystany do dostarczenia ładunku na serwer. W zależności od poziomu łaty i luki, ładunek może być dość łagodny lub wystarczająco poważny, aby spowodować, że haker uzyska dostęp do cennych danych. Najlepszym środkiem zaradczym dla ataku na ujawnianie źródła i innych rodzajów ataków jest poprawienie systemu operacyjnego, serwera internetowego i wszystkich aplikacji serwerowych na najbardziej aktualny poziom oraz utrzymanie aktywnego programu do zarządzania poprawkami. Hacker etyczny musi znać wszystkie techniki gromadzenia informacji, aby zidentyfikować potencjał luki w zabezpieczeniach serwerów sieciowych i aplikacji internetowych. Powód tej wiedzy jest tak ważny dla etycznego hackera, dlatego że mogą bronić się przed tymi samymi atakami i wdrażać środki zapobiegające atakom.

Techniki zarządzania łatkami

Zarządzanie poprawkami odgrywa kluczową rolę w zapobieganiu i ograniczaniu ryzyka ataku na serwery WWW i aplikacje internetowe. Zarządzanie poprawkami to proces aktualizacji odpowiednich poprawek i poprawek wymaganych przez dostawcę systemu. Właściwe zarządzanie poprawkami polega na wybraniu sposobu instalowania i weryfikowania poprawek oraz testowaniu tych poprawek w sieci nieprodukcyjnej przed instalacją. Powinieneś przechowywać dziennik wszystkich poprawek zastosowanych w każdym systemie. Aby zainstalować łatkę łatwiej, możesz użyć zautomatyzowanych systemów zarządzania łatkami dostarczanych przez PatchLink, St. Bernard Software, Microsoft i innych dostawców oprogramowania, aby ocenić swoje systemy i zdecydować, które łaty wdrożyć.

Pierwszy tydzień w pracy jako administrator sieci

Jako świeżo zatrudniony administrator sieci dla małej firmy zatrudniającej 40 pracowników, moim obowiązkiem było przejrzenie konfiguracji i poprawek dla małej sieci z dwoma serwerami. Firma korzystała z IIS 5.0 na serwerze Windows 2000, który od trzech lat obsługiwał korporacyjną stronę internetową. Serwery zostały zainstalowane i skonfigurowane przez firmę konsultingową na trzy lata przed moim dołączeniem do personelu. Zawartość witryny była regularnie aktualizowana przez asystenta marketingowego, ale na serwerze nie wprowadzono żadnych innych aktualizacji. Rozpocząłem aktualizację i zarządzanie poprawkami na serwerze sieciowym. Firma nie posiadała zapory ogniowej chroniącej połączenie z Internetem, a od czasu instalacji system operacyjny Windows Server nie był objęty żadnymi łatami ani poprawkami. Oprogramowanie serwera IIS było również nieaktualne. Wszystko to stanowiło ogromne zagrożenie dla bezpieczeństwa organizacji, a zarządzanie poprawkami było najwyższym priorytetem dla ochrony serwera WWW i aplikacji na nim działających. Po wprowadzeniu poprawek zabezpieczeń i poprawek do systemu operacyjnego, a następnie IIS, odkryłem, że szkodliwe oprogramowanie, takie jak robak Code Red i liczne wirusy, już zaatakowały system. Wprowadzanie poprawek i poprawek oraz aktualizacja definicji wirusów zajęły kilka dni, zanim serwer WWW został zaktualizowany. Na szczęście dla małej firmy udało mi się zaktualizować oprogramowanie systemu operacyjnego i serwera WWW i wdrożyć system zarządzania poprawkami, zanim sieć została uszkodzona lub nastąpiło poważne naruszenie bezpieczeństwa.

Narzędzia hakerskie

Aplikacja N-Stalker Web Application Security Scanner pozwala ocenić aplikację internetową pod kątem wielu luk, w tym skryptów krzyżowych, iniekcji SQL, przepełnienia bufora i ataków polegających na modyfikowaniu parametrów.

Metasploit Framework jest darmowym narzędziem służącym do testowania lub hakowania systemów operacyjnych lub oprogramowania serwera sieciowego. Exploity mogą być używane jako wtyczki, a testy mogą być wykonywane z platformy Windows lub Unix. Metasploit był pierwotnie narzędziem wiersza poleceń, ale teraz ma interfejs przeglądarki internetowej. Korzystając z Metasploit, hakerzy mogą pisać własne exploity, jak również wykorzystywać standardowe exploity.

CORE IMPACT i SAINT Vulnerability Scanner są komercyjnymi narzędziami wykorzystywanymi do testowania i naruszania systemów operacyjnych i oprogramowania serwera sieciowego.

Metody wzmacniania haseł internetowych

Administrator serwera sieciowego może wiele rzeczy wzmocnić serwer (zwiększyć jego bezpieczeństwo). Oto sposoby na zwiększenie bezpieczeństwa serwera WWW:

* Zmień nazwę konta administratora i użyj silnego hasła. Aby zmienić nazwę konta administratora w systemie Windows, otwórz Menedżera użytkowników, kliknij prawym przyciskiem myszy konto Administrator i wybierz Zmień nazwę.

* Wyłącz domyślne witryny i witryny FTP. Proces wyłączania domyślnych witryn internetowych opisano wcześniej: kliknij prawym przyciskiem myszy domyślną witrynę sieci Web w Menedżerze usług IIS i wybierz Zatrzymaj. Ten sam proces działa dla domyślnej witryny FTP.

* Usuń nieużywane aplikacje z serwera, takie jak WebDAV. Niepotrzebne aplikacje można usunąć na serwerze za pomocą apletu Dodaj / Usuń programy w Panelu sterowania systemu Windows.

* Wyłącz przeglądanie katalogu w ustawieniach konfiguracyjnych serwera WWW.

* Dodaj uwagę prawną do witryny, aby poinformować potencjalnych napastników o skutkach włamań do witryny.

* Zastosuj najnowsze poprawki, poprawki i dodatki Service Pack do systemu operacyjnego i oprogramowania serwera WWW.

* Przeprowadź sprawdzanie wartości wejściowych dla formularzy internetowych i ciągów zapytań, aby zapobiec przepełnieniu bufora lub atakom z użyciem złośliwych danych wejściowych.

* Wyłącz zdalną administrację.

* Użyj skryptu do odwzorowania nieużywanych rozszerzeń plików na komunikat o błędzie 404 ("Nie znaleziono pliku").

* Włącz audyt i logowanie.

* Użyj zapory sieciowej między serwerem WWW i Internetem, a portem zezwól tylko na porty (takie jak 80 i 443) przez zaporę.

* Zastąp metodę GET metodą POST podczas wysyłania danych do serwera WWW.

Luki w zabezpieczeniach aplikacji sieci Web

Oprócz zrozumienia, w jaki sposób haker może wykorzystać serwer sieciowy, ważne jest, aby etyczny hacker znał luki w aplikacjach internetowych. W tej sekcji omówimy działanie aplikacji internetowych oraz cele hakowania aplikacji internetowych. Zbadamy także anatomię ataku aplikacji WWW i niektóre rzeczywiste zagrożenia aplikacji internetowych. Na koniec przyjrzymy się hakowaniu w Google i środkom zaradczym, które powinniście znać. Aplikacje internetowe to programy, które znajdują się na serwerze internetowym, aby zapewnić funkcjonalność użytkownika wykraczającą poza samą stronę internetową. Zapytania baz danych, poczta internetowa, grupy dyskusyjne i blogi to przykłady aplikacji internetowych. Aplikacja internetowa wykorzystuje architekturę klient / serwer, z przeglądarką internetową jako klientem i serwerem WWW działającym jako serwer aplikacji. JavaScript jest popularnym sposobem implementacji aplikacji internetowych. Ponieważ aplikacje internetowe są szeroko wdrażane, każdy użytkownik z przeglądarką może wchodzić w interakcje z większością narzędzi do witryn. Celem włamania się do aplikacji sieciowej jest uzyskanie poufnych danych. Aplikacje internetowe mają krytyczne znaczenie dla bezpieczeństwa systemu, ponieważ zazwyczaj łączą się z bazą danych zawierającą informacje, takie jak tożsamości z numerami kart kredytowych i hasłami. Luki w aplikacjach internetowych zwiększają zagrożenie, jakie hakerzy będą wykorzystywać w systemie operacyjnym oraz na serwerze WWW lub w aplikacjach internetowych. Aplikacje internetowe są zasadniczo kolejnymi drzwiami do systemu i mogą zostać wykorzystane do naruszenia systemu. Hakowanie aplikacji internetowych jest podobne do hakowania innych systemów. Hakerzy wykonują pięciostopniowy proces: skanują sieć, zbierają informacje, testują różne scenariusze ataków, a na koniec planują i rozpoczynają atak. Kroki są wymienione poniżej:

Skanowanie → Zbieranie informacji → Testowanie → Planowanie ataku → Uruchomienie ataku

Zagrożenia w sieci Web i środki zaradcze

Wiele zagrożeń aplikacji internetowych istnieje na serwerze WWW. Oto najczęściej występujące zagrożenia i ich środki zaradcze:

Cross – site scripting: Parametr wprowadzony do formularza internetowego jest przetwarzany przez aplikację internetową. Poprawna kombinacja zmiennych może spowodować dowolne wykonanie polecenia. Przeciwdziałanie: sprawdź poprawność plików cookie, ciągów zapytań, pól formularzy i ukrytych pól.

Przeciwdziałaniem skryptom krzyżowym jest zamiana znaków lewego i prawego nawiasu kwadratowego (<i>) za pomocą & lt; i & gt; za pomocą skryptów serwera. Przeciwdziałanie atakom SSL polega na zainstalowaniu serwera proxy i zakończeniu SSL na serwerze proxy lub zainstalowaniu sprzętowego akceleratora SSL i zakończeniu SSL na tej warstwie.

Injection SQL Wstawianie poleceń SQL do adresu URL powoduje, że serwer bazy danych zrzuca, zmienia, usuwa lub tworzy informacje w bazie danych. Środki zaradcze : Sprawdź poprawność zmiennych użytkownika.

Wstrzykiwanie poleceń Haker wstawia polecenia programowania do formularza internetowego. Przeciwdziałanie: Używaj bibliotek specyficznych dla języka dla języka programowania.

Zatruwanie ciastek i szpiegowanie Haker uszkadza lub kradnie pliki cookie. Środki zaradcze: nie przechowuj haseł w ciasteczku; wdrażać limity czasu plików cookie; i uwierzytelniać pliki cookie.

Przepełnienie bufora Ogromne ilości danych są wysyłane do aplikacji internetowej za pośrednictwem formularza internetowego w celu wykonywania poleceń. Środki zaradcze: Sprawdź poprawność długości wejściowej użytkownika; przeprowadzić sprawdzanie granic.

Uwierzytelnianie podczas uwierzytelniania Haker przechwytuje sesję po uwierzytelnieniu użytkownika. Środek zaradczy: Użyj protokołu SSL do szyfrowania ruchu.

D**irectory Traversal / Unicode** Haker przegląda foldery w systemie za pomocą przeglądarki internetowej lub Eksploratora Windows. Środki zaradcze: Zdefiniuj prawa dostępu do prywatnych folderów na serwerze WWW; zastosuj poprawki i poprawki.

Narzędzia hakerskie

Instant Source pozwala hakerowi na przeglądanie i edycję kodu źródłowego HTML. Można go używać bezpośrednio z poziomu przeglądarki internetowej.

Wget to narzędzie wiersza poleceń, którego haker może użyć do pobrania całej witryny, uzupełnij wszystkie pliki. Haker może wyświetlać kod źródłowy w trybie offline i testować określone ataki przed uruchomieniem ich na prawdziwym serwerze WWW.

WebSleuth używa technologii spidering do indeksowania całej witryny. Na przykład WebSleuth może pobrać wszystkie adresy e-mail z różnych stron witryny.

BlackWidow może skanować i mapować wszystkie strony witryny, aby utworzyć profil witryny.

SiteScope mapuje połączenia w aplikacji internetowej i pomaga w dekonstrukcji programu.

WSDigger to narzędzie do testowania usług internetowych zawierające przykładowe wtyczki ataków wstrzyknięcia SQL, cross-site scripting i inne ataki internetowe.

Burp to oparte na systemie Windows narzędzie do automatycznego ataku na aplikacje internetowe. Może być również używany do odgadywania haseł w aplikacjach internetowych i wykonywania ataków typu "man-in-the-middle".

Google Hacking

Google hacking odnosi się do korzystania z zaawansowanej wyszukiwarki Google w celu lokalizowania wartościowych celów lub wyszukiwania cennych informacji, takich jak hasła. Wiele narzędzi, takich jak http://johnny.ihackstuff.com i Acunetix Web Vulnerability Scanner, zawiera listę hackerów Google zorganizowanych w bazie danych, aby ułatwić wyszukiwanie. Na przykład możesz wprowadzić hasło

hasło lub dokumentację medyczną w wyszukiwarce Google i sprawdzić, jakie informacje są dostępne. Wiele razy Google może pobierać informacje bezpośrednio z prywatnych baz danych lub dokumentów.

Ćwiczenie 8 .5

Używanie Acunetix Web Vulnerability Scanner

1. Pobierz i zainstaluj Acunetix Web Vulnerability Scanner ze strony www.acunetix.com.

2. Otwórz skaner internetowy i wybierz Plik ✐ Nowe skanowanie, aby otworzyć Kreatora skanowania:

3. Postępuj zgodnie z instrukcjami kreatora; zaakceptuj domyślne wartości początkowego skanowania.

4. Wyświetl raport skanowania po zakończeniu skanowania. Zwróć uwagę na słabe punkty serwera i aplikacji w raporcie skanowania.

5. Utwórz kolejne skanowanie za pomocą kreatora i wybierz docelowy serwer laboratoryjny lub serwer WWW VM. Zobacz i przeanalizuj raport skanowania dla twojego serwera laboratoryjnego.

Internetowe techniki łamania haseł

Jako etyczny musisz znać techniki wykorzystywane przez hakerów do łamania haseł internetowych. Obejmuje to możliwość wyświetlania różnych typów uwierzytelniania, wiedzy o tym, czym jest narzędzie do łamania haseł, identyfikowania klasyfikacji technik łamania haseł i znajomości dostępnych środków zaradczych. Przyjrzymy się każdemu w następnych sekcjach.

Typy uwierzytelniania

Serwery WWW i aplikacje internetowe obsługują wiele typów uwierzytelniania. Najczęstszym jest uwierzytelnianie HTTP. Istnieją dwa rodzaje uwierzytelniania HTTP: podstawowy i skrócony. Podstawowe uwierzytelnianie HTTP wysyła nazwę użytkownika i hasło w postaci zwykłego tekstu, podczas gdy uwierzytelnianie skrótu powoduje skasowanie poświadczeń i wykorzystuje do uwierzytelniania model wyzwanie-odpowiedź. Ponadto serwery WWW i aplikacje internetowe obsługują następujące rodzaje uwierzytelniania:

Uwierzytelnianie NTLM Ten typ wykorzystuje Internet Explorer i serwery IIS. NTLM bardziej nadaje się do wewnętrznego uwierzytelniania w intranecie korzystającym z systemów operacyjnych Microsoft. Serwery Windows 2000 i 2003 wykorzystują uwierzytelnianie Kerberos dla bezpieczniejszej opcji.

Uwierzytelnianie oparte na certyfikatach Ten typ używa certyfikatu x.509 dla technologii kluczy publicznych / prywatnych.

Uwierzytelnienie oparte na tokenach Token, taki jak SecurID, to urządzenie sprzętowe wyświetlające kod uwierzytelniający przez 60 sekund; użytkownik używa tego kodu do logowania się do sieci.

Uwierzytelnianie biometryczne Ten typ wykorzystuje charakterystykę fizyczną, taką jak odcisk palca, tęczówka oka lub odcisk dłoni do uwierzytelnienia użytkownika.

Ataki hasłowe i łamanie haseł

Trzy typy ataków hasłowych są następujące:

Słownik Używa haseł, które można znaleźć w słowniku

Brute-Force Zgaduje złożone hasła, które używają liter, cyfr i znaków specjalnych

Hybrydowy Wykorzystuje słowa słownika o numerze lub znaku specjalnym jako zamiennika litery

Password cracker to program przeznaczony do odszyfrowywania haseł lub wyłączania hasła

ochrona. Password cracker polegają na wyszukiwaniu słownikowych (atakach) lub metodach brute – force w celu złamania haseł.

Pierwszym krokiem ataku słownikowego jest wygenerowanie listy potencjalnych haseł, które można znaleźć w słowniku. Haker zazwyczaj tworzy tę listę za pomocą programu generującego słownik lub słowników, które można pobrać z Internetu. Następnie lista słów słownikowych jest zaszyfrowana lub zaszyfrowana. Ta lista skrótów jest porównywana z hashowanym hasłem, które haker próbuje złamać. Haker może uzyskać zakodowane hasło, wykrywając go z sieci przewodowej lub bezprzewodowej lub bezpośrednio z pliku Security Accounts Manager (SAM) lub plików haseł shadow na dysku twardym systemu. Na koniec program wyświetli niezaszyfrowaną wersję hasła. Crackery haseł słownikowych mogą wykrywać tylko hasła będące słowami słownikowymi. Jeśli użytkownik zaimplementował silne hasło, można zaimplementować brutalne wymuszenie łamania haseł. Brutalne łamacze haseł wypróbowują każdą możliwą kombinację liter, cyfr i znaków specjalnych, co zajmuje dużo więcej czasu niż atak słownikowy ze względu na liczbę permutacji. Ćwicz 8.6 przeprowadzi cię przez narzędzie do łamania haseł o nazwie Brutus.

Ćwiczenie 8 .6

Korzystanie z Password Cracker

1. Pobierz i zainstaluj Brutus ze strony www.hoobie.net.

2. Otwórz Brutusa i wpisz adres serwera WWW w polu docelowym.

3. Kliknij przycisk Start i wyświetl hasła w polu wyników pozytywnego uwierzytelnienia u dołu ekranu.

Narzędzie hakerskie

Webcracker to narzędzie, które używa listy słów, aby spróbować zalogować się do serwera WWW. Szuka dla odpowiedzi "przeniesiony obiekt HTTP 302", aby zgadnąć hasło. Z tej odpowiedzi narzędzie może określić używany typ uwierzytelniania i spróbować zalogować się do systemu.

Najlepszym sposobem na łamanie haseł jest zaimplementowanie silnych haseł o długości co najmniej ośmiu znaków (stary standard to sześć), które zawierają znaki alfanumeryczne. Nazwy użytkowników i hasła powinny być różne, ponieważ wiele nazw użytkowników jest przesyłanych w postaci zwykłego tekstu. Złożone hasła wymagające wielkich liter, małych liter i cyfr lub znaków specjalnych są trudniejsze do złamania. Powinieneś również wdrożyć silny mechanizm uwierzytelniania, taki jak Kerberos lub tokeny, aby chronić hasła podczas przesyłania.

Podsumowanie

Serwery internetowe i ataki aplikacji internetowych są zawsze przedmiotem największej troski przy rosnącym wykorzystaniu Internetu. Serwery internetowe i Internet są wykorzystywane przez klientów do wyszukiwania firm, dokonywania zakupów online, uzyskiwania dostępu do baz danych w bankach i firmach inwestycyjnych oraz przeprowadzania wielu innych przeszukiwań bazy danych. Wraz ze wzrostem tego zastosowania potencjalna informacja docelowa staje się coraz bardziej wartościowa. Numery kart kredytowych, dane osobowe i numery ubezpieczenia społecznego są złotym celem hakerów, a wszystkie te informacje są przechowywane w bazach danych aplikacji internetowych. Serwer WWW i hakowanie aplikacji internetowych to metody wykorzystywane przez hakerów do próby naruszenia zabezpieczeń serwera WWW i dostarczania exploitów, które przyniosą cenne

informacje. Hacker etyczny musi być dobrze zorientowany w identyfikowaniu potencjalnych luk w zabezpieczeniach i środkach zaradczych, aby zapobiegać atakom na serwer sieciowy.

Do Zapamiętania!

* Poznałeś typy luk w zabezpieczeniach serwerów WWW. Błędna konfiguracja, system operacyjny lub błędy aplikacji i błędy, domyślna instalacja systemu operacyjnego i oprogramowania serwera WWW, brak zarządzania poprawkami oraz brak odpowiednich zasad i procedur bezpieczeństwa to luki w zabezpieczeniach serwerów WWW.

* Poznałeś powszechne zagrożenia aplikacji internetowych. Cross-site scripting, SQL i iniekcja poleceń, zatruwanie plików cookie i snooping, przepełnienie bufora, przechwytywanie uwierzytelniania i przechodzenie do katalogu są powszechnymi zagrożeniami dla aplikacji internetowych.

* Poznałeś hakowanie przez Google. Google hacking obejmuje korzystanie z wyszukiwarki Google w celu zlokalizowania haseł, numerów kart kredytowych, dokumentacji medycznej lub innych poufnych informacji.

* Zapoznałeś się z technikami zarządzania poprawkami. Zarządzanie poprawkami jest ważne dla zapewnienia, że system jest na bieżąco z najnowszymi poprawkami bezpieczeństwa. Należy zdefiniować i zastosować proces testowania, stosowania i rejestrowania poprawek w systemie.

* Poznałeś różne mechanizmy uwierzytelniania dla serwerów internetowych. HTTP basic i skrót uwierzytelnianie, NTLM, tokeny, dane biometryczne i certyfikaty to wszystkie metody uwierzytelniania na serwerze sieciowym.

* Dowiedziałeś się, jak działają crackery haseł. Crakery haseł używają zaszyfrowanego pliku słownika do złamania hasła.

* Poznałeś typy ataków haseł. Słownik, hybryda i brute-force są tymi trzema rodzaje ataków haseł.