Hakowanie serwerów WWW

Cele kształcenia

Większość organizacji uważa swoją obecność w sieci za przedłużenie ich samych. Organizacje utrzymują strony internetowe związane z ich działalnością w sieci World Wide Web, aby zapewnić sobie obecność w sieci. Serwery sieciowe są kluczowym elementem infrastruktury sieciowej. Pojedyncza luka w konfiguracji serwera WWW może doprowadzić do naruszenia bezpieczeństwa na stronach internetowych. Dlatego bezpieczeństwo serwera WWW ma kluczowe znaczenie dla normalnego funkcjonowania organizacji.

Koncepcje serwera WWW

Aby zrozumieć hakowanie serwera WWW, niezbędne jest zrozumienie koncepcji serwera WWW, w tym tego, czym jest serwer WWW, jak działa i innych powiązanych z nim elementów. Ta sekcja zawiera krótkie omówienie serwera WWW i jego architektury. Wyjaśni również typowe czynniki lub błędy, które umożliwiają atakującym zhakowanie serwera WWW. W tej sekcji opisano również wpływ ataków na serwery WWW.

Operacje serwera WWW

Serwer WWW to system komputerowy, który przechowuje, przetwarza i dostarcza strony internetowe klientom globalnym za pośrednictwem protokołu HTTP (Hypertext Transfer Protocol). Ogólnie rzecz biorąc, klient inicjuje proces komunikacji za pośrednictwem żądań HTTP. Gdy klient chce uzyskać dostęp do dowolnego zasobu, takiego jak strony internetowe, zdjęcia i filmy, przeglądarka klienta generuje żądanie HTTP, które jest wysyłane do serwera WWW. W zależności od żądania serwer www pobiera żądane informacje/treści z serwerów przechowywania danych lub aplikacji i odpowiada na żądanie klienta odpowiednią odpowiedzią HTTP. Jeśli serwer WWW nie może znaleźć żądanych informacji, generuje komunikat o błędzie.

Komponenty serwera WWW

Serwer WWW składa się z następujących elementów:

Główny dokument

Katalog główny dokumentów to jeden z głównych katalogów plików serwera WWW, w którym przechowywane są krytyczne pliki HTML związane ze stronami internetowymi o nazwie domeny, które będą wysyłane w odpowiedzi na żądania. Na przykład, jeśli żądany adres URL to www.certifiedhacker.com, a katalog główny dokumentu nosi nazwę „certroot” i jest przechowywany w katalogu /admin/web, to /admin/web/certroot jest adresem katalogu dokumentu.

Jeśli pełne żądanie to www.certifiedhacker.com/P-folio/index.html, serwer wyszuka ścieżkę do pliku /admin/web/certroot/P-folio/index.html.

Root serwera

Jest to katalog główny najwyższego poziomu w drzewie katalogów, w którym przechowywana jest konfiguracja i błędy serwera, pliki wykonywalne i pliki dziennika. Składa się z kodu implementującego serwer. Katalog główny serwera składa się ogólnie z czterech plików. Jeden plik poświęcony jest kodowi implementującemu serwer, natomiast pozostałe trzy to podkatalogi, a mianowicie -conf, -logs i -cgi-bin, które służą do konfiguracji informacji, dzienników i plików wykonywalnych.

Wirtualne drzewo dokumentów

Wirtualne drzewo dokumentów zapewnia przechowywanie na innej maszynie lub dysku po zapełnieniu oryginalnego dysku. Rozróżnia wielkość liter i może służyć do zapewnienia bezpieczeństwa na poziomie obiektu. W powyższym przykładzie w katalogu głównym dokumentu, dla żądania www.certifiedhacker.com/P-folio/index.html, serwer może również wyszukać ścieżkę pliku /admin/web/certroot/P-foiio/index.htmi, jeśli katalog admin/web/certroot jest przechowywany na innym dysku.

Wirtualny Hosting

Jest to technika hostowania wielu domen lub stron internetowych na tym samym serwerze. Ta technika umożliwia współdzielenie zasobów między różnymi serwerami. Jest stosowany w dużych firmach, w których zasoby firmy mają być dostępne i zarządzane globalnie.

Oto rodzaje hostingu wirtualnego:

o Hosting oparty na nazwie

o Hosting oparty na protokole internetowym (IP).

o Hosting oparty na portach

Proxy

Serwer proxy znajduje się między klientem WWW a serwerem WWW. Dzięki umieszczeniu serwerów proxy wszystkie żądania od klientów są przekazywane do serwera WWW za pośrednictwem serwerów proxy. Służą one do zapobiegania blokowaniu adresów IP i zachowania anonimowości.

Architektura serwera WWW typu open source

Architektura serwera WWW typu open source zwykle wykorzystuje Linux, Apache, MySQL i PHP, często nazywane pakietem oprogramowania LAMP, jako główne komponenty. Poniżej przedstawiono funkcje głównych komponentów w architekturze serwera WWW typu open source:

Linux jest systemem operacyjnym (OS) serwera WWW i zapewnia bezpieczną platformę

Apache to komponent serwera WWW, który obsługuje każde żądanie i odpowiedź HTTP

MySQL to relacyjna baza danych używana do przechowywania zawartości i informacji konfiguracyjnych serwera WWW

PHP to technologia warstwy aplikacji używana do generowania dynamicznych treści internetowych

Architektura serwera WWW usług IIS

Internet Information Service (IIS) to aplikacja serwera WWW opracowana przez firmę Microsoft dla systemu Windows. Usługi IIS dla systemu Windows Server to elastyczny, bezpieczny i łatwy w zarządzaniu serwer WWW do hostowania dowolnych treści w sieci. Obsługuje HTTP, HTTP Secure (HTTPS), File Transfer Protocol (FTP), FTP Secure (FTPS), Simple Mail Transfer Protocol (SMTP) i Network News Transfer Protocol (NNTP). Ma kilka składników, w tym odbiornik protokołów, taki jak HTTP.sys, oraz usługi, takie jak World Wide Web Publishing Service (usługa WWW) i usługa aktywacji procesów systemu Windows (WAS). Każdy składnik działa w rolach aplikacji i serwera WWW. Funkcje te mogą obejmować słuchanie żądań, zarządzanie procesami i odczytywanie plików konfiguracyjnych.

Problemy z bezpieczeństwem serwera WWW

Serwer WWW to aplikacja sprzętowa/programowa, która hostuje strony internetowe i udostępnia je przez Internet. Serwer WWW wraz z przeglądarką z powodzeniem realizuje architekturę modelu klient-serwer. W tym modelu serwer WWW pełni rolę serwera, a przeglądarka klienta. Aby hostować strony internetowe, serwer sieciowy przechowuje strony internetowe witryn internetowych i dostarcza określoną stronę internetową na żądanie. Każdy serwer WWW ma nazwę domeny i adres IP powiązany z tą nazwą domeny. Serwer WWW może obsługiwać więcej niż jedną witrynę internetową. Dowolny komputer może pełnić rolę serwera WWW, jeśli ma zainstalowane określone oprogramowanie serwera (program serwera WWW) i jest podłączony do Internetu. Serwery internetowe są wybierane na podstawie ich zdolności do obsługi programowania po stronie serwera, charakterystyki bezpieczeństwa, publikowania, wyszukiwarek i narzędzi do tworzenia witryn. Apache, Microsoft IIS, Nginx, Google i Tomcat to jedne z najczęściej używanych programów serwera WWW. Osoba atakująca zazwyczaj wykorzystuje luki w komponencie oprogramowania i błędy konfiguracji, aby przejąć kontrolę nad serwerami sieciowymi. Organizacje mogą bronić się przed większością ataków na poziomie sieci i systemu operacyjnego, stosując środki bezpieczeństwa sieci, takie jak zapory ogniowe, systemy wykrywania włamań (IDS) i systemy zapobiegania włamaniom (IPS), a także przestrzegając standardów i wytycznych bezpieczeństwa. Zmusza to atakujących do zwrócenia uwagi na ataki na poziomie serwera WWW i aplikacji internetowej, ponieważ serwer WWW, na którym znajdują się aplikacje internetowe, jest dostępny z dowolnego miejsca przez Internet. To sprawia, że serwery sieciowe są atrakcyjnym celem. Źle skonfigurowane serwery sieciowe mogą stwarzać luki nawet w najbardziej starannie zaprojektowanych zaporach sieciowych. Atakujący mogą wykorzystać źle skonfigurowane serwery internetowe ze znanymi lukami w zabezpieczeniach, aby zagrozić bezpieczeństwu aplikacji internetowych. Ponadto serwery internetowe ze znanymi lukami w zabezpieczeniach mogą zaszkodzić bezpieczeństwu organizacji. Jak pokazano na poniższym rysunku, bezpieczeństwo organizacji obejmuje siedem poziomów od stosu 1 do stosu 7.

Typowe cele hakowania serwerów WWW

Atakujący przeprowadzają ataki na serwery sieciowe, mając na uwadze określone cele. Cele te mogą być techniczne lub nietechniczne. Na przykład osoby atakujące mogą naruszyć zabezpieczenia serwera WWW i wykraść poufne informacje w celu uzyskania korzyści finansowych lub po prostu z ciekawości. Oto niektóre typowe cele ataków na serwer WWW:

Kradzież danych karty kredytowej lub innych poufnych danych uwierzytelniających przy użyciu technik phishingu

Integracja serwera z botnetem w celu przeprowadzenia ataku typu „odmowa usługi” (DoS) lub rozproszonego ataku DoS (DDoS)

Włamanie do bazy danych

Uzyskiwanie aplikacji o zamkniętym kodzie źródłowym

Ukrywanie i przekierowywanie ruchu

Eskalacja uprawnień

Niektóre ataki są przeprowadzane z powodów osobistych, a nie dla korzyści finansowych:

Z czystej ciekawości

Za ukończenie samodzielnie postawionego wyzwania intelektualnego

Za zniszczenie reputacji docelowej organizacji

Niebezpieczne luki w zabezpieczeniach wpływające na bezpieczeństwo serwera WWW

Serwer WWW skonfigurowany przez słabo przeszkolonych administratorów systemu może mieć luki w zabezpieczeniach. Niedostateczna wiedza, zaniedbania, lenistwo i nieuwaga w kwestii bezpieczeństwa mogą stanowić największe zagrożenie dla bezpieczeństwa serwera WWW. Poniżej przedstawiono niektóre typowe niedopatrzenia, które sprawiają, że serwer WWW jest podatny na ataki:

Brak aktualizacji serwera WWW przy użyciu najnowszych poprawek

Używanie wszędzie tych samych poświadczeń administratora systemu

Umożliwienie nieograniczonego ruchu wewnętrznego i wychodzącego

Uruchamianie niezabezpieczonych aplikacji i serwerów

Wpływ ataków na serwer WWW

Atakujący na serwer sieciowy mogą spowodować różnego rodzaju szkody w organizacji. Poniżej przedstawiono niektóre rodzaje szkód, jakie osoby atakujące mogą wyrządzić serwerowi WWW.

Włamanie na konta użytkowników: Ataki na serwery internetowe koncentrują się głównie na włamaniu do kont użytkowników. Jeśli atakujący włamie się na konto użytkownika, może uzyskać dużą ilość przydatnych informacji. Osoba atakująca może wykorzystać przejęte konto użytkownika do przeprowadzania dalszych ataków na serwer sieciowy.

Zniekształcenie strony internetowej: Atakujący mogą całkowicie zmienić wygląd strony internetowej, zastępując jej oryginalne dane. Niszczą docelową witrynę, zmieniając elementy wizualne i wyświetlając różne strony z własnymi wiadomościami.

Wtórne ataki ze strony internetowej: osoba atakująca, która włamuje się na serwer sieciowy, może użyć tego serwera do przeprowadzania dalszych ataków na różne witryny internetowe lub systemy klienckie.

Dostęp root do innych aplikacji lub serwera: Dostęp root to najwyższy poziom uprawnień do logowania się na serwerze, niezależnie od tego, czy serwer jest serwerem dedykowanym, częściowo dedykowanym czy wirtualnym serwerem prywatnym. Atakujący mogą wykonać dowolne działanie, gdy uzyskają uprawnienia administratora do serwera.

Manipulowanie danymi: osoba atakująca może zmienić lub usunąć dane z serwera WWW, a nawet zastąpić je złośliwym oprogramowaniem, aby narazić użytkowników łączących się z serwerem WWW.

Kradzież danych: Dane należą do podstawowych aktywów organizacji. Atakujący mogą uzyskać dostęp do poufnych danych, takich jak dane finansowe, plany na przyszłość lub kod źródłowy programu.

Uszkodzenie reputacji firmy: Ataki na serwer sieciowy mogą ujawnić dane osobowe klientów firmy, szkodząc reputacji firmy. W rezultacie klienci tracą zaufanie do firmy i boją się udostępnić firmie swoje dane osobowe.

Dlaczego serwery WWW są zagrożone?

Istnieją nieodłączne zagrożenia bezpieczeństwa związane z serwerami internetowymi, sieciami lokalnymi (LAN), w których znajdują się witryny internetowe, oraz użytkownikami końcowymi, którzy uzyskują dostęp do tych witryn za pomocą przeglądarek.

Perspektywa webmastera: Z perspektywy webmastera największym problemem związanym z bezpieczeństwem jest to, że serwer WWW może narazić sieć LAN lub korporacyjny intranet na

zagrożenia stwarzane przez Internet. Zagrożenia te mogą mieć postać wirusów, trojanów, atakujących lub naruszenia bezpieczeństwa danych. Błędy w oprogramowaniu są często źródłem luk w zabezpieczeniach. Serwery internetowe, które są dużymi i złożonymi urządzeniami, również wiążą się z tymi nieodłącznymi zagrożeniami. Ponadto otwarta architektura serwerów WWW umożliwia uruchamianie dowolnych skryptów po stronie serwera podczas odpowiadania na żądania zdalne. Każdy skrypt Common Gateway Interface (CGI) zainstalowany na serwerze WWW może zawierać błędy, które stanowią potencjalne luki w zabezpieczeniach.

Perspektywa administratora sieci: Z perspektywy administratora sieci źle skonfigurowany serwer WWW powoduje potencjalne luki w zabezpieczeniach sieci LAN. Chociaż celem serwera WWW jest zapewnienie kontrolowanego dostępu do sieci, nadmierna kontrola może prawie uniemożliwić korzystanie z sieci. W środowisku intranetowym administrator sieci musi starannie skonfigurować serwer sieciowy, aby uprawnieni użytkownicy byli rozpoznawani i uwierzytelniani, a grupom użytkowników przypisywano odrębne uprawnienia dostępu.

Perspektywa użytkownika końcowego: zwykle użytkownik końcowy nie dostrzega żadnego bezpośredniego zagrożenia, ponieważ surfowanie po sieci wydaje się zarówno bezpieczne, jak i anonimowe. Flowever, aktywna zawartość, taka jak formanty ActiveX i aplety Java, umożliwia szkodliwym aplikacjom, takim jak wirusy, wtargnięcie do systemu użytkownika. Ponadto aktywna zawartość ze strony internetowej, która jest wyświetlana w przeglądarce użytkownika, może zostać wykorzystana jako kanał dla złośliwego oprogramowania w celu ominięcia zapory sieciowej i przedostania się do sieci LAN.

Poniżej przedstawiono niektóre niedopatrzenia, które mogą zagrozić serwerowi sieciowemu:

Niewłaściwe uprawnienia do plików i katalogów

Instalacja serwera z ustawieniami domyślnymi

Włączone niepotrzebne usługi, w tym zarządzanie treścią i zdalna administracja

Konflikt bezpieczeństwa z wymaganiami biznesowymi dotyczącymi łatwości użytkowania

Brak odpowiedniej polityki bezpieczeństwa, procedur i konserwacji

Niewłaściwe uwierzytelnianie z systemami zewnętrznymi

Domyślne konta z domyślnymi hasłami lub bez haseł

Niepotrzebne pliki domyślne, zapasowe lub przykładowe

Błędne konfiguracje serwera WWW, systemu operacyjnego i sieci

Błędy w oprogramowaniu serwera, systemie operacyjnym i aplikacjach internetowych

Błędnie skonfigurowane certyfikaty Secure Sockets Layer (SSL) i ustawienia szyfrowania

Funkcje administracyjne lub debugujące, które są włączone lub dostępne na serwerach WWW

Korzystanie z certyfikatów z podpisem własnym i certyfikatów domyślnych

Nieużywanie dedykowanego serwera do usług sieciowych

Ataki na serwer WWW

Atakujący może użyć wielu technik, aby skompromitować serwer WWW, takich jak DoS/DDoS, przejęcie serwera systemu nazw domen (DNS), wzmocnienie DNS, przechodzenie przez katalogi, man in the middle (MITM)/sniffing, phishing, zniekształcenie strony internetowej, serwer WWW błędna konfiguracja, dzielenie odpowiedzi HTTP, zatruwanie pamięci podręcznej sieci, brutalna siła Secure Shell (SSH) i łamanie haseł serwera WWW. Ta sekcja szczegółowo opisuje te techniki ataku.

Przejęcie serwera DNS

System nazw domen (DNS) tłumaczy nazwę domeny na odpowiadający jej adres IP. Użytkownik wysyła do serwera DNS zapytanie o nazwę domeny, a serwer DNS odpowiada odpowiednim adresem IP. Podczas przejmowania serwera DNS osoba atakująca naraża serwer DNS i zmienia jego ustawienia mapowania, aby przekierowywać do nieuczciwego serwera DNS, który przekierowywałby żądania użytkownika do nieuczciwego serwera atakującego. W rezultacie, gdy użytkownik wprowadzi prawidłowy adres URL w przeglądarce, ustawienia przekierują go na fałszywą stronę atakującego.

Atak wzmacniający DNS

Rekurencyjne zapytanie DNS to metoda żądania mapowania DNS. Zapytanie przechodzi rekurencyjnie przez serwery DNS, dopóki nie znajdzie określonej nazwy domeny do mapowania adresu IP. Poniżej przedstawiono kroki związane z przetwarzaniem rekurencyjnych żądań DNS; kroki te przedstawiono na poniższym rysunku.

• Krok 1:

Użytkownicy, którzy chcą przetłumaczyć nazwę domeny na odpowiadający jej adres IP, wysyłają zapytanie DNS do podstawowego serwera DNS określonego we właściwościach protokołu kontroli transmisji (TCP)/IP.

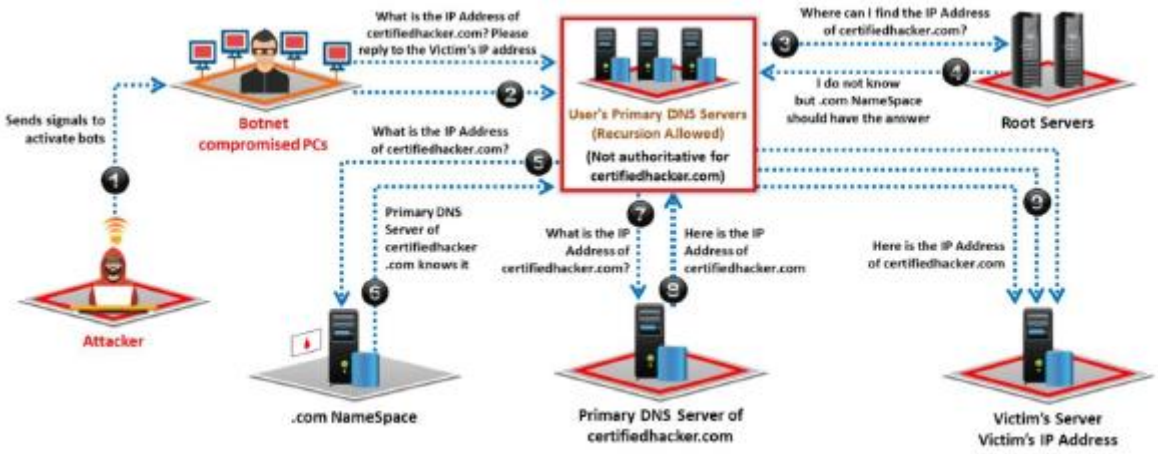
Kroki od 2 do 7:

Jeśli żądane mapowanie DNS nie istnieje na podstawowym serwerze DNS użytkownika, serwer przekazuje żądanie do serwera głównego. Serwer główny przekazuje żądanie do przestrzeni nazw .com, gdzie użytkownik może znaleźć mapowania DNS. Ten proces jest powtarzany rekurencyjnie, dopóki mapowanie DNS nie zostanie rozwiązane.

• Krok 8:

Ostatecznie, gdy system znajdzie podstawowy serwer DNS dla żądanego mapowania DNS, generuje pamięć podręczną dla adresu IP na podstawowym serwerze DNS użytkownika.

Atakujący wykorzystują rekurencyjne zapytania DNS do przeprowadzenia ataku wzmacniającego DNS, który skutkuje atakami DDoS na serwer DNS ofiary. Poniżej przedstawiono kroki związane z atakiem wzmacniającym DNS; kroki te przedstawiono na poniższym rysunku.



Krok 1:

Atakujący instruuje zaatakowane hosty (boty) do wysyłania zapytań DNS w sieci.

Krok 2:

Wszystkie zainfekowane hosty fałszują adres IP ofiary i wysyłają zapytania DNS do podstawowego serwera DNS skonfigurowanego w ustawieniach TCP/IP ofiary.

Kroki od 3 do 8:

Jeśli żądane mapowanie DNS nie istnieje na głównym serwerze DNS ofiary, serwer przekazuje żądania do serwera głównego. Serwer główny przekazuje żądanie do domeny .com lub odpowiedniej przestrzeni nazw domeny najwyższego poziomu (TLD). Ten proces powtarza się rekurencyjnie, dopóki główny serwer DNS ofiary nie rozwiąże żądania mapowania DNS.

Krok 9:

Gdy główny serwer DNS znajdzie mapowanie DNS dla żądania ofiary, wysyła odpowiedź mapowania DNS na adres IP ofiary. Ta odpowiedź trafia do ofiary, ponieważ boty używają adresu IP ofiary. Odpowiedzi na liczne żądania mapowania DNS wysyłane przez boty skutkują atakiem DDoS na serwerze DNS ofiary.

Ataki z przechodzeniem przez katalogi

Atakujący może być w stanie przeprowadzić atak z przechodzeniem przez katalog dzięki luce w kodzie aplikacji internetowej. Ponadto źle załatane lub skonfigurowane oprogramowanie serwera WWW może narazić serwer WWW na atak z przechodzeniem katalogu. Konstrukcja serwerów sieciowych w pewnym stopniu ogranicza publiczny dostęp. Directory traversal to wykorzystanie protokołu HTTP, dzięki któremu osoby atakujące mogą uzyskać dostęp do zastrzeżonych katalogów i wykonywać polecenia poza katalogiem głównym serwera WWW, manipulując adresem URL (Uniform Resource Locator). W atakach z przechodzeniem katalogów osoby atakujące używają sekwencji kropka-kropka-ukośnik (../), aby uzyskać dostęp do zastrzeżonych katalogów poza katalogiem głównym serwera WWW. Atakujący mogą użyć metody trial-anderror, aby przejść poza katalog główny i uzyskać dostęp do poufnych informacji w systemie. Osoba atakująca wykorzystuje oprogramowanie serwera WWW (program serwera WWW) do wykonania ataku na katalogi przejściowe. Osoba atakująca zazwyczaj przeprowadza ten atak za pomocą przeglądarki. Serwer WWW jest narażony na ten atak, jeśli akceptuje dane wejściowe z przeglądarki bez odpowiedniej walidacji.

Zniekształcenie strony internetowej

Zniekształcenie strony internetowej odnosi się do nieautoryzowanych zmian wprowadzonych do treści pojedynczej strony internetowej lub całej witryny internetowej, skutkujących zmianami w wyglądzie strony internetowej lub witryny internetowej. Hakerzy włamują się do serwerów sieciowych i modyfikują hostowaną witrynę, wstrzykując kod w celu dodania obrazów, wyskakujących okienek lub tekstu do strony w taki sposób, że zmienia się wygląd strony. W niektórych przypadkach osoba atakująca może zastąpić całą witrynę zamiast zmieniać tylko jedną stronę.

Zniekształcone strony narażają odwiedzających na propagandę lub wprowadzające w błąd informacje, dopóki nieautoryzowane zmiany nie zostaną wykryte i poprawione. Atakujący używają różnych metod, takich jak wstrzykiwanie MySQL, aby uzyskać dostęp do witryny internetowej w celu jej zniszczenia. Oprócz zmiany wyglądu docelowej witryny osoby atakujące niszczą witryny w celu zainfekowania komputerów odwiedzających, czyniąc witrynę podatną na ataki wirusów. W związku z tym niszczenie strony internetowej nie tylko wprowadza w zakłopotanie organizację docelową poprzez zmianę wyglądu jej strony internetowej, ale ma również na celu wyrządzenie szkody odwiedzającym ją.

Błędna konfiguracja serwera WWW

Błędna konfiguracja serwera WWW odnosi się do słabości konfiguracji infrastruktury sieciowej, które można wykorzystać do przeprowadzania różnych ataków na serwery sieciowe, takich jak przeglądanie katalogów, włamania do serwerów i kradzież danych. Oto niektóre błędne konfiguracje serwera WWW:

Pełne komunikaty debugowania/błędów

Anonimowi lub domyślni użytkownicy/hasła

Przykładowe pliki konfiguracyjne i skryptowe

Funkcje zdalnej administracji

Niepotrzebne usługi włączone

Błędnie skonfigurowane/domyślne certyfikaty SSL

Przykład błędnej konfiguracji serwera WWW

„Zapewnienie bezpieczeństwa konfiguracji serwera wymaga czujności” — Open Web Application Security

Projekt (OWASP)

Administratorzy, którzy niewłaściwie konfigurują serwery WWW, mogą pozostawić w nim poważne luki, dając atakującemu szansę na wykorzystanie źle skonfigurowanego serwera WWW w celu naruszenia jego bezpieczeństwa i uzyskania poufnych informacji. Luki w zabezpieczeniach niewłaściwie skonfigurowanych serwerów WWW mogą być związane z konfiguracją, aplikacjami, plikami, skryptami lub stronami internetowymi. Osoba atakująca szuka takich wrażliwych serwerów sieciowych, aby przeprowadzić atak. Błędna konfiguracja serwera WWW umożliwia atakującemu wejście do docelowej sieci organizacji. Te luki w serwerze mogą również pomóc atakującemu ominąć uwierzytelnianie użytkownika. Po wykryciu problemy te można łatwo wykorzystać i doprowadzić do całkowitego naruszenia bezpieczeństwa witryny internetowej hostowanej na docelowym serwerze internetowym. Jak pokazano na poniższym rysunku, konfiguracja może pozwolić każdemu na przeglądanie strony

stanu serwera, która zawiera szczegółowe informacje o bieżącym wykorzystaniu serwera WWW, w tym informacje o bieżących hostach i przetwarzanych żądaniach.

```
<Location /server-status>
SetHandler server-status
</Location>
```

Jak pokazano na poniższym rysunku, konfiguracja może wyświetlać szczegółowe komunikaty o błędach.

```
display_error = On
log_errors = On
error_log = syslog
ignore_repeated_errors = Off
```

Atak z podziałem odpowiedzi HTTP

Atak z podziałem odpowiedzi HTTP to atak oparty na sieci Web, w którym osoba atakująca oszukuje serwer, wprowadzając nowe wiersze do nagłówków odpowiedzi wraz z dowolnym kodem. Polega na dodaniu danych odpowiedzi nagłówka do pola wejściowego, dzięki czemu serwer podzieli odpowiedź na dwie odpowiedzi. Ten typ ataku wykorzystuje luki w walidacji danych wejściowych. Cross-site scripting (XSS), cross-site request forgery (CSRF) i wstrzyknięcie Structured Query Language (SQL) to przykłady tego typu ataków. W tym ataku atakujący kontroluje parametr wejściowy i sprytnie konstruuje nagłówek żądania, który wywołuje dwie odpowiedzi z serwera. Atakujący zmienia pojedyncze żądanie, aby wyglądało na dwa żądania, dodając dane odpowiedzi nagłówka do pola wejściowego. Z kolei serwer WWW odpowiada na każde żądanie. Osoba atakująca może przekazać złośliwe dane do podatnej na ataki aplikacji, a aplikacja umieszcza te dane w nagłówku odpowiedzi HTTP. Atakujący może kontrolować pierwszą odpowiedź, aby przekierować użytkownika do złośliwej witryny, podczas gdy przeglądarka internetowa odrzuci inne odpowiedzi.

Przykład ataku z podziałem odpowiedzi HTTP

W tym przykładzie atakujący wysyła żądanie podziału odpowiedzi do serwera WWW. Serwer dzieli odpowiedź na dwie części i wysyła pierwszą odpowiedź do atakującego, a drugą do ofiary. Po otrzymaniu odpowiedzi z serwera WWW ofiara żąda usługi, podając dane uwierzytelniające. Jednocześnie atakujący żąda strony indeksu. Następnie serwer WWW wysyła odpowiedź na żądanie ofiary do atakującego, a ofiara pozostaje niedoinformowana.

Atak zatruwający pamięć podręczną sieci Web

Zatruwanie pamięci podręcznej sieci Web obniża niezawodność pośredniego źródła pamięci podręcznej sieci Web. W tym ataku osoba atakująca zamienia zawartość pamięci podręcznej na losowy adres URL z zainfekowaną zawartością. Użytkownicy źródła pamięci podręcznej sieci mogą nieświadomie używać zatrutej zawartości zamiast prawdziwej i zabezpieczonej zawartości, żądając wymaganego adresu URL za pośrednictwem pamięci podręcznej sieci. Osoba atakująca zmusza pamięć podręczną serwera WWW do opróżnienia rzeczywistej zawartości pamięci podręcznej i wysyła specjalnie spreparowane żądanie zapisania w pamięci podręcznej. W takim przypadku wszyscy użytkownicy tej pamięci podręcznej serwera WWW otrzymają złośliwą zawartość, dopóki serwery nie opróżnią pamięci podręcznej serwera WWW. Ataki polegające na zatruwaniu pamięci podręcznej sieci Web są możliwe, jeśli serwer WWW i aplikacja mają wady związane z podziałem odpowiedzi HTTP.

Brutalny atak SSH

Atakujący używają protokołów SSH do tworzenia zaszyfrowanego tunelu SSH między dwoma hostami w celu przesyłania niezaszyfrowanych danych przez niezabezpieczoną sieć. Zwykle SSH działa na porcie TCP 22. Aby przeprowadzić atak na SSH, atakujący skanuje cały serwer SSH za pomocą botów (wykonuje skanowanie portu na porcie TCP 22) w celu zidentyfikowania możliwych luk. Za pomocą ataku brute-force atakujący uzyskuje dane logowania w celu uzyskania nieautoryzowanego dostępu do tunelu SSH. Atakujący, który uzyska dane logowania SSH, może użyć tych samych tuneli SSH do przesyłania złośliwego oprogramowania i innych środków wykorzystania do ofiar bez wykrycia. Atakujący używają narzędzi takich jak Nmap i Ncrack na platformie Linux do przeprowadzenia ataku typu brute-force SSH.

Łamanie haseł do serwerów WWW

Atakujący próbuje wykorzystać słabości do zhakowania dobrze dobranych haseł. Najczęściej spotykane hasła to hasło, root, administrator, admin, demo, test, guest, qwerty, nazwy zwierząt domowych i tak dalej. Atakujący atakuje głównie następujące elementy poprzez łamanie haseł serwera WWW:

Serwery SMTP i FTP

Udziały internetowe

Tunele SSH

Uwierzytelnianie formularza internetowego

Atakujący używają różnych metod, takich jak socjotechnika, fałszowanie, phishing, koń trojański lub wirus, podsłuchiwanie i rejestrowanie naciśnięć klawiszy, aby złamać hasło do serwera WWW. W przypadku wielu prób włamań atakujący zaczyna od złamania hasła, aby udowodnić serwerowi sieciowemu, że jest prawidłowym użytkownikiem.

Techniki łamania haseł do serwerów WWW

Łamanie haseł to najpowszechniejsza metoda uzyskiwania nieautoryzowanego dostępu do serwera WWW poprzez wykorzystywanie wadliwych i słabych mechanizmów uwierzytelniania. Po złamaniu hasła osoba atakująca może użyć hasła do przeprowadzenia dalszych ataków. Przedstawiamy kilka szczegółów na temat różnych narzędzi i technik wykorzystywanych przez atakujących do łamania haseł. Atakujący mogą wykorzystywać techniki łamania haseł w celu wyodrębniania haseł z serwerów WWW, serwerów FTP, serwerów SMTP i tak dalej. Mogą łamać hasła ręcznie lub za pomocą zautomatyzowanych narzędzi, takich jak THC Hydra, Ncrack i RainbowCrack.

Poniżej przedstawiono niektóre techniki wykorzystywane przez atakujących do łamania haseł:

Zgadywanie: Jest to najczęstsza metoda łamania haseł. W tej metodzie atakujący odgaduje możliwe hasła ręcznie lub za pomocą zautomatyzowanych narzędzi wyposażonych w słowniki. Większość ludzi używa imion swoich zwierząt domowych, imion bliskich, numerów rejestracyjnych, dat urodzenia lub innych słabych haseł, takich jak „QWERTY”, „hasło”, „admin” itp., aby móc je łatwo zapamiętać . Atakujący wykorzystuje to ludzkie zachowanie do łamania haseł.

Atak słownikowy: Atak słownikowy wykorzystuje predefiniowany plik zawierający różne kombinacje słów, a zautomatyzowany program wprowadza te słowa pojedynczo, aby sprawdzić, czy któreś z nich jest hasłem. Może to nie być skuteczne, jeśli hasło zawiera znaki specjalne i symbole. Jeśli hasło jest prostym słowem, można je szybko znaleźć. W porównaniu z atakiem brute-force atak słownikowy jest mniej czasochłonny.

Atak brute force: W metodzie brutalnej siły testowane są wszystkie możliwe kombinacje znaków; na przykład test może zawierać kombinacje wielkich liter od A do Z, cyfr od 0 do 9 i małych liter od a do z. Ta metoda jest przydatna do identyfikowania haseł składających się z jednego lub dwóch słów. Jeśli hasło składa się z wielkich i małych liter oraz znaków specjalnych, złamanie hasła za pomocą ataku siłowego może zająć miesiące lub lata.

Atak hybrydowy: Atak hybrydowy jest potężniejszy niż powyższe techniki, ponieważ wykorzystuje zarówno atak słownikowy, jak i atak brute-force, a także wykorzystuje symbole i liczby.

Inne ataki na serwer WWW

Ataki DoS/DDoS

Atak DoS/DDoS polega na zalewaniu celów dużą ilością fałszywych żądań, tak aby cel przestał działać i stał się niedostępny dla legalnych użytkowników. Wykorzystując atak DoS/DDoS na serwer sieciowy, osoba atakująca próbuje wyłączyć serwer sieciowy lub uniemożliwić legalnym użytkownikom. Atak DoS/DDoS na serwer sieciowy często jest skierowany na serwery sieciowe o wysokim profilu, takie jak serwery banków, bramki płatności kartami kredytowymi, a nawet główne serwery nazw. Aby spowodować awarię serwera WWW, na którym działa aplikacja, osoba atakująca atakuje następujące usługi w celu wykorzystania zasobów serwera WWW za pomocą fałszywych żądań:

Przepustowość sieci

Pamięć serwera

Mechanizm obsługi wyjątków aplikacji

Użycie procesora

Miejsce na dysku twardym

Miejsce na bazę danych

Uwaga: pełne omówienie ataków DoS/DDoS można znaleźć w Module 10: Denial-of-Service.

Atak typu Man-in-the-Middle

Ataki typu man-in-the-middle/manipulator-in-the-middle (MITM) umożliwiają atakującemu dostęp do poufnych informacji poprzez przechwytywanie i modyfikowanie komunikacji między użytkownikiem końcowym a serwerami internetowymi. W ataku MITM lub ataku podsłuchowym intruz przechwytuje lub modyfikuje wiadomości wymieniane między użytkownikiem a serwerem WWW, podsłuchując lub włamując się do połączenia. Dzięki temu osoba atakująca może ukraść poufne informacje o użytkowniku, takie jak dane bankowe, nazwy użytkownika i hasła, przesyłane przez Internet na serwer sieciowy. Atakujący podszywając się pod proxy, nakłania ofiarę do połączenia się z serwerem WWW. Jeśli ofiara uwierzy i zaakceptuje żądanie atakującego, wówczas cała komunikacja między użytkownikiem a serwerem WWW przechodzi przez atakującego. W ten sposób atakujący może wykraść poufne informacje o użytkowniku.

Uwaga: pełne omówienie ataków man-in-the-middle (MITM) zawiera Moduł 11: Przejęcie sesji.

Ataki phishingowe

Atakujący przeprowadzają atak phishingowy, wysyłając wiadomość e-mail zawierającą złośliwy link i nakłaniając użytkownika do kliknięcia go. Kliknięcie łącza przekieruje użytkownika do fałszywej strony internetowej, która wygląda podobnie do legalnej strony internetowej. Atakujący tworzą takie strony

internetowe, umieszczając swój adres na serwerach sieciowych. Gdy ofiara kliknie złośliwe łącze, wierząc, że jest to prawidłowy adres witryny, zostaje przekierowana do złośliwej witryny znajdującej się na serwerze atakującego. Witryna prosi użytkownika o wprowadzenie poufnych informacji, takich jak nazwy użytkownika, hasła, dane konta bankowego i numery ubezpieczenia społecznego, i ujawnia dane atakującemu. Później osoba atakująca może być w stanie nawiązać sesję z legalną witryną internetową, używając skradzionych danych uwierzytelniających ofiary, aby wykonać złośliwe operacje na docelowej legalnej witrynie internetowej.

Uwaga: pełne omówienie ataków typu phishing można znaleźć w Module 09: Inżynieria społeczna.

Ataki na aplikacje internetowe

Nawet jeśli serwery internetowe są bezpiecznie skonfigurowane lub są zabezpieczone za pomocą środków bezpieczeństwa sieci, takich jak zapory ogniowe, źle zakodowana aplikacja internetowa wdrożona na serwerze internetowym może zapewnić atakującemu ścieżkę do naruszenia bezpieczeństwa serwera internetowego. Jeśli twórcy stron internetowych nie przyjmą bezpiecznych praktyk kodowania podczas tworzenia aplikacji internetowych, osoby atakujące mogą być w stanie wykorzystać luki w zabezpieczeniach i naruszyć bezpieczeństwo aplikacji internetowych i serwerów internetowych. Atakujący może przeprowadzać różne rodzaje ataków na podatne aplikacje internetowe, aby naruszyć zabezpieczenia serwera WWW.

• Atak Server-Side Request Forgery (SSRF): Atakujący wykorzystują luki w zabezpieczeniach związane z fałszowaniem żądań po stronie serwera (SSRF), które wynikają z niebezpiecznego korzystania z funkcji aplikacji na publicznych serwerach internetowych w celu wysyłania spreparowanych żądań do serwerów wewnętrznych lub zaplecza. Serwer zaplecza uważa, że żądanie jest wysyłane przez serwer WWW, ponieważ znajdują się w tej samej sieci, i odpowiada przechowywanymi w nim danymi.

• Manipulowanie parametrami/formularzami: w tego typu atakach manipulacyjnych osoba atakująca manipuluje parametrami wymienianymi między klientem a serwerem w celu zmodyfikowania danych aplikacji, takich jak dane uwierzytelniające i uprawnienia użytkownika, a także cena i ilość produktów.

• Manipulowanie plikami cookie: Ataki polegające na manipulowaniu plikami cookie mają miejsce, gdy plik cookie jest wysyłany ze strony klienta na serwer. W modyfikacji trwałych i nietrwałych plików cookies pomagają różnego rodzaju narzędzia.

• Ataki typu unvalidated input i file-injection: Ataki typu unvalidated input i file-injection są przeprowadzane poprzez dostarczenie niesprawdzonych danych wejściowych lub poprzez wstrzyknięcie plików do aplikacji internetowej.

• Przejęcie sesji: Przejęcie sesji to atak, w którym osoba atakująca wykorzystuje, kradnie, przewiduje i negocjuje mechanizm kontroli rzeczywistej ważnej sesji internetowej w celu uzyskania dostępu do uwierzytelnionych części aplikacji internetowej.

• Ataki SQL Injection: SQL Injection wykorzystuje lukę w zabezpieczeniach bazy danych do ataków. Atakujący wstrzykuje złośliwy kod do ciągów znaków, które są następnie przekazywane do serwera SQL w celu wykonania.

• Directory Traversal: Directory Traversal to wykorzystanie protokołu HTTP, dzięki któremu atakujący mogą uzyskać dostęp do zastrzeżonych katalogów i wykonywać polecenia poza głównym katalogiem serwera WWW, manipulując adresami URL.

• Atak typu „odmowa usługi” (DoS): Atak typu DoS ma na celu przerwanie działania strony internetowej lub serwera w celu uniemożliwienia dostępu użytkownikom, dla których jest przeznaczony.

• Ataki Cross-Site Scripting (XSS): w tej metodzie atakujący wstrzykuje znaczniki HTML lub skrypty do docelowej witryny internetowej.

• Ataki z przepełnieniem bufora: projekt większości aplikacji internetowych pomaga im w utrzymaniu pewnej ilości danych. Jeśli ta ilość przekroczy dostępną przestrzeń dyskową, aplikacja może ulec awarii lub wykazywać inne luki w działaniu. Atakujący wykorzystuje tę przewagę i zalewa aplikację nadmiarem danych, powodując atak przepełnienia bufora.

• Atak Cross-Site Request Forgery (CSRF): osoba atakująca wykorzystuje zaufanie uwierzytelnionego użytkownika do przekazania złośliwego kodu lub poleceń do serwera WWW.

• Ataki Command Injection: W tego rodzaju ataku haker zmienia zawartość strony internetowej, używając kodu HTML i identyfikując pola formularza, które nie mają prawidłowych ograniczeń.

• Ujawnienie kodu źródłowego: Ujawnienie kodu źródłowego jest wynikiem błędów typograficznych w skryptach lub błędnej konfiguracji, na przykład nieudzielenia uprawnień do wykonywania skryptowi lub katalogowi. Ujawnienie kodu źródłowego może czasami umożliwić atakującym dostęp do poufnych informacji o poświadczeniach bazy danych i tajnych kluczach w celu naruszenia bezpieczeństwa serwera WWW.

Uwaga: pełne omówienie ataków na aplikacje internetowe zawiera Moduł 14: Hakowanie aplikacji internetowych.

Metodologia ataku na serwer WWW

W poprzedniej sekcji opisano ataki, które można przeprowadzić w celu naruszenia bezpieczeństwa serwera WWW. W tej sekcji wyjaśniono, w jaki sposób osoba atakująca przeprowadza pomyślny atak na serwer WWW. Wprowadza również narzędzia do hakowania serwerów WWW, z których mogą korzystać osoby atakujące. Narzędzia te wydobywają krytyczne informacje podczas procesu hakowania. Atak na serwer WWW zazwyczaj obejmuje wcześniej zaplanowane działania zwane metodologią ataku, którą atakujący stosuje, aby osiągnąć cel, jakim jest naruszenie zabezpieczeń docelowego serwera WWW. Atakujący włamują się do serwera WWW w wielu etapach. Na każdym etapie atakujący próbuje zebrać informacje o lukach i uzyskać nieautoryzowany dostęp do serwera WWW. Poniżej przedstawiono różne etapy metodologii ataku na serwery WWW.

Zbieranie informacji

Każdy atakujący stara się zebrać jak najwięcej informacji o docelowym serwerze WWW. Atakujący zbiera informacje, a następnie je analizuje, aby znaleźć luki w obecnych mechanizmach bezpieczeństwa serwera WWW.

Podstawa serwera WWW

Celem odcisku stopy jest zebranie informacji o aspektach bezpieczeństwa serwera WWW za pomocą narzędzi lub technik odcisku stopy. Wykorzystując footprinting, atakujący mogą określić możliwości zdalnego dostępu do serwera WWW, jego porty i usługi oraz inne aspekty jego bezpieczeństwa.

Kopia lustrzana witryny

Kopia lustrzana witryny to metoda kopiowania witryny i jej zawartości na inny serwer w celu przeglądania w trybie offline. Dzięki dublowanej witrynie osoba atakująca może wyświetlić szczegółową strukturę witryny.

Skanowanie w poszukiwaniu luk w zabezpieczeniach

Skanowanie pod kątem luk w zabezpieczeniach to metoda znajdowania luk w zabezpieczeniach i błędnych konfiguracji serwera WWW. Atakujący skanują w poszukiwaniu luk za pomocą zautomatyzowanych narzędzi znanych jako skanery luk w zabezpieczeniach.

Przejęcie sesji

Atakujący mogą dokonać przejęcia sesji po zidentyfikowaniu bieżącej sesji klienta. Atakujący przejmuje pełną kontrolę nad sesją użytkownika poprzez przejęcie sesji.

Hakowanie haseł do serwerów WWW

Atakujący używają metod łamania haseł, takich jak ataki siłowe, ataki hybrydowe i ataki słownikowe, aby złamać hasło serwera WWW.

Zbieranie informacji

Zbieranie informacji to pierwszy i jeden z najważniejszych kroków w kierunku zhakowania docelowego serwera WWW. Na tym etapie atakujący zbiera jak najwięcej informacji o serwerze docelowym, używając różnych narzędzi i technik. Informacje uzyskane w tym kroku pomagają atakującemu w ocenie stanu bezpieczeństwa serwera WWW. Atakujący mogą przeszukiwać Internet, grupy dyskusyjne, tablice ogłoszeń itd. w celu zebrania informacji o organizacji docelowej. Atakujący mogą używać narzędzi, takich jak who.is i Whois Lookup, w celu wyodrębnienia informacji, takich jak nazwa domeny celu, adres IP i numer systemu autonomicznego.

who.is

who.is jest przeznaczony do wykonywania różnych funkcji wyszukiwania whois. Pozwala użytkownikowi na wyszukiwanie domeny whois, wyszukiwanie adresu IP whois oraz przeszukiwanie bazy danych whois w celu znalezienia odpowiednich informacji na temat rejestracji i dostępności domen.

Oto kilka dodatkowych narzędzi do zbierania informacji:

Whois Lookup(https://whois.domointools.com)

Whois (https://www.whois.com)

Domain Dossier (https://centrolops.net)

Find Subdomains (https://pentest-tools.com)

SmartWhois (https://www.tomos.com)

Uwaga: Pełne omówienie technik zbierania informacji znajduje się w Module 02: Ślad i rozpoznanie.

Zbieranie informacji z pliku Robots.txt

Właściciel witryny tworzy plik robots.txt zawierający listę plików lub katalogów, które robot indeksujący powinien zaindeksować w celu dostarczenia wyników wyszukiwania. Źle napisane pliki robots.txt mogą spowodować całkowite zaindeksowanie plików i katalogów stron internetowych. Jeśli

poufne pliki i katalogi są indeksowane, osoba atakująca może łatwo uzyskać informacje, takie jak hasła, adresy e-mail, ukryte łącza i obszary członkostwa. Jeśli właściciel docelowej witryny sieci Web zapisze plik robots.txt bez zezwolenia na indeksowanie stron z ograniczeniami w celu udostępnienia wyników wyszukiwania, osoba atakująca może nadal przeglądać plik robots.txt witryny w celu wykrycia plików z ograniczeniami, a następnie przeglądać je w celu zebrania informacji. Osoba atakująca wpisuje adres URL/robots.txt w pasku adresu przeglądarki, aby wyświetlić plik robots.txt witryny docelowej. Osoba atakująca może również pobrać plik robots.txt docelowej witryny za pomocą narzędzia Wget.

Wykorzystanie Footprintingu serwera WWW/przechwytywanie banerów

Wykonując analizę zasobów serwera WWW, osoba atakująca może zebrać cenne dane na poziomie systemu, takie jak szczegóły konta, systemu operacyjnego, wersji oprogramowania, nazw serwerów i szczegółów schematu bazy danych. Narzędzie Telnet może służyć do śledzenia serwera WWW i zbierania informacji, takich jak nazwa serwera, typ serwera, system operacyjny i uruchomione aplikacje. Ponadto narzędzia do śledzenia śladów, takie jak ID Serve, httprecon i Netcraft, mogą być używane do śledzenia śladów serwera WWW. Te narzędzia do śledzenia mogą wyodrębniać informacje z serwera docelowego. Tutaj badamy funkcje i typy informacji, które te narzędzia mogą zbierać z serwera docelowego.

Narzędzia do obliczania śladu serwera sieci Web

Netcat

Netcat to narzędzie sieciowe, które odczytuje i zapisuje dane w połączeniach sieciowych przy użyciu protokołu TCP/IP. Jest to niezawodne narzędzie „zaplecza" używane bezpośrednio lub sterowane przez inne programy i skrypty. Jest to również narzędzie do debugowania i eksploracji sieci. Poniżej przedstawiono polecenia używane do przechwytywania banerów dla witryny www.moviescope.com jako przykład do zbierania informacji, takich jak typ i wersja serwera.

o # nc —w www. moviescope.com 80 — naciśnij [Enter]

o GET / HTTP/1.0 - naciśnij dwukrotnie [Enter].

Telnet

Telnet to protokół sieciowy klient-serwer, który jest szeroko stosowany w Internecie lub sieciach LAN. Zapewnia sesje logowania dla użytkownika w Internecie. Pojedynczy terminal podłączony do innego komputera emuluje sesję za pomocą usługi Telnet. Podstawowe problemy związane z bezpieczeństwem usługi Telnet są następujące.

o Nie szyfruje danych przesyłanych przez połączenie,

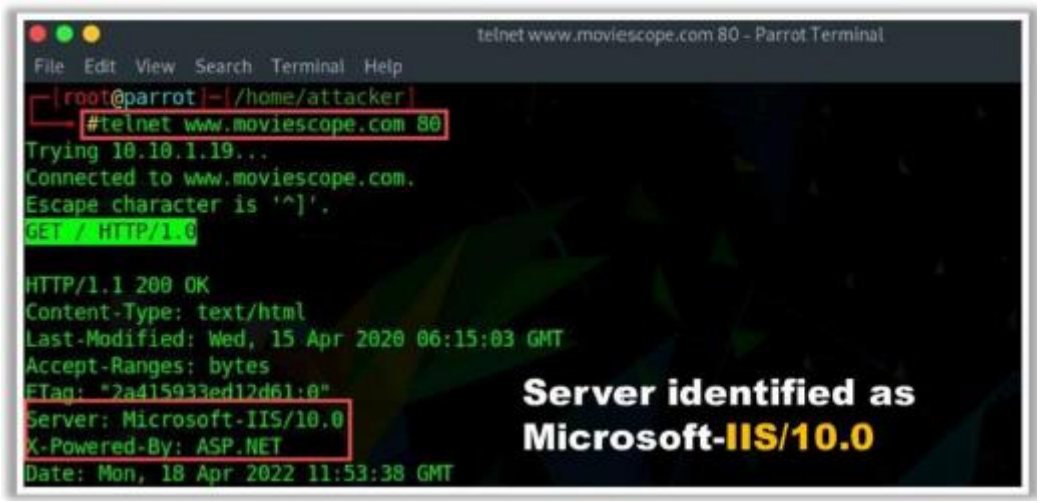
o Brak schematu uwierzytelniania.

Telnet umożliwia atakującemu wykonanie ataku polegającego na przechwyceniu banera. Sonduje serwery HTTP, aby określić pole serwera w nagłówku odpowiedzi HTTP. Na przykład następująca procedura jest wykorzystywana do wyliczenia hosta działającego na http (TCP 80).

o Poproś Telnet o połączenie z hostem na określonym porcie za pomocą polecenia # telnet www.moviescope.com 80 i naciśnij Enter. Pojawi się pusty ekran.

o Wpisz GET / HTTP/1.0 i naciśnij dwukrotnie Enter.

Serwer HTTP odpowiada informacją pokazaną na zrzucie ekranu.



httprecon

httprecon to narzędzie do zaawansowanego pobierania odcisków palców serwerów WWW. To narzędzie przeprowadza ataki polegające na przechwytywaniu banerów, wyliczaniu kodów stanu i analizie kolejności nagłówków na docelowym serwerze WWW oraz zapewnia dokładne informacje o odciskach palców serwera WWW. httprecon wykonuje następujące przypadki testowe analizy nagłówków na docelowym serwerze WWW:

o Uzasadnione żądanie GET dla istniejącego zasobu

o Wyjątkowo długie żądanie GET (Uniform Resource Identifier (URi) >1024 bajty)

o Typowe żądanie GET dla nieistniejącego zasobu

o Wspólne żądanie HEAD dla istniejącego zasobu

o Wyliczenie z OPTIONS, które jest dozwolone

o Metoda HTTP DELETE, która zwykle nie jest dozwolona

o Metoda HTTP TEST, która nie jest zdefiniowana

o Wersja protokołu HTTP/9.8, która nie istnieje

o Żądanie GET zawierające wzorce ataków (np. : ../ i%%)

ID Serve

ID Serve to proste narzędzie do identyfikacji serwera internetowego. Poniżej znajduje się lista jego możliwości.

o Identyfikacja serwera HTTP: ID Serve może zidentyfikować markę, model i wersję oprogramowania serwera witryny. ID Serve wysyła te informacje w preambule odpowiedzi na zapytania sieciowe, ale informacje te nie są widoczne dla użytkownika.

o Identyfikacja serwera innego niż HTTP: Większość serwerów internetowych innych niż HTTP (np. FTP, SMTP, POP i NEWS) musi przesyłać linię zawierającą numeryczny kod stanu i znak czytelne powitanie dla każdego łączącego się klienta. W związku z tym ID Serve może również łączyć się z serwerami innymi

niż sieciowe, aby odbierać i zgłaszać wiadomość powitalną serwera. Zwykle ujawnia to markę, model, wersję i inne potencjalnie przydatne informacje serwera.

o Odwrotne wyszukiwanie DNS: Gdy użytkownicy ID Serve wprowadzą nazwę domeny lub adres URL witryny lub serwera, aplikacja użyje DNS do określenia adresu IP tej domeny. Czasami jednak warto postąpić w innym kierunku, aby określić nazwę domeny powiązaną ze znanym adresem IP. Ten proces, znany jako odwrotne wyszukiwanie DNS, jest również wbudowany w ID Serve. ID Serve próbuje określić powiązaną nazwę domeny dla dowolnego wprowadzonego adresu IP.

Oto kilka dodatkowych narzędzi do śledzenia śladów:

NetCraft (https://www.netcroft.com)

Uniscan (https://sourceforge.net)

Nmap (https://nmop.org)

Ghost Eye (https://github.com)

Skipfish (https://code.google.com)

Wyliczanie informacji o serwerze WWW za pomocą Nmap

Nmap, wraz z Nmap Scripting Engine (NSE), może wyodrębnić dużą ilość cennych informacji z docelowego serwera WWW. Oprócz poleceń Nmap, NSE udostępnia skrypty, które ujawniają atakującemu różnego rodzaju przydatne informacje o docelowym serwerze. Osoba atakująca używa następujących poleceń Nmap i skryptów NSE w celu wyodrębnienia informacji. Odkryj domeny wirtualne za pomocą mapy hosta:

$nmap --script mapa hosta <host>

Wykryj podatny na ataki serwer, który używa metody TRACE:

nmap --script http-trace -p80 localhost

Zbieraj konta e-mail za pomocą http-google-email:

$nmap --script http-google-email <host>

Wylicz użytkowników za pomocą http-userdir-enum:

nmap -p80 --script http-userdir -enum localhost

Wykryj ślad HTTP:

$nmap -p80 --script śledzenie http <host>

Sprawdź, czy serwer WWW jest chroniony przez zaporę sieciową (WAF) lub IPS:

$nmap -p80 --script http-waf-detect --script-args="http-wafdetect.

uri=/testphp.vulnweb.com/artists.php,http-wafdetect.

wykryjBodyChanges" www.modsecurity.org

Wymień popularne aplikacje internetowe

$nmap --script http-enum -p80 <host>

Pobierz plik robots.txt

$nmap -p80 --script http-robots.txt <host>

Poniżej przedstawiono kilka dodatkowych poleceń Nmap używanych do wyodrębniania informacji o serwerze WWW:

nmap -sV -O -p target IP addreess

nmap -sV --script http-enum target IP addreess

nmap docelowy adres IP -p 80 --script = http-frontpage-login

nmap --script http-passwd --script-args http-passwd.root =/ target IP addreess

Dublowanie witryny

Kopia lustrzana witryny kopiuje całą witrynę i jej zawartość na dysk lokalny. Witryna lustrzana ujawnia pełny profil struktury katalogów witryny, struktury plików, linków zewnętrznych, obrazów, stron internetowych i tak dalej. Dzięki lustrzanej witrynie docelowej osoba atakująca może łatwo zmapować katalogi witryny i uzyskać cenne informacje. Osoba atakująca, która kopiuje witrynę internetową, nie musi być online, aby przejść przez witrynę docelową. Ponadto osoba atakująca może uzyskać cenne informacje, przeszukując komentarze i inne elementy w kodzie źródłowym HTML pobranych stron internetowych. Do skopiowania docelowej witryny na dysk lokalny można użyć wielu narzędzi do tworzenia kopii lustrzanych witryn; przykłady obejmują WebCopier Pro, HTTrack Web Site Copier, Website Ripper Copier i Cyotek WebCopy.

WebCopier Pro

WebCopier Pro to przeglądarka offline do pobierania stron internetowych i przechowywania ich lokalnie, dzięki czemu można je później przeglądać/analizować. Pozwala atakującym przeanalizować strukturę witryny i znaleźć martwe linki.

Oto kilka dodatkowych narzędzi do tworzenia kopii lustrzanych witryn:

HTTrack Web Site Copier (https://www.httrock.com)

Website Ripper Copier (https://www.tensons.com)

Cyotek WebCopy (https://www.cyotek.com)

Portable Offline Browser (http://www.metoproducts.com)

Offline Explorer Enterprise (https://metoproducts.com)

Znajdowanie domyślnych poświadczeń serwera WWW

Administratorzy lub pracownicy ochrony używają interfejsów administracyjnych do bezpiecznego konfigurowania, zarządzania i monitorowania serwerów aplikacji internetowych. Wiele interfejsów administracyjnych serwera WWW jest publicznie dostępnych i znajduje się w katalogu głównym. Często te poświadczenia interfejsu administracyjnego nie są poprawnie skonfigurowane i pozostają ustawione na wartości domyślne. Atakujący próbują zidentyfikować działający interfejs aplikacji docelowego serwera WWW, przeprowadzając skanowanie portów. Po zidentyfikowaniu działającego

interfejsu administracyjnego osoba atakująca używa następujących technik w celu zidentyfikowania domyślnych danych logowania:

• Zapoznaj się z dokumentacją interfejsu administracyjnego i określ domyślne hasła

• Użyj wbudowanej bazy danych Metasploit do przeskanowania serwera Użyj zasobów online, takich jak Open Sez Me (https://open-sez.me) i cirt.net (https://cirt.net/passwords), aby zidentyfikować domyślne hasła

• Próbować odgadywania haseł i ataków siłowych

Te domyślne poświadczenia mogą zapewnić dostęp do interfejsu administracyjnego, narażając serwer WWW i umożliwiając atakującemu wykorzystanie głównej aplikacji internetowej.

cirt.net

cirt.net to baza danych wyszukiwania domyślnych haseł, poświadczeń i portów.

Znajdowanie domyślnej zawartości serwera WWW

Większość serwerów aplikacji internetowych ma domyślną zawartość i funkcjonalności, które umożliwiają atakującym przeprowadzanie ataków. Poniżej przedstawiono niektóre typowe domyślne treści i funkcje, które osoba atakująca próbuje zidentyfikować na serwerach WWW.

Administratorzy debugują i testują funkcjonalność

Funkcjonalności przeznaczone dla administratorów do debugowania, diagnozowania i testowania aplikacji internetowych i serwerów WWW zawierają przydatne informacje konfiguracyjne oraz stan środowiska uruchomieniowego zarówno serwera, jak i działających na nim aplikacji. Dlatego te funkcje są głównymi celami atakujących.

Przykładowa funkcjonalność w celu zademonstrowania typowych zadań

Wiele serwerów zawiera różne przykładowe skrypty i strony zaprojektowane w celu zademonstrowania pewnych funkcji serwera aplikacji i interfejsów programowania aplikacji (API). Często serwery WWW nie zabezpieczają tych skryptów przed atakującymi, a te przykładowe skrypty albo zawierają luki w zabezpieczeniach, które mogą zostać wykorzystane przez atakujących, albo implementują funkcje, które umożliwiają atakującym wykorzystanie.

Publicznie dostępne potężne funkcje

Niektóre serwery internetowe zawierają zaawansowane funkcje przeznaczone dla personelu administracyjnego i ograniczone do użytku publicznego. Jednak osoby atakujące próbują wykorzystać tak potężne funkcje, aby naruszyć bezpieczeństwo serwera i uzyskać do niego dostęp. Na przykład niektóre serwery aplikacji umożliwiają wdrażanie archiwów sieciowych przez ten sam port HTTP, z którego korzysta aplikacja. Atakujący może użyć typowych platform eksploatacyjnych, takich jak Metasploit, do przeprowadzenia skanowania w celu zidentyfikowania domyślnych haseł, załadowania tylnych drzwi i uzyskania dostępu do serwera docelowego z poziomu powłoki poleceń.

Instrukcje instalacji serwera

Osoba atakująca próbuje zidentyfikować podręczniki serwera, które mogą zawierać przydatne informacje dotyczące konfiguracji i instalacji serwera. Dostęp do tych informacji umożliwia atakującemu przygotowanie odpowiedniej struktury do wykorzystania zainstalowanego serwera WWW.

Narzędzia takie jak Nikto2 mogą służyć do identyfikacji domyślnych treści.

Nikto2

Nikto to skaner luk w zabezpieczeniach szeroko stosowany do identyfikowania potencjalnych luk w aplikacjach internetowych i serwerach internetowych.

Znajdowanie list katalogów serwera WWW

Kiedy serwer WWW otrzymuje żądanie dotyczące katalogu, a nie pliku, odpowiada na to żądanie w następujący sposób.

Zwróć domyślny zasób w katalogu: Serwer może zwrócić domyślny zasób w katalogu, taki jak index.html.

Return Error: Serwer może zwrócić błąd, taki jak kod stanu HTTP 403, wskazujący, że żądanie jest niedozwolone.

Zwróć listę zawartości katalogu: Serwer może zwrócić listę pokazującą zawartość katalogu. Przykładowa lista katalogów jest pokazana na zrzucie ekranu.

Chociaż listy katalogów nie mają istotnego znaczenia z punktu widzenia bezpieczeństwa, czasami zawierają następujące luki, które umożliwiają atakującym złamanie zabezpieczeń aplikacji internetowych:

Niewłaściwa kontrola dostępu

Nieumyślny dostęp do katalogu głównego serwerów

Ogólnie rzecz biorąc, po wykryciu katalogu na serwerze WWW osoba atakująca wysyła żądanie dotyczące tego katalogu i próbuje uzyskać dostęp do listy katalogów. Atakujący próbują również wykorzystać podatne na ataki oprogramowanie serwera WWW, które zapewnia dostęp do list katalogów. Atakujący używają narzędzi, takich jak Dirhunt i Sitechecker, aby znaleźć listę katalogów docelowego serwera WWW.

Dirhunt

Dirhunt to robot indeksujący zoptymalizowany pod kątem wyszukiwania i analizowania katalogów. To narzędzie może znaleźć interesujące wyniki, jeśli serwer ma włączony tryb „indeksowania”. Dirhunt jest również przydatny, jeśli lista katalogów nie jest włączona. Wykrywa katalogi z fałszywymi błędami 404, katalogi, w których utworzono pusty plik indeksu w celu ukrycia rzeczy i tak dalej.

Skanowanie w poszukiwaniu luk w zabezpieczeniach

Skanowanie pod kątem luk w zabezpieczeniach jest przeprowadzane w celu zidentyfikowania luk w zabezpieczeniach i błędnych konfiguracji docelowego serwera WWW lub sieci. Skanowanie pod kątem luk w zabezpieczeniach ujawnia potencjalne słabości serwera docelowego, które można wykorzystać w ataku na serwer WWW. W fazie skanowania luk atakujący wykorzystują techniki sniffingu w celu uzyskania danych o ruchu sieciowym w celu określenia aktywnych systemów, usług sieciowych i aplikacji. Zautomatyzowane narzędzia, takie jak Acunetix Web Vulnerability Scanner, służą do skanowania pod kątem luk w zabezpieczeniach na serwerze docelowym i znajdowania hostów, usług i luk w zabezpieczeniach.

Internetowy skaner luk w zabezpieczeniach Acunetix

Acunetix Web Vulnerability Scanner (WVS) skanuje strony internetowe i wykrywa luki w zabezpieczeniach. Acunetix WVS sprawdza aplikacje internetowe pod kątem iniekcji SQL, XSS i tak dalej. Zawiera zaawansowane narzędzia do testowania za pomocą pióra, które ułatwiają ręczne przeprowadzanie audytów bezpieczeństwa i tworzy profesjonalne raporty z audytów bezpieczeństwa i zgodności z przepisami w oparciu o technologię AcuSensor. Obsługuje testowanie formularzy internetowych i obszarów chronionych hasłem, stron z CAPTCHA, mechanizmami jednokrotnego logowania i uwierzytelniania dwuskładnikowego. Wykrywa języki aplikacji, typy serwerów WWW i witryny zoptymalizowane pod kątem smartfonów. Acunetix indeksuje i analizuje różne typy stron internetowych, w tym HTML5, Simple Object Access Protocol (SOAP) oraz Asynchronous JavaScript i Extensible Markup Language (AJAX), obsługuje skanowanie usług sieciowych uruchomionych na serwerze oraz skanowanie portów serwera WWW.

Poniżej przedstawiono kilka dodatkowych narzędzi do wykrywania luk w zabezpieczeniach:

Fortify Weblnspect (https://www.microfocus.com)

Tenable.io (https://www.tenable.com)

ImmuniWeb (https://www.immuniweb.com)

Invicti (htips://www.invicti.com)

Znajdowanie luk w zabezpieczeniach, które można wykorzystać

Luki i błędy programistyczne w projekcie oprogramowania prowadzą do luk w zabezpieczeniach. Atakujący wykorzystują te luki do przeprowadzania różnych ataków na poufność, dostępność lub integralność systemu. Luki w zabezpieczeniach oprogramowania, takie jak błędy programistyczne w programie, usłudze lub oprogramowaniu systemu operacyjnego lub jądrze, mogą zostać wykorzystane do wykonania złośliwego kodu. Wiele publicznych repozytoriów luk w zabezpieczeniach, które są dostępne online, umożliwia dostęp do informacji o różnych lukach w oprogramowaniu. Atakujący przeszukują strony z exploitami, takie jak Packet Storm (https://pocketstormsecurity.com) i Exploit Database (https://www.exploit-db.com) w poszukiwaniu możliwych do wykorzystania luk w zabezpieczeniach serwera WWW w oparciu o jego system operacyjny i aplikacje. Atakujący wykorzystują informacje zebrane na poprzednich etapach, aby znaleźć odpowiednie luki za pomocą Exploit Database. Wykorzystanie tych luk umożliwia atakującym wykonanie polecenia lub pliku binarnego na docelowej maszynie w celu uzyskania wyższych uprawnień niż istniejące lub obejścia mechanizmów bezpieczeństwa. Atakujący korzystający z tych exploitów mogą nawet uzyskać dostęp do kont użytkowników uprzywilejowanych i poświadczeń.

Przejęcie sesji

Prawidłowe identyfikatory sesji mogą zostać podsłuchane w celu uzyskania nieautoryzowanego dostępu do serwera WWW i przechwycenia jego danych. Osoba atakująca może przejąć lub ukraść prawidłową zawartość sesji przy użyciu różnych technik, takich jak przewidywanie tokenów sesji, odtwarzanie sesji, utrwalanie sesji, sidejacking i XSS. Korzystając z tych technik, osoba atakująca próbuje przechwycić prawidłowe sesyjne pliki cookie i identyfikatory w ustanowionych sesjach. Atakujący używa narzędzi takich jak Burp Suite, JHijack i Ettercap do automatyzacji przejmowania sesji.

Burp Suite

Burp Suite to narzędzie do testowania bezpieczeństwa sieci, które może przejąć identyfikatory sesji w ustanowionych sesjach. Narzędzie Sequencer w Burp Suite testuje losowość tokenów sesji. Za pomocą

tego narzędzia osoba atakująca może przewidzieć następny możliwy token identyfikatora sesji i użyć go do przejęcia prawidłowej sesji.

Oto kilka dodatkowych narzędzi do przejmowania sesji:

JHijack (https://sourceforge.net)

Ettercap (https://www.ettercop-project.org)

CookieCatcher (https://github.com)

Cookie Cadger (https://github.com)

Uwaga: Pełne omówienie koncepcji i technik związanych z przejmowaniem sesji można znaleźć w sekcji Moduł 11: Przejęcie sesji.

Hakowanie hasła do serwera WWW

W tej fazie hakowania serwera WWW osoba atakująca próbuje złamać hasła do serwera WWW. Atakujący może zastosować wszystkie możliwe techniki łamania haseł w celu wyodrębnienia haseł, w tym zgadywanie haseł, ataki słownikowe, ataki brute-force, ataki hybrydowe, wstępnie obliczone skróty, ataki oparte na regułach, ataki sieci rozproszonej i ataki tęczy. Atakujący potrzebuje cierpliwości, aby złamać hasła, ponieważ niektóre z tych technik są żmudne i czasochłonne. Atakujący może również użyć zautomatyzowanych narzędzi, takich jak Hashcat, THC Hydra i Ncrack, aby złamać hasła internetowe i skróty.

Hashcat

Hashcat to cracker kompatybilny z wieloma systemami operacyjnymi i platformami, który może wykonywać multihash (MD4, 5; SHA - 224, 256, 384, 512; RIPEMD-160; itp.), Łamanie haseł na wielu urządzeniach. Tryby ataku tej THC Hydra

THC Hydra to równoległy łamacz logowania, który może atakować wiele protokołów. To narzędzie jest kodem sprawdzającym koncepcję, który zapewnia badaczom i konsultantom ds. bezpieczeństwa możliwość zademonstrowania, jak łatwo byłoby uzyskać nieautoryzowany zdalny dostęp do systemu. Obecnie to narzędzie obsługuje następujące protokoły: Asterisk; protokół archiwizacji Apple (AFP); Uwierzytelnianie, autoryzacja i rozliczanie Cisco (AAA); autoryzacja Cisco; włączenie Cisco; system równoległych wersji (CVS); Ognisty Ptak; FTP; HTTP-FORM-GET; HTTP-FORMPOST; HTTP-GET; NAGŁÓWEK HTTP; HTTP-POST; HTTP PROXY; HTTPS-FORM-GET; HTTPSFORM-POST; HTTPS-GET; HTTPS-HEAD; HTTPS-POST; Http Proxy; ICQ; Wiadomość internetowa protokołu dostępu (IMAP); Czat internetowy (IRC); Lekki protokół dostępu do katalogów (LDAP); Memcached; MongoDB; Serwer Microsoft SQL; MySQL; protokół kontroli sieci (NCP); protokół przesyłania wiadomości sieciowych (NNTP); Słuchacz Wyroczni; Identyfikator systemu Oracle (SID); Wyrocznia; PC-wszędzie; sieciowy system plików komputera osobistego (PC-NFS); POP3; Postgres; Radmin; protokół pulpitu zdalnego (RDP); Rexec; Zaloguj się; rsz; protokół przesyłania strumieniowego w czasie rzeczywistym (RTSP); SAP R/3; protokół inicjowania sesji (SIP); blok komunikatów serwera (SMB); Prosty protokół przesyłania poczty (SMTP); Numer SMTP; Prosty protokół zarządzania siecią (SNMP) vl+v2+v3; SKARPETKI5; SSH (vl i v2); klucz SSH; Obalenie; TeamSpeak (TS2); Telnet; uwierzytelnianie VMware; Przetwarzanie w sieci wirtualnej (VNC); oraz Extensible Messaging and Presence Protocol (XMPP).

Oto kilka dodatkowych narzędzi do łamania haseł:

Ncrack (https://nmop.org)

Rainbow crack (https://project-roinbowcrock.com)

Wfuzz (http://www.edge-security.com)

Wireshark (https://www.wireshork.org)

Używanie serwera aplikacji jako serwera proxy

Serwery sieci Web są czasami konfigurowane do wykonywania funkcji, takich jak przekazywanie lub zwrotne proxy HTTP. Serwery internetowe z włączonymi tymi funkcjami są wykorzystywane przez osoby atakujące do przeprowadzania następujących ataków:

Atakowanie systemów stron trzecich w Internecie

Łączenie się z dowolnymi hostami w wewnętrznej sieci organizacji

Łączenie się z innymi usługami działającymi na samym hoście proxy

Atakujący używają żądań GET i CONNECT, aby używać wrażliwych serwerów internetowych jako serwerów proxy do łączenia się i uzyskiwania informacji z systemów docelowych za pośrednictwem tych serwerów internetowych.

Narzędzia ataku na serwer WWW: Metasploit

Metasploit Framework to zestaw narzędzi do testów penetracyjnych, platforma rozwoju exploitów i narzędzie badawcze, które obejmuje setki działających zdalnie exploitów dla różnych platform. Wykonuje w pełni zautomatyzowaną eksploatację serwerów WWW, wykorzystując znane luki w zabezpieczeniach i wykorzystując słabe hasła przez Telnet, SSH, HTTP i SNMP.

Atakujący może użyć następujących funkcji Metasploit do przeprowadzenia ataku na serwer WWW:

Weryfikacja luk w pętli zamkniętej

Symulacje phishingu

Inżynieria społeczna

Ręczne brutalne wymuszanie

Eksploatacja ręczna

Unikaj wiodących rozwiązań obronnych

Metasploit umożliwia testerom piór wykonanie następujących czynności:

Szybko wykonuj testy pióra, automatyzując powtarzalne zadania i wykorzystując wielopoziomowe ataki

Oceń bezpieczeństwo aplikacji internetowych, systemów sieciowych i końcowych, a także użytkowników poczty e-mail

Tuneluj dowolny ruch przez zainfekowane cele, aby skierować się głęboko do sieci

Dostosuj treść i szablon raportów wykonawczych, audytowych i technicznych

Architektura Metasploita

Metasploit Framework to platforma eksploatacyjna typu open source, która zapewnia badaczom bezpieczeństwa i testerom pióra jednolity model szybkiego rozwoju exploitów, ładunków, koderów,

generatorów bez operacji (NOP) i narzędzi rozpoznawczych. Framework ponownie wykorzystuje duże fragmenty kodu, które w przeciwnym razie użytkownik musiałby skopiować lub ponownie zaimplementować na podstawie poszczególnych exploitów. Struktura ma modułową architekturę i zachęca do ponownego wykorzystania kodu w różnych projektach. Ramę można podzielić na kilka różnych części, z których najniższym poziomem jest rdzeń ramy. Rdzeń frameworka jest odpowiedzialny za implementację wszystkich wymaganych interfejsów, które umożliwiają interakcję z modułami exploitów, sesjami i wtyczkami. Obsługuje badanie luk w zabezpieczeniach, opracowywanie exploitów i tworzenie niestandardowych narzędzi bezpieczeństwa.

Moduły Metasploit

Moduł exploitów Metasploit

Jest to podstawowy moduł Metasploit służący do enkapsulacji pojedynczego exploita, za pomocą którego użytkownicy atakują wiele platform. Ten moduł ma uproszczone pola metainformacji. Korzystając z funkcji Mixins, użytkownicy mogą również dynamicznie modyfikować zachowanie exploitów, przeprowadzać ataki typu brute-force i podejmować próby pasywnych exploitów. System można wykorzystać za pomocą Metasploit Framework, wykonując następujące kroki:

o Skonfiguruj aktywnego exploita

o Sprawdź opcje exploitów

o Wybierz cel

o Wybierz ładunek

o Uruchom exploita

Moduł ładunku Metasploit

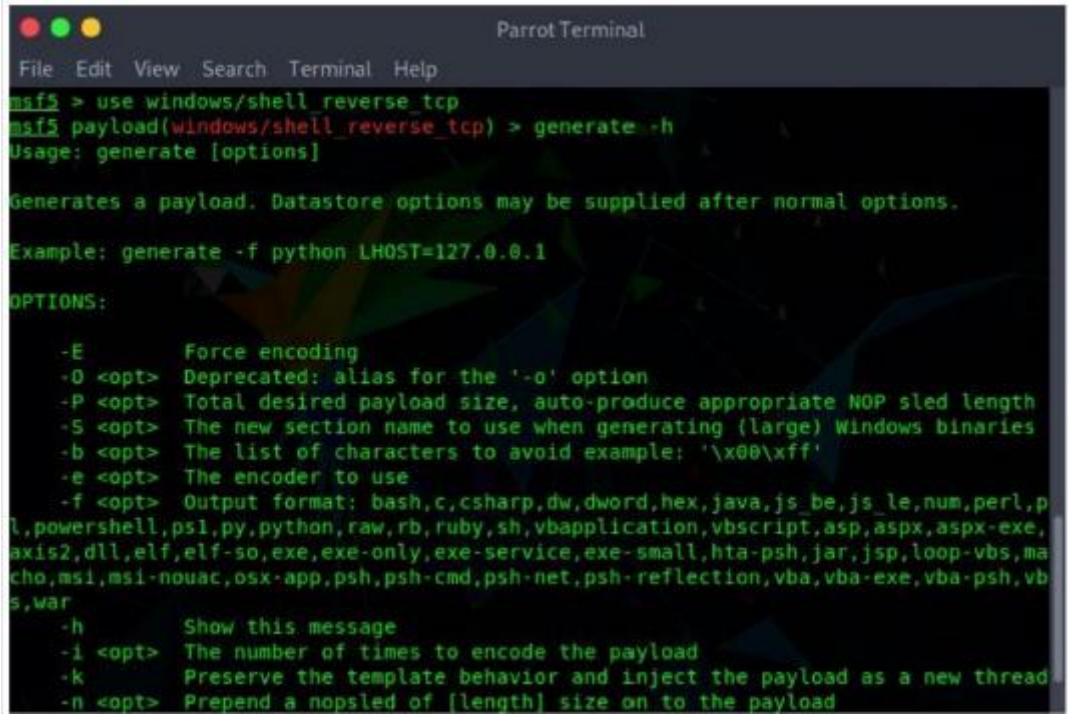
Exploit przenosi ładunek w swoim plecaku, kiedy włamuje się do systemu, a następnie zostawia tam plecak. Metasploit Framework zapewnia następujące trzy typy modułów ładunku.

o Single: samowystarczalny i całkowicie samodzielny

o Stagers: Konfiguruje połączenie sieciowe między atakującym a ofiarą

o Etapy: pobierane przez moduły stagera

Moduł ładunku Metasploit może przesyłać i pobierać pliki z systemu, robić zrzuty ekranu i zbierać skróty haseł. Może nawet przejąć ekran, mysz i klawiaturę, aby zdalnie sterować komputerem. Moduł ładunku ustanawia kanał komunikacyjny między platformą Metasploit a hostem ofiary. Łączy w sobie dowolny kod, który jest wykonywany w wyniku udanego exploita. Aby wygenerować ładunki, ładunek jest najpierw wybierany za pomocą polecenia pokazanego na zrzucie ekranu.



Moduł pomocniczy Metasploit

Moduły pomocnicze Metasploit mogą służyć do wykonywania dowolnych, jednorazowych działań, takich jak skanowanie portów, DoS, a nawet fuzzing. Obejmuje narzędzia i moduły oceniające bezpieczeństwo celu oraz moduły pomocnicze, takie jak skanery, moduły DoS i fuzzery. Polecenie show pomocniczy w Metasploit może być użyte do wyświetlenia listy wszystkich dostępnych modułów pomocniczych w Metasploit. Wszystkie moduły w Metasploit inne niż te używane do wykorzystania są modułami pomocniczymi. Metasploit wykorzystuje moduły pomocnicze jako rozszerzenie do różnych celów innych niż eksploatacja. Moduły pomocnicze są przechowywane w katalogu modułów/auxiliary/ głównego katalogu frameworka. Do uruchomienia modułu pomocniczego można użyć polecenia run lub exploit.

Podstawowa definicja modułu pomocniczego jest następująca:

require 'msf/core'

p "My Auxiliary Module"

class Metasploit3 < Msf::Auxiliary

end # for the class definition

Moduł Metasploit NOPS

Moduły NOP generują instrukcje no-operation służące do blokowania buforów. Polecenia generowania można użyć do wygenerowania sanek NOP o dowolnym rozmiarze i wyświetlenia ich w zadanym formacie.

Opcje:

-b <opcja>. Lista znaków, których należy unikać ('\xOO\xff')

-h\ Baner pomocy

-s <opt>: Oddzielona przecinkami lista rejestrów do zapisania

-t <opt>: typ wyjścia (Ruby, Perl, C lub surowy)

msf nop(opcja2)>

Następujące polecenie służy do generowania sań NOP o określonej długości:

msf > użyj x86/opty2

msf nop (opty2) > wygeneruj -h

Użycie: generuj [opcje] długość

Następujące polecenie służy do generowania 50-bajtowych sanek NOP:

msf > use x86/opty2

msf nop (opty2) > generate -h

Usage : generate [options] length

The following command is used to generate a 50-byte NOP sled:

msf nop (opty2) > generate -t c 50

unsigned char buf [ ] =

" \xf5\ x3d\ x05 \ xl 5\xf 8\ x67 \ xba\ x7d\ x08\ xd6\ x66\ x9f \ xb8\ x2d \ xb6"

" \ x24 \ xbe\ xbl \ x3f \ x43\ xld\ x93\ xb2\ x37 \ x35\ x84 \ xd5\ xl 4 \ x40\ xb4"

" \ xb3\ x41 \ xb9\ x48\ x04 \ x99\ x46\ xa9\ xb0 \ xb7\ x2f \ xfd\ x96\ x4a \ x98"

" \ x92 \ xb5\ xd4 \ x4f\ x91

msf nop (opty2) >

Narzędzia ataku na serwer WWW

Immunity's CANVAS

CANVAS firmy Immunity zapewnia testerom penetracyjnym i specjalistom ds. exploitów, zautomatyzowany system exploitów oraz kompleksowy, niezawodny rozwój struktury exploitów. Zapewnia takie funkcje, jak wykorzystywanie po stronie klienta, eskalacja uprawnień, http tunelowana eskalacja uprawnień, zdalna eksploatacja jądra, zaawansowana technologia backdoor i zaawansowana technologia ataków internetowych. Oto kilka dodatkowych narzędzi ataku na serwer WWW:

THC Hydra (https://github.com)

HULK DoS (https://github.com)

MPack (https://sourceforge.net)

w3af (https://w3of.org)

Środki zaradcze w przypadku ataku na serwer sieci Web

W poprzednich sekcjach omówiliśmy korzyści płynące z dobrze poinformowanej postawy bezpieczeństwa serwera WWW, niebezpieczeństwo stwarzane przez ataki na serwer WWW,

metodologię stosowaną w atakach na serwer WWW oraz narzędzia, które pomagają atakującemu w przeprowadzaniu ataków na serwer WWW. W tej sekcji omówimy narzędzia i techniki stosowane do zabezpieczania serwerów WWW. W tej sekcji omówiono również różne metody wykrywania ataków na serwer WWW, środki zaradcze i techniki obrony. Ponadto w tej sekcji opisano typowe narzędzia bezpieczeństwa służące do zabezpieczania serwera WWW przed możliwymi atakami. Narzędzia te skanują w poszukiwaniu luk w zabezpieczeniach serwera docelowego i aplikacji internetowych, wysyłają alerty w przypadku prób włamania, skanują w poszukiwaniu złośliwego oprogramowania na serwerze internetowym i wykonują inne działania związane z oceną bezpieczeństwa.

Umieść serwery sieci Web w oddzielnym segmencie bezpieczeństwa bezpiecznego serwera w sieci

Idealna sieć hostingowa powinna składać się z trzech segmentów: segmentu internetowego; bezpieczny segment bezpieczeństwa serwera, który jest często nazywany strefą zdemilitaryzowaną (DMZ); oraz sieć wewnętrzną. Pierwszym krokiem do zabezpieczenia serwerów WWW jest umieszczenie ich oddzielnie w strefie DMZ, która jest odizolowana od sieci publicznej i wewnętrznej sieci hostingowej. Umieszczenie serwerów WWW w oddzielnym segmencie dodaje bariery bezpieczeństwa między serwerami WWW a siecią wewnętrzną, a także między serwerami WWW a zewnętrzną siecią publiczną. Ta separacja pozwala administratorowi na umieszczanie zapór ogniowych i stosowanie kontroli dostępu w oparciu o reguły bezpieczeństwa dla sieci wewnętrznej, jak również dla ruchu internetowego w kierunku strefy DMZ. Taka sieć hostingowa może zapobiegać atakom na serwer WWW ze strony zewnętrznych atakujących lub złośliwych osób z wewnątrz. Segmentacja sieci dzieli sieć na różne segmenty, z których każdy ma własny koncentrator lub przełącznik. Pozwala administratorom sieci chronić jeden segment przed innymi poprzez egzekwowanie zapór ogniowych i reguł bezpieczeństwa w zależności od pożądanego poziomu bezpieczeństwa. W sieci podzielonej na segmenty osoba atakująca, która naruszy jeden segment sieci, nie będzie w stanie naruszyć bezpieczeństwa innych segmentów sieci. Weźmy przykładową sieć hostingową, która została podzielona przez administratora w taki sposób, że serwer WWW znajduje się w strefie DMZ.

Środki zaradcze: poprawki i aktualizacje

Poniżej przedstawiono różne środki zaradcze dla bezpiecznych aktualizacji i zarządzania poprawkami serwerów sieciowych:

Skanuj w poszukiwaniu istniejących luk; regularnie łatać i aktualizować oprogramowanie serwera.

Przed zastosowaniem jakiegokolwiek dodatku Service Pack, poprawki lub poprawki zabezpieczeń należy przeczytać i przejrzeć całą odpowiednią dokumentację.

Zastosuj wszystkie aktualizacje, niezależnie od ich typu, na zasadzie „w razie potrzeby”.

Przetestuj pakiety serwisowe i poprawki w reprezentatywnym środowisku nieprodukcyjnym przed ich wdrożeniem w środowisku produkcyjnym.

Upewnij się, że pakiety serwisowe, poprawki i poprawki zabezpieczeń są spójne na wszystkich kontrolerach domeny (DC).

Upewnij się, że przerwy w działaniu serwera są zaplanowane i że dostępny jest pełny zestaw taśm z kopiami zapasowymi i awaryjnych dysków naprawczych.

Zachowaj plan wycofania, który umożliwi powrót systemu i przedsiębiorstwa do ich pierwotnego stanu sprzed nieudanej implementacji.

Zaplanuj okresowe aktualizacje pakietów serwisowych w ramach konserwacji operacyjnej i nigdy nie spóźniaj się o więcej niż dwa pakiety serwisowe.

Wyłącz wszystkie nieużywane mapowania rozszerzeń skryptów.

Unikaj używania domyślnych konfiguracji wysyłanych z serwerami sieciowymi.

Korzystaj z wirtualnych poprawek w organizacji, ponieważ zapewniają one dodatkowe możliwości identyfikacji/rejestrowania.

Opracuj plan odzyskiwania po awarii, aby poradzić sobie z błędami zarządzania poprawkami.

Przeprowadź szeroko zakrojoną ocenę ryzyka, aby określić, które segmenty sieci są najbardziej podatne lub narażone na wysokie ryzyko, które należy najpierw załatać.

Wykonaj szczegółowy spis wszystkich punktów końcowych, usług i zależności.

Wdrażając poprawkę w całym systemie, upewnij się, że jest ona najpierw wykonywana w środowisku testowym.

Wdróż system ostrzegania o łatkach.

Użyj aplikacji do zarządzania poprawkami lub systemu, takiego jak SolarWinds Patch Manager, aby zautomatyzować procedurę.

Regularnie przeprowadzaj monitorowanie i raportowanie, aby mieć pewność, że procesy zarządzania poprawkami i aktualizacjami działają skutecznie.

Zmniejsz swoją ekspozycję na ryzyko stron trzecich, ograniczając liczbę używanych wersji oprogramowania.

Wszystkie operacje na łatkach i aktualizacjach powinny zostać zweryfikowane i udokumentowane pod kątem dostępności, analizy i potwierdzenia.

Opracuj ustandaryzowaną metodologię zarządzania poprawkami i aktualizacjami zabezpieczeń w ramach SDLC.

Środki zaradcze: protokoły i konta

Środki zaradcze: protokoły

Poniżej przedstawiono różne środki zaradcze dotyczące korzystania z bezpiecznych protokołów na serwerach sieciowych:

Zablokuj wszystkie niepotrzebne porty, ruch ICMP i niepotrzebne protokoły, takie jak NetBIOS i SMB.

Wzmocnij stos TCP/IP i konsekwentnie stosuj najnowsze poprawki i aktualizacje oprogramowania systemowego.

Jeśli używane są niezabezpieczone protokoły, takie jak Telnet, POP3, SMTP i FTP, należy podjąć odpowiednie środki w celu zapewnienia bezpiecznego uwierzytelniania i komunikacji, na przykład za pomocą zasad IPsec.

Jeśli potrzebny jest dostęp zdalny, upewnij się, że połączenia zdalne są odpowiednio zabezpieczone za pomocą protokołów tunelowania i szyfrowania.

Wyłącz WebDAV (Web Distributed Authoring and Versioning), jeśli nie jest używana przez aplikację, lub zapewnij jej bezpieczeństwo, jeśli jest to wymagane.

Do komunikacji z serwerem internetowym należy używać bezpiecznych protokołów, takich jak Transport Layer Security (TLS)/SSL.

Upewnij się, że niezidentyfikowane serwery FTP działają w nieszkodliwej części drzewa katalogów, która różni się od drzewa serwera WWW.

Upewnij się, że baner usługi HTTP jest prawidłowo skonfigurowany i zawiera szczegółowe informacje o urządzeniu hosta, takie jak wersja i typ systemu operacyjnego.

Odizoluj serwery pomocnicze, takie jak serwery LDAP, od lokalnej podsieci, aby odfiltrować ruch przez zaporę przed wejściem do sieci lokalnej.

Upewnij się, że wszystkie aplikacje do przesyłania plików przez serwer WWW są wykonywane przez FTPS w celu lepszego szyfrowania i ochrony danych.

Środki zaradcze: konta

W celu zabezpieczenia kont użytkowników na serwerze WWW można zastosować następujące środki zaradcze:

Usuń wszystkie nieużywane moduły i rozszerzenia aplikacji.

Wyłącz nieużywane domyślne konta użytkowników utworzone podczas instalacji systemu operacyjnego.

Podczas tworzenia nowego katalogu głównego sieci Web nadaj odpowiednie (najmniej możliwe) uprawnienia NTFS anonimowym użytkownikom serwera sieci Web IIS w celu uzyskania dostępu do zawartości sieci Web.

Wyeliminuj zbędnych użytkowników bazy danych i procedury składowane oraz postępuj zgodnie z zasadą najniższych uprawnień dla aplikacji bazy danych, aby chronić się przed zatruciem zapytaniami SQL.

Używaj bezpiecznych uprawnień internetowych, uprawnień NTFS i mechanizmów kontroli dostępu .NET Framework, w tym autoryzacji adresów URL.

Spowalniaj ataki siłowe i słownikowe dzięki silnym zasadom haseł oraz wdrażaj audyty i alerty w przypadku niepowodzenia logowania.

Uruchamiaj procesy przy użyciu najmniej uprzywilejowanych kont oraz najmniej uprzywilejowanych usług i kont użytkowników.

Ogranicz dostęp administratora lub administratora do minimalnej liczby użytkowników i prowadź rejestr tego samego.

Utrzymuj dzienniki wszystkich działań użytkowników w postaci zaszyfrowanej na serwerze WWW lub w oddzielnej maszynie w intranecie.

Wyłącz wszystkie nieinteraktywne konta, które powinny istnieć, ale nie wymagają interaktywnego logowania.

Korzystaj z bezpiecznych sieci VPN, takich jak OpenVPN, uzyskując dostęp do platform wieloserwerowych lub uzyskując dostęp do danych z modeli sieci międzyserwerowych, co pomaga korzystać z jednego konta w celu uzyskania dostępu do wielu serwerów.

Użyj menedżerów haseł, takich jak KeePass, aby zachować odpowiednią politykę haseł dla wielu kont użytkowników.

Włącz funkcję Separacji obowiązków (SoD) w ustawieniach konfiguracji serwera.

Zmuszaj użytkowników do okresowej zmiany haseł do swoich kont, tworząc zasady wygasania haseł.

Włącz funkcję blokowania konta użytkownika, ustawiając limit liczby nieudanych prób logowania.

Zaimplementuj 2FA lub MFA jako dodatkową warstwę bezpieczeństwa dla kont użytkowników.

Środki zaradcze: pliki i katalogi

W celu zabezpieczenia plików i katalogów w sieci można zastosować następujące środki zaradcze serwera:

Wyeliminuj niepotrzebne pliki w plikach .jar.

Wyeliminuj poufne informacje konfiguracyjne w kodzie bajtowym.

Unikaj mapowania katalogów wirtualnych między dwoma różnymi serwerami lub przez sieć.

Monitoruj i sprawdzaj wszystkie logi usług sieciowych, logi dostępu do stron internetowych, logi serwera bazy danych

(np. Microsoft SQL Server, MySQL i Oracle) oraz często rejestruje system operacyjny.

Wyłącz udostępnianie list katalogów.

Wyeliminuj pliki inne niż internetowe, takie jak pliki archiwów, pliki kopii zapasowych, pliki tekstowe i pliki nagłówkowe/dołączane pliki.

Wyłącz obsługę niektórych typów plików, tworząc mapę zasobów.

Upewnij się, że aplikacje internetowe lub pliki i skrypty witryn internetowych są przechowywane na partycji lub dysk niezależny od systemu operacyjnego, dzienników i innych plików systemowych.

Uruchom serwer WWW w katalogu piaskownicy, aby uniemożliwić dostęp do plików systemowych.

Unikaj odwoływania się w adresie URL do wszystkich typów plików innych niż sieciowe.

Uruchom procesy serwera WWW z najmniej wymaganymi uprawnieniami i przyznaj dostęp tylko do niezbędnego katalogu.

Wyklucz metaznaki podczas przetwarzania danych wprowadzanych przez użytkownika, aby zapewnić prawidłowe filtrowanie wejścia.

Zastosuj narzędzia do sprawdzania integralności plików, aby weryfikować zawartość sieci i wykrywać włamania.

Wykrywanie prób włamania na serwer WWW

Osoba atakująca, która uzyskuje dostęp do serwera sieciowego poprzez naruszenie bezpieczeństwa poprzez znane luki w zabezpieczeniach serwera sieciowego, może próbować zainstalować backdoory

(skrypty). Te backdoory umożliwiają atakującemu uzyskanie dostępu, przeprowadzanie ataków phishingowych lub wysyłanie wiadomości e-mail ze spamem. Ofiara pozostaje nieświadoma ataku na serwer WWW, dopóki serwer nie zostanie umieszczony na czarnej liście spamu lub dopóki atakujący nie przekieruje odwiedzających docelowej witryny hostowanej na serwerze sieciowym do innej witryny. W związku z tym atak na serwer WWW jest trudny do wykrycia, chyba że wystąpią takie złośliwe zdarzenia. Do czasu wystąpienia tych zdarzeń może być za późno na reakcję, ponieważ atakującemu już się udało. Dlatego wymagany jest mechanizm wykrywania próby włamania do serwera WWW na jego wczesnym etapie, aby zapobiec uszkodzeniu serwera WWW. Gdy osoba atakująca instaluje backdoora na serwerze sieciowym, rozmiar plików zainfekowanych tym backdoorem automatycznie się zwiększa. System wykrywania zmian w witrynie internetowej (WDS) to skrypt działający na serwerze w celu wykrycia zmian wprowadzonych w dowolnym pliku wykonywalnym lub obecności nowego pliku na serwerze internetowym, takiego jak HTML, JavaScript (JS), PHP, Active Server Pages (ASP), Perl i Python. Działa poprzez okresowe porównywanie wartości skrótu plików na serwerze z ich odpowiednimi głównymi wartościami skrótu w celu wykrycia wszelkich zmian w bazie kodu. Jeśli wykryje jakąkolwiek zmianę na serwerze, ostrzega użytkownika, aby podjął niezbędne działania. Dzięki temu WDS pomaga w wykrywaniu prób włamań do serwera WWW na wczesnych etapach ataku. Na przykład DirectoryMonitor to zautomatyzowane narzędzie, które przegląda całe foldery internetowe, wykrywa wszelkie zmiany wprowadzone w bazie kodu i ostrzega użytkownika za pośrednictwem wiadomości e-mail.

Jak bronić się przed atakami na serwer WWW

Obrona przed atakami na serwer WWW obejmuje następujące elementy.

Porty

Regularnie monitoruj wszystkie porty na serwerze WWW, aby zapobiec niepotrzebnemu ruchowi w kierunku docelowego serwera WWW. Jeśli ruch nie jest monitorowany, docelowy serwer WWW będzie narażony na ataki złośliwego oprogramowania. Nie zezwalaj na publiczny dostęp do portu 80 dla HTTP lub do portu 443 dla HTTPS; ruch do tych portów powinien być ograniczony. Jeśli port 80 pozostanie otwarty, serwer będzie narażony na ataki DoS, które zużywają zasoby serwera. Ruch w intranecie powinien być szyfrowany lub ograniczony w celu zabezpieczenia serwera WWW. Atakujący próbują ukryć swoją tożsamość, fałszując adres IP legalnego użytkownika. Przetwarzając plik dziennika zabezpieczeń za pomocą reguły „odmów ten adres IP” w pliku zestawu reguł zapory sieciowej lub tworząc polecenie „routed blackhole”, system docelowy może bronić się przed atakami na serwer WWW.

Certyfikaty serwera

Certyfikaty serwera gwarantują bezpieczeństwo i są podpisane przez zaufany organ. Jednak osoba atakująca może naruszyć certyfikowane serwery przy użyciu sfałszowanych certyfikatów w celu przechwycenia bezpiecznej komunikacji, przeprowadzając ataki MITM. Istnieją różne techniki unikania takich ataków MITM. Oto niektóre z nich.

o Korzystaj z bezpośredniej walidacji certyfikatów.

o Korzystaj z nowatorskiego protokołu, który nie zależy od stron trzecich w zakresie walidacji certyfikatów.

o Zezwól domenom na bezpośrednie i bezpieczne sprawdzanie ich certyfikatów przy użyciu wcześniej ustanowione dane uwierzytelniające użytkownika.

o Użyj solidnej konstrukcji kryptograficznej, która usprawnia sprawdzanie tożsamości serwera i eliminuje ograniczenia rozwiązań innych firm.

o Upewnij się, że zakresy danych certyfikatu są ważne i że certyfikaty są używane zgodnie z ich przeznaczeniem.

o Upewnij się, że certyfikat nie został unieważniony i że klucz publiczny certyfikatu jest ważny aż do zaufanego urzędu głównego.

Maszyna, konfiguracja

Plik machine.config zapewnia mechanizm zabezpieczania informacji poprzez zmianę ustawień na poziomie komputera. Wpływa na wszystkie inne aplikacje. Plik machine.config zawiera ustawienia maszyny dla platformy .Net, które mają wpływ na bezpieczeństwo. Za pomocą pliku machine.config można wykonać następujące czynności:

o Upewnij się, że chronione zasoby są mapowane na HttpForbiddenHandler i że nieużywane HttpModules zostały usunięte

o Upewnij się, że śledzenie jest wyłączone <trace enable="false"/>, a kompilacje debugowania są wyłączone

o Sprawdź, czy błędy ASP.NET nie są zwracane do klienta

o Sprawdź ustawienia stanu sesji

o Bezpieczeństwo dostępu do kodu

W celu zapewnienia bezpieczeństwa dostępu do kodu można zastosować następujące środki.

o Wdrażaj praktyki bezpiecznego kodowania, aby uniknąć ujawnienia kodu źródłowego i ataków sprawdzających poprawność danych wejściowych.

o Ogranicz ustawienia zasad bezpieczeństwa dostępu kodu, aby upewnić się, że nie ma uprawnień do wykonywania kodu pobranego z Internetu lub intranetu.

o Skonfiguruj usługi IIS, aby odrzucały adresy URL, aby zapobiegać przechodzeniu przez ścieżki, blokuj polecenia systemowe i narzędzia z restrykcyjnymi listami kontroli dostępu (ACL) oraz instaluj nowe poprawki i aktualizacje.

o Jeśli cele nie zaimplementują zabezpieczeń dostępu do kodu na swoich serwerach WWW, istnieje możliwość wykonania złośliwego kodu.

Poniżej przedstawiono inne środki ochrony przed atakami na serwer WWW:

Zastosuj ograniczone listy ACL i zablokuj zdalną administrację rejestru.

Zabezpiecz SAM (tylko serwery autonomiczne).

Upewnij się, że ustawienia związane z bezpieczeństwem są odpowiednio skonfigurowane i że dostęp do pliku metabazy jest ograniczony za pomocą zaostrzonych uprawnień NTFS.

Usuń niepotrzebne filtry ISAPI (Internet Server Application Programming Interface) z serwera WWW.

Usuń wszystkie niepotrzebne udziały plików, w tym domyślne udziały administracyjne, jeśli nie są wymagane.

Zabezpiecz udziały za pomocą ograniczonych uprawnień NTFS.

Przenieś witryny i katalogi wirtualne do partycji innych niż systemowe i użyj uprawnień internetowych usług IIS, aby ograniczyć dostęp.

Usuń wszystkie niepotrzebne mapowania skryptów usług IIS dla opcjonalnych rozszerzeń plików, aby uniknąć wykorzystywania błędów w rozszerzeniach ISAPI, które obsługują te typy plików.

Włącz minimalny poziom audytu na serwerze internetowym i używaj uprawnień NTFS do ochrony plików dziennika.

Użyj dedykowanej maszyny jako serwera WWW.

Ostrożnie twórz mapowania adresów URL do serwerów wewnętrznych.

Nie instaluj serwera IIS na kontrolerze domeny.

Korzystaj ze śledzenia identyfikatora sesji po stronie serwera i dopasowuj połączenia za pomocą znaczników czasu, adresów IP itp.

Jeśli serwer bazy danych, taki jak Microsoft SQL Server, ma być używany jako baza danych zaplecza, zainstaluj go na osobnym serwerze.

Korzystaj z narzędzi bezpieczeństwa dostarczanych z oprogramowaniem serwera WWW i skanerami, które automatyzują i upraszczają proces zabezpieczania serwera WWW.

Fizycznie chroń maszynę serwera WWW w bezpiecznej maszynowni.

Nie podłączaj serwera IIS do Internetu, dopóki nie zostanie w pełni zabezpieczony.

Nie zezwalaj nikomu na lokalne logowanie się do urządzenia poza administratorem.

Skonfiguruj osobne anonimowe konto użytkownika dla każdej aplikacji, jeśli hostowanych jest wiele aplikacji internetowych.

Ogranicz funkcjonalność serwera do obsługi tylko używanych technologii sieciowych.

Filtruj i filtruj przychodzące żądania ruchu.

Przechowuj pliki i skrypty witryn na osobnej partycji lub dysku.

Użyj skutecznej usługi ochrony przed botami, takiej jak DataDome, aby wykrywać botnety w czasie rzeczywistym.

Jak bronić się przed rozdzielaniem odpowiedzi HTTP i zatruwaniem pamięci podręcznej sieci

Podczas ustawiania plików cookie usuń znak powrotu karetki (CR) i znak nowego wiersza (LF) przed wstawieniem danych do nagłówka odpowiedzi HTTP. Najlepszą praktyką jest używanie produktów innych firm do testowania luk w zabezpieczeniach i obrony przed iniekcją CRLF. Upewnij się, że silniki aplikacji danych są aktualne.

Technika randomizacji portów źródłowych protokołu User Datagram Protocol (UDP) chroni serwery przed fałszowaniem odpowiedzi na ślepo. Ogranicz liczbę jednoczesnych zapytań rekurencyjnych i zwiększ czas życia (TTL) legalnych rekordów. Poniżej przedstawiono niektóre metody obrony przed atakami polegającymi na dzieleniu odpowiedzi HTTP i zatruwaniem pamięci podręcznej sieci:

Administrator serwera

o Używaj najnowszego oprogramowania serwera WWW

o Regularnie aktualizuj/poprawiaj system operacyjny i serwer WWW

o Uruchom skaner podatności na ataki sieciowe

Deweloperzy aplikacji

o Ogranicz dostęp aplikacji internetowej do unikalnych adresów IP

o Nie zezwalaj na znaki CR (%0d lub \r) i LF (%0a lub \n).

o Zgodność ze specyfikacją RFC 2616 dla protokołu HTTP/1.1

o Przeanalizuj wszystkie dane wprowadzone przez użytkownika lub inne formy kodowania przed użyciem ich w nagłówkach HTTP

Serwery proxy

o Unikaj dzielenia przychodzących połączeń TCP pomiędzy różnymi klientami

o Używaj różnych połączeń TCP z serwerem proxy dla różnych hostów wirtualnych

o Prawidłowo zaimplementuj „utrzymanie nagłówka hosta żądania".

Jak bronić się przed przejęciem DNS

Do obrony przed przejęciem DNS można zastosować następujące techniki:

Wybierz rejestratora akredytowanego przez Internet Corporation for Assigned Names and Numbers (ICANN) i zachęć go do ustawienia REGISTRAR-LOCK na nazwie domeny.

Chroń informacje o koncie rejestrującego.

Uwzględnij przejmowanie DNS w reagowaniu na incydenty i planowaniu ciągłości biznesowej.

Użyj narzędzi/usług monitorowania DNS, aby monitorować adres IP serwera DNS i ustawiać alerty.

Unikaj pobierania kodeków audio i wideo oraz innych programów do pobierania z niezaufanych witryn.

Zainstaluj program antywirusowy i regularnie go aktualizuj.

Zmień domyślne hasło routera.

Ogranicz transfery stref i używaj blokad skryptów w przeglądarce.

Rozszerzenia zabezpieczeń systemu nazw domen (DNSSEC): Dodaje dodatkową warstwę do DNS, która zapobiega włamaniom.

Zasady silnych haseł i zarządzanie użytkownikami: Stosowanie silnych haseł jeszcze bardziej zwiększa bezpieczeństwo.

Lepsze umowy dotyczące poziomu usług (SLA) od dostawców usług DNS: rejestrując serwery DNS u dostawców usług DNS, dowiedz się, z kim należy się kontaktować w przypadku wystąpienia problemu, jak uzyskać dobrą jakość odbioru i wsparcia oraz czy infrastruktura serwera DNS jest uodporniony na ataki.

Konfigurowanie serwera DNS master-slave w sieci: Użyj DNS master-slave i skonfiguruj serwer master bez dostępu do Internetu. Utrzymuj dwa serwery podrzędne, aby nawet jeśli atakujący zhakuje serwer podrzędny, będzie on aktualizowany tylko wtedy, gdy otrzyma aktualizację od serwera głównego.

Stałe monitorowanie serwerów DNS: Stałe monitorowanie serwerów DNS zapewnia, że nazwa domeny zwraca poprawny adres IP.

Zapewnij bezpieczeństwo routera: Zmień domyślną nazwę użytkownika i hasło routera. Aktualizuj oprogramowanie układowe, aby zapewnić bezpieczeństwo przed nowymi lukami w zabezpieczeniach.

Korzystaj z usługi VPN: Utwórz tunele szyfrowane za pomocą wirtualnej sieci prywatnej (VPN) do bezpiecznej prywatnej komunikacji przez Internet. Ta funkcja chroni wiadomości przed podsłuchem i nieautoryzowanym dostępem.

Korzystaj z usług ochrony zapory sieciowej, aby chronić oryginalne programy rozpoznawania nazw DNS i odfiltrowywać nieuczciwy ruch rozpoznawania nazw DNS.

Utrzymuj odpowiednie systemy ochrony, takie jak MFA i zabezpieczenia sprzętowe, aby zapewnić kontrolowany dostęp do serwera DNS.

Zainstaluj rozszerzenia blokujące skrypty w przeglądarce.

Używaj tylko bezpiecznych i renomowanych sieci VPN zamiast bezpłatnych usług VPN, które mogą śledzić Twoje działania i rejestrować je do wykorzystania w przyszłości.

Skanery bezpieczeństwa aplikacji internetowych

Hybryda Syhunta

Skaner Syhunt Hybrid automatyzuje testy bezpieczeństwa aplikacji internetowych i chroni infrastrukturę internetową organizacji przed zagrożeniami bezpieczeństwa aplikacji internetowych. Syhunt Dynamic indeksuje strony internetowe i wykrywa XSS, problemy między katalogami, wstrzykiwanie błędów, wstrzykiwanie kodu SQL, próby wykonania poleceń i kilka innych ataków. Syhunt Hybrid tworzy sygnatury w celu wykrywania luk w zabezpieczeniach aplikacji i zapobiega wylogowaniu. Analizuje JavaScript (JS), rejestruje podejrzane odpowiedzi i testuje błędy do przeglądu.

N-Stalker X

N-Stalker to skaner bezpieczeństwa aplikacji internetowych, który wyszukuje luki w zabezpieczeniach przed atakami, takimi jak clickjacking, iniekcja SQL i XSS. Umożliwia indeksowanie pająka w całej aplikacji i tworzenie makr sieciowych do uwierzytelniania formularzy. Zapewnia również możliwości proxy dla ataków typu „drive-thru" i identyfikuje komponenty za pomocą odwrotnych serwerów proxy, które dystrybuują różne platformy w tym samym adresie URL aplikacji.

Poniżej przedstawiono kilka dodatkowych skanerów bezpieczeństwa aplikacji internetowych:

Invicti (https://www.invicti.com)

Burp Suite (https://www.portswigger.net)

Wapiti (https://wopiti-sconner.github.io)

WebScarab (https://www.owosp.org)

WPSec (https://wpsec.com)

Tinfoil Security (https://www.tinfoilsecurity.com)

Skipfish (https://code.google.com)

Detectify (https://detectify.com)

Fortify on Demand (https://www.microfocus.com)

OWASP Zed Attack Proxy (ZAP) (https://www.zaproxy.org)

SonarQube (https://www.sonarqube.org)

Arachni (https://www.arachni-scanner.com)

w3af (https://w3af.org)

Grabber (http://rgaucher.info)

Vega (https://subgraph.com)

Skanery bezpieczeństwa serwera WWW

Qualys Community Edition

Qualys Community Edition wykrywa zasoby IT, zarządza lukami w zabezpieczeniach, skanuje aplikacje internetowe i utrzymuje inwentaryzację zasobów w chmurze. Oferuje zarządzanie lukami w zabezpieczeniach, aby identyfikować niebezpieczne błędy i natychmiast je naprawiać. Qualys może również oceniać luki w całej wewnętrznej infrastrukturze IT, a także w zewnętrznych zasobach, aby zapewnić bezpieczeństwo.

Poniżej przedstawiono kilka dodatkowych skanerów bezpieczeństwa serwera WWW:

Observatory (https://observotory.mozillo.org)

WordPress Security Scan (https://hockertorget.com)

Web Vulnerability Scanner (https://pentest-tools.com)

Nikto2 (https://cirt.net)

ImmuniWeb (https://www.immuniweb.com)

Narzędzia do monitorowania infekcji złośliwym oprogramowaniem serwera sieci Web

Wykrywanie złośliwego oprogramowania QualysGuard

QualysGuard Malware Detection umożliwia organizacjom proaktywne skanowanie ich stron internetowych w poszukiwaniu złośliwego oprogramowania oraz zapewnia automatyczne alerty i szczegółowe raporty, aby umożliwić szybką identyfikację i rozwiązanie problemu. Umożliwia organizacjom ochronę klientów przed infekcjami złośliwym oprogramowaniem i ochronę reputacji marki.

Poniżej przedstawiono kilka dodatkowych narzędzi do monitorowania infekcji złośliwym oprogramowaniem serwera WWW:

Sucuri SiteCheck (https://sucuri.net)

Usuwanie złośliwego oprogramowania SiteLock (https://www.sitelock.com)

Quttera (https://quttera.com)

Web Inspecktor (https://www.webinspector.com)

SiteGuarding (https://www.siteguarding.com)

Narzędzia bezpieczeństwa serwera WWW

Fortify Weblnspect to zautomatyzowane rozwiązanie do testów dynamicznych, które wykrywa problemy z konfiguracją, a także identyfikuje i nadaje priorytety lukom w zabezpieczeniach uruchomionych aplikacji. Naśladuje rzeczywiste techniki hakerskie i zapewnia wszechstronną dynamiczną analizę złożonych aplikacji i usług internetowych. Pulpity nawigacyjne i raporty Weblnspect zapewniają organizacjom widoczność i dokładną ocenę ryzyka swoich aplikacji.

Oto kilka dodatkowych narzędzi zabezpieczających serwer WWW:

Acunetix Web Vulnerability Scanner (https://www.ocunetix.com)

NetlQ Secure Configuration Manager (https://www.netiq.com)

SAINT Security Suite (https://www.corson-soint.com)

Sophos Intercept X for Server (https://www.sophos.com)

UpGuard (https://www.upguord.com)

Narzędzia do testowania piórem serwerów sieciowych

CORE Impact

CORE Impact znajduje luki w zabezpieczeniach serwera internetowego organizacji. To narzędzie pozwala użytkownikowi ocenić stan bezpieczeństwa serwera WWW przy użyciu tych samych technik, które są obecnie stosowane przez cyberprzestępców. Skanuje w poszukiwaniu możliwych luk w zabezpieczeniach serwera WWW, importuje wyniki skanowania i uruchamia exploity w celu przetestowania zidentyfikowanych luk. Może również skanować serwery sieciowe, stacje robocze, zapory ogniowe, routery i różne aplikacje w poszukiwaniu luk w zabezpieczeniach; zidentyfikować, które luki stanowią realne zagrożenie dla sieci; określić potencjalny wpływ wykorzystywanych podatności; ustalać priorytety i wykonywać wysiłki naprawcze.

Oto kilka dodatkowych narzędzi do testowania pióra serwera WWW:

Immunity CANVAS (https://www.immunityinc.com)

Arachni (https://www.orochni-sconner.com)

WebSurgery (https://sunrisetech.gr)

Mitmprox (https://mitmproxy.org)

Webalizer (https://webolizer.net)

Zarządzanie poprawkami

Deweloperzy zawsze próbują znaleźć błędy w serwerze WWW i je naprawić. Poprawki błędów są dystrybuowane w postaci łatek, które zapewniają ochronę przed znanymi lukami w zabezpieczeniach. Niezałatane lub wrażliwe łatki mogą stworzyć lukę w zabezpieczeniach serwera WWW. W tej sekcji opisano rolę łatek, aktualizacji i poprawek w zabezpieczaniu serwerów WWW. Ta sekcja zawiera

również wskazówki dotyczące wyboru odpowiednich poprawek, uaktualnień, poprawek i ich odpowiednich źródeł i bezpieczne zarządzanie poprawkami.

Łatki i poprawki

Łatka to niewielka część oprogramowania zaprojektowana w celu naprawienia problemów, luk w zabezpieczeniach i błędów, a także poprawy użyteczności lub wydajności programu komputerowego lub danych pomocniczych. Łatkę można uznać za naprawę problemu programistycznego. Luka w oprogramowaniu to słabość programu, która czyni go podatnym na ataki złośliwego oprogramowania. Dostawcy oprogramowania dostarczają łatki, które zapobiegają nadużyciom i zmniejszają prawdopodobieństwo zagrożeń wykorzystujących określoną lukę w zabezpieczeniach. Łatki obejmują poprawki i aktualizacje wielu znanych błędów lub problemów. Poprawka to publicznie opublikowana aktualizacja, dostępna dla wszystkich klientów. System bez łatek jest znacznie bardziej podatny na ataki niż system regularnie łatany. Jeśli osoba atakująca może zidentyfikować lukę, zanim zostanie ona naprawiona, system może być podatny na ataki złośliwego oprogramowania. Poprawka to pakiet używany do rozwiązania krytycznego defektu w aktywnym środowisku i zawiera poprawkę dotyczącą pojedynczego problemu. Aktualizuje określoną wersję produktu. Poprawki zapewniają szybkie rozwiązania i zapewniają rozwiązanie problemów. Zastosuj poprawki do poprawek oprogramowania w systemach produkcyjnych. Dostawcy informują użytkowników o najnowszych poprawkach za pośrednictwem poczty elektronicznej lub udostępniają je na swojej oficjalnej stronie internetowej. Poprawki to aktualizacje, które rozwiązują określony problem klienta i nie zawsze są rozpowszechniane poza organizacją klienta. Dostawcy czasami dostarczają poprawki w postaci zestawu poprawek, nazywanego połączoną poprawką lub dodatkiem Service Pack.

Co to jest PatchManagement?

Według https://www.techtarget.com/searchenterprisedesktop/ zarządzanie poprawkami to obszar zarządzania systemami, który obejmuje pozyskiwanie, testowanie i instalowanie wielu poprawek (zmian kodu) w administrowanym systemie komputerowym. Zarządzanie poprawkami to metoda obrony przed lukami w zabezpieczeniach, które powodują luki w zabezpieczeniach lub uszkodzenie danych. Jest to proces skanowania pod kątem luk w zabezpieczeniach sieci, wykrywania pominiętych poprawek bezpieczeństwa i poprawek, a następnie wdrażania odpowiednich poprawek, gdy tylko będą dostępne w celu zabezpieczenia sieci. Obejmuje następujące zadania:

Wybieranie, weryfikowanie, testowanie i stosowanie poprawek

Aktualizowanie wcześniej zastosowanych poprawek bieżącymi poprawkami

Lista poprawek zastosowanych wcześniej do bieżącego oprogramowania

Repozytoria nagrań lub magazyny łat dla łatwego wyboru

Przypisywanie i wdrażanie zastosowanych poprawek

Zautomatyzowany proces zarządzania poprawkami obejmuje następujące kroki.

Wykryj: Użyj narzędzi do wykrywania brakujących poprawek bezpieczeństwa.

Oceń: ocenia problem(y) i związaną z nim dotkliwość poprzez łagodzenie czynników, które mogą mieć wpływ na decyzję.

Zdobądź: Pobierz poprawkę do testów.

Test: Najpierw zainstaluj poprawkę na komputerze testowym, aby zweryfikować konsekwencje aktualizacji.

Wdrożenie: Wdróż poprawkę na komputerach i upewnij się, że nie wpłynie to na aplikacje.

Zachowaj: Zapisz się, aby otrzymywać powiadomienia o lukach w zabezpieczeniach, gdy zostaną one zgłoszone.

Instalacja Patcha

Instalacja poprawki obejmuje następujące zadania.

Identyfikowanie odpowiednich źródeł aktualizacji i poprawek

Ważne jest, aby zidentyfikować odpowiednie źródła aktualizacji i poprawek. Łatki i aktualizacje, które nie są instalowane z zaufanych źródeł, mogą sprawić, że serwer docelowy będzie jeszcze bardziej podatny na ataki, zamiast wzmacniać jego zabezpieczenia. Dlatego wybór odpowiednich źródeł aktualizacji i poprawek odgrywa kluczową rolę w zabezpieczaniu serwerów WWW. Poniżej przedstawiono niektóre metody identyfikowania odpowiednich źródeł aktualizacji i poprawek.

o Utwórz plan zarządzania poprawkami, który pasuje do środowiska operacyjnego i celów biznesowych.

o Znajdź odpowiednie aktualizacje i poprawki na stronach domowych aplikacji lub dostawców systemów operacyjnych.

o Zalecaną metodą śledzenia problemów związanych z proaktywnym instalowaniem poprawek jest zarejestrowanie się w witrynach głównych w celu otrzymywania alertów.

Instalacja Patcha

Użytkownicy mogą uzyskiwać dostęp do poprawek bezpieczeństwa i instalować je za pośrednictwem sieci World Wide Web. Patche można zainstalować na dwa sposoby.

o Instalacja ręczna

W tej metodzie użytkownik pobiera poprawkę od dostawcy i instaluje ją.

o Automatyczna instalacja

W tej metodzie aplikacje korzystają z funkcji automatycznej aktualizacji, aby aktualizować się samodzielnie.

Implementacja i weryfikacja poprawki bezpieczeństwa lub aktualizacji

o Przed zainstalowaniem jakiejkolwiek poprawki sprawdź źródło.

o Użyj odpowiedniego programu do zarządzania poprawkami, aby sprawdzić poprawność wersji plików i sum kontrolnych przed wdrożeniem poprawek bezpieczeństwa.

o Narzędzie do zarządzania poprawkami musi być w stanie monitorować załatane systemy,

o Zespół zarządzający poprawkami powinien regularnie sprawdzać dostępność aktualizacji i poprawek.

Narzędzia do zarządzania poprawkami

GFI LanGuard

Oprogramowanie do zarządzania poprawkami GFI LanGuard automatycznie skanuje sieć użytkownika, a także instaluje i zarządza poprawkami bezpieczeństwa i niezwiązanymi z bezpieczeństwem. Obsługuje komputery z systemami operacyjnymi Microsoft®, MAC OS X® i Linux®, a także wiele aplikacji innych firm. Umożliwia automatyczne pobieranie brakujących poprawek, a także ich wycofywanie, co skutkuje spójnie skonfigurowanym środowiskiem, które jest chronione przed zagrożeniami i lukami w zabezpieczeniach.

Oto kilka dodatkowych narzędzi do zarządzania poprawkami:

Symantec Client Management Suite (https://www.broadcom.com)

Solarwinds Patch Manager (https://www.solarwinds.com)

Kaseya Patch Management (https://www.kaseya.com)

Software Vulnerability Manager (https://www.flexera.com)

Ivanti Patch for Endpoint Manager (https://www.ivanti.com)

Podsumowanie modułu

W tym module szczegółowo omówiliśmy ogólne pojęcia związane z serwerami WWW; różne zagrożenia i ataki na serwer WWW; metodologia ataku na serwer sieciowy, w tym gromadzenie informacji, śledzenie serwera sieciowego, dublowanie witryn internetowych, skanowanie pod kątem luk w zabezpieczeniach, przejmowanie sesji i hakowanie haseł do serwerów sieciowych; oraz różne narzędzia do hakowania serwerów WWW. Ponadto omówiliśmy różne środki zaradcze, które można zastosować, aby zapobiec próbom włamań do serwerów sieciowych przez cyberprzestępców. Omówiliśmy również, jak zabezpieczyć serwery WWW za pomocą różnych narzędzi bezpieczeństwa. Moduł zakończyliśmy szczegółową dyskusją na temat koncepcji zarządzania poprawkami. W następnym module szczegółowo omówimy, w jaki sposób osoby atakujące, w tym etyczni hakerzy i testerzy pióra, włamują się do aplikacji internetowych.