Trojany i backdoory to dwa sposoby, w jakie haker może uzyskać dostęp do systemu docelowego. Występują w wielu różnych odmianach, ale wszystkie mają jedną wspólną cechę: muszą być zainstalowane przez inny program lub użytkownik musi zostać oszukiwany w celu zainstalowania trojana lub backdoora w swoim systemie. Trojany i backdoory są potencjalnie szkodliwymi narzędziami w pakiecie narzędzi etycznego hakera i powinny być używane rozsądnie do testowania bezpieczeństwa systemu lub sieci. Wirusy i robaki mogą być równie destrukcyjne dla systemów i sieci, jak trojany i backdoory. W rzeczywistości wiele wirusów zawiera pliki wykonywalne trojana i może zainfekować system, a następnie stworzyć backdoor dla hakerów. Tu omówimy podobieństwa i różnice między trojanami, backdoorami, wirusami i robakami. Wszystkie te typy szkodliwego kodu lub złośliwego oprogramowania są ważne dla etycznych hakerów, ponieważ są powszechnie używane przez hakerów do ataków i narażania systemów.

Trojany i backdoory

Trojany i backdoory to typy złośliwego oprogramowania wykorzystywanego do infekowania i naruszania systemów komputerowych. Trojan to złośliwy program podszywający się jako coś łagodnego. W wielu przypadkach wydaje się, że trojan wykonuje pożądaną funkcję dla użytkownika, ale faktycznie umożliwia hakerom dostęp do systemu komputerowego użytkownika. Trojany są często pobierane wraz z innym programem lub pakietem oprogramowania. Po zainstalowaniu w systemie mogą spowodować kradzież i utratę danych, a także awarie lub awarie systemu. Trojany mogą być również używane jako punkty uruchamiania innych ataków, takich jak rozproszona odmowa usługi (DDoS). Wiele trojanów wykorzystuje się do manipulowania plikami na komputerze ofiary, zarządzania procesami, zdalnego uruchamiania poleceń, przechwytywania naciśnięć klawiszy, oglądania wyświetlanych obrazów i restartowania lub zamykania zainfekowanych hosty. Wyrafinowane trojany mogą łączyć się z inicjatorem lub ogłaszać infekcję trojana na kanale IRC (Internet Relay Chat). Trojany jeżdżą na plecach innych programów i są zwykle instalowane w systemie bez wiedzy użytkownika. Trojan może zostać wysłany do systemu ofiary na wiele sposobów, na przykład:

* Załącznik do komunikatora internetowego

* IRC

* Załącznik do wiadomości e-mail

* Udostępnianie plików NetBIOS

* Pobrany program internetowy

Wiele fałszywych programów rzekomo legalnych programów, takich jak freeware, narzędzia spyware -removal, optymalizatory systemu, wygaszacze ekranu, muzyka, zdjęcia, gry i filmy mogą instalować trojana w systemie, po pobraniu. Reklamy na stronach internetowych darmowych programów, plików muzycznych lub plików wideo zachęcają ofiarę do zainstalowania trojana; program ma wówczas dostęp do systemu na poziomie systemu docelowego, gdzie może być destrukcyjny i podstępny. Poniższa tabela zawiera listę typowych trojanów i ich domyślnych numerów portów.

Trojan	Protokół	Port
BackOrifice	UDP	31337 lub 31338
Deep Throat	UDP	2140 i 3150
NetBus	TCP	12345 i 12346

Whack-a-Mole	TCP	12361 i 12362
NetBus2	TCP	20034
GirlFriend	TCP	21544
Master's Paradise	TCP	3129, 40421, 40422, 40423 i 40426

Backdoor to program lub zestaw powiązanych programów, które haker instaluje w systemie docelowym, aby umożliwić dostęp do systemu w późniejszym czasie. Backdoor może zostać osadzony w złośliwym trojanie. Celem instalacji backdoora w systemie jest zapewnienie hakerom dostępu do systemu w dowolnym momencie. Kluczem jest to, że haker wie, jak dostać się do backdoora niewykryty i może go użyć do dalszego hakowania systemu i poszukiwania ważnych informacji. Dodawanie nowej usługi jest najczęstszą techniką ukrywania tylnych drzwi w systemie operacyjnym Windows. Przed instalacją backdoora, haker musi zbadać system, aby znaleźć usługi, które są uruchomione. Ponownie wykorzystanie dobrych technik gromadzenia informacji ma kluczowe znaczenie dla poznania, jakie usługi lub programy już działają w systemie docelowym. W większości przypadków haker instaluje backdoora, który dodaje nową usługę i nadaje jej niepozorną nazwę lub, jeszcze lepiej, wybiera usługę, która nigdy nie była używana i która jest aktywowana ręcznie lub całkowicie wyłączona. Ta technika jest skuteczna, ponieważ w przypadku próby hackowania administrator systemu zwykle koncentruje się na poszukiwaniu czegoś dziwnego w systemie, pozostawiając wszystkie istniejące usługi niezaznaczone. Technika backdoora jest prosta, ale skuteczna: haker może wrócić na maszynę z najmniejszą widocznością w dziennikach serwera. Usługa backdoor pozwala hakerowi na używanie wyższych uprawnień - w większości przypadków jako konta systemowego.

Trojany zdalne (RAT) to klasa tylnych drzwi, które umożliwiają zdalną kontrolę nad zaatakowaną maszyną. Dostarczają pozornie użyteczne funkcje dla użytkownika i jednocześnie otwierają port sieciowy na komputerze ofiary. Po uruchomieniu RAT zachowuje się jak plik wykonywalny, wchodząc w interakcje z pewnymi kluczami rejestru odpowiedzialnymi za uruchamianie procesów i czasami tworząc własne usługi systemowe. W przeciwieństwie do typowych backdoorów, RAT podłącza się do systemu operacyjnego ofiary i zawsze pakuje się w dwa pliki: plik klienta i plik serwera. Serwer jest zainstalowany na zainfekowanym komputerze, a klient jest używany przez intruza do kontrolowania zaatakowanego systemu. Programy RAT umożliwiają hakerowi przejęcie kontroli nad systemem docelowym w dowolnym momencie. W rzeczywistości jednym ze wskazań, że system został wykorzystany, jest nietypowe zachowanie systemu, takie jak poruszanie się myszy we własnym oknie lub wyskakujące okna pojawiające się w systemie bezczynności.

Słowo przestrogi dotyczące ćwiczeń z trojanami

Celowo opuściłem wszelkie ćwiczenia krok po kroku dotyczące trojanów i backdoorów, ponieważ nie chcę promować instalowania ich w systemach produkcyjnych i utraty danych. Jednak najlepszym sposobem nauczenia się korzystania z tych narzędzi i ich możliwości jest zainstalowanie ich i przetestowanie. Oto moje zalecenie, aby nauczyć się etycznych umiejętności hakowania za pomocą trojanów i backdoorów. Weź starszy komputer, którego nie masz zamiaru używać ponownie, lub kup drugi dysk twardy na laptopa (tak właśnie zrobiłem). Zainstaluj system operacyjny Windows bez włączonych dodatków Service Pack i aktualizacji. Nie instaluj żadnych programów antywirusowych ani zapór ogniowych. Następnym krokiem jest naprawdę zwariowana instalacja wszystkich trojanów, rootkitów i narzędzi backdoorów wymienionych tutaj. Umożliwi to naukę i testowanie narzędzi bez blokowania przez skanowanie antywirusowe lub osobistą zaporę ogniową, próbującą chronić

komputer. Po zakończeniu możesz ponownie zainstalować system Windows lub po prostu wyłączyć dysk twardy dla dysku głównego. Ostatnią propozycją, jeśli szukasz małego, niedrogiego komputera do użycia jako maszyna testowa, jest zakup niedrogiego netbooka z systemem Windows i używanie go do instalowania i testowania narzędzi.

Kanały Jawny i Tajny

Kanał jawny jest normalnym i legalnym sposobem komunikowania się programów w systemie komputerowym lub sieci. Ukryty kanał wykorzystuje programy lub ścieżki komunikacji w sposób, który nie był zamierzony. Trojany mogą używać ukrytych kanałów do komunikacji. Niektóre trojany klienckie używają ukrytych kanałów do wysyłania instrukcji do komponentu serwera w zaatakowanym systemie. To czasami utrudnia komunikację trojana, aby go rozszyfrować i zrozumieć. Niespodziewany system wykrywania włamań (IDS) wykrywający transmisję między trojanem a serwerem nie oznaczałby tego jako czegoś niezwykłego. Korzystając z ukrytego kanału, trojan może komunikować się lub "dzwonić do domu" niewykryty, a haker może wysyłać polecenia do składnika klienta niewykryte.

Korzystanie z ukrytego kanału

Jeremiah Denton, jeniec wojenny podczas wojny w Wietnamie, używał tajnego kanału do komunikowania się bez wiedzy porywaczy. Denton był przesłuchiwany przez japońskiego reportera telewizyjnego, a ostatecznie nagranie wideo z przesłuchania trafiło do Stanów Zjednoczonych. Gdy amerykańscy agenci wywiadowi oglądali taśmę, jeden z nich zauważył, że Denton mrugał w niezwykły sposób. Odkryli, że miga literami alfabetu Morse'a. Litery to T-O-R-T-U-R-E, a Denton mrugał nimi w kółko. Jest to rzeczywisty przykład tego, w jaki sposób można użyć ukrytego kanału do wysłania niewykrytego komunikatu komunikacyjnego. Innym przykładem użycia komputera do przekazywania informacji za pośrednictwem ukrytego kanału jest użycie cechy charakterystycznej pliku do dostarczania informacji, a nie samego pliku. Komputerowy przykład ukrytego kanału polega na utworzeniu pozornie niewinnego pliku komputerowego o 16 bajtach. Plik może zawierać dowolne dane, ponieważ nie jest to ważna informacja. Plik można następnie wysłać pocztą e-mail do innej osoby. Ponownie wydaje się to niewinne, ale prawdziwa komunikacja ma numer 16. Rozmiar pliku to ważne dane, a nie zawartość pliku.

Niektóre ukryte kanały opierają się na technice zwanej tunelowaniem, która pozwala na przenoszenie jednego protokołu na inny protokół. Tunelowanie protokołu ICMP (Internet Control Message Protocol) to metoda wykorzystania żądania echa ICMP i echa-odpowiedzi do przenoszenia dowolnego ładunku, którego atakujący może użyć, w celu ukradkowego dostępu do kontrolowanego systemu lub kontroli nad nim. Polecenie ping jest ogólnie przyjętym narzędziem do rozwiązywania problemów i korzysta z protokołu ICMP. Z tego powodu wiele routerów, przełączników, zapór ogniowych i innych urządzeń filtrujących pakiety zezwala na przesyłanie protokołu ICMP przez urządzenie. Dlatego ICMP jest doskonałym wyborem protokołów tunelowania.

Narzędzia hakerskie

Loki jest narzędziem hakerskim, które zapewnia dostęp do powłoki przez ICMP, co czyni go trudniejszym do wykrycia niż backdoory oparte na protokołach TCP lub UDP. Jeśli chodzi o sieć, w sieci przesyłanych jest szereg pakietów ICMP. Jednak haker naprawdę wysyła polecenia od klienta Loki i wykonuje je na serwerze.

Rodzaje trojanów

Trojany mogą być tworzone i wykorzystywane do przeprowadzania różnych ataków. Oto niektóre z najczęstszych typów trojanów:

Trojany zdalnego dostępu (RAT) : Służy do uzyskania zdalnego dostępu do systemu.

Trojany wysyłające dane : Używane do wyszukiwania danych w systemie i dostarczania danych do hakera.

Destrukcyjne trojany : Używane do usuwania lub uszkadzania plików w systemie.

Trojany typu "odmowa usługi" : Służy do uruchamiania ataku typu "odmowa usługi".

Trojany proxy : Służą do tunelowania ruchu lub ataków hakerskich za pośrednictwem innych systemów.

Trojany FTP : Używane do tworzenia serwerów FTP w celu kopiowania plików do systemu.

Oprogramowanie zabezpieczające : Trojany służące do zatrzymywania oprogramowania antywirusowego.

Jak działają Trojany z odwracaniem połączeń

Odwracające połączenie trojany umożliwiają atakującemu dostęp do komputera w sieci wewnętrznej z zewnątrz. Haker może zainstalować prosty program trojana w systemie w sieci wewnętrznej, takim jak odwrotny serwer powłoki WWW. Regularnie (zwykle co 60 sekund) wewnętrzny serwer próbuje uzyskać dostęp do zewnętrznego systemu nadrzędnego w celu pobrania poleceń. Jeśli atakujący wpisał coś w systemie głównym, to polecenie jest pobierane i wykonywane w systemie wewnętrznym. Odwrotny serwer powłoki WWW używa standardowego protokołu HTTP. Jest to niebezpieczne, ponieważ jest trudne do wykrycia: wygląda na to, że klient przegląda sieć z sieci wewnętrznej.

Narzędzia hakerskie

TROJ_QAZ to trojan, który zmienia nazwę pliku notatnika.exe na note.com a następnie kopiuje się jako plik notepad.exe do folderu Windows. Spowoduje to uruchomienie trojana za każdym razem, gdy użytkownik uruchomi Notatnik. Ma backdoora, którego zdalny użytkownik lub haker może użyć do połączenia się z komputerem i kontrolowania go za pomocą portu 7597. TROJ_QAZ infekuje także Rejestr tak, że jest ładowany za każdym razem, gdy uruchamiany jest system Windows. Tini to mały i prosty backdoor trojan dla systemów operacyjnych Windows. Nasłuchuje na na porcie 7777 i daje hakerowi zdalny wiersz polecenia w systemie docelowym. Aby połączyć się z serwerem Tini, haker telnetuje do portu 7777. Donald Dick to backdoor Trojan dla systemów operacyjnych Windows, który pozwala hakerowi na pełny dostęp do systemu przez Internet. Haker może czytać, pisać, usuwać lub uruchamiać dowolny program w systemie. Donald Dick zawiera również keylogger i parser rejestru i może wykonywać funkcje takie jak otwieranie lub zamykanie tacy CD-ROM. Atakujący wykorzystuje klienta do wysyłania poleceń do podsłuchiwanego przez ofiarę na predefiniowanym porcie. Donald Dick używa domyślnego portu 23476 lub 23477. NetBus jest trojanem Windows GUI i ma podobną funkcjonalność do Donalda Dicka. Dodaje klucz rejestru HKEY_CURRENT_USER \ NetBus Server i modyfikuje klucz HKEY_CURRENT_USER \ NetBus Server \ General \ TCPPort. Jeśli NetBus jest skonfigurowany do automatycznego uruchamiania, dodaje wpis rejestru o nazwie NetBus Server Pro w HKEY_LOCAL_MACHINE \ Software \ Microsoft \Windows \ CurrentVersion \ RunServices.

SubSeven to trojan, który może być skonfigurowany do powiadamiania hakera, gdy zainfekowany komputer łączy się z Internetem i może informować hakerów o systemie. Powiadomienie to może zostać wykonane przez sieć IRC, przez ICQ lub przez e-mail. SubSeven może spowolnić działanie

systemu i generować komunikaty o błędach w zainfekowanym systemie. Back Orifice 2000 to narzędzie do zdalnej administracji, za pomocą którego atakujący może kontrolować system poprzez połączenie TCP / IP za pomocą interfejsu GUI. Back Orifice nie pojawia się na liście zadań ani na liście procesów i kopiuje się do Rejestru, aby uruchamiał się przy każdym uruchomieniu komputera. Nazwa pliku, którą uruchamia, jest konfigurowalna, zanim zostanie zainstalowana. Back Orifice modyfikuje klucz egzystyczny HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ RunServices. Wtyczki BackOrifice dodają funkcje do programu BackOrifice. Wtyczki zawierają kryptograficznie silne szyfrowanie Triple DES, zdalny pulpit z opcjonalną kontrolą myszy i klawiatury, zaszyfrowane transfery plików metodą drag-and-drop, przeglądanie systemu plików typu Explorer, graficzne zdalne edytowanie rejestru, niezawodne protokoły komunikacyjne UDP i ICMP oraz ukrywanie Możliwości, które osiąga się za pomocą ICMP zamiast TCP i UDP. BoSniffer wydaje się być poprawką dla Back Orifice, ale w rzeczywistości jest serwerem Back Orifice z zainstalowaną wtyczką SpeakEasy. Jeśli BoSniffer.exe, plik wykonywalny BoSniffer, jest uruchamiany w systemie docelowym, próbuje zalogować się na wcześniej określony serwer IRC na kanale #BO_OWNED z losową nazwą użytkownika. Następnie przystępuje do ogłoszenia swojego adresu IP i niestandardowego komunikatu co kilka minut, aby społeczność hackerów mogła używać tego systemu jako zombie na przyszłe ataki. ComputerSpy Key Logger to program, który haker może wykorzystać do rejestrowania działań komputera na komputerze, takich jak odwiedzane strony internetowe; loginy i hasła dla ICQ, MSN, AOL, AIM i Yahoo! Messenger lub poczta internetowa; bieżące aplikacje, które są uruchomione lub wykonane; Czaty internetowe; i e-mail. Program może nawet wykonywać migawki całego pulpitu Windows w określonych odstępach czasu. Beast to trojan uruchamiany w pamięci przeznaczonej dla usługi WinLogon.exe. Po zainstalowaniu program wstawia się do Eksploratora Windows lub Internet Explorera. Jedną z najbardziej charakterystycznych cech Beasta jest to, że jest to trojan typu "wszystko w jednym", co oznacza, że klient, serwer i edytor serwera są przechowywane w tej samej aplikacji. CyberSpy to trojan telnet, który kopiuje się do katalogu systemowego Windows i rejestruje się w rejestrze systemowym, tak aby uruchamiał się za każdym razem, gdy zainfekowany system jest ponownie uruchamiany. Po wykonaniu tej czynności wysyła powiadomienie za pośrednictwem poczty elektronicznej lub ICQ, a następnie rozpoczyna słuchanie wcześniej określonego portu TCP / IP. Subroot to trojan zdalnej administracji, z którego haker może połączyć się z systemem ofiary na porcie TCP 1700. LetMeRule! jest trojanem zdalnego dostępu, który można skonfigurować do nasłuchu na dowolnym porcie w systemie docelowym. Zawiera wiersz polecenia, którego atakujący używa do kontrolowania systemu docelowego. Może usuwać wszystkie pliki w określonym katalogu, wykonywać pliki na zdalnym hoście lub przeglądać i modyfikować rejestr. Firekiller 2000 wyłącza programy antywirusowe i zapory programowe. Na przykład, jeśli program Norton AntiVirus znajduje się w trybie automatycznego skanowania na pasku zadań, a aktywowana jest zapora AtGuard, program zatrzymuje się zarówno po uruchomieniu, jak i powoduje, że oba instalacje nie nadają się do użytku na dysku twardym. Następnie należy je ponownie zainstalować, aby przywrócić ich funkcjonalność. Firekiller 2000 działa ze wszystkimi najważniejszymi programami zabezpieczającymi, w tym AtGuard, Norton AntiVirus i McAfee Antivirus. Programy Hard Drive Killer Pro oferują możliwość całkowitego i trwałego niszczenia wszystkich danych w dowolnym systemie DOS lub Windows. Program po uruchomieniu usuwa pliki i infekuje i restartuje system w ciągu kilku sekund. Po ponownym uruchomieniu wszystkie dyski twarde podłączone do systemu są formatowane w sposób nieodwracalny w ciągu jednej do dwóch sekund, niezależnie od rozmiaru dysku twardego

Jak działa trojan Netcat

Netcat to trojan używający interfejsu wiersza poleceń do otwierania portów TCP lub UDP w systemie docelowym. Haker może następnie telnetować się do tych otwartych portów i uzyskać dostęp do powłoki systemu docelowego. W ćwiczeniu 5.1 pokazano, jak korzystać z Netcat.

W przypadku etycznego hackera ważne jest, aby wiedzieć, jak korzystać z Netcat.

Ćwiczenie 5.1

Korzystanie z Netcat

Pobierz wersję Netcat dla swojego systemu. Istnieje wiele wersji Netcata dla wszystkich systemów operacyjnych Windows. Ponadto Netcat został pierwotnie opracowany dla systemu Unix i jest dostępny w wielu dystrybucjach Linuksa, w tym BackTrack.

Netcat musi działać zarówno na kliencie, jak i na serwerze. Strona serwera połączenia jest włączona przez atrybut -l i służy do utworzenia portu nasłuchiwania. Na przykład użyj następującego polecenia, aby włączyć detektor Netcat na serwerze:

nc -L -p 123 -t -e cmd.exe

Na kliencie Netcat uruchom następującą komendę, aby połączyć się z detektorem Netcat na serwerze:

nc <adres ip serwera> <port nasłuchiwania na serwerze>

Klient powinien wtedy mieć otwartą powłokę wiersza poleceń z serwera.

Nietypowe zachowanie systemu jest zwykle oznaką ataku trojana. Działania takie jakuruchamianie i uruchamianie programów bez inicjacji użytkownika; Otwieranie lub zamykanie szuflad CD-ROM; ustawienia tapet, tła lub wygaszacza ekranu zmieniają się same; ekran przesuwa się do góry nogami; a program przeglądarki otwierający dziwne lub nieoczekiwane strony internetowe jest oznaką ataku trojana. Każda akcja, która jest podejrzana lub nie została zainicjowana przez użytkownika, może wskazywać na atak trojana.

Wskazania wirusa lub trojana

Carrie używała swojego komputera w pracy i zauważyła, że komputer działa wolno. Gdy próbowała otwierać pliki w Microsoft Word, jej system wyświetlałby komunikat o błędzie, a następnie nie mogła używać pewnych funkcji w programie. W ciągu ostatnich 24 godzin nie otrzymała żadnych nowych wiadomości e-mail; zwykle otrzymywała około 50 wiadomości dziennie, więc wydawało się to nieco niezwykłe. Wreszcie, jej klient powiedział, że otrzymał duplikaty e-maili z jej ostatniego tygodnia, co wydawało się dziwne. Dlatego Carrie zadzwoniła do Johna, administratora sieci firmowej, i poprosiła go, aby spojrzał na jej komputer, aby ustalić, co powoduje spowolnienie komputera i inne problemy z programem Microsoft Outlook. John spojrzał na komputer Carrie i zauważył, że definicje wirusów miały 6 miesięcy. Program antywirusowy ciągle pojawiał się z oknami wskazującymi, że definicje wirusów były nieaktualne, ale Carrie po prostu je zignorowała i ciągle zamykała wyskakujące okna. John zaktualizował definicje antywirusowe i przeprowadził pełne skanowanie systemu. Program antywirusowy ustalił, że system został zainfekowany 114 wirusami i trojanami. Program antywirusowy był w stanie oczyścić infekcje i przywrócić komputer do poprzedniego niezainfekowanego stanu. John testował Microsoft Outlooka, aby upewnić się, że rzeczywiście działa, gdy zauważył kilka wiadomości e-mail od internetowych serwisów horoskopów, witryn rozrywkowych i stron internetowych z grami online. John usunął z komputera kilka wątpliwych programów. Najwyraźniej Carrie nie zdawała sobie sprawy, że tego typu pliki do pobrania mogą uszkodzić jej komputer. Oprogramowanie sieciowe do przesyłania aktualizacji wirusów do wszystkich stacji roboczych, sterowania sieciowego w celu zapobiegania instalowaniu nieautoryzowanego oprogramowania i szkolenia dotyczącego świadomości bezpieczeństwa użytkowników mogło zapobiec wystąpieniu tego incydentu.

Wrappery to pakiety oprogramowania, które mogą być używane do dostarczania trojana. wrapper wiąże prawidłowy plik z plikiem trojana. Zarówno legalne oprogramowanie, jak i trojan są łączone w jeden plik wykonywalny i instalowane podczas uruchamiania programu. Zasadniczo gry lub inne animowane instalacje są używane jako opakowania, ponieważ zabawiają użytkownika podczas instalowania trojana. W ten sposób użytkownik nie zauważa wolniejszego przetwarzania, które ma miejsce podczas instalowania trojana w systemie - użytkownik widzi tylko zainstalowaną prawidłową aplikację.

Narzędzia hakerskie

Graffiti to animowana gra, którą można owinąć trojanem. Bawi użytkownika animowaną grą, podczas gdy trojan instalowany jest w tle. Silk Rope 2000 to opakowanie, które łączy serwer BackOrifice z dowolną inną specyfikacją podanie. ELiTeWrap to zaawansowane opakowanie EXE dla systemu Windows używane do instalowania i uruchamiania programów. ELiTeWrap może utworzyć program instalacyjny w celu wyodrębnienia plików do katalogu i wykonać programy lub pliki wsadowe, które wyświetlają menu pomocy lub kopiują pliki w systemie docelowym. Icon Converter Plus to program konwersji, który tłumaczy ikony pomiędzy różnymi formatami. Osoba atakująca może użyć tego typu aplikacji do ukrycia złośliwego kodu lub trojana, aby użytkownicy zostali oszukani w celu wykonania go, sądząc, że jest to legalna aplikacja.

Trojan Construction Kit i Trojan Makers

Kilka narzędzi generujących trojany umożliwia hakerom tworzenie własnych trojanów. Takie zestawy narzędzi pomagają hakerom skonstruować trojany, które można dostosować. Te narzędzia mogą być niebezpieczne i mogą się wycofać, jeśli nie zostaną wykonane poprawnie. Nowe trojany tworzone przez hakerów zwykle mają dodatkową zaletę polegającą na przechodzeniu niewykrytym przez skanowanie antywirusowe i narzędzia do skanowania trojana, ponieważ nie pasują do żadnych znanych sygnatur. Niektóre zestawy trojanów dostępne na wolności to: Senna Spy Generator, Trojan Horse Construction Kit v2.0, Progenic Mail Trojan Construction Kit i Pandora's Box.

Trojan . Środki zaradcze

Większość komercyjnych programów antywirusowych ma funkcje anty-trojańskie, a także funkcje wykrywania i usuwania programów szpiegujących. Narzędzia te mogą automatycznie skanować dyski twarde podczas uruchamiania w celu wykrycia programów typu backdoor i trojanów, zanim mogą spowodować uszkodzenie. Po zainfekowaniu systemu trudniej go wyczyścić, ale można to zrobić za pomocą dostępnych na rynku narzędzi. Chociaż dostępnych jest kilka komercyjnych narzędzi do usuwania antywirusów lub trojanów, moją osobistą rekomendacją jest Norton Internet Security. Norton Internet Security obejmuje osobistą zaporę ogniową, system wykrywania włamań, oprogramowanie antywirusowe, antyspyware, antyphishing i skanowanie poczty e-mail. Norton Internet Security wyczyści większość trojanów również z systemu. Oprogramowanie zabezpieczające działa dzięki znanym sygnaturom złośliwego oprogramowania, takim jak trojany i wirusy. Naprawa szkodliwego oprogramowania odbywa się za pomocą definicji złośliwego oprogramowania. Podczas instalowania i używania jakiegokolwiek osobistego oprogramowania zabezpieczającego lub oprogramowania antywirusowego i anty-trojańskiego, musisz upewnić się, że oprogramowanie ma wszystkie aktualne definicje. Aby zapewnić dostępność najnowszych poprawek i poprawek, należy połączyć system z Internetem, aby oprogramowanie mogło stale aktualizować definicje i poprawki dotyczące złośliwego oprogramowania. Ważne jest, aby używać komercyjnych aplikacji do czyszczenia systemu zamiast bezpłatnych narzędzi, ponieważ wiele narzędzi do usuwania freeware może dalej infekować system. Ponadto wiele komercyjnych programów zabezpieczających zawiera komponent wykrywania włamań, który będzie monitorował port i może identyfikować porty, które zostały otwarte

lub pliki, które uległy zmianie. Kluczem do zapobiegania instalowaniu trojanów i backdoorów w systemie jest informowanie użytkowników, aby nie instalowali aplikacji pobranych z Internetu ani nie otwierali załączników wiadomości e-mail od stron, których nie znają. Wielu administratorów systemu nie daje użytkownikom uprawnień systemowych niezbędnych do zainstalowania programów w ich systemie z tego właśnie powodu. Prawidłowe korzystanie z technologii internetowych powinno być uwzględnione w regularnych szkoleniach na temat świadomości bezpieczeństwa pracowników.

Monitorowanie portów i narzędzia do wykrywania koni trojańskich

Fport zgłasza wszystkie otwarte porty TCP / IP i UDP i odwzorowuje je na aplikację będącą właścicielem. Możesz użyć fport, aby szybko zidentyfikować nieznane otwarte porty i związane z nimi aplikacje. TCPView to program systemu Windows, który wyświetla szczegółowe wykazy wszystkich punktów końcowych TCP i UDP w systemie, w tym adresy lokalne i zdalne oraz stan połączeń TCP. Po uruchomieniu TCPView wylicza wszystkie aktywne punkty końcowe TCP i UDP, rozdzielając wszystkie adresy IP na ich wersje nazw domen. PrcView to narzędzie przeglądarki procesów, które wyświetla szczegółowe informacje o procesach działających pod kontrolą systemu Windows. PrcView zawiera wersję wiersza polecenia, za pomocą której możesz pisać skrypty sprawdzające, czy proces jest uruchomiony, a jeśli tak, to go zabić. Inzider to przydatne narzędzie, które wymienia procesy w systemie Windows i porty, z których każdy nasłuchuje. Inzider może wykryć niektóre trojany. Na przykład BackOrifice wstrzykuje się do innych procesów, więc nie jest widoczny w Menedżerze zadań jako oddzielny proces, ale ma otwarty port, na którym nasłuchuje. Tripwire weryfikuje integralność systemu. Automatycznie oblicza skróty kryptograficzne wszystkich kluczowych plików systemowych lub dowolnego pliku, który ma być monitorowany pod kątem modyfikacji. Oprogramowanie Tripwire działa, tworząc bazową migawkę systemu. Okresowo skanuje te pliki, ponownie oblicza informacje i widzi, czy którakolwiek z informacji uległa zmianie. Jeśli nastąpiła zmiana, oprogramowanie wywołuje alarm. Dsniff to zbiór narzędzi używanych do audytu sieci i testowania penetracji. Dsniff, filesnarf, mailsnarf, msgsnarf, urlsnarf i WebSpy pasywnie monitorują sieć w poszukiwaniu interesujących danych, takich jak hasła, wiadomości e-mail i przesyłanie plików. Arpspoof, dnsspoof i macof ułatwiają przechwytywanie ruchu sieciowego normalnie niedostępnego dla atakującego z powodu przełączania warstwy 2. Sshmitm i webmitm realizują aktywne ataki man-in-the-middle przeciwko przekierowanym sesjom Secure Shell (SSH) i HTTP Over SSL (HTTPS), wykorzystując słabe powiązania w infrastrukturze klucza publicznego (PKI) ad hoc.

Sprawdzanie systemu za pomocą weryfikacji plików systemowych

System Windows 2003 zawiera funkcję o nazwie Ochrona plików systemu Windows (WFP), która zapobiega zastępowaniu chronionych plików. WFP sprawdza integralność pliku, gdy próbuje się zastąpić plik SYS, DLL, OCX, TTF lub EXE. Gwarantuje to, że tylko pliki zweryfikowane przez Microsoft są używane do zastąpienia plików systemowych. Kolejne narzędzie, sigverif, sprawdza, jakie pliki Microsoft podpisał cyfrowo w systemie. W ćwiczeniu 5.2 użyjemy tego narzędzia.

Ćwiczenie 5. 2

Weryfikacja podpisu

Uruchomimy sigverif, sprawdzanie poprawności podpisu i porównamy wyniki z aktualnie działającymi procesami w Menedżerze zadań:

1. Naciśnij Ctrl + Alt + Del i wybierz Uruchom Menedżera zadań.

2. Kliknij kartę Procesy. Zwróć uwagę na wszelkie nietypowe procesy i czas procesora, z którego korzystają. Wszelkie procesy wykorzystujące stale wysoki procent czasu procesora mogą wskazywać na wirusa lub infekcję trojana.

3. Kliknij kartę Wydajność w Menedżerze zadań, aby wyświetlić bieżące użycie procesora.

4. Kliknij Start → Uruchom

5. Wpisz sigverif i kliknij Start.

6. W programie sigverif wybierz Zaawansowane, aby wyświetlić raport weryfikacji podpisu.

7. Kliknij przycisk Wyświetl dziennik, aby wyświetlić raport.

System File Checker to kolejne narzędzie oparte na wierszu poleceń służące do sprawdzania, czy program trojański zastąpił pliki. Jeśli Kontroler plików systemowych wykryje, że plik został nadpisany, pobiera znany, dobry plik z folderu Windows \ system32 \ dllcache i zastępuje niezweryfikowany plik. Polecenie uruchomienia System File Checker to sfc / scannow.

Wirusy i robaki

Wirusy i robaki mogą być używane do infekowania systemu i modyfikowania systemu, aby umożliwić hakerowi uzyskanie dostępu. Wiele wirusów i robaków zawiera trojany i backdoory. W ten sposób wirus lub robak jest nośnikiem i pozwala szkodliwemu kodowi, takim jak trojany i backdoory, przenosić się z systemu na system w taki sposób, że kontakt między ludźmi umożliwia rozprzestrzenianie się zarazków. Wirus i robak są podobne pod tym względem, że oba są formami złośliwego oprogramowania (malware). Wirus infekuje inny plik wykonywalny i używa tego programu do rozprzestrzeniania się. Kod wirusa jest wstrzykiwany do wcześniej niezłośliwego programu i rozprzestrzenia się, gdy program jest uruchamiany. Przykładami programów obsługujących wirusy są makra, gry, załączniki do wiadomości e-mail, skrypty Visual Basic i animacje. Robak jest pod wieloma względami podobny do wirusa, ale nie potrzebuje programu przewoźnika. Robak może sam się replikować i przenosić się z zainfekowanego hosta na inny host. Robak rozprzestrzenia się z systemu do systemu automatycznie, ale wirus potrzebuje innego programu, aby się rozprzestrzeniać. Wirusy i robaki wykonują się bez wiedzy lub pożądania użytkownika końcowego.

Rodzaje wirusów

Wirusy są klasyfikowane według dwóch czynników: co infekują i jak infekują. Wirus może zainfekować następujące składniki systemu:

* Sektory systemowe

* Pliki

* Makra (takie jak makra Microsoft Word)

* Pliki towrzyszące (obsługujące pliki systemowe, takie jak pliki DLL i INI)

* Klastry dyskowe

* Pliki Batch (pliki BAT)

* Kod źródłowy

Wirus infekuje poprzez interakcję z systemem zewnętrznym. Wirusy muszą być przenoszone przez inny program wykonywalny. Dołączając się do łagodnego pliku wykonywalnego wirus może

rozprzestrzeniać się dość szybko, ponieważ użytkownicy lub system uruchamiają plik wykonywalny. Wirusy są klasyfikowane zgodnie z ich techniką infekcji, w następujący sposób:

Wirusy polimorficzne : Wirusy te kodują kod w inny sposób w przypadku każdej infekcji i mogą się zmieniać w różne formy, aby uniknąć wykrycia.

Niewidzialne wirusy : Wirusy te ukrywają normalne cechy wirusów, takie jak modyfikowanie oryginalnego znacznika daty i daty pliku, aby zapobiec wykryciu wirusa jako nowego pliku w systemie.

Szybkie i powolne infekcje : Wirusy te mogą uniknąć wykrycia poprzez infekcję bardzo szybko lub bardzo powoli. Może to czasami umożliwić programowi zainfekowanie systemu bez wykrycia przez program antywirusowy.

Rzadkie infekcje : Wirusy te infekują tylko kilka systemów lub aplikacji.

Wirusy pancerne : Wirusy te są szyfrowane, aby zapobiec wykryciu.

Wirusy wieloczęściowe : Te zaawansowane wirusy powodują liczne infekcje.

Wirusy kosmiczne (Space-Filler) : Wirusy te dołączają się do pustych obszarów plików.

Wirusy tunelujące : Wirusy te są przesyłane za pośrednictwem innego protokołu lub szyfrowane, aby zapobiec wykryciu lub umożliwić przejście przez zaporę.

Wirusy zakamuflowane : Te wirusy wydają się być innym programem.

Wirusy NTFS i Active Directory : Wirusy te atakują system plików NT lub Active Directory w systemach Windows.

Osoba atakująca może napisać niestandardowy skrypt lub wirus, który nie zostanie wykryty przez programy antywirusowe. Ponieważ wykrywanie i usuwanie wirusów opiera się na sygnaturach programu, haker musi jedynie zmienić sygnaturę lub wygląd wirusa, aby zapobiec wykryciu. Sygnatura lub definicja wirusa to sposób, w jaki program antywirusowy jest w stanie określić, czy system jest zainfekowany przez wirusa. Dopóki wirus nie zostanie wykryty, a firmy antywirusowe mają szansę zaktualizować definicje wirusów, wirus nie zostanie wykryty. Dodatkowy czas może upłynąć, zanim użytkownik zaktualizuje program antywirusowy, dzięki czemu system będzie podatny na infekcję. Pozwala to osobie atakującej uniknąć wykrycia i usunięcia antywirusa na pewien czas. Krytycznym środkiem zaradczym dla infekcji wirusowej jest utrzymywanie aktualnych definicji wirusów w programie antywirusowym. Jednym z najbardziej długich wirusów był wirus Melissa rozprzestrzeniający się za pośrednictwem Microsoft Word Macros. Melissa zainfekowała wielu użytkowników, dołączając do dokumentu Word, a gdy plik został skopiowany lub wysłany pocztą elektroniczną, wirus rozprzestrzenił się wraz z plikiem. Oszustwa wirusowe to wiadomości e-mail wysyłane do użytkowników zazwyczaj z ostrzeżeniem o ataku wirusa. E-maile z fałszywym alarmem wirusowym zwykle zawierają dziwaczne stwierdzenia o szkodach, które mogą być spowodowane przez wirusa, a następnie oferują pobranie łaty naprawczej od znanych firm, takich jak Microsoft lub Norton. Inne fałszywe alarmy zalecają użytkownikom usunięcie pewnych krytycznych plików systemowych w celu usunięcia wirusa. Oczywiście, jeśli użytkownik zastosuje się do tych zaleceń, będą one z pewnością miały negatywne konsekwencje. Aby dowiedzieć się, czy wiadomość e-mail dotycząca wirusa jest prawidłowa, przejrzyj listę fałszerstw wirusów na stronie domowej home.mcafee.com/virusinfo.

Metody wykrywania wirusów

Do wykrywania wirusów wykorzystywane są następujące techniki:

* Skanowanie

* Sprawdzanie integralności za pomocą sum kontrolnych

* Przechwytywanie na podstawie sygnatury wirusów

Proces wykrywania i usuwania wirusów przebiega następująco:

1. Wykryj atak jako wirus. Nie wszystkie anormalne zachowania można przypisać wirusowi.

2. Śledź procesy za pomocą narzędzi, takich jak handle.exe, listdlls.exe, fport.exe, netstat.exe i pslist.exe, i porównaj podobieństwa między atakowanymi systemami.

3. Wykryj zawartość wirusa, szukając zmodyfikowanych, zastąpionych lub usuniętych plików. Nowe pliki, zmieniono atrybuty pliku lub pliki biblioteki współużytkowanej.

4. Pobierz wektor infekcji i wyizoluj go. Następnie zaktualizuj definicje antywirusowe i przeszukuj wszystkie systemy.

W ćwiczeniu 5.3 stworzymy wirusa testowego.

Ćwiczenie 5.3

Tworzenie wirusa testowego

Wirus testowy można utworzyć, wpisując poniższy kod w Notatniku i zapisując plik jako EICAR.COM. Twój program antywirusowy powinien odpowiedzieć, gdy spróbujesz go otworzyć, uruchomić lub skopiować.

X5O! P% @ AP [4 \ PZX54 (P ^) 7CC) 7} $ EICAR-STANDARD-ANTIVIRUS-TEST-FILE! $ H + H *

Robakom można zapobiec infekowaniu systemów w podobny sposób, jak wirusom. Robaki mogą być trudniejsze do zatrzymania, ponieważ rozprzestrzeniają się samodzielnie, co oznacza, że nie wymagają interwencji użytkownika w celu zainstalowania i dalszego rozprzestrzeniania szkodliwego oprogramowania. Robaki można wykryć za pomocą oprogramowania antywirusowego zawierającego definicje robaków. Worms, co najważniejsze, musi zostać powstrzymany przed rozprzestrzenianiem się. W tym celu administrator może wymagać wyłączenia systemów. Najlepszą metodą usuwania robaków z systemów sieciowych jest najpierw usunięcie komputera z sieci, a następnie uruchomienie oprogramowania zabezpieczającego w celu wyczyszczenia robaka.

Podsumowanie

Trojany, backdoory, wirusy i robaki to wszystkie formy złośliwego oprogramowania, które infekują systemy i albo powodują uszkodzenie danych, albo infekują system, aby haker mógł uzyskać dalszy dostęp do systemu. Rodzaje wirusów, sposoby ich infekowania i sposób ich użycia to cele przygorwania etycznego hakera. Najlepszym sposobem zapobiegania infekowaniu systemów przez złośliwe oprogramowanie jest zapewnienie, że oprogramowanie zabezpieczające Internet jest instalowane i aktualizowane na podstawie sygnatur i definicji wirusów i trojanów. Ponadto można uniknąć złośliwego oprogramowania dzięki przeszkoleniu użytkowników w zakresie bezpieczeństwa, aby uniemożliwić im otwieranie i uruchamianie plików, których nie znają lub nie mogą zweryfikować.

Do Zapamiętania!

* Zapoznałeś się z definicją trojana. Trojany to złośliwe fragmenty kodu przenoszone przez oprogramowanie do systemu docelowego.

* Dowiedziałeś się, co to jest ukryty kanał. Ukryty kanał wykorzystuje komunikację w sposób niezgodny z przeznaczeniem. Tunelowanie ICMP, odwrotna strona WWW i ataki typu "man-in-the -middle" są powszechnymi ukrytymi kanałami.

* Zapoznałeś się z definicją backdoora. Backdoor jest zazwyczaj składnikiem trojana. Służy do utrzymywania dostępu po wykryciu i usunięciu początkowego osłabienia systemu. Zwykle przyjmuje postać otwartego portu w systemie, który jest zagrożony.

* Dowiedziałeś się, czym jest trojan i jak działa. Trojany są używane głównie do zdobywania i zachowaj dostęp w systemie docelowym. Trojan często znajduje się głęboko w systemie i dokonuje zmian w rejestrze, które pozwalają mu osiągnąć cel, jakim jest zdalne narzędzie administracyjne.

* Poznałeś najlepsze środki zaradcze dla koni trojańskich. Świadomość i środki zapobiegawcze są najlepszą obroną przed trojanami.

* Dowiedziałeś się, jak wirus różni się od robaka. Wirusy muszą dołączać się do innych programów, a robaki rozprzestrzeniają się automatycznie.

* Poznałeś różne typy wirusów. Polimorficzne, ukryte, szybkie infekcje, powolne infekcje, rzadkie infekcje, opancerzone, wieloczęściowe, wgłębienia, tunelowanie, kamuflaż, NTFS i wirusy AD to wszelkiego rodzaju wirusy