ATAKI SIECIOWE I KOMPUTEROWE

Jako specjalista ds. bezpieczeństwa IT musisz być świadomy sposobów, w jakie intruz może zaatakować Twoją sieć. Ataki obejmują nieautoryzowane próby dostępu do zasobów lub systemów sieciowych, próby zniszczenia lub uszkodzenia informacji oraz próby uniemożliwienia autoryzowanym użytkownikom dostępu do zasobów. Musisz dobrze rozumieć zarówno bezpieczeństwo sieci, jak i bezpieczeństwo komputerowe. Bezpieczeństwo sieci obejmuje ochronę infrastruktury sieciowej, jak i samodzielnych systemów. Dlatego bezpieczeństwo komputerowe jest konieczne, aby chronić komputery i laptopy, które nie są częścią infrastruktury sieciowej, ale nadal zawierają ważne lub poufne informacje. Środki ochronne obejmują badanie bezpieczeństwa fizycznego (aż do sprawdzenia zamków w drzwiach) i ocenę ryzyka związanego z brakiem bezpieczeństwa fizycznego. Ten moduł daje Ci solidne podstawy dotyczące działań atakujących. Podobnie jak funkcjonariusze organów ścigania muszą być świadomi metod stosowanych przez przestępców, Ty musisz wiedzieć, co robią atakujący komputerowi. W jaki sposób atak typu „odmowa usługi" może zostać wykorzystany do zamknięcia firmy? W jaki sposób robaki i wirusy mogą zostać wprowadzone do korporacyjnej bazy danych firmy? Jak można zabrać laptopa z biura, nie narażając się na ryzyko złapania lub zatrzymania intruza? Ten moduł przedstawia przegląd metod ataku i środków ochronnych. Aby zrozumieć znaczenie bezpieczeństwa fizycznego, dowiesz się również, że wykwalifikowany atakujący może otworzyć zamek w ciągu kilku sekund.

OPROGRAMOWANIE ZŁOŚLIWE (MALWARE)

Zazwyczaj ataki sieciowe są inicjowane w celu kradzieży danych, które mogą być wykorzystane lub sprzedane w celu osiągnięcia korzyści finansowych lub realizacji celów społeczno-politycznych. Ataki sieciowe zwykle koncentrują się na organizacjach i ich połączonych ze sobą komputerach stacjonarnych i serwerach, ale urządzenia osobiste (takie jak telefony komórkowe i inne urządzenia podłączone do Internetu) są również celem ataków i wykorzystania złośliwego oprogramowania. Złośliwe oprogramowanie to złośliwe oprogramowanie, takie jak wirus, robak lub program trojański, wprowadzone do sieci w celu pomocy atakującym w osiągnięciu ich celów. Granice między tymi kategoriami złośliwego oprogramowania zacierają się, a zaawansowane złośliwe oprogramowanie ma teraz bogatą funkcjonalność zależną od celu, która obejmuje wiele kategorii. Tabele w tym module pokazują złośliwe oprogramowanie obejmujące wiele kategorii. Wcześniej głównym celem złośliwego oprogramowania było niszczenie lub uszkadzanie danych lub wyłączanie sieci lub systemu komputerowego. Obecnie częściej celem jest zarabianie pieniędzy. Dziesiątki organizacji zajmujących się cyberprzestępczością ma magazyny pełne programistów, którzy nie robią nic poza pisaniem złośliwego oprogramowania z sygnaturami nieznanymi programom antywirusowym. Malware było kiedyś skierowane konkretnie na systemy Windows, Linux i inne tradycyjne systemy operacyjne. Teraz jest przeznaczone do atakowania tabletów, smartfonów i innych urządzeń podłączonych do Internetu. Poniższe sekcje obejmują różne typy złośliwego oprogramowania używanego przez atakujących. Rysunek 3-1 Wiadomość e-mail phishing

BAJTY BEZPIECZEŃSTWA

Specjaliści ds. bezpieczeństwa ustalili, że za atakiem SolarWinds w 2020 r. stała wysoce wyrafinowana grupa cyberprzestępców. Grupa ta, zwana Silverfish, korzystała z zasobów serwerów należących do innej organizacji cyberprzestępczej znanej jako EvilCorp. Eksperci oficjalnie nie zidentyfikowali kraju zaangażowanego w grupę Silverfish, ale wskazówki wskazują na Rosję. Kiedy uczysz się, jak korzystać z narzędzia bezpieczeństwa, pamiętaj, że cyberprzestępcy również uczą się, jak go używać. Z tego powodu organizacje potrzebują etycznych hakerów, którzy wiedzą, jak korzystać z narzędzi bezpieczeństwa, aby bronić się przed atakami cyberprzestępców.

Wirusy

Wirus to program, który dołącza się do pliku lub innego programu, często wysyłany pocztą elektroniczną. Kluczowym słowem jest „dołącza". Wirus nie istnieje samodzielnie, więc nie może się replikować ani działać bez obecności gospodarza. Wirus dołącza się do pliku lub programu gospodarza (takiego jak Microsoft Word), tak jak grypa dołącza się do organizmu gospodarza, a następnie wykonuje to, do czego został zaprojektowany przez twórcę. Nadawca wiadomości phishingowej wykorzystuje socjotechnikę, aby nakłonić użytkownika do kliknięcia linku do fałszywej witryny. Gdy użytkownik kliknie link, fałszywa witryna próbuje ukraść dane logowania ofiary i informacje o karcie kredytowej, jednocześnie pobierając złośliwy kod na komputer ofiary.

Ransomware, rodzaj wirusa, który blokuje system docelowy do czasu zapłacenia okupu, to rosnący trend wśród wirusów. Przez lata twórcy ransomware stali się bardziej wyrafinowani. Obecnie często można znaleźć wirusa ransomware, który przechwytuje dane uwierzytelniające do pamięci masowej w chmurze i uniemożliwia użytkownikom dostęp do tych kont, a także do plików na ich urządzeniach lokalnych. Zła wiadomość na temat wirusów jest taka, że nie ma niezawodnej metody zapobiegania ich przyłączaniu się do komputerów, niezależnie od tego, jak bardzo jesteś wykwalifikowany jako specjalista ds. bezpieczeństwa. Dostępnych jest wiele pakietów oprogramowania antywirusowego, ale żaden nie może zagwarantować ochrony, ponieważ nowe wirusy są stale tworzone. Oprogramowanie antywirusowe porównuje sygnatury (hasze lub wzorce kodu) i typowe złośliwe zachowania programowe (analiza heurystyczna) znanych wirusów z każdym plikiem na komputerze; jeśli istnieje zgodność, oprogramowanie ostrzega, że program lub plik jest zainfekowany. Te sygnatury są przechowywane w pliku sygnatur wirusów, który utrzymuje oprogramowanie antywirusowe. Jeśli jednak wirus nie jest znany, oprogramowanie antywirusowe nie wykrywa zgodności. Dlatego regularne aktualizowanie plików sygnatur wirusów jest kluczowe. Wiele pakietów oprogramowania antywirusowego oferuje automatyczne aktualizacje. Na przykład dzięki Symantec Endpoint Protection (SEP) administratorzy mogą skonfigurować serwer, który obsługuje wysyłanie aktualizacji antywirusowych na komputery klienckie w organizacji. Oprócz używania oprogramowania antywirusowego do zwalczania złośliwego oprogramowania, specjaliści ds. bezpieczeństwa używają urządzeń zabezpieczających sieć i sandboxingu. Urządzenia zabezpieczające sieć mogą monitorować całe sieci i przechwytywać złośliwe oprogramowanie, zanim dotrze ono do użytkowników. Sandboxing pozwala użytkownikom uruchamiać programy w bezpiecznym, odizolowanym obszarze operacyjnym, który zapobiega zapisywaniu złośliwych plików na dysku twardym. Sandboxing jest często używany przez specjalistów ds. bezpieczeństwa w celu bezpiecznego testowania, czy plik zawiera złośliwe oprogramowanie.

Opis wirusa

Ryuk Wirus ransomware. Ryuk był odpowiedzialny za ponad jedną trzecią wszystkich ataków ransomware w 2020 roku. Ryuk jest używany w atakach na firmy, szpitale i samorządy. Ryuk szyfruje krytyczne pliki i zazwyczaj żąda wielomilionowego okupu. FormBook FormBook to rodzina złośliwych programów, które kradną dane i przechwytują formularze. Próbuje ukraść zawartość Schowka systemu Windows, rejestrować to, co wpisujesz na klawiaturze, i kraść dane podczas przeglądania sieci. Jest sprzedawany jako „złośliwe oprogramowanie jako usługa" na forach hakerskich. Hakerzy mogą kupić subskrypcję i używać narzędzia FormBook. FormBook jest zwykle dystrybuowany za pośrednictwem wiadomości spamowych zawierających złośliwe załączniki. CryptoLocker CryptoLocker jest obecnie mniej rozpowszechniony, ale jest uważany za ojca wielu wirusów ransomware. CryptoLocker stał się terminem odnoszącym się do rodzin wirusów ransomware. W 2016 r. szacowano, że zainfekował ponad 250 000 komputerów. To złośliwe oprogramowanie blokuje pliki użytkownika w zaszyfrowanym kontenerze i wymaga od ofiary zapłacenia okupu za ich odszyfrowanie. Podobnie jak większość

złośliwego oprogramowania, jest ono dostarczane za pośrednictwem wiadomości e-mail, której celem jest nakłonienie użytkowników do kliknięcia złośliwego łącza lub załącznika. Po zainfekowaniu komputera ofiary mają określony czas na zapłacenie okupu, jeśli chcą odzyskać swoje pliki. Malware MalumPOS ma na celu urządzenia odpowiedzialne za przetwarzanie płatności, zwane systemami POS (point of sale). Wirus MalumPOS został użyty w połowie 2015 r. do atakowania urządzeń POS w sieciach hotelowych. Wirus ten został zaprogramowany do wyszukiwania, przechwytywania, kopiowania i eksfiltracji informacji o kartach płatniczych (np. numerów kart kredytowych/debetowych i innych informacji przechowywanych na pasku magnetycznym karty kredytowej). Ataki na POS były rzadkie w 2020 r., ale nowy szczep wydaje się być skierowany wyłącznie na informacje identyfikujące osobę, a nie pełne informacje o karcie płatniczej. Carbanak Ten wirus rozprzestrzenia się za pośrednictwem wiadomości e-mail phishing, które prawie zawsze są skierowane do instytucji finansowych. Te wiadomości e-mail phishing zawierają dokument Word i złośliwy plik .cpl. (Pamiętaj o tym podczas nadchodzącego ćwiczenia dekodowania base-64.) Kiedy po raz pierwszy uzyskuje dostęp do systemu, złośliwe oprogramowanie uruchamia szereg kontroli, aby upewnić się, że może uzyskać odpowiednie uprawnienia do dalszego ataku. Kiedy odpowiednie uprawnienia zostaną uzyskane lub zweryfikowane, złośliwe oprogramowanie otwiera tylne drzwi do kilku zdalnych serwerów pod kontrolą nieznanego (do tej pory) złośliwego podmiotu. To złośliwe oprogramowanie zostało wykorzystane do ułatwienia oszukańczych transakcji w systemach transferu środków i bankomatach instytucji finansowych.

This message was created automatically by mail delivery software. A message that you sent could not be delivered to one or more of its recipients. This is a permanent error. The following address (es) failed:

CustomerService@MSIGroupInc.com

This message has been rejected because it has a potentially executable attachment "Price.cpl"

This form of attachment has been used by recent viruses or other malware. If you meant to send this file then please package it up as a zip file and resend it.

[Message header deleted for brevity]

boundary="--------sghsfzfldbjbzqmztbdx"--------

sghsfzfldbj bzqmztbdx

Content-Type: text/html; charset="us-ascii"

Content-Transfer-Encoding: 7bit

<html><body>

:))

</body></html>

--------sghsfzfldbjbzqmztbdx

Content-Type: application/octet-stream; name="Price.cpl"

Content-Transfer-Encoding: base64

Content-Disposition: attachment; filename="Price.cpl"

TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAg

AAAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9TIG1vZGUuDQ0KJAAAAAAAAA

ABQRQAATAEDAA+kgUEAAAAAAAAAAOAADiELAQUMAAwAAAACAAAAAAAAAQBUAAAAQAAAAIAAAAAAAEAAQAAAAAgAABA

AAAAAAAAA

[Several pages of code cut for brevity]

Ten tajemniczy kod został zakodowany w bazie 64. Przypomnijmy, że baza 2 (binarna), baza 8 (ósemkowa) i baza 16 (szesnastkowa) to powszechne systemy liczbowe, których używają komputery. Baza 64 to kolejny system, który powinieneś znać. Uruchomienie dekodera bazy 64 w kodzie Price.cpl ujawnia następujący podejrzany kod programistyczny:

This program cannot be run in DOS mode.

user32.dll CloseHandle() CreateFileAb GetWindowsDirectory WriteFile

strcat kernel32.dll Shell Execute shell32 KERNEL32.DLL USER32.DLL

GetProcAddress LoadLibrary ExitProcess Virtual FreeMessageBox

Ten kod pokazuje, że w załączniku dzieje się coś podejrzanego. Pierwszy wiersz, „Ten program nie może być uruchomiony w trybie DOS", identyfikuje tekst, który następuje po nim jako program, który ostrzega, że załącznik e-mail zawiera ukryty program komputerowy. W trzecim wierszu wykonywana powłoka zwiększa podejrzaną naturę załącznika Price. cpl. Powłoka to wykonywalny fragment kodu programistycznego, który tworzy interfejs do systemu operacyjnego w celu wydawania poleceń systemowych i nie powinien pojawiać się w załączniku e-mail. Odwołania do User32.dll, a zwłaszcza Kernel32. dll, powinny również wzbudzić podejrzenia, ponieważ pliki bibliotek dołączanych dynamicznie (DLL) są plikami wykonywalnymi. Ponadto Kernel32.dll odpowiada za zarządzanie pamięcią i operacje wejścia/wyjścia, więc odwołanie do tego pliku w załączniku e-mail powinno wzbudzić więcej niż podejrzenia; powinno podnieść ciśnienie krwi. Możesz zobaczyć, że odrzucenie tej wiadomości e-mail przez dostawcę poczty e-mail było zasadne.

Aktywność 3-1: Identyfikowanie nowych wirusów komputerowych i robaków

Czas trwania: 30 minut

Cel: Zbadanie niektórych aktualnych zagrożeń wirusami komputerowymi.

Opis: Jako specjalista ds. bezpieczeństwa musisz być na bieżąco z wieloma nowymi wirusami i robakami, które mogą atakować sieci i komputery. Jeśli jeden komputer zostanie naruszony, wszystkie komputery w Twojej sieci mogą zostać naruszone. Wiele zapór sieciowych nie wykrywa złośliwego oprogramowania dołączonego do programu wykonywalnego lub makrowirusa (omówionego później w tej sekcji), więc specjaliści ds. bezpieczeństwa muszą przeszkolić użytkowników w zakresie zagrożeń związanych z instalowaniem oprogramowania, w tym gier i grafiki, na komputerze. Pamiętaj, że zapora sieciowa nie bada pakietów wewnątrz sieci, więc złośliwe oprogramowanie może rozprzestrzeniać się wewnątrz organizacji niezależnie od tego, jak skuteczna jest zapora. Dobrym miejscem do nauki o nowych zagrożeniach jest Internet.

1. Uruchom przeglądarkę internetową i przejdź do en.wikipedia.org.

2. Na stronie głównej wpisz Ryuk (ransomware) w polu wyszukiwania w prawym górnym rogu, a następnie kliknij lupę. Jaki jest prawdopodobny kraj pochodzenia tego złośliwego oprogramowania?

3. Podaj krótki opis oprogramowania ransomware Ryuk i sposoby ochrony przed nim.

4. Następnie przejdź do www.mcafee.com/enterprise/en-ca/threat-center.html.

5. Przewiń w dół, aż zobaczysz najnowszą listę zagrożeń cyberbezpieczeństwa.

6. Wypisz pięć najnowszych wirusów lub robaków wyświetlanych na tej stronie.

7. Wybierz jeden z wirusów lub robaków wymienionych w kroku 6. Podsumuj przegląd tego złośliwego oprogramowania. Które kraje są najbardziej dotknięte? Wymień i krótko opisz niektóre techniki wykorzystywane przez to złośliwe oprogramowanie do infekowania systemów. Czy istnieją jakieś rozwiązania chroniące systemy przed tym wirusem? Jeśli tak, to jakie?

8. Pozostaw przeglądarkę internetową otwartą do następnej aktywności

BAJTY BEZPIECZEŃSTWA

Specjaliści ds. bezpieczeństwa mają wiele źródeł informacji o aktualnych lukach lub możliwych atakach sieciowych. Możesz odwiedzić wiele doskonałych stron internetowych, aby dowiedzieć się więcej o lukach w zabezpieczeniach systemów operacyjnych i aplikacji. Jedną ze stron, którą każdy specjalista ds. bezpieczeństwa powinien dodać do zakładek w przeglądarce internetowej, jest witryna Common Vulnerabilities and Exposures firmy Mitre Corporation pod adresem cve.mitre.org. Inne pomocne strony to www.packetstormsecurity.com, www.exploit-db.com, www.securityfocus.com, Microsoft Security Bulletins , www .kb.cert.org/vuls i oczywiście www.google.com. Identyfikując wszystkie luki w zabezpieczeniach związane z systemami operacyjnymi i aplikacjami klienta, możesz określić, jakiego typu atak zastosować w sieci podczas przeprowadzania testu bezpieczeństwa. Możesz również odkryć lukę związaną z innym systemem operacyjnym, która może zostać wykorzystana do naruszenia bezpieczeństwa systemu operacyjnego klienta. Pamiętaj, aby myśleć nieszablonowo. Testowanie bezpieczeństwa to coś więcej niż zapamiętywanie narzędzi i reguł; opiera się w dużej mierze na kreatywności i wyobraźni.

UWAGA

Jedną z trudności w pisaniu o bezpieczeństwie sieci jest zróżnicowana terminologia używana przez profesjonalistów. Specjaliści ds. bezpieczeństwa czasami używają zamiennie terminów „luka” i „narażenie”. Podręcznik metodologii testowania bezpieczeństwa Open Source (OSSTMM) próbuje rozwiązać ten problem, ale dopóki wszystkie organizacje zawodowe nie przyjmą jednego standardu, niejednoznaczność będzie dominować.

Wirusy makro

Wirus makro to wirus zakodowany jako makro w programach obsługujących język programowania makro, taki jak Visual Basic for Applications (VBA). Na przykład możesz napisać makro, które jest zasadniczo listą poleceń, w programie Microsoft Word, które podświetla zawartość dokumentu (Ctrl1A), kopiuje wybrane dane (Ctrl1C), a następnie wkleja informacje do innej części dokumentu (Ctrl1V). Wirusy makro mogą być kodowane w celu wykonywania szeregu złośliwych działań, takich jak usuwanie ważnych plików, kradzież haseł i historii przeglądarki internetowej lub zezwalanie na zdalny

dostęp do urządzenia. Te polecenia można ustawić tak, aby uruchamiały się automatycznie zaraz po otwarciu pliku. Wirusy makro istnieją od dziesięcioleci. Aplikacje pakietu Microsoft Office, takie jak Word, Excel i Outlook, automatycznie podejmują środki w celu przeciwdziałania wirusom makro i zapobiegania ich uruchamianiu. Fakt, że oprogramowanie do zwiększania produktywności pilnie chroni przed wirusami makro, podkreśla, że nadal stanowią one wyraźne i obecne zagrożenie. Makrowirus, który po raz pierwszy zaatakował komputery Apple Mac w 2017 r., wstrzykując śmiercionośny kod do systemu operacyjnego, nadal infekuje społeczność użytkowników komputerów Mac. Najbardziej niesławnym makrowirusem jest Melissa, który pojawił się w 1999 r. Został zainicjowany po tym, jak użytkownik otworzył zainfekowany dokument; wirus wysłał następnie wiadomość e-mail do pierwszych 50 kontaktów, które znalazł w książce adresowej zainfekowanego komputera. Makrowirus jest przykładem ataku trojańskiego i służy jako konkretny przykład tego, jak złośliwy ładunek może zostać dostarczony do niczego niepodejrzewającego celu. W przeszłości wirusy były tworzone przez programistów, którzy uznali wyzwanie stworzenia destrukcyjnego programu za satysfakcjonujące. Dzisiaj nawet osoby niebędące programistami mogą łatwo tworzyć wirusy. W rzeczywistości każdy, kto ma dostęp do Internetu, może znaleźć wiele stron internetowych, na których można dowiedzieć się, jak krok po kroku stworzyć wirusa. Ten łatwy dostęp przyczynia się do problemów, z którymi musisz się zmierzyć jako specjalista ds. bezpieczeństwa. Przydatne jest wczucie się w sytuację przestępców komputerowych i, podobnie jak profiler FBI, próba zrozumienia ich sposobu myślenia. Dobrym miejscem na początek jest odwiedzenie stron internetowych twórców wirusów i sprawdzenie, co mają do powiedzenia. Na przykład wyszukiwanie w Google frazy „Macro Virus Tutorial" kieruje do wielu stron internetowych. Poniższy fragment pochodzi z http://web.textfiles.com/virus/mactut.txt i poprzedza instrukcje dotyczące tworzenia i używania makrowirusa w celu oczyszczenia autora z odpowiedzialności za niewłaściwe użycie. Chociaż tekst został napisany w połowie lat 90., nadal dokładnie odzwierciedla „pirackie" nastawienie niektórych twórców złośliwego oprogramowania. Gdybyś miał surfować po ciemnych rejonach sieci w poszukiwaniu złośliwego oprogramowania i narzędzi hakerskich, znalazłbyś podobne komentarze innych łobuzów oznaczających ich towary. Hakerzy i twórcy złośliwego kodu nie wykonują swojej pracy tylko dla pieniędzy; lubią też być pierwszymi, którzy naruszą lukę, a tym samym uzyskać restige i prawa do przechwałek.

LEGALESE

I SHALL NOT BE HELD RESPONSIBLE FOR ANY DAMAGE CREATED BE IT DIRECT OR INDIRECT USE OF THE PUBLICISED MATERIAL. THIS DOCUMENT IS COPYRIGHT 1996 TO ME, DARK NIGHT OF VBB. HEREWITH I GRANT ANYBODY LICENSE TO REDISTRIBUTE THIS DOCUMENT AS LONG AS IT IS KEPT IN WHOLE AND MY COPYRIGHT NOTICE IS NOT REMOVED. SO IF I FIND ANY LAMERS WHO JUST TAKE THE CODE PUBLISHED HERE AND SAY IT IS THEIR OWN I WILL SEE THAT THEY'LL BE PUNISHED. (BELIEVE IT OR NOT:-))!!! INTRODUCTION MANY OF YOU MAY BE WONDERING RIGHT NOW WHO I AM AND WHO VBB IS. COME ON LAMERS! GET ALIVE. VBB IS ONE OF THE COOLEST VIRUS GROUPS AROUND. YOU CAN'T TELL ME YOU'VE NEVER HEARD OF US. WELL, OK I'LL ADMIT IT. WE'RE NOT THAT POPULAR YET, BUT THAT'LL COME. SO FOR NOW HERE'S MY CONTRIBUTION TO THE GROUP AS THE LEADER. WELCOME TO THE MACROVIRUS WRITING TUTORIAL PART 1! ENJOY! ! THE TOOLS FIRST OF ALL YOU'LL NEED MS WORD 6.0 OR UP (DUH), THEN YOU MAY WANT TO GET VBB'S MACRO DISASSEMBLER BY AURODREPH SO THAT YOU CAN STUDY ENCRYPTED MACROS. ALSO YOU SHOULD MAKE BACK-UPS OF YOUR NORMAL. DOT TEMPLATE IN YOUR WINWORD6\TEMPLATE\DIRECTORY, AS THIS IS HE DOCUMENT COMMONLY INFECTED BY MACRO VIRII. SO WATCH OUT. ALSO I RECOMMEND TO HAVE AT LEAST A SMALL KNOWLEDGE OF WORD BASIC, SO THAT YOU KIND A KNOW WHAT'S GOING ON. WELL, THAT'S IT. YOU'VE MADE IT THIS FAR. IT'S NOW TIME TO GET INTO THE MACRO VIRUS GENERALS. . . .

UWAGA Łączenie się ze stronami oferującymi narzędzia hakerskie lub informacje na temat tworzenia wirusów może być niebezpieczne. Wiele z tych stron zawiera programy trojańskie i wirusy, które mogą naruszyć bezpieczeństwo Twojego komputera .

Reszta dokumentu została usunięta z powodu ograniczeń miejsca. Jednak widać, że znalezienie informacji na temat tworzenia makrowirusa jest aż nadto łatwe.

Aktywność 3-2: Identyfikacja wirusów makro

Czas trwania: 30 minut

Cel: Zbadanie obecnych wirusów makro, które stanowią zagrożenie dla użytkowników. Opis: Chociaż wirusy makro istnieją od dawna, nadal stanowią realne i poważne zagrożenie dla komputerów. Powinieneś być świadomy nowych trendów w zakresie wirusów makro. W tej aktywności przejrzysz niektóre zastosowania wirusów makro, a następnie dowiesz się, jak je tworzyć.

1. Uruchom przeglądarkę internetową, jeśli to konieczne, i przejdź do witryny ww.virusbulletin.com/virusbulletin/2014/07/vba-not-dead.

2. Wykres w artykule pokazuje znaczny spadek aktywności wirusów makro od 2001 do 2006 roku. Zastanów się, dlaczego wykorzystanie wirusów makro wzrosło od 2012 roku.

3. W jaki sposób dokumenty Word i arkusze kalkulacyjne Excel są zaprojektowane tak, aby oszukiwać użytkowników i zmuszać ich do uruchamiania makr?

4. Wymień niektóre z ostatnich złośliwych oprogramowań, które wykorzystywały wirusy makro. (Zobacz sekcję „Ostateczny ładunek").

5. Użyj Google, aby wyszukać, jak utworzyć makrowirusa. Czy znalazłeś jakieś strony lub filmy z instrukcjami dotyczącymi tworzenia makrowirusa?

6. Przeczytaj lub obejrzyj samouczek, który odkryłeś w kroku 5. Czy tworzenie makrowirusa wydaje się trudne czy łatwe?

7. Pozostaw przeglądarkę internetową otwartą do następnej czynności.

Robaki

Robak to program, który replikuje się i rozprzestrzenia bez konieczności dołączania się do hosta (w przeciwieństwie do wirusa, który musi dołączyć się do hosta). Samorozprzestrzenianie się pozwala złośliwemu oprogramowaniu „przeszukiwać" sieć i próbować zainfekować inne znalezione urządzenia. Z powodu tego „przeszukiwania" nazywa się go robakiem. Najbardziej niesławnymi robakami są Stuxnet (omówiony w Ćwiczeniu 3-3), Code Red i Conficker. Teoretycznie robak, który replikuje się wielokrotnie na każdego zainfekowanego użytkownika, może zainfekować każdy komputer na świecie w krótkim czasie. Taki wynik jest mało prawdopodobny, ale jak w przypadku wielu schematów piramidalnych, można zobaczyć, jak robak może rozprzestrzeniać się w całej sieci, a nawet w Internecie. Bankowość internetowa, zakupy i inne formy handlu elektronicznego muszą stawić czoła zagrożeniu, jakie robaki stanowią dla infrastruktury komputerów i serwerów, a także dla komputerów i urządzeń mobilnych używanych przez ich klientów.

Trojany

Najbardziej podstępne ataki na sieci i komputery na całym świecie odbywają się za pośrednictwem programów trojańskich. Trojany maskują się jako przydatne programy i mogą zainstalować tylne drzwi lub rootkity na komputerze. Tylne drzwi lub rootkity to programy, które dają atakującym sposób na odzyskanie dostępu do zaatakowanego komputera później. Rootkit jest tworzony po ataku i zwykle ukrywa się w narzędziach systemu operacyjnego, więc prawie niemożliwe jest jego wykrycie. Back Orifice to dobry przykład trojana, który był popularny w ciągu ostatniej dekady. Umożliwia atakującym przejęcie pełnej kontroli nad zaatakowanym komputerem, podobnie jak działa Windows Remote Desktop, z tą różnicą, że Back Orifice działa bez wiedzy użytkownika. Program istnieje od 1999 r., ale obecnie jest reklamowany jako narzędzie administracyjne, a nie hakerskie. Programista, który napisał Backdoor.Slackbot.B, na przykład, może kontrolować komputer za pomocą Internet Relay Chat (IRC), który jest na porcie 6667. Dobry programowy lub sprzętowy firewall najprawdopodobniej zidentyfikuje ruch korzystający z nieznanych portów, ale trojany korzystające ze wspólnych portów, takich jak port TCP 80 (HTTP) lub port UDP 53 (DNS), są trudniejsze do wykrycia. Ponadto wielu użytkowników domowych i małych firm nie zarządza, które porty są otwarte, a które zamknięte w ich irewallach.

BAJTY BEZPIECZEŃSTWA

Wiele produktów zapór programowych dla użytkowników domowych dobrze rozpoznaje programy skanujące porty lub wykrywa próby połączeń z komputera przez podejrzany port, taki jak port 6667. Jednak wiele z tych zapór prosi użytkowników o zezwolenie lub niedozwolenie na ten ruch. Problem polega na tym, że użytkownicy, którzy nie są świadomi tych trojanów, po prostu klikają Zezwalaj, gdy są ostrzegani o podejrzanej aktywności na porcie. Ponadto wiele trojanów używa standardowych portów do przeprowadzania ataków, co utrudnia przeciętnym użytkownikom odróżnienie podejrzanej aktywności od normalnego ruchu internetowego. Należy edukować użytkowników sieci o tych podstawowych koncepcjach, jeśli żadna korporacyjna zapora ani polityka korporacyjna nie ustanawia zasad i ograniczeń w celu zwalczania trojanów.

Oprogramowanie szpiegujące

Jeśli przeszukasz sieć, wpisując słowo kluczowe „oprogramowanie szpiegujące”, zostaniesz zasypany setkami linków. Niektórzy zachwalają usuwanie oprogramowania szpiegującego, ale inni instalują oprogramowanie szpiegujące na komputerze, gdy użytkownik kliknie przycisk Tak w oknie dialogowym pytającym, czy komputer powinien zostać sprawdzony pod kątem oprogramowania szpiegującego (patrz Rysunek 3-2). Po kliknięciu przycisku Tak rozpoczyna się instalacja oprogramowania szpiegującego. Program szpiegujący wysyła informacje z zainfekowanego komputera do osoby, która zainicjowała zainstalowanie programu szpiegującego na komputerze. Informacje te mogą obejmować poufne dane finansowe, hasła, kody PIN — praktycznie dowolne dane przechowywane na komputerze. Musisz upewnić się, że użytkownicy rozumieją, że takie zbieranie informacji jest możliwe i że programy szpiegujące mogą rejestrować każde naciśnięcie klawisza. To takie proste. Ten typ technologii nie tylko istnieje, ale jest powszechny. Można go używać do rejestrowania i wysyłania wszystkiego, co użytkownik wpisuje, do nieznanej osoby znajdującej się po drugiej stronie świata. Powiedz użytkownikom, że nie powinni zakładać, że fizyczne środki bezpieczeństwa, takie jak zamknięte drzwi, wystarczą, aby powstrzymać wszystkich intruzów.

Aktywność 3-4: Identyfikowanie oprogramowania szpiegującego

Czas trwania: 30 minut

Cel: Zbadanie powszechnych programów szpiegujących.

Opis: Specjaliści ds. bezpieczeństwa sieci wiedzą, że oprogramowanie szpiegujące jest jednym z najgorszych typów złośliwych ataków na sieci korporacyjne. Oprogramowanie szpiegujące może zostać zainstalowane na dowolnym komputerze na różne sposoby; najczęstszym podejściem jest automatyczna instalacja oprogramowania szpiegującego po kliknięciu przez użytkownika hiperłącza lub uruchomieniu programu bez weryfikacji jego autentyczności. Powinieneś być świadomy wszelkich nowych programów szpiegujących, a także oprogramowania, które może usunąć oprogramowanie szpiegujące z komputera.

1. Uruchom przeglądarkę internetową, jeśli to konieczne, i przejdź do www.google.com. Wpisz spyware w polu wyszukiwania, a następnie naciśnij Enter.

2. Wypisz niektóre wyniki wyszukiwania.

3. Napisz opis oprogramowania szpiegującego na podstawie jednej ze stron wymienionych w kroku 2.

4. W przeglądarce internetowej przejdź do us-cert.cisa.gov.

5. Na stronie głównej wpisz spyware w polu wyszukiwania, a następnie naciśnij Enter.

6. Kliknij łącze Recognizing and Avoiding Spyware. Przeczytaj artykuł Security Tip i napisz krótki opis, w którym omówisz sekcje artykułu: „Skąd wiesz?", „Jak możesz zapobiec?" i „Jak usunąć?".

7. Pozostaw przeglądarkę internetową otwartą do następnej aktywności.

Adware

Różnica między spyware a adware jest cienka. Oba programy mogą zostać zainstalowane bez wiedzy użytkownika o ich obecności. Adware jednak czasami wyświetla baner, który powiadamia użytkowników o swojej obecności. Głównym celem adware jest określenie nawyków zakupowych użytkownika, aby przeglądarki internetowe mogły wyświetlać reklamy dostosowane do użytkownika. Gromadzenie nawyków zakupowych stanowi naruszenie bezpieczeństwa i prywatności, a informacje te są prawdopodobnie wysyłane z powrotem do hakerów, którzy wdrożyli adware.

Aktywność 3-4: Identyfikacja spyware

Wymagany czas: 30 minut

Cel: Zbadanie powszechnych programów spyware.

Opis: Profesjonaliści ds. bezpieczeństwa sieci wiedzą, że spyware jest jednym z najgorszych typów złośliwych ataków na sieci korporacyjne. Spyware może zostać zainstalowany na dowolnym komputerze na różne sposoby; najczęstszym podejściem jest automatyczna instalacja spyware po kliknięciu przez użytkownika hiperłącza lub uruchomieniu programu bez weryfikacji jego autentyczności. Powinieneś być świadomy wszelkich nowych programów spyware, a także oprogramowania, które może usunąć spyware z komputera.

1. W razie potrzeby uruchom przeglądarkę internetową i przejdź do www.google.com. Wpisz spyware w polu wyszukiwania, a następnie naciśnij Enter.

2. Wypisz niektóre wyniki wyszukiwania.

3. Napisz opis spyware na podstawie jednej ze stron wymienionych w kroku 2.

4. W przeglądarce internetowej przejdź do us-cert.cisa.gov.

5. Na stronie głównej wpisz spyware w polu wyszukiwania, a następnie naciśnij nter.

6. Kliknij łącze Rozpoznawanie i unikanie spyware. Przeczytaj artykuł Security Tip i napisz krótki opis, w którym omówisz sekcje „Skąd wiesz?”, „Jak możesz zapobiec?” i „Jak usunąć?” artykułu.

7. Pozostaw przeglądarkę internetową otwartą do następnej czynności.

BAJTY BEZPIECZEŃSTWA

Bezpieczeństwo sieci zaczyna się od zrozumienia przez każdego użytkownika, jak podatny na ataki jest komputer. Jednak świadomość obecności złośliwego oprogramowania, tak jak świadomość nieuczciwych telemarketerów, którzy dzwonią do Ciebie w porze kolacji, może lepiej przygotować Cię do podejmowania właściwych decyzji. Jeśli ktoś zaoferuje Ci sprzedaż nieruchomości na Tahiti za 99,95 USD przez telefon i poprosi o numer Twojej karty kredytowej, odmówisz. Użytkownicy komputerów powinni być tak samo sceptyczni, gdy zostaną poproszeni o kliknięcie przycisku OK lub zainstalowanie bezpłatnej gry komputerowej.

OCHRONA PRZED ATAKAMI ZŁOŚLIWEGO OPROGRAMOWANIA

Ochrona organizacji przed atakami złośliwego oprogramowania jest trudna, ponieważ codziennie pojawiają się nowe wirusy, robaki i trojany. Na szczęście oprogramowanie antywirusowe może wykryć wiele programów złośliwych. Na przykład, Rysunek 3-3 pokazuje oprogramowanie antywirusowe Malwarebytes wykrywające potencjalnie niechciany program. Ważne jest również edukowanie użytkowników na temat tego typu ataków i innych ataków, omówionych później w tej sekcji. W końcu użytkowników nie można załatać. Programy antywirusowe mogą łagodzić niektóre ryzyka związane ze złośliwym oprogramowaniem, ale użytkownicy, którzy nie są odpowiednio przeszkoleni, mogą otwierać luki w sieci, przed którymi żadna technologia nie jest w stanie się zabezpieczyć. Ochrona antywirusowa musi być wdrożona na komputerach użytkowników, ale powinna być również wdrożona na serwerach (takich jak serwery poczty e-mail), aby wyeliminować złośliwe oprogramowanie, zanim dotrze ono do komputerów użytkowników. Rozwiązania sprzętowe mogą również wykrywać i usuwać złośliwe oprogramowanie dla całych sieci, takich jak urządzenia Unified Threat Management (UTM).

Edukacja użytkowników

Bez względu na to, jak bardzo starasz się chronić sieć przed wprowadzeniem złośliwego oprogramowania, niemal niemożliwe jest zapobiegnięcie infekcji. Można jednak zminimalizować szkody i częstotliwość, z jaką komputery są infekowane. Ważnym nietechnicznym czynnikiem jest przeprowadzenie ustrukturyzowanego szkolenia wszystkich pracowników i kadry kierowniczej. W rzeczywistości wiele agencji rządowych USA wprowadza obowiązkowe programy świadomości bezpieczeństwa, a wiele firm z sektora prywatnego postępuje zgodnie z ich przykładem. Prostą, ale skuteczną metodą edukowania użytkowników jest wysyłanie miesięcznych aktualizacji zabezpieczeń do wszystkich pracowników, aby poinformować ich o najnowszych wirusach, oprogramowaniu szpiegującym i oprogramowaniu reklamowym wykrytym w Internecie. Oprócz ustrukturyzowanego szkolenia, niektóre organizacje aktywnie phishingują swoich pracowników i wysyłają ich do treści szkoleniowych, jeśli klikną link, którego nie powinni klikać. Aby zapobiec wprowadzaniu złośliwego kodu do sieci korporacyjnych, wiele organizacji uważa, że umieszczanie aplikacji na białej liście jest ostatnią linią obrony. Umieszczanie aplikacji na białej liście występuje w kilku formach, ale ostatecznie pozwala na uruchamianie na komputerze tylko zatwierdzonych programów. Na przykład programy takie jak Winword.exe, Excel.exe i Safari.exe byłyby umieszczane na białej liście. Wszystkie programy, które nie znajdują się na białej liście, nie będą mogły zostać uruchomione na komputerze użytkownika, w tym złośliwy program dołączony do wiadomości e-mail phishingowej z linkiem, który użytkownik klika. Innym zaleceniem, które powinieneś przekazać klientowi, jest aktualizacja plików sygnatur wirusów, gdy tylko będą dostępne u dostawcy. Większość oprogramowania antywirusowego

aktualizuje plik sygnatury automatycznie lub wyświetla monit użytkownikowi. Organizacja nie może polegać na czujności pracowników w zakresie ochrony swoich systemów, dlatego roztropne jest scentralizowanie wszystkich aktualizacji antywirusowych z serwera korporacyjnego. Aby przeciwdziałać wprowadzaniu oprogramowania szpiegującego i reklamowego do sieci korporacyjnej, powinieneś zainwestować w produkt antywirusowy. Chociaż wiele pakietów antywirusowych nie rozwiązuje w pełni problemu oprogramowania szpiegującego i reklamowego, jest to ważny pierwszy krok. W chwili pisania tego tekstu dwa popularne programy do usuwania oprogramowania szpiegującego i reklamowego to HitmanPro i Malwarebytes Anti-alware (MBAM). Inne witryny oferują podobne programy, ale pamiętaj, aby zachować ostrożność podczas pobierania programów z nieznanych witryn. E-mail to główny sposób, w jaki złośliwe oprogramowanie dostaje się do organizacji. Szkolenie pracowników w zakresie bezpiecznych praktyk e-mailowych oraz rozpoznawania i unikania wiadomości phishingowych jest niezbędne. Wiadomość phishingowa to wiadomość e-mail wysyłana przez hakera, która podszywa się pod legalną wiadomość e-mail. Wiadomości phishingowe zazwyczaj zawierają załączniki ze złośliwym oprogramowaniem lub osadzone łącza, które pobierają złośliwe oprogramowanie, jeśli użytkownik kliknie łącza. Możesz również pomóc chronić sieć, instalując zaporę sieciową. Wielu czołowych dostawców oprogramowania antywirusowego oferuje zapory programowe dla użytkowników domowych i małych firm, którzy nie mają zainstalowanej zapory sprzętowej ani systemu wykrywania włamań (IDS). Firmy korzystające z zapór sieciowych mogą postępować zgodnie z instrukcjami konfiguracji dostawcy. Na przykład robak W32/Sobig.F używa portu UDP 8998 do kontaktowania się z serwerem atakującego. Blokując cały ruch wychodzący na tym porcie, możesz zapobiec wystąpieniu tego ataku. Wiele usług jest również domyślnie uruchamianych na komputerze, chociaż nie muszą tak być. Na przykład przeciętny użytkownik domowy lub właściciel małej firmy zazwyczaj nie używa Telnetu. Ta usługa nie powinna być aktywna na większości komputerów, ponieważ jest podatna na wiele ataków zewnętrznych.

Unikanie taktyk wzbudzania strachu

Byłbyś zaskoczony, jak wielu użytkowników nie wie, że kliknięcie ikony w wiadomości e-mail może aktywować wirusa lub trojana lub umożliwić innej osobie dostęp do ich komputerów ze zdalnej lokalizacji. W związku z tym niektórzy specjaliści ds. bezpieczeństwa stosują taktyki wzbudzania strachu, aby nastraszyć użytkowników i zmusić ich do przestrzegania środków bezpieczeństwa. Ich podejście polega na tym, aby powiedzieć użytkownikom, że jeśli nie podejmą określonej czynności, ich systemy komputerowe zostaną zaatakowane przez każdego niezadowolonego, który ma dostęp do Internetu. Ta metoda jest czasami stosowana w celu generowania biznesu dla testerów bezpieczeństwa i w tym kontekście jest nie tylko nieetyczna, ale również sprzeczna z zasadami zaangażowania OSSTMM. Zasada stanowi: „Strach, niepewność i wątpliwości nie mogą być stosowane w prezentacjach sprzedażowych lub marketingowych, witrynach internetowych, materiałach pomocniczych, raportach lub dyskusjach na temat testów bezpieczeństwa w celu sprzedaży lub dostarczania testów bezpieczeństwa. Obejmuje to, ale nie ogranicza się do faktów dotyczących przestępstw, profilowania przestępców lub hakerów oraz statystyk”. Twoje podejście do użytkowników lub potencjalnych klientów powinno promować świadomość, a nie wzbudzać strach. Należy zwrócić uwagę użytkownikom, jak ważne jest, aby nie instalować programów — zwłaszcza tych niezatwierdzonych przez firmę — na swoich urządzeniach ze względu na możliwość wprowadzenia złośliwego oprogramowania. Użytkownicy powinni być świadomi potencjalnych zagrożeń, a nie się ich bać. Ponadto podczas szkolenia użytkowników należy pamiętać o rozwijaniu wiedzy, którą już posiadają. Na przykład niektórzy użytkownicy znają program Windows Remote Assistance lub inne programy do zdalnego sterowania, takie jak TeamViewer i VNC. Doświadczenie użytkowników z tymi programami ułatwia im zadanie wyjaśnienia, w jaki sposób intruz może przejąć kontrolę nad ich komputerami, ponieważ wiedzą już, że ta technologia jest dostępna.

ATAKI INTRUDENTÓW NA SIECI I KOMPUTERY

Atak jest definiowany jako każda próba uzyskania dostępu, uszkodzenia lub użycia zasobów sieciowych lub systemów komputerowych przez osobę nieupoważnioną. Zazwyczaj atak ma miejsce, gdy wykorzystywana jest słabość lub podatność. Eksploatacja to specjalnie opracowany ciąg danych mający na celu wykorzystanie podatności. Bezpieczeństwo sieci dotyczy bezpieczeństwa komputerów lub urządzeń, które są częścią infrastruktury sieciowej. Bezpieczeństwo komputerowe definiuje się jako zabezpieczenie samodzielnego urządzenia komputerowego, które nie jest częścią infrastruktury sieciowej. FBI, CIA i Interpol ostrzegają, że przestępczość komputerowa jest najszybciej rosnącym rodzajem przestępczości na świecie. W końcu atakowanie sieci korporacyjnej z wygody domu jest znacznie łatwiejsze niż włamanie się do firmy o 3:00 rano. Mówiąc o trudnościach w ściganiu przestępców komputerowych, agent FBI Arnold Aanui Jr. z Wydziału Cyberprzestępczości FBI w Honolulu stwierdził w wywiadzie: „Nawet jeśli FBI namierzy komputer użyty w przestępstwie, jeśli więcej niż jedna osoba ma do niego dostęp, FBI nie może aresztować domniemanego sprawcy, ponieważ którykolwiek z użytkowników mógł popełnić przestępstwo". Jeśli prawo nie ulegnie zmianie, tak aby kara za popełnienie tych przestępstw stała się bardziej odstraszająca, specjaliści ds. bezpieczeństwa będą zajęci przez wiele lat.

BAJTY BEZPIECZEŃSTWA

W zamożnej dzielnicy na Hawajach FBI wtargnęło do spokojnego domu mieszkalnego z nakazami w ręku, gotowe aresztować lokatora i skonfiskować jego komputer stacjonarny, który rzekomo zawierał zapisy transakcji narkotykowych i inne obciążające dowody. Kiedy funkcjonariusze FBI ostrożnie wchodzili do przodu domu, usłyszeli strzał z tylnej sypialni. Kiedy weszli do pokoju, zobaczyli mężczyznę siedzącego na łóżku i strzelbę kalibru 12 opartą o zamknięte drzwi. Właśnie opróżnił nabój do komputera, niszcząc dyski twarde tak dokładnie, że danych nie można było odzyskać. Agenci FBI mogli spróbować wysłać dyski do laboratorium specjalizującego się w odzyskiwaniu danych z dysków twardych, ale zdecydowali się tego nie robić, ponieważ uważali, że mają wystarczająco dużo dowodów z innych źródeł.

Ataki typu DoS

Jak sama nazwa wskazuje, atak typu DoS uniemożliwia legalnym użytkownikom dostęp do zasobów sieciowych. W przypadku ataku DoS atakujący nie próbują uzyskać dostępu do informacji na zdalnym komputerze. Mogą jednak użyć ataku, aby sparaliżować sieć. Jako tester bezpieczeństwa zazwyczaj nie instalujesz wirusa ani robaka na komputerze klienta w ramach testów. Podobnie powinieneś wiedzieć, jak może nastąpić atak DoS i próbować chronić przed nim firmę, ale przeprowadzanie ataku samodzielnie nie jest mądre. Zrobienie tego byłoby jak wysadzenie rafinerii przez konsultanta ds. bezpieczeństwa po zatrudnieniu go do poszukiwania zagrożeń bezpieczeństwa. Musisz po prostu wyjaśnić, w jaki sposób atak może zostać przeprowadzony. Starym, ale przydatnym przykładem ataku DoS jest atak Ping of death. Ten atak powoduje, że komputer ofiary zawiesza się i przestaje działać. Nie jest to już tak powszechne, jak pod koniec lat 90. Atakujący tworzy pakiet ICMP większy niż maksymalnie dozwolone 65 535 bajtów. Duży pakiet jest fragmentowany na mniejsze pakiety i ponownie składany w miejscu docelowym. System użytkownika w miejscu docelowym nie jest w stanie obsłużyć ponownie złożonego, zbyt dużego pakietu, co powoduje awarię lub zawieszenie systemu. Jest to również przykład ataku przepełnienia bufora, który zostanie omówiony później w tym module.

Ataki typu Distributed Denial-of-Service

Atak typu Distributed Denial-of-Service (DDoS) jest przeprowadzany na hosta z wielu serwerów lub stacji roboczych. W ataku DDoS sieć może zostać zalana miliardami pakietów; zazwyczaj każdy uczestnik ataku wysyła tylko kilka z całkowitej liczby pakietów. Jeśli jeden serwer bombarduje atakowany serwer setkami, a nawet tysiącami pakietów, dostępna przepustowość sieci może spaść do tego stopnia, że uprawnieni użytkownicy zauważą pogorszenie wydajności. Wyobraź sobie teraz 1000 serwerów lub nawet 10 000 rozproszonych serwerów, z których każdy wysyła kilka tysięcy pakietów IP do atakowanego serwera. Oto masz: atak DDoS. Pamiętaj, że uczestnicy ataku często nie są świadomi, że ich komputery biorą udział w ataku. Oni również zostali zaatakowani przez sprawcę. W rzeczywistości, w jednym ataku DDoS, firma została zalana pakietami IP z tysięcy routerów internetowych i serwerów internetowych należących do Yahoo.com. Dark DDoS to zasłona dymna, która ma odwrócić uwagę obrońców sieci, podczas gdy ma miejsce inny, bardziej ukryty i prawdopodobnie bardziej szkodliwy atak. Skupiając obrońców sieci na ciągłym „hałaśliwym" ataku DDoS, atakujący może przeprowadzić oszukańczą transakcję lub eksfiltrację danych, które mogłyby zostać wykryte, gdyby obrońcy nie skupili się na DDoS.

BAJTY BEZPIECZEŃSTWA

Specjaliści ds. bezpieczeństwa będą badać jeden z najbardziej rozpowszechnionych ataków DDoS na świecie od lat. Estonia, w Europie Północnej, padła ofiarą ataku DDoS w 2007 r., który zamknął rządowe witryny internetowe, banki i inne instytucje finansowe. Złośliwy ruch pochodził z całego świata, w tym ze Stanów Zjednoczonych i Kanady. Ataki DDoS są trudne do zatrzymania, ponieważ właściciele zainfekowanych komputerów, nazywani zombie, nie są świadomi, że ich systemy wysyłają złośliwe pakiety do ofiary oddalonej o tysiące mil. Te zainfekowane komputery są zwykle częścią botnetu (sieci komputerów „robotów"), wykonującego instrukcje z centralnej lokalizacji lub systemu. Aby uzyskać więcej informacji, wyszukaj „Estonia DDoS".

Ataki przepełnienia bufora

Na przestrzeni lat miało miejsce wiele ataków przepełnienia bufora na różnych systemach operacyjnych. W ataku przepełnienia bufora atakujący znajduje lukę w źle napisanym kodzie, który nie sprawdza określonej ilości wykorzystanej pamięci. Jeśli program definiuje rozmiar zmiennej wynoszący 64 bajty (całkowita ilość pamięci, jaką zmienna ma wykorzystać), a program zapisuje dane ponad 64-bajtowym znacznikiem bez wywoływania błędu lub zapobiegania wystąpieniu tego zdarzenia, mamy do czynienia z przepełnieniem bufora. Na przykład oprogramowanie wirtualizacji QEMU zarezerwowało bufor o rozmiarze 512 bajtów do odbierania danych z dysku wirtualnego, ale badacz znalazł sposób na wysłanie więcej niż 512 bajtów i przejęcie kontroli nad hostem maszyny wirtualnej z wnętrza maszyny wirtualnej. Zasadniczo atakujący pisze kod, który przepełnia bufor, co jest możliwe, ponieważ program akceptuje niezweryfikowane dane wejściowe użytkownika. Sztuką jest nie wypełniać przepełnionej pamięci bezsensownymi danymi, ale wypełnić ją wykonywalnym kodem programu. W ten sposób system operacyjny uruchamia kod, a program atakującego robi coś szkodliwego. Zazwyczaj kod podnosi uprawnienia atakującego do poziomu administratora lub tworzy usługę, która pozwala atakującemu na zdalny dostęp do systemu docelowego. W obronie programistów, większość z nich nie jest odpowiednio przeszkolona w zakresie pisania programów z myślą o bezpieczeństwie komputerowym. W przeszłości programy były pisane dla łatwości użytkowania i tworzenia wydajnego kodu wykonywalnego, który działał szybko i wykorzystywał jak najmniej zasobów komputerowych. Obecnie panuje tendencja, aby upewnić się, że programiści są świadomi, w jaki sposób ich kod może być podatny na ataki, ale sprawdzanie luk w zabezpieczeniach jako standardowa praktyka nadal nie jest powszechne. Gałąź cyberbezpieczeństwa zwana DevSecOps

zajmuje się potrzebą programistów, aby tworzyli kod z myślą o bezpieczeństwie. Wiele instytucji edukacyjnych oferuje kursy pisania programów z uwzględnieniem bezpieczeństwa. Niezależne i sponsorowane inicjatywy, takie jak Open Web Application Security Project (OWASP) i Building Security In Maturity Model (BSIMM), zachęcają do bezpiecznego rozwoju i pomagają organizacjom tworzyć lepsze oprogramowanie. W firmie Microsoft programiści są teraz nagradzani za pisanie kodu, który później nie ujawnia się jako luka w zabezpieczeniach systemu. W Ćwiczeniu 3-5 badasz oprogramowanie z lukami w zabezpieczeniach spowodowanymi przeoczeniem czynnika bezpieczeństwa w projekcie programu.

Aktywność 3-5: Badanie luk w zabezpieczeniach oprogramowania

Czas trwania: 30 minut

Cel: Zbadanie niektórych luk w zabezpieczeniach opublikowanych przez amerykański zespół ds. gotowości na wypadek awarii komputera (US-CERT). Opis: Jako specjalista ds. bezpieczeństwa przeprowadzający test bezpieczeństwa w sieci klienta musisz zbadać wszelkie luki w zabezpieczeniach, które mogą zostać wykorzystane. Po odkryciu luk w zabezpieczeniach, które mogą mieć wpływ na sieć klienta, musisz udokumentować swoje ustalenia i przedstawić zalecenia w celu rozwiązania problemu. W tej aktywności zbadasz luki w zabezpieczeniach zgłoszone przez US-CERT i dowiesz się, jakie rozwiązania lub zalecenia możesz przekazać klientom.

1. W razie potrzeby uruchom przeglądarkę internetową i przejdź na stronę www.us-cert.gov/ncas.

2. Przewiń w dół i kliknij łącze Wyświetl biuletyny, a następnie kliknij najnowszy biuletyn.

3. Zbadaj pierwsze kilka luk w zabezpieczeniach. Wybierz jedną i użyj linków w kolumnie „Źródło i informacje o poprawce”, aby odpowiedzieć na następujące pytania: Jakie zalecenia dałbyś komuś, czyj system został wykorzystany z powodu tej luki? Czy można coś zrobić, aby zapobiec wykorzystaniu tej luki?

4. Zamknij przeglądarkę internetową.

Ćwiczenie 3-5 daje wgląd w luki w oprogramowaniu wykorzystywane do wykorzystania systemu operacyjnego lub oprogramowania działającego w systemie operacyjnym. Zazwyczaj głównym celem ataku przepełnienia bufora jest wstawienie kodu do nadpisanego obszaru pamięci, który podnosi uprawnienia atakującego lub daje atakowi zdalny dostęp do maszyny.

Podsłuchiwanie

Atakujący może podsłuchiwać niezaszyfrowaną komunikację sieciową, aby przechwycić poufne informacje lub zebrać dane uwierzytelniające, które mogą zostać wykorzystane do rozszerzenia ataku. Podsłuchiwanie można przeprowadzić za pomocą narzędzi do podsłuchiwania zaprojektowanych do przechwytywania kopii pakietów wysyłanych przez sieć (np. tcpdump i Wireshark). Później te przechwycone pakiety, zwykle przechowywane w pliku .pcap, można zrekonstruować i przeszukać pod kątem danych i danych uwierzytelniających. Przydatne narzędzia do przeglądania plików .pcap obejmują NetWitness Investigator i CapAnalysis firmy RSA. Aby bronić się przed zagrożeniem podsłuchiwania, urządzenia sieciowe i aplikacje powinny być zmuszone do komunikowania się wyłącznie za pomocą szyfrowanych protokołów i używania ważnych, zaufanych certyfikatów.

Ataki typu Man-in-the-Middle

Jednym z kroków poza podsłuchiwaniem jest atak typu Man-in-the-Middle. Atakujący mogą wstrzyknąć się między dwie strony lub systemy komunikujące się ze sobą, aby manipulować przesyłanymi tam i z powrotem wiadomościami.

Przejęcie sesji sieciowej

Przejęcie sesji sieciowej umożliwia atakującemu dołączenie do sesji TCP i sprawienie, że obie strony będą uważać się za drugą stronę. Jest to złożony atak wykraczający poza zakres tej książki.

ROZWIĄZYWANIE PROBLEMU BEZPIECZEŃSTWA FIZYCZNEGO

Ochrona sieci przed atakami nie zawsze jest problemem oprogramowania. Powinieneś mieć podstawowe umiejętności ochrony sieci przed atakami fizycznymi. Niezależnie od tego, jak skuteczna jest Twoja zapora sieciowa, musisz zabezpieczyć serwery i komputery przed atakiem z wewnątrz organizacji. W rzeczywistości istnieje większe prawdopodobieństwo, że atakujący, który włamie się do sieci, jest z wewnątrz firmy, a nie z zewnątrz.

BAJTY BEZPIECZEŃSTWA

Na bazie wojskowej na Hawajach, pickup zaparkował przed budynkiem biurowym, a kierowca wszedł do budynku i wszedł do pustego biura. Odłączył komputer od sieci, wyniósł go z biura, umieścił na platformie ciężarówki i odjechał, aby nigdy więcej go nie zobaczyć. Kiedy kierownictwo wyższego szczebla przesłuchało pracowników, pracownicy powiedzieli, że pamiętają, jak widzieli kogoś wychodzącego z budynku z komputerem, ale założyli, że był to pracownik pomocy technicznej. Bezpieczeństwo fizyczne jest tak silne, jak najsłabsze ogniwo. Wszyscy pracownicy muszą być świadomi tego, co dzieje się w ich środowisku pracy. Na przykład, jeśli zauważą nieznajomego siedzącego przed komputerem i pobierającego pliki, powinni skontaktować się z ochroną, a następnie skonfrontować się z tą osobą. Pracownicy powinni być czujni i nie polegać wyłącznie na pracownikach ochrony, którzy zwrócą uwagę.

Keyloggery

Keyloggery to urządzenia sprzętowe lub oprogramowanie, które można wykorzystać do przechwytywania naciśnięć klawiszy na komputerze. Jeśli przeprowadzasz test bezpieczeństwa w systemie i musisz uzyskać hasła, keyloggery mogą być pomocnym narzędziem. Oczywiście, powinieneś mieć pisemną zgodę klienta przed użyciem programowego lub sprzętowego keyloggera. Keyloggery programowe zachowują się jak wirusy lub trojany. Sprzętowy keylogger to małe urządzenie — często mniejsze niż cal długości. Zazwyczaj można je zainstalować w mniej niż 30 sekund. Keyloggery mogą być używane przez organizacje i osoby, które chcą monitorować aktywność użytkowników w swoich systemach komputerowych. Organy ścigania i eksperci kryminalistyczni również używają keyloggerów w tym samym celu monitorowania. Większość sprzętowych keyloggerów to małe urządzenia, które podłącza się do portu USB w klawiaturze i portu USB z tyłu komputera. Te keyloggery przechowują naciśnięcia klawiszy użytkowników wewnętrznie, więc urządzenie do rejestrowania naciśnięć klawiszy często musi zostać wyjęte, aby zbadać zawartość. Wiele keyloggerów ma wbudowane Wi-Fi, dzięki czemu można zdalnie odzyskać zapisane naciśnięcia klawiszy bez konieczności wyjmowania urządzenia. Niektóre klawiatury Wi-Fi mają nawet wbudowane keyloggery Wi-Fi. Niektóre popularne sprzętowe keyloggery to KeyGrabber i KeyGhost. Po zainstalowaniu KeyGrabber automatycznie zaczyna rejestrować naciśnięcia klawiszy. Aby przejść do trybu odtwarzania, użytkownicy mogą wprowadzić kombinację klawiszy, aby włączyć ukryty dysk flash. Na tym dysku flash użytkownicy mogą znaleźć LOG.TXT, który zawiera dziennik dotyczący każdego naciśnięcia klawisza wprowadzonego od

czasu zainstalowania urządzenia. Atakujący mogą również używać urządzeń keylogger. Nieuczciwy pracownik może podłączyć keylogger do komputera kierownika i później odzyskać poufne informacje. Zainstalowanie tego urządzenia wymaga dostępu do komputera, co może stanowić problem, jeśli biuro kierownika jest zamknięte. Jeśli atakujący używa keyloggera obsługującego Wi-Fi, informacje o naciśnięciach klawiszy można pobrać zdalnie, eliminując potrzebę uzyskiwania dostępu do biura kierownika w przyszłości. Przypomnijmy, że keyloggery są również dostępne jako oprogramowanie (spyware) ładowane na komputerze, a pobrane informacje można wysłać e-mailem lub przesłać do zdalnej lokalizacji. Podczas losowych testów wizualnych komputerów w swojej organizacji zwróć uwagę na podejrzany sprzęt podłączony do kabla klawiatury, który nie został zainstalowany przez personel ochrony. Ta kontrola to prosty sposób monitorowania keyloggerów (lub nawet systemów komputerowych), których firma nie zainstalowała.

Za zamkniętymi drzwiami

Jako specjalista ds. bezpieczeństwa powinieneś znać rodzaje zamków używanych do zabezpieczania aktywów firmy. Jeśli intruz uzyska fizyczny dostęp do serwera — niezależnie od tego, czy działa na systemie Linux, Windows czy innym systemie operacyjnym — nie ma znaczenia, jak dobry jest Twój firewall lub IDS. Szyfrowanie lub egzekwowanie infrastruktury klucza publicznego (PKI) również nie pomoże w tej sytuacji. Jeśli intruzi mogą siedzieć przed Twoim serwerem, mogą go zhakować. Mówiąc prościej, zamknij swój serwer. Tak samo jak terroryści mogą nauczyć się, jak stworzyć bombę, wykonując badania w Internecie, atakujący mogą znaleźć niezliczone artykuły na temat wytrychów. Jedna strona internetowa „Lockpicking-by Deviant Ollam” (http://deviating.net/lockpicking/) omawia podatności różnych zamków i zawiera filmy pokazujące techniki wytrychów. W ciągu zaledwie kilku dni ćwiczeń przeciętna osoba może nauczyć się, jak wytrychować typowy amerykański zamek domowy w mniej niż pięć minut. Ci, którzy mają więcej wolnego czasu, na przykład hakerzy, mogą nauczyć się otwierać zamek zasuwkowy w mniej niż 30 sekund. Jeśli odpowiadasz za ochronę infrastruktury sieciowej, w której pracują pracownicy na nocną zmianę, nie zakładaj, że zamknięte drzwi lub szafki powstrzymają nieuczciwych pracowników, którzy mają dużo wolnego czasu. Zazwyczaj mniej pracowników jest w pobliżu w niestandardowych godzinach pracy, co ułatwia im dostęp do obszarów, do których normalnie nie mają dostępu. Twoja serwerownia powinna mieć najlepszy zamek, na jaki stać Twoją firmę. Poświęć trochę czasu na przyjrzenie się zamkom używanym przez organizacje takie jak Departament Obrony, gdzie ochrona zasobów może być kwestią życia lub śmierci. Wydanie od 5000 do 10 000 dolarów na zamek nie jest niczym niezwykłym w tych organizacjach.

BAJTY BEZPIECZEŃSTWA

Niektóre legalne strony internetowe oferują narzędzia i instrukcje dotyczące otwierania zamków dla policji lub pracowników ochrony. Często wymagają wypełnienia formularza, ale może się to opłacić, jeśli planujesz zostać specjalistą ds. bezpieczeństwa. Na przykład, jeśli przeprowadzasz test bezpieczeństwa w organizacji, która ma zamkniętą serwerownię i chcesz uzyskać do niej dostęp, wiedza, jak otworzyć zamek, może być przydatna. Pamiętaj jednak, że musisz uzyskać pisemną zgodę kierownictwa przed przeprowadzeniem tego poziomu testów. Zamawiając narzędzia do otwierania zamków, pamiętaj, że wiele stanów lub krajów uważa samo posiadanie tych narzędzi za przestępstwo. Pamiętaj, że posiadanie niektórych narzędzi hakerskich jest również nielegalne.

Zamki obrotowe, które wymagają wciśnięcia sekwencji ponumerowanych prętów, są trudniejsze do złamania niż zamki zasuwkowe. Jednak żaden z typów zamków nie rejestruje, kto wszedł do zamkniętego pomieszczenia, więc niektóre firmy wymagają korzystania z dostępu za pomocą karty w celu zwiększenia bezpieczeństwa. W przypadku tej metody karta jest skanowana, a posiadacz karty otrzymuje dostęp, dokumentując jednocześnie czas wejścia. Ta metoda umożliwia również jednej

karcie dostęp do kilku drzwi bez konieczności wydawania wielu kluczy lub zapamiętywania przez użytkowników różnych kombinacji. Biometryczne urządzenia zabezpieczające, które odczytują odciski palców lub skany siatkówki, są również używane do ograniczania dostępu do bezpiecznych obszarów. Urządzenia biometryczne mogą uzupełniać tradycyjne zamki fizyczne i zapewniać drugi czynnik uwierzytelniania lub mogą być używane samodzielnie, bez tradycyjnego zamka fizycznego. Tradycyjne zamki z kombinacjami numerowanymi są podatne na udostępnianie hasła osobie nieupoważnionej. Urządzenia biometryczne unikają tej podatności.

BAJTY BEZPIECZEŃSTWA

Urządzenia zabezpieczające biometryczne są użyteczną opcją uwierzytelniania dostępu, ale nie są pozbawione wad. Niektóre skanery biometryczne można oszukać, umożliwiając nieupoważnionym użytkownikom dostęp do bezpiecznych zasobów, chociaż ulepszenia technologii biometrycznej zmniejszyły tę możliwość. Niektóre smartfony są wyposażone w blokadę biometryczną odcisku palca lub funkcję rozpoznawania twarzy, która może być używana do uwierzytelniania dostępu do telefonu. Te funkcje bezpieczeństwa były w przeszłości łatwo omijane. W jednym przypadku zdjęcie zostało użyte do oszukania rozpoznawania twarzy. Biometria powinna być używana z inną metodą autoryzacji, taką jak kod dostępu, aby zapewnić uwierzytelnianie wieloczynnikowe, które jest bezpieczniejsze.

PODSUMOWANIE MODUŁU

• Specjaliści ds. bezpieczeństwa muszą być świadomi ataków, które mogą mieć miejsce na infrastrukturę sieciową, komputery, telefony komórkowe i inne urządzenia z dostępem do Internetu.

• Ataki sieciowe i komputerowe mogą być przeprowadzane zarówno przez osoby wewnętrzne, jak i zewnętrzne.

• Złośliwe oprogramowanie (malware) — takie jak wirusy, robaki i konie trojańskie — może atakować sieć lub komputer. Wirus przyłącza się do hosta. Robak może się replikować i rozprzestrzeniać bez przyłączania się do hosta. Trojan podszywa się pod przydatny program lub aplikację i może zainstalować tylne drzwi lub rootkita na komputerze.

• Użytkownicy mogą nieumyślnie instalować programy szpiegujące, myśląc, że instalują oprogramowanie w celu ochrony swoich komputerów. Oprogramowanie szpiegujące może rejestrować informacje z komputera użytkownika i wysyłać je do atakującego.

• Specjaliści ds. bezpieczeństwa mogą zminimalizować szkody i prawdopodobieństwo infekcji, stosując się do najlepszych praktyk i wdrażając środki techniczne i nietechniczne.

• Programy typu adware mogą być również instalowane bez wiedzy użytkowników. Są one wykorzystywane do rozpoznawania wzorców zakupowych użytkowników w celu wysyłania reklam internetowych dostosowanych do ich nawyków zakupowych.

• Atak typu „odmowa usługi” (DoS) uniemożliwia autoryzowanym użytkownikom dostęp do zasobów sieciowych. Atak jest zwykle przeprowadzany poprzez nadmierne wykorzystanie przepustowości, pamięci i cykli procesora.

• Rozproszony atak typu „odmowa usługi” (DDoS) to atak na hosta z wielu serwerów lub komputerów.

• Głównym celem przepełnienia bufora jest wstawienie kodu wykonywalnego do obszaru pamięci, który podnosi uprawnienia atakującego do poziomu administratora lub umożliwia atakującemu zdalny dostęp do systemu docelowego.

• W ataku Ping of Death atakujący tworzy pakiet ICMP większy niż maksymalne 65 535 bajtów, co powoduje awarię lub zawieszenie systemu odbiorcy. Większość dzisiejszych systemów nie jest dotknięta tym exploitem.

• W przypadku przejęcia sesji sieciowej atakujący dołącza do sesji TCP i sprawia, że obie strony myślą, że jest drugą stroną.

• Keyloggery umożliwiają monitorowanie tego, co jest wprowadzane do systemu komputerowego. Można je łatwo zainstalować na złączu klawiatury i przechowywać informacje wewnętrznie. Personel ochrony powinien przeprowadzać losowe kontrole sprzętu komputerowego w celu wykrycia tych urządzeń.

• Bezpieczeństwo fizyczne jest odpowiedzialnością każdego. Wszystkie systemy stacjonarne i serwery muszą być fizycznie zabezpieczone.