LOCAL AREA NETWORKS

WPROWADZENIE

Omówimy ogólne kwestie związane z bezpieczeństwem sieci lokalnej (LAN). Zabezpieczenie sieci LAN ma zasadnicze znaczenie dla zabezpieczenia Internetu, ponieważ w sieci LAN znajduje się większość atakujących, ofiar, klientów, serwerów, zapór ogniowych, routerów i innych urządzeń. Naruszone systemy LAN w Internecie otwierają inne węzły w tej sieci lokalnej w celu ataku i narażenia innych systemów na ryzyko w całym Internecie. Wiele ogólnych zagadnień, o których mowa w niniejszym dokumencie, zostało bardziej szczegółowo opisanych później

KWESTIE POLITYKI I PROCEDURY

Trzydzieści lat temu prawie wszyscy użytkownicy komputerów mieli konta na wspólnym komputerze mainframe lub minikomputerze. Jeden menedżer systemu był odpowiedzialny za bezpieczeństwo, tworzenie kopii zapasowych, odzyskiwanie po awarii, zarządzanie kontami, zasady i wszystkie inne powiązane kwestie. Obecnie wszyscy użytkownicy są administratorami systemów, a w wielu przypadkach to osoby są odpowiedzialne za kilka systemów. Ponieważ luka pojedynczego komputera może zagrozić całej sieci LAN, konieczne jest ustanowienie reguł, które umożliwią wszystkim współpracę w celu zapewnienia wzajemnej wydajności i obrony. Ale tam, gdzie zasady i procedury mogą być scentralizowane, powinny tak być, ponieważ większość użytkowników nie traktuje procedur bezpieczeństwa wystarczająco poważnie. Następna lista, zmodyfikowana na podstawie wniosku o komentarz (RFC) 2196 Internet Engineering Task Force (IETF), zawiera ogólny zarys zasad i procedur bezpieczeństwa związanych z siecią LAN, które należy przynajmniej wziąć pod uwagę.

1. Ramy polityki administracyjnej

a. Kwestie bezpieczeństwa informacji

i. Procedury zarządzania hasłami

1. Czy hasła są przydzielane lub wybierane przez użytkownika?

2. Czy obowiązują procedury kontroli haseł?

3. Czy są egzekwowane zasady dotyczące haseł (np. Minimalna długość, dozwolone i wymagane znaki, wygaśnięcie, czarna lista)?

4. Ile haseł jest wymaganych, aby uzyskać dostęp do wszystkich systemów?

ii. Ochrona Antywirusowa

1. Czy serwery są chronione?

2. Czy istnieje „zapora wirusowa” poczty e-mail?

3. Czy ochrona antywirusowa jest działaniem zarządzanym centralnie, czy zależy od każdego użytkownika?

4. W jaki sposób użytkownicy utrzymują aktualną bazę sygnatur wirusów?

iii. Szyfrowanie i certyfikaty

iv. Obsługa zdarzeń bezpieczeństwa

b. Problemy z łącznością sieciową

i. Dostęp telefoniczny

ii. Huby a przełączniki

iii. Identyfikacja i uwierzytelnienie

1. Hasła i zarządzanie

2. Systemy uwierzytelniania

3. Uwierzytelnianie dwuskładnikowe?

4. Pojedyncze logowanie?

5. Biometria

c. Bezpieczeństwo lokalizacji fizycznej i odzyskiwanie po awarii

i. Fizyczne bezpieczeństwo systemów

ii. Linie dostępu telefonicznego i modemy

iii. Planowanie kopii zapasowych

iv. Dostęp do serwerów

v. Przechowywanie i ograniczanie dostępu do nośników kopii zapasowych

vi. Odzyskiwanie po awarii i plany awaryjne

d. System operacyjny i bezpieczeństwo sieci LAN

i. Problemy specyficzne dla systemu operacyjnego

1. Monitorowanie luk w zabezpieczeniach systemu operacyjnego

2. Stosowanie poprawek bezpieczeństwa

3. Zabezpieczenie systemu operacyjnego (OS) podczas instalacji

4. Audyt systemów

ii. Czy jest używany protokół dynamicznej konfiguracji hosta (DHCP)?

iii. Oprogramowanie i procedury do analizy dzienników

iv. Testowanie podatności

v. Narzędzia do wykrywania włamań

2. Struktura zasad użytkownika

a. Napisana, opublikowana polityka bezpieczeństwa sieci

b. Polityka odpowiedniego korzystania z sieci / Internetu (AUP)

c. Szkolenie i edukacja użytkowników

i. Bezpieczeństwo (kwestie ogólne)

ii. Znaczenie ochrony danych klientów, informacji o klientach i innych prywatnych informacji, takich jak dokumentacja medyczna i informacje o pacjencie

iii. Zasady i AUP

iv. Sugestie dotyczące bezpieczeństwa

d. Wirus ochrona

i. Korzystanie z oprogramowania antywirusowego

ii. Utrzymywanie aktualnej bazy sygnatur wirusów

e. Wybór dobrych haseł

f. Najlepsze praktyki

i. E-mail (netykieta i obsługa załączników)

ii. Przeglądarka (upewnij się, że Java, JavaScript, ActiveX i inne automatyczne wykonywanie czy kod jest aktualny i określony przez producenta.

iii. Pakiet Microsoft Office

1. Korzystanie z makr

2. Implikacje dla zarządzania dokumentami

iv. Ochrona plików na serwerze i własnym systemie

1. Korzystanie z „udziałów" systemu Windows i sieciowego systemu plików UNIX (NFS)

2. Korzystanie z NetWare, New Technology File System (NTFS) i UNIX kontrola dostępu

i. Dostrzeżenie możliwego kompromisu (metody identyfikacji włamań lub inna nieuprawniona działalność)

ii. Co robić i z kim się skontaktować w przypadku podejrzenia kompromisu

Nie każdy problem będzie dotyczył wszystkich sieci, ale każda sieć LAN jest jednostką nieustannie ewoluującą, a zasady rządzące jej działaniem również muszą ewoluować.

BEZPIECZEŃSTWO FIZYCZNE

Fizyczna ochrona miejsca jest bardzo ważna, ale zbyt często pomijana. Jednym z powodów, dla których często brakuje zabezpieczeń witryny, jest to, że niektóre zasady i procedury mogą być postrzegane jako komunikaty dla pracowników, że nie są im zaufane. Niemniej jednak, bezpieczeństwo lokacji fizycznej obejmuje wiele aspektów ochrony

PROBLEMY Z WARSTWĄ FIZYCZNĄ

Sama sieć LAN ma szereg dodatkowych luk w zabezpieczeniach, ponieważ systemy i media są tak bardzo rozproszone. W tej sekcji omówiono zabezpieczenie infrastruktury LAN

Sniffery i rozgłaszane sieci LAN

Tradycyjne schematy kontroli dostępu do mediów w sieci LAN (MAC) działają przy założeniu logicznej, jeśli nie fizycznej, topologii rozgłoszeniowej. W sieci nadawczej każda stacja słyszy każdą transmisję. Podczas pracy w trybie promiscuous stacja LAN czyta każdą ramkę, która przechodzi, niezależnie od

tego, czy ramka jest adresowana do stacji, czy nie. Kiedy w latach 80. XX wieku pojawiło się oprogramowanie do analizy protokołów lub sniffera, każda stacja w sieci LAN stała się potencjalnym narzędziem do analizy i zarządzania siecią - lub ukradkiem podsłuchującym. Ponieważ tak wiele aplikacji sieciowych, w szczególności aplikacji opartych na protokole kontroli transmisji / protokole internetowym (TCP / IP), przesyła hasła i pliki w postaci zwykłego tekstu, tego typu oprogramowanie jest potencjalnie bardzo niebezpieczne.

Wiele źródeł oferuje bardzo wydajne i bardzo elastyczne komercyjne oprogramowanie do wyszukiwania pakietów, takie jak SnifferPro firmy Network Associates i LANalyzer firmy Novell. Pakiety te mają zwykle dodatkowe możliwości, takie jak monitorowanie sieci, monitorowanie wydajności i analiza ruchu. Przed 1990 rokiem analiza protokołów sieciowych wymagała specjalnego sprzętu połączonego z siecią. Obecnie duża liczba pakietów oprogramowania do wykrywania pakietów TCP / IP może pomóc intruzowi, ponieważ można je zainstalować bezpośrednio na laptopie lub komputerze stacjonarnym danej osoby. Niektóre z tych pakietów obejmują:

* WireShark (Windows, MacOS i UNIX)

* BUTTsniffer (Windows NT)

* Monitor sieci (bezpłatny z Windows NT i dla Windows NT)

* Sniffit (Linux, SunOS, Solaris, FreeBSD, Irix)

* snort (UNIX i Windows)

* Solsniff (Solaris)

* tcpdump (MacOS i UNIX)

* WinDump (DOS)

Stosunkowo niewiele środków zaradczych można podjąć przeciwko tego rodzaju narzędziom. Na szczęście działają one tylko w sieci rozgłoszeniowej, takiej jak sieć LAN z koncentratorem. Jeśli na przykład koncentrator Ethernet zostanie zastąpiony przełącznikiem, jedynym rozgłaszanym ruchem do wszystkich hostów w sieci są te ramki, które są faktycznie adresowane do adresu rozgłoszeniowego sieci LAN. W takim przypadku stacja może wykrywać tylko ruch przychodzący do stacji lub ze stacji za pomocą oprogramowania sniffer. Zastąpienie wszystkich koncentratorów przełącznikami może być nieracjonalne w wielu środowiskach, ale umieszczenie wszystkich serwerów na przełączniku zamiast koncentratora poprawi zarówno wydajność, jak i bezpieczeństwo. Inne narzędzia sieciowe, które mogą wykryć hosta z kartą sieciową (NIC) w trybie swobodnym, takie jak AntiSniff (Windows) i wartownik (UNIX). Te narzędzia działają, wykonując szereg testów w celu wykrycia rozwiązłego hosta; następnie sprawdzają systemy operacyjne hosta sieciowego, aktywność systemu nazw domen (DNS) oraz opóźnienia sieci i komputera. Snifferów można pokonać za pomocą kryptografii. Korzystanie z bezpiecznego IP (IPsec) i Secure Shell (SSH) dla aplikacji TCP / IP może zapewnić prywatność i integralność całej komunikacji i aplikacji. Informacje o IPsec są dostępne na stronie www.ipsechowto. org / x202.html, a SSH jest dostępne w SSH Communications Security (www.ssh.com).

Ataki na zakład przemysłowy

Najpopularniejszym medium używanym obecnie w sieciach LAN jest miedziany, nieekranowany kabel typu skrętka (UTP). Wszystkie media miedziane, w tym kabel UTP i kabel koncentryczny, emitują pole magnetyczne z powodu zmieniającego się prądu w przewodzie. Urządzenia monitorujące Van Eck mogą zdalnie wychwytywać te emanacje i odtwarzać ramki na przewodzie lub naciśnięcia klawiszy na

maszynie. Choć może się to wydawać naciągane, luka jest bardzo realna. Rząd USA i wojsko mają zestaw norm dotyczących zmniejszania i ograniczania promieniowania elektromagnetycznego (EMR) zwany TEMPEST, a Agencja Bezpieczeństwa Narodowego (NSA) posiada listę produktów zgodnych z TEMPEST. Rzeczywiście, ta luka w zabezpieczeniach może nie stanowić poważnego problemu w większości sieci organizacyjnych, ale jest kilka sieci, w których jest to problem. Alternatywą dla obudowania stacji roboczych w klatkach Faradaya (tj. Warstwami siatki miedzianej otaczającej wszystkie komponenty) jest generowanie losowego szumu elektronicznego, który maskuje znaczące promieniowane transmisje danych.

Jednym ze sposobów zmniejszenia lub wyeliminowania EMR jest zmniejszenie lub wyeliminowanie ilości mediów miedzianych w sieci. Na przykład światłowód nie ma EMR, ponieważ na linii nie ma prądu. Nie eliminuje EMR na samym pulpicie, ale zapobiega jego wejściu do wszystkich połączonych kabli światłowodowych. Użytkownicy mogą również być źródłem niektórych rodzajów ataków typu „odmowa usługi" (DoS), celowo lub przypadkowo. Rozważmy sieci Ethernet z kablami koncentrycznymi (10BASE-5 lub 10BASE-2), w których węzły są podłączone do wspólnego medium LAN. W obu przypadkach kabel koncentryczny ma rezystor terminujący na końcu przewodu, aby wyeliminować odbicie sygnału. Usunięcie rezystora powoduje powstanie dodatkowego szumu na przewodzie, który może blokować cały ruch w sieci. Rezystory na końcu kabla powinny znajdować się poza zasięgiem użytkowników, jeśli to w ogóle możliwe. Podobne ataki DoS mogą wystąpić, gdy użytkownicy zmodyfikują schemat okablowania sieci. Usunięcie rezystorów terminujących to tylko jedna czynność, która może powodować problemy. Koncentratory w obszarach wspólnych mogą być odłączone lub mieć usunięte złącza sieciowe. Połączenie typu hub-to-hub z token ring może zostać rozłączone, co spowoduje zerwanie integralności pierścienia, a tym samym uniemożliwi hostom sieci LAN komunikację z innymi hostami i odmowę dostępu do usług użytkownikom. Ważne jest, aby fizyczna sieć była zabezpieczona w jak największym stopniu. Menedżerowie sieci LAN powinni uczyć użytkowników, jak unikać przypadkowych problemów, które mogą wystąpić, a nawet rozpoznawać nikczemne ataki.

Modemy, serwery dial-up i linie telefoniczne

Modemy w dowolnym miejscu w sieci LAN stanowią potencjalne zagrożenie, zwłaszcza te, które są podłączone bezpośrednio do systemu użytkownika, z oficjalnymi sankcjami lub bez nich. Modemy mogą zapewnić tylne drzwi do sieci LAN, prawdopodobnie z pominięciem zapory, silnego uwierzytelniania, serwera proxy i wszelkich innych zabezpieczeń sieciowych. Chociaż modemy telefoniczne są mniej powszechne we współczesnych architekturach sieci LAN, nadal są używane do łączenia się z routerami / mostami podczas ćwiczeń związanych z rozwiązywaniem problemów z siecią. Należy zachować ostrożność, jak omówiono w tej sekcji, jeśli w celu uzyskania dostępu do urządzeń w sieci LAN używane są modemy telefoniczne. Ogólnie rzecz biorąc, wszystkie modemy powinny być skoncentrowane na serwerze dial-up sieci. W większości przypadków indywidualne systemy użytkowników powinny mieć zakaz posiadania modemów w sieci. Jest to jednak trudna reguła do wyegzekwowania, ponieważ laptopy i rosnąca liczba komputerów stacjonarnych zawierają fabrycznie zainstalowane modemy, a użytkownik zawsze może podłączyć modem zewnętrzny do portu szeregowego dowolnego systemu. To jest przykład, dlaczego menedżerowie ds. Bezpieczeństwa muszą integrować zasady z kulturą organizacji. W przeciwnym razie użytkownicy znajdą sposób na obejście zasad, które postrzegają jako zaporowe i uciążliwe, a modemy są jednym ze sposobów obejścia korporacyjnej zapory ogniowej. Szczególnie niebezpieczne są modemy w trybie automatycznej odpowiedzi. Chociaż większość firm nie reklamuje swoich numerów telefonicznych, numery te nie pozostają długo w tajemnicy przed kimś, kto chce je znaleźć. Każdy, kto ma książkę telefoniczną, może z łatwością rozpocząć mapowanie bloku firmowych numerów telefonów w organizacji. Na przykład,

jeśli główny numer to 802-555-3700, atakujący mają od czego zacząć. Gdy napastnicy dzwonią na główny numer i proszą recepcjonistkę o numer faksu organizacji, uzyskują jeszcze więcej informacji. Korzystając z oprogramowania typu war-dialer, napastnicy mogą przeskanować cały blok numerów telefonów (np. 555–3700 do 555–3799) i uzyskać listę aktywnych numerów, które odpowiadają tonem i co ten ton reprezentuje (np. faks, modem itp.). Jeśli użytkownik ma automatyczną odpowiedź modem na komputerze, atakujący mogą uzyskać dostęp do systemu użytkownika bez podania hasła. Menedżerowie ds. Bezpieczeństwa powinni współpracować z lokalnymi firmami telefonicznymi w celu uzyskania numerów telefonów dla linii modemowych, których nie ma w bloku telefonicznym organizacji. Serwer dial-up jest zatem miejscem koncentracji modemów i uwierzytelniania użytkowników dial-up. Istnieje kilka strategii uwierzytelniania na serwerze dial-up, z których najsilniejszą jest jakaś forma uwierzytelniania dwuskładnikowego, na przykład kombinacji hasła i tokena. Innym silnym mechanizmem ochrony jest zaimplementowanie mechanizmu oddzwaniania, dzięki któremu po zalogowaniu się w dobrej wierze użytkownika system rozłącza się i oddzwania na wstępnie skonfigurowany numer telefonu. Jest to bardzo skuteczny schemat, który działa dobrze w przypadku telepracowników stacjonarnych, ale nie w przypadku pracowników korzystających z roamingu. Ponadto osoby atakujące były znane z manipulowania przy centralnym przełączniku firmy telefonicznej w celu przekierowania połączenia z przypisanego numeru do własnego modemu atakującego. Gdy użytkownik wymaga dwóch oddzielnych logowań, jednego do serwera dial-up, a następnie do serwera domeny, ograniczenia bezpieczeństwa powinny określać, co może zrobić dzwoniący po przejściu pierwszego testu. Jeden z autorów tego rozdziału współpracował z firmą, która miała wspólny tajny (oksymoron) numer telefonu dla swojego banku modemów, a następnie jedną wspólną nazwę użytkownika i hasło dla wszystkich użytkowników w celu uwierzytelnienia na serwerze dial-up. Aby uzyskać dostęp do plików i udostępnionych zasobów sieciowych, użytkownik musiał następnie uwierzytelnić się na kontrolerze domeny. Jednak po przejściu identyfikacji i uwierzytelnienia dla pierwszego serwera, osoba atakująca znalazła się w sieci LAN organizacji i miała pełny, nieskrępowany dostęp do Internetu oraz tożsamość, która wskazywała na ewentualne nadużycie. Niektóre wytyczne dotyczące zabezpieczania serwerów dial-up obejmują:

* Utrzymuj i monitoruj dzienniki telefoniczne.

* Skonfiguruj całe oprogramowanie i modemy tak, aby wylogowanie użytkownika wymusiło odłączenie modemu, a odłączenie modemu wymusiło wylogowanie użytkownika.

* Skonfiguruj modemy tak, aby po każdym połączeniu wracały do domyślnej konfiguracji.

* Jeśli to możliwe, zastosuj mechanizm oddzwaniania.

* Używaj uwierzytelniania dwuskładnikowego dla użytkowników mobilnych.

* Okresowo skanuj wewnętrzne numery telefonów w poszukiwaniu nieautoryzowanych modemów.

* Zapobiegaj wyświetlaniu jakichkolwiek komunikatów banerowych, gdy użytkownik łączy się z modemem, a na pewno nie wyświetlaj żadnych komunikatów powitalnych.

* Należy przeszkolić dział pomocy technicznej organizacji w zakresie technik socjotechnicznych i zabronić im podawania numerów telefonów modemów, nazw użytkowników lub innych poufnych informacji, które mogą pomóc atakującym

Problemy z bezprzewodową siecią LAN

Bezprzewodowe sieci LAN (WLAN) mają luki w zabezpieczeniach ich przewodowych odpowiedników. Najbardziej oczywistą różnicą między sieciami przewodowymi i bezprzewodowymi jest sam nośnik.

Chociaż sieci LAN oparte na miedzi emitują niewielką ilość promieniowania, które może zostać przechwycone, cała podstawa bezprzewodowych sieci LAN polega na przesyłaniu danych przy użyciu stosunkowo silnego promieniowania w jakiejś formie. Istnieją sieci WLAN oparte na sygnałach podczerwieni, które nie mogą przenikać przez ściany budynków i dzięki temu zapewniają pewien stopień bezpieczeństwa ze względu na ograniczoną propagację tych sygnałów. Takie sieci LAN zwykle znajdują się w sieciach wymagających wysokiego poziomu bezpieczeństwa. Jednak większość dzisiejszych sieci WLAN wykorzystuje techniki transmisji radiowej. W tych sieciach każdy na pobliskiej ulicy może użyć urządzenia nasłuchującego do przechwycenia danych, a nawet przechwycenia identyfikatorów sieciowych wymaganych do połączenia z siecią LAN. Praktyczny zakres przechwytywania jest regulowany przez prawo odwrotnych kwadratów dla siły sygnału (zmniejsza się ona jako kwadrat odległości od źródła) oraz przez czułość i charakterystykę sygnału do szumu odbiorników. Na szczęście w samej warstwie fizycznej istnieje pewna miara bezpieczeństwa. Sieci LAN oparte na standardzie IEEE (Institute of Electrical and Electronics Engineers) w standardzie 802.11 wykorzystują techniki rozproszenia widma bezpośredniego (DSSS) lub widma rozproszonego z przeskokiem częstotliwości (FHSS). Jak zwykle w zależności od zasięgu i poziomu hałasu możliwe jest podsłuchiwanie. Jednak interpretacja sygnałów jest trudniejsza ze względu na sposób, w jaki DSSS i Praca FHSS. Aby nadać sens transmisji, odbiornik musi znać albo kod chipowania używany w sieci DSSS, albo wzorzec przeskoku częstotliwości w implementacji FHSS. Bez takich informacji sygnał będzie wydawał się niczym innym jak szumem tła w pasmach radiowych przemysłowych, naukowych i medycznych (ISM) dla nielegalnego odbiornika. Nie jest to problem nie do pokonania dla potencjalnego podsłuchującego, ale współczynnik pracy jest znacznie wyższy w porównaniu z technikami radiowej łączności wąskopasmowej. Podejście z widmem rozproszonym zapewnia również większą niezawodność w obliczu zakłóceń spowodowanych odmową usługi (tj. Celowym zagłuszaniem), ponieważ sygnał jest rozproszony w szerokim zakresie częstotliwości. Niektóre urządzenia sprzedawane są również z komponentami oprogramowania, które umożliwiają dostrojenie wokół zakłóceń. Na przykład poprawka IEEE 802.11g wykorzystuje nowszy ortogonalne zwielokrotnianie z podziałem częstotliwości (OFDM) z 802.11a dla wyższych prędkości danych, ale jest wstecznie kompatybilna z 802.11b przy użyciu DSSS, który już używał tego samego pasma częstotliwości ISM. Obsługiwane są szybkości transmisji danych DSSS 1, 2, 5,5 i 11 Mb / s, a także szybkości transmisji danych OFDM 6, 9, 12, 18, 24, 48 i 54 Mb / s. IEEE wymaga tylko obowiązkowych szybkości transmisji danych OFDM przy użyciu 6, 12 i 24 Mb / s, niezależnie od tego, czy jest to 802.11a, czy 802.11g OFDM. Aby zapewnić większą prywatność niż zapewniana przez samą warstwę fizyczną, standard 802.11 zawiera opcjonalną metodę szyfrowania zwaną Wired Equivalent Privacy (WEP). Ta technika jest naprawdę opcjonalna, więc nie wszyscy dostawcy obsługują standard. WEP domyślnie używa 40-bitowej formy algorytmu RC4, chociaż niektóre produkty obsługują silniejsze wersje 128-bitowe. Dobrym pomysłem jest wybranie produktu, który oferuje więcej niż tylko wersję 40-bitową, ponieważ 40-bitowa przestrzeń klawiszy nie zapewnia dużego bezpieczeństwa, biorąc pod uwagę dzisiejszą moc obliczeniową. Ponieważ WEP nie oferuje silnego szyfrowania i nie opisuje standardowego mechanizmu wymiany kluczy, wielu dostawców wdrożyło metody tunelowania warstwy trzeciej, takie jak te stosowane w wirtualnych sieciach prywatnych (VPN), aby zapewnić większą prywatność. Te podejścia oparte na sieci VPN zazwyczaj wykorzystują inne procesy szyfrowania (np. Szyfrowanie Microsoft Point-to-Point), takie jak stosowane w protokole tunelowania Point-to-Point (PPTP), które używają dłuższych kluczy niż WEP i często obsługują infrastrukturę kluczy publicznych (PKI) lub inne mechanizmy wymiany kluczy. Niektóre implementacje zapewniają również uwierzytelnianie za pomocą standardów, takich jak usługa zdalnego dostępu telefonicznego użytkownika (RADIUS), co zapewnia bardziej elastyczne zarządzanie klientami. Główny problem polega na tym, że nie wszystkie te podejścia są interoperacyjne i niekoniecznie obsługują wiele protokołów. WEP może być również używany do uwierzytelniania, aby zapobiec nieautoryzowanemu dostępowi do samej sieci WLAN.

Takie uwierzytelnianie dodaje kolejną warstwę ochrony do kombinacji nazwy użytkownika i hasła używanej przez typowe oprogramowanie serwera. Przed uzyskaniem dostępu do zasobów informacyjnych na serwerze klient musi najpierw uzyskać dostęp do fizycznego nośnika. Korzystając ze schematu klucza współdzielonego, urządzenie bezprzewodowe musi mieć ten sam klucz szyfrowania, co punkt dostępu do sieci LAN, urządzenie umożliwiające łączność bezprzewodową przewodowa część sieci LAN. Wszelkie przesyłane dane muszą być zaszyfrowane za pomocą klucza, w przeciwnym razie ramka zostanie zignorowana. Wiele produktów dostępu bezprzewodowego ma również możliwość tworzenia list kontroli dostępu na podstawie adresów MAC w celu filtrowania połączeń LAN. Standard bezpieczeństwa IEEE 802.11i-2004 lub 802.11i, wdrożony jako Wi-Fi Protected Access II (WPA2), jest poprawką do oryginalnego IEEE 802.11. WPA2 został pierwotnie opracowany przez Wi-Fi Alliance (www.wi-fi.org). Ten standard określa mechanizmy bezpieczeństwa dla sieci bezprzewodowych. Zastąpił on krótką klauzulę uwierzytelniania i prywatności pierwotnego standardu IEEE 802.11 szczegółową klauzulą bezpieczeństwa. W trakcie tego procesu wycofał oryginalną metodę szyfrowania WEP. Poprawka została później włączona do opublikowanego standardu IEEE 802.11-2007. Podsumowując, menedżerowie sieci powinni wziąć pod uwagę następujące elementy bezpieczeństwa podczas oceny składników sieci bezprzewodowej:

Schematy warstw fizycznych

* Podczerwień. Nie przenika przez ściany i jest dobra do zastosowań wymagających wysokiego bezpieczeństwa.

* FHSS. Przeskakiwanie sygnału zapewnia dobry poziom bezpieczeństwa, ale złożoność techniki ogranicza przepustowość.

* DSSS. Niski „współczynnik rozprzestrzeniania" może zwiększyć dostępną przepustowość, ale także możliwość przechwytywania i zagłuszania.

* OFDM. Używany do wyższych szybkości transmisji danych w nowszych sieciach WLAN, ale może być bardziej wrażliwy na szum i zakłócenia.

Opcje szyfrowania

* WEP. Przestarzałe w 2004 roku, powszechnie używane klucze 40-, 64- lub 128-bitowe z algorytmem Rivest Cipher 4 (RC4).

* Dostęp zabezpieczony Wi-Fi II. Bardziej bezpieczna alternatywa dla WEP, wykorzystująca tryb licznika Advanced Encryption Standard (AES) / protokół CBC-MAC (CCMP) .5

* Alternatywne metody szyfrowania. Często bezpieczniejsze niż WEP i WPA2, ale nie zawsze interoperacyjne.

Metody uwierzytelniania

* Wired Equivalent Privacy. Używa trybu klucza wstępnego (PSK), który wymaga od klientów posiadania tego samego klucza szyfrowania, co punkt dostępu sieci LAN, co powoduje problemy z zarządzaniem kluczami.

* Dostęp zabezpieczony Wi-Fi II. WPA2 obsługuje uwierzytelnianie IEEE 802.1X / EAP lub technologię PSK.

* Lista kontroli dostępu. Umożliwia tylko niektórym klientom fizyczny dostęp do sieci LAN na podstawie adresu MAC; zwiększa to złożoność zarządzania klientami.

* Uwierzytelnianie na serwerze. Elastyczne uwierzytelnianie użytkowników za pomocą RADIUS dla dodatkowej warstwy ochrony przed nielegalnymi połączeniami

PROBLEMY Z SYSTEMEM OPERACYJNYM SIECI

We wczesnych latach 90-tych często spotyka się komputery stacjonarne z systemem operacyjnym Windows i sieciowym systemem operacyjnym Novell NetWare (NOS). Aplikacje komputerowe działały w systemie Windows, a NetWare był używany tylko do przenoszenia plików do i ze współdzielonej przestrzeni plików lub do drukowania dokumentów. Dzisiaj różnica między systemem operacyjnym dla komputerów stacjonarnych, systemem operacyjnym serwera i systemem NOS zniknęła. Systemy operacyjne, takie jak Linux, MacOS, UNIX i Windows, zapewniają pakiety aplikacji komputerowych z funkcjami sieciowymi, w tym protokołami komunikacyjnymi, takimi jak TCP / IP. Istnieją pewne ogólne uwagi dotyczące bezpieczeństwa we wszystkich sieciach LAN, niezależnie od konkretnego systemu operacyjnego:

* Korzystaj z możliwości oferowanych przez system operacyjny, aby stosować silne hasła.

* Twórz zasady dotyczące haseł, które wymuszają silne hasła. Okresowo zmieniaj hasła i nie zezwalaj na ich ponowne użycie. Okresowo kontroluj hasła za pomocą narzędzi do łamania haseł, takich jak L0phtCrack (Windows) lub crack (UNIX). Upewnij się, że konta administratora i roota otrzymały hasła, które nie są szeroko rozpowszechniane ani odgadywane.

* Wyłącz (lub odinstaluj) wszelkie usługi, które nie są używane.

* Aktualizuj system operacyjny i aplikacje oraz instaluj najnowsze poprawki zabezpieczeń.

* Ostrożnie zarządzaj listami kontroli dostępu do plików i innych zasobów systemowych / sieciowych.

* Ściśle zdefiniuj użytkowników, grupy i relacje zaufania sieci / domeny.

* Dokładnie zabezpiecz wszystkie uruchomione aplikacje.

* Zaloguj się jako administrator lub root tylko wtedy, gdy jest to konieczne; w przeciwnym razie zaloguj się jako zwykły użytkownik.

* Zezwalaj operatorom i administratorom na logowanie się tylko lokalnie na serwerach.

* Ogranicz korzystanie z kont gości, kont demo lub anonimowych.

* Jeśli to możliwe, umieść pliki rozruchowe i systemowe, a także pliki aplikacji i dane na różnych partycjach, dyskach twardych lub kontrolerach wejścia / wyjścia (I / O).

* Regularnie kontroluj systemy serwerowe.

* Pliki dziennika monitora.

* Usuń dyskietki, dyski CD, DVD i pendrive'y z serwerów po stabilnej konfiguracji systemu.

* Stosuj najlepsze praktyki branżowe podczas zabezpieczania systemu operacyjnego.

* Regularnie używaj narzędzi do oceny podatności, aby skanować serwery.

* Użyj narzędzi do wykrywania włamań, aby monitorować potencjalne ataki na sieć LAN, które są uruchamiane z sieci wewnętrznej.

* Jeśli używasz prostego protokołu zarządzania siecią (SNMP) do administrowania siecią, ostrożnie wybieraj nazwy społeczności i blokuj zewnętrzny dostęp do usługi SNMP. Tam, gdzie to możliwe, bazy informacji zarządzania (MIB) powinny być tylko do odczytu.

* Unikaj używania rekordu zasobu DNS HINFO (informacje o hoście) do identyfikacji typu jednostki centralnej i zainstalowanego systemu operacyjnego.

Określone luki w systemie operacyjnym wykraczają poza zakres tego rozdziału; całe książki i strony internetowe poświęcone są zabezpieczaniu niektórych z tych pojedynczych systemów operacyjnych. Menedżerowie sieci muszą przynajmniej monitorować witrynę internetową producenta swojego systemu operacyjnego i wszystkie inne witryny, które zapewniają bezpieczeństwo sieciowej sieci. Poniższe sekcje zawierają ogólne spostrzeżenia i komentarze dotyczące różnych sieciowych systemów operacyjnych.

UNIX

UNIX to najstarszy system operacyjny, który jest nadal szeroko rozpowszechniony (i wciąż rośnie). Czytelnicy potrzebujący wskazówek dotyczących Novell Netware powinni zapoznać się z Rozdziałem 18 w czwartym wydaniu tego podręcznika. Pierwotnie opracowany w 1969 roku w AT&T Bell Laboratories, UNIX stał się pierwszym systemem operacyjnym integrującym komunikację sieciową, kiedy TCP / IP został dołączony do Berkeley Software Development (BSD) 4.2 UNIX w 1984 roku. UNIX był tradycyjnie zarezerwowany dla systemów serwerowych i zagorzałych użytkowników komputerów. Wraz z rozwojem interfejsu X-Windows dla UNIX i szerokim wdrożeniem Linuksa od połowy lat 90-tych, UNIX i jego warianty stanowią jedyną znaczącą konkurencję dla Windows w środowisku desktopowym i serwerowym. Podobnie jak TCP / IP i sam Internet, system UNIX został opracowany pod kątem funkcjonalności i użytku w zaufanej społeczności użytkowników. W związku z tym, chociaż UNIX ma wiele potężnych narzędzi, nie ma spójnej architektury zabezpieczeń ani nie jest z natury bezpiecznym systemem operacyjnym. UNIX ma większość podstawowych zabezpieczeń systemu operacyjnego: hasła, listy kontroli dostępu, grupy, poziomy uprawnień użytkowników i tak dalej. Ale UNIX jest również wyposażony w szeroką gamę usług (demonów) włączonych domyślnie, w tym protokół przesyłania plików (FTP), Telnet, finger, echo, chargeen, daytime, Remote Procedure Call (RPC), BIND i inne. Ponadto prawie każdy demon UNIX miał jakąś lukę w zabezpieczeniach zgłaszaną w takim czy innym czasie, przy czym przepełnienia bufora były dość powszechne. Jest wiele rzeczy, które administrator powinien wziąć pod uwagę podczas zabezpieczania systemu UNIX / Linux. Oprócz opisanych powyżej kroków ogólnych menedżer zabezpieczeń może również:

* Wyłącz (lub usuń) wszelkie nieużywane usługi, w szczególności finger, demona nazwy BIND (nazwany), RPC, sendmail, Trivial FTP (tftp), Post Office Protocol (POP), Internet Message Access Protocol (IMAP), sadmind, mountd, i sieciowy system plików (NFS).

* Zainstaluj najnowszą wersję i poprawkę bezpieczeństwa całego zainstalowanego oprogramowania.

* Zachowaj szczególną ostrożność podczas konfigurowania list kontroli dostępu i innych funkcji udostępniania.

* Zapobiegaj uruchamianiu Sendmaila w trybie demona (wyłącz przełącznik -bd) na maszynach, które nie są ani serwerami pocztowymi, ani przekaźnikami poczty.

* Ogranicz użycie protokołów zdalnego dostępu „r”.

* Użyj plików haseł w tle.

* Zaimplementuj opakowania TCP, aby kontrolować dostęp do usług.

* Rozważ użycie szyfrowanych protokołów komunikacyjnych, takich jak Secure Shell (SSH) lub Secure Sockets Layer (SSL), aby uzyskać dostęp zdalny. Zapobiegaj przesyłaniu haseł w postaci zwykłego tekstu przez Internet.

Jedną z najważniejszych możliwości menedżera sieci / bezpieczeństwa jest audyt systemów serwerowych Windows w celu ochrony ich integralności. Te narzędzia są częścią podstawowego systemu operacyjnego lub zestawu Windows NT Resource Kit:

* netstat sprawdza otwarte porty.

* lsof wyświetla ukrytą przestrzeń plików i połączenia sieciowe.

* tcpdump wyświetla ruch sieciowy.

* który wyświetla zalogowanych użytkowników i plik dziennika utmp.

* last wyświetla historię logowania i plik dziennika wtmp.

* lastb wyświetla historię złych logowań (i plik dziennika btmp).

* syslogd to centralny serwer do zarządzania i rejestrowania komunikatów systemowych.

* TCPWrapper monitoruje i zarządza przychodzącymi żądaniami usług.

MacOS

Systemy operacyjne Macintosh w większości ustąpiły miejsca innym platformom. To powiedziawszy, nadal warto o nich wspomnieć, ponieważ udział Apple w rynku we wszystkich dziedzinach został nieco wzmocniony w ostatnich latach dzięki jego sile w urządzeniach mobilnych i tabletach. Macintosh był pierwszym systemem operacyjnym dla komputerów stacjonarnych, który obejmował sieci i udostępnianie zasobów za pośrednictwem AppleTalk jako integralne elementy. Ale jak UNIX a wcześniej TCP / IP, MacOS został zaprojektowany z myślą o wygodzie i użyteczności, ale nie ze względu na bezpieczeństwo. Ze względu na swój charakter peer-to-peer, MacOS tradycyjnie miał wiele potencjalnych zagrożeń. Chociaż Windows i UNIX mogą również działać w trybie peer-to-peer, początkujący użytkownik na ogół nie wiedziałby, jak współdzielić zasoby, a tym samym nie może przypadkowo otworzyć dziur. Na przykład nikczemny użytkownik sieci Mac może szybko sprawdzić, jakie serwery i udziały są dostępne w sieci, korzystając z oryginalnego akcesorium Chooser. Komputery Mac miały stosunkowo niewielkie zabezpieczenia. Ochrona hasłem była zapewniana domyślnie tylko w niektórych laptopach i nawet chroniony hasłem wygaszacz ekranu nie był standardowo dostarczany z systemem. Krótko mówiąc, różnica między zdeterminowanym napastnikiem a komputerem Mac jest bardzo mała. Wymagane było oprogramowanie innej firmy, aby zapewnić ochronę hasłem przed dostępem do systemu i plików lub do ochrony danych za pomocą szyfrowania dysku. Wirusy i robaki na komputerach Mac nadal są znacznie mniej rozpowszechnione niż ich odpowiedniki w systemie Windows, ale komputery Mac nie są całkowicie odporne. Po pierwsze, te wirusy, od których zależy oprogramowanie Microsoft Office Suite będzie działać, ponieważ wersje programów Word i Excel dla komputerów Mac wykorzystują makra. Po drugie, ataki internetowe skierowane na TCP / IP - takie jak ping-of-death, Teardrop i SMURF - mogą nadal wpływać na serwer Mac. Dostępnych jest więcej opcji dodatkowych zabezpieczeń niż w przeszłości, dzięki pakietom takim jak NortonTM Antivirus dla Mac i Norton Internet Security for Mac R są podobne do swoich odpowiedników w innych systemach operacyjnych. Mac OS przeszedł fundamentalną transformację od ostatniego „klasycznego” wydania OS 9 w 1999 roku. Wraz z pojawieniem się OS X, Apple przedstawił swoją pierwszą platformę opartą na UNIX, która była wstępnie ładowana na wszystkie komputery Macintosh od 2002 roku. Wersja 10.5

(Leopard) został wydany w 2007 roku i dodał szereg ulepszeń bezpieczeństwa dla zajęcie się słabymi punktami tradycyjnych platform, w tym:

* Bezpieczne konto gościa

* Zapora warstwy aplikacji

* Podpisywanie aplikacji

* Piaskownice

* Pełne szyfrowanie dysku

* Randomizacja biblioteki

Intencją Apple było zapewnienie większego wyprzedzania ataków, a także odporności na nie, a firma kontynuowała opracowywanie lepszych zabezpieczeń przez cały cykl życia systemu OS X. Obecnie w wersji 10.8 (Mountain Lion), która została wydana w 2012 roku, platforma zawiera wiele tych samych funkcji, co poprzednie iteracje, z ulepszoną kontrolą administracyjną i opcjami prywatności. Jedno z największych wyzwań związanych z bezpieczeństwem koncepcyjnie nie jest unikalne dla komputerów Macintosh, ale wraz ze zwiększoną integracją usług iCloud firmy Apple w systemie OS X (nie wspominając o iOS w przestrzeni mobilnej), istnieje większe ryzyko przenoszenia plików z pamięci lokalnej do sieciowej . Użytkownicy oczekują dostępu do danych z dowolnego urządzenia w dowolnym miejscu i czasie, a ta wygoda sprawia, że wszystkie zgubione lub skradzione laptopy, tablety i telefony stanowią poważne ryzyko.

Podczas gdy fortuny MacOS rosły, malały i rosły, nadal odnotowuje się mniej incydentów bezpieczeństwa, ponieważ większa popularność innych platform ułatwia ich poznanie, ponieważ jest więcej potencjalnych celów i ponieważ jeden atak może wpłynąć na więcej systemów . Innymi słowy, jest mniej ataków na komputery Mac, ponieważ społeczność hakerów nie jest z nimi zbyt zaznajomiona, a także jest mniej atrakcyjnych celów wartych kosztów alternatywnych. Mimo to równie ważne jest, aby aktualizować wersję systemu MacOS, podobnie jak w przypadku innych systemów operacyjnych.

WNIOSEK

Dobry administrator może zabezpieczyć prawie każdy NOS, chociaż żaden NOS nie jest początkowo bezpieczny. Administrator sieci potrzebuje ciągłej czujności i monitorowania, jednocześnie zdając sobie sprawę, że system operacyjny jest tylko częścią ogólnego planu bezpieczeństwa dla sieci LAN i usług sieciowych. Większość administratorów sieci, ze względu na charakter swojej pracy i szkolenia, koncentruje się wyłącznie na komputerach podłączonych do sieci LAN oraz do systemu operacyjnego i oprogramowania sieci LAN. Niestety podejście to jest zbyt wąskie w swoim zakresie. Oprogramowanie zapory osobistej może być również wykorzystywane do ochrony poszczególnych systemów przed atakiem, ale prawie wszystkie te produkty są zorientowane na ataki oparte na protokole IP i ataki pomijane, które wykorzystują natywny system operacyjny sieciowej sieci kontaktów. Routery, zapory sieciowe i serwery proxy są niezbędne do ochrony systemów LAN przed atakiem ze źródła zewnętrznego. Administrator sieci musi również zapewnić narzędzia do ochrony serwerów i stacji roboczych przed innymi użytkownikami w sieci LAN.