SYSTEMY OCHRONY SIECI

Hakerzy mają do dyspozycji wiele narzędzi do atakowania sieci. Widziałeś, jak skanowanie portów i enumeracja umożliwiają atakującym określenie usług działających na komputerach i uzyskanie dostępu do zasobów sieciowych. W tym module przyjrzysz się systemom ochrony sieci, które mogą być używane do zmniejszania narażenia na te ataki i ograniczania ich występowania. W tym module omówiono routery, zapory sprzętowe i programowe, filtrowanie sieci, systemy wykrywania i zapobiegania włamaniom oraz honeypoty. System ochrony sieci może również obejmować zespół reagowania na incydenty bezpieczeństwa, który jest zespołem osób odpowiedzialnych za ochronę dużej sieci.

UŻYWANIE SYSTEMÓW OCHRONY SIECI

Aby chronić sieć przed atakami, specjaliści ds. bezpieczeństwa muszą wiedzieć, jak korzystać z systemów ochrony sieci, takich jak routery, zapory sieciowe, systemy wykrywania i zapobiegania włamaniom, filtrowanie sieci i honeypoty. Na potrzeby tej książki system ochrony sieci to po prostu dowolne urządzenie lub system zaprojektowany w celu ochrony sieci. Urządzenie Unified Threat Management (UTM) to pojedyncze urządzenie, które łączy wiele funkcji ochrony sieci, takich jak te wykonywane przez routery, zapory sieciowe, systemy wykrywania i zapobiegania włamaniom, sieci VPN, systemy filtrowania sieci oraz systemy wykrywania i filtrowania złośliwego oprogramowania. Na przykład nowoczesne routery Cisco mogą wykonywać funkcje zapory sieciowej, translację adresów (translację adresów sieciowych i translację adresów portów) oraz zapobieganie włamaniom oprócz funkcji routera. Termin urządzenie zabezpieczające może opisywać zarówno UTM, jak i systemy ochrony sieci. W miarę jak technologia sprzętowa staje się coraz bardziej wydajna, urządzenia zabezpieczające mogą wykonywać te same funkcje, które kiedyś były wymagane przy użyciu kilku dedykowanych systemów. Zmniejszają również nakład pracy administracyjnej, ponieważ wiele funkcji ochrony sieci jest zarządzanych za pośrednictwem wspólnego interfejsu. W tej sekcji zapoznasz się z systemami ochrony sieci, obserwując, jak routery służą do ograniczania ataków sieciowych.

Wykorzystanie routerów do redukcji ataków sieciowych

Routery, które działają na warstwie sieciowej stosu protokołów TCP/IP, to urządzenia sprzętowe używane do wysyłania pakietów do różnych segmentów sieci. Ich głównym celem jest redukcja ruchu rozgłoszeniowego przechodzącego przez sieć i wybór najlepszej ścieżki do przesyłania pakietów. Na przykład, jeśli router A w Hiszpanii chce wysłać pakiet do routera B w Iowa, pakiet prawdopodobnie może podążać kilkoma ścieżkami. Routery wykorzystują protokoły routingu w tym procesie podejmowania decyzji o najlepszej ścieżce, które działają w następujący sposób:

• Protokół routingu stanu łącza — router używający protokołu routingu stanu łącza wysyła reklamy stanu łącza do innych routerów; reklamy te identyfikują topologię sieci i wszelkie zmiany lub ścieżki ostatnio odkryte w sieci. Na przykład, jeśli nowy router lub ścieżka stanie się dostępna dla pakietu, informacja ta jest wysyłana do wszystkich innych routerów uczestniczących w sieci. Ta metoda jest wydajna, ponieważ tylko nowe informacje są wysyłane przez sieć. Przykładem protokołu routingu stanu łącza jest protokół Open Shortest Path First (OSPF).

• Protokół routingu wektora odległości — jeśli router używa protokołu routingu wektora odległości, przekazuje swoją tabelę routingu (zawierającą wszystkie możliwe ścieżki, które odkrył) sąsiednim routerom w sieci. Te sąsiednie routery przekazują następnie tabelę routingu swoim sąsiadom. Dwa przykłady protokołów routingu wektora odległości

to protokół Routing Internet Protocol w wersji 2 (RIPv2) i Enhanced Interior Gateway Routing Protocol (EIGRP).

• Protokół routingu wektora ścieżki — protokół routingu wektora ścieżki wykorzystuje dynamicznie aktualizowane ścieżki lub tabele routingu do przesyłania pakietów z jednej autonomicznej sieci do drugiej. Nie jest używany w sieciach LAN, ponieważ jest używany głównie przez dostawców usług internetowych i duże organizacje z wieloma połączeniami internetowymi z innymi dostawcami usług internetowych i organizacjami. Głównym protokołem routingu wektora ścieżki jest protokół Border Gateway Protocol (BGP), protokół routingu, którego dostawca usług internetowych używa do przesyłania pakietów do ich miejsc docelowych w Internecie. Jako specjalista ds. bezpieczeństwa Twoim głównym zmartwieniem jest potwierdzenie, że router filtruje określony ruch, a nie projektowanie infrastruktury routera i określanie protokołu routingu używanego przez organizację. Poniższa sekcja wyjaśnia, jak router Cisco jest skonfigurowany do filtrowania ruchu.

BAJTY BEZPIECZEŃSTWA

BGP ma pewne luki w zabezpieczeniach. Na przykład atakujący mogą przejąć przestrzeń IP należącą do innego dostawcy usług internetowych, wstrzykując złośliwą reklamę routingu BGP dla prefiksu sieciowego, którego nie posiadają. W prima aprilis 2020 r., gdy świat oswajał się z pandemią COVID-19, ruch internetowy, który miał przepływać przez ponad 200 dostawców usług internetowych w chmurze i sieci dostarczania treści, został przekierowany przez Rostelcom, rosyjskiego państwowego dostawcę usług telekomunikacyjnych. Ponad 8000 tras ruchu internetowego było dotkniętych przez około dwie godziny, spowalniając lub zatrzymując ruch pochodzący z lub przeznaczony dla Amazon, Google, Facebook i wielu innych witryn. Aby uzyskać więcej informacji na temat tego incydentu przejęcia BGP, odwiedź stronę www.darkreading.com/edge-articles/101-why-bgp-hijacking-just-won-t-die.

Konfigurowanie podstawowych routerów sprzętowych

W tej sekcji routery Cisco są używane jako przykład, ponieważ są szeroko stosowane; miliony routerów Cisco są używane przez firmy na całym świecie. Ponieważ Cisco stało się tak powszechnym standardem wśród profesjonalistów sieciowych, dostawcy oferujący konkurencyjne produkty często projektują swoje interfejsy konfiguracyjne tak, aby były podobne do Cisco. Tak więc, chociaż informacje w tej sekcji mogą pomóc w przeprowadzaniu testów bezpieczeństwa w firmach wykorzystujących routery Cisco w swoich sieciach, nie będziesz całkowicie zagubiony, jeśli zobaczysz produkt konkurencji Cisco, takiej jak Juniper. Zasady, których uczysz się w tym module, można zastosować do innych typów routerów. W Ćwiczeniu 13-1 odwiedzasz witrynę Cisco i przeglądasz niektóre produkty Cisco. Jeśli nigdy nie widziałeś routera ani nie pracowałeś z interfejsami omówionymi w tej sekcji, zdjęcia produktów na tej stronie mogą dać ci wyobrażenie o tym, z czym będziesz pracować jako profesjonalista ds. bezpieczeństwa. Pamiętaj, że router Cisco to system wbudowany, który do działania wykorzystuje system operacyjny Cisco Internetwork Operating System (IOS).

Wizyta na stronie internetowej Cisco

Wymagany czas: 30 minut

Cel: Przegląd produktów routingowych Cisco.

Opis: Produkty routingowe Cisco będą ważną częścią Twojej pracy jako specjalisty ds. bezpieczeństwa, ponieważ wiele firm z nich korzysta. W tej aktywności odwiedzasz stronę internetową firmy i przeglądasz informacje o podatnościach, które Cisco udostępnia swoim klientom. Informacje te mogą być pomocne, jeśli wykonujesz test bezpieczeństwa w sieci przy użyciu routerów Cisco.

1. Uruchom przeglądarkę internetową i przejdź do www.cisco.com. Na stronie głównej Cisco kliknij Produkty i usługi w górnym menu, kliknij Sieci w lewym panelu, a następnie kliknij Routery.

2. Na stronie Routery kliknij Produkty na pasku nawigacyjnym. W momencie pisania tego tekstu strona routerów Cisco grupuje swoje routery w sześciu kategoriach: Oddział, Agregacja WAN, Dostawca usług, Przemysł, Wirtualny i Mały biznes. Zapoznaj się z dostępnymi typami produktów. Do której kategorii należy główny router w Twojej szkole? Być może będziesz musiał zapytać swojego instruktora, jakiego typu routera używa Twoja szkoła. Jeśli nie jest to produkt Cisco, kto jest dostawcą?

3. Przejdź do https://tools.cisco.com/security/center/. W polu tekstowym wyszukiwania Cisco Security wpisz ios i naciśnij Enter, aby wyświetlić listę tematów związanych z lukami w zabezpieczeniach systemu IOS. Przeanalizuj niektóre niedawne luki w zabezpieczeniach systemu Cisco IOS.

4. Przejdź do https://nvd.nist.gov. Kliknij 1 (znak plus) obok pozycji Luki w zabezpieczeniach, aby otworzyć menu Luki w zabezpieczeniach, a następnie kliknij Szukaj i statystyki, aby otworzyć stronę Bazy danych luk w zabezpieczeniach. W polu wyszukiwania słów kluczowych wpisz Cisco ios i naciśnij Enter. Przez resztę tej aktywności korzystaj z tej witryny i zwróconych informacji.

5. Przeanalizuj wyniki wyszukiwania. Ile rekordów zostało zwróconych?

6. Kliknij łącza zaczynające się od CVE-, aby przeczytać szczegółowe informacje o niektórych lukach w zabezpieczeniach. Znajdź CVE z bazą CVSS co najmniej 7. Co luka umożliwia atakującemu? W przypadku luk w oprogramowaniu witryna NVD udostępnia łącza do witryny dostawcy, aby znaleźć poprawkę lub obejście. Kliknij łącze do witryny Cisco i przeczytaj informacje. Co zaleca Cisco?

7. Zamknij przeglądarkę i wyloguj się z systemu Windows, aby wykonać następną czynność.

Jak widać z lektury, system Cisco IOS ma luki w zabezpieczeniach, podobnie jak każdy system operacyjny, dlatego specjaliści ds. bezpieczeństwa muszą wziąć pod uwagę typ używanego routera podczas przeprowadzania testu bezpieczeństwa.

BAJTY BEZPIECZEŃSTWA

Podczas konferencji Black Hat poświęconej bezpieczeństwu komputerowemu 24-letni badacz o nazwisku Michael Lynn otrzymał od Cisco polecenie, aby nie wygłaszał prezentacji na temat luk w zabezpieczeniach, które znalazł w routerach internetowych Cisco. Pan Lynn twierdził, że luki te umożliwią hakerom przejęcie sieci korporacyjnych i rządowych. Cisco argumentowało, że ujawnienie jego ustaleń opinii publicznej było nielegalne i że pan Lynn znalazł luki, dokonując inżynierii wstecznej produktu Cisco, co jest również nielegalne w Stanach Zjednoczonych. Większość firm technologicznych nie chce, aby luki w zabezpieczeniach ich produktów były ujawniane opinii publicznej, dopóki nie będą miały szansy samodzielnie naprawić problemu lub nie będą mogły kontrolować, jakie informacje są udostępniane opinii publicznej. Kwestia ujawniania informacji będzie obecna przez jakiś czas i z całą pewnością wpłynie na testerów bezpieczeństwa.

Składniki routera Cisco

Aby pomóc Ci zrozumieć, w jaki sposób routery są używane jako systemy ochrony sieci, ta sekcja opisuje składniki routera Cisco. Podobnie jak administrator systemu musi rozumieć polecenia do konfigurowania serwera, administratorzy routerów Cisco muszą znać polecenia do konfigurowania routera Cisco. Wiele składników routera Cisco jest podobnych do składników komputera, więc poniższe składniki powinny wydawać się znajome:

• Pamięć o dostępie swobodnym (RAM) — Ten składnik przechowuje bieżącą konfigurację routera, tabele routingu i bufory. Jeśli wyłączysz router, zawartość zapisana w pamięci RAM zostanie usunięta. Wszelkie zmiany wprowadzone w konfiguracji routera, takie jak zmiana wyświetlanego monitu, są przechowywane w pamięci RAM i nie są trwałe, chyba że zapiszesz konfigurację.

• Pamięć RAM nieulotna (NVRAM) — Ten składnik przechowuje plik konfiguracyjny routera, ale informacje nie zostaną utracone, jeśli router zostanie wyłączony.

• Pamięć flash — Ten składnik przechowuje system operacyjny IOS używany przez router. To pamięć nadpisywalna, więc możesz uaktualnić system IOS, jeśli Cisco wyda nową wersję lub bieżąca wersja systemu IOS zostanie uszkodzona.

• Pamięć tylko do odczytu (ROM) — Ten komponent zawiera minimalną wersję systemu Cisco IOS, która jest używana do uruchomienia routera, jeśli pamięć flash zostanie uszkodzona. Możesz uruchomić router, a następnie naprawić wszelkie problemy z systemem IOS, ewentualnie instalując nową, nieuszkodzoną wersję.

• Interfejsy — Te komponenty to punkty łączności sprzętowej z routerem i komponenty, które najbardziej Cię interesują. Na przykład port Ethernet to interfejs, który łączy się z siecią LAN i może być skonfigurowany tak, aby ograniczać ruch z określonego adresu IP, podsieci lub sieci.

Jako specjalista ds. bezpieczeństwa powinieneś znać podstawowe polecenia Cisco, aby wyświetlać informacje w tych komponentach. Na przykład, aby zobaczyć, jakie informacje są przechowywane w pamięci RAM, administrator Cisco używa tego polecenia (z pogrubionym tekstem wskazującym rzeczywiste polecenie):

RouterB# show running-config

Here’s an example of the abbreviated output of this command for a production router:

Building configuration...

Current configuration : 4422 bytes

! version 12.4

service timestamps debug datetime msec localtime

service timestamps log datetime msec localtime

no service password-encryption

!

hostname R3825_2

!

boot-start-marker

boot-end-marker

!

card type t100

logging buffered 51200 debugging

```
!
no aaa new-model
!
resource policy
!
clock timezone Hawaii -10
network-clock-participate wic 0
network-clock-select 1 T1 0/0/0
ip subnet-zero
ip cef
!
interface GigabitEthernet0/0
description $ETH-LAN$$ETH-SW-LAUNCH$$INTF-INFO-GE 0/0$
ip address 192.168.10.3 2 55.255.255.0
duplex auto
speed auto
media-type rj45
negotiation auto
h323-gateway voip interface
h323-gateway voip bind srcaddr 192.168.10.3
!
interface Serial0/0/0:23
no ip address
isdn switch-type primary-ni
isdn incoming-voice voice
isdn bind-l3 ccm-manager
no cdp enable
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.10.1
!
```

ip http server

username netdef privilege 15 secret 5

1pod7$ZZWTCxA9O8iBSJbd3tIlL1

!

end

RouterB#

Konfiguracja routera Cisco

Router Cisco ma dwa tryby dostępu: tryb użytkownika i tryb uprzywilejowany. W trybie użytkownika administrator może wykonywać podstawowe testy rozwiązywania problemów i wyświetlać informacje przechowywane na routerze. W trybie uprzywilejowanym administrator może wykonywać pełne zadania konfiguracji routera. Możesz sprawdzić, w jakim trybie dostępu się znajdujesz, patrząc na monit. Nazwa routera, po której następuje symbol >, na przykład Router>, oznacza, że jesteś w trybie użytkownika. Nazwa routera, po której następuje znak #, na przykład Router#, oznacza, że jesteś w trybie uprzywilejowanym, zwanym również trybem włączania. Podczas pierwszego logowania do routera Cisco domyślnie jesteś w trybie użytkownika. Aby zmienić tryb na uprzywilejowany, wprowadź polecenie enable, które można skrócić do en. Zazwyczaj musisz wprowadzić hasło, aby użyć tego polecenia, chyba że administrator routera Cisco ma niewielkie doświadczenie i nie określił hasła. Po przejściu do trybu uprzywilejowanego należy wprowadzić inne polecenie w jednym z następujących trybów, aby skonfigurować router:

• Tryb konfiguracji globalnej — w tym trybie można skonfigurować ustawienia routera, które mają wpływ na ogólne działanie routera, takie jak zmiana wyświetlanego baneru routera, gdy użytkownik łączy się ze zdalnego hosta za pośrednictwem Telnetu. Baner może wskazywać, że router jest zabezpieczony lub nie powinien być dostępny dla nieautoryzowanego personelu. Aby użyć tego trybu, wprowadź polecenie configure terminal w wierszu poleceń Router#. Możesz również wprowadzić skrócone polecenie, które interpreter poleceń Cisco rozumie, o ile nie jest tak krótkie, że jest niejednoznaczne. Dlatego polecenie config t również działa. Następnie monit zmienia się na Router (config) #, aby wskazać globalny tryb konfiguracji. Podczas korzystania z routera lub przełącznika Cisco znajomość monitów ma kluczowe znaczenie.

• Tryb konfiguracji interfejsu — w tym trybie konfigurujesz interfejs na routerze, taki jak port szeregowy lub Fast Ethernet. Aby użyć tego trybu, najpierw wejdź w tryb konfiguracji globalnej (za pomocą polecenia config t). Następnie wprowadź polecenie trybu konfiguracji interfejsu i nazwę interfejsu, który chcesz skonfigurować, na przykład interface fastethernet 0/0. Monit zmieni się na Router (config-if) #, aby wskazać tryb konfiguracji interfejsu.

Teraz, gdy rozumiesz podstawowe tryby, w których może działać router Cisco, co opisuje niektóre typowe polecenia służące do przeglądania komponentów routera Cisco. Jeśli chcesz poznać wszystkie polecenia dostępne w trybie konfiguracji globalnej, wpisz znak zapytania (?) po monicie Router(config)#. Administrator Cisco musi znać wiele innych poleceń, które nie są omówione w tym kursie. Najważniejsza konfiguracja, jaką wykonują specjaliści ds. bezpieczeństwa, dotyczy interfejsów routera. Pakiety mogą być filtrowane lub oceniane na interfejsach routera przed przekazaniem do następnego routera lub sieci wewnętrznej. Aby kontrolować przepływ ruchu przez router, używane są listy dostępu, jak wyjaśniono w następnej sekcji.

Korzystanie z list kontroli dostępu

Listy kontroli dostępu to listy reguł bezpieczeństwa, które analizują ruch przychodzący i wychodzący oraz określają, czy ruch ten zostanie odrzucony lub dozwolony w określonym interfejsie. Każdy interfejs routera może mieć dwie unikalne listy kontroli dostępu, jedną do analizowania ruchu przychodzącego i jedną do analizowania ruchu wychodzącego. Istnieje kilka typów list kontroli dostępu, ale ta sekcja koncentruje się na listach dostępu IP. Listy dostępu IP to listy adresów IP, podsieci lub sieci, do których dostęp jest dozwolony lub zabroniony przez interfejs routera. Na routerze Cisco administrator może utworzyć dwa typy list dostępu:

• Standardowe listy dostępu IP

• Rozszerzone listy dostępu IP

UWAGA : Cisco odnosi się do list dostępu IP jako do „list kontroli dostępu", ale odnosi się do konkretnego pliku zawierającego listę poleceń jako do „listy dostępu".

Standardowe listy dostępu IP

Standardowe listy dostępu IP mogą ograniczać ruch IP wchodzący lub wychodzący z interfejsu routera na podstawie tylko jednego kryterium: adresu IP źródłowego. Rysunek 13-1 przedstawia sieć składającą się z dwóch routerów. Sieć 1 (10.0.0.0) jest podłączona do interfejsu Fast Ethernet (FE0/0) na routerze A. Interfejs szeregowy routera A (S0/1) jest podłączony do interfejsu szeregowego routera B (S0/0). Sieć 2 (192.168.10.0) jest podłączona do interfejsu Fast Ethernet routera B (FE0/0), a sieć 3 (173.110.0.0) jest podłączona do innego interfejsu Fast Ethernet routera B (FE0/1). Administrator Cisco, który chce ograniczyć cały ruch z sieci 3 przed wejściem do sieci 1, może utworzyć standardową listę dostępu IP, która wygląda następująco:

access-list 1 deny 173.110.0.0 0.0.255.255

access-list permit any

Rozszerzone listy dostępu IP

Standardowa lista dostępu IP jest ograniczona do źródłowych adresów IP. Tak więc, jeśli chcesz ograniczyć użytkownikowi możliwość wysyłania pakietu na określony adres IP (adres IP docelowy), nie możesz użyć standardowej listy dostępu IP. Rozszerzone listy dostępu IP mogą ograniczać ruch IP wchodzący lub wychodzący z interfejsu routera na podstawie następujących kryteriów:

• Źródłowy adres IP

• Docelowy adres IP

• Typ protokołu

• Numer portu aplikacji

Konfigurowanie rozszerzonej listy dostępu IP jest bardzo podobne do konfigurowania standardowej listy dostępu IP. Administrator sieci może zdecydować, do którego interfejsu zastosować listę dostępu, na podstawie kilku zmiennych. Na przykład router może mieć interfejs łączący się z linią OC3 lub T4. Listę dostępu można stosować tylko do tego interfejsu, a nie do innego interfejsu podłączonego do kabla CAT 6. Listy dostępu to nic więcej niż listy; nie stają się skuteczne, dopóki nie zostaną zastosowane do interfejsów. Szczegółowe omówienie składni list dostępu wykracza poza zakres tego kursu. Ponieważ jednak Twoja praca może obejmować testowanie sieci z routerami, powinieneś zbadać listy dostępu bardziej szczegółowo samodzielnie lub na innym kursie. Jeśli zdecydujesz się na

przykład uzyskać certyfikat Cisco Certified Network Associate (CCNA), musisz wiedzieć, jak tworzyć, konfigurować i stosować listy dostępu do interfejsów. Wiedza, którą zdobędziesz dzięki uzyskaniu tego certyfikatu, jest dobrym uzupełnieniem Twojego arsenału testowania bezpieczeństwa.

OCHRONA ZA POMOCĄ ZAPOR TECHNICZNYCH

Zapory ogniowe mogą być urządzeniami sprzętowymi z wbudowanymi systemami operacyjnymi lub oprogramowaniem zainstalowanym w systemach komputerowych ogólnego przeznaczenia. Zapory ogniowe służą dwóm głównym celom: kontrolowaniu dostępu do ruchu wchodzącego do sieci wewnętrznej i kontrolowaniu ruchu opuszczającego sieć wewnętrzną. Zapory ogniowe można instalować w sieci, aby chronić wewnętrzną sieć firmy przed zagrożeniami występującymi w Internecie. W dużych sieciach przedsiębiorstw zapory ogniowe mogą również chronić wewnętrzne segmenty sieci, takie jak te zawierające tylko serwery aplikacji, przed innymi wewnętrznymi segmentami sieci — na przykład tymi zawierającymi stacje robocze pracowników. Na przykład typowe podejście do zapory ogniowej przedsiębiorstwa polega na ograniczeniu portu pulpitu zdalnego TCP 3389, używanego do zdalnego administrowania serwerami aplikacji, tylko do segmentu sieci administratora systemu i zezwalaniu tylko na porty 80 i 443 dla ruchu internetowego w segmencie sieci zawierającym stacje robocze pracowników. W tym przykładzie wyraźnie widać, że typowi pracownicy nie muszą administrować serwerami aplikacji, więc takie podejście odzwierciedla filozofię najmniejszych uprawnień. Zapory ogniowe sprzętowe i programowe mają zalety i wady. Jednak zamiast przedstawiać zalecenia, ten moduł skupia się na tym, jak zapory sieciowe wpisują się w strategię bezpieczeństwa. Krótko mówiąc, wadą sprzętowych zapór sieciowych jest to, że jesteś ograniczony sprzętem zapory, takim jak liczba interfejsów, które obejmuje. W przypadku zapory sieciowej programowej możesz łatwo dodać karty sieciowe do serwera, na którym działa oprogramowanie. Wadą zapór sieciowych programowych jest to, że możesz musieć martwić się o problemy z konfiguracją, takie jak wymagania dotyczące pamięci, wymagania dotyczące miejsca na dysku twardym, liczba obsługiwanych procesorów itd. Zapory sieciowe programowe są również zależne od systemu operacyjnego, na którym są uruchomione. Na przykład zapora systemu Windows jest dostępna w systemach Windows 10 i Windows Server 2016. Innym przykładem jest iptables, dołączony do Kali Linux. Sprzętowe zapory sieciowe, takie jak Cisco Adaptive Security Appliance (omówione później w tym module), są zwykle szybsze i mogą obsłużyć większą przepustowość niż zapory sieciowe programowe. Jak widać, router może być również używany do filtrowania ruchu wchodzącego lub wychodzącego z jego interfejsu. Filtrowanie można skonfigurować za pomocą list dostępu, które ograniczają ruch na podstawie adresu IP źródłowego, adresu IP docelowego, protokołu i portu. Jednakże zapora sieciowa jest specjalnie zaprojektowana jako system ochrony sieci i ma więcej funkcji bezpieczeństwa niż router.

Badanie technologii zapory sieciowej

Widziałeś wiele metod, których atakujący używają do skanowania sieci i uruchamiania exploitów. Zapory sieciowe mogą pomóc w zmniejszeniu tych ataków, wykorzystując kilka technologii:

- Translacja adresów sieciowych
- Listy dostępu
- Filtrowanie pakietów
- Inspekcja pakietów stanowych
- Inspekcja warstwy aplikacji

Tłumaczenie adresów sieciowych

Podstawową funkcją bezpieczeństwa zapory sieciowej jest tłumaczenie adresów sieciowych (NAT). Jednym z zadań specjalisty ds. bezpieczeństwa jest ukrycie wewnętrznej sieci przed osobami z zewnątrz. Dzięki NAT wewnętrzne prywatne adresy IP są mapowane na publiczne zewnętrzne adresy IP, ukrywając wewnętrzną infrastrukturę przed nieautoryzowanym personelem. Na przykład użytkownik z prywatnym adresem IP 10.1.1.15 ma swój adres mapowany na zewnętrzny adres IP 193.145.85.200. Świat zewnętrzny widzi tylko zewnętrzny adres IP i nie zna wewnętrznych adresów IP używanych przez firmę. Po poznaniu adresu IP komputera lub serwera hakerzy skanują ten system w poszukiwaniu otwartych lub podatnych portów. Ukrywanie adresów IP przed hakerami może pomóc zapobiec powodzeniu tych skanów. Aby uwzględnić wiele adresów, które muszą zostać zmapowane, wiele organizacji używa tłumaczenia adresów portów (PAT), które jest pochodną NAT. Umożliwia mapowanie tysięcy wewnętrznych adresów IP na jeden zewnętrzny adres IP.

Listy dostępu

Jak omówiono w sekcji o routerach, listy dostępu służą do filtrowania ruchu na podstawie adresu IP źródłowego, adresu IP docelowego oraz portów lub usług. Zapory sieciowe również wykorzystują tę technologię, jak zobaczysz później w sekcji o zaporze Cisco Adaptive Security Appliance. Po zrozumieniu, jak utworzyć listę dostępu na routerze, utworzenie jej na zaporze sieciowej jest podobnym procesem.

Filtrowanie pakietów

Inną podstawową funkcją bezpieczeństwa, jaką wykonuje zapora sieciowa, jest filtrowanie pakietów. Filtry pakietów przeszukują pakiety na podstawie informacji w nagłówku pakietu, takich jak:

- Typ protokołu
- Adres IP
- Port TCP/UDP

Inspekcja pakietów stanowych

Zapory sieciowe zwykle wykonują podstawowe filtrowanie wykonywane przez router o krok dalej, wykonując inspekcję pakietów stanowych (SPI). Filtry pakietów stanowych rejestrują informacje specyficzne dla sesji dotyczące połączenia sieciowego, w tym portów używanych przez klienta, w pliku zwanym tabelą stanów.

W tej tabeli stanów kilka wewnętrznych hostów używających prywatnych adresów IP nawiązało połączenia z zewnętrznymi adresami IP. Jeden host nawiązał sesję Telnet (port 23), dwa hosty nawiązały połączenia HTTP (port 80), a jeden host niedawno zamknął połączenie z serwerem poczty e-mail (port 25). Ta tabela stanów to sposób, w jaki zapora śledzi stan połączeń, w oparciu o to, jakiego rodzaju ruchu oczekuje się w sesji dwukierunkowej. Skanowanie portów polegające na podszywaniu się lub wysyłaniu pakietów po trzyetapowym uzgadnianiu jest nieskuteczne, jeśli zapora używa tabeli stanów. Jeśli haker próbuje wysłać (podszyć się) pakiet SYN/ACK z adresu IP, który nie znajduje się w tabeli stanów, pakiet zostaje odrzucony. Przypomnijmy, że pakiet SYN/ACK jest wysyłany dopiero po odebraniu pakietu SYN. Filtry pakietów stanowych rozpoznają typy anomalii, które większość routerów ignoruje, takie jak setki lub tysiące pakietów SYN/ACK wysyłanych do komputera, nawet jeśli komputer nie wysłał żadnych pakietów SYN. Ponieważ bezstanowe filtry pakietów obsługują każdy pakiet oddzielnie, nie są odporne na podszywanie się i ataki DoS.

Inspekcja warstwy aplikacji

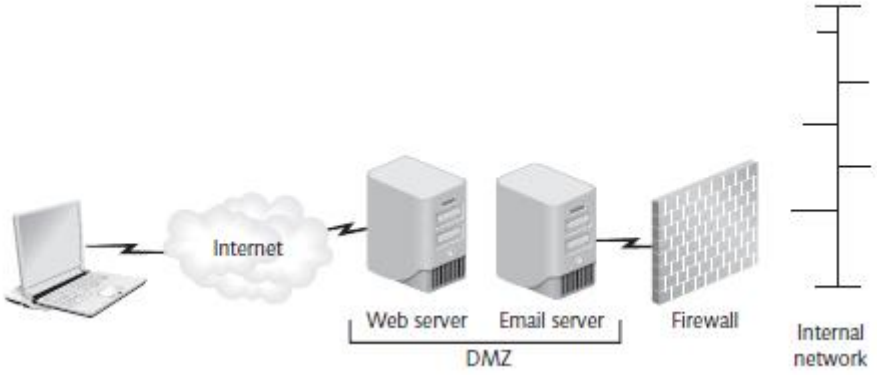
Zapora sieciowa uwzględniająca aplikacje inspekcjonuje ruch sieciowy na wyższym poziomie w modelu OSI niż tradycyjna zapora sieciowa z inspekcją pakietów stanowych. SPI zapewnia, że źródło, miejsce docelowe i port pakietu są sprawdzane przed przekazaniem pakietu, ale zapora sieciowa wykonująca inspekcję warstwy aplikacji upewnia się również, że protokół aplikacji ruchu sieciowego jest typem dozwolonym przez regułę. Na przykład wiele trojanów omija zapory sieciowe, uruchamiając odwrotną powłokę, która pochodzi z zainfekowanego systemu i łączy się ze zdalnym systemem kontrolowanym przez hakera. Ta odwrotna powłoka jest bezpiecznym tunelem poleceń i kontroli hakera i zwykle jest maskowana przez użycie powszechnie dozwolonego portu wychodzącego, takiego jak port 443. Kanał kontrolowany przez hakera przenika następnie z wnętrza sieci na zewnątrz przez dozwolony port wychodzący. Stacje robocze używają portu 443 wychodzącego do przeglądania stron internetowych za pośrednictwem protokołu HTTPS. Jeśli odwrotna powłoka używa protokołów Telnet lub SSH na porcie 443, zapora sieciowa rozpoznająca aplikacje może uniemożliwić odwrotnej powłoce połączenie się z portem zarezerwowanym dla ruchu HTTP. Niektóre zapory sieciowe rozpoznające aplikacje działają jako serwer proxy dla wszystkich połączeń, pełniąc w ten sposób funkcję sieci bezpieczeństwa dla serwerów lub klientów (lub obu), w zależności od tego, co zapora chroni. Jeśli zapora sieciowa rozpoznająca aplikacje chroni na przykład serwer WWW, zapobiega ona przepełnieniom bufora, które są ukierunkowane na określony protokół aplikacji, taki jak luka ISAPI w oprogramowaniu serwera WWW IIS. Zapora sieciowa rozpoznająca aplikacje, która chroni aplikację internetową, jest znana jako zapora sieciowa aplikacji internetowej (WAF). Zapory sieciowe, które mają zaawansowane funkcje, takie jak rozpoznawanie aplikacji i wykrywanie włamań, są reklamowane jako zapory sieciowe nowej generacji przez wiele firm zajmujących się bezpieczeństwem. Seria Cisco FirePOWER, seria Fortinet FortiGate i seria Sophos XG to przykłady zapór sieciowych nowej generacji.

Wdrażanie zapory sieciowej

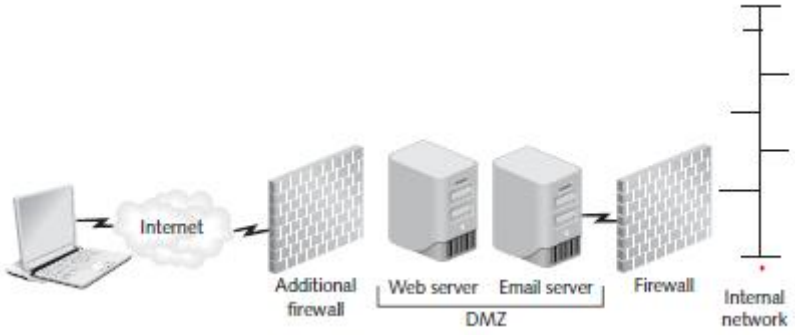
Używanie pojedynczej zapory sieciowej między wewnętrzną siecią firmy a Internetem może być niebezpieczne, ponieważ jeśli hakerzy naruszą zaporę, uzyskają pełny dostęp do sieci wewnętrznej. Aby zmniejszyć to ryzyko, większość topologii zapór sieciowych przedsiębiorstw korzysta ze strefy zdemilitaryzowanej, omówionej w poniższej sekcji, aby dodać warstwę obrony.

Strefa zdemilitaryzowana

Strefa zdemilitaryzowana (DMZ) to mała sieć zawierająca zasoby, które firma chce udostępnić użytkownikom Internetu; taka konfiguracja pomaga utrzymać bezpieczeństwo w wewnętrznej sieci firmy. Strefa DMZ znajduje się między Internetem a siecią wewnętrzną i jest czasami nazywana „siecią perymetryczną”.



Należy pamiętać, że użytkownicy Internetu mogą uzyskać dostęp do DMZ bez przechodzenia przez zaporę. Lepszą strategią bezpieczeństwa jest umieszczenie dodatkowej zapory w konfiguracji sieciowej



Aby użytkownicy mogli uzyskać dostęp do sieci wewnętrznej z Internetu, muszą przejść przez dwie zapory. Ta konfiguracja jest prawdopodobnie najczęstszą konstrukcją topologii zapory przedsiębiorstwa.

Badanie zapory Cisco Adaptive Security Appliance Firewall

Dobrym sposobem na poznanie działania zapory jest przyjrzenie się konfiguracji jednej z najczęściej używanych zapór: zapory Cisco Adaptive Security Appliance (ASA). Cisco ASA zastąpiło zaporę Cisco PIX i dodało zaawansowane funkcje modułowe, takie jak wykrywanie i zapobieganie włamaniom oraz bardziej zaawansowaną inspekcję warstwy aplikacji. W poniższych sekcjach przedstawiono niektóre polecenia konfiguracji zapory ASA, aby uzyskać pojęcie o tym, co powinni wiedzieć specjaliści ds. bezpieczeństwa. Przejdziesz przez proces konfigurowania ASA w celu utworzenia reguł segmentujących serwery sieciowe z terminali, które zezwalają na ruch tylko na kilku portach.

Konfigurowanie zapory ASA

Po zalogowaniu się do zapory ASA za pośrednictwem protokołu SSH pojawia się monit logowania podobny do monitu logowania do routera Cisco:

Jeśli nie masz uprawnień do korzystania z tego urządzenia sieciowego XYZ Hawaii, wyloguj się natychmiast!

Nazwa użytkownika: admin

Hasło: ********

W tym przykładzie administrator utworzył baner ostrzegający, że każda osoba próbująca się połączyć musi uzyskać autoryzację przed kontynuowaniem. Ten baner może wydawać się stratą czasu, ale służy celowi prawnemu. Gdyby baner głosił „Witamy, prosimy o zalogowanie się”, intruzi mogliby nie zostać pociągnięci do odpowiedzialności, jeśli włamaliby się do Twojej sieci. System prawny USA wycofał już zarzuty przeciwko hakerom, którzy weszli na strony ze słowem „Witamy” w banerach. Po zalogowaniu się przy użyciu prawidłowego hasła zapora wyświetla następujące informacje:

Wpisz help lub ‘?’ aby uzyskać listę dostępnych poleceń.

ciscoasa>

Monit jest taki sam, jaki widziałeś podczas logowania się do routera Cisco — nazwa routera, po której następuje symbol > — więc wiesz, że jesteś w trybie użytkownika. Aby wejść w tryb uprzywilejowany, wpisujesz to samo polecenie enable (en, w tym przykładzie), które jest używane dla routera Cisco, a następnie pojawia się monit o podanie hasła:

ciscoasa> en

Password: ********

Po wprowadzeniu prawidłowego hasła zostaniesz przeniesiony do trybu uprzywilejowanego, co zostanie wskazane przez monit #. Wprowadzenie znaku ? ujawnia więcej poleceń dostępnych w trybie uprzywilejowanym. Następnie, aby wejść do trybu konfiguracji w ASA, użyj tego samego polecenia, co na routerze Cisco: configure terminal lub configure t. Następnie sprawdź, w jaki sposób zapora używa list dostępu do filtrowania ruchu. Następująca lista dostępu o nazwie PERMITTED_TRAFFIC pokazuje określone połączenia VPN do kilku szaf okablowania:

ciscoasa (config) # show run access-list

access-list PERMITTED_TRAFFIC remark VPN-CONC1 TO TERMINAL CLOSET1B

access-list PERMITTED_TRAFFIC extended permit ip

host 10.13.61.98 host 10.13.61.18

access-list PERMITTED_TRAFFIC remark VPN-CONC2 TO TERMINAL CLOSET1B

access-list PERMITTED_TRAFFIC extended permit ip host 10.13.61.99

host 10.13.61.19

access-list PERMITTED_TRAFFIC remark VPN-CONC3 TO TERMINAL CLOSET1B

access-list PERMITTED_TRAFFIC extended permit ip host 10.13.61.100

host 10.13.61.20

access-list NONE extended deny ip any any log

access-list CAP-ACL extended permit ip any any

Następnie spójrz na listę grup obiektów w konfiguracji ASA. Grupa obiektów to sposób na zorganizowanie hostów, sieci, usług, protokołów lub typów ICMP w grupy, tak aby reguła zapory mogła być stosowana do wszystkich obiektów jednocześnie, zamiast do każdego z osobna. W tym przykładzie kilka hostów jest członkami grupy obiektów VIRTUAL_TERMINALS:

ciscoasa# show run object-group

object-group network VIRTUAL_TERMINALS

network-object host 10.11.11.67

network-object host 10.11.11.68

network-object host 10.11.11.69

W poniższym przykładzie zwróć uwagę na grupę obiektów dla sieci. Nazywa się AD_SERVERS, nazwa wybrana przez administratora zapory do reprezentowania serwerów Active Directory. Obecnie w grupie jest tylko jeden host, ale administrator zapory może ją rozszerzyć, gdy dodanych zostanie więcej

serwerów Active Directory. Następna jest grupa obiektów dla usług, która jest zorganizowana jako AD_TCP i AD_UDP. Wcześniej dowiedziałeś się, które porty muszą być otwarte na zaporze, aby usługi kontrolera domeny Active Directory mogły działać, więc porty wymienione w tym przykładzie powinny wyglądać znajomo

object-group network AD_SERVERS

network-object host 10.0.0.25

object-group service AD_TCP tcp

port-object eq domain

port-object eq 88

port-object eq 135

port-object eq ldap

port-object eq 445

port-object eq 1026

object-group service AD_UDP udp

port-object eq domain

port-object eq 88

port-object eq ntp

port-object eq 389

Na koniec, usługi aplikacji, które powinny być dozwolone przez zaporę, są zorganizowane w grupie obiektów APP_SERVICES. Zauważ, że dozwolone są web (WWW, HTTPS), FTP (FTP, FTP-data), email (POP3, SMTP) i udostępnianie plików (port 445):

object-group service APP_SERVICES tcp

port-object eq ftp-data

port-object eq ftp

port-object eq smtp

port-object eq www

port-object eq pop3

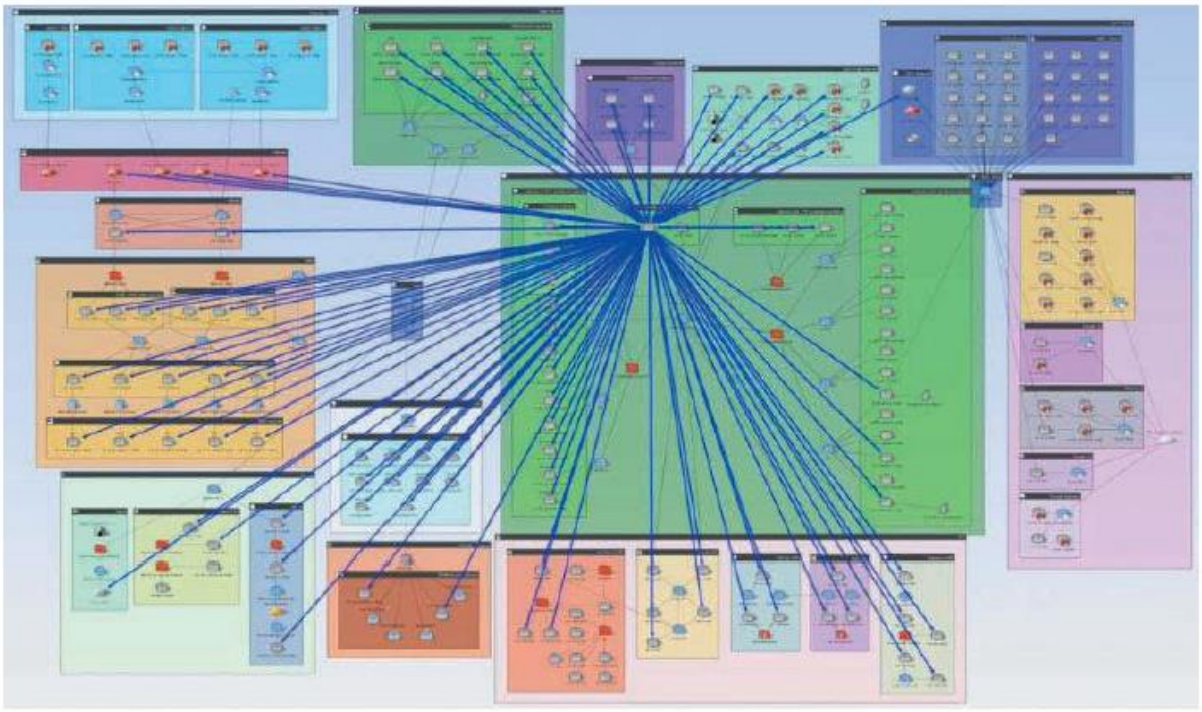
port-object eq https

port-object eq 445

Korzystanie z narzędzi do konfiguracji i analizy ryzyka dla zapór sieciowych i routerów

Łatanie systemów to tylko jeden element ich ochrony przed naruszeniem. Musisz je również bezpiecznie skonfigurować. Na szczęście dostępnych jest wiele zasobów do tego zadania. Jedną z najlepszych stron internetowych do wyszukiwania testów porównawczych konfiguracji i narzędzi do oceny konfiguracji routerów i zapór sieciowych Cisco jest Center for Internet Security (CIS,

www.cisecurity.org/cis-benchmarks/). Test porównawczy to branżowy konsensus najlepszych praktyk konfiguracji dotyczących tego, jak (za pomocą wskazówek krok po kroku) i dlaczego (wyjaśniając powody podjęcia tych kroków) zabezpieczyć router lub zaporę sieciową Cisco. W przypadku urządzeń Cisco użyj testu porównawczego CIS Cisco IOS; najnowsza wersja to obecnie 16.0. Przeglądanie wszystkich kroków konfiguracji w tych testach porównawczych może zająć sporo czasu. Z tego powodu CIS oferuje przydatne narzędzie o nazwie Configuration Assessment Tool (CAT), które jest szybsze i łatwiejsze w użyciu. Wersje CAT są dostępne zarówno dla systemów *nix, jak i Windows. Jeśli masz czas i dostęp do laboratorium z routerem lub zaporą Cisco, pobierz narzędzie CAT i uruchom je w systemie Windows lub Kali Linux. Warto wspomnieć o komercyjnym narzędziu RedSeal (redseal.net), unikalnym narzędziu do analizy i mapowania ryzyka sieciowego. Podobnie jak narzędzie CIS RAT, RedSeal może identyfikować luki w konfiguracji routerów lub zapór, ale generuje również profesjonalnie wyglądające raporty, które można dostosować do logo firmy. Oprócz analizowania plików konfiguracyjnych z routerów i zapór, RedSeal może analizować systemy IPS, a także skanowanie luk w systemie operacyjnym w celu uzyskania szczegółowej analizy i mapowania. Rysunek przedstawia mapę ryzyka sieciowego generowaną po wprowadzeniu plików konfiguracyjnych routera i zapory Cisco oraz skanów Nessus w RedSeal.



Analizuje ona konfiguracje wszystkich urządzeń w sieci w celu określenia, jaki dostęp jest dozwolony. Rozważając architekturę, która ma być używana do ochrony sieci, dostęp jest określany poprzez łączenie reguł i list kontroli dostępu w każdym urządzeniu wzdłuż ścieżki sieciowej. Aby zobaczyć szczegóły dozwolonej ścieżki, kliknij odpowiedni wiersz. RedSeal jest wyjątkowy, ponieważ pokazuje graficzną reprezentację luk odkrytych w kontekście sieci, w której zostały znalezione. Raport i mapa RedSeal mogą być szczególnie przydatne w przekazywaniu informacji kierownictwu wyższego szczebla; format graficzny jest łatwiejszy do zrozumienia niż strony rozwlekłych raportów. (Pamiętaj stare przysłowie: Obraz jest wart tysiąca słów.) RedSeal jest przydatnym narzędziem do przedstawiania statusu bezpieczeństwa sieci.

OCHRONA ZA POMOCĄ SYSTEMÓW WYKRYWANIA I ZAPOBIEGANIA WŁAMANIOM

Systemy wykrywania włamań (IDS) monitorują urządzenia sieciowe, aby administratorzy ds. bezpieczeństwa mogli identyfikować trwające ataki i je zatrzymywać. Na przykład, aby użytkownicy mogli uzyskać dostęp do serwera internetowego, zapora sieciowa musi zezwalać na otwarcie portu 80. Niestety, otwarcie tego portu może również umożliwić hakerowi zaatakowanie serwera internetowego. IDS bada ruch przechodzący przez połączenie do portu 80 i porównuje go ze znanymi exploitami, podobnie jak oprogramowanie antywirusowe, używając pliku sygnatur do identyfikacji wirusów. Jeśli atakujący próbuje wykorzystać znaną lukę w zabezpieczeniach serwera internetowego, IDS wysyła alert o ataku, aby administrator serwera internetowego mógł podjąć działania. Systemy zapobiegania włamaniom (IPSS) są podobne do IDS, ale wykonują dodatkowy krok, wykonując pewnego rodzaju działanie w celu zapobieżenia włamaniu, zamiast tylko powiadamiać administratorów o ataku. W poniższej sekcji opisano dwa typy systemów wykrywania i zapobiegania włamaniom: oparte na sieci i oparte na hoście.

IDS-y i IPS-y oparte na sieci i hoście

IDSS/IPS-y oparte na sieci monitorują aktywność w segmentach sieci. Zasadniczo wyczuwają ruch przepływający przez sieć i powiadamiają administratora zabezpieczeń, gdy dzieje się coś podejrzanego. Niektóre z tych systemów mogą również blokować ruch. IDS-y/IPS-y oparte na hoście są najczęściej używane do ochrony krytycznego serwera sieciowego lub serwera bazy danych, chociaż mogą również działać na stacjach roboczych. Oprogramowanie IDS lub IPS jest instalowane w systemie, który próbujesz chronić, podobnie jak instalowanie oprogramowania antywirusowego na komputerze stacjonarnym. IDS-y można również klasyfikować według sposobu reakcji po wykryciu podejrzanego zachowania. Systemy, które nie podejmują żadnych działań w celu zatrzymania lub zapobieżenia aktywności, nazywane są systemami pasywnymi. Oczywiście wysyłają alert i rejestrują aktywność, podobnie jak ochroniarz w centrum handlowym będący świadkiem zbrojnego napadu. Systemy aktywne również rejestrują zdarzenia i wysyłają alerty, ale mogą również współpracować z routerami i zaporami sieciowymi w celu zatrzymania ataku. Na przykład aktywny system IDS może wysłać listę dostępu do routera, który zamyka interfejs, aby uniemożliwić atakującym uszkodzenie sieci. Niektóre aktywne systemy IDS wysyłają fałszywe pakiety resetowania, które oszukują stosy TCP/IP zarówno ofiary, jak i atakującego, aby zerwały złośliwe połączenie. Czas od rozpoczęcia ataku do momentu naruszenia systemu może wynosić zaledwie milisekundy, co jest zbyt szybkie, aby człowiek mógł podjąć działanie. Z tego powodu dostawcy zaczęli koncentrować swoje wysiłki marketingowe na systemach IPS. Istnieje różnica między aktywnym systemem IDS a prawdziwym systemem IPS. Prawdziwy oparty na sieci system IPS jest instalowany w linii do infrastruktury sieciowej, co oznacza, że ruch musi przejść przez system IPS przed wejściem do sieci lub wyjściem z niej. Aktywny system IDS po prostu wyczuwa ruch i może zostać wyłączony lub odłączony od sieci bez wpływu na łączność sieciową. Ponieważ system IPS jest w linii, ogólnie rzecz biorąc, jest bardziej zdolny do zatrzymania złośliwego ruchu niż aktywny system IDS, szczególnie w przypadku ataków opartych na protokole UDP. Wiele obecnych systemów IDS obejmuje funkcje IPS i często ma opcjonalne moduły, takie jak wykrywanie złośliwego oprogramowania i filtrowanie sieci. Ponadto dostępne są systemy IPS oparte na hoście; działają na poziomie systemu operacyjnego (lub jądra) i przechwytują ruch, który nie jest dozwolony przez zasady hosta. Ponieważ systemy IPS oparte na hoście współdzielą zasoby z systemem operacyjnym, na którym działają, mogą spowalniać wydajność, jeśli sprzęt nie jest odpowiedni. System IDS oparty na anomaliach używa poziomu bazowego normalnej aktywności, a następnie wysyła alert, jeśli aktywność znacznie odbiega od tego poziomu bazowego. Większość rozwiązań IDS/IPS ma wbudowane funkcje wykrywania anomalii. Producenci systemów IDS zazwyczaj oferują funkcjonalność IPS jako opcję w większości swoich produktów IDS — stąd tendencja do jednoczesnego używania terminów IDS i IPS. Poświęć trochę czasu na zbadanie narzędzi wymienionych w tabeli, aby dowiedzieć się więcej o tych produktach. Systemy IDS i IPS odgrywają ważną rolę w obronie przed atakami sieciowymi. W

połączeniu z routerami, zaporami sieciowymi i innymi kontrolami technicznymi mogą pomóc Ci chronić sieć, którą masz zabezpieczyć.

Filtrowanie sieci

Atakujący zazwyczaj atakują stacje robocze użytkowników, które zazwyczaj mają dostęp do Internetu. Jeśli uda im się zmusić wewnętrznego użytkownika do odwiedzenia złośliwej witryny lub zainstalowania złośliwego kodu z załącznika do wiadomości e-mail, nie muszą przebijać się przez zaporę sieciową. Po zainstalowaniu kodu trojana na stacji roboczej użytkownika atakujący mogą kontrolować trojana zdalnie za pomocą poleceń, które mogą wydawać się normalnym ruchem. Mogą wykorzystać to zagrożenie, aby rozprzestrzenić się w sieci, uruchamiając skanowanie sieci z zainfekowanej stacji roboczej, kradnąc dane dostępne na lub z systemu ofiary, łamiąc hasła systemowe i wykorzystując luki w zabezpieczeniach, które odkryją w innych systemach. Atakujący mogą ukryć aktywność poleceń i kontroli wewnątrz tego, co wydaje się normalnym ruchem HTTP i HTTPS. W takiej sytuacji filtrowanie sieci może zostać użyte do wykrycia prób dostępu użytkownika do znanych złośliwych witryn i zablokowania tych prób, a niektóre systemy filtrowania sieci mogą faktycznie blokować złośliwy kod, zanim dotrze on do stacji roboczej użytkownika lub zanim będzie miał szansę połączyć się z systemem kontroli atakującego poza siecią. Firmy, które sprzedają i wspierają te urządzenia filtrujące sieć, często kategoryzują domeny do różnych grup. Na przykład, jeśli użytkownik odwiedzi PNC.com, filtr sieciowy zidentyfikuje to żądanie w kategorii „Finanse/Bankowość internetowa" i zezwoli na ruch. Jednak jeśli użytkownik zażąda exploit-db.com, filtr sieciowy może sklasyfikować to żądanie jako „Strony hakerskie" i odrzucić żądanie. A co ze stronami internetowymi, które nie zostały jeszcze skategoryzowane? Firmy mogą zdecydować się na zablokowanie dostępu do nieskategoryzowanych stron, aby uniknąć ryzyka, że użytkownicy odwiedzą nowo utworzoną domenę atakującego. Blokowanie dostępu do nieskategoryzowanych stron jest bardzo skuteczną praktyką bezpieczeństwa, ale może powodować niedogodności dla użytkowników. Zorganizowani cyberprzestępcy często próbują włamać się do popularnych stron internetowych, które mają największe szanse na zainfekowanie tysięcy odwiedzających witrynę złośliwym kodem. Tego typu masowe naruszenia są wykorzystywane do inicjowania pobierania typu drive-by, w którym odwiedzający witrynę pobierają złośliwy kod bez swojej wiedzy. Zwykle drive-by download wykorzystuje lukę w zabezpieczeniach przeglądarki lub aplikacji innej firmy, takiej jak Adobe Reader lub Microsoft Office. Ponieważ złośliwe witryny i kod zmieniają się codziennie, dostawcy systemów filtrowania stron internetowych muszą stale aktualizować swoje podpisy i bazy danych złośliwych witryn. Przykładami dostawców oferujących produkty do filtrowania stron internetowych na zasadzie subskrypcji są Fortiguard (www.fortinet.com/support/support-services/fortiguard-security-subscriptions/web-filtering) i Cisco Umbrella (https://umbrella.cisco.com/solutions/web-content-filtering).

Centrum Operacji Bezpieczeństwa

Systemy IDS, IPS i honeypoty (opisane w następnej sekcji), które pomagają utrzymać bezpieczeństwo sieci, wymagają wiedzy administracyjnej, aby je skonfigurować, uruchomić i konserwować. W mniejszych firmach, gdy dochodzi do zdarzenia związanego z bezpieczeństwem, administratorzy zazwyczaj muszą posprzątać bałagan, a następnie sporządzić raport dla kierownictwa lub działu prawnego lub współpracować z organami ścigania. W przypadku dużych organizacji, które mają poufne lub krytyczne dane, zwykła wiedza administracyjna nie wystarczy, aby przeprowadzić działania następcze i ocenę szkód, naprawę ryzyka i konsultacje prawne. W przypadku tego typu organizacji może być konieczne zalecenie utworzenia Centrum Operacji Bezpieczeństwa (SOC). Duże organizacje potrzebują stałego zespołu, którego członkowie odpowiadają wyłącznie za funkcje reagowania na zagrożenia bezpieczeństwa. Inną funkcją SOC jest monitorowanie artefaktów pozostawionych przez atakujących, które wskazują, że system lub sieć zostały naruszone; są one często nazywane

wskaźnikami naruszenia. Narzędzia Security Information and Event Management (SIEM) mogą pomóc zespołom identyfikować ataki i wskaźniki naruszenia poprzez zbieranie, agregowanie i korelowanie danych dziennika i alertów z routerów, zapór sieciowych, systemów IDS/IPS, dzienników punktów końcowych, urządzeń filtrujących sieć, honeypotów i innych narzędzi bezpieczeństwa. Łączenie alertów z tych urządzeń zapewnia analitykowi monitorującemu bezpieczeństwo kontekst umożliwiający podejmowanie bardziej świadomych decyzji. Popularne komercyjne produkty SIEM obejmują HP ArcSight, RSA EnVision i IBM QRadar. Produkty SIEM typu open source obejmują AlienVault OSSIM i LOGalyze.

KORZYSTANIE Z HONEYPOTÓW

Honeypot to komputer umieszczony na obwodzie sieci, który zawiera informacje lub dane mające na celu zwabienie, a następnie złapanie hakerów. Głównym celem jest odwrócenie uwagi hakerów od atakowania legalnych zasobów sieciowych. Specjalista ds. bezpieczeństwa konfiguruje komputer tak, aby miał luki w zabezpieczeniach, dzięki czemu hakerzy spędzają czas, próbując wykorzystać te luki. Innym celem honeypotów jest umożliwienie hakerom łączenia się z „fałszywym" komputerem na tyle długo, aby zostali wykryci, jak w filmach, gdy FBI chce, aby przestępca pozostał na telefonie wystarczająco długo, aby ustalić jego lokalizację. Ponadto honeypot może służyć jako doskonały system gromadzenia danych i wczesnego ostrzegania, aby pomóc scharakteryzować nowe ataki i zagrożenia; informacje te ułatwiają specjalistom ds. bezpieczeństwa obronę sieci przed nimi. Aby uzyskać więcej informacji na temat honeypotów, odwiedź stronę www.honeynet.org. Ta strona internetowa oferuje ćwiczenia i wyzwania, które zachęcają użytkowników do udziału, zawiera dokumenty dotyczące honeypotów i obejmuje prezentacje warsztatowe opisujące projekt Honeynet. Jeśli zdecydujesz się wziąć udział w ćwiczeniach, możesz skorzystać z laboratorium komputerowego odizolowanego od serwerów produkcyjnych lub sieci. Należy użyć komputera testowego ze względu na możliwość infekcji wirusem lub uszkodzenia danych.

Jak działają honeypoty

Jeśli atakujący mogą dostać się do Twojej wewnętrznej sieci, mogą wywołać spustoszenie. Honeypot wydaje się mieć ważne dane lub poufne informacje przechowywane na nim. Na przykład może przechowywać fałszywe dane finansowe, które kuszą hakerów do próby przeglądania danych. Rząd i przemysł prywatny od wielu lat używają honeypotów, aby zwabić atakujących do obszarów sieciowych z dala od prawdziwych danych. Zasadniczo uważa się, że jeśli hakerzy odkryją lukę w systemie, poświęcą czas na jej wykorzystanie i przestaną szukać innych obszarów do wykorzystania i uzyskania dostępu do zasobów firmy. Honeypoty umożliwiają również specjalistom ds. bezpieczeństwa zbieranie danych o atakujących. W ten sposób myśliwy staje się zwierzyną. Dostępne są zarówno komercyjne, jak i open-source honeypoty. Dobra wiadomość jest taka, że tworzenie honeypotów bez poświęcania potężnego serwera do tego zadania jest teraz możliwe. Wirtualne honeypoty są tworzone przy użyciu języka programowania, a nie konfigurując urządzenia fizycznego. Możesz pobrać bezpłatny kod open-source i zainstalować go na komputerze a*nix lub Windows. W Ćwiczeniu 13-2 zbadasz kilka honeypotów open-source.

Badanie pułapki typu open source o nazwie honeypot

Czas trwania: 30 minut

Cel: zapoznanie się z pułapką typu open source o nazwie honeypot o nazwie OpenCanary.

Opis: jako specjalista ds. bezpieczeństwa możesz potrzebować skonfigurować pułapkę typu honeypot, aby opóźnić i wykryć atakujących. W tej aktywności przyjrzysz się pułapce typu open source o nazwie honeypot o nazwie OpenCanary.

1. Uruchom przeglądarkę internetową, jeśli to konieczne, i przejdź do witryny opencanary.org.

2. Przeczytaj stronę główną OpenCanary.

3. W sekcji Usługi kliknij łącze Linux Web Server i przejrzyj plik konfiguracyjny.

4. Które porty włącza plik konfiguracyjny? Jakie oprogramowanie jest obsługiwane z tych portów?

5. Wróć na stronę główną i kliknij następujące łącza, aby przejrzeć konfiguracje dla każdego z nich: Windows Server, MySQL Server, MSSQL Server.

6. Zamknij przeglądarkę.

Jeśli czas na to pozwoli, możesz pobrać i zainstalować OpenCanary. Możesz również skonfigurować laboratorium i poćwiczyć korzystanie z pułapek typu honeypot. OpenCanary może oszukać Nmap (i atakujących), sprawiając wrażenie, że wykrył serwer RDP lub SQL uruchomiony w systemie.

PODSUMOWANIE MODUŁU

• Specjaliści ds. bezpieczeństwa mogą używać różnych systemów ochrony sieci, aby chronić sieć, takich jak routery, zapory sieciowe, systemy wykrywania i zapobiegania włamaniom, filtry sieciowe, honeypoty i urządzenia Unified Threat Management (UTM), które łączą wiele funkcji ochrony sieci na jednym urządzeniu.

• Routery używają list dostępu do akceptowania lub blokowania ruchu przez swoje interfejsy. W routerach Cisco listy dostępu mogą być używane do filtrowania ruchu wchodzącego i wychodzącego z sieci. Listy dostępu są stosowane do interfejsów na routerze.

• Zapory sieciowe mogą być sprzętowe lub programowe i służą do kontrolowania ruchu wchodzącego i wychodzącego z sieci lub podsieci. Cisco ASA to popularna zapora sieciowa. Zapory sieciowe mogą być używane do tworzenia wewnętrznych segmentów sieciowych i uniemożliwiania atakującym dostępu do kanałów poleceń i kontroli spoza chronionej sieci.

• Zapory sieciowe używają NAT, filtrowania pakietów, list kontroli dostępu, inspekcji pakietów stanowych i inspekcji warstwy aplikacji do filtrowania przychodzącego i wychodzącego ruchu sieciowego.

• DMZ to mała sieć zawierająca zasoby, która znajduje się między Internetem a siecią wewnętrzną, czasami nazywana „siecią perymetryczną”. Jest używana, gdy firma chce udostępnić zasoby użytkownikom Internetu, ale jednocześnie zachować oddzieloną sieć wewnętrzną firmy.

• Systemy wykrywania włamań monitorują ruch sieciowy, aby administratorzy mogli identyfikować ataki występujące w sieci. Na przykład komputer odbierający tysiące pakietów SYN na różnych portach w krótkim okresie czasu może wskazywać, że intruz skanuje sieć.

• Systemy IDS oparte na sieci monitorują aktywność w segmentach sieci, podczas gdy systemy IDS oparte na hoście są używane do ochrony poszczególnych punktów końcowych.

• Pasywne systemy IDS nie zapobiegają wystąpieniu aktywności; po prostu ostrzegają i rejestrują aktywność. Aktywne systemy IDS rejestrują i wysyłają alerty, ale także współpracują z routerami i zaporami sieciowymi i mogą zamknąć port lub interfejs routera, jeśli wykryją możliwe włamania.

• Podobnie jak systemy IDS, systemy zapobiegania włamaniom (IPS) wykrywają złośliwą aktywność. Jednak IPS-y są umieszczane w infrastrukturze sieciowej (IPS oparte na sieci) lub na hoście (IPS oparte na hoście) i mogą blokować lub zapobiegać złośliwej aktywności. Dostawcy IDS zazwyczaj oferują produkty, które mogą być używane jako IDS lub IPS.

• Bezpieczna konfiguracja routerów i zapór jest łatwiejsza dzięki narzędziom testowym, takim jak bezpłatne narzędzia dostępne na stronie internetowej CIS. Narzędzia komercyjne, takie jak RedSeal, są pomocne w analizowaniu i mapowaniu zagrożeń sieciowych.

• Filtrowanie sieci może blokować witryny zawierające złośliwy kod, takie jak te używane w atakach drive-by download. Ponieważ witryny często się zmieniają, korzystanie z usługi subskrypcji w celu aktualizacji kategorii domen filtrowania sieci i sygnatur antywirusowych jest ważnym środkiem ochronnym.

• Duże organizacje mogą potrzebować utworzyć Centrum Operacji Bezpieczeństwa (SOC), które składa się z ekspertów posiadających umiejętności i przeszkolenie umożliwiające wykrywanie i reagowanie na incydenty bezpieczeństwa sieci.

• Honeypoty to komputery emulujące serwery z fałszywymi informacjami i lukami w zabezpieczeniach, zaprojektowane w celu odciągnięcia hakerów od legalnych zasobów sieciowych i zachęcenia ich do poświęcenia czasu na wykorzystywanie luk w zabezpieczeniach honeypotów.