Moduł ćwiczeń i quizów

16.5.1

Pakiet Tracer - Zabezpieczanie urządzeń sieciowych

W tym ćwiczeniu skonfigurujesz router i przełącznik na podstawie listy wymagań.

Zabezpieczenie urządzeń sieciowych

Zabezpieczenie urządzeń sieciowych

16.5.2

Laboratorium - Zabezpieczenie urządzeń sieciowych

Celem tego ćwiczenia jest realizacja następujących zadań:

- Część 1: Konfigurowanie podstawowych ustawień urządzenia
- Część 2: Konfigurowanie podstawowych zabezpieczeń routera
- Część 3: Konfigurowanie podstawowych zabezpieczeń przełącznika

16.5.3

Czego się nauczyłem przerabiając ten moduł?

Zagrożenia i podatności

Ataki mogą być bardzo niszczycielskie i mogą doprowadzić do straty czasu i pieniędzy poprzez uszkodzenie lub kradzież ważnych danych. Intruzi, którzy uzyskali dostęp przez modyfikację oprogramowania czy wykorzystanie luki, są często nazywani podmiotami zagrożeń. Po uzyskaniu dostępu do sieci przez podmiot zagrożenia mogą pojawić się cztery rodzaje zagrożeń: kradzież informacji, utrata danych i manipulacja, kradzież tożsamości i zakłócenie usługi. Istnieją trzy główne podatności lub luki: technologiczne, konfiguracyjne i dotyczące polityki bezpieczeństwa. Cztery klasy zagrożeń fizycznych to: sprzęt, środowisko, elektryczne i konserwacja.

Ataki sieciowe

Malware jest skrótem od malicious software - złośliwe oprogramowanie. Jest to kod lub oprogramowanie zaprojektowane specjalnie do niszczenia, zakłócania, kradzieży lub wyrządzania „złych” lub nielegalnych działań na danych, hostach lub sieciach. Wirusy, robaki i konie trojańskie są rodzajami złośliwego oprogramowania. Ataki sieciowe można podzielić na trzy główne kategorie: rekonesans, ataki dostępu oraz ataki odmowy wykonania usługi (DoS). Cztery klasy zagrożeń fizycznych to: sprzęt, środowisko, elektryczne i konserwacja. Trzy rodzaje ataków rozpoznania to: zapytania internetowe, masowe testy ping i skanowanie portów. Cztery rodzaje ataków dostępu to: ataki na hasło (siłowy, koń trojański, analiza pakietów), wykorzystywanie zaufania, przekierowanie portów i man-in-the-middle. Dwa rodzaje ataków zakłóceń usług to: DoS i DDoS.

Działania zaradcze przeciw atakom sieciowym

Aby ograniczyć ataki sieciowe, należy najpierw zabezpieczyć urządzenia, w tym routery, przełączniki, serwery i hosty. Większość organizacji stosuje podejście dogłębnej obrony do bezpieczeństwa. Wymaga to kombinacji urządzeń sieciowych i usług współpracujących ze sobą. W celu ochrony użytkowników i zasobów organizacji przed zagrożeniami TCP/IP zaimplementowano kilka urządzeń i usług bezpieczeństwa: VPN, zapora ASA, IPS, ESA / WSA i serwer AAA. Urządzenia infrastrukturalne powinny mieć kopie zapasowe plików konfiguracyjnych i obrazów IOS na FTP lub podobnym serwerze plików. Jeśli komputer lub router ulegnie awarii, dane lub konfigurację można przywrócić za pomocą kopii zapasowej. Najbardziej skutecznym sposobem ograniczania ataku robaka jest pobranie aktualizacji zabezpieczeń od dostawcy systemu operacyjnego i zaktualizowanie

wszystkich zagrożonych systemów. Aby zarządzać krytycznymi poprawkami bezpieczeństwa, należy upewnić się, że wszystkie systemy końcowe automatycznie pobierają aktualizacje. AAA jest sposobem kontroli, która sprawdza kto ma pozwolenie na dostęp do sieci (uwierzytelnienie), co może zrobić, gdy tam jest (autoryzacja) oraz obserwować działania, jakie zostały wykonane podczas uzyskiwania dostępu do sieci (ewidencjonowanie). Zapory sieciowe znajdują się między dwiema lub więcej sieciami, kontrolują ruch między nimi i pomagają zapobiegać nieautoryzowanemu dostępowi. Serwery dostępne dla użytkowników zewnętrznych są zwykle zlokalizowane w specjalnej sieci zwanej DMZ. Zapory wykorzystują różne techniki określania dozwolonego lub blokowanego dostępu do sieci, w tym: filtrowanie pakietów, filtrowanie aplikacji, filtrowanie adresów URL i SPI. Zabezpieczenie urządzeń punktów końcowych ma kluczowe znaczenie dla bezpieczeństwa sieci. Firma musi mieć dobrze udokumentowane zasady, które mogą obejmować korzystanie z oprogramowania antywirusowego i zapobiegania włamaniom na hosty. Bardziej kompleksowe rozwiązanie bezpieczeństwa punktów końcowych polega na kontroli dostępu do sieci.

Bezpieczeństwo urządzeń

Ustawienia zabezpieczeń są skonfigurowane domyślne, gdy nowy system operacyjny jest instalowany na urządzeniu. Ten poziom bezpieczeństwa jest niewystarczający. W przypadku routerów Cisco można użyć funkcji Cisco AutoSecure w celu zabezpieczenia systemu. W przypadku większości OS domyślne nazwy użytkownika i hasła powinny zostać natychmiast zmienione, dostęp do zasobów systemowych powinien być ograniczony tylko do osób, które są upoważnione do korzystania z tych zasobów, a wszelkie niepotrzebne usługi i aplikacje powinny zostać wyłączone i odinstalowane, jeśli to możliwe. W celu ochrony urządzeń w sieci, ważne jest użycie silnych haseł. Tekst szyfrujący jest często łatwiejszy do zapamiętania niż proste hasła. Jest również dłuższy i trudniejszy do odgadnięcia. W przypadku routerów i przełączników zaszyfruj wszystkie hasła w postaci zwykłego tekstu, ustaw minimalną dopuszczalną długość hasła, powstrzymuj ataki polegające na zgadywaniu hasła metodą siłową, oraz wyłącz dostęp do trybu uprzywilejowanego EXEC po określonym czasie nieaktywności. Skonfiguruj odpowiednie urządzenia do obsługi SSH i wyłącz nieużywane usługi.

16.5.4

Moduł quizu - Podstawy bezpieczeństwa sieci

1. Który komponent ma chronić przed nieautoryzowaną komunikacją do i z komputera?

- zapora
- antymalware
- centrum zabezpieczeń
- program antywirusowy

- skaner portów

2. Które polecenie spowoduje zablokowanie prób logowania na RouterA przez okres 30 sekund, jeśli w ciągu 10 sekund wykonano dwie nieudane próby logowania?

- RouterA(config)# **login block-for 10 attempts 2 within 30**
- RouterA(config)# **login block-for 30 attempts 2 within 10**
- RouterA(config)# **login block-for 30 attempts 10 within 2**
- RouterA(config)# **login block-for 2 attempts 30 within 10**

3. Jaki może być cel ewidencjonowania jako funkcji bezpieczeństwa sieciowego?

- do dostarczenia funkcjonalności pytań i odpowiedzi
- wymaga od użytkowników aby udowodnili, że są tymi za których się podają
- do śledzenia działań użytkownika
- do określenia, do których zasobów użytkownicy mają mieć dostęp

4. Jaki rodzaj ataku może wiązać się z wykorzystaniem narzędzi, takich jak nslookup i fping**?**

- odmowa usługi (DoS)
- atak robaka
- atak w celu uzyskania dostępu
- ataki rozpoznania

5. Jaka jest zaleta SSH w porównaniu z Telnet w przypadku zdalnego zarządzania routerem?

- wykorzystanie protokołu TCP
- autoryzacja
- szyfrowanie
- połączenia przez wiele linii VTY

6. Co jest jednym z najskuteczniejszych dostępnych narzędzi bezpieczeństwa do ochrony użytkowników przed zagrożeniami zewnętrznymi?

- ( ) serwery patch
- ( ) router, który uruchamia usługi AAA
- ( ) zapory
- ( ) techniki szyfrowania hasła

7. Jaki rodzaj zagrożenia sieciowego ma na celu uniemożliwienie autoryzowanym użytkownikom dostępu do zasobów?

- ( ) ataki rozpoznania
- ( ) ataki w celu uzyskania dostępu
- ( ) wykorzystanie zaufania
- ( ) atak typu DoS

8. Które trzy usługi świadczone są w ramach AAA? (Wybierz trzy odpowiedzi).

- [ ] ewidencjonowanie
- [ ] automatyczna konfiguracja
- [ ] wyważanie
- [ ] automatyzacja
- [ ] autoryzacja
- [ ] uwierzytelnianie

9. Który atak złośliwego kodu jest samodzielny i próbuje wykorzystać konkretną lukę w atakowanym systemie?

- ( ) atak socjotechniczny
- ( ) koń trojański
- ( ) wirus
- ( ) robak

10. Niektóre routery i przełączniki w pomieszczeniu sieciowym działały nieprawidłowo po awarii klimatyzatora. Jaki rodzaj zagrożenia opisuje ta sytuacja?

- ( ) konserwacji
- ( ) konfiguracyjne
- ( ) środowiskowe
- ( ) elektryczne

11. Co oznacza termin podatność?

- ( ) komputer zawierający poufne informacje
- ( ) metoda ataku w celu wykorzystania celu
- ( ) znany cel lub maszyna ofiary
- ( ) potencjalne zagrożenie, które tworzy haker
- ( ) słaby punkt, który sprawia, że cel jest podatny na atak

12. Jakie trzy kroki konfiguracyjne muszą być wykonane, aby wdrożyć dostęp SSH do routera? (Wybierz trzy odpowiedzi).

- [ ] unikalna nazwa hosta
- [ ] jakieś unikalne hasło
- [ ] nazwa domeny IP
- [ ] hasło trybu uprzywilejowanego
- [ ] konto użytkownika
- [ ] hasło na linii konsoli

13. Jaki jest cel ataku rozpoznania sieci?

- ( ) odkrywanie i mapowanie systemów
- ( ) wyłączanie systemów lub usług sieciowych
- ( ) odmawianie dostępu do zasobów przez uprawnionych użytkowników

- nieautoryzowana manipulacja danymi

14. Ze względów bezpieczeństwa administrator sieci musi zagwarantować, że lokalne komputery nie mogą komunikować się ze sobą za pomocą pakietów ping. Które ustawienia pomogą wykonać to zadanie?

- ustawienia zapory
- ustawienia systemu plików
- ustawienia kart elektronicznych
- ustawienia adresów MAC

15. Administrator sieci ustanawia połączenie z przełącznikiem przez SSH. Jaka cecha jednoznacznie opisuje połączenie SSH?

- zdalny dostęp do przełącznika za pomocą połączenia telefonicznego
- dostęp do przełącznika za pomocą bezpośrednio podłączonego komputera i kabla konsoli
- bezpośredni dostęp do przełącznika za pomocą programu emulacji terminala
- dostęp poza pasmem do przełącznika za pomocą wirtualnego terminala z uwierzytelnianiem hasłem
- zdalny dostęp do przełącznika, w którym dane są szyfrowane podczas sesji

Sprawdź

Rozwiązanie

Resetuj

16.4 Bezpieczeństwo urządzeń

17.0 Wprowadzenie