Bezpieczeństwo urządzeń

16.4.1

Cisco AutoSecure

Jednym z obszarów sieci, który wymaga szczególnej uwagi, aby utrzymać bezpieczeństwo, są urządzenia. Prawdopodobnie masz już hasło do komputera, smartfona lub tabletu. Czy jest tak silne, jak może być? Czy używasz innych narzędzi, aby zwiększyć bezpieczeństwo swoich urządzeń? W tym temacie dowiesz się, jak.

Ustawienia zabezpieczeń są ustawione na wartości domyślne, gdy nowy system operacyjny jest instalowany na urządzeniu. W większości przypadków, ten poziom bezpieczeństwa jest niewystarczający. W przypadku routerów Cisco można użyć funkcji Cisco AutoSecure w celu zabezpieczenia systemu, jak pokazano w przykładzie.

```
Router# auto secure
                --- AutoSecure Configuration ---
*** AutoSecure configuration enhances the security of
the router but it will not make router absolutely secure
from all security attacks ***
```

W dodatku istnieje kilka prostych kroków, które powinny zostać podjęte i które stosuje się do większości systemów operacyjnych:

- Domyślne nazwy użytkownika i domyślne hasła należy natychmiast zmienić.
- Dostęp do zasobów systemu powinien być ograniczony tylko do osób, które są uprawnione do korzystania z tych zasobów.
- Wszystkie niepotrzebne usług i aplikacje powinny być wyłączone i odinstalowane o ile to możliwe.

Często urządzenia dostarczone przez producenta były przechowywane przez pewien czas w magazynie i nie posiadają zainstalowanych najnowszych uaktualnień. Ważne jest aby dokonać aktualizacji jego oprogramowania i zainstalować wszelkie poprawki zabezpieczeń.

16.4.2

Hasła

W celu ochrony urządzeń w sieci, ważne jest użycie silnych haseł. Oto standardowe wytyczne, których należy przestrzegać:

- Użyj hasła o długości co najmniej ośmiu znaków, najlepiej 10 lub więcej. Im dłuższe tym bezpieczniejsze hasło.
- Stosuj skomplikowane hasła. O ile to dozwolone zawieraj w nich zestaw wielkich i małych liter, cyfr, symboli i znaków spacji.
- Unikaj haseł opartych na powtórzeniu tych samych słów, typowych słów ze słownika, sekwencji liter i liczb, nazw użytkownika, nazwisk i imion krewnych lub zwierząt, informacji biograficznych, takich jak miejsce urodzenia, numery identyfikacyjne, nazwy przodków lub innych łatwo identyfikowalnych elementów informacji.
- Celowo wprowadzaj błędy lub przekręcenia w haśle. Na przykład: Smith = Smyth = 5mYth lub Security = 5ecur1ty.
- Zmieniaj często hasła. Jeśli hasło zostanie nieświadomie naruszone, okno możliwości użycia hasła przez podmiot zagrożenia jest ograniczone.
- Nie zapisuj haseł i nie zostawiaj je w widocznych miejscach, np. na biurku lub monitorze.

Tabele pokazują przykłady silnych i słabych haseł.

Słabe hasła

Słabe hasło	Dlaczego jest słabe
sekret	Proste słowo ze słownika
nowak	Panieńskie nazwisko matki
toyota	Marka samochodu
jan1967	Imię i data urodzin użytkownika
Niebieskiptak23	Typowe słowa i liczby

Silne hasła

Silne hasła	Dlaczego są silne
b67n42d39c	Kombinacja łącząca znaki alfanumeryczne
12^h u4@1p7	Kombinacja łącząca znaki alfanumeryczne a także symbole i spacje

Na routerach Cisco, spacje na początku hasła są ignorowane, ale po pierwszym znaku już nie. Dlatego jednym ze sposobów tworzenia silnego hasła jest użycie spacji w haśle i utworzenie wyrażenia składającego się z wielu wyrazów. Jest to fraza szyfrująca. Fraza szyfrująca jest często łatwiejsza do zapamiętania niż proste hasła. Jest również dłuższe i trudniejsze do odgadnięcia.

16.4.3

Dodatkowe zabezpieczenia hasła

Silne hasła są użyteczne jedynie kiedy są tajne. Istnieje kilka kroków, które można podjąć, aby zapewnić, że hasła pozostaną tajne na routerze Cisco i przełączniku, w tym:

- Szyfrowanie wszystkich haseł w postaci zwykłego tekstu
- Ustawianie minimalnej dopuszczalnej długości hasła
- Blokowanie ataków siłowych zgadywania haseł
- Wyłączenie nieaktywnego dostępu w trybie uprzywilejowanym EXEC po upływie określonego czasu.

Jak pokazano w przykładowej konfiguracji na rysunku, polecenie **service password-encryption** trybu konfiguracji globalnej uniemożliwia nieupoważnionym osobom przeglądanie haseł w postaci zwykłego tekstu w pliku konfiguracyjnym. To polecenie szyfruje wszystkie hasła w postaci zwykłego tekstu. Zauważ w przykładzie, że hasło „Cisco” zostało zaszyfrowane jako „03095A0F034F”.

Aby upewnić się, że wszystkie skonfigurowane hasła mają minimalną określoną długość, użyj polecenia **security passwords min-length** *length* w trybie konfiguracji globalnej. Na rysunku każde nowe skonfigurowane hasło musiałoby mieć minimalną długość ośmiu znaków.

Podmioty zagrożeń mogą używać oprogramowania do łamania haseł do przeprowadzenia ataku siłowego (brute-force) na urządzenie sieciowe. Ten atak nieustannie próbuje odgadnąć prawidłowe hasła, dopóki któreś nie zadziała. Użyj polecenia **login block-for # attempts # within #** konfiguracji globalnej, aby zniechęcić do tego typu ataku. Na przykład w tej komendzie polecenie **login block-for 120 attempts 3 within 60** zablokuje próby logowania na vty przez 120 sekund, jeśli wystąpią trzy nieudane próby logowania w ciągu 60 sekund.

Administratorzy sieci mogą się rozproszyć i przypadkowo pozostawić otwartą sesję uprzywilejowanego trybu EXEC na terminalu. Może to umożliwić wewnętrznemu podmiotowi zagrożenia dostęp do zmiany lub usunięcia konfiguracji urządzenia.

Domyślnie, routery Cisco wylogują sesję EXEC po 10 minutach bezczynności. Można jednak zmniejszyć to ustawienie za pomocą polecenia **exec-timeout** *minutes seconds* w trybie konfiguracji linii. Polecenie to można zastosować na liniach console, aux i vty. Na rysunku, mówimy urządzeniu Cisco, aby automatycznie odłączało nieaktywnego użytkownika na linii vty po tym, jak użytkownik będzie bezczynny przez 5 minut i 30 sekund.

```
R1(config)# service password-encryption
R1(config)# security passwords min-length 8
R1(config)# login block-for 120 attempts 3 within 60
R1(config)# line vty 0 4
R1(config-line)# password cisco123
R1(config-line)# exec-timeout 5 30
R1(config-line)# transport input ssh
R1(config-line)# end
R1#
R1# show running-config | section line vty
line vty 0 4
  password 7 094F471A1A0A
  exec-timeout 5 30
  login
  transport input ssh
R1#
```

16.4.4

Włączenie SSH

Telnet upraszcza zdalny dostęp do urządzenia, ale nie jest bezpieczny. Dane zawarte w pakiecie telnet są nadawane w postaci niezaszyfrowanej. Z tego powodu zaleca się, aby uruchomić Secure Shell (SSH) jako narzędzie do bezpiecznego zdalnego dostępu.

Możliwe jest skonfigurowanie urządzenia Cisco do obsługi SSH, wykonując następujące sześć kroków:

Krok 1. Configure a unique device hostname. Urządzenie musi mieć unikalną nazwę hosta inną niż domyślna.

Krok 2. Configure the IP domain name. Skonfiguruj nazwę domeny IP sieci za pomocą polecenia **ip-domain name** trybu konfiguracji globalnej.

Krok 3. Generate a key to encrypt SSH traffic. SSH szyfruje ruch między źródłem a miejscem docelowym. Aby to zrobić, należy wygenerować unikalny klucz uwierzytelnienia za pomocą polecenia konfiguracji globalnej **crypto key generate rsa general-keys modulus** *bits*. Modules *bits* określa rozmiar klucza i może być skonfigurowany od 360 bitów do 2048 bitów. Im większa wartość bitowa, tym bardziej bezpieczny klucz. Jednak większe wartości bitowe również wymagają dłuższego czasu szyfrowania i deszyfrowania informacji. Minimalna zalecana długość modułu to 1024 bity.

Krok 4. Verify or create a local database entry. Utwórz wpis nazwy użytkownika lokalnej bazy danych za pomocą polecenia **username** trybu konfiguracji globalnej. W tym przykładzie użyto parametru **secret**, aby hasło zostało zaszyfrowane przy użyciu MD5.

Krok 5. Authenticate against the local database. Użyj polecenia **login local** konfiguracji linii, aby uwierzytelnić wiersz vty w lokalnej bazie danych.

Krok 6. Enable vty inbound SSH sessions. Domyślnie żadna sesja wejściowa nie jest dozwolona na liniach vty. Można określić wiele protokołów wejściowych, w tym Telnet i SSH za pomocą polecenia **transport input [ssh | telnet]**.

Jak pokazano na przykładzie, router R1 jest skonfigurowany w domenie span.com. Informacje te są używane wraz z wartością bitową określoną w poleceniu **crypto key generate rsa general-keys modulus** w celu utworzenia klucza szyfrowania.

Następnie tworzony jest lokalny wpis bazy danych dla użytkownika o nazwie Bob. Wreszcie, wiersze vty są skonfigurowane do uwierzytelniania w lokalnej bazie danych i akceptowania tylko przychodzących sesji SSH.

```
Router# configure terminal
Router(config)# hostname R1
R1(config)# ip domain name span.com
R1(config)# crypto key generate rsa general-keys modulus 1024
The name for the keys will be: Rl.span.com % The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

```
Dec 13 16:19:12.079: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)#
R1(config)# username Bob secret cisco
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# exit
R1(config)#
```

16.4.5

Wyłącz nieużywane usługi

Routery i przełączniki Cisco uruchamiają się z listą aktywnych usług, które mogą lub nie będą wymagane w Twojej sieci. Wyłącz wszelkie nieużywane usługi, aby zachować zasoby systemowe, takie jak procesor i pamięć RAM, i aby uniemożliwić podmiotom zagrożenia ich wykorzystanie. Rodzaje usług, które są domyślnie włączone, będą się różnić w zależności od wersji IOS. Na przykład IOS-XE zazwyczaj będą miały otwarte tylko porty HTTPS i DHCP. Możesz to sprawdzić za pomocą polecenia **show ip ports all**, jak pokazano w przykładzie.

```
Router# show ip ports all
Proto Local Address              Foreign Address            State       PID/Program Name
TCB       Local Address              Foreign Address            (state)
tcp   :::443                     :::*                       LISTEN      309/[IOS]HTTP CORE
tcp   *:443                      *:*                        LISTEN      309/[IOS]HTTP CORE
udp   *:67                        0.0.0.0:0                              387/[IOS]DHCPD Receive
Router#
```

Wersje IOS sprzed IOS-XE używają polecenia **show control-plane host open-ports**. Wspominamy to polecenie, ponieważ możesz je zobaczyć na starszych urządzeniach. Wyjście jest podobne. Należy jednak zauważyć, że ten starszy router ma uruchomiony niebezpieczny serwer HTTP i Telnet. Obie te usługi powinny być wyłączone. Jak pokazano na przykładzie, wyłącz HTTP za pomocą polecenia **no ip http server** trybu konfiguracji globalnej. Wyłącz Telnet, określając tylko SSH w poleceniem konfiguracji linii, **transport input ssh**.

```
Router# show control-plane host open-ports
```

```
Active internet connections (servers and established)
Prot        Local Address      Foreign Address                 Service    State
 tcp                *:23                *:0                   Telnet   LISTEN
 tcp                *:80                *:0               HTTP CORE   LISTEN
 udp                *:67                *:0           DHCPD Receive   LISTEN
Router# configure terminal
Router(config)# no ip http server
Router(config)# line vty 0 15
Router(config-line)# transport input ssh
```

16.4.6

Packet Tracer - Konfiguracja bezpiecznych haseł i SSH

Administrator sieci poprosił o przygotowanie RTA i SW1 do wdrożenia. Zanim zostaną one podłączone do sieci, muszą być włączone środki bezpieczeństwa.

Konfiguracja bezpiecznych haseł i SSH

Konfiguracja bezpiecznych haseł i SSH

16.4.7

Laboratorium - Konfiguracja urządzeń sieciowych za pomocą SSH

Celem tego ćwiczenia jest realizacja następujących zadań:

- Część 1: Konfigurowanie podstawowych ustawień urządzenia
- Część 2: Konfigurowanie routera dla zdalnego dostępu poprzez SSH
- Część 3: Konfiguracja dostępu do przełącznika poprzez SSH
- Część 4: Uruchamianie SSH z linii poleceń CLI w przełączniku

Konfigurowanie dostępu do urządzeń sieciowych

16.3
Działania zaradcze atakom sieciowym

16.5
Moduł ćwiczeń i quizów