

Laboratorium - Zbadaj procedury odzyskiwania hasła

Cele

Część 1: Zbieranie informacji na temat rejestru konfiguracyjnego

- Określenie znaczenia rejestru konfiguracyjnego.
- Opisanie zachowania się routera dla różnych wartości rejestru konfiguracyjnego.

Część 2: Dokumentowanie procedury odzyskiwania hasła dla konkretnego routera Cisco

- Poznawanie i rejestrowanie procesu odzyskiwania hasła na określonym routerze Cisco.
- Odpowiedz na pytania na podstawie przeprowadzonych badań.

Tło / scenariusz

Celem tego ćwiczenia jest poznanie procedury odzyskiwania lub kasowania hasła umożliwiającego dostęp do trybu uprzywilejowanego na określonym routerze Cisco. Komenda `enable password` umożliwia zabezpieczenie dostępu użytkownika do trybu uprzywilejowanego oraz trybu konfiguracji globalnej na urządzeniach Cisco. Hasło dostępu do trybu uprzywilejowanego ustawione za pomocą komendy `enable password` można odzyskać wykonując odpowiednią procedurę. Hasło ustawione za pomocą komendy `enable secret` jest automatycznie szyfrowane i dlatego podczas procedury odzyskiwania może być ono tylko zastąpione nowym hasłem.

Aby ominąć hasło, użytkownik musi zapoznać się z pracą w trybie monitora ROM (rommon) oraz ustawieniami rejestru konfiguracyjnego w routerach Cisco. ROMMON to oprogramowanie zapisane w pamięci ROM, zawierające zbiór podstawowych poleceń. Polecenia te mogą być użyte do rozwiązywania problemów podczas procesu uruchamiania routera oraz w przypadku problemów z systemem IOS.

Niniejsze laboratorium rozpocznieś od poznania znaczenia i ustawień rejestru konfiguracyjnego dla urządzeń Cisco. Następnie poznasz szczegółowo dokładną procedurę odzyskiwania hasła dla konkretnego routera Cisco.

Wymagane zasoby

- Urządzenie z dostępem do Internetu

Instrukcje

Część 1: Zbadaj rejestr konfiguracji

Aby odzyskać lub skasować hasło dostępu do trybu uprzywilejowanego, użytkownik będzie korzystać z interfejsu ROMMON. Tryb ten umożliwi zignorowanie konfiguracji startowej przez router podczas jego uruchamiania. Po uruchomieniu routera użytkownik uzyska dostęp do trybu uprzywilejowanego, nadpisze bieżącą konfigurację przy użyciu zapisanej konfiguracji startowej, a następnie odzyska lub skasuje hasło. Po wykonaniu tych czynności zostanie przywrócony domyślny proces uruchamiania routera wykorzystujący konfigurację startową.

Rejestr konfiguracyjny routera odgrywa istotną rolę w procesie odzyskiwania hasła. W pierwszej części tego ćwiczenia poznasz rolę rejestru konfiguracyjnego routera oraz znaczenie konkretnych jego wartości.

Krok 1: Opisz przeznaczenie rejestru konfiguracyjnego.

Jakie jest znaczenie rejestru konfiguracyjnego?

Jakie polecenie zmienia rejestr konfiguracji w trybie konfiguracji globalnej?

Jakie polecenie zmienia rejestr konfiguracyjny w trybie ROMMON?

Krok 2: Opisz wartości rejestru konfiguracyjnego oraz ich znaczenie.

Sprawdź i zanotuj zachowanie się routera dla następujących wartości rejestru konfiguracyjnego.

0x2102

0x2142

Opisz na czym polega różnica w procesie startowania routera dla powyższych dwóch wartości rejestru konfiguracyjnego?

Część 2: Udokumentuj procedurę odzyskiwania hasła dla określonego routera Cisco

W części 2 możesz opisać dokładnie procedurę odzyskiwania lub kasowania hasła dla konkretnego routera Cisco oraz odpowiedzieć na pytania w oparciu o wyniki twoich doświadczeń. Instruktor dostarczy Ci konkretny model routera do ćwiczenia.

Krok 1: Szczegółowy proces odzyskiwania hasła na konkretnym routerze Cisco.

Poznaj oraz wykonaj listę czynności i poleceń, które są wymagane, by odzyskać lub skasować hasło trybu uprzywilejowanego lub hasło zaszyfrowane w routerze Cisco. Opisz swoimi słowami wykonywane czynności.

Krok 2: Odpowiedz na pytania dotyczące procedury odzyskiwania hasła.

Korzystając z procesu odzyskiwania hasła, odpowiedz na poniższe pytania.

Jak znaleźć bieżącą wartość ustawienia rejestru konfiguracyjnego?

Opisz proces przechodzenia do trybu ROMMON.

Jakie polecenia są wymagane, aby przejść do interfejsu ROMMON?

Jaki komunikat można otrzymać w trakcie restartowania routera?

Dlaczego ważne jest, aby załadować konfigurację startową do konfiguracji bieżącej?

Dlaczego tak ważne jest, aby zmienić rejestr konfiguracyjny do pierwotnej wartości po odzyskaniu hasła?

Pytania do przemyślenia

Dlaczego ważne jest zabezpieczenie polegające na fizycznym zabezpieczeniu routera przed nieautoryzowanym dostępem?