

Password Recovery

Pre Cisco routers

Účel: Rekonfigurovať Cisco zariadenie (Router, Switch) ktoré je zabezpečené neznámym heslom pre vstup do privilegovaného režimu. Treba dosiahnuť stav, aby bolo umožnené vstúpiť do privilegovaného režimu a zameniť neznáme heslo za vlastné, pri zachovaní existujúcich konfiguračných nastavení.

Scenár: Bývalý administrátor zanechal zariadenia zaheslované svojim heslom, ktoré nie je nikomu vo firme známe. Nový administrátor má prevziať zariadenia do svojej správy a zachovať existujúce konfiguračné nastavenia.

Postup (platný pre router Cisco 2600 family, 2800 family) :

1. Spustiť vzdialený prístup (Hyperterminal) cez konzolu
2. Po spustení routera v prvej fáze bootovania prerušiť bootovanie príkazom *Ctrl-Break* (platí pre *Hyperterminal*). Vstúpime do režimu *rommon*.

```
rommon 1>
```

3. V režime *rommon* rekonfigurovať registre tak, aby pri štarte zariadenia bol obchádzaný štartovací konfiguračný súbor : 0x2142

```
rommon 1> confreg 0x2142
```

4. Reštartovať zariadenie

```
rommon 2>reset
```

5. Pri inicializačnej procedúre ignorovať štartovací konfiguračný dialog (odpovedať no, no, no...)

6. Vstúpiť do privilegovaného režimu, musí fungovať bez hesla

```
Router>enable
```

```
Router#
```

7. Overiť, že štartovací konfiguračný súbor obsahuje všetky existujúce konfigurácie a že aktívny bežiaci konfiguračný súbor obsahuje iba základné defaultné nastavenia

```
Router# SHOW STARTUP-CONFIG
```

```
Router#SHOW RUNNING-CONFIG
```

8. Nahrať štartovaciu konfiguráciu ako bežiacu

```
Router#copy STARTUP-CONFIG RUNNING-CONFIG
```

POZOR!!! Opačný príkaz Router#copy RUNNING-CONFIG STARTUP-CONFIG spôsobí nenávratnú stratu existujúcej štartovacej konfigurácie!!!

9. Vytvoriť vlastné heslo pre vstup do privilegovaného režimu:

```
Router#configure terminal
```

```
Router(config)#enable secret cisco
```

10. Overiť, že všetky konfigurované rozhrania sú aktívne a funkčné (rozhrania budú v režime shut)

```
Router(config)#int fa 0/0
```

```
Router(config-if)#no shut
```

... opakovať pre všetky nakonfigurované rozhrania

11. Rekonfigurovať registre tak, aby pri ďalšom spustení zariadenia bola automaticky aktivovaná štartovacia konfigurácia ako bežiacia

```
Router(config)#config-register 0x2102
```

POZOR!!! Ak zabudnete vykonať tento krok, nebude pri ďalšom spustení zariadenia aktivovaná štartovacia konfigurácia a zariadenie sa bude správať, ako keby nemala funkčnú NVRAM

12. Opravenú bežiacu konfiguráciu nahráť ako štartovaciu

```
Router#copy RUNNING-CONFIG STARTUP-CONFIG
```