سیسکو به پارسی

بازیابی رمز روتر سیسکو – آموزش مقدماتی

نوشته:
شفق زندی

سایت سیسکو به پارسی http://blog.shafagh.com/persian
انجمن سیسکو به پارسی http://forum.shafagh.com

بازیابی پسورد روتر Password Recovery

انسان فراموشکار است و در صورت فراموش کردن رمز دستگاه، استفاده از آن مقدور نخواهد بود. Password Recovery عملیاتی است که در آن Password فراموش شده سیسکو را تغییر میدهیم. برای این کار دسترسی فیزیکی به دستگاه بواسطه ارتباط به کنسول و دسترسی به کلید برق روتر، حداقل موارد مورد نیاز هستند. بصورت نرمال روتر از مراحل زیر برای Boot شدن استفاده میکند:

۱.روتر روشن شده و توسط ROM راه اندازی میشود.
۲.روتر Configuration-Register را چک میکند.
۳.روتر فایل Configuration را داخل NVRAM، Load میکند تا IOS را بخواند.
۴.براساس Configuration، IOS را انتخاب میکند و IOS را درون RAM، Decompress و نهایتا اجرا میکند.

Configuration-Register یک عدد به میزان ۲ بایت است که بصورت HEX نشان داده میشود. توسط این مقدار مشخص میگردد تا روتر از چه منبعی و به چه صورتی Boot شود. در ضمن سرعت پورت Console و مشخصات دیگری نیز توسط این ۲ بایت معین میگردند که از حوصله بحث ما خارج است.

با توجه به اینکه وقتی سیستم بالا می آید از شما Password را سوال میکند و این رمز در Configuration ذخیره شده است، برای اینکه از دست Password خلاص شویم باید روتر را بدون Configuration بالا آوریم (زیرا پسورد درون تنظیمات قرار دارد) برای این کار باید سراغ Configuration-Register رفت و مرحله ای که در آن Configuration خوانده میشود را از کار انداخت. برای این کار باید Configuration-Register را به 0x2142 تغییر داد. اما مشکل اینجاست که دسترسی نرم افزاری به Router نداریم (رمز عبور گمشده است) پس باید روتر را بصورت سخت افزاری خاموش و روشن (ریست) کنیم.

در زمان بوت شدن IOS از کلید های Control + Break روی صفحه کلید (بواسطه کنسول) استفاده میکنیم تا این مرحله دچار Break شده و ما را به ROMMON ببرد. در ROMMON میتوانیم با دستور confreg 0x2142 روتر را موظف کنیم تا فایل Configuration را نخوانده و مثل یک روتر جدید، بدون تنظیم بوت شود.

بعد از تغییر Confreg دستور i یا Initialize را زده تا روتر Reload شود. پس از آنکه روتر بدون تنظیم بالا می آید، درون Enable رفته و محتویات NVRAM را درون Running Config کپی میکنیم تا تنظیماتمان از بین نرود. سپس Enable Secret یا هر Password ی که فراموش کردیم را تغییر داده و درون NVRAM کپی میکنیم، (Copy running-config startup-config) سپس مقدار Configuration-register را به عدد 0x2102 برمیگردانیم.

Cisco in Persian

مراحل به ترتیب عملکرد:

۱	روتر را ریبوت میکنیم (از طریق برق)
۲	در حین بوت شدن روتر CONTROL+BREAK
۳	*ROMMON>* **confreg 0x2142**
۴	*ROMMON>* **i**
۵	دستور i موجب میشود تا روتر را ریبوت شود (مخفف Initialize در صورتیکه عمل نکرد خاموش روشن کنید)
۶	*Router>* **enable**
۷	*Router#* **copy startup-config running-config**
۸	*Router#* **config terminal**
۹	*Router(config)#* **enable secret newpassword**
۱۰	*Router(config)#* **configuration-register 0x2102**
۱۱	*Router(config)#* **exit**
۱۲	*Router#* **copy running-config startup-config**

Cisco in Persian

باید توجه داشت که در مرحله ۶ از NVRAM به RAM کپی میکنیم و پس از تغییر Password، بار دیگر در مرحله ۱۱ از RAM به NVRAM کپی انجام میشود تا Configuration را از دست نداده و تنها رمز را تغییر دهیم.

نکته مهم دیگر آن است که هر بار که فایلی به NVRAM ریخته میشود جای فایل قبلی را میگیرد (یا Replace میشود) اما وقتی فایلی به RAM کپی میشود با محتویات کنونی RAM ادغام یا Merge میشود.

از آنجا که دستور Shutdown در تنظیمات جدید روتر روی Interface ها بصورت پیش فرض قرار دارد بعد از مرحله Password Recovery باید Interface ها را یک به یک no shutdown کنیم.