ایمن سازی روتر سیسکو

امروز بحث امنیت روترها بسیار داغ و جدی شده است برای همین در این مقاله چند نکته کوچک ولی مهم را برای شما یادآوری میکنیم.

چون خود روتر میتواند یک هدف خوب برای انواع حملات باشد به شکلی که اگر کسی مثلا مسیریاب مرزی شما رو High Load کند عبور ترافیک به مشکل بر خورده و شبکه شما در ارتباط با اینترنت فلج میشود لذا چند نکته که استفاده از آنها ما را به حداکثر امنیت میرساند را باید رعایت کنیم.

۱- **پورت های خطرناک را ببندید** :یکی از مهم ترین نکات امنیتی این است که اگر از چیزی استفاده نمی کنید آن را غیرفعال کنید

130 deny tcp any any range 135 140 (497235 matches)

140 deny udp any any range 135 140 (8303931 matches)

150 deny tcp any any eq 445 (24650346 matches)

160 deny tcp any any eq 449 (11 matches)

170 deny tcp any any eq daytime (39 matches)

180 deny tcp any any range 27000 27020 (6547 matches)

190 deny udp any any range 27000 27020 (290 matches)

200 deny tcp any any range 1024 1030 (24568 matches)

210 deny tcp any any range 1363 1380 (174634 matches)

220 deny udp any any eq 11751 (23 matches)

230 deny tcp any any eq 11751 (441 matches)

240 deny udp any any eq 1434 (10814 matches)

250 deny tcp any any eq 1433 (536911 matches)

260 deny udp any any eq 1433 (193 matches)

270 deny tcp any any eq 1434 (9133 matches)

280 deny tcp any any eq 554 (191 matches)

290 deny tcp any any eq 7070 (225 matches)

300 deny tcp any any eq 2773 (5923 matches)

310 deny tcp any any eq 54283 (590 matches)

320 deny udp any any eq echo (812 matches)

330 deny tcp any any eq echo (44 matches)

340 deny tcp any any eq discard (44 matches)

350 deny udp any any eq 554 (204 matches)

360 deny udp any any eq 7070 (8 matches)

370 deny tcp any any eq 8866 (261 matches)

380 deny tcp any any eq 9898 (230 matches)

390 deny tcp any any eq 10000 (271 matches)

400 deny tcp any any eq 10080 (1031 matches)

410 deny tcp any any eq 12345 (432 matches)

420 deny tcp any any eq 17300 (221 matches)

430 deny tcp any any eq 8554 (255 matches)

440 deny udp any any eq 8554 (8 matches)

450 deny udp any any eq 4444 (90 matches)

460 deny tcp any any eq 4444 (3850 matches)

470 deny tcp any any eq 5554 (369 matches)

480 deny udp any any eq 1500 (173 matches)

490 deny tcp any any eq 1919 (8152 matches)

500 deny tcp any any eq 2967 (5250 matches)

510 deny udp any any eq 2967 (101 matches)

520 deny tcp any any eq 1425 (10084 matches)

530 deny tcp any any eq 6667 (18607 matches)

540 deny tcp any any eq 8943 (221 matches)

550 deny tcp any any eq 4662 (3630 matches)

560 deny tcp any any eq 1034 (2946 matches)

570 deny tcp any any eq 81 (9123 matches)

580 deny tcp any any eq 8181 (420 matches)

590 deny tcp any any eq 2339 (6884 matches)

600 deny tcp any any eq 31337 (331 matches)

610 deny tcp any any eq 2745 (6134 matches)

620 deny tcp any any eq 37 (39 matches)

630 deny tcp any any eq 1500 (9704 matches)

640 deny tcp any any eq 1501 (9367 matches)

650 deny tcp any any eq 1502 (9473 matches)

660 deny tcp any any eq 1503 (9126 matches)

670 deny udp any any eq 1501 (160 matches)

680 deny udp any any eq 1502 (258 matches)

690 deny udp any any eq 1503 (168 matches)

700 deny tcp any any eq 1214 (11340 matches)

710 deny udp any any eq 65506 (326 matches)

720 deny udp any any eq 3410 (158 matches)

730 deny udp any any eq 3128 (148 matches)

740 deny udp any any eq 3127 (202 matches)

750 deny udp any any eq 8080 (207 matches)

760 deny udp any any eq 1111 (408 matches)

770 deny udp any any eq 8998 (9 matches)

780 deny udp any any eq 27374 (51 matches)

790 deny udp any any eq 1214 (107 matches)

800 deny udp any any eq 9999 (36 matches)

810 deny udp any any eq tftp

820 deny udp any any eq 2745 (208 matches)

830 deny tcp any any eq 1080 (10329 matches)

850 deny tcp any any eq sunrpc (42 matches)

860 deny tcp any any eq nntp (46 matches)

870 deny tcp any any eq drip (4244 matches)

880 deny tcp any any eq exec (1 match)

890 deny udp any any eq rip (1 match)

900 deny udp any any eq ntp (58094 matches)

910 deny tcp any any eq 2283 (6850 matches)

920 deny tcp any any eq 2535 (6262 matches)

930 deny udp any any eq 1026 (1711 matches)

940 permit ip any any (864701348 matches)

950 permit icmp any any

لازم است یک ACL با سیاست خودتان و مثلا پورت های عمومی خطرآفرین تهیه و انرا روی اینترفیس ورودی اعمال کنید.

```
conf t
int gig0/0
ip acce firewall in
ip acce firewall out
```

2 – باز هم توصیه میشود دسترسی Telnet را با SSH جایگزین کنید.

یکی از مسائلی که ممکن است باعث به خطر افتادن امنیت روتر های مرزی که دارای IP Valid روی پورت های خود میباشد عملیات Burst Force برای پیدا کردن دسترسی Telnet میباشد. در درجه اول توصیه میشود که به جای تلنت از SSH استفاده کنید .

۳ – آدرس های عمومی را در درگاه وروردی اینترنت جهت جلوگیری از Spoofing ببندید و یک نکته حرفه ای اینکه یک BGP Peeringبا شبکه team-cymruبرقرار کنید و ورودی route ها را باز بگذارید این شرکت IP های BOGONN را برای شما ارسال میکند و این لیست خود به خود آپدیت و جلوی route شما به این دسته از IPP ها را میگیرد:

```
access-list 111 deny ip 127.0.0.0 0.255.255.255 any

access-list 111 deny ip 192.168.0.0 0.0.0.255 any

access-list 111 deny ip 172.16.0.0 0.0.255.255 any

access-list 111 deny ip 10.0.0.0 0.255.255.255 any

access-list 111 deny ip host 0.0.0.0 any

access-list 111 deny ip 224.0.0.0 31.255.255.255 any

access-list 111 deny icmp any any redirect
```

4 – دسترسی SNMP را یا ببندید یا محدود کنید:

```
no snmp-server or<
```

snmp-server community SnMp@@!!123 RO 197

ip acce e 197

permit udp “trusted host ips” host “router ip” eq snmp

deny ip any any

۵- به جای enable password از enable secret استفاده کنید و پسورها را hash کنید:

service password-encryption

enable secret 5 f77a8a14ff273beddf3a6a3d3632158b/

username amirkhosro privilege 15 secret 5 $f77a8a14ff273beddf3a6a3d3632158b$.

این باعث میشود که دسترسی به پسورد شما حتی اگر کسی فایل کانفیگ روتر را هم داشته باشد غیر ممکن شود چون MD5مثلا یک الگریتم یک طرفه است!

۶- سرویس بازنگاری پسورد را غیر فعال کنید : بدین ترتیب اگر کسی دسترسی فیزیکی هم به روتر پیدا کند نمیتواند پسور شما را ریکاور کند!

R1(config)#no service password-recovery
WARNING:
Executing this command will disable password recovery me
chanism.
Do not execute this command without another plan for
password recovery.

Are you sure you want to continue? [yes/no]:yes

۷- سرویس هایی که بدرد شما نمیخورد را disable کنید:

شما باید بدانید از چه سرویس هایی استفاده می کنید و از کدام ها استفاده نمی کنید. در زیر چند سرویس آورده شده است ولی ممکن است بعضی از سرویس های آورده شده در سناریوی شما کاربرد داشته باشد و ممکن است نداشته باشد پس دقت کنید.

Disable Echo, Chargen and discard
no service tcp-small-servers
no service udp-small-servers

Disable finger
no service finger

Disable the httpd interface
no ip http server

Disable ntp (if you are not using it)
ntp disable

Disable source routing
no ip source-route

Disable Proxy Arp
no ip proxy-arp روی تمامی اینترفیس ها

Disable ICMP redirects
interface gig0/0
no ip redirects روی تمامی اینترفیس ها

Disable Multicast route Caching
interface gig0/0 (your external interface)
no ip mroute-cache روی تمامی اینترفیس ها

Disable CDP
no cdp run

Disable direct broadcast (protect against Smurf attacks)
no ip directed-broadcast روی تمامی اینترفیس ها

۸– فقط IP های ست شده روی هر اینترفیس را مجاز کنید مثلا:

Core-Router#sh run int fastEthernet 0/1.300
Building configuration…

Current configuration : 281 bytes
!
interface FastEthernet0/1.300
description esfehan

```
encapsulation dot1Q 300
ip address 217.218.1.1 255.255.255.248
no ip redirects
no ip unreachables
no ip proxy-arp
end
Core-Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Core-Router(config)#ip acce e 130
Core-Router(config-ext-nacl)#per ip 217.218.1.0 0.0.0.7 an
Core-Router(config-ext-nacl)#per ip 217.218.1.0 0.0.0.7 any
Core-Router(config-ext-nacl)#per icmp any any
Core-Router(config-ext-nacl)#deny ip any any
Core-Router(config-ext-nacl)#exit
Core-Router(config)#int fas 0/1.300
Core-Router(config-subif)#ip acce 130 in
```

و صد البته روی اینترفیس خروجی فقط IP های شناخته شده شبکه خودتان را اجازه ترانزیت ترافیک بدهید.

مثلا شما یک کلاس ۲۴/ دارید ۲۴/۲۱۷.۲۱۸.۱۰:

```
Core-Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Core-Router(config)#ip acce e 131
Core-Router(config-ext-nacl)#per ip 217.218.1.0 0.0.0.255 any
Core-Router(config-ext-nacl)#per ip any 217.218.1.0 0.0.0.255
Core-Router(config-ext-nacl)#per icmp any any
Core-Router(config-ext-nacl)#deny ip any any
Core-Router(config-ext-nacl)#exit
Core-Router(config)#int gig 0/0 ( outside interface )
ip acce 131 in
ip acce 131 out
```

۹- همه چیز را لاگ کنید:

```
logging trap debugging
logging 192.168.1.10
```

برای افزایش امنیت یک مسیریاب راه های زیادی وجود دارد مثلا کنترل منابع در control-plane و ... این نکات همانطور که در ابتدا اشاره شد حداقل کارهایی است که میبایست برای امنیت مسیریاب انجام دهید. این نکته هم بد نیست بدانید که اگر از گران ترین دستگاه هم استفاده کنید اما به درستی نکات امنیتی را رعایت نکرده باشید به راحتی از دستگاه شما عبور می کنند و البته هیچ وقت امنیت ۱۰۰ درصد نیست ولی میتوان خطرات را کاهش داد.