

پیکربندی امن

MikroTik RouterOS



مرکز مدیریت راهبردی افتا

SCRO-MIKROTIK-ROUTEROS -0.0

اسفند ۹۵

فهرست

پیش گفتار	۴
مقدمه	۵
تنظیمات	۸
SCRO-1: به روز رسانی Package های RouterOS	۸
SCRO-2: امن سازی پورت های فیزیکی	۹
SCRO-2-1: غیر فعال نمودن واسط های بلا استفاده	۹
SCRO-2-2: غیر فعال نمودن پورت کنسول	۹
SCRO-3: امن سازی سرویس ها	۱۰
SCRO-3-1: غیر فعال سازی سرویس های غیر ضروری	۱۰
SCRO-3-2: استفاده از سرویس HTTPS بجای HTTP	۱۱
SCRO-3-3: استفاده از الگوریتم های رمزنگاری قدرتمندتر در SSH	۱۲
SCRO-3-4: غیر فعال نمودن Package های غیر ضروری	۱۲
SCRO-3-5: تغییر شماره پورت سرویس های کاربردی	۱۳
SCRO-3-6: اختصاص ACL جهت دسترسی به سرویس های کاربردی	۱۳
SCRO-3-7: بلاک نمودن WinBox Discovery	۱۴
SCRO-3-8: غیر فعال نمودن Network Neighbor Discovery	۱۴
SCRO-4: امن سازی حساب کاربری	۱۵
SCRO-4-1: تغییر نام حساب کاربری admin پیش فرض سیستم	۱۵
SCRO-4-2: ایجاد رمز عبور پیچیده برای حساب های کاربری	۱۵
SCRO-4-3: اختصاص ACL جهت دسترسی به حساب های کاربری	۱۶
SCRO-5: Firewall	۱۶
SCRO-5-1: فعال سازی Firewall	۱۶
SCRO-5-2: غیر فعال سازی Service Port های غیر ضروری	۱۷

۱۸.....	SCRO-5-3: استفاده از Reverse Path Filtering
۱۸.....	SCRO-5-4: استفاده از Port Knocking
۱۹.....	SCRO-5-5: استفاده از Firewall Scripts
۲۴.....	SCRO-5-6: بستن دسترسی از کشورهای غیرضروری
۲۵.....	SCRO-6: Log
۲۶.....	SCRO-7: NTP
۲۷.....	SCRO-8: SNMP
۲۸.....	پیوست
۳۰.....	جدول ممیزی

پیش گفتار

مرکز مدیریت راهبردی افتا^۱ به منظور ساماندهی امنیت تجهیزات در حوزه فاوا^۲، پروژه «پیکربندی امن محصولات IT در کشور» را آغاز نموده است. یکی از گام‌های اساسی در این پروژه ارائه چک‌لیست و راهنمای پیکربندی امن برای محصولات IT می‌باشد. ارائه چک‌لیست برای محصولات داخلی بر عهده تولیدکننده محصول می‌باشد. تولید کننده ملزم است، چک‌لیست خود را در غالب ارائه شده از سمت مرکز افتا ارائه دهد. چک‌لیست‌های ارائه شده، توسط مرکز افتا مورد ارزیابی قرار گرفته و منتشر می‌گردد. سازمان‌های دولتی ملزم به استفاده از چک‌لیست‌های مذکور برای محصولات در حال استفاده خود هستند. همچنین سازمان‌های دولتی موظفند قبل از استفاده از محصولات IT، آن‌را مطابق چک‌لیست امنیتی مورد تایید مرکز افتا پیکربندی نمایند.

توجه به این نکته حائز اهمیت می‌باشد که چک‌لیست‌های ارائه شده، یک امنیت سطح پایه برای محصول ایجاد می‌نماید و سازمان‌ها ملزم هستند که برای رسیدن به سطح امنیت مورد نیاز خود، پس از اجرای مدیریت ریسک^۳، الزامات دیگری را نیز به این تنظیمات اضافه و مستند نمایند.

^۱ امنیت فضای تولید و تبادل اطلاعات

^۲ فناوری اطلاعات و ارتباطات

^۳ Risk management

مقدمه

این سند راهنمایی برای پیکربندی امن MikroTik RouterOS است. در این سند مقادیر و تنظیمات امن برای سیاست‌های پیکربندی محصول مذکور ارائه شده است. مخاطب با استفاده از این سند توانایی پیاده‌سازی تنظیمات ارائه شده را خواهد داشت.

این سند توسط شرکت "فناوران توسعه امن ناجی" و به درخواست و تحت نظارت مرکز مدیریت راهبردی افتا تهیه گردیده است و از تلاش کارشناسان آن شرکت صمیمانه قدردانی می‌گردد. مرکز مدیریت راهبردی افتا ضمن استقبال از نظرات کارشناسان و متخصصان این حوزه برای غنای بیشتر این سند و دیگر اسناد مقاوم سازی، آمادگی دریافت پیشنهادات سازنده از طریق آدرس پست الکترونیکی Hardening@aftasec.ir را اعلام می‌دارد.

در ادامه، تنظیمات مورد نیاز برای پیکربندی امن MikroTik RouterOS آمده است. در این سند هر تنظیم با یک نام لاتین و شماره مختص آن آورده شده است. برای هر الزام دو بخش شرح اجمالی و نحوه پیاده‌سازی ارائه شده است. در بخش شرح اجمالی، توضیحی مختصر از ماهیت الزام بیان گردیده و در بخش نحوه پیاده‌سازی نیز، راهنمایی برای پیاده‌سازی الزام توسط مدیر سامانه ارائه شده است.

جدول ۱: گروه بندی و اختصار سازی نام برای محصولات IT

محصولات IT	
شماره گروه	نام گروه
AV	نرم افزار آنتی ویروس
AS	سرویس دهنده نرم افزارهای کاربردی ^۴
AU	احراز اصالت ^۵
AT	اتوماسیون
CM	نرم افزار مدیریت پیکربندی ^۶
DB	سیستم مدیریت پایگاه داده
DA	نرم افزار کاربردی رومیزی ^۷
DC	سرویس گیرنده رومیزی ^۸
DS	سرویس دایرکتوری ^۹
DN	DNS سرور
ES	ایمیل سرور
EA	نرم افزار کاربردی سازمانی ^{۱۰}
FI	دیوار آتش ^{۱۱}
HD	تجهیزات قابل حمل ^{۱۲}
IM	مدیریت هویت ^{۱۳}
ID	سیستم تشخیص نفوذ ^{۱۴}

^۴ Application Server

^۵ Authentication

^۶ Configuration Management System

^۷ Desktop Application

^۸ Desktop Client

^۹ Directory Service

^{۱۰} Enterprise Application

^{۱۱} Firewall

^{۱۲} Handheld Device

^{۱۳} Identity Management

^{۱۴} Intrusion Detection System

محصولات IT	
شماره گروه	نام گروه
MS	سرویس دهنده ایمیل ^{۱۵}
MO	راهکارهای موبایلی ^{۱۶}
RO	مسیریاب شبکه ^{۱۷}
SW	سوئیچ شبکه
OS	سیستم عامل
PD	تجهیزات جانبی ^{۱۸}
SR	سرویس دهنده ^{۱۹}
VI	نرم افزار مجازی سازی ^{۲۰}
WB	مرورگر وب
WS	سرویس دهنده وب

^{۱۵} Mail Server

^{۱۶} Mobile Solution

^{۱۷} Network Router

^{۱۸} Peripheral Device

^{۱۹} Server

^{۲۰} Virtualization Software

تنظیمات

SCRO-1: به روزرسانی Package های RouterOS

شرح اجمالی:

از نسخه ۵,۲۱ به بعد RouterOS، ویژگی Automatic Upgrade اضافه شده است. این ویژگی امکان نصب آخرین به روزرسانی های RouterOS را برای Package های نصب شده روی سیستم را فراهم می آورد. با انجام به روزرسانی Package ها از آسیب پذیری های احتمالی بر روی هر یک از آنها می توان جلوگیری نمود.

نحوه پیاده سازی:

جهت به روزرسانی محصولات میکروتیک روش ذیل توصیه می گردد:

- به صورت پیش فرض RouterOS به سایت اصلی میکروتیک مراجعه و نسبت به دانلود بسته های به روزرسانی اقدام می کند. در این صورت از منوی QuickSet بر روی Check For Update کلیک نمایید و از منوی باز شده گزینه Current را انتخاب نموده و اقدام به به روزرسانی بسته های RouterOS نمایید.
 - می توان این پروسه را به صورت خودکار با استفاده از Script ذیل انجام داد.
- برای ورژن بعد از 6.31

```
/system package update
Check-for-updates once
: delay 1s;
: If ([get status] = "New version is available") do= {install}
```

برای ورژن پیش از 6.31

```
System package update
Check-for-updates
: delay 1s;
:if ( [get current-version] != [get latest-version]) do={ upgrade }
```


SCRO-2: امن سازی پورت های فیزیکی

SCRO-2-1: غیر فعال نمودن واسطه های بلا استفاده

شرح اجمالی:

در صورتی که هر نوع واسی که به صورت فیزیکی در حال استفاده قرار ندارد غیر فعال گردد، حتی اگر فرد مهاجم به اتاق سرور و سخت افزار دسترسی پیدا کند باید از واسطه های موجود استفاده کند که در این صورت ترافیک Live از بین می رود و سیستم Log و SIEM متوجه واقعه خواهند شد.

نحوه پیاده سازی:

- ابتدا فهرست تمام واسطه ها را استخراج نمایید.

```
/interface print
```

- سپس با استفاده از ایندکس مربوطه اقدام به غیر فعال نمودن آن نمایید.

```
/interface set 4,5 disabled=yes
```

SCRO-2-2: غیر فعال نمودن پورت کنسول

شرح اجمالی:

در صورت قرار گیری RouterOS در محیط های ناامن، فرد مهاجم با اتصال پورت کنسول می تواند هر نوع دسترسی را برای خود فراهم نماید. از این رو ایجاد راهکاری جهت مدیریت محدود در سیستم اکیدا توصیه می گردد.

نحوه پیاده سازی:

- با استفاده از دستور ذیل می توان این قابلیت را غیر فعال نمود.

```
/system console disable numbers=0
```

- جهت بررسی وضعیت کنسول دستور ذیل را اجرا نمایید.

```
/system console print
```

SCRO-3: امن سازی سرویس ها

SCRO-3-1: غیر فعال سازی سرویس های غیر ضروری

شرح اجمالی:

هر سرویس موجود می تواند یک هدف بالقوه جهت حمله یک مهاجم باشد. از این رو غیر فعال سازی سرویس های غیر ضروری سطح آسیب پذیری سیستم را کاهش می دهد. RouterOS نیز دارای سرویس های مدیریتی و کاربردی پیش فرضی می باشد که برخی از آنها همانند Telnet و http به صورت ذاتی دچار آسیب می باشند.

نحوه پیاده سازی:

- ابتدا فهرست تمام سرویس ها را استخراج نمایید.

```
/ip service print
```

- سپس اقدام به غیر فعال نمودن آن نمایید.

```
/ip service disable [find name=telnet]  
/ip service disable [find name=ftp]  
/ip service disable [find name=www]  
/ip service disable [find name=www-ssl]  
/ip service disable [find name=api]  
/ip service disable [find name=api-ssl]  
/tool bandwidth-server set enabled=no  
/ip dns set allow-remote-requests=no  
/ip socks set enabled=no
```

- همچنین سرویس مربوط به MAC Telnet و MAC Winbox غیر فعال گردد.

```
/tool mac-server set [find] disabled=yes  
/tool mac-server mac-winbox set [find] disabled=yes  
/tool mac-server ping set enabled=no
```

- و در نهایت سرویس RoMON را در صورت عدم نیاز غیر فعال نمایید.

```
/tool romon set enabled=no
```

SCRO-3-2: استفاده از سرویس HTTPS بجای HTTP

شرح اجمالی:

در صورت نیاز به استفاده از سرویس HTTP، توصیه می گردد از سرویس HTTPS به صورت جایگزین استفاده گردد. در سرویس HTTP ترافیک به صورت رمز نشده در حال انتقال است که به راحتی توسط مهاجم قابل شنود و تفسیر می باشد.

نحوه پیاده سازی:

- ابتدا یک CA Certificate ایجاد نمایید.

```
/certificate add name=my-rtr-ca common-name=my-rtr-ca key-usage=key-cert-sign,crl-sign
```

- سپس CA Certificate را امضا نمایید.

```
/certificate sign my-rtr-ca
```

- حالا یک Certificate برای دسترسی HTTPS ایجاد نمایید.

```
/certificate add name=my-rtr common-name=my-rtr key-usage=tls-server
```

- Certificate ایجاد شده را امضا نمایید.

```
/certificate sign ca=my-rtr-ca my-rtr
```

- Certificate های ایجاد شده را به عنوان Trusted در سیستم نشان گذاری نمایید.

```
/certificate set trusted=yes my-rtr-ca
```

```
/certificate set trusted=yes my-rtr
```

- Certificate مربوطه را به سرویس HTTPS اختصاص دهید.

```
/ip service set www-ssl certificate=my-rtr
```

SCRO-3-3: استفاده از الگوریتم‌های رمزنگاری قدرتمندتر در SSH

شرح اجمالی:

از نسخه 6.30 به بعد استفاده از رمزنگاری قدرتمندتر برای SSH در دسترس قرار گرفته است. در کلاینت‌هایی مانند Putty استفاده از الگوریتم‌های قدرتمندتر به صورت پیش‌فرض فعال می‌باشد، پس استفاده از این نوع الگوریتم‌ها باید در سمت سرور SSH فعال گردد. از ماه نوامبر 2016 یک راه الزامی برای غیرفعال نمودن الگوریتم‌های ضعیف‌تر به جهت استفاده عمومی‌تر از SSH وجود ندارد، از این رو تنها گزینه، فعال نمودن الگوریتم‌های رمزنگاری قدرتمندتر در SSH می‌باشد.

نحوه پیاده‌سازی:

- با استفاده از دستور ذیل می‌توان این قابلیت را فعال نمود.

```
/ip ssh set strong-crypto=yes
```

* در ارتباطات مدیریتی RouterOS استفاده از ماژول رمزنگاری منطبق با استاندارد FIPS 140-2 الزامی است.

SCRO-3-4: غیرفعال نمودن Package‌های غیرضروری

شرح اجمالی:

هر Package موجود می‌تواند یک هدف بالقوه جهت حمله یک مهاجم باشد. از این رو غیرفعال سازی Package‌های غیرضروری سطح آسیب پذیری سیستم را کاهش می‌دهد. RouterOS نیز دارای Package‌های مدیریتی و کاربردی پیش‌فرضی می‌باشد که غیرفعال نمودن آن‌ها از موارد توصیه شده می‌باشد.

نحوه پیاده‌سازی:

- با استفاده از دستور ذیل می‌توان Package‌های نصب شده و وضعیت آن‌ها را در RouterOS مشاهده نمود.

```
/system package print
```

- سپس با استفاده از دستور ذیل می‌توان Package‌های غیرضروری را غیرفعال نمود.

```
/system package disable MPLS
```

در مقابل عبارت Disable نام Package ای را که می خواهید غیرفعال گردد، قرار دهید.

SCRO-3-5: تغییر شماره پورت سرویس های کاربردی

شرح اجمالی:

بر اساس RFC 1700 هر سرویسی دارای شماره پورت ثبت شده می باشد و هر مهاجمی با انجام یک اسکن اولیه روی پورت های باز، به ماهیت سرویس آن پی خواهد برد. از این رو با تغییر شماره پورت یک سرویس، می توان امکان بهره برداری از آن سرویس را دشوارتر کرد.

نحوه پیاده سازی:

- با استفاده از دستور ذیل می توان شماره پورت مربوط به سرویس های RouterOS را مشاهده نمود.

```
/ip service print
```

- سپس با استفاده از دستور ذیل می توان شماره پورت مربوط به یک سرویس در RouterOS را تغییر داد.

```
/ip service set ssh port=1224
```

SCRO-3-6: اختصاص ACL جهت دسترسی به سرویس های کاربردی

شرح اجمالی:

ACL دسترسی به سرویس ها را کنترل می نماید. با استفاده از Access List دسترسی به سرویس های RouterOS تنها از تعداد مشخصی IP و یا Network قابل دسترسی خواهد بود. با کاهش تعداد IP هایی که توانایی دسترسی به RouterOS را دارند سطوح حمله را کاهش و امنیت RouterOS را افزایش می دهید. این ACL ها به ازای هر سرویس قابل تعریف می باشد. بدین ترتیب سطوح مدیریت را می توان به صورت توزیع شده پیکربندی نمود.

نحوه پیاده سازی:

با استفاده از دستور ذیل می توان آدرس مجاز را برای سرویس مورد نظر در RouterOS پیکربندی نمود.

```
/ip service set ssh address=192.168.130.0/24
```

SCRO-3-7: بلاک نمودن WinBox Discovery

شرح اجمالی:

یکی از سرویس‌های مشهور RouterOS جهت مدیریت آن WinBox می‌باشد. هر مهاجمی پس از استفاده از ابزارهای اسکن و مشاهده وجود این سرویس آن را به یکی از نقاط آسیب‌پذیر تبدیل می‌کند. در صورت نیاز به استفاده از این سرویس می‌توان قابلیت Discovery را غیرفعال نمود.

نحوه پیاده‌سازی:

- با استفاده از دستور ذیل می‌توان نسبت به غیرفعال نمودن WinBox Discovery در RouterOS اقدام نمود.

```
/tool mac-server  
add disabled=yes interface=all  
/tool mac-server ping  
set enabled=no
```

- در این مرحله در فایروال یک سری Rule جهت محدود نمودن دسترسی به سرویس WinBox و اجازه دسترسی از کامپیوتر ادمین به آن فراهم شده است.

```
/ip firewall filter  
add action=drop chain=input comment="block mikrotik discovery" disabled=no dst-port=5678  
protocol=udp  
add action=drop chain=input comment="ALL WINBOX REQUEST by MAC Address"  
disabled=no dst-port=20561 protocol=udp  
add action=drop chain=input comment="ALL WINBOX REQUEST EXCEPT FROM MY  
PC" disabled=no dst-port=8291 protocol=tcp src-address=!192.168.2.6
```

SCRO-3-8: غیرفعال نمودن Network Neighbor Discovery

شرح اجمالی:

سرویس Network Neighbor Discovery را می‌توان بعنوان سرویسی که در زمان Troubleshooting، اطلاعات مناسبی در اختیار مدیر سیستم قرار می‌دهد، به شمار آورد. فعال بودن همیشگی آن به معنای آن است که هر شنود کننده‌ای که در مجاورت آن قرار گیرد از اطلاعات آن بهره‌مند خواهد بود. این نوع نشت اطلاعات برای فرد

مهاجم بسیار سودمند خواهد بود. لذا توصیه می گردد پس از مرحله راه اندازی و تست Topology شبکه، نسبت به غیرفعال نمودن آن اقدام نمایید.

نحوه پیاده سازی:

با استفاده از دستور ذیل می توان نسبت به غیرفعال نمودن Network Neighbor Discovery در RouterOS اقدام نمود.

```
/ip neighbor discovery settings set default=no default-for-dynamic=no  
/ip neighbor discovery set [find] discover=no  
/ipv6 nd set [find] disabled=yes
```

SCRO-4: امن سازی حساب کاربری

SCRO-4-1: تغییر نام حساب کاربری admin پیش فرض سیستم

شرح اجمالی:

یکی از حملاتی که یک مهاجم جهت به دست آوردن کنترل یک سیستم به آن مبادرت می کند، حمله Brute Force Login می باشد. با در نظر گرفتن این نکته که در هر سیستمی یک نام کاربری پیش فرض مانند admin وجود دارد که اولین هدف برای این نوع حملات می باشد، لذا تغییر نام های پیش فرض همیشه توصیه می گردد.

نحوه پیاده سازی:

با استفاده از دستور ذیل می توان نام کاربر پیش فرض را در RouterOS تغییر داد.

```
/user set admin name=NewAdminName
```

SCRO-4-2: ایجاد رمز عبور پیچیده برای حساب های کاربری

شرح اجمالی:

در حملات Brute Force Login در صورت نبود رمز عبور پیچیده و طول کمتر از ۱۰ کاراکتر، به سادگی و در کمتر از چند دقیقه رمز عبور شکسته شده و مهاجم وارد سیستم می گردد. حال با ایجاد رمز عبور با حداقل ۱۲ کاراکتر و ترکیب کارکترهای عدد، حروف بزرگ و کوچک و کاراکترهای خاص می توان این زمان را به چند صد سال افزایش داد.

نحوه پیاده سازی:

با استفاده از دستور ذیل می توان رمز عبور کاربران را در RouterOS تغییر داد.

```
/user set admin password=#123xX&123"%
```

SCRO-4-3: اختصاص ACL جهت دسترسی به حساب های کاربری

شرح اجمالی:

ACL دسترسی به حساب های کاربری را کنترل می نماید. با استفاده از Access List می توان دسترسی به حساب های کاربری RouterOS تنها از تعداد مشخصی IP و یا Network محدود نمود. با کاهش تعداد IP هایی که توانایی دسترسی به RouterOS را دارند سطوح حمله را کاهش و امنیت RouterOS را افزایش می دهید. این ACL ها به ازای هر حساب کاربری قابل تعریف می باشد. بدین ترتیب سطوح مدیریت را می توان به صورت توزیع شده پیکربندی نمود.

نحوه پیاده سازی:

با استفاده از دستور ذیل می توان آدرس مجاز را برای حساب های کاربری مورد نظر در RouterOS پیکربندی نمود.

```
/user set VPNadmin address=192.168.130.0/24
```

Firewall: SCRO-5

SCRO-5-1: فعال سازی Firewall

شرح اجمالی:

در RouterOS می توان از ویژگی فیلتر نمودن Packet ها یا همان Firewall بهره برد. این قابلیت فیلتر نمودن از لایه ۲ تا لایه ۷ را دارا می باشد و با داشتن ویژگی های متعدد مانند Stateful Packet Inspection, Layer-7 protocol detection, traffic classification و ویژگی های کاربردی دیگر تقریباً تمام نیازهای امنیتی مربوط به این بخش را پوشش می دهد. لذا بکارگیری Firewall جزو توصیه های مهم در RouterOS می باشد.

نحوه پیاده سازی:

با استفاده از مجموعه دستورات IP Firewall می توان rule متناظر با ترافیک مجاز را در سیستم وارد نمود. مانند دستورات ذیل جهت محافظت RouterOS تنها از شبکه داخلی و اختصاص مجوز به پروتکل ICMP به تمامی Interface ها تا از هر نقطه ای بتوان آن را Ping نمود.

```
/ip firewall filter
add chain=input connection-state=invalid action=drop \
    comment="Drop Invalid connections"
add chain=input connection-state=established action=accept \
    comment="Allow Established connections"
add chain=input protocol=icmp action=accept \
    comment="Allow ICMP"
add chain=input src-address=192.168.0.0/24 action=accept \
    in-interface=! ether1
add chain=input action=drop comment="Drop everything else "
```

SCRO-5-2: غیر فعال سازی Service Port های غیر ضروری

شرح اجمالی:

در شبکه هایی که به وسیله RouterOS به صورت NAT پیاده سازی شده اند، هاست هایی که پشت NAT قرار دارند به صورت واقعی تمام ارتباطات end to end، NAT نمی شوند. از این رو برخی از سرویس ها و پروتکل ها برای اینکه از پشت NAT بتوانند کارایی خود را حفظ نمایند نیاز به یک NAT-helper دارند. این NAT-helper ها در RouterOS به عنوان Service Ports معرفی می گردند. توصیه می شود جهت کاهش سطح حملات، Service Port های غیر ضروری غیر فعال گردند.

نحوه پیاده سازی:

- ابتدا فهرستی از Service Port های فعال روی RouterOS را استخراج نمایید.

```
/ip firewall service-port print
```

- سپس هریک از Service Port هایی که غیر ضروری می باشد را با استفاده از دستور ذیل غیر فعال نمایید.

```
/ip firewall service-port disable sip
```

SCRO-5-3: استفاده از Reverse Path Filtering

شرح اجمالی:

این ویژگی هر Packet ای را که به نظر Spoof شده می باشد -مانند Packet ای که از یک شبکه با Subnet داخلی به سمت بیرون، ولی با یک Source IP مجزا از آن شبکه می آید- را Drop می نماید. این سناریو در مواردی که یک کامپیوتر دچار آلودگی بدافزاری شده باشد، پیش خواهد آمد و در انجام حملات DDoS نیز از این موضوع استفاده می شود.

نحوه پیاده سازی:

با استفاده از دستور ذیل می توان RF-filter را در RouterOS پیکربندی نمود.

```
/ip settings set rp-filter=strict
```

نکته: این پیکربندی در مواقعی که RouterOS به صورت Multi-Home پیکربندی شده باشد ایجاد اختلال می نماید.

SCRO-5-4: استفاده از Port Knocking

شرح اجمالی:

Port Knocking روشی برای اضافه نمودن IP ها به صورت پویا در قوانین و لیست آدرس های موجود در فایروال برای مدت محدودی از زمان می باشد. بدین وسیله پورت های مورد نیاز جهت یک کلاینت به صورت موقت در دسترسی آن کلاینت قرار داده می شود. لذا مهاجمین با استفاده از روش هایی مانند Port Scanning، نمی توانند از وجود این پورت های باز (در زمانی که درخواستی برای باز شدن آن نیست) باخبر شوند. بدین وسیله پورت ها و سرویس های آسیب پذیر از رصد مهاجمان در امان می مانند.

نحوه پیاده سازی:

- ابتدا شبکه های داخلی و ایمن را در RouterOS تعریف می نماییم.

```
/add address=192.168.30.0-192.168.30.254 comment="LAN Address" disabled=no list=\n"Safe Addresses"
```

- سپس Rule مربوط به Knock را اضافه می‌نماییم.

```
/add action=add-src-to-address-list address-list=knock-knock address-list-timeout=15s  
chain=input comment="Knock 1" disabled=no dst-port=1337 protocol=tcp  
/add action=add-src-to-address-list address-list="Safe Addresses" address-list-timeout=3h  
chain=input comment="Knock 2 - OK" disabled=no dst-port=17954 protocol=udp src-  
address-list= knock-knock
```

- تنها به "Safe Addresses" اجازه اتصال به RouterOS را می‌دهیم.

```
/add action=accept chain=input comment="Only Allow Access from Safe Addresses"  
disabled=no src-address-list="Safe Addresses"
```

- هر نوع ترافیک دیگری را Drop می‌نماییم.

```
/add action=drop chain=input comment="Drop Everything Else" disabled=no
```

- در سیستم client (CMD) با استفاده از Knock.exe دستور ذیل را اجرا نمایید تا درخواست برای باز شدن پورت به RouterOS ارسال گردد.

```
Knock.exe 192.168.1.1 1337:tcp 17954:udp
```

SCRO-5-5: استفاده از Firewall Scripts

شرح اجمالی:

در RouterOS می‌توان جهت جلوگیری از حملات شناخته شده از اسکریپت‌های آماده‌ای که قوانینی را در فایروال اضافه می‌نماید استفاده نمود. این اسکریپت‌ها به صورت دستوراتی می‌باشند که RouterOS، کلاپنت‌ها و سرویس‌های موجود را Harden می‌نماید. استفاده از این اسکریپت‌ها بسیار معمول بوده و پیشنهاد می‌گردد با توجه به سرویس‌های موجود از آن‌ها استفاده نمود.

نحوه پیاده‌سازی:

برخی از این اسکریپت‌ها به شرح ذیل می‌باشد که تنها به کپی نمودن در Terminal مربوط به RouterOS از آن‌ها می‌توان استفاده نمود.

- بلاک نمودن ICMP روی WAN Interface

```
/ Ip firewall filter
Add action=drop chain=input comment="Block ICMP on WAN interface" in-
interface=pppoe-out1 protocol=icmp
```

- اجازه استفاده از ICMP

```
/ Ip firewall filter
Add chain = icmp protocol = icmp icmp-options = 0: 0 action = accept \ comment = "echo
reply"
Add = icmp protocol = icmp icmp-options = 3: 0 action = accept \ comment = "net
unreachable"
Icmp-options = 3: 1 action = accept \ comment = "host unreachable"
Add chain = icmp protocol = icmp icmp-options = 4: 0 action = accept \ comment = "allow
source quench"
Add chain = icmp protocol = icmp icmp-options = 8: 0 action = accept \ comment = "allow
echo request"
Add chain = icmp protocol = icmp icmp-options = 11: 0 action = accept \ comment = "allow
time exceed"
Add chain = icmp protocol = icmp icmp-options = 12: 0 action = accept \ comment = "allow
parameter bad"
Add chain = icmp action = drop comment = "deny all other types"
```

- بلاک نمودن Login تصادفی در Brute Force (Random User / Password Login)

```
FTP login error 10 times per minute
/ Ip firewall filter
Add == protocol = tcp dst-port = 21 src-address-list = ftp_blacklist action = drop \ comment =
"drop ftp brute forcers"
Add chain = output action = accept protocol = tcp content = "530 Login incorrect" dst-limit =
1 / 1m, 9, dst-address / 1m
Add chain = output action = add-dst-to-address-list protocol = tcp content = "530 Login
incorrect" \ address-list = ftp_blacklist address-list-timeout = 3h
```

- جلوگیری از SSH Brute Force و بلاک نمودن برای ۱۰ روز بعد از تلاش مکرر

```
/ Ip firewall filter
Add chain = input protocol = tcp dst-port = 22 src-address-list = ssh_blacklist action = drop \
comment = "drop ssh brute forcers" disabled = no
Add chain = input protocol = tcp dst-port = 22 connection-state = new \ src-address-list =
ssh_stage3 action = add-src-to-address-list address-list = ssh_blacklist \ address-list-timeout =
10d comment = "" Disabled = no
Add chain = input protocol = tcp dst-port = 22 connection-state = new \ src-address-list =
ssh_stage2 action = add-src-to-address-list address-list = ssh_stage3 \ address-list-timeout =
```

```
1m comment = "" Disabled = no
Add chain = input protocol = tcp dst-port = 22 connection-state = new src-address-list =
ssh_stage1 action = add-src-to-address-list address-list = ssh_stage2 address-list-timeout = 1m
comment = "" Disabled = no
Add chain = input protocol = tcp dst-port = 22 connection-state = new action = add-src-to-
address-list \ address-list = ssh_stage1 address-list-timeout = 1m comment = "" disabled = no
Add chain = forward protocol = tcp dst-port = 22 src-address-list = ssh_blacklist action = drop
\ comment = "drop ssh brute downstream" disabled = no
```

• Drop نمودن ترافیک Port Scan

```
/ Ip firewall filter
3,1 action = add-src-to-address-list address-list = "port scanners" address-list-timeout = 2w
comment = "Port scanners to list" Disabled = no
Add chain = input protocol = tcp tcp-flags = fin, syn,! Rst! Psh! Ack! Urg action = add-src-to-
address-list address-list = Timeout = 2w comment = "NMAP FIN Stealth scan"
Syn action = add-src-to-address-list address-list = "port scanners" address-list-timeout = 2w
comment = "SYN / FIN scan"
Add chain = input protocol = tcp tcp-flags = syn, rst action = add-src-to-address-list address-
list = "port scanners" address-list-timeout = 2w comment = "SYN / RST scan"
Add-src-to-address-list address-list = "port scanners" address-list-timeout = 2w comment =
"FIN / PSH / URG scan"
Synch, rst, psh, ack, urg action = add-src-to-address-list address-list = "port scanners" address-
list-timeout = 2w comment = "ALL / ALL scan"
Add chain = input protocol = tcp tcp-flags =! Fin! Syn! Rst! Psh! Ack!! Urg action = add-src-
to-address-list address-list = "port scanners" address-list -timeout = 2w comment = "NMAP
NULL scan"
```

```
/ Ip firewall filter
Add chain = input src-address-list = "port scanners" action = drop comment = "dropping port
scanners" disabled = no
Add chain = forward src-address-list = "port scanners" action = drop comment = "dropping
port scanners" disabled = no
```

• محافظت از کاربران (Forward Chain - Traffic Passing Through the Router)

```
/ Ip firewall filter
Add chain = forward connection-state = invalid \ action = drop comment = "drop invalid
connections"
Add chain = forward connection-state = established action = accept \ comment = "allow
already established connections"
```

```
Add chain = forward connection-state = related action = accept \ comment = "allow connected connections"
```

• بلاک نمودن Bogon IP Addresses

```
/ Ip firewall filter
Add chain = forward src-address = 0.0.0.0 / 8 action = drop \ comment = "Block Bogon IP addresses"
Add chain = forward dst-address = 0.0.0.0 / 8 action = drop
Add chain = forward src-address = 127.0.0.0 / 8 action = drop
Add chain = forward dst-address = 127.0.0.0 / 8 action = drop
Add chain = forward src-address = 224.0.0.0 / 3 action = drop
Add chain = forward dst-address = 224.0.0.0 / 3 action = drop
```

• جهش نمودن به Chain های جدید

```
/ Ip firewall filter
Add chain = forward protocol = tcp action = jump jump-target = tcp \ comment = "Make jumps to new chains"
Add chain = forward protocol = udp action = jump jump-target = udp
Add chain = forward protocol = icmp action = jump jump-target = icmp
```

• ایجاد یک TCP Chain و جلوگیری از برخی پورت های TCP آسیب پذیر (بر حسب نیاز پورت ها را تغییر دهید)

```
/ Ip firewall filter
Add chain = tcp protocol = tcp dst-port = 69 action = drop \ comment = "TFTP deny"
Add = tcp protocol = tcp dst-port = 111 action = drop \ comment = "deny RPC portmapper"
Add = tcp protocol = tcp dst-port = 135 action = drop \ comment = "deny RPC portmapper"
Add chain = tcp protocol = tcp dst-port = 137-139 action = drop \ comment = "deny NBT"
Add chain = tcp protocol = tcp dst-port = 445 action = drop \ comment = "deny cifs"
Add chain = tcp protocol = tcp dst-port = 2049 action = drop comment = "dfs NFS"
Add chain = tcp protocol = tcp dst-port = 12345-12346 action = drop comment = "NetBus deny"
Add chain = tcp protocol = tcp dst-port = 20034 action = drop comment = "deny NetBus"
Add chain = tcp protocol = tcp dst-port = 3133 action = drop comment = "deny BackOrifice"
Add chain = tcp protocol = tcp dst-port = 67-68 action = drop comment = "DHCP deny"
```

• ایجاد یک UDP Chain و جلوگیری از برخی پورت های UDP آسیب پذیر (بر حسب نیاز پورت ها را تغییر دهید)

```
#Create UDP chain and deny some UDP ports in it (revise port numbers as needed).
/ Ip firewall filter
Add chain = udp protocol = udp dst-port = 69 action = drop comment = "TFTP deny"
Add chain = udp protocol = udp dst-port = 111 action = drop comment = "deny PRC
portmapper"
Add chain = udp protocol = udp dst-port = 135 action = drop comment = "deny PRC
portmapper"
Add chain = udp protocol = udp dst-port = 137-139 action = drop comment = "deny NBT"
Add chain = udp protocol = udp dst-port = 2049 action = drop comment = "deny NFS"
Add chain = udp protocol = udp dst-port = 3133 action = drop comment = "deny
BackOriffice"
```

- بلاک نمودن پورت‌های مورد استفاده برخی از ویروس‌ها

```
/ Ip firewall filter
add action=drop chain=virus comment="Blaster Worm" dst-port=135-139 protocol=tcp
add action=drop chain=virus comment="Blaster Worm" dst-port=445 protocol=tcp
add action=drop chain=virus comment="Messenger Worm" dst-port=135-139 protocol=udp
add action=drop chain=virus comment="Blaster Worm" dst-port=445 protocol=udp
add action=drop chain=virus comment=_____ dst-port=593 protocol=tcp
add action=drop chain=virus comment=_____ dst-port=1024-1030 protocol=tcp
add action=drop chain=virus comment=MyDoom dst-port=1080 protocol=tcp
add action=drop chain=virus comment=_____ dst-port=1214 protocol=tcp
add action=drop chain=virus comment="ndm requester" dst-port=1363 protocol=tcp
add action=drop chain=virus comment="ndm server" dst-port=1364 protocol=tcp
add action=drop chain=virus comment="screen cast" dst-port=1368 protocol=tcp
add action=drop chain=virus comment=hromgrafx dst-port=1373 protocol=tcp
add action=drop chain=virus comment=cichlid dst-port=1377 protocol=tcp
add action=drop chain=virus comment="Bagle Virus" dst-port=2745 protocol=tcp
add action=drop chain=virus comment=Dumaru.Y dst-port=2283 protocol=tcp
add action=drop chain=virus comment=Beagle dst-port=2535 protocol=tcp
add action=drop chain=virus comment=Beagle.C-K dst-port=2745 protocol=tcp
add action=drop chain=virus comment=MyDoom dst-port=3127-3128 protocol=tcp
add action=drop chain=virus comment="Backdoor OptixPro" dst-port=3410 protocol=tcp
add action=drop chain=virus comment=Sasser dst-port=5554 protocol=tcp
add action=drop chain=virus comment=Beagle.B dst-port=8866 protocol=tcp
add action=drop chain=virus comment=Dabber.A-B dst-port=9898 protocol=tcp
add action=drop chain=virus comment=Dumaru.Y dst-port=10000 protocol=tcp
add action=drop chain=virus comment=MyDoom.B dst-port=10080 protocol=tcp
add action=drop chain=virus comment=NetBus dst-port=12345 protocol=tcp
add action=drop chain=virus comment=Kuang2 dst-port=17300 protocol=tcp
add action=drop chain=virus comment=SubSeven dst-port=27374 protocol=tcp
```



```
add action=drop chain=virus comment="PhatBot, Agobot, Gaobot" dst-port=65506
protocol=tcp
add action=jump chain=forward comment="jump to the virus chain" jump-target=virus
add chain=input comment="Accept established connections" connection-state=established
add chain=input comment="Accept related connections" connection-state=related
add action=drop chain=input comment="invalid connections" connection-state=invalid
add chain=input comment=UDP protocol=udp
add action=drop chain=forward comment="invalid connections" connection-state=invalid
```

- بلاک نمودن درخواست DNS از WAN Interface

```
/ Ip firewall filter
add action=drop chain=input comment="BLOCK DNS REQUEST ON WAN INTERFACE"
dst-port=53 in-interface=pppoe-out1 protocol=udp
```

- بلاک نمودن ترافیک P2P / Torrent

```
/ip firewall mangle
add action=mark-packet chain=postrouting comment="p2p download" disabled=no layer7-
protocol=p2p_www new-packet-mark="p2p download" passthrough=no
add action=mark-packet chain=postrouting disabled=no layer7-protocol=p2p_dns new-packet-
mark="p2p download" passthrough=no
```

```
/ip firewall filter
add action=drop chain=forward comment="Block P2p_www Packets / Zaib" disabled=no
layer7-protocol=p2p_www
add action=drop chain=forward comment="Block P2p_dns Packets / Zaib" disabled=no
layer7-protocol=p2p_dns
add action=drop chain=forward comment="Block General P2P Connections , default mikrotik
p2p colelction / zaib" disabled=no p2p=all-p2p
```

SCRO-5-6: بستن دسترسی از کشورهای غیر ضروری

شرح اجمالی:

طبق اصل "حداقل دسترسی"، اکیدا توصیه می شود تنها دسترسی از مبدا کشورهای که ترافیک مجاز باید از آنها رخ دهد وجود داشته باشد. برحسب مشاهدات رویدادهای یک فایروال و یا مسیریاب که در لبه یک شبکه قرار دارد، بیشترین حملات از مبدا کشورهای می باشد که هیچ نوع توجیه برای باز بودن دسترسی برای آنها

نیست و بسیاری از این کشورهای در Blacklist های مربوط به Spammer دیده می شوند. از این رو بستن دسترسی از اینگونه کشورها از لحاظ امنیت بسیار مهم می باشد.

نحوه پیاده سازی:

در این مثال ما تنها دسترسی از IP های ایران را به RouterOS باز می نماییم. حال با در نظر گرفتن نوع روابط کاری می توان این دسترسی را به سایر کشورها بسط داد.

- ابتدا لیست IP های مربوط به کشور مورد نظر را به صورت فایل دانلود می نماییم.

```
/tool fetch url=http://www.iwik.org/ipcountry/mikrotik/IR
```

- سپس فایل را به صورت یک Address-List در فایروال اضافه می نماییم.

```
/import file-name=IR
```

- سپس یک Firewall Rule جهت مجاز نمودن ترافیک تنها در RouterOS اضافه می نماییم.

```
/ip firewall  
add action=drop chain=input in-interface=ether1 log=yes src-address-list=!IR
```

نکته: این Rule باید در اولویت بالایی قرار گیرد تا Rule های دسترسی پایین تر را تحت الشعاع قرار دهد.

Log :SCRO-6

شرح اجمالی:

با بررسی رویدادهای RouterOS می توان از وقوع حملات و مشکلات احتمالی در ساختار شبکه و یا حتی مشکلات ناشی از سخت افزار و نرم افزار مطلع شد. این ویژگی حتی منجر به توسعه محصولاتی جهت پالایش رویدادهای مختلف مانند SIEM شده است.

نگهداری رویدادها به صورت پیش فرض در حافظه داخلی RouterOS می باشد. لذا استخراج مناسب وقایع و ارسال آنها به یک Syslog بسیار مهم می باشد.

نحوه پیاده سازی:

ابتدا باید شرایطی برای ایجاد Log در بخش هایی از RouterOS در آن ها Action وجود دارد، مانند فایروال، مهیا گردد. از این رو به طور مثال در هر قانون ایجاد شده در فایروال گزینه مربوط به Log را فعال می نماییم و یا یک قانون کلی برای Log نمودن تمامی پکت های ورودی و خروجی به RouterOS ایجاد نماییم.

```
/add chain=forward action=log disabled=no
```

سپس یک Action جهت ارسال logs به syslog سرور تعریف می نماییم.

```
/system logging action add name=syslog-serve target=remote remote=192.168.10.10 remote-port=514 src-address=192.168.10.1
```

و در نهایت در RouterOS لاگ های مربوطه، به طور مثال لاگ های مربوط به فایروال، جهت ارسال به Syslog Server تعریف می نماییم.

```
/system logging add topic=firewall action=syslogserver
```

NTP :SCRO-7

شرح اجمالی:

یکی از سرویس های حیاتی زیرساختی، NTP می باشد که با همزمانی سخت افزارها و نرم افزارهای مختلف، مدیریت و مشاهده رویدادها را کاراتر می نماید. در صورت همزمان نبودن RouterOS و در صورت وقوع یک حمله نمی توان رویداد ثبت شده را به درستی ردیابی و تفسیر نمود. همچنین اگر از بازه های زمانی در قانون فایروال استفاده شده باشد در صورت همزمان نبودن RouterOS عملاً کارایی آن قانون به مخاطره خواهد افتاد.

نحوه پیاده سازی:

- ابتدا باید منطقه زمانی صحیح را مشخص نماییم.

```
/system clock set time-zone=+3:30
```

- سپس تنظیمات NTP Client را انجام می دهیم.

```
/system ntp client set enabled=yes primary-ntp=192.168.0.2 secondary-ntp=192.168.0.3 mode=unicast
```

SNMP:SCRO-8

شرح اجمالی:

SNMP سرویس مدیریتی/مشاهده‌ای می‌باشد که جزو ابزارهای قدرتمند یک مدیر شبکه برای دستیابی به پیکربندی و رویدادهای RouterOS می‌باشد. به مانند سایر تجهیزات Active شبکه، RouterOS نیز از SNMP نسخه ۳ جهت افزایش امنیت پشتیبانی می‌کند. این سرویس به صورت پیش فرض غیرفعال می‌باشد و با توجه به پشتیبانی آن از متدهای امنیتی مانند priv جهت مدل امنیتی، SHA1 جهت پروتکل احراز هویت و AES جهت رمزنگاری در SNMP نسخه ۳، می‌توان از نهایت امنیت پیش‌بینی شده برای این سرویس بهره برد. از نسخه 6.18، پشتیبانی از OID blacklisting به RouterOS افزوده شده است.

نحوه پیاده‌سازی:

ابتدا یک Community با پیکربندی امن را جایگزین Community پیش فرض در RouterOS تعریف می‌نماییم. در صورتی که می‌خواهید امکان مدیریت نیز از طریق SNMP فراهم شود ویژگی Write Access را نیز برای آن فعال نمایید.

```
/snmp community set [ find default=yes ] name=snmpv3user security=private authentication-  
password=snmpv3authPass authentication-protocol=SHA1 encryption-  
password=snmpv3encPass encryption-protocol=AES read-access=yes write-access=no  
addresses=10.0.0.0/24
```

سپس سرویس SNMP را با Community تنظیم شده پیکربندی می‌نماییم.

```
/snmp set enabled=yes location="The Management" contact=mng@example.com trap-  
community=snmpv3user trap-version=3 trap-interfaces=ether1
```

پیوست

در این بخش چک لیستی به منظور ممیزی محصول مورد نظر ارائه شده است. چک لیست شامل سه جدول است. جدول اول، جدول ممیز می باشد. در این جدول، اطلاعات مربوط به شخصی که پیکربندی امن را انجام می دهد یا آن را ممیزی می کند، وارد می شود. همچنین نتایج پیکربندی یا ممیزی به صورت اختصار در این جدول درج می گردد. جدول دوم، محل وارد کردن مشخصات سروری است که MikroTik RouterOS روی آن نصب شده است. جدول سوم، جدول تنظیماتی است که باید بررسی یا اعمال شوند. در صورت صحت اعمال تنظیم در هر ردیف، ستون وضعیت مربوط به آن با علامت ✓ نمایش داده خواهد شد.

ممیز		
نام: ایمیل: تلفن:	تاریخ:	
توضیحات	تعداد	تنظیمات
		تطابق
		عدم تطابق
		تنظیمات حذف شده
		تنظیمات اضافه شده
		مجموع تنظیمات اعمال شده

مشخصات سرور	
	آدرس MAC
	آدرس IP
	نام ماشین
	شماره اموال
نام: ایمیل: تلفن:	مدیر سیستم
	تاریخ

جدول ممیزی

جدول ممیزی خلاصه ای از تمامی الزامات بیان شده در متن سند می باشد. قابل ذکر است که ستون های "وضعیت" و "قابلیت پیاده سازی" باید توسط ممیز و برای هر سیستم حاوی این برنامه تکمیل گردد. در ستون وضعیت، ممیز باید از عبارات های "قبول" و "رد" متناسب با وضعیت الزام در محصول مورد ارزیابی استفاده نماید. در ستون قابلیت پیاده سازی، ممیز باید قابلیت پیاده سازی الزام برای محصول مورد ارزیابی را با عبارات "دارد" و "ندارد" بیان نماید. در صورتی که الزامی برای محصول مذکور قابلیت پیاده سازی نداشته باشد، علت عدم قابلیت پیاده سازی آن باید در ذیل جدول توضیح داده شود.

شناسه	وضعیت	تنظیمات	قابلیت پیاده سازی تنظیمات	مقدار پیش فرض	مقدار مطلوب
SCRO-1		به روز رسانی			
SCRO-1		به روز رسانی Package های RouterOS	دارد	ندارد	مطابق نحوه پیاده سازی اجرا گردد.
SCRO-2		امن سازی پورت های فیزیکی			
SCOS-2-1		غیر فعال نمودن Interface های بلا استفاده	دارد	فعال	غیر فعال
SCOS-2-2		غیر فعال نمودن پورت کنسول	دارد	فعال	غیر فعال
SCRO-3		امن سازی سرویس ها			
SCRO-3-1		غیر فعال سازی سرویس های غیر ضروری	دارد	فعال	غیر فعال
SCRO-3-2		استفاده از سرویس HTTPS بجای HTTP	دارد	HTTP	HTTPS

فعال	فعال	دارد	استفاده از الگوریتم های رمزنگاری قدرتمندتر در SSH		SCRO-3-3
فعال	غیرفعال	دارد	غیرفعال نمودن Package های غیرضروری		SCRO-3-4
تغییر شماره پورت	به ازای هر پورت متفاوت می باشد.	دارد	تغییر شماره پورت سرویس های کاربردی		SCRO-3-5
کاهش IP هایی که دسترسی به RouterOS را دارند.	ندارد	دارد	اختصاص ACL جهت دسترسی به سرویس های کاربردی		SCRO-3-6
غیرفعال	فعال	دارد	بلاک نمودن WinBox Discovery		SCRO-3-7
غیرفعال	فعال	دارد	غیرفعال نمودن Network Neighbor Discovery		SCRO-3-8
			امن سازی حساب کاربری		SCRO-4
تغییر نام کاربر admin	admin	دارد	تغییر نام حساب کاربری admin پیش فرض سیستم		SCRO-4-1
حداقل ۱۲ کاراکتر	ندارد	دارد	ایجاد رمز عبور پیچیده برای حساب های کاربری		SCRO-4-2
کاهش IP هایی که دسترسی به RouterOS را دارند.	ندارد	دارد	اختصاص ACL جهت دسترسی به حساب های کاربری		SCRO-4-3
			Firewall		SCRO-5
مطابق نحوه پیاده سازی اجرا گردد.	ندارد	دارد	فعال سازی Firewall		SCRO-5-1

مطابق نحوه پیاده سازی اجرا گردد.	فعال	دارد	غیرفعال سازی Service Port های غیر ضروری	SCRO-5-2
مطابق نحوه پیاده سازی اجرا گردد.	ندارد	دارد	استفاده از Reverse Path Filtering	SCRO-5-3
مطابق نحوه پیاده سازی اجرا گردد.	ندارد	دارد	استفاده از Port Knocking	SCRO-5-4
مطابق نحوه پیاده سازی اجرا گردد.	ندارد	دارد	استفاده از Firewall Scripts	SCRO-5-5
مطابق نحوه پیاده سازی اجرا گردد.	ندارد	دارد	بستن دسترسی از کشورهای غیر ضروری	SCRO-5-6
مطابق نحوه پیاده سازی اجرا گردد.	ندارد	دارد	Log	SCRO-6
مطابق نحوه پیاده سازی اجرا گردد.	ندارد	دارد	NTP	SCRO-7
مطابق نحوه پیاده سازی اجرا گردد.	ندارد	دارد	SNMP	SCRO-8