پیکربندی امن

MikroTik RouterOS

مرکز مدیریت راهبردی افتا

SCRO-MIKROTIK-ROUTEROS -0.0

اسفند ۹۵

فهرست

پیش‌گفتار

مرکز مدیریت راهبردی افتا[1] به منظور ساماندهی امنیت تجهیزات در حوزه فاوا[2]، 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 چک لیست‌های 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[3]، الزامات دیگری را نیز به این تنظیمات اضافه و مستند نمایند.

[1] امنیت فضای تولید و تبادل اطلاعات
[2] فناوری اطلاعات و ارتباطات
[3] 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: گروه‌بندی و اختصارسازی نام برای محصولات IT

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

[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	
نام گروه	شماره گروه
سرویس‌دهنده ایمیل[۱۵]	MS
راهکارهای موبایلی[۱۶]	MO
مسیریاب شبکه[۱۷]	RO
سوئیچ شبکه	SW
سیستم عامل	OS
تجهیزات جانبی[۱۸]	PD
سرویس دهنده[۱۹]	SR
نرم‌افزار مجازی‌سازی[۲۰]	VI
مرورگر وب	WB
سرویس‌دهنده وب	WS

[۱۵] Mail Server
[۱۶] Mobile Solution
[۱۷] Network Router
[۱۸] Peripheral Device
[۱۹] Server
[۲۰] Virtualization Software

تنظیمات

SCRO-1: به‌روزرسانی Packageهای RouterOS

شرح اجمالی:

از نسخه ۵,۲۱ به بعد RouterOS، ویژگی Automatic Upgrade اضافه شده است. این ویژگی امکان نصب آخرین بروزرسانی‌های RouterOS را برای Packageهای نصب شده روی سیستم را فراهم می‌آورد. با انجام بروزرسانی Packageها از آسیب پذیری‌های احتمالی بر روی هر یک از آن‌ها می‌توان جلوگیری نمود.

نحوه پیاده‌سازی:

جهت بروزرسانی محصولات میکروتیک روش ذیل توصیه می‌گردد:

- به صورت پیش‌فرض RouterOS به سایت اصلی میکروتیک مراجعه و نسبت به دانلود بسته‌های بروزرسانی اقدام می‌کند. 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 بروزرسانی بسته‌های RouterOS نمایید.
- می‌توان 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: امن‌سازی پورت‌های فیزیکی

SCRO-2-1: غیرفعال نمودن واسط‌های 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 واسط‌های موجود استفاده کند که در این صورت ترافیک Live از بین می‌رود و سیستم Log و SIEM متوجه واقعه خواهند شد.

نحوه پیاده‌سازی:

- ابتدا فهرست تمام واسط‌ها را استخراج نمایید.

```
/interface print
```

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

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

SCRO-2-2: غیرفعال نمودن پورت کنسول

شرح اجمالی:

درصورت قرارگیری RouterOS در محیط‌های ناامن، فرد مهاجم با اتصال پورت کنسول می‌تواند هر نوع دسترسی را برای خود فراهم نماید. از این رو ایجاد راهکاری جهت مدیریت محدود در سیستم اکیدا توصیه می‌گردد.

نحوه پیاده‌سازی:

- با استفاده از دستور ذیل می‌توان 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: امن‌سازی سرویس‌ها

SCRO-3-1: غیرفعال سازی سرویس‌های غیر ضروری

شرح اجمالی:

هر سرویس موجود می‌تواند یک هدف بالقوه جهت حمله یک مهاجم باشد. از این رو غیرفعال سازی سرویس‌های غیر ضروری سطح آسیب‌پذیری سیستم را کاهش می‌دهد. RouterOS نیز دارای سرویس‌های مدیریتی و کاربردی پیش‌فرضی می‌باشد که برخی از آن‌ها همانند Telnet و http به صورت ذاتی دچار آسیب می‌باشند.

نحوه پیاده‌سازی:

- ابتدا فهرست تمام سرویس‌ها را استخراج نمایید.

```
/ip service print
```

- سپس اقدام به غیرفعال 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 غیرفعال 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 غیرفعال 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 می‌گردد 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 می‌باشد.

نحوه پیاده‌سازی:

- 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
```

- Certificateهای 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 می‌خواهید غیرفعال گردد، قرار دهید.

SCRO-3-5: تغییر شماره پورت سرویس‌های کاربردی

شرح اجمالی:

بر اساس RFC 1700 هر سرویسی دارای شماره پورت ثبت شده می‌باشد و هر مهاجمی با انجام یک اسکن اولیه روی پورت‌های باز، به ماهیت سرویس آن پی خواهد برد. از این رو با تغییر شماره پورت یک سرویس، می‌توان امکان بهره‌برداری از آن سرویس را دشوارتر کرد.

نحوه پیاده‌سازی:

- با استفاده از دستور ذیل می‌توان شماره پورت مربوط به سرویس‌های RouterOS را مشاهده نمود.

```
/ip service print
```

- سپس با استفاده از دستور ذیل می‌توان 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 سرویس‌های کاربردی

شرح اجمالی:

ACL دسترسی به سرویس‌ها را کنترل می‌نماید. با استفاده از Access List دسترسی به سرویس‌های RouterOS تنها از تعداد مشخصی IP و یا Network قابل دسترس خواهد بود. با کاهش تعداد IPهایی که توانایی دسترسی به RouterOS را دارند سطوح حمله را کاهش و امنیت RouterOS را افزایش می‌دهید. این ACLها به ازای هر سرویس قابل تعریف می‌باشد. بدین ترتیب سطوح مدیریت را می‌توان به صورت توزیع شده پیکربندی نمود.

نحوه پیاده‌سازی:

با استفاده از دستور ذیل می‌توان 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 می‌گردد پس از مرحله راه‌اندازی و تست Topology شبکه، نسبت به غیرفعال نمودن آن اقدام نمایید.

نحوه پیاده‌سازی:

با استفاده از دستور ذیل می‌توان 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: امن‌سازی حساب کاربری

SCRO-4-1: تغییر نام حساب کاربری admin پیش‌فرض سیستم

شرح اجمالی:

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

نحوه پیاده‌سازی:

با استفاده از دستور ذیل می‌توان نام کاربر پیش‌فرض را در RouterOS تغییر داد.

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

SCRO-4-2: ایجاد رمزعبور پیچیده برای حساب‌های کاربری

شرح اجمالی:

در حملات Brute Force Login درصورت 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 می‌گردد. حال با ایجاد رمز عبور با حداقل ۱۲ کاراکتر و ترکیب کارکترهای عدد، حروف بزرگ و کوچک و کاراکترهای خاص می‌توان این زمان را به چند صد سال افزایش داد.

نحوه پیاده‌سازی:

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

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

SCRO-4-3: اختصاص ACL جهت دسترسی به حساب‌های کاربری

شرح اجمالی:

ACL دسترسی به حساب‌های کاربری را کنترل می‌نماید. با استفاده از Access List می‌توان دسترسی به حساب‌های کاربری RouterOS تنها از تعداد مشخصی IP و یا Network محدود نمود. با کاهش تعداد IPهایی که توانایی دسترسی به RouterOS را دارند سطوح حمله را کاهش و امنیت RouterOS را افزایش می‌دهید. این ACLها به ازای هر حساب کاربری قابل تعریف می‌باشد. بدین ترتیب سطوح مدیریت را می‌توان به صورت توزیع شده پیکربندی نمود.

نحوه پیاده‌سازی:

با استفاده از دستور ذیل می‌توان آدرس مجاز را برای حساب‌های 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 می‌توان از ویژگی فیلتر نمودن Packetها یا همان Firewall بهره برد. این Firewall قابلیت فیلتر نمودن از لایه ۲ تا لایه ۷ را دارا می‌باشد و با داشتن ویژگی‌های متعدد مانند Stateful Packet Inspection، Layer-7 protocol detection، traffic classification و ویژگی‌های کاربردی دیگر تقریبا تمام نیازهای امنیتی مربوط به این بخش را پوشش می‌دهد. لذا بکارگیری Firewall جزو توصیه‌های مهم در RouterOS می‌باشد.

نحوه پیاده‌سازی:

با استفاده از مجموعه دستورات IP Firewall می‌توان 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 Interfaceها تا از هر نقطه‌ای 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: غیرفعال سازی Service Portهای غیرضروری

شرح اجمالی:

در شبکه‌هایی که به وسیله RouterOS به صورت NAT پیاده‌سازی شده‌اند، هاست‌هایی که پشت NAT قرار دارند به صورت واقعی تمام ارتباطات end to end، NAT نمی‌شوند. از این رو برخی از سرویس‌ها و پروتکل‌ها برای اینکه از پشت NAT بتوانند کارایی خود را حفظ نمایند نیاز به یک NAT-helper دارند. این NAT-helperها در RouterOS به عنوان Service Ports معرفی می‌گردند. توصیه می‌شود جهت کاهش سطح حملات، Service Portهای غیرضروری غیرفعال گردند.

نحوه پیاده‌سازی:

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

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

- سپس هریک از Service Portهایی که غیرضروری می‌باشد را با استفاده از دستور ذیل غیرفعال 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 می‌باشد -مانند Packet ای که از یک شبکه با Subnet داخلی به سمت بیرون، ولی با یک Source IP مجزا از آن شبکه می‌آید- را Drop می‌نماید. 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 می‌شود.

نحوه پیاده‌سازی:

با استفاده از دستور ذیل می‌توان 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 می‌نماید.

SCRO-5-4: استفاده از Port Knocking

شرح اجمالی:

Port Knocking روشی برای اضافه نمودن IPها به صورت پویا در قوانین و لیست آدرس‌های موجود در فایروال برای مدت محدودی از زمان می‌باشد. بدین وسیله پورت‌های مورد نیاز جهت یک کلاینت به صورت موقت در دسترسی آن کلاینت قرار داده می‌شود. لذا مهاجمین با استفاده از روش‌هایی مانند Port Scanning، نمی‌توانند از وجود این پورت‌های باز (در زمانی که درخواستی برای باز شدن آن نیست) باخبر شوند. بدین وسیله پورت‌ها و سرویس‌های آسیب‌پذیر از رصد مهاجمان در امان می‌مانند.

نحوه پیاده‌سازی:

- ابتدا شبکه‌های داخلی و ایمن را در RouterOS تعریف می‌نماییم.

```
/add address=192.168.30.0-192.168.30.254 comment="LAN Address" disabled=no list=\
"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، کلاینت‌ها 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 Chainهای 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 پورت‌های TCP آسیب‌پذیر (بر حسب نیاز پورت‌ها 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 BackOriffice"
Add chain = tcp protocol = tcp dst-port = 67-68 action = drop comment = "DHCP deny"
```

- ایجاد یک UDP Chain و جلوگیری از برخی پورت‌های UDP آسیب‌پذیر (بر حسب نیاز پورت‌ها 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 Torrent / P2P

```
/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 غیرضروری

شرح اجمالی:

طبق اصل "حداقل دسترسی"، اکیدا توصیه می‌شود تنها دسترسی از مبدا کشورهایی 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 کشورهایی می‌باشد که هیچ نوع توجیه برای باز بودن دسترسی برای آن‌ها

نیست و بسیاری از این کشورهای در Blacklistهای مربوط به Spammer دیده می‌شوند. از این رو بستن دسترسی از اینگونه کشورها از لحاظ امنیت بسیار مهم می‌باشد.

نحوه پیاده‌سازی:

در این مثال ما تنها دسترسی از IPهای ایران را به RouterOS باز می‌نماییم. حال با درنظر گرفتن نوع روابط کاری می‌توان این دسترسی را به سایر کشورها بسط داد.

- ابتدا لیست IPهای مربوط به کشور مورد نظر را به صورت فایل دانلود می‌نماییم.

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

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

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

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

```
/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 Ruleهای دسترسی پایین‌تر را تحت الشعاع قرار دهد.

SCRO-6: Log

شرح اجمالی:

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

نگهداری رویدادها به صورت پیش‌فرض در حافظه داخلی RouterOS می‌باشد. لذا استخراج مناسب وقایع و ارسال آن‌ها به یک Syslog بسیار مهم می‌باشد.

نحوه پیاده‌سازی:

ابتدا باید شرایطی برای ایجاد Log در بخش‌هایی از RouterOS در آن‌ها 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 می‌نماییم و یا یک قانون کلی برای Log نمودن تمامی پکت‌های ورودی و خروجی به RouterOS ایجاد نمایید.

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

سپس یک Action جهت ارسال logs به syslog سرور تعریف می‌نماییم.

```
/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 لاگ‌های مربوطه، به طور مثال لاگ‌های مربوط به فایروال، جهت ارسال به Syslog Server تعریف می‌نماییم.

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

NTP :SCRO-7

شرح اجمالی:

یکی از سرویس‌های حیاتی زیرساختی، NTP می‌باشد که با همزمانی سخت‌افزارها و نرم‌افزارهای مختلف، مدیریت و مشاهده رویدادها را کاراتر می‌نماید. در صورت همزمان نبودن RouterOS و درصورت وقوع یک حمله نمی‌توان رویداد ثبت شده را به درستی ردیابی و تفسیر نمود. همچنین اگر از بازه‌های زمانی در قانون فایروال استفاده شده باشد در صورت همزمان نبودن RouterOS عملا کارایی آن قانون به مخاطره خواهد افتاد.

نحوه پیاده‌سازی:

- ابتدا باید منطقه زمانی صحیح را مشخص نمایید.

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

- سپس تنظیمات NTP Client را انجام می‌دهیم.

```
/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 پیش‌فرض 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 پیش‌فرض در RouterOS تعریف می‌نماییم. درصورتی 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 می‌باشد. در این جدول، اطلاعات مربوط به شخصی که پیکربندی امن را انجام می‌دهد یا آن را ممیزی می‌کند، وارد می‌شود. همچنین نتایج پیکربندی یا ممیزی به صورت اختصار در این جدول درج می‌گردد. 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	
ممیز: نام: ---------- ایمیل: ---------- تلفن: ----------	**تاریخ:**

تنظیمات	**تعداد**	**توضیحات**
تطابق		
عدم تطابق		
تنظیمات حذف شده		
تنظیمات اضافه شده		
مجموع تنظیمات اعمال شده		

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

جدول ممیزی

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

شناسه	وضعیت	تنظیمات	قابلیت پیاده‌سازی تنظیمات	مقدار پیش‌فرض	مقدار مطلوب
SCRO-1		به‌روزرسانی			
SCRO-1		به‌روزرسانی Packageهای RouterOS	دارد	ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.
SCRO-2		امن سازی پورت‌های فیزیکی			
SCOS-2-1		غیرفعال نمودن Interfaceهای بلا استفاده	دارد	فعال	غیرفعال
SCOS-2-2		غیرفعال نمودن پورت کنسول	دارد	فعال	غیرفعال
SCRO-3		امن سازی سرویس‌ها			
SCRO-3-1		غیرفعال سازی سرویس‌های غیر ضروری	دارد	فعال	غیرفعال
SCRO-3-2		استفاده از سرویس HTTPS بجای HTTP	دارد	HTTP	HTTPS

SCRO-3-3		استفاده از الگوریتم‌های رمزنگاری قدرتمندتر در SSH	دارد	فعال	فعال
SCRO-3-4		غیرفعال نمودن Packageهای غیرضروری	دارد	غیرفعال	فعال
SCRO-3-5		تغییر شماره پورت سرویس‌های کاربردی	دارد	به ازای هر پورت متفاوت می‌باشد.	تغییر شماره پورت
SCRO-3-6		اختصاص ACL جهت دسترسی به سرویس‌های کاربردی	دارد	ندارد	کاهش IPهایی که دسترسی به RouterOS را دارند.
SCRO-3-7		بلاک نمودن WinBox Discovery	دارد	فعال	غیرفعال
SCRO-3-8		غیرفعال نمودن Network Neighbor Discovery	دارد	فعال	غیرفعال
SCRO-4		امن سازی حساب کاربری			
SCRO-4-1		تغییر نام حساب کاربری admin پیش‌فرض سیستم	دارد	admin	تغییر نام کاربر admin
SCRO-4-2		ایجاد رمزعبور پیچیده برای حساب‌های کاربری	دارد	ندارد	حداقل ۱۲ کاراکتر
SCRO-4-3		اختصاص ACL جهت دسترسی به حساب‌های کاربری	دارد	ندارد	کاهش IPهایی که دسترسی به RouterOS را دارند.
SCRO-5		Firewall			
SCRO-5-1		فعال سازی Firewall	دارد	ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.

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