تجارت الکترونیک

و

امنیت شبکه

پودمان ۴

امنیت شبکه

به هر فعالیتی که منجر به محافظت از شبکه شود امنیت شبکه می گویند .

امنیت شبکه شامل روش هایی است که :

برای محافظت از شبکه های رایانه ای در مقابل **دسترسی های غیر مجاز** و **سوء استفاده در شبکه** استفاده می شود.

مهاجم یا نفوذگر

به هر شخص یا عنصری در شبکه که حمله ای علیه سیستم انجام دهد ، مهاجم یا نفوذگر می گویند.

*حملات از یک آسیب پذیری برای رسیدن به نتایج مورد نظر استفاده می کنند.

*هک: نفوذ بدون اجازه به سیستم های رایانه ای

*هکر : به افرادی که هک می کنند هکر گفته می شود.

انواع مهاجم (هکر ها):

۱- کراکر (هکر های کلاه سیاه): کراکر ها افرادی هستند به صورت **غیر قانونی** به حریم شبکه سازمان و کاربران وارد شده و اطلاعات آنها را به سرقت می برند .

۲-هکر (قانونمند- هکر های کلاه سفید): این افراد به صورت **قانونی** اقدام به تست نفوذ روی شبکه می کنند و هدف آنها بالا بردن امنیت یک سازمان است

۳-هکر-واکر (کلاه خاکستری) هدف هکرهای کلاه خاکستری استفاده از اطلاعات سایر کامپیوترها به هر مقصودی است ولی صدمه‌ای به کامپیوتر وارد نمی‌کند. نام دیگر این گروه Whacker می‌باشد هدف اصلی واکر استفاده از اطلاعات سایر کامپیوترها به مقصود مختلف می‌باشد .

تست آسیب پذیری

این کار توسط کارشناس تست نفوذ و آسیب پذیری انجام می شود. (**ETHICAL HACKING**) کارشناسان تست نفوذ همان هکر ها ی قانونمند هستند .

هکرها مراحلی را که کراکر ها برای نفوذ به سیستم انجام می دهند طی کرده و نتایج کار خود را در قالب گزارشی از آسیب های موجود در آن سیستم یا شبکه به مدیران آن سازمان تحویل می دهند.

فازهایی که یک هکر انجام می دهد:

فاز ۱ :جمع آوری اطلاعات Foot printing فاز ۲ :پویش Scanning

فاز ۳ :ایجاد و حفظ دسترسی (حمله) فاز ۴ :پاک کردن رد پاها

فاز ۱ :جمع آوری اطلاعات Foot printing

در این فاز ؛ هکر قانونمند با استفاده از ابزارهای متعدد تا جایی که امکان دارد در در مورد سازمان مورد هدف اطلاعات کسب می کند.

ابزارهای آنلاینی برای این کار وجود دارد از جمله :(Google Hacking-Whois-Arin-Ripe)

جمع آوری اطلاعات به دو روش انجام می گیرد:

شناسایی غیرفعال : به صورت نامحسوس اقدام به جمع آوری اطلاعات می کنند ؛ بنابراین شناسایی آنها مشکل است .

شناسایی فعال: به کاوش شبکه برای کشف رایانه های افراد و آدرس IP و منابع شبکه می پردازد.(ممکن است شناسایی شود)

اطلاعاتی از جمله : محدوده آدرس IP های هدف ؛ نام دامنه ؛ اطلاعات کارکنان سازمان ؛ شماره تماس و ...

یکی از تکنیک های رایج در زمینه جمع آوری اطلاعات استفاده از موتور جستجوی گوگل است Google Hacking

کارگاه ۱ جمع آوری اطلاعات از تارنما Foot printing

اطلاع از مشخصات فردی شخصی که مالکیت تارنما را دارد	اگر شخصی یک دامنه برای تارنمای خود ثبت کرده باشد ؛ مشخصات آن فرد در یک بانک اطلاعاتی جامع ثبت می شود .(نام و نام خانوادگی – شماره تلفن و تاریخ ثبت و انقضا و ...) و هر کاربر اینترنت قادر به مشاهده اطلاعات مدیر یا صاحب تارنما است . **جهت مشاهده این اطلاعات :** در مرورگر http://www.whois.com را اجرا می کنیم .در کادر جستجوی نشانی تارنما آدرس مورد نظر را وارد کنید . و روی دکمه whois کلیک کنید تا مشخصات صاحب دامنه ؛ نشانی رایانامه و ... نمایش داده شود .
اطلاع ازسرویس دهنده تارنما	با استفاده از دستور nslookup می توان به آدرس IP سرویس دهنده دسترسی پیدا کرد. برای اطلاع از نام سرور و IP آن از این دستور استفاده می شود.
مسیر رسیدن به آدرس IP هدف	استفاده از دستور Traceert

تفاوت Ping و nslookup در چیست؟

از دستور nslookup برای اطلاع از نام دامنه –نام و IP سرورآن استفاده می شود.

برای بدست آوردن IP یک سایت از URL سایت مورد نظر Ping می گیریم . با اجرای این دستور چندین بسته (Packet) ارتباط شبکه ای بین چندین نقطه را بررسی می کند.

```
C:\Users\Hana>nslookup chap.sch.ir
Server:  TK2510_0FFC7A
Address:  192.168.1.1

Non-authoritative answer:
Name:    chap.sch.ir
Address:  37.228.138.195


C:\Users\Hana>ping     chap.sch.ir

Pinging chap.sch.ir [37.228.138.195] with 32 bytes of data:
Reply from 37.228.138.195: bytes=32 time=25ms TTL=52
Reply from 37.228.138.195: bytes=32 time=62ms TTL=52
Reply from 37.228.138.195: bytes=32 time=58ms TTL=52
Reply from 37.228.138.195: bytes=32 time=51ms TTL=52

Ping statistics for 37.228.138.195:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 25ms, Maximum = 62ms, Average = 49ms

C:\Users\Hana>
```

با استفاده از دستور tracert می توان مسیر رسیدن به آدرس IP هدف و آدرس مسیریاب های میانی را پیدا کرد.

از مشکلات این دستور امکان وجود فایروال در میانه راه و عدم اجازه عبور بسته ها ی tracert است .

```
C:\Users\Hana>tracert 37.228.138.195

Tracing route to 37.228.138.195.pol.ir [37.228.138.195]
over a maximum of 30 hops:

  1    <1 ms     2 ms     3 ms  TK2510_0FFC7A [192.168.1.1]
  2     *        *        *     Request timed out.
  3     *        *        *     Request timed out.
  4    58 ms    35 ms    37 ms  10.222.99.87
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7     *        *        *     Request timed out.
  8    54 ms    38 ms    48 ms  10.221.57.30
  9    53 ms    58 ms    36 ms  10.221.59.2
 10    30 ms    34 ms    50 ms  10.222.119.1
 11    30 ms    38 ms    43 ms  10.201.184.92
 12    26 ms    41 ms    48 ms  10.241.0.61
 13     *        *        *     Request timed out.
 14    57 ms    38 ms    38 ms  37.228.138.195.pol.ir [37.228.138.195]
 15    42 ms    28 ms    48 ms  37.228.138.195.pol.ir [37.228.138.195]

Trace complete.

C:\Users\Hana>
```

فاز ۲ :پویش Scanning

تعریف درگاه : یک آدرس مجازی برای برنامه های مبتنی بر شبکه است و یک عدد بین ۱ تا ۶۵۵۳۵ برای هر برنامه اختصاص داده می شود .

به عنوان مثال :

شماره درگاه	کاربرد (سرویس)
۸۰	برای استاندارد HTTP در وب است (انتقال ابر متن)
۸۱۹۲	اپلیکیشن ارتباط با مسیریاب میکروتیک(winbox)
۲۳	دسترسی راه دورtelnet
۲۲	اتصالات امنssh
۴۴۳	درگاه رمزنگاری شده https(پروتکل امن انتقال متن)
۵۳	سرویس دهنده DNS(نام دامنه)
۲۱	FTP

با استفاده از اطلاعات بدست آمده از مرحله قبل برای پیداکردن نقاط ضعف شبکه استفاده می کند .

زمانی که یک دستگاه از طریق شبکه به دستگاهی دیگر متصل می‌گردد، یک پورت TCP یا UDP بین ۰ تا ۶۵۵۳۵ به آن اختصاص داده می‌شود.

پویش درگاه : (Port Scanning)یکی از روش‌هایی است که نفوذگران برای تشخیص سرویس‌های راه‌اندازی شده در یک میزبان هدف (host target) استفاده می‌کنند.

نکته : یکی از نقاط آسیب پذیر در سیستم های رایانه ای ؛ درگاه های باز ونداشتن نظارت روی آن ها است . اگر درگاهی باز باشد هکر می تواند از طریق این درگاه به کل سیستم نفوذ کرده و آن را مختل کند . بنابراین باید از بسته بودن درگاه هایی که استفاده نمی شود اطمینان حاصل کرد.

اسکن پورت : فرایندی است که طی آن تمام پورت‌های یک آدرس IP بررسی می‌شود تا پورت‌های باز یا بسته‌ی آن به دست بیاید. یک نرم‌افزار اسکن پورت از پورت صفر شروع کرده و تا پورت ۶۵۵۳۵ را مورد بررسی قرار می‌دهد. برای انجام این کار تنها کافی است که این نرم‌افزار به هر یک از پورت‌ها یک درخواست فرستاده و منتظر

یک پاسخ بماند. در ساده‌ترین حالت، نرم‌افزار این کار را تک به تک برای هر پورت انجام می‌دهد. سرور مقصد نیز یک پاسخ ارسال کرده و به نرم‌افزار می‌گوید که آیا پورت باز است یا خیر.

سوال : آیا روش پویش درگاه تمام درگاه ها را اسکن می کند؟

اسکن پورت فقط می‌تواند روشی برای پیدا کردن پورت‌های قابل دسترسی یا در معرض دید شبکه باشد. اگر در سر راه ؛ فایروال شبکه وجود داشته باشد ممکن است که جلوی درخواست را بگیرد و ارتباط آن را قطع کند.

کارگاه ۲ پویش درگاه سیستم هدف

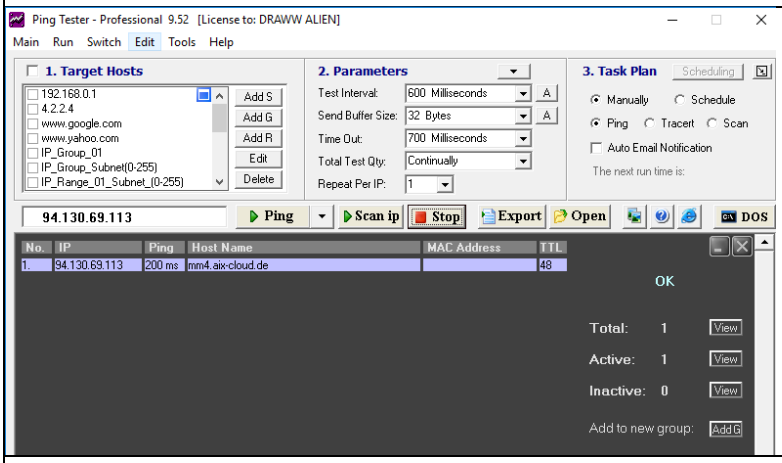
یکی از ابزارهای جامع برای پویش درگاه ها Net Tools می باشد.**(درگاه های باز باز مشخص می شود)**

پس از اجرای برنامه از منوی Start گزینه Network Tools> Port scanner را اجرا نموده و پس از وارد نمودن IP هدف درگاه های باز نمایش داده می شود.

نکته ۱: برای اطلاع از درگاه های باز سیستم خود ؛ آدرس IP سیستم هدف را 127.0.0.1 قرار می دهیم .

نکته۲ : در محیط CMD برای اطلاع از درگاه های باز سیستم خود از دستور netstat استفاده می نماییم .

کارگاه ۳ پویش آدرس IP های فعال شبکه هدف



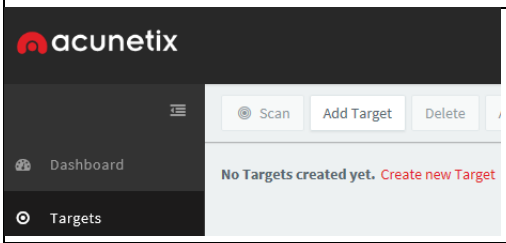
Ping Tester ابزاری است که برای مدیریت شبکه کاربرد دارد .

پس از اجرای نرم افزار آدرس IP هدف را وارد نموده و پویش می کنیم .

پس از چند ثانیه مکث در صورتی که IP فعال باشد نمایش داده می شود.

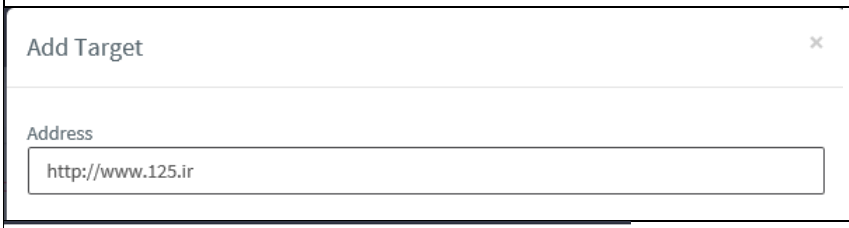
نکته : با استفاده از دکمه Tracert می توانیم به مسیر رسیدن به آدرس IP هدف و آدرس مسیریاب های میانی دسترسی پیدا کنیم .

پویش آسیب پذیری با ابزار Acunetix



یکی از برنامه های کاربردی در زمینه پویش و کشف آسیب پذیری تارنما ابزار Acunetix می باشد.

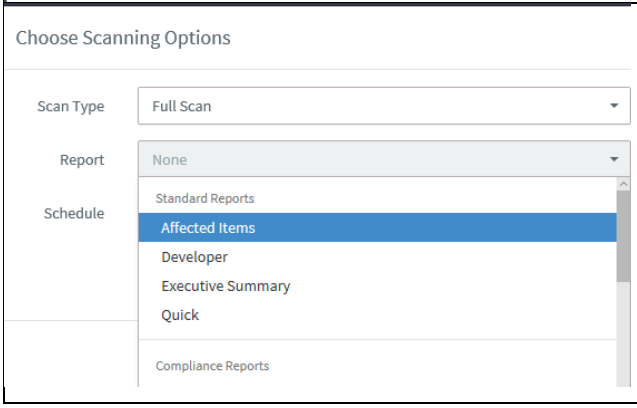
از منوی Target گزینه Creat new Target را اجرا می کنیم .



سپس آدرس تارنمای هدف را وارد می نماییم .

(مثلا تارنمای www.125.ir)

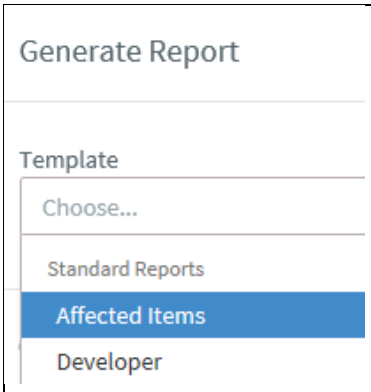
روی دکمه Add Target کلیک می کنیم .



سپس در منوی Target از بالای صفحه گزینه Scan را انتخاب می کنیم .

در بخش Reportنوع گزارش را Affected Items (موارد موثر) انتخاب می کنیم تا موارد دارای آسیب را گزارش گیری نماید.

Schedule را روی Instant قرار می دهیم که گزارش گیری(فوری) انجام شود .



یکی از امکانات این ابزارگزارش گیری از پویش است .برای این کار تب Report را انتخاب می نماییم سپس روی دکمه New Report را کلیک می کنیم . گزینه All vulnerabilities را انتخاب می نماییم و در کادر باز شده گزینه Affected Items را برمی گزینیم .
و در نهایت روی دکمه Generate Report کلیک نموده و نوع گزارش را تعیین می کنیم .

فاز ۳ :ایجاد و حفظ دسترسی (حمله)

هکر پس از شناسایی نقاط آسیب پذیر ؛ حمله خود را آغاز می کند.
*پس از دسترسی به سیستم هدف ؛ باید برای اجرای حملات بعدی ؛ دسترسی خود را حفظ کرد . برای این کار از Backdoor استفاده می کنند.

تعریف Backdoor: نقاطی در برنامه است که امکان دستیابی به یک سیستم را بدون بررسی و کنترل امنیتی فراهم می کند.
(ضعف برنامه – ارسال یک بدافزار در قالب رایانامه) می تواند به ایجاد Backdoor کمک کند.
یعنی یک درگاه برای خود باز کرده و از آن طریق وارد سیستم کاربر می شود.

حملات (Denial of service)

در حملات Dos: هدف هکر ایجاد اختلال و یا قطع سرویس دهی سرور به کاربران است (هکر شروع به ارسال ترافیک با حجم بالا به سمت سرور می کند و به قدری سرور را درگیر جواب دادن به این ترافیک می کند که سرور توان پاسخ دادن به کاربران مجاز را نداشته باشد.

حملات DDOS

در این حالت هکر از چندین و یا چندین هزار سیستم شروع به ارسال همزمان ترافیک می کند . سرور در چنین حالتی Crash می کند.
مثال : تارنمای GitHub در فوریه ۲۰۱۸ مورد حمله DDOS قرار گرفت

یکی از قویترین شیوه های هکرها برای آسیب رساندن به شرکت ها و سازمان ها، استفاده از حمله عدم پذیرش سرویس DoS است. این روش یکی از خطرناک ترین راه های حمله است که می تواند باعث قطع شدن سرویس بشود . به دلیل وجود روش های گوناگون و ابزارهای رایگان، حمله عدم پذیرش سرویس در سال های اخیر نقش پر رنگتری پیدا کرده است . هرچند که با تنظیم صحیح فایروال می شود جلوی خیلی از این ابزارها را گرفت اما هکرها با توسعه ابزارها و شیوه های حمله، می توانند این محدودیت ها رو دور بزنند.

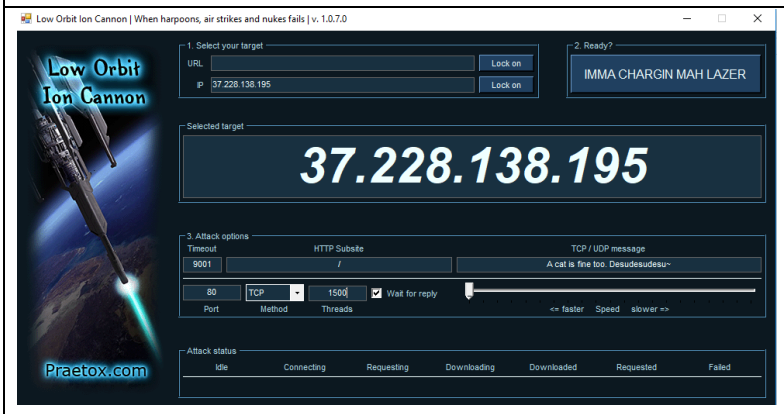
حمله عدم پذیرش سرویسDoS

حمله DoS تلاشی است برای جلوگیری از دسترسی کاربران به سرویس یا سرور و در نهایت تعطیل کردن سرویس. این هدف با پر کردن صف درخواست های سرور با درخواست های تقلبی انجام می شود.
عموما دو گونه حمله DoS داریم، یکی که به از کار افتادن سرور منتج می شود و دیگری که سرویس را مشغول می نماید.

حمله عدم پذیرش سرویس توزیع شدهDDoS

در صورتیکه کامپیوترهای زیادی در حمله DoS به یک هدف مشارکت داشته باشند،به آن حمله DDoSگفته می شود.
سناریوی انجام این حمله : ابتدا تعداد زیادی کامپیوتر (آلوده می نماید) با نصب و اجرای ابزار حمله DoS از طریق آن کامپیتورها، حمله اصلی انجام می شود . کامپیوترهای آلوده شده تحت فرمان هکر (شبکه زامبی) معمولا به هزاران کامپیوتر و حتی صدها هزار می رسند. این شیوه باعث می شود که قربانی نتواند با بلاک کردن IP جلوی حمله را بگیرد. (هکرها معمولا با پخش کردن تروجان این شبکه زامبی را به دست می آورند هرچه شبکه زامبی بزرگتر باشه، حمله موفق تر خواهد بود.)

کارگاه ۴ شبیه سازی حمله DDOS در کارگاه رایانه



برای حملهDOS ابزارهای زیادی وجود دارد برای حمله به سرور و سر ریز کردن درخواست های ارسالی همچنین برای کنترل شبکه زامبی از ابزار LOIC (Low Orbit Ion Cano)استفاده می شود .
با این ابزار یک کاربر به راحتی می تواند علیه سرورهای کوچک حمله DoS انجام دهد . (با ارسال درخواست هایUDP ، TCP و HTTP به قربانی) . در این نرم افزار هکر کافی است آدرس آی‌پی سرور وارد کند. url و یا IP سرور رو وارد کنید و سپس با انتخاب پارامترهای حمله، اقدام به DoS کنید. با فشردن دکمه IMMA CHARGIN MAH LAZER و پس از چند ثانیه، سایت از دسترس خارج می شود.

نکته : اگر حمله با استفاده از ابزار LOIC انجام شود ؛ IP سیستم شما به قربانی نمایش داده می شود .توجه کنید که استفاده از پراکسی هم بی فایده است زیرا با این کار به سرور پراکسی حمله می کنید و نه سروری که هدف شماست !

پس از نصب ،در کادر selected Target آدرس IP هدف را وارد می نماییم .

در کادر Attack option نوع و پارامترهای حمله تعیین می شود .

برای شروع حمله دکمه Ready را کلیک می کنیم .

فایروال(Firewall)

فایروال یک سرویس امنیتی در شبکه های رایانه ای است که وظیفه اصلی آن بررسی بسته های اطلاعاتی و حذف بسته های مشکوک است .به این عمل فیلترینگ می گویند .

سرویس IDS و سرویس IPS

یکی از سرویس های تشخیص حملات ؛ سرویس IDS(Intrusion Detection system) نام دارد .

*سرویس IDS با سرویس IPS (Intrusion Prevention system) برای جلوگیری از حمله همراه است.

به عبارت دیگر ؛ سرویس IDS قادر به شناسایی انواع حملات و سرویس IPS قادر به جلوگیری و خنثی کردن حملات است

سرویس فایروال Firewall

یکی از سرویس های بسیار مهم که در تمامی سیستم ها و شبکه ها وجود دارد ، سرویس فایروال است .

- این سرویس از ورود بسته های مشکوک به شبکه جلوگیری می کند .
- فایروال سرویسی است که به صورت نرم افزاری و سخت افزاری ارائه می شود.
- فایروال نرم افزاری همانند سایر نرم افزارها روی سیستم عامل نصب می شود.
- به بررسی بسته ها به وسیله فایروال فیلتر کردن بسته ها می گویند .
- فایروال ویندوز: نرم افزارهای ISA Server و Kerio control
- برخی از نرم افزارهای آنتی ویروس نمونه ای از فایروال نرم افزاری هستند.
- فایروال سخت افزاری روی بردهای سخت افزاری پیاده سازی شده ؛ و در قالب یک سخت افزار مستقل عرضه می شوند.
- این نوع فایروال ها تنظیمات پیشرفته تری نسبت به نوع نرم افزاری دارند و برای شبکه های بزرگ استفاده می شوند .
- مزیت آن : بار ترافیکی کمتری روی شبکه دارد.

فرض کنید شبکه داخلی یک سازمان باید از طریق یک فایروال به اینترنت متصل شود ...

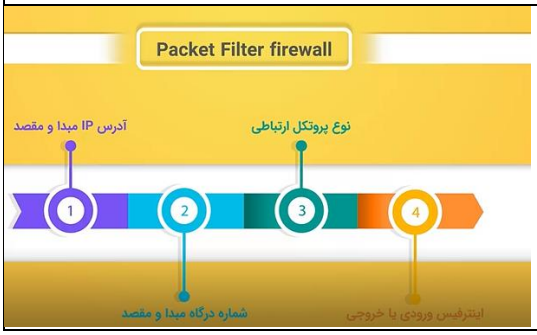
مدیر یک شبکه می خواهد شرایطی را برای این اتصال ایجاد کند :

- ✓ یک رایانه از سمت شبکه خارجی به داخلی نتواند بسته ارسال کند .
- ✓ پروتکل TCP روی درگاه ۲۳ از یک کلاینت شبکه داخلی به خارجی باز باشد.

مدیر باید فایروال های مختلف را بررسی کند!

انواع فایروال بر اساس فیلترینگ

Packet Filter Firewall : با استفاده از مجموعه ای از قوانین (Rule) که برای آنها تعریف می شوند ؛ بسته های ورودی و خروجی را بررسی می کند . بر اساس قوانین (Rule) ها تصمیم می گیرد بسته را عبور دهد و یا مانع ورود آن می شود.



رول ها ی فایروال بر اساس اطلاعات :☜

نوشته می شود .

مدیر رول های مدنظر خود و اقدام لازم برای هر یک را در جدول فایروال می نویسد .

زمانیکه بسته ای قصد عبور از فایروال Pack Filter را داشته باشد ؛ اطلاعات بسته با رول های جدول مقایسه شده و در صورت مطابقت با یکی از آنها ، مطابق نوع اقدام مشخص شده در آن رول با بسته رفتار می شود.

ضعف این نوع فایروال : عدم تشخیص وضعیت جریان های ترافیکی شبکه

Stateful Inspection Firewall : (فایروال حالت منذ) : این فایروال در حافظه Cache خود یک جدول وضعیت دارد .

برای هر بسته علاوه بر آدرس IP درگاه و نوع پروتکل یک فیلد دیگر به نام State در نظر گرفته می شود .

مثلا اگر بخواهیم بسته های TCP را مدیریت کنیم از این نوع فایروال استفاده می شود.

ضعف این نوع فایروال : محدودیت در خواندن محتویات بسته

Application Proxy Firewall :بین کلاینت و سرور قرار می گیرد.

زمانیکه کلاینت و سرور بخواهند برای هم بسته ارسال کنند ؛ ابتدا فایروال بسته را دریافت کرده و محتوای آن را بررسی می کند سپس بسته را به مقصد ارسال کرده و خودش را به عنوان فرستنده بسته معرفی می کند. با توجه به عملکرد این فایروال بسته هایی که دارای اطلاعات مخرب هستند فیلتر می شوند .

سرویس پراکسی یک سرویس میانجی است که هم می تواند به صورت نرم افزاری و هم به صورت سخت افزاری روی رایانه کاربر نصب شود و به صورت واسطه ای میان کاربر و شبکه قرار بگیرد .

نکته : اگر روی یک رایانه مستقل نصب شود و بین شبکه داخلی و خارجی قرار گیرد ؛ پراکسی سرور نامیده می شود .

کاربران برای دسترسی به شبکه خارجی درخواست خود را به پراکسی سرور ارسال می کنند و پراکسی پس از ارسال درخواست به شبکه خارجی و برگشت پاسخ ؛ نتیجه را برای کاربر ارسال کرده و در حافظه کش خود نیز نگهداری می کند تا در صورت درخواست مجدد از سوی کاربران بلافاصله از آن استفاده کند .

- به جای بررسی ترافیک مجاز یا غیرمجاز از روی آدرس IP و درگاه ؛ فقط برنامه های مجاز را بررسی می کند . به دلیل اینکه این فایروال روی اپلیکیشن ها تمرکز دارد به آن Application level Gateway گفته می شود .
- این فایروال به صورت پراکسی نیز عمل می کند. و پیش از برقراری ارتباط بین سرویس گیرنده و سرویس دهنده راه دور ؛ در میان آنها قرار گرفته ؛ اپلیکیشن ها را مدیریت می کند.

محاسن فایروال Application Proxy Firewall:

- فایروال توانایی Cache کردن اطلاعات است . به همین دلیل سرعت پاسخگویی در شبکه بالا می رود.
- آدرس IP مبدا بسته مخفی است و به همین دلیل امنیت بالا می رود .

نکته : فایروال های سرویس وب WAF(Web Application Firewall) : وظیفه بررسی ترافیک اپلیکیشن های وب را بر عهده دارند .

کارگاه ۵ فعال سازی فایروال سیستم عامل

متداول ترین فایروال نرم افزاری ؛ فایروال ویندوز است .

*روش فیلترینگ در این فایروال از نوع Packet Filter است .

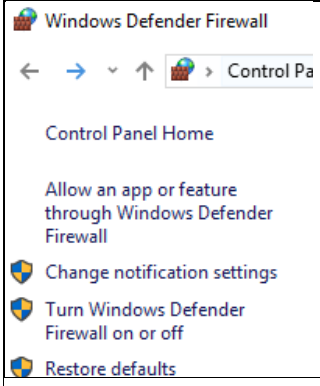
فعال بودن فایروال امنیت رایانه شما را چندین برابر افزایش می دهد .

۱–از کنترل پنل گزینه Windows Defender Firewall را انتخاب کنید

۲–فایروال آنتی ویروس را غیرفعال کنید.

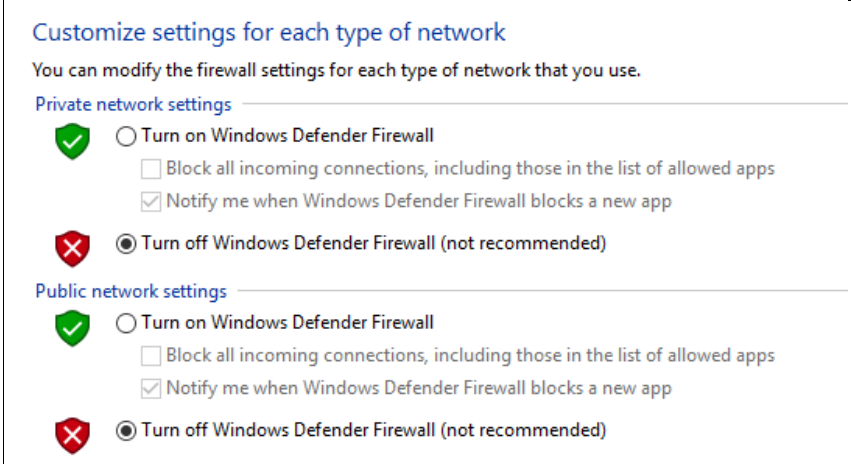
وارد تنظیمات انتی ویروس شده (کلید F5) گزینه personal firewall گزینه System Integration و در آخر گزینه personal firewall completely disabled را انتخاب و Ok می کنیم .

۳–فایروال ویندوز را فعال کنید .



گزینه Turn windows Defender Firewall on or off را انتخاب کرده سپس از کادر محاوره ای ظاهر شده فایروال ویندوز را فعال کنید

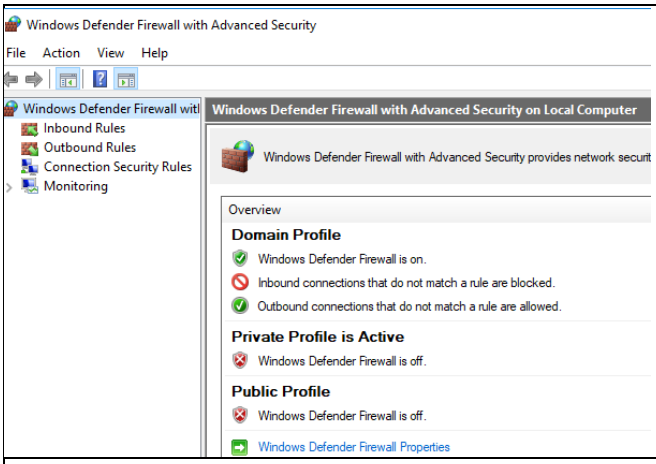
۴–فایروال ویندوز را Turn on کنید



جریان های ورودی و خروجی در فایروال

Outbound Traffic :جریان بسته های خروجی از رایانه به سمت خارج از شبکه را ترافیک خروجی می گویند.

Inbound Traffic :جریان بسته های ورودی از شبکه بیرونی به سمت رایانه را ترافیک ورودی می گویند



در فایروال ویندوز می توانیم جریان های ورودی و خروجی را مدیریت نماییم . برای این کار از گزینه Advanced Setting استفاده می نماییم .

دیواره آتش (firewall) داخلی سیستم عامل ویندوز این امکان را به شما می‌دهد که بدون نصب هیچ برنامه‌ی جانبی دیگر دسترسی به اینترنت را بلوکه کنید، یک لیست سفید درست کنید یا جلوی دسترسی به یک سری از پورت‌ها و آی‌پی آدرس‌ها را بگیرید.

دیواره آتش شامل سه پروفایل مختلف است. که می‌توانید با دستورات مختلف آن‌ها را برای شبکه‌های خصوصی و عمومی خود فعال کنید. این انتخاب‌های گسترده و خوب درون دیواره آتش که با یک سیستم حفاظتی پیشرفته است تعبیه شده‌اند که برای اولین بار در ویندوز ویستا به نمایش درآمده بودند.

به این ترتیب با استفاده از دیواره آتش سیستم عامل می‌توانید ضریب امنیت خود و شبکه‌ی خود را در حد قابل قبولی بالاتر برده و کنترل بیشتری روی آن داشته باشید.

برای این منظور بخش‌های مختلف دیواره آتش و چگونگی استفاده از آن را بررسی خواهیم کرد.

برای دسترسی به فایروال پیشرفته ویندوز گزینه Advanced settings را انتخاب کنید.

پیکربندی پروفایل‌های شبکه

فایروال ویندوز از سه پروفایل مختلف زیر استفاده می‌کند:

Domain : زمانی که کامپیوتر شما به دامنه‌ای متصل است.

Private : زمانی که کامپیوتر شما به شبکه‌ای خصوصی مثلاً «work» یا «home» متصل است.

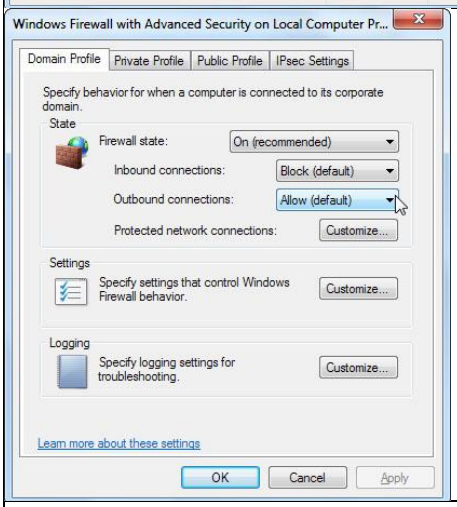
Public: زمانی که کامپیوتر شما به یک شبکه عمومی مانند یک نقطه دستیابی Wi-Fi متصل شده یا مستقیماً به اینترنت متصل است .

نکته : ویندوز همیشه در هنگام اتصال از شما سؤال می‌کند که آیا این شبکه‌ای که با ان متصل شده‌اید خصوصی است یا عمومی.

ممکن است یک کامپیوتر از چندین پروفایل استفاده کند، این بستگی به موقعیت دارد. برای مثال، امکان دارد یک لپ‌تاپ هنگامی که در محل کار به دامنه متصل است از پروفایل domain استفاده کند، هنگامی که در خانه به یک شبکه خصوصی متصل است از پروفایل private و زمانی که در یک محل عمومی به Wi-Fi متصل است از پروفایل Public

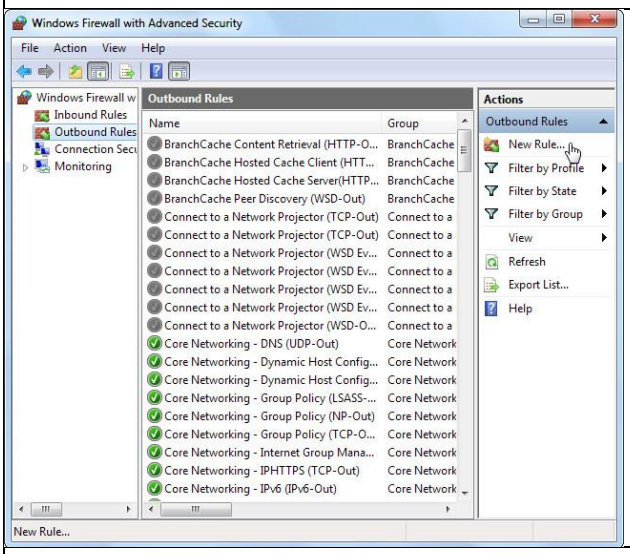
برای پیکربندی فایروال کافی است بر روی Windows Firewall Properties کلیک کنید.

فایروال ویندوز برای هر پروفایل یک سربرگ جداگانه در نظر گرفته است. ویندوز برای حالت پیش‌فرض به تمامی ترافیک خروجی و ورودی اجازه رفت و آمد داده است. ولی شما می‌توانید تمامی ترافیک خروجی را بسته و برای هر ارتباط یک دستور خاص بنویسید. این تنظیمات بسته به پروفایل هستند، شما می‌توانید از یک لیست سفید برای هر شبکه خاص استفاده کنید.



اگر شما ارتباطات outbound را مسدود کنید، شما هیچ پیغامی مبنی بر بلوکه شدن برنامه دریافت نخواهید کرد و برنامه بدون هیچ سر و صدایی به هیچ چیز دسترسی نخواهد داشت.

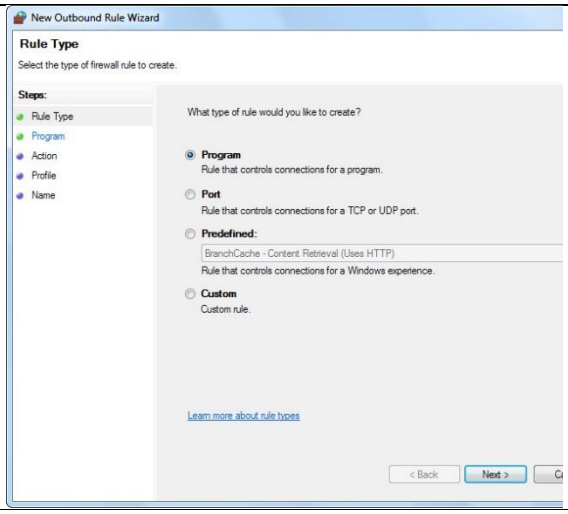
ایجاد یک دستور(Rule)

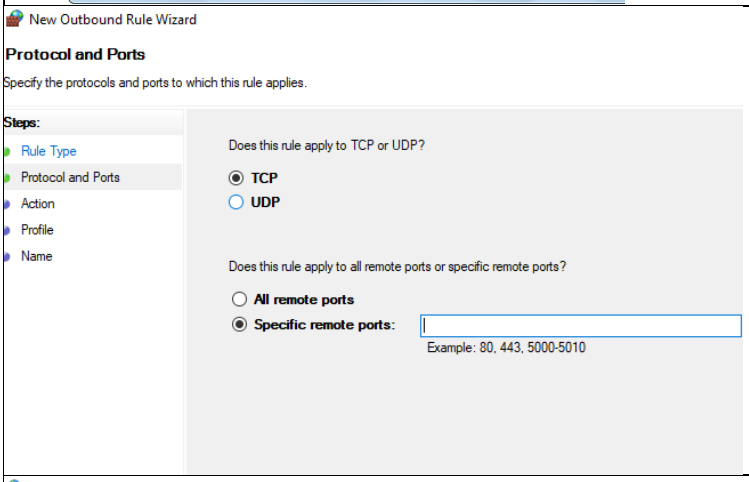


برای ایجاد یک دستور یا قانون جدید، یکی از دو گزینه «Inbound Rules» یا «Outbound Rules»را از درون دسته‌بندی‌ها انتخاب کنید و سپس Create Rule را بزنید .

- در پنجره جدید شما توانایی انتخاب بین ۴ نوع مختلف از دستورات را دارید:

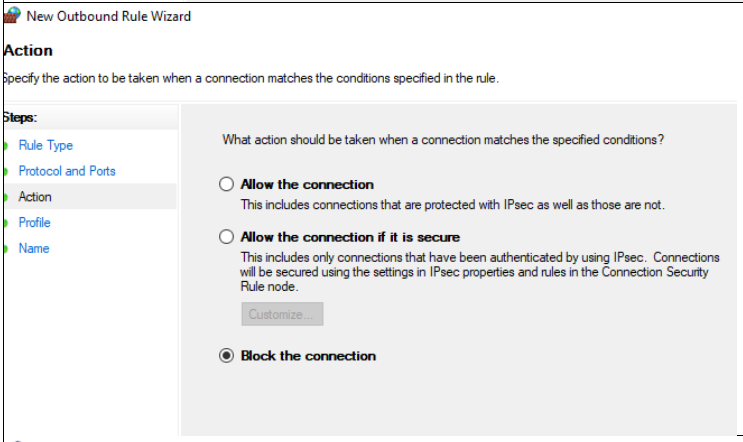
Program	مسدود کردن یا اجازه دادن به یک برنامه.
Port	تغییرات در دسترسی به پورت‌ها و پروتکل‌ها
Predefined	استفاده از دستورات از پیش نوشته شده
Custom	مخلوطی از سه حالت قبل یعنی مسدود کردن یا اجازه دادن به برنامه و پورت‌ها یا آی‌پی آدرس‌ها به همراه یکدیگر



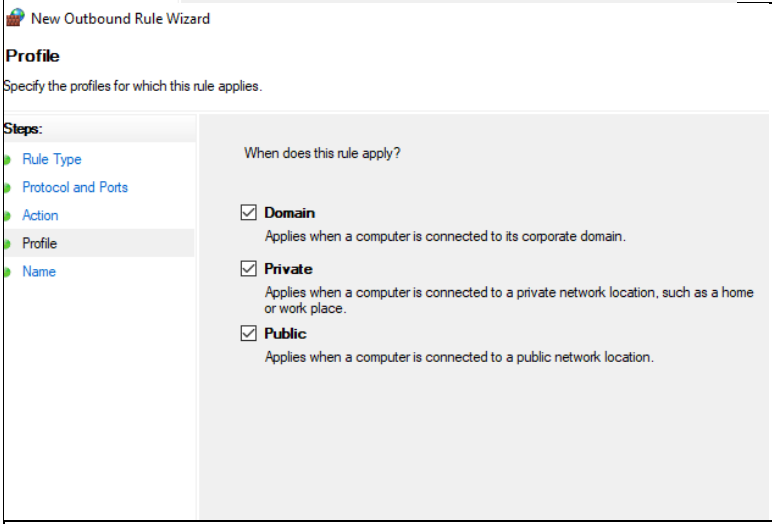


برای مسدود نمودن پورت گزینه Port را انتخاب می کنیم . سپس پروتکل مورد نظر را برمی گزینیم .

پورتهایی که در نظر داریم تا مسدود شوند را وارد می نماییم . (در صورتیکه چند پورت باشد با علامت کاما از هم جدا می کنیم)



اگر قصد بلوک کردن پورت را داریم گزینه مربوطه را انتخاب می کنیم .



پروفایل مورد نظر را انتخاب می کنیم . (بهتر است هر سه گزینه انتخاب شود)

در مرحله پایانی نامی برای رول در نظر می گیریم .

گزارش گیری از رخداد های فایروال:

- بررسی درستی رول های اضافه شده و عیب یابی رول هایی که دچار مشکل شده اند.
- بررسی اینکه آیا فایروال باعث اختلال در نرم افزاری شده است یا خیر؟
- بررسی درگاه هایی که بسته شده اند و بسته هایی که حذف شده اند .
- بررسی اینکه درون شبکه یک آدرس IP و یا گروهی از آدرس IP در تلاش هستند به فایروال و یا قسمت های مهم دیگر دسترسی پیدا کنند یا خیر ؟

کارگاه ۶ فعال سازی گزارش گیری فایروال ویندوز

Advanced settings را انتخاب نموده و در بخش راست صفحه گزینه Properties را انتخاب می کنیم .

فایروال سخت افزاری

ساز و کارهای دفاعی و محافظتی در سطوح شبکه :

MAC Filtering	دسترسی کاربران به شبکه را بر اساس مک آدرس آنها اعتبار سنجی می کند.
Packet Filtering	با استفاده از سازو کار IDSو IPS بر اساس آدرس IP تصمیم می گیرد بسته از شبکه رد شود یا خیر
Stateful Filtering	در سطح اپلیکیشن انجام می شود . یکی از قویترین انواع فیلترینگ است
دستگاه های UTM	یکی از قدرتمند ترین تجهیزات فعال در شبکه هستند که انواع فیلترینگ را انجام می دهند و علاوه بر آن سرویس هایی مانند Anti-spam-AntiVirus-IDPS-IPsec/VPN

عملیات فیلترینگ در فایروال ؛ دردو قسمت انجام می شود :

۱–در لبه ورودی و هنگام ورود بسته به فایروال

۲–در لبه خروجی و قبل از خروج بسته ها

سرویس فایروال یکی از مهمترین سرویس های روی مسیریاب میکروتیک است که امکاناتی از قبیل :

- ✓ فیلترینگ از نوع stateful
- ✓ فیلترینگ اپلیکیشن
- ✓ فیلترینگ بر اساس آدرس IP و درگاه و اندازه و محتوای بسته

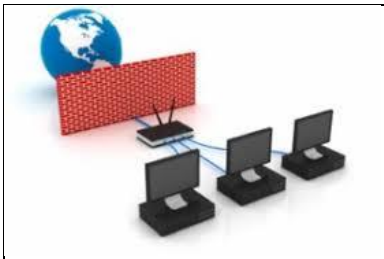
در فایروال میکروتیک (همانند فایروال ویندوز) دو نوع ترافیک ورودی و خروجی وجود دارد که به هر یک از این نوع ترافیک ها یک زنجیر ترافیک یا Chain گفته می شود .

Input Chain	ترافیک از سمت یک سرویس گیرنده یا شبکه می آید و به خود فایروال ختم می شود
Output Chain	حالتی است که مبدا ترافیک فایروال است و به سمت یک سرویس گیرنده یا شبکه بیرونی ختم می شود
*در فایروال میکروتیک یک حالت دیگر وجود دارد که در فایروال ویندوز وجود ندارد که به آن Forward chain گفته می شود حالتی است که ترافیک از یک شبکه یا سرویس گیرنده ارسال می شود و از درون فایروال عبور می کند و به مقصد خود می رسد.	

جایگاه فایروال در شبکه

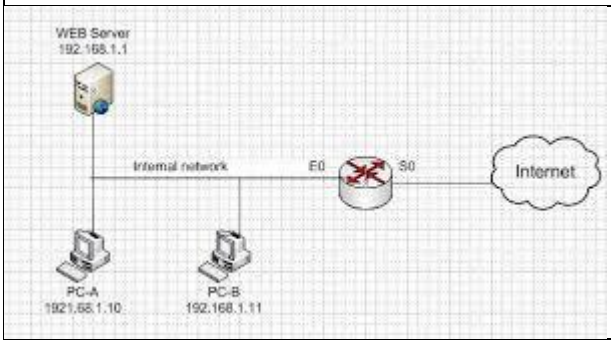
با توجه به نوع شبکه و هدف فایروال ؛ جایگاه قرارگیری آن متفاوت می باشد:

- لبه شبکه : برای محافظت از شبکه داخلی (بین شبکه داخلی و خارجی قرار می گیرد)



- بین سرورهای شبکه و شبکه داخلی

برای تفکیک شبکه داخلی یک سازمان از سرورهای آن سازمان فایروال از هر دو شبکه محافظت می کند .



کارگاه ۷ مسدود کردن دسترسی از طریق Winbox به میکروتیک

در فایروال میکروتیک تنظیماتی انجام می دهیم که سرویس گیرنده های شبکه خارجی نتوانند از طریق Winbox با مسیریاب میکروتیک ارتباط برقرار کنند .

۱–پس از ورود به محیط Winbox از منوی IP گزینه Firewall و یک رول جدید ایجاد می کنیم .
۲– سربرگ General را انتخاب می کنیم سپس گزینه Input را انتخاب می کنیم .
۳– مقدار گزینه Dst-Asress را برای آن تعیین کنید . بهتر است برابر با مقدار اینترفیس اتصال به اینترنت باشد .
۴– پروتکل مقصد را برابر با مقدار tcp و پورت آن را برابر با مقدار ۸۲۹۱
۵–سربرگ Action مقدار عبارت Drop را انتخاب می کنیم .
۶– اتصال به میکروتیک با IP مورد نظر قطع می شود .
۷– در انتهای رول مقدار Packet تعداد بسته های ارسال شده از سمت خارج شبکه به سمت میکروتیک برابر با یک مقداری غیر از صفر خواهد بود .

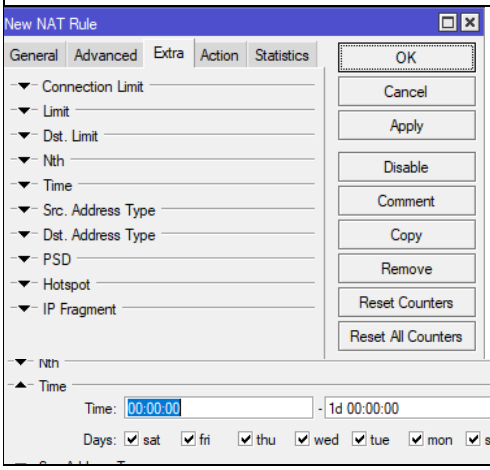
کارگاه ۸ مسدود کردن دسترسی به Winbox از طریق مک آدرس

برای مسدود سازی دسترسی به میکروتیک از طریق مک آدرس با استفاده از منوی Tolls گزینه Mac server می توان دسترسی به میکروتیک را محدود نمود .

پس از این کار اتصال به میکروتیک حتی از طریق IP مدیر نیز مسدود می شود .

توصیه می شود که این کار انجام نشود.

با استفاده از IP>Firewall تب Extra از بخش Time برای کلاینت ها می توانیم محدودیت زمانی ایجاد نماییم.



در قسمت Time ساعت و در قسمت Days روزهای هفته مشخص می شود.

کارگاه ۹ مسدود سازی Ping به میکروتیک
جهت مسدود سازی دستور Ping (هم از شبکه داخلی و هم از شبکه خارجی) نکته : با این کار هکرها دچار سردرگمی می شوند .
۱–با استفاده از IP>Firewall و یک فایروال برای آن می نویسیم . ۲–از آنجا که مقصد ترافیک میکروتیک می باشد رول از نوع input انتخاب می شود . ۳–برای اینکه کسی نتواند میکروتیک را ping کند در قسمت آدرس مبدا و مقصد را خالی می گذاریم . ۴–دستور Ping با پروتکل ICMP کار می کند . ۵–در تب Action گزینه reject را انتخاب می کنیم با این کار هکر ها دچار سردرگمی می شوند. ۶–