پودمان ۴

تنظیمات امنیت شبکه

هر سازمان یا کار و کسب مبتنی بر شبکه نیاز به سیاست‌های امنیتی دارد که مدبرانه تدوین شده باشند؛ زیرا انواع خطرات از بیرون و درون سازمان به‌وسیله هکرها، رقبا و یا کشورهای خارجی، منافع سازمان را تهدید می‌کند. با اجرای دقیق سیاست‌های امنیتی، سازمان‌ها می‌توانند تهدیدها را کاهش دهند. برنامه‌های سازمان برای محافظت از دارایی‌های سازمان شامل سرمایه‌های فیزیکی و داده‌ها و اطلاعات، از سیاست‌های امنیتی استفاده می‌کنند. فرایند تکمیل و اصلاح سیاست‌های امنیتی هیچ‌گاه متوقف نشده، متناسب با تغییر فناوری و نیازهای کاربران به‌روز می‌شود. راهکارهای امنیت شبکه شامل تعیین مجوزهای کاربران، آموزش کاربران برای مقابله با خطرات، تعیین معیارها و روش سنجش امنیت سازمان و مؤثر بودن سیاست‌های امنیتی و به‌روزرسانی آنها متناسب با اهداف سازمان و مدیریت آن است. در این پودمان هنرجویان با اتکا بر دانش و مهارت قادر خواهند بود ضمن آشنایی با مراحل تست آسیب‌پذیری شبکه، با استفاده از ابزارهایی مانند فایروال سخت‌افزاری و نرم‌افزاری از حملات احتمالی جلوگیری کنند.

واحد یادگیری ۴

شایستگی تنظیمات امنیت شبکه

آیا تا به حال پی برده اید

- برای محافظت از شبکه کارگاه مدرسه خود چه نوع فایروالی را پیشنهاد می کنید؟
- برای جلوگیری از ورود افراد خانواده به برخی از تارنماها چه راهکاری پیشنهاد می‌دهید؟
- مدیر شبکه یک سازمان بزرگ برای محافظت از شبکه سازمان چه راهکارهای امنیتی را باید اتخاذ کند؟
- چگونه می‌توان از دسترسی افراد غیرمجاز به فایروال شرکت جلوگیری کرد؟
- چگونه می‌توان دسترسی کارمندان به برخی از شبکه‌های اجتماعی را مسدود کرد؟

هدف از این واحد شایستگی، حفاظت از شبکه به کمک فایروال‌های نرم‌افزاری و سخت‌افزاری است.

استاندارد عملکرد

کشف نقاط ضعف شبکه و حفاظت از شبکه در برابر حملات به کمک فایروال نرم‌افزاری و سخت‌افزاری

امنیت شبکه

چرا اسناد مهم خود را در گاو صندوق نگهداری می‌کنیم؟
چرا درِ اتاق بایگانی شرکت خود را قفل می‌کنیم؟
چرا برای ورود به رایانه خود گذرواژه تعیین می‌کنیم؟
آیا تاکنون اخبار سرقت‌های اینترنتی را شنیده‌اید؟
آیا تاکنون نگران سرقت اینترنتی از حسابتان بوده‌اید؟
چرا رایانه خود را به‌طور منظم ویروس‌یابی می‌کنیم؟
آیا حفظ و نگهداری گذرواژه برای برقراری امنیت کافی است؟

سیستم‌های بانکداری، شرکت‌های خدمات گردشگری، سیستم‌های دانشگاهی و آموزشی، سازمان بورس و همه سیستم‌های اداری، اقتصادی، اجتماعی و سیاسی به واسطه زیرساخت فناوری اطلاعات به حیات خود ادامه می‌دهند. اگر خللی در امنیت ایجاد شود، قطعاً صدمات زیادی به این سیستم‌ها وارد خواهد شد؛ بنابراین امروزه متخصصان حوزه فناوری اطلاعات بیشترین تمرکز خود را روی افزایش حداکثری امنیت این زیرساخت معطوف کرده‌اند.

در سال ۲۰۱۴، یاهو بزرگ‌ترین هک تاریخ را تجربه کرد و اطلاعات ۵۰۰ میلیون کاربر آن به دست هکرها افتاد.

جلوگیری از سرقت و افشای اطلاعات تنها یکی از جنبه‌های امنیت است. علاوه بر این، دسترسی به اطلاعات در زمان مورد نیاز و عدم تغییر اطلاعات در مسیر ارسال نیز از جنبه‌های دیگر امنیت محسوب می‌شوند. با این حال هیچ فرد یا سازمانی نمی‌تواند ادعا کند که ۱۰۰ درصد امنیت را تأمین کرده است.

فعالیت گروهی

با هم‌گروهی خود، برای هر یک از موارد ستون راست، یک اقدام امنیتی مناسب از ستون چپ انتخاب کنید.

کیف کارت‌های اعتباری	استفاده از الگوی قفل و فعال کردن حالت خاموش شدن به هنگام سرقت
رایانه همراه	اطمینان از سالم بودن قفل‌ها و استفاده از دزدگیر
گوشی هوشمند	در دسترس قرار ندادن گذرواژه شخصی و استفاده نکردن از یک گذرواژه واحد
منزل مسکونی	اطمینان از سالم بودن قفل‌ها و استفاده از دوربین مداربسته و دزدگیر و حفاظ
خودرو شخصی	تهیه نسخه پشتیبان از اطلاعات مهم و استفاده از گذرواژه قوی

به هر فعالیتی که منجر به محافظت از شبکه شود، امنیت شبکه می‌گویند. امنیت شبکه شامل روش‌هایی است که برای محافظت از شبکه‌های رایانه‌ای در مقابل دسترسی‌های غیرمجاز و سوءاستفاده در شبکه استفاده می‌شود.

هر فردی که قصد دارد در حوزه شبکه و امنیت اطلاعات فعالیت کند، باید با تعاریف و اصطلاحات مهم در این حوزه آشنا باشد (جدول ۱).

جدول ۱ـ اصطلاحات امنیتی حوزه امنیت

اصطلاحات امنیتی	توضیح
دارایی	هر موجودیتی که ارزش محافظت داشته باشد دارایی تلقی می‌شود. برای مثال، اطلاعات مالی مربوط به مشتریان یک بانک یا اطلاعات دانش‌آموزان در مدارس به عنوان دارایی‌های آن سازمان محسوب می‌شود.
آسیب‌پذیری	هرگونه نقطه ضعف که موجب به خطر افتادن منابع یک سیستم شود، آسیب‌پذیری نام دارد. به عبارتی هرگونه نقطه ضعف یا خلل سخت‌افزاری و نرم‌افزاری در طراحی، پیاده‌سازی یا اجرا که بتوان از آن سوء استفاده و سیاست‌های امنیتی را نقض کرد، نوعی آسیب‌پذیری است.
تهدیدات امنیتی	عاملی یا حالتی که در صورت مهیا بودن شرایط، توانایی نقض امنیت را خواهد داشت و موجب آسیب می‌شود. به بیان دیگر تهدید، یک خطر احتمالی است که از یک نقطه آسیب‌پذیر در سیستم سوء استفاده می‌کند.
حمله	یک عمل هوشمندانه برای فرار از سرویس‌های امنیتی و نقض امنیت سیستم است. حمله زمانی رخ می‌دهد که سیستمی به‌خاطر وجود نقاط آسیب‌پذیر به خطر بیفتد.
سرویس امنیتی	سرویسی که امنیت سیستم‌های پردازش داده و انتقال اطلاعات سازمان را تضمین می‌کند. این سرویس‌ها اصولاً برای مقابله با حملات امنیتی مورد استفاده قرار می‌گیرند. سرویس احراز هویت یک نمونه از این سرویس‌ها به شمار می‌آید.
احراز (تصدیق) هویت	اطمینان از اینکه کاربر مقابل ما دقیقاً همان شخصی است که ادعا می‌کند، احراز هویت نامیده می‌شود. هدف احراز هویت تأمین یکپارچگی است. برای مثال یک مشتری بانک، به‌وسیله نام کاربری و گذرواژه خود وارد نرم‌افزار سیستم بانکی شده، در صفحه مربوط به خود تراکنش‌های مالی انجام می‌دهد.
حفظ حریم خصوصی	حفظ حریم خصوصی عبارت است از مقاومت در مقابل افشای اطلاعاتی که می‌توان از بستر شبکه استخراج کرد. برای مثال کدملی یک فرد موضوع محرمانه‌ای به شمار نمی‌آید؛ ولی حریم خصوصی آن شخص محسوب می‌شود.
سازوکار امنیتی	به پیاده‌سازی قوانینی که برای حفظ امنیت دارایی‌های یک سازمان تعیین می‌شوند، سازوکار امنیتی می‌گویند. برای مثال برای بررسی زمان ورود و خروج کارمندان یک اداره از دوربین‌های مدار بسته و دستگاه‌های حضور و غیاب استفاده می‌شود. بنابراین به کمک نصب دستگاه حضور و غیاب و دوربین مدار بسته قانون امنیتی «کارمند باید به موقع در محل کارش حاضر شود» و همچنین «باید ورود و خروج همه افراد به اداره بررسی شود» پیاده‌سازی شده است.

فیلم

فیلم شماره ۱۲۲۲۶: امنیت در شبکه

فعالیت کارگاهی

پس از مشاهده فیلم، برای هر یک از موارد ذکر شده در جدول یک مصداق بنویسید.

اصطلاح	مثال
دارایی	
آسیب‌پذیری	
تهدیدات امنیتی	
سازوکار امنیتی	
حمله	

مهاجم

به هر شخص یا عنصر در شبکه که حمله‌ای علیه سیستم انجام دهد، مهاجم یا نفوذگر می‌گویند.
هر حمله دارای حمله‌کننده یا مهاجم است. مهاجم حمله خود را علیه یک هدف مشخص انجام می‌دهد.
حملات از یک آسیب‌پذیری برای رسیدن به نتایج مورد نظر استفاده می‌کنند.

انواع مهاجم یا نفوذگر

هکر: هک به معنی نفوذ بدون اجازه به سیستم‌های رایانه‌ای است. به افرادی که اقدام به این کار می‌کنند هکر گفته می‌شود. هکرها بر اساس اهدافی که دارند به چندین گروه تقسیم می‌شوند (شکل ۱).

شکل ۱ــ انواع هکرها

هکر غیرقانونی (کراکر): در بیشتر موارد زمانی که از هکر نام می‌بریم این نوع از هکرها مدنظر هستند. این افراد کسانی هستند که سعی در ورود غیرقانونی به حریم شبکه سازمان‌ها و کاربران و به سرقت بردن اطلاعات آنها دارند. به این افراد هکر مجرم (Criminal Hacker (Cracker)) می‌گویند و از هکرهای کلاه سیاه هستند.
هکر اخلاقی (قانون‌مند): این افراد که در حوزه شبکه و امنیت متخصص هستند، با استفاده از ابزارهای هک و نفوذ، سعی در پیدا کردن نقاط آسیب‌پذیر در سیستم‌های امنیتی سازمان‌ها دارند تا مدیران آن سازمان‌ها این نقاط ضعف را برطرف کنند. هدف این افراد ارزیابی سطح امنیتی زیرساخت فناوری سازمان‌ها است. این هکرها از نوع هکرهای کلاه سفید هستند.

پژوهش

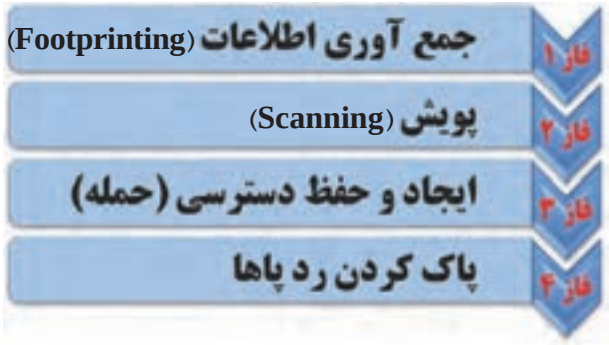
با جست‌وجو در اینترنت، اطلاعات لازم را در خصوص انواع هکرهای کلاه رنگی پیدا کنید.

تست آسیب‌پذیری

معمولاً زمانی که یک هکر قصد نفوذ به یک سیستم یا شبکه اطلاعاتی را دارد، ابتدا به‌وسیله حملات غیرفعال، اطلاعات لازم را در مورد سیستم هدف خود به‌دست می‌آورد. ممکن است این فرایند چندین ساعت، روز یا ماه طول بکشد. پس از اینکه نفوذگر اطلاعات جامع و دقیقی از هدف خود به‌دست آورد، با یک برنامه‌ریزی دقیق، به‌وسیله حملات فعال به آن سیستم یا شبکه حمله کرده، به اهداف خود دست می‌یابد.

امروزه با توجه به افزایش بی‌شمار حملات و با توجه به اینکه کراکرها از هر فرصتی برای سوء استفاده بهره می‌برند، مدیران سازمان‌ها باید تمهیدات ویژه‌ای برای حفظ و حراست از اطلاعات خود داشته باشند. دسته‌ای از افراد و سازمان‌ها متخصصان حوزه امنیت هستند و فعالیت آنها تست نفوذ و آسیب‌پذیری سیستم‌ها و شبکه‌های رایانه‌ای است. کارشناس تست نفوذ و آسیب‌پذیری یکی از مشاغلی است که در حوزه امنیت اطلاعات وجود دارد و سازمان‌های بی‌شماری درصدد استخدام این افراد هستند.

کارشناسان تست نفوذ یا هکرهای قانونمند مراحلی را که کراکرها برای نفوذ به سیستم‌ها انجام می‌دهند، طی می‌کنند و نتایج کار خود را در قالب گزارشی از آسیب‌پذیری‌های موجود در آن سیستم یا شبکه به مدیران آن سازمان تحویل می‌دهند. در تست آسیب‌پذیری امنیت زیرساخت‌ها و نرم‌افزارها، فازهایی که یک هکر اخلاقی انجام می‌دهد به‌صورت زیر است:



فاز۱: جمع‌آوری اطلاعات

معمولاً گام اول در حملات، جمع‌آوری اطلاعات است و Footprinting نامیده می‌شود. در این فرایند، هکر قانونمند با استفاده از ابزارهای متعدد، تا جایی که امکان دارد در مورد سازمان مورد هدف، اطلاعات کسب می‌کند. جمع‌آوری اطلاعات به دو روش انجام می‌شود:

ـ **شناسایی غیرفعال:** هکر در این روش به‌صورت نامحسوس مشغول جمع‌آوری اطلاعات می‌شود و شناسایی وی بسیار مشکل است. برای مثال هکر با زیر نظر گرفتن محل کار فرد مورد هدف، از زمان ورود و خروج وی مطلع می‌شود و یا با جست‌وجو در اطلاعات اینترنتی طرف مقابل، اطلاعاتی از وی به‌دست می‌آورد.

ـ **شناسایی فعال:** هکر به کاوش شبکه برای کشف رایانه‌های افراد، آدرس‌های IP و منابع شبکه می‌پردازد. در این روش ممکن است ردپای هکر در شبکه بماند و شناسایی شود.

معمولاً اطلاعاتی که در این مرحله به‌دست می‌آید شامل محدوده آدرس IPهای هدف، نام دامنه، اطلاعات کارکنان سازمان، شماره تلفن‌ها و مواردی از این قبیل است. یکی از تکنیک‌های رایج در زمینه جمع‌آوری اطلاعات، استفاده از موتور جست‌وجوی گوگل است که Google Hacking نام دارد.

فعالیت منزل

در رابطه با Google Hacking تحقیق کنید.

کارگاه ۱ جمع آوری اطلاعات از تارنما

هر فردی که قصد دارد یک دامنه برای تارنمای خود به ثبت برساند، باید مشخصات خود را به عنوان صاحب آن دامنه ثبت کند. این اطلاعات در یک بانک اطلاعاتی جامع ثبت می‌شود و در اختیار تمام کاربران قرار دارد و هر کاربر اینترنت قادر به مشاهده اطلاعات مدیر یا صاحب دامنه تارنما است. این اطلاعات شامل نام و نام خانوادگی، شماره تلفن و نمابر، نشانی پستی شرکت، رایانامه، تاریخ ثبت، تاریخ انقضای دامنه و... است. جهت مشاهده این اطلاعات از ابزار Whois استفاده می‌کنیم.

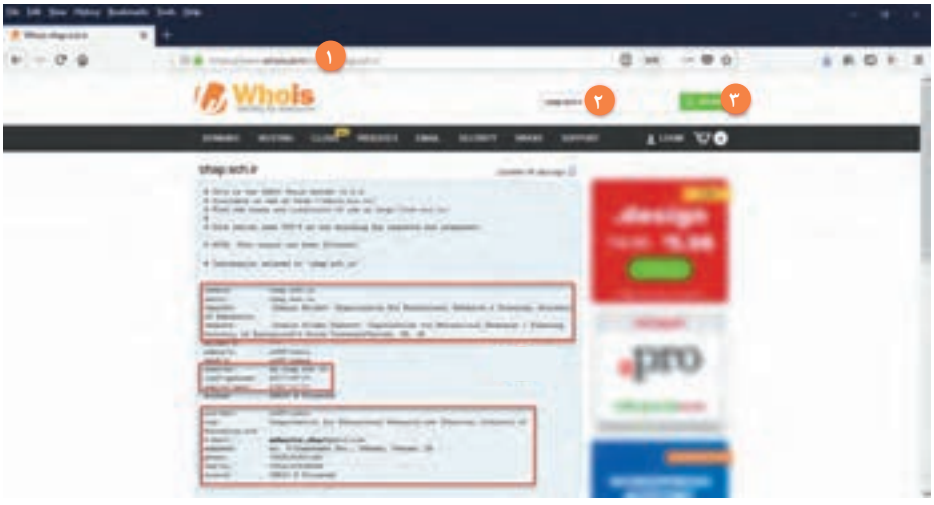
۱ در مرورگر نشانی https://www.whois.com را وارد کنید.

۲ تارنمای هدف را تعیین کنید.

درکادر جست‌وجو، نشانی تارنمای www.chap.sch.ir را وارد کنید.

۳ اطلاعات تارنمای هدف را مشاهده کنید.

روی دکمه Whois کلیک کنید. مشخصات صاحب دامنه، نشانی، نشانی رایانامه، شماره تلفن و تاریخ انقضای تارنما را به خاطر بسپارید (شکل ۲).



شکل ۲ــ تارنمای Whois

پژوهش

کاربرد تارنمای ripe.net و arin.net چیست؟

۴ آدرس سرویس‌دهنده تارنمای هدف را به دست آورید.

با استفاده از دستور nslookup می‌توان با داشتن Host Name یک کاربر یا تارنما، آدرس IP آن را پیدا کرد. این دستور به مدیران شبکه امکان تست و رفع اشکال سرویس DNS را می‌دهد. با دستور nslookup و استفاده از اطلاعات به‌دست آمده از Whois می‌توان آدرس سرویس‌دهنده‌ها را پیدا کرد.

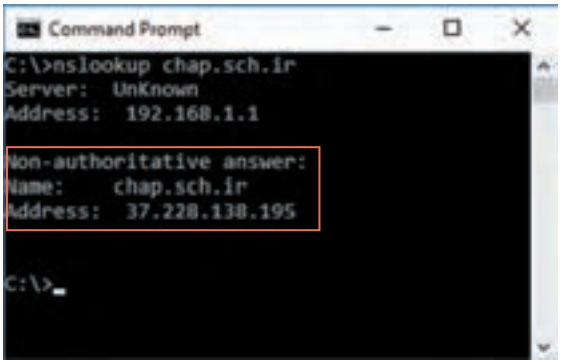
پنجره CMD را باز کرده، دستور nslookup chap.sch.ir را اجرا کنید. آدرس IP به‌دست آمده را یادداشت کنید (شکل ۳).

کنجکاوی

اجرای دستور nslookup به تنهایی چه کاربردی دارد؟

جدول ۲ــ پارامترهای کاربردی دستور nslookup

پارامتر	کاربرد
Ls	نمایش اطلاعات مربوط به DNS Domain به‌صورت فهرست
a	فهرست کردن نام و نام مستعار برای میزبان مورد نظر
d	فهرست کردن تمام رکوردها
t TYPE	فهرست کردن رکوردهای یک نوع مشخص
exit	خروج از دستور nslookup



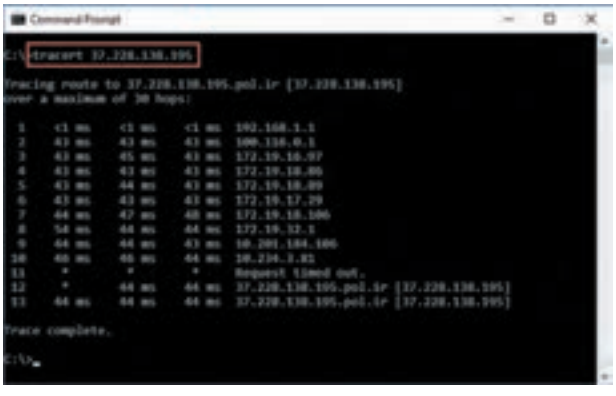
شکل ۳ــ اجرای دستور nslookup در محیط CMD

پژوهش

تفاوت دستور ping و nslookup چیست؟

۵ مسیر رسیدن به سرویس‌دهنده تارنمای هدف را تعیین کنید.

با استفاده از دستور tracert می‌توان مسیر رسیدن به آدرس IP هدف و آدرس مسیریاب‌های میانی را پیدا کرد.



شکل ۴ــ اجرای دستور tracert در محیط CMD

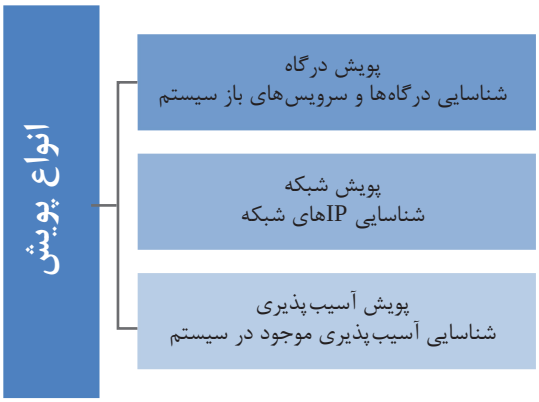
از مشکلات این دستور امکان وجود فایروال در میانه راه و عدم اجازه عبور بسته‌های tracert است.

در پنجره CMD آدرس IP به‌دست آمده از مرحله ۴ را وارد کنید (شکل ۴).

تا اینجا اطلاعاتی در مورد هدف پیدا شد، البته ابزارهای متعددی در این زمینه وجود دارد که می‌توان با جست‌وجو در اینترنت آنها را یافت. پس از پیدا کردن اطلاعاتی در مورد هدف، باید اطلاعات تکمیلی را با استفاده از ابزارهای پویش به‌دست آورد.

فاز ۲: پویش (Scanning)

در این مرحله هکر از اطلاعات به‌دست آمده از مرحله قبل برای پیدا کردن نقاط ضعف شبکه استفاده می‌کند. هکر به راحتی می‌تواند با ابزارهای موجود در این بخش به نقاط آسیب‌پذیر هدف دست پیدا کند (شکل ۵).



شکل ۵ــ انواع پویش

پویش درگاه

دانا در شهر تهران است و با کوشا در شهر شیراز در ارتباط است. دانا در حال ارسال چند پرونده برای کوشا است و هم زمان با او چت هم می‌کند. در این حالت دو برنامه به‌صورت هم‌زمان بین یک مبدأ و مقصد در حال اجرا است. برای تفکیک داده‌های ارسالی از هر برنامه، مفهومی به نام درگاه (port) مطرح می‌شود. به عبارتی درگاه یک آدرس مجازی برای برنامه‌های مبتنی بر شبکه است و یک شماره بین ۱ تا ۶۵۵۳۵ برای هر برنامه اختصاص می‌یابد. بنابراین اطلاعات هر برنامه‌ای که بین مبدأ و مقصد رد و بدل می‌شود با داده‌های درگاه‌های دیگر تداخل پیدا نمی‌کند. دانا برای ارسال پرونده‌ها از درگاه شماره ۲۰ استفاده می‌کند و روی درگاه شماره ۱۹۴ با کوشا چت می‌کند.

کنجکاوی

جدول روبه‌رو را با مراجعه به کتاب همراه هنرجو کامل کنید.

شماره درگاه	کاربرد (سرویس)
۸۰	
۸۲۹۱	
۲۳	
۲۲	
۴۴۳	
۵۳	
۲۱	

یکی از نقاط آسیب‌پذیر در سیستم‌های رایانه‌ای، درگاه‌های باز و نداشتن نظارت روی آنها است. اگر درگاهی باز باشد، هکر می‌تواند از طریق این درگاه باز به کل سیستم نفوذ کرده، آن را مختل کند. بنابراین باید از بسته بودن درگاه‌هایی که استفاده نمی‌شوند، اطمینان حاصل کرد.

کارگاه ۲ پویش درگاه سیستم هدف

Net Tools 5 یکی از ابزارهای جامع برای پویش است. در این کارگاه فقط قصد داریم از ابزار پویش درگاه در این نرم‌افزار استفاده کنیم. پس از نصب برنامه، مراحل زیر را انجام دهید:

۱ **برنامه Net Tools 5 را اجرا کنید.**

۲ **فرمان پویش درگاه را اجرا کنید.**

از منوی Start گزینهٔ Network Tools و پس از آن گزینهٔ Port Scanner را انتخاب کنید (شکل ۶).

۳ **آدرس IP هدف و درگاه‌ها را برای پویش تعیین کنید.**

در پنجره Port Scanner، آدرس IP هدف و محدوده شماره درگاه‌های موردنظر برای پویش را وارد کنید (شکل ۶).

۴ **درگاه‌های IP هدف را پویش کنید.**

شکل ۶ــ تعیین درگاه‌های باز هدف در ابزار Net Tools

روی دکمه Scan کلیک کنید. پس از چند دقیقه، تمام درگاه‌های باز فهرست می‌شوند.

۵ **درگاه‌های رایانه خود را پویش کنید.**

برای مشاهده درگاه‌های باز رایانه خود، آدرس IP سیستم هدف را 127.0.0.1 قرار دهید. همچنین می‌توانید در محیط CMD با دستور netstat فهرست درگاه‌های باز را مشاهده کنید.

نرم‌افزارهای زیادی برای پویش وجود دارند که قابلیت‌های مختلفی دارند. ممکن است دو ابزار پویش یک هدف را پویش کنند اما نتایج یکسانی ارائه ندهند.

پویش شبکه

با توجه به اینکه در مرحله جمع‌آوری اطلاعات، آدرس‌های IP هدف مشخص شد، در این فرایند دستگاه‌های فعال در شبکه شناسایی می‌شوند. منظور از دستگاه‌های فعال، رایانه‌ها یا دیگر دستگاه‌هایی است که آدرس IP دارند و در شبکه فعالیت می‌کنند.

کارگاه ۳ پویش آدرس‌های IP فعال (زنده) شبکه هدف

Ping Tester ابزاری است که برای مدیریت شبکه کاربرد فراوانی دارد، این ابزار واسط گرافیکی ساده و خوبی دارد و می‌توان دستورات ping و tracert را درون آن اجرا کرد. از قابلیت‌های کاربردی این ابزار می‌توان به موارد زیر اشاره کرد:

- پویش آدرس‌های IP به‌صورت تکی و گروهی
- زمان‌بندی برای انجام پویش
- تهیه خروجی به‌صورت پرونده متنی

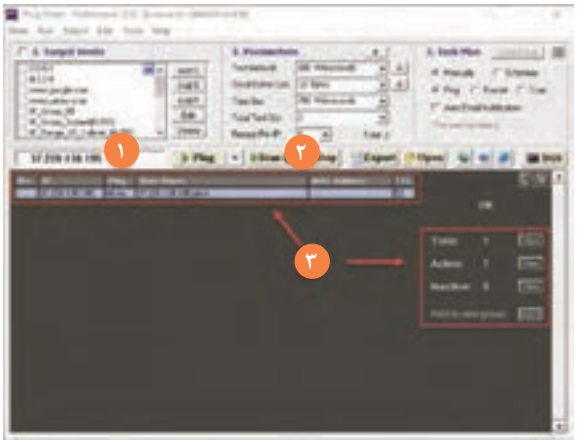
۱ پس از نصب ابزار Ping Tester آن را باز کنید.

۲ آدرس IP سیستم هدف را تعیین کنید.

در کادر مشخص شده، آدرس IP سیستم هدف را که در کارگاه شماره ۱ به‌دست آوردید، تایپ کنید (۱).

۳ آدرس IP هدف را پویش و نتیجه را مشاهده کنید.

دکمه Scan را کلیک کنید (۲). پس از چند ثانیه، گزارش پویش IP را مشاهده می‌کنید (شکل ۷). این آدرس IP فعال است و می‌توان روی آن تست نفوذ انجام داد.



شکل ۷ــ تعیین IPهای فعال در ابزار Ping Tester

ابزارهای دیگری مانند Angry IP Scanner، Softperfect Network Scanner و NMAP نیز وجود دارند که می‌توانند IPهای فعال را در شبکه هدف شناسایی کنند و یک نقشه کلی از شبکه هدف ارائه دهند.

پویش آسیب‌پذیری‌ها

یکی از مهم‌ترین مراحل در شناسایی و پویش سیستم هدف، پویش آسیب‌پذیری است. پس از پیدا شدن آسیب‌پذیری‌های سیستم هدف، با انتخاب یک حمله متناسب با آسیب‌پذیری‌ها می‌توان به سیستم نفوذ کرد. ابزارهای متعددی برای این منظور وجود دارد، یکی از ابزارهای پرکاربرد و قوی در این زمینه ابزار Acunetix است که روی پویش آسیب‌پذیری تارنماها متمرکز است. پس از نصب این ابزار، واسط گرافیکی ابزار روی صفحه تارنما باز شده، تست نفوذ را آغاز می‌کنیم.

فیلم

فیلم شماره ۱۲۲۲۷: پویش آسیب‌پذیری با ابزار Acunetix

علاوه بر ابزار Acunetix، می‌توانید از ابزارهای متنوعی مانند Retina، Nessus، Nagios و ابزارهای دیگری استفاده کنید.

فعالیت گروهی

با استفاده از ابزار Acunetix تارنمای chap.sch.ir را پویش کنید و گزارش پویش را در قالب PDF آماده کنید، سپس با گزارش گروه‌های دیگر مقایسه کنید.

فاز ۳: ایجاد و حفظ دسترسی (حمله)

پس از اینکه هکر از طریق ابزارهای پویش، نقاط آسیب‌پذیر یک سیستم را تشخیص داد، حمله واقعی خود را آغاز می‌کند. پس از دسترسی به سیستم هدف، باید برای اجرای حملات بعدی، دسترسی خود را حفظ کرد. برای این کار از Backdoorها استفاده می‌شود.

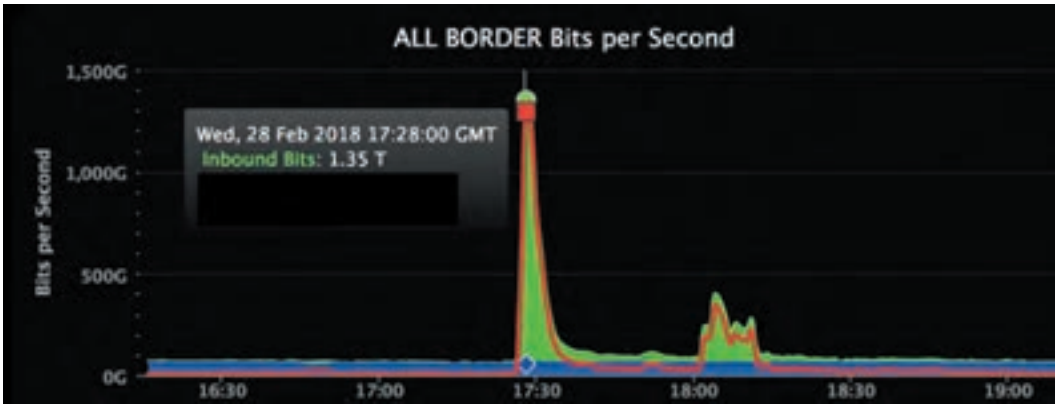
Backdoor نقاطی در برنامه است که امکان دستیابی به یک سیستم را بدون بررسی و کنترل امنیتی فراهم می‌کند. ممکن است به دلیل ضعف برنامه‌ها چنین نقاطی در برنامه وجود داشته باشد. همچنین نفوذگر می‌تواند با ارسال یک بدافزار در قالب رایانامه و... شما را به نصب آن برنامه روی سیستم خود ترغیب کند. بدین ترتیب یک درگاه برای خود باز کرده، از آن طریق وارد سیستم کاربر می‌شود. برای جلوگیری از این حمله باید از ابزارهای امنیتی کامل و جامع استفاده کرد و از نصب برنامه‌های ناشناخته جلوگیری کرد.

حملات DoS و DDoS

در حملات DoS (Denial of Service)، هدف هکر ایجاد اختلال و یا قطع سرویس‌دهی سرور به کاربران است. برای مثال دانشجویان برای مشاهده نمره امتحان خود به تارنمای دانشگاه رجوع می‌کنند. اکنون اگر هکر بتواند دسترسی دانشجویان به سرور را قطع کند، طوری که دانشجویان نتوانند به تارنما وصل شوند، حمله هکر موفقیت‌آمیز بوده است. هکر می‌تواند شروع به ارسال ترافیک با حجم بالا به سمت سرور کند و به قدری سرور را درگیر جواب دادن به این ترافیک کند که سرور توان پاسخ دادن به کاربران مجاز را نداشته باشد!

نوع دیگر این حمله، حمله DDoS است. در این حالت هکر به جای ارسال ترافیک تنها از یک سیستم، از چندین و شاید چندین هزار سیستم شروع به ارسال هم‌زمان ترافیک می‌کند. شاید این اتفاق برای شما نیز افتاده باشد، برای مثال ممکن است کاربران یک سیستم در یک زمان خاص، همه برای درخواست سرویس به سمت سرور ترافیک ارسال کنند. در این حالت اصطلاحاً سرور Crash می‌کند و از سرویس خارج می‌شود.

تارنمای محبوب GitHub که همهٔ کدنویسان آن را می‌شناسند، ۲۸ام فوریه ۲۰۱۸ در معرض گسترده‌ترین حمله DDoS جهان قرار گرفته است. در این حمله مهاجمان موفق شدند تا در هر ثانیه ۱۲۶٫۹ میلیون بسته ارسال کنند (شکل ۸).



شکل ۸ــ نمودار آمار ترافیک تارنمای GitHub

کارگاه ۴ شبیه‌سازی حمله DDoS در کارگاه رایانه

ابزار LOIC یکی از ابزارهای حمله DoS است. پس از نصب این برنامه روی تمام رایانه‌های کارگاه، می‌توان به‌طور هم‌زمان از همه رایانه‌ها شروع به ارسال بسته به سمت سیستم هدف کرد. مراحل زیر را روی تمام رایانه‌های کارگاه انجام دهید:

۱ برنامه LOIC را نصب و اجرا کنید.

پرونده نصب ابزار در لوح فشرده همراه کتاب موجود است. آن را روی رایانه خود نصب کنید. پس از نصب آن را اجرا کنید(شکل ۹).

۲ سیستم هدف را تعیین کنید.

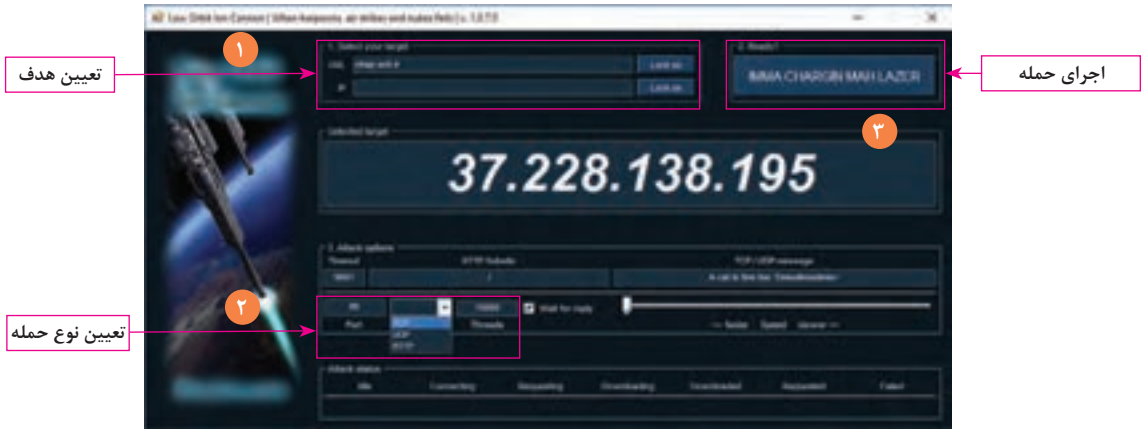
هدف ما تارنمای chap.sch.ir است. در قسمت انتخاب هدف نشانی این تارنما یا آدرس IP آن را وارد کرده، سپس دکمه Lock on را کلیک کنید. در کادر Selected Target آدرس IP هدف نمایش داده می‌شود (۱).

۳ نوع و پارامترهای حمله را تعیین کنید.

در کادر Attack Options باید نوع و پارامترهای حمله را تعیین کنید. قصد داریم یک حمله روی درگاه ۸۰ TCP انجام دهیم. در کادر Port عدد ۸۰ را بنویسید و TCP را درکادر Method انتخاب کنید. در کادر Threads باید تعداد جریان‌های ارتباطی با هدف را مشخص کنید، هرچه این عدد بزرگ‌تر باشد، سیستم هدف بیشتر درگیر خواهد شد و زودتر از پا در می‌آید. عدد ۱۵۰۰۰ یا بیشتر را در این کادر وارد کنید (۲).

۴ حمله را اجرا کنید.

برای شروع حمله، دکمه کادر Ready را کلیک کنید (شکل ۹). برای مشاهده بسته‌های ارسالی به سمت هدف، می‌توانید ابزار Wireshark را نصب کرده، ترافیک عبوری را مشاهده کنید.



شکل ۹ــ ابزار LOIC برای اجرای حمله DoS

تارنمای http://www.norse-corp.com گزارش لحظه‌ای از حملات را به صورت برخط در اختیار شما قرار می‌دهد. با بررسی حملات متوجه می‌شوید که چه حملاتی بیشترین تکرار را دارند و چه کشورهایی بیشتر مورد هدف هستند (شکل ۱۰).

شکل ۱۰ــ نمای حملات برخط در تارنمای norse-corp.com

فاز۴: پاک کردن ردپاها

آخرین فاز در حملات، پاک کردن ردپاها برای جلوگیری از شناسایی هکر است. هکرها روش‌های مختلفی برای پاک کردن آثار حمله و ردپای خود به‌کار می‌برند. یکی از معمول‌ترین روش‌ها، پاک کردن پرونده‌های Log در سرویس Event Viewer ویندوز است. علاوه بر این ابزارهای متعددی برای از بین بردن رد پاها وجود دارند که با جست‌وجو در اینترنت می‌توانید آنها را دریافت و آزمایش کنید.

پژوهش

برخی از ابزارهای پاک کردن پرونده‌های Log را از اینترنت جست‌وجو کرده، گزارش آن را در کلاس ارائه کنید.

جدول ارزشیابی شایستگی‌های غیرفنی، ایمنی، بهداشت و توجهات زیست‌محیطی

شایستگی‌ها	شرایط عملکرد (ابزار، مواد، تجهیزات، زمان، مکان و...)	نتایج ممکن	استاندارد (شاخص‌ها/داوری/نمره‌دهی)		نمره
شایستگی‌های غیرفنی	مسئولیت‌پذیری، ابراز تعهد به سازمان متبوع ـ مستندسازی، پایبندی به مستندسازی در نظام کنترل کیفیت ـ زبان فنی	قابل‌قبول	حفظ امانت در قبال اطلاعات سازمان یا افرادی که برای آنها تست نفوذ انجام می‌دهد ـ رعایت مصالح سازمانی و عرفی در فیلترینگ ـ سعه‌صدر و صبوری در برخورد با نارضایتی‌های کاربران در برابر محدودسازی دسترسی ـ تهیه پلان کلی از شبکه و دستگاه‌ها ـ ثبت سیاست‌های اعمال شده در فایروال ـ بازگرداندن تنظیمات به حالت اولیه پس از انجام تمرینات	۲	
ایمنی و بهداشت	اتصال صحیح جریان برق دستگاه فایروال ـ جلوگیری از مسدودسازی کلیه ارتباطات مدیر شبکه به دستگاه فایروال				
توجهات زیست‌محیطی		غیرقابل قبول	توجه به ایمنی و بهداشت محیط کارگاه	۱	
نگرش	دقت در نوشتن رول‌های فایروال و تنظیم آدرس‌ها در فیلترینگ فایروال‌ها				
* این شایستگی‌ها در ارزشیابی پایانی واحد یادگیری باید مورد توجه قرار گیرند.					

ارزشیابی مرحله ۱

مراحل کار	شرایط عملکرد (ابزار، مواد، تجهیزات، زمان، مکان و ...)	نتایج ممکن	استاندارد (شاخص‌ها/داوری/نمره‌دهی)		نمره
کاوش شبکه و تارنما	مکان: کارگاه استاندارد رایانه تجهیزات: شبکه‌ای از رایانه‌ها که نرم‌افزارهای کاوش و تست نفوذ روی آنها نصب باشد. زمان: ۴۵ دقیقه	بالاتر از حد انتظار	جمع‌آوری اطلاعات یک تارنمای خاص و آدرس IP آن ـ پویش محدوده مشخصی از درگاه‌ها ـ پویش شبکه در مدت زمان معین و تهیه گزارش متنی ـ پویش آسیب‌پذیری‌های تارنما و تهیه گزارش و یافتن حمله مناسب برای هر نوع آسیب‌پذیری	۳	
		درحد انتظار	جمع‌آوری اطلاعات یک تارنمای خاص و آدرس IP آن ـ پویش محدوده مشخصی از درگاه‌ها ـ پویش شبکه در مدت زمان معین و تهیه گزارش متنی ـ پویش آسیب‌پذیری‌های تارنما و تهیه گزارش	۲	
		پایین‌تر از حد انتظار	جمع‌آوری اطلاعات یک تارنمای خاص و آدرس IP آن	۱	

فایروال (Firewall)

چرا مأموران ایست بازرسی در فرودگاه یا جاده مسافران را مورد بازرسی قرار می‌دهند؟
چه لزومی دارد که اطلاعاتی که در شبکه رد و بدل می‌شوند، بازرسی شوند؟
چگونه می‌توان روش بازرسی در فرودگاه را در سیستم‌های رایانه‌ای و شبکه پیاده کرد؟
لزوم بازرسی کالاها در گمرک چیست؟

دنیای اینترنت بسیار ناامن است و هر لحظه امکان دارد به‌وسیله فرد یا گروهی هک شویم؛ بنابراین متخصصان حوزه امنیت راهکارهایی برای جلوگیری از حملات و تهدیدات ارائه داده‌اند.

- یکی از سرویس‌های تشخیص حملات، سرویس IDS (Intrusion Detection Systems) نام دارد. این سرویس عموماً با یک سرویس دیگر برای جلوگیری از حملات همراه است که IPS (Intrusion Prevention Systems) نامیده می‌شود. سرویس IDS با توجه به پایگاه داده‌ای که از الگوی حملات دارد قادر به شناسایی انواع حملات و سرویس IPS قادر به جلوگیری و خنثی کردن حملات است.
- یکی دیگر از سرویس‌های مهم برای جلوگیری از حملات در شبکه‌ها، آنتی ویروس و هرزنامه (Spam) است که از ورود ویروس‌ها و هرزنامه‌ها به شبکه و سیستم‌ها جلوگیری می‌کنند.
- یکی از سرویس‌های بسیار مهم که در تمامی سیستم‌ها و شبکه‌ها وجود دارد، سرویس فایروال (Firewall) است. این سرویس توانایی‌های زیادی در جلوگیری از ورود بسته‌های مشکوک به شبکه دارد و به دلیل مقبولیت زیاد در بین سازمان‌ها مورد استفاده بسیاری از سازمان‌ها است. به همین خاطر یکی از فرصت‌های شغلی برای افراد فعال در حوزه امنیت، نصب و پیکربندی فایروال است.

همان‌طور که در جامعه باید امنیت حاصل شود، در سیستم‌های رایانه‌ای هم باید تبادل اطلاعات بین رایانه‌ها بازبینی شود تا اطمینان از سلامت ارتباطات حاصل شود.

برای بازبینی بسته‌های اطلاعاتی در سیستم‌های رایانه‌ای و شبکه‌ها از فایروال استفاده می‌شود. فایروال سرویسی است که به‌صورت نرم‌افزاری یا سخت‌افزاری ارائه می‌شود و سیستم‌های رایانه‌ای را از دسترسی نفوذگران محافظت کرده، تمام بسته‌های عبوری را بررسی می‌کند و در صورت تشخیص غیرمجاز بودن بسته، از ورود آن به شبکه جلوگیری می‌کند.

فایروال نرم‌افزاری مثل بقیه نرم‌افزارها روی سیستم‌عامل نصب می‌شود. به بررسی بسته‌ها به‌وسیله فایروال، فیلترکردن بسته‌ها می‌گویند. هزینه این نوع فایروال کم است و به آسانی به‌وسیله کاربر قابل تنظیم و راه‌اندازی است. فایروال ویندوز، نرم‌افزارهای ISA Server و Kerio Control و برخی از نرم‌افزارهای آنتی‌ویروس نمونه‌ای از فایروال نرم‌افزاری هستند.

فایروال‌های سخت‌افزاری روی بردهای سخت‌افزاری پیاده‌سازی شده، در قالب یک سخت‌افزار مستقل عرضه می‌شوند (شکل ۱۱). این نوع فایروال‌ها تنظیمات پیشرفته‌تری نسبت به نوع نرم‌افزاری دارند و برای شبکه‌های بزرگ استفاده می‌شوند و بار ترافیکی کمتری روی شبکه دارند؛ اما در عوض هزینه آنها بیشتر است و باید یک متخصص شبکه آن را پیکربندی و آزمایش کند. سرویس فایروال مسیریاب میکروتیک از این نمونه است.

شکل ۱۱ــ یک نمونه فایروال سخت‌افزاری

کنجکاوی

یک آموزشگاه رایانه با سه کارگاه را در نظر بگیرید که مدرسان به‌صورت مستقل در این کارگاه‌ها تدریس می‌کنند. به دلیل اتصال هنرجویان به اینترنت، حجم اینترنت مدرسه زودتر از موعد تمام می‌شود و دسترسی به اینترنت در برخی روزها در هنگام تدریس قطع می‌شود و همین‌طور بیشتر سیستم‌ها ویروسی می‌شوند و مسئول آموزشگاه همیشه مشغول نصب ویندوز است. آیا با نصب فایروال در این آموزشگاه، مشکل حل می‌شود؟ اگر پاسخ شما بلی است، چه نوع فایروالی را پیشنهاد می‌دهید؟ چرا؟

انواع فایروال بر اساس فیلترینگ

در این بخش سه نوع بسیار مهم و کاربردی فایروال‌ها را بررسی می‌کنیم:

Packet Filter ـ

این فایروال‌ها با استفاده از مجموعه‌ای از قوانین که برای آنها تعریف می‌شوند، بسته‌های ورودی و خروجی را بررسی می‌کنند و تصمیم می‌گیرند که بسته را عبور دهند یا دور بیندازند. به این قوانین، رول (Rule) می‌گویند. رول‌های فایروال براساس اطلاعات زیر نوشته می‌شوند:

- نوع پروتکل
- آدرس IP مبدأ
- شماره درگاه مبدأ
- آدرس IP مقصد
- شماره درگاه مقصد
- رابط کارت شبکه (اینترفیس)

در این فایروال‌ها تعدادی رول پشت سر هم نوشته شده است که هر بسته ورودی از ابتدای فهرست با تک تک رول‌ها مطابقت داده می‌شود و به محض اینکه با یک رول تطابق داشته باشد، بر اساس آن رول یا عبور داده می‌شود و یا دور انداخته می‌شود. بنابراین رول‌های بعدی بررسی نخواهند شد.

از مزایای این فایروال‌ها می‌توان به سادگی کار با آن و سرعت عملکرد آن اشاره کرد؛ زیرا درگیر پردازش محتوای بسته‌ها نمی‌شوند. در عوض در شناسایی بسیاری از حملات اینترنتی ضعیف هستند و توانایی مسدودسازی اکثر اپلیکیشن‌ها را ندارند. یک نمونه از این فایروال‌ها، فایروال‌های شخصی نام دارند که روی سیستم‌عامل کاربر و سرورها نصب می‌شوند. فایروال ویندوز و برنامه‌های آنتی‌ویروس نسخه Internet Security نمونه‌ای از فایروال شخصی هستند.

Stateful Firewall ـ

این نوع فایروال که به فایروال حالت‌مند هم معروف است به شیوه دقیق‌تری کار می‌کند. عملکرد این فایروال به این صورت است که در حافظه cache خود یک جدول وضعیت بسته دارد. برای هر بسته علاوه بر آدرس IP، درگاه و نوع پروتکل یک فیلد دیگر به نام state در نظر گرفته می‌شود. این نوع فایروال علاوه بر مواردی که در فایروال Packet Filter مطرح شد با بررسی حالت‌های مختلف بسته‌ها، به راحتی قادر به اعمال فیلترینگ روی ارتباطات و برنامه‌ها است. این کار مدت زمان بیشتری برای بررسی تمام بسته‌ها لازم دارد در عین حال امنیت بیشتری در پی دارد و قیمت آن نیز گران‌تر است.

در نظر بگیرید شما در شبکه داخلی هستید و قصد دارید در فایروال رولی بنویسید که سرویس‌گیرنده‌های شبکه داخلی بتوانند بسته‌های TCP را به شبکه خارجی ارسال کنند؛ اما هیچ کس از طرف شبکه خارجی به شبکه داخلی

نتواند بسته TCP ارسال کند. حال اگر درون فایروال رولی بنویسید که «تمام بسته‌هایی که از سمت شبکه خارجی به داخل شبکه می‌آیند را فیلتر کن» تصور می‌شود که به خواسته خود می‌رسید اما زمانی که کاربران شبکه داخلی بسته TCP ارسال می‌کنند، شبکه خارجی نمی‌تواند جواب این بسته‌ها را به ما برگرداند چون بسته‌های TCP از سمت شبکه خارجی به شبکه داخلی را فیلتر کرده‌ایم. این مشکل به‌وسیله Packet Filter Firewall قابل حل نیست و حتماً باید از Stateful Firewall استفاده کرد.

ـ Application Proxy Firewall

سرویس پراکسی یک سرویس میانجی است که هم می‌تواند به‌صورت نرم‌افزاری روی رایانه کاربر نصب شود و واسطه‌ای بین کاربر و شبکه باشد، هم می‌تواند روی یک رایانه مستقل نصب شود و بین شبکه داخلی و خارجی قرار گیرد که در این صورت پراکسی سرور نامیده می‌شود.

کاربران برای دسترسی به شبکه خارجی، درخواست‌های خود را به پراکسی سرور ارسال می‌کنند و پراکسی پس از ارسال درخواست به شبکه خارجی و برگشت پاسخ، نتیجه را برای کاربر ارسال کرده، در حافظه cache خود نیز نگهداری می‌کند تا در صورت درخواست مجدد از سوی کاربران، بلافاصله از آن استفاده کند؛ بنابراین امکان تهیه گزارش از ارتباطات کاربران با شبکه خارجی فراهم شده، سرعت پاسخگویی به کاربران و امنیت شبکه داخلی افزایش می‌یابد. Application Proxy Firewall نیز عملکردی مشابه دارد و نسبت به Packet Filter امن‌تر است. به جای بررسی ترافیک‌های مجاز یا ممنوع از روی آدرس IP و درگاه، فقط برنامه‌های مجاز را بررسی می‌کند. به دلیل اینکه این فایروال روی اپلیکیشن‌ها تمرکز دارد نام Application level Gateway به آن اطلاق می‌شود. همچنین این فایروال به‌صورت پراکسی نیز عمل می‌کند و پیش از برقراری ارتباط بین سرویس‌گیرنده و سرویس‌دهنده راه دور، در میان آنها قرار گرفته، اپلیکیشن‌ها را مدیریت می‌کند. یکی از محاسن این فایروال‌ها توانایی cache کردن اطلاعات است بنابراین سرعت پاسخگویی در شبکه بالا می‌رود. همچنین آدرس IP مبدأ بسته نیز مخفی است و به همین خاطر امنیت بیشتری خواهند داشت. فایروال‌های سرویس وب WAF(Web Application Firewall) از این دسته هستند و وظیفه آنها بررسی ترافیک اپلیکیشن‌های وب است.

فیلم

پویانمایی شماره ۱۲۲۲۸: انواع فایروال

پژوهش

درباره فایروال‌های Next_Generation تحقیق کنید.

فایروال نرم‌افزاری

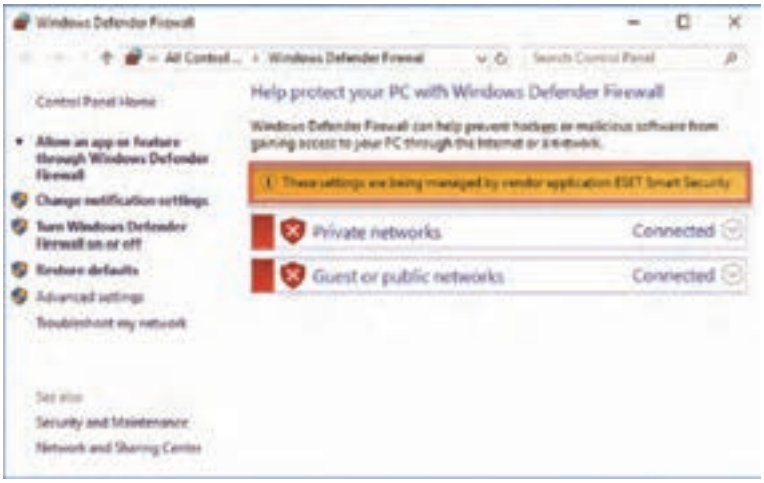
متداول‌ترین فایروال نرم‌افزاری فایروال ویندوز است. روش فیلترینگ در این فایروال از نوع Packet Filter است.

کارگاه ۵ فعال‌سازی فایروال سیستم عامل

فعال بودن فایروال ویندوز، امنیت رایانه شما را چندین برابر افزایش خواهد داد. پیش از فعال‌سازی آن باید این نکته را مدنظر داشته باشید که در صورت نصب آنتی‌ویروس‌های نسخه Internet Security، فایروال ویندوز غیرفعال شده، آنتی‌ویروس نقش فایروال را ایفا می‌کند. برای کار کردن با فایروال ویندوز ابتدا باید فایروال آنتی‌ویروس را غیر فعال کرد.

۱ بررسی کنید کدام یک از فایروال‌های ویندوز یا آنتی‌ویروس فعال هستند.

برای تغییر تنظیمات فایروال وارد کنترل پَنل شده، Windows Defender Firewall را انتخاب کنید (شکل ۱۲).



شکل ۱۲ــ صفحه اصلی تنظیمات فایروال ویندوز

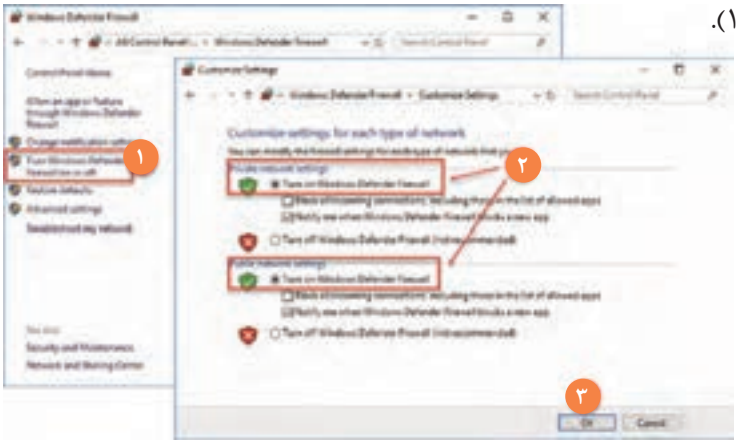
۲ فایروال آنتی‌ویروس را غیرفعال کنید.

وارد تنظیمات آنتی‌ویروس شده، پس از فشردن کلید F5 گزینه Personal Firewall را انتخاب کنید (۱). از فهرست بازشو گزینه System Integration را انتخاب کنید (۲). گزینه personal firewall is completely disabled را از بخش System Integration انتخاب کنید (۳). پس از کلیک دکمه OK امکان فعال کردن فایروال ویندوز وجود دارد (شکل ۱۳).

شکل ۱۳ــ غیرفعال کردن فایروال نرم‌افزار NOD32

۳ فایروال ویندوز را فعال کنید.

مانند مرحله ۱ پنجره تنظیمات فایروال را باز کرده، گزینه Turn windows Defender firewall on or off را انتخاب کنید (۱). هر دو گزینه Private Network و Public Network را روی Turn on تنظیم کنید (۲). روی دکمه OK کلیک کنید (شکل ۱۴).



شکل ۱۴ــ فعال کردن فایروال ویندوز

پژوهش

برای فعال و غیرفعال کردن فایروال ویندوز در محیط CMD چه باید کرد؟

جریان‌های ورودی و خروجی در فایروال

جریان بسته‌های خروجی از رایانه به سمت خارج از شبکه را ترافیک خروجی (Outbound Traffic) می‌نامند و جریان بسته‌های ورودی از شبکه بیرونی به سمت رایانه را ترافیک ورودی (Inbound Traffic) می‌نامند (شکل ۱۵).

شکل ۱۵ــ انواع جریان‌ها در فایروال

فایروال ویندوز این توانایی را دارد که روی هر دو نوع ترافیک مدیریت انجام داده، آن را مورد ارزیابی قرار دهد.

برای مشاهده رول‌های فایروال، در کنترل پنل پس از باز کردن Firewall روی گزینه Advanced Setting کلیک کنید.

دو نوع رول مشاهده می‌شود که Inbound Rules قوانین مربوط به ترافیک ورودی و Outbound Rules قوانین مربوط به ترافیک خروجی است (شکل ۱۶).

شکل ۱۶ــ انواع رول‌ها در فایروال

پژوهش

قسمت Connection Security Rules برای چه نوع ارتباطاتی کاربرد دارد؟

فعالیت کارگاهی

با توجه به نوع ارتباطات، جدول زیر را کامل کنید.

نوع درخواست	نوع Rule
هیچ رایانه‌ای از اینترنت نتواند به این سیستم دسترسی پیدا کند.	Inbound
روی این سیستم تارنمای گوگل فیلتر شود	
	Outbound
	Inbound

پروفایل‌ها در فایروال

هنگامی که برای اولین بار به یک شبکه متصل می‌شوید، پنجره Set Network Location ظاهر می‌شود و از شما می‌خواهد که نوع Location خود را مشخص کنید. با این انتخاب به‌Firewall اعلام می‌کنید که در حال حاضر به چه شبکه‌ای متصل شده و باید چه تنظیمات امنیتی را به کار ببرد (شکل ۱۷).

شکل ۱۷ــ پنجره Set Network Location

Home Network: هنگامی استفاده می‌شود که شما تمامی کاربران شبکه را می‌شناسید و اطمینان دارید که افراد مطمئنی هستند. در این حالت File Sharing فعال می‌شود، دسترسی به منابع اشتراکی بدون نیاز به گذرواژه فراهم می‌شود و به‌وسیله دیگر سرویس‌گیرنده‌های شبکه دیده می‌شوید.

Work Network: عملکرد این حالت هم مانند حالت قبلی است اما میزان اعتماد به کاربران کمتر است و احتمال حمله به سیستم شما ممکن است به میزان کمی افزایش یابد.

Public Network: در صورت اتصال به شبکه عمومی، ویندوز محتاط‌تر عمل می‌کند چون این گزینه مربوط به مکان‌هایی است که قابل اعتماد نیستند و هرگونه کاربری ممکن است در شبکه عمومی وجود داشته

باشد. برای مثال زمانی که به شبکه فرودگاه متصل می‌شوید، باید شبکه عمومی را انتخاب کنید. در این حالت دسترسی به منابع اشتراکی فراهم نمی‌شود و در شبکه دیده نمی‌شوید.
حالت Home Network و Work Network چون از سطح امنیتی بالاتری برخوردار هستند با عنوان پروفایل Private شناخته می‌شوند و حالت Public Network با عنوان پروفایل Public شناخته می‌شود. بنابراین در هر رول باید مشخص کنیم که این رول روی چه شبکه‌ای اعمال شود. مثلاً ممکن است یک رول برای مسدودسازی دسترسی کاربران شبکه‌های عمومی و ناشناس به سیستم خود بنویسیم. از طرفی در شبکه خانگی خودمان، دوستان و افرادی که در Private Network ما هستند، بتوانند به سیستم ما وصل شوند. پس باید این رول را فقط برای شبکه Public بنویسیم.
در فایروال سه نوع پروفایل وجود دارد:

- **Domain**: زمانی که رایانه شما به دامنه‌ای متصل است.
- **Private**: زمانی که رایانه شما به شبکه‌ای خصوصی مانند «work» یا «home» متصل است.
- **Public**: زمانی که رایانه شما به یک شبکه عمومی مانند یک Wi_Fi Hotspot متصل شده یا مستقیماً به اینترنت متصل است.

یادداشت

تمام رول‌های ثبت شده درون فایروال را می‌توان بر اساس نیاز فعال یا غیر فعال کرد. برای مثال برخی مواقع نیاز دارید که به وسیله یک سرویس‌گیرنده دیگر در شبکه Public دیده شوید و پرونده به اشتراک بگذارید. در اینجا به جای غیرفعال کردن فایروال کافی است رول مربوط به این کار را درون فایروال پیدا کرده، آن را غیرفعال کنید.

فیلم

فیلم شماره ۱۲۲۲۹: مسدودسازی درگاه در فایروال ویندوز

فعالیت کارگاهی

در فایروال ویندوز رولی بنویسید که رایانه شما نتواند از DHCP Server کارگاه رایانه، آدرس IP بگیرد.

گزارش‌گیری(Log) از رخدادهای فایروال

گزارش‌گیری از فایروال یکی از کارهای مدیریتی مهم است که به شما اطلاعات بسیار مهمی می‌دهد:

- بررسی درستی رول‌هایی که اضافه شده‌اند و عیب‌یابی رول‌هایی که دچار مشکل شده‌اند.
- بررسی اینکه آیا فایروال باعث اختلال در نرم‌افزاری شده است یا خیر؟
- بررسی درگاه‌هایی که بسته شده‌اند و بسته‌هایی که حذف شده‌اند.
- بررسی اینکه درون شبکه، یک آدرس IP و یا گروهی از آدرس‌های IP در تلاش هستند به فایروال و یا قسمت‌های مهم دیگر دسترسی پیدا کنند یا خیر.

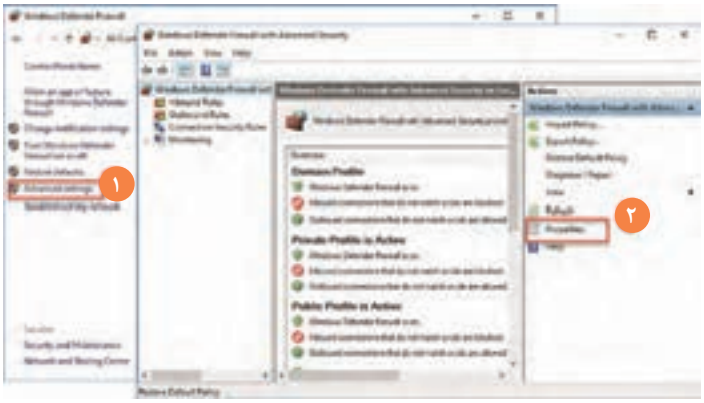
یادداشت

به طور پیش‌فرض قابلیت گزارش‌گیری فایروال ویندوز غیر فعال است، در صورت لزوم باید آن را تنظیم و فعال کنید.

کارگاه ۶ فعال‌سازی گزارش‌گیری فایروال ویندوز

۱ پنجره خصوصیات فایروال را بازکنید.

از کنترل پنل فایروال را باز کرده، از منوی سمت چپ گزینه Advanced Settings را انتخاب کنید (۱). سپس در پنجره باز شده، از سمت راست گزینه Properties را انتخاب کنید (شکل۱۸).



شکل ۱۸ـ خصوصیات فایروال

۲ به تنظیمات Logging وارد شوید.

در کادر باز شده، برای هر کدام از پروفایل های شبکه یک سربرگ مشاهده می‌شود. این مرحله را برای هر سه برگه اعمال کنید. در انتهای کادر در قسمت Logging روی دکمهٔ Customize کلیک کنید تا تنظیمات گزارش‌گیری نمایان شود (۲).

۳ اطلاعات گزارش را تنظیم کنید.

در کادر باز شده مسیر و نام گزارش را وارد کنید و در صورت تمایل حداکثر حجم پرونده گزارش را نیز مشخص کنید. در قسمت پایین این کادر در صورت انتخاب Yes برای گزینه Log dropped packets گزارش‌گیری برای بسته‌های حذف شده انجام می‌شود. در صورت انتخاب Yes برای گزینه Log successful connections گزارش‌گیری برای بسته‌هایی انجام می‌شودکه از فایروال عبور داده شده‌اند (شکل ۱۹).

شکل ۱۹ـ ایجاد Log از عملکرد فایروال

یادداشت

برای مشاهده پرونده Log باید با دسترسی Administrator آن را باز کنید.

۴ گزارش ایجاد شده را بررسی کنید.

ساختار پرونده Log از دو بخش تشکیل شده است. قسمت سرایند فیلدهای موجود در گزارش را مشخص می‌کند و قسمت بدنه گزارش، عملکرد فایروال را نشان می‌دهد. در این گزارش بسته‌های حذف شده و همین‌طور نوع بسته‌های ارسالی و بسته‌های دریافتی مشخص هستند (شکل ۲۰).

شکل ۲۰ـ محتویات پرونده Log

فعالیت گروهی

با توجه به رول‌هایی که تاکنون در فایروال نوشته‌اید، یک گزارش از عملکرد فایروال ایجاد کنید و نتایج آن را با پرونده گزارش گروه‌های دیگر مقایسه کنید و نتیجه را در کلاس بررسی کنید.

ارزشیابی مرحله ۲

مراحل کار	شرایط عملکرد (ابزار، مواد، تجهیزات، زمان، مکان و...)	نتایج ممکن	استاندارد (شاخص‌ها/داوری/نمره دهی)		نمره
استفاده از فایروال نرم‌افزاری	مکان: کارگاه استاندارد رایانه تجهیزات: شبکه‌ای از رایانه‌ها که نرم‌افزار فایروال روی آنها نصب باشد. زمان: ۳۰ دقیقه	بالاتر از حد انتظار	فعال و غیرفعال کردن فایروال نرم‌افزاری ـ ایجاد Ruleهای Inbound و Outbound بر اساس نیاز ـ مسدود کردن یک سرویس برای یک کاربر یا گروه خاص ـ فعال کردن گزارش‌گیری در فایروال	۳	
		در حد انتظار	فعال و غیرفعال کردن فایروال نرم‌افزاری ـ ایجاد Rule در قسمت‌های Inbound و Outbound بر اساس نیاز ـ مسدود کردن یک سرویس برای یک کاربر یا گروه خاص	۲	
		پایین‌تر از حد انتظار	فعال و غیر فعال کردن فایروال نرم‌افزاری	۱	

فایروال سخت‌افزاری

وظیفه اصلی فایروال مانند مأموران بازرسی در گیت‌های فرودگاه، کنترل ترافیک است.
با توجه به تهدیدات و حملاتی که روزافزون بوده و به‌صورت گسترده اتفاق می‌افتد، سازوکارهای دفاعی و محافظتی مختلفی در سطوح مختلف در شبکه اتخاذ می‌شود.

- اولین و ساده‌ترین سازوکار MAC Filtering است که دسترسی کاربران به شبکه را براساس مک آدرس آنها اعتبارسنجی می‌کند.
- در دید وسیع‌تر و جامع‌تر Packet Filtering و سازوکارهایی همچون IDS و IPS قرار می‌گیرند که براساس آدرس IP بسته‌ها تصمیم‌گیری می‌کنند که بسته به شبکه وارد شود یا خیر.
- به‌طور اختصاصی در سطح اپلیکیشن نیز فیلترینگ Stateful انجام می‌گیرد و مبنای فیلترینگ، وضعیت بسته‌ها است که یکی از قوی‌ترین انواع فیلترینگ است.
- دستگاه‌های UTM یکی از قدرتمندترین تجهیزات فعال در شبکه هستند که انواع فیلترینگ را انجام می‌دهند و علاوه بر آن سرویس‌هایی مانند Anti-Spam، AntiVirus، IPsec/VPN، IDPS و برخی سرویس‌های امنیتی دیگر را به‌صورت یکپارچه ارائه می‌دهند.

عملیات فیلترینگ در فایروال دو قسمت انجام می‌شود (شکل ۲۱):

شکل ۲۱ــ نمای کلی فایروال سخت‌افزاری

۱ در لبه ورودی و هنگام ورود بسته‌ها به فایروال
۲ در لبه خروجی و قبل از خروج بسته‌ها

سرویس فایروال یکی از مهم‌ترین سرویس‌های روی مسیریاب میکروتیک است که امکاناتی از قبیل موارد زیر را ارائه می‌دهد:

- فیلترینگ از نوع Stateful
- فیلترینگ اپلیکیشن
- فیلترینگ براساس آدرس IP و درگاه و اندازه و محتوای بسته

به همین دلیل بسیاری از نیازمندی‌های امنیتی مدیران شبکه سازمان‌ها و شبکه‌های کوچک و متوسط را برآورده می‌کند.

در فایروال میکروتیک مانند فایروال ویندوز دو نوع ترافیک ورودی و خروجی وجود دارد. در اینجا به هر یک از این نوع ترافیک‌ها یک زنجیره ترافیک یا chain گفته می‌شود (شکل ۲۲).

شکل ۲۲ــ زنجیره‌های ترافیک در فایروال

۱ Input Chain: حالتی است که ترافیک از سمت یک سرویس‌گیرنده یا شبکه می‌آید و به خود فایروال ختم می‌شود.

۲ Output Chain: حالتی است که مبدأ ترافیک فایروال است و به سمت یک سرویس‌گیرنده یا شبکه بیرونی ختم می‌شود.

در فایروال میکروتیک برخلاف فایروال ویندوز یک حالت دیگر وجود دارد که Forward Chain نامیده می‌شود.

۳ Forward Chain: حالتی است که ترافیک از یک شبکه یا سرویس‌گیرنده ارسال می‌شود و از درون فایروال عبور می‌کند و به مقصد خود می‌رسد.

فیلم

پویانمایی شماره ۱۲۲۳۰: انواع ترافیک در فایروال سخت‌افزاری

جایگاه فایروال در شبکه

ممکن است برای شما سؤال پیش بیاید که برای پیاده‌سازی صحیح و اصولی شبکه، فایروال باید در کجا قرار بگیرد؟ با توجه به نوع شبکه و هدف ما از قرار دادن فایروال در شبکه ممکن است فایروال در مکان‌های متفاوتی قرار بگیرد. در اینجا دو جایگاه بسیار مهم بررسی می‌شود:

۱ **لبه شبکه:** در این سناریو، فایروال برای محافظت از شبکه داخلی، بین شبکه خارجی و شبکه داخلی قرار می‌گیرد. این فایروال هم ترافیکی که از سمت خارج به شبکه داخلی می‌آید و هم ترافیکی که از سمت شبکه داخلی به سمت خارج می‌رود را کنترل می‌کند (شکل ۲۳).

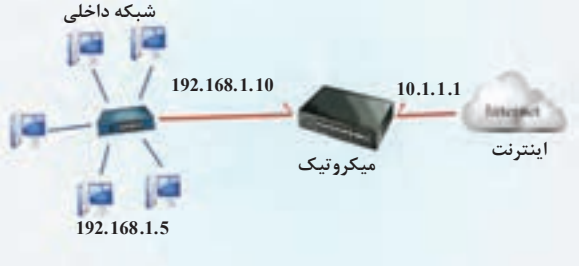
شکل ۲۳ـ محل قرارگیری فایروال بین شبکه داخلی و شبکه خارجی

شکل ۲۴ـ محل قرارگیری فایروال با تفکیک شبکه داخلی و سرورهای سازمان

۲ **بین سرورهای شبکه و شبکه داخلی:** عموماً از این سناریو برای تفکیک شبکه داخلی یک سازمان از قسمت سرورهای آن سازمان استفاده می‌شود. فایروال در اینجا وظیفهٔ تفکیک این دو شبکه و محافظت از هر دو را به عهده دارد (شکل ۲۴).

در این سناریو سرورهای سازمان به‌صورت اختصاصی در یک شبکه جدا قرار داده می‌شوند و بخش سرورها فقط پاسخگوی درخواست‌ها هستند و عموماً خود سرورها شروع‌کننده ارتباط نیستند. مزیت این سناریو این است که کاربرانی که از شبکه خارجی قصد سرویس‌گیری از سرورها را دارند وارد شبکه داخلی سازمان نمی‌شوند و امنیت شبکه داخلی بالاتر می‌رود. همچنین در برخی موارد حتی کاربران سازمان هم حق دسترسی به همه سرورها را ندارند و فقط مدیران شبکه و افرادی که آنها تعیین می‌کنند، می‌توانند به سرورها دسترسی داشته باشند.

برای اجرای کارگاه‌های بعدی نیاز به پیاده‌سازی سناریوی شبکه با میکروتیک داریم (شکل ۲۵).
اولین گام در ایجاد امنیت در شبکه برقراری امنیت خود میکروتیک است، برای این منظور باید روش‌های دسترسی به میکروتیک را کنترل کرد. یکی از روش‌های متداول دسترسی به میکروتیک از طریق برنامه WinBox است. برای ایجاد امنیت باید مشخص کنیم که چه کسانی اجازه اتصال از طریق WinBox به میکروتیک را دارند.



شکل ۲۵ـ سناریوی کاربردی پودمان

کارگاه ۷ مسدود کردن دسترسی از طریق WinBox به میکروتیک

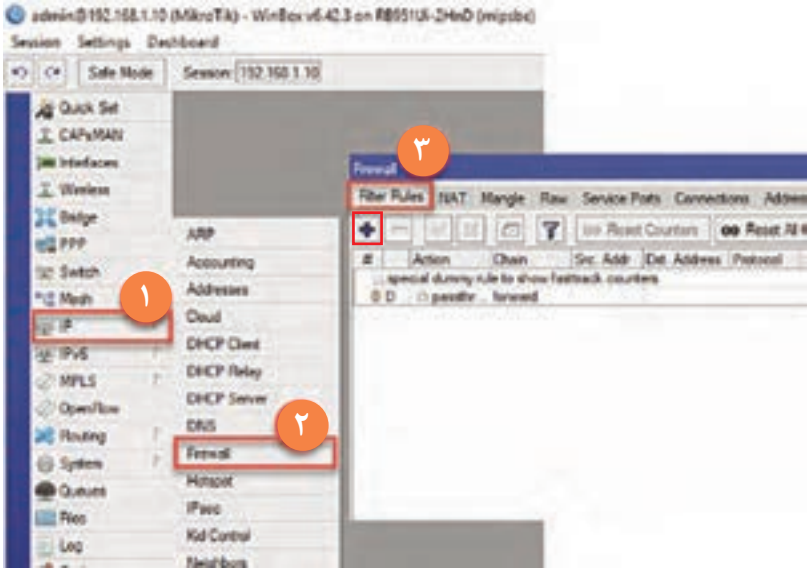
با توجه به سناریوی شکل ۲۵ قصد داریم روی فایروال میکروتیک تنظیماتی انجام دهیم که سرویس گیرنده‌های شبکه خارجی(اینترنت) نتوانند از طریق WinBox با مسیریاب میکروتیک ارتباط برقرار کنند. در شکل ۲۵ سرویس‌گیرنده‌های شبکه خارجی از طریق اینترفیس 10.1.1.1 مسیریاب می‌توانند با آن ارتباط داشته باشند. پس باید تنظیمات موردنظر را روی این اینترفیس انجام دهیم .

۱ به تنظیمات فایروال میکروتیک وارد شوید.

پس از باز کردن پنجره WinBox از منوی سمت چپ، گزینه IP را انتخاب کنید (۱). از منوی ظاهر شده Firewall را انتخاب کنید (۲).

۲ یک رول جدید ایجاد کنید.

روی سربرگ Filter Rules کلیک کرده (۳)، روی دکمه ➕ کلیک کنید (شکل ۲۶).



شکل ۲۶ـ ایجاد رول جدید در فایروال میکروتیک

۳ نوع chain را تعیین کنید.

سربرگ General را انتخاب کنید. مقصد ترافیک، خود میکروتیک است، پس گزینه Input را در مقابل Chain انتخاب کنید (۱).

۴ آدرس IP مقصد بسته‌های سرویس‌گیرنده‌های خارجی را تعیین کنید.

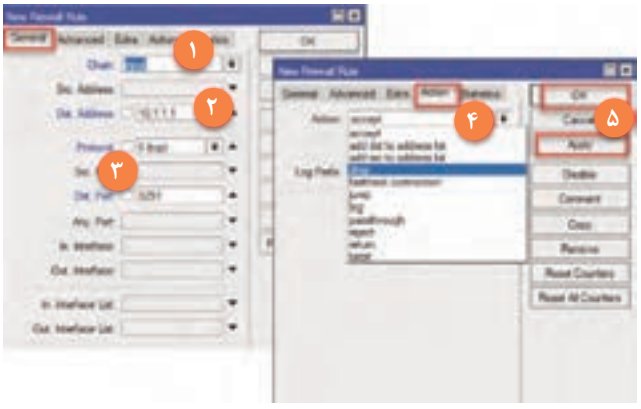
سرویس‌گیرنده‌های شبکه خارجی از طریق آدرس 10.1.1.1 می‌توانند با میکروتیک ارتباط برقرار کنند. پس آدرس مقصد بسته‌های آنها 10.1.1.1 خواهد بود. مقابل Dst.Address آدرس 10.1.1.1 میکروتیک را وارد کنید (۲).

۵ پروتکل و درگاه مقصد را مشخص کنید.

برنامه WinBox روی پروتکل TCP8291 کار می‌کند. پس مقابل Protocol، گزینه TCP و مقابل Dst.Port شماره ۸۲۹۱ را بنویسید (۳).

۶ نوع اقدام فایروال را مشخص کنید.

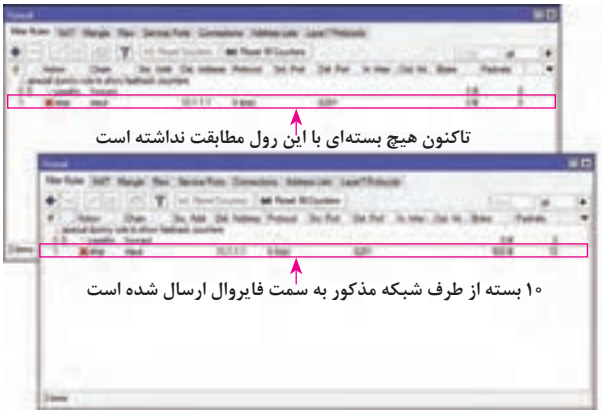
سربرگ Action را انتخاب کنید. مقابل گزینه Action، عبارت drop را انتخاب کنید (۴). با انتخاب این Action هر بسته‌ای که با این رول مطابقت داشته باشد، دور انداخته خواهد شد. این Action به صورتی است که هیچ پیام ICMP مبنی بر حذف بسته به سمت مبدأ ارسال نمی‌شود. دکمه Apply و سپس OK را بزنید (شکل ۲۷).



شکل ۲۷ـ تنظیمات رول

۷ صحت عملکرد رول را بررسی کنید.

پس از ایجاد رول باید مطمئن شویم که رول به درستی کار می‌کند. برای این منظور می‌توان از سمت شبکه خارجی اقدام به اتصال به WinBox کرد تا ببینیم فایروال دسترسی سرویس‌گیرنده خارجی را مسدود می‌کند یا خیر. راه دیگر این است که از روی خود رول متوجه شویم که بسته‌ای با این رول مطابقت داده می‌شود یا خیر (شکل ۲۸).



شکل ۲۸ـ نحوه بررسی صحت عملکرد رول‌ها

در انتهای هر رول فیلدی به‌نام Packets وجود دارد که تعداد بسته‌های مطابقت داده شده با این رول را نشان می‌دهد. درصورتی‌که عددی غیر از صفر در این فیلد باشد به این معنی است که رول ما درست کار می‌کند (شکل ۲۸).

با تست این رول مشاهده می‌شود که هیچ

سرویس‌گیرنده‌ای از سمت شبکه خارجی نمی‌تواند از طریق WinBox به آدرس IP 10.1.1.1 مسیریاب متصل شود. اما اگر فردی مک آدرس اینترفیس مسیریاب را داشته باشد به راحتی از طریق WinBox به آن متصل می‌شود!

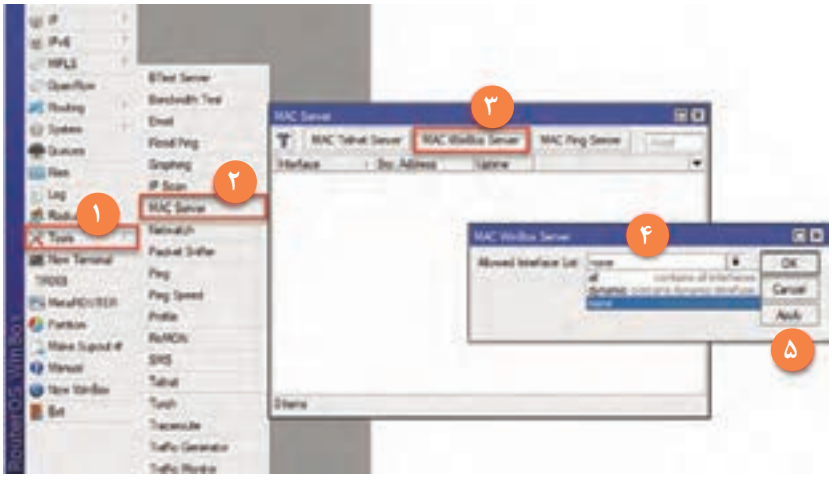
کارگاه ۸ مسدودسازی دسترسی به WinBox از طریق مک آدرس

رولی که در کارگاه ۷ نوشته شد فقط روی آدرس IP و درگاه انجام می‌شود. پس باید برای مسدود کردن دسترسی به WinBox از طریق مک آدرس هم تنظیمات جداگانه‌ای انجام دهیم. (شکل ۲۹).

۱ برنامه WinBox را باز کنید.

۲ به پنجره تنظیمات MAC Server وارد شوید.

از منوی سمت چپ گزینه Tools را انتخاب کرده (۱)، از منوی ظاهر شده گزینه MAC Server را انتخاب کنید(۲).



شکل ۲۹ـ مسدود کردن دسترسی به وسیله مک آدرس

۳ دسترسی WinBox از طریق MAC Address را مسدود کنید.

در پنجره MAC Server دکمه MAC WinBox Server را انتخاب کنید(۳) و در پنجره MAC WinBox Server برای عبارت Allowed Interface List گزینه none را انتخاب کرده (۴)، دکمه Apply و سپس OK را بزنید (۵).

توجه داشته باشید که با این عمل دیگر هیچ کس حتی خود شما نمی‌تواند از طریق WinBox با استفاده از مک آدرس به میکروتیک متصل شود. پس دقت کنید که از طریق آدرس IP دسترسی خود را مسدود نکنید.

با توجه به سناریوهای انجام شده، حالا فقط سرویس‌گیرنده‌های شبکه داخلی می‌توانند از طریق WinBox به میکروتیک متصل شوند.

فیلم

فیلم شماره ۱۲۲۳۱: ایجاد محدودیت زمانی برای کلاینت‌ها

فعالیت کارگاهی

رولی بنویسید که در شبکه داخلی کاربران نتوانند از طریق Winbox به میکروتیک متصل شوند و فقط مدیر شبکه امکان اتصال داشته باشد. این تنظیمات را به شیوه‌ای انجام دهید که اگر کاربری قصد حمله از طریق درگاه Winbox را داشته باشد، موفق به این کار نشود.

کارگاه ۹ مسدود سازی ping به میکروتیک

برای مسدودسازی دستور ping اقدامات جالبی می‌توان انجام داد که هکر یا شخصی که میکروتیک را ping می‌کند به اشتباه بیفتد. می‌خواهیم تنظیماتی انجام دهیم که هیچ‌کس چه از شبکه داخلی و چه از شبکه خارجی نتواند میکروتیک را ping کند.

۱ وارد تنظیمات فایروال میکروتیک شوید.

پس از باز کردن پنجره WinBox از منوی سمت چپ، گزینه IP را انتخاب کنید. از منوی ظاهر شده Firewall را انتخاب کنید.

۲ یک رول ایجاد کنید.

روی سربرگ Filter Rules کلیک کرده، روی دکمه ➕ کلیک کنید.

۳ نوع رول را انتخاب کنید.

در این سناریو چون مقصد ترافیک به میکروتیک ختم می‌شود، رول باید از نوع input انتخاب شود.

۴ آدرس مبدأ و مقصد ترافیک را تنظیم کنید.

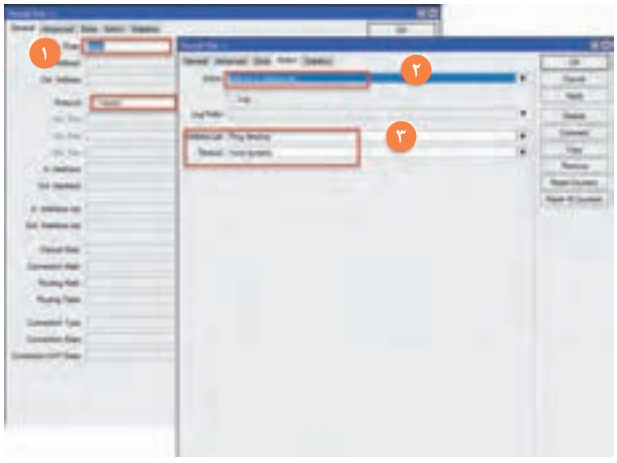
برای اینکه هیچ‌کس نتواند مسیریاب را ping کند، آدرس مبدأ و مقصد را خالی بگذارید.

۵ نوع ترافیک را مشخص کنید.

دستور ping با پروتکل ICMP کار می‌کند. پروتکل را icmp انتخاب کنید.

۶ Action مناسب را انتخاب کنید.

در برگه Action به جای گزینه Drop یا Tarpit می‌توان از Reject استفاده کرد (شکل ۳۰). این Action دقیقاً مثل Drop عمل می‌کند؛ اما در عوض می‌توان یک پیام مشخص شده را برای کاربر ارسال کرد. زمانی که دسترسی ping مسدود باشد، با ping کردن میکروتیک، به‌صورت پیش‌فرض پیام Request TimeOut برای کاربر ارسال می‌شود. اما وقتی Reject کنیم یک پیام دلخواه از فهرست پیام‌ها انتخاب و برای کاربر ارسال می‌شود.



شکل ۳۰ـ تنظیمات Action Reject برای رول

در فهرست Reject with یک پیام را انتخاب کنید. این فهرست شامل چند پیام است که کاربر می‌تواند یکی از آنها را انتخاب کند؛ اما نمی‌توان موارد دلخواه را وارد این فهرست کرد.

۷ رول را ذخیره کنید.

ابتدا دکمه Apply و سپس OK را بزنید.

با این رول مدیر شبکه هم مانند بقیه افراد نمی‌تواند میکروتیک را ping کند. برای حل این مشکل می‌توان یک رول جدید ایجاد کرد و دسترسی مدیر شبکه را فراهم کرد.

فیلم

فیلم شماره ۱۲۲۳۲: اجازه دسترسی به میکروتیک با ping

فعالیت کارگاهی

رولی بنویسید که فقط مدیر شبکه بتواند شبکه خارجی را ping کند.

کارگاه ۱۰ شناسایی افرادی که میکروتیک را ping می‌کنند

در این کارگاه قصد داریم تنظیماتی انجام دهیم که هم افرادی که مسیریاب را ping می‌کنند و هم اینترفیسی که ping می‌شود را شناسایی کنیم. با این شیوه مشخص می‌شود که افراد ping کننده متعلق به چه شبکه‌ای هستند. برای این منظور باید دو رول جداگانه بنویسیم و مکان این رول‌ها در فهرست فایروال باید قبل از رولی باشد که ترافیک‌های icmp را drop می‌کند.

۱ وارد تنظیمات فایروال میکروتیک شوید.

۲ یک رول ایجاد کنید.

۳ نوع رول را انتخاب کنید.

در این سناریو چون مقصد ترافیک به میکروتیک ختم می‌شود، رول باید از نوع input انتخاب شود. چون اطلاع نداریم که چه کسانی و از چه اینترفیسی، مسیریاب را ping می‌کنند. فیلد آدرس مبدأ و مقصد را خالی بگذارید.

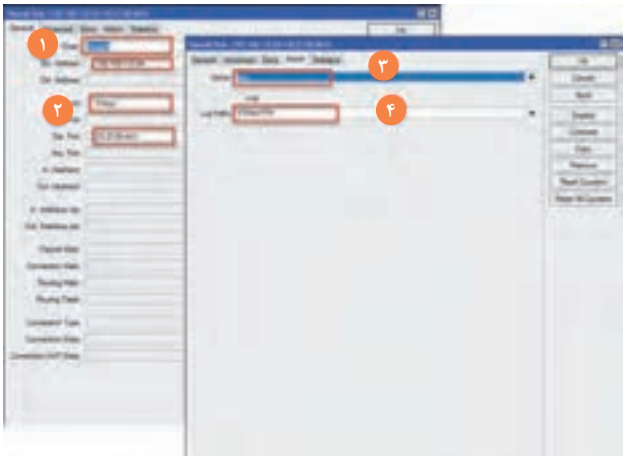
۴ نوع ترافیک را مشخص کنید.

دستور ping با پروتکل ICMP کار می‌کند. پس پروتکل را icmp انتخاب کنید.

۵ Action مناسب را انتخاب کنید.

در برگه Action از فهرست Actionها، گزینه add src to address list را انتخاب کنید، سپس در مقابل قسمت Address List یک نام متناسب با این اقدام بنویسید. با تعریف این رول، افراد ping کننده شناسایی می‌شوند (شکل ۳۱).

یکی از امکانات میکروتیک Address List است. در این فهرست‌ها می‌توان هم به‌صورت دستی و هم خودکار، فهرستی از آدرس‌های IP را قرار داد. زمان نوشتن رول‌ها این Address listها کاربرد فراوانی دارند.



شکل ۳۱ــ ایجاد رول برای شناسایی ping کننده‌ها

در هر رولی که با اکشن add src to address list ایجاد شده باشد، آدرس مبدأ بسته‌هایی که با این رول تطابق داشته باشد درون یک آدرس فهرست ذخیره می‌شود. مدیر شبکه هنگام ایجاد رول باید یک نام برای این فهرست اختصاص دهد. برای مشاهده محتویات فهرست وارد تنظیمات فایروال شوید سپس برگه Address List را باز کنید.

۶ رول را ذخیره کنید.

اکنون آدرس IP هر کاربری که مسیریاب را ping کند در برگه Address List فایروال قابل مشاهده است. قدم بعدی مشخص کردن اینترفیسی است که این کاربران از آنجا اقدام به ping می‌کنند. برای این منظور دقیقاً یک رول دیگر مانند رول قبل ایجاد کنید. فقط Action مرحله ۵ را add dst to address list انتخاب کنید و یک نام برایش بنویسید. حالا به راحتی می‌توان ردگیری کرد که چه کسانی از چه شبکه‌هایی مسیریاب شما را ping می‌کنند.

کارگاه ۱۱ گزارش‌گیری از عملکرد فایروال

یکی از امکانات مهم میکروتیک برای مدیران شبکه، امکان گزارش‌گیری از رخدادها و تغییرات درون میکروتیک است. در سرویس فایروال نیز می‌توان امکانی فراهم کرد تا از ترافیک عبوری Log گرفته شود، تا مدیر شبکه بررسی کند که چه اتفاقی درون فایروال در حال رخ دادن است.

در این کارگاه قصد گزارش‌گیری و تعیین مقصد ترافیک وب و FTP را داریم که از شبکه داخلی به سمت شبکه خارجی ارسال می‌شود.

۱ وارد تنظیمات فایروال میکروتیک شوید.

۲ یک رول ایجاد کنید.

۳ آدرس مبدأ بسته‌ها را انتخاب کنید.

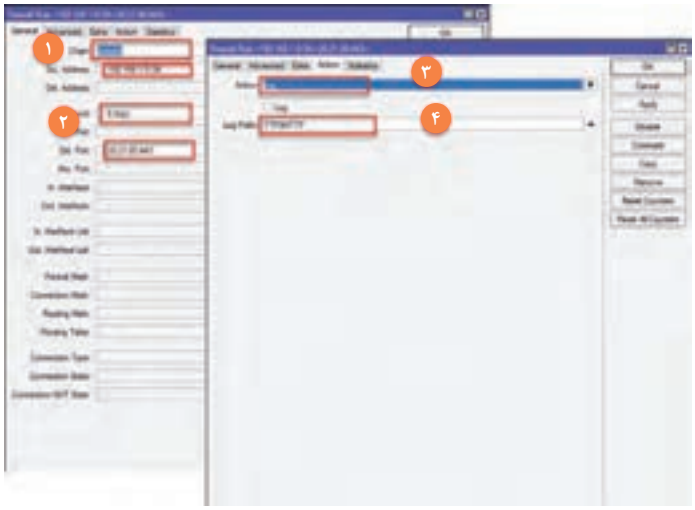
چون مبدأ ترافیک شبکه داخلی است، Src Address را 192.168.1.0 /24 قرار دهید (۱).

۴ پروتکل و شماره درگاه‌ها را مشخص کنید.

هر دو سرویس وب و انتقال پرونده روی پروتکل TCP کار می‌کنند. در مقابل Dst.Port به ترتیب شماره درگاه‌ها را نوشته و با کاما از هم جدا کنید: 21,20,443,80 (۲).

۵ Action را روی Log قرار دهید.

در برگه Action گزینه Log را انتخاب کنید (۳). برای اینکه Log این رول را به‌صورت واضح ببینید در مقابل عبارت Log Prefix یک نام کوتاه بنویسید (شکل ۳۲).



شکل ۳۲ـ ایجاد رول با اکشن log

۶ رول را ذخیره کنید.

برای مشاهده Logهای سیستم از منوی اصلی WinBox گزینه Log را انتخاب کنید. در اینجا همه Logهای سیستم قابل مشاهده است. Logهایی که به‌وسیله رولِ این کارگاه تولید شده‌اند، به واسطه Log Prefix قابل مشاهده هستند.

یادداشت

Log گرفتن روی میکروتیک بار پردازشی ایجاد می‌کند و زیاد بودن رول‌های Log ممکن است عملکرد میکروتیک را با اختلال مواجه کند؛ بنابراین باید در Logگیری دقت کرد که رول‌ها به اندازه و به دقت نوشته شوند.

فیلترینگ تارنماو اپلیکیشن

در سناریوهایی که تا اینجا بررسی شد، فایروال از نوع Packet Filter در نظر گرفته شده بود. این نوع از فایروال‌ها فقط از طریق بررسی شماره درگاه و آدرس IP و به‌طورکلی سرایند بسته تصمیم‌گیری می‌کنند و اقدامی روی بسته انجام می‌دهند.

نوع دوم فایروال یعنی Statefulها، با توجه به State یا وضعیت بسته تصمیم‌گیری می‌کنند. برای درک بهتر این نوع فایروال لازم است انواع وضعیت‌های هر بسته را یاد بگیریم:

- **New**: زمانی که یک سیستم، قصد ایجاد ارتباط دارد، برای اولین بار یک بسته به سمت مقصد خود ارسال می‌کند. در این حالت وضعیت این بسته در حالت New است. مانند کسی که به فرد دیگری سلام می‌کند.
- **Establish**: مقصد در جواب فرستنده، یک پیام تأیید ارتباط مانند جواب سلام، تحت قالب Establish ارسال می‌کند. در اینجا مبدأ نیز باید یک پیام Establish به سمت مقصد ارسال کند، تا مقصد هم بداند که ارتباط دوطرفه ایجاد شده است.
- **Related**: پس از ایجاد ارتباط، مبدأ داده‌های خود را تحت عنوان Related ارسال می‌کند و مقصد نیز داده‌های درخواست شده را برای مبدأ ارسال می‌کند.
- **Invalid**: بسته‌هایی که وضعیت آنها به‌وسیله فایروال تشخیص داده نمی‌شوند و یا دچار مشکل هستند، وضعیت Invalid دارند.
- **Untracked**: بسته‌هایی که برای عبور از سازوکار بررسی وضعیت بسته در فایروال تنظیم شده‌اند.

زمانی که قصد داریم یک تارنما را مسدود کنیم، بنا به دلایل متعددی نمی‌توان آدرسIP آن تارنما را مسدود کرد. برای مثال ممکن است آن تارنما IPهای زیادی داشته باشد یا IPهای آن مدام تغییر کنند و یا آن تارنما پشت یک NAT باشد و IP واقعی خودش نباشد. بنابراین باید از روش دیگری به نام فیلترینگ لایه اپلیکیشن یا فیلترینگ لایه ۷ استفاده کرد. یکی از ملزومات این شیوه فیلترینگ یادگیری نوشتن Regex (Regular Expression) است. Regex شیوه‌ای است که در برخی زبان‌های برنامه‌نویسی از جمله C++ و پایتون استفاده می‌شود. این شیوه عموماً برای جست‌وجو و یا جایگذاری یک عبارت درون یک متن استفاده می‌شود. برای یادگیری این شیوه باید با نمادهای آن آشنا شوید (جدول ۳).

جدول ۳ـ نمادهای Regex

نماد	توضیح
^	به ابتدای متن اشاره می‌کند. نویسه‌ای که بعد از ^ می‌آید باید ابتدای متن مورد جست‌وجو باشد.
.	به معنای یک نویسه است.
*	به معنای تکرار صفر بار تا بی‌نهایت بار از هر نویسه‌ای است.
()	نویسه‌های درون پرانتز به عنوان یک گروه در نظر گرفته می‌شوند.
$	به انتهای متن اشاره می‌کند. نویسه‌ای که قبل از آن می‌آید باید آخرین نویسه متن مورد جست‌وجو باشد.
|	به معنای یا است و می‌تواند چند عبارت را با هم or کند.
[]	مجموعه‌ای از نویسه‌های مجاز را مشخص می‌کند.
\	برای جست‌وجوی نویسه‌هایی که در Regex مفهوم خاصی دارند، استفاده می‌شود که قبل از نویسه \ قرار می‌دهند.

می خواهیم رولی بنویسیم که دسترسی کاربران شبکه داخلی به تارنمای گوگل را مسدود کند. بنابراین باید یک عبارت منظم بنویسیم که عبارت google.com را شامل شود. عبارت منظم یا Regex آن می‌تواند به‌صورت .*$(google.com).*. باشد.

برای مثال عبارت .*$(google\.com).*^ با عبارت‌های زیر مطابقت دارد:

google.com w.google.com www.google.com.1 gmail.google.com

اما با عبارات زیر تطابق ندارد:

Google GOOGLE.COM www.Google.com gooGle.com

مشاهده می‌شود که Regex روی بزرگی و کوچکی حروف حساس است. برای حل این مسئله می‌توان حالت‌های مختلفی که کاربران این عبارت را می‌نویسند پیدا کرد و با نماد | آنها را از هم جدا کرد. Regex آن به شکل زیر است:

^.*(google.com|GOOGLE.COM|Google.com).*$

اما باید دقت کرد که تعداد حالاتی که کاربر این عبارت را وارد می‌کند بسیار زیاد است و باید یک راه کوتاه‌تر انتخاب کرد به همین دلیل می‌توان از نماد [] استفاده کرد تا این مشکل برطرف شود.

^.*([gG][oO][oO][gG][lL][eE].+[cC][oO][mM]).*$

اکنون عبارت google.com با هر حالتی که حروف آن بزرگ یا کوچک باشند در متن پیدا می‌شوند.

فعالیت کارگاهی

به تارنمای regex101.com یا regexr.com مراجعه کنید و صحت Regexهایی را که می‌نویسید بررسی کنید.

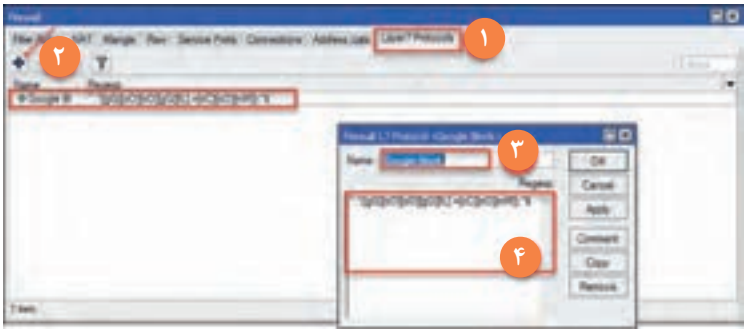
کارگاه ۱۲ مسدودسازی دسترسی کاربران شبکه داخلی به تارنمای گوگل

به دلیل اینکه نمی‌توان تارنمای گوگل را با آدرس IP فیلتر کرد، باید با استفاده از فیلترینگ لایه ۷ این کار انجام شود.

۱ تنظیمات فایروال را باز کنید.

۲ برای تارنمای گوگل یک Regex بنویسید.

سربرگ Layer 7 Protocols را انتخاب (۱) و یک Regex ایجاد کنید (۲). یک نام متناسب با Regex برای آن انتخاب کنید (۳)، سپس Regex را که نوشته‌اید در کادر پایین بچسبانید (Paste) (۴). در انتها دکمه Apply و OK را کلیک کنید (شکل ۳۳).



شکل ۳۳ـ ایجاد Regex

۳ یک رول جدید ایجاد کنید.

۴ Chain صحیح را برای رول انتخاب کنید.

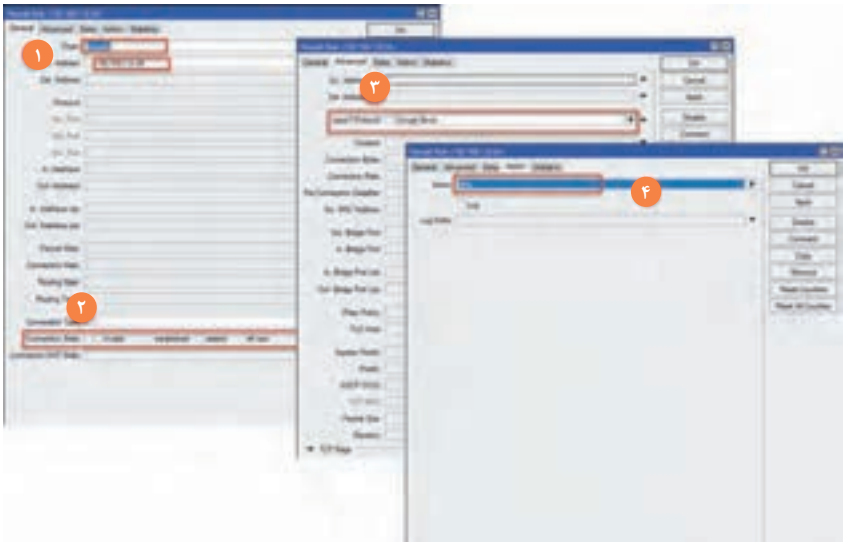
به دلیل اینکه مبدأ ترافیک در شبکه داخلی و مقصد آن در شبکه خارجی است؛ بنابراین ترافیک فقط از فایروال عبور می‌کند و Chain آن باید forward انتخاب شود (شکل ۳۴).

۵ آدرس مبدأ ترافیک را مشخص کنید.

آدرس مبدأ ترافیک را 192.168.1.0 /24 قرار دهید (۱).

۶ وضعیت ارتباط را مشخص کنید.

قصد داریم بسته‌هایی که از سمت شبکه داخلی به سوی تارنمای گوگل هدایت می‌شوند را بررسی کنیم، بنابراین در مقابل عبارت Connection State گزینه New را انتخاب کنید (۲).



شکل ۳۴ـ ایجاد یک رول برای فیلترینگ گوگل

۷ Regex را به رول معرفی کنید.

به سربرگ Advanced بروید و مقابل عبارت Layer 7 Protocol، نام Regex را از فهرست انتخاب کنید (۳).

۸ Action رول را انتخاب کنید.

به سربرگ Action بروید و drop را انتخاب کنید (۴).

۹ رول را ذخیره کنید.

فعالیت کارگاهی

با جست‌وجو در اینترنت Regexهای آماده را برای اپلیکیشن‌های مختلف جست‌وجو کنید و سناریوی مسدودسازی آن اپلیکیشن‌ها را انجام دهید.

فیلم

فیلم شماره ۱۲۲۳۳: مسدودسازی پویش درگاه میکروتیک

فعالیت کارگاهی

رول‌های موردنیاز برای افزایش امنیت و جلوگیری از حملات را در شبکه داخلی و مسیریاب تنظیم کنید، طوری که در نهایت تمام ترافیک‌های ناشناخته را مسدود کند.

ارزشیابی مرحله ۳

مراحل کار	شرایط عملکرد (ابزار، مواد، تجهیزات، زمان، مکان و ...)	نتایج ممکن	استاندارد (شاخص‌ها/داوری/نمره دهی)		نمره
استفاده از فایروال سخت‌افزاری	مکان: کارگاه استاندارد رایانه تجهیزات: شبکه‌ای از رایانه‌ها که به اینترنت و دستگاه فایروال متصل باشند زمان: ۳۰ دقیقه	بالاتر از حد انتظار	فعال کردن فایروال و ایجاد رول ـ مسدودسازی دسترسی به فایروال ـ مسدودسازی سرویس‌های غیرضروری روی فایروال ـ ایجاد رول‌های فیلترینگ ترافیک و فیلترینگ بر اساس درگاه و آدرس IP ـ انواع فیلترینگ محتوا و اپلیکیشن‌ها و حملات شبکه و تارنماها ـ تشخیص صحیح اولویت و ترتیب رول‌ها و خلاصه‌سازی آنها ـ گزارش‌گیری از فایروال و تحلیل گزارش	۳	
		در حد انتظار	فعال کردن فایروال و ایجاد رول ـ مسدودسازی دسترسی به فایروال ـ مسدودسازی سرویس‌های غیرضروری روی فایروال ـ ایجاد رول‌های فیلترینگ انواع ترافیک و فیلترینگ بر اساس درگاه و آدرس IP	۲	
		پایین‌تر از حد انتظار	فعال کردن فایروال و ایجاد رول ـ تشخیص انواع Chainها در فایروال ـ بستن دسترسی یک IP	۱	

معیار شایستگی انجام کار:
کسب حداقل نمره ۲ از مرحله استفاده از فایروال سخت‌افزاری
کسب حداقل نمره ۲ از بخش شایستگی‌های غیر فنی، ایمنی، بهداشت، توجهات زیست‌محیطی و نگرش
کسب حداقل میانگین ۲ از مراحل کار

جدول ارزشیابی پایانی

شرح کار:

۱ـ کاوش شبکه و تارنما

۲ـ استفاده از فایروال نرم‌افزاری

۳ـ استفاده از فایروال سخت‌افزاری

استاندارد عملکرد:

کشف نقاط ضعف شبکه و حفاظت از شبکه در برابر حملات به کمک فایروال نرم‌افزاری و سخت‌افزاری

شاخص‌ها:

شماره مرحله کار	شاخص‌های مرحله کار
۱	کاوش یک شبکه نمونه با استفاده از نرم‌افزار و تعیین نقاط آسیب‌پذیر شبکه
۲	فعال‌سازی فایروال نرم‌افزاری ـ ایجاد رول‌های مورد نیاز در فایروال ـ فعال و غیر فعال‌سازی رول‌ها بر حسب نیاز ـ باز و مسدود کردن درگاه و سرویس در فایروال بر اساس نیاز ـ مسدودسازی تارنما در صورت نیاز
۳	ایجاد رول‌های مورد نیاز ـ فعال و غیر فعال‌سازی رول‌ها بر حسب نیازـ باز و مسدود کردن درگاه و سرویس در فایروال براساس نیاز ـ مسدودسازی تارنما در صورت نیاز

شرایط انجام کار و ابزار و تجهیزات:

مکان: کارگاه رایانه مطابق استاندارد تجهیزات هنرستان‌ها

تجهیزات: شبکه‌ای از رایانه‌ها که نرم‌افزارهای کاوش و تست نفوذ و فایروال روی آن نصب باشد ـ دستگاه فایروال ـ مودم ADSL و اینترنت

زمان: ۱۰۵ دقیقه (کاوش شبکه و تارنما ۴۵ دقیقه ـ استفاده از فایروال نرم‌افزاری ۳۰ دقیقه ـ استفاده از فایروال سخت‌افزاری ۳۰ دقیقه)

معیار شایستگی:

ردیف	مرحله کار	حداقل نمره قبولی از ۳	نمره هنرجو
۱	کاوش شبکه و تارنما	۱	
۲	استفاده از فایروال نرم‌افزاری	۱	
۳	استفاده از فایروال سخت‌افزاری	۲	
	شایستگی‌های غیر فنی، ایمنی، بهداشت، توجهات زیست‌محیطی و نگرش: مسئولیت‌پذیری، ابراز تعهد به سازمان متبوع ـ مستندسازی، پایبندی به مستندسازی در نظام کنترل کیفیت ـ زبان فنی اتصال صحیح جریان برق فایروال سخت‌افزاری ـ جلوگیری از مسدود کردن کلیه ارتباطات مدیر شبکه به فایروال سخت‌افزاری دقت در نوشتن رول‌های فایروال و تنظیم آدرس‌ها در فیلترینگ فایروال	۲	
	میانگین نمرات		*

* حداقل میانگین نمرات هنرجو برای قبولی و کسب شایستگی، ۲ است.