یادداشت

پودمان ۴

تنظیمات امنیت شبکه

واحد یادگیری ۴

شایستگی تنظیمات امنیت شبکه

مقدمات تدریس

الف) مفاهیم کلیدی

مفاهیم کلیدی			
فایروال	آسیب‌پذیری	حملات سایبری	احراز هویت
هکر	محرمانگی	مهاجم	پویش

ب) تجهیزات لازم

سخت‌افزارهای لازم

- Mikrotik Router
- Wireless Modem

نرم‌افزارهای لازم

- Net Tools
- Ping Tester
- Acunetix
- Loic
- WinBox

جلسه	کارگاه (موضوع)	شماره صفحات	اهداف توانمندسازی	فعالیت‌های تکمیلی
۲۲	امنیت شبکه، مهاجم، تست آسیب‌پذیری، کارگاه ۱	۱۴۹_۱۵۴	آشنایی با مفهوم امنیت و آسیب‌پذیری‌ها، جمع‌آوری اطلاعات از تارنما	کاوش یک شبکه با استفاده از نرم‌افزار، جمع‌آوری اطلاعات تارنمای هدف و آدرس آن، استفاده از انواع دستورات خط فرمان برای جمع‌آوری اطلاعات تارنمای هدف، تعیین نقاط آسیب‌پذیر شبکه
۲۳	پویش، کارگاه ۲ و ۳	۱۵۵_۱۵۷	پویش برای تست آسیب‌پذیری‌های زیرساخت و نرم‌افزارها	به‌کارگیری انواع پویش برای پیدا کردن آسیب‌پذیری‌ها، پویش درگاه‌ها، آسیب‌پذیری‌ها و آدرس‌های سیستم هدف با ابزار مناسب، کشف آسیب‌پذیری‌های شبکه و تهیه گزارش
۲۴	ایجاد و حفظ دسترسی، کارگاه ۴	۱۵۸_۱۶۰	توانایی شبیه‌سازی حملات	شناخت حمله مناسب هر آسیب‌پذیری، شناخت انواع حملات اختلال سرویس، شبیه‌سازی حمله اختلال سرویس توزیع‌شده با ابزار مناسب
۲۵	فایروال، کارگاه ۵ و ۶	۱۶۱_۱۶۹	آشنایی با کاربرد فایروال و استفاده از فایروال نرم‌افزاری	توانایی فعال‌سازی فایروال نرم‌افزاری، شناخت رول‌های ثبت شده در فایروال و ایجاد رول‌ها براساس نیاز، مسدودسازی یک سرویس برای کاربر یا گروه خاص، مسدودسازی درگاه با فایروال، فعال کردن گزارش‌گیری از رخدادهای فایروال، تنظیم و بررسی اطلاعات گزارش‌گیری
۲۶	فایروال سخت‌افزاری، کارگاه ۷ و ۸	۱۷۰_۱۷۴	استفاده از فایروال سخت‌افزاری	تنظیمات فایروال میکروتیک، مسدودسازی سرویس‌های غیرضروری روی فایروال، مسدودسازی دسترسی با ابزارهای مناسب در میکروتیک
۲۷	کارگاه ۹ و ۱۰	۱۷۵_۱۷۷	استفاده از فایروال سخت‌افزاری	نوشتن رول‌های مسدودسازی دسترسی به میکروتیک و سرویس‌های غیرضروری، شناسایی کاربرانی که به میکروتیک دسترسی دارند، ایجاد رول‌های فیلترینگ ترافیک و فیلترینگ درگاه
۲۸	کارگاه ۱۱ و ۱۲	۱۷۷_۱۸۱	استفاده از فایروال سخت‌افزاری	تشخیص صحیح اولویت رول‌ها و خلاصه‌سازی آنها، گزارش‌گیری از عملکرد فایروال و تحلیل گزارش، گزارش‌گیری از رخدادها و تغییرات میکروتیک، فیلترینگ تارنما و اپلیکیشن و حملات شبکه، مسدودسازی دسترسی کاربران به تارنمای خاص، مسدودسازی پویش درگاه میکروتیک

طرح درس روزانه (هفتگی) پیشنهادی				
پایه: دوازدهم		درس: تجارت الکترونیک و امنیت شبکه		
پیام جلسه (هدف کلی): آشنایی با مفهوم امنیت (شبکه، سازمان، اطلاعات)، شناخت آسیب‌پذیری‌های شبکه و عواقب آن				
فعالیت	اهداف یادگیری	کار هنرآموز	کار هنرجو	مدت (دقیقه)
ارزشیابی رفتار ورودی	سنجش میزان آگاهی هنرجویان از مفاهیم امنیت شبکه	معطوف‌کردن توجه هنرجویان به ریسک‌ها و تهدیدهایی که در سیستم‌های روزمره مانند سیستم بانکداری و... وجود دارد. (امنیت شبکه‌های اجتماعی، درگاه‌های پرداخت الکتریکی و...). آشنایی با اصطلاحات امنیتی حوزه امنیت شبکه (دارایی، تهدید، حمله، آسیب‌پذیری و...)	مشارکت در فرایند تشخیص ریسک‌ها و تهدیدهای امنیتی (سرقت‌های اینترنتی مانند برداشت از حساب و از دست دادن گذرواژه، و ...) و تشخیص مصادیق امنیتی براساس هرم امنیتی که قبلاً آموخته است.	۲۰
ایجاد انگیزه	کاربرد مفاهیم تهدید، مهاجم و آسیب‌پذیری و انجام تست آسیب‌پذیری	هنرجویان را به دو/ چند دسته تقسیم کند و از آنها بخواهد تا با جست‌وجو در اینترنت فهرستی از اخبار جدید جرایم رایانه‌ای و مواردی از هک‌های معروف که خسارت زیادی را به‌دنبال داشته تهیه کنند. هک اخلاقی را بیان و اهداف هکر اخلاقی و سایر انواع هکر را بیان کند.	هنرجو در مورد انواع مهاجم‌های شبکه‌های رایانه‌ای تحقیق کند. تفاوت هک اخلاقی و سایر انواع هک را تشخیص دهد. مهاجم‌های کلاه رنگی و اهداف آنها را فرابگیرد.	۲۰
ارائه مفاهیم کلیدی (توضیح هنرآموز)	توضیح کامل مفاهیم کلیدی (دانشی) و ایجاد علاقه و انگیزه در هنرجویان (بینشی)	مفاهیم کلیدی مطرح‌شده در این واحد یادگیری را برای هنرجو تشریح کند. اصطلاحات آسیب‌پذیری، تهدید، مهاجم و ... را بیان کند. تست آسیب‌پذیری به‌صورت عملی انجام شود.	می‌توان مفاهیم را از طریق یک مسابقه مطرح کرد تا مشارکت در پاسخگویی و تعامل با هنرآموز در فرایند تدریس بهتر صورت گیرد.	۲۰
انجام فعالیت کارگاهی شماره ۱ (تمرین هنرجویان)	هنرجو اولین مرحله تست نفوذ را بشناسد و توانایی جمع‌آوری اطلاعات اولیه را کسب کند.	هنرآموز توضیح کامل در خصوص فعالیت کارگاهی ۱ به هنرجو بدهد.	هنرجویان به‌صورت گروهی اقدام به انجام فعالیت کارگاه ۱ می‌کنند.	۶۰

طرح درس روزانه (هفتگی) پیشنهادی				
پایه: دوازدهم		درس: تجارت الکترونیک و امنیت شبکه		
پیام جلسه (هدف کلی): آشنایی با مفهوم امنیت (شبکه، سازمان، اطلاعات)، شناخت آسیب‌پذیری‌های شبکه و عواقب آن				
نظارت بر عملکرد هنرجویان و ارزیابی فعالیت‌ها	بررسی نقاط ضعف هنرجویان در درک مفاهیم کلیدی	رفتار هنرجو را در حین اجرای تکالیف زیر نظر داشته باشد و در صورت لزوم از هنرجویان مستعدتر برای آموزش مفاهیم به آنها کمک بگیرد.	در گروه های دونفری مفاهیم برای یکدیگر شرح داده شود.	۶۰
انجام فعالیت کارگاهی شماره ۲ (تمرین هنرجویان)	هنرجو باید فاز ۲ تست آسیب‌پذیری امنیت زیرساخت و نرم‌افزارها را بشناسد و بتواند اقدام به پویش درگاه سیستم هدف کند.	هنرآموز توضیح کامل در خصوص فعالیت کارگاهی ۲ به هنرجو بدهد.	هنرجو با ابزار پویش به‌صورت گروهی اقدام به انجام فعالیت کارگاه ۲ می‌کند و با ابزار مناسب درگاه‌های شبکه را به منظور تست آسیب‌پذیری پویش می‌کند.	۶۰
نظارت بر عملکرد هنرجویان و ارزیابی فعالیت‌ها	بررسی نقاط ضعف هنرجویان در اجرای عملی دستورات و ابزارها	رفتار هنرجو را در حین اجرای تکالیف زیر نظر داشته باشد و در صورت لزوم از هنرجویان مستعدتر برای آموزش مفاهیم به آنها کمک بگیرد.	هنرجویان ممتاز موظف به ارائه مفاهیم به هنرجویان ضعیف‌تر باشند.	۶۰
انجام فعالیت کارگاهی شماره ۳ (تمرین هنرجویان)	هنرجو باید حملات اختلال سرویس را بشناسد و بتواند آدرس‌های فعال، درگاه‌های باز و... را پویش کند.	هنرآموز توضیح کامل در خصوص فعالیت کارگاهی ۳ به هنرجو بدهد.	هنرجو به‌صورت گروهی اقدام به انجام فعالیت کارگاه ۳ می‌کند.	۶۰
نظارت بر عملکرد هنرجویان و ارزیابی فعالیت‌ها	بررسی نقاط ضعف هنرجویان در درک مفاهیم کلیدی	رفتار هنرجو را در حین اجرا زیر نظر داشته باشد و در صورت لزوم از هنرجویان مستعدتر برای آموزش مفاهیم به آنها کمک بگیرد.	هنرجویان ممتاز موظف به ارائه مفاهیم به هنرجویان ضعیف‌تر باشند.	۶۰
دریافت بازخورد از تدریس	هنرجو بتواند فعالیت منزل کتاب را انجام دهد.	هنرجو را درخصوص نحوه انجام فعالیت راهنمایی کند. انجام تکالیف به‌صورت گروهی باشد.	سهم‌بندی وظایف کار پروژه بین اعضای گروه و تحویل در زمان‌بندی تعیین‌شده	۶۰
ابزارهای موردنیاز	ویدئو پروژکتور، رایانه، تخته آموزشی، دفتر یادداشت، نرم‌افزارهای لازم			

د) ورود به بحث

امروزه تهدیدهای سایبری همه جا وجود دارند، و خیلی بیشتر، پیچیده‌تر و ماهرانه‌تر شده‌اند. بنابراین لازم است هر شرکت یا سازمانی ضریب امنیتی سیستم خود را افزایش دهد. شناخت انواع حملات و راه‌های جلوگیری از آنها موضوع مهمی است.

در این پودمان با معرفی هک قانونی و نقش هکر قانونی کار را شروع می‌کنیم. انواع تهدیدهایی که شبکه با آنها مواجه است را بررسی می‌کنیم و چهار مرحله هک قانونی را از شناسایی تا پوشاندن رد پا معرفی می‌کنیم. همچنین تکنیک‌ها و ابزارهای تست نفوذ را بررسی می‌کنیم و با انواع فایروال و روش‌های فیلترینگ آشنا می‌شویم.

ایجاد انگیزه در هنرجویان

امروزه در کنار استفاده از رایانش ابری، مجازی‌سازی، شبکه اجتماعی و سایر تکنولوژی‌های جدید، تهدیدهای سایبری نیز تهاجمی‌تر، پیچیده‌تر و ماهرانه‌تر شده‌اند. حمله‌کننده‌ها ممکن است یک کارمند عصبانی، گروه‌های مجرمانه و یا دولت‌ها باشند. حملاتِ از نوع جرایم سایبری، هک و جاسوسی افراد حقیقی یا سازمان‌ها را قربانی می‌کنند و اطلاعات گوناگونی از جمله اطلاعات بانک‌ها، اطلاعات علمی، گذرواژه‌ها و یا اطلاعات یک کشور را مورد حمله و دسترسی قرار می‌دهند. نحوه حملات، همچنین مکانیزم‌های مقابله با آنها در طول زمان تغییر کرده است. بنابراین شرکت‌ها با چالش‌های مختلفی برای محافظت از زیرساخت‌هایشان مواجه هستند.

می‌توانید مثال‌هایی از تاریخچه انواع هک را بیان کنید:

- اولین هک در سال ۱۹۷۱ رخ داد. زمانی که جان دریپر با نام مستعار کاپیتان کرانچ، دستگاه Blue Box را برای هک تلفن ساخت تا به تماس‌های تلفنی دسترسی پیدا کند.
- در سال ۱۹۸۸ رابرت موریس دانشجوی فارغ‌التحصیل دانشگاه Cornell یک Worm روی ARPANET اجرا کرد. موریس ۶۰۰۰ رایانه دولتی را از کار انداخت و از دانشگاه اخراج شد. او سه سال به‌صورت مشروط آزاد بود و ۱۰۰۰۰ دلار جریمه شد.

به‌تدریج که جرایم رایانه‌ای شدت گرفت و با هدف تأمین امنیت شبکه‌ها، کلاهبرداری‌های مالی، هک‌کردن و سوءاستفاده‌های رایانه‌ای به عنوان یک جرم شناخته شد.

عناوین شغلی امنیت شبکه عبارت‌اند از:

- ناظر شبکه
- تحلیلگر امنیت
- مدیر بحران
- تحلیلگر بحران
- مدیر امنیت
- کارشناس تست نفوذ

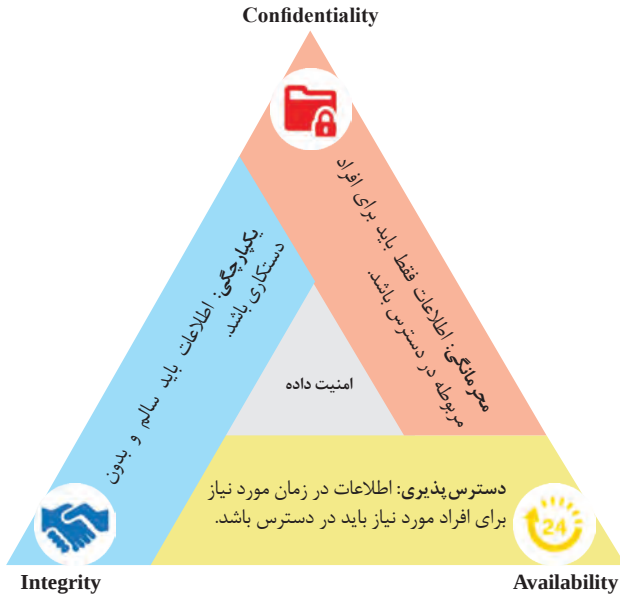
در شکل زیر مهارت‌های لازم متخصص امنیت شبکه نشان داده شده است.

تدریس

امنیت شبکه

هرم امنیت اطلاعات

امنیت شبکه و اطلاعات بر سه پایه حفظ یکپارچگی (Integrity)، در دسترس بودن (Availability) و محرمانگی (Confidentiality) استوار است. با قرارگیری این سه عنصر در کنار هم، امنیت حاصل می‌شود. اگر یکی از این عناصر نقض شود، امنیت سازمان یا شبکه، مختل می‌شود. شکل صفحهٔ بعد هرم امنیت اطلاعات را نشان می‌دهد. اصطلاحاً این سه عامل CIA نامیده می‌شوند.



عنوان	مصداق
محرمانگی	هیچ فرد غیرمجازی نتواند وارد پروفایل فرد شود و از جزئیات اطلاعات سفر باخبر شود.
در دسترس بودن	فرد در هر لحظه بتواند وارد سامانه شود.
یکپارچگی	اطلاعات مربوط به سفر، زمانی که به‌وسیله کاربر پایانه بررسی می‌شود با اطلاعات وارد شده به‌وسیله کاربر یکسان باشد.

عنوان	سیستم بانکداری
محرمانگی	اطلاعات حساب هر فرد تنها به وسیله خودش قابل رؤیت باشد و سایر افراد نتوانند موجودی حساب وی را ببینند.
در دسترس بودن	شخص صاحب حساب در هر زمانی بتواند از موجودی حساب خود مطلع شود و یا انتقال وجه انجام دهد.
یکپارچگی	برای بررسی تراکنش مالی مشتری، کارمند بانک و مشتری هر دو از هر جایی بتوانند یک مقدار موجودی را بدون اختلاف ببینند.

در جدول صفحه بعد مشخص می‌شود که در هر یک از مصادیق بیان شده، کدام اصل امنیت نقض شده است.

مصداق	اصل امنیت
○ کارمند بتواند پرونده‌های داده‌ای مهم را پاک کند. ○ حقوق خود را در پایگاه داده دستمزد شرکت، تغییر دهد. ○ یک رایانه موجود در شبکه را به یک بدافزار آلوده کند. ○ سامانه‌های شرکت را تخریب کند.	یکپارچگی
نفوذگر بتواند به روش‌های مختلف به اطلاعات در سطح شبکه دسترسی پیدا کند و از آنها سوءاستفاده کند.	در دسترس بودن
فاش شدن اطلاعات کارت اعتباری، شماره حساب و گذرواژه، هنگام خرید آنلاین از طریق سامانه‌های اینترنتی با کارت اعتباری	محرمانگی

توضیحات بیشتری از مفاهیم مهم امنیتی به همراه مثال در جدول زیر آمده است.

اصطلاح امنیتی	تعریف	مثال
دارایی (Assets)	هر اداره یا سازمان نیازمند یک طرح حفاظت امنیتی است. حال چه چیزی به محافظت نیاز دارد؟ دارایی دارایی منابع قابل لمس و غیرقابل لمسی است که می‌توان آنها را ارزش‌گذاری کرد.	قابل لمس: رایانه و چاپگر غیرقابل لمس: اسرار شرکت ـ بانک‌های اطلاعاتی ـ اسناد ـ اطلاعات‌حسابداری
آسیب‌پذیری	هدف آسیب‌پذیری، دسترسی غیرقانونی به یک دارایی است.	نوشتن گذرواژه روی کاغذ ـ باگ‌های برنامه‌ها
تهدید (Threat)	هر چیزی که به‌صورت عمدی یا تصادفی از یک آسیب‌پذیری استفاده می‌کند، یک دارایی را به دست می‌آورد و به آن آسیب وارد می‌کند. (شرایطی که باعث ایجاد اختلال در امنیت می‌شود.)	استفاده از برنامه Team Viewer و تغییر سطح دسترسی می‌تواند یک تهدید باشد ـ انواع نرم‌افزارهای مخرب
خطر (Risk)	قرار گرفتن در معرض یک رویداد به‌وسیله فرد یا عنصر دیگر است که می‌تواند منجر به اختلال در کار و کسب، ضرر مالی یا سایر آسیب‌پذیری‌ها شود.	به‌روز نبودن سیستم‌عامل ـ تغییر سطح دسترسی کاربر ـ عدم استفاده از فایروال
حمله (Attack)	تجاوز به امنیت سیستم و دارایی ارزشمند اطلاعاتی سازمان که ناشی از تهدید از طریق آسیب‌پذیری سیستم رخ می‌دهد، حمله است.	حملات اختلال سرویس ـ حملات مرد میانی حملات تزریق SQL
حریم خصوصی	فرض کنید شخصی در بانک برای انجام امور بانکی خود با صدای بلند، شماره ملی خود را به کارمند بانک اعلام می‌کند. ممکن است سایر مشتریان و کارمندان به طور ناخودآگاه از شماره ملی وی مطلع شوند. پس شماره ملی شخص، یک موضوع محرمانه نیست زیرا بقیه افراد حاضر در بانک کد ملی را شنیده‌اند. ولی لزومی ندارد که سایر اشخاص شماره ملی وی را بدانند زیرا جزء حریم خصوصی است.	
احراز هویت	قبل از آنکه محتوای یک پیام اهمیت داشته باشد، باید اطمینان حاصل کنیم که پیام را از طرف شخصی که می‌شناسیم دریافت کرده‌ایم و کسی قصد فریب ندارد. روش بیومتریک (Biometric) : (اثرانگشت، صدا، الگوی شبکیه یا عنبیه چشم، تشخیص چهره، هندسه دست و ...)	
کنترل دسترسی	کنترل دسترسی افراد غیرمجاز به شبکه و توانایی منع آنها	

مهاجم

مهاجم از آسیب‌پذیری‌ها و نقاط ضعف سیستم استفاده می‌کند تا به اطلاعات دسترسی پیدا کند. اصلی‌ترین سؤال برای بیان نیاز به استفاده از هک قانونی این است که:

برای اینکه بتوانیم امنیت را در شبکه برقرار کنیم، چه تدابیر امنیتی باید اتخاذ کنیم؟

هک قانونی یا هک اخلاقی چیست؟

زمانی که هکرها از مهارت خود برای انجام کارهای مفید استفاده می‌کنند، هک قانونی یا هک اخلاقی انجام می‌دهند. مثلاً شبکه یک سازمان را بررسی می‌کنند تا ببینند آیا در برابر حملات خارجی آسیب‌پذیر است یا نه. این نوع هک برای تقویت امنیت شبکه ضروری است و یکی از مهارت‌های لازم برای هر متخصص امنیت IT است.

هک قانونی سازوکاری برای بررسی سیستم‌ها فراهم می‌کند تا نقاط آسیب‌پذیر را شناسایی کند و وظیفه هکر قانونی، شناسایی نقاط آسیب‌پذیر است.

هک قانونی ← اجرای فعالیت‌های امنیتی ← بهبود امنیت ← محافظت از اطلاعات حساس

لازم است این نکات اخلاقی در هک قانونی تذکر داده شوند:

- نیاز به اجازه صریح برای انجام فعالیت‌های هک قانونی از مدیر سازمان یا مالک سیستم است.
- هدف از هک قانونی کمک به مدیران سیستم برای محافظت بهتر از داده‌ها و افزایش امنیت است.
- اشخاص حقیقی و تارنماها و سرورها را تجسس نکنیم و روی سیستم‌هایی که اجازه بررسی آنها را نداریم، هیچ فعالیت غیرقانونی انجام ندهیم.

پاسخ به فعالیت‌ها

پژوهش
صفحه ۱۵۱

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

هکرها گروه‌های مختلف و طرز فکرهای متفاوتی دارند و هر کدام هدف خاصی را دنبال می‌کنند. در شکل صفحه بعد انواع هکر کلاه رنگی را مشاهده می‌کنید.

هکرهای کلاه صورتی که نام دیگر آنها **Booter** است، سواد برنامه‌نویسی ندارند و فقط به منظور جلب توجه دیگران با چند نرم‌افزار خرابکارانه دست به هک کردن می‌زنند و به آزار و اذیت دیگران می‌پردازند.

هکرهای کلاه آبی خارج از یک شرکت مشاوره ایمنی، در نرم‌افزارها به دنبال باگ‌های امنیتی می‌گردند و آنها را گزارش می‌کنند. معمولاً شرکت‌ها برنامه‌هایی را که نوشته‌اند برای مدتی در اختیار این افراد می‌گذارند تا مشکلات احتمالی امنیتی آن قبل از عرضه به بازار کشف و حل شود.

کلاه زردها افرادی هستند که از تواناییشان در جهت‌های مثبت استفاده می‌کنند و علت انتخاب این رنگ الهام گرفته شده از خورشید است.

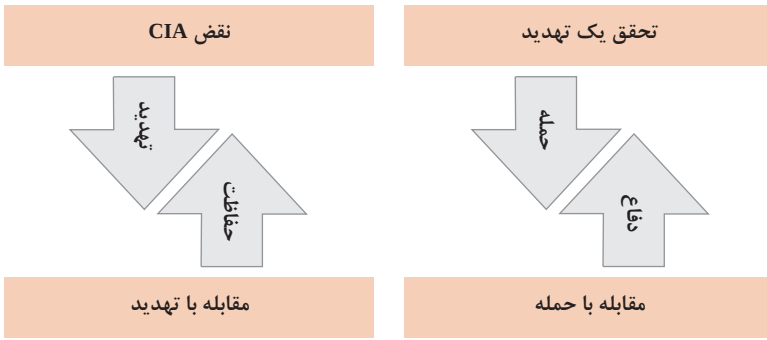
کلاه بنفش‌ها اغلب خودشان را هک می‌کنند. بدین صورت که سیستم جدید می‌خرند و سیستم قدیمی خود را هک می‌کنند تا مهارت خودشان در هک را بسنجند.

هکرهای کلاه سبز متخصصین حوزه امنیت بوده که توانمندی بالایی در دفاع از فضای سایبری دارند و مقابل حملات سایبری، اقدامات پدافندی مناسبی نشان می‌دهند.

کلاه قرمزها مانند کلاه خاکستری‌ها موضعشان مشخص و شفاف نیست. آنها معمولاً در سطح سازمان‌ها و وزارتخانه‌ها و مجموعه‌های حساس دست به عملیات هک می‌زنند و به طور کلی به دنبال اطلاعات حساس و فوق‌سری هستند.

سایر انواع هکرها نیز به‌صورت زیر دسته‌بندی می‌شوند.

Hacktivism	گروهی از هکرها که به دلایل سیاسی اعتراض خود را با هک کردن نشان می‌دهند.
Suicide Hacker	هکرهایی که نسبت به عواقب کارشان (دستگیر شدن و...) بی‌تفاوت هستند.
Script Kiddie	هکرهای تازه کاری که از ابزارهای آماده استفاده می‌کنند. (غیرخلاق)
Phreak	هکرهایی که دانش خوبی درباره سیستم‌های تلفنی داشته و سعی می‌کنند با هک کردن سیستم‌های تلفنی به صورت رایگان از آن استفاده کنند.
Red Team	تیمی از هکرها شامل سرپرست و افراد زیرمجموعه با مسئولیت‌های خاص مانند: نوشتن Malware code هستند. این تیم با قرارداد رسمی کار می‌کند و ملزم به ارائه گزارش تست نفوذ به طرف قرارداد است. این گزارش خروجی تکنیک‌های تست نفوذ است که سطح امنیت شبکه یا سرور را مورد ارزیابی قرار می‌دهد و براساس آن راهکار مناسب ارائه می‌شود.



آزمایش آسیب‌پذیری

آسیب‌پذیری ← ضعف در حفاظت از شبکه

یکی از روش‌های تست آسیب‌پذیری، استفاده از محیط‌های Sandbox است. هنرآموز می‌تواند از تارنماهای زیر برای تدریس استفاده کند.

- در تارنمای US-CERT (United States Computer Emergency Readiness Team) بخشی با نام Recent Vulnerabilities (آسیب‌پذیری‌های اخیر) وجود دارد.
- اگر می‌خواهید بدانید تارنمای شما قابل هک است یا خیر و یا به طور کلی امنیت تارنمای خود را بررسی کنید، از تارنمای acunetix استفاده کنید. به‌صورت آنلاین یا با نصب برنامه می‌توانید آسیب‌پذیری‌های تارنمای مورد نظر را پیدا کنید.
- تارنمای Google hacking Database (GHDB) و انتخاب گزینه Files Containing Passwords از فهرست Category به توسعه‌دهنده این امکان را می‌دهد تا آسیب‌پذیری‌هایی که یک تارنما را ناامن می‌کند، پیدا کند.

پاسخ به فعالیت‌ها

فعالیت منزل
صفحه ۱۵۳

در رابطه با Google Hacking تحقیق کنید.
Google Hacking به معنی هک کردن گوگل نیست. بلکه به معنی استفاده از روش‌های جست‌وجوی پیشرفته برای دریافت اطلاعات است. با Google Hacking یک هکر می‌تواند تارنماهای دارای نقاط ضعف و آسیب‌پذیری را پیدا کند.

عملگرهای جست‌وجوی پیشرفته گوگل	
intitle	جست‌وجو در تگ <title>Google</title> تارنماها (جست‌وجو در متون عنوان تارنماها)
inurl	جست‌وجو در آدرس تارنماها (جست‌وجوی عبارت معین در متن آدرس)
intext	جست‌وجو در متون تارنماها
site	جست‌وجوی صفحات یک تارنمای خاص ــ در پسوند دامنه‌ها
filetype	جست‌وجوی پرونده‌های معین

تمرین: تمام صفحاتی که درگاه ۸۰۸۰ دارند ولی درون آنها متن ۸۰۸۰ وجود ندارد را جست‌وجو کنید.

inurl:8080 - intext:8080

تمرین: صفحات دارای **ftp** عمومی را جست‌وجو کنید.

inurl:ftp intext:«Index of»

اگر صفحه‌ای مربوط به **FTP** عمومی باشد در آن عبارت **«Index of»** وجود دارد. بنابراین تارنماهایی که در آدرس آنها عبارت **«ftp»** و در صفحات آنها متن **«Index of»** وجود دارد را جست‌وجو می‌کنیم.

تمرین: نام کاربری و گذرواژه تارنماها را جست‌وجو کنید.

inurl:group_concat(username, filetype:php

تمرین: تارنماهای عمومی دارای دوربین مداربسته زنده را جست‌وجو کنید.

inurl:/view/index.shtml

توجه: بهترین راه جلوگیری از **Google Hacking** یادگیری آن و تست صفحات تارنمای خود با دستورات آن است.

کارگاه ۱ــ جمع آوری اطلاعات از تارنما

برای بررسی دقیق‌تر، اطلاعات به‌دست آمده از whois را با تارنمای whatismyipaddress مقایسه کنید. شکل زیر این تارنما را نشان می‌دهد.

Footprinting ← جمع آوری اطلاعات درباره سیستم هدف یا قربانی

اطلاعات به دست آمده از تارنمای ripe برای آدرس IP که در بالا به‌دست آوردیم، در شکل زیر قابل مشاهده است.

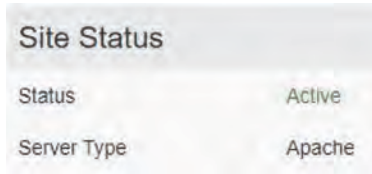
مراحل Footprinting

- **گام ۱:** شناسایی تارنمای هدف با استفاده از موتورهای جست‌وجو
- **گام ۲:** به دست آوردن اطلاعات جزئی‌تر در مورد هدف
- **گام ۳:** به دست آوردن اطلاعات با دستور Nslookup

با استفاده از سه گام بالا، تارنمای chap.sch.ir را بررسی می‌کنیم.
ابتدا عنوان «چاپ کتاب درسی» را در تارنمای google جست‌وجو می‌کنیم تا نام دامنه chap.sch.ir را پیدا کنیم.

در تارنمای who.is اطلاعات جزئی‌تری برای نام دامنه مورد نظر جست‌وجو می‌کنیم. شکل مقابل محل ورود اطلاعات اولیه که شامل نام دامنه یا آدرس IP است را برای این تارنما نشان می‌دهد.

هدف ما به‌دست آوردن اطلاعاتی مانند آدرس IP، DNS، Neme Server، Web server سیستم‌عامل سرویس‌دهنده وب، تلفن، رایانامه، Ranking و... است.



شکل مقابل نوع سرویس‌دهنده تارنمای هدف را نشان می‌دهد. همچنین تاریخ‌های مهم مانند تاریخ انقضا، تاریخ آخرین به‌روزرسانی و نام سرویس‌دهنده‌هایی که تارنما روی آنها ثبت شده را می‌توان مشاهده کرد.

سربرگ DNS Records شامل رکوردهایی است که اطلاعات Name Serveها را نگهداری می‌کنند. توضیح پارامترهای آن را در جدول زیر مشاهده می‌کنید.

اطلاعات DNS Records	
A	آدرس IP (IPv4)
MX	آدرس سرویس‌دهنده ایمیل (Mail Exchange)
AAAA	آدرس IPv6 (۱۲۸ بیتی است یعنی ۴ برابر Ipv4 که ۳۲ بیتی است، پس چهار A دارد.)

در شکل زیر رکوردهای DNS تارنمای هدف قابل مشاهده است.

پاسخ به فعالیت‌ها

تکمیل کارگاه
صفحه ۱۵۴

جمع‌آوری اطلاعات از طریق دستورات خط فرمان نیز امکان‌پذیر است.
اتصال اینترنت را برقرار کنید و از پنجره cmd دستور nslookup را به‌صورت زیر تایپ کنید.

nslookup -type=a chap.sch.ir 8.8.8.8

آدرس IP به‌دست آمده را با IPهای قبل مقایسه کنید.
آدرس IP به‌دست آمده را در تارنمای ripe.net جست‌وجو کنید.

```
C:\WINDOWS\system32>nslookup -type=a chap.sch.ir 8.8.8.8
Server:  google-public-dns-a.google.com
Address:  8.8.8.8

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

```
inetnum:        37.228.135.0 - 37.228.139.255
netname:        IR-PARS-20120410
org:            ORG-PO1-RIPE
admin-c:        PNOC5-RIPE
tech-c:         PNOC5-RIPE
country:        IR
status:         ALLOCATED PA
notify:         registry@parsonline.net
mnt-by:         RIPE-NCC-HM-MNT
mnt-by:         PARSONLINE-MNT
mnt-routes:     PARSONLINEDC-MNT
mnt-domains:    PARSONLINEDC-MNT
created:        2016-08-10T08:15:48Z
last-modified:  2017-06-17T09:20:56Z
source:         RIPE
```

```
organisation:    ORG-PO1-RIPE
org-name:        Pars Online PJS
org-type:        LIR
address:         222 Khoramshahr Ave
address:         15337
address:         Tehran
address:         IRAN, ISLAMIC REPUBLIC OF
phone:           +98 21 8220 8333
fax-no:          +98 21 8874 9505
e-mail:          registry@parsonline.net
```

```
route:           37.228.138.0/24
origin:          AS60976
mnt-by:          PARSONLINEDC-MNT
created:         2017-12-23T10:34:56Z
last-modified:   2017-12-23T10:34:56Z
source:          RIPE
```

همان‌طور که در شکل بالا مشاهده می‌کنید، محدوده آدرس‌های IP نام، آدرس، شماره تلفن و AS تارنمای هدف به دست می‌آید.
AS: دامنه‌ای است که سازمان‌ها می‌گیرند تا IPهای سازمان اختصاصی باشد. با این کار IPهای تحت آن دامنه برای سازمان ثبت می‌شوند و در کل دنیا سازمان با آن شناسایی می‌شود.

تکمیل کارگاه
صفحه ۱۵۴

در مرحله ۵ از کارگاه می‌توانید مطالب تکمیلی زیر را انجام دهید.
دستور Tracert:
ابزار خط فرمان است که بسته را در اینترنت مسیریابی و مسیر و زمان انتقال را مشخص می‌کند.
سؤال: وقتی تارنمایی را باز می‌کنید این درخواست چه مسیری را طی می‌کند تا به تارنمای مورد نظر برسد؟
سؤال: حالتی را در نظر بگیرید که مدیر شبکه شرکتی هستید که دارای چند شعبه در شهرهای مختلف است و در حال حاضر ارتباط با یک یا چند بخش دچار اختلال شده است. ممکن است این مشکل علل مختلفی داشته باشد مثلاً یک یا چند روتر از کار افتاده باشند یا مسیر ارتباطی بین روترها دچار اختلال شده باشد. در این صورت چگونه می‌توانید محدوده مشکل پیش آمده را تعیین کنید؟
برای پاسخ به این سؤالات بهتر است با عملکرد tracert آشنا شویم.
Tracert با ارسال بسته‌های ICMP با TTLهای متفاوت مسیر را مشخص می‌کند. در مسیر ارسالی بسته‌ها با گذر از هر روتر حداقل یکی از TTLهای آنها کاسته می‌شود.

به بیان دیگر هر بسته برای عبور از هر روتر باید حداقل یک TTL عوارض بپردازد تا بتواند عبور کند. در صورتی که پردازش هر Packet در روتر بیش از یک ثانیه طول بکشد به ازای هر ثانیه TTL بیشتری از Packet کم می‌شود. زمانی که TTL بسته به صفر می‌رسد، روتر باید یک بسته ICMP Time Exceeded Message را به کامپیوتر مبدأ برگرداند.

دستور Tracert اولین بسته با TTL=۱ را ارسال می‌کند تا اولین روتر را پیدا کند و هر بار به مقدار TTL یکی اضافه می‌کند. این فرایند تا زمانی انجام می‌شود که مقدار TTL به حداکثر مجاز خودش برسد یا اینکه به مقصد برسیم. پس Tracert از بسته‌های ICMP Time Exceeded Message که روترها به مبدأ می‌فرستند برای تعیین مسیر استفاده می‌کند. البته بعضی از روترها هم هستند که بسته‌هایی را که TTL آنها به پایان رسیده را دور می‌اندازند و بسته ICMP Time Exceeded Message را به مبدأ نمی‌فرستند. بنابراین به‌وسیله Tracert قابل شناسایی نیستند.

Tracert توپولوژی شبکه به همراه دستگاه‌های واسطه را پیدا می‌کند.

دستور PathPing:

اطلاعات و آمار مشخص برای رفع مشکل را ارائه می‌دهد و مسیر را مشخص می‌کند.

- این دستور ویژگی‌های Ping و Tracert را با هم ترکیب می‌کند.
- بسته‌هایی را به هر روتر ارسال و نتیجه را محاسبه می‌کند.
- از بین رفتن بسته‌ها در هر روتر یا لینک را با انجام محاسباتی مشخص می‌کند.
- حدود ۴ الی ۵ دقیقه (۲۷۵ ثانیه) طول می‌کشد تا محاسبات انجام و نتیجه را نشان دهد.
- توصیه می‌شود برای اجرای این دستورها، محیط Command Prompt را با راست‌کلیک در حالت Run as Administrator اجرا کنید.

دو شکل زیر دستور ping و Tracert را برای گوگل نشان می‌دهند.

```
C:\WINDOWS\system32>tracert google.com

Tracing route to google.com [172.217.16.174]
over a maximum of 30 hops:

  1     1 ms    <1 ms    <1 ms  192.168.1.1
  2    15 ms    15 ms    14 ms  10.140.192.102
  3    15 ms    14 ms    14 ms  10.140.199.101
  4    15 ms    14 ms    15 ms  10.140.0.29
  5    14 ms    16 ms    14 ms  10.140.0.122
  6    15 ms    15 ms    15 ms  217.219.0.115
  7    15 ms    15 ms    15 ms  185.57.203.33
  8     *        *        *     Request timed out.
  9    21 ms    47 ms    20 ms  10.201.147.250
 10    27 ms    25 ms    22 ms  10.201.147.214
 11    95 ms    91 ms    92 ms  85.132.90.253
 12     *        *        *     Request timed out.
 13   101 ms    99 ms    99 ms  72.14.212.229
 14   104 ms   100 ms   100 ms  108.170.252.1
 15   101 ms    99 ms   100 ms  64.233.175.171
 16   102 ms    98 ms    99 ms  fra15s11-in-f174.1e100.net [172.217.16.174]

Trace complete.

C:\WINDOWS\system32>
```

```
C:\WINDOWS\system32>ping google.com

Pinging google.com [216.58.214.110] with 32 bytes of data:
Reply from 216.58.214.110: bytes=32 time=103ms TTL=49
Reply from 216.58.214.110: bytes=32 time=100ms TTL=49
Reply from 216.58.214.110: bytes=32 time=100ms TTL=49
Reply from 216.58.214.110: bytes=32 time=99ms TTL=49

Ping statistics for 216.58.214.110:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 99ms, Maximum = 103ms, Average = 100ms
```

پژوهش
صفحه ۱۵۳

کاربرد تارنمای ripe.net و arin.net چیست؟

- **نمایش محدوده آدرس‌های IP**
- **تاریخ ایجاد و تغییر دامنه**
- **نام، آدرس و تلفن ثبت‌کننده دامنه**
- **نمایش AS**

ripe.net	تخصیص Ipv6، Ipv4 و AS به ISPها و سازمان‌های مخابراتی و شرکت‌های بزرگ
arin.net	تخصیص آدرس IP

کنجکاوی
صفحه ۱۵۴

اجرای دستور nslookup به تنهایی چه کاربردی دارد؟
برای بررسی نام دامنه و IP سرور است.

پژوهش
صفحه ۱۵۴

تفاوت دستور ping و nslookup چیست؟
Ping با ارسال چندین بسته (packet) ارتباط شبکه‌ای بین چند نقطه را بررسی می‌کند.
Nslookup برای بررسی نام دامنه و IP سرور است.

Ping	ساده‌ترین کاربرد Ping تست ارتباط بین دو نقطه از شبکه است. ○ نشان می‌دهد، آیا دو کامپیوتر یکدیگر را می‌بینند یا خیر. ○ مدت زمان ارسال و دریافت بسته اطلاعاتی را برآورد می‌کند. ○ وظیفه بررسی قابلیت دسترسی با پروتکل ICMP را دارد. Ping ابتدا بسته ICMP Echo Request را به سمت رایانه مقصد ارسال می‌کند. اگر رایانه مقابل این بسته را دریافت کند بسته‌ای به نامه ICMP Echo Reply را به سمت مبدأ ارسال می‌کند و خبر دریافت بسته اطلاعاتی اولیه را به‌صورت خودکار می‌دهد. به‌طور پیش فرض تعداد ارسال بسته Echo Request چهار عدد است.
Nslookup	Nslookup ابزاری است که معمولاً برای رفع مشکل در DNS به کار می‌رود. ○ Query گرفتن از DNS به‌صورت دستی ○ بررسی اطلاعات مربوط به نحوه تنظیم DNS در رایانه ○ مشخص می‌کند چه رکورد DNS باید resolved شود. ○ نام host و آدرس IP سرور DNS را نشان می‌دهد. ○ کپی گرفتن از تمامی رکوردهای سرور ○ دارای دو حالت غیرتعاملی (Non Interactive) و تعاملی (Interactive) است.

شکل‌های زیر به ترتیب حالت غیرتعاملی و تعاملی را نشان می‌دهد.

```
C:\WINDOWS\system32>nslookup google.com
Server:  UnKnown
Address:  192.168.1.1

Non-authoritative answer:
Name:    google.com
Addresses:  2a00:1450:4001:814::200e
          172.217.16.174
```

```
C:\WINDOWS\system32>nslookup
DNS request timed out.
    timeout was 2 seconds.
Default Server:  UnKnown
Address:  192.168.1.1

> google.com
Server:  UnKnown
Address:  192.168.1.1

Non-authoritative answer:
Name:    google.com
Addresses:  2a00:1450:4001:812::200e
          216.58.214.110

> set type=mx
> google.com
Server:  UnKnown
Address:  192.168.1.1

Non-authoritative answer:
google.com      MX preference = 30, mail exchanger = alt2.aspmx.l.google.com
google.com      MX preference = 20, mail exchanger = alt1.aspmx.l.google.com
google.com      MX preference = 40, mail exchanger = alt3.aspmx.l.google.com
google.com      MX preference = 10, mail exchanger = aspmx.l.google.com
google.com      MX preference = 50, mail exchanger = alt4.aspmx.l.google.com
>
```

سوییچ‌های دستور nslookup	
بررسی نام دامنه و IP سرور	بدون پارامتر
تبدیل نام دامنه به IP	nslookup <domainname>
تهیه لیست از اطلاعات DNS دامنه	Ls
تبدیل سرور DNS به سرور مورد نظر	Server
تغییر نوع اطلاعات بررسی‌شده	Set type
تغییر پورت	Set port
تعیین تعداد ورودی‌ها	Set retry
نمایش صفحه راهنمای سوییچ‌های دستور	Help یا /?

جدول همه سوییچ‌های دستور Ping و Nslookup در کتاب همراه هنرجو آمده است.

کنجکاوی
صفحه ۱۵۵

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

شماره درگاه	پروتکل	کاربرد (سرویس)
۸۰	HTTP	پروتکل انتقال ابرمتن (پروتکل www)
۸۱۹۲	Winbox	اپلیکیشن ارتباط با مسیریاب میکروتیک
۲۳	Telnet	دسترسی از راه دور
۲۲	SSH	پروتکل مدیریت و دسترسی به شبکه از راه دور
۴۴۳	HTTPS	پروتکل امن انتقال ابرمتن
۵۳	DNS	سرویس‌دهنده نام دامنه (جلوگیری از حملات DDoS)
۲۱	FTP	پروتکل ftp فرمان کنترل

کارگاه ۲ــ پویش درگاه سیستم هدف

هدف از این کارگاه استفاده از روش‌هایی است که به ما کمک می‌کنند تا با اطلاعات اولیه‌ای که در مرحله جمع‌آوری به‌دست آوردیم به اطلاعات جزئی‌تری از سیستم هدف دست پیدا کنیم. همچنین بتوانیم اطلاعاتی در مورد نوع سیستم‌عامل و نسخه و سرویس‌پک آن، پورت‌های باز و سرویس‌های در حال اجرا نیز به دست آوریم.

هدف از پویش ← سوءاستفاده از یک آسیب‌پذیری ← برطرف کردن آسیب‌پذیری

پویش (Scanning)

- آسیب‌پذیری‌های شناخته‌شده را پیدا می‌کند.
- گزارش تهیه می‌کند.
- به‌وسیله یک متخصص امنیت شبکه یا کاربر معمولی اجرا می‌شود.
- به‌صورت منظم اجرا می‌شود.

در تارنمای sectools، فهرستی از برترین ابزارهای امنیتی و پویشگرها به همراه توضیحات مختصری درباره آنها وجود دارد. هنرآموزان می‌توانند با گروه‌بندی هنرجویان خود تحقیق در مورد عملکرد و قابلیت‌های هر پویشگر را به آنها بسپارند.

تست نفوذ ← فرایند پیدا کردن ضعف‌های امنیتی ← اجرای حملات مختلف برای دسترسی به سیستم

تست نفوذ

- از پویش‌های آسیب‌پذیری برای دسترسی به یک سیستم استفاده می‌کند.
- نیاز به یک متخصص در تمام زمینه‌های سیستم‌های رایانه‌ای (سیستم‌عامل‌ها، بانک‌های اطلاعاتی، سرورهای وب و دستگاه‌های شبکه) دارد. اغلب به‌وسیله یک شرکت بیرونی انجام می‌شود.
- گزارش تست نفوذ شامل روش‌ها و راه‌حل‌هایی برای کاهش ضعف‌ها است.
- سالی یک‌بار و با استفاده از ابزارها و تکنیک‌های مختلف و به‌وسیله یک متخصص انجام می‌شود.

پویش ≠ تست نفوذ

پویش آسیب‌پذیری	تست نفوذ
متخصص داخلی امنیت	مشاور بیرونی
بازه‌های زمانی منظم	سالیانه
گزارش جامع	گزارش مختصر
هزینه کم	هزینه بسیار بالا

مراحل فرایند پویش

- شناسایی سیستم‌های فعال در شبکه
- شناسایی پورت‌های باز روی سیستم‌های فعال در شبکه
- شناسایی سرویس‌هایی که روی پورت‌های باز قرار دارند.
- شناسایی نوع سیستم‌عامل روی سیستم‌های فعال
- شناسایی نقاط ضعف و آسیب‌پذیری‌ها روی سیستم‌های فعال
- رسم نقشه Hostهای آسیب‌پذیر شبکه
- هکر با استفاده از پروکسی آدرس IP خود را پنهان می‌کند

با استفاده از دستور **netstat – a** در **cmd** می‌توان پورت‌هایی از سیستم که در حالت فعال یا **Listening** هستند را مشاهده کرد.

کنجکاوی: چرا باید از فعالیت **Port Scanning**ها در شبکه جلوگیری کنیم؟
زیرا اطلاعاتی که جمع‌آوری می‌کنند می‌تواند به عنوان پیش‌درآمد برای حمله استفاده شود.

کنجکاوی: چگونه در برابر پویش پورت محافظت کنیم؟

- تست سیستم با ابزارهای پویش (ابزار **Net tools**)
- مسدود کردن پورت‌های باز غیرفعال یا مسدودکردن پورت‌های غیرضروری

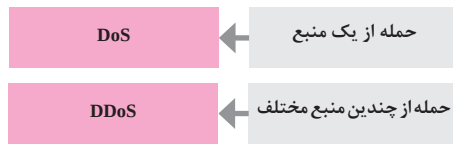
تکمیل کارگاه ۲
صفحه ۱۵۶

کارگاه ۳ــ پویش آدرس‌های IP فعال (زنده) شبکه هدف

هدف از این کارگاه ایجاد و حفظ دسترسی (حمله) است.
حملات DoS: حمله محروم‌سازی از سرویس، به تلاش برای خارج‌کردن ماشین و منابع شبکه از دسترس کاربران مجاز می‌پردازد.
DDoSمخفف (Distributed Denial of Service) به معنی سرازیرکردن تقاضاهای زیاد به یک سرور و استفاده بیش‌ازحد از منابع (پردازنده، پایگاه داده، پهنای باند، حافظه و...) است. به‌طوری‌که به دلیل حجم بالای پردازش سرویس‌دهی عادی آن به کاربرانش دچار اختلال شده یا از دسترس خارج شود.
حمله DDoS به‌طور کلی تلاش برای قطع موقت یا دائمی یا تعلیق خدمات یک میزبان متصل به اینترنت است. یکی از روش‌های معمول این حمله شامل اشباع ماشین هدف با درخواست‌های ارتباط خارجی است به‌طوری که ماشین هدف، نمی‌تواند به ترافیک قانونی پاسخ دهد یا پاسخ‌ها با سرعت کم داده می‌شوند و یا در دسترس نیستند. چنین حملاتی منجر به سرریز داده‌های سرور می‌شوند.
حمله DDoS، کامپیوتر هدف را وادار به راه‌اندازی مجدد و یا از بین بردن منابعش می‌کند، به‌گونه‌ای که نتواند به دستگاه‌های مورد نظرش سرویسی ارائه دهد و سیاست‌های مورد قبول ارائه‌دهندگان سرویس‌های اینترنتی را نقض کند.
تارنمای digitalattackmap بر مبنای داده‌هایی که از همه شبکه‌ها جمع‌آوری می‌کند، حملات روزانه DoS را نشان می‌دهد.

کارگاه ۴ــ شبیه‌سازی حمله DDoS در کارگاه رایانه

در این کارگاه از Loic برای ایجاد حجم وسیعی از ترافیک به منظور مصرف پهنای باند و منابع شبکه یا برنامه‌ها استفاده می‌کنیم. این حجم بالا از ترافیک باعث می‌شود عملکرد سیستم کاهش پیدا کند و یک سرویس را از دست بدهیم.
کاربری که از Loic استفاده می‌کند می‌تواند حمله DoS را روی تارنمای هدف با استفاده از بسته‌های TCP و UDP یا HTTP به‌صورت Flooding در سرور اجرا کند.



روش Loic

اگر رایانه‌ای به تنهایی از Loic استفاده کند نمی‌تواند بسته‌ها را به اندازه کافی تولید کند تا یک سرور را از کار بیندازد. بنابراین لازم است هزاران رایانه یک سرور مشخص را هدف بگیرند تا بتوانند تأثیر چشمگیری داشته باشند.

برخی ویژگی‌های Loic:
یک ابزار قانونی برای تست‌کردن است.

- رابط کاربری ساده‌ای دارد.
- تنها یک مهاجم کافی نیست.
- نیاز به حملات DDoS هماهنگ شده دارد.
- منبع را جعل نمی‌کند و آدرس IP را تغییر نمی‌دهد.

پاسخ به فعالیت‌ها

تکمیل کارگاه
صفحه ۱۵۹

نحوه استفاده از Loic:
برای تعیین هدف لازم است نشانی تارنما یا IP هدف را وارد کنید.
پس از اجرا تعداد بسته‌های تولید شده، با استفاده از گزینه Requested در ناحیه Attack Status قابل مشاهده است.
برای توقف حمله از دکمه Stop Flooding استفاده کنید.
برای مشاهده تأثیر حمله می‌توان با استفاده از Task Manager میزان مصرف CPU را بررسی کرد.
با ارسال ترافیک بیش از 50G در ثانیه، قربانی با مشکل جدی مواجه می‌شود.

پژوهش
صفحه ۱۶۰

برخی از ابزارهای پاک‌کردن پرونده‌های Log را از اینترنت جست‌وجو کنید.
روش ۱: از جست‌وجوی ویندوز پنجره Event Viewer را باز کنید. در ساختار درختی روی Log رویداد مورد نظر راست‌کلیک و Clear Log را بزنید.
روش ۲: در cmd دستور زیر را بنویسید.

```
wevtutil cl <LogName> [/bu:<backup_file_name>]
```

روش ۳: در cmd دستور زیر را بنویسید.

```
for /F "tokens=*" %1 in ('wevtutil.exe el') DO wevtutil.exe cl "%1"
```

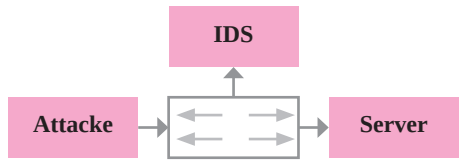
روش ۴: در PowerShell یکی از دستورات زیر را بنویسید.

```
Get-EventLog -LogName * | ForEach { Clear-EventLog $_.Log }
wevtutil el | Foreach-Object {wevtutil cl "$_"}
```

فایروال (Firewall)

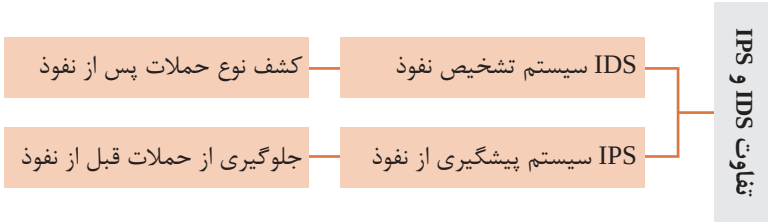
فایروال مانند در یک ساختمان است و به بسته‌هایی که مجوز ورود یا خروج از شبکه را دارند اجازه می‌دهد و در مقابل از ورود یا خروج بسته‌های غیرمجاز جلوگیری می‌کند.

شکل زیر عملکرد IDS را نشان می‌دهد. IDS در مسیر شبکه قرار دارد و یک کپی از ترافیکی که از سمت مهاجم به سرور فرستاده می‌شود به IDS ارسال می‌شود. IDS ترافیک را آنالیز می‌کند و Delay زیادی دارد. اما استفاده از IDS همیشه مقرون به‌صرفه نیست. زیرا به تعداد زیادی IDS نیاز داریم. بنابراین در شبکه‌های LAN، IDS را به موازات ترافیک قرار می‌دهند تا یک کپی از ترافیک را گرفته و آنالیز کند. همچنین تأخیر کمی داشته باشد. از طرفی در این مدل اگر IDS خراب شود، تأثیری روی ترافیک نخواهد داشت.



همان‌طور که در شکل زیر مشاهده می‌کنید، IPS در مسیر ترافیک قرار می‌گیرد. یعنی ترافیک باید دقیقاً از IPS عبور کند. بنابراین ترافیک وارد حسگر امنیتی می‌شود، سپس بررسی شده و اگر حمله‌ای تشخیص داده شود جلوی آن گرفته می‌شود و در غیراین صورت ترافیک رد می‌شود.

از آنجا که IPS در مسیر ترافیک است روی ترافیک تأخیر ایجاد می‌کند، از طرفی اگر IPS قطع شود ترافیک را تحت‌تأثیر قرار می‌دهد. بنابراین مکانیزم‌هایی وجود دارد تا اگر IPS خراب شد، جلوی ترافیک را بگیرد یا آن را عبور دهد.



IDS و IPSها در لایه ۲ کار می‌کنند. بنابراین وابسته به دستگاه‌هایی مانند سوئیچ و فایروال هستند و عمل مسیریابی انجام نمی‌دهند.

سه وظیفه اصلی IDSها

۱ بررسی
۲ تشخیص
۳ برخورد با نفوذ

انواع IDS

Anomaly Based: در این روش الگوها و قواعد خاصی برای رفتارهای عادی پیدا می‌کنیم. رفتارهایی که از این الگوها پیروی نمی‌کنند و انحرافی بیش از حدمعمول دارند، به‌عنوان ناهنجاری شناخته می‌شوند. چون الگوی ثابتی وجود ندارد، آستانه انحراف را در نظر می‌گیرند. مثلاً اگر کاربری در طول روز بیش از بیست بار ورود و خروج به سیستم انجام دهد و یا ساعت ۲ بامداد به سیستم وارد شود و یا بیشتر از حد مجاز تارنمای سازمان را بازدید کند، می‌تواند به عنوان یک رفتار غیرعادی درنظر گرفته شود.

Signature_Based: در این روش یک پایگاه داده مشخص از الگوهای تعریف شده وجود دارد و درصورتی که دسترسی به سامانه با الگوهای موجود در پایگاه داده شباهت داشته باشد، نفوذ درنظر گرفته می‌شود.

IPS ترافیک موجود در سطح شبکه را نظارت و حملات و فعالیت‌های مخرب را قبل از وقوع شناسایی می‌کند. در صورت تشخیص حمله، بسته‌های مورد استفاده حمله را از بین می‌برد و به بسته‌های مجاز اجازه عبور می‌دهد.

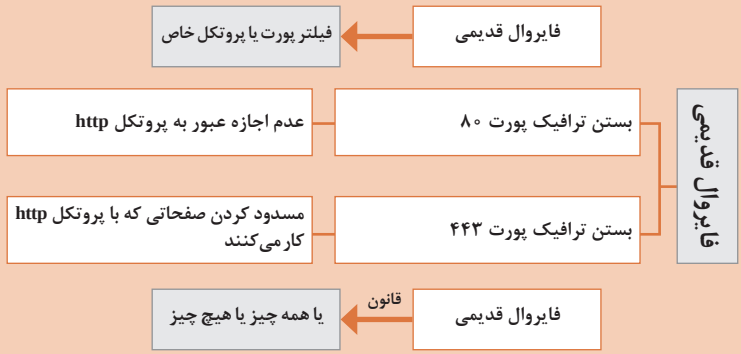
عملکرد IPS:

۱ بررسی چگونگی دسترسی با استانداردهای مشخص (بررسی پورت‌ها، پروتکل‌ها و پهنای باند مجاز برای دسترسی به سرور و تارنماها)
۲ ایجاد بانک اطلاعاتی جامع از تمام الگوهای بدافزارها و رفتار نفوذگرها و مقایسه دسترسی‌ها با این الگوها
۳ ایجاد یک فضای ذخیره‌سازی از مشخصات کاربری برای افرادی که مجاز به استفاده از سامانه هستند.

پاسخ به فعالیت‌ها

پژوهش
صفحه ۱۶۳

درباره فایروال‌های Next_Generation تحقیق کنید.



هنرآموز می‌تواند ذهن هنرجو را با این چالش مواجه کند که:
آیا می‌توانیم با فایروال مجوز استفاده از یک پورت را فقط به یک نرم‌افزار یا تارنمای خاص بدهیم؟
در ادامه شرح ویژگی‌های فایروال‌های نسل بعدی را مشاهده می‌کنیم.
ویژگی‌های فایروال‌های NGFW:

- □ امکانات استاندارد یک فایروال: (مانند فایروال‌های قدیمی)
  - ✓ مسدود کردن پورت‌ها و پروتکل‌ها
  - ✓ دارای سرویس شبکه خصوصی مجازی (VPN) و NAT
- □ شناسایی و فیلترینگ نرم‌افزارها:
  - ✓ تشخیص نوع ترافیک یک نرم‌افزار و فیلترینگ پورت یا سرویس براساس نوع نرم‌افزار
  - ✓ جلوگیری از نرم‌افزارهای مخرب در استفاده از پورت‌های معمول و غیرمعمول برای ورود به شبکه و آسیب‌رسانی
- □ واکاوی SSH و SSL :
  - ✓ واکاوی ترافیک رمزنگاری شده پروتکل‌های SSL و SSH
  - ✓ رمزگشایی ترافیک و رمزگذاری و ارسال پس از تأیید سالم‌بودن و عدم وجود ترافیک غیرمجاز
  - ✓ جلوگیری از مخفی‌شدن کدهای مخرب در ترافیک رمزنگاری شده به‌وسیله نرم‌افزارهای مخرب
  - ✓ جلوگیری از ورود ترافیک به شبکه
- □ تشخیص و پیشگیری از نفوذ
- □ هماهنگی با سرویس‌های Active Directory
- □ فیلترینگ کدهای مخرب:
  - ✓ جلوگیری از فعالیت کدهای مخرب با شناسایی تارنماهای مخرب و ذخیره آنها در پایگاه داده
  - ✓ تشخیص و جلوگیری از برخی حملات مانند Phishing و شناسایی ویروس‌ها و تروجان‌ها

کارگاه ۵ــ فعال‌سازی فایروال سیستم‌عامل

هدف از این کارگاه آموزش نحوه کار با فایروال نرم‌افزاری است. ویندوز به‌طور پیش‌فرض برای همه پروفایل‌ها inbound connections را مسدود می‌کند و به outbound connections اجازه عبور می‌دهد. اما می‌توان outbound connectionsها را نیز بلوکه کرد و قوانینی برای عبور نوع خاصی از اتصالات ایجاد کرد. اگر outbound connectionsها را مسدود کنید، زمانی که یک برنامه مسدود می‌شود اخطاری را دریافت نخواهید کرد.

پاسخ به فعالیت‌ها

پژوهش
صفحه ۱۶۵

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

نام دستور	روش استفاده
SC	SC Stop <Firewall service name>
	SC Start <Firewall service name>
NET	Net Stop <Firewall service name> NET Stop “Windows Firewall”
	Net Start MpsSvc
REG	Reg Add HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile /V EnableFirewall /T REG_DWORD /D “۰” /F
	برای فعال‌سازی فایروال در دستور بالا به‌جای عدد ۰ از ۱ استفاده می‌کنیم.
Netsh	Netsh Firewall Set Opmode Disable
	Netsh Firewall Set Opmode Enable

پژوهش
صفحه ۱۶۶

قسمت Connection Security Rules برای چه نوع ارتباطاتی کاربرد دارد؟
این گزینه که جزء تنظیمات پیشرفته (Advanced Setting) فایروال ویندوز است، در سمت چپ پنجره فایروال ویندوز قرار دارد و قوانین مربوط به ارتباطات مختلف مانند تونل، تشخیص هویت و غیره در این قسمت هستند.

فعالیت کارگاهی
صفحه ۱۶۶

با توجه به نوع ارتباطات جدول زیر را کامل کنید.

نوع درخواست	نوع Rule
هیچ رایانه‌ای نتواند از اینترنت به سیستم دسترسی پیدا کند.	Inbound
روی این سیستم تارنمای گوگل فیلتر شود.	Outbound
ارتباط یک برنامه مشخص با اینترنت فیلتر شود.	Outbound
محدود کردن دسترسی	Inbound

تکمیل کارگاه
صفحه ۱۶۶

قوانین فایروال ویندوز	
مسدود کردن/ مجوز دادن به یک برنامه	Program
مسدود کردن/ مجوز دادن به یک درگاه، محدوده درگاه یا پروتکل	Port
قانون فایروال از پیش تعریف شده ویندوز (مانند Remote Desktop)	Predefined
ترکیبی از برنامه، درگاه و آدرس IP را برای مسدود کردن یا مجوزدادن مشخص می‌کند.	Custom

مثال ۱: ارتباط یک برنامه مشخص با اینترنت را فیلتر کنید.
از جست‌وجوی ویندوز برنامه Windows Defender Firewall with Advanced Security را باز کنید.
۱ سمت چپ گزینه Outbound Rules را انتخاب کنید.
۲ سمت راست از ناحیه Action گزینه New Rule... را بزنید.
۳ در کادر باز شده گزینه Program را انتخاب و دکمه Next را بزنید.
۴ با دکمه Browse مسیر پرونده اجرایی برنامه مورد نظر را انتخاب کنید.
۵ در صفحه Action، Block the connection را انتخاب کنید.
تمرین: دسترسی همه برنامه‌ها به جز برنامه‌های خاصی را به اینترنت مسدود کنید.
تمرین: برنامه را تنها زمانی که به یک شبکه عمومی وصل می‌شود، مسدود کنید.
تمرین: یکی از قوانینی را که ساخته‌اید غیرفعال یا حذف کنید.
مثال ۲: یک برنامه را از طریق درگاه و آدرس IP که برنامه به آن متصل است مسدود کنید.
۱ یک قانون از نوع Inbound و Custom تعریف کنید.
۲ برنامه‌ای را که می‌خواهید محدودش کنید، انتخاب کنید.
۳ در کادر Protocol and Ports نوع پروتکل و درگاه را مشخص کنید(مثلاً ۸۰ و ۴۴۳). Next را بزنید.
۴ در کادر بعدی Allow the connection را بزنید.

فعالیت کارگاهی
صفحه ۱۶۷

در فایروال ویندوز رولی بنویسید که رایانه شما نتواند از DHCP Server کارگاه رایانه، آدرس IP بگیرد.
زمانی‌که یک رایانه در شبکه قرار می‌گیرد، درخواست خود را برای اختصاص IP به پروتکل DHCPS از نوع UDP و شماره ۶۷ ارسال می‌کند و منتظر پاسخ از پروتکل dhcpc به شماره درگاه ۶۸ می‌شود.
ابتدا با حساب مدیر وارد شوید و در پنجره Windows Defender Firewall از Control Panel گزینه Advanced Settings از منوی سمت چپ را بزنید.
یک رول جدید از نوع Inbound تعریف کنید. گزینه port و سپس UDP با شماره درگاه ۶۷ را وارد کنید.

فایروال سخت‌افزاری

فایروال میکروتیک امکان تعریف رول‌های مختلف براساس پارامترهای متعدد را در اختیار مدیر شبکه قرار می‌دهد. این امر سبب شده تا امروزه روترهای میکروتیک به عنوان فایروال نرم‌افزاری و سخت‌افزاریِ محبوب و ارزان قیمت شناخته شوند.
یکی از قابلیت‌های فایروال ایجاد فیلترینگ است. در فیلترینگ بسته‌هایی که از روتر عبور می‌کنند تحت کنترل قرار می‌گیرند و براساس قوانینی که به آنها Rule گفته می‌شود فیلتر می‌شوند. فایروال براساس رول‌های تعیین شده کار می‌کند.

هر رول از دو قسمت تشکیل شده است:
قسمت اول: ترافیک بسته‌ها را مشخص می‌کند (ترافیک ورودی و یا خروجی از میکروتیک).
قسمت دوم: عملیاتی است که روی بسته‌ها انجام می‌شود.
مثال‌هایی از زنجیره‌های ترافیک در فایروال:
Input Chain: بسته‌هایی که مقصدشان میکروتیک است.
- ارسال بسته‌های ICMP برای Ping کردن روتر میکروتیک
- اتصال به میکروتیک با استفاده از WinBox و SSH و...

Output Chain: بسته‌هایی که از روتر میکروتیک خارج می‌شوند.
- بسته‌هایی که از داخل روتر به سیستم یا دستگاهی Telnet می‌زنند.

روتر سعی در اتصال به سرویس‌دهنده‌های DNS و NTP و... را داشته باشد.
Forward Chain: ترافیکی که از روتر عبور می‌کند.
- فرایند ارسال بسته از یک کارت شبکه روتر به کارت شبکه دیگر آن
- یک سیستم داخلی درخواست تارنمایی را از اینترنت داشته باشد و روتر نقش Gateway در شبکه را داشته باشد.

هر زمان بسته‌ای وارد میکروتیک شود، از این زنجیره‌ها عبور کرده و در جدول‌ها (Filter، Nat و Mangle) مورد پردازش قرار می‌گیرد.

تمرین

مسدودسازی دسترسی به Telnet

روش سوم دسترسی به میکروتیک، پروتکل Telnet است. برای دسترسی از طریق telnet باید از محیط cmd اقدام کنید. در این روش، محیط میکروتیک به‌صورت گرافیکی نیست. بنابراین لازم است توانایی کار در محیط دستوری میکروتیک را داشته باشید. پروتکل telnet به‌صورت پیش‌فرض روی پورت شماره ۲۳ کار می‌کند. در این سناریو قصد داریم با مسدودسازی، از دسترسی افراد به telnet، از طریق شبکه داخلی و اینترنت جلوگیری کنیم. مراحل را دنبال کنید:

۱ یک رول جدید تعریف کنید. در پنجره New Firewall Rule از سربرگ General نوع Chain را روی Input قرار دهید.

۲ نوع Action را از سربرگ آن روی drop قرار دهید. (در اینجا پروتکل tcp با شماره پورت مربوط به telnet را drop می‌کنیم.)

نکته: در ویندوز برای فعال کردن سرویس telnet باید در محیط جست‌وجو یا منوی استارت عبارت windows features را تایپ کرده، گزینه Turn Windows features on or off را انتخاب کنید، سپس از پنجره باز شده گزینه Telnet Client را فعال کنید.

بهتر است ارتباط telnet روی میکروتیک را ببندیم. زیرا ارتباط امنی نیست. به این دلیل که اطلاعات را به‌صورت آشکار ارسال می‌کند. بنابراین می‌توان به جای Telnet از SSH استفاده کرد.

کارگاه ۸ـ مسدودسازی دسترسی به WinBox از طریق مک آدرس

این کارگاه را می‌توانید با یک تمرین ساده شروع کنید.

تمرین

هیچ سیستمی نتواند از طریق Winbox به روتر متصل شود.

از منوی اصلی گزینه IP و از زیرمنوی بازشده Firewall را انتخاب می‌کنیم. در پنجره بازشده از بخش FilterRule روی ADD کلیک می‌کنیم. در پنجره باز شده فیلتر مورد نظر را ایجاد می‌کنیم. برای دیدن فهرست پورت‌ها از منوی اصلی گزینه IP و از زیرمنوی بازشده Services را انتخاب می‌کنیم. در پنجره بازشده فهرست پورت‌ها نشان داده می‌شود.

پاسخ به فعالیت‌ها

تکمیل کارگاه
صفحه ۱۷۴

اگر بخواهید رایانه‌ای را که با آدرس‌های IP متعدد قصد ورود به میکروتیک شما را دارد بلاک کنید، تنها راه بلاک کردن آدرس مک آن است.

مراحل مسدودسازی آدرس مک:

۱ با WinBox به میکروتیک متصل شوید.

۲ از منوی IP، گزینه Firewall را انتخاب کنید.

۳ از بخش Filter Rules روی علامت + (دکمه New Filter Rule) برای تنظیمات رول جدید کلیک کنید.

۴ نوع بسته را در بخش Chain روی Input قرار دهید.

۵ از سربرگ Advanced آدرس مک مورد نظر را در قسمت Src. Mac Address بنویسید.

۶ از سربرگ Action گزینه Action را روی Drop قرار دهید.

۷ دکمه Apply و سپس Ok را بزنید.

فعالیت کارگاهی
صفحه ۱۷۵

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.

- **به مراحل قبلی که در کارگاه ۸ نوشتید یک رول جدید از نوع Forward اضافه کنید.**
- **آدرس مبدأ (Src. Address) را روی IP مدیر تنظیم کنید تا اجازه دسترسی داشته باشد.**
- **از زبانه Action گزینه Accept را انتخاب کنید.**
- **اما این رول هیچ‌گاه بررسی نمی‌شود. زیرا به‌وسیله رول قبلی مسدود می‌شود.**
- **برای حل این مسئله ترتیب رول‌ها را با درگ کردن جابه‌جا می‌کنیم. به این ترتیب با اولویت‌بندی محدودیت دسترسی مدیر را از بین می‌بریم.**

به‌طور کلی بهتر است رول‌هایی که اکشن آنها Accept است و سپس رول‌هایی با اکشن drop نوشته شوند.

دقت داشته باشید در فایروال میکروتیک ترتیب اعلام قوانین از بالا به پایین است و اگر رولی مبنی بر Accept برای Ping تنظیم شده باشد و بالاتر از رول فعلی قرار بگیرد، Ping بسته نخواهد شد.

کارگاه ۹ــ مسدودسازی ping به میکروتیک

هدف از این کارگاه حفاظت از شبکه در مقابل حملات DDoS است. می‌خواهیم به درخواست‌های ping پاسخ داده شود ولی نه به‌صورت کامل تا در عیب‌یابی با مشکلی مواجه نشویم.

پاسخ به فعالیت‌ها

تکمیل کارگاهی
صفحه ۱۷۵

اکشن Tarpit دقیقاً مانند Drop، بسته‌ها را حذف می‌کند. اما یک تفاوت اساسی هم با Drop دارد. اگر به‌جای drop از اکشن tarpit استفاده کنید، Session بسته نمی‌شود و به نوعی هنگ می‌کند. در این حالت هکر یا کلاینت نمی‌تواند بفهمد که دسترسی او محدود شده یا اینکه مسیر ارتباطی مشکل دارد و یا مشکل دیگری وجود دارد. این اکشن بیشتر برای حفظ امنیت به‌کارمی‌رود.

فعالیت کارگاهی
صفحه ۱۷۶

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

در صورتی که بخواهیم فقط یکی از کلاینت‌های شبکه داخلی بتواند میکروتیک را Ping کند، از اکشن Accept استفاده می‌کنیم. زیرا هر رولی که با این اکشن نوشته شود به معنی این است که فایروال به بسته‌های این ارتباط اجازه عبور داده را می‌دهد.

- **یک رول جدید از نوع input ایجاد می‌کنیم.**
- **آدرس مبدأ (Src. Address) را روی IP مدیر تنظیم می‌کنیم.**

کارگاه ۱۱ــ گزارش‌گیری از عملکرد فایروال

اکشن **Passthrough** نیز به نوعی برای گزارش‌گیری استفاده می‌شود. این اکشن مانند یک شمارنده عمل می‌کند و فقط تعداد بسته‌های رسیده از پروتکل تعیین شده را محاسبه می‌کند. اما همانند **Log** روی میکروتیک بار پردازشی ایجاد نمی‌کند و بیشتر برای آمارگیری و مباحث کیفیت سرویس به‌کار می‌رود.
اکشن **FastTrack Connection** مصرف منابع **RAM** و **CPU** را کاهش می‌دهد.
اکشن **Jump**: هر چه تعداد رول‌های فایروال بیشتر شود، بار ترافیکی بیشتری روی روتر ایجاد می‌شود. در نتیجه .**RAM** و **CPU** بیشتر درگیر می‌شوند و کارایی سیستم پایین می‌آید.
برای حل این مشکل می‌توان خطوط رول‌ها را دسته‌بندی کرد تا بسته‌ای که وارد می‌شود، فقط با رول‌های متناظر مطابقت داده شود و با همه رول‌ها درگیرنشود. به‌عنوان مثال رول‌های **icmp** را دسته‌بندی می‌کنیم تا زمانی که یک بسته **icmp** وارد فایروال می‌شود، فقط با رول‌های **icmp** بررسی و مطابقت یابد.

تمرین: رول‌های مربوط به **icmp** را دسته‌بندی و برای آنها رول‌های مسدودسازی بنویسید.

- ابتدا یک سرگروه برای این پروتکل ایجاد می‌کنید.
- نوع آن را **input** قرار دهید.
- در سربرگ **Action** نوع آن را **jump** و در مقابل **Jump Target** یک نام دلخواه برای گروه انتخاب کنید.

حال می‌توانیم رول‌های مورد نظر را در این گروه تعریف کنیم.

- یک رول با اکشن **log** تعریف کنید و نوع آن را روی نام گروه تنظیم کنید، سپس آدرس مبدأ را **192.168.100.1** قرار دهید.

بنابراین اگر از سمت **192.168.100.1** یک بسته با نامی بیاید که برای گروه قرار دادید، از آن **Log** می‌گیرد.
اکشن **Return** زمانی که بخواهیم در برنامه‌نویسی از یک حلقه خارج شویم، به‌کارمی‌رود. در اینجا هم عملکردی مشابه دارد. یعنی اگر یک دسته رول برای یک پروتکل نوشته باشیم و بخواهیم از چرخه خارج شویم، از این رول استفاده می‌کنیم.

تکمیل کارگاهی
صفحه ۱۷۷

فیلترینگ تارنما یا اپلیکیشن

میکروتیک یک ابزار امنیتی قدرتمند برای مسدودسازی تارنما است. می‌خواهیم دسترسی به تارنمای فیسبوک و یوتیوب و... را برای کاربران شبکه داخلی مسدود کنیم. برای مسدودسازی چنین تارنماهایی لازم است رول‌های فایروالی ایجاد کنیم که هر ارتباطی از طریق روتر میکروتیک به این تارنماها را **drop** کند.
هر رول فیلترینگ میکروتیک دو بخش دارد:

۱ بخش شرط (**Condition**) شامل خصوصیات شرط مانند:

- نوع زنجیره ترافیک (**chain**)
- آدرس مبدأ (**Source Address**)
- آدرس مقصد (**Destination Address**)

تکمیل کارگاهی
صفحه ۱۷۸

- نوع پروتکل (Protocol Type)
- درگاه مبدأ (Source Port)
- درگاه مقصد (Destination Port)
- و مقدار پروتکل لایه ۷

۲ بخش عمل (Action)

با انتخاب اکشن drop هر ترافیکی مسدود می‌شود.

Regex (Regular Expressions) الگویی برای جایگذاری عبارت در رشته است. این عباراتِ باقاعده که به‌وسیله بیشتر زبان‌های برنامه‌نویسی پشتیبانی می‌شوند مانند هر زبانی دارای syntax و دستورات مخصوص به خود است. کاربرد اصلی Regex، جست‌وجوی عبارات یا جست‌وجو و جایگزینی عبارت در متن است.

پروتکل لایه ۷ از Regex برای مطابقت واژه کلیدی با آدرس URL استفاده می‌کند. بنابراین می‌توان هر ترافیکی که از واژه‌های کلیدی فیسبوک، یوتیوب و... استفاده می‌کنند را مسدود کنیم.

پروتکل لایه ۷، یک روش جست‌وجوی الگو در جریان داده ICMP، UDP و TCP است. تطبیق‌دهنده لایه ۷، ۱۰ بسته اولیه یا ۲ کیلوبایت اولیه جریان ارتباطی را جمع‌آوری و الگو را در داده جمع‌آوری شده جست‌وجو می‌کند. اگر الگو در داده جمع‌آوری شده پیدا نشد، به جست‌وجو ادامه نمی‌دهد. در این‌صورت حافظه اختصاص داده شده به این کار خالی شده و پروتکل به‌عنوان ناشناخته در نظر گرفته می‌شود. باید به این نکته توجه داشته باشید که مصرف حافظه با افزایش تعداد ارتباطات به‌طور قابل توجهی بیشتر خواهد شد.

از آنجا که تطبیق‌دهنده لایه هفتم به ارتباط دوطرفه (ورودی/خروجی) برای بررسی بسته‌ها نیاز دارد، باید قانون‌های لایه هفتم را در زنجیره Forward قرار دهیم.

جدول زیر برخی قوانین Regex که در نوشتن الگو استفاده می‌شود را نشان می‌دهد.

عبارت	توضیح عملکرد
[abc]	انتخاب یکی از نویسه‌های a، b یا c در متن
[^abc]	انتخاب هر نویسه‌ای به جز a، b یا c علامت ^ در [] به‌معنی Not است.
[a-z]	انتخاب هر کاراکتری در محدوده a تا z
[a-zA-Z]	انتخاب هر نویسه‌ای در محدوده a تا z یا A تا Z
^	شروع خط
$	پایان خط
\A	شروع رشته
\z	پایان رشته
.	هر نویسه تکی (به جز خط جدید یا line break)
\s	هر نویسه از نوع whitespace
\S	هر نویسه به‌جز whitespace

عبارت	توضیح عملکرد
/[\s]/	انتخاب فضاهای خالی وspace های متن
\d	انتخاب نویسه عددی (۰ تا ۹)
\D	انتخاب نویسه غیرعددی
\w	هر نوع نویسه از نوع کلمه به‌جز فضاهای خالی (حروف، اعداد و زیرخط)
\W	هر نوع نویسه به‌جز کلمه (نویسه‌های به‌جز حروف، اعداد و زیرخط)
\b	اولین یا آخرین نویسه رشته از نوع کلمه (حروف، اعداد و زیرخط) Boundary به معنای مرز است.
\t	فاصله‌هایی که به واسطه زدن دکمه Tab در متن ایجاد شده است را انتخاب می‌کند.
(a|b)	a یا b
a?	هیچ یا یک a
a*	هیچ یا هر تعداد a (صفر یا بیشتر)
a+	یک یا هر تعداد a
a{۳}	دقیقاً ۳ عدد a

مثال	کاربرد
\[g-s]\	انتخاب تمام حروف بین g و s
"^Net"	انتخاب تمام رشته‌هایی که با Net شروع می‌شوند.
"net$"	انتخاب تمام رشته‌هایی که به net ختم می‌شوند.
"^abc$"	انتخاب رشته‌ای که با abc شروع و به آن نیز ختم می‌شود. (برای پیداکردن دقیقاً یک رشته مورد نظر به‌کار می‌رود.)
[o]\b	انتخاب تمام حروف o در متن به شرطی که حرف o در مرز بین کلمات باشد و اگر در وسط کلمه‌ای مانند (tool) باشد آن را انتخاب نمی‌کند.
[o]\B	تمام حروف o را انتخاب می‌کند به‌شرطی‌که در مرز کلمات نباشد و اول یا وسط کلمه باشد.
b(a|e|i)d	با رشته‌هایی که حرف اول آنها b و حرف دوم یکی از حروف a، e یا i باشد و حرف سوم آنها هم d باشد مطابقت دارد.
۱۲۳?۴	عدد ۳ اختیاری است. پس با اعداد ۱۲۴ و ۱۲۳۴ مطابقت دارد.
ab*	با رشته‌های ac، abc، abbc و... مطابقت دارد.
b\w+	تمام حروف b که بعدش ۱ یا بیشتر نویسه است را انتخاب می‌کند.

کارگاه ۱۲ــ فیلترینگ تارنما و اپلیکیشن

هدف از این کارگاه ایجاد پروتکل لایه ۷ و مسدودسازی تارنما با استفاده از regex است.

تکمیل کارگاهی
صفحه ۱۸۰

گام اول: ایجاد پروتکل لایه ۷ برای انتخاب تارنمای موردنظر

- پنجره **WinBox** را باز کنید. از منوی سمت چپ، گزینه **IP** را انتخاب کنید. از منوی ظاهر شده **Firewall** را انتخاب کنید. سپس روی سربرگ **Layer7 Protocols** کلیک کنید.
- روی دکمه + برای ایجاد یک پروتکل لایه ۷ جدید با **regex** کلیک کنید.
- در کادر ورودی **Name**، یک نام درنظر بگیرید. (می توانید نام تارنمایی که می خواهید دسترسی آن را مسدود کنید را بنویسید.)
- در فیلد ورودی **regex** عبارت «**^.*(facebook.com).*$**» را بنویسید.
- دکمه **Apply** و سپس **OK** را بزنید.

یادداشت: برای مسدودسازی تارنمای یوتیوب از نام youtube.com در regex استفاده کنید.

^.*(youtube.com).*$

همچنین می توانید در فیلد regex عبارت «^.*(youtube.com|facebook.com).*$» را بنویسید. اسامی سایر تارنماها را هم می توانید با قرار دادن « | » بین اسامی آنها اضافه کنید.

گام دوم: ایجاد رول فایروال برای مسدودسازی تارنمای انتخابی

- در سربرگ **Filter Rules** روی دکمه + کلیک کنید تا پنجره **New Firewall Rule** ظاهر شود.
- در سربرگ **General**، از لیست **Chain** گزینه **Forward** را انتخاب کنید.
- از آنجاکه می خواهیم دسترسی همه کاربران را مسدود کنیم، آدرس مبدأ و مقصد را خالی رها می کنیم. برای مسدود کردن دسترسی کاربر خاص، آدرس IP او را در **Src. Address** می نویسیم.
- از لیست **Protocol**، (**tcp**) را انتخاب کنید.
- در سربرگ **Advanced** از لیست **Layer7 Protocol**، پروتکل لایه ۷ را که قبلاً اینجا کردید انتخاب کنید.
- در سربرگ **Action** گزینه **drop** را انتخاب کنید.
- دکمه **Apply** و سپس **OK** را بزنید.

رول بالا دسترسی همه کاربران را به تارنمای موردنظر مسدود می کند. گاهی می خواهیم دسترسی این تارنما برای کاربر خاصی فعال باشد. برای این منظور یک رول دیگر از نوع Accept ایجاد می کنیم و در Src Address، آدرس IP کاربر موردنظر را می نویسیم. سپس اولویت رول Accept را قبل از رول Drop قرار می دهیم.

مراحل:

- در سربرگ **Filter Rules** روی دکمه + کلیک کنید تا پنجره **Firewall Rule** ظاهر شود.
- در سربرگ **General**، از لیست **Chain** گزینه **Forward** را انتخاب کنید.
- در کادر ورودی **Src. Address**، آدرس IP کاربری که می خواهیم به تارنمای مسدود شده، دسترسی داشته باشد را می نویسیم.

- از لیست **Protocol**، (**tcp**) را انتخاب کنید.
- در سربرگ **Advanced** از لیست **Layer7 Protocol**، پروتکل لایه ۷ را که قبلاً اینجا کردید و می‌خواهید اجازه آن را به کاربر بدهید، انتخاب کنید.
- در سربرگ **Action** گزینه **accept** را انتخاب کنید.
- دکمه **Apply** و سپس **OK** را بزنید.

روش دوم: برای انجام عملیات بالا با استفاده از ترمینال کدهای زیر را تایپ کنید. (در کد زیر از نام **Block** برای تعریف پروتکل استفاده شده است)

```
/ip firewall layer7-protocol
add name=Block
regexp="^.*(youtube.com|facebook.com).*\$"
/ip firewall filter
add action=reject chain=forward layer7-protocol=Block
```

نکته: برخی از نمادها و دستورات **Regex** مخصوص یک یا چند زبان برنامه‌نویسی خاص هستند و در زبان دیگری کاربرد ندارند.