با ایران توشه
یک قدم جلوتر
باش!

ایران توشه
توشه ای برای موفقیت



ایران توشه، مرجع دانلود فایل های کمک آموزشی دانش آموزان و کنکوری ها

همه چیز
برای موفقیت
تو!

- دانلود رایگان آزمون های آزمایشی قلمچی، خیلی سبز، گاج و ...
- دانلود رایگان گام به گام تمامی دروس
- دانلود رایگان نمونه سوالات امتحانی (نوبت اول و دوم) و امتحانات نهایی
- دانلود رایگان جزوه های کمک آموزشی و شب امتحانی

کافیست هر فایلی که نیاز دارید را در گوگل به این صورت جستجو کنید:

فایل مورد نیاز + ایران توشه

مثال:

دانلود گام به گام دوازدهم تجربی ایران توشه



irantooshe.ir

t.me/irantooshe

گام به گام تجارت الکترونیک و امنیت
شبکه دوازدهم
پودمان چهارم

عنوان فصل: تنظیمات امنیت شبکه

از صفحه‌ی ۱۴۷ تا صفحه‌ی ۱۸۲ کتاب

در این فایل پاسخ فعالیت‌ها، کارهای کلاسی، تمرین‌ها و پرسش‌های فصل تنظیمات امنیت شبکه آمده است.

مباحث فصل: تست آسیب‌پذیری، فازهای نفوذ، فایروال نرم‌افزاری و فایروال میکروتیک

تهیه‌شده در ایران‌توشه، توشه‌ای برای موفقیت

irantooshe.ir

فهرست پرسش‌ها

۱ صفحه ۱۴۹ · فعالیت گروهی — انتخاب اقدام امنیتی مناسب ۵

۲ صفحه ۱۵۱ · فعالیت کارگاهی — مصداق اصطلاحات امنیتی ۵

۳ صفحه ۱۵۱ · پژوهش — انواع هکرهای کلاه‌رنگی ۵

۴ صفحه ۱۵۵ · کنجکاوی — شماره درگاه‌های متداول ۶

۵ صفحه ۱۶۲ · کنجکاوی — فایروال برای آموزشگاه رایانه ۷

۶ صفحه ۱۶۳ · پژوهش — فایروال‌های Next-Generation ۷

۷ صفحه ۱۶۴ · کارگاه ۵ — فعال‌سازی فایروال سیستم‌عامل ۷

۸ صفحه ۱۶۵ · پژوهش — فعال و غیرفعال کردن فایروال ویندوز در CMD ۸

۹ صفحه ۱۶۶ · فعالیت کارگاهی — نوع Rule بر اساس نوع ارتباط ۸

۱۰ صفحه ۱۶۷ · فعالیت کارگاهی — رول مسدودکردن دریافت IP از DHCP در فایروال ویندوز ۸

ایران توشه
توشه ای برای موفقیت

۱۱ صفحه ۱۶۸ · کارگاه ۶ — فعال‌سازی گزارش‌گیری فایروال ویندوز ۹

۱۲ صفحه ۱۶۹ · فعالیت گروهی — تهیه و مقایسه‌ی گزارش فایروال ۹

۱۳ صفحه ۱۷۲ · کارگاه ۷ — مسدودکردن دسترسی WinBox از شبکه‌ی خارجی ۱۰

۱۴ صفحه ۱۷۴ · کارگاه ۸ — مسدودسازی WinBox از طریق مک‌آدرس ۱۰

۱۵ صفحه ۱۷۵ · فعالیت کارگاهی — فقط مدیر شبکه از طریق WinBox متصل شود ۱۰

۱۶ صفحه ۱۷۵ · کارگاه ۹ — مسدودسازی ping به میکروتیک ۱۱

۱۷ صفحه ۱۷۶ · فعالیت کارگاهی — فقط مدیر شبکه بتواند شبکه‌ی خارجی را ping کند ۱۱

۱۸ صفحه ۱۷۶ · کارگاه ۱۰ — شناسایی افرادی که مسیریاب را ping می‌کنند ۱۲

۱۹ صفحه ۱۷۷ · کارگاه ۱۱ — گزارش‌گیری از ترافیک وب و FTP در فایروال ۱۲

۲۰ صفحه ۱۷۹ · فعالیت کارگاهی — آزمودن Regex ۱۲

۲۱ صفحه ۱۸۰ · کارگاه ۱۲ — مسدودسازی تارنمای گوگل با فیلترینگ لایه ۷ ..... ۱۳

۲۲ صفحه ۱۸۱ · فعالیت کارگاهی — Regex اپلیکیشن‌ها و مسدودسازی ترافیک ناشناخته ۱۳

۱ صفحه ۱۴۹ فعالیت گروهی

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

اقدام امنیتی مناسب

مورد	اقدام امنیتی
کیف کارت‌های اعتباری	در دسترس قرار ندادن گذرواژه‌ی شخصی و استفاده نکردن از یک گذرواژه‌ی واحد
رایانه‌ی همراه	تهیه‌ی نسخه‌ی پشتیبان از اطلاعات مهم و استفاده از گذرواژه‌ی قوی
گوشی هوشمند	استفاده از الگوی قفل و فعال کردن حالت خاموش شدن به هنگام سرقت
منزل مسکونی	اطمینان از سالم بودن قفل‌ها و استفاده از دوربین مداربسته، دزدگیر و حفاظ
خودرو شخصی	اطمینان از سالم بودن قفل‌ها و استفاده از دزدگیر

این جواب ممکن است دقیق نباشد.

۲ صفحه ۱۵۱ فعالیت کارگاهی

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

مصداق اصطلاحات

اصطلاح	مثال
دارایی	اطلاعات حساب مشتریان بانک، پرونده‌ی تحصیلی دانش‌آموزان
آسیب‌پذیری	نصب نبودن به‌روزرسانی سیستم‌عامل، گذرواژه‌ی ضعیف، درگاه باز بدون نظارت
تهدیدات امنیتی	ویروس و بدافزار، دسترسی غیرمجاز، قطع برق یا خرابی تجهیزات
سازوکار امنیتی	فایروال، آنتی‌ویروس، دوربین مداربسته و دستگاه حضور و غیاب
حمله	ارسال رایانامه‌ی آلوده برای نصب بدافزار روی سیستم کاربر

این جواب ممکن است دقیق نباشد.

۳ صفحه ۱۵۱ پژوهش

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

- **کلاه سفید:** هکر قانونمند که با مجوز سازمان تست نفوذ می‌کند تا امنیت را بالا ببرد.

- **کلاه سیاه:** هکر غیرقانونی (کراکر) که برای تخریب یا سرقت اطلاعات نفوذ می‌کند.
- **کلاه خاکستری:** گاهی قانونی و گاهی غیرقانونی عمل می‌کند.
- **کلاه آبی:** متخصصی که پیش از عرضه، نرم‌افزار را برای یافتن ضعف آزمایش می‌کند یا فردی برای انتقام‌جویی.
- **کلاه سبز:** تازه‌کار علاقه‌مند به یادگیری هک.
- **کلاه قرمز:** مدافعی که با مهاجمان سیاه مقابله می‌کند.

این جواب ممکن است دقیق نباشد.

۴ صفحه ۱۵۵ کنجکاوی

جدول شماره‌ی درگاه و کاربرد (سرویس) را کامل کنید.

درگاه‌های متداول

شماره‌ی درگاه	سرویس
80	وب (HTTP)
443	وب امن (HTTPS)
23	Telnet (مدیریت از راه دور بدون رمزنگاری)
22	SSH (مدیریت از راه دور امن)
53	DNS
21	FTP (انتقال فایل)
8192	برنامه‌ی خاص (احتمالاً سرویس‌های مدیریتی/آنتی‌ویروس)

این جواب ممکن است دقیق نباشد.

این فایل توسط سایت ایران‌توشه تهیه شده است.
irantooshe.ir

۵ صفحه ۱۶۲ کنجکاوی

آیا با نصب فایروال در این آموزشگاه، مشکل حل می‌شود؟ اگر پاسخ شما بلی است، چه نوع فایروالی را پیشنهاد می‌دهید؟ چرا؟

بله، تا حد زیادی. فایروال می‌تواند سایت‌ها و برنامه‌های پرمصرف و آلوده را مسدود، دسترسی هر کارگاه را محدود و ترافیک ورودی مخرب را متوقف کند. چون سه کارگاه و چند مدرس مستقل داریم و نیاز به کنترل متمرکز، گزارش‌گیری و مدیریت پهنای باند هست، یک **فایروال سخت‌افزاری** (مثل فایروال/مسیریاب میکروتیک) پیشنهاد می‌شود و روی رایانه‌ها هم فایروال نرم‌افزاری و آنتی‌ویروس فعال بماند. همچنین پراکسی‌سرور برای کنترل مصرف اینترنت مفید است.

این جواب ممکن است دقیق نباشد.

۶ صفحه ۱۶۳ پژوهش

درباره‌ی فایروال‌های Next-Generation تحقیق کنید.

فایروال نسل بعد (NGFW) علاوه بر فیلتر بسته‌ها (IP و درگاه) و بررسی وضعیت اتصال، لایه‌ی برنامه را هم می‌شناسد و امکانات زیر را یک‌جا ارائه می‌دهد:

- شناسایی و کنترل برنامه‌ها (مثلاً مسدودکردن یک شبکه‌ی اجتماعی خاص)
- سیستم تشخیص و جلوگیری از نفوذ (IDS/IPS)
- بازرسی عمیق بسته‌ها (DPI) و بازرسی ترافیک رمزشده
- فیلتر وب و آنتی‌ویروس و هوش تهدید
- شناسایی کاربر (نه فقط آدرس IP)

این جواب ممکن است دقیق نباشد.

ایران توشه
توشه ای برای موفقیت

۷ صفحه ۱۶۴ کارگاه ۵

فایروال ویندوز را فعال کنید.

1. از Control Panel گزینه‌ی Windows Defender Firewall را باز و بررسی می‌کنیم کدام فایروال (ویندوز یا آنتی‌ویروس) فعال است.
2. اگر آنتی‌ویروس نقش فایروال را دارد، فایروال شخصی آن را از تنظیمات آنتی‌ویروس غیرفعال می‌کنیم.

3. گزینه‌ی Turn Windows Defender Firewall on or off را انتخاب می‌کنیم.
4. هر دو گزینه‌ی Private network و Public network را روی Turn on می‌گذاریم و OK می‌زنیم.

۸ صفحه ۱۶۵ پژوهش

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

با دسترسی مدیر (Run as administrator):

```
netsh advfirewall set allprofiles state on
netsh advfirewall set allprofiles state off
```

این جواب ممکن است دقیق نباشد.

۹ صفحه ۱۶۶ فعالیت کارگاهی

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

نوع Rule

نوع درخواست	Rule نوع
هیچ رایانه‌ای از اینترنت نتواند به این سیستم دسترسی پیدا کند.	Inbound
روی این سیستم تارنمای گوگل فیلتر شود	Outbound
فقط رایانه‌های شبکه‌ی داخلی بتوانند به سرویس وب این سیستم دسترسی داشته باشند	Inbound

این جواب ممکن است دقیق نباشد.

ایران توشه
توشه ای برای موفقیت

۱۰ صفحه ۱۶۷ فعالیت کارگاهی

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

1. در Windows Defender Firewall گزینه‌ی Advanced settings را باز می‌کنیم.
2. Inbound Rules را انتخاب و New Rule را می‌زنیم.
3. نوع رول را Port انتخاب می‌کنیم.
4. پروتکل UDP و درگاه محلی 68 (درگاه سرویس‌گیرنده‌ی DHCP) را وارد می‌کنیم.
5. گزینه‌ی Block the connection را انتخاب می‌کنیم.

6. پروفایل‌ها (Domain, Private, Public) را انتخاب و برای رول نام (مثلاً Block DHCP) می‌گذاریم.
7. برای آزمایش، کارت شبکه را غیرفعال و فعال می‌کنیم؛ دیگر آدرس IP از DHCP دریافت نمی‌شود.

این جواب ممکن است دقیق نباشد.

۱۱ صفحه ۱۶۸ کارگاه ۶

گزارش‌گیری (Log) فایروال ویندوز را فعال کنید.

1. فایروال را از کنترل پنل باز و Advanced Settings را انتخاب می‌کنیم؛ سپس از سمت راست Properties را می‌زنیم.
2. در هر یک از سه برگه‌ی پروفایل (Domain, Private, Public) در بخش Logging روی Customize کلیک می‌کنیم.
3. مسیر و نام فایل گزارش و حداکثر حجم آن را تعیین می‌کنیم.
4. گزینه‌ی Log dropped packets را روی Yes (برای بسته‌های حذف‌شده) و در صورت نیاز Log successful connections را روی Yes می‌گذاریم و OK می‌زنیم.
5. فایل گزارش را با دسترسی Administrator باز می‌کنیم.

۱۲ صفحه ۱۶۹ فعالیت گروهی

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

پس از فعال‌کردن Log، چند بار ارتباطی را که با رول‌ها مسدود یا مجاز شده است ایجاد می‌کنیم (مثلاً دریافت IP از DHCP). در فایل گزارش، سرآیند (فیلدهای date، time، action، protocol، src-ip، dst-ip، src-port، dst-port و ...) و بدنه (ردیف‌های DROP و ALLOW) دیده می‌شود.

در مقایسه‌ی گروه‌ها معمولاً تفاوت‌ها ناشی از رول‌های متفاوت و ترافیک آزمایشی هر گروه است؛ رول‌های درست باعث ثبت ردیف DROP برای ترافیک مسدودشده می‌شوند. نتیجه: Log ابزار مهمی برای بررسی صحت رول‌ها و عیب‌یابی است.

این جواب ممکن است دقیق نباشد.

این فایل توسط سایت ایران‌توشه تهیه شده است.
irantooshe.ir

۱۳ صفحه ۱۷۲ کارگاه ۷

روی فایروال میکروتیک تنظیماتی انجام دهید که سرویس‌گیرنده‌های شبکه‌ی خارجی نتوانند از طریق WinBox با مسیریاب ارتباط برقرار کنند.

۱. در WinBox منوی IP → Firewall و برگه‌ی Filter Rules را باز و «+» را می‌زنیم.

۲. در برگه‌ی General: Chain = input (چون مقصد ترافیک خود میکروتیک است).

۳. Dst. Address = 10.1.1.1 (آدرس اینترفیس متصل به شبکه‌ی خارجی).

۴. Protocol = tcp و Dst. Port = 8291 (درگاه WinBox).

۵. در برگه‌ی Action گزینه‌ی drop را انتخاب و Apply و OK را می‌زنیم.

۶. با تلاش برای اتصال از شبکه‌ی خارجی یا مشاهده‌ی فیلد Packets (عدد غیر صفر) صحت رول را بررسی می‌کنیم.

۱۴ صفحه ۱۷۴ کارگاه ۸

دسترسی به WinBox از طریق مک‌آدرس را مسدود کنید.

۱. در WinBox منوی Tools → MAC-Server را باز می‌کنیم.

۲. روی دکمه‌ی MAC WinBox Server کلیک می‌کنیم.

۳. در فهرست Allowed Interface List گزینه‌ی none را انتخاب و Apply و OK را می‌زنیم.

توجه: پس از این کار هیچ‌کس (حتی مدیر) با مک‌آدرس به میکروتیک وصل نمی‌شود؛ پس باید دسترسی از طریق آدرس IP برقرار باشد.

این جواب ممکن است دقیق نباشد.

۱۵ صفحه ۱۷۵ فعالیت کارگاهی

رولی بنویسید که در شبکه‌ی 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.

دو رول می‌نویسیم و ترتیب آن‌ها مهم است (رول مجاز بالاتر از رول مسدودکننده):

۱. رول اول: Chain = input، Protocol = tcp، Dst. Port = 8291، Src. Address = 192.168.1.5 (آدرس رایانه‌ی مدیر)، Action = accept.

ایران توشه
توشه ای برای موفقیت

2. رول دوم: Chain = input، Protocol = tcp، Dst. Port = 8291، In. Interface = اینترفیس شبکه‌ی داخلی، Action = drop.

3. برای جلوگیری از حدس رمز، در صورت لزوم درگاه WinBox را در IP → Services تغییر یا دسترسی را به آدرس مدیر محدود می‌کنیم و MAC-Server را مطابق کارگاه ۸ می‌بندیم.

این جواب ممکن است دقیق نباشد.

---

۱۶ صفحه ۱۷۵ کارگاه ۹

تنظیماتی انجام دهید که هیچ‌کس چه از شبکه‌ی داخلی و چه از شبکه‌ی خارجی نتواند میکروتیک را ping کند.

1. در IP → Firewall → Filter Rules رول جدید می‌سازیم.
2. Chain = input.
3. آدرس مبدأ و مقصد را خالی می‌گذاریم.
4. Protocol = icmp.
5. در برگه‌ی Action گزینه‌ی drop (یا reject با پیام دلخواه از فهرست) را انتخاب می‌کنیم.
6. Apply و OK را می‌زنیم.

با این رول مدیر شبکه هم نمی‌تواند ping کند؛ برای حل آن، یک رول accept جداگانه برای آدرس مدیر، بالاتر از این رول، می‌نویسیم.

---

۱۷ صفحه ۱۷۶ فعالیت کارگاهی

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

1. رول اول (مجاز برای مدیر): Chain = forward، Protocol = icmp، Src. Address = 192.168.1.5، Out. Interface = اینترفیس خارجی، Action = accept.
2. رول دوم (مسدود برای بقیه): Chain = forward، Protocol = icmp، Src. Address = 192.168.1.0/24، Out. Interface = اینترفیس خارجی، Action = drop.
3. رول accept باید بالاتر از رول drop در فهرست قرار بگیرد.

این جواب ممکن است دقیق نباشد.

ایران توشه

۱۸ صفحه ۱۷۶ کارگاه ۱۰

تنظیماتی انجام دهید که هم افرادی که مسیریاب را ping می‌کنند و هم اینترفیسی که ping می‌شود را شناسایی کنید.

1. دو رول با Chain = input و Protocol = icmp (آدرس مبدأ و مقصد خالی) می‌سازیم؛ هر دو باید قبل از رول drop مربوط به icmp باشند.
2. در رول اول، Action را add src to address list می‌گذاریم و نام فهرست (مثلاً ping-src) را می‌نویسیم.
3. در رول دوم، Action را add dst to address list و نام فهرست (مثلاً ping-dst) می‌گذاریم.
4. از برگه‌ی Address Lists فایروال، آدرس‌های ثبت‌شده را مشاهده می‌کنیم.

۱۹ صفحه ۱۷۷ کارگاه ۱۱

گزارش‌گیری و تعیین مقصد ترافیک وب و FTP را که از شبکه‌ی داخلی به شبکه‌ی خارجی ارسال می‌شود، انجام دهید.

1. رول جدید در Filter Rules.
2. Src. Address = 192.168.1.0/24.
3. Protocol = tcp و Dst. Port = 80,443,20,21.
4. در برگه‌ی Action گزینه‌ی log را انتخاب و برای Log Prefix نام کوتاهی (مثلاً web-ftp) می‌نویسیم.
5. از منوی Log گزارش‌ها را با پیشوند انتخابی مشاهده می‌کنیم.

نکته: زیاد بودن رول‌های Log بار پردازشی دارد و ممکن است عملکرد میکروتیک را مختل کند.

این جواب ممکن است دقیق نباشد.

توشه ای برای موفقیت

۲۰ صفحه ۱۷۹ فعالیت کارگاهی

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

عبارت ^.*(google\.com)*.$ را در تارنمای آزمایش Regex وارد می‌کنیم. مثال‌های google.com، www.google.com و mail.google.com تطابق دارند؛ GOOGLE.COM یا www.Google.com تطابق ندارند چون Regex به بزرگی و کوچکی حروف حساس است. برای حل آن از عبارت ^.*([gG][oO][oO][gG][lL][eE]\.[cC][oO][mM]).*$ استفاده می‌کنیم.

این جواب ممکن است دقیق نباشد.

۲۱ صفحه ۱۸۰ کارگاه ۱۲

دسترسی کاربران شبکه‌ی داخلی به تارنمای گوگل را مسدود کنید.

1. در Firewall → IP برگه‌ی Layer7 Protocols را باز و «+» می‌زنیم، نام (مثلاً block-google) و Regex را وارد می‌کنیم و OK می‌زنیم.
2. رول جدید در Filter Rules می‌سازیم.
3. Chain = forward (ترافیک فقط از فایروال عبور می‌کند).
4. Src. Address = 192.168.1.0/24.
5. Connection State = new.
6. در برگه‌ی Advanced مقابل Layer7 Protocol نام Regex را انتخاب می‌کنیم.
7. در برگه‌ی Action گزینه‌ی drop را می‌گذاریم و Apply و OK می‌زنیم.

۲۲ صفحه ۱۸۱ فعالیت کارگاهی

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

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

1. Regex آماده‌ی برنامه (مثلاً پیام‌رسان یا شبکه‌ی اجتماعی مورد نظر مدیر شبکه) را پیدا و در Layer7 Protocols وارد می‌کنیم و مانند کارگاه ۱۲ رول drop می‌سازیم.
2. ابتدا رول‌های مجاز را می‌نویسیم: accept برای ترافیک established, related، برای ارتباط مدیر، و برای سرویس‌های لازم (DNS، وب).
3. drop برای ترافیک invalid.
4. در انتهای فهرست رول، یک رول drop برای کل ترافیک ورودی/عبوری باقی‌مانده می‌گذاریم تا هر ترافیک ناشناخته مسدود شود.

ترتیب رول‌ها مهم است: رول‌های مجاز بالاتر و رول مسدودکننده‌ی نهایی در پایین فهرست قرار می‌گیرد.

این جواب ممکن است دقیق نباشد.

ایران توشه
توشه‌ای برای موفقیت