نام: _____ تاریخ: _____ نمره: _____

پروکسی در برابر VPN کاربرگ

مقایسهٔ سرورهای پراکسی و شبکه‌های خصوصی مجازی، تفاوت‌های رمزگذاری و مسیریابی در سطح برنامه در برابر سطح سیستم

مرور یادگیری VPN

یادگیرنده
وضعیت دانشجویی
مسیر مدافع شبکه

امن
وضعیت اتصال
محافظت از بسته‌های داده

فعال
محافظت در برابر نشت
محافظت در برابر نشت DNS و IPv6

خوش آمدید! این بستهٔ فعالیت شما را در آشنایی با اصول بنیادین شبکه‌های خصوصی مجازی (VPN) راهنمایی می‌کند. می‌آموزید تونل‌های رمزگذاری‌شده چگونه از داده‌های شما محافظت می‌کنند، پروتکل‌های شبکه چگونه کار می‌کنند و چگونه می‌توان نشت‌های حریم خصوصی را شناسایی و کاهش داد.

ایستگاه‌های بررسی کاربرگ

- ☐ **بخش 1-4: بر مفاهیم و پروتکل‌های VPN مسلط شوید.**
- ☐ **بخش 5-7: جدول‌های متقاطع و جدول‌های جست‌وجوی کلمه را حل کنید.**
- ☐ **بخش 8-9: مطالعات موردی و چالش رمز را حل کنید.**
- ☐ **بخش 10: صفحه‌های پرسش‌های متداول مقدماتی و پیشرفته را مرور کنید.**
- ☐ **بخش 11: 10 واقعیت جالب دنیای واقعی را کاوش کنید.**
- ☐ **تکمیلی: چالش سریع فکر کن**

باز کردن راهنمای VPN در VPN.com

URL: https://www.vpn.com/vpn/

نقشهٔ راه یادگیری VPN شما

- پراکسی‌های برنامه را با رمزگذاری VPN در سطح سیستم مقایسه کنید.
- قابلیت‌های SOCKS5 را در مقایسه با پروکسی‌های ساده HTTP شناسایی کنید.
- نحوهٔ در معرض قرار گرفتن برنامه‌های پس‌زمینه توسط پراکسی‌های مبتنی بر مرورگر را تحلیل کنید.
- درک کنید ISPها ترافیک رمزگذاری‌نشده را روی تونل‌های پروکسی چگونه ثبت می‌کنند.
- ابزار مسیریابی مناسب را بر اساس نیاز به سرعت و امنیت انتخاب کنید.

دستورالعمل‌های کاربرگ مقایسهٔ پروکسی

به پرسش‌های چندگزینه‌ای و درست/نادرست پاسخ دهید، جمله‌های جای‌خالی را با استفاده از بانک واژه‌ها کامل کنید، تعاریف را تطبیق دهید و جدول‌های کلمات متقاطع و جست‌وجوی کلمه را حل کنید. دانسته‌های خود را دربارهٔ مقایسهٔ پروکسی‌ها و VPNها به کار ببرید. و در پایان، فعالیت تکمیلی «سریع فکر کن».

پروکسی در برابر VPN (مقدمه)

پروکسی‌ها و VPNها کارکردهای متفاوتی در حریم خصوصی دیجیتال دارند. سرور پروکسی به‌عنوان تغییر مسیر در لایهٔ برنامه عمل می‌کند و نشانی IP شما را برای برنامه‌های مشخص بدون رمزگذاری داده‌ها پنهان می‌کند. VPN در سطح شبکه کار می‌کند و تمام ترافیک سیستم را با رمزگذاری ایمن می‌کند. انتخاب ابزار درست به نیازهای امنیتی شما بستگی دارد.

هر ایستگاه بررسی را با دقت بخوانید و پاسخ درست را انتخاب کنید یا بنویسید.

ایستگاه بررسی 1: چالش چندگزینه‌ای

1 1. یک پروکسی استاندارد HTTP در کدام لایهٔ مدل OSI کار می‌کند؟

- A. لایهٔ فیزیکی
- B. لایهٔ شبکه
- C. لایهٔ برنامه
- D. لایهٔ پیوند داده

2 2. مزیت کلیدی پروتکلی SOCKS5 نسبت به پراکسی‌های استاندارد HTTP چیست؟

- A. رمزگذاری کامل بار را اجباری می‌کند
- B. از مسیریابی هر ترافیک TCP/UDP پشتیبانی می‌کند
- C. در برابر نشت DNS مصون است
- D. مستقیماً در فضای هسته اجرا می‌شود

3 3. چرا VPN عموماً از سرور پراکسی امن‌تر است؟

- A. روی سخت‌افزار راه‌دور سریع‌تر اجرا می‌شود
- B. همهٔ ترافیک شبکه را در سطح کل سیستم رمزگذاری می‌کند
- C. به جدول‌های مسیریابی محلی نیازی ندارد
- D. تأخیر شبکه را به‌طور کامل از بین می‌برد

4 4. کدام نوع پراکسی ترافیک را به‌طور پیش‌فرض بدون هیچ رمزگذاری تغییر مسیر می‌دهد؟

- A. یک پراکسی ساده HTTP
- B. پروکسی HTTPS رمزگذاری‌شده
- C. کلاینت امن WireGuard
- D. یک سرور VPN مبهم‌سازی‌شده

5 5. هنگام استفاده از پراکسی مرورگر، ترافیک برنامه‌های پس‌زمینه چه می‌شود؟

- A. به‌طور خودکار رمزگذاری می‌شود
- B. توسط سرور پروکسی مسدود می‌شود
- C. از طریق تونل پراکسی مسیریابی می‌شود
- D. پراکسی را دور می‌زند و IP شما را آشکار می‌کند

ایستگاه بررسی 2: چالش درست یا نادرست

پرسش 6

6. پراکسی SOCKS5 همهٔ بارهای بسته‌هایی را که از سرور عبور می‌کنند رمزگذاری می‌کند.

درست نادرست

پرسش 7

7. VPN در لایهٔ شبکه کار می‌کند تا همهٔ ترافیک سیستم را ایمن کند.

درست نادرست

پرسش 8

8. پروکسی‌ها عموماً از VPNها سریع‌ترند، زیرا رمزگذاری عمیق بسته انجام می‌دهند.

درست نادرست

پرسش 9

9. پیکربندی پراکسی مستلزم تنظیم تغییر مسیر ترافیک درون برنامه‌های مشخص است.

درست نادرست

پرسش 10

10. استفاده از پروکسی از ترافیک داده شما در برابر ردیابی ISP محلی محافظت نمی‌کند.

درست نادرست

ایستگاه بررسی 3: درج اصطلاح کلیدی

هر جملهٔ زیر را بخوانید و جای خالی را با واژهٔ درست از بانک واژگان پر کنید.

1. یک _____ لایهٔ برنامه ترافیک مرورگر مشخصی را بدون ایمن‌سازی سایر برنامه‌ها هدایت می‌کند.
2. یک _____ قوی همهٔ بسته‌های داده دستگاه را کپسوله و رمزگذاری می‌کند.
3. پروتکل _____ میان لایه‌های برنامه و انتقال قرار دارد.
4. پراکسی‌های HTTP در _____ مدل OSI کار می‌کنند.
5. سرورهای پراکسی استاندارد فاقد _____ بارها هستند و داده را آسیب‌پذیر می‌گذارند.
6. VPN برای همهٔ کارت‌های شبکه حفاظت _____ فراهم می‌کند.

بانک واژگان

افزونه | پروکسی | تونل VPN | رمزگذاری | سراسری | لایهٔ کاربرد | یودی‌پی | SOCKS5

پاسخ‌های خود را اینجا بنویسید:

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____

ایستگاه بررسی 4: تطبیق مفاهیم شبکه

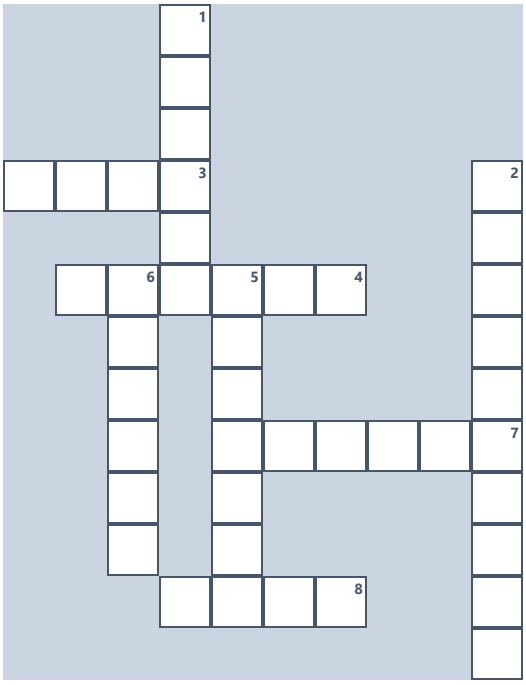
تطبیق تعاریف

هر اصطلاح واژگان در سمت راست را با نوشتن حرف متناظر (A-H) در کادر ورودی قابل‌پرکردن به تعریف درست آن در سمت چپ وصل کنید.

1. پراکسی HTTP	A	مسیریابی در سطح سیستم‌عامل که ترافیک همهٔ برنامه‌ها را رمزگذاری می‌کند.
2. پراکسی SOCKS5	B	لایهٔ برنامه کاربردی که پروتکل‌های استاندارد پروکسی وب در آن کار می‌کنند.
3. تونل VPN	C	توانایی SOCKS5 در رله کردن UDP و TCP، برخلاف پراکسی‌های HTTP ساده.
4. سراسر سیستم	D	افزونهٔ کلاینتی که فقط ترافیک داخل جعبه‌شنی مرورگر را پنهان می‌کند.
5. لایهٔ 7 مدل OSI	E	رمزگذاری و کپسوله‌سازی که همهٔ ترافیک پس‌زمینهٔ دستگاه را در بر می‌گیرد.
6. پشتیبانی UDP	F	وضعیت ترافیک که در آن داده‌های پروکسی رمزگذاری‌نشده برای ISPها قابل مشاهده می‌ماند.
7. پراکسی مرورگر	G	پروکسی لایهٔ برنامه که ترافیک مشخصی از مرورگر وب را تغییر مسیر می‌دهد.
8. دید ISP	H	پروتکل پراکسی بین لایه‌های برنامه و انتقال، بدون رمزگذاری.

ایستگاه بررسی 5: جدول‌کلمات

جدول کلمات متقاطع را با تایپ حروف در خانه‌های سفید فعال حل کنید. شماره‌ها با سرنخ‌های زیر مطابقت دارند.



افقی

3. پروتکل واسط میان لایهٔ برنامه و انتقال، بدون رمزگذاری (4)

4. توان SOCKS5 در انتقال UDP علاوه بر TCP، برخلاف پراکسی‌های ساده HTTP (6)

7. ابزار کلاینتی که فقط ترافیک داخل سندباکس مرورگر را پنهان می‌کند (6)

8. رمزگذاری و کپسوله‌سازی همهٔ ترافیک پس‌زمینهٔ دستگاه (4)

عمودی

1. مسیریابی در سطح سیستم‌عامل که ترافیک همهٔ برنامه‌ها را رمزگذاری می‌کند (6)

2. لایه‌ای که پروتکل‌های پراکسی استاندارد وب در آن کار می‌کنند (10)

5. وضعیت ترافیک که در آن داده‌های رمزگذاری‌نشدهٔ واسط برای ISP قابل مشاهده می‌ماند (7)

6. واسط لایهٔ برنامه که ترافیک مشخصی از مرورگر وب را بازهدایت می‌کند (6)

ایستگاه بررسی 5 – فعالیت جایگزین: سرنخ‌های دسترس‌پذیر جدول‌کلمات

کاربران صفحه‌خوان و صفحه‌کلید می‌توانند پاسخ‌های جدول کلمات متقاطع را مستقیماً در فیلدهای متنی زیر تایپ کنند.

افقی

3 افقی: پروتکل واسط میان لایهٔ برنامه و انتقال، بدون رمزگذاری (4 حرف):

4 افقی: توان SOCKS5 در انتقال UDP علاوه بر TCP، برخلاف پراکسی‌های ساده HTTP (6 حرف):

7 افقی: ابزار کلاینتی که فقط ترافیک داخل سندباکس مرورگر را پنهان می‌کند (6 حرف):

8 افقی: رمزگذاری و کپسوله‌سازی همهٔ ترافیک پس‌زمینهٔ دستگاه (4 حرف):

عمودی

1 عمودی: مسیریابی در سطح سیستم‌عامل که ترافیک همهٔ برنامه‌ها را رمزگذاری می‌کند (6 حرف):

2 عمودی: لایه‌ای که پروتکل‌های پراکسی استاندارد وب در آن کار می‌کنند (10 حرف):

5 عمودی: وضعیت ترافیک که در آن داده‌های رمزگذاری‌نشدهٔ واسط برای ISP قابل مشاهده می‌ماند (7 حرف):

6 عمودی: واسط لایهٔ برنامه که ترافیک مشخصی از مرورگر وب را بازهدایت می‌کند (6 حرف):

ایستگاه بررسی 6: جدول کلمات پنهان

8 اصطلاح کلیدی واژگان را که در جدول زیر پنهان شده‌اند پیدا کنید. کلمات می‌توانند افقی، عمودی یا مورب باشند.

ه	ی	ظ	و	ح	ظ	س	ت	غ	ذ	ح	ص	غ	ش	ظ
ن	س	ع	ض	ت	ک	ف	ق	ی	ج	ژ	ر	پ	ا	ب
پ	ک	س	ط	و	ژ	ز	و	ژ	و	ن	ک	ز	ث	ع
ش	و	ک	ه	ن	و	ز	ف	ا	ر	د	ث	ذ	ص	ص
ژ	ر	ا	ع	ظ	ل	خ	ش	ش	ع	غ	ی	ف	ک	ک
خ	پ	س	پ	ف	ا	ظ	د	ض	د	ف	پ	پ	م	ث
ی	ق	ه	گ	ت	ی	ی	م	ی	ح	ز	خ	ی	ی	ث
ر	ص	ث	ع	ن	ه	ظ	پ	گ	د	ب	ا	ی	ض	ث
س	ژ	ا	ث	ض	ک	ث	ج	خ	ذ	ه	ث	غ	ع	ش
ا	ج	ذ	ف	ی	ا	ق	ج	ع	ل	چ	ش	ا	ا	ع
ر	ط	ص	ظ	ک	ر	و	ع	ز	غ	ل	ک	د	ف	ت
س	ص	ه	پ	ح	ب	ف	ن	م	ن	ر	ا	غ	ن	ی
ه	ه	ژ	ح	ذ	ر	ش	غ	و	ز	س	س	ق	ط	خ
ظ	ع	خ	ی	ا	د	ض	ت	ل	ح	گ	پ	ه	ف	ه
ب	خ	س	ی	خ	ز	ض	ظ	ص	ن	پ	س	ی	ه	ح

فهرست واژگان

پروکسی ساکس تونل سراسری لایه‌کاربرد یودیپی افزونه دیده‌شدن

ایستگاه بررسی 6 – فعالیت جایگزین: تطبیق دسترس‌پذیر واژگان

هر یک از 8 اصطلاح واژگان موجود در جدول کلمات پنهان را با نوشتن حرف (A-H) در جای خالی به تعریف درست آن وصل کنید.

اصطلاحات واژگان
A. پروکسی
B. ساکس
C. تونل
D. سراسری
E. لایه‌کاربرد
F. یودیپی
G. افزونه
H. دیده‌شدن

	تعاریف و فیلدهای تطبیق
	1. لایه‌ای که پروتکل‌های پراکسی استاندارد وب در آن کار می‌کنند.
	2. توان SOCKS5 در انتقال UDP علاوه بر TCP، برخلاف پراکسی‌های ساده HTTP.
	3. واسط لایهٔ برنامه که ترافیک مشخصی از مرورگر وب را بازهدایت می‌کند.
	4. ابزار کلاینتی که فقط ترافیک داخل سندباکس مرورگر را پنهان می‌کند.
	5. رمزگذاری و کپسوله‌سازی همهٔ ترافیک پس‌زمینهٔ دستگاه.
	6. مسیریابی در سطح سیستم‌عامل که ترافیک همهٔ برنامه‌ها را رمزگذاری می‌کند.
	7. وضعیت ترافیک که در آن داده‌های رمزگذاری‌نشدهٔ واسط برای ISP قابل مشاهده می‌ماند.
	8. پروتکل واسط میان لایهٔ برنامه و انتقال، بدون رمزگذاری.

ایستگاه بررسی 7: چالش کلمات درهم‌ریخته

حروف زیر را مرتب کنید تا مفاهیم و اصطلاحات کلیدی VPN آشکار شوند. پاسخ‌هایتان را در کادرهای پرشدنی بنویسید.

1. و پ ک س ی ر
2. ت ن ل و
3. ل ا ر ر ا ک د ه ب ی
4. ه و ز ن ا ف
5. س س ک ا
6. ر س س ا ی ر
7. پ ی ی ی د و
8. ی ه ن د د ش د

فعالیت تکمیلی: سریع فکر کن

برای هر دسته 3 پاسخ بنویسید. هر کس زودتر فهرست را کامل کند برنده است.

1	تفاوت‌های پراکسی و VPN		
2	چیزهایی که بدون VPN رمزگذاری‌نشده می‌مانند		
3	روش‌های تشخیص شبکهٔ Wi-Fi جعلی		
4	کارهایی که یک واسطه در زندگی روزمره انجام می‌دهد		
5	موقعیت‌هایی که پراکسی کافی است		
6	دستگاه‌هایی که می‌توانند از VPN استفاده کنند		
7	انواع پراکسی که می‌شناسید		
8	چیزهایی که یک VPN می‌تواند پنهان کند		
9	افسانه‌ها دربارهٔ VPNها		
10	وعده‌هایی که یک ارائه‌دهندهٔ VPN خوب می‌دهد		
11	چیزهایی که VPN نمی‌تواند از آن‌ها محافظتتان کند		
12	واژه‌هایی از این کاربرگ که می‌خواهید به خاطر بسپارید		
13	دلایل استفاده از VPN در سفر		
14	موقعیت‌هایی که VPN می‌خواهید		
15	جاهایی که از VPN استفاده می‌کنید		

ایستگاه بررسی 8: مطالعات موردی VPN

مفاهیمی را که آموخته‌اید برای حل سناریوهای واقعی زیر به کار ببرید.

سارا (دانشجوی کافه)

👩‍💻 «سلام! من در Coffee & Bytes هستم و به یک شبکهٔ باز به نام 'Free_Wi-Fi_No_Password' وصلم. باید وارد ایمیل مدرسه‌ام شوم و یکی از دوستانم می‌گوید یک پروکسی رایگان مرورگر برای امن ماندن کافی است. آیا پروکسی از ورود و فایل‌های من محافظت می‌کند یا به VPN نیاز دارم؟»

Alex (دانشجوی مسافر)

👨‍💻 «من خارج از کشورم و یک مستند زیست‌شناسی که در کشور خودم میزبانی می‌شود پیام 'This video is not available in your current location.' را نشان می‌دهد. یکی از هم‌کلاسی‌هایم از پروکسی استفاده می‌کند و من VPN دارم. چرا من مسدود شده‌ام و کدام ابزار بهتر کار می‌کند؟»

ایستگاه بررسی 9: رمزگشایی

برای تکمیل آموزش مقایسهٔ پروکسی، این پیام محرمانه دربارهٔ تونل‌زنی امن را رمزگشایی کنید.

کلید رمزگذاری حرف به عدد

ا=1 ب=2 پ=3 ت=4 ث=5 ج=6 چ=7 ح=8 خ=9 د=10 ذ=11

ر=12 ز=13 ژ=14 س=15 ش=16 ص=17 ض=18 ط=19 ظ=20 ع=21 غ=22

ف=23 ق=24 ک=25 گ=26 ل=27 م=28 ن=29 و=30 ه=31 ی=32

1	2		25	32	23	1	12	4		12	32	15	28		12	32	32	22	4

32	15	25	30	12	3

پیام رمزگشایی‌شده:

نکته: هر عدد نشان‌دهندهٔ یک حرف فارسی از کلید بالا است.

ایستگاه بررسی 10: پرسش‌های متداول VPN – مقدماتی (بخش A)

رایج‌ترین پرسش‌ها و پاسخ‌هایی را که مشتریان بالقوه دربارهٔ استفاده از شبکه‌های خصوصی مجازی دارند مرور کنید.

Q1: VPN چیست و چگونه کار می‌کند؟

شبکهٔ خصوصی مجازی (VPN) اتصال اینترنت شما را رمزگذاری می‌کند و ترافیک شما را از طریق یک سرور راه‌دور امن عبور می‌دهد. این کار IP عمومی شما را پنهان می‌کند و آنچه ناظران شبکهٔ محلی و ISP شما دربارهٔ ترافیک عبوری از تونل VPN می‌بینند را محدود می‌کند.

Q2: سرور پروکسی چیست؟

سرور پراکسی واسطه‌ای است که درخواست‌ها را میان برنامهٔ شما و سرور مقصد ارسال می‌کند. وب‌سایت به‌جای IP شما، IP پراکسی را می‌بیند، اما فقط ترافیک برنامه‌هایی که برای استفاده از پراکسی پیکربندی شده‌اند تغییر مسیر می‌دهد و پراکسی ساده آن ترافیک را رمزگذاری نمی‌کند.

Q3: آیا VPN مرا در فضای آنلاین کاملاً ناشناس می‌کند؟

خیر. هرچند VPN نشانی IP شما را پنهان و ترافیک را رمزگذاری می‌کند، همچنان می‌توانید از طریق کوکی‌های مرورگر، حساب‌های فعال (مانند Google یا Facebook)، انگشت‌نگاری مرورگر، یا اگر ارائه‌دهندهٔ VPN شما داده‌هایتان را ثبت کند، ردیابی شوید.

Q4: آیا VPN سرعت اینترنت من را کاهش می‌دهد؟

بله، اندکی. فرایند رمزگذاری و فاصلهٔ فیزیکی تا سرور VPN تأخیر و سربار اضافه می‌کنند. این تأثیر بسته به ارائه‌دهنده، پروتکل، فاصلهٔ سرور، دستگاه و شرایط شبکه متفاوت است.

Q5: آیا پراکسی همان VPN است؟

خیر. پراکسی ترافیک برنامه‌های مشخصی را معمولاً بدون رمزگذاری رله می‌کند. VPN در لایهٔ شبکه یک تونل رمزگذاری‌شده می‌سازد که همهٔ ترافیک دستگاه، از جمله برنامه‌های پس‌زمینه را حمل می‌کند.

ایستگاه بررسی 10: پرسش‌های متداول VPN – مقدماتی (بخش B)

رایج‌ترین پرسش‌ها و پاسخ‌هایی را که مشتریان بالقوه دربارهٔ استفاده از شبکه‌های خصوصی مجازی دارند مرور کنید.

Q6: آیا می‌توانم از پراکسی رایگان استفاده کنم؟

می‌توانید، اما پروکسی‌های رایگان اغلب توسط اپراتورهای ناشناس اداره می‌شوند. چون یک پروکسی ساده ترافیک را رمزگذاری نمی‌کند، اپراتور آن می‌تواند صفحات رمزگذاری‌نشده را ببیند و حتی تغییر دهد. پیش از استفاده بررسی کنید چه کسی سرویس را اداره می‌کند.

Q7: آیا پراکسی لاگ نگه می‌دارد؟

می‌تواند. پروکسی هر درخواستی را که ارسال می‌کند پردازش می‌کند، بنابراین اپراتور آن ممکن است آدرس IP شما، سایت‌هایی که بازدید می‌کنید و زمان آن را ثبت کند. بررسی کنید چه کسی آن را اداره می‌کند و سیاست حریم خصوصی آن چه می‌گوید.

Q8: چه زمانی پراکسی کافی است؟

پراکسی می‌تواند برای کارهای کم‌ریسک کافی باشد، مانند تغییر موقعیت ظاهری یک مرورگر. برای کار بانکی، Wi-Fi عمومی یا محافظت از همهٔ برنامه‌های یک دستگاه، VPN انتخاب ایمن‌تری است، زیرا همهٔ ترافیک را رمزگذاری می‌کند.

Q9: آیا پراکسی می‌تواند از همهٔ برنامه‌های گوشی من محافظت کند؟

خیر. فقط برنامه‌هایی که تنظیم پراکسی را رعایت می‌کنند از آن استفاده می‌کنند؛ بقیه مستقیم وصل می‌شوند. برنامهٔ VPN در عوض همهٔ برنامه‌های گوشی را از تونل رمزگذاری‌شدهٔ خود عبور می‌دهد.

Q10: پروکسی SOCKS5 چیست؟

SOCKS5، که در RFC 1928 تعریف شده، پروتکل پروکسی‌ای است که میان لایه‌های برنامه و انتقال قرار می‌گیرد. می‌تواند اتصال‌های TCP و دیتاگرام‌های UDP را رله کند و از احراز هویت پشتیبانی می‌کند، اما رمزگذاری داخلی ندارد. [1]

ایستگاه بررسی 10: پرسش‌های متداول VPN – پیشرفته (بخش C)

جنبه‌های فنی و ساختاری شبکه‌های خصوصی مجازی و پروتکل‌های تونل‌سازی امن را بررسی کنید.

Q1: پروکسی‌ها و VPNها در کدام لایه‌های شبکه کار می‌کنند؟

پراکسی HTTP در لایهٔ برنامه (Layer 7) کار می‌کند و درخواست‌های وب را می‌فهمد. SOCKS5 میان لایهٔ برنامه و انتقال قرار می‌گیرد. پروتکل‌های VPN مانند IPsec یا WireGuard در لایهٔ شبکه کار می‌کنند، بنابراین می‌توانند همهٔ ترافیک IP دستگاه را حمل کنند.

Q2: آیا سایت HTTPS از طریق پروکسی رمزگذاری‌شده می‌ماند؟

بله. وقتی یک سایت HTTPS را از طریق پروکسی باز می‌کنید، رمزگذاری TLS به‌صورت سرتاسری میان مرورگر و سایت اجرا می‌شود، بنابراین پروکسی دامنه را می‌بیند اما محتوای صفحه را نه. صفحات HTTP ساده همچنان خوانا می‌مانند.

Q3: نشت WebRTC چیست و VPN چگونه از آن جلوگیری می‌کند؟

WebRTC یک پروتکل مرورگر است که حتی هنگام فعال بودن VPN می‌تواند نشانی‌های IP محلی و عمومی واقعی شما را فاش کند. VPNهای ممتاز درخواست‌های WebRTC را در برنامه‌های دسکتاپ/موبایل و افزونه‌های مرورگر خود مسدود یا جعل می‌کنند.

Q4: پراکسی شفاف چیست و چه کسانی از آن استفاده می‌کنند؟

پراکسی شفاف ترافیک را بدون هیچ تنظیمی روی دستگاه کاربر رهگیری می‌کند. مدارس، شرکت‌ها و ISPها از آن برای کش یا فیلتر محتوا استفاده می‌کنند. کاربران اغلب نمی‌دانند پراکسی در کار است و هیچ حریم خصوصی‌ای برایشان فراهم نمی‌کند.

Q5: مبهم‌سازی چگونه مسدودسازی VPN را دور می‌زند؟

مبهم‌سازی (یا «Stealth VPN») ترافیک VPN را طوری پنهان می‌کند که شبیه ترافیک HTTPS معمولی (پورت 443) به نظر برسد. این کار می‌تواند به عبور از بازرسی عمیق بسته (DPI) کمک کند که دولت‌ها یا شبکه‌های مدرسه و دفتر برای مسدود کردن VPN به کار می‌برند.

ایستگاه بررسی 10: پرسش‌های متداول VPN – پیشرفته (بخش D)

جنبه‌های فنی و ساختاری شبکه‌های خصوصی مجازی و پروتکل‌های تونل‌سازی امن را بررسی کنید.

Q6: Split Tunneling چیست و چه زمانی باید از آن استفاده کنم؟

Split Tunneling به شما اجازه می‌دهد انتخاب کنید کدام برنامه‌ها از تونل رمزگذاری‌شدهٔ VPN عبور کنند و کدام مستقیماً به اینترنت وصل شوند. از آن استفاده کنید تا برنامه‌های بانکی حساس از VPN عبور کنند و بازی‌های محلی مستقیماً وصل شوند و تأخیر ناشی از VPN را نداشته باشند.

Q7: چرا پراکسی ممکن است سریع‌تر از اتصال VPN به نظر برسد؟

پراکسی ساده رمزگذاری را رد می‌کند و فقط ترافیک یک برنامه را مدیریت می‌کند، بنابراین پردازش کمتری اضافه می‌کند. VPN هر بستهٔ دستگاه را رمزگذاری می‌کند. با پروتکل‌های مدرن این تفاوت اغلب اندک است و پراکسی حفاظت بسیار کمتری ارائه می‌دهد.

Q8: آیا وب‌سایت‌ها می‌توانند تشخیص دهند که از پراکسی یا VPN استفاده می‌کنم؟

اغلب، بله. بسیاری از سایت‌ها نشانی‌های IP را با فهرست سرورهای پروکسی و VPN شناخته‌شده مقایسه می‌کنند و پروکسی‌های HTTP ممکن است سرایندهایی مانند Via یا X-Forwarded-For اضافه کنند. سرویس‌های پخش معمولاً هر دو را مسدود می‌کنند.

Q9: محافظت در برابر نشت DNS چیست؟

محافظت در برابر نشت DNS دستگاه شما را وادار می‌کند پرس‌وجوهای جست‌وجوی وب‌سایت (پرس‌وجوهای DNS) را به‌جای سرورهای ISP شما، از طریق سرورهای DNS خصوصی و رمزگذاری‌شدهٔ VPN ارسال کند. این کار مانع می‌شود ISP شما بتواند ردیابی کند از چه سایت‌هایی بازدید می‌کنید.

Q10: آیا پروکسی می‌تواند جلوی محدودسازی سرعت توسط ISP را بگیرد؟

به‌ندرت. یک پراکسی ساده ترافیک را رمزگذاری نمی‌کند، بنابراین ISP همچنان می‌تواند نوع فعالیت را ببیند. VPN انواع ترافیک را پنهان می‌کند، اما هیچ‌یک از این دو ابزار ازدحام یا سقف داده را برطرف نمی‌کند.

بخش 11: 10 واقعیت جالب و بینش‌های دنیای واقعی دربارهٔ VPN

این واقعیت‌ها و بینش‌های بسیار ارزشمند و دنیای واقعی دربارهٔ تاریخچه، بازار و فناوری VPNها را مرور کنید.

1. استاندارد SOCKS

نسخهٔ 5 پروتکل SOCKS در مارس 1996 توسط IETF به‌عنوان RFC 1928 منتشر شد و هنوز مشخصات مرجع پروکسی‌های SOCKS5 مورد استفادهٔ مرورگرها و برنامه‌ها در امروز است. [1]

2. لایهٔ SHIM

RFC 1928 پروتکل SOCKS را به‌عنوان لایه‌ای واسط میان لایه‌های برنامه و انتقال توصیف می‌کند، بنابراین نمی‌تواند ترافیک لایهٔ شبکه مانند ICMP را هدایت کند. [1]

3. رله UDP

SOCKS5 فرمان UDP ASSOCIATE را افزود که به پروکسی اجازه می‌دهد علاوه بر اتصال‌های TCP، دیتاگرام‌های UDP را هم رله کند؛ کاری که پروکسی‌های ساده HTTP انجام نمی‌دهند. [1]

4. پورت پیش‌فرض SOCKS

کلاینت‌های SOCKS5 به‌طور پیش‌فرض، طبق RFC 1928، به پورت TCP 1080 سرور پروکسی متصل می‌شوند؛ بسیاری از سرویس‌های پروکسی به کاربران اجازه می‌دهند پورت‌های دیگری انتخاب کنند. [1]

5. واسطه‌های HTTP

استاندارد HTTP (RFC 9110) پروکسی را عاملی برای ارسال پیام تعریف می‌کند که کلاینت آن را انتخاب می‌کند و درخواست‌ها را به سمت سرور مبدأ بازپخش می‌کند.

6. بازرسی عمیق بسته

بازرسی عمیق بسته (DPI) محتوای بسته‌ها و الگوهای ترافیک را بررسی می‌کند؛ ترافیک پراکسی رمزگذاری‌نشده کاملاً برای آن قابل‌مشاهده است، در حالی که ترافیک VPN اطلاعات بسیار کمتری را آشکار می‌کند.

7. VPNهای لایهٔ شبکه

IPsec که در NIST SP 800-77 توصیف شده، از ترافیک در لایهٔ شبکه محافظت می‌کند، بنابراین بسته‌های IP هر برنامه را می‌توان بدون راه‌اندازی جداگانه برای هر برنامه ایمن کرد. [2]

8. دامنهٔ فقط-مرورگر

پراکسی تنظیم‌شده در یک مرورگر فقط بر همان مرورگر اثر می‌گذارد؛ کلاینت‌های ایمیل، بازی‌ها و به‌روزرسانی‌های سیستم همچنان از اتصال عادی دستگاه استفاده می‌کنند.

9. Tor در برابر پراکسی‌ها

Tor ترافیک را از طریق سه رلهٔ داوطلب (نگهبان، میانی و خروجی) می‌فرستد و معمولاً از طریق یک پروکسی SOCKS محلی به آن دسترسی پیدا می‌شود و لایه‌هایی می‌افزاید که یک پروکسی تنها نمی‌تواند.

10. مبادلهٔ سرعت

پروکسی‌ها می‌توانند سریع‌تر به نظر برسند، زیرا رمزگذاری را رد می‌کنند، اما پروتکل‌های مدرن VPN مانند WireGuard سربار اندکی اضافه می‌کنند و در عین حال تمام ترافیک دستگاه را محافظت می‌کنند.

منابع و مراجع فنی

نشریات ارجاع‌شده، مشخصات رمزنگاری و استانداردهای رسمی اسنادی که در سراسر این کاربرگ استفاده شده‌اند.

منابع علمی و صنعتی

[1] IETF. (1996). RFC 1928: SOCKS Protocol Version 5.
https://datatracker.ietf.org/doc/html/rfc1928

[2] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.
https://csrc.nist.gov/pubs/sp/800/77/r1/final

[3] WireGuard. (n.d.). WireGuard: fast, modern, secure VPN tunnel.
https://www.wireguard.com/

[4] WireGuard. (n.d.). Protocol & Cryptography.
https://www.wireguard.com/protocol/

[5] OpenVPN. (n.d.). OpenVPN 2.6 Manual.
https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

کلید پاسخ: مقایسهٔ سرورهای پروکسی و شبکه‌های خصوصی مجازی، تفاوت‌های رمزگذاری و مسیردهی در سطح برنامه یا کل سیستم

1 لایهٔ OSI پروکسی

پروتکل‌ها

پاسخ درست: C

نکتهٔ آموزشی

پراکسی‌های استاندارد HTTP/HTTPS در لایهٔ کاربرد (لایهٔ 7) کار می‌کنند و ترافیک مرورگر مشخصی را تغییر مسیر می‌دهند. آن‌ها مسیریابی شبکهٔ سراسری سیستم ندارند. منبع: Tor Project Foundation.

2 پرسش 2

پاسخ درست: B

نکتهٔ آموزشی

SOCKS5 ترافیک TCP و UDP را بین لایه‌های برنامه و انتقال رله می‌کند اما به‌طور پیش‌فرض رمزگذاری نمی‌کند، در حالی که پراکسی‌های HTTP درخواست‌های وب را مدیریت می‌کنند.

3 رمزگذاری سیستم VPN

امنیت وای‌فای

پاسخ درست: B

نکتهٔ آموزشی

VPN همهٔ ترافیک سیستم‌عامل را در سطح کل سیستم کپسوله و رمزگذاری می‌کند، در حالی که پراکسی فقط ترافیک برنامه‌های پیکربندی‌شدهٔ خاص را تغییر مسیر می‌دهد. منبع: Deloitte Advisory.

4 نبود رمزگذاری در پروکسی

کنترل‌های مسیریابی

پاسخ درست: A

نکتهٔ آموزشی

پروکسی‌های HTTP ترافیک مرورگر را در لایهٔ برنامه بدون رمزگذاری محتوای بسته‌ها ارسال می‌کنند، یعنی اپراتور شبکه یا ISP شما همچنان می‌تواند ترافیک محتوای شما را ردیابی کند. منبع: IETF Proxy Vulnerabilities.

5 آسیب‌پذیری دور زدن

حریم خصوصی

پاسخ درست: D

نکتهٔ آموزشی

پروکسی‌های مرورگر قوانین را فقط روی خود مرورگر وب اعمال می‌کنند. برنامه‌های پس‌زمینه، به‌روزرسانی‌های سیستم‌عامل و کلاینت‌های ایمیل پروکسی را دور می‌زنند و نشانی IP اصلی شما را آشکار می‌کنند. منبع: W3C Consortium.

کلید پاسخ: ایستگاه بررسی 2 – درست یا نادرست

6 پرسش 6

پاسخ درست: نادرست

نکتهٔ آموزشی

SOCKS5 ترافیک را بین لایه‌های برنامه و انتقال رله می‌کند اما به‌طور پیش‌فرض هیچ رمزگذاری انجام نمی‌دهد، بنابراین محتوای بسته‌ها در مسیر خوانا می‌ماند.

7 تونل‌های لایهٔ شبکه

سرعت‌ها

پاسخ درست: درست

نکتهٔ آموزشی

VPN با اجرا در لایهٔ شبکه، ترافیک خروجی دستگاه شما را مسیریابی و رمزگذاری می‌کند و می‌تواند به محافظت از ترافیک در سطح کل سیستم کمک کند. منبع: Deloitte Advisory.

8 محدودیت رمزگذاری پروکسی

خطر شنود

پاسخ درست: نادرست

نکتهٔ آموزشی

پروکسی‌ها گاهی می‌توانند سریع‌تر باشند، اما این به آن دلیل است که رمزگذاری انجام نمی‌دهند. نبود این رمزگذاری داده‌ها را در برابر بازرسی آسیب‌پذیر می‌کند. منبع: IETF Proxy Vulnerabilities.

9 تغییر مسیر در سطح برنامه

دیوارهای آتش

پاسخ درست: درست

نکتهٔ آموزشی

برخلاف VPNهای سراسر سیستم، سرورهای پروکسی به راه‌اندازی دستی درون تنظیمات مرورگر یا فیلدهای پروکسی ویژهٔ هر برنامه نیاز دارند. منبع: W3C Consortium.

10 خطر ردیابی توسط ISP

بدون لاگ

پاسخ درست: درست

نکتهٔ آموزشی

چون پروکسی‌های استاندارد HTTP/SOCKS5 داده‌های بار را رمزگذاری نمی‌کنند، ISP محلی شما دید کامل به فعالیت‌های آنلاین شما دارد. منبع: EDRi Retention Guidelines.

کلیدهای واژگان و معیار نمره‌دهی

بارم‌بندی معلم: برای هر تطبیق درست (در مجموع 8 امتیاز) و اصطلاح بافتی (در مجموع 6 امتیاز) 1 امتیاز بدهید.

ایستگاه بررسی 4: کلید پاسخ – تطبیق مفاهیم

G. 1. پراکسی HTTP	H. 2. پراکسی SOCKS5	E. 3. تونل VPN	A. 4. سراسر سیستم
B. 5. لایهٔ 7 مدل OSI	C. 6. پشتیبانی UDP	D. 7. پراکسی مرورگر	F. 8. دید ISP

ایستگاه بررسی 3: کلید پاسخ – اصطلاحات کلیدی

1 پروکسی	2 تونل VPN	3 SOCKS5	4 لایهٔ کاربرد
5 رمزگذاری	6 سراسری		

ایستگاه بررسی 6 – فعالیت جایگزین: کلید پاسخ – تطبیق واژگان

1 E – لایه‌کاربرد	2 F – یودیپی	3 A – پروکسی	4 G – افزونه
5 C – تونل	6 D – سراسری	7 H – دیده‌شدن	8 B – ساکس

یادداشت‌های بحث برای مدرسان

اصطلاحات کلیدی:
بررسی کنید که دانش‌آموزان بتوانند پراکسی HTTP، پراکسی SOCKS5 و تونل VPN را با کلمات خودشان توضیح دهند و برای هر کدام مثالی بزنند.

مطالعات موردی:
از دانش‌آموزان بخواهید پیشنهادهای خود را بر پایهٔ واقعیت‌های کاربرگ ارائه کنند، نه نظر شخصی.

ارزیابی منابع:
از دانش‌آموزان بخواهید دست‌کم یک ادعا را در منابع کاربرگ بررسی کنند و دربارهٔ اینکه چرا ارقام، قیمت‌ها و قوانین ممکن است با گذشت زمان تغییر کنند گفت‌وگو کنید.

کلیدهای معما و یادداشت‌های معلم

پاسخ جدول کلمات

ه	ی	ظ	و	ح	ظ	س	ت	غ	ذ	ح	ص	غ	ش	ظ
ن	س	ع	ض	ت	ک	ف	ق	ی	ج	ژ	ر	پ	ا	ب
پ	ک	س	ط	و	ژ	ز	و	ن	ک	ز	ث	ش	ع
ش	و	ک	ه	ن	و	ز	ف	ا	ر	د	ث	ذ	ص	ص
ژ	ر	ا	ع	ظ	ل	خ	ش	ش	غ	ع	ی	ف	ک	ک
خ	پ	س	پ	ف	ا	ظ	د	ض	د	ف	پ	پ	م	ث
ی	ق	ه	گ	ت	ی	ی	م	ی	ح	ز	خ	ی	ی	ث
ر	ص	ث	ع	ن	ه	ظ	پ	گ	ب	ا	ی	ض	ث
س	ژ	ا	ث	ض	ک	ث	چ	خ	ذ	ه	ث	غ	ع	ش
ا	چ	ذ	ف	ی	ا	ق	چ	ع	ل	چ	ش	ا	ا	ع
ر	ط	ص	ظ	ک	ر	و	ع	ز	غ	ل	ک	د	ف	ت
س	ص	ه	پ	ح	ب	ف	م	ن	ر	ا	غ	ن	ی
ه	ژ	ح	ذ	ر	ش	غ	و	ز	س	س	ق	ط	خ
ظ	ع	خ	ی	ا	د	ض	ل	ح	گ	پ	ه	ف	ه
ب	خ	س	ی	خ	ز	ض	ظ	ص	ن	پ	س	ی	ه	ح

پاسخ جدول‌کلمات



راهنمای معلم برای پاسخ‌های جدول کلمات متقاطع

افقی

3 افقی: ساکس پروتکل واسط میان لایهٔ برنامه و انتقال، بدون رمزگذاری (4 حرف)

4 افقی: یودیپی توان SOCKS5 در انتقال UDP علاوه بر TCP، برخلاف پراکسی‌های ساده HTTP (6 حرف)

7 افقی: افزونه ابزار کلاینتی که فقط ترافیک داخل سندباکس مرورگر را پنهان می‌کند (6 حرف)

8 افقی: تونل رمزگذاری و کپسوله‌سازی همهٔ ترافیک پس‌زمینهٔ دستگاه (4 حرف)

عمودی

1 عمودی: سراسری مسیریابی در سطح سیستم‌عامل که ترافیک همهٔ برنامه‌ها را رمزگذاری می‌کند (6 حرف)

2 عمودی: لایه‌کاربرد لایه‌ای که پروتکل‌های پراکسی استاندارد وب در آن کار می‌کنند (10 حرف)

5 عمودی: دیده‌شدن وضعیت ترافیک که در آن داده‌های رمزگذاری‌نشدهٔ واسط برای ISP قابل مشاهده می‌ماند (7 حرف)

6 عمودی: پروکسی واسط لایهٔ برنامه که ترافیک مشخصی از مرورگر وب را بازهدایت می‌کند (6 حرف)

کلید پاسخ کلمات درهم‌ریخته و رمزگشایی

کلید نمره‌دهی برای فعالیت بازچینی واژگان و چالش رمز مخفی.

کلید مرتب‌سازی کلمات

1. ویکسیر — پروکسی
2. تنلو — تونل
3. لاررااکدهبی — لایهکاربرد
4. هوزناف — افزونه
5. سسکا — ساکس
6. رسسایر — سراسری
7. پیییدو — یودیپی
8. یهنددشد — دیدهشدن

کلید چالش رمز مخفی

"تغییر مسیر ترافیک با پروکسی"

کلید پاسخ مطالعات موردی

A سناریو A: امنیت شبکهٔ عمومی

شنود و رمزگذاری | معمای سارا

راهنمای نمره‌دهی

پاسخ‌های دانش‌آموز باید نکات زیر را پوشش دهد:

- خطرها: شنود بسته، رهگیری داده و حمله‌های مرد میانی. فردی در همان شبکهٔ کافه می‌تواند جزئیات ورود یا فایل تکلیف او را ضبط کند.
- پروکسی در برابر VPN: یک پروکسی ساده مرورگر ترافیک او را رمزگذاری نمی‌کند. VPN هر چیزی را روی دستگاه رمزگذاری می‌کند و بسته‌های شنودشده را برای شنودگران محلی ناخوانا می‌کند.

B سناریو B: دسترسی به منابع مسدودشده

مسدودسازی جغرافیایی و IPها | دوراهی Alex

راهنمای نمره‌دهی

پاسخ‌های دانش‌آموز باید نکات زیر را پوشش دهد:

- دلیل مسدود شدن: میزبان پخش از مسدودسازی جغرافیایی استفاده می‌کند که IP محلی مسافر را به کشور فیزیکی او نگاشت می‌کند و بر اساس مجوزهای قلمرویی آن را مسدود می‌کند.
- کدام بهتر است: هر دو به او IP کشور خودش را می‌دهند، اما پراکسی فقط برنامهٔ پیکربندی‌شده را پوشش می‌دهد، در حالی که VPN همهٔ ترافیک دستگاه او را هم رمزگذاری می‌کند.