نام: _____ تاریخ: _____ نمره: _____

VPN چیست
کاربرگ

تمرین‌های عملی در پروتکل‌های شبکه، تونل‌زنی و کنترل‌های امنیتی.

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

- مفهوم تونل‌سازی و کپسوله‌سازی داده را توضیح دهید.
- پیکربندی‌های استاندارد پروتکل و روش‌های رمزگذاری را شناسایی کنید.
- نقش سرورها و پنهان‌سازی IP در شبکه‌های خصوصی مجازی را تحلیل کنید.
- درک کنید ISPها مرور شما را چگونه ردیابی می‌کنند و VPN چگونه از آن جلوگیری می‌کند.
- مرزهای عملیاتی توپولوژی شبکهٔ مجازی را از هم تفکیک کنید.

دستورالعمل‌های راهنمای VPN چیست

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 درباره سناریوهای واقعی در بخش مطالعهٔ موردی به کار ببرید. و در پایان، فعالیت تکمیلی «سریع فکر کن».

VPN چیست؟ (مقدمه)

شبکهٔ خصوصی مجازی فقط یک کلید حریم خصوصی نیست. تونلی رمزگذاری‌شده است که ترافیک اینترنت شما را از طریق یک سرور راه‌دور عبور می‌دهد. این کار نشانی IP شما را پنهان می‌کند، مانع می‌شود ISP شما از فعالیت‌های آنلاین‌تان گزارش تهیه کند و داده‌های شما را در شبکه‌های عمومی ایمن می‌کند. درک اصطلاحات برای حفظ ایمنی دیجیتال ضروری است.

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

ایستگاه بررسی 1: چالش چندگزینه‌ای

1. کارکرد اصلی شبکهٔ خصوصی مجازی (VPN) چیست؟

- A. برای افزایش سرعت رندر مرورگر اینترنت
- B. رمزگذاری بسته‌های داده و پنهان کردن IP عمومی شما
- C. برای ذخیرهٔ محلی پایگاه‌های داده کوکی وب‌سایت
- D. برای جایگزینی سخت‌افزار فیزیکی رایانهٔ شما

2. تونل‌زنی شبکه در زمینهٔ VPN چیست؟

- A. حذف فایل‌های گزارش تکراری شبکه
- B. نصب فایل‌های ذخیره‌سازی پایگاه دادهٔ محلی
- C. اشتراک‌گذاری فایل‌ها با رایانه‌های محلی دیگر
- D. محصور کردن یک بستهٔ شبکه درون بستهٔ امن دیگر

3. کدام استاندارد رمزگذاری به‌طور گسترده برای محافظت از ترافیک VPN استفاده می‌شود؟

- A. رمزگذاری قدیمی DES
- B. استاندارد مدرن AES-256
- C. کدگذاری متنی ساده base64
- D. رمزنگاری استاندارد rot13

4. کدام بخش از ترافیک شبکهٔ شما توسط VPN رمزگذاری می‌شود؟

- A. فقط کارهای چاپ شبکهٔ محلی دستگاه
- B. مسیر فیزیکی کابل اترنت
- C. کل بخش بار داده‌ای بستهٔ شبکه
- D. فقط تاریخچهٔ جست‌وجوی مرورگر وب شما

5. اصطلاح «رمزگذاری» در شبکه به چه معناست؟

- A. تبدیل داده‌های متن ساده به متن رمزی ناخوانا
- B. حذف سوابق ارتباطی قدیمی
- C. افزایش محدودیت‌های سرعت پهنای باند محلی شما
- D. اشتراک‌گذاری عمومی کلیدهای دسترسی پایگاه داده

ایستگاه بررسی 2: چالش درست یا نادرست

6 پرسش 6

6. VPN ترافیک شما را رمزگذاری می‌کند تا از شنود محلی در Wi-Fi عمومی جلوگیری شود.

درست نادرست

7 پرسش 7

7. VPN پیکربندی سخت‌افزاری دستگاه روتر شما را به‌طور فیزیکی تغییر می‌دهد.

درست نادرست

8 پرسش 8

8. پروتکل‌های تونل‌زنی بسته‌های داده را در یک لایهٔ انتقال رمزگذاری‌شده می‌پیچند.

درست نادرست

9 پرسش 9

9. رمزگذاری متقارن از همان کلید برای رمزگذاری و رمزگشایی ترافیک استفاده می‌کند.

درست نادرست

10 پرسش 10

10. استفاده از VPN اتصال اینترنت شما را از نظر فیزیکی در برابر هر قطع برق آفلاین مصون می‌کند.

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. برای ایمن‌سازی ترافیک شما، VPN بسته‌های داده را درون پروتکل دیگری می‌پیچد؛ فرایندی که _____ نام دارد.

2. اگر هنگام استریم سرعت دانلود پایین باشد، ممکن است به‌دلیل محدود بودن _____ شبکه باشد.

3. سرویس استریمی که فقط در یک کشور خاص در دسترس است، برای محدود کردن کاربران جهانی از یک _____ استفاده می‌کند.

4. قواعد اتصال که پارامترهای رمزگذاری و اتصال را تعریف می‌کنند، _____ VPN نام دارند.

5. رایانهٔ شما از یک _____ محلی برای پایش ترافیک شبکه و مسدود کردن اتصال‌های ناامن استفاده می‌کند.

6. وقتی به VPN وصل می‌شوید، داده‌هایتان برای پنهان کردن IP عمومی از طریق یک _____ راه دور مسیریابی می‌شود.

بانک واژگان

پروتکل | پهنای باند | تونل‌زنی | حریم خصوصی | دیوار آتش | ژئوبلاک | سرور | ISP

پاسخ‌های خود را اینجا بنویسید:

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

ایستگاه بررسی 4: تطبیق مفاهیم شبکه

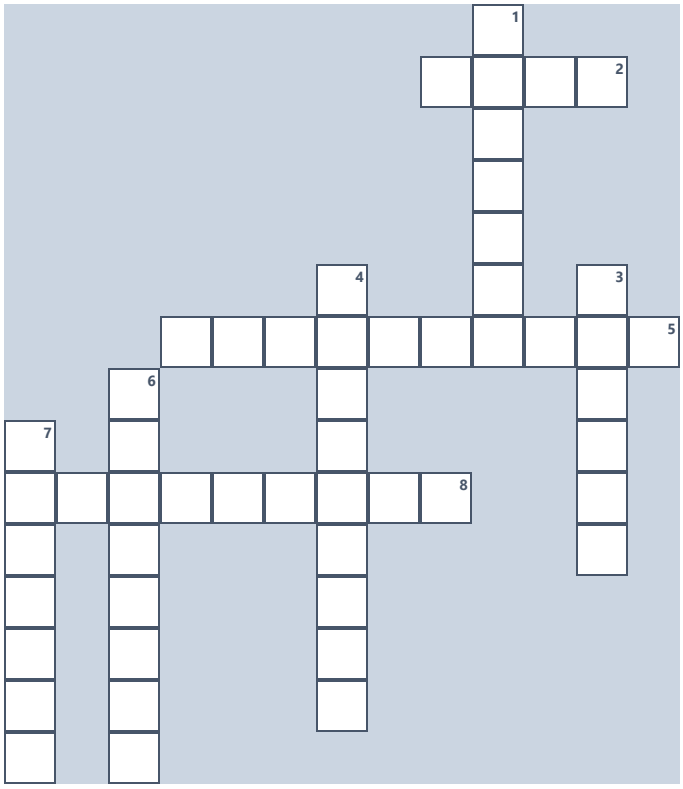
تطبیق تعاریف

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. تونل‌زنی	A	رایانهٔ راه‌دوری که ترافیک شما را مسیریابی می‌کند و IP شما را پنهان می‌کند.
2. پروتکل	B	ارائه‌دهندهٔ خدمات اینترنتی که ترافیک شما را حمل می‌کند و می‌تواند فعالیت رمزگذاری‌نشده را ببیند.
3. پهنای باند	C	محدودیتی که دسترسی به وب را بر پایهٔ موقعیت فیزیکی مانع می‌شود.
4. سرور	D	سامانهٔ امنیتی که ترافیک غیرمجاز را پایش و مسدود می‌کند.
5. محدودیت جغرافیایی	E	مجموعه‌ای از قواعد که تعیین می‌کند داده چگونه در شبکه منتقل می‌شود.
6. دیوار آتش	F	حالت رهایی از ردیابی یا نظارت عمومی.
7. حریم خصوصی	G	بیشینهٔ نرخ انتقال داده در یک اتصال.
8. ارائه‌دهندهٔ اینترنت (ISP)	H	پوشاندن بسته‌های داده درون بستهٔ دیگر برای انتقال امن.

ایستگاه بررسی 5: جدول‌کلمات

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



افقی

2. رایانهٔ راه‌دوری که ترافیک شما را مسیریابی می‌کند و IP شما را پنهان می‌سازد (4)

5. شرکت تأمین‌کنندهٔ اینترنت (ISP) که اگر رمزگذاری نشود، ترافیک شما را ثبت می‌کند (10)

8. وضعیت رهایی از ردیابی یا نظارت عمومی (9)

عمودی

1. پیچیدن بسته‌های داده درون بستهٔ دیگر برای انتقال امن (7)

3. مجموعهٔ قواعدی که تعیین می‌کند داده چگونه روی شبکه منتقل شود (6)

4. بیشینهٔ نرخ انتقال داده در یک اتصال (9)

6. سامانهٔ امنیتی که ترافیک غیرمجاز را پایش و مسدود می‌کند (8)

7. محدودیتی که دسترسی به وب را بر اساس مکان فیزیکی مسدود می‌کند (7)

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

2 افقی: رایانهٔ راه‌دوری که ترافیک شما را مسیریابی می‌کند و IP شما را پنهان می‌سازد (4 حرف):

5 افقی: شرکت تأمین‌کنندهٔ اینترنت (ISP) که اگر رمزگذاری نشود، ترافیک شما را ثبت می‌کند (10 حرف):

8 افقی: وضعیت رهایی از ردیابی یا نظارت عمومی (9 حرف):

عمودی

1 عمودی: پیچیدن بسته‌های داده درون بستهٔ دیگر برای انتقال امن (7 حرف):

3 عمودی: مجموعهٔ قواعدی که تعیین می‌کند داده چگونه روی شبکه منتقل شود (6 حرف):

4 عمودی: بیشینهٔ نرخ انتقال داده در یک اتصال (9 حرف):

6 عمودی: سامانهٔ امنیتی که ترافیک غیرمجاز را پایش و مسدود می‌کند (8 حرف):

7 عمودی: محدودیتی که دسترسی به وب را بر اساس مکان فیزیکی مسدود می‌کند (7 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.

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

فهرست واژگان

تونلزنی
پروتکل
پهناییباند
سرور
ژیوبلاک
دیواراتش
حریمخصوصی
ارایهدهنده

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. تونلزنی
B. پروتکل
C. پهناییباند
D. سرور
E. ژیوبلاک
F. دیواراتش
G. حریمخصوصی
H. ارایهدهنده

تعاریف و فیلدهای تطبیق	
1. مجموعهٔ قواعدی که تعیین می‌کند داده چگونه روی شبکه منتقل شود.	
2. محدودیتی که دسترسی به وب را بر اساس مکان فیزیکی مسدود می‌کند.	
3. سامانهٔ امنیتی که ترافیک غیرمجاز را پایش و مسدود می‌کند.	
4. وضعیت رهایی از ردیابی یا نظارت عمومی.	
5. شرکت تأمین‌کنندهٔ اینترنت (ISP) که اگر رمزگذاری نشود، ترافیک شما را ثبت می‌کند.	
6. پیچیدن بسته‌های داده درون بستهٔ دیگر برای انتقال امن.	
7. رایانهٔ راه‌دوری که ترافیک شما را مسیریابی می‌کند و IP شما را پنهان می‌سازد.	
8. بیشینهٔ نرخ انتقال داده در یک اتصال.	

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. ل ن ت ز ی ن و _____
2. د پ ن ا ه ب ا ی ن _____
3. ب ژ ل ک و ا ی _____
4. خ ی ص م و ص ح ر ی _____
5. ت و ل پ ک ر _____
6. و ر س ر _____
7. د ش ر ا ت ی ا و _____
8. د ی د ه ا ه ر ه ن ا _____

فعالیت تکمیلی: سریع فکر کن

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

1	چیزهایی که یک نشانی IP می‌تواند آشکار کند		
2	افسانه‌ها دربارهٔ VPNها		
3	چیزهایی که در اینترنت جابه‌جا می‌شوند		
4	وعده‌هایی که یک ارائه‌دهندهٔ VPN خوب می‌دهد		
5	رازهایی که رمزگذاری می‌کنید		
6	چیزهایی که VPN نمی‌تواند از آن‌ها محافظتتان کند		
7	روش‌های تشخیص شبکهٔ Wi-Fi جعلی		
8	واژه‌های مرتبط با حریم خصوصی		
9	دستگاه‌هایی که می‌توانند از VPN استفاده کنند		
10	چیزهایی که با فشردن «اتصال» رخ می‌دهند		
11	جاهایی که از VPN استفاده می‌کنید		
12	دلایل استفاده از VPN در سفر		
13	چیزهای واقعی که شبیه تونل هستند		
14	واژه‌هایی از این کاربرگ که می‌خواهید به خاطر بسپارید		
15	واژه‌هایی برای توضیح VPN به یک کودک		

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 نشسته‌ام. یک شبکهٔ عمومی ناامن به نام 'Free_Wi-Fi_No_Password' وجود دارد. می‌خواهم وارد ایمیل مدرسه‌ام شوم و تکلیفم را آپلود کنم، اما نگران هکرها هستم. استفاده از این شبکه بدون VPN چه خطرهایی دارد و VPN چگونه از داده‌های من محافظت می‌کند؟»

Alex (دانشجوی مسافر)

👨‍💻 «وای نه! برای یک پروژه به خارج از کشور سفر کرده‌ام و می‌خواهم یک مستند زیست‌شناسی را که روی سروری در کشور خودم میزبانی می‌شود تماشا کنم. اما سایت پیام 'This video is not available in your current location.' را نشان می‌دهد. چرا مسدود شده‌ام و VPN چگونه می‌تواند به تماشای آن کمک کند؟»

ایستگاه بررسی 9: رمزگشایی

VPN ترافیک شما را رمزگذاری می‌کند تا ایمن شود. از کلید حرف-به-عدد زیر استفاده کنید و با نوشتن حرف‌های متناظر در جاهای خالی، پیام امنیت سایبری 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		32	17	30	17	9		28	32	12	8		4	20	23	1	8	28

29	28	1		27	29	30	4

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: چرا باید از VPN استفاده کنم؟

VPN از حریم خصوصی دیجیتال شما محافظت می‌کند، اتصال شما را در شبکه‌های Wi-Fi عمومی (مانند کافه‌ها یا فرودگاه‌ها) ایمن می‌کند، ممکن است وقتی ISP نوع ترافیک رمزگذاری‌شده را شناسایی نکند، کاهش سرعت مبتنی بر فعالیت را کم کند، محدودیت‌های جغرافیایی را دور می‌زند تا به محتوای جهانی دسترسی پیدا کنید، و به ایمن‌سازی منابع کار از راه دور کمک می‌کند.

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 استفاده از VPN قانونی است؟

استفاده از VPN در بسیاری از کشورها قانونی است، اما برخی حوزه‌های قضایی خدمات VPN را محدود، تنظیم یا مسدود می‌کنند. کاربران باید پیش از استفاده قوانین محلی فعلی را بررسی کنند. برای جزئیات بیشتر، راهنماهای قانونی‌بودن را در VPN.com مطالعه کنید.

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 VPN رایگان استفاده کنم؟

VPNهای رایگان ممکن است به تبلیغات، ویژگی‌های محدود، تحلیل‌های استفاده، سقف داده یا مدل‌های درآمدزایی دیگر متکی باشند. کاربران باید پیش از استفاده سیاست حریم خصوصی، مالکیت، ممیزی‌ها و مدل کسب‌وکار ارائه‌دهنده را بررسی کنند.

Q7: سیاست «بدون‌لاگ» چیست؟

سیاست بدون ثبت گزارش مشخص می‌کند ارائه‌دهنده می‌گوید کدام داده‌های فعالیت و اتصال را نگه نمی‌دارد. دامنهٔ دقیق آن متفاوت است، بنابراین خوانندگان باید سیاست و یافته‌های ممیزی مستقل را بررسی کنند.

Q8: چگونه بهترین VPN را انتخاب کنم؟

به دنبال سیاست‌های عدم ثبت لاگِ ممیزی‌شده، پروتکل‌های قوی (WireGuard، OpenVPN)، مکان‌های امن سرور، سرعت بالا، سرورهای فقطRAM، قابلیت kill switch و صلاحیت قضایی خارج از اتحادهای تبادل اطلاعات اطلاعاتی (مانند 5/9/14 چشم) باشید.

Q9: آیا می‌توانم VPN را روی گوشی و تلویزیون هوشمند خود استفاده کنم؟

بله. ارائه‌دهندگان مدرن VPN برنامه‌های اختصاصی برای Linux، Windows، macOS، Android، iOS و تلویزیون‌های هوشمند و همچنین راه‌اندازی روی روتر برای محافظت از همهٔ دستگاه‌های شبکهٔ خانگی شما ارائه می‌دهند.

Q10: کلید قطع (Kill Switch) چیست؟

Kill Switch قابلیتی امنیتی است که اگر اتصال VPN قطع شود، دستگاه شما را به‌طور خودکار از اینترنت جدا می‌کند. این کار از نشت داده‌های رمزگذاری‌نشده یا IP واقعی شما جلوگیری می‌کند.

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

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

Q1: تفاوت OpenVPN، WireGuard و IKEv2 چیست؟

WireGuard یک پروتکل مدرن و سبک است (فقط حدود 4,000 خط کد) که سرعت بالا و زمان اتصال کوتاه ارائه می‌دهد. OpenVPN یک پروتکل متن‌باز بسیار امن و محک‌خورده است. IKEv2 به‌دلیل توانایی اتصال مجدد سریع هنگام تغییر شبکه برای دستگاه‌های موبایل عالی است. [4]

Q2: مسیریابی دو VPN یا Multi-Hop چیست؟

روش چندجهشی ترافیک شما را به‌صورت متوالی از دو یا چند سرور VPN عبور می‌دهد. این کار لایهٔ رمزگذاری دوم اضافه می‌کند و اگر یک سرور آسیب ببیند، کمک می‌کند نشانی IP واقعی شما از جهش دوم پنهان بماند.

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: سرورهای فقطRAM چیستند و چرا اهمیت دارند؟

سرورهای سنتی داده را روی هارددیسک می‌نویسند که می‌تواند توقیف یا آسیب‌دیده شود. سرورهای فقط-RAM (بدون دیسک) کاملاً در حافظهٔ فرار (RAM) اجرا می‌شوند. وقتی سرور مجدداً راه‌اندازی یا خاموش شود، داده‌های موجود در حافظه پاک می‌شوند.

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: رازداری پیشرو (Perfect Forward Secrecy) چگونه کار می‌کند؟

PFS تضمین می‌کند که برای هر نشست یک کلید رمزگذاری منحصربه‌فرد و موقت تولید شود. حتی اگر کلید خصوصی در آینده فاش شود، نمی‌توان از آن برای رمزگشایی نشست‌های گذشته یا آینده استفاده کرد، زیرا آن‌ها از کلیدهای مستقل استفاده کرده‌اند.

Q8: ائتلاف‌های 5/9/14 Eyes چیستند و چرا باید برایم مهم باشند؟

صلاحیت قضایی می‌تواند بر فرایند حقوقی‌ای که یک ارائه‌دهنده ممکن است با آن روبه‌رو شود اثر بگذارد، اما خطر عملی برای حریم خصوصی به این هم بستگی دارد که ارائه‌دهنده چه داده‌هایی را نگه می‌دارد، معماری فنی، مالکیت، گزارش‌دهی شفافیت و سابقهٔ ممیزی آن چیست.

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 VPN می‌تواند محدودسازی اینترنت توسط ISP را دور بزند؟

گاهی. وقتی ISP به‌طور انتخابی فعالیت‌های قابل‌شناسایی را کند می‌کند، VPN ممکن است کمک کند، اما بر ازدحام، سقف داده، محدودیت‌های سرعت در سطح حساب یا کیفیت ضعیف شبکه غلبه 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. نخستین پروتکل VPN

PPTP (Point-to-Point Tunneling Protocol) توسط گروهی از فروشندگان از جمله Microsoft توسعه یافت و در ژوئیهٔ 1999 برای پشتیبانی از VPNهای دسترسی راه‌دور به‌صورت RFC 2637 منتشر شد. [6]

2. ارزش‌گذاری بازار

بازار جهانی VPN رشد سریعی داشته است که ناشی از افزایش نیاز به دورکاری و تقاضاهای امنیتی سازمانی است.

3. انقلاب WIREGUARD

WireGuard کدبیس بسیار ساده‌شده‌ای دارد که برای کارایی طراحی شده و بررسی آسیب‌پذیری‌های امنیتی آن را از پروتکل‌های سنتی آسان‌تر می‌کند. [4]

4. استانداردهای سخت‌گیرانهٔ ممیزی

ارائه‌دهندگان برتر VPN حسابرسان بیرونی (مانند Cure53 یا PwC) را استخدام می‌کنند تا بررسی‌های مستقل کد انجام دهند و تأیید کنند که هیچ فعالیت کاربری ثبت نمی‌کنند.

5. خاستگاه اتحاد EYES-5

اتحاد Five Eyes از توافق اطلاعات سیگنالی UKUSA در سال 1946 میان آمریکا و بریتانیا شکل گرفت و بعدها کانادا، استرالیا و نیوزیلند به آن پیوستند.

6. بازرسی عمیق بسته

بازرسی عمیق بسته (DPI) محتوای بسته‌ها و الگوهای ترافیک را بررسی می‌کند، نه فقط سرآیندها را، و برخی دیوارهای آتش از آن برای شناسایی و مسدود کردن پروتکل‌های رایج VPN استفاده می‌کنند.

7. استفادهٔ سازمانی

درصد زیادی از کارکنان سازمان‌ها در سراسر جهان از VPNهای امن برای ورود به پایگاه‌های داده داخلی استفاده می‌کنند و این امر آن را به استاندارد امنیتی کلیدی تبدیل کرده است.

8. VPNهای غیرمتمرکز

VPNهای غیرمتمرکز (dVPN) ترافیک را در شبکه‌ای از گره‌های مدیریت‌شده توسط همتایان توزیع می‌کنند و وابستگی به یک ارائه‌دهندهٔ متمرکز را کاهش می‌دهند.

9. گمنامی Tor در برابر VPN

VPN ترافیک را از یک ارائه‌دهندهٔ واحد عبور می‌دهد، در حالی که Tor (The Onion Router) ترافیک را از سه رله داوطلب (نگهبان، میانی و خروجی) می‌فرستد تا هیچ رله‌ای هر دو سر را نشناسد.

10. هزینهٔ نقض داده‌ها

به‌کارگیری مدل دسترسی امن اعتماد صفر همراه با VPN به سازمان‌ها کمک می‌کند از مالکیت فکری محافظت کنند و اثر مالی نقض داده را کاهش دهند.

منابع و مراجع فنی

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

منابع علمی و صنعتی

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

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

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

[4] Donenfeld, J. A. (2017). WireGuard: Next Generation Kernel Network Tunnel. NDSS Symposium.
https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/wireguard-next-generation-kernel-network-tunnel/

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

[6] IETF. (1999). RFC 2637: Point-to-Point Tunneling Protocol (PPTP).
https://datatracker.ietf.org/doc/html/rfc2637

کلید پاسخ: کاربرگ VPN چیست

1 کارکرد اصلی

پروتکل‌ها

پاسخ درست: B

نکتهٔ آموزشی

وظیفهٔ اصلی VPN برقراری تونل رمزگذاری‌شده‌ای است که داده‌های بار بسته را محافظت می‌کند و IP عمومی کاربر را پنهان می‌سازد. منبع: IETF Tunnel RFC.

2 تونل‌زنی شبکه

تأخیر

پاسخ درست: D

نکتهٔ آموزشی

پروتکل‌های تونل‌زنی بسته‌های داده اصلی را درون بسته‌های حامل بیرونی کپسوله می‌کنند تا با امنیت از شبکه‌های عمومی عبور کنند. منبع: IETF Tunnel RFC.

3 پرسش 3

پاسخ درست: B

نکتهٔ آموزشی

کدام استاندارد رمزگذاری به‌طور گسترده برای محافظت از ترافیک VPN استفاده می‌شود؟ → استاندارد مدرن AES-256

4 مؤلفه‌های رمزگذاری‌شده

کنترل‌های مسیریابی

پاسخ درست: C

نکتهٔ آموزشی

VPN کل بخش بار بسته‌های دادهٔ IP را رمزگذاری می‌کند و محتوای انتقال را محرمانه نگه می‌دارد. منبع: IETF Tunnel RFC.

5 پرسش 5

پاسخ درست: A

نکتهٔ آموزشی

رمزگذاری از یک الگوریتم و یک کلید استفاده می‌کند تا متن ساده را به متن رمزشدهٔ ناخوانا تبدیل کند.

کلید پاسخ: ایستگاه بررسی 2 – درست یا نادرست

6 **مسدودسازی شنود** — پنهان‌سازی IP — پاسخ درست: درست

نکتهٔ آموزشی

تونل‌های رمزگذاری‌شده تضمین می‌کنند محموله‌های بسته برای کسانی که داده را روی شبکه‌های Wi-Fi محلی رهگیری می‌کنند ناخوانا بماند. منبع: Deloitte Advisory.

7 **تغییرات سخت‌افزاری** — سرعت‌ها — پاسخ درست: نادرست

نکتهٔ آموزشی

VPNها تونل‌های شبکهٔ نرم‌افزاری هستند و سخت‌افزار روتر دروازهٔ شما را از نظر فیزیکی تغییر نمی‌دهند. منبع: Cure53 Audit.

8 **بسته‌های تونل‌زنی** — خطر شنود — پاسخ درست: درست

نکتهٔ آموزشی

تونل‌زنی با پیچیدن بسته‌های شبکهٔ اصلی درون سرایندهای انتقال برای عبور کار می‌کند. منبع: IETF Tunnel RFC.

9 **کلیدهای متقارن** — دیوارهای آتش — پاسخ درست: درست

نکتهٔ آموزشی

رمزنگاری متقارن از یک کلید مشترک هم برای رمزگذاری و هم برای رمزگشایی جریان‌های شبکه استفاده می‌کند. منبع: WireGuard Project.

10 **مصونیت از قدرت** — بدون لاگ — پاسخ درست: نادرست

نکتهٔ آموزشی

VPN فقط سیگنال‌های اتصال فعال را رمزگذاری می‌کند؛ نمی‌تواند از قطع سرویس ناشی از قطعی برق محلی جلوگیری کند. 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

H 1. تونل‌زنی	E 2. پروتکل	G 3. پهنای باند	A 4. سرور
C 5. محدودیت جغرافیایی	D 6. دیوار آتش	F 7. حریم خصوصی	B 8. ارائه‌دهندهٔ اینترنت (ISP)

ایستگاه بررسی 3: کلید پاسخ – اصطلاحات کلیدی

1 تونل‌زنی	2 پهنای باند	3 ژئوبلاک	4 پروتکل
5 دیوار آتش	6 سرور		

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

1 B – پروتکل	2 E – ژیوبلاک	3 F – دیواراتش	4 G – حریم‌خصوصی
5 H – ارایه‌دهنده	6 A – تونلزنی	7 D – سرور	8 C – پهناییباند

یادداشت‌های بحث برای مدرسان

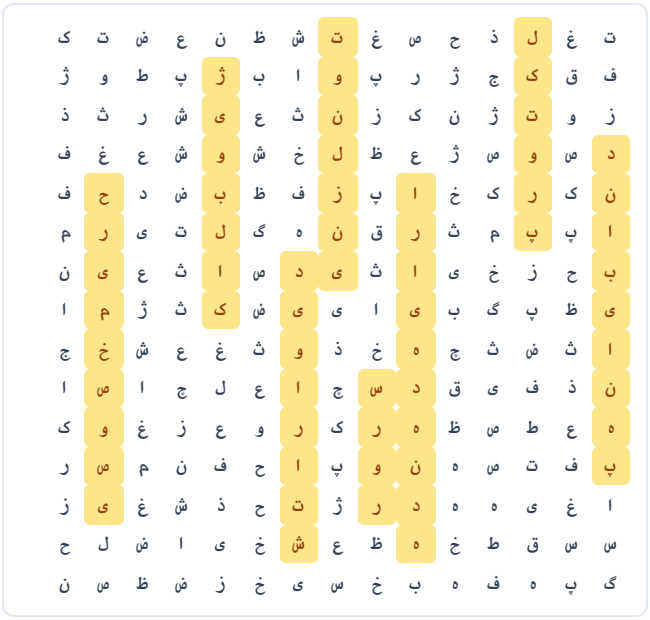
اصطلاحات کلیدی:
بررسی کنید که دانش‌آموزان بتوانند تونل‌زنی، پروتکل و پهنای باند را با کلمات خودشان توضیح دهند و برای هر کدام مثالی بزنند.

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

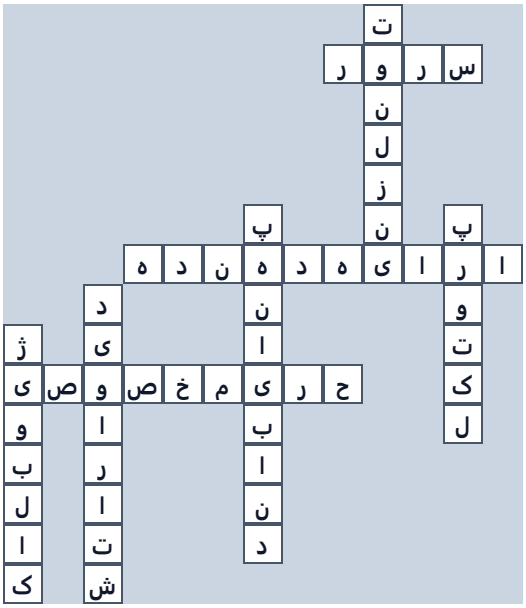
ارزیابی منابع:
از دانش‌آموزان بخواهید دست‌کم یک ادعا را در منابع کاربرگ بررسی کنند و دربارهٔ اینکه چرا ارقام، قیمت‌ها و قوانین ممکن است با گذشت زمان تغییر کنند گفت‌وگو کنید.

کلیدهای معما و یادداشت‌های معلم

پاسخ جدول کلمات



پاسخ جدول‌کلمات



راهنمای معلم برای پاسخ‌های جدول کلمات متقاطع

افقی

2 افقی: سرور رایانهٔ راه‌دوری که ترافیک شما را مسیریابی می‌کند و IP شما را پنهان می‌سازد (4 حرف)

5 افقی: ارایه‌دهنده شرکت تأمین‌کنندهٔ اینترنت (ISP) که اگر رمزگذاری نشود، ترافیک شما را ثبت می‌کند (10 حرف)

8 افقی: حریم‌خصوصی وضعیت رهایی از ردیابی یا نظارت عمومی (9 حرف)

عمودی

1 عمودی: تونلزنی پیچیدن بسته‌های داده درون بستهٔ دیگر برای انتقال امن (7 حرف)

3 عمودی: پروتکل مجموعهٔ قواعدی که تعیین می‌کند داده چگونه روی شبکه منتقل شود (6 حرف)

4 عمودی: پهناباند بیشینهٔ نرخ انتقال داده در یک اتصال (9 حرف)

6 عمودی: دیواراتش سامانهٔ امنیتی که ترافیک غیرمجاز را پایش و مسدود می‌کند (8 حرف)

7 عمودی: ژیوبلاک محدودیتی که دسترسی به وب را بر اساس مکان فیزیکی مسدود می‌کند (7 حرف)

کلید پاسخ کلمات درهم‌ریخته و رمزگشایی

کلید نمره‌دهی برای فعالیت بازچینی واژگان و چالش رمز مخفی.

کلید مرتب‌سازی کلمات

1. لنتزینو — تونلزنی
2. دپناهباین — پهناییاند
3. بژلکوای — ژیوبلاک
4. خیصموصحری — حریمخصوصی
5. تولپکر — پروتکل
6. ورسر — سرور
7. دشراتیاو — دیواراتش
8. دیدهاهرهنا — ارایهدهنده

کلید چالش رمز مخفی

"محافظت حریم خصوصی با تونل امن"

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.
- محافظت VPN: محتوای بسته‌های شبکه را رمزگذاری می‌کند و وقتی VPN درست پیکربندی شده باشد، ترافیک تونل رهگیری‌شده را برای شنودگران منفعل شبکهٔ 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.
- VPN چگونه کمک می‌کند: پنهان کردن مکان واقعی او با مسیریابی ترافیک از طریق سروری در کشور خودش. سایت IP کشور خود او را می‌بیند و دسترسی را مجاز می‌کند.