نام: _____ تاریخ: _____ نمره: _____

راهنمای امن‌ترین VPN

تحلیل فنی طراحی VPN با امنیت بالا، سرورهای حافظهٔ فرار فقط-RAM، امنیت دسترسی Zero Trust، دفاع‌های خصوصی DNS رمزگذاری‌شده در برابر نشت و پیکربندی‌های ممیزی‌شدهٔ WireGuard.

مرور آموزشی راهنمای امن‌ترین 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 بررسی استانداردهای فنی VPNهای بسیار امن راهنمایی می‌کند. با سخت‌افزار سرور فقط-RAM، امنیت دسترسی اعتماد صفر، resolverهای DNS رمزگذاری‌شدهٔ خصوصی و پیکربندی‌های ممیزی‌شدهٔ WireGuard آشنا می‌شوید.

ایستگاه‌های بررسی کاربرگ

- [ ] **بخش 1-4: بر پیکربندی‌های VPN و امنیت شبکه 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 بهترین VPNهای VPN.com

URL: https://www.vpn.com/vpn/most-secure-vpn/

نقشهٔ راه یادگیری امن‌ترین VPN شما

- معماری فنی و استانداردهای رمزگذاری در راهنمای امن‌ترین VPN را تحلیل کنید.
- تنظیمات کلاینت را برای جلوگیری از نشت ترافیک IP، DNS و WebRTC پیکربندی کنید.
- پروتکل‌های تونل‌زنی اختصاصی را با پیاده‌سازی‌های استاندارد مقایسه کنید.

دستورالعمل راهنمای امن‌ترین VPN

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 سخت‌افزار سرورهای فقط-RAM و سامانه‌های Zero Trust به کار ببرید. و در پایان، فعالیت تکمیلی «سریع فکر کن».

زیرساخت‌های فقطRAM و شبکه‌های اعتماد صفر (مقدمه)

VPN واقعاً امن بر چارچوب zero trust، سرورهای فقط-RAM برای جلوگیری از افشای گزارش‌ها هنگام توقیف دیسک، حل‌کننده‌های DNS رمزگذاری‌شدهٔ خصوصی و پروتکل‌های ممیزی‌شده مانند WireGuard تکیه دارد. این کنترل‌های ترکیبی از دارایی‌های دیجیتال باارزش در برابر تهدیدهای رهگیری دفاع می‌کنند.

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

ایستگاه بررسی 1: چالش چندگزینه‌ای

1 1. کدام معماری برای تضمین بالاترین امنیت در سرورهای مدرن VPN اساسی است؟

- A) زیرساخت سرور فقط-RAM
- B) ذخیره‌سازی مبتنی بر دیسک
- C) مسیریابی DNS پویا
- D) فعال‌سازی هدایت پورت

2 2. کدام پروتکل برای امن‌ترین و مدرن‌ترین پیکربندی‌های VPN به‌طور گسترده توصیه می‌شود؟

- A) WireGuard
- B) PPTP
- C) L2TP/IPSec
- D) SSTP

3 3. کدام چارچوب امنیتی تأیید پیوستهٔ هر اتصال را بدون استثنا الزامی می‌کند؟

- A) معماری Zero Trust
- B) دیوارهای آتش محیطی
- C) مسیریابی پویا
- D) کلیدهای مخفی مشترک

4 4. نقش اصلی محافظت از نشت DNS در کلاینت VPN چیست؟

- A) همهٔ درخواست‌های DNS را از طریق حل‌کننده‌های رمزگذاری‌شدهٔ خصوصی مسیریابی کنید
- B) مبهم‌سازی بسته‌های IP
- C) ذخیرهٔ محلی پرس‌وجوهای DNS در حافظهٔ نهان
- D) غیرفعال کردن سرورهای نام

5 5. مسیریابی Multi-Hop چگونه امنیت کلی تونل VPN را افزایش می‌دهد؟

- A) داده را به‌صورت متوالی از دو سرور جداگانه عبور می‌دهد
- B) سرعت فشرده‌سازی را افزایش می‌دهد
- C) داده‌ها را با رمزهای کم‌امنیت رمزگذاری می‌کند
- D) دیوارهای آتش را دور می‌زند

ایستگاه بررسی 2: چالش درست یا نادرست

6 پرسش 6

6. سرورهای فقطRAM فایل‌های لاگ را در حافظهٔ زودگذر ذخیره می‌کنند که با راه‌اندازی مجدد پاک می‌شود.

درست نادرست

7 پرسش 7

7. WireGuard از الگوریتم‌های رمزنگاری مدرنی استفاده می‌کند که کمتر در برابر گلوگاه‌های سرعت آسیب‌پذیرند.

درست نادرست

8 پرسش 8

8. Kill Switch در VPN با مسدود کردن همهٔ ترافیک شبکه در صورت قطع تونل کار می‌کند.

درست نادرست

9 پرسش 9

9. ممیزی‌های مستقل شخص ثالث برای راستی‌آزمایی تعهدات امنیتی بی‌ربط هستند.

درست نادرست

10 پرسش 10

10. مدل‌های اعتماد صفر فرض می‌کنند همهٔ اتصال‌های شبکهٔ داخلی به‌طور پیش‌فرض امن‌اند.

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. مدیران با استقرار چارچوب سخت‌گیرانهٔ _____ امنیت را اعمال می‌کنند.
2. مسیریابی بسته‌ها از چند نقطهٔ ورود مستلزم پیکربندی امن _____ است.
3. برای جلوگیری از نشت داده از درایوهای دزدیده‌شده، از طراحی _____ استفاده می‌کنیم.
4. ربایش توسط ISP با پیکربندی ویژگی‌های بومی _____ کاهش می‌یابد.
5. برای مسدود کردن ترافیک هنگام قطع اتصال، سازوکار _____ را فعال کنید.
6. برای به حداقل رساندن لاگ‌های ذخیره‌شده، ارائه‌دهنده‌ای کاملاً _____ انتخاب کنید.

بانک واژگان

اعتماد صفر | پروتکل | چندجهشی | حفاظت از DNS ممیزی‌شده | رمزگذاری | سرور فقط رم | قطع اضطراری

پاسخ‌های خود را اینجا بنویسید:

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

ایستگاه بررسی 4: تطبیق مفاهیم VPN و شبکه

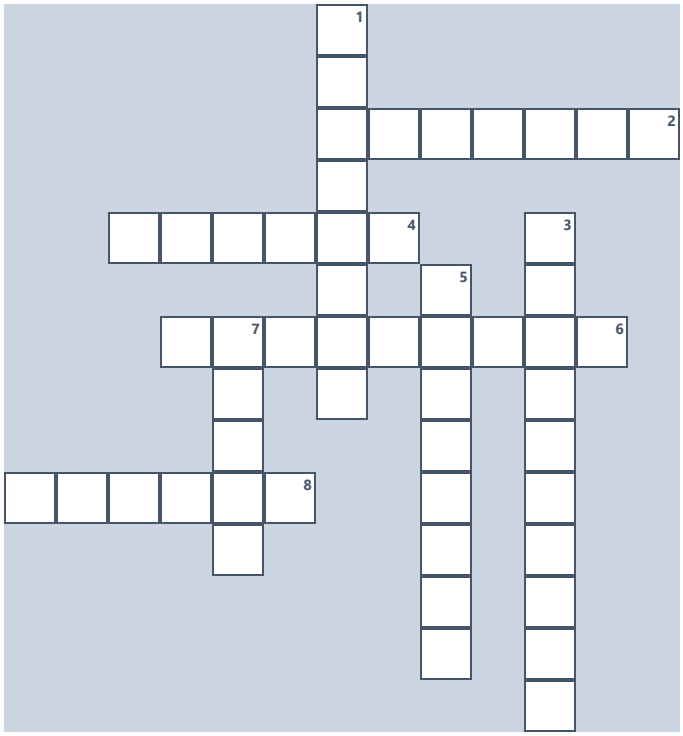
تطبیق تعاریف

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. اعتماد صفر	A	زیرساختی که به‌طور مستقل بازرسی شده و تأیید می‌کند هیچ گزارشی ذخیره نمی‌شود.
2. چندجهشی (Multi-Hop)	B	درهم‌سازی رمزنگاری داده‌های بار برای ایمن‌سازی انتقال.
3. سرور فقطRAM	C	چارچوب امنیتی که احراز هویت مداوم همهٔ کاربران را الزامی می‌کند.
4. محافظت DNS	D	مجموعه‌ای از قواعد فنی که تعیین می‌کند داده‌ها چگونه بسته‌بندی و ارسال شوند.
5. Kill Switch	E	مسیریابی آبشاری VPN که دو گره سرور را به هم زنجیر می‌کند.
6. سیستم ممیزی‌شده	F	معماری سروری که از حافظهٔ فرار برای ذخیرهٔ بارهای داده استفاده می‌کند.
7. رمزگذاری	G	اعمال پرس‌وجوهای DNS خصوصی برای محافظت از جست‌وجوهای سرور نام.
8. پروتکل	H	سازوکار ایمن‌شکست که اگر VPN از کار بیفتد ترافیک را مسدود می‌کند.

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. مسیریابی آبشاری VPN که دو گرهٔ سرور را به هم زنجیر می‌کند (7)

4. اعمال پرس‌وجوهای خصوصی برای محافظت از جست‌وجوی نام‌سرورها (6)

6. چارچوب امنیتی که احراز هویت مداوم همهٔ کاربران را الزامی می‌کند (9)

8. مجموعهٔ قواعد فنی که تعیین می‌کند داده چگونه بسته‌بندی و ارسال شود (6)

عمودی

1. سامانه‌ای که به‌طور مستقل بازرسی شده و ذخیره نشدن هیچ لاگی را تأیید می‌کند (8)

3. سازوکار ایمنی که اگر VPN از کار بیفتد ترافیک را مسدود می‌کند (10)

5. درهم‌ریزی رمزنگاشتی بارهای داده برای ایمن‌سازی انتقال (8)

7. معماری سروری که برای نگهداری بارهای داده از حافظهٔ فرار استفاده می‌کند (5)

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: مسیریابی آبشاری VPN که دو گرهٔ سرور را به هم زنجیر می‌کند (7 حرف):

4 افقی: اعمال پرس‌وجوهای خصوصی برای محافظت از جست‌وجوی نام‌سرورها (6 حرف):

6 افقی: چارچوب امنیتی که احراز هویت مداوم همهٔ کاربران را الزامی می‌کند (9 حرف):

8 افقی: مجموعهٔ قواعد فنی که تعیین می‌کند داده چگونه بسته‌بندی و ارسال شود (6 حرف):

عمودی

1 عمودی: سامانه‌ای که به‌طور مستقل بازرسی شده و ذخیره نشدن هیچ لاگی را تأیید می‌کند (8 حرف):

3 عمودی: سازوکار ایمنی که اگر VPN از کار بیفتد ترافیک را مسدود می‌کند (10 حرف):

5 عمودی: درهم‌ریزی رمزنگاشتی بارهای داده برای ایمن‌سازی انتقال (8 حرف):

7 عمودی: معماری سروری که برای نگهداری بارهای داده از حافظهٔ فرار استفاده می‌کند (5 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	چ	ش	ظ	ن	ع	ض	ت	ک
ف	ق	ک	ج	ژ	ر	پ	ن	ا	ب	د	پ	ط	و	ژ
ز	و	ت	ژ	ن	ک	ز	د	ث	ع	ی	ش	ر	ث	ذ
ر	ص	و	ص	ژ	ع	ظ	ج	خ	ش	ا	ش	ع	غ	ف
ف	ک	ر	ک	خ	ق	پ	ه	ف	ظ	ن	ض	د	م	ف
ص	پ	پ	م	ث	ط	ق	ش	ه	گ	ا	ت	ی	م	م
د	ح	ز	خ	ی	ع	ث	ی	ر	ص	س	ث	ع	ی	ن
ا	ظ	پ	گ	ب	ا	ا	ی	م	ض	ث	ژ	ا	ز	ث
م	ض	ث	چ	خ	ض	ذ	ث	ز	غ	ع	ش	چ	ی	ذ
ت	ف	ی	ق	چ	ط	ف	ع	گ	ل	چ	ا	ا	ش	ع
ع	ط	ص	ظ	ک	ر	ق	و	ذ	ع	ز	غ	ک	د	ف
ا	ت	ص	ه	پ	ا	ط	ح	ا	ف	ن	م	ر	ه	ا
غ	ی	ه	ه	ژ	ر	ر	ح	ر	ذ	ش	غ	ز	س	س
ق	ط	خ	ظ	ع	ی	م	خ	ی	ی	ا	ض	ل	ح	گ
پ	ه	ف	ه	ب	خ	س	ی	خ	ز	ض	ظ	ص	ن	پ

فهرست واژگان

اعتمادصفر
چندجهشی
فقطرم
دیاناس
قطعاضطراری
ممیزیشده
رمزگذاری
پروتکل

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. اعتمادصفر
B. چندجهشی
C. فقطرم
D. دیاناس
E. قطعاضطراری
F. ممیزیشده
G. رمزگذاری
H. پروتکل

	تعاریف و فیلدهای تطبیق
	1. سازوکار ایمنی که اگر VPN از کار بیفتد ترافیک را مسدود می‌کند.
	2. اعمال پرس‌وجوهای خصوصی برای محافظت از جست‌وجوی نام‌سرورها.
	3. مسیریابی آبشاری VPN که دو گرهٔ سرور را به هم زنجیر می‌کند.
	4. مجموعهٔ قواعد فنی که تعیین می‌کند داده چگونه بسته‌بندی و ارسال شود.
	5. درهم‌ریزی رمزنگاشتی بارهای داده برای ایمن‌سازی انتقال.
	6. معماری سروری که برای نگهداری بارهای داده از حافظهٔ فرار استفاده می‌کند.
	7. سامانه‌ای که به‌طور مستقل بازرسی شده و ذخیره نشدن هیچ لاگی را تأیید می‌کند.
	8. چارچوب امنیتی که احراز هویت مداوم همهٔ کاربران را الزامی می‌کند.

ایستگاه بررسی 7: چالش کلمات درهم‌ریخته

حروف زیر را مرتب کنید تا مفاهیم و اصطلاحات کلیدی شبکه خصوصی مجازی (VPN) آشکار شوند. پاسخ‌هایتان را در کادرهای ورودی ارائه‌شده بنویسید.

1. د ا م ع ا ص ف ر ت _____
2. ف م ر ط ق _____
3. ق ط ر ر ط ض ی ا ا ع _____
4. گ ر ی ا ذ ر م ز _____
5. ه ی ج د چ ش ن _____
6. ا ن د ا س ی _____
7. م ه ی ش د م ز ی _____
8. و ل پ ک ت ر _____

فعالیت تکمیلی: سریع فکر کن

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

1. قفل‌ها یا کلیدهایی که هر روز استفاده می‌کنید
2. چیزهایی که یک VPN می‌تواند پنهان کند
3. چیزهایی که VPN را امن می‌کنند
4. افسانه‌ها دربارهٔ VPNها
5. دلایل استفاده از VPN در سفر
6. جاهای امن در دنیای واقعی
7. واژه‌هایی به معنی «محافظت‌شده»
8. وعده‌هایی که یک ارائه‌دهندهٔ VPN خوب می‌دهد
9. واژه‌های مرتبط با حریم خصوصی
10. انواع ممیزی یا بازرسی
11. واژه‌هایی از این کاربرگ که می‌خواهید به خاطر بسپارید
12. چیزهایی که یک هکر می‌خواهد بدزدد
13. روش‌های تشخیص شبکهٔ Wi-Fi جعلی
14. جاهایی که از VPN استفاده می‌کنید
15. چیزهایی که ارائه‌دهندهٔ اینترنت شما می‌تواند ببیند

ایستگاه بررسی 8: مطالعات موردی VPN و شبکه

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

مطالعهٔ موردی 1: مستحکم‌سازی زیرساخت سازمانی

👷

سناریو: یک بانک شرکتی در حال بازطراحی توپولوژی دسترسی از راه دور خود است. آن‌ها به یک معماری zero trust نیاز دارند که همهٔ دستگاه‌های کلاینت را به سرورهای امن پیوند دهد.

پرسش برای بحث: مزیت اصلی ریزبخش‌بندی شبکه (micro-segmentation) تحت مدل VPN مبتنی بر Zero Trust چیست؟

مطالعهٔ موردی 2: حفاظت‌های سرور فقط-RAM

👷

سناریو: یک ارائه‌دهندهٔ VPN متمرکز بر امنیت سرورهای خود را ارتقا می‌دهد تا ضبط فیزیکی سرور تاریخچهٔ گزارش‌های کاربران را افشا نکند.

پرسش برای بحث: توضیح دهید پیکربندی‌های سخت‌افزاری فقط-RAM چگونه از استخراج پزشکی قانونی داده هنگام ضبط فیزیکی سرور جلوگیری می‌کنند.

ایستگاه بررسی 9: رمزگشایی

مهندس شبکه کانال‌های مسیریابی و تونل‌های کلاینت را ایمن می‌کند. از کلید حرف-به-عدد زیر استفاده کنید و با نوشتن حرف‌های متناظر در جاهای خالی، پیام 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

10	29	28	16	13	12	1	32	32	1	12	1	10	
10	32	29	25	29	28	32	1	1	12	27	1	4	32	6	32	10

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 پاسخ‌ها دربارهٔ شبکه‌های خصوصی مجازی (VPN) و تونل‌زنی را مرور کنید.

Q1: چه چیزی یک VPN را «امن‌ترین» می‌کند؟

ترکیبی از Zero Trust، سرورهای فقط-RAM و پروتکل‌های ممیزی‌شده.

Q2: سرورهای فقط-RAM چیستند؟

سرورهایی که در حافظهٔ فرار اجرا می‌شوند و طوری طراحی شده‌اند که هیچ گزارشی روی دیسک ذخیره نکنند.

Q3: VPN اعتماد صفر چیست؟

چارچوبی که هر درخواست دسترسی و اتصال را به‌طور پیوسته تأیید می‌کند.

Q4: چرا WireGuard امن تلقی می‌شود؟

پایگاه کد کوچک و به‌راحتی قابل ممیزی دارد و از رمزهای مدرن استفاده می‌کند.

Q5: VPNهای امن چگونه از نشت DNS جلوگیری می‌کنند؟

با مسیریابی همهٔ پرس‌وجوها از طریق تفکیک‌کننده‌های DNS خصوصی و رمزگذاری‌شده.

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

رایج‌ترین پرسش‌ها و پاسخ‌ها دربارهٔ شبکه‌های خصوصی مجازی (VPN) و تونل‌زنی را مرور کنید.

Q6: آیا یک VPN امن به ممیزی نیاز دارد؟

بله، ممیزی‌های مستقل ادعاهای بدون ثبت لاگ و امنیت کد را تأیید می‌کنند.

Q7: نقش کیل‌سوییچ چیست؟

اگر اتصال VPN قطع شود، ترافیک شبکه را بلافاصله متوقف می‌کند.

Q8: در VPNهای امن از چه رمزگذاری‌ای استفاده می‌شود؟

AES-256 و ChaCha20 استانداردهای صنعتی برای رمزگذاری هستند.

Q9: آیا مسیریابی Multi-Hop امن است؟

بله، دو سرور یا بیشتر را زنجیره می‌کند تا از تحلیل ترافیک جلوگیری کند.

Q10: صلاحیت قضایی فراساحلی چگونه کمک می‌کند؟

ممکن است محدود کند کدام قوانین اعمال می‌شوند، اما مصونیت مطلق ارائه نمی‌دهد.

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

جنبه‌های فنی پیشرفتهٔ پروتکل‌های تونل‌سازی VPN، یکپارچه‌سازی کلاینت‌های موبایل و استقرار سازمانی را بررسی کنید.

Q1: سرورهای فقط-RAM چگونه خطر ضبط داده را از بین می‌برند؟

چون روی RAM اجرا می‌شوند، کشیدن دوشاخه داده‌های نگهداری‌شده در حافظه را پاک می‌کند.

Q2: اعتماد صفر چگونه جایگزین امنیت پیرامونی استاندارد می‌شود؟

با هر کلاینت مانند یک عامل خصمانه رفتار می‌کند و احراز هویت پیوسته را الزامی می‌کند.

Q3: چه چیزی ممیزی کد WireGuard را آسان‌تر می‌کند؟

کد Linux آن کمتر از 4,000 خط است، بسیار کوچک‌تر از پشته‌های معمول VPN. [4]

Q4: DNSSEC چگونه از پرس‌وجوهای DNS محافظت می‌کند؟

رکوردهای DNS را امضا می‌کند تا حل‌کننده‌ها بتوانند پاسخ‌های جعلی یا دستکاری‌شده را تشخیص دهند.

Q5: Multi-Hop چگونه همبستگی ترافیک را پیچیده می‌کند؟

با جدا کردن IPهای ورودی و خروجی در ارائه‌دهندگان میزبانی مختلف.

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

جنبه‌های فنی پیشرفتهٔ پروتکل‌های تونل‌سازی VPN، یکپارچه‌سازی کلاینت‌های موبایل و استقرار سازمانی را بررسی کنید.

Q6: چرا حوزه‌های قضایی Five Eyes برای VPN پرخطرند؟

کشورهای عضو اطلاعات را به اشتراک می‌گذارند و ممکن است برای دسترسی به داده‌های کاربران از دستورهای قانونی استفاده کنند.

Q7: کیل‌سوییچ در سطح هسته چگونه پیاده‌سازی می‌شود؟

از قوانین دیوار آتش سیستم (مانند iptables یا WFP) برای مسدود کردن egress استفاده می‌کند.

Q8: رازداری پیشرو در دست‌دهی VPN چیست؟

کلیدهای نشست یکتا تولید می‌کند تا نشست‌های گذشته قابل رمزگشایی نباشند.

Q9: VPNهای امن چگونه نشت WebRTC را کاهش می‌دهند؟

با مسدود کردن درخواست‌های WebRTC یا مسیریابی آن‌ها از طریق تونل.

Q10: ممیزی‌های مستقل چگونه رعایت حریم خصوصی را تضمین می‌کنند؟

ممیزان آزمون نفوذ انجام می‌دهند و پیکربندی سرورها را بازرسی می‌کنند.

بخش 11: 10 واقعیت و بینش دنیای واقعی دربارهٔ VPN

واقعیت‌های دنیای واقعی دربارهٔ سرعت رمزگذاری VPN، ممیزی پروتکل‌ها، اتصال موبایل و کار راه‌دور سازمانی را مرور کنید.

1. بینش VPN

سرورهای فقطRAM سیستم‌عامل خود را هنگام بوت در حافظه بارگذاری می‌کنند، بنابراین پس از راه‌اندازی مجدد چیزی روی دیسک باقی نمی‌ماند.

2. بینش VPN

WireGuard از چارچوب Noise با ChaCha20، Curve25519، Poly1305، BLAKE2s و HKDF استفاده می‌کند. [3]

3. بینش VPN

اعتماد صفر دسترسی را به‌ازای هر منبع می‌دهد و بر اساس موقعیت شبکه هیچ اعتماد ضمنی‌ای ایجاد نمی‌کند (NIST SP 800-207). [1]

4. بینش VPN

اتحاد اطلاعاتی Five Eyes شامل آمریکا، بریتانیا، کانادا، استرالیا و نیوزیلند است.

5. بینش VPN

نشت‌های WebRTC زمانی رخ می‌دهند که مرورگرها از طریق پرس‌وجوهای STUN نشانی IP عمومی واقعی کلاینت را آشکار کنند.

6. بینش VPN

محرمانگی پیشروی کامل (PFS) تضمین می‌کند که لو رفتن یک کلید بلندمدت، کلیدهای نشست گذشته را آشکار نمی‌کند. [3]

7. بینش VPN

Cure53، یک شرکت امنیتی مستقر در برلین، ممیزی‌های چند ارائه‌دهندهٔ VPN را منتشر کرده است.

8. بینش VPN

نشت DNS زمانی رخ می‌دهد که پرس‌وجوهای DNS از تونل VPN عبور نکنند و به سرورهای نام ISP محلی بروند.

9. بینش VPN

تراشه‌های RAM فرار برای نگهداری داده‌ها به برق دائم نیاز دارند و با خاموش شدن، محتوایشان را از دست می‌دهند.

10. بینش VPN

سامانه‌های اعتماد صفر سازمانی پیش از اجازهٔ اتصال به منابع امن، بررسی‌های وضعیت دستگاه را اعمال می‌کنند. [1]

منابع و مراجع فنی

راهنمای مطالعه و پازل‌های تعاملی از استانداردها، مشخصات فنی و چارچوب‌های مقرراتی جهانی گردآوری شده‌اند.

منابع علمی و صنعتی

[1] NIST. (2020). SP 800-207: Zero Trust Architecture.
https://csrc.nist.gov/pubs/sp/800/207/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] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.
https://csrc.nist.gov/pubs/sp/800/77/r1/final

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

کلید پاسخ: ایستگاه بررسی 1 – چندگزینه‌ای

1 **سرور فقطRAM** فقطRAM پاسخ درست: A

نکتهٔ آموزشی

سرورهای فقطRAM هیچ لاگی روی دیسک ذخیره نمی‌کنند و داده‌ها با راه‌اندازی مجدد پاک می‌شوند. منبع: Most Secure VPN.

2 **پرسش 2** پاسخ درست: A

نکتهٔ آموزشی

WireGuard یک پایگاه کد کوچک و قابل ممیزی را با رمزهای مدرن ترکیب می‌کند.

3 **مدل اعتماد صفر** اعتماد صفر پاسخ درست: A

نکتهٔ آموزشی

مدل‌های اعتماد صفر انطباق دستگاه را پیش از دسترسی به‌طور مداوم راستی‌آزمایی می‌کنند. منبع: Most Secure VPN.

4 **محافظت DNS** محافظت DNS پاسخ درست: A

نکتهٔ آموزشی

محافظت در برابر نشت DNS پرس‌وجوهای جست‌وجو را از طریق حل‌کننده‌های خصوصی مسیریابی می‌کند. منبع: Most Secure VPN.

5 **تونل‌های چندجهشی** چندجهشی (Multi-hop) پاسخ درست: A

نکتهٔ آموزشی

مسیریابی چندجهشی دو گرهٔ سرور جداگانه را به‌صورت متوالی زنجیر می‌کند. منبع: Most Secure VPN.

کلید پاسخ: ایستگاه بررسی 2 – درست یا نادرست

6 سرور فقطRAM — فقطRAM — پاسخ درست: درست

نکتهٔ آموزشی

سخت‌افزار سرور فقطRAM هیچ داده‌ای روی دیسک نمی‌نویسد و با راه‌اندازی مجدد پاک می‌شود. منبع: Most Secure VPN.

7 سرعت WireGuard — WIREGUARD — پاسخ درست: درست

نکتهٔ آموزشی

WireGuard از رمزنگاری مدرنی استفاده می‌کند که از گلوگاه‌های پردازشی دوری می‌کند. استناد: Most Secure VPN.

8 Kill Switch — کلید قطع ایمن‌شکست — پاسخ درست: درست

نکتهٔ آموزشی

Kill Switch در صورت قطع اتصال VPN همهٔ ترافیک را مسدود می‌کند. منبع: Most Secure VPN.

9 ممیزی‌های شخص ثالث — ممیزی‌های ضروری — پاسخ درست: نادرست

نکتهٔ آموزشی

ممیزی‌های شخص ثالث برای راستی‌آزمایی ادعاهای حریم خصوصی شرکت‌ها ضروری هستند. منبع: Most Secure VPN.

10 پرسش 10 — پاسخ درست: نادرست

نکتهٔ آموزشی

Zero Trust هیچ اعتماد ضمنی بر اساس موقعیت شبکه اعطا نمی‌کند.

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

C 1. اعتماد صفر	E 2. چندجهشی (Multi-Hop)	F 3. سرور فقطRAM	G 4. محافظت DNS
H 5. Kill Switch	A 6. سیستم ممیزی‌شده	B 7. رمزگذاری	D 8. پروتکل

ایستگاه بررسی 3: کلید پاسخ – اصطلاحات کلیدی

1 اعتماد صفر	2 چندجهشی	3 سرور فقط رم	4 حفاظت از DNS
5 قطع اضطراری	6 ممیزی‌شده		

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

1 E – قطعاضطراری	2 D – دیاناس	3 B – چندجهشی	4 H – پروتکل
5 G – رمزگذاری	6 C – فقطرم	7 F – ممیزیشده	8 A – اعتمادصفر

یادداشت‌های بحث برای مدرسان

اصطلاحات کلیدی:
بررسی کنید که دانش‌آموزان بتوانند اعتماد صفر، چندجهشی (Multi-Hop) و سرور فقطRAM 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.

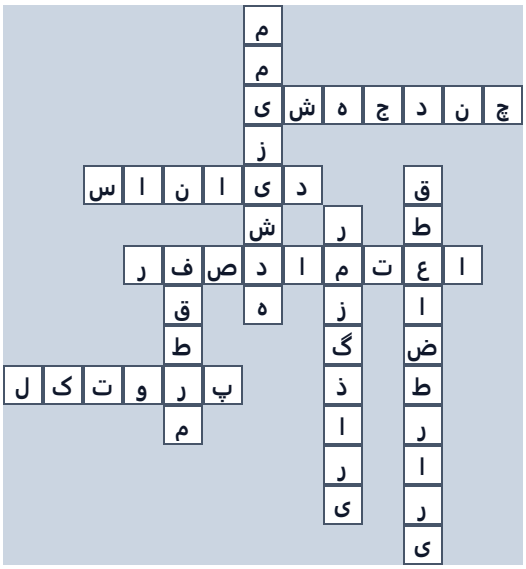
ارزیابی منابع:
از دانش‌آموزان بخواهید دست‌کم یک ادعا را در منابع کاربرگ بررسی کنند و دربارهٔ اینکه چرا ارقام، قیمت‌ها و قوانین ممکن است با گذشت زمان تغییر کنند گفت‌وگو کنید.

کلیدهای معما و یادداشت‌های معلم

پاسخ جدول کلمات

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

پاسخ جدول‌کلمات



راهنمای معلم برای پاسخ‌های جدول کلمات متقاطع

افقی

2 افقی: چندجهشی مسیریابی آبشاری VPN که دو گرهٔ سرور را به هم زنجیر می‌کند (7 حرف)

4 افقی: دیاناس اعمال پرس‌وجوهای خصوصی برای محافظت از جست‌وجوی نام‌سرورها (6 حرف)

6 افقی: اعتمادصفر چارچوب امنیتی که احراز هویت مداوم همهٔ کاربران را الزامی می‌کند (9 حرف)

8 افقی: پروتکل مجموعهٔ قواعد فنی که تعیین می‌کند داده چگونه بسته‌بندی و ارسال شود (6 حرف)

عمودی

1 عمودی: ممیزیشده سامانه‌ای که به‌طور مستقل بازرسی شده و ذخیره نشدن هیچ لاگی را تأیید می‌کند (8 حرف)

3 عمودی: قطعاضطراری سازوکار ایمنی که اگر VPN از کار بیفتد ترافیک را مسدود می‌کند (10 حرف)

5 عمودی: رمزگذاری درهم‌ریزی رمزنگاشتی بارهای داده برای ایمن‌سازی انتقال (8 حرف)

7 عمودی: فقطرم معماری سروری که برای نگهداری بارهای داده از حافظهٔ فرار استفاده می‌کند (5 حرف)

کلید پاسخ کلمات درهم‌ریخته و رمزگشایی

کلید نمره‌دهی برای فعالیت بازچینی واژگان و چالش رمز مخفی.

کلید مرتب‌سازی کلمات

1. دامعاصفرت — اعتمادصفر
2. فمرطق — فقطرم
3. قطررطضیااع — قطعاضطراری
4. گریاذرمز — رمزگذاری
5. هیجدچشن — چندجهشی
6. انداسی — دیاناس
7. مهیشدمزی — ممیزیشده
8. ولپکتر — پروتکل

کلید چالش رمز مخفی

"دارایی ارزشمند دیجیتال را ایمن کنید"

کلید پاسخ مطالعات موردی

A مطالعهٔ موردی 1: مستحکم‌سازی زیرساخت سازمانی

پاسخ معلم

راهنمای نمره‌دهی

پاسخ‌های دانش‌آموز باید نکات زیر را پوشش دهد:

- تحلیل سناریو: یک بانک سازمانی در حال بازطراحی توپولوژی دسترسی راه‌دور خود است. آن‌ها معماری اعتماد صفر می‌خواهند که همهٔ دستگاه‌های کلاینت را به سرورهای امن پیوند دهد.
- راهبرد و راه‌حل پیشنهادی: راهنمای نمره‌دهی: توضیح دهید که ریزبخش‌بندی دسترسی را به منابع مشخص محدود می‌کند و در صورت نفوذ به یک دستگاه، از حرکت جانبی تهدید جلوگیری می‌کند.

B مطالعهٔ موردی 2: حفاظت‌های سرور فقط-RAM

پاسخ معلم

راهنمای نمره‌دهی

پاسخ‌های دانش‌آموز باید نکات زیر را پوشش دهد:

- تحلیل سناریو: یک ارائه‌دهندهٔ VPN امنیت‌محور سرورهای خود را ارتقا می‌دهد تا توقیف فیزیکی سرور تاریخچهٔ گزارش‌های کاربران را افشا نکند.
- راهبرد و راه‌حل پیشنهادی: راهنمای نمره‌دهی: توضیح دهید که سرورهای RAM-Only فضای ذخیره‌سازی دیسک فیزیکی ندارند. قطع برق به‌طور خودکار همهٔ داده‌های موقت در حافظهٔ فرّار را پاک می‌کند.