نام: _____ تاریخ: _____ نمره: _____

امنیت و رمزگذاری Wi-Fi عمومی

حمله‌های مرد میانی، نقاط دسترسی جعلی، شنود بسته، تونل‌های VPN و رمزگذاری HTTPS.

مرور آموزشی امنیت Wi-Fi عمومی

خوش آمدید! این بستهٔ فعالیت شما را در بررسی امنیت Wi-Fi عمومی راهنمایی می‌کند. با شبکه‌های رمزگذاری‌نشده، حملات مرد میانی (MitM)، نقاط دسترسی جعلی، شنود بسته‌ها، تونل‌های VPN و امنیت انتقال HTTPS آشنا می‌شوید.

ایستگاه‌های بررسی کاربرگ

- [ ] **بخش 1-4: بر امنیت سایبری و پیشگیری از تهدید 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**

ایمن‌شده
رمزگذاری داده
استاندارد AES 256 بیتی

منطبق
استانداردهای جهانی
چارچوب‌های GDPR و CCPA

اعتماد صفر
سیاست دسترسی
احراز هویت چندعاملی

باز کردن راهنمای امنیت سایبری VPN.com

URL: https://www.vpn.com/cybersecurity/public-wifi-security/

نقشهٔ راه یادگیری امنیت Wi-Fi عمومی شما

- خطرهای رایج Wi-Fi عمومی، از جمله شنود بسته‌ها و نقاط دسترسی جعلی را شناسایی کنید.
- برای ایمن‌سازی داده‌های در حال انتقال، تونل‌های رمزگذاری VPN را پیاده‌سازی کنید.
- HTTPS و تنظیمات امن مرورگر وب را برای کارکنان دورکار اعمال کنید.

راهنمای دستورالعمل‌های امنیت Wi-Fi عمومی

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 امنیت دسترسی از راه دور به کار ببرید. و در پایان، فعالیت تکمیلی «سریع فکر کن».

امنیت Wi-Fi عمومی و حفاظت از انتقال (مقدمه)

نقاط اتصال Wi-Fi عمومی رمزگذاری‌نشده ترافیک شبکه را در معرض شنود بسته و جعل Evil Twin قرار می‌دهند. عبور دادن ترافیک از تونل‌های رمزگذاری امن VPN و اعمال قواعد HSTS فقط-HTTPS از نشست‌ها در برابر رهگیری شبکهٔ محلی محافظت می‌کند.

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

ایستگاه بررسی 1: چالش چندگزینه‌ای

1. حملهٔ مرد میانی (MitM) چیست؟

- A. رهگیری و تغییر ارتباطات میان دو طرف در یک شبکهٔ مشترک
- B. روش استخراج پایگاه داده که رکوردهای کاربران را هدف می‌گیرد
- C. اشباع وب‌سرورها با درخواست‌های ترافیک شبکه
- D. پاک کردن حجم‌های ذخیره‌سازی درایو سخت محلی

2. نقطهٔ دسترسی جعلی (Evil Twin) چیست؟

- A. هات‌اسپات Wi-Fi مخربی که با همان SSID یک شبکهٔ قانونی پیکربندی شده است
- B. ابزار مدیریتی برای پایش پشتیبان‌های پایگاه داده
- C. پیکربندی دروازهٔ امن VPN
- D. یک رکورد DNS که سرورهای ایمیل مجاز را نگاشت می‌کند

3. VPN چگونه از ترافیک Wi-Fi عمومی محافظت می‌کند؟

- A. همهٔ بسته‌های شبکه را در تونل رمزگذاری‌شده می‌پیچد و آن‌ها را برای sniffer ناخوانا می‌کند
- B. همهٔ درخواست‌های اتصال ورودی را به‌طور خودکار مسدود می‌کند
- C. نشانی MAC کارت شبکهٔ فیزیکی را تغییر می‌دهد
- D. کوکی‌های ذخیره‌شده را در مرورگر وب حذف می‌کند

4. شنود بسته (packet sniffing) چیست؟

- A. استفاده از ابزارهای سخت‌افزاری یا نرم‌افزاری برای ضبط و ثبت بسته‌های شبکه
- B. اسکن پوشه‌های محلی برای یافتن فایل‌های تکراری
- C. محدود کردن امتیازهای خواندن پایگاه داده بر اساس نقش کاربران
- D. رمزگذاری درایوهای ذخیره‌سازی با کلیدهای AES-256

5. نقش HTTPS چیست؟

- A. رمزگذاری ترافیک نشست میان مرورگر و سرور وب
- B. فیلتر کردن پیام‌های ایمیل ورودی در دروازه
- C. فشرده‌سازی تصاویر برای بارگذاری سریع‌تر صفحه‌ها
- D. مدیریت ساختار فایل‌ها در ذخیره‌ساز متصل به شبکه

ایستگاه بررسی 2: چالش درست یا نادرست

6 پرسش 6

6. کاربران متصل می‌توانند به‌آسانی داده‌های متنی ساده را در شبکه‌های Wi-Fi عمومی باز ضبط کنند.

درست ○ نادرست ○

7 پرسش 7

7. نقاط دسترسی مخرب (Evil Twin) همیشه توسط مدیران شبکه مجاز شناخته می‌شوند.

درست ○ نادرست ○

8 پرسش 8

8. VPN در محافظت از ترافیک در برابر شنود بسته‌ها در شبکه‌های عمومی بی‌اثر است.

درست ○ نادرست ○

9 پرسش 9

9. HTTPS فقط مسیر URL را رمزگذاری می‌کند و محتوای بسته را به‌صورت متن ساده باقی می‌گذارد.

درست ○ نادرست ○

10 پرسش 10

10. هات‌اسپات‌های وای‌فای با امنیت WPA3 حفاظت قوی‌تری نسبت به شبکه‌های باز و بدون گذرواژه ارائه می‌دهند.

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. ربودن گذرواژه‌های خصوصی در وای‌فای عمومی، _____ ارتباطات است.
2. تحلیل بسته‌های خام در شبکهٔ محلی از _____ بسته استفاده می‌کند.
3. هات‌اسپات جعلی که وای‌فای هتل را تقلید می‌کند، یک _____ است.
4. ایمن‌سازی ترافیک وب هنگام انتقال مستلزم رمزگذاری با _____ است.
5. رمزگذاری همهٔ خروجی‌های شبکه از یک _____ کلاینت استفاده می‌کند.
6. مسیر ارتباطی رمزگذاری‌شده در شبکه‌های عمومی یک _____ است.

بانک واژگان

اسنیفینگ | تونل | دوقلوی شیطانی | دیوار آتش | شنود | HTTPS | VPN | WPA3

پاسخ‌های خود را اینجا بنویسید:

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

ایستگاه بررسی 4: تطبیق مفاهیم امنیت

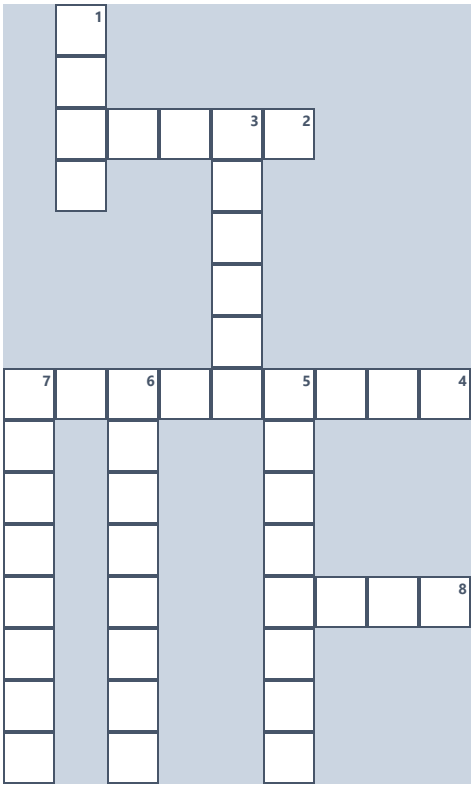
تطبیق تعاریف

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. شنود	A	استاندارد نوین امنیت Wi-Fi.
2. شنود	B	مسیر امن داده در حین انتقال.
3. دوقلوی شیطانی	C	پالایش ترافیک ورودی.
4. HTTPS	D	هات‌اسپات مخرب که Wi-Fi را تقلید می‌کند.
5. VPN	E	خواندن ترافیک در حال انتقال.
6. تونل	F	ضبط بسته‌های داده‌ای شبکه.
7. WPA3	G	شبکهٔ خصوصی مجازی رمزگذاری‌شده.
8. دیوار آتش	H	انتقال امن وب.

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. هات‌اسپات جعلی که وای‌فای را تقلید می‌کند. (5)

4. معیار نوین امنیت وای‌فای. (9)

8. مسیر امن داده در حال انتقال. (4)

عمودی

1. خواندن ترافیک در حال انتقال. (4)

3. شبکهٔ خصوصی مجازی رمزگذاری‌شده. (6)

5. انتقال امن وب. (8)

6. ضبط بسته‌های داده شبکه. (8)

7. فیلتر کردن ترافیک ورودی. (8)

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: هات‌اسپات جعلی که وای‌فای را تقلید می‌کند. (5 حرف):

4 افقی: معیار نوین امنیت وای‌فای. (9 حرف):

8 افقی: مسیر امن داده در حال انتقال. (4 حرف):

عمودی

1 عمودی: خواندن ترافیک در حال انتقال. (4 حرف):

3 عمودی: شبکهٔ خصوصی مجازی رمزگذاری‌شده. (6 حرف):

5 عمودی: انتقال امن وب. (8 حرف):

6 عمودی: ضبط بسته‌های داده شبکه. (8 حرف):

7 عمودی: فیلتر کردن ترافیک ورودی. (8 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	ذ	ح	س	غ	ش	د	ظ	ن	ع	ض	ت	ک	ف
ق	ج	و	ژ	ر	پ	ا	ی	ب	پ	و	ط	و	ژ	ز
و	ژ	ل	ن	ک	ز	ث	و	ع	ش	ی	ر	ث	ذ	ص
ص	ژ	ق	ع	ظ	خ	ش	ا	ش	ع	پ	غ	ف	ک	ک
ن	خ	و	پ	ف	ا	ظ	ر	ض	د	ی	ف	پ	م	ث
م	ق	د	ه	گ	س	ت	ا	ی	م	ا	ح	ز	خ	ی
ا	ث	ص	ث	ع	ت	ن	ت	س	ظ	ن	پ	گ	ب	ا
ل	ی	ض	ث	ژ	ا	ا	ش	ث	ن	ض	ث	چ	خ	ذ
ا	ث	غ	ع	ش	ن	چ	ذ	ف	ی	ی	ق	چ	ع	ل
ص	چ	ا	ا	ع	د	ت	ط	ص	ظ	ک	ف	و	ع	ز
ت	غ	ک	ف	ت	ا	و	ص	ه	پ	د	ح	ی	ف	ن
ا	م	ر	ا	غ	ر	ن	ی	ه	و	ه	ژ	ح	ن	ذ
ش	غ	ز	س	س	د	ل	ق	ن	ط	خ	ظ	ع	خ	گ
ی	ا	ض	ل	ح	گ	پ	ش	ه	ف	ه	ب	خ	س	ی
خ	ز	ض	ظ	س	ن	پ	س	ی	ه	ح	و	ط	م	گ

فهرست واژگان

شنود
اسنیفینگ
دوقلو
اتصالامن
وی‌پیان
تونل
استاندارد
دیواراتش

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. شنود
B. اسنیفینگ
C. دوقلو
D. اتصالامن
E. وپیان
F. تونل
G. استاندارد
H. دیواراتش

تعاریف و فیلدهای تطبیق
1. معیار نوین امنیت وای‌فای.
2. هات‌اسپات جعلی که وای‌فای را تقلید می‌کند.
3. ضبط بسته‌های داده شبکه.
4. مسیر امن داده در حال انتقال.
5. فیلتر کردن ترافیک ورودی.
6. خواندن ترافیک در حال انتقال.
7. شبکهٔ خصوصی مجازی رمزگذاری‌شده.
8. انتقال امن وب.

ایستگاه بررسی 7: چالش کلمات درهم‌ریخته

حروف زیر را مرتب کنید تا مفاهیم و اصطلاحات کلیدی امنیت سایبری آشکار شوند. پاسخ‌هایتان را در کادرهای ورودی ارائه‌شده بنویسید.

1. و ش د ن
2. د و ل ق و
3. و پ ی ن ا ی
4. ن د ر ا ا د ا س ت
5. ف ی س گ ی ا ن ن
6. م ن ا ا ا ل ت ص
7. ن ت ل و
8. ا ی ر ش د ت ا و

فعالیت تکمیلی: سریع فکر کن

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

1	دلایل به‌روزرسانی نرم‌افزار		
2	دستگاه‌هایی که به‌طور خودکار به Wi-Fi وصل می‌شوند		
3	اطلاعاتی که هرگز نباید به اشتراک بگذارید		
4	عادت‌های ایمن که می‌توانید از امروز شروع کنید		
5	روش‌های ایمن ماندن در کافه		
6	دستگاه‌هایی که می‌توانند هک شوند		
7	چیزهایی که یک هکر در Wi-Fi باز می‌تواند ببیند		
8	نشانه‌های شبکهٔ Wi-Fi جعلی		
9	جایگزین‌های Wi-Fi عمومی		
10	نشانه‌های هشدار در یک ایمیل		
11	کارهایی که در Wi-Fi عمومی انجام نمی‌دهید		
12	جاهایی که Wi-Fi رایگان دارند		
13	روش‌های محافظت از حساب‌هایتان		
14	نشانه‌های آلوده بودن رایانه		
15	نام‌های Wi-Fi که مشکوک به نظر می‌رسند		

ایستگاه بررسی 8: مطالعات موردی امنیت سایبری

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

مطالعهٔ موردی 1: مهار شنود بسته‌ها در Wi-Fi عمومی



سناریو: یک مدیر فروش دورکار که به شبکهٔ Wi-Fi عمومی فرودگاه وصل است، متوجه می‌شود چند ایمیل حساس کسب‌وکار که به‌صورت متن ساده ارسال شده‌اند اندکی پس از ارسال نشت کرده‌اند.

پرسش برای بحث: ریسک‌های شبکهٔ عمومی را تحلیل کنید و یک راه‌حل رمزگذاری ترافیک را شرح دهید.

مطالعهٔ موردی 2: دفاع در برابر هات‌اسپات جعلی دوقلوی شرور



سناریو: مهاجمان یک نقطهٔ دسترسی بی‌سیم جعلی به نام «CoffeeShop_Guest» را مستقر می‌کنند که هات‌اسپات یک کافهٔ معتبر را تقلید می‌کند و ترافیک شبکهٔ مهمانان بی‌خبر را ضبط می‌کند.

پرسش برای بحث: مراحل راستی‌آزمایی برای تشخیص و مسدود کردن نقاط دسترسی جعلی را شرح دهید.

ایستگاه بررسی 9: رمزگشایی

متخصص امنیت سایبری از دارایی‌های شبکه در برابر عوامل تهدید آنلاین محافظت 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

25	32	23	1	12	4		32	12	1	11	26	13	28	12
1	2		32	28	30	28	21		32	1	23	32	1	30
						29	1	32	3	32	30			

پیام رمزگشایی‌شده:

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

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

پرسش‌ها و پاسخ‌های رایج دربارهٔ کاهش تهدیدهای آنلاین را مرور کنید.

Q1: چرا Wi-Fi عمومی ناامن است؟

Wi-Fi عمومی باز، ترافیک را در هوا رمزگذاری نمی‌کند، بنابراین افراد نزدیک می‌توانند هر دادهٔ محافظت‌نشده را بگیرند. [2]

Q2: شنود بسته (packet sniffing) چیست؟

packet sniffer داده‌های خام جاری روی رابط شبکه را ضبط می‌کند و گذرواژه‌های متن ساده و جزئیات ترافیک را افشا می‌کند.

Q3: Evil Twin چیست؟

نقطهٔ دسترسی جعلی که هکرها راه می‌اندازند و نام و تنظیمات یک هات‌اسپات Wi-Fi محلی مورد اعتماد را تقلید می‌کند.

Q4: VPN چگونه از من محافظت می‌کند؟

ترافیک شما را از طریق یک تونل رمزگذاری‌شده مسیریابی می‌کند و فعالیت مرور شما را از شنودگرهای شبکهٔ محلی پنهان می‌کند.

Q5: آیا HTTPS در Wi-Fi عمومی از من محافظت می‌کند؟

بله، داده‌های مبادله‌شده میان مرورگر و وب‌سایت را رمزگذاری می‌کند و VPN لایهٔ محافظتی دیگری اضافه می‌کند.

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

پرسش‌ها و پاسخ‌های رایج دربارهٔ کاهش تهدیدهای آنلاین را مرور کنید.

Q6: WPA3 چیست؟

استاندارد مدرن Wi-Fi Protected Access که رمزگذاری قوی‌تر و محافظت در برابر حملات فرهنگ‌لغت آفلاین ارائه می‌دهد. [1]

Q7: آیا Wi-Fi عمومی می‌تواند بدافزار منتقل کند؟

بله، مهاجمان می‌توانند ترافیک را رهگیری کنند و درخواست‌های دانلود مخرب (دانلودهای drive-by) را به نشست مرورگر شما تزریق کنند.

Q8: خطر اشتراک‌گذاری فایل چیست؟

اگر اشتراک‌گذاری فایل فعال باشد، سایر کاربران شبکهٔ عمومی می‌توانند پوشهٔ محلی شما را بخوانند یا تغییر دهند.

Q9: captive portal چیست؟

صفحهٔ ورودی که شبکه‌های هتل یا کافه برای دادن دسترسی اینترنت به کار می‌برند و گاهی مهاجمان می‌توانند آن را جعل کنند.

Q10: آیا باید وقتی از Wi-Fi استفاده نمی‌کنم آن را خاموش کنم؟

بله، خاموش کردن Wi-Fi از اتصال خودکار دستگاه شما به شبکه‌های نامطمئن جلوگیری می‌کند.

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

جنبه‌های فنی پیشرفتهٔ چارچوب‌های امنیتی، تحلیل بدافزار و انطباق داده را بررسی کنید.

Q1: حملهٔ مرد میانی چگونه از DNS سوءاستفاده می‌کند؟

با استفاده از جعل DNS روی یک مسیریاب سرکش برای هدایت مرورگرهای هدف به صفحه‌های فرود فیشینگ شبیه‌ساز به جای دامنه‌های هدف.

Q2: ربایش نشست چیست؟

مهاجمی که کوکی نشست رمزگذاری‌نشده را روی Wi-Fi عمومی شنود می‌کند و آن را وارد می‌کند تا ورود با اعتبارنامه را دور بزند.

Q3: SSL stripping چیست؟

حملهٔ MitM که در آن مهاجم درخواست امن HTTPS کاربر را به HTTP رمزگذاری‌نشده تنزل می‌دهد و اطلاعات ورود را به‌صورت متن ساده ضبط می‌کند.

Q4: HSTS چگونه در برابر SSL stripping محافظت می‌کند؟

HTTP Strict Transport Security مرورگرها را وادار می‌کند فقط از طریق HTTPS متصل شوند و بازگشت به HTTP رمزگذاری‌نشده را رد می‌کند. [3]

Q5: VPN با تونل‌بندی تفکیکی چیست؟

پیکربندی که فقط ترافیک شرکتی را از VPN عبور می‌دهد و داده‌های اینترنت عمومی را مستقیم می‌فرستد، که می‌تواند خطر افشای مسیر نشت را داشته باشد.

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

جنبه‌های فنی پیشرفتهٔ چارچوب‌های امنیتی، تحلیل بدافزار و انطباق داده را بررسی کنید.

Q6: چرا WPA2 در برابر KRACK آسیب‌پذیر است؟

حملهٔ نصب مجدد کلید (Key Reinstallation Attack) از دست‌تکانی چهارمرحله‌ای WPA2 سوءاستفاده می‌کند تا بسته‌ها را بدون گذرواژهٔ Wi-Fi رمزگشایی کند.

Q7: انزوای کلاینت چیست؟

تنظیم امنیتی روتر که مانع می‌شود دستگاه‌های متصل به Wi-Fi مستقیماً با یکدیگر ارتباط برقرار کنند و شنود محلی را مسدود می‌کند.

Q8: مهاجمان چگونه از سرورهای DNS جعلی استفاده می‌کنند؟

آن‌ها روترهای مخرب را طوری پیکربندی می‌کنند که سرورهای DNS جعلی به کلاینت‌ها بدهند و بتوانند همهٔ جست‌وجوهای وب را رهگیری و بازنویسی کنند.

Q9: آیا VPN می‌تواند آدرس MAC محلی من را پنهان کند؟

خیر. نشانی‌های MAC شناسه‌های محلی لایه 2 هستند؛ به‌جای آن از تنظیم داخلی تصادفی‌سازی MAC دستگاه خود (نشانی خصوصی) استفاده کنید.

Q10: حملهٔ جعل پورتال اسیرکننده چیست؟

مهاجمی که درگاه احراز هویت جعلی را روی hotspot جعلی میزبانی می‌کند تا به بهانهٔ دسترسی رایگان به Wi-Fi اعتبارنامه را بدزدد.

بخش 11: 10 واقعیت و بینش دنیای واقعی دربارهٔ امنیت سایبری

واقعیت‌های دنیای واقعی دربارهٔ نقض‌های امنیتی، سازوکارهای دفاعی و استانداردهای انطباق را مرور کنید.

1. بینش امنیت

کارکنان راه‌دور اغلب از Wi-Fi در کافه‌ها، هتل‌ها و فرودگاه‌ها استفاده می‌کنند، جایی که نمی‌توانند امنیت شبکه را کنترل کنند.

2. بینش امنیت

hotspot جعلی Evil Twin می‌تواند نام و نشانی MAC دقیق یک شبکهٔ مورد اعتماد را کپی کند و دستگاه‌ها را گمراه کند.

3. بینش امنیت

نرم‌افزارهای شنود بسته مانند Wireshark رایگان‌اند و می‌توانند گذرواژه‌های HTTP رمزگذاری‌نشده را به‌صورت متن ساده نمایش دهند.

4. بینش امنیت

امنیت WPA3 از احراز هویت همزمان برابرها (SAE) برای محافظت در برابر حملات brute force محلی استفاده می‌کند.

5. بینش امنیت

حمله‌های SSL stripping با رهگیری تغییر مسیرهای اولیهٔ HTTP در دروازه، حفاظت‌های پایهٔ HTTPS را دور می‌زنند.

6. بینش امنیت

سرایندهای پاسخ HTTP Strict Transport Security (HSTS) مانع بازگشت مرورگرها به اتصال‌های رمزگذاری‌نشدهٔ HTTP می‌شوند. [3]

7. بینش امنیت

خاموش کردن «اتصال خودکار» مانع از اتصال گوشی‌های هوشمند به شبکه‌های مخرب مشابه در فضاهای عمومی می‌شود.

8. بینش امنیت

پیکربندی‌های VPN «همیشه روشن» سازمانی، همهٔ ترافیک شبکهٔ کارکنان دورکار را از دیوارهای آتش شرکتی عبور می‌دهند.

9. بینش امنیت

نقاط دسترسی مخرب می‌توانند پاسخ‌های DNS جعلی بدهند و دامنه‌های هدف را به سرورهای فیشینگ هدایت کنند.

10. بینش امنیت

بدون VPN، سایر کاربران در یک هات‌اسپات باز می‌توانند ببینند دستگاه شما با کدام سایت‌ها و سرورها ارتباط می‌گیرد.

منابع و مراجع فنی

راهنمای مطالعه و پازل‌های تعاملی از استانداردهای جهانی NIST، OWASP و انطباق با حریم خصوصی داده گردآوری شده‌اند.

منابع علمی و صنعتی

[1] Wi-Fi Alliance. (n.d.). Security.
https://www.wi-fi.org/discover-wi-fi/security

[2] Federal Trade Commission. (2023). Are Public Wi-Fi Networks Safe? What You Need To Know.
https://consumer.ftc.gov/articles/are-public-wi-fi-networks-safe-what-you-need-know

[3] MDN Web Docs. (n.d.). Strict-Transport-Security header.
https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/Strict-Transport-Security

[4] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.
https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

[5] CISA. (n.d.). Malware, Phishing, and Ransomware.
https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

کلید پاسخ: ایستگاه بررسی 1 – چندگزینه‌ای

1 پرسش 1

پاسخ درست: A

نکتهٔ آموزشی

حملهٔ مرد میانی (MitM) چیست؟ → رهگیری و تغییر ارتباطات میان دو طرف در یک شبکهٔ مشترک

2 پرسش 2

پاسخ درست: A

نکتهٔ آموزشی

نقطهٔ دسترسی جعلی (Evil Twin) چیست؟ → هات‌اسپات Wi-Fi مخربی که با همان SSID یک شبکهٔ قانونی پیکربندی شده است

3 پرسش 3

پاسخ درست: A

نکتهٔ آموزشی

VPN چگونه از ترافیک Wi-Fi عمومی محافظت می‌کند؟ → همهٔ بسته‌های شبکه را در تونل رمزگذاری‌شده می‌پیچد و آن‌ها را برای sniffer ناخوانا می‌کند

4 پرسش 4

پاسخ درست: A

نکتهٔ آموزشی

شنود بسته (packet sniffing) چیست؟ → استفاده از ابزارهای سخت‌افزاری یا نرم‌افزاری برای ضبط و ثبت بسته‌های شبکه

5 پرسش 5

پاسخ درست: A

نکتهٔ آموزشی

نقش HTTPS چیست؟ → رمزگذاری ترافیک نشست میان مرورگر و سرور وب

کلید پاسخ: ایستگاه بررسی 2 – درست یا نادرست

6 پرسش 6

پاسخ درست: درست

نکتهٔ آموزشی

کاربران متصل می‌توانند به‌آسانی داده‌های متنی ساده را در شبکه‌های Wi-Fi عمومی باز ضبط کنند.

7 پرسش 7

پاسخ درست: نادرست

نکتهٔ آموزشی

نادرست: Evil Twin یک هات‌اسپات غیرمجاز است که مهاجم برای تقلید از یک هات‌اسپات واقعی راه می‌اندازد.

8 پرسش 8

پاسخ درست: نادرست

نکتهٔ آموزشی

نادرست: VPN ترافیک را در یک تونل رمزگذاری می‌کند، بنابراین اسنیفرهای محلی نمی‌توانند آن را بخوانند.

9 پرسش 9

پاسخ درست: نادرست

نکتهٔ آموزشی

نادرست: HTTPS کل تبادل HTTP، از جمله مسیر URL و محتوای صفحه، را رمزگذاری می‌کند.

10 پرسش 10

پاسخ درست: درست

نکتهٔ آموزشی

هات‌اسپات‌های وای‌فای با امنیت WPA3 حفاظت قوی‌تری نسبت به شبکه‌های باز و بدون گذرواژه ارائه می‌دهند.

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

E 1. شنود	F 2. شنود	D 3. دوقلوی شیطانی	H 4. HTTPS
G 5. VPN	B 6. تونل	A 7. WPA3	C 8. دیوار آتش

ایستگاه بررسی 3: کلید پاسخ – اصطلاحات کلیدی

1 شنود	2 اسنیفینگ	3 دوقلوی شیطانی	4 HTTPS
5 VPN	6 تونل		

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

1 G – استاندارد	2 C – دوقلو	3 B – اسنیفینگ	4 F – تونل
5 H – دیواراتش	6 A – شنود	7 E – وی‌پیان	8 D – اتصالامن

یادداشت‌های بحث برای مدرسان

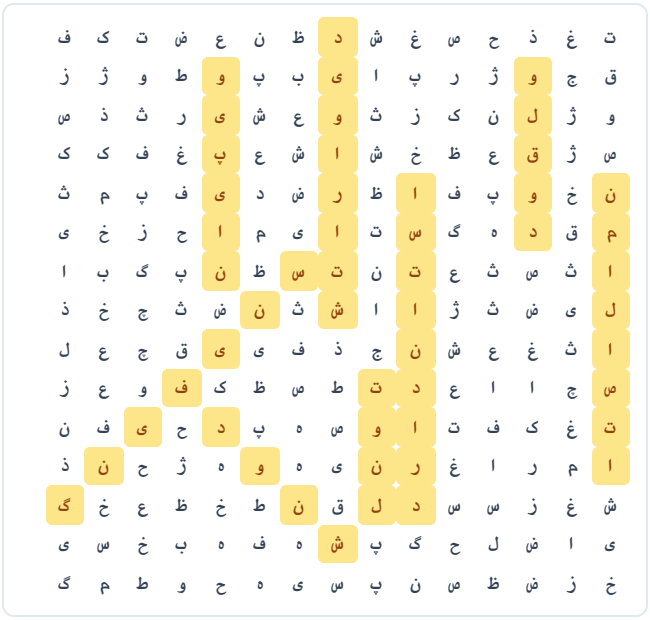
اصطلاحات کلیدی:
بررسی کنید که دانش‌آموزان بتوانند شنود، شنود و دوقلوی شیطانی را با کلمات خودشان توضیح دهند و برای هر کدام مثالی بزنند.

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

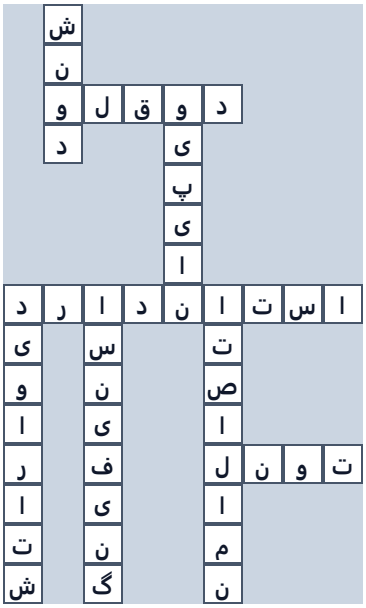
ارزیابی منابع:
از دانش‌آموزان بخواهید دست‌کم یک ادعا را در منابع کاربرگ بررسی کنند و دربارهٔ اینکه چرا ارقام، قیمت‌ها و قوانین ممکن است با گذشت زمان تغییر کنند گفت‌وگو کنید.

کلیدهای معما و یادداشت‌های معلم

پاسخ جدول کلمات



پاسخ جدول‌کلمات



راهنمای معلم برای پاسخ‌های جدول کلمات متقاطع

افقی

2 افقی: دوقلو هات‌اسپات جعلی که وای‌فای را تقلید می‌کند. (5 حرف)

4 افقی: استاندارد معیار نوین امنیت وای‌فای. (9 حرف)

8 افقی: تونل مسیر امن داده در حال انتقال. (4 حرف)

عمودی

1 عمودی: شنود خواندن ترافیک در حال انتقال. (4 حرف)

3 عمودی: ویپیان شبکهٔ خصوصی مجازی رمزگذاری‌شده. (6 حرف)

5 عمودی: اتصالامن انتقال امن وب. (8 حرف)

6 عمودی: اسنیفینگ ضبط بسته‌های داده شبکه. (8 حرف)

7 عمودی: دیواراتش فیلتر کردن ترافیک ورودی. (8 حرف)

کلید پاسخ کلمات درهم‌ریخته و رمزگشایی

کلید نمره‌دهی برای فعالیت بازچینی واژگان و چالش رمز مخفی.

کلید مرتب‌سازی کلمات

1. وشدن — شنود
2. دولقو — دوقلو
3. وپینای — وپیپان
4. ندرااداست — استاندارد
5. فیسگیانن — اسنیفینگ
6. منااالتص — اتصالامن
7. نتلو — تونل
8. ایرشدتاو — دیواراتش

کلید چالش رمز مخفی

"رمزگذاری ترافیک وایفای عمومی با وپیپان"

کلید پاسخ مطالعات موردی

A مطالعهٔ موردی 1: مهار شنود بسته‌ها در Wi-Fi عمومی

پاسخ معلم

راهنمای نمره‌دهی

پاسخ‌های دانش‌آموز باید نکات زیر را پوشش دهد:

- تحلیل سناریو: یک مدیر فروش راه‌دور که به Wi-Fi عمومی فرودگاه متصل است متوجه می‌شود چند ایمیل حساس کاری مدت کوتاهی پس از ارسال به‌صورت متن ساده افشا شده‌اند.
- راهبرد و راه‌حل پیشنهادی: استفاده از کلاینت VPN سازمانی را روی همهٔ ایستگاه‌های کاری راه‌دور الزامی کنید. افزونه‌های مرورگر فقط-HTTPS را اعمال کنید و پروتکل‌های رمزگذاری‌نشده (مانند HTTP و FTP) را در دیوار آتش کلاینت مسدود کنید.

B مطالعهٔ موردی 2: دفاع در برابر هات‌اسپات جعلی دوقلوی شرور

پاسخ معلم

راهنمای نمره‌دهی

پاسخ‌های دانش‌آموز باید نکات زیر را پوشش دهد:

- تحلیل سناریو: مهاجمان یک نقطهٔ دسترسی بی‌سیم جعلی با نام 'CoffeeShop_Guest' راه‌اندازی می‌کنند که از یک نقطهٔ دسترسی معتبر کافه تقلید می‌کند و ترافیک شبکهٔ مهمانان بی‌خبر را ضبط می‌کند.
- راهبرد و راه‌حل توصیه‌شده: آدرس‌های MAC مربوط به BSSID نقاط دسترسی را ممیزی کنید تا اصالت شبکه تأیید شود. اعتبارسنجی وضعیت کلاینت را برای مسدود کردن اتصال به شبکه‌های باز اعمال کنید و برای کار حساس هات‌اسپات‌های سلولی را الزامی کنید.