نام: _____ تاریخ: _____ نمره: _____

وب تاریک در برابر وب عمیق: امنیت و تفاوت‌ها

نمایه‌سازی موتور جست‌وجو، پایگاه‌های داده وب عمیق، مسیریابی پیازی Tor، گمنامی شبکه و خطرات

مرور آموزشی وب تاریک در برابر وب عمیق

خوش آمدید! این بستهٔ فعالیت شما را در شناخت تفاوت‌های وب عمیق و وب تاریک راهنمایی می‌کند. با پایگاه‌های دادهٔ نمایه‌نشده، مسیریابی پیازی (Onion Routing) در مرورگر Tor، دامنه‌های رمزنگاشتی .onion و خطرهای امنیتی ناشناس‌ماندن 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/dark-web-vs-deep-web/

نقشهٔ راه یادگیری راهبرد وب عمیق و تاریک شما

- وب عمیق (پایگاه‌های داده نمایه‌نشده) را با وب تاریک (سرویس‌های onion) مقایسه کنید.
- درک کنید مسیریابی پیازی ترافیک شبکه را چگونه رمزگذاری و بازپخش می‌کند.
- خطرهای امنیتی دسترسی به سایت‌های تأییدنشدهٔ شبکهٔ Tor را ارزیابی کنید.
- سیاست‌های دروازهٔ امن و جعبه‌شنی را برای خزش اطلاعات تهدید مستقر کنید.
- قالب نشانی رمزنگاری‌شدهٔ دامنه‌های سرویس onion را تحلیل کنید.

دستورالعمل‌های راهنمای وب عمیق و وب تاریک

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 حریم خصوصی در وب عمیق و وب تاریک به کار ببرید. و در پایان، فعالیت تکمیلی «سریع فکر کن».

پایگاه‌های داده وب عمیق در برابر مسیریابی پیازی وب تاریک (مقدمه)

وب عمیق شامل صفحات فهرست‌نشده پشت گذرواژه و ورود است، مانند ایمیل‌های خصوصی یا درگاه‌های بانکی سازمانی. وب تاریک زیرمجموعه‌ای از وب عمیق است که عمداً پنهان شده و برای دسترسی گمنام به مرورگرهای تخصصی (مانند Tor) و شبکه‌های onion نیاز دارد.

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

ایستگاه بررسی 1: چالش چندگزینه‌ای

1. وب عمیق چه تفاوتی با وب سطحی دارد؟

- A. صفحات وب عمیق توسط موتورهای جستجوی عمومی نمایه نمی‌شوند
- B. ترافیک وب عمیق غیرقانونی است و مجریان قانون آن را پایش می‌کنند
- C. دسترسی به وب‌سایت‌های وب عمیق به مرورگرهای تخصصی مانند Tor نیاز دارد
- D. صفحه‌های وب عمیق همیشه سریع‌تر از صفحه‌های وب سطحی بارگذاری می‌شوند

2. به دارک وب چگونه دسترسی پیدا می‌شود؟

- A. از طریق مرورگرهای تخصصی که از شبکه‌های مسیریابی پیازی استفاده می‌کنند
- B. با پیکربندی تنظیمات DNS سفارشی روی مسیریاب‌های استاندارد
- C. از طریق کنسول‌های جست‌وجوی وب سطحی خصوصی و فقط با دعوت‌نامه
- D. با نصب یک افزونهٔ مرورگر استاندارد مسدودکنندهٔ تبلیغات

3. کدام ساختار بزرگ‌ترین بخش وب عمیق را تشکیل می‌دهد؟

- A. پایگاه‌های داده کاربری و حساب‌های خصوصی محافظت‌شده با گذرواژه
- B. تالارهای گفتگوی غیرقانونی بازار سیاه که کالاهای غیرمجاز معامله می‌کنند
- C. پروتکل‌های رمزنگاری‌نشدهٔ اشتراک فایل همتابه‌همتا
- D. پایگاه‌های داده حافظهٔ پنهان موتورهای جست‌وجوی عمومی

4. مسیریابی پیازی با ترافیک شبکه چه می‌کند؟

- A. بسته‌ها را رمزگذاری می‌کند و از طریق چند رله مسیریابی می‌کند
- B. با دور زدن گره‌های ISP سرعت دانلود را افزایش می‌دهد
- C. شماره‌های سریال سخت‌افزار دستگاه را به رکوردهای IP نگاشت می‌کند
- D. کوکی‌های مرورگر وب را پس از هر کلیک حذف می‌کند

5. کدام پسوند دامنه منحصراً در شبکه‌های Tor استفاده می‌شود؟

- A. پسوند سطح بالای رمزنگاری‌شدهٔ .onion
- B. پسوند تجاری قدیمی و استاندارد .com
- C. پسوند غیرمتمرکز .eth مبتنی بر بلاکچین Web3
- D. پسوند فناوری کد کشور .ai

ایستگاه بررسی 2: چالش درست یا نادرست

6 **پرسش درست/نادرست 6**

6. وب عمیق و وب تاریک به یک بخش از شبکه اشاره دارند.

درست نادرست

7 **پرسش درست/نادرست 7**

7. درگاه‌های اینترانت شرکتی بخشی از وب عمیق هستند.

درست نادرست

8 **پرسش درست/نادرست 8**

8. مسیریابی پیازی بسته‌های داده را در هر گره عبوری به‌طور کامل رمزگشایی می‌کند.

درست نادرست

9 **پرسش درست/نادرست 9**

9. دسترسی به وب تاریک دستگاه‌ها را در معرض ریسک بالای بدافزار قرار می‌دهد.

درست نادرست

10 **پرسش درست/نادرست 10**

10. موتورهای جست‌وجوی وب استاندارد سایت‌های onion را می‌خزند و نمایه‌سازی می‌کنند.

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. پورتال‌های خصوصی بانکی در بخش نمایه‌نشدهٔ _____ قرار دارند.
2. گره‌های تخصصی Tor سرویس‌های پنهان _____ را میزبانی می‌کنند.
3. وب‌سایت‌های Tor از پسوند سطح بالای رمزنگاشتی _____ استفاده می‌کنند.
4. مسیردهی چندلایهٔ رمزگذاری‌شدهٔ ترافیک _____ نامیده می‌شود.
5. موتورهای جست‌وجوی سطح وب صفحاتی را می‌خزند که به‌طور عمومی _____ هستند.
6. شبکه‌های پیازی آی‌پی کلاینت را رمزگذاری می‌کنند تا _____ کاربر حفظ شود.

بانک واژگان

onion. پایگاه داده گره ورودی گمنامی مسیریابی پیازی نمایه‌شده وب تاریک وب عمیق

پاسخ‌های خود را اینجا بنویسید:

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

ایستگاه بررسی 4: تطبیق مفاهیم امنیت

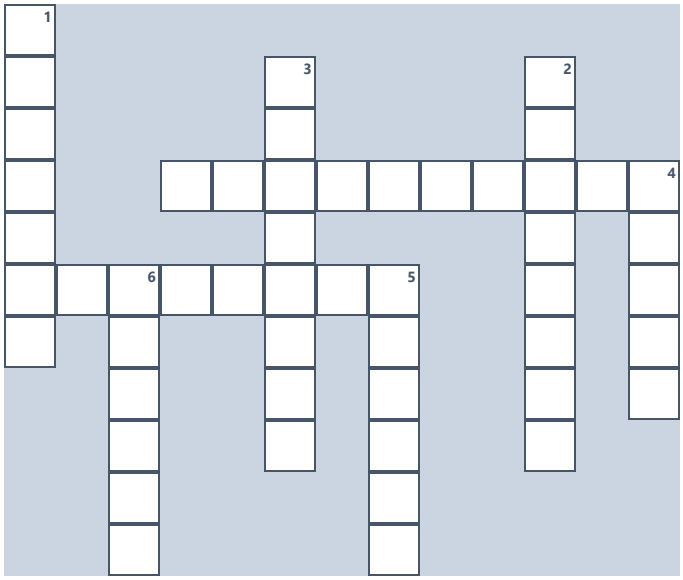
تطبیق تعاریف

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. بخش وب عمیق	A	بخش شبکهٔ رمزگذاری‌شده که فقط از طریق مرورگرهای ویژه در دسترس است.
2. پورتال وب تاریک	B	رمزگذاری داده به‌صورت لایه‌ای و ارسال آن از طریق سه گره.
3. پسوند Onion	C	فضای ذخیره‌سازی امن پشت‌صحنه که سوابق سیستمی نمایه‌نشده را نگه می‌دارد.
4. مسیریابی Tor	D	پسوند دامنهٔ سطح بالا با ماهیت رمزنگاری که در شبکه‌های Tor استفاده می‌شود.
5. صفحات ایندکس‌شده	E	گرهٔ نقطهٔ ورود که برای دسترسی به شبکهٔ Tor استفاده می‌شود.
6. ناشناسی کاربر	F	محتوای وب سطحی که فهرست‌شده و در Google قابل جست‌وجوست.
7. پایگاه داده خصوصی	G	پنهان نگه داشتن آدرس‌های IP عمومی کلاینت از سرورها.
8. دروازهٔ ورودی	H	محتوای وب فهرست‌نشده مانند ورودهای خصوصی، ایمیل‌ها و رکوردهای پایگاه داده.

ایستگاه بررسی 5: جدول‌کلمات

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



افقی

4. ذخیره‌سازی امن پشتیبان که رکوردهای نمایه‌نشدهٔ سیستم را نگه می‌دارد (10)

5. گره نقطهٔ ورود که برای دسترسی به شبکهٔ Tor به کار می‌رود (8)

عمودی

1. بخش شبکهٔ رمزگذاری‌شده که فقط با مرورگرهای ویژه در دسترس است (7)

2. رمزگذاری داده در لایه‌ها و بازپخش آن از طریق سه گره (8)

3. محتوای وب سطحی که در گوگل گردآوری شده و قابل جست‌وجو است (8)

4. پسوند دامنهٔ سطح بالای رمزنگاشتی که در شبکه‌های Tor به کار می‌رود (5)

5. پنهان نگه داشتن آی‌پی عمومی کلاینت از سرورها (6)

6. محتوای وب نمایه‌نشده مانند ورودهای خصوصی، ایمیل‌ها و رکوردهای پایگاه داده (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

4 افقی: ذخیره‌سازی امن پشتیبان که رکوردهای نمایه‌نشدهٔ سیستم را نگه می‌دارد (10 حرف):

5 افقی: گره نقطهٔ ورود که برای دسترسی به شبکهٔ Tor به کار می‌رود (8 حرف):

عمودی

1 عمودی: بخش شبکهٔ رمزگذاری‌شده که فقط با مرورگرهای ویژه در دسترس است (7 حرف):

2 عمودی: رمزگذاری داده در لایه‌ها و بازپخش آن از طریق سه گره (8 حرف):

3 عمودی: محتوای وب سطحی که در گوگل گردآوری شده و قابل جست‌وجو است (8 حرف):

4 عمودی: پسوند دامنهٔ سطح بالای رمزنگاشتی که در شبکه‌های Tor به کار می‌رود (5 حرف):

5 عمودی: پنهان نگه داشتن آی‌پی عمومی کلاینت از سرورها (6 حرف):

6 عمودی: محتوای وب نمایه‌نشده مانند ورودهای خصوصی، ایمیل‌ها و رکوردهای پایگاه داده (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.

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

فهرست واژگان

وبعمیق وبتاریک پیازی مسیریابی نمایهشده گمنامی پایگاهداده گرهورودی

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. وبعمیق
B. وبتاریک
C. پیازی
D. مسیریابی
E. نمایهشده
F. گمنامی
G. پایگاهداده
H. گرهورودی

	تعاریف و فیلدهای تطبیق
	1. پنهان نگه داشتن آی‌پی عمومی کلاینت از سرورها.
	2. ذخیره‌سازی امن پشتیبان که رکوردهای نمایه‌نشدهٔ سیستم را نگه می‌دارد.
	3. رمزگذاری داده در لایه‌ها و بازپخش آن از طریق سه گره.
	4. محتوای وب نمایه‌نشده مانند ورودهای خصوصی، ایمیل‌ها و رکوردهای پایگاه داده.
	5. بخش شبکهٔ رمزگذاری‌شده که فقط با مرورگرهای ویژه در دسترس است.
	6. پسوند دامنهٔ سطح بالای رمزنگاشتی که در شبکه‌های Tor به کار می‌رود.
	7. گره نقطهٔ ورود که برای دسترسی به شبکهٔ Tor به کار می‌رود.
	8. محتوای وب سطحی که در گوگل گردآوری شده و قابل جست‌وجو است.

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. ع و م ی ق ب
2. پ ی ز ا ی
3. ی م ن ه ش ه د ا
4. ه د ا ه گ ا د پ ا ی
5. ر ک ا ت و ی ب
6. ب ی ر ا م ی س ی
7. م گ ا ی ن م
8. و ر ر ی گ د و ه

فعالیت تکمیلی: سریع فکر کن

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

1	دلایل دوری از وب تاریک		
2	چیزهایی که موتور جست‌وجو نمی‌تواند پیدا کند		
3	دستگاه‌هایی که می‌توانند هک شوند		
4	دلایل قانونی استفاده از Tor		
5	دلایل به‌روزرسانی نرم‌افزار		
6	نشانه‌های هشدار در یک ایمیل		
7	چیزهایی که به‌طور غیرقانونی در وب تاریک فروخته می‌شوند		
8	افرادی که می‌توانید برای کمک فناوری اطلاعات از آن‌ها بپرسید		
9	عادت‌های ایمن که می‌توانید از امروز شروع کنید		
10	کارهایی که پس از نشت داده باید انجام داد		
11	چیزهایی که به وب عمیق تعلق دارند		
12	سایت‌هایی که با ورود به حساب استفاده می‌کنید		
13	واژه‌های مرتبط با گمنامی		
14	اطلاعاتی که هرگز نباید به اشتراک بگذارید		
15	چیزهایی که «زیر سطح» قرار دارند		

ایستگاه بررسی 8: مطالعات موردی امنیت سایبری

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

مطالعهٔ موردی 1: شناسایی نشت داده



سناریو: یک ممیزی امنیتی شرکتی کشف می‌کند رکوردهای حساس پایگاه دادهٔ مشتریان در یک بازار onion معامله می‌شوند. این داده در Google نمایه نشده است.

پرسش برای بحث: توضیح دهید کدام بخش‌های وب درگیر هستند و این نشت چگونه رخ داد.

مطالعهٔ موردی 2: ناشناسی در برابر خطرهای بدافزار



سناریو: یک تحلیلگر می‌خواهد فیدهای اطلاعات تهدید را در یک وب‌سایت Tor بررسی کند. او مرورگر Tor را دانلود می‌کند و به سایت دسترسی پیدا می‌کند.

پرسش برای بحث: مزایای گمنامی را ارزیابی کنید و مراحل کاهش خطر بدافزار 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

1	2	12	2	12	1	25	32	28	1	29	28	26	
32	13	1	32	3	32	2	1	32	12	32	15	28	

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: وب عمیق چیست؟

وب عمیق شامل همهٔ صفحات وبی است که موتورهای جست‌وجو نمی‌توانند فهرست‌بندی کنند، از جمله بانکداری آنلاین، پایگاه‌های داده ایمیل و مجلات پولی.

Q2: وب تاریک چیست؟

وب تاریک زیرمجموعه‌ای کوچک از وب عمیق است که عمداً پنهان شده و فقط از طریق مرورگرهای تخصصی با شبکه‌های onion در دسترس است.

Q3: موتورهای جست‌وجو چگونه صفحه‌ها را ایندکس می‌کنند؟

موتورها برنامه‌های خودکار (عنکبوت‌ها) را اجرا می‌کنند تا پیوندهای عمومی را دنبال کنند و صفحه‌هایی را که خزش را از طریق دستورهای ربات مسدود نکرده‌اند نمایه کنند.

Q4: چرا بانکداری آنلاین بخشی از وب عمیق به شمار می‌رود؟

پورتال‌های بانکی پشت صفحه‌های ورود و گذرواژه قرار دارند و موتورهای جست‌وجوی عمومی را از نمایه‌سازی صفحه‌های صورت‌حساب حساب بازمی‌دارند.

Q5: مسیریابی پیازی (Onion Routing) در مرورگر Tor چیست؟

مسیریابی پیازی روشی برای انتقال است که ترافیک را به‌صورت لایه‌ای رمزگذاری می‌کند و از چند رله عبور می‌دهد تا نشانی‌های IP کاربر پنهان شود.

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

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

Q6: آیا دسترسی به دارک‌وب غیرقانونی است؟

خیر. دسترسی به دارک‌وب در بیشتر کشورها قانونی است، هرچند مشارکت در بازارهای غیرقانونی یا فعالیت‌های سایبری ممنوع است.

Q7: چرا سایت‌های دارک‌وب کند بارگذاری می‌شوند؟

ترافیک از دست‌کم سه رلهٔ جهانی (ورودی، میانی، خروجی) مسیریابی و رمزگشایی می‌شود که تأخیر انتقال را افزایش می‌دهد.

Q8: پسوند دامنهٔ .onion به چه معناست؟

پسوند دامنهٔ سطح بالای تخصصی است که در شبکه‌های Tor استفاده می‌شود و به‌جای سرورهای DNS استاندارد، به آدرس‌های تولیدشده با رمزنگاری اشاره می‌کند.

Q9: لینک‌های دارک‌وب چه خطراتی دارند؟

این سایت‌ها هیچ غربالگری امنیتی ندارند و کاربران را در معرض نرخ‌های بالای آلودگی به بدافزار، اسکریپت‌های فیشینگ و کلاهبرداری‌های تراکنشی قرار می‌دهند.

Q10: چه کسی پروتکل مسیریابی شبکهٔ Tor را ساخت؟

این فناوری ابتدا در دههٔ 1990 توسط آزمایشگاه پژوهشی نیروی دریایی ایالات متحده برای محافظت از ارتباطات دولتی توسعه یافت.

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

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

Q1: گره‌های میانی چگونه از ناشناسی در Tor محافظت می‌کنند؟

هر گره فقط یک لایه از داده‌های مسیریابی را رمزگشایی می‌کند و فقط جهش قبلی و جهش بعدی را می‌شناسد، نه هرگز هم مبدأ و هم مقصد را.

Q2: نقش گرهٔ خروجی چیست؟

گرهٔ خروجی آخرین لایهٔ رمزگذاری را رمزگشایی می‌کند و ترافیک را به سرور مقصد عمومی یا سرور onion می‌فرستد.

Q3: دروازهٔ پل‌های Tor چیست؟

پل‌ها رله‌های ورودی Tor فهرست‌نشده‌ای هستند که برای دور زدن مسدودسازی‌های ISP و سانسور در مناطقی که دسترسی به مرورگر Tor را محدود می‌کنند، به کار می‌روند.

Q4: بازیگران دارک‌وب چگونه از رمزارز سوءاستفاده می‌کنند؟

عاملان از ارزهای دیجیتال ناشناس برای انجام معاملات مالی در بازارهای تاریک استفاده می‌کنند و بررسی‌های استاندارد تراکنش بانکی را دور می‌زنند.

Q5: چرا موتورهای جست‌وجوی استاندارد نمی‌توانند پایگاه‌های داده عمیق را بخزند؟

خزنده‌ها نمی‌توانند اعتبارنامه‌های ورود را وارد کنند، CAPTCHAهای امنیتی را حل کنند یا اسکریپت‌های پرس‌وجوی SQL سمت سرور لازم برای دسترسی به پایگاه‌های داده عمیق را اجرا کنند.

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

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

Q6: سرور دایرکتوری در شبکه‌های Tor چیست؟

سروری مورد اعتماد است که فهرست رله‌های ورودی، میانی و خروجی فعال را که کلاینت‌ها برای ساخت مسیرهای مسیریابی استفاده می‌کنند نگه می‌دارد.

Q7: بازیگران مخرب چگونه شنود گرهٔ خروجی را انجام می‌دهند؟

اپراتورهای مخرب گره خروجی می‌توانند ترافیک HTTP رمزگذاری‌نشده را هنگام خروج از شبکهٔ Tor شنود کنند و نام‌های کاربری و کوکی‌ها را بدزدند.

Q8: تفاوت Tor و I2P چیست؟

Tor از فهرست رلهٔ متمرکز و گره‌های خروجی برای دسترسی به وب عمومی استفاده می‌کند، در حالی که I2P برای میزبانی داخلی ساختار همتابه‌همتای غیرمتمرکز دارد.

Q9: نهادهای مجری قانون چگونه بازارهای دارک‌وب را ردیابی می‌کنند؟

نهادها از تحلیل بلاکچین استفاده می‌کنند، محل استقرار فیزیکی سرور را ردیابی می‌کنند و عملیات طعمه اجرا می‌کنند تا اپراتورها را شناسایی کنند.

Q10: نشت DNS چگونه ناشناسی کلاینت را به خطر می‌اندازد؟

نشت DNS زمانی رخ می‌دهد که پرس‌وجوهای DNS مرورگر به‌جای مسیریابی از طریق شبکهٔ رمزگذاری‌شدهٔ Tor، مستقیماً از طریق ISP محلی ارسال شوند.

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

وب عمیق بسیار بزرگ‌تر از وب سطحی قابل جست‌وجوست، چون بیشتر محتوا پشت ورود و پایگاه‌های داده قرار دارد.

2. بینش امنیت

وب تاریک بخش کوچک و عمداً پنهان وب عمیق است که با ابزارهایی مانند Tor به آن دسترسی پیدا می‌شود.

3. بینش امنیت

مسیریابی Tor بسته‌های داده را سه بار رمزگذاری می‌کند و در هر گرهٔ رله مانند پیاز یک لایهٔ رمزگذاری را کنار می‌زند.

4. بینش امنیت

Tor از پروژهٔ مسیریابی پیازی که آزمایشگاه پژوهشی نیروی دریایی ایالات متحده اجرا می‌کرد پدید آمد و کد آن به‌صورت نرم‌افزار آزاد منتشر شد. [1]

5. بینش امنیت

نشانی‌های Onion رشته‌های الفبایی-عددی 56 نویسه‌ای هستند که به‌صورت رمزنگاری از جفت‌کلیدهای عمومی تولید می‌شوند.

6. بینش امنیت

گره‌های خروجی می‌توانند ترافیک متن ساده را بخوانند، یعنی برای داده‌های نشست امن در Tor همچنان TLS/HTTPS لازم است.

7. بینش امنیت

سایت‌های اینترانت، درایوهای ابری و پایگاه‌های داده خصوصی بزرگ‌ترین بخش‌های ذخیره‌سازی داده در وب عمیق را تشکیل می‌دهند.

8. بینش امنیت

موتورهای جست‌وجوی تخصصی مانند DuckDuckGo پورتال‌های onion اجرا می‌کنند تا جست‌وجوی ناشناس در شبکه‌های Tor ممکن شود.

9. بینش امنیت

بیش از 2 میلیون کاربر روزانه برای دور زدن سانسور و حفظ حریم خصوصی ارتباطات به شبکهٔ Tor متصل می‌شوند.

10. بینش امنیت

عملیات‌های جهانی مجری قانون (مانند Operation Bayonet) با توقیف سخت‌افزار میزبانی، بازارهای تاریک بزرگ را تعطیل کردند.

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] Tor Project. (n.d.). Why is it called Tor?
https://support.torproject.org/about/why-is-it-called-tor/

[2] Tor Project. (n.d.). How do Onion Services work?
https://community.torproject.org/onion-services/overview/

[3] Tor Project. (n.d.). Users – Tor Metrics.
https://metrics.torproject.org/userstats-relay-country.html

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

[5] 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

کلید پاسخ: ایستگاه بررسی 1 – چندگزینه‌ای

1 نمایه‌سازی جست‌وجو — وب عمیق — پاسخ درست: A

نکتهٔ آموزشی

صفحه‌های وب عمیق پشت دیوارهای ورود و پایگاه‌های داده قرار دارند و مانع از خزش عنکبوت‌های جست‌وجو در آن‌ها می‌شوند. منبع: IETF RFC 3986.

2 دسترسی به Tor — وب تاریک — پاسخ درست: A

نکتهٔ آموزشی

وب تاریک از سرویس‌های onion پنهانی تشکیل شده که فقط از طریق مرورگرهایی مانند Tor در دسترس‌اند. منبع: IETF RFC 3986.

3 پایگاه‌های داده عمیق — پایگاه‌های داده — پاسخ درست: A

نکتهٔ آموزشی

حساب‌های دارای گذرواژه و سوابق شرکتی بزرگ‌ترین بخش وب عمیق را تشکیل می‌دهند. منبع: NIST Digital Identity.

4 مسیریابی پیازی — شبکهٔ Tor — پاسخ درست: A

نکتهٔ آموزشی

مسیریابی پیازی بسته‌های داده را به‌صورت لایه‌ای رمزگذاری می‌کند و برای ناشناسی آن‌ها را از چند گره عبور می‌دهد. منبع: IETF RFC 3986.

5 دامنهٔ Onion — پسوند — پاسخ درست: A

نکتهٔ آموزشی

پسوند دامنهٔ رمزنگاری‌شدهٔ.onion ترافیک را درون Tor و بدون DNS عمومی مسیریابی می‌کند. منبع: IETF RFC 3986.

کلید پاسخ: ایستگاه بررسی 2 – درست یا نادرست

6 بخش‌های وب — ساختار — پاسخ درست: نادرست

نکتهٔ آموزشی

وب عمیق همهٔ صفحات فهرست‌نشده را دربر می‌گیرد، در حالی که وب تاریک زیربخش کوچک و رمزگذاری‌شدهٔ onion است. منبع: IETF RFC 3986.

7 اینترانت‌های شرکتی — وب عمیق — پاسخ درست: درست

نکتهٔ آموزشی

سایت‌های اینترانت پشت درگاه‌های گذرواژه‌دار قرار دارند و نمایه نمی‌شوند، یعنی جزو وب عمیق هستند. منبع: NIST Digital Identity.

8 رمزگذاری لایه‌ای — رله‌ها — پاسخ درست: نادرست

نکتهٔ آموزشی

رله‌های Onion برای حفظ ناشناسی کاربر فقط یک لایهٔ مسیریابی را رمزگشایی می‌کنند، نه کل بسته را. منبع: IETF RFC 3986.

9 مواجهه با بدافزار — تهدیدها — پاسخ درست: درست

نکتهٔ آموزشی

بازارهای وب تاریک هیچ فیلتر امنیتی ندارند و خطر شدید آلودگی به بدافزار را به همراه دارند. منبع: Center for Internet Security (CIS).

10 پرسش 10 — پاسخ درست: نادرست

نکتهٔ آموزشی

خزندگان موتورهای جست‌وجوی معمولی از Tor استفاده نمی‌کنند، بنابراین نمی‌توانند به سایت‌های .onion برسند یا آن‌ها را نمایه کنند.

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. بخش وب عمیق	A 2. پورتال وب تاریک	D 3. پسوند Onion	B 4. مسیریابی Tor
F 5. صفحات ایندکس‌شده	G 6. ناشناسی کاربر	C 7. پایگاه داده خصوصی	E 8. دروازهٔ ورودی

ایستگاه بررسی 3: کلید پاسخ – اصطلاحات کلیدی

1 وب عمیق	2 وب تاریک	3 .onion	4 مسیریابی پیازی
5 نمایه‌شده	6 گمنامی		

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

1 F – گمنامی	2 G – پایگاه‌داده	3 D – مسیریابی	4 A – وبعمیق
5 B – وبتاریک	6 C – پیازی	7 H – گرهورودی	8 E – نمایه‌شده

یادداشت‌های بحث برای مدرسان

اصطلاحات کلیدی:
بررسی کنید که دانش‌آموزان بتوانند بخش وب عمیق، پورتال وب تاریک و پسوند Onion 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.

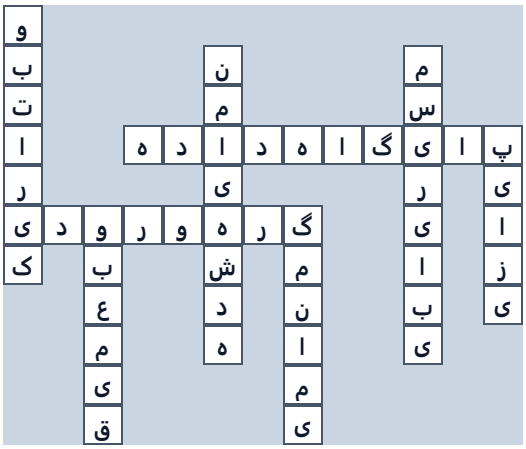
ارزیابی منابع:
از دانش‌آموزان بخواهید دست‌کم یک ادعا را در منابع کاربرگ بررسی کنند و دربارهٔ اینکه چرا ارقام، قیمت‌ها و قوانین ممکن است با گذشت زمان تغییر کنند گفت‌وگو کنید.

کلیدهای معما و یادداشت‌های معلم

پاسخ جدول کلمات

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

پاسخ جدول‌کلمات



راهنمای معلم برای پاسخ‌های جدول کلمات متقاطع

افقی

4 افقی: پایگاهداده ذخیره‌سازی امن پشتیبان که رکوردهای نمایه‌نشدهٔ سیستم را نگه می‌دارد (10 حرف)

5 افقی: گرهورودی گره نقطهٔ ورود که برای دسترسی به شبکهٔ Tor به کار می‌رود (8 حرف)

عمودی

1 عمودی: وبتاریک بخش شبکهٔ رمزگذاری‌شده که فقط با مرورگرهای ویژه در دسترس است (7 حرف)

2 عمودی: مسیریابی رمزگذاری داده در لایه‌ها و بازپخش آن از طریق سه گره (8 حرف)

3 عمودی: نمایهشده محتوای وب سطحی که در گوگل گردآوری شده و قابل جست‌وجو است (8 حرف)

4 عمودی: پیازی پسوند دامنهٔ سطح بالای رمزنگاشتی که در شبکه‌های Tor به کار می‌رود (5 حرف)

5 عمودی: گمنامی پنهان نگه داشتن آی‌پی عمومی کلاینت از سرورها (6 حرف)

6 عمودی: وبعمیق محتوای وب نمایه‌نشده مانند ورودهای خصوصی، ایمیل‌ها و رکوردهای پایگاه داده (6 حرف)

کلید پاسخ کلمات درهم‌ریخته و رمزگشایی

کلید نمره‌دهی برای فعالیت بازچینی واژگان و چالش رمز مخفی.

کلید مرتب‌سازی کلمات

1. عومیقب — وبعمیق
2. پیزای — پیازی
3. یمنهشهدا — نمایهشده
4. هداهگادپای — پایگاهداده
5. رکاتویب — وبتاریک
6. بیرامیسی — مسیریابی
7. مگاینم — گمنامی
8. وررِیگدوه — گرهورودی

کلید چالش رمز مخفی

"گمنامی کاربر با مسیریابی پیازی"

کلید پاسخ مطالعات موردی

A مطالعهٔ موردی 1: شناسایی نشت داده

پاسخ معلم

راهنمای نمره‌دهی

پاسخ‌های دانش‌آموز باید نکات زیر را پوشش دهد:

- تحلیل سناریو: یک ممیزی امنیتی سازمانی کشف می‌کند که رکوردهای حساس پایگاه داده مشتریان در یک بازار onion معامله می‌شوند. این داده‌ها در Google نمایه نشده‌اند.
- راهبرد و راه‌حل پیشنهادی: بخش‌های دخیل: پایگاه داده خصوصی به وب عمیق تعلق دارد (نمایه‌نشده اما امن). بازار معامله‌کنندهٔ داده‌های دزدیده‌شده در وب تاریک (شبکهٔ onion) است. چگونه رخ داد: هکرها دفاع‌های سرور را دور زدند، پایگاه داده را از وب عمیق دزدیدند و برای فرار از ردیابی نیروهای قانون آن را به‌صورت ناشناس در وب تاریک عرضه کردند.

B مطالعهٔ موردی 2: ناشناسی در برابر خطرهای بدافزار

پاسخ معلم

راهنمای نمره‌دهی

پاسخ‌های دانش‌آموز باید نکات زیر را پوشش دهد:

- تحلیل سناریو: یک تحلیلگر می‌خواهد خوراک‌های اطلاعات تهدید را در یک وب‌سایت Tor بررسی کند. او مرورگر Tor را دانلود می‌کند و به سایت دسترسی پیدا می‌کند.
- راهبرد و راه‌حل توصیه‌شده: مزایا: Tor ترافیک را از سه گره عبور می‌دهد و IP شرکتی تحلیل‌گر را پنهان می‌کند. ریسک‌ها و کاهش آن‌ها: پیوندهای دارک‌وب هیچ غربالگری اعتباری ندارند. تحلیل‌گران باید Tor را داخل ماشین‌های مجازی (VM) ایزوله اجرا کنند، جاوااسکریپت را در تنظیمات Tor غیرفعال کنند و برای حفاظت از شبکهٔ شرکتی از دانلود هر فایلی خودداری کنند.