نام: _____ تاریخ: _____ نمره: _____

تحلیل بدافزار و کاهش تهدید راهنما

تروجان‌ها، باج‌افزار، جاسوس‌افزار، روت‌کیت‌ها، جعبه‌شنی‌های مجازی‌سازی، مهار

مرور آموزشی تحلیل بدافزار

خوش آمدید! این بستهٔ فعالیت شما را در تحلیل و پیشگیری از بدافزار راهنمایی می‌کند. با جاسوس‌افزار، تروجان، بارهای باج‌افزار، ابزارهای مهندسی معکوس، رفتار روت‌کیت و راهبردهای مهار 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/malware/

نقشهٔ راه یادگیری کاهش خطر بدافزار شما

- میان انواع بدافزار تروجان، کرم و روت‌کیت تمایز قائل شوید.
- اجرای مجازی‌سازی سندباکس را برای تحلیل کد پیاده‌سازی کنید.
- برنامه‌های مهار و پاک‌سازی برای محموله‌های فعال باج‌افزار طراحی کنید.

دستورالعمل راهنمای تحلیل بدافزار

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 کاهش اثر بدافزار به کار ببرید. و در پایان، فعالیت تکمیلی «سریع فکر کن».

تحلیل بدافزار و مهار تهدید (مقدمه)

کدهای مخرب مانند تروجان‌ها، کرم‌ها و باج‌افزارها تهدیدهای پرتأثیری برای نقاط پایانی و سرورها هستند. تیم‌های امنیتی بدافزار را درون جعبه‌ماسه‌های مجازی تحلیل می‌کنند و کنترل‌های سریع جداسازی شبکه را برای مهار گسترش محموله اجرا می‌کنند.

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

ایستگاه بررسی 1: چالش چندگزینه‌ای

1 1. ویژگی تعیین‌کنندهٔ اسب تروا چیست؟

- A. خود را به‌جای نرم‌افزار قانونی جا می‌زند تا کاربران را فریب دهد که آن را اجرا کنند
- B. به‌طور خودکار در خطوط شبکهٔ محلی تکثیر می‌شود
- C. فایل‌های داخل جعبه‌شنی‌های مجازی ایزوله را آلوده می‌کند
- D. ترافیک ارائه‌دهندهٔ خدمات اینترنت را رهگیری می‌کند

2 2. کدام نوع بدافزار فایل‌ها را رمزگذاری می‌کند و درخواست پول می‌کند؟

- A. باج‌افزار
- B. جاسوس‌افزار
- C. روت‌کیت
- D. تبلیغ‌افزار

3 3. چه چیزی نمایندهٔ جاسوس‌افزار است؟

- A. بدافزاری که برای پایش پنهانی ضربه‌های کلید و فعالیت‌های مرورگر کاربر طراحی شده است
- B. کد برنامه‌ای که درون یک کانتینر مجازی جعبه‌شنی اجرا می‌شود
- C. به‌روزرسانی‌های ضدبدافزار که از رجیستری‌های پایگاه داده دانلود می‌شوند
- D. تنظیم خودکار روشنایی صفحه

4 4. چرا توسعه‌دهندگان بدافزار از روت‌کیت استفاده می‌کنند؟

- A. برای پنهان کردن فرایندهای فعال و فایل‌های مخرب از سیستم‌عامل
- B. افزایش سرعت پردازش CPU در نقاط پایانی
- C. برای تهیهٔ پشتیبان از فایل‌های پایگاه داده در گاوصندوق‌های ابری امن
- D. برای بهبود عمر باتری لپ‌تاپ‌ها

5 5. سندباکس در تحلیل بدافزار به چه معناست؟

- A. اجرای فایل‌های مشکوک در یک گاوصندوق مجازی ایزوله برای مشاهدهٔ ایمن رفتار
- B. اسکن هش فایل‌ها در برابر پایگاه‌های داده تهدیدهای شناخته‌شده
- C. بازیابی پشتیبان‌های پایگاه داده پس از نفوذ
- D. قطع روترهای شبکهٔ محلی از خطوط عمومی

ایستگاه بررسی 2: چالش درست یا نادرست

6 پرسش 6

6. کرم‌های رایانه‌ای برای انتشار در شبکه‌های محلی به تعامل کاربر انسانی نیاز دارند.

درست نادرست

7 پرسش 7

7. adware همیشه بی‌خطر است و رفتار کاربر یا سابقهٔ مرورگر را ردیابی نمی‌کند.

درست نادرست

8 پرسش 8

8. بازیابی پشتیبان‌های آفلاین سالم به قربانیان اجازه می‌دهد فایل‌های رمزگذاری‌شده را بدون پرداخت باج بازیابی کنند.

درست نادرست

9 پرسش 9

9. آنتی‌ویروس مبتنی بر امضا بدافزار روز صفر را پیش از آنکه امضایی برای آن وجود داشته باشد، به‌طور قابل اعتماد متوقف می‌کند.

درست نادرست

10 پرسش 10

10. بدافزار بدون فایل، اسکریپت‌های مخرب را در حافظهٔ سیستم اجرا می‌کند و از نوشتن فایل روی دیسک پرهیز 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. بدافزاری که به‌صورت یک برنامهٔ کاربردی ایمن پنهان شده، _____ است.
2. بارهای مخربی که سامانه‌های پایگاه داده را برای دریافت پول قفل می‌کنند، _____ هستند.
3. کی‌لاگرهایی که پنهانی گذرواژه‌ها را ضبط می‌کنند، نمونه‌ای از _____ هستند.
4. پنهان شدن در عمق هستهٔ سیستم‌عامل مستلزم یک _____ است.
5. تحلیل فایل‌های مشکوک در یک خزانهٔ ایزوله از یک _____ مجازی استفاده می‌کند.
6. متوقف کردن گسترش بارهای بدافزار فعال مستلزم _____ فوری شبکه است.

بانک واژگان

باج‌افزار | بدون فایل | تروجان | جاسوس‌افزار | روتکیت | سندباکس | کرم | مهار

پاسخ‌های خود را اینجا بنویسید:

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

ایستگاه بررسی 4: تطبیق مفاهیم امنیت

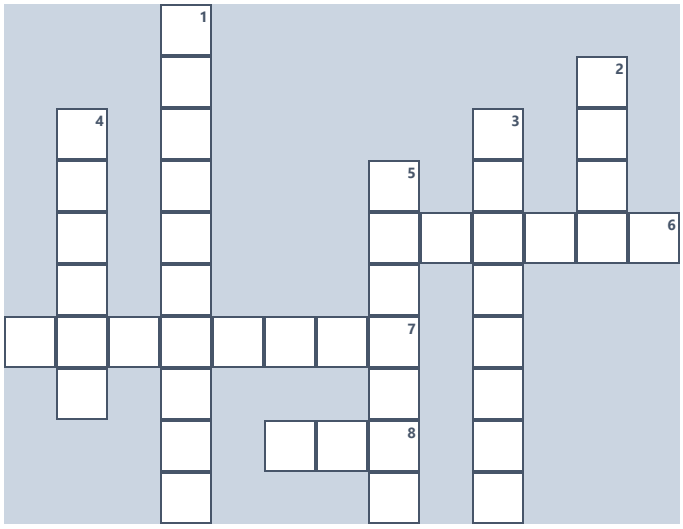
تطبیق تعاریف

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. تروجان	A	برنامه‌ای که برای نظارت و ثبت پنهانی فعالیت و ورودی‌های کاربر طراحی شده است.
2. باج‌افزار	B	بدافزاری که مستقیماً در RAM اجرا می‌شود تا از شناسایی توسط پویشگرهای دیسک جلوگیری کند.
3. جاسوس‌افزار	C	محدودکردن نقاط انتهایی آلوده برای جلوگیری از گسترش بارهای مخرب تهدید.
4. روت‌کیت	D	نرم‌افزار مخربی که به‌شکل یک برنامهٔ کمکیِ بی‌خطر یا مفید درآمده است.
5. سندباکس	E	بدافزار خودتکثیر که بدون اقدام انسانی در شبکه‌ها پخش می‌شود.
6. مهار	F	بدافزاری که حافظهٔ ذخیره‌سازی سیستم را رمزگذاری می‌کند و برای تحویل کلید پرداخت می‌خواهد.
7. کرم	G	محیط مجازی جداشده که برای تحلیل ایمن فایل‌های مخرب استفاده می‌شود.
8. بدون فایل	H	بدافزار پنهان‌کار که در عمق هستهٔ سیستم پنهان می‌شود تا کنترل مدیریتی را حفظ کند.

ایستگاه بررسی 5: جدول‌کلمات

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



افقی

6. نرم‌افزار مخرب که به شکل یک برنامهٔ کاربردی بی‌خطر یا مفید پنهان شده است. (6)

7. بدافزاری که مستقیم در RAM اجرا می‌شود تا از شناسایی توسط پویشگرهای دیسک بگریزد. (8)

8. بدافزار خودتکثیرشونده که بدون اقدام انسان در شبکه‌ها پخش می‌شود. (3)

عمودی

1. برنامه‌ای که برای نظارت و ثبت پنهانی فعالیت و ورودی‌های کاربر طراحی شده است. (10)

2. محدود کردن نقاط پایانی آلوده برای جلوگیری از گسترش بارهای تهدید. (4)

3. بدافزاری که حافظهٔ سیستم را رمزگذاری می‌کند و برای تحویل کلید پول می‌خواهد. (8)

4. بدافزار نهان‌کار که در عمق هستهٔ سیستم پنهان می‌شود تا کنترل مدیریتی را حفظ کند. (6)

5. محیط مجازی ایزوله که برای تحلیل ایمن فایل‌های مخرب به کار می‌رود. (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

6 افقی: نرم‌افزار مخرب که به شکل یک برنامهٔ کاربردی بی‌خطر یا مفید پنهان شده است. (6 حرف):

7 افقی: بدافزاری که مستقیم در RAM اجرا می‌شود تا از شناسایی توسط پویشگرهای دیسک بگریزد. (8 حرف):

8 افقی: بدافزار خودتکثیرشونده که بدون اقدام انسان در شبکه‌ها پخش می‌شود. (3 حرف):

عمودی

1 عمودی: برنامه‌ای که برای نظارت و ثبت پنهانی فعالیت و ورودی‌های کاربر طراحی شده است. (10 حرف):

2 عمودی: محدود کردن نقاط پایانی آلوده برای جلوگیری از گسترش بارهای تهدید. (4 حرف):

3 عمودی: بدافزاری که حافظهٔ سیستم را رمزگذاری می‌کند و برای تحویل کلید پول می‌خواهد. (8 حرف):

4 عمودی: بدافزار نهان‌کار که در عمق هستهٔ سیستم پنهان می‌شود تا کنترل مدیریتی را حفظ کند. (6 حرف):

5 عمودی: محیط مجازی ایزوله که برای تحلیل ایمن فایل‌های مخرب به کار می‌رود. (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.

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

فهرست واژگان

تروجان باجافزار جاسوسافزار روتکیت سندباکس مهار کرم بدونفایل

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. تروجان
B. باجافزار
C. جاسوسافزار
D. روتکیت
E. سندباکس
F. مهار
G. کرم
H. بدونفایل

	تعاریف و فیلدهای تطبیق
	1. بدافزار نهان‌کار که در عمق هستهٔ سیستم پنهان می‌شود تا کنترل مدیریتی را حفظ کند.
	2. محدود کردن نقاط پایانی آلوده برای جلوگیری از گسترش بارهای تهدید.
	3. بدافزاری که مستقیم در RAM اجرا می‌شود تا از شناسایی توسط پویشگرهای دیسک بگریزد.
	4. بدافزار خودتکثیرشونده که بدون اقدام انسان در شبکه‌ها پخش می‌شود.
	5. بدافزاری که حافظهٔ سیستم را رمزگذاری می‌کند و برای تحویل کلید پول می‌خواهد.
	6. برنامه‌ای که برای نظارت و ثبت پنهانی فعالیت و ورودی‌های کاربر طراحی شده است.
	7. نرم‌افزار مخرب که به شکل یک برنامهٔ کاربردی بی‌خطر یا مفید پنهان شده است.
	8. محیط مجازی ایزوله که برای تحلیل ایمن فایل‌های مخرب به کار می‌رود.

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

فعالیت تکمیلی: سریع فکر کن

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

1	جاهایی که می‌توان برنامه‌های ایمن را دانلود کرد		
2	دستگاه‌هایی که می‌توانند هک شوند		
3	چیزهایی که پشتیبان می‌گیرید		
4	نشانه‌های هشدار در یک ایمیل		
5	نشانه‌های بدافزار در گوشی		
6	انواع بدافزار که می‌شناسید		
7	انواع فایل که باید با آن‌ها محتاط بود		
8	روش‌هایی که بدافزار وارد رایانه می‌شود		
9	عادت‌های ایمن که می‌توانید از امروز شروع کنید		
10	واژه‌های مرتبط با امنیت سایبری		
11	کارهایی که پس از نشت داده باید انجام داد		
12	دلایل به‌روزرسانی نرم‌افزار		
13	جانوران یا شخصیت‌هایی با نام‌هایی شبیه بدافزار		
14	چیزهایی که بدافزار می‌تواند بدزدد		
15	کارهایی که اگر روی پیوند اشتباه کلیک کردید باید انجام دهید		

ایستگاه بررسی 8: مطالعات موردی امنیت سایبری

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

مطالعهٔ موردی 1: مهار بار باج‌افزار در سازمان



سناریو: یک شبکهٔ محلی سازمانی توسط باج‌افزار فعال نفوذ شده است. سرورهای فایل کلیدی شروع به نمایش پسوند فایل .locked کرده‌اند. سیاست‌های مهار را برقرار کنید.

پرسش برای بحث: مراحل مهار را شرح دهید و پروتکل بازیابی داده را بیان کنید.

مطالعهٔ موردی 2: تزریق حافظهٔ بدافزار بدون فایل



سناریو: یک تحلیلگر الگوهای اسکریپت مشکوکی را شناسایی می‌کند که با ابزارهای مدیریتی استاندارد مستقیماً در RAM فرّار سیستم اجرا می‌شوند، اما هیچ فایل مخربی روی دیسک وجود ندارد.

پرسش برای بحث: راهبرد تحلیل حافظه را توضیح دهید و ابزارهای مسدودسازی اجرای بدون فایل (fileless) را مشخص کنید.

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

32	12	1	4	23	12		32	32	1	15	1	29	16

19	1	24	29		12	10		12	1	13	23	1	10	2

32	29	1	32	1	3

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: بدافزار چیست؟

نرم‌افزار مخربی که عوامل تهدید برای آسیب زدن، ربودن یا سرقت داده از دستگاه‌ها و شبکه‌ها طراحی کرده‌اند.

Q2: تفاوت ویروس و کرم چیست؟

ویروس برای پخش شدن به اقدام انسان (مانند باز کردن فایل) نیاز دارد، در حالی که کرم به‌طور خودکار در شبکه‌ها پخش می‌شود.

Q3: اسب تروا چگونه رایانه را آلوده می‌کند؟

کاربران را با تظاهر به برنامهٔ بی‌ضرر یا ایمن فریب می‌دهد و محموله مخرب خود را در آن پنهان می‌کند.

Q4: باج‌افزار چیست؟

نوعی بدافزار که فایل‌های سیستم هدف را رمزگذاری می‌کند و در ازای کلید رمزگشایی، پرداخت مالی می‌طلبد. [1]

Q5: جاسوس‌افزار چیست؟

نرم‌افزار مخربی که پنهانی ضربه‌های کلید، گذرواژه‌ها و عادت‌های مرور کاربر را ضبط می‌کند تا برای مهاجمان بفرستد.

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

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

Q6: سندباکس‌سازی به چه معناست؟

اجرای فایل‌های مشکوک در یک محیط مجازی امن و ایزوله برای مشاهدهٔ رفتار آن‌ها بدون خطر برای سیستم‌های تولید.

Q7: بدافزار بدون فایل چیست؟

بدافزاری که مستقیماً در حافظهٔ سیستم (RAM) با ابزارهای قانونی اجرا می‌شود و برای دور زدن پویشگرهای ساده، فایلی روی دیسک نمی‌نویسد.

Q8: روت‌کیت چگونه از بدافزار محافظت می‌کند؟

فرایندها و فایل‌های مخرب را پنهان می‌کند، اغلب با دستکاری هستهٔ سیستم‌عامل، بنابراین اسکنرهای آنتی‌ویروس ممکن است آنها را از دست بدهند.

Q9: پایش رفتار پویا چیست؟

اسکن آنتی‌ویروسی که فرایندهای فعال را به‌صورت بلادرنگ پایش می‌کند تا اقدام‌های رایج بدافزار، مانند رمزگذاری انبوه فایل‌ها، را مسدود کند.

Q10: چرا مهار در پاسخ به رخداد فوری است؟

جداسازی نقاط انتهایی در معرض خطر مانع انتشار محموله‌های فعال بدافزار به سایر دستگاه‌های شبکه می‌شود.

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

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

Q1: توسعه‌دهندگان بدافزار چگونه اسکنرهای آنتی‌ویروس مبتنی بر امضا را دور می‌زنند؟

آن‌ها از چندریختی استفاده می‌کنند و با هر آلودگی هش و ساختار کد فایل را تغییر می‌دهند، در حالی که رفتار مخرب یکسان می‌ماند.

Q2: خطر ابزارهای دومنظوره در کمپین‌های بدافزار چیست؟

مهاجمان از ابزارهای مدیریتی قانونی (مانند PowerShell یا Sysinternals) استفاده می‌کنند تا در ترافیک عادی شبکه ادغام شوند و تشخیص را دشوار کنند.

Q3: process hollowing چگونه بارهای مخرب را اجرا می‌کند؟

یک فرایند مشروع سیستمی را در حالت تعلیق اجرا می‌کند، کد حافظهٔ آن را با بدافزار جایگزین می‌کند و اجرا را از سر می‌گیرد.

Q4: نقش سرور فرمان و کنترل (C2) چیست؟

سرور راه‌دوری که هکرها اداره می‌کنند تا به بدافزار در حال اجرا روی ماشین‌های آلوده دستور و بار ارسال کنند.

Q5: چرا تشخیص کی‌لاگر دشوار است؟

کی‌لاگرهای ساده منابع CPU بسیار کمی مصرف می‌کنند و فرایندهای خود را درون ابزارهای معتبر فضای کاربر پنهان می‌کنند.

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

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

Q6: مبهم‌سازی کد چگونه تحلیل بدافزار را به تأخیر می‌اندازد؟

کد منبع را رمزگذاری یا بازچینی می‌کند و آن را برای ابزارهای تحلیلگر و اسکنرهای امنیتی ناخوانا می‌کند.

Q7: کارکرد بوت‌کیت چیست؟

روت‌کیتی که فرایند راه‌اندازی (MBR، بوت‌سکتور یا میان‌افزار UEFI) را آلوده می‌کند، بنابراین پیش از بارگذاری سیستم‌عامل اجرا می‌شود.

Q8: اسکن اکتشافی چگونه تهدیدهای روز صفر را شناسایی می‌کند؟

به‌جای جست‌وجوی هش تطبیقی در پایگاه‌داده، الگوهای کد مشکوک و دستورهای مدیریتی را اسکن می‌کند.

Q9: تهدید ربایش DLL چیست؟

وادار کردن یک برنامهٔ مشروع به بارگذاری یک کتابخانهٔ پیوند پویای (DLL) مخرب با قرار دادن آن در مسیر پوشهٔ برنامه.

Q10: خطوط لولهٔ تحلیل خودکار بدافزار چگونه از مجازی‌سازی استفاده می‌کنند؟

آن‌ها فایل‌های مشکوک را روی چند ماشین مجازی سیستم‌عامل اجرا می‌کنند و به‌طور خودکار گزارش‌های رفتار و فایل‌های PCAP شبکه تولید می‌کنند.

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

اسب‌های تروا همچنان روش آلودگی رایجی هستند، چون کد مخرب را درون برنامه‌هایی که بی‌خطر به نظر می‌رسند پنهان می‌کنند.

2. بینش امنیت

IC3 در FBI در سال 2025 بیش از 3,600 شکایت باج‌افزار دریافت کرد و زیان‌های گزارش‌شده از 32 میلیون دلار فراتر رفت. [3]

3. بینش امنیت

کرم‌ها می‌توانند با سوءاستفاده از آسیب‌پذیری‌های وصله‌نشدهٔ پروتکل، مانند EternalBlue در SMB، به‌سرعت در شبکه‌ها پخش شوند.

4. بینش امنیت

بدافزار بدون فایل تشخیصش دشوار است، زیرا از طریق ابزارهای قانونی در حافظه اجرا می‌شود و ردپای کمی روی دیسک بر جا می‌گذارد.

5. بینش امنیت

sandboxهای تحلیل معمولاً پس از هر اجرا به یک اسنپ‌شات تمیز بازمی‌گردند تا هر آزمون از وضعیت شناخته‌شده شروع شود.

6. بینش امنیت

روت‌کیت‌ها می‌توانند فراخوانی‌های سیستمی هسته را تغییر دهند و نتایج تشخیصی نادرست به اسکنرهای ضدبدافزار گزارش کنند.

7. بینش امنیت

مبهم‌سازی کد از ابزارهای بسته‌بندی برای فشرده‌سازی و پنهان کردن ساختار واقعی بار دودویی بدافزار استفاده می‌کند.

8. بینش امنیت

بدافزار چندریخت با هر نسخهٔ جدید کد خود و در نتیجه درهم‌ساز فایل را تغییر می‌دهد تا از بررسی‌های امضا بگریزد.

9. بینش امنیت

ربایش DLL از پیکربندی‌های ترتیب جست‌وجو در سیستم‌عامل‌های رایج مانند ویندوز سوءاستفاده می‌کند.

10. بینش امنیت

فروشندگان امنیتی هر روز تعداد بسیار زیادی نمونهٔ بدافزار جدید پیدا می‌کنند، بنابراین امضاها به به‌روزرسانی مداوم نیاز دارند.

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

[2] CISA. (2023). #StopRansomware Guide.
https://www.cisa.gov/stopransomware/ransomware-guide

[3] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.
https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[4] FBI Internet Crime Complaint Center. (n.d.). Ransomware.
https://www.ic3.gov/CrimeInfo/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 پرسش 1 — پاسخ درست: A

نکتهٔ آموزشی

ویژگی تعیین‌کنندهٔ اسب تروا چیست؟ → خود را به‌جای نرم‌افزار قانونی جا می‌زند تا کاربران را فریب دهد که آن را اجرا کنند

2 پرسش 2 — پاسخ درست: A

نکتهٔ آموزشی

کدام نوع بدافزار فایل‌ها را رمزگذاری می‌کند و درخواست پول می‌کند؟ → باج‌افزار

3 پرسش 3 — پاسخ درست: A

نکتهٔ آموزشی

چه چیزی نمایندهٔ جاسوس‌افزار است؟ → بدافزاری که برای پایش پنهانی ضربه‌های کلید و فعالیت‌های مرورگر کاربر طراحی شده است

4 پرسش 4 — پاسخ درست: A

نکتهٔ آموزشی

چرا توسعه‌دهندگان بدافزار از روت‌کیت استفاده می‌کنند؟ → برای پنهان کردن فرایندهای فعال و فایل‌های مخرب از سیستم‌عامل

5 پرسش 5 — پاسخ درست: A

نکتهٔ آموزشی

سندباکس در تحلیل بدافزار به چه معناست؟ → اجرای فایل‌های مشکوک در یک گاوصندوق مجازی ایزوله برای مشاهدهٔ ایمن رفتار

کلید پاسخ: ایستگاه بررسی 2 – درست یا نادرست

6 پرسش 6

پاسخ درست: نادرست

نکتهٔ آموزشی

نادرست: کرم‌ها خودتکثیر هستند و بدون هیچ اقدام کاربر در شبکه‌ها پخش می‌شوند.

7 پرسش 7

پاسخ درست: نادرست

نکتهٔ آموزشی

نادرست: تبلیغ‌افزار (adware) همیشه بی‌ضرر نیست؛ بخش زیادی از آن مرور را برای هدف‌گیری تبلیغات ردیابی می‌کند.

8 پرسش 8

پاسخ درست: درست

نکتهٔ آموزشی

درست: پشتیبان‌های آفلاین سالم فایل‌های رمزگذاری‌شده را بدون پرداخت بازیابی می‌کنند، هرچند داده‌های دزدیده‌شده همچنان ممکن است نشت کنند.

9 پرسش 9

پاسخ درست: نادرست

نکتهٔ آموزشی

نادرست: اسکنرهای مبتنی بر امضا به یک نمونهٔ شناخته‌شده نیاز دارند، بنابراین بدافزار روز صفر کاملاً جدید می‌تواند از آن‌ها عبور کند.

10 پرسش 10

پاسخ درست: درست

نکتهٔ آموزشی

بدافزار بدون فایل، اسکریپت‌های مخرب را در حافظهٔ سیستم اجرا می‌کند و از نوشتن فایل روی دیسک پرهیز می‌کند.

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

D 1. تروجان	F 2. باج‌افزار	A 3. جاسوس‌افزار	H 4. روت‌کیت
G 5. سندباکس	C 6. مهار	E 7. کرم	B 8. بدون فایل

ایستگاه بررسی 3: کلید پاسخ – اصطلاحات کلیدی

1 تروجان	2 باج‌افزار	3 جاسوس‌افزار	4 روتکیت
5 سندباکس	6 مهار		

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

1 D – روتکیت	2 F – مهار	3 H – بدون‌فایل	4 G – کرم
5 B – باج‌افزار	6 C – جاسوس‌افزار	7 A – تروجان	8 E – سندباکس

یادداشت‌های بحث برای مدرسان

اصطلاحات کلیدی:
بررسی کنید که دانش‌آموزان بتوانند تروجان، باج‌افزار و جاسوس‌افزار را با کلمات خودشان توضیح دهند و برای هر کدام مثالی بزنند.

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

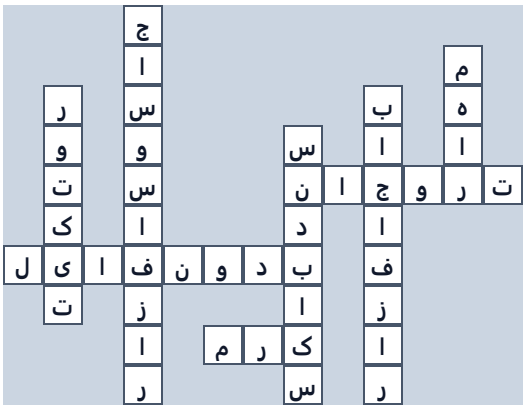
ارزیابی منابع:
از دانش‌آموزان بخواهید دست‌کم یک ادعا را در منابع کاربرگ بررسی کنند و دربارهٔ اینکه چرا ارقام، قیمت‌ها و قوانین ممکن است با گذشت زمان تغییر کنند گفت‌وگو کنید.

کلیدهای معما و یادداشت‌های معلم

پاسخ جدول کلمات

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

پاسخ جدول‌کلمات



راهنمای معلم برای پاسخ‌های جدول کلمات متقاطع

افقی

6 افقی: تروجان نرم‌افزار مخرب که به شکل یک برنامهٔ کاربردی بی‌خطر یا مفید پنهان شده است. (6 حرف)

7 افقی: بدونفایل بدافزاری که مستقیم در RAM اجرا می‌شود تا از شناسایی توسط پویشگرهای دیسک بگریزد. (8 حرف)

8 افقی: کرم بدافزار خودتکثیرشونده که بدون اقدام انسان در شبکه‌ها پخش می‌شود. (3 حرف)

عمودی

1 عمودی: جاسوسافزار برنامه‌ای که برای نظارت و ثبت پنهانی فعالیت و ورودی‌های کاربر طراحی شده است. (10 حرف)

2 عمودی: مهار محدود کردن نقاط پایانی آلوده برای جلوگیری از گسترش بارهای تهدید. (4 حرف)

3 عمودی: باجافزار بدافزاری که حافظهٔ سیستم را رمزگذاری می‌کند و برای تحویل کلید پول می‌خواهد. (8 حرف)

4 عمودی: روتکیت بدافزار نهان‌کار که در عمق هستهٔ سیستم پنهان می‌شود تا کنترل مدیریتی را حفظ کند. (6 حرف)

5 عمودی: سندباکس محیط مجازی ایزوله که برای تحلیل ایمن فایل‌های مخرب به کار می‌رود. (7 حرف)

کلید پاسخ کلمات درهم‌ریخته و رمزگشایی

کلید نمره‌دهی برای فعالیت بازچینی واژگان و چالش رمز مخفی.

کلید مرتب‌سازی کلمات

1. وتجانر — تروجان
2. اوجاسرفزاس — جاسوسافزار
3. بساسدکن — سندباکس
4. رمک — کرم
5. فزاراباج — باجافزار
6. یکرتتو — روتکیت
7. امره — مهار
8. ندفلبیاو — بدونفایل

کلید چالش رمز مخفی

"شناسایی رفتاری بدافزار در نقاط پایانی"

کلید پاسخ مطالعات موردی

A مطالعهٔ موردی 1: مهار بار باج‌افزار در سازمان

پاسخ معلم

راهنمای نمره‌دهی

پاسخ‌های دانش‌آموز باید نکات زیر را پوشش دهد:

- تحلیل سناریو: شبکهٔ محلی یک شرکت توسط باج‌افزار فعال نفوذ شده است. سرورهای فایل کلیدی شروع به نمایش پسوندهای فایل .locked کرده‌اند. سیاست‌های مهار را تعیین کنید.
- راهبرد و راه‌حل توصیه‌شده: همهٔ سرورهای آسیب‌دیده را از شبکهٔ محلی جدا کنید. نشست‌های مدیریتی فعال را پایان دهید. فایل‌های آسیب‌ندیده را از یک سامانهٔ پشتیبان آفلاین امن با قفل نوشتن بازیابی کنید.

B مطالعهٔ موردی 2: تزریق حافظهٔ بدافزار بدون فایل

پاسخ معلم

راهنمای نمره‌دهی

پاسخ‌های دانش‌آموز باید نکات زیر را پوشش دهد:

- تحلیل سناریو: یک تحلیلگر الگوهای اسکریپت‌نویسی مشکوکی را شناسایی می‌کند که با ابزارهای مدیریتی استاندارد مستقیماً در RAM فرّار سیستم اجرا می‌شوند، اما هیچ فایل مخربی روی دیسک وجود ندارد.
- راهبرد و راه‌حل پیشنهادی: ابتدا نقاط انتهایی آسیب‌دیده را ایزوله کنید و تصویر حافظه بگیرید. گزارش‌های PowerShell و WMI را بررسی کنید، اسکریپت‌های تأییدنشده را با AppLocker مسدود کنید و سپس برای پاک شدن بار مخرب راه‌اندازی مجدد کنید.