שם: _____ תאריך: _____ ציון: _____

אינטרנט אפל לעומת אינטרנט עמוק: אבטחה ו הבדלים

אינדוקס במנועי חיפוש, מסדי נתונים של הרשת העמוקה, ניתוב בצל של Tor, אנונימיות ברשת וסיכונים

סקירת למידה: הרשת האפלה לעומת הרשת העמוקה

אובטח

הצפנת נתונים

תקן AES של 256 סיביות

תואם

תקנים עולמיים

מסגרות GDPR ו-CCPA

אפס אמון

מדיניות גישה

אימות רב-גורמי

ברוכים הבאים! חוברת הפעילויות הזו תדריך אתכם דרך ההבדלים בין הרשת העמוקה (Deep Web) לרשת האפלה (Dark Web). תחקרו מסדי נתונים לא מאונדקסים, ניתוב Onion בדפדפן Tor, דומיינים קריפטוגרפיים בסיומת .onion וסיכוני אבטחה הקשורים לאנונימיות.

נקודות הביקורת בדף העבודה

- [ ] **חלק 1-4: שלטו באבטחת סייבר ובמניעת איומים.**
- [ ] **חלק 5-7: פתרו תשבצים ופאזלי חיפוש מילים.**
- [ ] **חלק 8-9: פתרו מקרי בוחן ואתגר צופן.**
- [ ] **חלק 10: סקרו את דפי השאלות הנפוצות הבסיסיים והמתקדמים.**
- [ ] **חלק 11: חקרו 10 עובדות מעניינות מהעולם האמיתי.**
- [ ] **בונוס: אתגר חשבו מהר**

פתחו את מדריך אבטחת הסייבר של VPN.com

URL: https://www.vpn.com/cybersecurity/dark-web-vs-deep-web/

מפת הלמידה שלכם: אסטרטגיית הרשת העמוקה והאפלה

- השוו בין הרשת העמוקה (מסדי נתונים שאינם מאונדקסים) לרשת האפלה (שירותי onion).
- הבינו כיצד ניתוב בצלי (Onion Routing) מצפין ומעביר תעבורת רשת.
- העריכו את סיכוני האבטחה בגישה לאתרים לא מאומתים ברשת Tor.
- פרסו מדיניות שער מאובטח ובידוד בארגז חול לסריקת מודיעין איומים.
- נתחו את פורמט הכתובת הקריפטוגרפי של דומיינים של שירותי onion.

הוראות למדריך האינטרנט העמוק והאפל

ענו על שאלות אמריקאיות ועל שאלות נכון/לא נכון, השלימו את המשפטים החסרים בעזרת בנק המילים, התאימו הגדרות ופתרו את התשבץ ואת תפזורת המילים. יישמו את הידע שלכם בנושא פרטיות ברשת העמוקה והאפלה. ולסיום, פעילות הבונוס "חשבו מהר".

מסדי נתונים באינטרנט העמוק לעומת ניתוב בצל באינטרנט האפל (מבוא)

הרשת העמוקה כוללת דפים שאינם מאונדקסים מאחורי סיסמאות וכניסות, כמו דוא"ל פרטי או פורטלים בנקאיים ארגוניים. הרשת האפלה היא תת-קבוצה של הרשת העמוקה שמוסתרת בכוונה, ודורשת דפדפנים ייעודיים (כמו Tor) ורשתות onion כדי לגשת אליה באלמוניות.

קראו כל נקודת ביקורת בעיון ובחרו או כתבו את התגובה הנכונה.

נקודת ביקורת 1: אתגר שאלות אמריקאיות

1. במה נבדל האינטרנט העמוק מהאינטרנט השטחי?

- A. דפי deep web אינם מאונדקסים על ידי מנועי חיפוש ציבוריים
- B. תעבורת הרשת העמוקה אינה חוקית ונמצאת במעקב של רשויות האכיפה
- C. אתרי רשת עמוקה דורשים דפדפנים מיוחדים כמו Tor לגישה
- D. דפי הרשת העמוקה נטענים תמיד מהר יותר מדפי הרשת הגלויה

2. כיצד ניגשים לרשת האפלה?

- A. דרך דפדפנים ייעודיים שמשתמשים ברשתות ניתוב בצל (onion routing)
- B. על ידי הגדרת הגדרות DNS מותאמות בנתבים רגילים
- C. דרך קונסולות חיפוש פרטיות של האינטרנט הגלוי בהזמנה בלבד
- D. על ידי התקנת תוסף דפדפן רגיל לחסימת פרסומות

3. איזה מבנה מהווה את החלק הגדול ביותר באינטרנט העמוק?

- A. מסדי נתוני משתמשים וחשבונות פרטיים המוגנים בסיסמה
- B. פורומי שוק שחור לא חוקיים הסוחרים בסחורות אסורות
- C. פרוטוקולי שיתוף קבצים לא מוצפנים בין עמיתים
- D. מסדי נתונים ציבוריים של מטמון מנועי חיפוש

4. מה עושה ניתוב בצל (Onion Routing) לתעבורת הרשת?

- A. הוא מצפין מנות ומנתב אותן דרך כמה ממסרים
- B. הוא מגביר את מהירויות ההורדה על ידי עקיפת צמתי ספק האינטרנט
- C. הוא ממפה מספרים סידוריים של חומרת ההתקן לרשומות IP
- D. הוא מוחק עוגיות דפדפן אחרי כל לחיצה

5. איזו סיומת דומיין משמשת באופן בלעדי ברשתות Tor?

- A. סיומת הרמה העליונה הקריפטוגרפית .onion
- B. סיומת .com המסחרית הוותיקה והרגילה
- C. סיומת blockchain מבוזרת של Web3 מסוג .eth
- D. סיומת הטכנולוגיה .ai של קוד מדינה

נקודת ביקורת 2: אתגר נכון או לא נכון

6 שאלה נכון/לא נכון 6

6. הרשת העמוקה והרשת האפלה מתייחסות לאותו מקטע רשת.

○ נכון ○ לא נכון

7 שאלה נכון/לא נכון 7

7. פורטלי אינטראנט ארגוניים הם חלק מהרשת העמוקה.

○ נכון ○ לא נכון

8 שאלה נכון/לא נכון 8

8. ניתוב Onion מפענח לחלוטין את חבילות הנתונים בכל צומת מעבר.

○ נכון ○ לא נכון

9 שאלה נכון/לא נכון 9

9. גישה ל-dark web חושפת מכשירים לסיכוני נוזקות גבוהים.

○ נכון ○ לא נכון

10 שאלה נכון/לא נכון 10

10. מנועי חיפוש רגילים סורקים ומאנדקסים אתרי onion.

○ נכון ○ לא נכון

נקודת ביקורת 3: השלמת מונחי מפתח

קראו כל משפט שלהלן והשלימו את החסר במונח הנכון מבנק המילים.

1. פורטלים בנקאיים פרטיים נמצאים בחלק הלא מאונדקס שנקרא _____ .
2. צמתי Tor מיוחדים מארחים שירותים חבויים של _____ .
3. אתרי Tor משתמשים בסיומת הדומיין העליונה הקריפטוגרפית _____ .
4. ניתוב תעבורה מוצפן רב-שכבתי נקרא _____ .
5. מנועי חיפוש של הרשת הגלויה סורקים דפים שמופיעים בהם _____ ציבורי.
6. רשתות בצל מצפינות כתובות IP של לקוחות כדי לשמור על _____ המשתמש.

בנק מילים

onion. | אינדוקס | אנונימיות | הרשת האפלה צומת | הרשת העמוקה | מסד נתונים | ניתוב בצל

כתבו את תשובותיכם כאן:

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

נקודת ביקורת 4: התאמת מושגים באבטחה

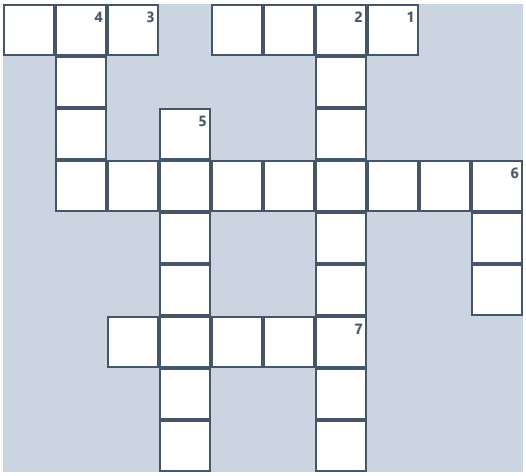
התאמת הגדרות

התאימו כל מונח אוצר מילים בצד ימין להגדרה הנכונה שלו בצד שמאל על ידי כתיבת האות המתאימה (A-H) בתיבת הקלט הניתנת למילוי.

1. מקטע האינטרנט העמוק	A	מקטע רשת מוצפן הנגיש רק דרך דפדפנים מיוחדים.
2. פורטל אינטרנט אפל	B	הצפנת נתונים בשכבות והעברתם דרך שלושה צמתים.
3. סיומת Onion	C	אחסון אחורי מאובטח המכיל רשומות מערכת שאינן מאונדקסות.
4. ניתוב Tor	D	סיומת דומיין עליונה קריפטוגרפית המשמשת ברשתות Tor.
5. עמודים מאונדקסים	E	צומת נקודת הכניסה המשמש לגישה לרשת Tor.
6. אנונימיות משתמש	F	תוכן האינטרנט השטחי שנאסף וניתן לחיפוש ב-Google.
7. מסד נתונים פרטי	G	הסתרת כתובות ה-IP הציבוריות של הלקוחות מפני שרתים.
8. שער כניסה	H	תוכן אינטרנט לא מאונדקס כמו כניסות פרטיות, דוא"ל ורשומות מסדי נתונים.

נקודת ביקורת 5: תשבץ

פתרו את התשבץ על ידי הקלדת אותיות בתיבות הלבנות הפעילות. המספרים מתאימים לרמזים שלהלן.



מאוזן

1. תוכן אינטרנט לא מאונדקס כמו כניסות פרטיות, הודעות דואר ורשומות מסדי נתונים (4)

3. סיומת דומיין עליונה קריפטוגרפית המשמשת ברשתות Tor (3)

6. הסתרת כתובות ה-IP הציבוריות של הלקוחות מפני השרתים (9)

7. הצפנת נתונים בשכבות והעברתם דרך שלושה צמתים (5)

מאונך

2. אחסון אחורי מאובטח שמארח רשומות מערכת לא מאונדקסות (9)

4. נקודת הכניסה שמשמשת לגישה לרשת Tor (4)

5. תוכן הרשת הגלויה שנאסף וניתן לחיפוש בגוגל (7)

6. מקטע רשת מוצפן הנגיש רק דרך דפדפנים מיוחדים (3)

נקודת ביקורת 5 – פעילות חלופית: רמזים נגישים לתשבץ

משתמשי קורא מסך ומקלדת יכולים להקליד את תשובות התשבץ ישירות בשדות הטקסט שלהלן.

מאוזן

1 מאוזן: תוכן אינטרנט לא מאונדקס כמו כניסות פרטיות, הודעות דואר ורשומות מסדי נתונים (4 אותיות):

3 מאוזן: סיומת דומיין עליונה קריפטוגרפית המשמשת ברשתות Tor (3 אותיות):

6 מאוזן: הסתרת כתובות ה-IP הציבוריות של הלקוחות מפני השרתים (9 אותיות):

7 מאוזן: הצפנת נתונים בשכבות והעברתם דרך שלושה צמתים (5 אותיות):

מאונך

2 מאונך: אחסון אחורי מאובטח שמארח רשומות מערכת לא מאונדקסות (9 אותיות):

4 מאונך: נקודת הכניסה שמשמשת לגישה לרשת Tor (4 אותיות):

5 מאונך: תוכן הרשת הגלויה שנאסף וניתן לחיפוש בגוגל (7 אותיות):

6 מאונך: מקטע רשת מוצפן הנגיש רק דרך דפדפנים מיוחדים (3 אותיות):

נקודת ביקורת 6: חיפוש מילה נסתרת

מצאו את 8 מונחי המפתח בלוח שלהלן. מילים יכולות להופיע אופקית, אנכית או באלכסון.

ט	ש	ל	ם	ס	ש	ו	צ	נ	כ	ג	ע	ח	ו	מ
ע	ל	ס	ש	ס	מ	ג	ו	א	צ	פ	פ	ה	י	ט
ב	א	ב	ג	נ	ת	י	מ	ט	י	ת	י	ש	צ	י
ם	ד	ל	ס	ל	ט	ד	ת	ח	ל	נ	ל	י	ס	נ
י	ז	צ	ל	ל	א	ס	ע	פ	צ	א	ד	צ	ו	ב
נ	פ	ב	ס	מ	נ	ח	ע	ב	ר	ד	פ	ו	פ	ם
ו	ק	ג	ם	ר	ו	ו	י	ע	ז	ם	ד	ל	ק	ל
ת	ד	ע	ש	נ	נ	ב	ק	מ	ב	א	ם	מ	ד	ס
נ	י	א	ד	מ	י	ד	ה	ו	ז	ח	ד	ע	ס	ל
ד	ה	ח	ע	ם	מ	פ	ה	ק	ע	ר	ה	א	א	ע
ס	נ	ל	נ	צ	י	ש	ס	ט	ע	צ	פ	ג	ל	נ
מ	ת	ב	ו	ע	ו	ש	ש	ט	א	ע	ם	ת	י	ת
כ	ו	ח	ל	ע	ת	ט	כ	כ	צ	נ	ז	ת	ס	ס
ז	ם	א	מ	ק	ו	ק	ב	ת	ע	ת	ו	ב	ז	כ
ם	ו	ט	מ	נ	מ	ש	ג	כ	ם	ב	ת	ו	ת	נ

רשימת מילים

עמוק | אפל | בצל | ניתוב | אינדוקס | אנונימיות | מסדנתונים | צומת

נקודת ביקורת 6 – פעילות חלופית: התאמת אוצר מילים נגישה

התאימו כל אחד מ-8 מונחי המילון מתפזורת המילים להגדרה הנכונה שלו על ידי כתיבת האות (A-H) במקום הריק.

מונחי אוצר מילים
A. עמוק
B. אפל
C. בצל
D. ניתוב
E. אינדוקס
F. אנונימיות
G. מסדנתונים
H. צומת

	הגדרות ושדות התאמה
	1. הסתרת כתובות ה-IP הציבוריות של הלקוחות מפני השרתים.
	2. אחסון אחורי מאובטח שמארח רשומות מערכת לא מאונדקסות.
	3. הצפנת נתונים בשכבות והעברתם דרך שלושה צמתים.
	4. תוכן אינטרנט לא מאונדקס כמו כניסות פרטיות, הודעות דואר ורשומות מסדי נתונים.
	5. מקטע רשת מוצפן הנגיש רק דרך דפדפנים מיוחדים.
	6. סיומת דומיין עליונה קריפטוגרפית המשמשת ברשתות Tor.
	7. נקודת הכניסה שמשמשת לגישה לרשת Tor.
	8. תוכן הרשת הגלויה שנאסף וניתן לחיפוש בגוגל.

נקודת ביקורת 7: אתגר מילים מבולבלות

סדרו מחדש את האותיות שלהלן כדי לחשוף מושגים ומונחים מרכזיים באבטחת סייבר. כתבו את תשובותיכם בתיבות הקלט המסופקות.

1. ועקמ
2. לצב
3. דאוסנקי
4. תסיננומסד
5. לפא
6. ונתבי
7. מאותיננייו
8. צתמו

פעילות בונוס: חשבו מהר

כתבו 3 תשובות לכל קטגוריה. מי שמסיים ראשון את הרשימה מנצח.

1	סיבות להתרחק מהרשת האפלה		
2	דברים שמנוע חיפוש לא יכול למצוא		
3	מכשירים שאפשר לפרוץ אליהם		
4	סיבות חוקיות להשתמש ב-Tor		
5	סיבות לעדכן תוכנה		
6	סימני אזהרה באימייל		
7	דברים שנמכרים באופן בלתי חוקי ברשת האפלה (dark web)		
8	אנשים שאפשר לבקש מהם עזרה ב-IT		
9	הרגלים בטוחים שאפשר להתחיל כבר היום		
10	דברים שעושים אחרי דליפת נתונים		
11	דברים השייכים לרשת העמוקה (deep web)		
12	אתרים שאתם משתמשים בהם עם התחברות		
13	מילים הקשורות לאלמוניות		
14	מידע שלעולם אסור לשתף		
15	דברים ששוכנים "מתחת לפני השטח"		

נקודת ביקורת 8: מקרי בוחן באבטחת סייבר

יישמו את המושגים שלמדתם כדי לפתור את התרחישים מהעולם האמיתי שלהלן.

מקרה בוחן 1: זיהוי דליפת נתונים



תרחיש: ביקורת אבטחה ארגונית מגלה שרשומות רגישות ממסד נתוני לקוחות נסחרות בשוק onion. הנתונים אינם מאונדקסים ב-Google.

שאלה לדיון: הסבירו אילו חלקים של האינטרנט מעורבים וכיצד הדליפה הזו התרחשה.

מקרה בוחן 2: אנונימיות לעומת סיכוני נוזקות



תרחיש: אנליסט רוצה לבדוק פידים של מודיעין איומים באתר Tor. הוא מוריד את דפדפן Tor וניגש לאתר.

שאלה לדיון: הערכו את יתרונות האלמוניות ותארו בקצרה את צעדי ההפחתה של סיכוני נוזקות.

נקודת ביקורת 9: פענוח הצופן

איש מקצוע באבטחת סייבר מגן על נכסי רשת מפני גורמי איום מקוונים. השתמשו במפתח האותיות-למספרים שלהלן כדי לפענח את ההודעה, וכתבו את האותיות המתאימות במקומות הריקים.

מפתח הצפנה של אות למספר

א=1 ב=2 ג=3 ד=4 ה=5 ו=6 ז=7 ח=8 ט=9

י=10 כ=11 ל=12 מ=13 נ=14 ס=15 ע=16 פ=17 צ=18

ק=19 ר=20 ש=21 ת=22 ך=23 ם=24 ן=25 ף=26 ץ=27

22	20	7	16	2		22	6	10	13	10	14	6	14	1		6	20	13	21
		8	9	2	6	1	13		12	18	2		2	6	22	10	14		

ההודעה המפוענחת:

טיפ: כל מספר מייצג אות עברית אחת מהמפתח שלמעלה.

נקודת ביקורת 10: שאלות נפוצות על אבטחת סייבר – בסיסי (חלק A)

עיינו בשאלות ותשובות נפוצות בנושא צמצום איומים ברשת.

Q1: מהי הרשת העמוקה?

הרשת העמוקה (deep web) כוללת את כל דפי האינטרנט שמנועי חיפוש אינם יכולים לאנדקס, כולל בנקאות מקוונת, מסדי נתוני דוא"ל ופרסומים מאחורי חומת תשלום.

Q2: מהי הרשת האפלה (dark web)?

הרשת האפלה היא תת-קבוצה קטנה של הרשת העמוקה, מוסתרת בכוונה ונגישה רק דרך דפדפנים ייעודיים המשתמשים ברשתות onion.

Q3: כיצד מנועי חיפוש מאנדקסים דפים?

מנועים מריצים תוכנות אוטומטיות (עכבישים) כדי לעקוב אחר קישורים ציבוריים ולאנדקס דפים שאינם חוסמים סריקה באמצעות הנחיות robot.

Q4: מדוע בנקאות מקוונת נחשבת חלק מהרשת העמוקה?

פורטלים בנקאיים נמצאים מאחורי חומות התחברות וסיסמאות, ולכן מנועי חיפוש ציבוריים אינם יכולים לאנדקס את דפי דוחות החשבון.

Q5: מהו ניתוב בצלים (Onion Routing) בדפדפן Tor?

ניתוב Onion היא שיטת שידור שמצפינה תעבורה בשכבות ומעבירה אותה דרך מספר ממסרים כדי להסוות כתובות IP של משתמשים.

נקודת ביקורת 10: שאלות נפוצות על אבטחת סייבר – בסיסי (חלק B)

עיינו בשאלות ותשובות נפוצות בנושא צמצום איומים ברשת.

Q6: האם גישה לרשת האפלה אסורה?

לא. הגישה לרשת האפלה חוקית ברוב המדינות, אך עיסוק בשווקים בלתי חוקיים או בפעילות סייבר בלתי חוקית אסור.

Q7: מדוע אתרי רשת אפלה נטענים לאט?

התעבורה מנותבת ומפוענחת דרך שלושה ממסרים גלובליים לפחות (כניסה, אמצע, יציאה), מה שמגדיל את השהיית השידור.

Q8: מה משמעות סיומת דומיין .onion?

זוהי סיומת דומיין עליון ייעודית המשמשת ברשתות Tor ומצביעה על כתובות שנוצרו קריפטוגרפית במקום על שרתי DNS סטנדרטיים.

Q9: אילו סיכונים קשורים לקישורי רשת אפלה?

לאתרים אין סינון אבטחה, מה שחושף משתמשים לשיעורי הדבקה גבוהים בנוזקות, לסקריפטים של פישינג ולהונאות עסקאות.

Q10: מי יצר את פרוטוקול הניתוב של רשת Tor?

הטכנולוגיה פותחה במקור על ידי מעבדת המחקר הימי של ארה"ב בשנות ה-1990 כדי להגן על תקשורת ממשלתית.

נקודת ביקורת 10: שאלות נפוצות על אבטחה – מתקדם (חלק C)

חקרו היבטים טכניים מתקדמים של מסגרות אבטחה, ניתוח נוזקות ועמידה בדרישות נתונים.

Q1: כיצד צמתי ביניים מגנים על האנונימיות ב-Tor?

כל צומת מפענח רק שכבה אחת של נתוני ניתוב, ולומד רק את הקפיצה הקודמת והבאה, אך לעולם לא את המקור והיעד גם יחד.

Q2: מהו תפקידו של צומת היציאה?

צומת היציאה מפענח את שכבת ההצפנה האחרונה ושולח את התעבורה אל שרת היעד הציבורי או שרת ה-onion.

Q3: מהי שער גשרי Tor (Tor bridges)?

גשרים (Bridges) הם ממסרי כניסה לא רשומים של Tor המשמשים לעקיפת חסימות של ספק האינטרנט וצנזורה באזורים המגבילים גישה לדפדפן Tor.

Q4: כיצד גורמי דארק-נט מנצלים מטבעות קריפטוגרפיים?

גורמים פועלים משתמשים במטבעות קריפטוגרפיים אנונימיים לביצוע עסקאות פיננסיות בשווקי חשכה, תוך התחמקות מבדיקות עסקאות בנקאיות סטנדרטיות.

Q5: מדוע מנועי חיפוש רגילים נכשלים בסריקת מסדי נתונים עמוקים?

זחלנים אינם יכולים להזין אישורי כניסה, לפתור CAPTCHA אבטחה או להריץ סקריפטים של שאילתות SQL בצד השרת הנדרשים לגישה למסדי נתונים עמוקים.

נקודת ביקורת 10: שאלות נפוצות על אבטחה – מתקדם (חלק D)

חקרו היבטים טכניים מתקדמים של מסגרות אבטחה, ניתוח נוזקות ועמידה בדרישות נתונים.

Q6: מהו שרת ספרייה ברשתות Tor?

זהו שרת מהימן שמנהל את רשימת הממסרים הפעילים (כניסה, אמצע ויציאה) שבהם משתמשים לקוחות לבניית נתיבי ניתוב.

Q7: כיצד גורמים זדוניים מבצעים האזנה בצומת יציאה?

מפעילי צמתי יציאה סוררים יכולים ליירט תעבורת HTTP לא מוצפנת כשהיא יוצאת מרשת Tor ולגנוב שמות משתמש ו-cookies.

Q8: מה ההבדל בין Tor ל-I2P?

Tor משתמש בספריית ממסרים ריכוזית ובצמתי יציאה לגישה לאינטרנט הציבורי, ואילו I2P משתמש במבנה עמית-לעמית מבוזר לאחסון פנימי.

Q9: כיצד גופי אכיפת חוק עוקבים אחר שווקי הרשת האפלה?

סוכנויות משתמשות בניתוח בלוקצ'יין, מאתרות הקמות אירוח של שרתים פיזיים ומפעילות מבצעי פיתיון כדי לזהות מפעילים.

Q10: כיצד דליפת DNS פוגעת באנונימיות הלקוח?

דליפות DNS מתרחשות כאשר שאילתות DNS של הדפדפן נשלחות ישירות דרך ספק האינטרנט המקומי במקום לעבור ברשת Tor המוצפנת.

חלק 11: 10 עובדות ותובנות מהעולם האמיתי על אבטחת סייבר

עיינו בעובדות מהעולם האמיתי על פריצות אבטחה, מנגנוני הגנה ותקני ציות.

1. תובנות על אבטחה

הרשת העמוקה גדולה בהרבה מרשת השטח הניתנת לחיפוש, שכן רוב התוכן נמצא מאחורי כניסות ומסדי נתונים.

2. תובנות על אבטחה

הרשת האפלה היא חלק קטן ומוסתר בכוונה של הרשת העמוקה, שאליו מגיעים באמצעות כלים כמו Tor.

3. תובנות על אבטחה

ניתוב Tor מצפין מנות נתונים שלוש פעמים, ומקלף שכבות הצפנה כמו בצל בכל צומת ממסר.

4. תובנות על אבטחה

Tor צמח מפרויקט הניתוב הבצלי (onion routing) של מעבדת המחקר הימי של ארה"ב, וקוד המקור שלו שוחרר כתוכנה חופשית. [1]

5. תובנות על אבטחה

כתובות Onion הן מחרוזות אלפאנומריות בנות 56 תווים שנוצרות בשיטות קריפטוגרפיות מזוגות מפתחות ציבוריים.

6. תובנות על אבטחה

צמתי יציאה יכולים לקרוא תעבורה בטקסט גלוי, כלומר עדיין נדרשים TLS/HTTPS ב-Tor עבור נתוני הפעלה מאובטחים.

7. תובנה על אבטחה

אתרי אינטראנט, כוננ ענן ומסדי נתונים פרטיים מהווים את מקטעי אחסון הנתונים הגדולים ביותר ברשת העמוקה.

8. תובנה על אבטחה

מנועי חיפוש ייעודיים כמו DuckDuckGo מפעילים שערי onion כדי לאפשר חיפושים אנונימיים ברשתות Tor.

9. תובנה על אבטחה

יותר מ-2 מיליון משתמשים מתחברים מדי יום לרשת Tor כדי לעקוף צנזורה ולשמור על פרטיות התקשורת.

10. תובנות על אבטחה

מבצעי אכיפת חוק עולמיים (כמו Operation Bayonet) סגרו שווקים אפלים גדולים על ידי תפיסת חומרת האירוח.

מקורות והפניות טכניים

מדריך הלימוד והפאזלים האינטראקטיביים נערכו על סמך תקנים גלובליים של NIST, OWASP ותאימות לפרטיות נתונים.

מקורות אקדמיים ותעשייתיים

[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

מפתח תשובות: נקודת ביקורת 1 – שאלות אמריקאיות

1 **אינדוקס במנועי חיפוש** אינטרנט עמוק — **תשובה נכונה: A**

הערה למורה

דפים באינטרנט העמוק נמצאים מאחורי חומות כניסה ומסדי נתונים, ולכן סורקי מנועי החיפוש אינם יכולים לזחול בהם. מקור: IETF RFC 3986.

2 **גישה ל-Tor** הרשת האפלה — **תשובה נכונה: A**

הערה למורה

הרשת האפלה (dark web) מורכבת משירותי onion נסתרים הנגישים רק דרך דפדפנים כמו Tor. מקור: IETF RFC 3986.

3 **מסדי נתונים עמוקים** מסדי נתונים — **תשובה נכונה: A**

הערה למורה

חשבונות מוגנים בסיסמה ורשומות ארגוניות מהווים את הפלח הגדול ביותר ברשת העמוקה. מקור: NIST Digital Identity.

4 **ניתוב Onion** רשת Tor — **תשובה נכונה: A**

הערה למורה

ניתוב Onion מצפין חבילות נתונים בשכבות ומעביר אותן דרך מספר צמתים לשם אנונימיות. מקור: IETF RFC 3986.

5 **דומיין Onion** סיומת — **תשובה נכונה: A**

הערה למורה

סיומת הדומיין הקריפטוגרפית.onion מנתבת תעבורה פנימית ברשת Tor ללא DNS ציבורי. מקור: IETF RFC 3986.

מפתח תשובות: נקודת ביקורת 2 – נכון או לא נכון

6 **מקטעי אינטרנט** מבנה

תשובה נכונה: לא נכון

הערה למורה

הרשת העמוקה כוללת את כל הדפים שאינם מאונדקסים, ואילו הרשת האפלה היא תת-מקטע onion קטן ומוצפן. מקור: IETF RFC 3986.

7 **אינטראנטים ארגוניים** אינטרנט עמוק

תשובה נכונה: נכון

הערה למורה

אתרי אינטראנט נמצאים מאחורי פורטלים מוגני סיסמה ואינם מאונדקסים, כלומר הם שייכים לרשת העמוקה. מקור: NIST Digital Identity.

8 **הצפנה בשכבות** ממסרים

תשובה נכונה: לא נכון

הערה למורה

ממסרי Onion מפענחים רק שכבת ניתוב אחת כדי להגן על אנונימיות המשתמש, ולעולם לא את החבילה כולה. מקור: IETF RFC 3986.

9 **חשיפה לנוזקות** איומים

תשובה נכונה: נכון

הערה למורה

בשווקים באינטרנט האפל אין סינון אבטחה, ולכן קיים בהם סיכון קיצוני להדבקה בנוזקות. מקור: Center for Internet Security (CIS).

10 **שאלה 10**

תשובה נכונה: לא נכון

הערה למורה

סורקי מנועי חיפוש רגילים אינם משתמשים ב-Tor, ולכן אינם יכולים להגיע לאתרי .onion או לאנדקס אותם.

מפתחות אוצר מילים ומחוון הערכה

מחוון הערכה למורה: תנו 1 נקודה לכל התאמה נכונה (סה"כ 8 נקודות) ולכל מונח הקשר (סה"כ 6 נקודות).

נקודת ביקורת 4: מפתח תשובות – התאמת מושגים

H 1. מקטע האינטרנט העמוק	A 2. פורטל אינטרנט אפל	D 3. סיומת Onion	B 4. ניתוב Tor
F 5. עמודים מאונדקסים	G 6. אנונימיות משתמש	C 7. מסד נתונים פרטי	E 8. שער כניסה

נקודת ביקורת 3: מפתח תשובות – מונחי מפתח

1 הרשת העמוקה	2 הרשת האפלה	3 .onion	4 ניתוב בצל
5 אינדוקס	6 אנונימיות		

נקודת ביקורת 6 – פעילות חלופית: מפתח תשובות – התאמת אוצר מילים

1 F – אנונימיות	2 G – מסדנתונים	3 D – ניתוב	4 A – עמוק
5 B – אפל	6 C – בצל	7 H – צומת	8 E – אינדוקס

הערות לדיון עבור מורים

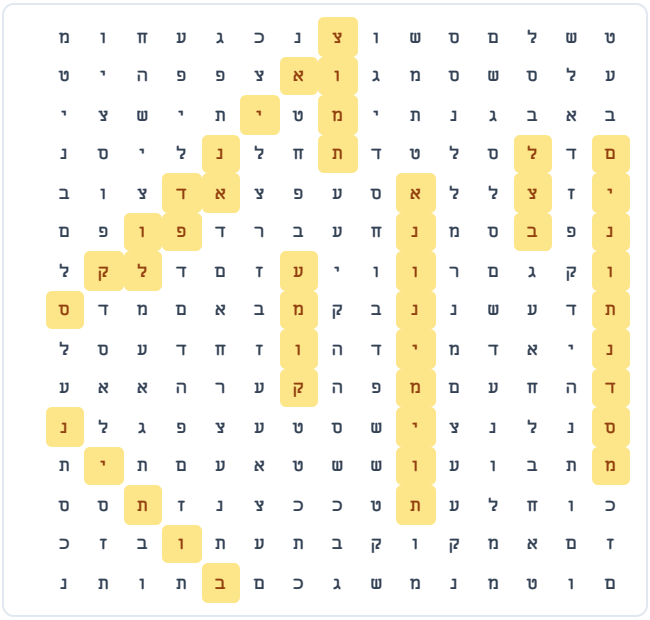
מונחי מפתח:
ודאו שהתלמידים מסבירים במילים שלהם את מקטע האינטרנט העמוק, פורטל אינטרנט אפל ו-סיומת Onion ונותנים דוגמה לכל אחד מהם.

מקרי בוחן:
בקשו מהתלמידים לבסס את ההמלצות שלהם על עובדות מדף העבודה ולא על דעות.

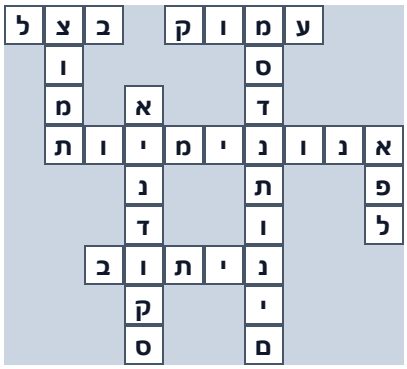
הערכת מקורות:
בקשו מהתלמידים לאמת לפחות טענה אחת במקורות של דף העבודה, ודונו מדוע נתונים, מחירים וכללים עשויים להשתנות עם הזמן.

מפתחות פאזלים והערות למורה

פתרון תפזורת



פתרון תשבץ



מדריך למורה לפתרונות התשבץ

מאוזן

1 מאוזן: עמוק תוכן אינטרנט לא מאונדקס כמו כניסות פרטיות, הודעות דואר ורשומות מסדי נתונים (4 אותיות)

3 מאוזן: בצל סיומת דומיין עליונה קריפטוגרפית המשמשת ברשתות Tor (3 אותיות)

6 מאוזן: אנונימיות הסתרת כתובות ה-IP הציבוריות של הלקוחות מפני השרתים (9 אותיות)

7 מאוזן: ניתוב הצפנת נתונים בשכבות והעברתם דרך שלושה צמתים (5 אותיות)

מאונך

2 מאונך: מסדנתונים אחסון אחורי מאובטח שמארח רשומות מערכת לא מאונדקסות (9 אותיות)

4 מאונך: צומת נקודת הכניסה שמשמשת לגישה לרשת Tor (4 אותיות)

5 מאונך: אינדוקס תוכן הרשת הגלויה שנאסף וניתן לחיפוש בגוגל (7 אותיות)

6 מאונך: אפל מקטע רשת מוצפן הנגיש רק דרך דפדפנים מיוחדים (3 אותיות)

מפתח פתרונות: מילים מבולבלות ופענוח הצופן

מפתח הערכה לפעילות פענוח מילות אוצר המילים ולאתגר הצופן הסודי.

מפתח פענוח מילים מבולבלות

1. ועקם — **עמוק**
2. לצב — **בצל**
3. דאוסנקי — **אינדוקס**
4. תסיננומסד — **מסדנתונים**
5. לפא — **אפל**
6. ונתבי — **ניתוב**
7. מאותינניו — **אנונימיות**
8. צתמו — **צומת**

מפתח אתגר הצופן הסודי

"שמרו אנונימיות בעזרת ניתוב בצל מאובטח"

מפתח תשובות למקרי הבוחן

A מקרה בוחן 1: זיהוי דליפת נתונים

פתרון למורה

הנחיות הערכה

תשובות התלמידים צריכות לכלול את הנקודות הבאות:

- ניתוח תרחיש: ביקורת אבטחה ארגונית מגלה שרשומות רגישות של מסד נתוני לקוחות נסחרות בשוק onion. הנתונים אינם מאונדקסים ב-Google.
- אסטרטגיה ופתרון מומלצים: מקטעים מעורבים: מסד הנתונים הפרטי שייך לרשת העמוקה (deep web) (לא מאונדקס אך מאובטח). השוק שסוחר בנתונים הגנובים נמצא ברשת האפלה (dark web) (רשת onion). איך זה קרה: האקרים עקפו את הגנות השרת, גנבו את מסד הנתונים מהרשת העמוקה ופרסמו אותו באופן אנונימי ברשת האפלה כדי להימלט ממעקב רשויות האכיפה.

B מקרה בוחן 2: אנונימיות לעומת סיכוני נוזקות

פתרון למורה

הנחיות הערכה

תשובות התלמידים צריכות לכלול את הנקודות הבאות:

- ניתוח תרחיש: אנליסט רוצה לבדוק פידים של מודיעין איומים באתר Tor. הוא מוריד את דפדפן Tor וניגש לאתר.
- אסטרטגיה ופתרון מומלצים: יתרונות: Tor מנתב תעבורה דרך שלושה צמתים ומסתיר את כתובת ה-IP הארגונית של האנליסט. סיכונים והפחתה: לקישורי רשת אפלה אין סינון מוניטין. אנליסטים חייבים להריץ את Tor בתוך מכונות וירטואליות מבודדות (VM), להשבית JavaScript בהגדרות Tor, ולהימנע מהורדת קבצים כלשהם כדי להגן על הרשת הארגונית.