نام: _____ تاریخ: _____ نمبر: _____

ڈارک ویب بمقابلہ ڈیپ ویب: سیکیورٹی اور فرق

سرچ انجن انڈیکسنگ، ڈیپ ویب ڈیٹا بیسز، Tor آنین روٹنگ، نیٹ ورک گمنامی اور خطرات

ڈارک ویب بمقابلہ ڈیپ ویب کا تعلیمی جائزہ

محفوظ شدہ
ڈیٹا کی خفیہ کاری
256 بٹ AES معیار

تعمیل شدہ
عالمی معیارات
GDPR اور CCPA فریم ورکس

زیرو ٹرسٹ
رسائی کی پالیسی
ملٹی فیکٹر تصدیق

خوش آمدید! یہ سرگرمی پیکٹ آپ کو ڈیپ ویب اور ڈارک ویب کے درمیان فرق سے متعارف کراتا ہے۔ آپ غیر انڈیکس شدہ ڈیٹا بیسز، Tor براؤزر کی Onion Routing، .onion کرپٹوگرافک ڈومینز، اور گمنامی کے سیکیورٹی خطرات کا جائزہ لیں گے۔

ورک شیٹ کے چیک پوائنٹس

- [ ] **حصہ 1-4: سائبر سیکیورٹی اور خطرات سے بچاؤ میں مہارت حاصل کریں۔**
- [ ] **حصہ 5-7: کراس ورڈ اور ورڈ سرچ پہیلیاں حل کریں۔**
- [ ] **حصہ 8-9: کیس اسٹڈیز اور سائفر چیلنج حل کریں۔**
- [ ] **حصہ 10: بنیادی اور اعلیٰ FAQ صفحات کا جائزہ لیں۔**
- [ ] **حصہ 11: 10 دلچسپ حقیقی دنیا کے حقائق دریافت کریں۔**
- [ ] **اضافی: تیزی سے سوچیں چیلنج**

VPN.com سائبر سیکیورٹی گائیڈ کھولیں

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

آپ کی ڈیپ اور ڈارک ویب کی حکمت عملی کا لرننگ روڈ میپ

- ڈیپ ویب (غیر انڈیکس شدہ ڈیٹا بیسز) کا ڈارک ویب (onion سروسز) سے موازنہ کریں۔
- سمجھیں کہ Onion Routing نیٹ ورک ٹریفک کو کیسے خفیہ کرتی اور آگے بھیجتی ہے۔
- غیر تصدیق شدہ Tor نیٹ ورک سائٹس تک رسائی کے سیکیورٹی خطرات کا جائزہ لیں۔
- تھریٹ انٹیلیجنس کرالنگ کے لیے محفوظ گیٹ وے اور سینڈ باکسنگ پالیسیاں تعینات کریں۔
- اونین سروس ڈومینز کے خفیہ کاری سے متعلق ایڈریس فارمیٹ کا تجزیہ کریں۔

ڈیپ اور ڈارک ویب گائیڈ کی ہدایات

کثیر انتخابی اور درست/غلط سوالات حل کریں، لفظوں کے ذخیرے کی مدد سے خالی جگہیں پُر کریں، تعریفوں کا ملان کریں، اور کراس ورڈ اور ورڈ سرچ پہیلیاں حل کریں۔ اپنے علم کو ڈیپ اور ڈارک ویب کی رازداری پر لاگو کریں۔ اور آخر میں اضافی سرگرمی "تیزی سے سوچیں"۔

ڈیپ ویب ڈیٹا بیس بمقابلہ ڈارک ویب اونین روٹنگ (تعارف)

ڈیپ ویب ان غیر انڈیکس شدہ صفحات پر مشتمل ہے جو پاس ورڈز اور لاگ اِنز کے پیچھے ہوتے ہیں، جیسے نجی ای میلز یا کارپوریٹ بینک پورٹلز۔ ڈارک ویب ڈیپ ویب کا ذیلی حصہ ہے جو جان بوجھ کر چھپایا گیا ہے، اور گمنام رسائی کے لیے خصوصی براؤزرز (جیسے Tor) اور onion نیٹ ورکس درکار ہوتے ہیں۔

ہر چیک پوائنٹ کو غور سے پڑھیں اور درست جواب منتخب کریں یا لکھیں۔

چیک پوائنٹ 1: کثیر انتخابی چیلنج

1. ڈیپ ویب کو سرفیس ویب سے کیا چیز ممتاز کرتی ہے؟

- A. ڈیپ ویب صفحات عوامی سرچ انجنوں میں انڈیکس نہیں ہوتے
- B. ڈیپ ویب ٹریفک غیر قانونی ہے اور قانون نافذ کرنے والے ادارے اس کی نگرانی کرتے ہیں
- C. ڈیپ ویب سائٹس تک رسائی کے لیے Tor جیسے خصوصی براؤزرز درکار ہوتے ہیں
- D. ڈیپ ویب صفحات ہمیشہ سرفیس ویب صفحات سے زیادہ تیزی سے لوڈ ہوتے ہیں

2. ڈارک ویب تک رسائی کیسے حاصل کی جاتی ہے؟

- A. اونین روٹنگ نیٹ ورکس استعمال کرنے والے مخصوص براؤزرز کے ذریعے
- B. معیاری راؤٹرز پر حسب ضرورت DNS سیٹنگز ترتیب دے کر
- C. نجی، صرف دعوت پر مبنی سرفیس ویب سرچ کنسولز کے ذریعے
- D. ایک معیاری ایڈ بلاکنگ براؤزر ایکسٹینشن انسٹال کر کے

3. کون سا ڈھانچہ ڈیپ ویب کا سب سے بڑا حصہ بناتا ہے؟

- A. پاس ورڈ سے محفوظ صارف ڈیٹا بیسز اور نجی اکاؤنٹس
- B. ممنوعہ اشیاء کی تجارت کرنے والے غیر قانونی بلیک مارکیٹ فورمز
- C. غیر خفیہ شدہ پیئر ٹو پیئر فائل شیئرنگ پروٹوکولز
- D. عوامی سرچ انجن کیش ڈیٹا بیسز

4. اونین راؤٹنگ نیٹ ورک ٹریفک کے ساتھ کیا کرتی ہے؟

- A. یہ پیکٹس کو خفیہ کرتا ہے اور انہیں متعدد ریلے کے ذریعے روٹ کرتا ہے
- B. یہ ISP نوڈز کو بائی پاس کر کے ڈاؤن لوڈ کی رفتار بڑھاتا ہے
- C. یہ ڈیوائس ہارڈ ویئر کے سیریل نمبرز کو IP ریکارڈز سے جوڑتا ہے
- D. یہ ہر کلک کے بعد ویب براؤزر کوکیز حذف کر دیتا ہے

5. کون سا ڈومین لاحقہ صرف Tor نیٹ ورکس پر استعمال ہوتا ہے؟

- A. خفیہ کاری سے متعلق .onion ٹاپ لیول ایکسٹینشن
- B. معیاری قدیم .com تجارتی ایکسٹینشن
- C. Web3 کی غیر مرکزی .eth بلاک چین ایکسٹینشن
- D. ملکی کوڈ .ai ٹیکنالوجی ایکسٹینشن

چیک پوائنٹ 2: درست یا غلط چیلنج

6 سوال (درست/غلط) 6

6. ڈیپ ویب اور ڈارک ویب ایک ہی نیٹ ورک حصے کو کہتے ہیں۔

درست غلط

7 سوال (درست/غلط) 7

7. کارپوریٹ انٹرانیٹ پورٹلز ڈیپ ویب کا حصہ ہیں۔

درست غلط

8 سوال (درست/غلط) 8

8. اونین روٹنگ ہر ٹرانزٹ نوڈ پر ڈیٹا پیکٹس کو مکمل طور پر ڈیکرپٹ کر دیتی ہے۔

درست غلط

9 سوال (درست/غلط) 9

9. ڈارک ویب تک رسائی ڈیوائسز کو میل ویئر کے بلند خطرات سے دوچار کرتی ہے۔

درست غلط

10 سوال (درست/غلط) 10

10. معیاری ویب سرچ انجن onion سائٹس کو کرال اور انڈیکس کرتے ہیں۔

درست غلط

چیک پوائنٹ 3: کلیدی اصطلاح شامل کرنا

ذیل میں ہر جملہ پڑھیں اور خالی جگہ کو ورڈ بینک سے درست اصطلاح کے ساتھ پُر کریں۔

1. نجی بینک پورٹلز غیر انڈیکسڈ _____ حصے میں موجود ہوتے ہیں۔
2. مخصوص Tor نوڈز پوشیدہ _____ سروسز کی میزبانی کرتے ہیں۔
3. Tor ویب سائٹس کرپٹوگرافک _____ ٹاپ لیول ایکسٹینشن استعمال کرتی ہیں۔
4. انکرپٹڈ کثیر پرتوں والے ٹریفک کے راستے کو _____ کہا جاتا ہے۔
5. سرفیس سرچ انجن ان صفحات کو کرال کرتے ہیں جو عوامی طور پر _____ ہوں۔
6. اونین نیٹ ورکس صارف کی _____ برقرار رکھنے کے لیے کلائنٹ IPs انکرپٹ کرتے ہیں۔

الفاظ کا بینک

انٹری نوڈ | انڈیکسڈ | اونین | ڈارک ویب | ڈیپ ویب | ڈیٹا بیس | روٹنگ | گمنامی

اپنے جوابات یہاں لکھیں:

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

چیک پوائنٹ 4: سیکیورٹی تصورات کا ملان

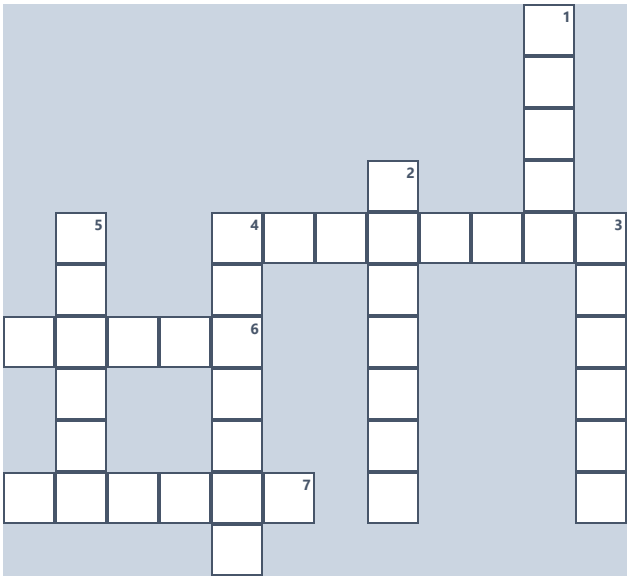
تعریفوں کا ملان

دائیں جانب کی ہر اصطلاح کو بائیں جانب کی درست تعریف سے ملائیں اور بھرے جانے والے ان پٹ باکس میں متعلقہ حرف (A-H) لکھیں۔

1. ڈیپ ویب کا حصہ	A	خفیہ کردہ نیٹ ورک حصہ جس تک صرف خصوصی براؤزرز سے رسائی ہوتی ہے۔
2. ڈارک ویب پورٹل	B	ڈیٹا کو تہوں میں خفیہ کر کے تین نوڈز کے ذریعے آگے بھیجنا۔
3. اونین ایکسٹینشن	C	غیر انڈیکس شدہ سسٹم ریکارڈز کی میزبانی کرنے والا محفوظ بیک اینڈ اسٹوریج۔
4. Tor روٹنگ	D	Tor نیٹ ورکس پر استعمال ہونے والا کرپٹوگرافک ٹاپ لیول ڈومین لاحقہ۔
5. انڈیکس شدہ صفحات	E	انٹری پوائنٹ نوڈ جو Tor نیٹ ورک تک رسائی کے لیے استعمال ہوتا ہے۔
6. صارف کی گمنامی	F	سرفیس ویب کا وہ مواد جو Google پر مرتب اور قابل تلاش ہے۔
7. نجی ڈیٹا بیس	G	کلائنٹ کے عوامی IP ایڈریسز کو سرورز سے پوشیدہ رکھنا۔
8. انٹری گیٹ وے	H	غیر انڈیکس شدہ ویب مواد جیسے نجی لاگ اِنز، ای میلز اور ڈیٹا بیس ریکارڈز۔

چیک پوائنٹ 5: کراس ورڈ پہیلی

فعال سفید خانوں میں حروف ٹائپ کر کے کراس ورڈ پہیلی حل کریں۔ نمبر نیچے دیے گئے سراغوں سے مطابقت رکھتے ہیں۔



افقی

3. Tor نیٹ ورک تک رسائی کے لیے استعمال ہونے والا داخلی نوڈ (8)

6. ڈیٹا کو پرتوں میں انکرپٹ کر کے تین نوڈز کے ذریعے آگے بھیجنا (5)

7. غیر انڈیکسڈ ویب مواد جیسے نجی لاگ اِن، ای میلز اور ڈیٹا بیس ریکارڈز (6)

عمودی

1. کرپٹوگرافک ٹاپ لیول ڈومین لاحقہ جو Tor نیٹ ورکس پر استعمال ہوتا ہے (5)

2. محفوظ بیک اینڈ اسٹوریج جو غیر انڈیکسڈ سسٹم ریکارڈز کی میزبانی کرتی ہے (7)

3. سرفیس ویب کا وہ مواد جو گوگل پر مرتب اور قابل تلاش ہو (6)

4. انکرپٹڈ نیٹ ورک کا حصہ جس تک صرف خصوصی براؤزرز سے رسائی ممکن ہے (7)

5. کلائنٹ کے عوامی IP ایڈریسز کو سرورز سے پوشیدہ رکھنا (6)

چیک پوائنٹ 5 – متبادل سرگرمی: قابلِ رسائی کراس ورڈ سراغ

اسکرین ریڈر اور کی بورڈ استعمال کرنے والے صارفین نیچے دیے گئے ٹیکسٹ فیلڈز میں کراس ورڈ کے جوابات براہ راست ٹائپ کر سکتے ہیں۔

افقی

3 افقی: Tor نیٹ ورک تک رسائی کے لیے استعمال ہونے والا داخلی نوڈ (8 حروف):

6 افقی: ڈیٹا کو پرتوں میں انکرپٹ کر کے تین نوڈز کے ذریعے آگے بھیجنا (5 حروف):

7 افقی: غیر انڈیکسڈ ویب مواد جیسے نجی لاگ اِن، ای میلز اور ڈیٹا بیس ریکارڈز (6 حروف):

عمودی

1 عمودی: کرپٹوگرافک ٹاپ لیول ڈومین لاحقہ جو Tor نیٹ ورکس پر استعمال ہوتا ہے (5 حروف):

2 عمودی: محفوظ بیک اینڈ اسٹوریج جو غیر انڈیکسڈ سسٹم ریکارڈز کی میزبانی کرتی ہے (7 حروف):

3 عمودی: سرفیس ویب کا وہ مواد جو گوگل پر مرتب اور قابل تلاش ہو (6 حروف):

4 عمودی: انکرپٹڈ نیٹ ورک کا حصہ جس تک صرف خصوصی براؤزرز سے رسائی ممکن ہے (7 حروف):

5 عمودی: کلائنٹ کے عوامی IP ایڈریسز کو سرورز سے پوشیدہ رکھنا (6 حروف):

چیک پوائنٹ 6: پوشیدہ الفاظ کی تلاش

نیچے گرڈ میں چھپی 8 اہم اصطلاحات تلاش کریں۔ الفاظ افقی، عمودی یا ترچھے ہو سکتے ہیں۔

ن	ا	س	گ	ج	ر	ک	ب	گ	س	ت	ن	ے	س	ن
ج	ش	ا	ت	ت	ڈ	ا	ی	ج	گ	ر	م	ا	ک	پ
ڈ	م	ب	ت	ر	و	گ	و	ٹ	ک	ٹ	ش	ن	ی	چ
ل	ا	ہ	م	ن	ک	ڈ	پ	چ	د	و	د	ج	ڈ	ا
گ	ر	ٹ	ی	ے	گ	ڈ	ی	ش	ا	ی	ر	ت	ن	ر
ی	و	ن	گ	ش	ل	ش	ڈ	ٹ	ن	چ	م	پ	ا	س
ا	ٹ	ب	د	س	ت	ی	ن	م	ٹ	و	پ	ک	ل	ی
ر	ن	ن	ی	ر	ٹ	ے	ر	س	ر	ے	گ	ب	ب	م
گ	گ	ل	ر	ا	ش	ش	ج	ت	ی	د	ش	ل	ت	ا
ل	ن	ب	ب	ج	ن	و	م	م	ن	ل	ش	ش	ج	ن
پ	ہ	ی	ب	م	ج	ک	ب	ی	و	ک	ر	ا	ڈ	م
ش	س	پ	ڈ	ج	ر	ٹ	ہ	ڈ	ڈ	ب	و	ڈ	ن	گ
ک	ت	ا	ر	پ	ک	ڈ	ا	ب	و	ب	گ	ی	ل	ت
ل	ٹ	ن	ڈ	م	ج	ت	ش	ل	م	پ	ج	ج	ٹ	ت
م	و	م	ر	ل	ے	و	گ	ش	گ	ل	ا	ا	ٹ	ہ

الفاظ کی فہرست

ڈیپویب ڈارکویب اونین روٹنگ انڈیکس گمنامی ڈیٹابیس انٹرینوڈ

چیک پوائنٹ 6 – متبادل سرگرمی: قابلِ رسائی الفاظ کا ملان

ورڈ سرچ کی 8 اصطلاحات میں سے ہر ایک کو اس کی درست تعریف سے ملائیں اور خالی جگہ میں حرف (A-H) لکھیں۔

اصطلاحات
A. ڈیپویب
B. ڈارکویب
C. اونین
D. روٹنگ
E. انڈیکس
F. گمنامی
G. ڈیٹابیس
H. انٹرینوڈ

تعریفیں اور ملان کے خانے	
1. کلائنٹ کے عوامی IP ایڈریسز کو سرورز سے پوشیدہ رکھنا۔	
2. محفوظ بیک اینڈ اسٹوریج جو غیر انڈیکسڈ سسٹم ریکارڈز کی میزبانی کرتی ہے۔	
3. ڈیٹا کو پرتوں میں انکرپٹ کر کے تین نوڈز کے ذریعے آگے بھیجنا۔	
4. غیر انڈیکسڈ ویب مواد جیسے نجی لاگ اِن، ای میلز اور ڈیٹا بیس ریکارڈز۔	
5. انکرپٹڈ نیٹ ورک کا حصہ جس تک صرف خصوصی براؤزرز سے رسائی ممکن ہے۔	
6. کرپٹوگرافک ٹاپ لیول ڈومین لاحقہ جو Tor نیٹ ورکس پر استعمال ہوتا ہے۔	
7. Tor نیٹ ورک تک رسائی کے لیے استعمال ہونے والا داخلی نوڈ۔	
8. سرفیس ویب کا وہ مواد جو گوگل پر مرتب اور قابل تلاش ہو۔	

چیک پوائنٹ 7: الجھے الفاظ کا چیلنج

سائبر سیکیورٹی کے اہم تصورات اور اصطلاحات ظاہر کرنے کے لیے نیچے دیے گئے حروف کو درست ترتیب میں لائیں۔ اپنے جوابات دیے گئے ان پٹ باکسز میں لکھیں۔

1. پ ڈ و ی ب ی
2. ا ن ی ن و
3. ا ڈ ی س ک ن
4. س ی ب ا ی ڈ ٹ
5. و ب ک ر ڈ ی ا
6. ن ر ٹ گ و
7. م گ ا ی ن م
8. ر ن ی ڈ ا و ن ٹ

اضافی سرگرمی: تیزی سے سوچیں

ہر زمرے کے لیے 3 جوابات لکھیں۔ جو سب سے پہلے فہرست مکمل کرے وہ جیتتا ہے۔

1	ڈارک ویب سے دور رہنے کی وجوہات			
2	وہ چیزیں جو سرچ انجن نہیں ڈھونڈ سکتا			
3	وہ ڈیوائسز جنہیں ہیک کیا جا سکتا ہے			
4	Tor استعمال کرنے کی قانونی وجوہات			
5	سافٹ ویئر اپ ڈیٹ کرنے کی وجوہات			
6	ای میل میں انتباہی علامات			
7	وہ چیزیں جو ڈارک ویب پر غیر قانونی طور پر فروخت ہوتی ہیں			
8	وہ لوگ جن سے آپ آئی ٹی مدد مانگ سکتے ہیں			
9	محفوظ عادات جو آپ آج شروع کر سکتے ہیں			
10	ڈیٹا لیک کے بعد کرنے کے کام			
11	وہ چیزیں جو ڈیپ ویب کا حصہ ہیں			
12	وہ سائٹس جو آپ لاگ ان کے ساتھ استعمال کرتے ہیں			
13	گمنامی سے متعلق الفاظ			
14	وہ معلومات جو آپ کو کبھی شیئر نہیں کرنی چاہئیں			
15	وہ چیزیں جو 'سطح کے نیچے' ہوتی ہیں			

چیک پوائنٹ 8: سائبر سیکیورٹی کیس اسٹڈیز

جو تصورات آپ نے سیکھے ہیں انہیں نیچے دیے گئے حقیقی منظرناموں کو حل کرنے میں استعمال کریں۔

کیس اسٹڈی 1: ڈیٹا لیک کی نشاندہی



منظرنامہ: ایک کارپوریٹ سیکیورٹی آڈٹ سے پتا چلتا ہے کہ کلائنٹ کے حساس ڈیٹا بیس ریکارڈز کا ایک onion مارکیٹ پلیس پر لین دین ہو رہا ہے۔ یہ ڈیٹا Google پر انڈیکس نہیں ہے۔

بحث کا سوال: وضاحت کریں کہ ویب کے کون سے حصے اس میں شامل ہیں اور یہ لیک کیسے ہوا۔

کیس اسٹڈی 2: گمنامی اور میل ویئر کے خطرات کا موازنہ



منظرنامہ: ایک تجزیہ کار Tor ویب سائٹ پر خطرے کی انٹیلی جنس فیڈز کی جانچ کرنا چاہتا ہے۔ وہ Tor براؤزر ڈاؤن لوڈ کر کے سائٹ تک رسائی حاصل کرتا ہے۔

بحث کا سوال: گمنامی کے فوائد کا جائزہ لیں اور میل ویئر کی روک تھام کے اقدامات بیان کریں۔

چیک پوائنٹ 9: سائفر حل کریں

سائبر سیکیورٹی پیشہ ور نیٹ ورک اثاثوں کو آن لائن خطرات پیدا کرنے والوں سے بچاتا ہے۔ نیچے دی گئی حرف سے عدد کی کلید استعمال کر کے خالی جگہوں میں متعلقہ حروف لکھ کر پیغام ڈی کرپٹ کریں۔

حرف سے عدد خفیہ کاری کی کلید

ا=1 ب=2 پ=3 ت=4 ٹ=5 ث=6 ج=7 چ=8 ح=9 خ=10 د=11 ڈ=12 ذ=13

ر=14 ڑ=15 ز=16 ژ=17 س=18 ش=19 ص=20 ض=21 ط=22 ظ=23 ع=24 غ=25 ف=26

ق=27 ک=28 گ=29 ل=30 م=31 ن=32 ں=33 و=34 ہ=35 ھ=36 ی=37 ے=38 ئ=39

37	28		26	14	1	20		38	18		29	32	5	34	14		32	37	32	34	1

37	31	1	32	31	29

ڈی کوڈ شدہ پیغام:

ٹپ: ہر نمبر اوپر دی گئی کلید کے ایک اردو حرف کو ظاہر کرتا ہے۔

چیک پوائنٹ 10: سائبر سیکیورٹی عمومی سوالات – بنیادی (حصہ A)

آن لائن خطرات کی روک تھام کے بارے میں عام سوالات اور جوابات کا جائزہ لیں۔

Q1: ڈیپ ویب کیا ہے؟

ڈیپ ویب ان تمام ویب صفحات پر مشتمل ہے جنہیں سرچ انجن انڈیکس نہیں کر سکتے، بشمول آن لائن بینکاری، ای میل ڈیٹا بیسز اور پے وال والے جرائد۔

Q2: ڈارک ویب کیا ہے؟

ڈارک ویب ڈیپ ویب کا ایک چھوٹا ذیلی حصہ ہے جو جان بوجھ کر چھپایا گیا ہے اور جس تک onion نیٹ ورکس استعمال کرنے والے خصوصی براؤزرز کے ذریعے ہی رسائی ہوتی ہے۔

Q3: سرچ انجن صفحات کو انڈیکس کیسے کرتے ہیں؟

انجن خودکار پروگرام (اسپائیڈرز) چلاتے ہیں جو عوامی لنکس کی پیروی کرتے ہیں، اور ان صفحات کو انڈیکس کرتے ہیں جو روبوٹ ہدایات سے کرالنگ بلاک نہیں کرتے۔

Q4: آن لائن بینکنگ کو ڈیپ ویب کا حصہ کیوں سمجھا جاتا ہے؟

بینکنگ پورٹلز لاگ اِن اور پاس ورڈز کے پیچھے ہوتے ہیں، جو عوامی سرچ انجنز کو اکاؤنٹ اسٹیٹمنٹ کے صفحات انڈیکس کرنے سے روکتے ہیں۔

Q5: Tor براؤزر Onion Routing کیا ہے؟

اونین روٹنگ ترسیل کا ایسا طریقہ ہے جو ٹریفک کو تہوں میں انکرپٹ کرتا ہے اور صارف کے IP ایڈریسز چھپانے کے لیے اسے متعدد ریلے سے گزارتا ہے۔

چیک پوائنٹ 10: سائبر سیکیورٹی عمومی سوالات – بنیادی (حصہ B)

آن لائن خطرات کی روک تھام کے بارے میں عام سوالات اور جوابات کا جائزہ لیں۔

Q6: کیا ڈارک ویب تک رسائی غیر قانونی ہے؟

نہیں۔ ڈارک ویب تک رسائی زیادہ تر ممالک میں قانونی ہے، اگرچہ غیر قانونی مارکیٹ پلیسز یا سائبر سرگرمیوں میں حصہ لینا ممنوع ہے۔

Q7: ڈارک ویب سائٹس لوڈ ہونے میں سست کیوں ہوتی ہیں؟

ٹریفک کم از کم تین عالمی ریلیز (انٹری، مڈل، ایگزٹ) کے ذریعے روٹ اور ڈی کرپٹ ہوتا ہے، جس سے ترسیلی تاخیر بڑھ جاتی ہے۔

Q8: .onion ڈومین سفکس کا کیا مطلب ہے؟

یہ Tor نیٹ ورکس پر استعمال ہونے والا مخصوص ٹاپ لیول ڈومین لاحقہ ہے، جو معیاری DNS سرورز کے بجائے کرپٹوگرافک طور پر بنائے گئے ایڈریسز کی طرف اشارہ کرتا ہے۔

Q9: ڈارک ویب لنکس سے کون سے خطرات وابستہ ہیں؟

سائٹس میں کوئی سیکیورٹی اسکریننگ نہیں ہوتی، جس سے صارفین میل ویئر انفیکشن کی بلند شرح، فشنگ اسکرپٹس اور ٹرانزیکشن فراڈ کا شکار ہو سکتے ہیں۔

Q10: Tor نیٹ ورک روٹنگ پروٹوکول کس نے بنایا؟

یہ ٹیکنالوجی اصل میں 1990 کی دہائی میں امریکی نیول ریسرچ لیبارٹری نے سرکاری مواصلات کے تحفظ کے لیے تیار کی تھی۔

چیک پوائنٹ 10: سیکیورٹی عمومی سوالات – اعلیٰ (حصہ C)

سیکیورٹی فریم ورکس، میل ویئر تجزیے اور ڈیٹا کمپلائنس کے جدید تکنیکی پہلوؤں کا جائزہ لیں۔

Q1: درمیانی نوڈز Tor کی گمنامی کا تحفظ کیسے کرتے ہیں؟

ہر نوڈ روٹنگ ڈیٹا کی صرف ایک تہہ کھولتا ہے اور صرف پچھلا اور اگلا ہاپ جانتا ہے، ماخذ اور منزل دونوں کبھی نہیں۔

Q2: ایگزٹ نوڈ کا کیا کردار ہے؟

ایگزٹ نوڈ خفیہ کاری کی آخری تہہ کو ڈی کرپٹ کرتا ہے اور ٹریفک کو عوامی منزل سرور یا onion سرور تک بھیج دیتا ہے۔

Q3: Tor برجز گیٹ وے کیا ہے؟

برجز غیر درج شدہ Tor انٹری ریلے ہیں جو ان خطوں میں ISP کی رکاوٹوں اور سنسرشپ کو بائی پاس کرنے کے لیے استعمال ہوتے ہیں جہاں Tor براؤزر تک رسائی محدود ہے۔

Q4: ڈارک ویب کے عناصر کرپٹو کرنسی کا کیسے استحصال کرتے ہیں؟

عناصر ڈارک مارکیٹ پلیسز پر مالی لین دین کرنے کے لیے گمنام کرپٹو کرنسیاں استعمال کرتے ہیں تاکہ معیاری بینکاری لین دین کی جانچ سے بچ سکیں۔

Q5: عام سرچ انجن گہرے ڈیٹا بیسز کو کرال کرنے میں ناکام کیوں رہتے ہیں؟

کرالرز لاگ اِن کریڈینشلز درج نہیں کر سکتے، سیکیورٹی CAPTCHAs حل نہیں کر سکتے، یا ڈیپ ڈیٹا بیسز تک رسائی کے لیے درکار بیک اینڈ SQL کوئری اسکرپٹس نہیں چلا سکتے۔

چیک پوائنٹ 10: سیکیورٹی عمومی سوالات – اعلیٰ (حصہ D)

سیکیورٹی فریم ورکس، میل ویئر تجزیے اور ڈیٹا کمپلائنس کے جدید تکنیکی پہلوؤں کا جائزہ لیں۔

Q6: Tor نیٹ ورکس میں ڈائریکٹری سرور کیا ہے؟

یہ ایک قابل اعتماد سرور ہے جو فعال انٹری، مڈل اور ایگزٹ ریلیز کی فہرست رکھتا ہے جنہیں کلائنٹس روٹنگ پاتھ بنانے کے لیے استعمال کرتے ہیں۔

Q7: بدنیت عناصر ایگزٹ نوڈ سنفنگ کیسے کرتے ہیں؟

روگ ایگزٹ نوڈ آپریٹرز Tor نیٹ ورک سے نکلتے وقت غیر خفیہ شدہ HTTP ٹریفک کو روک سکتے ہیں اور صارف نام اور کوکیز چرا سکتے ہیں۔

Q8: Tor اور I2P میں کیا فرق ہے؟

Tor عوامی ویب رسائی کے لیے مرکزی ریلے ڈائریکٹری اور ایگزٹ نوڈز استعمال کرتا ہے، جبکہ I2P اندرونی ہوسٹنگ کے لیے غیر مرکزی پیئر ٹو پیئر ڈھانچہ استعمال کرتا ہے۔

Q9: قانون نافذ کرنے والے ادارے ڈارک ویب مارکیٹوں کو کیسے ٹریک کرتے ہیں؟

ایجنسیاں بلاک چین تجزیہ استعمال کرتی ہیں، فزیکل سرور ہوسٹنگ سیٹ اپ کا سراغ لگاتی ہیں، اور آپریٹرز کی شناخت کے لیے فریبی کارروائیاں چلاتی ہیں۔

Q10: DNS لیک کلائنٹ کی گمنامی کو کیسے متاثر کرتا ہے؟

DNS لیک اس وقت ہوتے ہیں جب براؤزر کی DNS کوئریز خفیہ کردہ Tor نیٹ ورک کے ذریعے بھیجے جانے کے بجائے براہِ راست مقامی ISP کے ذریعے بھیجی جاتی ہیں۔

حصہ 11: 10 حقیقی دنیا کے سائبر سیکیورٹی حقائق اور بصیرتیں

سیکیورٹی خلاف ورزیوں، دفاعی نظاموں اور تعمیل کے معیارات کے بارے میں حقیقی دنیا کے حقائق کا جائزہ لیں۔

1. سیکیورٹی بصیرت

ڈیپ ویب قابلِ تلاش سرفیس ویب سے کہیں بڑا ہے، کیونکہ زیادہ تر مواد لاگ اِنز اور ڈیٹا بیسز کے پیچھے ہوتا ہے۔

2. سیکیورٹی بصیرت

ڈارک ویب ڈیپ ویب کا ایک چھوٹا، جان بوجھ کر چھپایا گیا حصہ ہے، جس تک Tor جیسے ٹولز کے ذریعے پہنچا جاتا ہے۔

3. سیکیورٹی بصیرت

Tor روٹنگ ڈیٹا پیکٹس کو تین بار خفیہ کرتی ہے، اور ہر ریلے نوڈ پر پیاز کی طرح خفیہ کاری کی تہیں اتارتی جاتی ہیں۔

4. سیکیورٹی بصیرت

Tor کی ابتدا امریکی نیول ریسرچ لیب کے چلائے گئے onion روٹنگ منصوبے سے ہوئی، اور اس کا کوڈ مفت سافٹ ویئر کے طور پر جاری کیا گیا۔ [1]

5. سیکیورٹی بصیرت

اونین ایڈریسز 56 حروف کی الفا نیومیرک اسٹرنگز ہوتے ہیں جو پبلک کی جوڑوں سے کرپٹوگرافک طور پر بنائے جاتے ہیں۔

6. سیکیورٹی بصیرت

ایگزٹ نوڈز کلیئر ٹیکسٹ ٹریفک پڑھ سکتے ہیں، یعنی محفوظ سیشن ڈیٹا کے لیے Tor پر بھی TLS/HTTPS درکار ہے۔

7. سیکیورٹی کی بصیرت

انٹرا نیٹ سائٹس، کلاؤڈ ڈرائیوز اور نجی ڈیٹا بیسز ڈیپ ویب پر ڈیٹا اسٹوریج کے سب سے بڑے حصوں کی نمائندگی کرتے ہیں۔

8. سیکیورٹی کی بصیرت

DuckDuckGo جیسے خصوصی سرچ انجن Tor نیٹ ورکس پر گمنام تلاش کی اجازت دینے کے لیے onion پورٹلز چلاتے ہیں۔

9. سیکیورٹی کی بصیرت

2 ملین سے زیادہ صارفین روزانہ سنسرشپ سے بچنے اور مواصلات کی رازداری برقرار رکھنے کے لیے Tor نیٹ ورک سے جڑتے ہیں۔

10. سیکیورٹی بصیرت

عالمی قانون نافذ کرنے والی کارروائیاں (جیسے Operation Bayonet) ہوسٹنگ ہارڈ ویئر ضبط کر کے بڑی ڈارک مارکیٹ پلیسز کو بند کر دیتی ہیں۔

تکنیکی حوالہ جات اور ماخذ

مطالعاتی گائیڈ اور انٹرایکٹو پہیلیاں عالمی NIST، OWASP اور ڈیٹا پرائیویسی کمپلائنس معیارات سے مرتب کی گئی ہیں۔

علمی اور صنعتی حوالہ جات

[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

جوابی کلید: چیک پوائنٹ 1 – کثیر انتخابی

1 سرچ انڈیکسنگ — ڈیپ ویب — درست جواب: A

تدریسی نوٹ

ڈیپ ویب کے صفحات لاگ اِن کی دیواروں اور ڈیٹا بیسز کے پیچھے ہوتے ہیں، جس سے سرچ اسپائیڈرز انہیں کرال نہیں کر پاتے۔ حوالہ: IETF RFC 3986۔

2 Tor تک رسائی — ڈارک ویب — درست جواب: A

تدریسی نوٹ

ڈارک ویب چھپی ہوئی onion سروسز پر مشتمل ہے جن تک صرف Tor جیسے براؤزرز کے ذریعے رسائی ممکن ہے۔ حوالہ: IETF RFC 3986۔

3 ڈیپ ڈیٹا بیسز — ڈیٹا بیسز — درست جواب: A

تدریسی نوٹ

پاس ورڈ سے محفوظ اکاؤنٹس اور کارپوریٹ ریکارڈز ڈیپ ویب کا سب سے بڑا حصہ بناتے ہیں۔ حوالہ: NIST Digital Identity۔

4 اونین روٹنگ — TOR نیٹ ورک — درست جواب: A

تدریسی نوٹ

اونین روٹنگ ڈیٹا پیکٹس کو تہوں میں انکرپٹ کرتی ہے اور گمنامی کے لیے انہیں متعدد نوڈز سے گزارتی ہے۔ حوالہ: IETF RFC 3986۔

5 اونین ڈومین — لاحقہ — درست جواب: A

تدریسی نوٹ

کرپٹوگرافک.onion ڈومین لاحقہ عوامی DNS کے بغیر Tor کے اندر ہی ٹریفک روٹ کرتا ہے۔ حوالہ: IETF RFC 3986۔

جوابی کلید: چیک پوائنٹ 2 – درست یا غلط

6 ویب سیگمنٹس — ساخت — درست جواب: غلط

تدریسی نوٹ

ڈیپ ویب تمام غیر انڈیکس شدہ صفحات کا احاطہ کرتا ہے، جبکہ ڈارک ویب ایک چھوٹا، خفیہ کردہ onion ذیلی حصہ ہے۔ حوالہ: IETF RFC 3986۔

7 کارپوریٹ انٹرانیٹس — ڈیپ ویب — درست جواب: درست

تدریسی نوٹ

انٹرا نیٹ سائٹس پاس ورڈ پورٹلز کے پیچھے ہوتی ہیں اور انڈیکس نہیں ہوتیں، یعنی وہ ڈیپ ویب سے تعلق رکھتی ہیں۔ حوالہ: NIST Digital Identity۔

8 تہہ دار خفیہ کاری — ریلے — درست جواب: غلط

تدریسی نوٹ

اونین ریلے صارف کی گمنامی کی حفاظت کے لیے صرف ایک روٹنگ تہہ ڈیکرپٹ کرتے ہیں، پورا پیکٹ کبھی نہیں۔ حوالہ: IETF RFC 3986۔

9 میل ویئر کا خطرہ — خطرات — درست جواب: درست

تدریسی نوٹ

ڈارک ویب مارکیٹ پلیسز میں کوئی سیکیورٹی فلٹرنگ نہیں ہوتی، جس سے میل ویئر انفیکشن کے شدید خطرات ہوتے ہیں۔ حوالہ: Center for Internet Security (CIS)۔

10 سوال 10 — درست جواب: غلط

تدریسی نوٹ

عام سرچ انجن کرالرز Tor استعمال نہیں کرتے، اس لیے وہ .onion سائٹس تک نہیں پہنچ سکتے اور انہیں انڈیکس نہیں کر سکتے۔

الفاظ کی کلید اور درجہ بندی کا معیار

استاد کی گریڈنگ روبرک: ہر درست ملان (کل 8 نمبر) اور سیاقی اصطلاح (کل 6 نمبر) کے لیے 1 نمبر دیں۔

چیک پوائنٹ 4: جوابی کلید – تصورات کا ملان

H 1. ڈیپ ویب کا حصہ	A 2. ڈارک ویب پورٹل	D 3. اونین ایکسٹینشن	B 4. Tor روٹنگ
F 5. انڈیکس شدہ صفحات	G 6. صارف کی گمنامی	C 7. نجی ڈیٹا بیس	E 8. انٹری گیٹ وے

چیک پوائنٹ 3: جوابی کلید – اہم اصطلاحات

1 ڈیپ ویب	2 ڈارک ویب	3 اونین	4 روٹنگ
5 انڈیکسڈ	6 گمنامی		

چیک پوائنٹ 6 – متبادل سرگرمی: جوابی کلید – الفاظ کا ملان

1 F – گمنامی	2 G – ڈیٹابیس	3 D – روٹنگ	4 A – ڈیپویب
5 B – ڈارکویب	6 C – اونین	7 H – انٹرینوڈ	8 E – انڈیکس

اساتذہ کے لیے بحث کے نوٹس

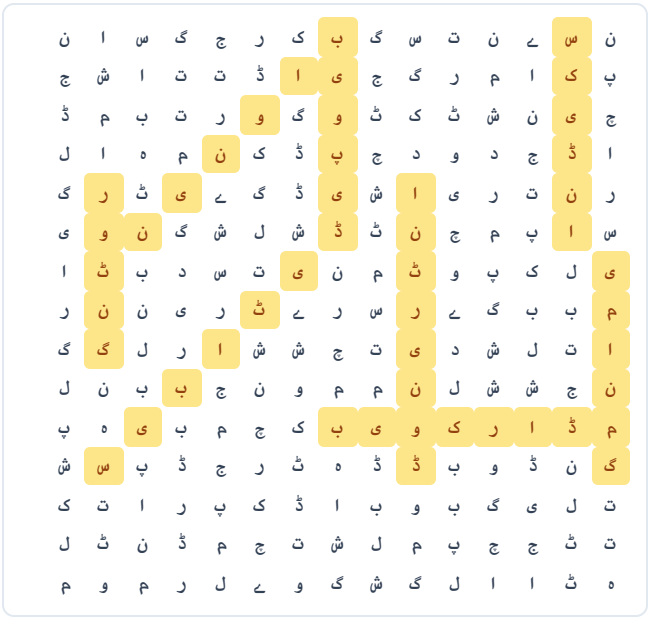
اہم اصطلاحات:
یقینی بنائیں کہ طلبہ ڈیپ ویب کا حصہ، ڈارک ویب پورٹل اور اونین ایکسٹینشن کو اپنے الفاظ میں سمجھا سکیں اور ہر ایک کی مثال دے سکیں۔

کیس اسٹڈیز:
طلبہ سے کہیں کہ اپنی سفارشات کو ورک شیٹ کے حقائق پر مبنی رکھیں، ذاتی رائے پر نہیں۔

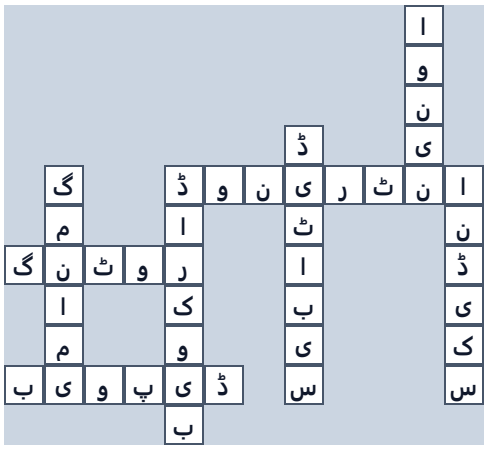
ماخذ کی جانچ:
طلبہ سے کہیں کہ ورک شیٹ کے ماخذ میں کم از کم ایک دعوے کی تصدیق کریں، اور اس پر بات کریں کہ اعداد و شمار، قیمتیں اور قواعد وقت کے ساتھ کیوں بدل سکتے ہیں۔

پہیلیوں کی کلیدیں اور استاد کے نوٹس

الفاظ کی تلاش کا حل



کراس ورڈ کا حل



کراس ورڈ حل کے لیے استاد کی گائیڈ

افقی

3 افقی: انٹرینوڈ Tor نیٹ ورک تک رسائی کے لیے استعمال ہونے والا داخلی نوڈ (8 حروف)

6 افقی: روٹنگ ڈیٹا کو پرتوں میں انکرپٹ کر کے تین نوڈز کے ذریعے آگے بھیجنا (5 حروف)

7 افقی: ڈیپویب غیر انڈیکسڈ ویب مواد جیسے نجی لاگ اِن، ای میلز اور ڈیٹا بیس ریکارڈز (6 حروف)

عمودی

1 عمودی: اونین کرپٹوگرافک ٹاپ لیول ڈومین لاحقہ جو Tor نیٹ ورکس پر استعمال ہوتا ہے (5 حروف)

2 عمودی: ڈیٹابیس محفوظ بیک اینڈ اسٹوریج جو غیر انڈیکسڈ سسٹم ریکارڈز کی میزبانی کرتی ہے (7 حروف)

3 عمودی: انڈیکس سرفیس ویب کا وہ مواد جو گوگل پر مرتب اور قابل تلاش ہو (6 حروف)

4 عمودی: ڈارکویب انکرپٹڈ نیٹ ورک کا حصہ جس تک صرف خصوصی براؤزرز سے رسائی ممکن ہے (7 حروف)

5 عمودی: گمنامی کلائنٹ کے عوامی IP ایڈریسز کو سرورز سے پوشیدہ رکھنا (6 حروف)

الفاظ کی ترتیب اور سائفر حل کی کلید

الفاظ کی ترتیب درست کرنے کی سرگرمی اور Secret Cipher Challenge کی گریڈنگ کلید۔

الفاظ کی ترتیب درست کرنے کی کلید

1. پڈوبی — ڈیپویب
2. انینو — اونین
3. اڈیسکن — انڈیکس
4. سیبایڈٹ — ڈیٹابیس
5. ویکرڈیا — ڈارکویب
6. نرٹگو — روٹنگ
7. مگاینم — گمنامی
8. رنیڈاونٹ — انٹرینوڈ

خفیہ سائفر چیلنج کی کلید

"اونین روٹنگ سے صارف کی گمنامی"

کیس اسٹڈیز کی جوابی کلید

A کیس اسٹڈی 1: ڈیٹا لیک کی نشاندہی

استاد کا حل

گریڈنگ کی ہدایت

طلبہ کے جوابات میں درج ذیل نکات شامل ہونے چاہییں:

- منظرنامے کا تجزیہ: ایک کارپوریٹ سیکیورٹی آڈٹ میں پتا چلتا ہے کہ حساس کلائنٹ ڈیٹا بیس ریکارڈز اونین مارکیٹ پلیس پر فروخت ہو رہے ہیں۔ ڈیٹا Google پر انڈیکس نہیں ہے۔
- تجویز کردہ حکمت عملی اور حل: شامل حصے: نجی ڈیٹا بیس ڈیپ ویب (غیر انڈیکس شدہ مگر محفوظ) سے تعلق رکھتا ہے۔ چوری شدہ ڈیٹا کی تجارت کرنے والی مارکیٹ ڈارک ویب (اونین نیٹ ورک) پر ہے۔ یہ کیسے ہوا: ہیکرز نے سرور کے دفاع کو بائی پاس کیا، ڈیپ ویب سے ڈیٹا بیس چرایا، اور قانون نافذ کرنے والے اداروں کی نگرانی سے بچنے کے لیے اسے ڈارک ویب پر گمنام طور پر لسٹ کر دیا۔

B کیس اسٹڈی 2: گمنامی اور میل ویئر کے خطرات کا موازنہ

استاد کا حل

گریڈنگ کی ہدایت

طلبہ کے جوابات میں درج ذیل نکات شامل ہونے چاہییں:

- منظرنامے کا تجزیہ: ایک تجزیہ کار Tor ویب سائٹ پر تھریٹ انٹیلی جنس فیڈز چیک کرنا چاہتا ہے۔ وہ Tor براؤزر ڈاؤن لوڈ کرتا ہے اور سائٹ تک رسائی حاصل کرتا ہے۔
- تجویز کردہ حکمت عملی اور حل: فوائد: Tor ٹریفک کو تین نوڈز کے ذریعے روٹ کرتا ہے، جس سے تجزیہ کار کا کارپوریٹ IP چھپ جاتا ہے۔ خطرات اور تدارک: ڈارک ویب لنکس کی ساکھ کی کوئی جانچ نہیں ہوتی۔ تجزیہ کاروں کو Tor الگ تھلگ ورچوئل مشینوں (VMs) کے اندر چلانا چاہیے، Tor سیٹنگز میں JavaScript بند کرنا چاہیے، اور کارپوریٹ نیٹ ورک کے تحفظ کے لیے کوئی بھی فائل ڈاؤن لوڈ کرنے سے گریز کرنا چاہیے۔