नाम: _____ दिनांक: _____ अंक: _____

डार्क वेब बनाम डीप वेब: सुरक्षा और अंतर

सर्च इंजन इंडेक्सिंग, डीप वेब डेटाबेस, Tor ओनियन रूटिंग, नेटवर्क गुमनामी और जोखिम

डार्क वेब बनाम डीप वेब सीखने का अवलोकन

सुरक्षित किया गया
डेटा एन्क्रिप्शन
256-बिट AES मानक

अनुपालक
वैश्विक मानक
GDPR और CCPA फ़्रेमवर्क

ज़ीरो-ट्रस्ट
एक्सेस नीति
मल्टी-फ़ैक्टर ऑथेंटिकेशन

स्वागत है! यह गतिविधि पैकेट आपको डीप वेब और डार्क वेब के बीच अंतरों से परिचित कराता है। आप अनइंडेक्स्ड डेटाबेस, Tor ब्राउज़र ऑनियन रूटिंग, .onion क्रिप्टोग्राफ़िक डोमेन और गुमनामी से जुड़े सुरक्षा जोखिमों का अध्ययन करेंगे।

वर्कशीट चेकपॉइंट

- [ ] **भाग 1-4: साइबर सुरक्षा और खतरों की रोकथाम में महारत हासिल करें।**
- [ ] **भाग 5-7: क्रॉसवर्ड और वर्ड सर्च पहेलियाँ हल करें।**
- [ ] **भाग 8-9: केस स्टडी और कूट संदेश की चुनौती हल करें।**
- [ ] **भाग 10: बुनियादी और उन्नत FAQ पेज देखें।**
- [ ] **भाग 11: 10 रोचक वास्तविक तथ्यों को जानें।**
- [ ] **अतिरिक्त: झटपट सोचें चुनौती।**

VPN.com साइबर सुरक्षा गाइड खोलें

URL: https://www.vpn.com/hi/saibhar-suraksha/dark-web-vs-deep-web/

आपका डीप और डार्क वेब रणनीति लर्निंग रोडमैप

- डीप वेब (गैर-इंडेक्स्ड डेटाबेस) की तुलना डार्क वेब (onion सेवाएँ) से करें।
- समझें कि Onion Routing नेटवर्क ट्रैफ़िक को कैसे एन्क्रिप्ट और रिले करती है।
- असत्यापित Tor नेटवर्क साइटों तक पहुँचने के सुरक्षा जोखिमों का मूल्यांकन करें।
- थ्रेट इंटेलिजेंस क्रॉलिंग के लिए सुरक्षित गेटवे और सैंडबॉक्सिंग नीतियाँ तैनात करें।
- onion सेवा डोमेन के क्रिप्टोग्राफ़िक पता प्रारूप का विश्लेषण करें।

डीप और डार्क वेब गाइड निर्देश

बहुविकल्पीय और सही/गलत प्रश्नों के उत्तर दें, शब्द बैंक की मदद से रिक्त स्थान भरें, परिभाषाओं का मिलान करें, और क्रॉसवर्ड तथा वर्ड सर्च पहेलियाँ हल करें। अपने ज्ञान को डीप और डार्क वेब गोपनीयता पर लागू करें। अंत में अतिरिक्त गतिविधि झटपट सोचें पूरी करें।

डीप वेब डेटाबेस बनाम डार्क वेब ऑनियन रूटिंग (परिचय)

डीप वेब में पासवर्ड और लॉगिन के पीछे के बिना इंडेक्स किए पेज आते हैं, जैसे निजी ईमेल या कॉर्पोरेट बैंक पोर्टल। डार्क वेब, डीप वेब का वह उपसमूह है जो जानबूझकर छिपाया गया है और जिसे गुमनाम रूप से खोलने के लिए विशेष ब्राउज़र (जैसे Tor) और onion नेटवर्क चाहिए।

प्रत्येक चेकपॉइंट को ध्यान से पढ़ें और सही उत्तर चुनें या लिखें।

चेकपॉइंट 1: बहुविकल्पीय चुनौती

1 **1. डीप वेब को सरफ़ेस वेब से क्या अलग करता है?**

- A. डीप वेब पेज सार्वजनिक सर्च इंजनों द्वारा इंडेक्स नहीं किए जाते
- B. डीप वेब ट्रैफ़िक अवैध है और कानून प्रवर्तन उसकी निगरानी करता है
- C. डीप वेब साइटों तक पहुँचने के लिए Tor जैसे विशेष ब्राउज़र चाहिए
- D. डीप वेब पेज हमेशा सरफ़ेस वेब पेजों से तेज़ लोड होते हैं

2 **2. डार्क वेब तक कैसे पहुँचा जाता है?**

- A. ओनियन रूटिंग नेटवर्क का उपयोग करने वाले विशेष ब्राउज़र के माध्यम से
- B. मानक राउटर पर कस्टम DNS सेटिंग कॉन्फ़िगर करके
- C. निजी, केवल-आमंत्रण वाले सरफ़ेस वेब सर्च कंसोल के माध्यम से
- D. मानक विज्ञापन-रोकने वाला ब्राउज़र एक्सटेंशन इंस्टॉल करके

3 **3. डीप वेब का सबसे बड़ा हिस्सा कौन-सी संरचना बनाती है?**

- A. पासवर्ड-संरक्षित उपयोगकर्ता डेटाबेस और निजी खाते
- B. अवैध सामान का व्यापार करने वाले गैरकानूनी ब्लैक मार्केट फ़ोरम
- C. अनएन्क्रिप्टेड पीयर-टू-पीयर फ़ाइल-शेयरिंग प्रोटोकॉल
- D. सार्वजनिक सर्च इंजन कैश डेटाबेस

4 **4. ऑनियन रूटिंग नेटवर्क ट्रैफ़िक के साथ क्या करती है?**

- A. यह पैकेट को एन्क्रिप्ट करता है और उन्हें कई रिले से भेजता है
- B. यह ISP नोड को दरकिनार करके डाउनलोड गति बढ़ाता है
- C. यह डिवाइस के हार्डवेयर सीरियल नंबर को IP रिकॉर्ड से जोड़ता है
- D. यह हर क्लिक के बाद वेब ब्राउज़र कुकीज़ हटा देता है

5 **5. कौन-सा डोमेन प्रत्यय केवल Tor नेटवर्क पर इस्तेमाल होता है?**

- A. क्रिप्टोग्राफ़िक .onion टॉप-लेवल एक्सटेंशन
- B. मानक पारंपरिक .com व्यावसायिक एक्सटेंशन
- C. Web3 विकेंद्रीकृत .eth ब्लॉकचेन एक्सटेंशन
- D. देश-कोड वाला .ai टेक्नोलॉजी एक्सटेंशन

चेकपॉइंट 2: सही या गलत चुनौती

6 प्रश्न tf 6

6. डीप वेब और डार्क वेब एक ही नेटवर्क खंड को कहते हैं।

○ सही ○ गलत

7 प्रश्न tf 7

7. कॉर्पोरेट इंट्रानेट पोर्टल डीप वेब का हिस्सा हैं।

○ सही ○ गलत

8 प्रश्न tf 8

8. ओनियन रूटिंग हर ट्रांज़िट नोड पर डेटा पैकेट को पूरी तरह डिक्रिप्ट कर देती है।

○ सही ○ गलत

9 प्रश्न tf 9

9. डार्क वेब तक पहुँचने से उपकरण मैलवेयर के उच्च जोखिम में आ जाते हैं।

○ सही ○ गलत

10 प्रश्न tf 10

10. मानक वेब सर्च इंजन ओनियन साइटों को क्रॉल और इंडेक्स करते हैं।

○ सही ○ गलत

चेकपॉइंट 3: मुख्य शब्द भरें

नीचे दिए गए प्रत्येक वाक्य को पढ़ें और रिक्त स्थान को वर्ड बैंक के सही शब्द से भरें।

1. निजी बैंक पोर्टल बिना इंडेक्स वाले _____ खंड में रहते हैं।
2. विशेष Tor नोड छिपी हुई _____ सेवाएं होस्ट करते हैं।
3. Tor वेबसाइट क्रिप्टोग्राफ़िक _____ टॉप-लेवल एक्सटेंशन इस्तेमाल करती हैं।
4. बैंक खाते या ईमेल जैसे लॉगिन के पीछे के _____ सर्च इंजन को दिखाई नहीं देते।
5. सरफ़ेस सर्च इंजन ऐसे पेज क्रॉल करते हैं जो सार्वजनिक रूप से खोजे जा सकने वाले _____ हैं।
6. Google जैसे _____ केवल इंडेक्स किए गए पेज दिखाते हैं; Tor नेटवर्क के पेज इनमें नहीं मिलते।

शब्दावली शब्द-बैंक

इंडेक्स पेज उपयोगकर्ता की गुमनामी खोज इंजन डार्क वेब डीप वेब डॉट ओनियन निजी पेज TOR रूटिंग

अपने उत्तर यहाँ लिखें:

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

चेकपॉइंट 4: सुरक्षा अवधारणा मिलान

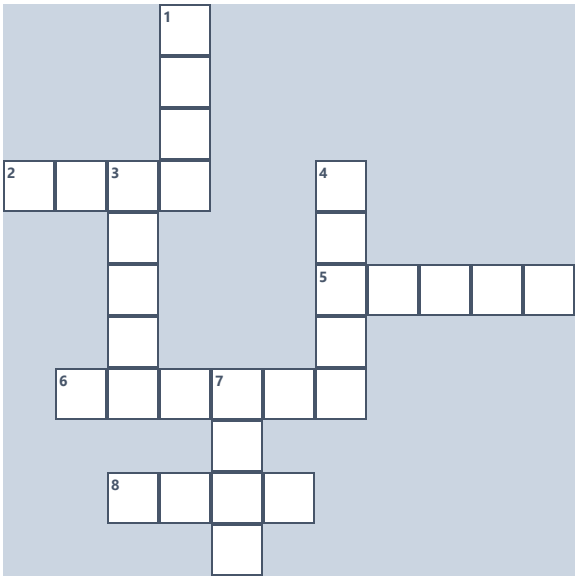
परिभाषा मिलान

बाईं ओर के प्रत्येक शब्दावली पद को दाईं ओर की सही परिभाषा से मिलाएँ; भरने योग्य इनपुट बॉक्स में संबंधित अक्षर (A-H) लिखें।

☐	**1. डीप वेब खंड**	**A**	एन्क्रिप्टेड नेटवर्क खंड जो केवल विशेष ब्राउज़रों से पहुँच योग्य है।
☐	**2. डार्क वेब पोर्टल**	**B**	डेटा को परतों में एन्क्रिप्ट करके तीन नोड से होकर रिले करना।
☐	**3. Onion एक्सटेंशन**	**C**	बिना इंडेक्स वाले सिस्टम रिकॉर्ड होस्ट करने वाला सुरक्षित बैकएंड स्टोरेज।
☐	**4. Tor रूटिंग**	**D**	Tor नेटवर्क पर उपयोग होने वाला क्रिप्टोग्राफ़िक टॉप-लेवल डोमेन प्रत्यय।
☐	**5. इंडेक्स किए गए पेज**	**E**	Tor नेटवर्क तक पहुँचने के लिए इस्तेमाल होने वाला एंट्री पॉइंट नोड।
☐	**6. उपयोगकर्ता की गुमनामी**	**F**	Google पर संकलित और खोजे जा सकने वाला सरफ़ेस वेब कंटेंट।
☐	**7. निजी डेटाबेस**	**G**	क्लाइंट के सार्वजनिक IP पते सर्वरों से छिपाकर रखना।
☐	**8. एंट्रेंस गेटवे**	**H**	बिना इंडेक्स वाली वेब सामग्री, जैसे निजी लॉगिन, ईमेल और डेटाबेस रिकॉर्ड।

चेकपॉइंट 5: क्रॉसवर्ड पहेली

सक्रिय सफ़ेद खानों में अक्षर टाइप करके क्रॉसवर्ड पहेली हल करें। संख्याएँ नीचे दिए गए संकेतों से मेल खाती हैं।



बाएँ से दाएँ

2. एन्क्रिप्टेड नेटवर्क खंड, जिस तक केवल विशेष ब्राउज़र से पहुंचा जा सकता है (4)

5. Google पर संकलित और खोजे जा सकने वाली सरफ़ेस वेब सामग्री (5)

6. Tor नेटवर्क पर इस्तेमाल होने वाला क्रिप्टोग्राफ़िक टॉप-लेवल डोमेन प्रत्यय (6)

8. वेबसाइट का एक अलग पृष्ठ, जिसे ब्राउज़र में खोला जाता है (4)

ऊपर से नीचे

1. निजी लॉगिन, ईमेल और डेटाबेस रिकॉर्ड जैसी बिना इंडेक्स की वेब सामग्री (4)

3. इंटरनेट पर एक पते के नीचे जुड़े वेब पेजों का समूह (5)

4. वह सेवा, जो इंटरनेट पर इंडेक्स किए गए पेज खोजकर दिखाती है (5)

7. लॉगिन के पीछे छिपा ऐसा पेज, जो सार्वजनिक खोज में नहीं आता (4)

चेकपॉइंट 5, वैकल्पिक: सुलभ क्रॉसवर्ड संकेत

स्क्रीन-रीडर और कीबोर्ड उपयोगकर्ता क्रॉसवर्ड के उत्तर सीधे नीचे दिए गए टेक्स्ट फ़ील्ड में टाइप कर सकते हैं।

बाएँ से दाएँ

2 बाएँ से दाएँ: एन्क्रिप्टेड नेटवर्क खंड, जिस तक केवल विशेष ब्राउज़र से पहुंचा जा सकता है (4 अक्षर):

5 बाएँ से दाएँ: Google पर संकलित और खोजे जा सकने वाली सरफ़ेस वेब सामग्री (5 अक्षर):

6 बाएँ से दाएँ: Tor नेटवर्क पर इस्तेमाल होने वाला क्रिप्टोग्राफ़िक टॉप-लेवल डोमेन प्रत्यय (6 अक्षर):

8 बाएँ से दाएँ: वेबसाइट का एक अलग पृष्ठ, जिसे ब्राउज़र में खोला जाता है (4 अक्षर):

ऊपर से नीचे

1 ऊपर से नीचे: निजी लॉगिन, ईमेल और डेटाबेस रिकॉर्ड जैसी बिना इंडेक्स की वेब सामग्री (4 अक्षर):

3 ऊपर से नीचे: इंटरनेट पर एक पते के नीचे जुड़े वेब पेजों का समूह (5 अक्षर):

4 ऊपर से नीचे: वह सेवा, जो इंटरनेट पर इंडेक्स किए गए पेज खोजकर दिखाती है (5 अक्षर):

7 ऊपर से नीचे: लॉगिन के पीछे छिपा ऐसा पेज, जो सार्वजनिक खोज में नहीं आता (4 अक्षर):

चेकपॉइंट 6: छिपे शब्द खोजें

नीचे दी गई ग्रिड में छिपे 8 प्रमुख शब्दावली शब्द खोजें। शब्द क्षैतिज, ऊर्ध्वाधर या तिरछे हो सकते हैं।

इ	ठ	दा	ज	द	दि	ते	वी	ति	च	ह	री	रा	व	त
सा	ज	स	ई	ते	घ	इ	नी	नि	ल	रि	द	जे	घ	छ
ई	पे	के	द	प	ति	के	ट	मि	जी	ट	सा	य	च	ऊ
नी	क्स	जी	इ	त	म	पे	ब	प	जि	पे	मी	ने	ले	इ
सी	डे	य	छ	र	डॉ	दे	कि	जा	सा	वा	ज	ड	रे	स
ख	इं	नि	फ	ढ	ट	मा	खो	ना	का	रे	डी	प	वे	ब
दे	सि	मी	क	पि	ओ	ता	ति	ज	ज	श	भ	ऊ	अ	ऊ
ए	रि	वि	श	य	नि	वि	व	वा	इं	पा	ल	च	से	कि
ब	य	घ	प	के	य	की	व	सि	री	ज	त	की	कि	सि
वे	ना	ने	पा	ते	न	ण	ए	ता	सा	मी	न	न	नी	ऋ
र्क	वे	ब	सा	इ	ट	ले	घ	ति	जि	ला	ए	जी	ले	वे
डा	ड	ल	द	जे	घ	के	च	से	दे	री	ए	पी	ब	उ
अ	जे	मि	घ	व	आ	च	मी	च	ट	थ	फ	पे	ग	ना
सी	का	ज	फ	नी	जी	ता	ठ	से	लि	ट	ज	आ	इ	से
रा	के	री	पा	वा	सि	य	नि	पि	ने	ख	के	वे	ऊ	ड

शब्दावली शब्द-सूची

वेबसाइट डार्कवेब खोजइंजन निजीपेज वेबपेज डॉटओनियन इंडेक्सपेज डीपवेब

चेकपॉइंट 6, वैकल्पिक: सुलभ शब्दावली मिलान

वर्ड सर्च के 8 शब्दावली पदों में से प्रत्येक को उसकी सही परिभाषा से मिलाएँ; खाली स्थान में अक्षर (A-H) लिखें।

शब्दावली के शब्द

- **A. वेबसाइट**
- **B. डार्कवेब**
- **C. खोजइंजन**
- **D. निजीपेज**
- **E. वेबपेज**
- **F. डॉटओनियन**
- **G. इंडेक्सपेज**
- **H. डीपवेब**

परिभाषाएँ और मिलान फ़ील्ड

1. Tor नेटवर्क पर इस्तेमाल होने वाला क्रिप्टोग्राफ़िक टॉप-लेवल डोमेन प्रत्यय।
2. Google पर संकलित और खोजे जा सकने वाली सरफ़ेस वेब सामग्री।
3. लॉगिन के पीछे छिपा ऐसा पेज, जो सार्वजनिक खोज में नहीं आता।
4. इंटरनेट पर एक पते के नीचे जुड़े वेब पेजों का समूह।
5. एन्क्रिप्टेड नेटवर्क खंड, जिस तक केवल विशेष ब्राउज़र से पहुंचा जा सकता है।
6. वह सेवा, जो इंटरनेट पर इंडेक्स किए गए पेज खोजकर दिखाती है।
7. निजी लॉगिन, ईमेल और डेटाबेस रिकॉर्ड जैसी बिना इंडेक्स की वेब सामग्री।
8. वेबसाइट का एक अलग पृष्ठ, जिसे ब्राउज़र में खोला जाता है।

चेकपॉइंट 7: उलझे शब्दों की चुनौती

नीचे के अक्षरों को सुलझाकर साइबर सुरक्षा की प्रमुख अवधारणाएँ और शब्द पता करें। अपने उत्तर दिए गए इनपुट बॉक्स में लिखें।

1. इ सा वे ट ब
2. खो न ज इं ज
3. ज वे पे ब
4. क्स ज पे इं डे
5. ब डा वे र्क
6. पे ज नि जी
7. य डॉ नि न ओ ट
8. डी ब वे प

अतिरिक्त गतिविधि: झटपट सोचें

हर श्रेणी में 3 उत्तर। जो सबसे पहले सूची भर दे, वह जीतता है।

1	डार्क वेब से दूर रहने के कारण			
2	ऐसी चीज़ें जिन्हें सर्च इंजन नहीं खोज पाता			
3	ऐसे डिवाइस जिन्हें हैक किया जा सकता है			
4	Tor इस्तेमाल करने के कानूनी कारण			
5	सॉफ़्टवेयर अपडेट करने के कारण			
6	ईमेल में चेतावनी के संकेत			
7	डार्क वेब पर गैरकानूनी रूप से बिकने वाली चीज़ें			
8	IT मदद के लिए आप जिनसे पूछ सकते हैं			
9	सुरक्षित आदतें जो आप आज से शुरू कर सकते हैं			
10	डेटा लीक के बाद की जाने वाली चीज़ें			
11	डीप वेब से जुड़ी चीज़ें			
12	लॉगिन के साथ इस्तेमाल होने वाली साइटें			
13	गुमनामी से जुड़े शब्द			
14	ऐसी जानकारी जो आपको कभी साझा नहीं करनी चाहिए			
15	ऐसी चीज़ें जो 'सतह के नीचे' होती हैं			

चेकपॉइंट 8: साइबर सुरक्षा केस स्टडी

नीचे दिए गए वास्तविक परिदृश्यों को हल करने के लिए सीखी हुई अवधारणाओं का उपयोग करें।

केस स्टडी 1: डेटा लीक की पहचान



परिदृश्य: एक कॉर्पोरेट सुरक्षा ऑडिट में पता चलता है कि संवेदनशील क्लाइंट डेटाबेस रिकॉर्ड एक onion मार्केटप्लेस पर बेचे जा रहे हैं। यह डेटा Google पर इंडेक्स नहीं है।

चर्चा प्रश्न: समझाइए कि कौन-से वेब खंड शामिल हैं और यह लीक कैसे हुआ।

केस स्टडी 2: गुमनामी बनाम मैलवेयर जोखिम



परिदृश्य: एक विश्लेषक किसी Tor वेबसाइट पर थ्रेट इंटेलिजेंस फ़ीड जाँचना चाहता है। वह Tor ब्राउज़र डाउनलोड करके साइट खोलता है।

चर्चा प्रश्न: गुमनामी के फ़ायदों का मूल्यांकन कीजिए और मैलवेयर से बचाव के चरण बताइए।

चेकपॉइंट 9: कूट संदेश को डिकोड करें

साइबर सुरक्षा पेशेवर नेटवर्क संपत्तियों को ऑनलाइन ख़तरा पैदा करने वालों से बचाता है। नीचे दी गई अक्षर-से-संख्या कुंजी का उपयोग करके संदेश को डिक्रिप्ट करें और खाली स्थानों में मेल खाते अक्षर लिखें।

अक्षर-से-संख्या एन्क्रिप्शन कुंजी

अ=1 आ=2 इ=3 ई=4 उ=5 ऊ=6 ऋ=7 ए=8 ऐ=9 ओ=10 औ=11 ऑ=12

क=13 ख=14 ग=15 घ=16 ङ=17 च=18 छ=19 ज=20 झ=21 ञ=22 ट=23 ठ=24

ड=25 ढ=26 ण=27 त=28 थ=29 द=30 ध=31 न=32 प=33 फ=34 ब=35 भ=36

म=37 य=38 र=39 ल=40 व=41 श=42 ष=43 स=44 ह=45 ा=46 ि=47 ी=48

ु=49 ू=50 ृ=51 े=52 ै=53 ो=54 ौ=55 ॉ=56 ं=57 ँ=58 ः=59 ़=60

्=61

10	32	47	38	32		39	50	23	47	57	15		44	52

5	33	38	54	15	13	39	61	28	46		15	49	37	32	46	37

39	45	28	46

डिकोड किया गया संदेश:

सुझाव: हर संख्या वर्णमाला में उस अक्षर की स्थिति दर्शाती है (जैसे 1 = अ, 2 = आ, 61 = ्)।

चेकपॉइंट 10: बुनियादी साइबर सुरक्षा FAQ (भाग A)

ऑनलाइन खतरों को कम करने से जुड़े आम सवाल और जवाब देखें।

Q1: डीप वेब क्या है?

डीप वेब में वे सभी वेब पेज शामिल हैं जिन्हें सर्च इंजन इंडेक्स नहीं कर सकते, जैसे ऑनलाइन बैंकिंग, ईमेल डेटाबेस और पेवॉल वाली पत्रिकाएँ।

Q2: डार्क वेब क्या है?

डार्क वेब, डीप वेब का एक छोटा उपसमूह है जो जानबूझकर छिपाया गया है और केवल onion नेटवर्क वाले विशेष ब्राउज़रों से पहुँचा जा सकता है।

Q3: सर्च इंजन पेजों को इंडेक्स कैसे करते हैं?

सर्च इंजन स्वचालित प्रोग्राम (स्पाइडर) चलाकर सार्वजनिक लिंक का अनुसरण करते हैं, और रोबोट निर्देशों से क्रॉलिंग न रोकने वाले पेज इंडेक्स करते हैं।

Q4: ऑनलाइन बैंकिंग को डीप वेब का हिस्सा क्यों माना जाता है?

बैंकिंग पोर्टल लॉगिन दीवारों और पासवर्ड के पीछे होते हैं, जिससे सार्वजनिक सर्च इंजन खाता विवरण वाले पेज इंडेक्स नहीं कर पाते।

Q5: Tor ब्राउज़र का Onion Routing क्या है?

ओनियन रूटिंग एक ट्रांसमिशन विधि है जो ट्रैफ़िक को परतों में एन्क्रिप्ट करती है और उपयोगकर्ता के IP पतों को छिपाने के लिए उसे कई रिले से गुज़ारती है।

चेकपॉइंट 10: बुनियादी साइबर सुरक्षा FAQ (भाग B)

ऑनलाइन खतरों को कम करने से जुड़े आम सवाल और जवाब देखें।

Q6: क्या डार्क वेब तक पहुँचना अवैध है?

नहीं। ज़्यादातर देशों में डार्क वेब तक पहुँचना कानूनी है, हालाँकि अवैध मार्केटप्लेस या साइबर गतिविधियों में शामिल होना निषिद्ध है।

Q7: डार्क वेब साइटें धीरे लोड क्यों होती हैं?

ट्रैफ़िक कम से कम तीन वैश्विक रिले (एंट्री, मिडिल, एग्ज़िट) से रूट और डिक्रिप्ट होता है, जिससे संचरण की लेटेंसी बढ़ती है।

Q8: .onion डोमेन सफ़िक्स का क्या अर्थ है?

यह Tor नेटवर्क पर उपयोग होने वाला विशेष टॉप-लेवल डोमेन प्रत्यय है, जो मानक DNS सर्वर के बजाय क्रिप्टोग्राफ़िक रूप से बनाए गए पतों की ओर इशारा करता है।

Q9: डार्क वेब लिंक से कौन-से जोखिम जुड़े हैं?

साइटों में कोई सुरक्षा जाँच नहीं होती, जिससे उपयोगकर्ता मैलवेयर संक्रमण की ऊँची दर, फ़िशिंग स्क्रिप्ट और लेन-देन घोटालों के जोखिम में आ जाते हैं।

Q10: Tor नेटवर्क रूटिंग प्रोटोकॉल किसने बनाया?

यह तकनीक मूल रूप से 1990 के दशक में अमेरिकी नौसेना अनुसंधान प्रयोगशाला ने सरकारी संचार की सुरक्षा के लिए विकसित की थी।

चेकपॉइंट 10: उन्नत सुरक्षा FAQ (भाग C)

सुरक्षा फ़्रेमवर्क, मैलवेयर विश्लेषण और डेटा अनुपालन के उन्नत तकनीकी पहलुओं को जानें।

Q1: मध्यवर्ती नोड Tor की गुमनामी की रक्षा कैसे करते हैं?

हर नोड रूटिंग डेटा की केवल एक परत डिक्रिप्ट करता है और केवल पिछला व अगला हॉप जानता है, स्रोत और गंतव्य दोनों कभी नहीं।

Q2: एग्ज़िट नोड की क्या भूमिका है?

एग्ज़िट नोड एन्क्रिप्शन की अंतिम परत खोलता है और ट्रैफ़िक को सार्वजनिक गंतव्य सर्वर या onion सर्वर तक भेज देता है।

Q3: Tor ब्रिज गेटवे क्या है?

ब्रिज बिना सूची वाले Tor एंट्री रिले हैं, जिनका उपयोग उन क्षेत्रों में ISP अवरोधों और सेंसरशिप को बायपास करने के लिए होता है जहाँ Tor ब्राउज़र की पहुँच सीमित है।

Q4: डार्क वेब के तत्व क्रिप्टोकरेंसी का दुरुपयोग कैसे करते हैं?

अपराधी डार्क मार्केटप्लेस पर वित्तीय लेन-देन करने के लिए गुमनाम क्रिप्टोकरेंसी का उपयोग करते हैं और मानक बैंकिंग लेन-देन जाँच से बचते हैं।

Q5: सामान्य सर्च इंजन डीप डेटाबेस को क्रॉल करने में विफल क्यों रहते हैं?

क्रॉलर लॉगिन क्रेडेंशियल दर्ज नहीं कर सकते, सुरक्षा CAPTCHA हल नहीं कर सकते, और डीप डेटाबेस तक पहुँचने के लिए आवश्यक बैकएंड SQL क्वेरी स्क्रिप्ट नहीं चला सकते।

चेकपॉइंट 10: उन्नत सुरक्षा FAQ (भाग D)

सुरक्षा फ़्रेमवर्क, मैलवेयर विश्लेषण और डेटा अनुपालन के उन्नत तकनीकी पहलुओं को जानें।

Q6: Tor नेटवर्क में डायरेक्टरी सर्वर क्या है?

यह एक भरोसेमंद सर्वर है जो सक्रिय एंट्री, मिडिल और एग्ज़िट रिले की सूची रखता है, जिनका उपयोग क्लाइंट रूटिंग पाथ बनाने में करते हैं।

Q7: दुर्भावनापूर्ण तत्व एग्ज़िट नोड स्निफ़िंग कैसे करते हैं?

रोग एग्ज़िट नोड ऑपरेटर Tor नेटवर्क से निकलते समय बिना एन्क्रिप्शन वाले HTTP ट्रैफ़िक को इंटरसेप्ट करके यूज़रनेम और कुकी चुरा सकते हैं।

Q8: Tor और I2P में क्या अंतर है?

Tor सार्वजनिक वेब एक्सेस के लिए केंद्रीकृत रिले डायरेक्टरी और एग्ज़िट नोड का उपयोग करता है, जबकि I2P आंतरिक होस्टिंग के लिए विकेंद्रीकृत पीयर-टू-पीयर संरचना का उपयोग करता है।

Q9: क़ानून प्रवर्तन एजेंसियाँ डार्क वेब बाज़ारों को कैसे ट्रैक करती हैं?

एजेंसियाँ ब्लॉकचेन विश्लेषण का उपयोग करती हैं, भौतिक सर्वर होस्टिंग सेटअप का पता लगाती हैं और संचालकों की पहचान के लिए डिकॉय ऑपरेशन चलाती हैं।

Q10: DNS लीक क्लाइंट की गुमनामी को कैसे खतरे में डालता है?

DNS लीक तब होते हैं जब ब्राउज़र की DNS क्वेरी एन्क्रिप्टेड Tor नेटवर्क से जाने के बजाय सीधे स्थानीय ISP से होकर भेजी जाती हैं।

भाग 11: 10 वास्तविक साइबर सुरक्षा तथ्य और अंतर्दृष्टियाँ

सुरक्षा उल्लंघनों, बचाव तंत्रों और अनुपालन मानकों से जुड़े वास्तविक तथ्य देखें।

1. सुरक्षा इनसाइट

डीप वेब खोजे जा सकने वाले सरफ़ेस वेब से कहीं बड़ा है, क्योंकि अधिकांश सामग्री लॉगिन और डेटाबेस के पीछे रहती है।

2. सुरक्षा इनसाइट

डार्क वेब, डीप वेब का एक छोटा, जानबूझकर छिपाया गया हिस्सा है, जिस तक Tor जैसे टूल्स से पहुँचा जाता है।

3. सुरक्षा इनसाइट

Tor रूटिंग डेटा पैकेट को तीन बार एन्क्रिप्ट करती है, और हर रिले नोड पर प्याज़ की परतों की तरह एन्क्रिप्शन की परतें उतारती जाती है।

4. सुरक्षा इनसाइट

Tor अमेरिकी नौसेना अनुसंधान प्रयोगशाला के चलाए onion routing प्रोजेक्ट से विकसित हुआ, और इसका कोड मुफ़्त सॉफ़्टवेयर के रूप में जारी किया गया। [1]

5. सुरक्षा इनसाइट

ओनियन पते 56 वर्णों की अक्षर-अंक स्ट्रिंग होते हैं, जो पब्लिक की जोड़ियों से क्रिप्टोग्राफ़िक रूप से बनाए जाते हैं।

6. सुरक्षा इनसाइट

एग्ज़िट नोड क्लियरटेक्स्ट ट्रैफ़िक पढ़ सकते हैं, यानी सुरक्षित सेशन डेटा के लिए Tor पर भी TLS/HTTPS ज़रूरी है।

7. सिक्योरिटी इनसाइट

इंट्रानेट साइटें, क्लाउड ड्राइव और निजी डेटाबेस डीप वेब के सबसे बड़े डेटा स्टोरेज खंड हैं।

8. सिक्योरिटी इनसाइट

DuckDuckGo जैसे विशेष सर्च इंजन Tor नेटवर्क पर गुमनाम खोज की अनुमति देने के लिए ओनियन पोर्टल चलाते हैं।

9. सिक्योरिटी इनसाइट

सेंसरशिप को बायपास करने और संचार की गोपनीयता बनाए रखने के लिए रोज़ाना 2 मिलियन से अधिक उपयोगकर्ता Tor नेटवर्क से जुड़ते हैं।

10. सुरक्षा इनसाइट

वैश्विक कानून प्रवर्तन अभियान (जैसे Operation Bayonet) होस्टिंग हार्डवेयर जब्त करके प्रमुख डार्क मार्केटप्लेस बंद कर देते हैं।

तकनीकी संदर्भ और स्रोत

यह अध्ययन गाइड और इंटरैक्टिव पहेलियाँ वैश्विक NIST, OWASP और डेटा गोपनीयता अनुपालन मानकों से तैयार की गई हैं।

शैक्षणिक और उद्योग संदर्भ

[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

उत्तर कुंजी: चेकपॉइंट 1 – बहुविकल्पीय

1 **सर्च इंडेक्सिंग** डीप वेब **सही उत्तर: A**

शिक्षण नोट

डीप वेब पेज लॉगिन दीवारों और डेटाबेस के पीछे होते हैं, जिससे सर्च स्पाइडर उन्हें क्रॉल नहीं कर पाते। उद्धरण: IETF RFC 3986।

2 **Tor एक्सेस** डार्क वेब **सही उत्तर: A**

शिक्षण नोट

डार्क वेब में छिपी हुई onion सेवाएँ होती हैं, जिन्हें केवल Tor जैसे ब्राउज़रों से खोला जा सकता है। उद्धरण: IETF RFC 3986।

3 **डीप डेटाबेस** डेटाबेस **सही उत्तर: A**

शिक्षण नोट

पासवर्ड-सुरक्षित खाते और कॉर्पोरेट रिकॉर्ड डीप वेब का सबसे बड़ा हिस्सा बनाते हैं। उद्धरण: NIST Digital Identity.

4 **ओनियन रूटिंग** Tor नेटवर्क **सही उत्तर: A**

शिक्षण नोट

ओनियन रूटिंग डेटा पैकेट को परतों में एन्क्रिप्ट करती है और गुमनामी के लिए उन्हें कई नोड से गुज़ारती है। उद्धरण: IETF RFC 3986.

5 **ओनियन डोमेन** प्रत्यय **सही उत्तर: A**

शिक्षण नोट

क्रिप्टोग्राफ़िक.onion डोमेन प्रत्यय सार्वजनिक DNS के बिना Tor के भीतर ही ट्रैफ़िक रूट करता है। उद्धरण: IETF RFC 3986।

उत्तर कुंजी: चेकपॉइंट 2 – सही या गलत

6 **वेब सेगमेंट** संरचना **सही उत्तर: गलत**

शिक्षण नोट

डीप वेब में सभी बिना इंडेक्स वाले पेज आते हैं, जबकि डार्क वेब एक छोटा, एन्क्रिप्टेड onion उपखंड है। उद्धरण: IETF RFC 3986।

7 **कॉर्पोरेट इंट्रानेट** डीप वेब **सही उत्तर: सही**

शिक्षण नोट

इंट्रानेट साइटें पासवर्ड पोर्टल के पीछे होती हैं और इंडेक्स नहीं होतीं, यानी वे डीप वेब का हिस्सा हैं। उद्धरण: NIST Digital Identity।

8 **लेयर एन्क्रिप्शन** रिले **सही उत्तर: गलत**

शिक्षण नोट

ओनियन रिले उपयोगकर्ता की गुमनामी बचाने के लिए केवल एक रूटिंग परत को डिक्रिप्ट करते हैं, पूरे पैकेट को कभी नहीं। उद्धरण: IETF RFC 3986.

9 **मैलवेयर का जोखिम** ख़तरे **सही उत्तर: सही**

शिक्षण नोट

डार्क वेब मार्केटप्लेस में कोई सुरक्षा फ़िल्टरिंग नहीं होती, इसलिए उनमें मैलवेयर संक्रमण का अत्यधिक जोखिम रहता है। उद्धरण: Center for Internet Security (CIS)।

10 **प्रश्न 10** **सही उत्तर: गलत**

शिक्षण नोट

आम सर्च इंजन क्रॉलर Tor का उपयोग नहीं करते, इसलिए वे .onion साइटों तक नहीं पहुँच सकते या उन्हें इंडेक्स नहीं कर सकते।

शब्दावली कुंजियाँ और ग्रेडिंग रूब्रिक

शिक्षक के लिए ग्रेडिंग रूब्रिक: हर सही मिलान (कुल 8 अंक) और संदर्भ शब्द (कुल 6 अंक) के लिए 1 अंक दें।

चेकपॉइंट 4: उत्तर – अवधारणा मिलान

H 1. डीप वेब खंड	A 2. डार्क वेब पोर्टल	D 3. Onion एक्सटेंशन	B 4. Tor रूटिंग
F 5. इंडेक्स किए गए पेज	G 6. उपयोगकर्ता की गुमनामी	C 7. निजी डेटाबेस	E 8. एंट्रेंस गेटवे

चेकपॉइंट 3: उत्तर – प्रमुख शब्द

1 डीप वेब	2 डार्क वेब	3 डॉट ओनियन	4 निजी पेज
5 इंडेक्स पेज	6 खोज इंजन		

चेकपॉइंट 6, वैकल्पिक: उत्तर – शब्द मिलान

1 F – डॉटओनियन	2 G – इंडेक्सपेज	3 D – निजीपेज	4 A – वेबसाइट
5 B – डार्कवेब	6 C – खोजइंजन	7 H – डीपवेब	8 E – वेबपेज

शिक्षकों के लिए चर्चा नोट

प्रमुख शब्द:
जाँचें कि क्या विद्यार्थी डीप वेब खंड, डार्क वेब पोर्टल और Onion एक्सटेंशन को अपने शब्दों में समझा सकते हैं और हर एक का उदाहरण दे सकते हैं।

केस स्टडी:
विद्यार्थियों से कहें कि वे अपनी सिफ़ारिशें राय के बजाय वर्कशीट के तथ्यों पर आधारित करें।

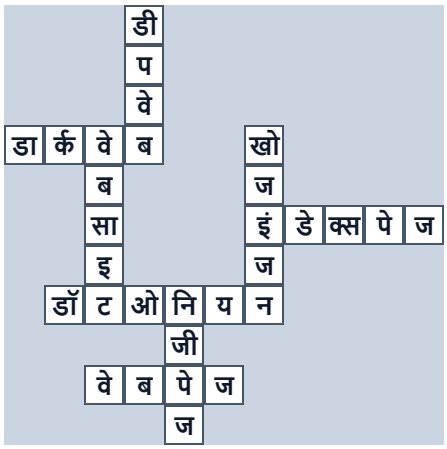
स्रोतों का मूल्यांकन:
विद्यार्थियों से वर्कशीट के स्रोतों में कम से कम एक कथन की पुष्टि करवाएँ और चर्चा करें कि आँकड़े, कीमतें और नियम समय के साथ क्यों बदल सकते हैं।

पहेलियों की कुंजियाँ और शिक्षक नोट

शब्द खोज समाधान

इ	ठ	दा	ज	द	दि	ते	वी	ति	च	ह	री	रा	व	त
सा	ज	स	ई	ते	घ	इ	नी	नि	ल	रि	द	जे	घ	छ
ई	पे	के	द	प	ति	के	ट	मि	जी	ट	सा	य	च	ऊ
नी	क्स	जी	इ	त	म	पे	ब	प	जि	पे	मी	ने	ले	इ
सी	डे	य	छ	र	डॉ	दे	कि	जा	सा	वा	ज	ड	रे	स
ख	इं	नि	फ	ढ	ट	मा	खो	ना	का	रे	डी	प	वे	ब
दे	सि	मी	क	पि	ओ	ता	ति	ज	ज	श	भ	ऊ	अ	ऊ
ए	रि	वि	श	य	नि	वि	व	वा	इं	पा	ल	च	से	कि
ब	य	घ	प	के	य	की	व	सि	री	ज	त	की	कि	सि
वे	ना	ने	पा	ते	न	ण	ए	ता	सा	मी	न	न	नी	ऋ
र्क	वे	ब	सा	इ	ट	ले	घ	ति	जि	ला	ए	जी	ले	वे
डा	ड	ल	द	जे	घ	के	च	से	दे	री	ए	पी	ब	उ
अ	जे	मि	घ	व	आ	च	मी	च	ट	थ	फ	पे	ग	ना
सी	का	ज	फ	नी	जी	ता	ठ	से	लि	ट	ज	आ	इ	से
रा	के	री	पा	वा	सि	य	नि	पि	ने	ख	के	वे	ऊ	ड

क्रॉसवर्ड समाधान



क्रॉसवर्ड समाधान के लिए शिक्षक गाइड

बाएँ से दाएँ

2 बाएँ से दाएँ: डार्कवेब एन्क्रिप्टेड नेटवर्क खंड, जिस तक केवल विशेष ब्राउज़र से पहुंचा जा सकता है (4 अक्षर)

5 बाएँ से दाएँ: इंडेक्सपेज Google पर संकलित और खोजे जा सकने वाली सरफ़ेस वेब सामग्री (5 अक्षर)

6 बाएँ से दाएँ: डॉटओनियन Tor नेटवर्क पर इस्तेमाल होने वाला क्रिप्टोग्राफ़िक टॉप-लेवल डोमेन प्रत्यय (6 अक्षर)

8 बाएँ से दाएँ: वेबपेज वेबसाइट का एक अलग पृष्ठ, जिसे ब्राउज़र में खोला जाता है (4 अक्षर)

ऊपर से नीचे

1 ऊपर से नीचे: डीपवेब निजी लॉगिन, ईमेल और डेटाबेस रिकॉर्ड जैसी बिना इंडेक्स की वेब सामग्री (4 अक्षर)

3 ऊपर से नीचे: वेबसाइट इंटरनेट पर एक पते के नीचे जुड़े वेब पेजों का समूह (5 अक्षर)

4 ऊपर से नीचे: खोजइंजन वह सेवा, जो इंटरनेट पर इंडेक्स किए गए पेज खोजकर दिखाती है (5 अक्षर)

7 ऊपर से नीचे: निजीपेज लॉगिन के पीछे छिपा ऐसा पेज, जो सार्वजनिक खोज में नहीं आता (4 अक्षर)

अक्षर-फेर शब्द और कूट संदेश हल कुंजी

शब्द-अनस्क्रैम्बल गतिविधि और Secret Cipher Challenge की ग्रेडिंग कुंजी।

शब्द अनस्क्रैम्बल कुंजी

1. इसावेटब — **वेबसाइट**
2. खोनजइंज — **खोजइंजन**
3. जवेपेब — **वेबपेज**
4. क्सजपेइंडे — **इंडेक्सपेज**
5. बडावेर्क — **डार्कवेब**
6. पेजनिजी — **निजीपेज**
7. यडॉनिनओट — **डॉटओनियन**
8. डीबवेप — **डीपवेब**

गुप्त कूट चुनौती कुंजी

"ओनियन रूटिंग से उपयोगकर्ता गुमनाम रहता"

केस स्टडी के उत्तर

A केस स्टडी 1: डेटा लीक की पहचान

शिक्षक समाधान

ग्रेडिंग दिशानिर्देश

छात्रों के उत्तरों में निम्नलिखित बिंदु शामिल होने चाहिए:

- परिदृश्य विश्लेषण: एक कॉर्पोरेट सुरक्षा ऑडिट में पता चलता है कि संवेदनशील क्लाइंट डेटाबेस रिकॉर्ड का सौदा एक onion मार्केटप्लेस पर हो रहा है। यह डेटा Google पर इंडेक्स नहीं है।
- अनुशंसित रणनीति और समाधान: शामिल सेगमेंट: निजी डेटाबेस डीप वेब का हिस्सा है (अनइंडेक्स्ड लेकिन सुरक्षित)। चुराए गए डेटा का सौदा करने वाला बाज़ार डार्क वेब (onion नेटवर्क) पर है। यह कैसे हुआ: हैकरों ने सर्वर की सुरक्षा को बायपास किया, डीप वेब से डेटाबेस चुराया, और कानून प्रवर्तन की ट्रैकिंग से बचने के लिए उसे डार्क वेब पर गुमनाम रूप से लिस्ट कर दिया।

B केस स्टडी 2: गुमनामी बनाम मैलवेयर जोखिम

शिक्षक समाधान

ग्रेडिंग दिशानिर्देश

छात्रों के उत्तरों में निम्नलिखित बिंदु शामिल होने चाहिए:

- परिदृश्य विश्लेषण: एक विश्लेषक Tor वेबसाइट पर थ्रेट इंटेलिजेंस फ़ीड जाँचना चाहता है। वह Tor ब्राउज़र डाउनलोड करता है और साइट खोलता है।
- अनुशंसित रणनीति और समाधान: लाभ: Tor ट्रैफ़िक को तीन नोड से गुज़ारता है, जिससे विश्लेषक का कॉर्पोरेट IP छिप जाता है। जोखिम और उपाय: डार्क वेब लिंक की कोई प्रतिष्ठा-जाँच नहीं होती। कॉर्पोरेट नेटवर्क की सुरक्षा के लिए विश्लेषकों को Tor को अलग-थलग वर्चुअल मशीन (VM) के भीतर चलाना चाहिए, Tor सेटिंग्स में JavaScript बंद करनी चाहिए और कोई भी फ़ाइल डाउनलोड करने से बचना चाहिए।