नाम: _____ दिनांक: _____ अंक: _____

प्रॉक्सी बनाम VPN वर्कशीट

प्रॉक्सी सर्वर और वर्चुअल प्राइवेट नेटवर्क की तुलना, एन्क्रिप्शन के अंतर, और ऐप-स्तर बनाम सिस्टम-व्यापी रूटिंग

VPN सीखने का अवलोकन

शिक्षार्थी
छात्र का दर्जा
नेटवर्क डिफ़ेंडर ट्रैक

सुरक्षित
कनेक्शन की स्थिति
डेटा पैकेट की ढाल बनाना

सक्रिय
लीक सुरक्षा
DNS और IPv6 लीक सुरक्षा

स्वागत है! यह गतिविधि पैकेट आपको वर्चुअल प्राइवेट नेटवर्क (VPN) के मूल सिद्धांतों से परिचित कराता है। आप जानेंगे कि एन्क्रिप्टेड टनल आपके डेटा को कैसे सुरक्षित करती हैं, नेटवर्क प्रोटोकॉल कैसे काम करते हैं, और गोपनीयता लीक की पहचान और उन्हें कम कैसे करें।

वर्कशीट चेकपॉइंट

- [ ] **भाग 1-4: VPN अवधारणाओं और प्रोटोकॉल 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 VPN गाइड खोलें

URL: https://www.vpn.com/hi/vpn/

आपका VPN लर्निंग रोडमैप

- एप्लिकेशन प्रॉक्सी की तुलना सिस्टम-व्यापी VPN एन्क्रिप्शन से करें।
- बुनियादी HTTP प्रॉक्सी की तुलना में SOCKS5 की क्षमताओं की पहचान करें।
- विश्लेषण करें कि ब्राउज़र-आधारित प्रॉक्सी बैकग्राउंड ऐप्स को कैसे असुरक्षित छोड़ देते हैं।
- समझें कि ISP प्रॉक्सी टनल पर बिना एन्क्रिप्ट किया ट्रैफ़िक कैसे लॉग करते हैं।
- स्पीड और सुरक्षा की ज़रूरतों के आधार पर सही रूटिंग टूल चुनें।

प्रॉक्सी तुलना वर्कशीट 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 प्रॉक्सी और VPN की तुलना पर लागू करें। अंत में अतिरिक्त गतिविधि झटपट सोचें पूरी करें।

प्रॉक्सी बनाम VPN (परिचय)

प्रॉक्सी और VPN अलग-अलग डिजिटल गोपनीयता कार्य करते हैं। प्रॉक्सी सर्वर एप्लिकेशन-लेयर रीडायरेक्ट की तरह काम करता है और डेटा को एन्क्रिप्ट किए बिना विशिष्ट प्रोग्राम के लिए आपका IP पता छिपाता है। VPN नेटवर्क स्तर पर काम करता है और एन्क्रिप्शन से पूरे सिस्टम का ट्रैफ़िक सुरक्षित करता है। सही टूल का चुनाव आपकी सुरक्षा आवश्यकताओं पर निर्भर करता है।

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

चेकपॉइंट 1: बहुविकल्पीय चुनौती

1. एक मानक HTTP प्रॉक्सी OSI मॉडल की किस लेयर पर काम करती है?

- A. भौतिक लेयर
- B. नेटवर्क लेयर
- C. ऐप्लिकेशन लेयर
- D. डेटा लिंक लेयर

2. मानक HTTP प्रॉक्सी की तुलना में SOCKS5 का एक प्रमुख प्रोटोकॉल लाभ क्या है?

- A. यह पूर्ण पेलोड एन्क्रिप्शन को लागू करता है
- B. यह किसी भी TCP/UDP ट्रैफ़िक रूटिंग का समर्थन करता है
- C. यह DNS लीक से पूरी तरह सुरक्षित है
- D. यह सीधे कर्नेल स्पेस में काम करता है

3. VPN आम तौर पर प्रॉक्सी सर्वर से अधिक सुरक्षित क्यों होता है?

- A. यह अधिक तेज़ रिमोट हार्डवेयर पर चलता है
- B. यह पूरे सिस्टम का सारा नेटवर्क ट्रैफ़िक एन्क्रिप्ट करता है
- C. इसे स्थानीय रूटिंग टेबल की आवश्यकता नहीं होती
- D. यह नेटवर्क लेटेंसी को पूरी तरह खत्म कर देता है

4. कौन-सा प्रॉक्सी प्रकार डिफ़ॉल्ट रूप से बिना किसी एन्क्रिप्शन के ट्रैफ़िक रीडायरेक्ट करता है?

- A. बेसिक HTTP प्रॉक्सी
- B. एन्क्रिप्टेड HTTPS प्रॉक्सी
- C. सुरक्षित WireGuard क्लाइंट
- D. ऑब्फ़स्केटेड VPN सर्वर

5. ब्राउज़र प्रॉक्सी इस्तेमाल करते समय बैकग्राउंड ऐप ट्रैफ़िक का क्या होता है?

- A. यह अपने-आप एन्क्रिप्ट हो जाता है
- B. इसे प्रॉक्सी सर्वर ब्लॉक कर देता है
- C. इसे प्रॉक्सी टनल के ज़रिए रूट किया जाता है
- D. यह प्रॉक्सी को बायपास करता है और आपका IP उजागर कर देता है

चेकपॉइंट 2: सही या गलत चुनौती

6 प्रश्न 6

6. SOCKS5 प्रॉक्सी सर्वर से गुज़रने वाले सभी पैकेट पेलोड को एन्क्रिप्ट करता है।

○ सही ○ गलत

7 प्रश्न 7

7. VPN पूरे सिस्टम के ट्रैफ़िक को सुरक्षित करने के लिए नेटवर्क लेयर पर काम करता है।

○ सही ○ गलत

8 प्रश्न 8

8. प्रॉक्सी आम तौर पर VPN से तेज़ होते हैं क्योंकि वे डीप पैकेट एन्क्रिप्शन करते हैं।

○ सही ○ गलत

9 प्रश्न 9

9. प्रॉक्सी कॉन्फ़िगर करने के लिए विशिष्ट ऐप्स के भीतर ट्रैफ़िक रीडायरेक्शन सेट करने पड़ते हैं।

○ सही ○ गलत

10 प्रश्न 10

10. प्रॉक्सी का उपयोग आपके डेटा ट्रैफ़िक को स्थानीय ISP की ट्रैकिंग से सुरक्षित नहीं करता।

○ 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. ऐप्लिकेशन-परत का _____ ब्राउज़र के चुनिंदा ट्रैफ़िक को मोड़ता है, लेकिन दूसरे ऐप को सुरक्षित नहीं करता।

2. एक मज़बूत _____ डिवाइस के सभी डेटा पैकेटों को एनकैप्सुलेट और एन्क्रिप्ट करता है।

3. _____ प्रोटोकॉल ऐप्लिकेशन और ट्रांसपोर्ट परतों के बीच बैठता है।

4. HTTP प्रॉक्सी OSI मॉडल की _____ परत पर काम करते हैं।

5. मानक प्रॉक्सी सर्वरों में पेलोड _____ नहीं होता, जिससे डेटा असुरक्षित रहता है।

6. डेटा को सुरक्षित मार्ग के भीतर लपेटकर भेजने की तकनीक _____ कहलाती है।

शब्दावली शब्द-बैंक

एन्क्रिप्शन ऐप्लिकेशन टनलिंग प्रॉक्सी लेयर सेवन वीपीएन टनल सॉक्स फ़ाइव ISP की दृश्यता

अपने उत्तर यहाँ लिखें:

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

चेकपॉइंट 4: नेटवर्क अवधारणा मिलान

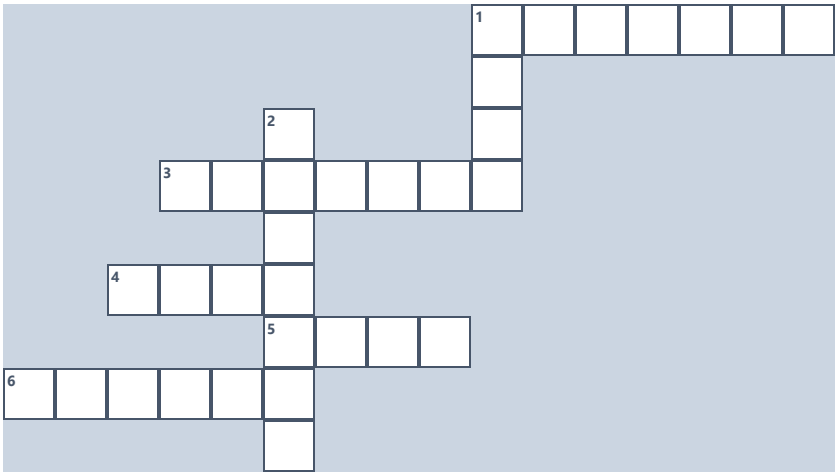
परिभाषा मिलान

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. HTTP प्रॉक्सी**	**A**	ऑपरेटिंग सिस्टम स्तर की रूटिंग जो सभी एप्लिकेशन ट्रैफ़िक को एन्क्रिप्ट करती है।
☐	**2. SOCKS5 प्रॉक्सी**	**B**	ऐप्लिकेशन लेयर, जहाँ मानक वेब प्रॉक्सी प्रोटोकॉल काम करते हैं।
☐	**3. VPN टनल**	**C**	SOCKS5 की TCP के साथ-साथ UDP को रिले करने की क्षमता, जो सादे HTTP प्रॉक्सी में नहीं होती।
☐	**4. सिस्टम-स्तर**	**D**	क्लाइंट एक्सटेंशन जो ट्रैफ़िक को केवल ब्राउज़र सैंडबॉक्स के भीतर छिपाता है।
☐	**5. OSI लेयर 7**	**E**	एन्क्रिप्शन और एनकैप्सुलेशन जो डिवाइस के सभी बैकग्राउंड ट्रैफ़िक को लपेटते हैं।
☐	**6. UDP सपोर्ट**	**F**	ट्रैफ़िक की वह स्थिति जिसमें बिना एन्क्रिप्ट किया प्रॉक्सी डेटा ISP को दिखता रहता है।
☐	**7. ब्राउज़र प्रॉक्सी**	**G**	ऐप्लिकेशन लेयर प्रॉक्सी जो विशिष्ट वेब ब्राउज़र ट्रैफ़िक को रीडायरेक्ट करती है।
☐	**8. ISP की दृश्यता**	**H**	ऐप्लिकेशन और ट्रांसपोर्ट लेयर के बीच का प्रॉक्सी प्रोटोकॉल, जिसमें कोई एन्क्रिप्शन नहीं होता।

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

1. ऐप्लिकेशन परत का प्रॉक्सी, जो ब्राउज़र के चुनिंदा वेब ट्रैफ़िक को दूसरी ओर मोड़ता है (7)

3. सादे HTTP प्रॉक्सी के विपरीत, SOCKS5 की TCP के साथ UDP को भी रिले करने की क्षमता (7)

4. आपके उपकरण और VPN सर्वर के बीच बना सुरक्षित संपर्क (4)

5. डेटा पैकेट को दूसरे पैकेट में लपेटकर नेटवर्क के पार भेजने की तकनीक (4)

6. वह ऐप्लिकेशन परत, जहाँ मानक वेब प्रॉक्सी प्रोटोकॉल काम करते हैं (6)

ऊपर से नीचे

1. जानकारी को कूट रूप में बदलकर दूसरों के लिए अपठनीय बनाने की विधि (4)

2. एन्क्रिप्शन और एनकैप्सुलेशन, जो डिवाइस के सारे बैकग्राउंड ट्रैफ़िक को लपेट लेता है (7)

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

1 बाएँ से दाएँ: ऐप्लिकेशन परत का प्रॉक्सी, जो ब्राउज़र के चुनिंदा वेब ट्रैफ़िक को दूसरी ओर मोड़ता है (7 अक्षर):

3 बाएँ से दाएँ: सादे HTTP प्रॉक्सी के विपरीत, SOCKS5 की TCP के साथ UDP को भी रिले करने की क्षमता (7 अक्षर):

4 बाएँ से दाएँ: आपके उपकरण और VPN सर्वर के बीच बना सुरक्षित संपर्क (4 अक्षर):

5 बाएँ से दाएँ: डेटा पैकेट को दूसरे पैकेट में लपेटकर नेटवर्क के पार भेजने की तकनीक (4 अक्षर):

6 बाएँ से दाएँ: वह ऐप्लिकेशन परत, जहाँ मानक वेब प्रॉक्सी प्रोटोकॉल काम करते हैं (6 अक्षर):

ऊपर से नीचे

1 ऊपर से नीचे: जानकारी को कूट रूप में बदलकर दूसरों के लिए अपठनीय बनाने की विधि (4 अक्षर):

2 ऊपर से नीचे: एन्क्रिप्शन और एनकैप्सुलेशन, जो डिवाइस के सारे बैकग्राउंड ट्रैफ़िक को लपेट लेता है (7 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।

र	दे	कि	जा	सा	वा	ड	क	रे	स	ख	नि	फ	ढ	मा
ना	का	रे	दे	सि	मी	क	ने	ले	पि	ता	ति	ज	श	भ
ऊ	अ	ऊ	ए	रि	वि	श	क्श	य	य	वि	व	वा	पा	ल
च	से	स	कि	य	घ	प	न	के	की	र	व	सि	री	त
की	कि	क्से	सि	ना	ए	ने	पा	ते	ण	ट	से	ए	ता	सा
न	मी	ए	न	नी	च	ऋ	वी	ले	घ	ति	न	व	जि	ला
र्थ	ए	जी	ले	ड	टी	ल	द	पी	जे	घ	के	लिं	न	च
म	से	दे	री	ए	टी	पी	उ	अ	ए	जे	मि	घ	ग	व
स	आ	च	मी	च	पी	ट	थ	फ	ग	न	ना	सी	का	ज
पी	फ	नी	जी	ता	प्रॉ	ठ	से	लि	ट	आ	ट	इ	से	रा
डी	के	री	पा	वा	क्सी	सि	य	नि	पि	ने	ख	न	के	वे
यू	ऊ	ड	नी	दे	ए	दि	भ	आ	नि	जे	वे	वे	ल	ष
ण	प	कि	से	य	ह	न्क्रि	ह	ते	रा	द	सा	सी	थ	जे
इ	मे	ला	ढ	पे	ऋ	वे	प्श	नी	वे	उ	थ	ह	जे	त
य	मी	रे	मि	दि	ए	ह	जे	न	जा	ढ	वी	रा	दा	पी

शब्दावली शब्द-सूची

एचटीटीपीप्रॉक्सी, वीपीएनटनल, लेयरसेवन, यूडीपीसमर्थन, कनेक्शन, टनलिंग, एन्क्रिप्शन, एक्सेस

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. एचटीटीपीप्रॉक्सी**
- **B. वीपीएनटनल**
- **C. लेयरसेवन**
- **D. यूडीपीसमर्थन**
- **E. कनेक्शन**
- **F. टनलिंग**
- **G. एन्क्रिप्शन**
- **H. एक्सेस**

परिभाषाएँ और मिलान फ़ील्ड

1. आपके उपकरण और VPN सर्वर के बीच बना सुरक्षित संपर्क।
2. डेटा पैकेट को दूसरे पैकेट में लपेटकर नेटवर्क के पार भेजने की तकनीक।
3. ऐप्लिकेशन परत का प्रॉक्सी, जो ब्राउज़र के चुनिंदा वेब ट्रैफ़िक को दूसरी ओर मोड़ता है।
4. जानकारी को कूट रूप में बदलकर दूसरों के लिए अपठनीय बनाने की विधि।
5. वह ऐप्लिकेशन परत, जहाँ मानक वेब प्रॉक्सी प्रोटोकॉल काम करते हैं।
6. सादे HTTP प्रॉक्सी के विपरीत, SOCKS5 की TCP के साथ UDP को भी रिले करने की क्षमता।
7. किसी सिस्टम, फ़ाइल या नेटवर्क तक पहुँचने की अनुमति।
8. एन्क्रिप्शन और एनकैप्सुलेशन, जो डिवाइस के सारे बैकग्राउंड ट्रैफ़िक को लपेट लेता है।

चेकपॉइंट 7: उलझे शब्दों की चुनौती

नीचे के अक्षरों को सुलझाकर VPN की प्रमुख अवधारणाएँ और शब्द पता करें। अपने उत्तर भरे जा सकने वाले इनपुट बॉक्स में लिखें।

1. **टी प्रॉ ए पी क्सी टी च** _____
2. **न ले र व से य** _____
3. **न क क्श ने** _____
4. **न प्श ए न्क्रि** _____
5. **ट ल न ए वी न पी** _____
6. **र्थ पी म यू स न डी** _____
7. **लिं ट ग न** _____
8. **स क्से ए** _____

अतिरिक्त गतिविधि: झटपट सोचें

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

1	प्रॉक्सी और VPN के बीच अंतर			
2	VPN के बिना अनएन्क्रिप्टेड रहने वाली चीज़ें			
3	नकली Wi-Fi नेटवर्क पहचानने के तरीके			
4	रोज़मर्रा की ज़िंदगी में बिचौलिया जो काम करता है			
5	ऐसी स्थितियाँ जिनमें प्रॉक्सी काफ़ी है			
6	ऐसे डिवाइस जो VPN इस्तेमाल कर सकते हैं			
7	आपके जाने-पहचाने प्रॉक्सी के प्रकार			
8	ऐसी चीज़ें जिन्हें VPN छिपा सकता है			
9	VPN के बारे में मिथक			
10	अच्छे VPN प्रदाता के वादे			
11	ऐसी चीज़ें जिनसे VPN आपको नहीं बचा सकता			
12	इस वर्कशीट के वे शब्द जिन्हें आप याद रखना चाहते हैं			
13	यात्रा के दौरान VPN इस्तेमाल करने के कारण			
14	ऐसी स्थितियाँ जिनमें आप VPN चाहेंगे			
15	ऐसी जगहें जहाँ आप VPN इस्तेमाल करेंगे			

चेकपॉइंट 8: VPN केस स्टडी

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

सारा (कॉफ़ी शॉप की छात्रा)

👱 "नमस्ते! मैं Coffee & Bytes में हूँ और 'Free_Wi-Fi_No_Password' नाम के खुले नेटवर्क पर हूँ। मुझे अपने स्कूल के ईमेल में लॉग इन करना है, और एक दोस्त कहता है कि सुरक्षित रहने के लिए मुफ़्त ब्राउज़र प्रॉक्सी काफ़ी है। क्या प्रॉक्सी मेरे लॉगिन और फ़ाइलों की सुरक्षा करेगा, या मुझे VPN चाहिए?"

Alex (यात्री छात्र)

👱 "मैं विदेश में हूँ और मेरे गृह देश में होस्ट की गई एक जीव विज्ञान डॉक्यूमेंट्री पर लिखा आ रहा है 'यह वीडियो आपकी वर्तमान लोकेशन में उपलब्ध नहीं है।' मेरा एक सहपाठी प्रॉक्सी इस्तेमाल करता है, और मेरे पास VPN है। मुझे ब्लॉक क्यों किया जा रहा है, और कौन-सा टूल बेहतर काम करेगा?"

चेकपॉइंट 9: कूट संदेश को डिकोड करें

अपनी प्रॉक्सी तुलना की ट्रेनिंग पूरी करने के लिए, सुरक्षित टनलिंग के बारे में यह गुप्त संदेश डिक्रिप्ट करें।

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

33	61	39	56	13	61	44	48		44	52		1	33	32	46

23	61	39	53	34	60	47	13		37	54	25	60	52	57

डिकोड किया गया संदेश:

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

चेकपॉइंट 10: बुनियादी VPN FAQ (भाग A)

वर्चुअल प्राइवेट नेटवर्क के उपयोग के बारे में संभावित ग्राहकों के सबसे आम सवाल और जवाब देखें।

Q1: VPN क्या है और यह कैसे काम करता है?

वर्चुअल प्राइवेट नेटवर्क (VPN) आपके इंटरनेट कनेक्शन को एन्क्रिप्ट करता है और आपके ट्रैफ़िक को एक सुरक्षित रिमोट सर्वर से भेजता है। इससे आपका सार्वजनिक IP पता छिप जाता है और VPN टनल से गुज़रने वाले ट्रैफ़िक के बारे में स्थानीय नेटवर्क पर नज़र रखने वाले और आपका ISP जो देख सकते हैं, वह सीमित हो जाता है।

Q2: प्रॉक्सी सर्वर क्या है?

प्रॉक्सी सर्वर एक मध्यस्थ है जो आपके एप्लिकेशन और गंतव्य सर्वर के बीच अनुरोध आगे भेजता है। वेबसाइट को आपके बजाय प्रॉक्सी का IP पता दिखता है, लेकिन केवल प्रॉक्सी का उपयोग करने के लिए कॉन्फ़िगर किए गए ऐप्स का ट्रैफ़िक ही मोड़ा जाता है, और बेसिक प्रॉक्सी उस ट्रैफ़िक को एन्क्रिप्ट नहीं करता।

Q3: क्या VPN मुझे ऑनलाइन पूरी तरह गुमनाम बना देता है?

नहीं। VPN आपका IP पता छिपाता है और ट्रैफ़िक एन्क्रिप्ट करता है, फिर भी आपको ब्राउज़र कुकी, सक्रिय खातों (जैसे Google या Facebook), ब्राउज़र फ़िंगरप्रिंटिंग, या VPN प्रदाता द्वारा आपका डेटा लॉग करने से ट्रैक किया जा सकता है।

Q4: क्या VPN मेरी इंटरनेट स्पीड धीमी कर देगा?

हाँ, थोड़ी। एन्क्रिप्शन प्रक्रिया और VPN सर्वर की भौतिक दूरी लेटेंसी और ओवरहेड बढ़ाती है। असर प्रोवाइडर, प्रोटोकॉल, सर्वर की दूरी, डिवाइस और नेटवर्क की स्थिति के अनुसार बदलता है।

Q5: क्या प्रॉक्सी एक VPN है?

नहीं। प्रॉक्सी चुनिंदा ऐप का ट्रैफ़िक रिले करता है, आमतौर पर बिना एन्क्रिप्शन के। VPN नेटवर्क परत पर एक एन्क्रिप्टेड टनल बनाता है, जो डिवाइस का सारा ट्रैफ़िक, बैकग्राउंड ऐप सहित, ले जाती है।

चेकपॉइंट 10: बुनियादी VPN FAQ (भाग B)

वर्चुअल प्राइवेट नेटवर्क के उपयोग के बारे में संभावित ग्राहकों के सबसे आम सवाल और जवाब देखें।

Q6: क्या मैं मुफ़्त प्रॉक्सी उपयोग कर सकता हूँ?

आप कर सकते हैं, लेकिन मुफ़्त प्रॉक्सी अक्सर अज्ञात संचालक चलाते हैं। चूँकि बुनियादी प्रॉक्सी ट्रैफ़िक को एन्क्रिप्ट नहीं करता, उसका संचालक अनएन्क्रिप्टेड पेज देख सकता है और बदल भी सकता है। उपयोग से पहले जाँच लें कि सेवा कौन चलाता है।

Q7: क्या प्रॉक्सी लॉग रखता है?

हाँ, ऐसा हो सकता है। प्रॉक्सी हर उस रिक्वेस्ट को संभालता है जिसे वह फ़ॉरवर्ड करता है, इसलिए उसका ऑपरेटर आपका IP पता, आपकी देखी गई साइटें और उनका समय रिकॉर्ड कर सकता है। जाँचें कि उसे कौन चलाता है और उसकी गोपनीयता नीति क्या कहती है।

Q8: प्रॉक्सी कब पर्याप्त होता है?

कम जोखिम वाले कार्यों के लिए प्रॉक्सी पर्याप्त हो सकता है, जैसे एक ब्राउज़र की दिखाई देने वाली लोकेशन बदलना। बैंकिंग, सार्वजनिक Wi-Fi या डिवाइस के हर ऐप की सुरक्षा के लिए VPN अधिक सुरक्षित विकल्प है, क्योंकि वह सारा ट्रैफ़िक एन्क्रिप्ट करता है।

Q9: क्या प्रॉक्सी मेरे फ़ोन के सभी ऐप्स की सुरक्षा कर सकता है?

नहीं। केवल वही ऐप प्रॉक्सी सेटिंग का सम्मान करते हैं जो उसका उपयोग करते हैं; बाकी सीधे कनेक्ट होते हैं। इसके बजाय VPN ऐप फ़ोन के सभी ऐप को अपनी एन्क्रिप्टेड टनल से रूट करता है।

Q10: SOCKS5 प्रॉक्सी क्या है?

RFC 1928 में परिभाषित SOCKS5 एक प्रॉक्सी प्रोटोकॉल है, जो एप्लिकेशन और ट्रांसपोर्ट लेयर के बीच काम करता है। यह TCP कनेक्शन और UDP डेटाग्राम रिले कर सकता है और ऑथेंटिकेशन को सपोर्ट करता है, लेकिन इसमें अंतर्निहित एन्क्रिप्शन नहीं है। [1]

चेकपॉइंट 10: उन्नत VPN FAQ (भाग C)

वर्चुअल प्राइवेट नेटवर्क और सुरक्षित टनलिंग प्रोटोकॉल के तकनीकी और संरचनात्मक पहलुओं को जानें।

Q1: प्रॉक्सी और VPN किन नेटवर्क लेयर पर काम करते हैं?

HTTP प्रॉक्सी एप्लिकेशन लेयर (Layer 7) पर काम करता है और वेब अनुरोधों को समझता है। SOCKS5 एप्लिकेशन और ट्रांसपोर्ट लेयर के बीच रहता है। IPsec या WireGuard जैसे VPN प्रोटोकॉल नेटवर्क लेयर पर काम करते हैं, इसलिए वे डिवाइस का सारा IP ट्रैफ़िक ले जा सकते हैं।

Q2: क्या प्रॉक्सी के ज़रिए HTTPS साइट एन्क्रिप्टेड रहती है?

हाँ। जब आप प्रॉक्सी के ज़रिए HTTPS साइट खोलते हैं, तो TLS एन्क्रिप्शन आपके ब्राउज़र और साइट के बीच एंड-टू-एंड चलता है, इसलिए प्रॉक्सी डोमेन देखता है लेकिन पेज की सामग्री नहीं। सादे HTTP पेज पढ़े जा सकते हैं।

Q3: WebRTC लीकिंग क्या है और VPN इसे कैसे रोकता है?

WebRTC एक ब्राउज़र प्रोटोकॉल है जो VPN सक्रिय होने पर भी आपके असली लोकल और सार्वजनिक IP पते उजागर कर सकता है। प्रीमियम VPN अपने डेस्कटॉप/मोबाइल ऐप और ब्राउज़र एक्सटेंशन में WebRTC अनुरोधों को ब्लॉक या स्पूफ़ करते हैं।

Q4: ट्रांसपेरेंट प्रॉक्सी क्या है और इसे कौन उपयोग करता है?

ट्रांसपेरेंट प्रॉक्सी उपयोगकर्ता के डिवाइस पर कोई सेटअप किए बिना ट्रैफ़िक को बीच में पकड़ लेता है। स्कूल, कंपनियाँ और ISP इनका उपयोग कैशिंग या सामग्री फ़िल्टरिंग के लिए करते हैं। उपयोगकर्ताओं को अक्सर पता नहीं होता कि कोई लगा है, और यह उन्हें कोई गोपनीयता नहीं देता।

Q5: ऑब्फ़स्केशन VPN ब्लॉक को कैसे बायपास करता है?

ऑब्फ़स्केशन (या "Stealth VPN") VPN ट्रैफ़िक को ऐसा रूप देता है कि वह सामान्य HTTPS ट्रैफ़िक (पोर्ट 443) जैसा दिखे। इससे सरकारों या स्कूल/ऑफ़िस नेटवर्क द्वारा VPN रोकने के लिए इस्तेमाल की जाने वाली डीप पैकेट इंस्पेक्शन (DPI) को पार करने में मदद मिल सकती है।

चेकपॉइंट 10: उन्नत VPN FAQ (भाग D)

वर्चुअल प्राइवेट नेटवर्क और सुरक्षित टनलिंग प्रोटोकॉल के तकनीकी और संरचनात्मक पहलुओं को जानें।

Q6: स्प्लिट टनलिंग क्या है और इसका उपयोग कब करना चाहिए?

स्प्लिट टनलिंग आपको चुनने देती है कि कौन से ऐप एन्क्रिप्टेड VPN टनल से जाएँ और कौन सीधे इंटरनेट से जुड़ें। संवेदनशील बैंकिंग ऐप को VPN से भेजने और स्थानीय गेम को सीधे जोड़ने के लिए इसका उपयोग करें, जिससे VPN से जुड़ी लेटेंसी से बचा जा सके।

Q7: प्रॉक्सी VPN कनेक्शन से तेज़ क्यों महसूस हो सकता है?

बेसिक प्रॉक्सी एन्क्रिप्शन छोड़ देता है और केवल एक ऐप का ट्रैफ़िक संभालता है, इसलिए प्रोसेसिंग कम लगती है। VPN डिवाइस के हर पैकेट को एन्क्रिप्ट करता है। आधुनिक प्रोटोकॉल के साथ अंतर अक्सर छोटा होता है, और प्रॉक्सी कहीं कम सुरक्षा देता है।

Q8: क्या वेबसाइटें पता लगा सकती हैं कि मैं प्रॉक्सी या VPN उपयोग करता हूँ?

अक्सर हाँ। कई साइटें IP पतों को ज्ञात प्रॉक्सी और VPN सर्वरों की सूचियों से मिलाती हैं, और HTTP प्रॉक्सी Via या X-Forwarded-For जैसे हेडर जोड़ सकते हैं। स्ट्रीमिंग सेवाएँ आम तौर पर दोनों को ब्लॉक करती हैं।

Q9: DNS Leak सुरक्षा क्या है?

DNS लीक सुरक्षा आपके डिवाइस को वेबसाइट लुकअप क्वेरी (DNS क्वेरी) अपने ISP के सर्वरों के बजाय VPN के निजी, एन्क्रिप्टेड DNS सर्वरों से भेजने के लिए बाध्य करती है। इससे आपका ISP यह ट्रैक नहीं कर पाता कि आप कौन-सी साइटें देखते हैं।

Q10: क्या प्रॉक्सी ISP थ्रॉटलिंग रोक सकता है?

कभी-कभार ही। साधारण प्रॉक्सी ट्रैफ़िक को एन्क्रिप्ट नहीं करता, इसलिए ISP अब भी देख सकता है कि गतिविधि किस प्रकार की है। VPN ट्रैफ़िक के प्रकार को छिपाता है, लेकिन कोई भी टूल भीड़भाड़ या डेटा सीमा की समस्या ठीक नहीं करता।

भाग 11: 10 रोचक VPN तथ्य और वास्तविक दुनिया की अंतर्दृष्टियाँ

VPN के इतिहास, बाज़ार और तकनीक से जुड़े इन बेहद उपयोगी, वास्तविक तथ्यों और अंतर्दृष्टियों को देखें।

1. SOCKS मानक

SOCKS Protocol Version 5 को IETF ने मार्च 1996 में RFC 1928 के रूप में प्रकाशित किया था और आज भी ब्राउज़र और ऐप द्वारा इस्तेमाल किए जाने वाले SOCKS5 प्रॉक्सी की संदर्भ विशिष्टता यही है। [1]

2. शिम लेयर

RFC 1928 SOCKS को एप्लिकेशन और ट्रांसपोर्ट लेयर के बीच एक शिम लेयर के रूप में बताता है, इसलिए यह ICMP जैसे नेटवर्क-लेयर ट्रैफ़िक को फ़ॉरवर्ड नहीं कर सकता। [1]

3. UDP रिले

SOCKS5 ने UDP ASSOCIATE कमांड जोड़ी, जिससे प्रॉक्सी TCP कनेक्शन के साथ UDP डेटाग्राम भी रिले कर सकता है; सादे HTTP प्रॉक्सी यह नहीं कर पाते। [1]

4. डिफ़ॉल्ट SOCKS पोर्ट

RFC 1928 के अनुसार, SOCKS5 क्लाइंट डिफ़ॉल्ट रूप से TCP पोर्ट 1080 पर प्रॉक्सी सर्वर से जुड़ते हैं; कई प्रॉक्सी सेवाएँ उपयोगकर्ताओं को दूसरे पोर्ट चुनने देती हैं। [1]

5. HTTP मध्यस्थ

HTTP मानक (RFC 9110) प्रॉक्सी को क्लाइंट द्वारा चुना गया संदेश-अग्रेषण एजेंट बताता है, जो अनुरोधों को ओरिजिन सर्वर की ओर आगे भेजता है।

6. डीप पैकेट इंस्पेक्शन

डीप पैकेट इंस्पेक्शन (DPI) पैकेट की सामग्री और ट्रैफ़िक पैटर्न की जाँच करता है; अनएन्क्रिप्टेड प्रॉक्सी ट्रैफ़िक उसे पूरी तरह दिखता है, जबकि VPN ट्रैफ़िक से बहुत कम जानकारी मिलती है।

7. नेटवर्क-लेयर VPN

NIST SP 800-77 में वर्णित IPsec नेटवर्क लेयर पर ट्रैफ़िक की रक्षा करता है, इसलिए हर एप्लिकेशन के IP पैकेट को प्रति-ऐप सेटअप के बिना सुरक्षित किया जा सकता है। [2]

8. केवल ब्राउज़र तक सीमित दायरा

एक ब्राउज़र में सेट किया गया प्रॉक्सी केवल उसी ब्राउज़र को प्रभावित करता है; ईमेल क्लाइंट, गेम और सिस्टम अपडेट डिवाइस के सामान्य कनेक्शन का ही उपयोग करते रहते हैं।

9. TOR बनाम प्रॉक्सी

Tor ट्रैफ़िक को तीन स्वयंसेवी रिले (गार्ड, मिडिल और एग्ज़िट) से भेजता है और आमतौर पर स्थानीय SOCKS प्रॉक्सी से पहुँचा जाता है, जो ऐसी परतें जोड़ता है जो अकेली प्रॉक्सी नहीं जोड़ सकती।

10. गति के बदले समझौता

प्रॉक्सी तेज़ लग सकते हैं क्योंकि वे एन्क्रिप्शन छोड़ देते हैं, लेकिन WireGuard जैसे आधुनिक VPN प्रोटोकॉल बहुत कम ओवरहेड जोड़ते हैं और डिवाइस का सारा ट्रैफ़िक सुरक्षित रखते हैं।

तकनीकी संदर्भ और स्रोत

इस वर्कशीट में उपयोग किए गए उद्धृत प्रकाशन, क्रिप्टोग्राफ़िक विनिर्देश और आधिकारिक दस्तावेज़ मानक।

शैक्षणिक और उद्योग संदर्भ

[1] IETF. (1996). RFC 1928: SOCKS Protocol Version 5.
https://datatracker.ietf.org/doc/html/rfc1928

[2] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.
https://csrc.nist.gov/pubs/sp/800/77/r1/final

[3] WireGuard. (n.d.). WireGuard: fast, modern, secure VPN tunnel.
https://www.wireguard.com/

[4] WireGuard. (n.d.). Protocol & Cryptography.
https://www.wireguard.com/protocol/

[5] OpenVPN. (n.d.). OpenVPN 2.6 Manual.
https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

उत्तर कुंजी: प्रॉक्सी सर्वर और वर्चुअल प्राइवेट नेटवर्क की तुलना, एन्क्रिप्शन के अंतर और ऐप-स्तरीय बनाम सिस्टम-व्यापी रूटिंग

1 **प्रॉक्सी का OSI लेयर** प्रोटोकॉल — **सही उत्तर: C**

शिक्षण नोट

मानक HTTP/HTTPS प्रॉक्सी एप्लिकेशन परत (Layer 7) पर काम करते हैं और विशिष्ट ब्राउज़र ट्रैफ़िक को रीडायरेक्ट करते हैं। उनमें सिस्टम-व्यापी नेटवर्क रूटिंग नहीं होती। उद्धरण: Tor Project Foundation।

2 **प्रश्न 2** — **सही उत्तर: B**

शिक्षण नोट

SOCKS5 ऐप्लिकेशन और ट्रांसपोर्ट लेयर के बीच TCP और UDP ट्रैफ़िक रिले करता है लेकिन डिफ़ॉल्ट रूप से एन्क्रिप्ट नहीं करता, जबकि HTTP प्रॉक्सी वेब अनुरोध संभालती हैं।

3 **VPN सिस्टम एन्क्रिप्शन** वाई-फ़ाई सुरक्षा — **सही उत्तर: B**

शिक्षण नोट

VPN पूरे ऑपरेटिंग सिस्टम के ट्रैफ़िक को सिस्टम-व्यापी रूप से समाहित और एन्क्रिप्ट करता है, जबकि प्रॉक्सी केवल कॉन्फ़िगर किए गए विशिष्ट एप्लिकेशन का ट्रैफ़िक ही मोड़ता है। संदर्भ: Deloitte Advisory।

4 **प्रॉक्सी में एन्क्रिप्शन की कमी** रूटिंग नियंत्रण — **सही उत्तर: A**

शिक्षण नोट

HTTP प्रॉक्सी ब्राउज़र ट्रैफ़िक को एप्लिकेशन लेयर पर फ़ॉरवर्ड करते हैं और पैकेट पेलोड को एन्क्रिप्ट नहीं करते, यानी आपका नेटवर्क ऑपरेटर या ISP अब भी आपके कंटेंट ट्रैफ़िक का पता लगा सकता है। उद्धरण: IETF Proxy Vulnerabilities।

5 **बायपास की कमज़ोरी** गोपनीयता — **सही उत्तर: D**

शिक्षण नोट

ब्राउज़र प्रॉक्सी केवल वेब ब्राउज़र पर ही नियम लागू करती हैं। बैकग्राउंड ऐप्स, ऑपरेटिंग सिस्टम अपडेट और ईमेल क्लाइंट प्रॉक्सी को बायपास करते हैं, जिससे आपका मूल IP पता उजागर हो जाता है। उद्धरण: W3C Consortium।

उत्तर कुंजी: चेकपॉइंट 2 – सही या गलत

6 **प्रश्न 6** **सही उत्तर: गलत**

शिक्षण नोट

SOCKS5 ऐप्लिकेशन और ट्रांसपोर्ट लेयर के बीच ट्रैफ़िक रिले करता है लेकिन डिफ़ॉल्ट रूप से कोई एन्क्रिप्शन नहीं करता, इसलिए रास्ते में पैकेट की सामग्री पढ़ी जा सकती है।

7 **नेटवर्क लेयर टनल** गति **सही उत्तर: सही**

शिक्षण नोट

नेटवर्क लेयर पर चलकर VPN आपके डिवाइस से बाहर जाने वाले ट्रैफ़िक को रूट और एन्क्रिप्ट करता है, जिससे पूरे सिस्टम के ट्रैफ़िक की सुरक्षा में मदद मिलती है। उद्धरण: Deloitte Advisory।

8 **प्रॉक्सी की एन्क्रिप्शन सीमा** स्निफ़िंग का जोखिम **सही उत्तर: गलत**

शिक्षण नोट

प्रॉक्सी कभी-कभी तेज़ हो सकते हैं, लेकिन इसका कारण यह है कि वे एन्क्रिप्शन नहीं करते। एन्क्रिप्शन की यह कमी डेटा को निरीक्षण के प्रति असुरक्षित छोड़ देती है। उद्धरण: IETF Proxy Vulnerabilities.

9 **ऐप-स्तरीय रीडायरेक्शन** फ़ायरवॉल **सही उत्तर: सही**

शिक्षण नोट

पूरे सिस्टम पर चलने वाले VPN के विपरीत, प्रॉक्सी सर्वर के लिए ब्राउज़र सेटिंग्स या ऐप-विशिष्ट प्रॉक्सी फ़ील्ड में मैन्युअल सेटअप करना पड़ता है। उद्धरण: W3C Consortium।

10 **ISP ट्रैकिंग का जोखिम** नो-लॉग्स **सही उत्तर: सही**

शिक्षण नोट

क्योंकि मानक HTTP/SOCKS5 प्रॉक्सी पेलोड डेटा को एन्क्रिप्ट नहीं करतीं, आपका स्थानीय ISP आपकी ऑनलाइन गतिविधियों को पूरी तरह देख सकता है। उद्धरण: EDRi Retention Guidelines।

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

G 1. HTTP प्रॉक्सी	H 2. SOCKS5 प्रॉक्सी	E 3. VPN टनल	A 4. सिस्टम-स्तर
B 5. OSI लेयर 7	C 6. UDP सपोर्ट	D 7. ब्राउज़र प्रॉक्सी	F 8. ISP की दृश्यता

चेकपॉइंट 3: उत्तर – प्रमुख शब्द

1 प्रॉक्सी	2 वीपीएन टनल	3 सॉक्स फ़ाइव	4 ऐप्लिकेशन
5 एन्क्रिप्शन	6 टनलिंग		

चेकपॉइंट 6, वैकल्पिक: उत्तर – शब्द मिलान

1 E – कनेक्शन	2 F – टनलिंग	3 A – एचटीटीपीप्रॉक्सी	4 G – एन्क्रिप्शन
5 C – लेयरसेवन	6 D – यूडीपीसमर्थन	7 H – एक्सेस	8 B – वीपीएनटनल

शिक्षकों के लिए चर्चा नोट

प्रमुख शब्द:
जाँचें कि क्या विद्यार्थी HTTP प्रॉक्सी, SOCKS5 प्रॉक्सी और VPN टनल 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।

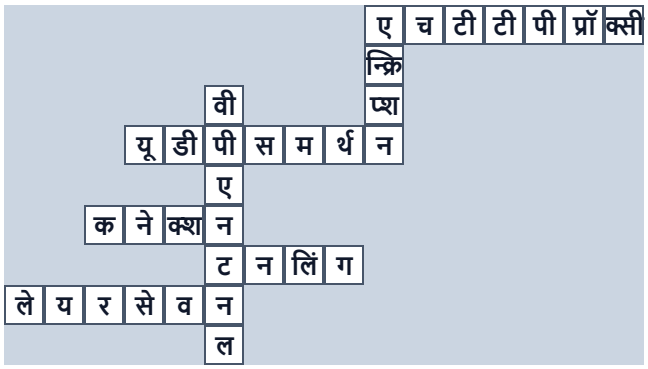
स्रोतों का मूल्यांकन:
विद्यार्थियों से वर्कशीट के स्रोतों में कम से कम एक कथन की पुष्टि करवाएँ और चर्चा करें कि आँकड़े, कीमतें और नियम समय के साथ क्यों बदल सकते हैं।

पहेलियों की कुंजियाँ और शिक्षक नोट

शब्द खोज समाधान

र	दे	कि	जा	सा	वा	ड	क	रे	स	ख	नि	फ	ढ	मा
ना	का	रे	दे	सि	मी	क	ने	ले	पि	ता	ति	ज	श	भ
ऊ	अ	ऊ	ए	रि	वि	श	क्श	य	य	वि	व	वा	पा	ल
च	से	स	कि	य	घ	प	न	के	की	र	व	सि	री	त
की	कि	क्से	सि	ना	ए	ने	पा	ते	ण	ट	से	ए	ता	सा
न	मी	ए	न	नी	च	ऋ	वी	ले	घ	ति	न	व	जि	ला
र्थ	ए	जी	ले	ड	टी	ल	द	पी	जे	घ	के	लिं	न	च
म	से	दे	री	ए	टी	पी	उ	अ	ए	जे	मि	घ	ग	व
स	आ	च	मी	च	पी	ट	थ	फ	ग	न	ना	सी	का	ज
पी	फ	नी	जी	ता	प्रॉ	ठ	से	लि	ट	आ	ट	इ	से	रा
डी	के	री	पा	वा	क्सी	सि	य	नि	पि	ने	ख	न	के	वे
यू	ऊ	ड	नी	दे	ए	दि	भ	आ	नि	जे	वे	वे	ल	ष
ण	प	कि	से	य	ह	न्क्रि	ह	ते	रा	द	सा	सी	थ	जे
इ	मे	ला	ढ	पे	ऋ	वे	प्श	नी	वे	उ	थ	ह	जे	त
य	मी	रे	मि	दि	ए	ह	जे	न	जा	ढ	वी	रा	दा	पी

क्रॉसवर्ड समाधान



क्रॉसवर्ड समाधान के लिए शिक्षक गाइड

बाएँ से दाएँ

1 बाएँ से दाएँ: एचटीटीपीप्रॉक्सी ऐप्लिकेशन परत का प्रॉक्सी, जो ब्राउज़र के चुनिंदा वेब ट्रैफ़िक को दूसरी ओर मोड़ता है (7 अक्षर)

3 बाएँ से दाएँ: यूडीपीसमर्थन सादे HTTP प्रॉक्सी के विपरीत, SOCKS5 की TCP के साथ UDP को भी रिले करने की क्षमता (7 अक्षर)

4 बाएँ से दाएँ: कनेक्शन आपके उपकरण और VPN सर्वर के बीच बना सुरक्षित संपर्क (4 अक्षर)

5 बाएँ से दाएँ: टनलिंग डेटा पैकेट को दूसरे पैकेट में लपेटकर नेटवर्क के पार भेजने की तकनीक (4 अक्षर)

6 बाएँ से दाएँ: लेयरसेवन वह ऐप्लिकेशन परत, जहाँ मानक वेब प्रॉक्सी प्रोटोकॉल काम करते हैं (6 अक्षर)

ऊपर से नीचे

1 ऊपर से नीचे: एन्क्रिप्शन जानकारी को कूट रूप में बदलकर दूसरों के लिए अपठनीय बनाने की विधि (4 अक्षर)

2 ऊपर से नीचे: वीपीएनटनल एन्क्रिप्शन और एनकैप्सुलेशन, जो डिवाइस के सारे बैकग्राउंड ट्रैफ़िक को लपेट लेता है (7 अक्षर)

अक्षर-फेर शब्द और कूट संदेश हल कुंजी

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

शब्द अनस्क्रैम्बल कुंजी

1. टीप्रॉएपीक्सीटीच → **एचटीटीपीप्रॉक्सी**
2. नलेरवसेय → **लेयरसेवन**
3. नकक्शने → **कनेक्शन**
4. नप्शएन्क्रि → **एन्क्रिप्शन**
5. टलनएवीनपी → **वीपीएनटनल**
6. र्थपीमयूसनडी → **यूडीपीसमर्थन**
7. लिंटगन → **टनलिंग**
8. सक्सेए → **एक्सेस**

गुप्त कूट चुनौती कुंजी

"प्रॉक्सी से अपना ट्रैफ़िक मोड़ें"

केस स्टडी के उत्तर

A परिदृश्य A: सार्वजनिक नेटवर्क की सुरक्षा

स्निफ़िंग और एन्क्रिप्शन | सारा की दुविधा

ग्रेडिंग दिशानिर्देश

छात्रों के उत्तरों में निम्नलिखित बिंदु शामिल होने चाहिए:

- जोखिम: पैकेट स्निफ़िंग, डेटा इंटरसेप्शन और मैन-इन-द-मिडिल हमले। उसी कॉफ़ी शॉप नेटवर्क पर मौजूद कोई व्यक्ति उसके लॉगिन विवरण या होमवर्क फ़ाइल को कैप्चर कर सकता है।
- प्रॉक्सी बनाम VPN: एक सामान्य ब्राउज़र प्रॉक्सी उसके ट्रैफ़िक को एन्क्रिप्ट नहीं करता। VPN डिवाइस पर सब कुछ एन्क्रिप्ट करता है, जिससे बीच में पकड़े गए पैकेट स्थानीय जासूसों के लिए पढ़ने योग्य नहीं रहते।

B परिदृश्य B: ब्लॉक किए गए संसाधनों तक पहुँचना

जियो-ब्लॉकिंग और IP | Alex की दुविधा

ग्रेडिंग दिशानिर्देश

छात्रों के उत्तरों में निम्नलिखित बिंदु शामिल होने चाहिए:

- ब्लॉक होने का कारण: स्ट्रीमिंग होस्ट जियो-ब्लॉकिंग का उपयोग करता है, जो यात्री के लोकल IP पते को उसके भौतिक देश से जोड़ता है और क्षेत्रीय लाइसेंसिंग के आधार पर उसे ब्लॉक कर देता है।
- कौन बेहतर काम करता है: दोनों उसे अपने देश का IP देते हैं, लेकिन प्रॉक्सी केवल कॉन्फ़िगर किए गए ऐप को कवर करता है, जबकि VPN उसके डिवाइस का सारा ट्रैफ़िक भी एन्क्रिप्ट करता है।