نام: _____ تاریخ: _____ نمبر: _____

پراکسی بمقابلہ VPN ورک شیٹ

پراکسی سرورز اور ورچوئل پرائیویٹ نیٹ ورکس کا موازنہ، خفیہ کاری کے فرق، اور ایپلیکیشن کی سطح بمقابلہ سسٹم گیر روٹنگ

VPN کا تعلیمی جائزہ

سیکھنے والا
طالب علم کی حیثیت
نیٹ ورک ڈیفینڈر ٹریک

محفوظ
کنکشن کی صورتحال
ڈیٹا پیکٹس کی حفاظت

فعال
لیک سے تحفظ
DNS اور IPv6 لیک سے تحفظ

خوش آمدید! یہ سرگرمی پیکٹ آپ کو ورچوئل پرائیویٹ نیٹ ورکس (VPNs) کے بنیادی اصولوں سے متعارف کراتا ہے۔ آپ جائزہ لیں گے کہ خفیہ ٹنلز آپ کے ڈیٹا کو کیسے محفوظ بناتی ہیں، نیٹ ورک پروٹوکولز کیسے کام کرتے ہیں، اور رازداری کے لیکس کی نشاندہی اور تدارک کیسے کیا جائے۔

ورک شیٹ کے چیک پوائنٹس

- [ ] حصہ 1-4: VPN کے تصورات اور پروٹوکولز 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 VPN گائیڈ کھولیں

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

آپ کا VPN لرننگ روڈ میپ

- ایپلیکیشن پراکسیز کا سسٹم گیر VPN خفیہ کاری سے موازنہ کریں۔
- بنیادی HTTP پراکسیز کے مقابلے میں SOCKS5 کی صلاحیتوں کی نشاندہی کریں۔
- تجزیہ کریں کہ براؤزر پر مبنی پراکسیاں پس منظر کی ایپس کو کیسے غیر محفوظ چھوڑ دیتی ہیں۔
- سمجھیں کہ ISPs پراکسی ٹنلز پر غیر خفیہ کردہ ٹریفک کو کیسے لاگ کرتے ہیں۔
- اسپیڈ اور سیکیورٹی کی ضروریات کے مطابق درست روٹنگ ٹول منتخب کریں۔

پراکسی موازنہ ورک شیٹ 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 پراکسیز اور VPN کے موازنے پر لاگو کریں۔ اور آخر میں اضافی سرگرمی "تیزی سے سوچیں"۔

پراکسی بمقابلہ VPN (تعارف)

پراکسیز اور VPNs مختلف ڈیجیٹل رازداری کے کام انجام دیتے ہیں۔ پراکسی سرور ایپلیکیشن لیئر ری ڈائریکٹ کے طور پر کام کرتا ہے، جو ڈیٹا کو انکرپٹ کیے بغیر مخصوص پروگراموں کے لیے آپ کا IP ایڈریس چھپاتا ہے۔ VPN نیٹ ورک سطح پر کام کرتا ہے اور تمام سسٹم ٹریفک کو خفیہ کاری سے محفوظ بناتا ہے۔ صحیح ٹول کا انتخاب آپ کی سیکیورٹی ضروریات پر منحصر ہے۔

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

چیک پوائنٹ 1: کثیر انتخابی چیلنج

1. معیاری HTTP پراکسی OSI ماڈل کی کس لیئر پر کام کرتی ہے؟
   - A. فزیکل لیئر
   - B. نیٹ ورک لیئر
   - C. ایپلی کیشن لیئر
   - D. ڈیٹا لنک لیئر

2. معیاری HTTP پراکسیز کے مقابلے میں SOCKS5 کا پروٹوکول کے لحاظ سے اہم فائدہ کیا ہے؟
   - A. یہ مکمل پے لوڈ خفیہ کاری نافذ کرتا ہے
   - B. یہ کسی بھی TCP/UDP ٹریفک کی روٹنگ کو سپورٹ کرتا ہے
   - C. یہ DNS لیکس سے محفوظ ہے
   - D. یہ براہِ راست کرنل اسپیس میں کام کرتا ہے

3. VPN عموماً پراکسی سرور سے زیادہ محفوظ کیوں ہوتا ہے؟
   - A. یہ زیادہ تیز ریموٹ ہارڈ ویئر پر چلتا ہے
   - B. یہ پورے سسٹم کے تمام نیٹ ورک ٹریفک کو خفیہ کرتا ہے
   - C. اسے مقامی روٹنگ ٹیبلز کی ضرورت نہیں ہوتی
   - D. یہ نیٹ ورک لیٹنسی کو مکمل طور پر ختم کر دیتا ہے

4. کون سی پراکسی قسم بطور ڈیفالٹ بغیر کسی خفیہ کاری کے ٹریفک کو ری ڈائریکٹ کرتی ہے؟
   - A. بنیادی HTTP پراکسی
   - B. خفیہ شدہ HTTPS پراکسی
   - C. محفوظ WireGuard کلائنٹ
   - D. ایک اوبفسکیٹڈ VPN سرور

5. براؤزر پراکسی استعمال کرتے وقت بیک گراؤنڈ ایپلیکیشن ٹریفک کے ساتھ کیا ہوتا ہے؟
   - A. یہ خودکار طور پر خفیہ ہو جاتا ہے
   - B. اسے پراکسی سرور بلاک کر دیتا ہے
   - C. اسے پراکسی ٹنل کے ذریعے روٹ کیا جاتا ہے
   - D. یہ پراکسی کو نظرانداز کر کے آپ کا IP ظاہر کر دیتا ہے

چیک پوائنٹ 2: درست یا غلط چیلنج

6 سوال 6

6. SOCKS5 پراکسی سرور سے گزرنے والے تمام پیکٹ پے لوڈز کو خفیہ کرتی ہے۔

درست غلط

7 سوال 7

7. VPN نیٹ ورک لیئر پر کام کر کے پورے سسٹم کے ٹریفک کو محفوظ بناتا ہے۔

درست غلط

8 سوال 8

8. پراکسیز عموماً VPNs سے تیز ہوتی ہیں کیونکہ وہ گہری پیکٹ انکرپشن کرتی ہیں۔

درست غلط

9 سوال 9

9. پراکسی ترتیب دینے کے لیے مخصوص ایپس کے اندر ٹریفک ری ڈائریکشنز مقرر کرنا ضروری ہے۔

درست غلط

10 سوال 10

10. پراکسی کا استعمال آپ کے ڈیٹا ٹریفک کو مقامی ISP کی ٹریکنگ سے محفوظ نہیں بناتا۔

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. ایپلیکیشن سطح کا _____ مخصوص براؤزر ٹریفک کو موڑتا ہے لیکن دوسری ایپس کو محفوظ نہیں کرتا۔
2. ایک مضبوط _____ آلے کے تمام ڈیٹا پیکٹس کو لپیٹتا اور انکرپٹ کرتا ہے۔
3. ایپلیکیشن اور ٹرانسپورٹ لیئرز کے درمیان _____ پروٹوکول واقع ہوتا ہے۔
4. HTTP پراکسیز OSI ماڈل کی _____ لیئر پر کام کرتی ہیں۔
5. معیاری پراکسی سرورز میں پے لوڈ کی _____ نہیں ہوتی جس سے ڈیٹا غیر محفوظ رہتا ہے۔
6. وی پی این تمام نیٹ ورک اڈاپٹرز کے لیے _____ تحفظ فراہم کرتا ہے۔

الفاظ کا بینک

ایپلیکیشن | پراکسی | خفیہ کاری | ساتویں پرت | سسٹم وائڈ | وی پی این ٹنل | یو ڈی پی | SOCKS5

اپنے جوابات یہاں لکھیں:

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

چیک پوائنٹ 4: نیٹ ورک تصورات کا ملان

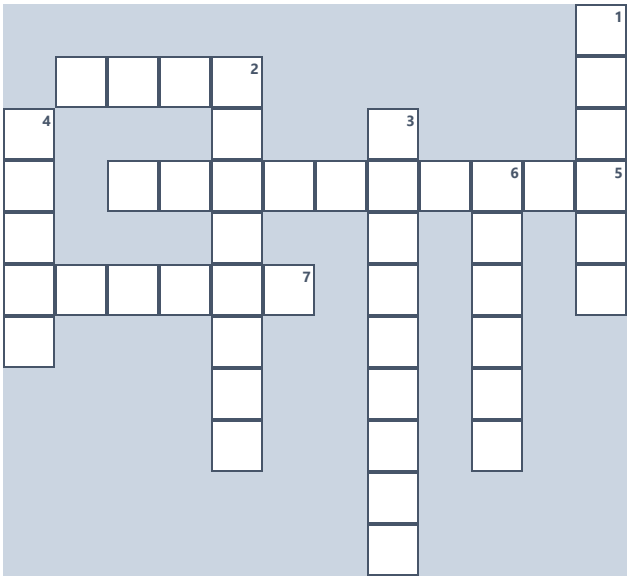
تعریفوں کا ملان

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. HTTP پراکسی	A	آپریٹنگ سسٹم کی سطح کی روٹنگ جو ایپلیکیشن کی تمام ٹریفک کو انکرپٹ کرتی ہے۔
2. SOCKS5 پراکسی	B	ایپلیکیشن لیئر، جہاں معیاری ویب پراکسی پروٹوکولز کام کرتے ہیں۔
3. VPN ٹنل	C	SOCKS5 کی TCP کے ساتھ ساتھ UDP کو بھی ریلے کرنے کی صلاحیت، جو سادہ HTTP پراکسیز میں نہیں ہوتی۔
4. پورے سسٹم کی سطح پر	D	کلائنٹ ایکسٹینشن جو ٹریفک کو صرف براؤزر سینڈ باکس کے اندر چھپاتی ہے۔
5. OSI لیئر 7	E	خفیہ کاری اور انکیپسولیشن جو ڈیوائس کی تمام پس منظر ٹریفک کو لپیٹتی ہے۔
6. UDP سپورٹ	F	ٹریفک کی وہ حالت جس میں غیر خفیہ کردہ پراکسی ڈیٹا ISPs کو نظر آتا رہتا ہے۔
7. براؤزر پراکسی	G	ایپلی کیشن لیئر پراکسی جو ویب براؤزر کے مخصوص ٹریفک کو ری ڈائریکٹ کرتی ہے۔
8. ISP کی مرئیت	H	ایپلیکیشن اور ٹرانسپورٹ لیئرز کے درمیان پراکسی پروٹوکول، جس میں کوئی خفیہ کاری نہیں ہوتی۔

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

2. ایپلیکیشن اور ٹرانسپورٹ لیئرز کے درمیان کام کرنے والا پروٹوکول، جس میں انکرپشن نہیں ہوتی (4)

5. انکرپشن اور انکیپسولیشن جو ڈیوائس کے پس منظر کے تمام ٹریفک کو لپیٹتی ہے (10)

7. SOCKS5 کی TCP کے علاوہ UDP کو بھی ریلے کرنے کی صلاحیت، جو سادہ HTTP پراکسیز میں نہیں ہوتی (6)

عمودی

1. کلائنٹ ایکسٹینشن جو صرف ویب سرفنگ ایپ کے سینڈ باکس کے اندر کا ٹریفک چھپاتی ہے (6)

2. آپریٹنگ سسٹم کی سطح کی روٹنگ جو تمام ایپلی کیشنز کے ٹریفک کو انکرپٹ کرتی ہے (8)

3. ایپلیکیشن لیئر جہاں معیاری ویب پراکسی پروٹوکول کام کرتے ہیں (9)

4. ٹریفک کی وہ حالت جس میں غیر انکرپٹڈ پراکسی ڈیٹا کو ISPs نظر آتا رہتا ہے (5)

6. ایپلیکیشن سطح کا ثالث سرور جو ویب براؤزر کے مخصوص ٹریفک کو موڑتا ہے (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

2 افقی: ایپلیکیشن اور ٹرانسپورٹ لیئرز کے درمیان کام کرنے والا پروٹوکول، جس میں انکرپشن نہیں ہوتی (4 حروف):

5 افقی: انکرپشن اور انکیپسولیشن جو ڈیوائس کے پس منظر کے تمام ٹریفک کو لپیٹتی ہے (10 حروف):

7 افقی: SOCKS5 کی TCP کے علاوہ UDP کو بھی ریلے کرنے کی صلاحیت، جو سادہ HTTP پراکسیز میں نہیں ہوتی (6 حروف):

عمودی

1 عمودی: کلائنٹ ایکسٹینشن جو صرف ویب سرفنگ ایپ کے سینڈ باکس کے اندر کا ٹریفک چھپاتی ہے (6 حروف):

2 عمودی: آپریٹنگ سسٹم کی سطح کی روٹنگ جو تمام ایپلی کیشنز کے ٹریفک کو انکرپٹ کرتی ہے (8 حروف):

3 عمودی: ایپلیکیشن لیئر جہاں معیاری ویب پراکسی پروٹوکول کام کرتے ہیں (9 حروف):

4 عمودی: ٹریفک کی وہ حالت جس میں غیر انکرپٹڈ پراکسی ڈیٹا ISPs کو نظر آتا رہتا ہے (5 حروف):

6 عمودی: ایپلیکیشن سطح کا ثالث سرور جو ویب براؤزر کے مخصوص ٹریفک کو موڑتا ہے (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۔

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

الفاظ کی فہرست

پراکسی ساکس ویپیاینٹنل سسٹموائڈ ساتویں‌پرت یوڈیپی براوزر مرئیت

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. پراکسی
B. ساکس
C. ویپیاینٹنل
D. سسٹموائڈ
E. ساتویں‌پرت
F. یوڈیپی
G. براوزر
H. مرئیت

تعریفیں اور ملان کے خانے	
1. ایپلیکیشن لیئر جہاں معیاری ویب پراکسی پروٹوکول کام کرتے ہیں۔	
2. SOCKS5 کی TCP کے علاوہ UDP کو بھی ریلے کرنے کی صلاحیت، جو سادہ HTTP پراکسیز میں نہیں ہوتی۔	
3. ایپلیکیشن سطح کا ثالث سرور جو ویب براؤزر کے مخصوص ٹریفک کو موڑتا ہے۔	
4. کلائنٹ ایکسٹینشن جو صرف ویب سرفنگ ایپ کے سینڈ باکس کے اندر کا ٹریفک چھپاتی ہے۔	
5. انکرپشن اور انکیپسولیشن جو ڈیوائس کے پس منظر کے تمام ٹریفک کو لپیٹتی ہے۔	
6. آپریٹنگ سسٹم کی سطح کی روٹنگ جو تمام ایپلی کیشنز کے ٹریفک کو انکرپٹ کرتی ہے۔	
7. ٹریفک کی وہ حالت جس میں غیر انکرپٹڈ پراکسی ڈیٹا ISPs کو نظر آتا رہتا ہے۔	
8. ایپلیکیشن اور ٹرانسپورٹ لیئرز کے درمیان کام کرنے والا پروٹوکول، جس میں انکرپشن نہیں ہوتی۔	

چیک پوائنٹ 7: الجھے الفاظ کا چیلنج

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

1. ا پ ک س ی ر
2. ن ی و ی ا ل ن ٹ ی پ
3. س ں ی ا پ ت و ر ت
4. ر و ا ز ب ر
5. س س ک ا
6. ئ ڈ م ا س و س ٹ
7. پ ی ی ی ڈ و
8. ت م ئ ی ر

اضافی سرگرمی: تیزی سے سوچیں

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

1	پراکسی اور VPN کے درمیان فرق		
2	VPN کے بغیر غیر خفیہ رہنے والی چیزیں		
3	جعلی Wi-Fi نیٹ ورک پہچاننے کے طریقے		
4	روزمرہ زندگی میں بیچ کا واسطہ بننے والے کام		
5	وہ حالات جن میں پراکسی کافی ہے		
6	وہ ڈیوائسز جو VPN استعمال کر سکتی ہیں		
7	آپ کی جانی پہچانی پراکسی کی اقسام		
8	وہ چیزیں جو VPN چھپا سکتا ہے		
9	VPN کے بارے میں غلط فہمیاں		
10	وہ وعدے جو اچھا VPN فراہم کنندہ کرتا ہے		
11	وہ چیزیں جن سے VPN آپ کو محفوظ نہیں رکھ سکتا		
12	اس ورک شیٹ کے وہ الفاظ جو آپ یاد رکھنا چاہتے ہیں		
13	سفر کے دوران VPN استعمال کرنے کی وجوہات		
14	وہ حالات جن میں آپ VPN چاہیں گے		
15	وہ مقامات جہاں آپ VPN استعمال کریں گے		

چیک پوائنٹ 8: VPN کیس اسٹڈیز

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

سارہ (کافی شاپ کی طالبہ)

👩‍💻 "ارے! میں Coffee & Bytes میں ہوں جہاں 'Free_Wi-Fi_No_Password' نام کا کھلا نیٹ ورک ہے۔ مجھے اپنی اسکول کی ای میل میں لاگ اِن کرنا ہے، اور ایک دوست کہتا ہے کہ محفوظ رہنے کے لیے مفت براؤزر پراکسی کافی ہے۔ کیا پراکسی میرے لاگ اِن اور فائلوں کو محفوظ رکھے گی، یا مجھے VPN چاہیے؟"

الیکس (مسافر طالب علم)

👨‍💻 "میں بیرون ملک ہوں اور میرے آبائی ملک میں ہوسٹ کی گئی ایک بائیولوجی ڈاکومینٹری کہتی ہے 'This video is not available in your current location.' ایک ہم جماعت پراکسی استعمال کرتا ہے، اور میرے پاس VPN ہے۔ مجھے کیوں بلاک کیا گیا ہے، اور کون سا ٹول بہتر کام کرے گا؟"

چیک پوائنٹ 9: سائفر حل کریں

اپنی پراکسی موازنے کی تربیت مکمل کرنے کے لیے محفوظ ٹنلنگ کے بارے میں یہ خفیہ 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

1	28		28	26	37	14	5		38	18		37	18	28	1	14	3

33	37	30	11	2		35	4	18	1	14

ڈی کوڈ شدہ پیغام:

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

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

ورچوئل پرائیویٹ نیٹ ورکس کے استعمال کے بارے میں ممکنہ صارفین کے سب سے عام سوالات اور جوابات کا جائزہ لیں۔

Q1: VPN کیا ہے اور یہ کیسے کام کرتا ہے؟

ورچوئل پرائیویٹ نیٹ ورک (VPN) آپ کے انٹرنیٹ کنکشن کو خفیہ کرتا ہے اور آپ کے ٹریفک کو محفوظ ریموٹ سرور کے ذریعے روٹ کرتا ہے۔ اس سے آپ کا عوامی IP ایڈریس چھپتا ہے اور VPN ٹنل سے گزرنے والے ٹریفک کے بارے میں مقامی نیٹ ورک کے مبصرین اور آپ کا ISP جو کچھ دیکھ سکتے ہیں وہ محدود ہو جاتا ہے۔

Q2: پراکسی سرور کیا ہے؟

پراکسی سرور ایک درمیانی واسطہ ہے جو آپ کی ایپلیکیشن اور منزل کے سرور کے درمیان درخواستیں آگے بھیجتا ہے۔ ویب سائٹ آپ کے بجائے پراکسی کا IP ایڈریس دیکھتی ہے، لیکن صرف وہی ایپس کا ٹریفک ری ڈائریکٹ ہوتا ہے جو پراکسی استعمال کرنے کے لیے ترتیب دی گئی ہوں، اور بنیادی پراکسی اس ٹریفک کو خفیہ نہیں کرتی۔

Q3: کیا VPN مجھے آن لائن مکمل طور پر گمنام بنا دیتا ہے؟

نہیں۔ اگرچہ VPN آپ کا IP ایڈریس چھپاتا اور ٹریفک خفیہ کرتا ہے، پھر بھی براؤزر کوکیز، فعال اکاؤنٹس (جیسے Google یا Facebook)، براؤزر فنگر پرنٹنگ کے ذریعے، یا اگر آپ کا VPN فراہم کنندہ آپ کا ڈیٹا لاگ کرے تو آپ کو ٹریک کیا جا سکتا ہے۔

Q4: کیا VPN میری انٹرنیٹ کی رفتار کو سست کر دے گا؟

ہاں، تھوڑا سا۔ خفیہ کاری کا عمل اور VPN سرور تک فزیکل فاصلہ لیٹنسی اور اضافی بوجھ بڑھاتے ہیں۔ اثر فراہم کنندہ، پروٹوکول، سرور کے فاصلے، آلے اور نیٹ ورک کے حالات کے مطابق مختلف ہوتا ہے۔

Q5: کیا پراکسی VPN ہے؟

نہیں۔ پراکسی مخصوص ایپس کا ٹریفک آگے بھیجتی ہے، عموماً بغیر خفیہ کاری کے۔ VPN نیٹ ورک لیئر پر خفیہ ٹنل بناتا ہے جو آلے کا تمام ٹریفک، بشمول بیک گراؤنڈ ایپس، لے جاتی ہے۔

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

ورچوئل پرائیویٹ نیٹ ورکس کے استعمال کے بارے میں ممکنہ صارفین کے سب سے عام سوالات اور جوابات کا جائزہ لیں۔

Q6: کیا میں مفت پراکسی استعمال کر سکتا ہوں؟

آپ کر سکتے ہیں، لیکن مفت پراکسیز اکثر نامعلوم آپریٹرز چلاتے ہیں۔ چونکہ بنیادی پراکسی ٹریفک کو خفیہ نہیں کرتی، اس کا آپریٹر غیر خفیہ صفحات دیکھ اور حتیٰ کہ بدل بھی سکتا ہے۔ استعمال سے پہلے دیکھ لیں کہ سروس کون چلاتا ہے۔

Q7: کیا پراکسی لاگز رکھتی ہے؟

ہاں ہو سکتا ہے۔ پراکسی ہر اس درخواست کو سنبھالتی ہے جو وہ آگے بھیجتی ہے، اس لیے اس کا آپریٹر آپ کا IP ایڈریس، آپ کی وزٹ کردہ سائٹس اور ان کا وقت ریکارڈ کر سکتا ہے۔ جانچیں کہ اسے کون چلاتا ہے اور اس کی رازداری کی پالیسی کیا کہتی ہے۔

Q8: پراکسی کب کافی ہوتی ہے؟

کم خطرے والے کاموں کے لیے پراکسی کافی ہو سکتی ہے، جیسے ایک براؤزر کا ظاہری مقام بدلنا۔ بینکنگ، عوامی وائی فائی یا ڈیوائس کی ہر ایپ کے تحفظ کے لیے VPN زیادہ محفوظ انتخاب ہے کیونکہ یہ تمام ٹریفک کو خفیہ کرتا ہے۔

Q9: کیا پراکسی میرے فون کی تمام ایپس کا تحفظ کر سکتی ہے؟

نہیں۔ صرف وہ ایپس پراکسی سیٹنگ استعمال کرتی ہیں جو اس کا احترام کرتی ہیں؛ باقی براہِ راست جڑتی ہیں۔ اس کے برعکس VPN ایپ فون کی تمام ایپس کو اپنی خفیہ ٹنل کے ذریعے روٹ کرتی ہے۔

Q10: SOCKS5 پراکسی کیا ہے؟

RFC 1928 میں بیان کردہ SOCKS5 ایک پروکسی پروٹوکول ہے جو ایپلیکیشن اور ٹرانسپورٹ لیئرز کے درمیان بیٹھتا ہے۔ یہ TCP کنکشنز اور UDP ڈیٹا گرامز ری لے کر سکتا ہے اور تصدیق کو سپورٹ کرتا ہے، لیکن اس میں بلٹ ان خفیہ کاری نہیں ہے۔ [1]

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

ورچوئل پرائیویٹ نیٹ ورکس اور محفوظ ٹنلنگ پروٹوکولز کے تکنیکی اور ساختی پہلوؤں کا جائزہ لیں۔

Q1: پراکسیز اور VPNs کن نیٹ ورک لیئرز پر کام کرتے ہیں؟

HTTP پراکسی ایپلیکیشن لیئر (Layer 7) پر کام کرتی ہے اور ویب درخواستوں کو سمجھتی ہے۔ SOCKS5 ایپلیکیشن اور ٹرانسپورٹ لیئرز کے درمیان بیٹھتا ہے۔ IPsec یا WireGuard جیسے VPN پروٹوکولز نیٹ ورک لیئر پر کام کرتے ہیں، اس لیے وہ ڈیوائس کا تمام IP ٹریفک لے جا سکتے ہیں۔

Q2: کیا HTTPS سائٹ پراکسی کے ذریعے بھی انکرپٹڈ رہتی ہے؟

ہاں۔ جب آپ پراکسی کے ذریعے HTTPS سائٹ کھولتے ہیں تو TLS خفیہ کاری آپ کے براؤزر اور سائٹ کے درمیان شروع سے آخر تک چلتی ہے، اس لیے پراکسی ڈومین دیکھتی ہے مگر صفحے کا مواد نہیں۔ سادہ HTTP صفحات پڑھے جا سکتے ہیں۔

Q3: WebRTC لیکنگ کیا ہے اور VPN اسے کیسے روکتا ہے؟

WebRTC ایک براؤزر پروٹوکول ہے جو VPN فعال ہونے کے باوجود آپ کے اصل مقامی اور عوامی IP ایڈریس ظاہر کر سکتا ہے۔ پریمیم VPNs اپنی ڈیسک ٹاپ/موبائل ایپس اور براؤزر ایکسٹینشنز میں WebRTC درخواستوں کو بلاک یا جعلی بنا دیتے ہیں۔

Q4: شفاف پراکسی کیا ہے اور اسے کون استعمال کرتا ہے؟

شفاف پراکسی صارف کی ڈیوائس پر کسی سیٹ اپ کے بغیر ٹریفک کو روک لیتی ہے۔ اسکول، کمپنیاں اور ISPs اسے کیشنگ یا مواد کی فلٹرنگ کے لیے استعمال کرتے ہیں۔ صارفین کو اکثر پتا نہیں ہوتا کہ کوئی لگی ہوئی ہے، اور یہ انہیں کوئی رازداری نہیں دیتی۔

Q5: اوبفسکیشن VPN بلاکس کو کیسے بائی پاس کرتی ہے؟

اوبفسکیشن (یا "اسٹیلتھ VPN") ٹریفک کو عام HTTPS ٹریفک (پورٹ 443) جیسا بنا دیتی ہے۔ اس سے حکومتوں یا اسکول/دفتر کے نیٹ ورکس کی طرف سے VPN روکنے کے لیے استعمال ہونے والی ڈیپ پیکٹ انسپیکشن (DPI) سے بچنے میں مدد مل سکتی ہے۔

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

ورچوئل پرائیویٹ نیٹ ورکس اور محفوظ ٹنلنگ پروٹوکولز کے تکنیکی اور ساختی پہلوؤں کا جائزہ لیں۔

Q6: اسپلٹ ٹنلنگ کیا ہے اور مجھے اسے کب استعمال کرنا چاہیے؟

اسپلٹ ٹنلنگ آپ کو منتخب کرنے دیتی ہے کہ کون سی ایپس خفیہ کردہ VPN ٹنل کے ذریعے روٹ ہوں اور کون سی براہ راست انٹرنیٹ سے جڑیں۔ اسے حساس بینکنگ ایپس کو VPN سے گزارنے کے لیے استعمال کریں جبکہ مقامی گیمز براہ راست جڑیں، تاکہ VPN سے شامل ہونے والی لیٹنسی سے بچا جا سکے۔

Q7: پراکسی VPN کنکشن سے تیز کیوں محسوس ہو سکتی ہے؟

بنیادی پراکسی خفیہ کاری چھوڑ دیتی ہے اور صرف ایک ایپ کا ٹریفک سنبھالتی ہے، اس لیے پروسیسنگ کم ہوتی ہے۔ VPN ڈیوائس کے ہر پیکٹ کو خفیہ کرتا ہے۔ جدید پروٹوکولز کے ساتھ فرق اکثر معمولی ہوتا ہے، اور پراکسی کہیں کم تحفظ دیتی ہے۔

Q8: کیا ویب سائٹس بتا سکتی ہیں کہ میں پراکسی یا VPN استعمال کرتا ہوں؟

اکثر ہاں۔ بہت سی سائٹس IP ایڈریسز کو معروف پراکسی اور VPN سرورز کی فہرستوں سے ملاتی ہیں، اور HTTP پراکسیز Via یا X-Forwarded-For جیسے ہیڈرز شامل کر سکتی ہیں۔ اسٹریمنگ سروسز عموماً دونوں کو بلاک کرتی ہیں۔

Q9: DNS لیک سے تحفظ کیا ہے؟

DNS لیک پروٹیکشن آپ کی ڈیوائس کو مجبور کرتا ہے کہ ویب سائٹ لُک آپ کوئریز (DNS کوئریز) آپ کے ISP کے سرورز کے بجائے VPN کے نجی، خفیہ کردہ DNS سرورز کے ذریعے بھیجے۔ اس سے آپ کا ISP یہ نہیں دیکھ پاتا کہ آپ کون سی سائٹس دیکھتے ہیں۔

Q10: کیا پراکسی ISP تھروٹلنگ روک سکتی ہے؟

شاذ و نادر۔ بنیادی پراکسی ٹریفک کو خفیہ نہیں کرتی، اس لیے ISP پھر بھی دیکھ سکتا ہے کہ یہ کس قسم کی سرگرمی ہے۔ VPN ٹریفک کی اقسام کو چھپاتا ہے، لیکن کوئی بھی ٹول بھیڑ یا ڈیٹا کی حدوں کو حل نہیں کرتا۔

حصہ 11: 10 دلچسپ VPN حقائق اور عملی بصیرتیں

VPNs کی تاریخ، مارکیٹ اور ٹیکنالوجی کے بارے میں ان نہایت قیمتی، حقیقی دنیا کے حقائق اور بصیرتوں کا جائزہ لیں۔

1. SOCKS معیار

SOCKS پروٹوکول ورژن 5 کو IETF نے مارچ 1996 میں RFC 1928 کے طور پر شائع کیا تھا اور یہ آج بھی براؤزرز اور ایپس میں استعمال ہونے والی SOCKS5 پروکسیز کی حوالہ جاتی تفصیل ہے۔ [1]

2. شِم لیئر

RFC 1928 SOCKS کو ایپلیکیشن اور ٹرانسپورٹ لیئرز کے درمیان ایک شم لیئر کے طور پر بیان کرتا ہے، اس لیے یہ ICMP جیسی نیٹ ورک لیئر ٹریفک کو فارورڈ نہیں کر سکتا۔ [1]

3. UDP ریلے

SOCKS5 نے UDP ASSOCIATE کمانڈ شامل کی، جو پروکسی کو TCP کنکشنز کے ساتھ ساتھ UDP ڈیٹا گرام بھی ری لے کرنے دیتی ہے، جو سادہ HTTP پروکسیز نہیں سنبھالتیں۔ [1]

4. ڈیفالٹ SOCKS پورٹ

RFC 1928 میں بیان کردہ ڈیفالٹ کے مطابق SOCKS5 کلائنٹس پروکسی سرور سے TCP پورٹ 1080 پر جڑتے ہیں؛ بہت سی پروکسی سروسز صارفین کو دوسری پورٹس چننے دیتی ہیں۔ [1]

5. HTTP ثالث

HTTP معیار (RFC 9110) پراکسی کو کلائنٹ کی منتخب کردہ پیغام آگے بھیجنے والی ایجنٹ قرار دیتا ہے، جو درخواستوں کو اصل سرور کی طرف ریلے کرتی ہے۔

6. ڈیپ پیکٹ انسپیکشن

ڈیپ پیکٹ انسپیکشن (DPI) پیکٹ کے مواد اور ٹریفک کے نمونوں کا جائزہ لیتی ہے؛ غیر خفیہ کردہ پراکسی ٹریفک اسے مکمل طور پر نظر آتی ہے، جبکہ VPN ٹریفک بہت کم ظاہر کرتی ہے۔

7. نیٹ ورک لیئر VPNs

NIST SP 800-77 میں بیان کردہ IPsec نیٹ ورک لیئر پر ٹریفک کا تحفظ کرتا ہے، اس لیے ہر ایپلی کیشن کے IP پیکٹس کو فی ایپ سیٹ اپ کے بغیر محفوظ بنایا جا سکتا ہے۔ [2]

8. صرف براؤزر تک دائرہ

ایک براؤزر میں ترتیب دی گئی پراکسی صرف اسی براؤزر پر اثر انداز ہوتی ہے؛ ای میل کلائنٹس، گیمز اور سسٹم اپ ڈیٹس ڈیوائس کا عام کنکشن ہی استعمال کرتے رہتے ہیں۔

9. ٹور بمقابلہ پراکسیز

Tor ٹریفک کو تین رضاکار ریلیز (گارڈ، مڈل اور ایگزٹ) کے ذریعے بھیجتا ہے اور عموماً مقامی SOCKS پراکسی کے ذریعے استعمال ہوتا ہے، جو ایسی تہیں شامل کرتا ہے جو ایک اکیلی پراکسی نہیں کر سکتی۔

10. رفتار کا سمجھوتہ

پراکسیز تیز لگ سکتی ہیں کیونکہ وہ انکرپشن چھوڑ دیتی ہیں، جبکہ WireGuard جیسے جدید VPN پروٹوکولز بہت کم اوور ہیڈ ڈالتے ہیں اور ڈیوائس کی تمام ٹریفک کو محفوظ رکھتے ہیں۔

تکنیکی حوالہ جات اور ماخذ

اس ورک شیٹ میں استعمال ہونے والی حوالہ دی گئی اشاعتیں، کرپٹوگرافک وضاحتیں اور سرکاری دستاویزی معیارات۔

علمی اور صنعتی حوالہ جات

[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/

جوابی کلید: پراکسی سرورز اور ورچوئل پرائیویٹ نیٹ ورکس کا موازنہ، خفیہ کاری کے فرق، اور ایپ کی سطح بمقابلہ پورے سسٹم کی روٹنگ

1 پراکسی OSI لیئر

پروٹوکولز

درست جواب: C

تدریسی نوٹ

معیاری HTTP/HTTPS پراکسیز ایپلی کیشن لیئر (Layer 7) پر کام کرتی ہیں اور مخصوص براؤزر ٹریفک کو ری ڈائریکٹ کرتی ہیں۔ ان میں پورے سسٹم کی نیٹ ورک روٹنگ نہیں ہوتی۔ حوالہ: Tor Project Foundation۔

2 سوال 2

درست جواب: B

تدریسی نوٹ

SOCKS5 ایپلیکیشن اور ٹرانسپورٹ لیئرز کے درمیان TCP اور UDP ٹریفک ریلے کرتا ہے لیکن بطور ڈیفالٹ خفیہ نہیں کرتا، جبکہ HTTP پراکسیز ویب درخواستیں سنبھالتی ہیں۔

3 VPN سسٹم خفیہ کاری

وائی فائی سیکیورٹی

درست جواب: B

تدریسی نوٹ

VPN پورے آپریٹنگ سسٹم کے ٹریفک کو سسٹم بھر میں لپیٹ کر خفیہ کرتا ہے، جبکہ پراکسی صرف مخصوص ترتیب شدہ ایپلیکیشنز کا ٹریفک ری ڈائریکٹ کرتی ہے۔ حوالہ: Deloitte Advisory۔

4 پراکسی میں انکرپشن کی کمی

روٹنگ کنٹرولز

درست جواب: A

تدریسی نوٹ

HTTP پراکسیز براؤزر ٹریفک کو ایپلی کیشن لیئر پر پیکٹ پے لوڈ کو خفیہ کیے بغیر آگے بھیجتی ہیں، یعنی آپ کا نیٹ ورک آپریٹر یا ISP پھر بھی آپ کے مواد کے ٹریفک کا سراغ لگا سکتا ہے۔ حوالہ: IETF Proxy Vulnerabilities۔

5 بائی پاس کی کمزوری

رازداری

درست جواب: D

تدریسی نوٹ

براؤزر پراکسیز اپنے رولز صرف ویب براؤزر پر لاگو کرتی ہیں۔ بیک گراؤنڈ ایپس، آپریٹنگ سسٹم اپ ڈیٹس اور ای میل کلائنٹس پراکسی کو بائی پاس کرتے ہیں، جس سے آپ کا اصل IP ایڈریس ظاہر ہو جاتا ہے۔ حوالہ: W3C Consortium۔

جوابی کلید: چیک پوائنٹ 2 – درست یا غلط

6 سوال 6

درست جواب: غلط

تدریسی نوٹ

SOCKS5 ایپلیکیشن اور ٹرانسپورٹ لیئرز کے درمیان ٹریفک ریلے کرتا ہے لیکن بطور ڈیفالٹ کوئی خفیہ کاری نہیں کرتا، اس لیے ترسیل کے دوران پیکٹ کا مواد پڑھنے کے قابل رہتا ہے۔

7 نیٹ ورک لیئر ٹنلز

رفتاریں

درست جواب: درست

تدریسی نوٹ

نیٹ ورک لیئر پر چل کر، VPN آپ کی ڈیوائس سے جانے والے ٹریفک کو روٹ اور خفیہ کرتا ہے، جو پورے سسٹم کے ٹریفک کے تحفظ میں مدد دیتا ہے۔ حوالہ: Deloitte Advisory۔

8 پراکسی انکرپشن کی حد

اسنفنگ کا خطرہ

درست جواب: غلط

تدریسی نوٹ

پراکسیز بعض اوقات تیز ہو سکتی ہیں، لیکن اس کی وجہ یہ ہے کہ وہ انکرپشن نہیں کرتیں۔ انکرپشن کی یہ کمی ڈیٹا کو معائنے کے لیے کمزور چھوڑ دیتی ہے۔ حوالہ: IETF Proxy Vulnerabilities۔

9 ایپ کی سطح پر ری ڈائریکشن

فائر والز

درست جواب: درست

تدریسی نوٹ

سسٹم بھر کے VPNs کے برعکس، پراکسی سرورز کو براؤزر سیٹنگز یا ایپلیکیشن کے مخصوص پراکسی فیلڈز میں دستی سیٹ اپ درکار ہوتا ہے۔ حوالہ: W3C Consortium۔

10 ISP ٹریکنگ کا خطرہ

نو لاگز

درست جواب: درست

تدریسی نوٹ

چونکہ معیاری HTTP/SOCKS5 پراکسیز پے لوڈ ڈیٹا کو خفیہ نہیں کرتیں، آپ کا مقامی ISP آپ کی آن لائن سرگرمیوں کو مکمل طور پر دیکھ سکتا ہے۔ حوالہ: EDRi Retention Guidelines۔

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

G .1 HTTP پراکسی	H .2 SOCKS5 پراکسی	E .3 VPN ٹنل	A .4 پورے سسٹم کی سطح پر
B .5 OSI لیئر 7	C .6 UDP سپورٹ	D .7 براؤزر پراکسی	F .8 ISP کی مرئیت

چیک پوائنٹ 3: جوابی کلید – اہم اصطلاحات

1 پراکسی	2 وی پی این ٹنل	3 SOCKS5	4 ایپلیکیشن
5 خفیہ کاری	6 سسٹم وائڈ		

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

1 E – ساتویں پرت	2 F – یوڈیپی	3 A – پراکسی	4 G – براوزر
5 C – ویپیاینٹنل	6 D – سسٹموائڈ	7 H – مرئیت	8 B – ساکس

اساتذہ کے لیے بحث کے نوٹس

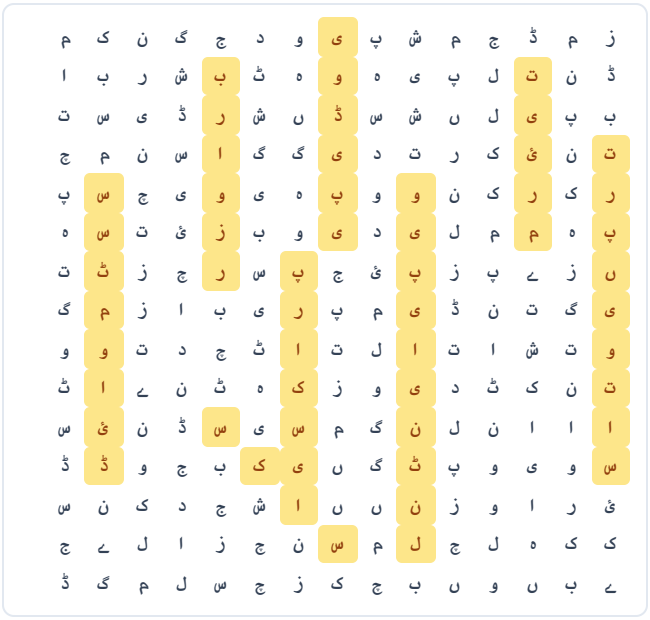
اہم اصطلاحات:
یقینی بنائیں کہ طلبہ HTTP پراکسی، SOCKS5 پراکسی اور VPN ٹنل کو اپنے الفاظ میں سمجھا سکیں اور ہر ایک کی مثال دے سکیں۔

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

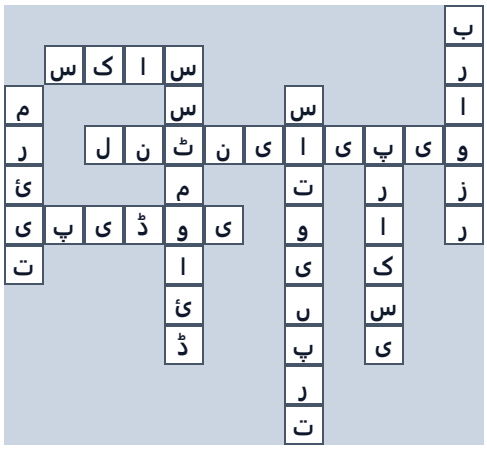
ماخذ کی جانچ:
طلبہ سے کہیں کہ ورک شیٹ کے ماخذ میں کم از کم ایک دعوے کی تصدیق کریں، اور اس پر بات کریں کہ اعداد و شمار، قیمتیں اور قواعد وقت کے ساتھ کیوں بدل سکتے ہیں۔

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

2 افقی: ساکس ایپلیکیشن اور ٹرانسپورٹ لیئرز کے درمیان کام کرنے والا پروٹوکول، جس میں انکرپشن نہیں ہوتی (4 حروف)

5 افقی: ویپیاینٹنل انکرپشن اور انکیپسولیشن جو ڈیوائس کے پس منظر کے تمام ٹریفک کو لپیٹتی ہے (10 حروف)

7 افقی: یوڈیپی SOCKS5 کی TCP کے علاوہ UDP کو بھی ریلے کرنے کی صلاحیت، جو سادہ HTTP پراکسیز میں نہیں ہوتی (6 حروف)

عمودی

1 عمودی: براوزر کلائنٹ ایکسٹینشن جو صرف ویب سرفنگ ایپ کے سینڈ باکس کے اندر کا ٹریفک چھپاتی ہے (6 حروف)

2 عمودی: سسٹموائڈ آپریٹنگ سسٹم کی سطح کی روٹنگ جو تمام ایپلی کیشنز کے ٹریفک کو انکرپٹ کرتی ہے (8 حروف)

3 عمودی: ساتویں‌پرت ایپلیکیشن لیئر جہاں معیاری ویب پراکسی پروٹوکول کام کرتے ہیں (9 حروف)

4 عمودی: مرئیت ٹریفک کی وہ حالت جس میں غیر انکرپٹڈ پراکسی ڈیٹا ISPs کو نظر آتا رہتا ہے (5 حروف)

6 عمودی: پراکسی ایپلیکیشن سطح کا ثالث سرور جو ویب براؤزر کے مخصوص ٹریفک کو موڑتا ہے (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. اپکسیر — پراکسی
2. نیویالنٹیپ — ویپیاینٹنل
3. سںیاپتورت — ساتویںپرت
4. روازبر — براوزر
5. سسکا — ساکس
6. ئڈماسوسٹ — سسٹموائڈ
7. پییڈو — یوڈیپی
8. تمئیر — مرئیت

خفیہ سائفر چیلنج کی کلید

"پراکسی سے ٹریفک کا راستہ بدلیں"

کیس اسٹڈیز کی جوابی کلید

A منظرنامہ A: عوامی نیٹ ورک کی سیکیورٹی

اسنفنگ اور خفیہ کاری | سارہ کی مشکل

گریڈنگ کی ہدایت

طلبہ کے جوابات میں درج ذیل نکات شامل ہونے چاہییں:

- خطرات: پیکٹ اسنفنگ، ڈیٹا کی مداخلت، اور مین ان دی مڈل حملے۔ اسی کافی شاپ کے نیٹ ورک پر موجود کوئی شخص اس کے لاگ اِن کی تفصیلات یا ہوم ورک فائل حاصل کر سکتا ہے۔
- پراکسی بمقابلہ VPN: ایک بنیادی براؤزر پراکسی اس کی ٹریفک کو انکرپٹ نہیں کرتی۔ VPN ڈیوائس پر ہر چیز کو انکرپٹ کرتا ہے، جس سے روکے گئے پیکٹس مقامی جاسوسوں کے لیے ناقابلِ مطالعہ ہو جاتے ہیں۔

B منظرنامہ B: بلاک شدہ وسائل تک رسائی

جیو بلاکنگ اور IPs | الیکس کی مشکل

گریڈنگ کی ہدایت

طلبہ کے جوابات میں درج ذیل نکات شامل ہونے چاہییں:

- بلاک ہونے کی وجہ: اسٹریمنگ ہوسٹ جیو بلاکنگ استعمال کرتا ہے، جو مسافر کے مقامی IP ایڈریس کو اس کے جسمانی ملک سے جوڑتی ہے اور علاقائی لائسنسنگ کی بنیاد پر اسے بلاک کر دیتی ہے۔
- کون سا بہتر کام کرتا ہے: دونوں اسے آبائی ملک کا IP دیتے ہیں، لیکن پراکسی صرف ترتیب دی گئی ایپ کا احاطہ کرتی ہے، جبکہ VPN اس کی ڈیوائس کی تمام ٹریفک کو بھی خفیہ کرتا ہے۔