نام: _____ تاریخ: _____ نمبر: _____

پبلک Wi-Fi سیکیورٹی اور خفیہ کاری

مین ان دی مڈل حملے، جعلی ایکسیس پوائنٹس، پیکٹ اسنفنگ، VPN ٹنلز، اور HTTPS خفیہ کاری۔

پبلک Wi-Fi سیکیورٹی سیکھنے کا 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 پبلک Wi-Fi سیکیورٹی سے متعارف کراتا ہے۔ آپ غیر خفیہ نیٹ ورکس، مین اِن دی مڈل (MitM) حملوں، روگ ایکسیس پوائنٹس، پیکٹ سنفنگ، VPN ٹنلز اور HTTPS ٹرانزٹ سیکیورٹی 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/public-wifi-security/

آپ کا پبلک Wi-Fi سیکیورٹی لرننگ روڈ میپ

- پیکٹ اسنفنگ اور جعلی ایکسیس پوائنٹس سمیت عوامی Wi-Fi کے عام خطرات کی نشاندہی کریں۔
- ٹرانزٹ ڈیٹا کو محفوظ بنانے کے لیے VPN خفیہ کاری ٹنلز نافذ کریں۔
- ریموٹ ورکرز کے لیے HTTPS اور محفوظ ویب براؤزر سیٹنگز نافذ کریں۔

پبلک Wi-Fi سیکیورٹی گائیڈ 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 ریموٹ ایکسیس کی سیکیورٹی پر لاگو کریں۔ اور آخر میں اضافی سرگرمی "تیزی سے سوچیں"۔

پبلک Wi-Fi کی سیکیورٹی اور ترسیل کے دوران تحفظ (تعارف)

غیر خفیہ کردہ عوامی Wi-Fi ہاٹ اسپاٹس نیٹ ورک ٹریفک کو پیکٹ سنفنگ اور Evil Twin جعل سازی کے سامنے کھلا چھوڑ دیتے ہیں۔ ٹریفک کو محفوظ VPN خفیہ کاری ٹنلز سے گزارنا اور صرف HTTPS والے HSTS اصول نافذ کرنا سیشنز کو مقامی نیٹ ورک کی مداخلت سے بچاتا ہے۔

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

چیک پوائنٹ 1: کثیر انتخابی چیلنج

1. مین اِن دی مڈل (MitM) حملہ کیا ہے؟

- A. مشترکہ نیٹ ورک پر دو فریقوں کے درمیان مواصلات کو روکنا اور بدلنا
- B. صارفین کے ریکارڈز کو نشانہ بنانے والی ڈیٹا بیس نکالنے کی تکنیک
- C. ویب سرورز کو نیٹ ورک ٹریفک کی درخواستوں سے مغلوب کرنا
- D. مقامی ہارڈ ڈرائیو اسٹوریج والیومز مٹانا

2. روگ ایکسیس پوائنٹ (ایول ٹون) کیا ہے؟

- A. بدنیت وائی فائی ہاٹ اسپاٹ جو جائز نیٹ ورک جیسے ہی SSID کے ساتھ ترتیب دیا گیا ہو
- B. ڈیٹا بیس بیک اپس کی نگرانی کے لیے استعمال ہونے والا انتظامی ٹول
- C. محفوظ VPN گیٹ وے کنفیگریشن
- D. ایک DNS ریکارڈ جو مجاز میل سرورز کو میپ کرتا ہے

3. VPN عوامی Wi-Fi ٹریفک کا تحفظ کیسے کرتا ہے؟

- A. یہ تمام نیٹ ورک پیکٹس کو خفیہ ٹنل میں لپیٹ دیتا ہے اور سنفرز کے لیے انہیں ناقابلِ مطالعہ بنا دیتا ہے
- B. یہ آنے والی تمام کنکشن درخواستوں کو خودکار طور پر بلاک کر دیتا ہے
- C. یہ فزیکل نیٹ ورک کارڈ کا MAC ایڈریس تبدیل کرتا ہے
- D. یہ ویب براؤزر میں کیش شدہ کوکیز حذف کرتا ہے

4. پیکٹ سنفنگ کیا ہے؟

- A. نیٹ ورک پیکٹس کو پکڑنے اور لاگ کرنے کے لیے ہارڈ ویئر یا سافٹ ویئر ٹولز استعمال کرنا
- B. مقامی ڈائریکٹریز میں مکرر فائلوں کی اسکیننگ
- C. صارف کے کردار کی بنیاد پر ڈیٹا بیس پڑھنے کی اجازتیں محدود کرنا
- D. AES-256 کیز استعمال کرتے ہوئے اسٹوریج ڈرائیوز کو خفیہ کرنا

5. HTTPS کا کردار کیا ہے؟

- A. براؤزر اور ویب سرور کے درمیان سیشن ٹریفک کو خفیہ کرنا
- B. گیٹ وے پر آنے والے ای میل پیغامات کو فلٹر کرنا
- C. صفحات تیزی سے لوڈ کرنے کے لیے تصاویر کو کمپریس کرنا
- D. نیٹ ورک سے منسلک اسٹوریج میں فائل ڈھانچوں کا انتظام کرنا

چیک پوائنٹ 2: درست یا غلط چیلنج

6 سوال 6

6. جڑے ہوئے صارفین کھلے عوامی Wi-Fi نیٹ ورکس پر سادہ متن ڈیٹا آسانی سے پکڑ سکتے ہیں۔

○ درست ○ غلط

7 سوال 7

7. روگ ایکسیس پوائنٹس (Evil Twins) کو نیٹ ورک ایڈمنسٹریٹرز ہمیشہ مجاز قرار دیتے ہیں۔

○ درست ○ غلط

8 سوال 8

8. VPN عوامی نیٹ ورکس پر پیکٹ سنفنگ کے خلاف ٹریفک کی حفاظت میں غیر مؤثر ہے۔

○ درست ○ غلط

9 سوال 9

9. HTTPS صرف URL پاتھ کو خفیہ کرتا ہے اور پیکٹ پے لوڈ کو سادہ متن میں چھوڑ دیتا ہے۔

○ درست ○ غلط

10 سوال 10

10. WPA3 سیکیورٹی استعمال کرنے والے وائی فائی ہاٹ اسپاٹس کھلے، بغیر پاس ورڈ والے نیٹ ورکس کے مقابلے میں زیادہ مضبوط تحفظ فراہم 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. عوامی Wi-Fi پر نجی پاس ورڈز حاصل کرنا مواصلات کی _____ ہے۔
2. مقامی نیٹ ورک پر خام پیکٹس کا تجزیہ کرنے کو پیکٹ _____ کہتے ہیں۔
3. ہوٹل کے Wi-Fi کی نقل کرنے والا جعلی ہاٹ اسپاٹ _____ ہوتا ہے۔
4. ویب ٹریفک کی ترسیل کو محفوظ بنانے کے لیے _____ سے انکرپٹ کرنا ضروری ہے۔
5. تمام نیٹ ورک آؤٹ پٹس کو انکرپٹ کرنے کے لیے کلائنٹ _____ استعمال ہوتا ہے۔
6. عوامی نیٹ ورکس پر انکرپٹڈ مواصلاتی راستہ _____ کہلاتا ہے۔

الفاظ کا بینک

ایول ٹوئن | پروٹوکول | ٹنل | ڈبلیو پی اے | سنیفنگ | مداخلت | وی پی این | HTTPS

اپنے جوابات یہاں لکھیں:

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

چیک پوائنٹ 4: سیکیورٹی تصورات کا ملان

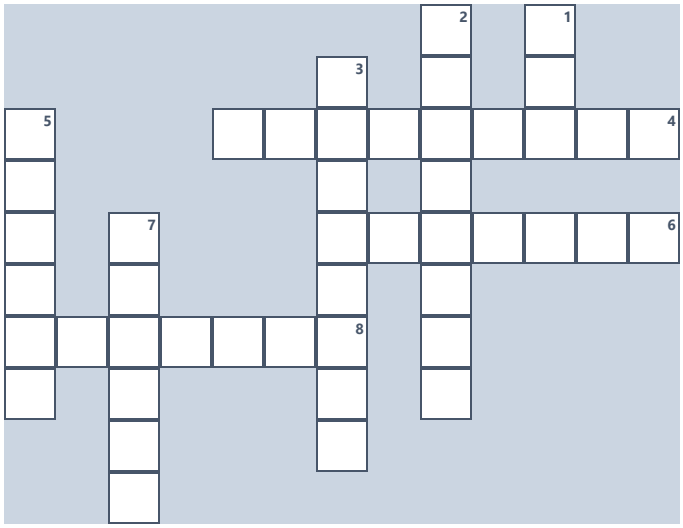
تعریفوں کا ملان

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. مداخلت	A	جدید Wi-Fi سیکیورٹی معیار۔
2. اسنفنگ	B	ترسیل کے دوران محفوظ ڈیٹا راستہ۔
3. ایول ٹوِن	C	آنے والی ٹریفک کی فلٹرنگ۔
4. HTTPS	D	Wi-Fi کی نقل کرنے والا جعلی ہاٹ اسپاٹ۔
5. VPN	E	منتقلی کے دوران ٹریفک پڑھنا۔
6. ٹنل	F	نیٹ ورک ڈیٹا پیکٹس کو پکڑنا۔
7. WPA3	G	خفیہ کردہ ورچوئل پرائیویٹ نیٹ ورک۔
8. فائر وال	H	محفوظ ویب ترسیل۔

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

4. جدید Wi-Fi سیکیورٹی معیار (9)

6. آنے والے ٹریفک کی فلٹرنگ (7)

8. انکرپٹڈ ورچوئل پرائیویٹ نیٹ ورک (7)

عمودی

1. ترسیل کے دوران ڈیٹا کا محفوظ راستہ (3)

2. محفوظ ویب ترسیل (8)

3. Wi-Fi کی نقل کرنے والا جعلی ہاٹ اسپاٹ (8)

5. نیٹ ورک ڈیٹا پیکٹس کو پکڑنا (6)

7. ٹرانزٹ میں ٹریفک پڑھنا (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

4 افقی: جدید Wi-Fi سیکیورٹی معیار (9 حروف):

6 افقی: آنے والے ٹریفک کی فلٹرنگ (7 حروف):

8 افقی: انکرپٹڈ ورچوئل پرائیویٹ نیٹ ورک (7 حروف):

عمودی

1 عمودی: ترسیل کے دوران ڈیٹا کا محفوظ راستہ (3 حروف):

2 عمودی: محفوظ ویب ترسیل (8 حروف):

3 عمودی: Wi-Fi کی نقل کرنے والا جعلی ہاٹ اسپاٹ (8 حروف):

5 عمودی: نیٹ ورک ڈیٹا پیکٹس کو پکڑنا (6 حروف):

7 عمودی: ٹرانزٹ میں ٹریفک پڑھنا (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۔

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

الفاظ کی فہرست

مداخلت
سنیفنگ
ایولٹوئن
پروٹوکول
ویپیاین
ٹنل
ڈبلیوپیاے
فائروال

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. مداخلت
B. سنیفنگ
C. ایولٹوئن
D. پروٹوکول
E. ویپیاین
F. ٹنل
G. ڈبلیوپیاے
H. فائروال

تعریفیں اور ملان کے خانے
1. جدید Wi-Fi سیکیورٹی معیار۔
2. Wi-Fi کی نقل کرنے والا جعلی ہاٹ اسپاٹ۔
3. نیٹ ورک ڈیٹا پیکٹس کو پکڑنا۔
4. ترسیل کے دوران ڈیٹا کا محفوظ راستہ۔
5. آنے والے ٹریفک کی فلٹرنگ۔
6. ٹرانزٹ میں ٹریفک پڑھنا۔
7. انکرپٹڈ ورچوئل پرائیویٹ نیٹ ورک۔
8. محفوظ ویب ترسیل۔

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. ا م خ ل ت د
2. ل ا ن ی ئ و ٹ و
3. ی و ا ن پ ی ی
4. و ے ا ی ی پ ڈ ب ل
5. ف ی گ س ن ن
6. و ل ٹ ک پ و ر و
7. ل ن ٹ
8. ا ر ل ف ا و ئ

اضافی سرگرمی: تیزی سے سوچیں

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

1	سافٹ ویئر اپ ڈیٹ کرنے کی وجوہات			
2	وہ ڈیوائسز جو Wi-Fi سے خود بخود کنیکٹ ہو جاتی ہیں			
3	وہ معلومات جو آپ کو کبھی شیئر نہیں کرنی چاہئیں			
4	محفوظ عادات جو آپ آج شروع کر سکتے ہیں			
5	کیفے میں محفوظ رہنے کے طریقے			
6	وہ ڈیوائسز جنہیں ہیک کیا جا سکتا ہے			
7	وہ چیزیں جو ہیکر کھلے Wi-Fi پر دیکھ سکتا ہے			
8	جعلی Wi-Fi نیٹ ورک کی علامات			
9	عوامی Wi-Fi کے متبادل			
10	ای میل میں انتباہی علامات			
11	وہ کام جو آپ عوامی Wi-Fi پر نہیں کرتے			
12	مفت Wi-Fi والے مقامات کے نام			
13	اپنے اکاؤنٹس کو محفوظ رکھنے کے طریقے			
14	کمپیوٹر کے متاثر ہونے کی علامات			
15	مشکوک لگنے والے Wi-Fi ناموں کی مثالیں			

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: عوامی Wi-Fi پر پیکٹ سنیفنگ کی روک تھام

🕵️

منظرنامہ: ایئرپورٹ کے عوامی Wi-Fi نیٹ ورک سے جڑا ہوا ایک ریموٹ سیلز ایگزیکٹو دیکھتا ہے کہ کئی حساس کاروباری ای میلز سادہ متن میں بھیجنے کے فوراً بعد لیک ہو گئیں۔

بحث کا سوال: عوامی نیٹ ورک کے خطرات کا تجزیہ کریں، اور ٹریفک کی خفیہ کاری کے حل کا خاکہ بیان کریں۔

کیس اسٹڈی 2: ایول ٹوئن جعلی ہاٹ اسپاٹ سے دفاع

🕵️

منظرنامہ: حملہ آور 'CoffeeShop_Guest' نام کا ایک جعلی وائرلیس ایکسیس پوائنٹ لگاتے ہیں جو ایک جائز کیفے ہاٹ اسپاٹ کی نقل کرتا ہے اور بے خبر مہمانوں کا نیٹ ورک ٹریفک حاصل کر لیتا ہے۔

بحث کا سوال: جعلی ایکسیس پوائنٹس کا پتا لگانے اور انہیں بلاک کرنے کے تصدیقی اقدامات تفصیل سے 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

28	26	37	14	5		37	39	1	26		37	39	1	34

33	37	14	28		5	3	14	28	32	1

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: پبلک Wi-Fi غیر محفوظ کیوں ہے؟

کھلا پبلک Wi-Fi ہوا میں ٹریفک کو انکرپٹ نہیں کرتا، اس لیے قریب موجود دوسرے لوگ کوئی بھی غیر محفوظ ڈیٹا حاصل کر سکتے ہیں۔ [2]

Q2: پیکٹ اسنفنگ کیا ہے؟

پیکٹ سنفر نیٹ ورک انٹرفیس پر بہنے والے خام ڈیٹا کو پکڑتا ہے اور سادہ متن پاس ورڈز اور ٹریفک کی تفصیلات ظاہر کر دیتا ہے۔

Q3: Evil Twin کیا ہے؟

ہیکرز کا بنایا ہوا جعلی ایکسیس پوائنٹ جو کسی قابلِ اعتماد مقامی وائی فائی ہاٹ اسپاٹ کے نام اور ترتیبات کی نقل کرتا ہے۔

Q4: VPN میرا تحفظ کیسے کرتا ہے؟

یہ آپ کے ٹریفک کو خفیہ ٹنل سے گزارتا ہے، جس سے آپ کی براؤزنگ سرگرمی مقامی نیٹ ورک اسنفرز سے چھپ جاتی ہے۔

Q5: کیا HTTPS عوامی Wi-Fi پر میرا تحفظ کرتا ہے؟

ہاں، یہ آپ کے براؤزر اور ویب سائٹ کے درمیان ہونے والے ڈیٹا کے تبادلے کو خفیہ کرتا ہے، اور VPN تحفظ کی ایک اضافی تہہ شامل کرتا 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: WPA3 کیا ہے؟

جدید Wi-Fi Protected Access معیار، جو مضبوط خفیہ کاری اور آف لائن ڈکشنری حملوں کے خلاف تحفظ فراہم کرتا ہے۔ [1]

Q7: کیا عوامی Wi-Fi میل ویئر پہنچا سکتا ہے؟

جی ہاں، حملہ آور ٹریفک کو روک سکتے ہیں اور آپ کے براؤزر سیشن میں نقصان دہ ڈاؤن لوڈ پرامپٹس (ڈرائیو بائی ڈاؤن لوڈز) داخل کر سکتے ہیں۔

Q8: فائل شیئرنگ کا کیا خطرہ ہے؟

اگر فائل شیئرنگ فعال ہو تو عوامی نیٹ ورک پر موجود دیگر صارفین آپ کی مقامی فولڈر ڈائریکٹری پڑھ یا تبدیل کر سکتے ہیں۔

Q9: کیپٹیو پورٹل کیا ہے؟

لاگ اِن صفحہ جسے ہوٹل یا کیفے کے نیٹ ورکس انٹرنیٹ رسائی دینے کے لیے استعمال کرتے ہیں، جس کی حملہ آور بعض اوقات جعل سازی کر سکتے ہیں۔

Q10: کیا استعمال نہ ہونے پر مجھے Wi-Fi بند کر دینا چاہیے؟

ہاں، Wi-Fi بند کرنے سے آپ کا آلہ ناقابل اعتماد نیٹ ورکس سے خودکار طور پر جڑنے سے رک جاتا ہے۔

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: مین اِن دی مڈل حملہ DNS کا استحصال کیسے کرتا ہے؟

ہدف ڈومینز کے بجائے ٹارگٹ براؤزرز کو ملتے جلتے فشنگ لینڈنگ صفحات پر بھیجنے کے لیے جعلی راؤٹر پر DNS اسپوفنگ استعمال کر کے۔

Q2: سیشن ہائی جیکنگ کیا ہے؟

حملہ آور عوامی وائی فائی پر غیر خفیہ سیشن کوکی سنفنگ کے ذریعے حاصل کرتا ہے اور اسے امپورٹ کر کے اسناد کے لاگ اِن کو بائی پاس کرتا ہے۔

Q3: SSL اسٹرپنگ کیا ہے؟

MitM حملہ جس میں حملہ آور صارف کی محفوظ HTTPS درخواست کو غیر خفیہ HTTP پر لے آتا ہے اور لاگ اِن سادہ متن میں حاصل کر لیتا ہے۔

Q4: HSTS، SSL اسٹرپنگ سے تحفظ کیسے دیتا ہے؟

HTTP Strict Transport Security براؤزرز کو صرف HTTPS کے ذریعے جڑنے پر مجبور کرتا ہے اور غیر خفیہ HTTP پر واپسی سے انکار کرتا ہے۔ [3]

Q5: اسپلٹ ٹنل VPN کیا ہے؟

ایسی کنفیگریشن جو صرف کارپوریٹ ٹریفک کو VPN سے گزارتی ہے اور عوامی انٹرنیٹ ڈیٹا براہِ راست بھیجتی ہے، جس سے لیک کے راستے کے انکشاف کا خطرہ ہو سکتا ہے۔

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: WPA2، KRACK کے لیے کمزور کیوں ہے؟

WPA2 Key Reinstallation Attack کے چار مراحل والے ہینڈ شیک کو استعمال کر کے Wi-Fi پاس ورڈ کے بغیر پیکٹس ڈی کرپٹ کر لیتا ہے۔

Q7: کلائنٹ آئسولیشن کیا ہے؟

راؤٹر کی سیکیورٹی ترتیب جو جڑی ہوئی وائی فائی ڈیوائسز کو آپس میں براہِ راست رابطہ کرنے سے روکتی ہے اور مقامی سنفنگ کو بلاک کرتی ہے۔

Q8: حملہ آور جعلی DNS سرورز کیسے استعمال کرتے ہیں؟

وہ جعلی راؤٹرز ترتیب دیتے ہیں جو کلائنٹس کو جعلی DNS سرورز تفویض کرتے ہیں، جس سے وہ تمام ویب لک اپس کو روک کر دوبارہ لکھ سکتے ہیں۔

Q9: کیا VPN میرا مقامی MAC ایڈریس چھپا سکتا ہے؟

نہیں۔ MAC ایڈریسز مقامی لیئر-2 شناخت کنندگان ہیں؛ اس کے بجائے اپنے آلے کی بلٹ ان MAC رینڈمائزیشن (نجی ایڈریس) سیٹنگ استعمال کریں۔

Q10: کیپٹو پورٹل اسپوفنگ حملہ کیا ہے؟

حملہ آور جو مفت وائی فائی رسائی کے بہانے اسناد چرانے کے لیے جعلی ہاٹ اسپاٹ پر جعلی تصدیقی پورٹل چلاتا ہے۔

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

ریموٹ ورکرز اکثر کیفے، ہوٹلوں اور ہوائی اڈوں پر Wi-Fi استعمال کرتے ہیں، جہاں وہ نیٹ ورک کی سیکیورٹی پر قابو نہیں رکھ سکتے۔

2. سیکیورٹی بصیرت

Evil Twin جعلی ہاٹ اسپاٹ کسی قابلِ اعتماد نیٹ ورک کا عین نام اور MAC ایڈریس نقل کر کے ڈیوائسز کو الجھا سکتا ہے۔

3. سیکیورٹی بصیرت

Wireshark جیسا پیکٹ اسنفنگ سافٹ ویئر مفت ہے اور غیر انکرپٹڈ HTTP پاس ورڈز کو سادہ متن میں دکھا سکتا ہے۔

4. سیکیورٹی بصیرت

WPA3 سیکیورٹی مقامی بروٹ فورس حملوں سے بچاؤ کے لیے Simultaneous Authentication of Equals (SAE) استعمال کرتی ہے۔

5. سیکیورٹی بصیرت

SSL اسٹرپنگ حملے گیٹ وے پر ابتدائی HTTP ری ڈائریکٹس کو روک کر بنیادی HTTPS تحفظات کو بائی پاس کرتے ہیں۔

6. سیکیورٹی بصیرت

HTTP Strict Transport Security (HSTS) ریسپانس ہیڈرز براؤزرز کو غیر خفیہ HTTP کنکشنز پر واپس جانے سے روکتے ہیں۔ [3]

7. سیکیورٹی کی بصیرت

'Auto-Connect' بند کرنے سے اسمارٹ فونز عوامی مقامات پر ملتے جلتے جعلی نیٹ ورکس سے جڑنے سے بچ جاتے ہیں۔

8. سیکیورٹی کی بصیرت

انٹرپرائز 'always-on' VPN کنفیگریشنز تمام ریموٹ ورکرز کی نیٹ ورک ٹریفک کو کارپوریٹ فائر والز سے گزرنے پر مجبور کرتی ہیں۔

9. سیکیورٹی کی بصیرت

روگ ایکسیس پوائنٹس جعلی DNS جوابات دے سکتے ہیں اور ہدف والے ڈومینز کو فشنگ سرورز کی طرف موڑ سکتے ہیں۔

10. سیکیورٹی بصیرت

VPN کے بغیر، کھلے ہاٹ اسپاٹ پر دوسرے صارفین دیکھ سکتے ہیں کہ آپ کی ڈیوائس کن سائٹس اور سرورز سے رابطہ کرتی ہے۔

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] Wi-Fi Alliance. (n.d.). Security.
https://www.wi-fi.org/discover-wi-fi/security

[2] Federal Trade Commission. (2023). Are Public Wi-Fi Networks Safe? What You Need To Know.
https://consumer.ftc.gov/articles/are-public-wi-fi-networks-safe-what-you-need-know

[3] MDN Web Docs. (n.d.). Strict-Transport-Security header.
https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/Strict-Transport-Security

[4] 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

[5] CISA. (n.d.). Malware, Phishing, and Ransomware.
https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

جوابی کلید: چیک پوائنٹ 1 – کثیر انتخابی

1 سوال 1 — درست جواب: A

تدریسی نوٹ

مین اِن دی مڈل (MitM) حملہ کیا ہے؟ → مشترکہ نیٹ ورک پر دو فریقوں کے درمیان مواصلات کو روکنا اور بدلنا

2 سوال 2 — درست جواب: A

تدریسی نوٹ

روگ ایکسیس پوائنٹ (ایول ٹون) کیا ہے؟ → بدنیت وائی فائی ہاٹ اسپاٹ جو جائز نیٹ ورک جیسے ہی SSID کے ساتھ ترتیب دیا گیا ہو

3 سوال 3 — درست جواب: A

تدریسی نوٹ

VPN عوامی Wi-Fi ٹریفک کا تحفظ کیسے کرتا ہے؟ → یہ تمام نیٹ ورک پیکٹس کو خفیہ ٹنل میں لپیٹ دیتا ہے اور سنفرز کے لیے انہیں ناقابلِ مطالعہ بنا دیتا ہے

4 سوال 4 — درست جواب: A

تدریسی نوٹ

پیکٹ سنفنگ کیا ہے؟ → نیٹ ورک پیکٹس کو پکڑنے اور لاگ کرنے کے لیے ہارڈ ویئر یا سافٹ ویئر ٹولز استعمال کرنا

5 سوال 5 — درست جواب: A

تدریسی نوٹ

HTTPS کا کردار کیا ہے؟ → براؤزر اور ویب سرور کے درمیان سیشن ٹریفک کو خفیہ کرنا

جوابی کلید: چیک پوائنٹ 2 – درست یا غلط

6 سوال 6

درست جواب: درست

تدریسی نوٹ

جڑے ہوئے صارفین کھلے عوامی Wi-Fi نیٹ ورکس پر سادہ متن ڈیٹا آسانی سے پکڑ سکتے ہیں۔

7 سوال 7

درست جواب: غلط

تدریسی نوٹ

غلط: Evil Twin ایک غیر مجاز ہاٹ اسپاٹ ہے جو حملہ آور اصلی ہاٹ اسپاٹ کی نقل کرنے کے لیے بناتا ہے۔

8 سوال 8

درست جواب: غلط

تدریسی نوٹ

غلط: VPN ٹریفک کو ٹنل میں خفیہ کرتا ہے، اس لیے مقامی سنفرز اسے پڑھ نہیں سکتے۔

9 سوال 9

درست جواب: غلط

تدریسی نوٹ

غلط: HTTPS پورے HTTP تبادلے کو خفیہ کرتا ہے، جس میں URL پاتھ اور صفحے کا مواد بھی شامل ہے۔

10 سوال 10

درست جواب: درست

تدریسی نوٹ

WPA3 سیکیورٹی استعمال کرنے والے وائی فائی ہاٹ اسپاٹس کھلے، بغیر پاس ورڈ والے نیٹ ورکس کے مقابلے میں زیادہ مضبوط تحفظ فراہم کرتے ہیں۔

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

E 1. مداخلت	F 2. اسنفنگ	D 3. ایول ٹون	H 4. HTTPS
G 5. VPN	B 6. ٹنل	A 7. WPA3	C 8. فائر وال

چیک پوائنٹ 3: جوابی کلید – اہم اصطلاحات

1 مداخلت	2 سنیفنگ	3 ایول ٹوئن	4 HTTPS
5 وی پی این	6 ٹنل		

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

1 G – ڈبلیوپیاے	2 C – ایولٹوئن	3 B – سنیفنگ	4 F – ٹنل
5 H – فائروال	6 A – مداخلت	7 E – وی پی این	8 D – پروٹوکول

اساتذہ کے لیے بحث کے نوٹس

اہم اصطلاحات:
یقینی بنائیں کہ طلبہ مداخلت، اسنفنگ اور ایول ٹون 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۔

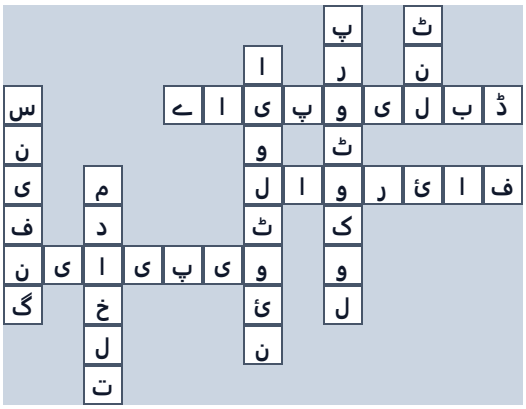
ماخذ کی جانچ:
طلبہ سے کہیں کہ ورک شیٹ کے ماخذ میں کم از کم ایک دعوے کی تصدیق کریں، اور اس پر بات کریں کہ اعداد و شمار، قیمتیں اور قواعد وقت کے ساتھ کیوں بدل سکتے ہیں۔

پہیلیوں کی کلیدیں اور استاد کے نوٹس

الفاظ کی تلاش کا حل

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

کراس ورڈ کا حل



کراس ورڈ حل کے لیے استاد کی گائیڈ

افقی

4 افقی: ڈبلیوپیاے جدید Wi-Fi سیکیورٹی معیار (9 حروف)

6 افقی: فائروال آنے والے ٹریفک کی فلٹرنگ (7 حروف)

8 افقی: ویپیاین انکرپٹڈ ورچوئل پرائیویٹ نیٹ ورک (7 حروف)

عمودی

1 عمودی: ٹنل ترسیل کے دوران ڈیٹا کا محفوظ راستہ (3 حروف)

2 عمودی: پروٹوکول محفوظ ویب ترسیل (8 حروف)

3 عمودی: ایولٹوئن Wi-Fi کی نقل کرنے والا جعلی ہاٹ اسپاٹ (8 حروف)

5 عمودی: سنیفنگ نیٹ ورک ڈیٹا پیکٹس کو پکڑنا (6 حروف)

7 عمودی: مداخلت ٹرانزٹ میں ٹریفک پڑھنا (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. امخلتد — مداخلت
2. لانیئوٹو — ایولٹوئن
3. یوانپپی — ویپیاین
4. وےاییپڈبل — ڈبلیوپیاے
5. فیگسنن — سنیفنگ
6. ولٹکپورو — پروٹوکول
7. لنٹ — ٹنل
8. ارلفاوئ — فائروال

خفیہ سائفر چیلنج کی کلید

"وائی فائی ٹریفک انکرپٹ کریں"

کیس اسٹڈیز کی جوابی کلید

A کیس اسٹڈی 1: عوامی Wi-Fi پر پیکٹ سنیفنگ کی روک تھام

استاد کا حل

گریڈنگ کی ہدایت

طلبہ کے جوابات میں درج ذیل نکات شامل ہونے چاہییں:

- منظرنامے کا تجزیہ: ہوائی اڈے کے عوامی Wi-Fi نیٹ ورک سے جڑا ایک ریموٹ سیلز ایگزیکٹو نوٹ کرتا ہے کہ کئی حساس کاروباری ای میلز سادہ متن میں بھیجنے کے فوراً بعد لیک ہو گئیں۔
- تجویز کردہ حکمت عملی اور حل: تمام ریموٹ ورک اسٹیشنز پر انٹرپرائز VPN کلائنٹ کا استعمال لازمی قرار دیں۔ صرف HTTPS والی براؤزر ایکسٹینشنز نافذ کریں، اور کلائنٹ فائر وال پر غیر خفیہ شدہ پروٹوکولز (جیسے HTTP اور FTP) بلاک کریں۔

B کیس اسٹڈی 2: ایول ٹوئن جعلی ہاٹ اسپاٹ سے دفاع

استاد کا حل

گریڈنگ کی ہدایت

طلبہ کے جوابات میں درج ذیل نکات شامل ہونے چاہییں:

- منظرنامے کا تجزیہ: حملہ آور 'CoffeeShop_Guest' نام کا ایک جعلی وائرلیس ایکسیس پوائنٹ لگاتے ہیں جو کیفے کے اصل ہاٹ اسپاٹ کی نقل کرتا ہے، اور بے خبر مہمانوں کا نیٹ ورک ٹریفک حاصل کر لیتے ہیں۔
- تجویز کردہ حکمت عملی اور حل: نیٹ ورک کی صداقت کی تصدیق کے لیے ایکسیس پوائنٹ BSSID MAC ایڈریسز کا آڈٹ کریں۔ کھلے نیٹ ورکس سے کنکشن کو روکنے کے لیے کلائنٹ پوسچر ویلیڈیشن نافذ کریں، اور حساس کام کے لیے سیلولر ہاٹ اسپاٹس لازمی قرار دیں۔