نام: _____ تاریخ: _____ نمبر: _____

سائبر سیکیورٹی کی بنیادی باتیں اور آن لائن خطرات روک تھام

سائبر سیکیورٹی کے خطرات، نیٹ ورک فائر والز، ملٹی فیکٹر توثیق، سیکیورٹی فریم ورکس

سائبر سیکیورٹی کی بنیادی باتوں کا تعلیمی جائزہ

محفوظ شدہ
ڈیٹا کی خفیہ کاری
256 بٹ AES معیار

تعمیل شدہ
عالمی معیارات
GDPR اور CCPA فریم ورکس

زیرو ٹرسٹ
رسائی کی پالیسی
ملٹی فیکٹر تصدیق

خوش آمدید! یہ سرگرمی پیکٹ آپ کو سائبر سیکیورٹی کی بنیادیات اور آن لائن خطرات سے بچاؤ کے اصولوں سے متعارف کراتا ہے۔ آپ میل ویئر کے خطرات، ملٹی فیکٹر تصدیق، نیٹ ورک فائر والز، اور واقعے کے ردعمل کے فریم ورکس 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/

آپ کا سائبر سیکیورٹی کی بنیادی باتوں کا لرننگ روڈ میپ

- میل ویئر، فشنگ اور کارپوریٹ نیٹ ورک میں دراندازی کے عام ذرائع کی نشاندہی کریں۔
- MFA، فائر والز اور اینڈ پوائنٹ ڈیفنس سمیت معیاری سائبر سیکیورٹی کنٹرولز نافذ کریں۔
- ڈیٹا بریچ کے اثرات کم کرنے کے لیے واقعے کے جواب کے طریقہ کار کا جائزہ لیں۔
- NIST ہدایات کے تحت ادارہ جاتی خطرے کے عوامل اور سیکیورٹی ہم آہنگی کا تجزیہ کریں۔
- خودکار کریڈینشل اسٹفنگ کے اثرات کم کرنے کے لیے سیکیورٹی حفظانِ صحت کے طریقے ترتیب دیں۔

سائبر سیکیورٹی رہنمائی کی ہدایات

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

سائبر سیکیورٹی کی بنیادی باتیں اور خطرات کی روک تھام (تعارف)

سائبر سیکیورٹی نیٹ ورکس، سسٹمز اور ڈیٹا کو غیر مجاز ڈیجیٹل حملوں سے بچاتی ہے۔ مضبوط سیکیورٹی عادات اپنانا، فائر والز ترتیب دینا، ملٹی فیکٹر توثیق لازمی کرنا، اور عملے کو خطرات پہچاننے کی تربیت دینا کارپوریٹ نیٹ ورک کے دفاع کے لازمی اجزاء ہیں۔

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

چیک پوائنٹ 1: کثیر انتخابی چیلنج

1. فشنگ حملے کا بنیادی مقصد کیا ہے؟

- A. اسناد اور حساس صارف ڈیٹا چرانا
- B. ویب سائٹ کی سرچ انجن میں نمایاں حیثیت بہتر بنانا
- C. نیٹ ورک بینڈ وڈتھ کی گنجائش بڑھانا
- D. بیک اپ ڈیٹا سینٹر ریپلیکیشن کا انتظام کرنا

2. کون سا میکانزم اکاؤنٹ کا مضبوط ترین تحفظ فراہم کرتا ہے؟

- A. ہارڈ ویئر کیز کے ساتھ ملٹی فیکٹر تصدیق
- B. پیچیدہ پاس ورڈز جو ہر تیس دن بعد اپ ڈیٹ کیے جائیں
- C. اکاؤنٹ لاگ اِن کو کاروباری اوقات تک محدود کرنا
- D. اکاؤنٹ کا صارف نام عوامی ڈائریکٹریز سے چھپانا

3. رینسم ویئر انفیکشن پے لوڈ کی تعریف کیا ہے؟

- A. سسٹم فائلوں کو خفیہ کرنا اور ادائیگی کا مطالبہ کرنا
- B. خاموشی سے کی اسٹروکس ریموٹ سرورز کو لاگ کرنا
- C. براؤزرز میں غیر مجاز اشتہارات داخل کرنا
- D. کرپٹو کرنسی مائن کرنے کے لیے مقامی CPU وسائل استعمال کرنا

4. زیرو ڈے ایکسپلائٹ سیکیورٹی دفاع پر کیسے اثر انداز ہوتا ہے؟

- A. یہ بغیر پیچ والی، نامعلوم کمزوریوں کو نشانہ بناتا ہے
- B. یہ کارپوریٹ فائر وال کو خودکار طور پر بند کر دیتا ہے
- C. یہ سسٹم کو ہارڈ ری بوٹ کرنے پر مجبور کرتا ہے
- D. اس کے ازالے کے لیے صفر بجٹ درکار ہے

5. کون سا فریم ورک کارپوریٹ سیکیورٹی کنٹرولز کو منظم کرتا ہے؟

- A. NIST سائبر سیکیورٹی فریم ورک کی ہدایات
- B. W3C HTML5 دستاویزی اسکیما کی تفصیلات
- C. پرنٹر ڈرائیور کی تنصیب کے دستی
- D. IETF روٹنگ پروٹوکول کی تعریفیں

چیک پوائنٹ 2: درست یا غلط چیلنج

6 سوال (درست/غلط) 6

6. فشنگ حملے صرف ذاتی ای میل اکاؤنٹس کو نشانہ بناتے ہیں۔

درست غلط

7 سوال (درست/غلط) 7

7. ملٹی فیکٹر تصدیق کریڈینشل اسٹفنگ حملوں کو بلاک کرنے میں مدد دیتی ہے۔

درست غلط

8 سوال (درست/غلط) 8

8. فائر والز غیر مجاز پورٹ رسائی کو بلاک کرنے کے لیے نیٹ ورک ٹریفک کا معائنہ کرتے ہیں۔

درست غلط

9 سوال (درست/غلط) 9

9. زیرو ڈے ایکسپلائٹس کے ازالے کے لیے معیاری اینٹی وائرس ڈیفینیشن اپ ڈیٹس درکار ہیں۔

درست غلط

10 سوال (درست/غلط) 10

10. ہنی پاٹ ایک ڈیکوئے سرور ہے جو سائبر مجرموں کو پھنسانے کے لیے استعمال ہوتا ہے۔

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. نیٹ ورک منتظمین آنے والے ٹریفک کو فلٹر کرنے کے لیے ایک _____ انسٹال کرتے ہیں۔
2. حملہ آور سسٹم پیچز کو بائی پاس کرنے کے لیے زیرو ڈے _____ استعمال کرتا ہے۔
3. حملہ آور ملازمین کے خلاف _____ مہمات چلانے کے لیے جعلی ای میلز بھیجتے ہیں۔
4. رینسم ویئر _____ کی ایک تباہ کن شکل ہے جو صارف کا ڈیٹا مقفل کر دیتی ہے۔
5. مضبوط پاس ورڈ _____ اپنانا اسناد کی چوری کے خطرات کم کرتا ہے۔
6. حساس مواصلات کے تحفظ کے لیے صارفین _____ پروٹوکولز استعمال کرتے ہیں۔

الفاظ کا بینک

انکرپشن ایکسپلائٹ حفظان صحت فائر وال فشنگ ملٹی فیکٹر میل ویئر ہنی پاٹ

اپنے جوابات یہاں لکھیں:

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

چیک پوائنٹ 4: سیکیورٹی تصورات کا ملان

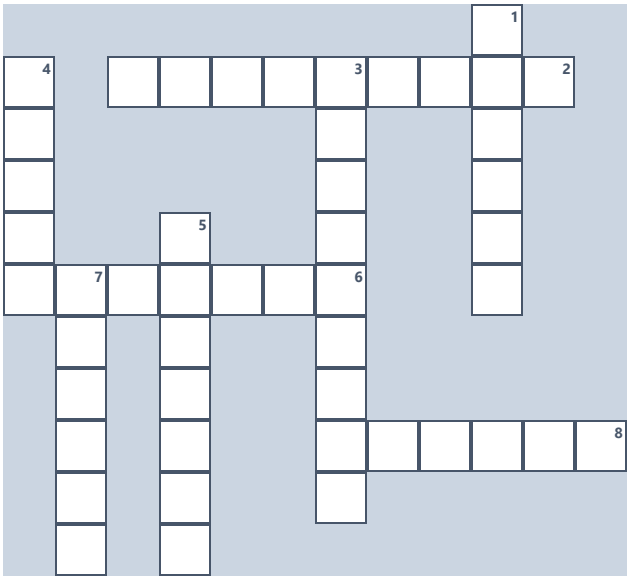
تعریفوں کا ملان

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. رینسم ویئر خطرہ		A — NIST جیسے منظم رہنما اصول جو سائبر خطرات کو سنبھالنے کے لیے استعمال ہوتے ہیں۔
2. ملٹی فیکٹر تصدیق		B — سیکیورٹی خلاف ورزیوں کو سنبھالنے اور ان کے اثرات کم کرنے کا منظم منصوبہ۔
3. زیرو ڈے استحصال		C — نیٹ ورک رکاوٹ جو سیکیورٹی رولز کی بنیاد پر ٹریفک کو فلٹر کرتی ہے۔
4. فریبی ہنی پاٹ		D — میل ویئر جو ڈیٹا کو خفیہ کرتا ہے اور ڈی کرپشن کے لیے مالی ادائیگی کا مطالبہ کرتا ہے۔
5. مداخلت فائر وال		E — وینڈر کا پیچ جاری ہونے سے پہلے نشانہ بنایا جانے والا کمزوری کا استحصال۔
6. واقعے کا ردِعمل		F — اسناد اور توثیقی کیز کے انتظام کے بہترین طریقے۔
7. پاس ورڈ کی صفائی و احتیاط		G — سیکیورٹی کی توثیق جس کے لیے دو یا زیادہ تصدیقی عوامل درکار ہوتے ہیں۔
8. سیکیورٹی فریم ورک		H — فریبی نظام جو بدنیت عناصر کو پھنسانے اور ان کا تجزیہ کرنے کے لیے بنایا جاتا ہے۔

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. میل ویئر جو ڈیٹا انکرپٹ کر کے ڈی کرپشن کے لیے مالی ادائیگی کا مطالبہ کرتا ہے (9)

6. نیٹ ورک کی رکاوٹ جو سیکیورٹی اصولوں کی بنیاد پر ٹریفک فلٹر کرتی ہے (7)

8. فریبی سسٹم جو بدنیت عناصر کو پھنسانے اور ان کا تجزیہ کرنے کے لیے بنایا جاتا ہے (6)

عمودی

1. ونڈر کا پیچ جاری ہونے سے پہلے نشانہ بنایا جانے والا کمزوری کا استحصال (6)

3. سیکیورٹی کی توثیق جس میں دو یا زیادہ تصدیقی عوامل درکار ہوتے ہیں (9)

4. سیکیورٹی خلاف ورزیوں سے نمٹنے اور ان کے اثرات کم کرنے کا منظم منصوبہ (5)

5. NIST جیسی منظم ہدایات جو سائبر خطرات کے انتظام میں استعمال ہوتی ہیں (7)

7. اسناد اور تصدیقی کیز کے انتظام کے بہترین طریقے (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: میل ویئر جو ڈیٹا انکرپٹ کر کے ڈی کرپشن کے لیے مالی ادائیگی کا مطالبہ کرتا ہے (9 حروف):

6 افقی: نیٹ ورک کی رکاوٹ جو سیکیورٹی اصولوں کی بنیاد پر ٹریفک فلٹر کرتی ہے (7 حروف):

8 افقی: فریبی سسٹم جو بدنیت عناصر کو پھنسانے اور ان کا تجزیہ کرنے کے لیے بنایا جاتا ہے (6 حروف):

عمودی

1 عمودی: وینڈر کا پیچ جاری ہونے سے پہلے نشانہ بنایا جانے والا کمزوری کا استحصال (6 حروف):

3 عمودی: سیکیورٹی کی توثیق جس میں دو یا زیادہ تصدیقی عوامل درکار ہوتے ہیں (9 حروف):

4 عمودی: سیکیورٹی خلاف ورزیوں سے نمٹنے اور ان کے اثرات کم کرنے کا منظم منصوبہ (5 حروف):

5 عمودی: NIST جیسی منظم ہدایات جو سائبر خطرات کے انتظام میں استعمال ہوتی ہیں (7 حروف):

7 عمودی: اسناد اور تصدیقی کیز کے انتظام کے بہترین طریقے (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۔

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

الفاظ کی فہرست

رینسمویئر ملٹیفیکٹر زیروڈے ہنیپاٹ فائروال ردعمل انتظام فریمورک

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. رینسمویئر
B. ملٹیفیکٹر
C. زیروڈے
D. ہنیپاٹ
E. فائروال
F. ردعمل
G. انتظام
H. فریمورک

تعریفیں اور ملان کے خانے
1. نیٹ ورک کی رکاوٹ جو سیکیورٹی اصولوں کی بنیاد پر ٹریفک فلٹر کرتی ہے۔
2. سیکیورٹی خلاف ورزیوں سے نمٹنے اور ان کے اثرات کم کرنے کا منظم منصوبہ۔
3. میل ویئر جو ڈیٹا انکرپٹ کر کے ڈی کرپشن کے لیے مالی ادائیگی کا مطالبہ کرتا ہے۔
4. سیکیورٹی کی توثیق جس میں دو یا زیادہ تصدیقی عوامل درکار ہوتے ہیں۔
5. اسناد اور تصدیقی کیز کے انتظام کے بہترین طریقے۔
6. NIST جیسی منظم ہدایات جو سائبر خطرات کے انتظام میں استعمال ہوتی ہیں۔
7. وینڈر کا پیچ جاری ہونے سے پہلے نشانہ بنایا جانے والا کمزوری کا استحصال۔
8. فریبی سسٹم جو بدنیت عناصر کو پھنسانے اور ان کا تجزیہ کرنے کے لیے بنایا جاتا ہے۔

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. و م س ی ر ی ئ ر ن
2. ے ز ر ڈ و ی
3. ر ف و ل ئ ا ا
4. م ظ ت ا ا ن
5. ک ف ل ر ی ی م ٹ ٹ
6. ا پ ہ ی ٹ ن
7. م ل ر ع د
8. ر م ک ف ر و ی

اضافی سرگرمی: تیزی سے سوچیں

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

1. سائبر سیکیورٹی کے شعبے میں ملازمتوں کے نام
2. سافٹ ویئر اپ ڈیٹ کرنے کی وجوہات
3. وہ چیزیں جنہیں فائر وال بلاک کر سکتا ہے
4. ای میل میں انتباہی علامات
5. وہ چیزیں جن کا آپ بیک اپ لیتے ہیں
6. سائبر حملے کی معروف اقسام
7. وہ چیزیں جنہیں ہنی پاٹ اپنی طرف کھینچ سکتا ہے
8. وہ معلومات جو آپ کو کبھی شیئر نہیں کرنی چاہئیں
9. کمپیوٹر کے متاثر ہونے کی علامات
10. ہیکرز کے بارے میں فلموں یا شوز کے نام
11. سیکیورٹی کی وہ تہیں جو آپ بنا سکتے ہیں
12. سیکیورٹی ڈرل میں مشق کرنے کی چیزیں
13. آپ کے جانے پہچانے سیکیورٹی ٹولز کے نام
14. وہ لوگ جن سے آپ آئی ٹی مدد مانگ سکتے ہیں
15. وہ الفاظ جو 'سائبر' سے شروع ہوتے ہیں

چیک پوائنٹ 8: سائبر سیکیورٹی کیس اسٹڈیز

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

کیس اسٹڈی 1: رینسم ویئر سے بحالی کی حکمت عملی



منظرنامہ: ایک کارپوریٹ نیٹ ورک رینسم ویئر سے متاثر ہو گیا ہے جس نے اہم ڈیٹا بیسز لاک کر دیے ہیں۔ حملہ آور $100,000 کی کرپٹو کرنسی ادائیگی کا مطالبہ کرتے ہیں۔ کمپنی کے پاس 24 گھنٹے پرانے آف لائن بیک اپس موجود ہیں۔

بحث کا سوال: ادائیگی کرنے کے خطرات کا تجزیہ کریں، اور بحالی کی حکمت عملی کا جائزہ لیں۔

کیس اسٹڈی 2: کریڈینشل اسٹفنگ سے دفاع



منظرنامہ: ایک آن لائن سروس پر کریڈینشل اسٹفنگ حملہ ہوتا ہے، جس میں ہیکرز دوسری سائٹس سے چرائے گئے لاکھوں یوزر نیم/پاس ورڈ جوڑوں کی جانچ کرتے ہیں۔

بحث کا سوال: اس حملے کا طریقہ کار تفصیل سے بیان کریں، اور دو دفاعی نظام 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

38	18		27	37	11	20	4		14	5	28	37	26		37	5	30	31

23	34	26	9	31		31	5	18	18

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: سائبر سیکیورٹی کا بنیادی مقصد کیا ہے؟

بنیادی مقصد نیٹ ورکس، ڈیوائسز اور ڈیٹا کو غیر مجاز رسائی، حملوں اور حادثاتی نقصان سے بچانا ہے۔

Q2: فشنگ اسپیئر فشنگ سے کیسے مختلف ہے؟

فشنگ ایک وسیع ای میل مہم ہے جو بے ترتیب صارفین کو نشانہ بناتی ہے، جبکہ اسپیئر فشنگ ذاتی نوعیت کے ڈیٹا کے ذریعے مخصوص افراد کو نشانہ بناتی ہے۔

Q3: نیٹ ورک فائر وال کیا ہے؟

فائر وال نیٹ ورک سیکیورٹی سسٹم ہے جو پہلے سے طے شدہ سیکیورٹی اصولوں کی بنیاد پر آنے اور جانے والے ٹریفک کی نگرانی اور فلٹرنگ کرتا ہے۔

Q4: ملٹی فیکٹر تصدیق (MFA) کیوں ضروری ہے؟

MFA دفاع کی ایک اہم تہہ شامل کرتا ہے، جو حملہ آوروں کے بنیادی پاس ورڈ کی اسناد چرانے یا توڑنے کے باوجود رسائی کو روکتا ہے۔

Q5: کمپیوٹر وائرس کی تعریف کیا ہے؟

وائرس خود کو نقل کرنے والا میل ویئر ہے جو صاف فائلوں سے چپک جاتا ہے اور چلائے جانے پر سسٹمز میں پھیل جاتا 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: رینسم ویئر مقامی ڈیٹا کو کیسے لاک کرتا ہے؟

رینسم ویئر صارف کی فائلوں کو خفیہ کرنے کے لیے کرپٹوگرافک الگورتھم استعمال کرتا ہے، جس سے وہ اس وقت تک ناقابل مطالعہ رہتی ہیں جب تک ڈی کرپشن کلید لاگو نہ کی جائے۔

Q7: زیرو ڈے کمزوری کیا ہے؟

زیرو ڈے سافٹ ویئر کی ایسی سیکیورٹی خامی ہے جو وینڈر کو معلوم نہیں ہوتی، اس لیے ایکسپلائٹ سے پہلے پیچ تیار کرنے کا وقت نہیں ملتا۔

Q8: NIST فریم ورک کا کیا کردار ہے؟

NIST فریم ورک رضاکارانہ رہنما اصول اور معیارات فراہم کرتا ہے جو اداروں کو سائبر سیکیورٹی کے خطرات کو سنبھالنے اور کم کرنے میں مدد دیتے ہیں۔

Q9: سیکیورٹی واقعے کے جواب کا منصوبہ کیا ہے؟

یہ سیکیورٹی کی خلاف ورزیوں اور نیٹ ورک کے متاثر ہونے کا پتا لگانے، انہیں محدود کرنے اور ان سے بحالی کے دستاویزی طریقہ کار کا مجموعہ ہے۔

Q10: سوشل انجینئرنگ صارفین کا استحصال کیسے کرتی ہے؟

سوشل انجینئرنگ نفسیاتی ہیرا پھیری کے ذریعے ملازمین کو پاس ورڈز ظاہر کرنے یا نقصان دہ فائلیں ڈاؤن لوڈ کرنے پر آمادہ کرتی 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: DDoS حملہ ویب سرورز کو کیسے مغلوب کرتا ہے؟

DDoS حملہ لاکھوں متاثرہ بوٹ نیٹ ڈیوائسز کو ہم آہنگ کر کے سرور کو ٹریفک سے بھر دیتا ہے، جس سے بینڈ وڈتھ اور CPU کی حدیں ختم ہو جاتی ہیں۔

Q2: متشاکل اور غیر متشاکل خفیہ کاری میں کیا فرق ہے؟

سمیٹرک خفیہ کاری خفیہ کاری اور ڈی کرپشن کے لیے ایک ہی کی استعمال کرتی ہے، جبکہ ایسمیٹرک خفیہ کاری پبلک اور پرائیویٹ کی جوڑا استعمال کرتی ہے۔

Q3: ہیکرز SQL انجیکشن حملے کیسے کرتے ہیں؟

حملہ آور فارم کے خانوں میں نقصان دہ SQL کمانڈز ڈالتے ہیں اور بیک اینڈ ڈیٹا بیس کو دھوکا دے کر غیر مجاز صارف ریکارڈز حاصل کر لیتے ہیں۔

Q4: نیٹ ورک دراندازی میں لیٹرل موومنٹ کیا ہے؟

یہ وہ تکنیک ہے جس میں حملہ آور سرور تک ابتدائی رسائی کا فائدہ اٹھا کر اندرونی نیٹ ورک پر دیگر باہم جڑے سسٹمز کو متاثر کرتے ہیں۔

Q5: DNS اسپوفنگ ویب ٹریفک کو کیسے ری ڈائریکٹ کرتی ہے؟

DNS اسپوفنگ نیم سرور کیش ریکارڈز میں ردوبدل کرتی ہے، جس سے جائز صارفین ہدف ڈومینز کے بجائے نقصان دہ ہم شکل ویب سائٹس پر پہنچ جاتے ہیں۔

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: ہارڈ ویئر سیکیورٹی ٹوکن کیا ہے؟

یہ ایک فزیکل ڈیوائس (جیسے YubiKey) ہے جو کرپٹوگرافک تصدیقی ثبوت بناتی ہے اور ریموٹ فشنگ کے خلاف زیادہ سے زیادہ دفاع فراہم کرتی ہے۔

Q7: سیکیورٹی ٹیمیں فریبی ہنی پوٹس کا استعمال کیسے کرتی ہیں؟

ٹیمیں مداخلتوں کا جلد پتا لگانے اور غیر مجاز عناصر کے حملوں کے پیٹرنز کا تجزیہ کرنے کے لیے غیر پروڈکشن ڈیکوئے سرورز تعینات کرتی ہیں۔

Q8: کم سے کم استحقاق کا اصول کیا ہے؟

یہ سیکیورٹی کا معیار ہے جس میں صارف کے رسائی کے حقوق کو ان کے کام کے کردار انجام دینے کے لیے ضروری کم سے کم حد تک محدود کیا جاتا ہے۔

Q9: مین-ان-دی-مڈل حملہ کنکشنز کا استحصال کیسے کرتا ہے؟

حملہ آور غیر خفیہ نیٹ ورکس پر دو ڈیوائسز کے درمیان مواصلات کو روک کر بدل دیتا ہے اور سیشن ٹوکنز اور اسناد چرا لیتا ہے۔

Q10: سمجھوتے کے اشارے (IOCs) کیا ہیں؟

IOCs فرانزک ڈیٹا کے اشارے ہیں، جیسے رجسٹری میں غیر معمولی تبدیلیاں یا مشکوک IP ٹریفک، جو ظاہر کرتے ہیں کہ سسٹم کی خلاف ورزی ہوئی 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

حملہ آور مسلسل انٹرنیٹ پر کمزور سرورز کی اسکیننگ کرتے ہیں اور ملازمین کے ان باکس میں فشنگ ای میلز بھیجتے ہیں۔

2. سیکیورٹی بصیرت

انسانی غلطی، جیسے فشنگ لنکس پر کلک کرنا، ڈیٹا کی خلاف ورزیوں میں ایک عام عنصر ہے، اسی لیے تربیت اہم ہے۔

3. سیکیورٹی بصیرت

ڈیٹا بریچ کی لاگتوں میں قانونی جرمانے، صارفین کا چھوڑ جانا، تفتیش اور مرمت شامل ہیں، اور یہ لاکھوں ڈالر تک پہنچ سکتی ہیں۔

4. سیکیورٹی بصیرت

فشنگ سے مزاحم MFA، جیسے ہارڈ ویئر سیکیورٹی کیز، MFA کی سب سے مضبوط قسم ہے اور وہ معیار ہے جس کی CISA تاکید کرتا ہے۔ [2]

5. سیکیورٹی بصیرت

رینسم ویئر انٹرپرائز نیٹ ورکس کے لیے ایک بڑا خطرہ بنا ہوا ہے، اور CISA آف لائن، خفیہ کردہ بیک اپس کو بنیادی دفاع کے طور پر اپنانے پر زور دیتا ہے۔ [4]

6. سیکیورٹی بصیرت

NIST سائبر سیکیورٹی فریم ورک 2.0 (2024) کے چھ بنیادی افعال ہیں: Govern، Identify، Protect، Detect، Respond، Recover۔ [1]

7. سیکیورٹی کی بصیرت

کریڈینشل اسٹفنگ بوٹس بینکنگ اور ای کامرس لاگ اِن پورٹلز پر لیک شدہ صارف نام اور پاس ورڈ کے جوڑوں کو بڑے پیمانے پر آزماتے ہیں۔

8. سیکیورٹی کی بصیرت

زیرو ڈے ایکسپلائٹ مارکیٹس دنیا بھر میں موجود ہیں، جہاں شدید نوعیت کی کمزوریاں پیچ ہونے سے پہلے بھاری رقوم میں بک سکتی ہیں۔

9. سیکیورٹی کی بصیرت

ہنی پاٹ ڈیکوئے سسٹم دراندازی کے الرٹس فوراً رپورٹ کرتا ہے کیونکہ جائز صارفین کے پاس اسے استعمال کرنے کی کوئی وجہ نہیں ہوتی۔

10. سیکیورٹی بصیرت

Transport Layer Security (TLS) براؤزر سیشنز کو خفیہ کرتا ہے، جس سے عوامی Wi-Fi نیٹ ورکس پر پیکٹ سنفنگ کی روک تھام ہوتی 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] NIST. (2024). The NIST Cybersecurity Framework (CSF) 2.0.
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[2] CISA. (n.d.). More than a Password.
https://www.cisa.gov/MFA

[3] 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

[4] CISA. (2023). #StopRansomware Guide.
https://www.cisa.gov/stopransomware/ransomware-guide

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

[6] NIST. (2025). SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile.
https://csrc.nist.gov/pubs/sp/800/61/r3/final

[7] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.
https://pages.nist.gov/800-63-4/sp800-63b.html

[8] OWASP. (n.d.). SQL Injection.
https://owasp.org/www-community/attacks/SQL_Injection

جوابی کلید: چیک پوائنٹ 1 – کثیر انتخابی

1 فشنگ حملے
فشنگ
درست جواب: A

تدریسی نوٹ

فشنگ مہمات جعلی ای میلز کے ذریعے اسناد اور حساس صارف ڈیٹا چرانے کی کوشش کرتی ہیں۔ حوالہ: OWASP Secure Configuration۔

2 اکاؤنٹ پروٹیکشن
MFA کی
درست جواب: A

تدریسی نوٹ

ہارڈ ویئر ٹوکنز استعمال کرنے والی ملٹی فیکٹر تصدیق (MFA) اکاؤنٹ رسائی کا سب سے مضبوط دفاع فراہم کرتی ہے۔ حوالہ: NIST Digital Identity۔

3 رینسم ویئر کا خطرہ
رینسم ویئر
درست جواب: A

تدریسی نوٹ

رینسم ویئر اہم سسٹمز اور ڈیٹا کو خفیہ کر دیتا ہے اور ڈی کرپشن کیز کے بدلے کرپٹو کرنسی میں ادائیگی کا مطالبہ کرتا ہے۔ حوالہ: Center for Internet Security (CIS)۔

4 زیرو ڈے کمزوری
زیرو ڈے
درست جواب: A

تدریسی نوٹ

زیرو ڈے خطرات ایسی غیر پیچ شدہ، نامعلوم سیکیورٹی خامیوں کا فائدہ اٹھاتے ہیں جن کا وینڈر پیچ دستیاب ہونے سے پہلے کا وقت ہو۔ حوالہ: OWASP Secure Configuration۔

5 سیکیورٹی فریم ورکس
فریم ورکس
درست جواب: A

تدریسی نوٹ

NIST جیسے فریم ورکس تنظیموں کو سائبر خطرات کا انتظام کرنے اور انہیں کم کرنے میں مدد کے لیے منظم ہدایات فراہم کرتے ہیں۔ حوالہ: NIST Digital Identity۔

جوابی کلید: چیک پوائنٹ 2 – درست یا غلط

6 ہدف شدہ فشنگ

فشنگ

درست جواب: غلط

تدریسی نوٹ

فشنگ حملے حملے کے راستے بڑھانے کے لیے کارپوریٹ نیٹ ورکس اور ذاتی اکاؤنٹس دونوں کو نشانہ بناتے ہیں۔ حوالہ: OWASP Secure Configuration۔

7 سوال 7

درست جواب: درست

تدریسی نوٹ

MFA دوسرا عنصر مانگتی ہے، اس لیے صرف چوری شدہ پاس ورڈ عموماً لاگ ان کے لیے کافی نہیں ہوتا۔

8 ٹریفک فائر وال

فائر وال

درست جواب: درست

تدریسی نوٹ

فائر والز غیر مجاز کنکشنز کو چھاننے کے لیے مخصوص نیٹ ورک پورٹس پر ٹریفک کا معائنہ کرتے اور اسے بلاک کرتے ہیں۔ حوالہ: Center for Internet Security (CIS)۔

9 زیرو ڈے ردعمل

زیرو ڈے

درست جواب: غلط

تدریسی نوٹ

زیرو ڈے خامیوں کے ازالے کے لیے کوڈ پیچز اور WAF فلٹرنگ درکار ہے کیونکہ ابھی سگنیچرز موجود نہیں ہوتے۔ حوالہ: OWASP Secure Configuration۔

10 فریبی ہنی پاٹس

ہنی پاٹ

درست جواب: درست

تدریسی نوٹ

ہنی پاٹس فریب دہی والے سرورز ہیں جنہیں سیکیورٹی ٹیمیں بدنیت عناصر کو پھنسانے، الرٹ حاصل کرنے اور ان کا مطالعہ کرنے کے لیے استعمال کرتی ہیں۔ حوالہ: Center for Internet Security (CIS)۔

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

D 1. رینسم ویئر خطرہ	G 2. ملٹی فیکٹر تصدیق	E 3. زیرو ڈے استحصال	H 4. فریبی ہنی پاٹ
C 5. مداخلت فائر وال	B 6. واقعے کا ردِعمل	F 7. پاس ورڈ کی صفائی و احتیاط	A 8. سیکیورٹی فریم ورک

چیک پوائنٹ 3: جوابی کلید – اہم اصطلاحات

1 فائر وال	2 ایکسپلائٹ	3 فشنگ	4 میل ویئر
5 حفظان صحت	6 انکرپشن		

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

1 E – فائروال	2 F – ردعمل	3 A – رینسمویئر	4 B – ملٹیفیکٹر
5 G – انتظام	6 H – فریمورک	7 C – زیروڈے	8 D – ہنیپاٹ

اساتذہ کے لیے بحث کے نوٹس

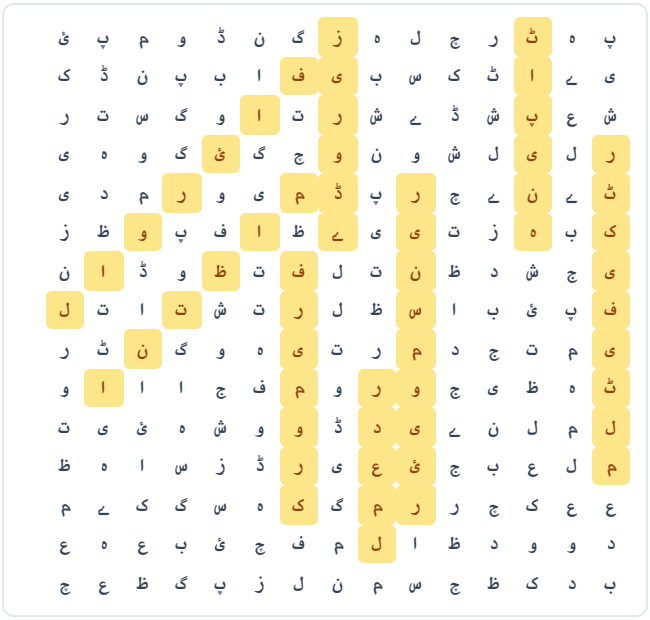
اہم اصطلاحات:
یقینی بنائیں کہ طلبہ رینسم ویئر خطرہ، ملٹی فیکٹر تصدیق اور زیرو ڈے استحصال کو اپنے الفاظ میں سمجھا سکیں اور ہر ایک کی مثال دے سکیں۔

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

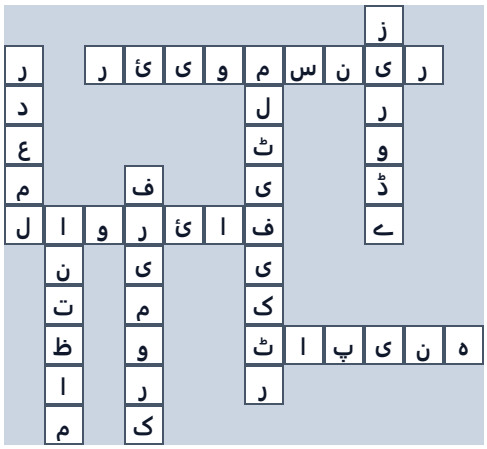
ماخذ کی جانچ:
طلبہ سے کہیں کہ ورک شیٹ کے ماخذ میں کم از کم ایک دعوے کی تصدیق کریں، اور اس پر بات کریں کہ اعداد و شمار، قیمتیں اور قواعد وقت کے ساتھ کیوں بدل سکتے ہیں۔

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: رینسمویئر میل ویئر جو ڈیٹا انکرپٹ کر کے ڈی کرپشن کے لیے مالی ادائیگی کا مطالبہ کرتا ہے (9 حروف)

6 افقی: فائروال نیٹ ورک کی رکاوٹ جو سیکیورٹی اصولوں کی بنیاد پر ٹریفک فلٹر کرتی ہے (7 حروف)

8 افقی: ہنیپاٹ فریبی سسٹم جو بدنیت عناصر کو پھنسانے اور ان کا تجزیہ کرنے کے لیے بنایا جاتا ہے (6 حروف)

عمودی

1 عمودی: زیروڈے وینڈر کا پیچ جاری ہونے سے پہلے نشانہ بنایا جانے والا کمزوری کا استحصال (6 حروف)

3 عمودی: ملٹیفیکٹر سیکیورٹی کی توثیق جس میں دو یا زیادہ تصدیقی عوامل درکار ہوتے ہیں (9 حروف)

4 عمودی: ردعمل سیکیورٹی خلاف ورزیوں سے نمٹنے اور ان کے اثرات کم کرنے کا منظم منصوبہ (5 حروف)

5 عمودی: فریمورک NIST جیسی منظم ہدایات جو سائبر خطرات کے انتظام میں استعمال ہوتی ہیں (7 حروف)

7 عمودی: انتظام اسناد اور تصدیقی کیز کے انتظام کے بہترین طریقے (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. ومسیریئرن — رینسمویئر
2. ےزرڈوی — زیروڈے
3. رفولئاا — فائروال
4. مظتاان — انتظام
5. کفلرییمٹٹ — ملٹیفیکٹر
6. اپہیٹن — ہنیپاٹ
7. ملرعد — ردعمل
8. رمکفروی — فریمورک

خفیہ سائفر چیلنج کی کلید

"ملٹی فیکٹر تصدیق سے سسٹم محفوظ"

کیس اسٹڈیز کی جوابی کلید

A کیس اسٹڈی 1: رینسم ویئر سے بحالی کی حکمت عملی

استاد کا حل

گریڈنگ کی ہدایت

طلبہ کے جوابات میں درج ذیل نکات شامل ہونے چاہییں:

- منظرنامے کا تجزیہ: ایک کارپوریٹ نیٹ ورک رینسم ویئر سے متاثر ہے، جس نے اہم ڈیٹا بیسز لاک کر دیے ہیں۔ حملہ آور 100,000 ڈالر کی کرپٹو کرنسی ادائیگی کا مطالبہ کرتے ہیں۔ کمپنی کے پاس 24 گھنٹے پہلے کے آف لائن بیک اپس موجود ہیں۔
- تجویز کردہ حکمت عملی اور حل: ادائیگی کے خطرات: ادائیگی فائل کی ڈی کرپشن کی ضمانت نہیں دیتی، کمپنی کو ادائیگی کرنے والا ہدف بنا دیتی ہے، اور مجرمانہ سرگرمی کو فنڈ کرتی ہے۔ بحالی کی حکمت عملی: ٹیم کو متاثرہ ہوسٹس الگ کرنے، متاثرہ سرورز صاف کرنے اور آف لائن بیک اپ سے ڈیٹا بحال کرنے چاہئیں۔ فوری دوبارہ انفیکشن روکنے کے لیے انہیں ابتدائی رسائی کا ذریعہ (فشنگ یا ایکسپلائٹ) پیچ کرنا ہوگا۔

B کیس اسٹڈی 2: کریڈینشل اسٹفنگ سے دفاع

استاد کا حل

گریڈنگ کی ہدایت

طلبہ کے جوابات میں درج ذیل نکات شامل ہونے چاہییں:

- منظرنامے کا تجزیہ: ایک آن لائن سروس کریڈینشل اسٹفنگ حملے کا سامنا کرتی ہے، جس میں ہیکرز دوسری سائٹس سے چرائے گئے لاکھوں صارف نام/پاس ورڈ جوڑوں کو آزماتے ہیں۔
- تجویز کردہ حکمت عملی اور حل: طریقہ کار: حملہ آور خودکار بوٹس کے ذریعے مختلف سائٹس پر پاس ورڈ کے دوبارہ استعمال کا فائدہ اٹھا کر صارف اکاؤنٹس میں لاگ اِن کرتے ہیں۔ دفاعی اقدامات: 1. ملٹی فیکٹر تصدیق (MFA) پاس ورڈ درست ہونے پر بھی لاگ اِن کوششوں کو بلاک کرتی ہے۔ 2. ریٹ لمٹنگ اور CAPTCHAs نافذ کرنے سے لاگ اِن اینڈ پوائنٹس پر اسپام کرنے والا خودکار بوٹ ٹریفک بلاک ہوتا ہے۔