नाम: _____ दिनांक: _____ अंक: _____

साइबर सुरक्षा की बुनियादी बातें और ऑनलाइन खतरे रोकथाम

साइबर सुरक्षा खतरे, नेटवर्क फ़ायरवॉल, बहु-कारक प्रमाणीकरण, सुरक्षा फ़्रेमवर्क

साइबर सुरक्षा की बुनियादी बातें: सीखने का अवलोकन

सुरक्षित किया गया
डेटा एन्क्रिप्शन
256-बिट AES मानक

अनुपालक
वैश्विक मानक
GDPR और CCPA फ़्रेमवर्क

ज़ीरो-ट्रस्ट
एक्सेस नीति
मल्टी-फ़ैक्टर ऑथेंटिकेशन

स्वागत है! यह गतिविधि पैकेट आपको साइबर सुरक्षा की बुनियादी बातों और ऑनलाइन खतरों की रोकथाम के मूल सिद्धांतों से परिचित कराता है। आप मैलवेयर खतरे, मल्टी-फ़ैक्टर प्रमाणीकरण, नेटवर्क फ़ायरवॉल और इंसिडेंट रिस्पॉन्स फ़्रेमवर्क का अध्ययन करेंगे।

वर्कशीट चेकपॉइंट

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

VPN.com साइबर सुरक्षा गाइड खोलें

URL: https://www.vpn.com/hi/saibhar-suraksha/

आपका साइबर सुरक्षा की बुनियादी बातें लर्निंग रोडमैप

- मैलवेयर, फ़िशिंग और कॉर्पोरेट नेटवर्क घुसपैठ के आम माध्यमों की पहचान करें।
- MFA, फ़ायरवॉल और एंडपॉइंट सुरक्षा सहित मानक साइबर सुरक्षा नियंत्रण लागू करें।
- डेटा उल्लंघन के प्रभाव घटाने के लिए घटना-प्रतिक्रिया प्रक्रियाओं का मूल्यांकन करें।
- NIST दिशानिर्देशों के तहत संगठनात्मक जोखिम कारकों और सुरक्षा संरेखण का विश्लेषण करें।
- स्वचालित क्रेडेंशियल स्टफ़िंग को कम करने के लिए सुरक्षा स्वच्छता अभ्यास कॉन्फ़िगर करें।

साइबर सुरक्षा गाइड के 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 खतरा रोकथाम पर लागू करें। अंत में अतिरिक्त गतिविधि झटपट सोचें पूरी करें।

साइबर सुरक्षा की बुनियादी बातें और खतरों की रोकथाम (परिचय)

साइबर सुरक्षा नेटवर्क, सिस्टम और डेटा को अनधिकृत डिजिटल हमलों से बचाती है। मज़बूत सुरक्षा आदतें विकसित करना, फ़ायरवॉल कॉन्फ़िगर करना, बहु-कारक प्रमाणीकरण अनिवार्य करना और कर्मचारियों को खतरे पहचानने का प्रशिक्षण देना कॉर्पोरेट नेटवर्क सुरक्षा के आवश्यक घटक हैं।

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

चेकपॉइंट 1: बहुविकल्पीय चुनौती

1 1. फ़िशिंग हमले का मुख्य उद्देश्य क्या है?

- A. क्रेडेंशियल और संवेदनशील उपयोगकर्ता डेटा चुराना
- B. वेबसाइट की सर्च इंजन दृश्यता बढ़ाना
- C. नेटवर्क बैंडविड्थ क्षमता बढ़ाना
- D. बैकअप डेटा सेंटर प्रतिकृति का प्रबंधन

2 2. कौन-सा तंत्र खाते की सबसे मज़बूत सुरक्षा देता है?

- A. हार्डवेयर कुंजियों का उपयोग करके मल्टी-फ़ैक्टर ऑथेंटिकेशन
- B. हर तीस दिन में बदले जाने वाले जटिल पासवर्ड
- C. खाते में लॉगिन को कार्य समय तक सीमित करना
- D. खाते का यूज़रनेम सार्वजनिक डायरेक्टरी से छिपाना

3 3. रैनसमवेयर संक्रमण पेलोड को क्या परिभाषित करता है?

- A. सिस्टम फ़ाइलों को एन्क्रिप्ट करके भुगतान की माँग करना
- B. चुपचाप कीस्ट्रोक रिमोट सर्वरों पर लॉग करना
- C. ब्राउज़र में अनधिकृत विज्ञापन डालना
- D. क्रिप्टोकरेंसी माइन करने के लिए लोकल CPU संसाधनों का उपयोग करना

4 4. ज़ीरो-डे एक्सप्लॉइट सुरक्षा बचावों को कैसे प्रभावित करता है?

- A. यह बिना पैच वाली, अज्ञात कमज़ोरियों को निशाना बनाता है
- B. यह कॉर्पोरेट फ़ायरवॉल अपने आप बंद कर देता है
- C. यह सिस्टम को हार्ड रीबूट करने के लिए बाध्य करता है
- D. इसके समाधान के लिए शून्य बजट चाहिए

5 5. कॉर्पोरेट सुरक्षा नियंत्रणों को कौन-सा फ़्रेमवर्क संचालित करता है?

- A. NIST साइबर सुरक्षा फ़्रेमवर्क के दिशानिर्देश
- B. W3C HTML5 दस्तावेज़ स्कीमा विनिर्देश
- C. प्रिंटर ड्राइवर इंस्टॉलेशन मैनुअल
- D. IETF रूटिंग प्रोटोकॉल परिभाषाएँ

चेकपॉइंट 2: सही या गलत चुनौती

6 प्रश्न tf 6

6. फ़िशिंग हमले केवल व्यक्तिगत ईमेल खातों को निशाना बनाते हैं।

सही गलत

7 प्रश्न tf 7

7. मल्टी-फ़ैक्टर ऑथेंटिकेशन क्रेडेंशियल स्टफ़िंग हमलों को ब्लॉक करने में मदद करता है।

सही गलत

8 प्रश्न tf 8

8. फ़ायरवॉल नेटवर्क ट्रैफ़िक की जाँच करके अनधिकृत पोर्ट एक्सेस को ब्लॉक करते हैं।

सही गलत

9 प्रश्न tf 9

9. ज़ीरो-डे एक्सप्लॉइट को ठीक करने के लिए मानक एंटी-वायरस डेफ़िनिशन अपडेट ही काफ़ी होते हैं।

सही गलत

10 प्रश्न tf 10

10. हनीपॉट एक डिकॉय सर्वर है जिसका उपयोग साइबर अपराधियों को फँसाने के लिए किया जाता है।

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. नेटवर्क प्रशासक आने वाला ट्रैफ़िक छानने के लिए _____ लगाते हैं।
2. हमलावर सिस्टम पैच को बायपास करने के लिए ज़ीरो-डे _____ का उपयोग करता है।
3. खाते की सुरक्षा बढ़ाने के लिए पासवर्ड के साथ _____ प्रमाणीकरण भी चालू रखें।
4. रैनसमवेयर _____ का विनाशकारी रूप है, जो उपयोगकर्ता का डेटा लॉक कर देता है।
5. संगठन अपनी जोखिम प्रबंधन प्रक्रियाओं को किसी मान्य सुरक्षा _____ के अनुसार व्यवस्थित करते हैं।
6. संवेदनशील संचार सुरक्षित रखने के लिए उपयोगकर्ता _____ प्रोटोकॉल लगाते हैं।

शब्दावली शब्द-बैंक

एक्सप्लॉइट | एन्क्रिप्शन | घटना प्रतिक्रिया | पासवर्ड स्वच्छता | फ़ायरवॉल | फ्रेमवर्क | मल्टी-फ़ैक्टर | मैलवेयर

अपने उत्तर यहाँ लिखें:

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

चेकपॉइंट 4: सुरक्षा अवधारणा मिलान

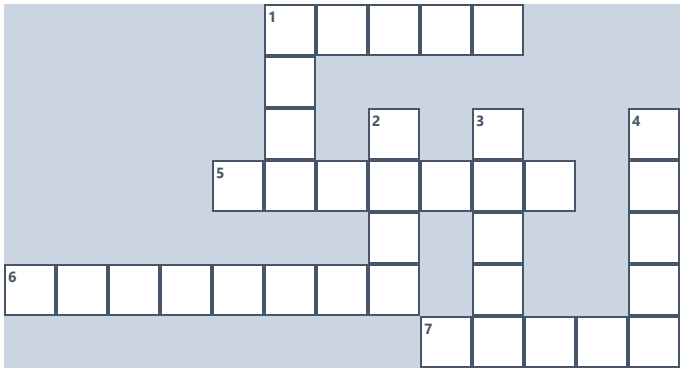
परिभाषा मिलान

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

☐	**1. रैनसमवेयर ख़तरा**	**A**	साइबर जोखिम प्रबंधित करने के लिए उपयोग होने वाले NIST जैसे संरचित दिशानिर्देश।
☐	**2. मल्टी-फ़ैक्टर ऑथ**	**B**	सुरक्षा उल्लंघनों को संभालने और घटाने की संरचित योजना।
☐	**3. ज़ीरो-डे एक्सप्लॉइट**	**C**	सुरक्षा नियमों के आधार पर ट्रैफ़िक को फ़िल्टर करने वाला नेटवर्क अवरोध।
☐	**4. डिकॉय हनीपॉट**	**D**	डेटा एन्क्रिप्ट करके डिक्रिप्शन के बदले पैसे माँगने वाला मैलवेयर।
☐	**5. इंट्रूज़न फ़ायरवॉल**	**E**	वेंडर द्वारा पैच जारी किए जाने से पहले निशाना बनाया गया भेद्यता एक्सप्लॉइट।
☐	**6. घटना प्रतिक्रिया**	**F**	क्रेडेंशियल और प्रमाणीकरण कुंजियों के प्रबंधन की सर्वोत्तम प्रथाएँ।
☐	**7. पासवर्ड स्वच्छता**	**G**	दो या अधिक प्रमाणीकरण कारकों की माँग करने वाला सुरक्षा सत्यापन।
☐	**8. सुरक्षा फ़्रेमवर्क**	**H**	दुर्भावनापूर्ण तत्वों को लुभाने और उनका विश्लेषण करने के लिए बनाया गया नकली सिस्टम।

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. सॉफ़्टवेयर की किसी कमज़ोरी का फ़ायदा उठाने वाला कोड या तरीका (5)

5. डेटा एन्क्रिप्ट करके डिक्रिप्शन के लिए पैसे मांगने वाला मैलवेयर (7)

6. ऐसा कनेक्शन, जिसमें भेजा गया डेटा बाहरी लोगों से सुरक्षित रहता है (8)

7. सिस्टम को नुकसान पहुंचाने या डेटा चुराने के लिए बना दुर्भावनापूर्ण सॉफ़्टवेयर (5)

ऊपर से नीचे

1. डेटा को कूट रूप में बदलना, ताकि सही कुंजी के बिना कोई उसे पढ़ न सके (4)

2. साइबर जोखिम प्रबंधित करने के लिए NIST जैसे संरचित दिशानिर्देश (4)

3. सुरक्षा नियमों के आधार पर ट्रैफ़िक छानने वाली नेटवर्क दीवार (5)

4. दो या अधिक प्रमाणीकरण कारकों की मांग करने वाला सुरक्षा सत्यापन (5)

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: सॉफ़्टवेयर की किसी कमज़ोरी का फ़ायदा उठाने वाला कोड या तरीका (5 अक्षर):

5 बाएँ से दाएँ: डेटा एन्क्रिप्ट करके डिक्रिप्शन के लिए पैसे मांगने वाला मैलवेयर (7 अक्षर):

6 बाएँ से दाएँ: ऐसा कनेक्शन, जिसमें भेजा गया डेटा बाहरी लोगों से सुरक्षित रहता है (8 अक्षर):

7 बाएँ से दाएँ: सिस्टम को नुकसान पहुंचाने या डेटा चुराने के लिए बना दुर्भावनापूर्ण सॉफ़्टवेयर (5 अक्षर):

ऊपर से नीचे

1 ऊपर से नीचे: डेटा को कूट रूप में बदलना, ताकि सही कुंजी के बिना कोई उसे पढ़ न सके (4 अक्षर):

2 ऊपर से नीचे: साइबर जोखिम प्रबंधित करने के लिए NIST जैसे संरचित दिशानिर्देश (4 अक्षर):

3 ऊपर से नीचे: सुरक्षा नियमों के आधार पर ट्रैफ़िक छानने वाली नेटवर्क दीवार (5 अक्षर):

4 ऊपर से नीचे: दो या अधिक प्रमाणीकरण कारकों की मांग करने वाला सुरक्षा सत्यापन (5 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।

द	प	ति	के	ट	मि	ट	ए	सा	य	च	ऊ	नी	जी	इ
त	ट	म	पे	ब	प	जि	न्क्रि	मै	मी	ने	ले	इ	सी	य
छ	इ	र	दे	कि	जा	सा	प्श	वा	ल	ड	रे	स	ख	नि
फ	प्लॉ	ढ	मा	ना	का	रे	न	दे	सि	वे	मी	क	पि	ता
ति	क्स	ज	श	भ	सु	ऊ	अ	ऊ	ए	रि	य	वि	म	श
य	ए	वि	व	वा	र	पा	रै	ल	च	से	कि	र	ल्टी	य
र्क	व	म	फ्रे	घ	क्षि	प	के	न	की	व	सि	री	फ़ै	त
ल	की	कि	सि	ना	त	ने	पा	ते	स	ण	ए	ता	क्ट	सा
वॉ	मी	न	नी	ऋ	ने	ले	घ	ति	जि	म	ला	ए	र	जी
र	ले	ड	ल	द	ट	जे	घ	के	च	से	वे	दे	री	ए
य	पी	उ	अ	जे	व	मि	घ	व	आ	च	मी	य	च	ट
फ़ा	थ	फ	ग	ना	र्क	सी	का	ज	फ	नी	जी	ता	र	ठ
से	लि	ट	आ	इ	से	रा	के	री	पा	वा	सि	य	नि	पि
ने	ख	के	वे	ऊ	ड	नी	दे	दि	भ	आ	नि	जे	वे	वे
ष	ण	प	कि	से	य	ह	ह	ते	रा	द	सा	सी	थ	जे

शब्दावली शब्द-सूची

एक्सप्लॉइट, रैनसमवेयर, फ्रेमवर्क, एन्क्रिप्शन, फ़ायरवॉल, मैलवेयर, मल्टीफ़ैक्टर, सुरक्षितनेटवर्क

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. एक्सप्लॉइट**
- **B. रैनसमवेयर**
- **C. फ्रेमवर्क**
- **D. एन्क्रिप्शन**
- **E. फ़ायरवॉल**
- **F. मैलवेयर**
- **G. मल्टीफ़ैक्टर**
- **H. सुरक्षितनेटवर्क**

परिभाषाएँ और मिलान फ़ील्ड

1. सुरक्षा नियमों के आधार पर ट्रैफ़िक छानने वाली नेटवर्क दीवार। ____
2. सिस्टम को नुकसान पहुंचाने या डेटा चुराने के लिए बना दुर्भावनापूर्ण सॉफ़्टवेयर। ____
3. सॉफ़्टवेयर की किसी कमज़ोरी का फ़ायदा उठाने वाला कोड या तरीका। ____
4. डेटा एन्क्रिप्ट करके डिक्रिप्शन के लिए पैसे मांगने वाला मैलवेयर। ____
5. दो या अधिक प्रमाणीकरण कारकों की मांग करने वाला सुरक्षा सत्यापन। ____
6. ऐसा कनेक्शन, जिसमें भेजा गया डेटा बाहरी लोगों से सुरक्षित रहता है। ____
7. साइबर जोखिम प्रबंधित करने के लिए NIST जैसे संरचित दिशानिर्देश। ____
8. डेटा को कूट रूप में बदलना, ताकि सही कुंजी के बिना कोई उसे पढ़ न सके। ____

चेकपॉइंट 7: उलझे शब्दों की चुनौती

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

1. इ प्लॉ ए ट क्स
2. फ्रे व र्क म
3. र फ़ा ल वॉ य
4. फ़ै र क्ट म ल्टी
5. वे र म स रै य न
6. प्शा न ए न्क्रि
7. य र मै वे ल
8. त र ने र्क सु व ट क्षि

अतिरिक्त गतिविधि: झटपट सोचें

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

1	साइबर सुरक्षा में नौकरियाँ			
2	सॉफ़्टवेयर अपडेट करने के कारण			
3	ऐसी चीज़ें जिन्हें फ़ायरवॉल ब्लॉक कर सकता है			
4	ईमेल में चेतावनी के संकेत			
5	ऐसी चीज़ें जिनका आप बैकअप लेते हैं			
6	साइबर हमलों के जाने-माने प्रकार			
7	ऐसी चीज़ें जिन्हें हनीपॉट लुभा सकता है			
8	ऐसी जानकारी जो आपको कभी साझा नहीं करनी चाहिए			
9	कंप्यूटर के संक्रमित होने के संकेत			
10	हैकर्स के बारे में फ़िल्में या शो			
11	सुरक्षा की वे परतें जो आप बना सकते हैं			
12	सुरक्षा ड्रिल में अभ्यास करने वाली चीज़ें			
13	आपके जाने-पहचाने सुरक्षा टूल			
14	IT मदद के लिए आप जिनसे पूछ सकते हैं			
15	'साइबर' से शुरू होने वाले शब्द			

चेकपॉइंट 8: साइबर सुरक्षा केस स्टडी

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

केस स्टडी 1: रैंसमवेयर रिकवरी रणनीति



परिदृश्य: एक कॉर्पोरेट नेटवर्क रैनसमवेयर से संक्रमित हो जाता है, जिससे महत्वपूर्ण डेटाबेस लॉक हो जाते हैं। हमलावर $100,000 की क्रिप्टोकरेंसी में भुगतान की माँग करते हैं। कंपनी के पास 24 घंटे पुराने ऑफ़लाइन बैकअप हैं।

चर्चा प्रश्न: भुगतान करने के जोखिमों का विश्लेषण करें, और रिकवरी रणनीति का मूल्यांकन करें।

केस स्टडी 2: क्रेडेंशियल स्टफ़िंग से बचाव



परिदृश्य: एक ऑनलाइन सेवा क्रेडेंशियल स्टफ़िंग हमले का सामना करती है, जिसमें हैकर अन्य साइटों से चुराए गए लाखों यूज़रनेम/पासवर्ड जोड़ों को आज़मा रहे हैं।

चर्चा प्रश्न: इस हमले की कार्यप्रणाली का विवरण दीजिए और दो रक्षा प्रणालियों की रूपरेखा बताइए।

चेकपॉइंट 9: कूट संदेश को डिकोड करें

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

अक्षर-से-संख्या एन्क्रिप्शन कुंजी

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

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

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

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

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

्=61

33	61	39	37	46	27	48	13	39	27		44	52		44	47	44	61	23	37

44	49	39	13	61	43	47	28		13	39	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 साइबर सुरक्षा FAQ (भाग A)

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

Q1: साइबर सुरक्षा का मुख्य उद्देश्य क्या है?

मुख्य उद्देश्य नेटवर्क, डिवाइस और डेटा को अनधिकृत एक्सेस, हमलों और आकस्मिक नुकसान से बचाना है।

Q2: फ़िशिंग स्पीयर फ़िशिंग से कैसे अलग है?

फ़िशिंग यादृच्छिक उपयोगकर्ताओं को निशाना बनाने वाला व्यापक ईमेल अभियान है, जबकि स्पीयर फ़िशिंग व्यक्तिगत डेटा के ज़रिए विशिष्ट व्यक्तियों को निशाना बनाती है।

Q3: नेटवर्क फ़ायरवॉल क्या है?

फ़ायरवॉल एक नेटवर्क सुरक्षा प्रणाली है जो पहले से तय सुरक्षा नियमों के आधार पर आने और जाने वाले ट्रैफ़िक की निगरानी और फ़िल्टरिंग करती है।

Q4: मल्टी-फ़ैक्टर ऑथेंटिकेशन (MFA) ज़रूरी क्यों है?

MFA रक्षा की एक अहम परत जोड़ता है, जो हमलावरों के प्राथमिक पासवर्ड क्रेडेंशियल चुराने या तोड़ लेने पर भी पहुँच को रोकता है।

Q5: कंप्यूटर वायरस की परिभाषा क्या है?

वायरस स्व-प्रतिकृति मैलवेयर है जो साफ़ फ़ाइलों से जुड़ जाता है और चलाए जाने पर सिस्टमों में फैलता है।

चेकपॉइंट 10: बुनियादी साइबर सुरक्षा FAQ (भाग B)

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

Q6: रैनसमवेयर लोकल डेटा को कैसे लॉक करता है?

रैनसमवेयर उपयोगकर्ता की फ़ाइलों को एन्क्रिप्ट करने के लिए क्रिप्टोग्राफ़िक एल्गोरिदम का उपयोग करता है, जिससे वे डिक्रिप्शन कुंजी लगाए जाने तक पढ़ी नहीं जा सकतीं।

Q7: ज़ीरो-डे कमज़ोरी क्या है?

ज़ीरो-डे सॉफ़्टवेयर में ऐसी सुरक्षा खामी है जिसकी जानकारी विक्रेता को नहीं होती, इसलिए एक्सप्लॉइट से पहले पैच बनाने का समय नहीं मिलता।

Q8: NIST फ़्रेमवर्क की क्या भूमिका है?

NIST फ़्रेमवर्क संगठनों को साइबर सुरक्षा जोखिम प्रबंधित और कम करने में मदद के लिए स्वैच्छिक दिशानिर्देश और मानक देता है।

Q9: सुरक्षा घटना प्रतिक्रिया योजना क्या है?

यह सुरक्षा उल्लंघनों और नेटवर्क समझौते का पता लगाने, उन्हें नियंत्रित करने और उनसे उबरने की दस्तावेज़ीकृत प्रक्रियाओं का समूह है।

Q10: सोशल इंजीनियरिंग उपयोगकर्ताओं का फ़ायदा कैसे उठाती है?

सोशल इंजीनियरिंग मनोवैज्ञानिक हेरफेर से कर्मचारियों को पासवर्ड बताने या दुर्भावनापूर्ण फ़ाइलें डाउनलोड करने के लिए बहकाती है।

चेकपॉइंट 10: उन्नत सुरक्षा FAQ (भाग C)

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

Q1: DDoS हमला वेब सर्वरों को कैसे अभिभूत करता है?

DDoS हमला लाखों संक्रमित बॉटनेट उपकरणों को समन्वित कर सर्वर पर ट्रैफ़िक की बाढ़ ला देता है, जिससे बैंडविड्थ और CPU की सीमाएँ समाप्त हो जाती हैं।

Q2: सममित और असममित एन्क्रिप्शन में क्या अंतर है?

सिमेट्रिक एन्क्रिप्शन एन्क्रिप्ट और डिक्रिप्ट करने के लिए एक ही कुंजी का उपयोग करता है, जबकि असिमेट्रिक एन्क्रिप्शन पब्लिक और प्राइवेट कुंजी जोड़े का उपयोग करता है।

Q3: हैकर SQL इंजेक्शन हमले कैसे करते हैं?

हमलावर फ़ॉर्म फ़ील्ड में दुर्भावनापूर्ण SQL कमांड डालकर बैकएंड डेटाबेस को धोखे से अनधिकृत उपयोगकर्ता रिकॉर्ड देने पर मजबूर करते हैं।

Q4: नेटवर्क घुसपैठ में लेटरल मूवमेंट क्या है?

यह वह तकनीक है जिसमें हमलावर सर्वर तक शुरुआती एक्सेस का फ़ायदा उठाकर आंतरिक नेटवर्क के अन्य जुड़े सिस्टम को समझौता करते हैं।

Q5: DNS स्पूफ़िंग वेब ट्रैफ़िक को कैसे भटकाती है?

DNS स्पूफ़िंग नेमसर्वर कैश रिकॉर्ड बदल देती है, जिससे वैध उपयोगकर्ता लक्षित डोमेन के बजाय दुर्भावनापूर्ण मिलते-जुलते वेबसाइटों पर पहुँच जाते हैं।

चेकपॉइंट 10: उन्नत सुरक्षा FAQ (भाग D)

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

Q6: हार्डवेयर सिक्योरिटी टोकन क्या है?

यह एक भौतिक डिवाइस (जैसे YubiKey) है जो क्रिप्टोग्राफ़िक प्रमाणीकरण प्रमाण बनाता है और दूरस्थ फ़िशिंग के विरुद्ध अधिकतम सुरक्षा देता है।

Q7: सुरक्षा टीमें डिकॉय हनीपॉट का उपयोग कैसे करती हैं?

टीमें शुरुआती चरण में घुसपैठ पकड़ने और अनधिकृत तत्वों के हमले के पैटर्न का विश्लेषण करने के लिए नॉन-प्रोडक्शन डिकॉय सर्वर तैनात करती हैं।

Q8: लीस्ट प्रिविलेज का सिद्धांत क्या है?

यह वह सुरक्षा मानक है जिसमें उपयोगकर्ता के एक्सेस अधिकार उनकी कार्य भूमिकाएँ निभाने के लिए ज़रूरी न्यूनतम तक सीमित किए जाते हैं।

Q9: मैन-इन-द-मिडल हमला कनेक्शन का दुरुपयोग कैसे करता है?

हमलावर बिना एन्क्रिप्शन वाले नेटवर्क पर दो उपकरणों के बीच संचार को बीच में रोकता और बदलता है, और सत्र टोकन तथा क्रेडेंशियल चुरा लेता है।

Q10: समझौते के संकेतक (IOC) क्या हैं?

IOC फ़ॉरेंसिक डेटा संकेत हैं, जैसे रजिस्ट्री में असामान्य बदलाव या संदिग्ध IP ट्रैफ़िक, जो दिखाते हैं कि सिस्टम में सेंध लगी थी।

भाग 11: 10 वास्तविक साइबर सुरक्षा तथ्य और अंतर्दृष्टियाँ

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

1. सुरक्षा इनसाइट

हमलावर लगातार इंटरनेट पर कमज़ोर सर्वरों को स्कैन करते रहते हैं और कर्मचारियों के इनबॉक्स में फ़िशिंग ईमेल भेजते हैं।

2. सुरक्षा इनसाइट

फ़िशिंग लिंक पर क्लिक करने जैसी मानवीय भूल डेटा ब्रीच का एक आम कारक है, इसीलिए प्रशिक्षण मायने रखता है।

3. सुरक्षा इनसाइट

डेटा उल्लंघन की लागत में कानूनी जुर्माने, ग्राहकों का छूटना, जाँच और मरम्मत शामिल हैं, और यह लाखों डॉलर तक पहुँच सकती है।

4. सुरक्षा इनसाइट

हार्डवेयर सिक्योरिटी कुंजियों जैसा फ़िशिंग-प्रतिरोधी MFA सबसे मज़बूत प्रकार का MFA है और वही मानक है जिसकी CISA सिफ़ारिश करता है। [2]

5. सुरक्षा इनसाइट

रैनसमवेयर एंटरप्राइज़ नेटवर्क के लिए एक बड़ा खतरा बना हुआ है, और CISA ऑफ़लाइन, एन्क्रिप्टेड बैकअप को एक प्रमुख बचाव के रूप में अपनाने का आग्रह करता है। [4]

6. सुरक्षा इनसाइट

NIST साइबर सुरक्षा फ़्रेमवर्क 2.0 (2024) के छह मुख्य कार्य हैं: Govern, Identify, Protect, Detect, Respond, Recover। [1]

7. सिक्योरिटी इनसाइट

क्रेडेंशियल स्टफ़िंग बॉट बैंकिंग और ई-कॉमर्स लॉगिन पोर्टलों पर लीक हुए यूज़रनेम और पासवर्ड जोड़ियों को बड़े पैमाने पर आज़माते हैं।

8. सिक्योरिटी इनसाइट

दुनिया भर में ज़ीरो-डे एक्सप्लॉइट बाज़ार मौजूद हैं, जहाँ उच्च-गंभीरता वाली कमज़ोरियाँ पैच होने से पहले बड़ी रकम में बिक सकती हैं।

9. सिक्योरिटी इनसाइट

हनीपॉट डिकॉय सिस्टम घुसपैठ के अलर्ट तुरंत देता है, क्योंकि वैध उपयोगकर्ताओं के पास उसे एक्सेस करने का कोई कारण नहीं होता।

10. सुरक्षा इनसाइट

Transport Layer Security (TLS) ब्राउज़र सत्रों को एन्क्रिप्ट करता है, जिससे सार्वजनिक Wi-Fi नेटवर्क पर पैकेट स्निफ़िंग रुकती है।

तकनीकी संदर्भ और स्रोत

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

शैक्षणिक और उद्योग संदर्भ

[1] 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

उत्तर कुंजी: चेकपॉइंट 1 – बहुविकल्पीय

1 फ़िशिंग हमले फ़िशिंग **सही उत्तर: A**

शिक्षण नोट

फ़िशिंग अभियान नकली ईमेल का उपयोग करके क्रेडेंशियल और संवेदनशील उपयोगकर्ता डेटा चुराने की कोशिश करते हैं। उद्धरण: OWASP Secure Configuration.

2 खाता सुरक्षा MFA कुंजी **सही उत्तर: A**

शिक्षण नोट

हार्डवेयर टोकन का उपयोग करने वाला मल्टी-फ़ैक्टर ऑथेंटिकेशन (MFA) खाता पहुँच की सबसे मज़बूत रक्षा देता है। संदर्भ: NIST Digital Identity।

3 रैनसमवेयर खतरा रैनसमवेयर **सही उत्तर: A**

शिक्षण नोट

रैनसमवेयर महत्वपूर्ण सिस्टम और डेटा को एन्क्रिप्ट कर देता है और डिक्रिप्शन कुंजियों के बदले क्रिप्टोकरेंसी में भुगतान माँगता है। स्रोत: Center for Internet Security (CIS)।

4 ज़ीरो-डे सुरक्षा कमज़ोरी ज़ीरो-डे **सही उत्तर: A**

शिक्षण नोट

ज़ीरो-डे खतरे अपैच्ड, अज्ञात सुरक्षा खामियों का फ़ायदा तब उठाते हैं जब तक विक्रेता का पैच उपलब्ध नहीं होता। उद्धरण: OWASP Secure Configuration।

5 सुरक्षा फ़्रेमवर्क फ़्रेमवर्क **सही उत्तर: A**

शिक्षण नोट

NIST जैसे फ़्रेमवर्क संगठनों को साइबर जोखिम प्रबंधित करने और कम करने में मदद के लिए संरचित दिशानिर्देश देते हैं। उद्धरण: NIST Digital Identity।

उत्तर कुंजी: चेकपॉइंट 2 – सही या गलत

6 **लक्षित फ़िशिंग** फ़िशिंग **सही उत्तर: गलत**

शिक्षण नोट

फ़िशिंग हमले एक्सप्लॉइट के रास्ते बढ़ाने के लिए कॉर्पोरेट नेटवर्क और व्यक्तिगत खातों, दोनों को निशाना बनाते हैं। उद्धरण: OWASP Secure Configuration.

7 **प्रश्न 7** **सही उत्तर: सही**

शिक्षण नोट

MFA दूसरा कारक माँगता है, इसलिए अकेला चोरी हुआ पासवर्ड आमतौर पर लॉग इन करने के लिए काफ़ी नहीं होता।

8 **ट्रैफ़िक फ़ायरवॉल** फ़ायरवॉल **सही उत्तर: सही**

शिक्षण नोट

फ़ायरवॉल विशिष्ट नेटवर्क पोर्ट पर ट्रैफ़िक की जाँच करके अनधिकृत कनेक्शनों को छानने के लिए उसे ब्लॉक करते हैं। उद्धरण: Center for Internet Security (CIS)।

9 **ज़ीरो-डे प्रतिक्रिया** ज़ीरो-डे **सही उत्तर: गलत**

शिक्षण नोट

ज़ीरो-डे खामियों को ठीक करने के लिए कोड पैच और WAF फ़िल्टरिंग चाहिए, क्योंकि उनके सिग्नेचर अभी मौजूद नहीं होते। उद्धरण: OWASP Secure Configuration।

10 **डिकॉय हनीपॉट** हनीपॉट **सही उत्तर: सही**

शिक्षण नोट

हनीपॉट भ्रामक सर्वर हैं जिनका उपयोग सुरक्षा टीमें दुर्भावनापूर्ण तत्वों को लुभाने, अलर्ट पाने और उनका अध्ययन करने के लिए करती हैं। उद्धरण: Center for Internet Security (CIS)।

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

D 1. रैनसमवेयर ख़तरा	G 2. मल्टी-फ़ैक्टर ऑथ	E 3. ज़ीरो-डे एक्सप्लॉइट	H 4. डिकॉय हनीपॉट
C 5. इंटूज़न फ़ायरवॉल	B 6. घटना प्रतिक्रिया	F 7. पासवर्ड स्वच्छता	A 8. सुरक्षा फ़्रेमवर्क

चेकपॉइंट 3: उत्तर – प्रमुख शब्द

1 फ़ायरवॉल	2 एक्सप्लॉइट	3 मल्टी-फ़ैक्टर	4 मैलवेयर
5 फ़्रेमवर्क	6 एन्क्रिप्शन		

चेकपॉइंट 6, वैकल्पिक: उत्तर – शब्द मिलान

1 E – फ़ायरवॉल	2 F – मैलवेयर	3 A – एक्सप्लॉइट	4 B – रैनसमवेयर
5 G – मल्टीफ़ैक्टर	6 H – सुरक्षितनेटवर्क	7 C – फ़्रेमवर्क	8 D – एन्क्रिप्शन

शिक्षकों के लिए चर्चा नोट

प्रमुख शब्द:
जाँचें कि क्या विद्यार्थी रैनसमवेयर ख़तरा, मल्टी-फ़ैक्टर ऑथ और ज़ीरो-डे एक्सप्लॉइट 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।

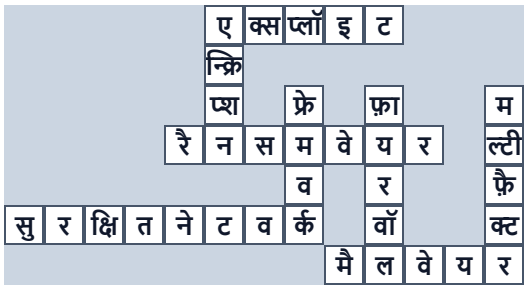
स्रोतों का मूल्यांकन:
विद्यार्थियों से वर्कशीट के स्रोतों में कम से कम एक कथन की पुष्टि करवाएँ और चर्चा करें कि आँकड़े, कीमतें और नियम समय के साथ क्यों बदल सकते हैं।

पहेलियों की कुंजियाँ और शिक्षक नोट

शब्द खोज समाधान

द	प	ति	के	ट	मि	ट	ए	सा	य	च	ऊ	नी	जी	इ
त	ट	म	पे	ब	प	जि	क्रि	मै	मी	ने	ले	इ	सी	य
छ	इ	र	दे	कि	जा	सा	प्श	वा	ल	ड	रे	स	ख	नि
फ	प्लॉ	ढ	मा	ना	का	रे	न	दे	सि	वे	मी	क	पि	ता
ति	क्स	ज	श	भ	सु	ऊ	अ	ऊ	ए	रि	य	वि	म	श
य	ए	वि	व	वा	र	पा	रै	ल	च	से	कि	र	ल्टी	य
र्क	व	म	फ्रे	घ	क्षि	प	के	न	की	व	सि	री	फ़ै	त
ल	की	कि	सि	ना	त	ने	पा	ते	स	ण	ए	ता	क्ट	सा
वॉ	मी	न	नी	ऋ	ने	ले	घ	ति	जि	म	ला	ए	र	जी
र	ले	ड	ल	द	ट	जे	घ	के	च	से	वे	दे	री	ए
य	पी	उ	अ	जे	व	मि	घ	व	आ	च	मी	य	च	ट
फ़ा	थ	फ	ग	ना	र्क	सी	का	ज	फ	नी	जी	ता	र	ठ
से	लि	ट	आ	इ	से	रा	के	री	पा	वा	सि	य	नि	पि
ने	ख	के	वे	ऊ	ड	नी	दे	दि	भ	आ	नि	जे	वे	वे
ष	ण	प	कि	से	य	ह	ह	ते	रा	द	सा	सी	थ	जे

क्रॉसवर्ड समाधान



क्रॉसवर्ड समाधान के लिए शिक्षक गाइड

बाएँ से दाएँ

1 बाएँ से दाएँ: एक्सप्लॉइट सॉफ़्टवेयर की किसी कमज़ोरी का फ़ायदा उठाने वाला कोड या तरीका (5 अक्षर)

5 बाएँ से दाएँ: रैनसमवेयर डेटा एन्क्रिप्ट करके डिक्रिप्शन के लिए पैसे मांगने वाला मैलवेयर (7 अक्षर)

6 बाएँ से दाएँ: सुरक्षितनेटवर्क ऐसा कनेक्शन, जिसमें भेजा गया डेटा बाहरी लोगों से सुरक्षित रहता है (8 अक्षर)

7 बाएँ से दाएँ: मैलवेयर सिस्टम को नुकसान पहुंचाने या डेटा चुराने के लिए बना दुर्भावनापूर्ण सॉफ़्टवेयर (5 अक्षर)

ऊपर से नीचे

1 ऊपर से नीचे: एन्क्रिप्शन डेटा को कूट रूप में बदलना, ताकि सही कुंजी के बिना कोई उसे पढ़ न सके (4 अक्षर)

2 ऊपर से नीचे: फ्रेमवर्क साइबर जोखिम प्रबंधित करने के लिए NIST जैसे संरचित दिशानिर्देश (4 अक्षर)

3 ऊपर से नीचे: फ़ायरवॉल सुरक्षा नियमों के आधार पर ट्रैफ़िक छानने वाली नेटवर्क दीवार (5 अक्षर)

4 ऊपर से नीचे: मल्टीफ़ैक्टर दो या अधिक प्रमाणीकरण कारकों की मांग करने वाला सुरक्षा सत्यापन (5 अक्षर)

अक्षर-फेर शब्द और कूट संदेश हल कुंजी

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

शब्द अनस्क्रैम्बल कुंजी

1. इप्लॉएटक्स — **एक्सप्लॉइट**
2. फ्रेवर्कम — **फ्रेमवर्क**
3. रफ़ालवॉय — **फ़ायरवॉल**
4. फ़ैरक्टमल्टी — **मल्टीफ़ैक्टर**
5. वेरमसरैयन — **रैनसमवेयर**
6. प्शनएन्क्रि — **एन्क्रिप्शन**
7. यरमैवेल — **मैलवेयर**
8. तरनेर्कसुवटक्षि — **सुरक्षितनेटवर्क**

गुप्त कूट चुनौती कुंजी

"प्रमाणीकरण से सिस्टम सुरक्षित करें"

केस स्टडी के उत्तर

A केस स्टडी 1: रैंसमवेयर रिकवरी रणनीति

शिक्षक समाधान

ग्रेडिंग दिशानिर्देश

छात्रों के उत्तरों में निम्नलिखित बिंदु शामिल होने चाहिए:

- परिदृश्य विश्लेषण: एक कॉर्पोरेट नेटवर्क रैनसमवेयर से संक्रमित है, जिसने ज़रूरी डेटाबेस लॉक कर दिए हैं। हमलावर $100,000 की क्रिप्टोकरेंसी की माँग कर रहे हैं। कंपनी के पास 24 घंटे पुराने ऑफ़लाइन बैकअप हैं।
- अनुशंसित रणनीति और समाधान: भुगतान के जोखिम: भुगतान करने से फ़ाइलों के डिक्रिप्ट होने की गारंटी नहीं मिलती, कंपनी भुगतान करने वाला निशाना मानी जाने लगती है, और अपराधी गतिविधि को धन मिलता है। रिकवरी रणनीति: टीम को संक्रमित होस्ट अलग करने, प्रभावित सर्वर वाइप करने और ऑफ़लाइन बैकअप से डेटा रिस्टोर करना चाहिए। तुरंत दोबारा संक्रमण रोकने के लिए उन्हें शुरुआती पहुँच का रास्ता (फ़िशिंग या एक्सप्लॉइट) पैच करना होगा।

B केस स्टडी 2: क्रेडेंशियल स्टफ़िंग से बचाव

शिक्षक समाधान

ग्रेडिंग दिशानिर्देश

छात्रों के उत्तरों में निम्नलिखित बिंदु शामिल होने चाहिए:

- परिदृश्य विश्लेषण: एक ऑनलाइन सेवा पर क्रेडेंशियल स्टफ़िंग हमला होता है, जिसमें हैकर दूसरी साइटों से चुराए गए लाखों यूज़रनेम/पासवर्ड जोड़ों को आज़माते हैं।
- अनुशंसित रणनीति और समाधान: कार्यप्रणाली: हमलावर कई साइटों पर पासवर्ड के दोबारा उपयोग का फ़ायदा उठाकर स्वचालित बॉट से उपयोगकर्ताओं के अकाउंट में लॉग इन करते हैं। बचाव: 1. मल्टी-फ़ैक्टर ऑथेंटिकेशन (MFA) पासवर्ड सही होने पर भी लॉगिन प्रयासों को रोकता है। 2. रेट-लिमिटिंग और CAPTCHA लगाने से लॉगिन एंडपॉइंट पर स्पैम करने वाला स्वचालित बॉट ट्रैफ़िक ब्लॉक होता है।