नाम: _____ दिनांक: _____ अंक: _____

रैनसमवेयर हमले और व्यवसाय रिकवरी

पेलोड निष्पादन, क्रिप्टोग्राफ़िक फ़ाइल एन्क्रिप्शन, ऑफ़लाइन बैकअप, नियंत्रण प्रक्रियाएँ और आपदा रिकवरी।

रैनसमवेयर हमले सीखने की रूपरेखा

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 रैंसमवेयर हमलों और बिज़नेस रिकवरी से परिचित कराता है। आप पेलोड निष्पादन, फ़ाइल एन्क्रिप्शन, ऑफ़लाइन बैकअप, खतरा नियंत्रण, क्रिप्टोकरेंसी भुगतान और डिज़ास्टर रिकवरी योजनाओं 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/ransomware-hamla/

आपका रैनसमवेयर रिकवरी लर्निंग रोडमैप

- Trojan, रैनसमवेयर और स्पाइवेयर पेलोड में अंतर करें।
- सुरक्षित सैंडबॉक्स परिवेशों में दुर्भावनापूर्ण फ़ाइलों का विश्लेषण करें।
- नेटवर्क को तेज़ी से अलग करने और नियंत्रित करने की प्रक्रियाएँ तैयार करें।

रैनसमवेयर हमले गाइड 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 रैनसमवेयर रिकवरी पर लागू करें। अंत में अतिरिक्त गतिविधि झटपट सोचें पूरी करें।

रैनसमवेयर हमले और डिज़ास्टर रिकवरी (परिचय)

रैनसमवेयर पेलोड सिस्टम स्टोरेज को क्रिप्टोग्राफ़िक रूप से लॉक कर देते हैं और डिक्रिप्शन कुंजियों के बदले क्रिप्टोकरेंसी में भुगतान माँगते हैं। इस खतरे को कम करने के लिए नेटवर्क आइसोलेशन नियम, सैंडबॉक्स में मैलवेयर विश्लेषण और मज़बूत एयर-गैप्ड कोल्ड बैकअप शामिल हैं।

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

चेकपॉइंट 1: बहुविकल्पीय चुनौती

1 **1. रैनसमवेयर हमले की मुख्य कार्यप्रणाली क्या है?**

- A. सिस्टम पहुँच रोकने के लिए उपयोगकर्ता फ़ाइलों का क्रिप्टोग्राफ़िक एन्क्रिप्शन
- B. फ़ॉर्म फ़ील्ड में दुर्भावनापूर्ण SQL कमांड डालना
- C. सार्वजनिक Wi-Fi कनेक्शन पर नेटवर्क पैकेट स्निफ़ करना
- D. SPF सत्यापन को बायपास करने के लिए ईमेल हेडर जाली बनाना

2 **2. ऑफ़लाइन (कोल्ड) बैकअप क्या है?**

- A. नेटवर्क से अलग किया गया स्टोरेज कॉपी, ताकि वह मैलवेयर के फैलाव से सुरक्षित रहे
- B. प्राथमिक वेब सर्वर की हार्ड ड्राइव पर रखा गया बैकअप
- C. सिस्टम रजिस्ट्री लॉग का अस्थायी कैश
- D. उपयोगकर्ता पासवर्ड रीसेट करने के लिए उपयोग किया जाने वाला प्रशासनिक टूल

3 **3. रैनसमवेयर हमले के दौरान सुरक्षा टीमों को संक्रमित सिस्टम कैसे अलग करने चाहिए?**

- A. नेटवर्क केबल तुरंत निकाल दें और वायरलेस इंटरफ़ेस बंद कर दें
- B. एंटीवायरस सिग्नेचर डेटाबेस अपग्रेड करें
- C. प्राथमिक DNS सर्वर बंद कर दें
- D. समझौता हुई फ़ाइलों के एक्सटेंशन का नाम बदलें

4 **4. सुरक्षा एजेंसियाँ रैनसमवेयर की माँग पूरी न करने की सलाह क्यों देती हैं?**

- A. धन देने से हमलावरों को प्रोत्साहन मिलता है और डिक्रिप्शन कुंजी मिलने की गारंटी नहीं होती
- B. यह सभी कॉर्पोरेट बीमा पॉलिसियों को अपने आप अमान्य कर देता है
- C. यह हर ग्राहक को अपने-आप ईमेल से सूचित करता है
- D. यह बचे हुए सिस्टम बैकअप फ़ाइलों को भ्रष्ट कर देता है

5 **5. डिज़ास्टर रिकवरी प्लान (DRP) क्या है?**

- A. सिस्टम के समझौते के बाद संचालन और डेटा को बहाल करने की संरचित प्रक्रिया
- B. इनबाउंड नेटवर्क पोर्ट को मैप करने वाला फ़ायरवॉल कॉन्फ़िगरेशन
- C. उपयोगकर्ता प्रशासनिक विशेषाधिकारों की सूची वाला डेटाबेस स्कीमा
- D. स्पूफ़ किए गए डोमेन को अस्वीकार करने वाला ईमेल प्रमाणीकरण प्रोटोकॉल

चेकपॉइंट 2: सही या गलत चुनौती

6 प्रश्न 6

6. रैनसमवेयर पेलोड नेटवर्क से जुड़े ऑनलाइन बैकअप तक आसानी से फैल सकते हैं।

- ◯ सही
- ◯ गलत

7 प्रश्न 7

7. क्रिप्टोकरेंसी में फिरौती देने से फ़ाइलों के सफलतापूर्वक डिक्रिप्ट होने की गारंटी मिलती है।

- ◯ सही
- ◯ गलत

8 प्रश्न 8

8. संक्रमित सिस्टमों को नेटवर्क से अलग करने से रैनसमवेयर को आस-पास के सिस्टमों में फैलने से रोकने में मदद मिलती है।

- ◯ सही
- ◯ गलत

9 प्रश्न 9

9. रैंसमवेयर सिस्टम स्टोरेज को एन्क्रिप्ट करने के लिए सिमेट्रिक क्रिप्टोग्राफ़ी का कभी उपयोग नहीं करता।

- ◯ सही
- ◯ गलत

10 प्रश्न 10

10. डेटा रिस्टोरेशन प्रक्रियाओं का नियमित परीक्षण आपदा रिकवरी का एक अहम हिस्सा 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. स्थानीय फ़ाइलों तक पहुँच रोकने में क्रिप्टोग्राफ़िक _____ का उपयोग होता है।
2. फ़ाइलें एन्क्रिप्ट करके फिरौती माँगने वाला साइबर _____ पूरे संगठन को ठप कर सकता है।
3. नेटवर्क से कटी हुई ऑफ़साइट स्टोरेज प्रतियाँ एक सुरक्षित _____ हैं।
4. मैलवेयर को फैलने से रोकने के लिए एंडपॉइंट नेटवर्क _____ ज़रूरी है।
5. फ़ाइलों को बंद करके उन्हें छुड़ाने के बदले पैसे माँगने वाला दुर्भावनापूर्ण प्रोग्राम _____ कहलाता है।
6. परिचालन डेटा फ़ाइलों की बहाली आपदा _____ कहलाती है।

शब्दावली शब्द-बैंक

आइसोलेशन · एन्क्रिप्शन · कोल्ड बैकअप · ट्रोजन · पेलोड · फ़ाइल लॉकर · रिकवरी · रैनसमवेयर हमला

अपने उत्तर यहाँ लिखें:

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

चेकपॉइंट 4: सुरक्षा अवधारणा मिलान

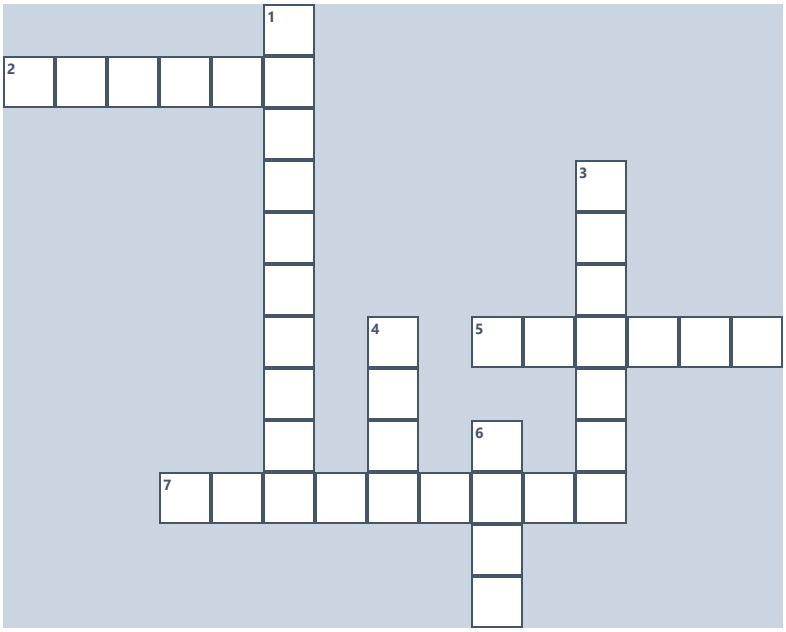
परिभाषा मिलान

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. एन्क्रिप्शन**	**A**	संक्रमित नेटवर्क सिस्टमों को डिस्कनेक्ट करना।
☐	**2. पेलोड**	**B**	साफ़ दिखने का भेष धरे दुर्भावनापूर्ण फ़ाइल।
☐	**3. कोल्ड बैकअप**	**C**	फ़ाइलों को क्रिप्टोग्राफ़िक रूप से लॉक करना।
☐	**4. आइसोलेशन**	**D**	बड़ी सिस्टम रुकावट की घटना।
☐	**5. फिरौती**	**E**	दुर्भावनापूर्ण सॉफ़्टवेयर चलाना।
☐	**6. रिकवरी**	**F**	डिस्कनेक्ट की गई ऑफ़लाइन प्रतिलिपि।
☐	**7. आपदा**	**G**	बैकअप से डेटाबेस रिस्टोर करना।
☐	**8. ट्रोजन**	**H**	क्रिप्टोग्राफ़िक कुंजी भुगतान अनुरोध।

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

2. संक्रमित नेटवर्क सिस्टम को अलग करना। (6)

5. नेटवर्क से कटी हुई ऑफ़लाइन प्रति। (6)

7. इंटरनेट से अलग रखी डेटा की प्रति, जो हमले से अछूती रहती है। (9)

ऊपर से नीचे

1. फ़ाइलें लॉक करके पैसे माँगने वाला साइबर अपराध। (10)

3. डेटा की इंटरनेट-आधारित सर्वर पर रखी सुरक्षित प्रति। (7)

4. फ़ाइलों को क्रिप्टोग्राफ़िक रूप से लॉक करना। (4)

6. बैकअप से डेटाबेस बहाल करना। (4)

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

2 बाएँ से दाएँ: संक्रमित नेटवर्क सिस्टम को अलग करना। (6 अक्षर):

5 बाएँ से दाएँ: नेटवर्क से कटी हुई ऑफ़लाइन प्रति। (6 अक्षर):

7 बाएँ से दाएँ: इंटरनेट से अलग रखी डेटा की प्रति, जो हमले से अछूती रहती है। (9 अक्षर):

ऊपर से नीचे

1 ऊपर से नीचे: फ़ाइलें लॉक करके पैसे माँगने वाला साइबर अपराध। (10 अक्षर):

3 ऊपर से नीचे: डेटा की इंटरनेट-आधारित सर्वर पर रखी सुरक्षित प्रति। (7 अक्षर):

4 ऊपर से नीचे: फ़ाइलों को क्रिप्टोग्राफ़िक रूप से लॉक करना। (4 अक्षर):

6 ऊपर से नीचे: बैकअप से डेटाबेस बहाल करना। (4 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।

ड रे र स ख नि फ आ ढ मा ना का रे दे सि
मी क क पि ता ति ज इ क्ला श भ ऊ अ ऊ ए
रि वि लॉ श य वि व सो वा उ पा ल च से कि
प य ल घ प के की ले व सि ड री त की कि
अ सि इ ना ने रै पा श ते ण ए बै ता सा मी
क न फ़ा नी ऋ न ले न घ ति जि ला क ए जी
बै ले ड ल द स जे घ को के री च से अ दे
न री ए पी उ म अ जे ल्ड मि घ व व आ प
इ च मी च ट वे थ फ बै ग ना सी क का ज
ला फ नी जी ता य ठ से क लि ट आ इ रि से
फ़ रा के री पा र वा सि अ य न नि पि ने ख
ऑ के वे ऊ ड ह नी दे प प्श दि भ आ नि जे
वे वे ष ण प म कि से न्क्रि य ह ह ते रा द
सा सी थ जे इ ला मे ए ला ढ पे ऋ वे नी वे
उ थ ह जे त य मी रे मि दि ए ह जे जा ढ

शब्दावली शब्द-सूची

एन्क्रिप्शन रैनसमवेयरहमला कोल्डबैकअप आइसोलेशन फ़ाइललॉकर रिकवरी क्लाउडबैकअप ऑफ़लाइनबैकअप

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. एन्क्रिप्शन**
- **B. रैनसमवेयरहमला**
- **C. कोल्डबैकअप**
- **D. आइसोलेशन**
- **E. फ़ाइललॉकर**
- **F. रिकवरी**
- **G. क्लाउडबैकअप**
- **H. ऑफ़लाइनबैकअप**

परिभाषाएँ और मिलान फ़ील्ड

1. नेटवर्क से कटी हुई ऑफ़लाइन प्रति।
2. इंटरनेट से अलग रखी डेटा की प्रति, जो हमले से अछूती रहती है।
3. फ़ाइलों को क्रिप्टोग्राफ़िक रूप से लॉक करना।
4. फ़ाइलों को बंद करके पैसे की माँग करने वाला दुर्भावनापूर्ण प्रोग्राम।
5. संक्रमित नेटवर्क सिस्टम को अलग करना।
6. डेटा की इंटरनेट-आधारित सर्वर पर रखी सुरक्षित प्रति।
7. फ़ाइलें लॉक करके पैसे माँगने वाला साइबर अपराध।
8. बैकअप से डेटाबेस बहाल करना।

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. **प्श ए न क्रि** _____

2. **प को बै अ क ल्ड** _____

3. **फ़ा ल लॉ र क इ** _____

4. **प उ क बै अ क्ला ड** _____

5. **ह य ला न म र वे रै म स** _____

6. **श ले आ सो न इ** _____

7. **व रि री क** _____

8. **प न अ ऑ इ फ़ बै क ला** _____

अतिरिक्त गतिविधि: झटपट सोचें

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

1	ऐसी जानकारी जो आपको कभी साझा नहीं करनी चाहिए			
2	ऐसे डिवाइस जिन्हें हैक किया जा सकता है			
3	फिरौती न देने के कारण			
4	सुरक्षित आदतें जो आप आज से शुरू कर सकते हैं			
5	आपके जाने-पहचाने सुरक्षा टूल			
6	अपने अकाउंट सुरक्षित रखने के तरीके			
7	कंप्यूटर के संक्रमित होने के संकेत			
8	बैकअप रखने की जगहें			
9	ऐसी फ़ाइलें जिन्हें आप कभी खोना नहीं चाहते			
10	रैनसमवेयर के फैलने के तरीके			
11	हमले के पहले घंटे में की जाने वाली चीज़ें			
12	हमले के दौरान संपर्क करने वाले लोग			
13	ऐसी चीज़ें जिन्हें रैनसमवेयर लॉक कर सकता है			
14	साइबर सुरक्षा से जुड़े शब्द			
15	ऐसे संगठन जिन्हें अक्सर निशाना बनाया जाता है			

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: एंटरप्राइज़ रैंसमवेयर पेलोड की रोकथाम



परिदृश्य: एक कॉर्पोरेट लोकल एरिया नेटवर्क में सक्रिय रैंसमवेयर घुस गया है। मुख्य फ़ाइल सर्वरों पर फ़ाइल एक्सटेंशन .locked दिखने लगे हैं।

चर्चा प्रश्न: रोकथाम के चरणों का विवरण दीजिए और डेटा रिकवरी प्रोटोकॉल की रूपरेखा बताइए।

केस स्टडी 2: ऑफ़लाइन बैकअप आर्किटेक्चर का मूल्यांकन



परिदृश्य: एक उद्यम ऐसी डेटा बैकअप रणनीति डिज़ाइन करना चाहता है जो बैकअप के कंप्रोमाइज़ होने का जोखिम घटाए, भले ही प्राथमिक लोकल नेटवर्क रैनसमवेयर द्वारा पूरी तरह हाइजैक हो जाए।

चर्चा प्रश्न: एक सुरक्षित ऑफ़लाइन बैकअप स्टोरेज वॉल्ट सिस्टम तैयार करें।

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

13	54	40	61	25		35	53	13	1	33		44	52		25	52	23	46

35	45	46	40		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: रैंसमवेयर क्या है?

रैनसमवेयर एक दुर्भावनापूर्ण सॉफ़्टवेयर है, जिसे कंप्यूटर सिस्टम या फ़ाइलों तक पहुँच तब तक रोकने के लिए बनाया गया है जब तक फिरौती की रकम न चुका दी जाए।

Q2: रैंसमवेयर कैसे फैलता है?

ईमेल फ़िशिंग अटैचमेंट, बिना पैच किए सॉफ़्टवेयर की कमज़ोरियों और समझौता किए गए रिमोट एक्सेस सिस्टम के ज़रिए। [1]

Q3: भुगतान क्रिप्टोकरेंसी में क्यों माँगा जाता है?

Bitcoin जैसी क्रिप्टोकरेंसी सापेक्ष गुमनामी देती हैं, जिससे कानून प्रवर्तन के लिए धन को ट्रैक करना कठिन हो जाता है।

Q4: क्या एंटीवायरस रैनसमवेयर को ब्लॉक करता है?

हाँ, लेकिन सिग्नेचर-आधारित एंटीवायरस नए बनाए गए ज़ीरो-डे रैनसमवेयर पेलोड के विरुद्ध विफल हो सकता है।

Q5: एयर-गैप्ड बैकअप क्या है?

ऐसी बैकअप कॉपी जिसका प्राथमिक नेटवर्क से कोई भौतिक या तार्किक कनेक्शन नहीं होता, जिससे वह फैलाव से सुरक्षित रहती है।

चेकपॉइंट 10: बुनियादी साइबर सुरक्षा FAQ (भाग B)

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

Q6: डबल एक्सटॉर्शन क्या है?

जब हमलावर न केवल फ़ाइलें एन्क्रिप्ट करते हैं बल्कि संवेदनशील डेटा भी चुरा लेते हैं, ताकि भुगतान न होने पर सार्वजनिक रूप से लीक करने की धमकी दे सकें।

Q7: डिक्रिप्टर क्या है?

सॉफ़्टवेयर उपयोगिता जिसमें लॉक की गई फ़ाइलों को वापस सादे पाठ में लाने के लिए आवश्यक क्रिप्टोग्राफ़िक कुंजी होती है।

Q8: आप रैनसमवेयर का शुरुआती दौर में पता कैसे लगाते हैं?

अचानक बड़े पैमाने पर फ़ाइल संशोधन और नाम बदलने की गतिविधि के लिए फ़ाइल सिस्टम की निगरानी करके।

Q9: बीमा की क्या भूमिका है?

साइबर बीमा रिकवरी लागत को कवर करने में मदद कर सकता है, लेकिन कवरेज की शर्तें और फिरौती भुगतान के नियम पॉलिसी के अनुसार अलग-अलग होते हैं।

Q10: क्या मुझे संक्रमित सिस्टम को रीबूट करना चाहिए?

नहीं, रीबूट करने से वोलेटाइल मेमोरी के सबूत नष्ट हो सकते हैं; इसके बजाय उसे नेटवर्क से अलग कर दें। [1]

चेकपॉइंट 10: उन्नत सुरक्षा FAQ (भाग C)

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

Q1: रैंसमवेयर असममित एन्क्रिप्शन का उपयोग कैसे करता है?

यह फ़ाइलों को एन्क्रिप्ट करने के लिए मैलवेयर में अंतर्निहित सार्वजनिक कुंजी का उपयोग करता है, और उन्हें डिक्रिप्ट करने के लिए हमलावर की निजी कुंजी चाहिए।

Q2: सिमेट्रिक एन्क्रिप्शन का भी उपयोग क्यों किया जाता है?

सिमेट्रिक एन्क्रिप्शन (जैसे AES) तेज़ है और विशाल डेटाबेस को मिनटों में लॉक कर सकता है, जबकि असिमेट्रिक कुंजियाँ AES कुंजी को सुरक्षित करती हैं।

Q3: लॉजिकल सेग्मेंटेशन क्या है?

नेटवर्क को अलग-थलग ज़ोन में बाँटना, जिससे मैलवेयर वर्कस्टेशन नोड से कोर सर्वरों तक पार्श्व रूप से नहीं फैल पाता।

Q4: WORM स्टोरेज क्या है?

राइट-वन्स, रीड-मेनी मीडिया, जो रैनसमवेयर पेलोड द्वारा बैकअप डेटा को संपादित, ओवरराइट या हटाए जाने से रोकता है।

Q5: शैडो कॉपी क्या हैं?

Windows द्वारा बनाए गए स्थानीय बैकअप स्नैपशॉट; रैंसमवेयर आमतौर पर एडमिनिस्ट्रेटिव टूल से सबसे पहले इन्हें हटा देता है।

चेकपॉइंट 10: उन्नत सुरक्षा FAQ (भाग D)

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

Q6: क्रेडेंशियल चोरी रैनसमवेयर को कैसे संभव बनाती है?

हमलावर लीक हुए एडमिन लॉगिन खरीदकर रिमोट डेस्कटॉप से साइन इन करते हैं और पूरे नेटवर्क में मैन्युअल रूप से रैनसमवेयर चलाते हैं।

Q7: ड्राई-रन रिस्टोरेशन टेस्टिंग क्या है?

बैकअप डेटाबेस को नियमित रूप से अलग टेस्ट एनवायरनमेंट में रिस्टोर करना, ताकि सत्यापित हो कि रिस्टोरेशन की गति और डेटा की अखंडता आपदा मानकों पर खरी उतरती है।

Q8: एंडपॉइंट डिटेक्शन (EDR) रैनसमवेयर को कैसे रोकता है?

प्रक्रिया व्यवहार (जैसे तेज़ एन्क्रिप्शन) का विश्लेषण करके और संदिग्ध ऐप्लिकेशन को तुरंत निलंबित करके।

Q9: रैनसमवेयर-एज़-ए-सर्विस (RaaS) मॉडल क्या है?

फ़्रैंचाइज़ी मॉडल जिसमें मैलवेयर डेवलपर भुगतान के प्रतिशत के बदले सहयोगियों को रैंसमवेयर बिल्डर किराये पर देते हैं।

Q10: बिना पैच वाला RDP रैंसमवेयर को कैसे ट्रिगर करता है?

खुले, बिना पैच वाले Remote Desktop Protocol गेटवे हमलावरों को लॉगिन पर ब्रूट-फ़ोर्स करने और मैलवेयर हाथ से चलाने की अनुमति देते हैं।

भाग 11: 10 वास्तविक साइबर सुरक्षा तथ्य और अंतर्दृष्टियाँ

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

1. सुरक्षा इनसाइट

रैनसमवेयर तत्व अक्सर Windows शैडो कॉपी हटाने और लोकल रिस्टोर रोकने के लिए vssadmin.exe जैसे टूल का उपयोग करते हैं। [1]

2. सुरक्षा इनसाइट

सिमेट्रिक AES-256 कुंजियाँ आमतौर पर फ़ाइल पेलोड को एन्क्रिप्ट करने में उपयोग होती हैं, जिन्हें फिर पब्लिक RSA कुंजियों से लॉक किया जाता है।

3. सुरक्षा इनसाइट

सफल रैनसमवेयर हमले से उबरने में हफ़्ते लग सकते हैं, इसीलिए परखे हुए ऑफ़लाइन बैकअप मायने रखते हैं।

4. सुरक्षा इनसाइट

FBI फिरौती देने का समर्थन नहीं करता और चेतावनी देता है कि भुगतान करने से आपका डेटा वापस मिलने की गारंटी नहीं होती। [2]

5. सुरक्षा इनसाइट

आपदा पुनर्प्राप्ति योजनाओं (DRP) में रिकवरी टाइम ऑब्जेक्टिव (RTO) और रिकवरी पॉइंट ऑब्जेक्टिव (RPO) तय होने चाहिए।

6. सुरक्षा इनसाइट

FBI ऐसे बैकअप की सलाह देता है जो एन्क्रिप्टेड और इम्यूटेबल हों, यानी जिन्हें बदला या मिटाया न जा सके। [3]

7. सिक्योरिटी इनसाइट

रैनसमवेयर डेवलपर पारंपरिक सिग्नेचर-आधारित एंटीवायरस स्कैनर को बायपास करने के लिए उन्नत ऑब्फ़स्केशन तकनीकों का उपयोग करते हैं।

8. सिक्योरिटी इनसाइट

नेटवर्क सेगमेंटेशन पार्श्व गति को सीमित करता है, जिससे रैंसमवेयर को पहले संक्रमित होस्ट से आगे फैलने से रोकने में मदद मिलती है। [3]

9. सिक्योरिटी इनसाइट

Remote Desktop Protocol (RDP) जैसी खुली, कमज़ोर ढंग से सुरक्षित रिमोट सेवाएँ रैनसमवेयर के प्रवेश का आम रास्ता हैं। [1]

10. सुरक्षा इनसाइट

CISA सलाह देता है कि एन्क्रिप्टेड बैकअप को ऑफ़लाइन रखें, क्योंकि कई रैंसमवेयर वेरिएंट पहुँच में आने वाले बैकअप को खोजकर मिटा देते हैं। [1]

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

[2] FBI Internet Crime Complaint Center. (n.d.). Ransomware.
https://www.ic3.gov/CrimeInfo/Ransomware

[3] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.
https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

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

[5] 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

उत्तर कुंजी: चेकपॉइंट 1 – बहुविकल्पीय

1 प्रश्न 1 सही उत्तर: A

शिक्षण नोट

रैनसमवेयर हमले की मुख्य कार्यप्रणाली क्या है? → सिस्टम पहुँच रोकने के लिए उपयोगकर्ता फ़ाइलों का क्रिप्टोग्राफ़िक एन्क्रिप्शन

2 प्रश्न 2 सही उत्तर: A

शिक्षण नोट

ऑफ़लाइन (कोल्ड) बैकअप क्या है? → नेटवर्क से अलग किया गया स्टोरेज कॉपी, ताकि वह मैलवेयर के फैलाव से सुरक्षित रहे

3 प्रश्न 3 सही उत्तर: A

शिक्षण नोट

रैनसमवेयर हमले के दौरान सुरक्षा टीमों को संक्रमित सिस्टम कैसे अलग करने चाहिए? → नेटवर्क केबल तुरंत निकाल दें और वायरलेस इंटरफ़ेस बंद कर दें

4 प्रश्न 4 सही उत्तर: A

शिक्षण नोट

सुरक्षा एजेंसियाँ रैनसमवेयर की माँग पूरी न करने की सलाह क्यों देती हैं? → धन देने से हमलावरों को प्रोत्साहन मिलता है और डिक्रिप्शन कुंजी मिलने की गारंटी नहीं होती

5 प्रश्न 5 सही उत्तर: A

शिक्षण नोट

डिज़ास्टर रिकवरी प्लान (DRP) क्या है? → सिस्टम के समझौते के बाद संचालन और डेटा को बहाल करने की संरचित प्रक्रिया

उत्तर कुंजी: चेकपॉइंट 2 – सही या गलत

6 **प्रश्न 6** — सही उत्तर: सही

शिक्षण नोट

रैनसमवेयर पेलोड नेटवर्क से जुड़े ऑनलाइन बैकअप तक आसानी से फैल सकते हैं।

7 **प्रश्न 7** — सही उत्तर: गलत

शिक्षण नोट

गलत: FBI चेतावनी देता है कि भुगतान करने से कोई डेटा वापस मिलने की गारंटी नहीं होती।

8 **प्रश्न 8** — सही उत्तर: सही

शिक्षण नोट

सही: CISA फैलाव रोकने के लिए संक्रमित होस्ट को अनप्लग करने या नेटवर्क को ऑफ़लाइन करने की सलाह देता है।

9 **प्रश्न 9** — सही उत्तर: गलत

शिक्षण नोट

गलत: रैनसमवेयर आमतौर पर AES जैसे तेज़ सिमेट्रिक सिफ़र से फ़ाइलें एन्क्रिप्ट करता है।

10 **प्रश्न 10** — सही उत्तर: सही

शिक्षण नोट

डेटा रिस्टोरेशन प्रक्रियाओं का नियमित परीक्षण आपदा रिकवरी का एक अहम हिस्सा है।

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

C 1. एन्क्रिप्शन	E 2. पेलोड	F 3. कोल्ड बैकअप	A 4. आइसोलेशन
H 5. फिरौती	G 6. रिकवरी	D 7. आपदा	B 8. ट्रोजन

चेकपॉइंट 3: उत्तर – प्रमुख शब्द

1 एन्क्रिप्शन	2 रैनसमवेयर हमला	3 कोल्ड बैकअप	4 आइसोलेशन
5 फ़ाइल लॉकर	6 रिकवरी		

चेकपॉइंट 6, वैकल्पिक: उत्तर – शब्द मिलान

1 C – कोल्डबैकअप	2 H – ऑफ़लाइनबैकअप	3 A – एन्क्रिप्शन	4 E – फ़ाइललॉकर
5 D – आइसोलेशन	6 G – क्लाउडबैकअप	7 B – रैनसमवेयरहमला	8 F – रिकवरी

शिक्षकों के लिए चर्चा नोट

प्रमुख शब्द:
जाँचें कि क्या विद्यार्थी एन्क्रिप्शन, पेलोड और कोल्ड बैकअप 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।

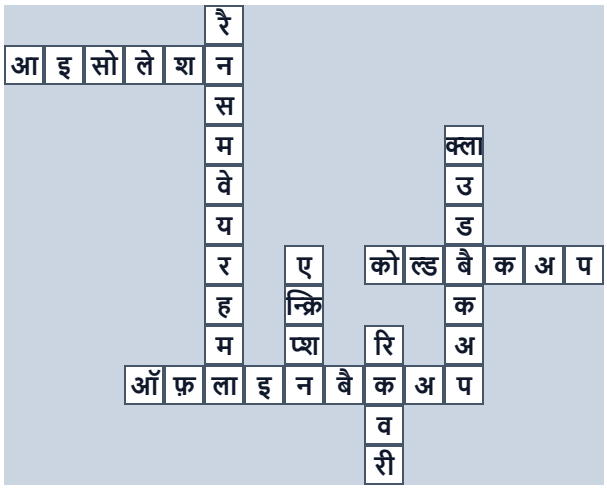
स्रोतों का मूल्यांकन:
विद्यार्थियों से वर्कशीट के स्रोतों में कम से कम एक कथन की पुष्टि करवाएँ और चर्चा करें कि आँकड़े, कीमतें और नियम समय के साथ क्यों बदल सकते हैं।

पहेलियों की कुंजियाँ और शिक्षक नोट

शब्द खोज समाधान

ड	रे	र	स	ख	नि	फ	आ	ढ	मा	ना	का	रे	दे	सि
मी	क	क	पि	ता	ति	ज	इ	क्ला	श	भ	ऊ	अ	ऊ	ए
रि	वि	लॉ	श	य	वि	व	सो	वा	उ	पा	ल	च	से	कि
प	य	ल	घ	प	के	की	ले	व	सि	ड	री	त	की	कि
अ	सि	इ	ना	ने	रै	पा	श	ते	ण	ए	बै	ता	सा	मी
क	न	फ़ा	नी	ऋ	न	ले	न	घ	ति	जि	ला	क	ए	जी
बै	ले	ड	ल	द	स	जे	घ	को	के	री	च	से	अ	दे
न	री	ए	पी	उ	म	अ	जे	ल्ड	मि	घ	व	व	आ	प
इ	च	मी	च	ट	वे	थ	फ	बै	ग	ना	सी	क	का	ज
ला	फ	नी	जी	ता	य	ठ	से	क	लि	ट	आ	इ	रि	से
फ़	रा	के	री	पा	र	वा	सि	अ	य	न	नि	पि	ने	ख
ऑ	के	वे	ऊ	ड	ह	नी	दे	प	प्श	दि	भ	आ	नि	जे
वे	वे	ष	ण	प	म	कि	से	न्क्रि	य	ह	ह	ते	रा	द
सा	सी	थ	जे	इ	ला	मे	ए	ला	ढ	पे	ऋ	वे	नी	वे
उ	थ	ह	जे	त	य	मी	रे	मि	दि	ए	ह	जे	जा	ढ

क्रॉसवर्ड समाधान



क्रॉसवर्ड समाधान के लिए शिक्षक गाइड

बाएँ से दाएँ

2 बाएँ से दाएँ: आइसोलेशन संक्रमित नेटवर्क सिस्टम को अलग करना। (6 अक्षर)

5 बाएँ से दाएँ: कोल्डबैकअप नेटवर्क से कटी हुई ऑफ़लाइन प्रति। (6 अक्षर)

7 बाएँ से दाएँ: ऑफ़लाइनबैकअप इंटरनेट से अलग रखी डेटा की प्रति, जो हमले से अछूती रहती है। (9 अक्षर)

ऊपर से नीचे

1 ऊपर से नीचे: रैनसमवेयरहमला फ़ाइलें लॉक करके पैसे माँगने वाला साइबर अपराध। (10 अक्षर)

3 ऊपर से नीचे: क्लाउडबैकअप डेटा की इंटरनेट-आधारित सर्वर पर रखी सुरक्षित प्रति। (7 अक्षर)

4 ऊपर से नीचे: एन्क्रिप्शन फ़ाइलों को क्रिप्टोग्राफ़िक रूप से लॉक करना। (4 अक्षर)

6 ऊपर से नीचे: रिकवरी बैकअप से डेटाबेस बहाल करना। (4 अक्षर)

अक्षर-फेर शब्द और कूट संदेश हल कुंजी

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

शब्द अनस्क्रैम्बल कुंजी

1. प्शएनक्रि → **एन्क्रिप्शन**
2. पकोबैअकल्ड → **कोल्डबैकअप**
3. फ़ालॉरकइ → **फ़ाइललॉकर**
4. पउकबैअक्लाड → **क्लाउडबैकअप**
5. हयलानमरवेरैमस → **रैनसमवेयरहमला**
6. शलेआसोनइ → **आइसोलेशन**
7. वरिरीक → **रिकवरी**
8. पनअऑइफ़बैकला → **ऑफ़लाइनबैकअप**

गुप्त कूट चुनौती कुंजी

"कोल्ड बैकअप से डेटा बहाल करें"

केस स्टडी के उत्तर

A केस स्टडी 1: एंटरप्राइज़ रैंसमवेयर पेलोड की रोकथाम

शिक्षक समाधान

ग्रेडिंग दिशानिर्देश

छात्रों के उत्तरों में निम्नलिखित बिंदु शामिल होने चाहिए:

- परिदृश्य विश्लेषण: एक कॉर्पोरेट लोकल एरिया नेटवर्क में सक्रिय रैनसमवेयर घुस गया है। मुख्य फ़ाइल सर्वर पर फ़ाइल एक्सटेंशन .locked दिखने लगे हैं।
- अनुशंसित रणनीति और समाधान: सभी प्रभावित सर्वरों को लोकल एरिया नेटवर्क से अलग करें। सक्रिय प्रशासनिक सेशन समाप्त करें। सुरक्षित, राइट-लॉक्ड ऑफ़लाइन बैकअप सिस्टम से बिना छेड़छाड़ वाली फ़ाइलें रिस्टोर करें।

B केस स्टडी 2: ऑफ़लाइन बैकअप आर्किटेक्चर का मूल्यांकन

शिक्षक समाधान

ग्रेडिंग दिशानिर्देश

छात्रों के उत्तरों में निम्नलिखित बिंदु शामिल होने चाहिए:

- परिदृश्य विश्लेषण: एक एंटरप्राइज़ ऐसी डेटा बैकअप रणनीति बनाना चाहता है जो प्राथमिक स्थानीय नेटवर्क पर रैंसमवेयर का पूरा कब्ज़ा हो जाने पर भी बैकअप के प्रभावित होने का जोखिम घटाए।
- अनुशंसित रणनीति और समाधान: राइट-वन्स-रीड-मेनी (WORM) स्टोरेज लागू करें। बैकअप सिस्टम को सभी नेटवर्क से अलग करके तार्किक एयर-गैप बनाएँ, और रोज़ फ़िज़िकल मीडिया बदलना अनिवार्य करें।