नाम: _____ दिनांक: _____ अंक: _____

मैलवेयर विश्लेषण और खतरा न्यूनीकरण गाइड

ट्रोजन, रैनसमवेयर, स्पाइवेयर, रूटकिट, वर्चुअलाइज़ेशन सैंडबॉक्स, कंटेनमेंट

मैलवेयर विश्लेषण: 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 मैलवेयर विश्लेषण और रोकथाम से परिचित कराता है। आप स्पाइवेयर, ट्रोजन, रैंसमवेयर पेलोड, रिवर्स-इंजीनियरिंग टूल, रूटकिट व्यवहार और नियंत्रण रणनीतियों 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/malware/

आपका मैलवेयर शमन लर्निंग रोडमैप

- Trojan, वर्म और रूटकिट मैलवेयर प्रकारों में अंतर करें।
- कोड विश्लेषण के लिए सैंडबॉक्स वर्चुअलाइज़ेशन निष्पादन लागू करें।
- सक्रिय रैनसमवेयर पेलोड के लिए रोकथाम और सैनिटाइज़ेशन योजनाएँ तैयार करें।

मैलवेयर विश्लेषण 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 मैलवेयर शमन पर लागू करें। अंत में अतिरिक्त गतिविधि झटपट सोचें पूरी करें।

मैलवेयर विश्लेषण और खतरा नियंत्रण (परिचय)

ट्रोजन, वर्म और रैंसमवेयर जैसे दुर्भावनापूर्ण कोड एंडपॉइंट और सर्वर के लिए गंभीर खतरे हैं। सुरक्षा टीमें मैलवेयर का विश्लेषण वर्चुअल सैंडबॉक्स में करती हैं और पेलोड का प्रसार रोकने के लिए तेज़ी से नेटवर्क आइसोलेशन नियंत्रण लागू करती हैं।

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

चेकपॉइंट 1: बहुविकल्पीय चुनौती

1 **1. ट्रोजन हॉर्स की परिभाषित विशेषता क्या है?**

- A. यह वैध सॉफ़्टवेयर का रूप धरकर उपयोगकर्ताओं को उसे चलाने के लिए बहकाता है
- B. यह स्थानीय नेटवर्क लाइनों पर अपने आप फैलता है
- C. यह अलग-थलग वर्चुअल सैंडबॉक्स के अंदर की फ़ाइलों को संक्रमित करता है
- D. यह इंटरनेट सेवा प्रदाता के ट्रैफ़िक को इंटरसेप्ट करता है

2 **2. किस प्रकार का मैलवेयर फ़ाइलें एन्क्रिप्ट करता है और भुगतान माँगता है?**

- A. रैंसमवेयर
- B. स्पाइवेयर
- C. रूटकिट
- D. एडवेयर

3 **3. स्पाइवेयर क्या दर्शाता है?**

- A. ऐसा मैलवेयर जो उपयोगकर्ता की कीस्ट्रोक और ब्राउज़र गतिविधियों की गुप्त निगरानी के लिए बनाया गया हो
- B. सैंडबॉक्स वाले वर्चुअल कंटेनर के भीतर चलने वाला प्रोग्राम कोड
- C. डेटाबेस रजिस्ट्री से डाउनलोड किए गए एंटी-मैलवेयर अपडेट
- D. स्क्रीन की चमक का स्वचालित समायोजन

4 **4. मैलवेयर डेवलपर रूटकिट का उपयोग क्यों करते हैं?**

- A. सक्रिय प्रक्रियाओं और दुर्भावनापूर्ण फ़ाइलों को ऑपरेटिंग सिस्टम से छिपाना
- B. एंडपॉइंट पर CPU प्रोसेसिंग गति बढ़ाना
- C. डेटाबेस फ़ाइलों का बैकअप सुरक्षित क्लाउड वॉल्ट में लेने के लिए
- D. लैपटॉप की बैटरी लाइफ़ सुधारने के लिए

5 **5. मैलवेयर विश्लेषण में सैंडबॉक्सिंग का क्या अर्थ है?**

- A. संदिग्ध फ़ाइलों को अलग वर्चुअल वॉल्ट में चलाकर उनका व्यवहार सुरक्षित रूप से देखना
- B. फ़ाइल हैश को ज्ञात खतरों के डेटाबेस से मिलाकर स्कैन करना
- C. घुसपैठ के बाद डेटाबेस बैकअप बहाल करना
- D. स्थानीय नेटवर्क राउटरों को सार्वजनिक लाइनों से अलग करना

चेकपॉइंट 2: सही या गलत चुनौती

6 प्रश्न 6

6. कंप्यूटर वर्म को स्थानीय नेटवर्क पर फैलने के लिए मानव उपयोगकर्ता की भागीदारी की आवश्यकता होती है।

○ सही ○ गलत

7 प्रश्न 7

7. एडवेयर हमेशा हानिरहित होता है और उपयोगकर्ता के व्यवहार या ब्राउज़र इतिहास को ट्रैक नहीं करता।

○ सही ○ गलत

8 प्रश्न 8

8. साफ़ ऑफ़लाइन बैकअप बहाल करने से पीड़ित फिरौती दिए बिना एन्क्रिप्टेड फ़ाइलें वापस पा सकते हैं।

○ सही ○ गलत

9 प्रश्न 9

9. सिग्नेचर-आधारित एंटीवायरस ज़ीरो-डे मैलवेयर को, उसका कोई सिग्नेचर बनने से पहले ही, भरोसेमंद तरीके से रोक देता है।

○ सही ○ गलत

10 प्रश्न 10

10. फ़ाइललेस मैलवेयर सिस्टम मेमोरी में दुर्भावनापूर्ण स्क्रिप्ट चलाता है और डिस्क पर फ़ाइलें लिखने से बचता 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. खुद की प्रतिलिपि बनाकर एक फ़ाइल से दूसरी फ़ाइल में फैलने वाला हानिकारक कोड _____ कहलाता है।

2. पैसे के लिए डेटाबेस सिस्टम को लॉक करने वाले दुर्भावनापूर्ण पेलोड _____ हैं।

3. पासवर्ड को चुपके से दर्ज करने वाले कीलॉगर _____ के उदाहरण हैं।

4. ऑपरेटिंग सिस्टम कर्नेल की गहराई में छिपने के लिए _____ चाहिए।

5. किसी फ़ाइल से जुड़े बिना नेटवर्क पर खुद फैल जाने वाला प्रोग्राम _____ कहलाता है।

6. सक्रिय मैलवेयर पेलोड को फैलने से रोकने के लिए तुरंत नेटवर्क _____ ज़रूरी है।

शब्दावली शब्द-बैंक

कंटेनमेंट | कंप्यूटर वर्म | ट्रोजन | फ़ाइललेस | रूटकिट | रैनसमवेयर | वायरस | स्पाइवेयर

अपने उत्तर यहाँ लिखें:

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

चेकपॉइंट 4: सुरक्षा अवधारणा मिलान

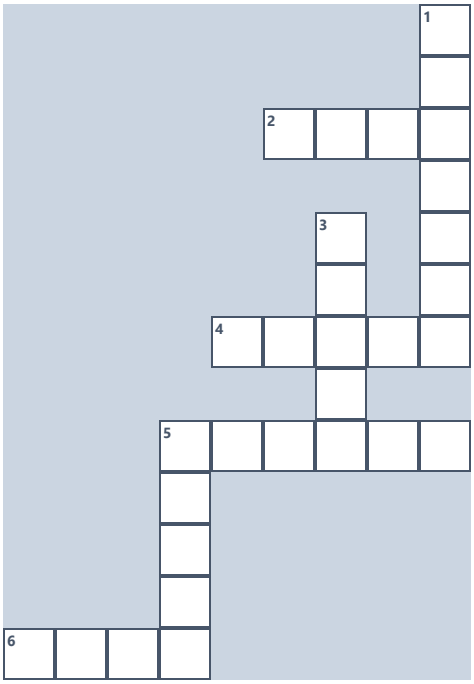
परिभाषा मिलान

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. ट्रोजन**	**A**	उपयोगकर्ता की गतिविधि और इनपुट को चुपके से मॉनिटर और रिकॉर्ड करने के लिए बना प्रोग्राम।
☐	**2. रैनसमवेयर**	**B**	डिस्क स्कैनर की नज़र से बचने के लिए सीधे RAM में चलने वाला मैलवेयर।
☐	**3. स्पाइवेयर**	**C**	खतरे के पेलोड को फैलने से रोकने के लिए संक्रमित एंडपॉइंट को सीमित करना।
☐	**4. रूटकिट**	**D**	हानिरहित या उपयोगी यूटिलिटी प्रोग्राम का भेष धरे दुर्भावनापूर्ण सॉफ़्टवेयर।
☐	**5. सैंडबॉक्स**	**E**	स्व-प्रतिकृति करने वाला मैलवेयर, जो मानवीय कार्रवाई के बिना नेटवर्क में फैलता है।
☐	**6. रोकथाम**	**F**	सिस्टम स्टोरेज को एन्क्रिप्ट करके कुंजी देने के बदले भुगतान माँगने वाला मैलवेयर।
☐	**7. वर्म**	**G**	दुर्भावनापूर्ण फ़ाइलों का सुरक्षित विश्लेषण करने के लिए उपयोग किया जाने वाला अलग-थलग वर्चुअल परिवेश।
☐	**8. फ़ाइललेस**	**H**	सिस्टम कर्नेल की गहराई में छिपा स्टील्थ मैलवेयर, जो प्रशासनिक नियंत्रण बनाए रखता है।

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. खुद की प्रतिलिपि बनाकर फैलने वाला हानिकारक कोड (4)

4. कंप्यूटर को चलाने वाले प्रोग्राम (5)

5. खुद को नेटवर्क पर फैलाने वाला दुर्भावनापूर्ण कीड़ा (6)

6. सिस्टम में गहराई से छिपकर रहने वाला प्रोग्राम (4)

ऊपर से नीचे

1. फ़ाइलें बंद करके फिरौती माँगने वाला प्रोग्राम (7)

3. चुपके से आपकी गतिविधि जासूसी करने वाला प्रोग्राम (5)

5. संक्रमण को आगे फैलने से रोकने की कार्रवाई (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

2 बाएँ से दाएँ: खुद की प्रतिलिपि बनाकर फैलने वाला हानिकारक कोड (4 अक्षर):

4 बाएँ से दाएँ: कंप्यूटर को चलाने वाले प्रोग्राम (5 अक्षर):

5 बाएँ से दाएँ: खुद को नेटवर्क पर फैलाने वाला दुर्भावनापूर्ण कीड़ा (6 अक्षर):

6 बाएँ से दाएँ: सिस्टम में गहराई से छिपकर रहने वाला प्रोग्राम (4 अक्षर):

ऊपर से नीचे

1 ऊपर से नीचे: फ़ाइलें बंद करके फिरौती माँगने वाला प्रोग्राम (7 अक्षर):

3 ऊपर से नीचे: चुपके से आपकी गतिविधि जासूसी करने वाला प्रोग्राम (5 अक्षर):

5 ऊपर से नीचे: संक्रमण को आगे फैलने से रोकने की कार्रवाई (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।

सा	स	ई	ते	घ	इ	नी	ल	रि	द	जे	घ	छ	ई	के
द	र	प	ति	के	ट	मि	ट	मै	सा	य	च	ऊ	नी	जी
इ	य	त	म	पे	ब	प	जि	मी	ल	ने	ले	इ	सी	य
छ	वे	र	दे	कि	जा	सा	वा	ड	रे	वे	स	ख	नि	फ
ढ	इ	मा	ना	का	रै	रे	दे	सि	मी	क	य	पि	रू	ता
ति	स्पा	ज	श	भ	न	ऊ	कं	अ	ऊ	ए	रि	र	ट	वि
स	र	य	वा	श	स	य	वि	प्यू	व	वा	पा	ल	कि	च
ट	से	कि	य	घ	म	प	के	की	ट	व	सि	री	ट	त
में	की	कि	सि	ना	वे	ने	पा	ते	ण	र	ए	ता	सा	मी
न	न	नी	ऋ	ले	य	घ	ति	जि	ला	ए	व	जी	ले	ड
टे	ल	द	जे	घ	र	के	च	से	दे	री	ए	र्म	पी	सॉ
कं	उ	अ	जे	मि	घ	व	आ	च	मी	च	ट	थ	फ़्ट	फ
ग	ना	सी	का	ज	फ	नी	जी	ता	ठ	से	लि	वे	ट	आ
इ	से	रा	के	री	पा	वा	सि	य	नि	पि	य	ने	ख	के
वे	ऊ	ड	नी	दे	दि	भ	आ	नि	जे	र	वे	वे	ष	ण

शब्दावली शब्द-सूची

रैनसमवेयर स्पाइवेयर रूटकिट कंटेनमेंट कंप्यूटरवर्म वायरस मैलवेयर सॉफ़्टवेयर

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. रैनसमवेयर**
- **B. स्पाइवेयर**
- **C. रूटकिट**
- **D. कंटेनमेंट**
- **E. कंप्यूटरवर्म**
- **F. वायरस**
- **G. मैलवेयर**
- **H. सॉफ़्टवेयर**

परिभाषाएँ और मिलान फ़ील्ड

1. संक्रमण को आगे फैलने से रोकने की कार्रवाई।
2. खुद की प्रतिलिपि बनाकर फैलने वाला हानिकारक कोड।
3. कंप्यूटर को चलाने वाले प्रोग्राम।
4. कंप्यूटर को नुकसान पहुँचाने वाला हर प्रकार का दुर्भावनापूर्ण सॉफ़्टवेयर।
5. चुपके से आपकी गतिविधि जासूसी करने वाला प्रोग्राम।
6. सिस्टम में गहराई से छिपकर रहने वाला प्रोग्राम।
7. फ़ाइलें बंद करके फिरौती माँगने वाला प्रोग्राम।
8. खुद को नेटवर्क पर फैलाने वाला दुर्भावनापूर्ण कीड़ा।

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. मयरैवेरसन
2. रूकिटट
3. कंटरर्मवप्यू
4. वेरयमैल
5. वेरस्पायइ
6. मेंकंनटटे
7. रवासय
8. रसॉवेयफ़्ट

अतिरिक्त गतिविधि: झटपट सोचें

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

1	सुरक्षित ऐप डाउनलोड करने की जगहें			
2	ऐसे डिवाइस जिन्हें हैक किया जा सकता है			
3	ऐसी चीज़ें जिनका आप बैकअप लेते हैं			
4	ईमेल में चेतावनी के संकेत			
5	फ़ोन में मैलवेयर होने के संकेत			
6	आपके जाने-पहचाने मैलवेयर के प्रकार			
7	ऐसे फ़ाइल प्रकार जिनसे सावधान रहना चाहिए			
8	मैलवेयर के पीसी में पहुँचने के तरीके			
9	सुरक्षित आदतें जो आप आज से शुरू कर सकते हैं			
10	साइबर सुरक्षा से जुड़े शब्द			
11	डेटा लीक के बाद की जाने वाली चीज़ें			
12	सॉफ़्टवेयर अपडेट करने के कारण			
13	मैलवेयर जैसे नामों वाले जानवर या किरदार			
14	ऐसी चीज़ें जिन्हें मैलवेयर चुरा सकता है			
15	गलत लिंक पर क्लिक हो जाने पर आप जो करेंगे			

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। नियंत्रण नीतियाँ स्थापित करें।

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

केस स्टडी 2: फ़ाइललेस मैलवेयर मेमोरी इंजेक्शन



परिदृश्य: एक विश्लेषक पाता है कि मानक प्रशासनिक टूल का उपयोग करके संदिग्ध स्क्रिप्टिंग पैटर्न सीधे वोलेटाइल सिस्टम RAM में चल रहे हैं, लेकिन डिस्क पर कोई दुर्भावनापूर्ण फ़ाइल नहीं है।

चर्चा प्रश्न: मेमोरी विश्लेषण रणनीति समझाइए और फ़ाइललेस एक्ज़ीक्यूशन को ब्लॉक करने वाले टूल 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

41	61	38	41	45	46	39		37	56	32	47	23	39		44	52

33	52	40	54	25		33	45	18	46	32	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: मैलवेयर क्या है?

खतरा पैदा करने वालों द्वारा बनाया गया दुर्भावनापूर्ण सॉफ़्टवेयर, जो डिवाइस और नेटवर्क को नुकसान पहुँचाने, हाइजैक करने या उनसे डेटा चुराने के लिए बना है।

Q2: वायरस और वर्म में क्या अंतर है?

वायरस को फैलने के लिए मानवीय क्रिया (जैसे फ़ाइल खोलना) चाहिए, जबकि वर्म नेटवर्कों में अपने-आप फैलता है।

Q3: ट्रोजन हॉर्स कंप्यूटर को कैसे संक्रमित करता है?

यह किसी हानिरहित या सुरक्षित प्रोग्राम का रूप धरकर उपयोगकर्ताओं को धोखा देता है और अपना दुर्भावनापूर्ण पेलोड भीतर छिपा लेता है।

Q4: रैनसमवेयर क्या है?

मैलवेयर का प्रकार जो लक्षित सिस्टम की फ़ाइलों को एन्क्रिप्ट करता है और डिक्रिप्शन कुंजी के बदले आर्थिक भुगतान की माँग करता है। [1]

Q5: स्पाइवेयर क्या है?

दुर्भावनापूर्ण सॉफ़्टवेयर, जो चुपचाप उपयोगकर्ता की कीस्ट्रोक, पासवर्ड और ब्राउज़िंग की आदतें रिकॉर्ड करके हमलावरों को भेज देता है।

चेकपॉइंट 10: बुनियादी साइबर सुरक्षा FAQ (भाग B)

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

Q6: सैंडबॉक्सिंग का क्या अर्थ है?

संदिग्ध फ़ाइलों को सुरक्षित, अलग वर्चुअल एनवायरनमेंट में चलाना, ताकि प्रोडक्शन सिस्टम को जोखिम दिए बिना उनके व्यवहार को देखा जा सके।

Q7: फ़ाइललेस मैलवेयर क्या है?

ऐसा मैलवेयर जो वैध यूटिलिटी का इस्तेमाल करके सीधे सिस्टम मेमोरी (RAM) में चलता है और बुनियादी स्कैनर से बचने के लिए डिस्क पर फ़ाइलें नहीं लिखता।

Q8: रूटकिट मैलवेयर की सुरक्षा कैसे करता है?

यह दुर्भावनापूर्ण प्रोसेस और फ़ाइलें छिपाता है, अक्सर ऑपरेटिंग सिस्टम कर्नेल को बदलकर, इसलिए एंटीवायरस स्कैनर उन्हें चूक सकते हैं।

Q9: डायनामिक बिहेवियर मॉनिटरिंग क्या है?

ऐसी एंटीवायरस स्कैनिंग जो चल रही प्रक्रियाओं की रीयल टाइम में निगरानी करती है, ताकि मैलवेयर जैसी गतिविधियाँ, जैसे बड़ी संख्या में फ़ाइलों का एन्क्रिप्शन, ब्लॉक की जा सकें।

Q10: घटना प्रतिक्रिया के दौरान नियंत्रण करना तत्काल क्यों ज़रूरी है?

समझौता किए गए एंडपॉइंट को अलग करने से सक्रिय मैलवेयर पेलोड अन्य नेटवर्क डिवाइस में फैलने से रुकते हैं।

चेकपॉइंट 10: उन्नत सुरक्षा FAQ (भाग C)

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

Q1: मैलवेयर डेवलपर सिग्नेचर-आधारित एंटीवायरस स्कैनर को कैसे बायपास करते हैं?

वे बहुरूपता (पॉलिमॉर्फिज़्म) का उपयोग करते हैं, यानी हर संक्रमण पर फ़ाइल का हैश और कोड संरचना बदल देते हैं, जबकि दुर्भावनापूर्ण व्यवहार वही रहता है।

Q2: मैलवेयर अभियानों में दोहरे-उपयोग वाले टूल का क्या जोखिम है?

हमलावर सामान्य नेटवर्क ट्रैफ़िक में घुल-मिल जाने के लिए वैध प्रशासनिक टूल (जैसे PowerShell या Sysinternals) का उपयोग करते हैं, जिससे पहचान मुश्किल हो जाती है।

Q3: प्रोसेस हॉलोइंग दुर्भावनापूर्ण पेलोड को कैसे चलाता है?

यह किसी वैध सिस्टम प्रोसेस को निलंबित अवस्था में शुरू करता है, उसके मेमोरी कोड को मैलवेयर से बदल देता है और निष्पादन फिर से शुरू कर देता है।

Q4: कमांड एंड कंट्रोल (C2) सर्वर की क्या भूमिका है?

हैकरों द्वारा चलाया जाने वाला रिमोट सर्वर, जो संक्रमित मशीनों पर चल रहे मैलवेयर को निर्देश और पेलोड भेजता है।

Q5: कीलॉगिंग का पता लगाना कठिन क्यों है?

बुनियादी कीलॉगर बहुत कम CPU संसाधन खाते हैं और अपनी प्रक्रियाओं को वैध यूज़र-स्पेस यूटिलिटी के भीतर छिपा लेते हैं।

चेकपॉइंट 10: उन्नत सुरक्षा FAQ (भाग D)

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

Q6: कोड ऑब्फ़स्केशन मैलवेयर विश्लेषण में देरी कैसे करता है?

यह सोर्स कोड को एन्क्रिप्ट या दोबारा व्यवस्थित करता है, जिससे वह विश्लेषक उपकरणों और सुरक्षा स्कैनर के लिए अपठनीय हो जाता है।

Q7: बूटकिट का कार्य क्या है?

रूटकिट जो बूट प्रक्रिया (MBR, बूट सेक्टर या UEFI फ़र्मवेयर) को संक्रमित करता है, इसलिए वह ऑपरेटिंग सिस्टम लोड होने से पहले चलता है।

Q8: हेयूरिस्टिक स्कैनिंग ज़ीरो-डे खतरों की पहचान कैसे करती है?

यह मिलते-जुलते डेटाबेस हैश की तलाश के बजाय संदिग्ध कोड पैटर्न और प्रशासनिक कमांड के लिए स्कैन करता है।

Q9: DLL हाइजैकिंग का खतरा क्या है?

किसी वैध एप्लिकेशन को उसकी डायरेक्टरी पाथ में रखकर दुर्भावनापूर्ण डायनामिक लिंक लाइब्रेरी (DLL) लोड करने के लिए मजबूर करना।

Q10: स्वचालित मैलवेयर विश्लेषण पाइपलाइन वर्चुअलाइज़ेशन का उपयोग कैसे करती हैं?

वे संदिग्ध फ़ाइलों को कई OS वर्चुअल मशीनों में चलाते हैं और व्यवहार लॉग तथा नेटवर्क PCAP फ़ाइलें अपने-आप बनाते 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

ट्रोजन हॉर्स संक्रमण का आम तरीका बने हुए हैं क्योंकि वे दुर्भावनापूर्ण कोड को ऐसे प्रोग्रामों के भीतर छिपाते हैं जो हानिरहित दिखते हैं।

2. सुरक्षा इनसाइट

FBI के IC3 को 2025 में रैनसमवेयर की 3,600 से अधिक शिकायतें मिलीं, जिनमें बताया गया नुकसान 32 मिलियन डॉलर से अधिक रहा। [3]

3. सुरक्षा इनसाइट

वर्म बिना पैच किए प्रोटोकॉल कमज़ोरियों का फ़ायदा उठाकर नेटवर्क पर तेज़ी से फैल सकते हैं, जैसे SMB में EternalBlue।

4. सुरक्षा इनसाइट

फ़ाइललेस मैलवेयर का पता लगाना कठिन होता है क्योंकि वह वैध टूल के ज़रिए मेमोरी में चलता है और डिस्क पर बहुत कम निशान छोड़ता है।

5. सुरक्षा इनसाइट

विश्लेषण सैंडबॉक्स आमतौर पर हर रन के बाद साफ़ स्नैपशॉट पर लौट जाते हैं, ताकि हर परीक्षण ज्ञात स्थिति से शुरू हो।

6. सुरक्षा इनसाइट

रूटकिट कर्नेल सिस्टम कॉल बदल सकते हैं और एंटी-मैलवेयर स्कैनर को झूठे डायग्नोस्टिक नतीजे दे सकते हैं।

7. सिक्योरिटी इनसाइट

कोड ऑब्फ़स्केशन पैकर यूटिलिटी का उपयोग करके मैलवेयर की वास्तविक बाइनरी पेलोड संरचना को संपीड़ित और छिपाता है।

8. सिक्योरिटी इनसाइट

पॉलिमॉर्फ़िक मैलवेयर सिग्नेचर जाँच से बचने के लिए हर नई प्रति के साथ अपना कोड, और इस तरह फ़ाइल हैश, बदल देता है।

9. सिक्योरिटी इनसाइट

DLL हाइजैकिंग Windows जैसे मानक ऑपरेटिंग सिस्टमों में सर्च ऑर्डर कॉन्फ़िगरेशन का फ़ायदा उठाती है।

10. सुरक्षा इनसाइट

सुरक्षा विक्रेताओं को रोज़ नए मैलवेयर नमूनों की भारी संख्या मिलती है, इसलिए सिग्नेचर को लगातार अपडेट करना पड़ता 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] CISA. (n.d.). Malware, Phishing, and Ransomware.
https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

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

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

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

ट्रोजन हॉर्स की परिभाषित विशेषता क्या है? → यह वैध सॉफ़्टवेयर का रूप धरकर उपयोगकर्ताओं को उसे चलाने के लिए बहकाता है

2 प्रश्न 2 सही उत्तर: A

शिक्षण नोट

किस प्रकार का मैलवेयर फ़ाइलें एन्क्रिप्ट करता है और भुगतान माँगता है? → रैंसमवेयर

3 प्रश्न 3 सही उत्तर: A

शिक्षण नोट

स्पाइवेयर क्या दर्शाता है? → ऐसा मैलवेयर जो उपयोगकर्ता की कीस्ट्रोक और ब्राउज़र गतिविधियों की गुप्त निगरानी के लिए बनाया गया हो

4 प्रश्न 4 सही उत्तर: A

शिक्षण नोट

मैलवेयर डेवलपर रूटकिट का उपयोग क्यों करते हैं? → सक्रिय प्रक्रियाओं और दुर्भावनापूर्ण फ़ाइलों को ऑपरेटिंग सिस्टम से छिपाना

5 प्रश्न 5 सही उत्तर: A

शिक्षण नोट

मैलवेयर विश्लेषण में सैंडबॉक्सिंग का क्या अर्थ है? → संदिग्ध फ़ाइलों को अलग वर्चुअल वॉल्ट में चलाकर उनका व्यवहार सुरक्षित रूप से देखना

उत्तर कुंजी: चेकपॉइंट 2 – सही या गलत

6 **प्रश्न 6** सही उत्तर: गलत

शिक्षण नोट

गलत: वर्म खुद को दोहराते हैं और उपयोगकर्ता की किसी कार्रवाई के बिना नेटवर्क में फैल जाते हैं।

7 **प्रश्न 7** सही उत्तर: गलत

शिक्षण नोट

गलत: एडवेयर हमेशा हानिरहित नहीं होता; उसका बड़ा हिस्सा विज्ञापन लक्षित करने के लिए ब्राउज़िंग को ट्रैक करता है।

8 **प्रश्न 8** सही उत्तर: सही

शिक्षण नोट

सही: साफ़ ऑफ़लाइन बैकअप भुगतान किए बिना एन्क्रिप्टेड फ़ाइलें बहाल कर देते हैं, हालाँकि चुराया गया डेटा फिर भी लीक हो सकता है।

9 **प्रश्न 9** सही उत्तर: गलत

शिक्षण नोट

गलत: सिग्नेचर स्कैनरों को ज्ञात नमूना चाहिए, इसलिए बिल्कुल नया ज़ीरो-डे मैलवेयर उनसे बच सकता है।

10 **प्रश्न 10** सही उत्तर: सही

शिक्षण नोट

फ़ाइललेस मैलवेयर सिस्टम मेमोरी में दुर्भावनापूर्ण स्क्रिप्ट चलाता है और डिस्क पर फ़ाइलें लिखने से बचता 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

D 1. ट्रोजन	F 2. रैनसमवेयर	A 3. स्पाइवेयर	H 4. रूटकिट
G 5. सैंडबॉक्स	C 6. रोकथाम	E 7. वर्म	B 8. फ़ाइललेस

चेकपॉइंट 3: उत्तर – प्रमुख शब्द

1 वायरस	2 रैनसमवेयर	3 स्पाइवेयर	4 रूटकिट
5 कंप्यूटर वर्म	6 कंटेनमेंट		

चेकपॉइंट 6, वैकल्पिक: उत्तर – शब्द मिलान

1 D – कंटेनमेंट	2 F – वायरस	3 H – सॉफ़्टवेयर	4 G – मैलवेयर
5 B – स्पाइवेयर	6 C – रूटकिट	7 A – रैनसमवेयर	8 E – कंप्यूटरवर्म

शिक्षकों के लिए चर्चा नोट

प्रमुख शब्द:
जाँचें कि क्या विद्यार्थी ट्रोजन, रैनसमवेयर और स्पाइवेयर 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

सा	स	ई	ते	घ	इ	नी	ल	रि	द	जे	घ	छ	ई	के
द	र	प	ति	के	ट	मि	ट	मै	सा	य	च	ऊ	नी	जी
इ	य	त	म	पे	ब	प	जि	मी	ल	ने	ले	इ	सी	य
छ	वे	र	दे	कि	जा	सा	वा	ड	रे	वे	स	ख	नि	फ
ढ	इ	मा	ना	का	रै	रे	दे	सि	मी	क	य	पि	रू	ता
ति	स्पा	ज	श	भ	न	ऊ	कं	अ	ऊ	ए	रि	र	ट	वि
स	र	य	वा	श	स	य	वि	प्यू	व	वा	पा	ल	कि	च
ट	से	कि	य	घ	म	प	के	की	ट	व	सि	री	ट	त
में	की	कि	सि	ना	वे	ने	पा	ते	ण	र	ए	ता	सा	मी
न	न	नी	ऋ	ले	य	घ	ति	जि	ला	ए	व	जी	ले	ड
टे	ल	द	जे	घ	र	के	च	से	दे	री	ए	र्म	पी	सॉ
कं	उ	अ	जे	मि	घ	व	आ	च	मी	च	ट	थ	फ़्ट	फ
ग	ना	सी	का	ज	फ	नी	जी	ता	ठ	से	लि	वे	ट	आ
इ	से	रा	के	री	पा	वा	सि	य	नि	पि	य	ने	ख	के
वे	ऊ	ड	नी	दे	दि	भ	आ	नि	जे	र	वे	वे	ष	ण

क्रॉसवर्ड समाधान



क्रॉसवर्ड समाधान के लिए शिक्षक गाइड

बाएँ से दाएँ

2 बाएँ से दाएँ: वायरस खुद की प्रतिलिपि बनाकर फैलने वाला हानिकारक कोड (4 अक्षर)

4 बाएँ से दाएँ: सॉफ़्टवेयर कंप्यूटर को चलाने वाले प्रोग्राम (5 अक्षर)

5 बाएँ से दाएँ: कंप्यूटरवर्म खुद को नेटवर्क पर फैलाने वाला दुर्भावनापूर्ण कीड़ा (6 अक्षर)

6 बाएँ से दाएँ: रूटकिट सिस्टम में गहराई से छिपकर रहने वाला प्रोग्राम (4 अक्षर)

ऊपर से नीचे

1 ऊपर से नीचे: रैनसमवेयर फ़ाइलें बंद करके फिरौती माँगने वाला प्रोग्राम (7 अक्षर)

3 ऊपर से नीचे: स्पाइवेयर चुपके से आपकी गतिविधि जासूसी करने वाला प्रोग्राम (5 अक्षर)

5 ऊपर से नीचे: कंटेनमेंट संक्रमण को आगे फैलने से रोकने की कार्रवाई (5 अक्षर)

अक्षर-फेर शब्द और कूट संदेश हल कुंजी

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

शब्द अनस्क्रैम्बल कुंजी

1. मयरैवेरसन — **रैनसमवेयर**
2. रूकिटट — **रूटकिट**
3. कंटरर्मवप्यू — **कंप्यूटरवर्म**
4. वेरयमैल — **मैलवेयर**
5. वेरस्पायइ — **स्पाइवेयर**
6. मेंकंनटटे — **कंटेनमेंट**
7. रवासय — **वायरस**
8. रसॉवेयफ़्ट — **सॉफ़्टवेयर**

गुप्त कूट चुनौती कुंजी

"व्यवहार मॉनिटर से पेलोड पहचानें"

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। रोकथाम (कंटेनमेंट) की नीतियाँ बनाएँ।
- 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: फ़ाइललेस मैलवेयर मेमोरी इंजेक्शन

शिक्षक समाधान

ग्रेडिंग दिशानिर्देश

छात्रों के उत्तरों में निम्नलिखित बिंदु शामिल होने चाहिए:

- परिदृश्य विश्लेषण: एक विश्लेषक मानक प्रशासनिक टूल से सीधे वोलेटाइल सिस्टम RAM में चल रहे संदिग्ध स्क्रिप्टिंग पैटर्न का पता लगाता है, लेकिन डिस्क पर कोई दुर्भावनापूर्ण फ़ाइल नहीं है।
- अनुशंसित रणनीति और समाधान: प्रभावित एंडपॉइंट को अलग करें और पहले मेमोरी इमेज कैप्चर करें। PowerShell और WMI लॉग की समीक्षा करें, AppLocker से अस्वीकृत स्क्रिप्ट ब्लॉक करें, फिर पेलोड हटाने के लिए रीबूट करें।