নাম: _____ তারিখ: _____ নম্বর: _____

সাইবার নিরাপত্তার মূল বিষয় ও অনলাইন হুমকি প্রতিরোধ

সাইবার নিরাপত্তা হুমকি, নেটওয়ার্ক ফায়ারওয়াল, মাল্টি-ফ্যাক্টর প্রমাণীকরণ, নিরাপত্তা কাঠামো

সাইবার নিরাপত্তার মূল বিষয় শিক্ষণ পরিচিতি

সুরক্ষিত
ডেটা এনক্রিপশন
256-বিট AES স্ট্যান্ডার্ড

সম্মতিপূর্ণ
বৈশ্বিক মান
GDPR ও CCPA কাঠামো

জিরো-ট্রাস্ট
অ্যাক্সেস নীতি
মাল্টি-ফ্যাক্টর অথেনটিকেশন

স্বাগতম! এই অ্যাক্টিভিটি প্যাকেট আপনাকে সাইবার নিরাপত্তার মূল বিষয় ও অনলাইন হুমকি প্রতিরোধের মৌলিক নীতি বিষয়ে গাইড করবে। আপনি ম্যালওয়্যার হুমকি, মাল্টি-ফ্যাক্টর প্রমাণীকরণ, নেটওয়ার্ক ফায়ারওয়াল এবং ঘটনা প্রতিক্রিয়া কাঠামো সম্পর্কে জানবেন।

ওয়ার্কশিট চেকপয়েন্ট

- [ ] **অংশ 1-4: সাইবার নিরাপত্তা ও হুমকি প্রতিরোধে দক্ষতা অর্জন করুন।**
- [ ] **অংশ 5-7: ক্রসওয়ার্ড ও ওয়ার্ড সার্চ ধাঁধা সমাধান করুন।**
- [ ] **অংশ 8-9: কেস স্টাডি ও সংকেতবার্তা চ্যালেঞ্জ সমাধান করুন।**
- [ ] **অংশ 10: প্রাথমিক ও উন্নত স্তরের FAQ পেজ পর্যালোচনা করুন।**
- [ ] **অংশ 11: 10টি আকর্ষণীয় বাস্তব তথ্য অন্বেষণ করুন।**
- [ ] **অতিরিক্ত: দ্রুত ভাবুন চ্যালেঞ্জ।**

VPN.com সাইবার নিরাপত্তা গাইড খুলুন

URL: https://www.vpn.com/bn/saibar-nirapotta/

আপনার সাইবার নিরাপত্তার মূল বিষয় শেখার রোডম্যাপ

- ম্যালওয়্যার, ফিশিং ও কর্পোরেট নেটওয়ার্কে অনুপ্রবেশের সাধারণ মাধ্যমগুলো শনাক্ত করুন।
- MFA, ফায়ারওয়াল এবং এন্ডপয়েন্ট ডিফেন্সসহ স্ট্যান্ডার্ড সাইবার নিরাপত্তা নিয়ন্ত্রণ বাস্তবায়ন করুন।
- ডেটা ব্রিচের প্রভাব কমাতে ঘটনা-প্রতিক্রিয়া পদ্ধতি মূল্যায়ন করুন।
- NIST নির্দেশিকার অধীনে প্রাতিষ্ঠানিক ঝুঁকির কারণ ও নিরাপত্তা সামঞ্জস্য বিশ্লেষণ করুন।
- স্বয়ংক্রিয় ক্রেডেনশিয়াল স্টাফিং প্রশমনে নিরাপত্তা-স্বাস্থ্যবিধি চর্চা কনফিগার করুন।

সাইবার নিরাপত্তা নির্দেশিকার নির্দেশনা

বহুনির্বাচনী ও সত্য/মিথ্যা প্রশ্নের উত্তর দিন, শব্দভাণ্ডার ব্যবহার করে শূন্যস্থান পূরণ করুন, সংজ্ঞা মেলান এবং ক্রসওয়ার্ড ও শব্দ খোঁজার ধাঁধা সমাধান করুন। হুমকি প্রতিরোধ বিষয়ে আপনার জ্ঞান প্রয়োগ করুন। শেষে অতিরিক্ত কার্যক্রম দ্রুত ভাবুন সম্পন্ন করুন।

সাইবার নিরাপত্তার মূল বিষয় ও হুমকি প্রতিরোধ (ভূমিকা)

সাইবার নিরাপত্তা নেটওয়ার্ক, সিস্টেম ও ডেটাকে অননুমোদিত ডিজিটাল আক্রমণ থেকে রক্ষা করে। দৃঢ় নিরাপত্তা অভ্যাস গড়ে তোলা, ফায়ারওয়াল কনফিগার করা, মাল্টি-ফ্যাক্টর প্রমাণীকরণ বাধ্যতামূলক করা এবং হুমকি চেনার বিষয়ে কর্মীদের প্রশিক্ষণ দেওয়া কর্পোরেট নেটওয়ার্ক প্রতিরক্ষার অপরিহার্য উপাদান।

প্রতিটি চেকপয়েন্ট মনোযোগ দিয়ে পড়ুন এবং সঠিক উত্তরটি বেছে নিন বা লিখুন।

চেকপয়েন্ট 1: বহুনির্বাচনী চ্যালেঞ্জ

1. 1. ফিশিং আক্রমণের প্রধান উদ্দেশ্য কী?
   - A. ক্রেডেনশিয়াল ও সংবেদনশীল ব্যবহারকারী ডেটা চুরি করা
   - B. ওয়েবসাইটের সার্চ ইঞ্জিন দৃশ্যমানতা বাড়ানো
   - C. নেটওয়ার্ক ব্যান্ডউইথ ক্ষমতা বাড়ানো
   - D. ব্যাকআপ ডেটা সেন্টার রেপ্লিকেশন পরিচালনা করা

2. 2. কোন প্রক্রিয়া সবচেয়ে শক্তিশালী অ্যাকাউন্ট সুরক্ষা দেয়?
   - A. হার্ডওয়্যার কী ব্যবহার করে মাল্টি-ফ্যাক্টর অথেন্টিকেশন
   - B. প্রতি ত্রিশ দিনে হালনাগাদ করা জটিল পাসওয়ার্ড
   - C. অ্যাকাউন্টে লগইন কর্মঘণ্টায় সীমাবদ্ধ করা
   - D. পাবলিক ডিরেক্টরি থেকে অ্যাকাউন্টের ইউজারনেম লুকানো

3. 3. র‍্যানসমওয়্যার সংক্রমণের পেলোডের বৈশিষ্ট্য কী?
   - A. সিস্টেম ফাইল এনক্রিপ্ট করে অর্থ দাবি করা
   - B. নীরবে দূরবর্তী সার্ভারে কিস্ট্রোক লগ করা
   - C. ব্রাউজারে অননুমোদিত বিজ্ঞাপন ঢুকিয়ে দেওয়া
   - D. ক্রিপ্টোকারেন্সি মাইন করতে স্থানীয় CPU সম্পদ ব্যবহার করা

4. 4. জিরো-ডে এক্সপ্লয়েট নিরাপত্তা প্রতিরক্ষায় কী প্রভাব ফেলে?
   - A. এটি প্যাচবিহীন, অজানা দুর্বলতাকে লক্ষ্য করে
   - B. এটি স্বয়ংক্রিয়ভাবে কর্পোরেট ফায়ারওয়াল বন্ধ করে দেয়
   - C. এটি সিস্টেমকে হার্ড রিবুট করতে বাধ্য করে
   - D. এর প্রতিকারে কোনো বাজেটই লাগে না

5. 5. কোন ফ্রেমওয়ার্ক কর্পোরেট নিরাপত্তা নিয়ন্ত্রণ পরিচালনা করে?
   - A. NIST সাইবারসিকিউরিটি ফ্রেমওয়ার্ক নির্দেশিকা
   - B. W3C HTML5 ডকুমেন্ট স্কিমা স্পেসিফিকেশন
   - C. প্রিন্টার ড্রাইভার ইনস্টলেশন ম্যানুয়াল
   - D. IETF রাউটিং প্রোটোকলের সংজ্ঞা

চেকপয়েন্ট 2: সত্য বা মিথ্যা চ্যালেঞ্জ

6 প্রশ্ন tf 6

6. ফিশিং আক্রমণ শুধু ব্যক্তিগত ইমেইল অ্যাকাউন্টকে লক্ষ্য করে।

সত্য মিথ্যা

7 প্রশ্ন tf 7

7. মাল্টি-ফ্যাক্টর প্রমাণীকরণ ক্রেডেনশিয়াল স্টাফিং আক্রমণ ঠেকাতে সহায়তা করে।

সত্য মিথ্যা

8 প্রশ্ন tf 8

8. ফায়ারওয়াল নেটওয়ার্ক ট্রাফিক পরীক্ষা করে অননুমোদিত পোর্ট অ্যাক্সেস ব্লক করে।

সত্য মিথ্যা

9 প্রশ্ন tf 9

9. জিরো-ডে এক্সপ্লয়েটের প্রতিকারে স্ট্যান্ডার্ড অ্যান্টিভাইরাস ডেফিনিশন হালনাগাদই যথেষ্ট।

সত্য মিথ্যা

10 প্রশ্ন tf 10

10. হানিপট হলো সাইবার অপরাধীদের টেনে আনতে ব্যবহৃত একটি ডিকয় সার্ভার।

সত্য মিথ্যা

চেকপয়েন্ট 3: মূল পরিভাষা বসানো

নিচের প্রতিটি বাক্য পড়ুন এবং ওয়ার্ড ব্যাংক থেকে সঠিক শব্দ দিয়ে শূন্যস্থান পূরণ করুন।

1. নেটওয়ার্ক প্রশাসকেরা আগত ট্রাফিক ছাঁকতে একটি _____ ইনস্টল করেন।
2. সিস্টেম প্যাচ এড়াতে আক্রমণকারী একটি জিরো-ডে _____ ব্যবহার করে।
3. কর্মীদের বিরুদ্ধে _____ প্রচারণা চালাতে আক্রমণকারীরা ভুয়া ইমেইল পাঠায়।
4. র‍্যানসমওয়্যার এমন এক ধ্বংসাত্মক _____ , যা ব্যবহারকারীর ডেটা তালাবদ্ধ করে।
5. শক্তিশালী পাসওয়ার্ড _____ বজায় রাখলে ক্রেডেনশিয়াল চুরির ঝুঁকি কমে।
6. সংবেদনশীল যোগাযোগ সুরক্ষিত রাখতে ব্যবহারকারীরা _____ প্রোটোকল প্রয়োগ করেন।

পরিভাষা শব্দভাণ্ডার

এক্সপ্লয়েট এনক্রিপশন ফায়ারওয়াল ফিশিং মাল্টিফ্যাক্টর ম্যালওয়্যার স্বাস্থ্যবিধি হানিপট সিস্টেম

এখানে আপনার উত্তর লিখুন:

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

চেকপয়েন্ট 4: নিরাপত্তা ধারণা মিলান

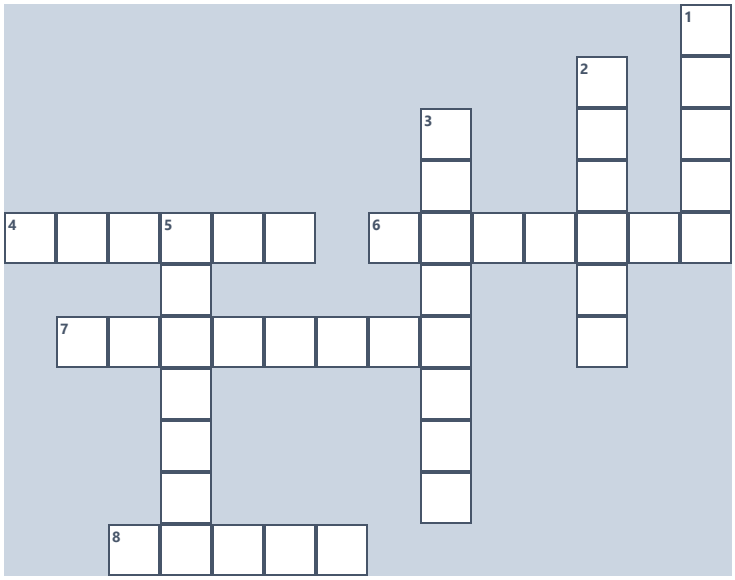
সংজ্ঞা মেলানো

পূরণযোগ্য ইনপুট বক্সে সংশ্লিষ্ট অক্ষর (A-H) লিখে বামদিকের প্রতিটি শব্দভাণ্ডার-পদকে ডানদিকের সঠিক সংজ্ঞার সঙ্গে মেলান।

☐	1. র‍্যানসমওয়্যার হুমকি	A	সাইবার ঝুঁকি পরিচালনায় ব্যবহৃত NIST-এর মতো কাঠামোবদ্ধ নির্দেশিকা।
☐	2. মাল্টি-ফ্যাক্টর প্রমাণীকরণ	B	নিরাপত্তা লঙ্ঘন সামলানো ও প্রশমনের কাঠামোবদ্ধ পরিকল্পনা।
☐	3. জিরো-ডে এক্সপ্লয়েট	C	নিরাপত্তা নিয়ম অনুযায়ী ট্রাফিক ফিল্টার করা নেটওয়ার্ক প্রতিবন্ধক।
☐	4. ডিকয় হানিপট	D	যে ম্যালওয়্যার ডেটা এনক্রিপ্ট করে ডিক্রিপশনের জন্য আর্থিক অর্থ দাবি করে।
☐	5. অনুপ্রবেশ ফায়ারওয়াল	E	ভেন্ডর প্যাচ প্রকাশের আগেই লক্ষ্য করা দুর্বলতা শোষণ।
☐	6. ঘটনা প্রতিক্রিয়া	F	ক্রেডেনশিয়াল ও প্রমাণীকরণ কী পরিচালনার সর্বোত্তম অনুশীলন।
☐	7. পাসওয়ার্ড স্বাস্থ্যবিধি	G	দুই বা ততোধিক অথেন্টিকেশন ফ্যাক্টর দাবি করা নিরাপত্তা যাচাইকরণ।
☐	8. নিরাপত্তা ফ্রেমওয়ার্ক	H	ক্ষতিকর ব্যক্তিদের প্রলুব্ধ করে বিশ্লেষণ করার জন্য তৈরি ডিকয় সিস্টেম।

চেকপয়েন্ট 5: ক্রসওয়ার্ড ধাঁধা

সক্রিয় সাদা ঘরে অক্ষর লিখে ক্রসওয়ার্ড পাজল সমাধান করুন। সংখ্যাগুলো নিচের সূত্রের সঙ্গে মেলে।



পাশাপাশি

4. বিক্রেতার প্যাচ প্রকাশের আগেই কাজে লাগানো দুর্বলতা-আক্রমণ (6)

6. ডেটা এনক্রিপ্ট করে ডিক্রিপশনের জন্য অর্থ দাবি করা ম্যালওয়্যার (7)

7. নিরাপত্তা-লঙ্ঘন সামলানো ও প্রশমনের কাঠামোবদ্ধ পরিকল্পনা (8)

8. সাইবার ঝুঁকি পরিচালনায় ব্যবহৃত NIST-এর মতো কাঠামোবদ্ধ নির্দেশিকা (5)

উপর-নিচ

1. দুই বা ততোধিক প্রমাণীকরণ উপাদান চাওয়া নিরাপত্তা-যাচাই (5)

2. নিরাপত্তা-নিয়মের ভিত্তিতে ট্রাফিক ছেঁকে দেওয়া নেটওয়ার্ক-প্রাচীর (6)

3. ক্রেডেনশিয়াল ও প্রমাণীকরণ কী পরিচালনার সর্বোত্তম অনুশীলন (8)

5. ক্ষতিকর পক্ষকে প্রলুব্ধ ও বিশ্লেষণ করতে সাজানো টোপ-সিস্টেম (7)

চেকপয়েন্ট 5, বিকল্প: সহজবোধ্য ক্রসওয়ার্ড সূত্র

স্ক্রিন-রিডার ও কিবোর্ড ব্যবহারকারীরা নিচের টেক্সট ফিল্ডে সরাসরি ক্রসওয়ার্ডের উত্তর লিখতে পারেন।

পাশাপাশি

4 পাশাপাশি: বিক্রেতার প্যাচ প্রকাশের আগেই কাজে লাগানো দুর্বলতা-আক্রমণ (6 অক্ষর):

6 পাশাপাশি: ডেটা এনক্রিপ্ট করে ডিক্রিপশনের জন্য অর্থ দাবি করা ম্যালওয়্যার (7 অক্ষর):

7 পাশাপাশি: নিরাপত্তা-লঙ্ঘন সামলানো ও প্রশমনের কাঠামোবদ্ধ পরিকল্পনা (8 অক্ষর):

8 পাশাপাশি: সাইবার ঝুঁকি পরিচালনায় ব্যবহৃত NIST-এর মতো কাঠামোবদ্ধ নির্দেশিকা (5 অক্ষর):

উপর-নিচ

1 উপর-নিচ: দুই বা ততোধিক প্রমাণীকরণ উপাদান চাওয়া নিরাপত্তা-যাচাই (5 অক্ষর):

2 উপর-নিচ: নিরাপত্তা-নিয়মের ভিত্তিতে ট্রাফিক ছেঁকে দেওয়া নেটওয়ার্ক-প্রাচীর (6 অক্ষর):

3 উপর-নিচ: ক্রেডেনশিয়াল ও প্রমাণীকরণ কী পরিচালনার সর্বোত্তম অনুশীলন (8 অক্ষর):

5 উপর-নিচ: ক্ষতিকর পক্ষকে প্রলুব্ধ ও বিশ্লেষণ করতে সাজানো টোপ-সিস্টেম (7 অক্ষর):

চেকপয়েন্ট 6: লুকানো শব্দ খোঁজা

নিচের গ্রিডে লুকানো ৪টি মূল শব্দভাণ্ডারের শব্দ খুঁজুন। শব্দগুলো অনুভূমিক, উল্লম্ব বা কোণাকুণি হতে পারে।

ক	সি	ল	দ	ঠ	হ	সা	শ	মে	দে	রা	কি	ঋ	তে	না
নে	ছ	য়া	য	প	উ	অ	উ	হা	ঋ	মা	বা	য	ফ	বা
ম	দে	ও	তি	ভ	ঘ	রে	ষ	ফ	নি	ঘ	দ	হ	স	ভ
রি	মি	র	লা	ম	হা	ডে	রো	জি	ঢ	প	ষ	ষ	রি	সি
না	তি	য়া	তা	ড	নি	ঊ	নি	রা	কি	থ	ট	সে	ঊ	লি
র	গ	ফা	নি	জা	রা	পি	ক্রে	ঋ	র	জি	লি	সি	ট	ভ
য়্যা	ণ	জে	গ	স	প	ঘ	রে	ডে	দি	ক্ট	মি	ঋ	স্টে	পা
ও	উ	অ	জে	কা	ত্তা	গ	ম	আ	ন	ঘ	ফ্যা	কি	ঘ	ম
ম	ঝ	ণ	ধ	গ	প্র	সি	রি	শ	ছ	শি	দ	ল্টি	সে	জি
স	নি	ঝ	রে	পে	তি	ফ্রে	জ	আ	আ	রে	য়া	মা	মা	স
ন	মে	তি	দে	রি	ক্রি	ম	ফ	সি	তি	সে	খ	ল	স	বে
র্যা	উ	ট	সে	দি	য়া	ও	দা	প	আ	সি	জে	বি	স্বা	বি
য	ড	দ	ষ	সা	ফ	য়া	ল	ল	তা	কে	ণ	রা	রি	স্থ্য
ণ	জে	ই	কে	পে	ঠ	র্ক	পি	ঊ	বে	সে	বে	উ	ণ	ল
জে	ঢ	ফ	কি	মে	কা	দা	ঋ	ল	জে	বে	ঠ	বি	কে	লে

পরিভাষা শব্দতালিকা

র্যানসমওয়্যার মাল্টিফ্যাক্টর জিরোডেহামলা হানিপটসিস্টেম ফায়ারওয়াল
নিরাপত্তাপ্রতিক্রিয়া ক্রেডেনশিয়ালস্বাস্থ্য ফ্রেমওয়ার্ক

চেকপয়েন্ট 6, বিকল্প: সহজবোধ্য শব্দভাণ্ডার মিলান

ফাঁকা জায়গায় অক্ষর (A-H) লিখে ওয়ার্ড সার্চের ৪টি শব্দভাণ্ডার-পদের প্রতিটিকে তার সঠিক সংজ্ঞার সঙ্গে মেলান।

পরিভাষা

A. র‍্যানসমওয়্যার

B. মাল্টিফ্যাক্টর

C. জিরোডেহামলা

D. হানিপটসিস্টেম

E. ফায়ারওয়াল

F. নিরাপত্তাপ্রতিক্রিয়া

G. ক্রেডেনশিয়ালস্বাস্থ্য

H. ফ্রেমওয়ার্ক

সংজ্ঞা ও মিলের ঘর

1. নিরাপত্তা-নিয়মের ভিত্তিতে ট্রাফিক ছেঁকে দেওয়া নেটওয়ার্ক-প্রাচীর।
2. নিরাপত্তা-লঙ্ঘন সামলানো ও প্রশমনের কাঠামোবদ্ধ পরিকল্পনা।
3. ডেটা এনক্রিপ্ট করে ডিক্রিপশনের জন্য অর্থ দাবি করা ম্যালওয়্যার।
4. দুই বা ততোধিক প্রমাণীকরণ উপাদান চাওয়া নিরাপত্তা-যাচাই।
5. ক্রেডেনশিয়াল ও প্রমাণীকরণ কী পরিচালনার সর্বোত্তম অনুশীলন।
6. সাইবার ঝুঁকি পরিচালনায় ব্যবহৃত NIST-এর মতো কাঠামোবদ্ধ নির্দেশিকা।
7. বিক্রেতার প্যাচ প্রকাশের আগেই কাজে লাগানো দুর্বলতা-আক্রমণ।
8. ক্ষতিকর পক্ষকে প্রলুব্ধ ও বিশ্লেষণ করতে সাজানো টোপ-সিস্টেম।

চেকপয়েন্ট 7: এলোমেলো শব্দ চ্যালেঞ্জ

সাইবার নিরাপত্তার মূল ধারণা ও পরিভাষা জানতে নিচের অক্ষরগুলো সাজান। উত্তর দেওয়া ইনপুট বাক্সে লিখুন।

1. ম য়্যা র্যা ও র স ন
2. লা জি ডে ম হা রো
3. ফা র ও ল য়া য়া
4. শি স্বা স্থ্য ল য়া ক্রে ডে ন
5. ফ্যা র মা ক্ট ল্টি
6. স্টে প সি হা ট ম নি
7. নি য়া প্র তি ক্রি রা ত্তা প
8. র্ক ফ্রে ও য়া ম

অতিরিক্ত কার্যক্রম: দ্রুত ভাবুন

প্রতিটি বিভাগে ৩টি উত্তর। যে প্রথমে তালিকা পূরণ করবে, সে জিতবে।

1	সাইবার নিরাপত্তার চাকরি			
2	সফটওয়্যার আপডেট করার কারণ			
3	একটি ফায়ারওয়াল যা যা ব্লক করতে পারে			
4	ইমেইলে সতর্কতার লক্ষণ			
5	যা যা আপনি ব্যাকআপ করেন			
6	সুপরিচিত সাইবার আক্রমণের ধরন			
7	একটি হানিপট যা যা আকৃষ্ট করতে পারে			
8	যে তথ্য আপনার কখনো শেয়ার করা উচিত নয়			
9	কম্পিউটার সংক্রমিত হওয়ার লক্ষণ			
10	হ্যাকারদের নিয়ে সিনেমা বা শো			
11	আপনি যেসব নিরাপত্তা স্তর তৈরি করতে পারেন			
12	নিরাপত্তা মহড়ায় যা যা অনুশীলন করবেন			
13	আপনার জানা নিরাপত্তা টুল			
14	IT সাহায্যের জন্য আপনি যাদের জিজ্ঞাসা করতে পারেন			
15	'সাইবার' দিয়ে শুরু হওয়া শব্দ			

চেকপয়েন্ট ৪: সাইবার নিরাপত্তা কেস স্টাডি

নিচের বাস্তব পরিস্থিতিগুলো সমাধান করতে শেখা ধারণাগুলো প্রয়োগ করুন।

কেস স্টাডি 1: র‍্যানসমওয়্যার পুনরুদ্ধার কৌশল



পরিস্থিতি: একটি কর্পোরেট নেটওয়ার্ক র‍্যানসমওয়্যারে সংক্রমিত হয়ে গুরুত্বপূর্ণ ডেটাবেস লক হয়ে গেছে। আক্রমণকারীরা ক্রিপ্টোকারেন্সিতে $100,000 দাবি করছে। কোম্পানির কাছে 24 ঘণ্টা আগের অফলাইন ব্যাকআপ আছে।

আলোচনার প্রশ্ন: অর্থ প্রদানের ঝুঁকি বিশ্লেষণ করুন এবং পুনরুদ্ধার কৌশল মূল্যায়ন করুন।

কেস স্টাডি 2: ক্রেডেনশিয়াল স্টাফিং প্রতিরক্ষা



পরিস্থিতি: একটি অনলাইন সেবা ক্রেডেনশিয়াল স্টাফিং আক্রমণের মুখে পড়ে, যেখানে হ্যাকাররা অন্য সাইট থেকে চুরি করা লক্ষ লক্ষ ইউজারনেম/পাসওয়ার্ড জোড়া পরীক্ষা করছে।

আলোচনার প্রশ্ন: এই আক্রমণের কার্যপ্রণালী বিস্তারিত বর্ণনা করুন এবং দুটি প্রতিরক্ষা ব্যবস্থার রূপরেখা দিন।

চেকপয়েন্ট 9: সংকেতবার্তা ডিকোড করুন

একজন সাইবার নিরাপত্তা পেশাজীবী অনলাইন হুমকিদাতাদের হাত থেকে নেটওয়ার্ক সম্পদ রক্ষা করেন। নিচের অক্ষর-থেকে-সংখ্যা কী ব্যবহার করে ফাঁকা ঘরে মিলে যাওয়া অক্ষর লিখে বার্তাটি ডিক্রিপ্ট করুন।

অক্ষর-থেকে-সংখ্যা এনক্রিপশন কী

অ=1 আ=2 ই=3 ঈ=4 উ=5 ঊ=6 ঋ=7 এ=8 ঐ=9 ও=10 ঔ=11 ক=12

খ=13 গ=14 ঘ=15 ঙ=16 চ=17 ছ=18 জ=19 ঝ=20 ঞ=21 ট=22 ঠ=23 ড=24

ঢ=25 ণ=26 ত=27 থ=28 দ=29 ধ=30 ন=31 প=32 ফ=33 ব=34 ভ=35 ম=36

য=37 র=38 ল=39 শ=40 ষ=41 স=42 হ=43 ৎ=44 া=45 ি=46 ী=47 ু=48

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

36	45	39	58	22	46	33	58	37	45	12	58	22	38	51

42	46	42	58	22	51	36	42	48	38	12	58	41	46	27

38	45	13	48	31

ডিকোড করা বার্তা:

পরামর্শ: প্রতিটি সংখ্যা বর্ণমালায় সেই অক্ষরের অবস্থান বোঝায় (যেমন 1 = অ, 2 = আ, 63 = ়)।

চেকপয়েন্ট 10: মৌলিক সাইবার নিরাপত্তা FAQ (অংশ A)

অনলাইন হুমকি প্রশমন নিয়ে প্রচলিত প্রশ্ন ও উত্তরগুলো দেখে নিন।

Q1: সাইবার নিরাপত্তার প্রধান উদ্দেশ্য কী?

মূল উদ্দেশ্য হলো অননুমোদিত অ্যাক্সেস, আক্রমণ ও দুর্ঘটনাজনিত ক্ষতি থেকে নেটওয়ার্ক, ডিভাইস ও ডেটা রক্ষা করা।

Q2: ফিশিং ও স্পিয়ার ফিশিং কীভাবে আলাদা?

ফিশিং হলো এলোমেলো ব্যবহারকারীদের লক্ষ্য করে চালানো বিস্তৃত ইমেইল ক্যাম্পেইন, আর স্পিয়ার ফিশিং ব্যক্তিগতকৃত তথ্য ব্যবহার করে নির্দিষ্ট ব্যক্তিদের লক্ষ্য করে।

Q3: নেটওয়ার্ক ফায়ারওয়াল কী?

ফায়ারওয়াল একটি নেটওয়ার্ক নিরাপত্তা ব্যবস্থা, যা আগে থেকে নির্ধারিত নিরাপত্তা নিয়মের ভিত্তিতে আগত ও বহির্গামী ট্রাফিক পর্যবেক্ষণ ও ফিল্টার করে।

Q4: মাল্টি-ফ্যাক্টর অথেনটিকেশন (MFA) কেন প্রয়োজনীয়?

MFA একটি গুরুত্বপূর্ণ প্রতিরক্ষা স্তর যোগ করে, ফলে আক্রমণকারী মূল পাসওয়ার্ড ক্রেডেনশিয়াল চুরি বা ক্র্যাক করলেও অ্যাক্সেস পায় না।

Q5: কম্পিউটার ভাইরাসের সংজ্ঞা কী?

ভাইরাস হলো স্বয়ং-প্রতিলিপিকারী ম্যালওয়্যার, যা পরিষ্কার ফাইলের সঙ্গে নিজেকে জুড়ে দেয় এবং চালু হলে সিস্টেমজুড়ে ছড়িয়ে পড়ে।

চেকপয়েন্ট 10: মৌলিক সাইবার নিরাপত্তা FAQ (অংশ B)

অনলাইন হুমকি প্রশমন নিয়ে প্রচলিত প্রশ্ন ও উত্তরগুলো দেখে নিন।

Q6: র‍্যানসমওয়্যার কীভাবে স্থানীয় ডেটা লক করে?

র‍্যানসমওয়্যার ব্যবহারকারীর ফাইল এনক্রিপ্ট করতে ক্রিপ্টোগ্রাফিক অ্যালগরিদম ব্যবহার করে, ফলে ডিক্রিপশন কী প্রয়োগ না করা পর্যন্ত ফাইল পড়া যায় না।

Q7: জিরো-ডে ভালনারেবিলিটি কী?

জিরো-ডে হলো সফটওয়্যারের এমন একটি নিরাপত্তা ত্রুটি, যা বিক্রেতার অজানা, ফলে এক্সপ্লয়েটের আগে প্যাচ তৈরির সময় থাকে না।

Q8: NIST ফ্রেমওয়ার্কের ভূমিকা কী?

NIST ফ্রেমওয়ার্ক স্বেচ্ছামূলক নির্দেশিকা ও মানদণ্ড দেয়, যা প্রতিষ্ঠানগুলোকে সাইবার নিরাপত্তা ঝুঁকি পরিচালনা ও কমাতে সাহায্য করে।

Q9: নিরাপত্তা ঘটনা প্রতিক্রিয়া পরিকল্পনা কী?

এটি নিরাপত্তা লঙ্ঘন ও নেটওয়ার্ক আপস শনাক্ত, নিয়ন্ত্রণ ও পুনরুদ্ধারের একটি নথিবদ্ধ কর্মপদ্ধতি।

Q10: সোশ্যাল ইঞ্জিনিয়ারিং কীভাবে ব্যবহারকারীদের কাজে লাগায়?

সোশ্যাল ইঞ্জিনিয়ারিং কর্মীদের পাসওয়ার্ড ফাঁস করতে বা ক্ষতিকর ফাইল ডাউনলোড করতে প্রতারিত করার জন্য মনস্তাত্ত্বিক কারসাজি ব্যবহার করে।

চেকপয়েন্ট 10: উন্নত নিরাপত্তা FAQ (অংশ C)

নিরাপত্তা কাঠামো, ম্যালওয়্যার বিশ্লেষণ ও ডেটা সম্মতির উন্নত প্রযুক্তিগত দিক অন্বেষণ করুন।

Q1: DDoS আক্রমণ কীভাবে ওয়েব সার্ভারকে অচল করে দেয়?

DDoS আক্রমণে লক্ষ লক্ষ আপসকৃত বটনেট ডিভাইস একসঙ্গে একটি সার্ভারে ট্রাফিকের বন্যা বইয়ে দেয়, ফলে ব্যান্ডউইথ ও CPU-র সীমা নিঃশেষ হয়ে যায়।

Q2: সিমেট্রিক ও অ্যাসিমেট্রিক এনক্রিপশনের মধ্যে পার্থক্য কী?

সিমেট্রিক এনক্রিপশনে এনক্রিপশন ও ডিক্রিপশনে একটিই কী ব্যবহৃত হয়, আর অ্যাসিমেট্রিক এনক্রিপশনে ব্যবহৃত হয় পাবলিক ও প্রাইভেট কী জোড়া।

Q3: হ্যাকাররা কীভাবে SQL ইনজেকশন আক্রমণ চালায়?

আক্রমণকারীরা ফর্ম ফিল্ডে ক্ষতিকর SQL কমান্ড দিয়ে ব্যাকএন্ড ডেটাবেসকে ধোঁকা দিয়ে অননুমোদিত ব্যবহারকারীর রেকর্ড বের করে আনে।

Q4: নেটওয়ার্ক অনুপ্রবেশে ল্যাটারাল মুভমেন্ট কী?

এটি এমন কৌশল, যেখানে আক্রমণকারীরা প্রাথমিক সার্ভার অ্যাক্সেস কাজে লাগিয়ে অভ্যন্তরীণ নেটওয়ার্কের অন্যান্য সংযুক্ত সিস্টেম আপস করে।

Q5: DNS স্পুফিং কীভাবে ওয়েব ট্রাফিক অন্যদিকে ঘুরিয়ে দেয়?

DNS স্পুফিং নেমসার্ভারের ক্যাশ রেকর্ড বদলে বৈধ ব্যবহারকারীদের আসল ডোমেইনের বদলে ক্ষতিকর নকল ওয়েবসাইটে পাঠায়।

চেকপয়েন্ট 10: উন্নত নিরাপত্তা FAQ (অংশ D)

নিরাপত্তা কাঠামো, ম্যালওয়্যার বিশ্লেষণ ও ডেটা সম্মতির উন্নত প্রযুক্তিগত দিক অন্বেষণ করুন।

Q6: হার্ডওয়্যার সিকিউরিটি টোকেন কী?

এটি একটি ভৌত ডিভাইস (যেমন YubiKey), যা ক্রিপ্টোগ্রাফিক প্রমাণীকরণ প্রমাণ তৈরি করে এবং দূরবর্তী ফিশিংয়ের বিরুদ্ধে সর্বোচ্চ সুরক্ষা দেয়।

Q7: নিরাপত্তা দলগুলো কীভাবে ডিকয় হানিপট ব্যবহার করে?

আগেভাগে অনুপ্রবেশ শনাক্ত করতে এবং অননুমোদিত ব্যক্তিদের আক্রমণের ধরন বিশ্লেষণ করতে টিমগুলো নন-প্রোডাকশন ডিকয় সার্ভার স্থাপন করে।

Q8: লিস্ট প্রিভিলেজের নীতি কী?

এটি এমন একটি নিরাপত্তা মানদণ্ড, যাতে ব্যবহারকারীর অ্যাক্সেস অধিকার তার কাজের ভূমিকা পালনের জন্য একান্ত প্রয়োজনীয় ন্যূনতম পর্যায়ে সীমিত রাখা হয়।

Q9: ম্যান-ইন-দ্য-মিডল আক্রমণ কীভাবে সংযোগের সুযোগ নেয়?

আক্রমণকারী এনক্রিপশনবিহীন নেটওয়ার্কে দুটি ডিভাইসের মধ্যকার যোগাযোগ আটকে পরিবর্তন করে এবং সেশন টোকেন ও ক্রেডেনশিয়াল চুরি করে।

Q10: ইন্ডিকেটর অব কম্প্রোমাইজ (IOC) কী?

IOC হলো ফরেনসিক ডেটার সূত্র, যেমন অস্বাভাবিক রেজিস্ট্রি পরিবর্তন বা বেআইনি IP ট্রাফিক, যা দেখায় যে একটি সিস্টেমে অনুপ্রবেশ ঘটেছে।

অংশ 11: 10টি বাস্তব সাইবার নিরাপত্তা তথ্য ও অন্তর্দৃষ্টি

নিরাপত্তা লঙ্ঘন, প্রতিরক্ষা কৌশল ও সম্মতির মান সম্পর্কে বাস্তব তথ্য দেখে নিন।

1. নিরাপত্তা ইনসাইট

আক্রমণকারীরা ক্রমাগত ইন্টারনেটে দুর্বল সার্ভার স্ক্যান করে এবং কর্মীদের ইনবক্সে ফিশিং ইমেইল পাঠায়।

2. নিরাপত্তা ইনসাইট

ফিশিং লিংকে ক্লিক করার মতো মানবিক ভুল ডেটা ফাঁসের একটি সাধারণ কারণ, তাই প্রশিক্ষণ গুরুত্বপূর্ণ।

3. নিরাপত্তা ইনসাইট

ডেটা ব্রিচের খরচের মধ্যে আইনি জরিমানা, গ্রাহক হারানো, তদন্ত ও মেরামত অন্তর্ভুক্ত এবং তা কয়েক মিলিয়ন ডলারে পৌঁছাতে পারে।

4. নিরাপত্তা ইনসাইট

হার্ডওয়্যার সিকিউরিটি কী-র মতো ফিশিং-প্রতিরোধী MFA হলো MFA-র সবচেয়ে শক্তিশালী ধরন এবং CISA-র জোর দেওয়া মান। [2]

5. নিরাপত্তা ইনসাইট

র‍্যানসমওয়্যার এন্টারপ্রাইজ নেটওয়ার্কের জন্য একটি বড় হুমকি হিসেবে রয়ে গেছে, এবং CISA প্রধান প্রতিরক্ষা হিসেবে অফলাইন, এনক্রিপ্টেড ব্যাকআপের পরামর্শ দেয়। [4]

6. নিরাপত্তা ইনসাইট

NIST সাইবারসিকিউরিটি ফ্রেমওয়ার্ক 2.0 (2024)-এ ছয়টি মূল কার্যক্রম আছে: Govern, Identify, Protect, Detect, Respond, Recover। [1]

7. সিকিউরিটি ইনসাইট

ক্রেডেনশিয়াল স্টাফিং বট ব্যাংকিং ও ই-কমার্স লগইন পোর্টালে বিপুল পরিমাণে ফাঁস হওয়া ইউজারনেম ও পাসওয়ার্ড জোড়া যাচাই করে।

8. সিকিউরিটি ইনসাইট

বিশ্বজুড়ে জিরো-ডে এক্সপ্লয়েট বাজার আছে, যেখানে প্যাচ হওয়ার আগে উচ্চ-তীব্রতার দুর্বলতা বড় অঙ্কে বিক্রি হতে পারে।

9. সিকিউরিটি ইনসাইট

হানিপট ডিকয় সিস্টেম অনুপ্রবেশের সতর্কতা তাৎক্ষণিকভাবে জানায়, কারণ বৈধ ব্যবহারকারীদের এতে প্রবেশের কোনো কারণ নেই।

10. নিরাপত্তা ইনসাইট

ট্রান্সপোর্ট লেয়ার সিকিউরিটি (TLS) ব্রাউজার সেশন এনক্রিপ্ট করে, ফলে পাবলিক Wi-Fi নেটওয়ার্কে প্যাকেট স্নিফিং প্রতিরোধ হয়।

প্রযুক্তিগত তথ্যসূত্র ও উৎস

স্টাডি গাইড ও ইন্টারঅ্যাক্টিভ ধাঁধাগুলো বৈশ্বিক NIST, OWASP এবং ডেটা গোপনীয়তা সম্মতির মানদণ্ড থেকে সংকলিত।

গবেষণামূলক ও শিল্পক্ষেত্রের তথ্যসূত্র

[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

উত্তরমালা: চেকপয়েন্ট 1 – বহুনির্বাচনী

1 **ফিশিং আক্রমণ** ফিশিং **সঠিক উত্তর: A**

শিক্ষণ নোট

ফিশিং ক্যাম্পেইন জাল ইমেইল ব্যবহার করে ক্রেডেনশিয়াল ও সংবেদনশীল ব্যবহারকারীর তথ্য চুরির চেষ্টা করে। তথ্যসূত্র: OWASP Secure Configuration।

2 **অ্যাকাউন্ট সুরক্ষা** MFA কী **সঠিক উত্তর: A**

শিক্ষণ নোট

হার্ডওয়্যার টোকেন ব্যবহারকারী মাল্টি-ফ্যাক্টর অথেনটিকেশন (MFA) অ্যাকাউন্ট অ্যাক্সেসের সবচেয়ে শক্তিশালী প্রতিরক্ষা দেয়। সূত্র: NIST Digital Identity।

3 **র‍্যানসমওয়্যার হুমকি** র‍্যানসমওয়্যার **সঠিক উত্তর: A**

শিক্ষণ নোট

র‍্যানসমওয়্যার গুরুত্বপূর্ণ সিস্টেম ও ডেটা এনক্রিপ্ট করে এবং ডিক্রিপশন কী-র জন্য ক্রিপ্টোকারেন্সিতে অর্থ দাবি করে। সূত্র: Center for Internet Security (CIS)।

4 **জিরো-ডে দুর্বলতা** জিরো-ডে **সঠিক উত্তর: A**

শিক্ষণ নোট

জিরো-ডে হুমকি ভেন্ডরের প্যাচ পাওয়ার আগেই আনপ্যাচড, অজানা নিরাপত্তা ত্রুটি কাজে লাগায়। উদ্ধৃতি: OWASP Secure Configuration।

5 **নিরাপত্তা কাঠামো** ফ্রেমওয়ার্ক **সঠিক উত্তর: A**

শিক্ষণ নোট

NIST-এর মতো ফ্রেমওয়ার্ক প্রতিষ্ঠানগুলোকে সাইবার ঝুঁকি পরিচালনা ও কমাতে কাঠামোবদ্ধ নির্দেশনা দিয়ে সাহায্য করে। সূত্র: NIST Digital Identity।

উত্তরমালা: চেকপয়েন্ট 2 – সত্য বা মিথ্যা

6 **লক্ষ্যভিত্তিক ফিশিং** ফিশিং — **সঠিক উত্তর: মিথ্যা**

শিক্ষণ নোট

আক্রমণের পথ বাড়াতে ফিশিং আক্রমণ কর্পোরেট নেটওয়ার্ক ও ব্যক্তিগত অ্যাকাউন্ট উভয়কেই লক্ষ্য করে। তথ্যসূত্র: OWASP Secure Configuration।

7 **প্রশ্ন 7** — **সঠিক উত্তর: সত্য**

শিক্ষণ নোট

MFA একটি দ্বিতীয় ফ্যাক্টর চায়, তাই শুধু চুরি হওয়া পাসওয়ার্ড দিয়ে সাধারণত লগইন করা যায় না।

8 **ট্রাফিক ফায়ারওয়াল** ফায়ারওয়াল — **সঠিক উত্তর: সত্য**

শিক্ষণ নোট

ফায়ারওয়াল নির্দিষ্ট নেটওয়ার্ক পোর্টের ট্রাফিক পরীক্ষা করে ও ব্লক করে, যাতে অননুমোদিত সংযোগ ছেঁকে ফেলা যায়। সূত্র: Center for Internet Security (CIS)।

9 **জিরো-ডে প্রতিক্রিয়া** জিরো-ডে — **সঠিক উত্তর: মিথ্যা**

শিক্ষণ নোট

জিরো-ডে ত্রুটি সারাতে কোড প্যাচ ও WAF ফিল্টারিং প্রয়োজন, কারণ এখনো কোনো সিগনেচার নেই। সূত্র: OWASP Secure Configuration।

10 **ডিকয় হানিপট** হানিপট — **সঠিক উত্তর: সত্য**

শিক্ষণ নোট

হানিপট হলো প্রতারণামূলক সার্ভার, যা নিরাপত্তা দল ক্ষতিকর ব্যক্তিদের প্রলুব্ধ করতে, সতর্কতা পেতে এবং তাদের নিয়ে গবেষণা করতে ব্যবহার করে। সূত্র: Center for Internet Security (CIS)।

শব্দভাণ্ডারের উত্তরমালা ও মূল্যায়ন রুব্রিক

শিক্ষকের মূল্যায়ন রুব্রিক: প্রতিটি সঠিক মিলের জন্য (মোট ৪ নম্বর) এবং প্রসঙ্গ পরিভাষার জন্য (মোট 6 নম্বর) 1 নম্বর দিন।

চেকপয়েন্ট 4: উত্তর – ধারণা মিলান

D 1. র‍্যানসমওয়্যার হুমকি	G 2. মাল্টি-ফ্যাক্টর প্রমাণীকরণ	E 3. জিরো-ডে এক্সপ্লয়েট	H 4. ডিকয় হানিপট
C 5. অনুপ্রবেশ ফায়ারওয়াল	B 6. ঘটনা প্রতিক্রিয়া	F 7. পাসওয়ার্ড স্বাস্থ্যবিধি	A 8. নিরাপত্তা ফ্রেমওয়ার্ক

চেকপয়েন্ট 3: উত্তর – মূল পরিভাষা

1 ফায়ারওয়াল	2 এক্সপ্লয়েট	3 ফিশিং	4 ম্যালওয়্যার
5 স্বাস্থ্যবিধি	6 এনক্রিপশন		

চেকপয়েন্ট 6, বিকল্প: উত্তর – শব্দ মিলান

1 E – ফায়ারওয়াল	2 F – নিরাপত্তাপ্রতিক্রিয়া	3 A – র্যানসমওয়্যার	4 B – মাল্টিফ্যাক্টর
5 G – ক্রেডেনশিয়ালস্বাস্থ্য	6 H – ফ্রেমওয়ার্ক	7 C – জিরোডেহামলা	8 D – হানিপটসিস্টেম

শিক্ষকদের জন্য আলোচনা নোট

মূল পরিভাষা:
যাচাই করুন শিক্ষার্থীরা র‍্যানসমওয়্যার হুমকি, মাল্টি-ফ্যাক্টর প্রমাণীকরণ ও জিরো-ডে এক্সপ্লয়েট নিজের ভাষায় ব্যাখ্যা করতে এবং প্রতিটির একটি উদাহরণ দিতে পারে কি না।

কেস স্টাডি:
শিক্ষার্থীদের বলুন তারা যেন মতামতের বদলে ওয়ার্কশিটের তথ্যের ভিত্তিতে সুপারিশ করে।

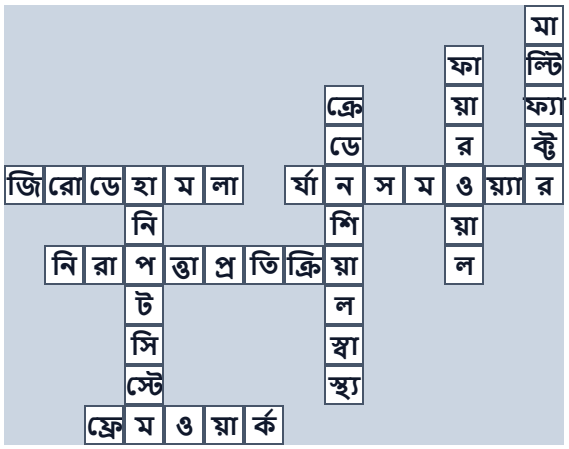
উৎস মূল্যায়ন:
শিক্ষার্থীদের ওয়ার্কশিটের উৎসে অন্তত একটি তথ্য যাচাই করতে বলুন এবং আলোচনা করুন কেন সংখ্যা, দাম ও নিয়ম সময়ের সঙ্গে বদলাতে পারে।

ধাঁধার উত্তরমালা ও শিক্ষকের নোট

শব্দ খোঁজার সমাধান

ক	সি	ল	দ	ঠ	হ	সা	শ	মে	দে	রা	কি	ঋ	তে	না
নে	ছ	য়া	য	প	উ	অ	উ	হা	ঋ	মা	বা	য	ফ	বা
ম	দে	ও	তি	ভ	ঘ	রে	ষ	ফ	নি	ঘ	দ	হ	স	ভ
রি	মি	র	লা	ম	হা	ডে	রো	জি	ঢ	প	ষ	ষ	রি	সি
না	তি	য়া	তা	ড	নি	ঊ	নি	রা	কি	থ	ট	সে	ঊ	লি
র	গ	ফা	নি	জা	রা	পি	ক্রে	ঋ	র	জি	লি	সি	ট	ভ
য়্যা	ণ	জে	গ	স	প	ঘ	রে	ডে	দি	ক্ট	মি	ঋ	স্টে	পা
ও	উ	অ	জে	কা	ত্তা	গ	ম	আ	ন	ঘ	ফ্যা	কি	ঘ	ম
ম	ঝ	ণ	ধ	গ	প্র	সি	রি	শ	ছ	শি	দ	ল্টি	সে	জি
স	নি	ঝ	রে	পে	তি	ফ্রে	জ	আ	আ	রে	য়া	মা	মা	স
ন	মে	তি	দে	রি	ক্রি	ম	ফ	সি	তি	সে	খ	ল	স	বে
র্যা	উ	ট	সে	দি	য়া	ও	দা	প	আ	সি	জে	বি	স্বা	বি
য	ড	দ	ষ	সা	ফ	য়া	ল	ল	তা	কে	ণ	রা	রি	স্থ্য
ণ	জে	ই	কে	পে	ঠ	র্ক	পি	ঊ	বে	সে	বে	উ	ণ	ল
জে	ঢ	ফ	কি	মে	কা	দা	ঋ	ল	জে	বে	ঠ	বি	কে	লে

ক্রসওয়ার্ডের সমাধান



ক্রসওয়ার্ড সমাধানের জন্য শিক্ষকের নির্দেশিকা

পাশাপাশি

4 পাশাপাশি: জিরোডেহামলা বিক্রেতার প্যাচ প্রকাশের আগেই কাজে লাগানো দুর্বলতা-আক্রমণ (6 অক্ষর)

6 পাশাপাশি: র্যানসমওয়্যার ডেটা এনক্রিপ্ট করে ডিক্রিপশনের জন্য অর্থ দাবি করা ম্যালওয়্যার (7 অক্ষর)

7 পাশাপাশি: নিরাপত্তাপ্রতিক্রিয়া নিরাপত্তা-লঙ্ঘন সামলানো ও প্রশমনের কাঠামোবদ্ধ পরিকল্পনা (8 অক্ষর)

8 পাশাপাশি: ফ্রেমওয়ার্ক সাইবার ঝুঁকি পরিচালনায় ব্যবহৃত NIST-এর মতো কাঠামোবদ্ধ নির্দেশিকা (5 অক্ষর)

উপর-নিচ

1 উপর-নিচ: মাল্টিফ্যাক্টর দুই বা ততোধিক প্রমাণীকরণ উপাদান চাওয়া নিরাপত্তা-যাচাই (5 অক্ষর)

2 উপর-নিচ: ফায়ারওয়াল নিরাপত্তা-নিয়মের ভিত্তিতে ট্রাফিক ছেঁকে দেওয়া নেটওয়ার্ক-প্রাচীর (6 অক্ষর)

3 উপর-নিচ: ক্রেডেনশিয়ালস্বাস্থ্য ক্রেডেনশিয়াল ও প্রমাণীকরণ কী পরিচালনার সর্বোত্তম অনুশীলন (8 অক্ষর)

5 উপর-নিচ: হানিপটসিস্টেম ক্ষতিকর পক্ষকে প্রলুব্ধ ও বিশ্লেষণ করতে সাজানো টোপ-সিস্টেম (7 অক্ষর)

এলোমেলো শব্দ ও সংকেতবার্তা সমাধানের উত্তরমালা

শব্দভাণ্ডার অক্ষর-সাজানো কার্যক্রম ও Secret Cipher Challenge-এর মূল্যায়ন উত্তরমালা।

শব্দ সাজানোর উত্তরমালা

1.	ময়্যার্যাওরসন	র্যানসমওয়্যার	5.	ফ্যারমাক্টল্টি	মাল্টিফ্যাক্টর
2.	লাজিডেমহারো	জিরোডেহামলা	6.	স্টেপসিহাটমনি	হানিপটসিস্টেম
3.	ফারওলয়ায়া	ফায়ারওয়াল	7.	নিয়াপ্রতিক্রিরাত্তাপ	নিরাপত্তাপ্রতিক্রিয়া
4.	শিস্বাস্থ্যলয়াক্রেডেন	ক্রেডেনশিয়ালস্বাস্থ্য	8.	র্কফ্রেওয়াম	ফ্রেমওয়ার্ক

গোপন সংকেত চ্যালেঞ্জের উত্তরমালা

"মাল্টিফ্যাক্টরে সিস্টেম সুরক্ষিত রাখুন"

কেস স্টাডির উত্তর

A কেস স্টাডি 1: র‍্যানসমওয়্যার পুনরুদ্ধার কৌশল

শিক্ষকের সমাধান

মূল্যায়ন নির্দেশিকা

শিক্ষার্থীদের উত্তরে নিচের বিষয়গুলো থাকা উচিত:

- পরিস্থিতি বিশ্লেষণ: একটি কর্পোরেট নেটওয়ার্ক র‍্যান্সমওয়্যারে সংক্রমিত হয়ে গুরুত্বপূর্ণ ডেটাবেস লক হয়ে গেছে। আক্রমণকারীরা $100,000 ক্রিপ্টোকারেন্সি দাবি করছে। কোম্পানির কাছে 24 ঘণ্টা আগের অফলাইন ব্যাকআপ আছে।
- প্রস্তাবিত কৌশল ও সমাধান: অর্থ দেওয়ার ঝুঁকি: অর্থ দিলে ফাইল ডিক্রিপশনের নিশ্চয়তা মেলে না, কোম্পানি অর্থ-প্রদানকারী লক্ষ্য হিসেবে চিহ্নিত হয় এবং অপরাধমূলক কর্মকাণ্ডে অর্থায়ন হয়। পুনরুদ্ধার কৌশল: দলটির উচিত সংক্রমিত হোস্ট আলাদা করা, আপসকৃত সার্ভার মুছে ফেলা এবং অফলাইন ব্যাকআপ থেকে ডেটা পুনরুদ্ধার করা। তাৎক্ষণিক পুনঃসংক্রমণ ঠেকাতে তাদের অবশ্যই প্রাথমিক প্রবেশপথ (ফিশিং বা এক্সপ্লয়েট) প্যাচ করতে হবে।

B কেস স্টাডি 2: ক্রেডেনশিয়াল স্টাফিং প্রতিরক্ষা

শিক্ষকের সমাধান

মূল্যায়ন নির্দেশিকা

শিক্ষার্থীদের উত্তরে নিচের বিষয়গুলো থাকা উচিত:

- পরিস্থিতি বিশ্লেষণ: একটি অনলাইন সেবা ক্রেডেনশিয়াল স্টাফিং আক্রমণের শিকার হয়, যেখানে হ্যাকাররা অন্য সাইট থেকে চুরি করা লক্ষ লক্ষ ব্যবহারকারীর নাম ও পাসওয়ার্ডের জোড়া পরীক্ষা করে দেখছে।
- প্রস্তাবিত কৌশল ও সমাধান: কার্যপদ্ধতি: আক্রমণকারীরা স্বয়ংক্রিয় বট ব্যবহার করে বিভিন্ন সাইটে পাসওয়ার্ড পুনর্ব্যবহারের সুযোগ নিয়ে ব্যবহারকারীর অ্যাকাউন্টে লগইন করে। প্রতিরক্ষা: 1. মাল্টি-ফ্যাক্টর অথেনটিকেশন (MFA) পাসওয়ার্ড সঠিক হলেও লগইন চেষ্টা আটকে দেয়। 2. রেট-লিমিটিং ও CAPTCHA চালু করলে লগইন এন্ডপয়েন্টে স্বয়ংক্রিয় বট ট্রাফিকের স্প্যাম আটকানো যায়।