নাম: _____ তারিখ: _____ নম্বর: _____

ম্যালওয়্যার বিশ্লেষণ ও হুমকি প্রশমন নির্দেশিকা

ট্রোজান, র‍্যানসমওয়্যার, স্পাইওয়্যার, রুটকিট, ভার্চুয়ালাইজেশন স্যান্ডবক্স, নিয়ন্ত্রণ

ম্যালওয়্যার বিশ্লেষণ শিক্ষণ সারসংক্ষেপ

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 ম্যালওয়্যার বিশ্লেষণ ও প্রতিরোধ বিষয়ে গাইড করবে। আপনি স্পাইওয়্যার, ট্রোজান, র‍্যানসমওয়্যার পেলোড, রিভার্স-ইঞ্জিনিয়ারিং টুল, রুটকিট আচরণ এবং নিয়ন্ত্রণ কৌশল 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/malware/

আপনার ম্যালওয়্যার প্রশমন শেখার রোডম্যাপ

- ট্রোজান, ওয়ার্ম ও রুটকিট ম্যালওয়্যারের ধরনের মধ্যে পার্থক্য করুন।
- কোড বিশ্লেষণের জন্য স্যান্ডবক্স ভার্চুয়ালাইজেশন এক্সিকিউশন বাস্তবায়ন করুন।
- সক্রিয় র‍্যানসমওয়্যার পেলোডের জন্য সীমাবদ্ধকরণ ও স্যানিটাইজেশন পরিকল্পনা নকশা করুন।

ম্যালওয়্যার বিশ্লেষণ গাইড নির্দেশনা

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

ম্যালওয়্যার বিশ্লেষণ ও হুমকি নিয়ন্ত্রণ (ভূমিকা)

ট্রোজান, ওয়ার্ম ও র‍্যানসমওয়্যারের মতো ক্ষতিকর কোড এন্ডপয়েন্ট ও সার্ভারের জন্য উচ্চ-প্রভাবের হুমকি। নিরাপত্তা দল ভার্চুয়াল স্যান্ডবক্সের ভেতরে ম্যালওয়্যার বিশ্লেষণ করে এবং পেলোড ছড়ানো ঠেকাতে দ্রুত নেটওয়ার্ক আইসোলেশন ব্যবস্থা নেয়।

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

চেকপয়েন্ট 1: বহুনির্বাচনী চ্যালেঞ্জ

1. ট্রোজান হর্সের সংজ্ঞায়ক বৈশিষ্ট্য কী?
   - A. এটি বৈধ সফটওয়্যারের ছদ্মবেশে ব্যবহারকারীকে প্রতারিত করে চালু করায়
   - B. এটি স্থানীয় নেটওয়ার্ক লাইন জুড়ে স্বয়ংক্রিয়ভাবে ছড়িয়ে পড়ে
   - C. এটি আলাদা ভার্চুয়াল স্যান্ডবক্সের ভেতরের ফাইল সংক্রমিত করে
   - D. এটি ইন্টারনেট সেবা সরবরাহকারীর ট্র্যাফিক মাঝপথে ধরে

2. কোন ধরনের ম্যালওয়্যার ফাইল এনক্রিপ্ট করে এবং অর্থ দাবি করে?
   - A. র‍্যানসমওয়্যার
   - B. স্পাইওয়্যার
   - C. রুটকিট
   - D. অ্যাডওয়্যার

3. স্পাইওয়্যার কী বোঝায়?
   - A. ব্যবহারকারীর কিস্ট্রোক ও ব্রাউজার কার্যকলাপ গোপনে পর্যবেক্ষণ করতে তৈরি ম্যালওয়্যার
   - B. স্যান্ডবক্স করা ভার্চুয়াল কনটেইনারের ভেতরে চলা প্রোগ্রাম কোড
   - C. ডেটাবেস রেজিস্ট্রি থেকে ডাউনলোড করা অ্যান্টি-ম্যালওয়্যার আপডেট
   - D. স্বয়ংক্রিয় স্ক্রিন উজ্জ্বলতা সমন্বয়

4. ম্যালওয়্যার ডেভেলপাররা কেন রুটকিট ব্যবহার করে?
   - A. অপারেটিং সিস্টেমের কাছ থেকে সক্রিয় প্রক্রিয়া ও ক্ষতিকর ফাইল লুকিয়ে রাখতে
   - B. এন্ডপয়েন্টে CPU প্রসেসিং গতি বাড়াতে
   - C. নিরাপদ ক্লাউড ভল্টে ডাটাবেস ফাইলের ব্যাকআপ রাখতে
   - D. ল্যাপটপের ব্যাটারি আয়ু বাড়াতে

5. ম্যালওয়্যার বিশ্লেষণে স্যান্ডবক্সিং বলতে কী বোঝায়?
   - A. আচরণ নিরাপদে পর্যবেক্ষণ করতে সন্দেহজনক ফাইল বিচ্ছিন্ন ভার্চুয়াল ভল্টে চালানো
   - B. পরিচিত হুমকির ডেটাবেসের বিরুদ্ধে ফাইল হ্যাশ স্ক্যান করা
   - C. অনুপ্রবেশের পর ডাটাবেস ব্যাকআপ পুনরুদ্ধার করা
   - D. স্থানীয় নেটওয়ার্ক রাউটারকে পাবলিক লাইন থেকে বিচ্ছিন্ন করা

চেকপয়েন্ট 2: সত্য বা মিথ্যা চ্যালেঞ্জ

6 প্রশ্ন 6

6. কম্পিউটার ওয়ার্ম স্থানীয় নেটওয়ার্কে ছড়াতে মানুষের ব্যবহারকারীর মিথস্ক্রিয়া প্রয়োজন করে।

- ◯ সত্য
- ◯ মিথ্যা

7 প্রশ্ন 7

7. অ্যাডওয়্যার সবসময় নিরীহ এবং ব্যবহারকারীর আচরণ বা ব্রাউজার ইতিহাস ট্র্যাক করে না।

- ◯ সত্য
- ◯ মিথ্যা

8 প্রশ্ন 8

8. পরিষ্কার অফলাইন ব্যাকআপ পুনরুদ্ধার করলে ভুক্তভোগীরা মুক্তিপণ না দিয়েই এনক্রিপ্ট হওয়া ফাইল ফিরে পেতে পারেন।

- ◯ সত্য
- ◯ মিথ্যা

9 প্রশ্ন 9

9. সিগনেচার-ভিত্তিক অ্যান্টিভাইরাস কোনো সিগনেচার তৈরি হওয়ার আগেই জিরো-ডে ম্যালওয়্যার নির্ভরযোগ্যভাবে ঠেকায়।

- ◯ সত্য
- ◯ মিথ্যা

10 প্রশ্ন 10

10. ফাইললেস ম্যালওয়্যার সিস্টেম মেমোরিতে ক্ষতিকর স্ক্রিপ্ট চালায়, ডিস্কে ফাইল লেখা এড়িয়ে।

- ◯ সত্য
- ◯ মিথ্যা

চেকপয়েন্ট 3: মূল পরিভাষা বসানো

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

1. নিরাপদ ইউটিলিটি প্রোগ্রামের ছদ্মবেশে থাকা ম্যালওয়্যারকে বলা হয় _____ ।
2. অর্থ আদায়ে ডেটাবেস সিস্টেম তালাবদ্ধ করা ক্ষতিকর পেলোডকে বলা হয় _____ ।
3. পাসওয়ার্ড গোপনে রেকর্ড করা কিলগার হলো _____ -এর উদাহরণ।
4. অপারেটিং সিস্টেম কার্নেলের গভীরে লুকিয়ে থাকতে একটি _____ লাগে।
5. বিচ্ছিন্ন ভল্টে সন্দেহজনক ফাইল বিশ্লেষণে একটি ভার্চুয়াল _____ ব্যবহৃত হয়।
6. সক্রিয় ম্যালওয়্যার পেলোড ছড়ানো থামাতে তাৎক্ষণিক নেটওয়ার্ক _____ দরকার।

পরিভাষা শব্দভাণ্ডার

ওয়ার্ম | কন্টেইনমেন্ট | জিম্মি ম্যালওয়্যার | ট্রোজান | ফাইললেস | রুটকিট | স্পাইওয়্যার | স্যান্ডবক্স

এখানে আপনার উত্তর লিখুন:

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

চেকপয়েন্ট 4: নিরাপত্তা ধারণা মিলান

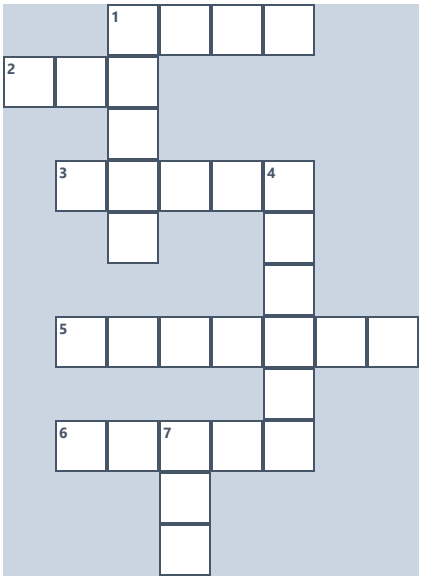
সংজ্ঞা মেলানো

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

☐	1. ট্রোজান	A	ব্যবহারকারীর কার্যকলাপ ও ইনপুট গোপনে পর্যবেক্ষণ ও রেকর্ড করার জন্য তৈরি প্রোগ্রাম।
☐	2. র‍্যানসমওয়্যার	B	ডিস্ক স্ক্যানারের শনাক্তকরণ এড়াতে সরাসরি RAM-এ চলা ম্যালওয়্যার।
☐	3. স্পাইওয়্যার	C	হুমকির পেলোড ছড়ানো ঠেকাতে সংক্রমিত এন্ডপয়েন্ট সীমিত করা।
☐	4. রুটকিট	D	নিরীহ বা কাজের ইউটিলিটি প্রোগ্রামের ছদ্মবেশে ক্ষতিকর সফটওয়্যার।
☐	5. স্যান্ডবক্স	E	মানুষের কোনো পদক্ষেপ ছাড়াই নেটওয়ার্কজুড়ে ছড়িয়ে পড়া স্বয়ংক্রিয়ভাবে বংশবিস্তারকারী ম্যালওয়্যার।
☐	6. নিয়ন্ত্রণ	F	যে ম্যালওয়্যার সিস্টেম স্টোরেজ এনক্রিপ্ট করে কী দেওয়ার বদলে অর্থ দাবি করে।
☐	7. ওয়ার্ম	G	ক্ষতিকর ফাইল নিরাপদে বিশ্লেষণ করতে ব্যবহৃত বিচ্ছিন্ন ভার্চুয়াল পরিবেশ।
☐	8. ফাইললেস	H	সিস্টেম কার্নেলের গভীরে লুকিয়ে প্রশাসনিক নিয়ন্ত্রণ ধরে রাখা গোপন ম্যালওয়্যার।

চেকপয়েন্ট 5: ক্রসওয়ার্ড ধাঁধা

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



পাশাপাশি

1. কোনো কাজ করার জন্য দেওয়া সম্মতি (4)

2. নিরীহ বা কাজের প্রোগ্রামের ছদ্মবেশে থাকা ক্ষতিকর সফটওয়্যার (3)

3. ডিস্ক স্ক্যানার ফাঁকি দিতে সরাসরি মেমোরিতে চলা ম্যালওয়্যার (5)

5. সিস্টেম স্টোরেজ এনক্রিপ্ট করে কী দেওয়ার বদলে অর্থ দাবি করা ম্যালওয়্যার (7)

6. গোপনে ব্যবহারকারীর কার্যকলাপ ও ইনপুট নজরে রাখা ও রেকর্ড করা প্রোগ্রাম (5)

উপর-নিচ

1. ইন্টারনেটের সঙ্গে সংযুক্ত থাকার অবস্থা (5)

4. কম্পিউটারকে কাজ করানোর নির্দেশমালা বা প্রোগ্রাম (6)

7. মানুষের পদক্ষেপ ছাড়াই নেটওয়ার্ক জুড়ে নিজেকে নকল করে ছড়ানো ম্যালওয়্যার (3)

চেকপয়েন্ট 5, বিকল্প: সহজবোধ্য ক্রসওয়ার্ড সূত্র

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

পাশাপাশি

1 পাশাপাশি: কোনো কাজ করার জন্য দেওয়া সম্মতি (4 অক্ষর):

2 পাশাপাশি: নিরীহ বা কাজের প্রোগ্রামের ছদ্মবেশে থাকা ক্ষতিকর সফটওয়্যার (3 অক্ষর):

3 পাশাপাশি: ডিস্ক স্ক্যানার ফাঁকি দিতে সরাসরি মেমোরিতে চলা ম্যালওয়্যার (5 অক্ষর):

5 পাশাপাশি: সিস্টেম স্টোরেজ এনক্রিপ্ট করে কী দেওয়ার বদলে অর্থ দাবি করা ম্যালওয়্যার (7 অক্ষর):

6 পাশাপাশি: গোপনে ব্যবহারকারীর কার্যকলাপ ও ইনপুট নজরে রাখা ও রেকর্ড করা প্রোগ্রাম (5 অক্ষর):

উপর-নিচ

1 উপর-নিচ: ইন্টারনেটের সঙ্গে সংযুক্ত থাকার অবস্থা (5 অক্ষর):

4 উপর-নিচ: কম্পিউটারকে কাজ করানোর নির্দেশমালা বা প্রোগ্রাম (6 অক্ষর):

7 উপর-নিচ: মানুষের পদক্ষেপ ছাড়াই নেটওয়ার্ক জুড়ে নিজেকে নকল করে ছড়ানো ম্যালওয়্যার (3 অক্ষর):

চেকপয়েন্ট 6: লুকানো শব্দ খোঁজা

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

তা বি নি ঘ ল মি কে ভ ড রা র ঈ তি গ ই
সে র ভ মা ণ জে ঘ চ অ ই হ ণ দ নে স
ঝ য়্যা কা জ রা ফ ঘ উ সে ন জি আ ড প পা
ধ ও দ জি কি না লি ই রে ফ লা চ ট্রো জা ন
ব ই দি শ জা জি রা দে ট মে র ই ক ও সি
দ স্পা ঠ হ সা ম্মি শ স মে দে রা কি ন য়া ঋ
তে না নে ছ য ম্যা প উ ফ অ উ ঋ মা র্ম বা
স য ফ বা ম ল দে তি ভ ট ঘ রে ষ ফ ঘ
লে দ হ স ভ ও রি মি ঢ ষ ও ষ রি সি না
ল তি তা ড ঊ য়্যা নি রা কি থ সে য়্যা ঊ লি গ
ই নি জা পি ঋ র জি লি ট ভ ণ জে র গ অ
ফা স ঘ রে দি মি ঋ পা উ অ জে কা গ নু ম
আ ঘ কি ঘ ঝ ণ ধ গ সি রি শ ছ ম দ সে
জি নি ঝ রে পে জ আ আ রে মা স তি মে তি দে
রি ফ সি তি সে খ স বে উ ট সে দি দা প আ

পরিভাষা শব্দতালিকা

ট্রোজান জিম্মিম্যালওয়্যার স্পাইওয়্যার ওয়ার্ম ফাইললেস অনলাইন সফটওয়্যার অনুমতি

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. ট্রোজান

B. জিম্মিম্যালওয়্যার

C. স্পাইওয়্যার

D. ওয়ার্ম

E. ফাইললেস

F. অনলাইন

G. সফটওয়্যার

H. অনুমতি

সংজ্ঞা ও মিলের ঘর

1. মানুষের পদক্ষেপ ছাড়াই নেটওয়ার্ক জুড়ে নিজেকে নকল করে ছড়ানো ম্যালওয়্যার।

2. ইন্টারনেটের সঙ্গে সংযুক্ত থাকার অবস্থা।

3. কোনো কাজ করার জন্য দেওয়া সম্মতি।

4. কম্পিউটারকে কাজ করানোর নির্দেশমালা বা প্রোগ্রাম।

5. সিস্টেম স্টোরেজ এনক্রিপ্ট করে কী দেওয়ার বদলে অর্থ দাবি করা ম্যালওয়্যার।

6. গোপনে ব্যবহারকারীর কার্যকলাপ ও ইনপুট নজরে রাখা ও রেকর্ড করা প্রোগ্রাম।

7. নিরীহ বা কাজের প্রোগ্রামের ছদ্মবেশে থাকা ক্ষতিকর সফটওয়্যার।

8. ডিস্ক স্ক্যানার ফাঁকি দিতে সরাসরি মেমোরিতে চলা ম্যালওয়্যার।

চেকপয়েন্ট 7: এলোমেলো শব্দ চ্যালেঞ্জ

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

1. জা ন ট্রো
2. স্পা র য়্যা ও ই
3. ল ফা স লে ই
4. র ও ট য়্যা স ফ
5. ও র ল ম্যা জি য়্যা ম্মি
6. য়া র্ম ও
7. ই ন অ লা ন
8. অ তি ম নু

অতিরিক্ত কার্যক্রম: দ্রুত ভাবুন

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

1	নিরাপদ অ্যাপ ডাউনলোডের জায়গা			
2	যেসব ডিভাইস হ্যাক হতে পারে			
3	যা যা আপনি ব্যাকআপ করেন			
4	ইমেইলে সতর্কতার লক্ষণ			
5	ফোনে ম্যালওয়্যার থাকার লক্ষণ			
6	আপনার জানা ম্যালওয়্যারের ধরন			
7	যেসব ফাইলের ধরন নিয়ে সতর্ক থাকতে হবে			
8	যেসব উপায়ে ম্যালওয়্যার PC-তে ঢোকে			
9	যেসব নিরাপদ অভ্যাস আপনি আজই শুরু করতে পারেন			
10	সাইবার নিরাপত্তার সঙ্গে সম্পর্কিত শব্দ			
11	ডেটা ফাঁসের পর যা করবেন			
12	সফটওয়্যার আপডেট করার কারণ			
13	ম্যালওয়্যারের মতো নামের প্রাণী বা চরিত্র			
14	ম্যালওয়্যার যা যা চুরি করতে পারে			
15	ভুল লিংকে ক্লিক করে ফেললে যা করবেন			

চেকপয়েন্ট 8: সাইবার নিরাপত্তা কেস স্টাডি

নিচের বাস্তব পরিস্থিতিগুলো সমাধান করতে শেখা ধারণাগুলো প্রয়োগ করুন।

কেস স্টাডি 1: এন্টারপ্রাইজ র‍্যানসমওয়্যার পেলোড নিয়ন্ত্রণ



পরিস্থিতি: একটি কর্পোরেট লোকাল এরিয়া নেটওয়ার্ক সক্রিয় র‍্যানসমওয়্যারে আক্রান্ত হয়েছে। মূল ফাইল সার্ভারগুলোতে .locked এক্সটেনশন দেখা যেতে শুরু করেছে। নিয়ন্ত্রণ নীতি প্রতিষ্ঠা করুন।

আলোচনার প্রশ্ন: নিয়ন্ত্রণমূলক ধাপগুলো বিস্তারিত বর্ণনা করুন এবং ডেটা পুনরুদ্ধার প্রোটোকলের রূপরেখা দিন।

কেস স্টাডি 2: ফাইলহীন ম্যালওয়্যারের মেমরি ইনজেকশন



পরিস্থিতি: একজন বিশ্লেষক স্ট্যান্ডার্ড অ্যাডমিনিস্ট্রেটিভ টুল ব্যবহার করে সরাসরি ভোলাটাইল সিস্টেম RAM-এ চলমান সন্দেহজনক স্ক্রিপ্টিং প্যাটার্ন শনাক্ত করেন, কিন্তু ডিস্কে কোনো ক্ষতিকর ফাইল নেই।

আলোচনার প্রশ্ন: মেমরি বিশ্লেষণ কৌশল ব্যাখ্যা করুন এবং ফাইললেস এক্সিকিউশন ব্লক করার টুল উল্লেখ করুন।

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

2	17	38	26		31	19	38	51		12	58	41	27	46	12	38

32	51	39	53	24		30	38	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: ম্যালওয়্যার কী?

হুমকিদাতাদের তৈরি ক্ষতিকর সফটওয়্যার, যা ডিভাইস ও নেটওয়ার্কের ক্ষতি করে, হাইজ্যাক করে বা ডেটা চুরি করে।

Q2: ভাইরাস ও ওয়ার্মের মধ্যে পার্থক্য কী?

ছড়াতে ভাইরাসের মানুষের পদক্ষেপ (যেমন ফাইল খোলা) দরকার হয়, আর ওয়ার্ম নেটওয়ার্কজুড়ে স্বয়ংক্রিয়ভাবে ছড়ায়।

Q3: ট্রোজান হর্স কীভাবে কম্পিউটারে সংক্রমণ ঘটায়?

এটি নিজেকে নিরীহ বা নিরাপদ প্রোগ্রাম সাজিয়ে ব্যবহারকারীদের ধোঁকা দেয় এবং ভেতরে ক্ষতিকর পেলোড লুকিয়ে রাখে।

Q4: র‍্যানসমওয়্যার কী?

একধরনের ম্যালওয়্যার, যা লক্ষ্য সিস্টেমের ফাইল এনক্রিপ্ট করে ডিক্রিপশন কী-র বিনিময়ে আর্থিক অর্থ দাবি করে। [1]

Q5: স্পাইওয়্যার কী?

যে ক্ষতিকর সফটওয়্যার গোপনে ব্যবহারকারীর কিস্ট্রোক, পাসওয়ার্ড ও ব্রাউজিং অভ্যাস রেকর্ড করে আক্রমণকারীদের কাছে পাঠায়।

চেকপয়েন্ট 10: মৌলিক সাইবার নিরাপত্তা FAQ (অংশ B)

অনলাইন হুমকি প্রশমন নিয়ে প্রচলিত প্রশ্ন ও উত্তরগুলো দেখে নিন।

Q6: স্যান্ডবক্সিং বলতে কী বোঝায়?

প্রোডাকশন সিস্টেমের ঝুঁকি ছাড়া আচরণ পর্যবেক্ষণ করতে সন্দেহজনক ফাইল নিরাপদ, বিচ্ছিন্ন ভার্চুয়াল পরিবেশে চালানো।

Q7: ফাইলবিহীন ম্যালওয়্যার কী?

যে ম্যালওয়্যার বৈধ ইউটিলিটি ব্যবহার করে সরাসরি সিস্টেম মেমোরিতে (RAM) চলে এবং সাধারণ স্ক্যানার এড়াতে ডিস্কে ফাইল লেখে না।

Q8: রুটকিট কীভাবে ম্যালওয়্যারকে রক্ষা করে?

এটি ক্ষতিকর প্রক্রিয়া ও ফাইল লুকিয়ে রাখে, প্রায়ই অপারেটিং সিস্টেম কার্নেল বিকৃত করে, ফলে অ্যান্টিভাইরাস স্ক্যানার সেগুলো ধরতে নাও পারে।

Q9: ডাইনামিক বিহেভিয়ার মনিটরিং কী?

সক্রিয় প্রসেসগুলোকে রিয়েল টাইমে পর্যবেক্ষণ করে ম্যালওয়্যারের সাধারণ কাজ, যেমন একসঙ্গে অনেক ফাইল এনক্রিপ্ট করা, ঠেকানোর অ্যান্টিভাইরাস স্ক্যানিং।

Q10: ঘটনা মোকাবিলার সময় নিয়ন্ত্রণ ব্যবস্থা জরুরি কেন?

আপসকৃত এন্ডপয়েন্ট বিচ্ছিন্ন করলে সক্রিয় ম্যালওয়্যার পেলোড অন্য নেটওয়ার্ক ডিভাইসে ছড়াতে পারে না।

চেকপয়েন্ট 10: উন্নত নিরাপত্তা FAQ (অংশ C)

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

Q1: ম্যালওয়্যার ডেভেলপাররা কীভাবে সিগনেচারভিত্তিক অ্যান্টিভাইরাস স্ক্যানার এড়ায়?

এরা পলিমরফিজম ব্যবহার করে, অর্থাৎ ক্ষতিকর আচরণ একই রেখে প্রতিটি সংক্রমণে ফাইলের হ্যাশ ও কোডের কাঠামো বদলে ফেলে।

Q2: ম্যালওয়্যার ক্যাম্পেইনে দ্বৈত-ব্যবহারের টুলের ঝুঁকি কী?

আক্রমণকারীরা স্বাভাবিক নেটওয়ার্ক ট্র্যাফিকের সঙ্গে মিশে যেতে (PowerShell বা Sysinternals-এর মতো) বৈধ প্রশাসনিক টুল ব্যবহার করে, ফলে শনাক্ত করা কঠিন হয়।

Q3: প্রসেস হোলোইং কীভাবে ক্ষতিকর পেলোড চালায়?

এটি একটি বৈধ সিস্টেম প্রক্রিয়া স্থগিত অবস্থায় চালু করে, তার মেমরি কোড ম্যালওয়্যার দিয়ে প্রতিস্থাপন করে এবং এক্সিকিউশন আবার শুরু করে।

Q4: কমান্ড অ্যান্ড কন্ট্রোল (C2) সার্ভারের ভূমিকা কী?

হ্যাকারদের পরিচালিত একটি রিমোট সার্ভার, যা আপসকৃত মেশিনে চলা ম্যালওয়্যারের কাছে নির্দেশ ও পেলোড পাঠায়।

Q5: কিলগিং শনাক্ত করা কেন কঠিন?

সাধারণ কিলগার খুব কম CPU রিসোর্স ব্যবহার করে এবং বৈধ ইউজার-স্পেস ইউটিলিটির ভেতরে তাদের প্রসেস লুকিয়ে রাখে।

চেকপয়েন্ট 10: উন্নত নিরাপত্তা FAQ (অংশ D)

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

Q6: কোড অবফাসকেশন কীভাবে ম্যালওয়্যার বিশ্লেষণে বিলম্ব ঘটায়?

এটি সোর্স কোড এনক্রিপ্ট বা পুনর্বিন্যস্ত করে, ফলে বিশ্লেষক সরঞ্জাম ও নিরাপত্তা স্ক্যানারের কাছে তা অপঠনযোগ্য হয়ে যায়।

Q7: বুটকিটের কাজ কী?

বুট প্রক্রিয়াকে (MBR, বুট সেক্টর বা UEFI ফার্মওয়্যার) সংক্রমিত করা একটি রুটকিট, ফলে এটি অপারেটিং সিস্টেম লোড হওয়ার আগেই চলে।

Q8: হিউরিস্টিক স্ক্যানিং কীভাবে জিরো-ডে হুমকি শনাক্ত করে?

এটি মিলে যাওয়া ডেটাবেস হ্যাশ খোঁজার পরিবর্তে সন্দেহজনক কোড প্যাটার্ন ও প্রশাসনিক কমান্ড স্ক্যান করে।

Q9: DLL হাইজ্যাকিংয়ের হুমকি কী?

কোনো বৈধ অ্যাপ্লিকেশনের ডিরেক্টরি পাথে একটি ক্ষতিকর ডাইনামিক লিংক লাইব্রেরি (DLL) রেখে অ্যাপ্লিকেশনটিকে সেটি লোড করতে বাধ্য করা।

Q10: স্বয়ংক্রিয় ম্যালওয়্যার বিশ্লেষণ পাইপলাইন কীভাবে ভার্চুয়ালাইজেশন ব্যবহার করে?

এরা সন্দেহজনক ফাইল একাধিক OS ভার্চুয়াল মেশিনে চালায় এবং স্বয়ংক্রিয়ভাবে আচরণ লগ ও নেটওয়ার্ক PCAP ফাইল তৈরি করে।

অংশ 11: 10টি বাস্তব সাইবার নিরাপত্তা তথ্য ও অন্তর্দৃষ্টি

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

1. নিরাপত্তা ইনসাইট

ট্রোজান হর্স এখনও একটি প্রচলিত সংক্রমণ পদ্ধতি, কারণ এরা নির্দোষ দেখতে প্রোগ্রামের ভেতরে ক্ষতিকর কোড লুকিয়ে রাখে।

2. নিরাপত্তা ইনসাইট

FBI-এর IC3 2025 সালে 3,600-এর বেশি র‍্যানসমওয়্যার অভিযোগ পেয়েছে, যেখানে জানানো ক্ষতির পরিমাণ $32 million ছাড়িয়ে গেছে। [3]

3. নিরাপত্তা ইনসাইট

SMB-তে EternalBlue-র মতো প্যাচ না করা প্রোটোকল দুর্বলতা কাজে লাগিয়ে ওয়ার্ম নেটওয়ার্কজুড়ে দ্রুত ছড়িয়ে পড়তে পারে।

4. নিরাপত্তা ইনসাইট

ফাইললেস ম্যালওয়্যার শনাক্ত করা কঠিন, কারণ এটি বৈধ টুলের মাধ্যমে মেমোরিতে চলে এবং ডিস্কে খুব কম চিহ্ন রেখে যায়।

5. নিরাপত্তা ইনসাইট

অ্যানালাইসিস স্যান্ডবক্স সাধারণত প্রতিটি রানের পর একটি পরিষ্কার স্ন্যাপশটে ফিরে যায়, যাতে প্রতিটি পরীক্ষা একটি জানা অবস্থা থেকে শুরু হয়।

6. নিরাপত্তা ইনসাইট

রুটকিট কার্নেল সিস্টেম কল পরিবর্তন করে অ্যান্টি-ম্যালওয়্যার স্ক্যানারকে মিথ্যা ডায়াগনস্টিক ফলাফল জানাতে পারে।

7. সিকিউরিটি ইনসাইট

কোড অবফাসকেশন ম্যালওয়্যারের প্রকৃত বাইনারি পেলোড কাঠামো সংকুচিত ও লুকাতে প্যাকার ইউটিলিটি ব্যবহার করে।

8. সিকিউরিটি ইনসাইট

পলিমরফিক ম্যালওয়্যার সিগনেচার পরীক্ষা এড়াতে প্রতিটি নতুন কপিতে নিজের কোড, এবং তাই ফাইলের হ্যাশও, বদলে ফেলে।

9. সিকিউরিটি ইনসাইট

DLL হাইজ্যাকিং উইন্ডোজের মতো প্রচলিত অপারেটিং সিস্টেমের সার্চ অর্ডার কনফিগারেশনের দুর্বলতা কাজে লাগায়।

10. নিরাপত্তা ইনসাইট

নিরাপত্তা বিক্রেতারা প্রতিদিন বিপুল সংখ্যক নতুন ম্যালওয়্যার নমুনা খুঁজে পান, তাই সিগনেচর ক্রমাগত হালনাগাদ করতে 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] 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

উত্তরমালা: চেকপয়েন্ট 1 – বহুনির্বাচনী

1 প্রশ্ন 1 — সঠিক উত্তর: A

শিক্ষণ নোট

ট্রোজান হর্সের সংজ্ঞায়ক বৈশিষ্ট্য কী? → এটি বৈধ সফটওয়্যারের ছদ্মবেশে ব্যবহারকারীকে প্রতারিত করে চালু করায়

2 প্রশ্ন 2 — সঠিক উত্তর: A

শিক্ষণ নোট

কোন ধরনের ম্যালওয়্যার ফাইল এনক্রিপ্ট করে এবং অর্থ দাবি করে? → র‍্যানসমওয়্যার

3 প্রশ্ন 3 — সঠিক উত্তর: A

শিক্ষণ নোট

স্পাইওয়্যার কী বোঝায়? → ব্যবহারকারীর কিস্ট্রোক ও ব্রাউজার কার্যকলাপ গোপনে পর্যবেক্ষণ করতে তৈরি ম্যালওয়্যার

4 প্রশ্ন 4 — সঠিক উত্তর: A

শিক্ষণ নোট

ম্যালওয়্যার ডেভেলপাররা কেন রুটকিট ব্যবহার করে? → অপারেটিং সিস্টেমের কাছ থেকে সক্রিয় প্রক্রিয়া ও ক্ষতিকর ফাইল লুকিয়ে রাখতে

5 প্রশ্ন 5 — সঠিক উত্তর: A

শিক্ষণ নোট

ম্যালওয়্যার বিশ্লেষণে স্যান্ডবক্সিং বলতে কী বোঝায়? → আচরণ নিরাপদে পর্যবেক্ষণ করতে সন্দেহজনক ফাইল বিচ্ছিন্ন ভার্চুয়াল ভল্টে চালানো

উত্তরমালা: চেকপয়েন্ট 2 – সত্য বা মিথ্যা

6 প্রশ্ন 6 — সঠিক উত্তর: মিথ্যা

শিক্ষণ নোট

মিথ্যা: ওয়ার্ম নিজে থেকে প্রতিলিপি তৈরি করে এবং কোনো ব্যবহারকারীর পদক্ষেপ ছাড়াই নেটওয়ার্কজুড়ে ছড়িয়ে পড়ে।

7 প্রশ্ন 7 — সঠিক উত্তর: মিথ্যা

শিক্ষণ নোট

মিথ্যা: অ্যাডওয়্যার সবসময় নিরীহ নয়; এর অনেকগুলো বিজ্ঞাপন লক্ষ্য করতে ব্রাউজিং ট্র্যাক করে।

8 প্রশ্ন 8 — সঠিক উত্তর: সত্য

শিক্ষণ নোট

সত্য: পরিষ্কার অফলাইন ব্যাকআপ মুক্তিপণ না দিয়েই এনক্রিপ্ট হওয়া ফাইল ফিরিয়ে আনে, যদিও চুরি হওয়া ডেটা তবুও ফাঁস হতে পারে।

9 প্রশ্ন 9 — সঠিক উত্তর: মিথ্যা

শিক্ষণ নোট

মিথ্যা: সিগনেচার স্ক্যানারের জন্য একটি পরিচিত নমুনা লাগে, তাই একেবারে নতুন জিরো-ডে ম্যালওয়্যার সেগুলোকে এড়িয়ে যেতে পারে।

10 প্রশ্ন 10 — সঠিক উত্তর: সত্য

শিক্ষণ নোট

ফাইললেস ম্যালওয়্যার সিস্টেম মেমোরিতে ক্ষতিকর স্ক্রিপ্ট চালায়, ডিস্কে ফাইল লেখা এড়িয়ে।

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. ট্রোজান	F 2. র‍্যানসমওয়্যার	A 3. স্পাইওয়্যার	H 4. রুটকিট
G 5. স্যান্ডবক্স	C 6. নিয়ন্ত্রণ	E 7. ওয়ার্ম	B 8. ফাইললেস

চেকপয়েন্ট 3: উত্তর – মূল পরিভাষা

1 ট্রোজান	2 জিম্মি ম্যালওয়্যার	3 স্পাইওয়্যার	4 রুটকিট
5 স্যান্ডবক্স	6 কন্টেইনমেন্ট		

চেকপয়েন্ট 6, বিকল্প: উত্তর – শব্দ মিলান

1 D – ওয়ার্ম	2 F – অনলাইন	3 H – অনুমতি	4 G – সফটওয়্যার
5 B – জিম্মিম্যালওয়্যার	6 C – স্পাইওয়্যার	7 A – ট্রোজান	8 E – ফাইললেস

শিক্ষকদের জন্য আলোচনা নোট

মূল পরিভাষা:
যাচাই করুন শিক্ষার্থীরা ট্রোজান, র‍্যানসমওয়্যার ও স্পাইওয়্যার 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।

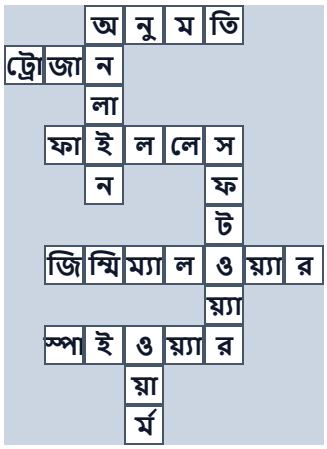
উৎস মূল্যায়ন:
শিক্ষার্থীদের ওয়ার্কশিটের উৎসে অন্তত একটি তথ্য যাচাই করতে বলুন এবং আলোচনা করুন কেন সংখ্যা, দাম ও নিয়ম সময়ের সঙ্গে বদলাতে পারে।

ধাঁধার উত্তরমালা ও শিক্ষকের নোট

শব্দ খোঁজার সমাধান

তা	বি	নি	ঘ	ল	মি	কে	ভ	ড	রা	র	ঈ	তি	গ	ই
সে	র	ভ	মা	ণ	জে	ঘ	চ	অ	ই	হ	ণ	দ	নে	স
ঝ	য়্যা	কা	জ	রা	ফ	ঘ	উ	সে	ন	জি	আ	ড	প	পা
ধ	ও	দ	জি	কি	না	লি	ই	রে	ফ	লা	চ	ট্রো	জা	ন
ব	ই	দি	শ	জা	জি	রা	দে	ট	মে	র	ই	ক	ও	সি
দ	স্পা	ঠ	হ	সা	ম্মি	শ	স	মে	দে	রা	কি	ন	য়া	খ
তে	না	নে	ছ	য	ম্যা	প	উ	ফ	অ	উ	খ	মা	র্ম	বা
স	য	ফ	বা	ম	ল	দে	তি	ভ	ট	ঘ	রে	ষ	ফ	ঘ
লে	দ	হ	স	ভ	ও	রি	মি	ঢ	ষ	ও	ষ	রি	সি	না
ল	তি	তা	ড	ঊ	য়্যা	নি	রা	কি	থ	সে	য়্যা	ঊ	লি	গ
ই	নি	জা	পি	খ	র	জি	লি	ট	ভ	ণ	জে	র	গ	অ
ফা	স	ঘ	রে	দি	মি	খ	পা	উ	অ	জে	কা	গ	নু	ম
আ	ঘ	কি	ঘ	ঝ	ণ	ধ	গ	সি	রি	শ	ছ	ম	দ	সে
জি	নি	ঝ	রে	পে	জ	আ	আ	রে	মা	স	তি	মে	তি	দে
রি	ফ	সি	তি	সে	খ	স	বে	উ	ট	সে	দি	দা	প	আ

ক্রসওয়ার্ডের সমাধান



ক্রসওয়ার্ড সমাধানের জন্য শিক্ষকের নির্দেশিকা

পাশাপাশি

1 পাশাপাশি: অনুমতি কোনো কাজ করার জন্য দেওয়া সম্মতি (4 অক্ষর)

2 পাশাপাশি: ট্রোজান নিরীহ বা কাজের প্রোগ্রামের ছদ্মবেশে থাকা ক্ষতিকর সফটওয়্যার (3 অক্ষর)

3 পাশাপাশি: ফাইললেস ডিস্ক স্ক্যানার ফাঁকি দিতে সরাসরি মেমোরিতে চলা ম্যালওয়্যার (5 অক্ষর)

5 পাশাপাশি: জিম্মিম্যালওয়্যার সিস্টেম স্টোরেজ এনক্রিপ্ট করে কী দেওয়ার বদলে অর্থ দাবি করা ম্যালওয়্যার (7 অক্ষর)

6 পাশাপাশি: স্পাইওয়্যার গোপনে ব্যবহারকারীর কার্যকলাপ ও ইনপুট নজরে রাখা ও রেকর্ড করা প্রোগ্রাম (5 অক্ষর)

উপর-নিচ

1 উপর-নিচ: অনলাইন ইন্টারনেটের সঙ্গে সংযুক্ত থাকার অবস্থা (5 অক্ষর)

4 উপর-নিচ: সফটওয়্যার কম্পিউটারকে কাজ করানোর নির্দেশমালা বা প্রোগ্রাম (6 অক্ষর)

7 উপর-নিচ: ওয়ার্ম মানুষের পদক্ষেপ ছাড়াই নেটওয়ার্ক জুড়ে নিজেকে নকল করে ছড়ানো ম্যালওয়্যার (3 অক্ষর)

এলোমেলো শব্দ ও সংকেতবার্তা সমাধানের উত্তরমালা

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

শব্দ সাজানোর উত্তরমালা

1. জানট্রো — **ট্রোজান**
2. স্পারয়্যাওই — **স্পাইওয়্যার**
3. লফাসলেই — **ফাইললেস**
4. রওটয়্যাসফ — **সফটওয়্যার**
5. ওরলম্যাজিয়্যাম্মি — **জিম্মিম্যালওয়্যার**
6. য়ার্মও — **ওয়ার্ম**
7. ইনঅলান — **অনলাইন**
8. অতিমনু — **অনুমতি**

গোপন সংকেত চ্যালেঞ্জের উত্তরমালা

"আচরণ নজরে ক্ষতিকর পেলোড ধরুন"

কেস স্টাডির উত্তর

A কেস স্টাডি 1: এন্টারপ্রাইজ র‍্যানসমওয়্যার পেলোড নিয়ন্ত্রণ

শিক্ষকের সমাধান

মূল্যায়ন নির্দেশিকা

শিক্ষার্থীদের উত্তরে নিচের বিষয়গুলো থাকা উচিত:

- পরিস্থিতি বিশ্লেষণ: একটি কর্পোরেট লোকাল এরিয়া নেটওয়ার্ক সক্রিয় র‍্যান্সমওয়্যারে আক্রান্ত হয়েছে। মূল ফাইল সার্ভারগুলোর ফাইল এক্সটেনশন .locked দেখাতে শুরু করেছে। নিয়ন্ত্রণ-নীতি প্রতিষ্ঠা করুন।
- প্রস্তাবিত কৌশল ও সমাধান: প্রভাবিত সব সার্ভার লোকাল এরিয়া নেটওয়ার্ক থেকে বিচ্ছিন্ন করুন। সক্রিয় প্রশাসনিক সেশন বন্ধ করুন। নিরাপদ, রাইট-লকড অফলাইন ব্যাকআপ সিস্টেম থেকে অক্ষত ফাইল পুনরুদ্ধার করুন।

B কেস স্টাডি 2: ফাইলহীন ম্যালওয়্যারের মেমরি ইনজেকশন

শিক্ষকের সমাধান

মূল্যায়ন নির্দেশিকা

শিক্ষার্থীদের উত্তরে নিচের বিষয়গুলো থাকা উচিত:

- পরিস্থিতি বিশ্লেষণ: একজন বিশ্লেষক স্ট্যান্ডার্ড প্রশাসনিক টুল ব্যবহার করে সরাসরি অস্থায়ী সিস্টেম RAM-এ চলমান সন্দেহজনক স্ক্রিপ্টিং প্যাটার্ন শনাক্ত করেন, কিন্তু ডিস্কে কোনো ক্ষতিকর ফাইল নেই।
- প্রস্তাবিত কৌশল ও সমাধান: আক্রান্ত এন্ডপয়েন্টগুলো আলাদা করুন এবং আগে একটি মেমরি ইমেজ সংগ্রহ করুন। PowerShell ও WMI লগ পর্যালোচনা করুন, AppLocker দিয়ে অননুমোদিত স্ক্রিপ্ট ব্লক করুন, তারপর পেলোড মুছতে রিবুট করুন।