Họ tên: _____ Ngày: _____ Điểm: _____

Kiến thức cơ bản về an ninh mạng và mối đe dọa trực tuyến Phòng ngừa

Mối đe dọa an ninh mạng, tường lửa mạng, xác thực đa yếu tố, khung bảo mật

TỔNG QUAN HỌC TẬP VỀ KIẾN THỨC CƠ BẢN AN NINH MẠNG

ĐÃ BẢO MẬT
MÃ HÓA DỮ LIỆU
Chuẩn AES 256 bit

TUÂN THỦ
TIÊU CHUẨN TOÀN CẦU
Khung GDPR và CCPA

ZERO TRUST
CHÍNH SÁCH TRUY CẬP
Xác thực đa yếu tố

Chào mừng bạn! Bộ hoạt động này hướng dẫn bạn về kiến thức cơ bản về an ninh mạng và cách phòng chống mối đe dọa trực tuyến. Bạn sẽ khám phá các mối đe dọa phần mềm độc hại, xác thực đa yếu tố, tường lửa mạng và các khung ứng phó sự cố.

CÁC ĐIỂM KIỂM TRA CỦA PHIẾU HỌC TẬP

- ☐ **Phần 1-4: Nắm vững an ninh mạng và phòng chống mối đe dọa.**
- ☐ **Phần 5-7: Giải các câu đố ô chữ và tìm từ.**
- ☐ **Phần 8-9: Giải các nghiên cứu tình huống và thử thách mật thư.**
- ☐ **Phần 10: Xem lại các trang câu hỏi thường gặp cơ bản và nâng cao.**
- ☐ **Phần 11: Khám phá 10 sự thật thú vị trong thực tế.**
- ☐ **Thưởng: thử thách Nghĩ nhanh.**

Mở Hướng dẫn an ninh mạng của VPN.com

URL: https://www.vpn.com/vi/an-ninh-mang/

Lộ trình học về kiến thức cơ bản về an ninh mạng của bạn

- Xác định các vector phổ biến của phần mềm độc hại, lừa đảo trực tuyến và xâm nhập mạng doanh nghiệp.
- Triển khai các biện pháp kiểm soát an ninh mạng tiêu chuẩn gồm MFA, tường lửa và bảo vệ điểm cuối.
- Đánh giá quy trình ứng phó sự cố nhằm giảm thiểu tác động của vi phạm dữ liệu.
- Phân tích các yếu tố rủi ro của tổ chức và sự phù hợp bảo mật theo hướng dẫn của NIST.
- Cấu hình các thực hành vệ sinh bảo mật để giảm thiểu tấn công nhồi thông tin đăng nhập tự động.

HƯỚNG DẪN VỀ AN NINH MẠNG

Trả lời các câu hỏi trắc nghiệm và đúng/sai, hoàn thành các câu điền vào chỗ trống bằng ngân hàng từ, ghép các định nghĩa, rồi giải ô chữ và tìm từ. Hãy vận dụng kiến thức của bạn về việc ngăn chặn mối đe dọa. Kết thúc với hoạt động thưởng Nghĩ nhanh.

KIẾN THỨC CƠ BẢN VỀ AN NINH MẠNG VÀ NGĂN CHẶN MỐI ĐE DỌA (GIỚI THIỆU)

An ninh mạng bảo vệ mạng, hệ thống và dữ liệu khỏi các cuộc tấn công kỹ thuật số trái phép. Xây dựng thói quen bảo mật vững chắc, cấu hình tường lửa, yêu cầu xác thực đa yếu tố và đào tạo nhân viên nhận biết mối đe dọa là những thành phần thiết yếu của phòng thủ mạng doanh nghiệp.

ĐỌC KỸ TỪNG ĐIỂM KIỂM TRA VÀ CHỌN HOẶC VIẾT CÂU TRẢ LỜI ĐÚNG.

Điểm kiểm tra 1: Thử thách trắc nghiệm

1. Mục tiêu chính của một cuộc tấn công lừa đảo trực tuyến (phishing) là gì?
   - A. Đánh cắp thông tin xác thực và dữ liệu nhạy cảm của người dùng
   - B. Nâng cao khả năng hiển thị của trang web trên công cụ tìm kiếm
   - C. Tăng băng thông mạng
   - D. Quản lý sao chép trung tâm dữ liệu dự phòng

2. Cơ chế nào cung cấp khả năng bảo vệ tài khoản mạnh nhất?
   - A. Xác thực đa yếu tố bằng khóa phần cứng
   - B. Mật khẩu phức tạp được cập nhật ba mươi ngày một lần
   - C. Giới hạn đăng nhập tài khoản trong giờ làm việc
   - D. Ẩn tên người dùng của tài khoản khỏi các danh bạ công khai

3. Điều gì xác định tải trọng lây nhiễm ransomware?
   - A. Mã hóa tệp hệ thống và đòi thanh toán
   - B. Âm thầm ghi lại thao tác gõ phím và gửi đến máy chủ từ xa
   - C. Chèn quảng cáo trái phép vào trình duyệt
   - D. Dùng tài nguyên CPU cục bộ để đào tiền mã hóa

4. Lỗ hổng zero-day ảnh hưởng đến các lớp phòng thủ bảo mật như thế nào?
   - A. Nhắm vào các lỗ hổng chưa được vá, chưa được biết đến
   - B. Tự động vô hiệu hóa tường lửa doanh nghiệp
   - C. Nó buộc hệ thống khởi động lại cứng
   - D. Nó không cần ngân sách để khắc phục

5. Khung nào điều chỉnh các biện pháp kiểm soát bảo mật của doanh nghiệp?
   - A. Hướng dẫn của Khung An ninh mạng NIST
   - B. Đặc tả lược đồ tài liệu W3C HTML5
   - C. Sổ tay hướng dẫn cài đặt trình điều khiển máy in
   - D. Các định nghĩa giao thức định tuyến của IETF

Điểm kiểm tra 2: Thử thách Đúng hoặc Sai

6 Câu hỏi đúng/sai 6

6. Tấn công phishing chỉ nhắm vào các tài khoản email cá nhân.

○ Đúng ○ Sai

7 Câu hỏi đúng/sai 7

7. Xác thực đa yếu tố giúp chặn các cuộc tấn công nhồi thông tin đăng nhập.

○ Đúng ○ Sai

8 Câu hỏi đúng/sai 8

8. Tường lửa kiểm tra lưu lượng mạng để chặn truy cập cổng trái phép.

○ Đúng ○ Sai

9 Câu hỏi đúng/sai 9

9. Khắc phục các cuộc khai thác zero-day đòi hỏi cập nhật định nghĩa diệt virus tiêu chuẩn.

○ Đúng ○ Sai

10 Câu hỏi đúng/sai 10

10. Honeypot là máy chủ mồi nhử dùng để dụ tội phạm mạng.

○ Đúng ○ Sai

Điểm kiểm tra 3: Điền thuật ngữ chính

Đọc từng câu dưới đây và điền vào chỗ trống thuật ngữ đúng từ Ngân hàng từ.

1. Quản trị viên mạng cài đặt một _____ để lọc lưu lượng đến.

2. Kẻ tấn công dùng một _____ lỗ hổng zero-day để vượt qua các bản vá hệ thống.

3. Kẻ tấn công gửi email giả mạo để thực hiện các chiến dịch _____ nhắm vào nhân viên.

4. Ransomware là một dạng _____ phá hoại khóa dữ liệu của người dùng.

5. Thiết lập _____ mạnh giúp giảm rủi ro bị đánh cắp thông tin xác thực.

6. Để bảo vệ liên lạc nhạy cảm, người dùng áp dụng các giao thức _____ .

NGÂN HÀNG TỪ VỰNG

AN TOÀN MẬT KHẨU | HONEYPOT | KHAI THÁC | LỪA ĐẢO TRỰC TUYẾN | MÃ HÓA | PHẦN MỀM ĐỘC HẠI | TƯỜNG LỬA | ỨNG PHÓ

Viết câu trả lời của bạn tại đây:

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

Điểm kiểm tra 4: Ghép nối khái niệm bảo mật

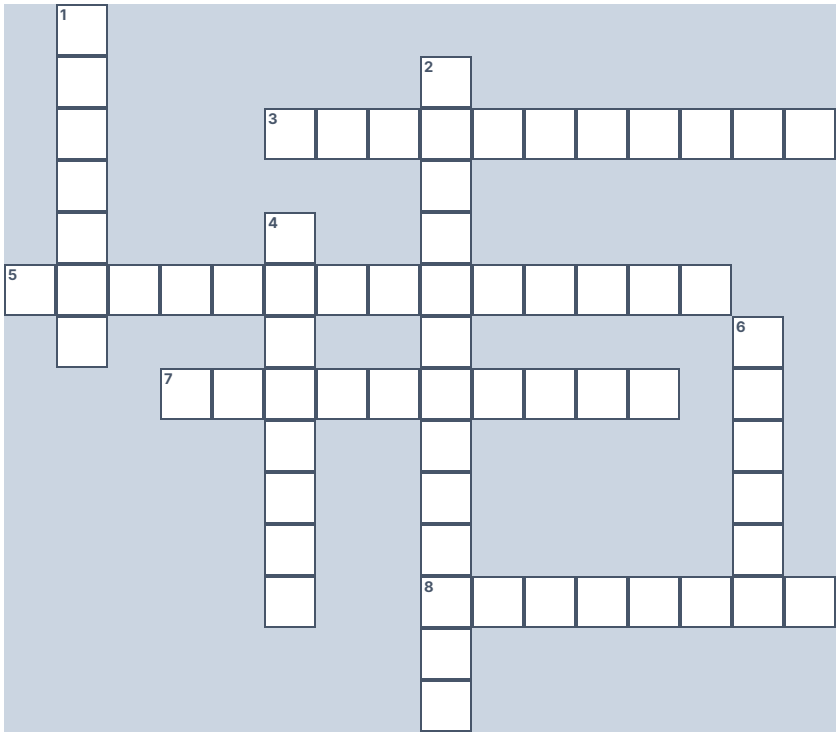
GHÉP ĐỊNH NGHĨA

Ghép mỗi thuật ngữ từ vựng ở bên trái với định nghĩa đúng ở bên phải bằng cách nhập chữ cái tương ứng (A-H) vào ô nhập liệu.

☐	1. Mối đe dọa mã độc tống tiền	A	Các hướng dẫn có cấu trúc như NIST dùng để quản lý rủi ro an ninh mạng.
☐	2. Xác thực đa yếu tố	B	Kế hoạch có cấu trúc để xử lý và giảm thiểu các sự cố vi phạm bảo mật.
☐	3. Khai thác lỗ hổng zero-day	C	Rào chắn mạng lọc lưu lượng dựa trên các quy tắc bảo mật.
☐	4. Honeypot mồi nhử	D	Phần mềm độc hại mã hóa dữ liệu và đòi tiền để giải mã.
☐	5. Tường lửa chống xâm nhập	E	Khai thác lỗ hổng bảo mật trước khi nhà cung cấp phát hành bản vá.
☐	6. Ứng phó sự cố	F	Các phương pháp hay nhất để quản lý thông tin xác thực và khóa xác thực.
☐	7. Vệ sinh mật khẩu	G	Xác thực bảo mật yêu cầu từ hai yếu tố xác thực trở lên.
☐	8. Khung bảo mật	H	Hệ thống mồi nhử được thiết lập để dụ và phân tích kẻ tấn công.

Điểm kiểm tra 5: Trò chơi ô chữ

Giải ô chữ bằng cách nhập chữ cái vào các ô trắng đang hoạt động. Các số tương ứng với các gợi ý bên dưới.



HÀNG NGANG

3. Hướng dẫn có cấu trúc như NIST dùng để quản lý rủi ro mạng (11)

5. Xác thực bảo mật yêu cầu hai hoặc nhiều yếu tố xác thực (14)

7. Phần mềm độc hại mã hóa dữ liệu và đòi tiền để giải mã (10)

8. Hệ thống mồi nhử được dựng lên để dụ và phân tích các tác nhân độc hại (8)

HÀNG DỌC

1. Khai thác lỗ hổng nhắm tới trước khi nhà cung cấp phát hành bản vá (7)

2. Thực hành tốt nhất để quản lý thông tin xác thực và khóa xác thực (13)

4. Rào chắn mạng lọc lưu lượng theo các quy tắc bảo mật (8)

6. Kế hoạch có cấu trúc để xử lý và giảm thiểu các vụ xâm phạm bảo mật (6)

Điểm kiểm tra 5, phương án khác: Gợi ý ô chữ dễ tiếp cận

Người dùng trình đọc màn hình và bàn phím có thể nhập trực tiếp đáp án ô chữ vào các trường văn bản bên dưới.

HÀNG NGANG

3 hàng ngang: Hướng dẫn có cấu trúc như NIST dùng để quản lý rủi ro mạng (11 chữ cái):

5 hàng ngang: Xác thực bảo mật yêu cầu hai hoặc nhiều yếu tố xác thực (14 chữ cái):

7 hàng ngang: Phần mềm độc hại mã hóa dữ liệu và đòi tiền để giải mã (10 chữ cái):

8 hàng ngang: Hệ thống mồi nhử được dựng lên để dụ và phân tích các tác nhân độc hại (8 chữ cái):

HÀNG DỌC

1 hàng dọc: Khai thác lỗ hổng nhắm tới trước khi nhà cung cấp phát hành bản vá (7 chữ cái):

2 hàng dọc: Thực hành tốt nhất để quản lý thông tin xác thực và khóa xác thực (13 chữ cái):

4 hàng dọc: Rào chắn mạng lọc lưu lượng theo các quy tắc bảo mật (8 chữ cái):

6 hàng dọc: Kế hoạch có cấu trúc để xử lý và giảm thiểu các vụ xâm phạm bảo mật (6 chữ cái):

Điểm kiểm tra 6: Tìm từ ẩn

Tìm 8 thuật ngữ từ vựng chính ẩn trong lưới bên dưới. Các từ có thể nằm ngang, dọc hoặc chéo.

U I R Q U P Y D Ê D Q Â A K Ô
Â Â Y L T O P Y E N O H I U Z
H P S A Ư N G P H O Q Ư H E L
K L E Ê M Ê P Đ K R K P R Ư Ê
T Â M O A B G N U H K O Ă S Đ
Â X N X Ư Q Ê R V A D Ô T N N
M Y O G Ô R Ê Ô T A S O S S I
N A D O M K Ă N Y T Đ E Ô Ơ Ư
A X H I T H X U V Ô I G Y G H
O M A D A Ư L G N Ơ Ư T G Ă R
T X A C T H Ư C Đ A Y Ê U T Ô
N A H D U D I Y I C K Ơ M H A
A Đ R A N S O M W A R E O I N
B M Â B Ê G Ă Ă O P L Ô U S G
X Đ X Q E V Ư Ê D P S N S I P

DANH SÁCH TỪ VỰNG

RANSOMWARE XACTHƯCĐAYÊUTÔ ZERODAY HONEYPOT TƯƠNGLƯA
ỨNGPHO ANTOANMÂTKHÂU KHUNGBAOMÂT

Điểm kiểm tra 6, phương án khác: Ghép từ vựng dễ tiếp cận

Ghép từng thuật ngữ trong số 8 thuật ngữ từ vựng ở phần Tìm từ với định nghĩa đúng bằng cách viết chữ cái (A-H) vào chỗ trống.

THUẬT NGỮ TỪ VỰNG
A. RANSOMWARE
B. XACTHƯCĐAYÊUTÔ
C. ZERODAY
D. HONEYPOT
E. TƯƠNGLƯA
F. ƯNGPHO
G. ANTOANMÂTKHÂU
H. KHUNGBAOMÂT

ĐỊNH NGHĨA VÀ CÁC TRƯỜNG GHÉP
1. Rào chắn mạng lọc lưu lượng theo các quy tắc bảo mật.
2. Kế hoạch có cấu trúc để xử lý và giảm thiểu các vụ xâm phạm bảo mật.
3. Phần mềm độc hại mã hóa dữ liệu và đòi tiền để giải mã.
4. Xác thực bảo mật yêu cầu hai hoặc nhiều yếu tố xác thực.
5. Thực hành tốt nhất để quản lý thông tin xác thực và khóa xác thực.
6. Hướng dẫn có cấu trúc như NIST dùng để quản lý rủi ro mạng.
7. Khai thác lỗ hổng nhắm tới trước khi nhà cung cấp phát hành bản vá.
8. Hệ thống mồi nhử được dựng lên để dụ và phân tích các tác nhân độc hại.

Điểm kiểm tra 7: Thử thách từ bị xáo trộn

Sắp xếp lại các chữ cái bên dưới để tìm ra các khái niệm và thuật ngữ chính về an ninh mạng. Viết đáp án của bạn vào các ô nhập đã cung cấp.

1. RWMOARAESN
2. ZRYADOE
3. NƯTGLAƯƠ
4. NÂTTÂAUMH KANO
5. YCUAĐAHÔƯÊ CXTT
6. OTEPHYON
7. HƯPOGN
8. MATBUKGHÂ ON

Hoạt động thưởng: Nghĩ nhanh

3 CÂU TRẢ LỜI CHO MỖI CHỦ ĐỀ. AI HOÀN THÀNH DANH SÁCH TRƯỚC SẼ THẮNG.

1	Những nghề trong lĩnh vực an ninh mạng			
2	Lý do cập nhật phần mềm			
3	Những thứ tường lửa có thể chặn			
4	Những dấu hiệu cảnh báo trong một email			
5	Những thứ bạn sao lưu			
6	Những loại tấn công mạng nổi tiếng			
7	Những thứ honeypot có thể nhử vào			
8	Những thông tin bạn không bao giờ nên chia sẻ			
9	Những dấu hiệu máy tính bị nhiễm			
10	Những bộ phim hoặc chương trình về tin tặc			
11	Những lớp bảo mật bạn có thể xây dựng			
12	Những điều cần luyện tập trong một buổi diễn tập bảo mật			
13	Những công cụ bảo mật bạn biết			
14	Những người bạn có thể nhờ giúp về CNTT			
15	Những từ bắt đầu bằng 'cyber'			

Điểm kiểm tra 8: Nghiên cứu tình huống về an ninh mạng

Hãy vận dụng các khái niệm bạn đã học để giải các tình huống thực tế dưới đây.

NGHIÊN CỨU TÌNH HUỐNG 1: CHIẾN LƯỢC KHÔI PHỤC SAU MÃ ĐỘC TỐNG TIỀN

👨‍💻

Tình huống: Mạng công ty bị nhiễm mã độc tống tiền, khóa các cơ sở dữ liệu quan trọng. Kẻ tấn công đòi khoản thanh toán tiền mã hóa $100,000. Công ty có các bản sao lưu ngoại tuyến từ 24 giờ trước.

Câu hỏi thảo luận: Phân tích rủi ro khi trả tiền và đánh giá chiến lược khôi phục.

NGHIÊN CỨU TÌNH HUỐNG 2: PHÒNG CHỐNG TẤN CÔNG NHỒI THÔNG TIN ĐĂNG NHẬP

👨‍💻

Tình huống: Một dịch vụ trực tuyến gặp cuộc tấn công nhồi thông tin đăng nhập, khi tin tặc thử hàng triệu cặp tên người dùng/mật khẩu bị đánh cắp từ các trang web khác.

Câu hỏi thảo luận: Hãy trình bày chi tiết cơ chế của cuộc tấn công này, và nêu hai hệ thống phòng thủ.

Điểm kiểm tra 9: Giải mã mật thư

Chuyên gia an ninh mạng bảo vệ tài sản mạng khỏi các tác nhân đe dọa trực tuyến. Hãy dùng bảng khóa Chữ-Số bên dưới để giải mã thông điệp bằng cách viết các chữ cái tương ứng vào chỗ trống.

KHÓA MÃ HÓA CHỮ SANG SỐ

A=1 Ă=2 Â=3 B=4 C=5 D=6 Đ=7 E=8 Ê=9 G=10

H=11 I=12 K=13 L=14 M=15 N=16 O=17 Ô=18 Ơ=19 P=20

Q=21 R=22 S=23 T=24 U=25 Ư=26 V=27 X=28 Y=29

4	1	17		27	9		11	9		24	11	18	16	10		4	2	16	10
28	1	5		24	11	26	5		7	1		29	9	25		24	18		

Thông điệp đã giải mã:

MẸO: MỖI SỐ ĐẠI DIỆN CHO VỊ TRÍ CỦA CHỮ CÁI ĐÓ TRONG BẢNG CHỮ CÁI (VÍ DỤ 1 = A, 2 = B, 29 = Y).

Điểm kiểm tra 10: Câu hỏi thường gặp cơ bản về an ninh mạng (Phần A)

Xem lại các câu hỏi và câu trả lời thường gặp về cách giảm thiểu các mối đe dọa trực tuyến.

Q1: Mục tiêu chính của an ninh mạng là gì?

Mục tiêu chính là bảo vệ mạng, thiết bị và dữ liệu khỏi truy cập trái phép, tấn công và hư hại ngẫu nhiên.

Q2: Phishing khác spear phishing như thế nào?

Phishing là chiến dịch email diện rộng nhắm vào người dùng ngẫu nhiên, còn spear phishing nhắm vào cá nhân cụ thể bằng dữ liệu được cá nhân hóa.

Q3: Tường lửa mạng là gì?

Tường lửa là hệ thống bảo mật mạng giám sát và lọc lưu lượng đi vào và đi ra dựa trên các quy tắc bảo mật được xác định trước.

Q4: Vì sao xác thực đa yếu tố (MFA) là cần thiết?

MFA bổ sung một lớp phòng thủ quan trọng, ngăn truy cập ngay cả khi kẻ tấn công đánh cắp hoặc bẻ khóa thông tin đăng nhập mật khẩu chính.

Q5: Điều gì định nghĩa một virus máy tính?

Virus là phần mềm độc hại tự sao chép, bám vào các tệp sạch và lây lan qua các hệ thống khi được thực thi.

Điểm kiểm tra 10: Câu hỏi thường gặp cơ bản về an ninh mạng (Phần B)

Xem lại các câu hỏi và câu trả lời thường gặp về cách giảm thiểu các mối đe dọa trực tuyến.

Q6: Ransomware khóa dữ liệu cục bộ như thế nào?

Ransomware dùng các thuật toán mật mã để mã hóa tệp của người dùng, khiến chúng không thể đọc được cho đến khi áp dụng khóa giải mã.

Q7: Lỗ hổng zero-day là gì?

Zero-day là lỗ hổng bảo mật trong phần mềm mà nhà cung cấp chưa biết, nên không có thời gian phát triển bản vá trước khi bị khai thác.

Q8: Khuôn khổ NIST đóng vai trò gì?

Khung NIST cung cấp các hướng dẫn và tiêu chuẩn tự nguyện để giúp các tổ chức quản lý và giảm rủi ro an ninh mạng.

Q9: Kế hoạch ứng phó sự cố bảo mật là gì?

Đây là một bộ quy trình được lập thành văn bản để phát hiện, ngăn chặn và khôi phục sau các vụ vi phạm bảo mật và xâm phạm mạng.

Q10: Kỹ thuật xã hội khai thác người dùng như thế nào?

Kỹ thuật xã hội dùng thao túng tâm lý để lừa nhân viên tiết lộ mật khẩu hoặc tải các tệp độc hại.

Điểm kiểm tra 10: Câu hỏi thường gặp nâng cao về bảo mật (Phần C)

Khám phá các khía cạnh kỹ thuật nâng cao của khung bảo mật, phân tích phần mềm độc hại và tuân thủ dữ liệu.

Q1: Tấn công DDoS làm quá tải máy chủ web như thế nào?

Tấn công DDoS điều phối hàng triệu thiết bị botnet bị chiếm quyền để làm ngập máy chủ bằng lưu lượng, làm cạn kiệt giới hạn băng thông và CPU.

Q2: Sự khác biệt giữa mã hóa đối xứng và bất đối xứng là gì?

Mã hóa đối xứng dùng một khóa duy nhất để mã hóa và giải mã, trong khi mã hóa bất đối xứng dùng một cặp khóa công khai và riêng tư.

Q3: Tin tặc thực hiện tấn công SQL injection như thế nào?

Kẻ tấn công nhập các lệnh SQL độc hại vào trường biểu mẫu, đánh lừa cơ sở dữ liệu phía sau để tiết lộ hồ sơ người dùng trái phép.

Q4: Di chuyển ngang trong các vụ xâm nhập mạng là gì?

Đây là kỹ thuật trong đó kẻ tấn công khai thác quyền truy cập máy chủ ban đầu để xâm phạm các hệ thống khác được kết nối trong mạng nội bộ.

Q5: Giả mạo DNS chuyển hướng lưu lượng web như thế nào?

Giả mạo DNS làm thay đổi bản ghi bộ nhớ đệm của máy chủ tên miền, đưa người dùng hợp lệ tới các trang web giả mạo thay vì tên miền mục tiêu.

Điểm kiểm tra 10: Câu hỏi thường gặp nâng cao về bảo mật (Phần D)

Khám phá các khía cạnh kỹ thuật nâng cao của khung bảo mật, phân tích phần mềm độc hại và tuân thủ dữ liệu.

Q6: Token bảo mật phần cứng là gì?

Đây là thiết bị vật lý (như YubiKey) tạo ra các bằng chứng xác thực mật mã, mang lại khả năng phòng thủ tối đa trước lừa đảo từ xa.

Q7: Các nhóm bảo mật dùng honeypot mồi nhử như thế nào?

Các nhóm triển khai máy chủ mồi nhử không thuộc môi trường sản xuất để phát hiện sớm các vụ xâm nhập và phân tích mẫu tấn công của các đối tượng trái phép.

Q8: Nguyên tắc đặc quyền tối thiểu là gì?

Đây là tiêu chuẩn bảo mật hạn chế quyền truy cập của người dùng ở mức tối thiểu tuyệt đối cần thiết để thực hiện vai trò công việc.

Q9: Tấn công trung gian (Man-in-the-Middle) khai thác các kết nối như thế nào?

Kẻ tấn công chặn và thay đổi thông tin liên lạc giữa hai thiết bị trên mạng không mã hóa, đánh cắp mã thông báo phiên và thông tin xác thực.

Q10: Các chỉ báo xâm phạm (IOC) là gì?

IOC là các manh mối pháp y, chẳng hạn như thay đổi registry bất thường hoặc lưu lượng IP giả mạo, cho thấy hệ thống đã bị xâm nhập.

Phần 11: 10 sự thật và hiểu biết thực tế về an ninh mạng

Xem lại các sự thật thực tế về vi phạm bảo mật, cơ chế phòng thủ và tiêu chuẩn tuân thủ.

1. THÔNG TIN VỀ AN NINH

Kẻ tấn công liên tục quét Internet để tìm máy chủ có lỗ hổng và gửi email lừa đảo trực tuyến (phishing) vào hộp thư của nhân viên.

2. THÔNG TIN VỀ AN NINH

Lỗi do con người, chẳng hạn nhấp vào liên kết lừa đảo, là yếu tố thường gặp trong các vụ rò rỉ dữ liệu, đó là lý do việc đào tạo rất quan trọng.

3. THÔNG TIN VỀ AN NINH

Chi phí vi phạm dữ liệu gồm tiền phạt pháp lý, mất khách hàng, điều tra và khắc phục, và có thể lên tới hàng triệu đô la.

4. THÔNG TIN VỀ AN NINH

MFA chống phishing, chẳng hạn khóa bảo mật phần cứng, là loại MFA mạnh nhất và là tiêu chuẩn mà CISA khuyến nghị. [2]

5. THÔNG TIN VỀ AN NINH

Ransomware vẫn là mối đe dọa lớn đối với mạng doanh nghiệp, và CISA khuyến nghị sao lưu ngoại tuyến, được mã hóa như một biện pháp phòng vệ chính. [4]

6. THÔNG TIN VỀ AN NINH

Khung An ninh mạng NIST 2.0 (2024) có sáu chức năng cốt lõi: Quản trị, Xác định, Bảo vệ, Phát hiện, Ứng phó, Phục hồi. [1]

7. THÔNG TIN VỀ BẢO MẬT

Bot nhồi thông tin đăng nhập thử hàng loạt các cặp tên người dùng và mật khẩu bị rò rỉ trên các cổng đăng nhập ngân hàng và thương mại điện tử.

8. THÔNG TIN VỀ BẢO MẬT

Thị trường khai thác zero-day tồn tại trên toàn thế giới, nơi các lỗ hổng mức độ nghiêm trọng cao có thể được bán với giá lớn trước khi được vá.

9. THÔNG TIN VỀ BẢO MẬT

Hệ thống mồi nhử honeypot báo động xâm nhập ngay lập tức vì người dùng hợp pháp không có lý do gì để truy cập nó.

10. THÔNG TIN VỀ AN NINH

Transport Layer Security (TLS) mã hóa các phiên trình duyệt, ngăn việc đánh hơi gói tin trên mạng Wi-Fi công cộng.

Tài liệu tham khảo kỹ thuật và nguồn

Tài liệu học tập và các câu đố tương tác được biên soạn từ các tiêu chuẩn toàn cầu của NIST, OWASP và tuân thủ quyền riêng tư dữ liệu.

TÀI LIỆU THAM KHẢO HỌC THUẬT VÀ NGÀNH

[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

Đáp án: Điểm kiểm tra 1 – Trắc nghiệm

1 **Tấn công phishing** PHISHING — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Các chiến dịch phishing cố gắng đánh cắp thông tin đăng nhập và dữ liệu nhạy cảm của người dùng bằng email giả mạo. Trích dẫn: OWASP Secure Configuration.

2 **Bảo vệ tài khoản** KHÓA MFA — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Xác thực đa yếu tố (MFA) bằng mã thông báo phần cứng cung cấp lớp phòng vệ truy cập tài khoản mạnh nhất. Trích dẫn: NIST Digital Identity.

3 **Mối đe dọa ransomware** RANSOMWARE — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Ransomware mã hóa các hệ thống và dữ liệu quan trọng, đòi thanh toán bằng tiền mã hóa để đổi lấy khóa giải mã. Trích dẫn: Center for Internet Security (CIS).

4 **Lỗ hổng zero-day** ZERO-DAY — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Các mối đe dọa zero-day khai thác những lỗ hổng bảo mật chưa được vá, chưa được biết đến trước khi nhà cung cấp phát hành bản vá. Trích dẫn: OWASP Secure Configuration.

5 **Các khung bảo mật** KHUNG LÀM VIỆC — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Các khung như NIST cung cấp hướng dẫn có cấu trúc để giúp tổ chức quản lý và giảm rủi ro an ninh mạng. Trích dẫn: NIST Digital Identity. [1]

Đáp án: Điểm kiểm tra 2 – Đúng hay Sai

6 **Phishing có mục tiêu** PHISHING — **Đáp án đúng: Sai**

GHI CHÚ CHO GIÁO VIÊN

Tấn công phishing nhắm vào cả mạng doanh nghiệp lẫn tài khoản cá nhân để mở rộng các hướng khai thác. Trích dẫn: OWASP Secure Configuration.

7 **Câu hỏi 7** — **Đáp án đúng: Đúng**

GHI CHÚ CHO GIÁO VIÊN

MFA yêu cầu một yếu tố thứ hai, nên chỉ riêng mật khẩu bị đánh cắp thường không đủ để đăng nhập.

8 **Tường lửa lưu lượng** TƯỜNG LỬA — **Đáp án đúng: Đúng**

GHI CHÚ CHO GIÁO VIÊN

Tường lửa kiểm tra và chặn lưu lượng trên các cổng mạng cụ thể để lọc bỏ các kết nối trái phép. Trích dẫn: Center for Internet Security (CIS).

9 **Ứng phó zero-day** ZERO-DAY — **Đáp án đúng: Sai**

GHI CHÚ CHO GIÁO VIÊN

Khắc phục lỗ hổng zero-day đòi hỏi bản vá mã và lọc WAF vì chưa có chữ ký. Nguồn: OWASP Secure Configuration.

10 **Honeypot mồi nhử** HONEYPOT — **Đáp án đúng: Đúng**

GHI CHÚ CHO GIÁO VIÊN

Honeypot là các máy chủ đánh lừa được đội bảo mật dùng để dụ, cảnh báo và nghiên cứu các tác nhân độc hại. Trích dẫn: Center for Internet Security (CIS).

Đáp án từ vựng và thang chấm điểm

Thang chấm điểm cho giáo viên: Cho 1 điểm với mỗi cặp ghép đúng (tổng cộng 8 điểm) và mỗi thuật ngữ ngữ cảnh (tổng cộng 6 điểm).

ĐIỂM KIỂM TRA 4: ĐÁP ÁN – GHÉP NỐI KHÁI NIỆM

D 1. Mối đe dọa mã độc tống tiền	G 2. Xác thực đa yếu tố	E 3. Khai thác lỗ hổng zero-day	H 4. Honeypot mồi nhử
C 5. Tường lửa chống xâm nhập	B 6. Ứng phó sự cố	F 7. Vệ sinh mật khẩu	A 8. Khung bảo mật

ĐIỂM KIỂM TRA 3: ĐÁP ÁN – THUẬT NGỮ CHÍNH

1 TƯỜNG LỬA	2 KHAI THÁC	3 LỪA ĐẢO TRỰC TUYẾN	4 PHẦN MỀM ĐỘC HẠI
5 AN TOÀN MẬT KHẨU	6 MÃ HÓA		

ĐIỂM KIỂM TRA 6, PHƯƠNG ÁN KHÁC: ĐÁP ÁN – GHÉP TỪ

1 E – TƯƠNGLỬA	2 F – ỨNGPHO	3 A – RANSOMWARE	4 B – XACTHƯCĐAYÊUTÔ
5 G – ANTOANMÂTKHÂU	6 H – KHUNGBAOMÂT	7 C – ZERODAY	8 D – HONEYPOT

GHI CHÚ THẢO LUẬN CHO GIÁO VIÊN

Thuật ngữ chính:
Kiểm tra xem học sinh có giải thích được Mối đe dọa mã độc tống tiền, Xác thực đa yếu tố và Khai thác lỗ hổng zero-day bằng lời của mình và nêu một ví dụ cho mỗi thuật ngữ hay không.

Nghiên cứu tình huống:
Yêu cầu học sinh dùng dữ kiện trong phiếu, không dùng phỏng đoán, để chứng minh khuyến nghị của mình.

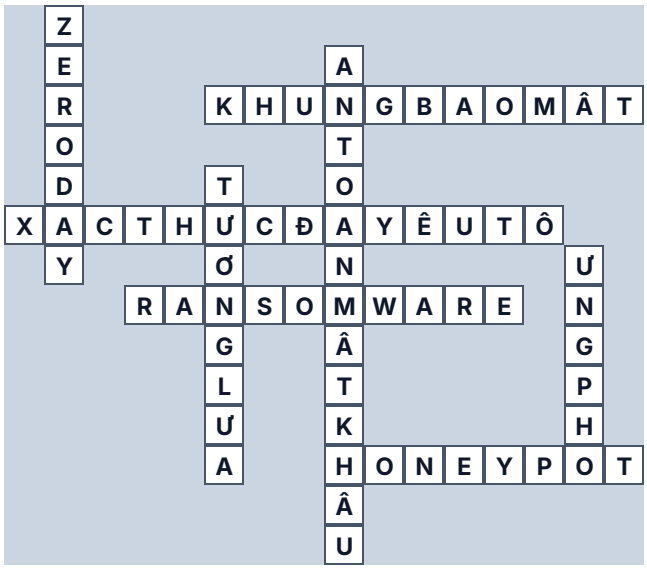
Đánh giá nguồn:
Yêu cầu học sinh kiểm chứng ít nhất một nhận định trong các nguồn của phiếu và thảo luận vì sao số liệu, giá cả và quy định có thể thay đổi theo thời gian.

Đáp án câu đố và ghi chú cho giáo viên

ĐÁP ÁN TÌM TỪ

U	I	R	Q	U	P	Y	D	Ê	D	Q	Â	A	K	Ô
Â	Â	Y	L	T	O	P	Y	E	N	O	H	I	U	Z
H	P	S	A	Ư	N	G	P	H	O	Q	Ư	H	E	L
K	L	E	Ê	M	Ê	P	Đ	K	R	K	P	R	Ư	Ê
T	Â	M	O	A	B	G	N	U	H	K	O	Ă	S	Đ
Â	X	N	X	Ư	Q	Ê	R	V	A	D	Ô	T	N	N
M	Y	O	G	Ô	R	Ê	Ô	T	A	S	O	S	S	I
N	A	D	O	M	K	Ă	N	Y	T	Đ	E	Ô	Ơ	Ư
A	X	H	I	T	H	X	U	V	Ô	I	G	Y	G	H
O	M	A	D	A	Ư	L	G	N	Ơ	Ư	T	G	Ă	R
T	X	A	C	T	H	Ư	C	Đ	A	Y	Ê	U	T	Ô
N	A	H	D	U	D	I	Y	I	C	K	Ơ	M	H	A
A	Đ	R	A	N	S	O	M	W	A	R	E	O	I	N
B	M	Â	B	Ê	G	Ă	Ă	O	P	L	Ô	U	S	G
X	Đ	X	Q	E	V	Ư	Ê	D	P	S	N	S	I	P

ĐÁP ÁN Ô CHỮ



HƯỚNG DẪN CHO GIÁO VIÊN VỀ ĐÁP ÁN Ô CHỮ

HÀNG NGANG

3 hàng ngang: KHUNGBAOMÂT Hướng dẫn có cấu trúc như NIST dùng để quản lý rủi ro mạng (11 chữ cái)

5 hàng ngang: XACTHƯCĐAYÊUTÔ Xác thực bảo mật yêu cầu hai hoặc nhiều yếu tố xác thực (14 chữ cái)

7 hàng ngang: RANSOMWARE Phần mềm độc hại mã hóa dữ liệu và đòi tiền để giải mã (10 chữ cái)

8 hàng ngang: HONEYPOT Hệ thống mồi nhử được dựng lên để dụ và phân tích các tác nhân độc hại (8 chữ cái)

HÀNG DỌC

1 hàng dọc: ZERODAY Khai thác lỗ hổng nhắm tới trước khi nhà cung cấp phát hành bản vá (7 chữ cái)

2 hàng dọc: ANTOANMÂTKHÂU Thực hành tốt nhất để quản lý thông tin xác thực và khóa xác thực (13 chữ cái)

4 hàng dọc: TƯỜNGLỬA Rào chắn mạng lọc lưu lượng theo các quy tắc bảo mật (8 chữ cái)

6 hàng dọc: ỨNGPHÓ Kế hoạch có cấu trúc để xử lý và giảm thiểu các vụ xâm phạm bảo mật (6 chữ cái)

Đáp án: Từ bị xáo trộn và mật thư

Đáp án cho hoạt động sắp xếp lại chữ cái từ vựng và Thử thách mật mã bí mật.

ĐÁP ÁN SẮP XẾP LẠI CHỮ CÁI

1. RWMOARAESN — **RANSOMWARE**
2. ZRYADOE — **ZERODAY**
3. NƯTGLAƯƠ — **TƯƠNGLỬA**
4. NÂTTÂAUMHKANO — **ANTOANMẬTKHẨU**
5. YCUAĐAHÔƯÊCXTT — **XACTHƯCĐAYÊUTÔ**
6. OTEPHYON — **HONEYPOT**
7. HƯPOGN — **ỨNGPHO**
8. MATBUKGHÂON — **KHUNGBAOMẬT**

KHÓA THỬ THÁCH MẬT THƯ BÍ MẬT

"BAO VÊ HÊ THÔNG BĂNG XAC THƯC ĐA YÊU TÔ"

Đáp án nghiên cứu tình huống

A Nghiên cứu tình huống 1: Chiến lược khôi phục sau mã độc tống tiền

Lời giải dành cho giáo viên

HƯỚNG DẪN CHẤM ĐIỂM

Câu trả lời của học sinh cần đề cập các điểm sau:

- Phân tích tình huống: Một mạng doanh nghiệp bị nhiễm ransomware, khóa các cơ sở dữ liệu quan trọng. Kẻ tấn công đòi khoản thanh toán 100.000 USD bằng tiền mã hóa. Công ty có các bản sao lưu ngoại tuyến từ 24 giờ trước.
- Chiến lược và giải pháp đề xuất: Rủi ro khi trả tiền: Việc trả tiền không bảo đảm giải mã được tệp, đánh dấu công ty là mục tiêu chịu trả tiền và tài trợ cho hoạt động tội phạm. Chiến lược khôi phục: Nhóm nên cô lập các máy chủ bị nhiễm, xóa sạch các máy chủ bị xâm nhập và khôi phục dữ liệu từ bản sao lưu ngoại tuyến. Họ phải vá vectơ truy cập ban đầu (lừa đảo trực tuyến (phishing) hoặc khai thác lỗ hổng) để ngăn tái nhiễm ngay lập tức.

B Nghiên cứu tình huống 2: Phòng chống tấn công nhồi thông tin đăng nhập

Lời giải dành cho giáo viên

HƯỚNG DẪN CHẤM ĐIỂM

Câu trả lời của học sinh cần đề cập các điểm sau:

- Phân tích tình huống: Một dịch vụ trực tuyến bị tấn công credential stuffing, trong đó tin tặc thử hàng triệu cặp tên người dùng/mật khẩu bị đánh cắp từ các trang khác.
- Chiến lược và giải pháp đề xuất: Cơ chế: Kẻ tấn công lợi dụng việc dùng lại mật khẩu trên nhiều trang, dùng bot tự động để đăng nhập vào tài khoản người dùng. Biện pháp phòng thủ: 1. Xác thực đa yếu tố (MFA) chặn các lần đăng nhập ngay cả khi mật khẩu đúng. 2. Áp dụng giới hạn tần suất và CAPTCHA chặn lưu lượng bot tự động gửi hàng loạt đến các điểm đăng nhập.