Họ tên: _____ Ngày: _____ Điểm: _____

Bảo mật và mã hóa Wi-Fi công cộng

Tấn công người đứng giữa, điểm truy cập giả mạo, bắt gói tin, đường hầm VPN và mã hóa HTTPS.

TỔNG QUAN BÀI HỌC VỀ BẢO MẬT WI-FI CÔNG CỘNG

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 bảo mật Wi-Fi công cộng. Bạn sẽ tìm hiểu về mạng không mã hóa, tấn công xen giữa (MitM), điểm truy cập giả mạo, nghe lén gói tin, đường hầm VPN và bảo mật truyền tải HTTPS.

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/bao-mat-wifi-cong-cong/

Lộ trình học về bảo mật Wi-Fi công cộng của bạn

- Xác định các rủi ro phổ biến của Wi-Fi công cộng, bao gồm nghe lén gói tin và điểm truy cập giả mạo.
- Triển khai các đường hầm mã hóa VPN để bảo mật dữ liệu khi truyền.
- Áp dụng HTTPS và cài đặt trình duyệt web an toàn cho nhân viên làm việc từ xa.

HƯỚNG DẪN VỀ BẢO MẬT WI-FI CÔNG CỘNG

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 bảo mật truy cập từ xa. Kết thúc với hoạt động thưởng Nghĩ nhanh.

BẢO MẬT WI-FI CÔNG CỘNG & BẢO VỆ DỮ LIỆU TRUYỀN TẢI (GIỚI THIỆU)

Các điểm phát Wi-Fi công cộng không mã hóa khiến lưu lượng mạng bị lộ trước việc đánh hơi gói tin và giả mạo Evil Twin. Việc buộc lưu lượng đi qua đường hầm mã hóa VPN an toàn và áp dụng các quy tắc HSTS chỉ HTTPS giúp bảo vệ các phiên khỏi bị chặn bắt trong mạng cục bộ.

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

Điểm kiểm tra 1: Thử thách trắc nghiệm

1 1. Tấn công xen giữa (Man-in-the-Middle, MitM) là gì?

- A. Chặn và thay đổi thông tin liên lạc giữa hai bên trên một mạng dùng chung
- B. Kỹ thuật trích xuất cơ sở dữ liệu nhắm vào hồ sơ người dùng
- C. Làm quá tải máy chủ web bằng các yêu cầu lưu lượng mạng
- D. Xóa sạch các ổ đĩa cứng cục bộ

2 2. Điểm truy cập giả mạo (Evil Twin) là gì?

- A. Điểm phát Wi-Fi độc hại được cấu hình cùng SSID với mạng hợp pháp
- B. Công cụ quản trị dùng để theo dõi bản sao lưu cơ sở dữ liệu
- C. Cấu hình cổng VPN an toàn
- D. Một bản ghi DNS ánh xạ các máy chủ thư được ủy quyền

3 3. VPN bảo vệ lưu lượng Wi-Fi công cộng như thế nào?

- A. Bọc mọi gói tin mạng trong một đường hầm mã hóa, khiến trình đánh hơi không đọc được
- B. Tự động chặn mọi yêu cầu kết nối đến
- C. Nó thay đổi địa chỉ MAC của card mạng vật lý
- D. Nó xóa các cookie đã lưu đệm trong trình duyệt web

4 4. Nghe lén gói tin (packet sniffing) là gì?

- A. Dùng công cụ phần cứng hoặc phần mềm để thu thập và ghi lại các gói tin mạng
- B. Quét các thư mục cục bộ để tìm tệp trùng lặp
- C. Hạn chế quyền đọc cơ sở dữ liệu theo vai trò người dùng
- D. Mã hóa ổ lưu trữ bằng khóa AES-256

5 5. Vai trò của HTTPS là gì?

- A. Mã hóa lưu lượng phiên giữa trình duyệt và máy chủ web
- B. Lọc các email đến tại cổng kết nối
- C. Nén hình ảnh để tải trang nhanh hơn
- D. Quản lý cấu trúc tệp trong bộ lưu trữ gắn mạng

Điểm kiểm tra 2: Thử thách Đúng hoặc Sai

6 Câu hỏi 6

6. Người dùng đã kết nối có thể dễ dàng thu thập dữ liệu văn bản thuần trên mạng Wi-Fi công cộng mở.

○ Đúng ○ Sai

7 Câu hỏi 7

7. Các điểm truy cập giả mạo (Evil Twin) luôn được quản trị viên mạng ủy quyền.

○ Đúng ○ Sai

8 Câu hỏi 8

8. VPN không hiệu quả trong việc bảo vệ lưu lượng khỏi việc đánh hơi gói tin trên mạng công cộng.

○ Đúng ○ Sai

9 Câu hỏi 9

9. HTTPS chỉ mã hóa đường dẫn URL, để tải trọng gói tin ở dạng văn bản thuần.

○ Đúng ○ Sai

10 Câu hỏi 10

10. Các điểm phát Wi-Fi dùng bảo mật WPA3 mang lại khả năng bảo vệ mạnh hơn các mạng mở, không có mật khẩu.

○ 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. Chiếm đoạt mật khẩu riêng tư trên Wi-Fi công cộng là hành vi _____ liên lạc.
2. Phân tích các gói thô trên mạng cục bộ là dùng kỹ thuật _____ .
3. Một điểm phát sóng giả mạo bắt chước Wi-Fi của khách sạn là một _____ .
4. Bảo vệ lưu lượng web khi truyền cần mã hóa bằng _____ .
5. Mã hóa toàn bộ dữ liệu đầu ra của mạng là dùng một ứng dụng khách _____ .
6. Một đường truyền thông được mã hóa qua các mạng công cộng là một _____ .

NGÂN HÀNG TỪ VỰNG

BẮT GÓI TIN | CHUẨN WPA | ĐƯỜNG HẦM | EVIL TWIN | HTTPS | NGHE LÉN | TƯỜNG LỬA | VPN

Viết câu trả lời của bạn tại đây:

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

Điểm kiểm tra 4: Ghép nối khái niệm bảo mật

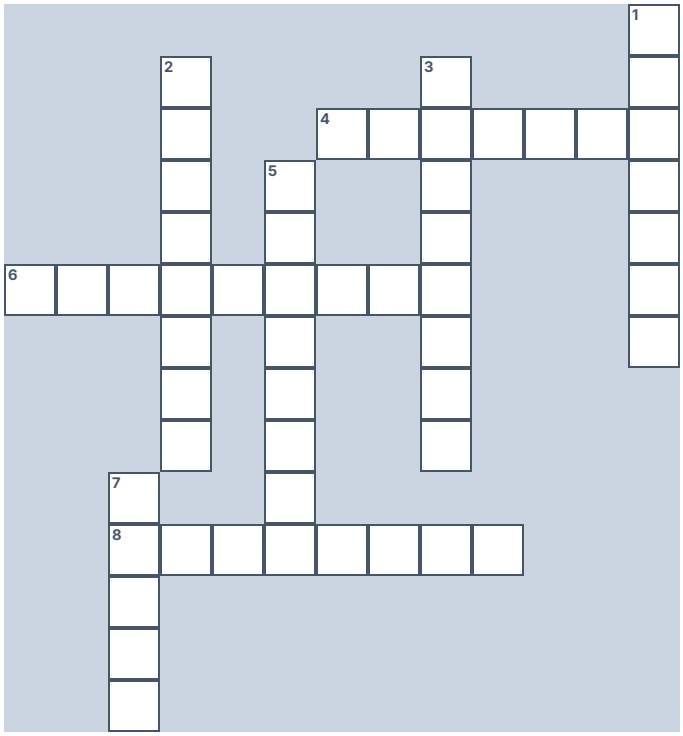
GHÉP ĐỊNH NGHĨA

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. CHẶN BẮT	A	Tiêu chuẩn bảo mật Wi-Fi hiện đại.
☐	2. NGHE LÉN GÓI TIN	B	Đường truyền dữ liệu an toàn khi truyền tải.
☐	3. EVIL TWIN	C	Lọc lưu lượng đến.
☐	4. HTTPS	D	Điểm phát sóng giả mạo bắt chước Wi-Fi.
☐	5. VPN	E	Đọc lưu lượng khi đang truyền.
☐	6. ĐƯỜNG HẦM	F	Bắt các gói dữ liệu mạng.
☐	7. WPA3	G	Mạng riêng ảo được mã hóa.
☐	8. TƯỜNG LỬA	H	Truyền tải web an toàn.

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

4. Đọc lưu lượng khi đang truyền (7)

6. Thu thập các gói dữ liệu mạng (9)

8. Lọc lưu lượng đến (8)

HÀNG DỌC

1. Mạng riêng ảo được mã hóa (7)

2. Đường dẫn dữ liệu an toàn khi truyền (8)

3. Chuẩn bảo mật Wi-Fi hiện đại (8)

5. Điểm phát sóng giả mạo bắt chước Wi-Fi (8)

7. Truyền tải web an toàn (5)

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

4 hàng ngang: Đọc lưu lượng khi đang truyền (7 chữ cái):

6 hàng ngang: Thu thập các gói dữ liệu mạng (9 chữ cái):

8 hàng ngang: Lọc lưu lượng đến (8 chữ cái):

HÀNG DỌC

1 hàng dọc: Mạng riêng ảo được mã hóa (7 chữ cái):

2 hàng dọc: Đường dẫn dữ liệu an toàn khi truyền (8 chữ cái):

3 hàng dọc: Chuẩn bảo mật Wi-Fi hiện đại (8 chữ cái):

5 hàng dọc: Điểm phát sóng giả mạo bắt chước Wi-Fi (8 chữ cái):

7 hàng dọc: Truyền tải web an toàn (5 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.

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

DANH SÁCH TỪ VỰNG

NGHELEN BẮTGOITIN EVILTWIN HTTPS MANGVPN ĐƯƠNGHÂM CHUẨNWPA TƯỜNGLỬA

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. NGHELEN
B. BĂTGOITIN
C. EVILTWIN
D. HTTPS
E. MANGVPN
F. ĐƯƠNGHÂM
G. CHUÂNWPA
H. TƯƠNGLƯA

ĐỊNH NGHĨA VÀ CÁC TRƯỜNG GHÉP
____ 1. Chuẩn bảo mật Wi-Fi hiện đại.
____ 2. Điểm phát sóng giả mạo bắt chước Wi-Fi.
____ 3. Thu thập các gói dữ liệu mạng.
____ 4. Đường dẫn dữ liệu an toàn khi truyền.
____ 5. Lọc lưu lượng đến.
____ 6. Đọc lưu lượng khi đang truyền.
____ 7. Mạng riêng ảo được mã hóa.
____ 8. Truyền tải web an toàn.

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. EENLNHG
2. LENVIWTI
3. GMVNNPA
4. ÂPAWNCHU
5. TOĂNIGBIT
6. PHTST
7. ĐMGHÂƯNƠ
8. NƯGATƯLƠ

Hoạt động thưởng: Nghĩ nhanh

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

1	Lý do cập nhật phần mềm			
2	Những thiết bị tự động kết nối với Wi-Fi			
3	Những thông tin bạn không bao giờ nên chia sẻ			
4	Những thói quen an toàn bạn có thể bắt đầu ngay hôm nay			
5	Những cách giữ an toàn ở quán cà phê			
6	Những thiết bị có thể bị tấn công			
7	Những thứ tin tặc có thể thấy trên Wi-Fi mở			
8	Những dấu hiệu của mạng Wi-Fi giả			
9	Những lựa chọn thay thế cho Wi-Fi công cộng			
10	Những dấu hiệu cảnh báo trong một email			
11	Những việc bạn không làm trên Wi-Fi công cộng			
12	Những nơi có Wi-Fi miễn phí			
13	Những cách bảo vệ tài khoản của bạn			
14	Những dấu hiệu máy tính bị nhiễm			
15	Những tên Wi-Fi có vẻ đáng ngờ			

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: NGĂN CHẶN NGHE LÉN GÓI TIN TRÊN WI-FI CÔNG CỘNG

👷

Tình huống: Một giám đốc kinh doanh làm việc từ xa kết nối với mạng Wi-Fi công cộng ở sân bay nhận thấy nhiều email kinh doanh nhạy cảm bị rò rỉ ngay sau khi gửi ở dạng văn bản thuần.

Câu hỏi thảo luận: Hãy phân tích các rủi ro của mạng công cộng, và nêu một giải pháp mã hóa lưu lượng.

NGHIÊN CỨU TÌNH HUỐNG 2: PHÒNG THỦ ĐIỂM PHÁT WI-FI GIẢ MẠO EVIL TWIN

👷

Tình huống: Kẻ tấn công triển khai một điểm truy cập không dây giả mạo tên 'CoffeeShop_Guest' bắt chước điểm phát sóng của một quán cà phê hợp pháp, thu thập lưu lượng mạng từ những khách không nghi ngờ.

Câu hỏi thảo luận: Hãy trình bày chi tiết các bước xác minh để phát hiện và chặn các điểm truy cập giả mạo.

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

15 1 11 17 1 14 26 25 14 26 19 16 10 15 1 16 10

5 18 16 10 5 18 16 10 4 2 16 10 27 20 16

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: Tại sao Wi-Fi công cộng không an toàn?

Wi-Fi công cộng mở không mã hóa lưu lượng trong không khí, nên những người ở gần có thể bắt được mọi dữ liệu không được bảo vệ. [2]

Q2: Bắt gói tin (packet sniffing) là gì?

Trình đánh hơi gói tin ghi lại dữ liệu thô chạy qua giao diện mạng, làm lộ mật khẩu dạng văn bản thuần và chi tiết lưu lượng.

Q3: Evil Twin là gì?

Điểm truy cập giả mạo do tin tặc dựng lên, mô phỏng tên và cài đặt của một điểm phát Wi-Fi cục bộ đáng tin cậy.

Q4: VPN bảo vệ tôi như thế nào?

Nó định tuyến lưu lượng của bạn qua một đường hầm được mã hóa, ẩn hoạt động duyệt web của bạn khỏi các công cụ nghe lén mạng cục bộ.

Q5: HTTPS có bảo vệ tôi trên Wi-Fi công cộng không?

Có, nó mã hóa dữ liệu trao đổi giữa trình duyệt và trang web, và VPN bổ sung thêm một lớp bảo vệ.

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: WPA3 là gì?

Tiêu chuẩn Wi-Fi Protected Access hiện đại, cung cấp mã hóa mạnh hơn và bảo vệ trước các cuộc tấn công từ điển ngoại tuyến. [1]

Q7: Wi-Fi công cộng có thể phát tán phần mềm độc hại không?

Có, kẻ tấn công có thể chặn lưu lượng và chèn các lời nhắc tải xuống độc hại (tải xuống tự động, drive-by downloads) vào phiên trình duyệt của bạn.

Q8: Rủi ro của việc chia sẻ tệp là gì?

Nếu bật chia sẻ tệp, những người dùng khác trên mạng công cộng có thể đọc hoặc sửa đổi thư mục cục bộ của bạn.

Q9: Captive portal là gì?

Trang đăng nhập mà mạng khách sạn hoặc quán cà phê dùng để cấp quyền truy cập internet, đôi khi có thể bị kẻ tấn công giả mạo.

Q10: Tôi có nên tắt Wi-Fi khi không sử dụng không?

Có, tắt Wi-Fi giúp thiết bị của bạn không tự động kết nối với các mạng không đáng tin cậy.

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 xen giữa (Man-in-the-Middle) khai thác DNS như thế nào?

Bằng cách dùng giả mạo DNS trên router độc hại để dẫn trình duyệt mục tiêu đến các trang đích lừa đảo trực tuyến (phishing) giống hệt thay vì tên miền thật.

Q2: Chiếm quyền phiên (session hijacking) là gì?

Kẻ tấn công đánh hơi cookie phiên không mã hóa trên Wi-Fi công cộng và nhập nó để bỏ qua đăng nhập bằng thông tin xác thực.

Q3: SSL stripping là gì?

Một cuộc tấn công MitM trong đó kẻ tấn công hạ cấp yêu cầu HTTPS an toàn của người dùng xuống HTTP không mã hóa, thu thập thông tin đăng nhập ở dạng văn bản thuần.

Q4: HSTS bảo vệ chống SSL stripping như thế nào?

HTTP Strict Transport Security buộc trình duyệt chỉ kết nối qua HTTPS và từ chối quay lại HTTP không mã hóa. [3]

Q5: VPN split-tunnel là gì?

Cấu hình chỉ định tuyến lưu lượng của doanh nghiệp qua VPN còn dữ liệu internet công cộng đi thẳng, có thể gây rủi ro lộ đường rò rỉ.

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: Vì sao WPA2 dễ bị tấn công KRACK?

Key Reinstallation Attack khai thác bắt tay bốn bước của WPA2 để giải mã các gói mà không cần mật khẩu Wi-Fi.

Q7: Cô lập máy khách (client isolation) là gì?

Cài đặt bảo mật của router ngăn các thiết bị Wi-Fi đang kết nối giao tiếp trực tiếp với nhau, chặn việc đánh hơi cục bộ.

Q8: Kẻ tấn công dùng máy chủ DNS giả mạo như thế nào?

Chúng cấu hình các router giả mạo để gán máy chủ DNS giả cho máy khách, cho phép chặn bắt và ghi lại mọi truy vấn web.

Q9: VPN có thể ẩn địa chỉ MAC cục bộ của tôi không?

Không. Địa chỉ MAC là định danh cục bộ ở lớp 2; hãy dùng cài đặt ngẫu nhiên hóa MAC (địa chỉ riêng tư) có sẵn của thiết bị thay thế.

Q10: Tấn công giả mạo cổng thông tin xác thực (captive portal) là gì?

Kẻ tấn công dựng cổng xác thực giả trên một điểm phát giả mạo để đánh cắp thông tin xác thực dưới vỏ bọc truy cập Wi-Fi miễn phí.

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

Nhân viên làm việc từ xa thường dùng Wi-Fi ở quán cà phê, khách sạn và sân bay, nơi họ không thể kiểm soát độ bảo mật của mạng.

2. THÔNG TIN VỀ AN NINH

Điểm phát giả mạo Evil Twin có thể sao chép chính xác tên và địa chỉ MAC của một mạng đáng tin cậy, gây nhầm lẫn cho các thiết bị.

3. THÔNG TIN VỀ AN NINH

Phần mềm bắt gói tin như Wireshark miễn phí và có thể hiển thị mật khẩu HTTP chưa mã hóa dưới dạng văn bản thuần.

4. THÔNG TIN VỀ AN NINH

Bảo mật WPA3 dùng cơ chế Xác thực đồng thời giữa các bên ngang hàng (SAE) để bảo vệ trước các cuộc tấn công dò mật khẩu cục bộ.

5. THÔNG TIN VỀ AN NINH

Các cuộc tấn công SSL stripping vượt qua các biện pháp bảo vệ HTTPS cơ bản bằng cách chặn các chuyển hướng HTTP ban đầu tại cổng mạng.

6. THÔNG TIN VỀ AN NINH

Các tiêu đề phản hồi HTTP Strict Transport Security (HSTS) ngăn trình duyệt quay lại kết nối HTTP không mã hóa. [3]

7. THÔNG TIN VỀ BẢO MẬT

Tắt 'Auto-Connect' giúp ngăn điện thoại thông minh kết nối với các mạng giả mạo trông giống thật ở nơi công cộng.

8. THÔNG TIN VỀ BẢO MẬT

Cấu hình VPN 'luôn bật' của doanh nghiệp buộc mọi lưu lượng mạng của nhân viên làm việc từ xa đi qua tường lửa của công ty.

9. THÔNG TIN VỀ BẢO MẬT

Các điểm truy cập giả mạo có thể đưa ra các câu trả lời DNS giả, chuyển hướng các tên miền mục tiêu đến máy chủ lừa đảo trực tuyến (phishing).

10. THÔNG TIN VỀ AN NINH

Nếu không có VPN, những người dùng khác trên điểm phát sóng mở có thể thấy thiết bị của bạn liên hệ với những trang web và máy chủ nào.

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] Wi-Fi Alliance. (n.d.). Security.

https://www.wi-fi.org/discover-wi-fi/security

[2] Federal Trade Commission. (2023). Are Public Wi-Fi Networks Safe? What You Need To Know.

https://consumer.ftc.gov/articles/are-public-wi-fi-networks-safe-what-you-need-know

[3] MDN Web Docs. (n.d.). Strict-Transport-Security header.

https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/Strict-Transport-Security

[4] 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

[5] CISA. (n.d.). Malware, Phishing, and Ransomware.

https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

Đáp án: Điểm kiểm tra 1 – Trắc nghiệm

1 Câu hỏi 1 — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Tấn công xen giữa (Man-in-the-Middle, MitM) là gì? → Chặn và thay đổi thông tin liên lạc giữa hai bên trên một mạng dùng chung

2 Câu hỏi 2 — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Điểm truy cập giả mạo (Evil Twin) là gì? → Điểm phát Wi-Fi độc hại được cấu hình cùng SSID với mạng hợp pháp

3 Câu hỏi 3 — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

VPN bảo vệ lưu lượng Wi-Fi công cộng như thế nào? → Bọc mọi gói tin mạng trong một đường hầm mã hóa, khiến trình đánh hơi không đọc được

4 Câu hỏi 4 — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Nghe lén gói tin (packet sniffing) là gì? → Dùng công cụ phần cứng hoặc phần mềm để thu thập và ghi lại các gói tin mạng

5 Câu hỏi 5 — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Vai trò của HTTPS là gì? → Mã hóa lưu lượng phiên giữa trình duyệt và máy chủ web

Đáp án: Điểm kiểm tra 2 – Đúng hay Sai

6 **Câu hỏi 6** — **Đáp án đúng: Đúng**

GHI CHÚ CHO GIÁO VIÊN

Người dùng đã kết nối có thể dễ dàng thu thập dữ liệu văn bản thuần trên mạng Wi-Fi công cộng mở.

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

GHI CHÚ CHO GIÁO VIÊN

Sai: Evil Twin là một điểm phát sóng trái phép do kẻ tấn công dựng lên để giả mạo một điểm phát sóng thật.

8 **Câu hỏi 8** — **Đáp án đúng: Sai**

GHI CHÚ CHO GIÁO VIÊN

Sai: VPN mã hóa lưu lượng trong một đường hầm, nên các công cụ nghe lén cục bộ không thể đọc được.

9 **Câu hỏi 9** — **Đáp án đúng: Sai**

GHI CHÚ CHO GIÁO VIÊN

Sai: HTTPS mã hóa toàn bộ phiên trao đổi HTTP, bao gồm cả đường dẫn URL và nội dung trang.

10 **Câu hỏi 10** — **Đáp án đúng: Đúng**

GHI CHÚ CHO GIÁO VIÊN

Các điểm phát Wi-Fi dùng bảo mật WPA3 mang lại khả năng bảo vệ mạnh hơn các mạng mở, không có mật khẩu.

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

E 1. CHẶN BẮT	F 2. NGHE LÉN GÓI TIN	D 3. EVIL TWIN	H 4. HTTPS
G 5. VPN	B 6. ĐƯỜNG HẦM	A 7. WPA3	C 8. TƯỜNG LỬA

ĐIỂM KIỂM TRA 3: ĐÁP ÁN – THUẬT NGỮ CHÍNH

1 NGHE LÉN	2 BẮT GÓI TIN	3 EVIL TWIN	4 HTTPS
5 VPN	6 ĐƯỜNG HẦM		

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

1 G – CHUÂNWPA	2 C – EVILTWIN	3 B – BẮTGOITIN	4 F – ĐƯƠNGHẦM
5 H – TƯƠNGLƯA	6 A – NGHELEN	7 E – MANGVPN	8 D – HTTPS

GHI CHÚ THẢO LUẬN CHO GIÁO VIÊN

Thuật ngữ chính:
Kiểm tra xem học sinh có giải thích được CHẶN BẮT, NGHE LÉN GÓI TIN và EVIL TWIN 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.

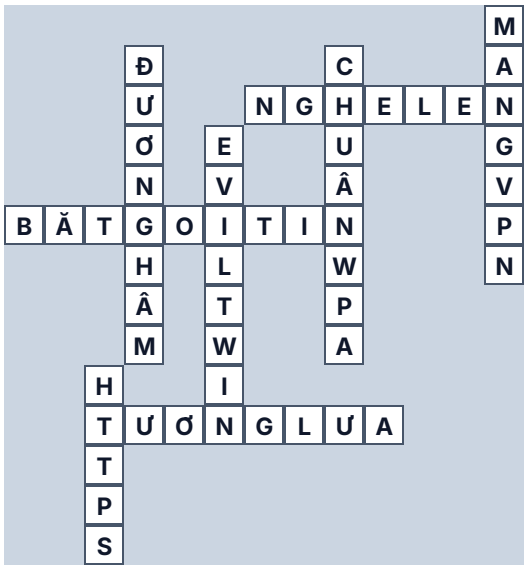
Đánh giá nguồn:
Yêu cầu học sinh kiểm chứng ít nhất một nhận định trong các nguồn của phiếu và thảo luận vì sao số liệu, giá cả và quy định có thể thay đổi theo thời gian.

Đáp án câu đố và ghi chú cho giáo viên

ĐÁP ÁN TÌM TỪ

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

ĐÁP ÁN Ô CHỮ



HƯỚNG DẪN CHO GIÁO VIÊN VỀ ĐÁP ÁN Ô CHỮ

HÀNG NGANG

4 hàng ngang: NGHELEN Đọc lưu lượng khi đang truyền (7 chữ cái)

6 hàng ngang: BĂTGOITIN Thu thập các gói dữ liệu mạng (9 chữ cái)

8 hàng ngang: TƯƠNGLƯA Lọc lưu lượng đến (8 chữ cái)

HÀNG DỌC

1 hàng dọc: MANGVPN Mạng riêng ảo được mã hóa (7 chữ cái)

2 hàng dọc: ĐƯƠNGHÂM Đường dẫn dữ liệu an toàn khi truyền (8 chữ cái)

3 hàng dọc: CHUÂNWPA Chuẩn bảo mật Wi-Fi hiện đại (8 chữ cái)

5 hàng dọc: EVILTWIN Điểm phát sóng giả mạo bắt chước Wi-Fi (8 chữ cái)

7 hàng dọc: HTTPS Truyền tải web an toàn (5 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.	E E N L N H G	NGHELEN	5.	T O Ă N I G B I T	BĂTGOITIN
2.	L E N V I W T I	EVILTWIN	6.	P H T S T	HTTPS
3.	G M V N N P A	MANGVPN	7.	Đ M G H Â Ư N Ơ	ĐƯƠNGHÂM
4.	Â P A W N C H U	CHUÂNWPA	8.	N Ư G A T Ư L Ơ	TƯƠNGLƯA

KHÓA THỬ THÁCH MẬT THƯ BÍ MẬT

"MA HOA LƯU LƯƠNG MANG CÔNG CÔNG BĂNG VPN"

Đáp án nghiên cứu tình huống

A Nghiên cứu tình huống 1: Ngăn chặn nghe lén gói tin trên Wi-Fi công cộng

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 giám đốc kinh doanh từ xa kết nối với mạng Wi-Fi sân bay công cộng nhận thấy nhiều email kinh doanh nhạy cảm bị rò rỉ ngay sau khi gửi dưới dạng văn bản thuần.
- Chiến lược và giải pháp đề xuất: Bắt buộc dùng ứng dụng khách VPN doanh nghiệp trên mọi máy trạm từ xa. Áp dụng các tiện ích mở rộng trình duyệt chỉ dùng HTTPS và chặn các giao thức không mã hóa (như HTTP và FTP) tại tường lửa của máy khách.

B Nghiên cứu tình huống 2: Phòng thủ điểm phát Wi-Fi giả mạo evil twin

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: Kẻ tấn công triển khai một điểm truy cập không dây giả mạo tên 'CoffeeShop_Guest' bắt chước điểm phát sóng hợp pháp của một quán cà phê, thu thập lưu lượng mạng từ những khách không hay biết.
- Chiến lược và giải pháp đề xuất: Kiểm tra địa chỉ MAC BSSID của điểm truy cập để xác minh tính xác thực của mạng. Thực thi xác thực trạng thái ứng dụng khách để chặn kết nối vào các mạng mở, và bắt buộc dùng điểm phát sóng di động cho công việc nhạy cảm.