Họ tên: _____ Ngày: _____ Điểm: _____

Web tối và web sâu: bảo mật và Điểm khác biệt

Lập chỉ mục công cụ tìm kiếm, cơ sở dữ liệu deep web, định tuyến củ hành Tor, ẩn danh mạng và các rủi ro

TỔNG QUAN HỌC TẬP VỀ DARK WEB VÀ DEEP WEB

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 sự khác biệt giữa Deep Web và Dark Web. Bạn sẽ khám phá các cơ sở dữ liệu không được lập chỉ mục, định tuyến củ hành (Onion Routing) của trình duyệt Tor, tên miền mật mã .onion và rủi ro bảo mật về tính ẩn danh.

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/dark-web-vs-deep-web/

Lộ trình học về chiến lược web sâu và web đen của bạn

- So sánh web sâu (cơ sở dữ liệu không được lập chỉ mục) với dark web (dịch vụ onion).
- Hiểu cách định tuyến Onion mã hóa và chuyển tiếp lưu lượng mạng.
- Đánh giá rủi ro bảo mật khi truy cập các trang mạng Tor chưa được xác minh.
- Triển khai cổng an toàn và chính sách sandbox cho việc thu thập thông tin tình báo về mối đe dọa.
- Phân tích định dạng địa chỉ mật mã của các tên miền dịch vụ onion.

HƯỚNG DẪN VỀ WEB SÂU VÀ WEB TỐI

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 quyền riêng tư trên deep web và dark web. Kết thúc với hoạt động thưởng Nghĩ nhanh.

CƠ SỞ DỮ LIỆU WEB SÂU VÀ ĐỊNH TUYẾN ONION CỦA WEB TỐI (GIỚI THIỆU)

Deep web gồm các trang chưa được lập chỉ mục nằm sau mật khẩu và đăng nhập, như email riêng tư hoặc cổng ngân hàng doanh nghiệp. Dark web là một tập con của deep web bị cố tình ẩn, đòi hỏi trình duyệt chuyên dụng (như Tor) và mạng onion để truy cập ẩn danh.

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

Điểm kiểm tra 1: Thử thách trắc nghiệm

1. Điều gì phân biệt deep web với surface web?

- A. Các trang web sâu không được các công cụ tìm kiếm công cộng lập chỉ mục
- B. Lưu lượng deep web là bất hợp pháp và bị cơ quan thực thi pháp luật giám sát
- C. Các trang deep web cần trình duyệt chuyên dụng như Tor để truy cập
- D. Các trang web sâu luôn tải nhanh hơn các trang web bề mặt

2. Làm thế nào để truy cập dark web?

- A. Qua các trình duyệt chuyên dụng sử dụng mạng định tuyến onion
- B. Bằng cách cấu hình DNS tùy chỉnh trên router thông thường
- C. Qua các bảng điều khiển tìm kiếm web bề mặt chỉ dành cho người được mời
- D. Bằng cách cài một tiện ích chặn quảng cáo tiêu chuẩn cho trình duyệt

3. Cấu trúc nào chiếm phần lớn nhất của deep web?

- A. Cơ sở dữ liệu người dùng được bảo vệ bằng mật khẩu và các tài khoản riêng tư
- B. Diễn đàn chợ đen bất hợp pháp mua bán hàng cấm
- C. Giao thức chia sẻ tệp ngang hàng không mã hóa
- D. Cơ sở dữ liệu bộ nhớ đệm của công cụ tìm kiếm công khai

4. Onion Routing tác động gì đến lưu lượng mạng?

- A. Mã hóa các gói tin và định tuyến chúng qua nhiều nút chuyển tiếp
- B. Tăng tốc độ tải xuống bằng cách bỏ qua các nút của ISP
- C. Nó ánh xạ số sê-ri phần cứng thiết bị với bản ghi IP
- D. Nó xóa cookie của trình duyệt web sau mỗi lần nhấp

5. Hậu tố tên miền nào chỉ được dùng trên các mạng Tor?

- A. Phần mở rộng cấp cao nhất .onion bằng mật mã
- B. Phần mở rộng thương mại .com truyền thống
- C. Phần mở rộng blockchain .eth phi tập trung của Web3
- D. Phần mở rộng công nghệ mã quốc gia .ai

Điểm kiểm tra 2: Thử thách Đúng hoặc Sai

6 Câu hỏi đúng/sai 6

6. Deep web và dark web là cùng một phân đoạn mạng.

○ Đúng ○ Sai

7 Câu hỏi đúng/sai 7

7. Cổng nội bộ doanh nghiệp là một phần của web sâu.

○ Đúng ○ Sai

8 Câu hỏi đúng/sai 8

8. Định tuyến Onion giải mã hoàn toàn các gói dữ liệu tại mọi nút trung chuyển.

○ Đúng ○ Sai

9 Câu hỏi đúng/sai 9

9. Truy cập dark web khiến thiết bị đối mặt với rủi ro phần mềm độc hại cao.

○ Đúng ○ Sai

10 Câu hỏi đúng/sai 10

10. Các công cụ tìm kiếm web tiêu chuẩn thu thập dữ liệu và lập chỉ mục các trang onion.

○ 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. Các cổng ngân hàng riêng tư nằm trong phân vùng chưa được lập chỉ mục là _____ .
2. Các nút Tor chuyên dụng lưu trữ các dịch vụ ẩn thuộc _____ .
3. Các trang Tor dùng phần mở rộng cấp cao nhất mật mã là _____ .
4. Cách dẫn lưu lượng được mã hóa nhiều lớp theo đường đi qua các nút được gọi là _____ .
5. Công cụ tìm kiếm web bề mặt thu thập những trang công khai và _____ .
6. Mạng Onion mã hóa IP của máy khách để duy trì tính _____ của người dùng.

NGÂN HÀNG TỪ VỰNG

ẨN DANH | CƠ SỞ DỮ LIỆU | DARK WEB | DEEP WEB | ĐÃ LẬP CHỈ MỤC | ĐỊNH TUYẾN TOR | ĐUÔI ONION | NÚT VÀO

Viết câu trả lời của bạn tại đây:

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

Điểm kiểm tra 4: Ghép nối khái niệm bảo mật

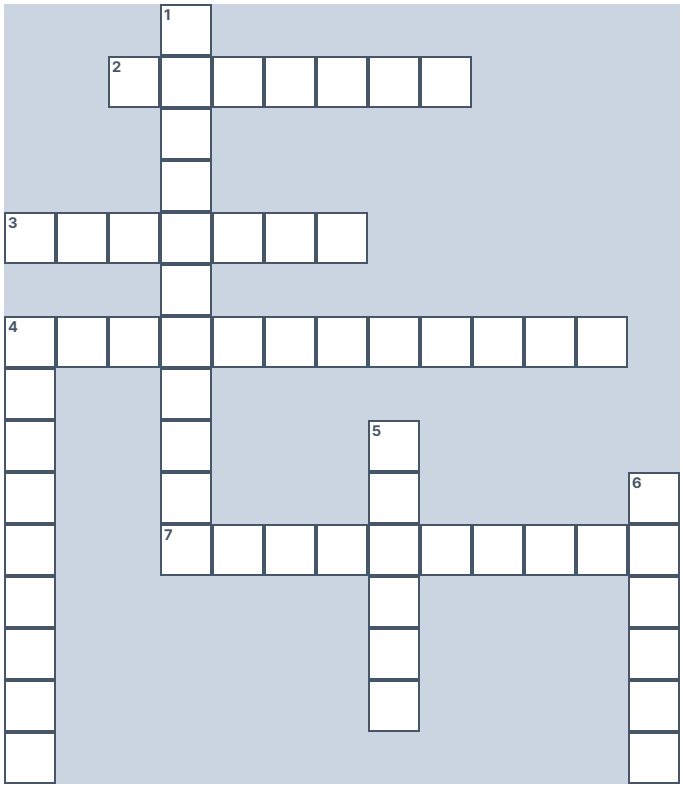
GHÉP ĐỊNH NGHĨA

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. Phân đoạn Deep Web	A	Phân đoạn mạng được mã hóa chỉ truy cập được qua các trình duyệt đặc biệt.
2. Cổng Dark Web	B	Mã hóa dữ liệu theo từng lớp và chuyển tiếp qua ba nút.
3. Phần mở rộng Onion	C	Bộ lưu trữ backend an toàn chứa các bản ghi hệ thống chưa được lập chỉ mục.
4. Định tuyến Tor	D	Hậu tố tên miền cấp cao nhất mật mã dùng trên mạng Tor.
5. Các trang đã lập chỉ mục	E	Nút điểm vào dùng để truy cập mạng Tor.
6. Tính ẩn danh của người dùng	F	Nội dung web bề mặt được tổng hợp và có thể tìm kiếm trên Google.
7. Cơ sở dữ liệu riêng tư	G	Giữ kín địa chỉ IP công khai của máy khách khỏi các máy chủ.
8. Cổng vào	H	Nội dung web không được lập chỉ mục như đăng nhập riêng tư, email và bản ghi cơ sở dữ liệu.

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

2. Phân đoạn mạng được mã hóa chỉ truy cập được qua các trình duyệt đặc biệt (7)

3. Nội dung web chưa lập chỉ mục như đăng nhập riêng tư, email và hồ sơ cơ sở dữ liệu (7)

4. Mã hóa dữ liệu theo từng lớp và chuyển tiếp qua ba nút (12)

7. Kho lưu trữ phía sau an toàn chứa các hồ sơ hệ thống chưa lập chỉ mục (10)

HÀNG DỌC

1. Nội dung web bề mặt được tổng hợp và tìm kiếm được trên Google (11)

4. Hậu tố tên miền cấp cao nhất mật mã dùng trên mạng Tor (9)

5. Giữ địa chỉ IP công khai của máy khách được che giấu khỏi máy chủ (6)

6. Nút điểm vào dùng để truy cập mạng Tor (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

2 hàng ngang: Phân đoạn mạng được mã hóa chỉ truy cập được qua các trình duyệt đặc biệt (7 chữ cái):

3 hàng ngang: Nội dung web chưa lập chỉ mục như đăng nhập riêng tư, email và hồ sơ cơ sở dữ liệu (7 chữ cái):

4 hàng ngang: Mã hóa dữ liệu theo từng lớp và chuyển tiếp qua ba nút (12 chữ cái):

7 hàng ngang: Kho lưu trữ phía sau an toàn chứa các hồ sơ hệ thống chưa lập chỉ mục (10 chữ cái):

HÀNG DỌC

1 hàng dọc: Nội dung web bề mặt được tổng hợp và tìm kiếm được trên Google (11 chữ cái):

4 hàng dọc: Hậu tố tên miền cấp cao nhất mật mã dùng trên mạng Tor (9 chữ cái):

5 hàng dọc: Giữ địa chỉ IP công khai của máy khách được che giấu khỏi máy chủ (6 chữ cái):

6 hàng dọc: Nút điểm vào dùng để truy cập mạng Tor (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.

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

DANH SÁCH TỪ VỰNG

DEEPWEB DARKWEB ĐUÔIONION ĐINHTUYÊNTOR ĐALÂPCHIMUC ÂNDANH CƠSƠDỮLIÊU NUTVAO

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. DEEPWEB

B. DARKWEB

C. ĐUÔIONION

D. ĐINHTUYÊNTOR

E. ĐALÂPCHIMUC

F. ÂNDANH

G. CƠSỞDỮLIÊU

H. NUTVAO

ĐỊNH NGHĨA VÀ CÁC TRƯỜNG GHÉP

1. Giữ địa chỉ IP công khai của máy khách được che giấu khỏi máy chủ.

2. Kho lưu trữ phía sau an toàn chứa các hồ sơ hệ thống chưa lập chỉ mục.

3. Mã hóa dữ liệu theo từng lớp và chuyển tiếp qua ba nút.

4. Nội dung web chưa lập chỉ mục như đăng nhập riêng tư, email và hồ sơ cơ sở dữ liệu.

5. Phân đoạn mạng được mã hóa chỉ truy cập được qua các trình duyệt đặc biệt.

6. Hậu tố tên miền cấp cao nhất mật mã dùng trên mạng Tor.

7. Nút điểm vào dùng để truy cập mạng Tor.

8. Nội dung web bề mặt được tổng hợp và tìm kiếm được trên Google.

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. PEDWBEE
2. NĐOIUNIOÔ
3. ĐHCILAUCPMÂ
4. ƯÊDUƠILCƠS
5. WBKRDEA
6. RTNTUOÊĐIYNH
7. NÂAHDN
8. TONAVU

Hoạt động thưởng: Nghĩ nhanh

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

1	Lý do nên tránh xa dark web			
2	Những thứ công cụ tìm kiếm không thể tìm thấy			
3	Những thiết bị có thể bị tấn công			
4	Những lý do hợp pháp để dùng Tor			
5	Lý do cập nhật phần mềm			
6	Những dấu hiệu cảnh báo trong một email			
7	Những thứ bị bán bất hợp pháp trên dark web			
8	Những người bạn có thể nhờ giúp về CNTT			
9	Những thói quen an toàn bạn có thể bắt đầu ngay hôm nay			
10	Những việc cần làm sau khi dữ liệu bị rò rỉ			
11	Những thứ thuộc về deep web			
12	Những trang web bạn dùng bằng cách đăng nhập			
13	Những từ liên quan đến ẩn danh			
14	Những thông tin bạn không bao giờ nên chia sẻ			
15	Những thứ nằm 'bên dưới bề mặt'			

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: NHẬN DIỆN RÒ RỈ DỮ LIỆU



Tình huống: Một cuộc kiểm toán an ninh doanh nghiệp phát hiện các bản ghi cơ sở dữ liệu khách hàng nhạy cảm đang được giao dịch trên một chợ onion. Dữ liệu này không được lập chỉ mục trên Google.

Câu hỏi thảo luận: Hãy giải thích những phân đoạn web nào có liên quan và vụ rò rỉ này đã xảy ra như thế nào.

NGHIÊN CỨU TÌNH HUỐNG 2: TÍNH ẨN DANH VÀ RỦI RO PHẦN MỀM ĐỘC HẠI



Tình huống: Một nhà phân tích muốn kiểm tra các nguồn tin tình báo về mối đe dọa trên một trang web Tor. Họ tải trình duyệt Tor và truy cập trang web.

Câu hỏi thảo luận: Hãy đánh giá lợi ích ẩn danh và nêu các bước giảm thiểu phần mềm độc hại.

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

10	12	26	3	16	6	1	16	11	16	10	26	19	12	6	25	16	10		
4	2	16	10	7	12	16	11	24	25	29	9	16	17	16	12	17	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: Deep web là gì?

Deep web gồm mọi trang web mà công cụ tìm kiếm không thể lập chỉ mục, bao gồm ngân hàng trực tuyến, cơ sở dữ liệu email và các tạp chí trả phí.

Q2: Dark web là gì?

Dark web là một tập con nhỏ của deep web được cố tình ẩn và chỉ truy cập được qua các trình duyệt chuyên dụng dùng mạng onion.

Q3: Công cụ tìm kiếm lập chỉ mục các trang như thế nào?

Các công cụ tìm kiếm chạy các chương trình tự động (spider) để theo các liên kết công khai, lập chỉ mục các trang không chặn việc thu thập bằng chỉ thị robot.

Q4: Vì sao ngân hàng trực tuyến được coi là một phần của deep web?

Cổng ngân hàng nằm sau các lớp đăng nhập và mật khẩu, ngăn các công cụ tìm kiếm công khai lập chỉ mục các trang sao kê tài khoản.

Q5: Định tuyến củ hành (Onion Routing) của trình duyệt Tor là gì?

Định tuyến Onion là phương thức truyền tải mã hóa lưu lượng theo từng lớp và chuyển qua nhiều nút chuyển tiếp để che giấu địa chỉ IP của người dùng.

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: Truy cập dark web có bất hợp pháp không?

Không. Truy cập dark web là hợp pháp ở hầu hết các quốc gia, dù tham gia các chợ bất hợp pháp hoặc hoạt động tấn công mạng thì bị cấm.

Q7: Vì sao các trang dark web tải chậm?

Lưu lượng được định tuyến và giải mã qua ít nhất ba nút chuyển tiếp toàn cầu (vào, giữa, ra), làm tăng độ trễ truyền.

Q8: Hậu tố tên miền .onion có nghĩa là gì?

Đây là hậu tố tên miền cấp cao nhất chuyên dụng dùng trên mạng Tor, trỏ đến các địa chỉ được tạo bằng mật mã thay vì máy chủ DNS tiêu chuẩn.

Q9: Các liên kết dark web có những rủi ro gì?

Các trang không có sàng lọc bảo mật, khiến người dùng đối mặt với tỷ lệ nhiễm phần mềm độc hại cao, các tập lệnh lừa đảo trực tuyến (phishing) và lừa đảo giao dịch.

Q10: Ai tạo ra giao thức định tuyến của mạng Tor?

Công nghệ này ban đầu được Phòng thí nghiệm Nghiên cứu Hải quân Hoa Kỳ phát triển vào những năm 1990 để bảo vệ liên lạc của chính phủ.

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: Các nút trung gian bảo vệ tính ẩn danh của Tor như thế nào?

Mỗi nút chỉ giải mã một lớp dữ liệu định tuyến, chỉ biết chặng trước và chặng sau, không bao giờ biết cả nguồn lẫn đích.

Q2: Vai trò của nút thoát (exit node) là gì?

Nút ra giải mã lớp mã hóa cuối cùng, gửi lưu lượng ra máy chủ đích công khai hoặc máy chủ onion.

Q3: Cổng cầu nối Tor là gì?

Bridge là các rơ-le đầu vào Tor không được liệt kê, dùng để vượt các chặn của ISP và kiểm duyệt ở những khu vực hạn chế truy cập trình duyệt Tor.

Q4: Các đối tượng trên dark web khai thác tiền mã hóa như thế nào?

Các đối tượng dùng tiền điện tử ẩn danh để thực hiện giao dịch tài chính trên các chợ đen, né tránh các kiểm tra giao dịch ngân hàng tiêu chuẩn.

Q5: Vì sao công cụ tìm kiếm thông thường không thể thu thập các cơ sở dữ liệu sâu?

Trình thu thập dữ liệu không thể nhập thông tin đăng nhập, giải CAPTCHA bảo mật hay chạy các script truy vấn SQL phía máy chủ cần thiết để truy cập các cơ sở dữ liệu web sâu.

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: Máy chủ thư mục trong mạng Tor là gì?

Đây là máy chủ đáng tin cậy duy trì danh sách các relay vào, giữa và thoát đang hoạt động mà máy khách dùng để xây dựng đường định tuyến.

Q7: Kẻ xấu thực hiện nghe lén tại nút thoát như thế nào?

Người vận hành nút thoát giả mạo có thể chặn lưu lượng HTTP không mã hóa khi nó rời mạng Tor, đánh cắp tên người dùng và cookie.

Q8: Tor và I2P khác nhau như thế nào?

Tor dùng danh mục nút chuyển tiếp tập trung và các nút ra để truy cập web công cộng, trong khi I2P dùng cấu trúc ngang hàng phi tập trung để lưu trữ nội bộ.

Q9: Các cơ quan thực thi pháp luật theo dõi các chợ dark web như thế nào?

Các cơ quan dùng phân tích blockchain, xác định các hệ thống máy chủ lưu trữ vật lý và thực hiện các chiến dịch nghi binh để nhận diện người vận hành.

Q10: Rò rỉ DNS làm tổn hại tính ẩn danh của máy khách như thế nào?

Rò rỉ DNS xảy ra khi các truy vấn DNS của trình duyệt được gửi thẳng qua ISP địa phương thay vì được định tuyến qua mạng Tor được mã hóa.

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

Deep web lớn hơn nhiều so với web bề mặt có thể tìm kiếm, vì phần lớn nội dung nằm sau đăng nhập và cơ sở dữ liệu.

2. THÔNG TIN VỀ AN NINH

Dark web là một phần nhỏ, được cố tình ẩn của deep web, truy cập bằng các công cụ như Tor.

3. THÔNG TIN VỀ AN NINH

Định tuyến Tor mã hóa các gói dữ liệu ba lần, bóc từng lớp mã hóa như bóc củ hành tại mỗi nút chuyển tiếp.

4. THÔNG TIN VỀ AN NINH

Tor phát triển từ dự án định tuyến onion do Phòng thí nghiệm Nghiên cứu Hải quân Hoa Kỳ thực hiện, và mã của nó được phát hành dưới dạng phần mềm miễn phí. [1]

5. THÔNG TIN VỀ AN NINH

Địa chỉ Onion là các chuỗi chữ và số gồm 56 ký tự được tạo bằng mật mã từ các cặp khóa công khai.

6. THÔNG TIN VỀ AN NINH

Nút thoát có thể đọc lưu lượng dạng văn bản thuần, nghĩa là vẫn cần TLS/HTTPS trên Tor để bảo vệ dữ liệu phiên.

7. THÔNG TIN VỀ BẢO MẬT

Các trang web nội bộ, ổ đĩa đám mây và cơ sở dữ liệu riêng tư là những phân đoạn lưu trữ dữ liệu lớn nhất trên deep web.

8. THÔNG TIN VỀ BẢO MẬT

Các công cụ tìm kiếm chuyên biệt như DuckDuckGo vận hành cổng onion để cho phép tìm kiếm ẩn danh trên mạng Tor.

9. THÔNG TIN VỀ BẢO MẬT

Hơn 2 triệu người dùng kết nối với mạng Tor mỗi ngày để vượt kiểm duyệt và giữ riêng tư khi liên lạc.

10. THÔNG TIN VỀ AN NINH

Các chiến dịch thực thi pháp luật toàn cầu (như Operation Bayonet) đã đóng cửa các chợ đen lớn bằng cách thu giữ phần cứng lưu trữ.

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] Tor Project. (n.d.). Why is it called Tor?
https://support.torproject.org/about/why-is-it-called-tor/

[2] Tor Project. (n.d.). How do Onion Services work?
https://community.torproject.org/onion-services/overview/

[3] Tor Project. (n.d.). Users – Tor Metrics.
https://metrics.torproject.org/userstats-relay-country.html

[4] CISA. (n.d.). Malware, Phishing, and Ransomware.
https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-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

Đáp án: Điểm kiểm tra 1 – Trắc nghiệm

1 **Lập chỉ mục tìm kiếm** WEB SÂU — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Các trang web sâu nằm sau tường đăng nhập và cơ sở dữ liệu, ngăn trình thu thập dữ liệu của công cụ tìm kiếm truy cập. Trích dẫn: IETF RFC 3986.

2 **Truy cập Tor** DARK WEB — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Dark web gồm các dịch vụ onion ẩn chỉ truy cập được qua các trình duyệt như Tor. Trích dẫn: IETF RFC 3986.

3 **Cơ sở dữ liệu sâu** CƠ SỞ DỮ LIỆU — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Các tài khoản được bảo vệ bằng mật khẩu và hồ sơ doanh nghiệp tạo nên phân khúc lớn nhất của deep web. Trích dẫn: NIST Digital Identity.

4 **Định tuyến Onion** MẠNG TOR — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Định tuyến Onion mã hóa gói dữ liệu theo từng lớp, chuyển tiếp qua nhiều nút để ẩn danh. Trích dẫn: IETF RFC 3986.

5 **Tên miền Onion** HẬU TỐ — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Hậu tố tên miền.onion mang tính mật mã định tuyến lưu lượng nội bộ trên Tor mà không cần DNS công cộng. Trích dẫn: IETF RFC 3986.

Đáp án: Điểm kiểm tra 2 – Đúng hay Sai

6 **Các phân đoạn web** CẤU TRÚC

Đáp án đúng: Sai

GHI CHÚ CHO GIÁO VIÊN

Deep web bao gồm mọi trang chưa được lập chỉ mục, còn dark web là một phân đoạn onion nhỏ, được mã hóa. Trích dẫn: IETF RFC 3986.

7 **Mạng nội bộ doanh nghiệp** WEB SÂU

Đáp án đúng: Đúng

GHI CHÚ CHO GIÁO VIÊN

Các trang web nội bộ (intranet) nằm sau cổng mật khẩu và không được lập chỉ mục, nghĩa là chúng thuộc deep web. Trích dẫn: NIST Digital Identity.

8 **Mã hóa theo lớp** NÚT TRUNG CHUYỂN

Đáp án đúng: Sai

GHI CHÚ CHO GIÁO VIÊN

Các nút chuyển tiếp Onion chỉ giải mã một lớp định tuyến để bảo vệ ẩn danh của người dùng, không bao giờ giải mã toàn bộ gói tin. Trích dẫn: IETF RFC 3986.

9 **Mức độ phơi nhiễm phần mềm độc hại** MỐI ĐE DỌA

Đáp án đúng: Đúng

GHI CHÚ CHO GIÁO VIÊN

Các chợ trên web tối không có bộ lọc bảo mật, tiềm ẩn nguy cơ nhiễm phần mềm độc hại rất cao. Trích dẫn: Center for Internet Security (CIS).

10 **Câu hỏi 10**

Đáp án đúng: Sai

GHI CHÚ CHO GIÁO VIÊN

Các trình thu thập dữ liệu của công cụ tìm kiếm thông thường không dùng Tor, nên chúng không thể truy cập hay lập chỉ mục các trang .onion.

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

H 1. Phân đoạn Deep Web	A 2. Cổng Dark Web	D 3. Phần mở rộng Onion	B 4. Định tuyến Tor
F 5. Các trang đã lập chỉ mục	G 6. Tính ẩn danh của người dùng	C 7. Cơ sở dữ liệu riêng tư	E 8. Cổng vào

ĐIỂM KIỂM TRA 3: ĐÁP ÁN – THUẬT NGỮ CHÍNH

1 DEEP WEB	2 DARK WEB	3 ĐUÔI ONION	4 ĐỊNH TUYẾN TOR
5 ĐÃ LẬP CHỈ MỤC	6 ẨN DANH		

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

1 F – ÂNDANH	2 G – CƠSỞDỮLIỆU	3 D – ĐINHTUYÊNTOR	4 A – DEEPWEB
5 B – DARKWEB	6 C – ĐUÔIONION	7 H – NUTVAO	8 E – ĐALÂPCHIMUC

GHI CHÚ THẢO LUẬN CHO GIÁO VIÊN

Thuật ngữ chính:
Kiểm tra xem học sinh có giải thích được Phân đoạn Deep Web, Cổng Dark Web và Phần mở rộng Onion 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.

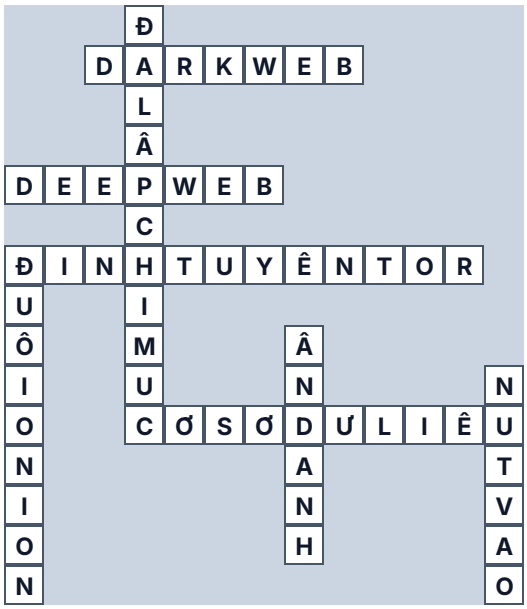
Đánh giá nguồn:
Yêu cầu học sinh kiểm chứng ít nhất một nhận định trong các nguồn của phiếu và thảo luận vì sao số liệu, giá cả và quy định có thể thay đổi theo thời gian.

Đáp án câu đố và ghi chú cho giáo viên

ĐÁP ÁN TÌM TỪ

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

ĐÁP ÁN Ô CHỮ



HƯỚNG DẪN CHO GIÁO VIÊN VỀ ĐÁP ÁN Ô CHỮ

HÀNG NGANG

2 hàng ngang: DARKWEB Phân đoạn mạng được mã hóa chỉ truy cập được qua các trình duyệt đặc biệt (7 chữ cái)

3 hàng ngang: DEEPWEB Nội dung web chưa lập chỉ mục như đăng nhập riêng tư, email và hồ sơ cơ sở dữ liệu (7 chữ cái)

4 hàng ngang: ĐINHTUYÊNTOR Mã hóa dữ liệu theo từng lớp và chuyển tiếp qua ba nút (12 chữ cái)

7 hàng ngang: CƠSỞDỮLIỆU Kho lưu trữ phía sau an toàn chứa các hồ sơ hệ thống chưa lập chỉ mục (10 chữ cái)

HÀNG DỌC

1 hàng dọc: ĐALÂPCHIMUC Nội dung web bề mặt được tổng hợp và tìm kiếm được trên Google (11 chữ cái)

4 hàng dọc: ĐUÔIONION Hậu tố tên miền cấp cao nhất mật mã dùng trên mạng Tor (9 chữ cái)

5 hàng dọc: ÂNDANH Giữ địa chỉ IP công khai của máy khách được che giấu khỏi máy chủ (6 chữ cái)

6 hàng dọc: NUTVAO Nút điểm vào dùng để truy cập mạng Tor (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. PEDWBEE — **DEEPWEB**
2. NĐOIUNIOÔ — **ĐUÔIONION**
3. ĐHCILAUCPMÂ — **ĐALÂPCHIMUC**
4. ƯÊDUƠILCƠS — **CƠSỞDỮLIỆU**
5. WBKRDEA — **DARKWEB**
6. RTNTUOÊĐIYNH — **ĐINHTUYÊNTOR**
7. NÂAHDN — **ÂNDANH**
8. TONAVU — **NUTVAO**

KHÓA THỬ THÁCH MẬT THƯ BÍ MẬT

"GIƯ ÂN DANH NGƯƠI DUNG BĂNG ĐINH TUYÊN ONION"

Đáp án nghiên cứu tình huống

A Nghiên cứu tình huống 1: Nhận diện rò rỉ dữ liệu

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 cuộc kiểm toán bảo mật doanh nghiệp phát hiện các bản ghi cơ sở dữ liệu khách hàng nhạy cảm đang được giao dịch trên một chợ onion. Dữ liệu không được lập chỉ mục trên Google.
- Chiến lược và giải pháp đề xuất: Các phân đoạn liên quan: Cơ sở dữ liệu riêng tư thuộc deep web (không được lập chỉ mục nhưng an toàn). Chợ giao dịch dữ liệu bị đánh cắp nằm trên dark web (mạng onion). Diễn biến: Tin tặc vượt qua hàng phòng thủ máy chủ, đánh cắp cơ sở dữ liệu từ deep web và đăng bán ẩn danh trên dark web để tránh bị cơ quan thực thi pháp luật theo dõi.

B Nghiên cứu tình huống 2: Tính ẩn danh và rủi ro phần mềm độc hại

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 nhà phân tích muốn kiểm tra các nguồn cấp tình báo mối đe dọa trên một trang web Tor. Họ tải trình duyệt Tor và truy cập trang.
- Chiến lược và giải pháp đề xuất: Lợi ích: Tor định tuyến lưu lượng qua ba nút, che giấu IP công ty của nhà phân tích. Rủi ro và biện pháp giảm thiểu: Các liên kết dark web không có sàng lọc về uy tín. Nhà phân tích phải chạy Tor bên trong máy ảo (VM) cô lập, tắt JavaScript trong cài đặt Tor và tránh tải xuống bất kỳ tệp nào để bảo vệ mạng công ty.