Nome: _____ Data: _____ Pontuação: _____

Dark web vs. deep web: segurança e Diferenças

Indexação em motores de pesquisa, bases de dados da deep web, encaminhamento onion do Tor, anonimato na rede e riscos

VISÃO GERAL DE APRENDIZAGEM SOBRE DARK WEB VS. DEEP WEB

PROTEGIDO

ENCRIPTAÇÃO DE DADOS

Norma AES de 256 bits

CONFORME

NORMAS GLOBAIS

Referenciais RGPD (GDPR) e CCPA

ZERO-TRUST

POLÍTICA DE ACESSO

Autenticação multifator

Bem-vindo! Este conjunto de atividades guia-te pelas diferenças entre a Web profunda e a Dark Web. Vais explorar bases de dados não indexadas, o encaminhamento onion do navegador Tor, domínios criptográficos .onion e os riscos de segurança do anonimato.

PONTOS DE CONTROLO DA FICHA DE TRABALHO

- [ ] **Partes 1-4: Domina a cibersegurança e a prevenção de ameaças.**
- [ ] **Partes 5-7: Resolve puzzles de palavras cruzadas e sopas de letras.**
- [ ] **Partes 8-9: Resolve estudos de caso e o desafio de cifra.**
- [ ] **Parte 10: Revê as páginas de perguntas frequentes básicas e avançadas.**
- [ ] **Parte 11: Explora 10 factos interessantes do mundo real.**
- [ ] **Bónus: desafio Pensa rápido.**

Abrir o Guia de Cibersegurança da VPN.com

URL: https://www.vpn.com/pt/ciberseguranca/dark-web-vs-deep-web/

O teu roteiro de aprendizagem sobre estratégia para a Web profunda e a Dark Web

- Compara a deep web (bases de dados não indexadas) com a dark web (serviços onion).
- Compreender como o Onion Routing encripta e retransmite o tráfego de rede.
- Avalia os riscos de segurança de aceder a sites não verificados da rede Tor.
- Implementa políticas de gateway seguro e de sandboxing para o rastreamento de informações sobre ameaças.
- Analisa o formato de endereço criptográfico dos domínios de serviços onion.

INSTRUÇÕES DO GUIA DA DEEP WEB E DA DARK WEB

Responde às perguntas de escolha múltipla e de verdadeiro/falso, completa as frases de preencher espaços com o banco de palavras, associa as definições e resolve as palavras cruzadas e a sopa de letras. Aplica os teus conhecimentos à privacidade na deep web e na dark web. Termina com a atividade bónus Pensa rápido.

BASES DE DADOS DA DEEP WEB VS ENCAMINHAMENTO ONION DA DARK WEB (INTRODUÇÃO)

A deep web é constituída por páginas não indexadas protegidas por palavras-passe e inícios de sessão, como e-mails privados ou portais bancários empresariais. A dark web é um subconjunto da deep web que está oculto intencionalmente, exigindo navegadores especializados (como o Tor) e redes onion para aceder de forma anónima.

LÊ CADA PONTO DE CONTROLO COM ATENÇÃO E ESCOLHE OU ESCREVE A RESPOSTA CORRETA.

Ponto de controlo 1: Desafio de escolha múltipla

1. O que distingue a deep web da web de superfície?

- A. As páginas da web profunda não são indexadas pelos motores de pesquisa públicos
- B. O tráfego da deep web é ilegal e monitorizado pelas autoridades policiais
- C. Os sites da deep web exigem browsers especializados como o Tor para serem acedidos
- D. As páginas da deep web carregam sempre mais depressa do que as da web de superfície

2. Como se acede à dark web?

- A. Através de navegadores especializados que utilizam redes de encaminhamento cebola (onion routing)
- B. Configurando definições de DNS personalizadas em routers padrão
- C. Através de consolas de pesquisa da web de superfície privadas, apenas por convite
- D. Instalando uma extensão de navegador padrão de bloqueio de anúncios

3. Que estrutura constitui a maior parte da deep web?

- A. Bases de dados de utilizadores e contas privadas protegidas por palavra-passe
- B. Fóruns ilegais do mercado negro que comercializam bens ilícitos
- C. Protocolos de partilha de ficheiros ponto a ponto não encriptados
- D. Bases de dados de cache de motores de busca públicos

4. O que faz o Onion Routing ao tráfego de rede?

- A. Encripta os pacotes e encaminha-os através de vários relays
- B. Aumenta as velocidades de transferência contornando os nós do ISP
- C. Associa os números de série do hardware do dispositivo a registos de IP
- D. Elimina os cookies do navegador após cada clique

5. Que sufixo de domínio é usado exclusivamente nas redes Tor?

- A. A extensão criptográfica de nível superior .onion
- B. A extensão comercial .com clássica e tradicional
- C. A extensão descentralizada Web3 .eth baseada em blockchain
- D. A extensão tecnológica de código de país .ai

Ponto de controlo 2: Desafio de verdadeiro ou falso

6 Pergunta (verdadeiro/falso) 6

6. A deep web e a dark web referem-se ao mesmo segmento da rede.

- ◯ Verdadeiro
- ◯ Falso

7 Pergunta (verdadeiro/falso) 7

7. Os portais de intranets empresariais fazem parte da deep web.

- ◯ Verdadeiro
- ◯ Falso

8 Pergunta (verdadeiro/falso) 8

8. O encaminhamento cebola decifra completamente os pacotes de dados em cada nó de trânsito.

- ◯ Verdadeiro
- ◯ Falso

9 Pergunta (verdadeiro/falso) 9

9. Aceder à dark web expõe os dispositivos a riscos elevados de software malicioso.

- ◯ Verdadeiro
- ◯ Falso

10 Pergunta (verdadeiro/falso) 10

10. Os motores de pesquisa web normais rastreiam e indexam sites onion.

- ◯ Verdadeiro
- ◯ Falso

Ponto de controlo 3: Inserção de termos-chave

Lê cada frase abaixo e preenche o espaço em branco com o termo correto do banco de palavras.

1. Os portais bancários privados encontram-se no segmento não indexado da _____ .
2. Nós Tor especializados alojam serviços ocultos da _____ .
3. Os sites Tor usam a sua própria _____ criptográfica de domínio de topo.
4. A passagem do tráfego encriptado por várias camadas de nós chama-se _____ .
5. Os motores de pesquisa da superfície rastreiam páginas que estão publicamente _____ .
6. As redes onion encriptam os IP dos clientes para manter o _____ dos utilizadores.

BANCO DE PALAVRAS DE VOCABULÁRIO

ANONIMATO | BASE DE DADOS | DARK WEB | DEEP WEB | ENCAMINHAMENTO | EXTENSÃO ONION | INDEXADAS | NÓ DE ENTRADA

Escreve aqui as tuas respostas:

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

Ponto de controlo 4: Associação de conceitos de segurança

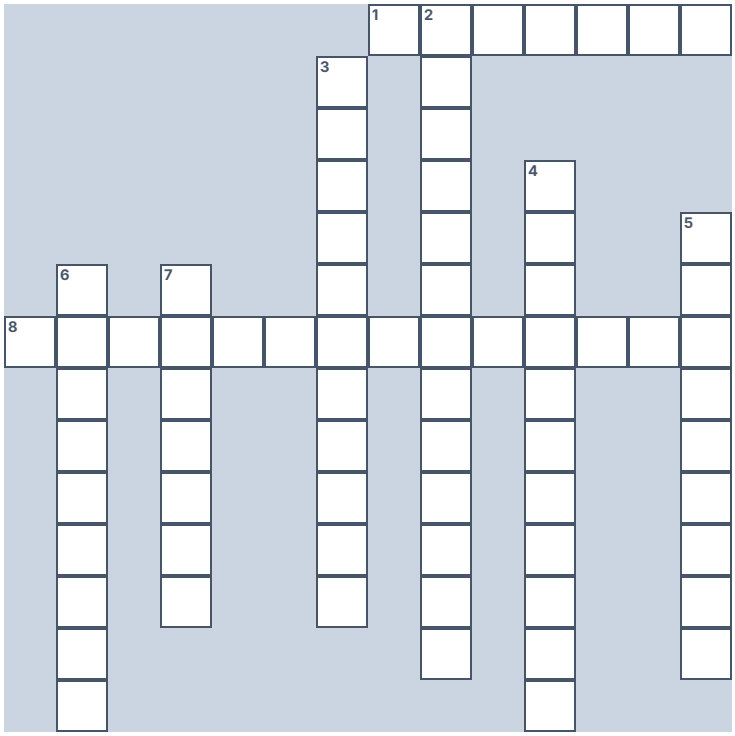
ASSOCIAÇÃO DE DEFINIÇÕES

Associa cada termo de vocabulário da esquerda à sua definição correta da direita, escrevendo a letra correspondente (A-H) na caixa de preenchimento.

1. Segmento da deep web	A	Segmento de rede encriptado acessível apenas através de navegadores especiais.
2. Portal da dark web	B	Encriptação dos dados em camadas e retransmissão através de três nós.
3. Extensão Onion	C	Armazenamento de back-end seguro que aloja registos de sistema não indexados.
4. Encaminhamento Tor	D	Sufixo criptográfico de domínio de topo usado nas redes Tor.
5. Páginas indexadas	E	O nó de ponto de entrada utilizado para aceder à rede Tor.
6. Anonimato do utilizador	F	Conteúdo da web de superfície compilado e pesquisável no Google.
7. Base de dados privada	G	Manter os endereços IP públicos dos clientes ocultos dos servidores.
8. Gateway de entrada	H	Conteúdo web não indexado, como inícios de sessão privados, e-mails e registos de bases de dados.

Ponto de controlo 5: Palavras cruzadas

Resolve as palavras cruzadas escrevendo letras nas caixas brancas ativas. Os números correspondem às pistas abaixo.



HORIZONTAIS

1. Conteúdo web não indexado, como inícios de sessão privados, emails e registos de bases de dados (7)

8. Encriptar os dados em camadas e retransmiti-los por três nós (14)

VERTICAIS

2. Sufixo criptográfico de domínio de topo usado nas redes Tor (13)

3. Nó de entrada usado para aceder à rede Tor (11)

4. Armazenamento seguro de retaguarda que aloja registos do sistema não indexados (11)

5. Manter os endereços IP públicos dos clientes ocultos dos servidores (9)

6. Conteúdo da web de superfície compilado e pesquisável no Google (9)

7. Segmento de rede encriptado, acessível apenas através de navegadores especiais (7)

Ponto de controlo 5, alternativa: Pistas acessíveis das palavras cruzadas

Os utilizadores de leitores de ecrã e de teclado podem escrever as respostas das palavras cruzadas diretamente nos campos de texto abaixo.

HORIZONTAIS

1 horizontal: Conteúdo web não indexado, como inícios de sessão privados, emails e registos de bases de dados (7 letras):

8 horizontal: Encriptar os dados em camadas e retransmiti-los por três nós (14 letras):

VERTICAIS

2 vertical: Sufixo criptográfico de domínio de topo usado nas redes Tor (13 letras):

3 vertical: Nó de entrada usado para aceder à rede Tor (11 letras):

4 vertical: Armazenamento seguro de retaguarda que aloja registos do sistema não indexados (11 letras):

5 vertical: Manter os endereços IP públicos dos clientes ocultos dos servidores (9 letras):

6 vertical: Conteúdo da web de superfície compilado e pesquisável no Google (9 letras):

7 vertical: Segmento de rede encriptado, acessível apenas através de navegadores especiais (7 letras):

Ponto de controlo 6: Sopa de letras

Encontra os 8 termos-chave de vocabulário escondidos na grelha abaixo. As palavras podem estar na horizontal, na vertical ou na diagonal.

N K T S V R Z E H E S C A L Q
O A D A R T N E E D O N C D A
I Z M K D A R K W E B V E N R
N U A S I W J M M H H E O N H
O R F K N T L R W H P N B U F
O Y O Y D W S H T W I X A P U
A N N Z E O I Q E M T I P V U
S O U U X K A B A E P M K A N
N V G G A P Q T X Y J K V J Y
E W Y P D J O I Z I J N A E I
T E N C A M I N H A M E N T O
X A S A S J F W E K Z K E K Q
E N B A S E D E D A D O S J A
F O K N D N C D H I B A P R L
P W T I Y F Y S G X W H F R T

LISTA DE PALAVRAS DE VOCABULÁRIO

DEEPWEB DARKWEB EXTENSAOONION ENCAMINHAMENTO INDEXADAS
ANONIMATO BASEDEDADOS NODEENTRADA

Ponto de controlo 6, alternativa: Associação acessível de vocabulário

Associa cada um dos 8 termos de vocabulário da sopa de letras à sua definição correta, escrevendo a letra (A-H) no espaço em branco.

TERMOS DE VOCABULÁRIO

- **A. DEEPWEB**
- **B. DARKWEB**
- **C. EXTENSAOONION**
- **D. ENCAMINHAMENTO**
- **E. INDEXADAS**
- **F. ANONIMATO**
- **G. BASEDEDADOS**
- **H. NODEENTRADA**

DEFINIÇÕES E CAMPOS DE ASSOCIAÇÃO

1. Manter os endereços IP públicos dos clientes ocultos dos servidores.
2. Armazenamento seguro de retaguarda que aloja registos do sistema não indexados.
3. Encriptar os dados em camadas e retransmiti-los por três nós.
4. Conteúdo web não indexado, como inícios de sessão privados, emails e registos de bases de dados.
5. Segmento de rede encriptado, acessível apenas através de navegadores especiais.
6. Sufixo criptográfico de domínio de topo usado nas redes Tor.
7. Nó de entrada usado para aceder à rede Tor.
8. Conteúdo da web de superfície compilado e pesquisável no Google.

Ponto de controlo 7: Desafio de palavras baralhadas

Desembaralha as letras abaixo para revelar conceitos e termos essenciais de cibersegurança. Escreve as tuas respostas nas caixas de resposta fornecidas.

1. **P E D W B E E** _____
2. **O N X S T E I A N O N O E** _____
3. **I A X N D S E A D** _____
4. **D O S E S D D A B A E** _____
5. **W B K R D E A** _____
6. **I N E M C N H T M E N A O A** _____
7. **M A T O A N N I O** _____
8. **A T A N D N E O D R E** _____

Atividade bónus: Pensa rápido

3 RESPOSTAS POR CATEGORIA. GANHA QUEM COMPLETAR PRIMEIRO A LISTA.

1	Razões para ficar longe da dark web			
2	Coisas que um motor de busca não consegue encontrar			
3	Dispositivos que podem ser hackeados			
4	Razões legais para usar o Tor			
5	Razões para atualizar o software			
6	Sinais de alerta num email			
7	Coisas vendidas ilegalmente na dark web			
8	Pessoas a quem podes pedir ajuda de TI			
9	Hábitos seguros que podes começar hoje			
10	Coisas a fazer depois de uma fuga de dados			
11	Coisas que pertencem à deep web			
12	Sites que usas com início de sessão			
13	Palavras relacionadas com anonimato			
14	Informações que nunca deves partilhar			
15	Coisas que ficam "debaixo da superfície"			

Ponto de controlo 8: Estudos de caso de cibersegurança

Aplica os conceitos que aprendeste para resolver os cenários reais abaixo.

ESTUDO DE CASO 1: IDENTIFICAÇÃO DE FUGAS DE DADOS



Cenário: Uma auditoria de segurança empresarial descobre que registos sensíveis da base de dados de clientes estão a ser negociados num mercado onion. Os dados não estão indexados no Google.

Questão para debate: Explica que segmentos da web estão envolvidos e como ocorreu esta fuga.

ESTUDO DE CASO 2: ANONIMATO VS. RISCOS DE MALWARE



Cenário: Um analista quer consultar feeds de informações sobre ameaças num site Tor. Transfere o navegador Tor e acede ao site.

Questão para debate: Avalia os benefícios de anonimato e descreve os passos de mitigação de malware.

Ponto de controlo 9: Decifrar o código

Um profissional de cibersegurança protege os ativos de rede contra agentes de ameaça online. Usa a chave Letra-Número abaixo para decifrar a mensagem, escrevendo as letras correspondentes nos espaços em branco.

CHAVE DE ENCRIPTAÇÃO DE LETRAS PARA NÚMEROS

A=1 B=2 C=3 D=4 E=5 F=6 G=7 H=8 I=9 J=10

K=11 L=12 M=13 N=14 O=15 P=16 Q=17 R=18 S=19 T=20

U=21 V=22 W=23 X=24 Y=25 Z=26

1	14	15	14	9	13	1	20	15		3	15	13

5	14	3	1	13	9	14	8	1	13	5	14	20	15		15	14	9	15	14

19	5	7	21	18	15

Mensagem decifrada:

DICA: CADA NÚMERO REPRESENTA A POSIÇÃO DESSA LETRA NO ALFABETO (P. EX., 1 = A, 2 = B, 26 = Z).

Ponto de controlo 10: Perguntas frequentes básicas sobre cibersegurança (Parte A)

Revê perguntas e respostas comuns sobre a mitigação de ameaças online.

Q1: O que é a deep web?

A deep web é constituída por todas as páginas web que os motores de pesquisa não conseguem indexar, incluindo o homebanking, bases de dados de e-mail e revistas científicas com acesso pago.

Q2: O que é a dark web?

A dark web é um pequeno subconjunto da deep web, intencionalmente oculto e acessível apenas através de navegadores especializados que usam redes onion.

Q3: Como indexam os motores de pesquisa as páginas?

Os motores executam programas automatizados (spiders) para seguir ligações públicas, indexando as páginas que não bloqueiam o rastreamento através de diretivas de robots.

Q4: Porque é que a banca online é considerada parte da deep web?

Os portais bancários ficam atrás de ecrãs de início de sessão e palavras-passe, o que impede os motores de busca públicos de indexar as páginas de extratos de conta.

Q5: O que é o encaminhamento cebola (Onion Routing) do navegador Tor?

O encaminhamento cebola é um método de transmissão que encripta o tráfego em camadas e o faz passar por vários relays para ocultar os endereços IP dos utilizadores.

Ponto de controlo 10: Perguntas frequentes básicas sobre cibersegurança (Parte B)

Revê perguntas e respostas comuns sobre a mitigação de ameaças online.

Q6: Aceder à dark web é ilegal?

Não. Aceder à dark web é legal na maioria dos países, embora seja proibido participar em mercados ilegais ou em atividades cibernéticas ilegais.

Q7: Porque demoram a carregar os sítios da dark web?

O tráfego é encaminhado e desencriptado através de pelo menos três retransmissores globais (entrada, intermédio, saída), o que aumenta a latência de transmissão.

Q8: O que significa o sufixo de domínio .onion?

É um sufixo de domínio de topo especializado usado nas redes Tor, que aponta para endereços gerados criptograficamente em vez de servidores DNS normais.

Q9: Que riscos estão associados às ligações da dark web?

Os sites não têm qualquer verificação de segurança, expondo os utilizadores a elevadas taxas de infeção por software malicioso, scripts de phishing e fraudes em transações.

Q10: Quem criou o protocolo de encaminhamento da rede Tor?

A tecnologia foi originalmente desenvolvida pelo Laboratório de Investigação Naval dos EUA na década de 1990 para proteger as comunicações governamentais.

Ponto de controlo 10: Perguntas frequentes avançadas sobre segurança (Parte C)

Explora aspetos técnicos avançados das estruturas de segurança, da análise de malware e da conformidade de dados.

Q1: Como é que os nós intermédios protegem o anonimato no Tor?

Cada nó desencripta apenas uma camada dos dados de encaminhamento, conhecendo apenas o salto anterior e o seguinte, nunca a origem e o destino em simultâneo.

Q2: Qual é o papel do nó de saída?

O nó de saída desencripta a última camada de encriptação, enviando o tráfego para o servidor de destino público ou para o servidor onion.

Q3: O que é um gateway de pontes Tor?

As pontes (bridges) são relés de entrada Tor não listados, usados para contornar bloqueios do ISP e a censura em regiões que restringem o acesso ao browser Tor.

Q4: Como exploram os agentes da dark web as criptomoedas?

Os agentes usam criptomoedas anónimas para executar transações financeiras em mercados obscuros, evitando as verificações bancárias normais.

Q5: Porque falham os motores de pesquisa convencionais ao rastrear bases de dados profundas?

Os rastreadores não conseguem introduzir credenciais de início de sessão, resolver CAPTCHAs de segurança nem executar os scripts de consulta SQL de back-end necessários para aceder às bases de dados da deep web.

Ponto de controlo 10: Perguntas frequentes avançadas sobre segurança (Parte D)

Explora aspetos técnicos avançados das estruturas de segurança, da análise de malware e da conformidade de dados.

Q6: O que é um servidor de diretório nas redes Tor?

É um servidor de confiança que mantém a lista de relays de entrada, intermédios e de saída ativos usados pelos clientes para construir os caminhos de encaminhamento.

Q7: Como realizam os agentes maliciosos a interceção de tráfego em nós de saída?

Os operadores de nós de saída fraudulentos podem intercetar o tráfego HTTP não encriptado quando sai da rede Tor, roubando nomes de utilizador e cookies.

Q8: Qual é a diferença entre o Tor e o I2P?

A Tor usa um diretório centralizado de retransmissores e nós de saída para o acesso à web pública, enquanto a I2P usa uma estrutura descentralizada ponto a ponto para alojamento interno.

Q9: Como acompanham as autoridades policiais os mercados da dark web?

As autoridades usam análise de blockchain, localizam as instalações físicas de alojamento de servidores e realizam operações de isco para identificar os operadores.

Q10: Como é que a fuga de DNS compromete o anonimato do cliente?

As fugas de DNS ocorrem quando as consultas DNS do navegador são enviadas diretamente através do ISP local, em vez de serem encaminhadas pela rede Tor encriptada.

Parte 11: 10 factos e perspetivas do mundo real sobre cibersegurança

Revê factos reais sobre violações de segurança, mecanismos de defesa e normas de conformidade.

1. PERSPETIVA SOBRE SEGURANÇA

A deep web é muito maior do que a web de superfície pesquisável, pois a maior parte do conteúdo está atrás de inícios de sessão e bases de dados.

2. PERSPETIVA SOBRE SEGURANÇA

A dark web é uma parte pequena e intencionalmente oculta da deep web, acessível com ferramentas como o Tor.

3. PERSPETIVA SOBRE SEGURANÇA

O encaminhamento da Tor encripta os pacotes de dados três vezes, retirando camadas de encriptação como as de uma cebola em cada nó retransmissor.

4. PERSPETIVA SOBRE SEGURANÇA

A Tor nasceu do projeto de onion routing do Laboratório de Investigação Naval dos EUA, e o seu código foi divulgado como software livre. [1]

5. PERSPETIVA SOBRE SEGURANÇA

Os endereços Onion são cadeias alfanuméricas de 56 caracteres geradas criptograficamente a partir de pares de chaves públicas.

6. PERSPETIVA SOBRE SEGURANÇA

Os nós de saída conseguem ler o tráfego em texto simples, o que significa que o TLS/HTTPS continua a ser necessário no Tor para dados de sessão seguros.

7. PERSPETIVA SOBRE SEGURANÇA

Os sites de intranet, as unidades na nuvem e as bases de dados privadas representam os maiores segmentos de armazenamento de dados da deep web.

8. PERSPETIVA SOBRE SEGURANÇA

Motores de pesquisa especializados como o DuckDuckGo disponibilizam portais onion para permitir pesquisas anónimas nas redes Tor.

9. PERSPETIVA SOBRE SEGURANÇA

Mais de 2 milhões de utilizadores ligam-se diariamente à rede Tor para contornar a censura e manter a privacidade das comunicações.

10. PERSPETIVA SOBRE SEGURANÇA

Operações policiais globais (como a Operation Bayonet) encerram grandes mercados da dark web através da apreensão do hardware de alojamento.

Referências técnicas e fontes

O guia de estudo e os puzzles interativos são compilados a partir das normas globais do NIST, da OWASP e de conformidade em matéria de privacidade de dados.

REFERÊNCIAS ACADÉMICAS E DO SETOR

[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

Soluções: Ponto de controlo 1 - Escolha múltipla

1 **Indexação por motores de pesquisa** DEEP WEB — **Resposta correta: A**

NOTA PARA O PROFESSOR

As páginas da deep web estão protegidas por ecrãs de início de sessão e bases de dados, o que impede os rastreadores dos motores de pesquisa de as percorrerem. Citação: IETF RFC 3986.

2 **Acesso à Tor** DARK WEB — **Resposta correta: A**

NOTA PARA O PROFESSOR

A dark web é constituída por serviços onion ocultos, acessíveis apenas através de navegadores como o Tor. Fonte: IETF RFC 3986.

3 **Bases de dados profundas** BASES DE DADOS — **Resposta correta: A**

NOTA PARA O PROFESSOR

As contas protegidas por palavra-passe e os registos empresariais formam o maior segmento da deep web. Citação: NIST Digital Identity.

4 **Encaminhamento cebola** REDE TOR — **Resposta correta: A**

NOTA PARA O PROFESSOR

O encaminhamento cebola encripta os pacotes de dados em camadas, retransmitindo-os por vários nós para garantir o anonimato. Citação: IETF RFC 3986.

5 **Domínio Onion** SUFIXO — **Resposta correta: A**

NOTA PARA O PROFESSOR

O sufixo de domínio criptográfico.onion encaminha o tráfego internamente na Tor sem DNS público. Fonte: IETF RFC 3986.

Soluções: Ponto de controlo 2 - Verdadeiro ou falso

6 **Segmentos da Web** ESTRUTURA — **Resposta correta: Falso**

NOTA PARA O PROFESSOR

A deep web abrange todas as páginas não indexadas, enquanto a dark web é um pequeno subsegmento onion encriptado. Fonte: IETF RFC 3986.

7 **Intranets empresariais** DEEP WEB — **Resposta correta: Verdadeiro**

NOTA PARA O PROFESSOR

Os sites de intranet estão atrás de portais protegidos por palavra-passe e não são indexados, o que significa que pertencem à deep web. Citação: NIST Digital Identity.

8 **Encriptação por camadas** RETRANSMISSORES — **Resposta correta: Falso**

NOTA PARA O PROFESSOR

Os relays Onion só decifram uma camada de encaminhamento para proteger o anonimato do utilizador, nunca o pacote inteiro. Citação: IETF RFC 3986.

9 **Exposição a software malicioso** AMEAÇAS — **Resposta correta: Verdadeiro**

NOTA PARA O PROFESSOR

Os mercados da dark web não têm filtragem de segurança, apresentando riscos extremos de infeção por malware. Citação: Center for Internet Security (CIS).

10 **Pergunta 10** — **Resposta correta: Falso**

NOTA PARA O PROFESSOR

Os rastreadores normais dos motores de busca não utilizam o Tor, pelo que não conseguem aceder nem indexar sites .onion.

Soluções de vocabulário e grelha de avaliação

Grelha de classificação do professor: atribui 1 ponto por cada correspondência correta (8 pontos no total) e por cada termo de contexto (6 pontos no total).

PONTO DE CONTROLO 4: SOLUÇÕES – ASSOCIAÇÃO DE CONCEITOS

H 1. Segmento da deep web	A 2. Portal da dark web	D 3. Extensão Onion	B 4. Encaminhamento Tor
F 5. Páginas indexadas	G 6. Anonimato do utilizador	C 7. Base de dados privada	E 8. Gateway de entrada

PONTO DE CONTROLO 3: SOLUÇÕES – TERMOS-CHAVE

1 DEEP WEB	2 DARK WEB	3 EXTENSÃO ONION	4 ENCAMINHAMENTO
5 INDEXADAS	6 ANONIMATO		

PONTO DE CONTROLO 6, ALTERNATIVA: SOLUÇÕES – ASSOCIAÇÃO DE PALAVRAS

1 F – ANONIMATO	2 G – BASEDEDADOS	3 D – ENCAMINHAMENTO	4 A – DEEPWEB
5 B – DARKWEB	6 C – EXTENSAOONION	7 H – NODEENTRADA	8 E – INDEXADAS

NOTAS DE DEBATE PARA PROFESSORES

Termos-chave:
Verifica se os alunos sabem explicar Segmento da deep web, Portal da dark web e Extensão Onion por palavras suas e dar um exemplo de cada.

Estudos de caso:
Pede aos alunos que justifiquem as recomendações com factos da ficha e não com suposições.

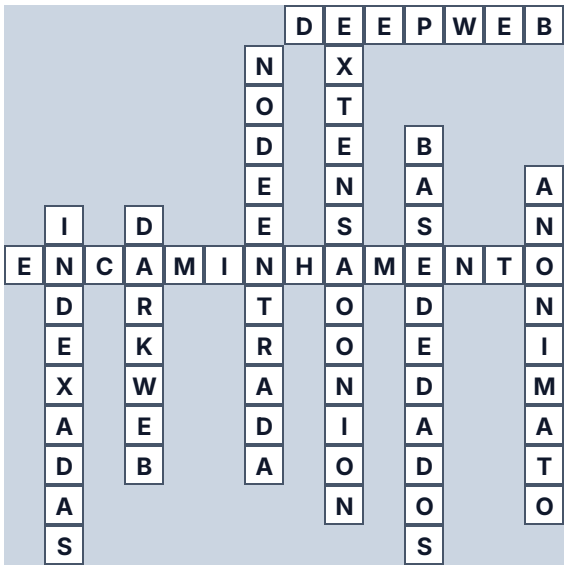
Avaliação das fontes:
Pede aos alunos que confirmem pelo menos uma afirmação nas fontes da ficha e discutam porque é que números, preços e regras podem mudar com o tempo.

Soluções dos puzzles e notas para o professor

SOLUÇÃO DO CAÇA-PALAVRAS

N	K	T	S	V	R	Z	E	H	E	S	C	A	L	Q
O	A	D	A	R	T	N	E	E	D	O	N	C	D	A
I	Z	M	K	D	A	R	K	W	E	B	V	E	N	R
N	U	A	S	I	W	J	M	M	H	H	E	O	N	H
O	R	F	K	N	T	L	R	W	H	P	N	B	U	F
O	Y	O	Y	D	W	S	H	T	W	I	X	A	P	U
A	N	N	Z	E	O	I	Q	E	M	T	I	P	V	U
S	O	U	U	X	K	A	B	A	E	P	M	K	A	N
N	V	G	G	A	P	Q	T	X	Y	J	K	V	J	Y
E	W	Y	P	D	J	O	I	Z	I	J	N	A	E	I
T	E	N	C	A	M	I	N	H	A	M	E	N	T	O
X	A	S	A	S	J	F	W	E	K	Z	K	E	K	Q
E	N	B	A	S	E	D	E	D	A	D	O	S	J	A
F	O	K	N	D	N	C	D	H	I	B	A	P	R	L
P	W	T	I	Y	F	Y	S	G	X	W	H	F	R	T

SOLUÇÃO DAS PALAVRAS CRUZADAS



GUIA DO PROFESSOR PARA AS SOLUÇÕES DAS PALAVRAS CRUZADAS

HORIZONTAIS

1 horizontal: DEEPWEB Conteúdo web não indexado, como inícios de sessão privados, emails e registos de bases de dados (7 letras)

8 horizontal: ENCAMINHAMENTO Encriptar os dados em camadas e retransmiti-los por três nós (14 letras)

VERTICAIS

2 vertical: EXTENSAOONION Sufixo criptográfico de domínio de topo usado nas redes Tor (13 letras)

3 vertical: NODEENTRADA Nó de entrada usado para aceder à rede Tor (11 letras)

4 vertical: BASEDEDADOS Armazenamento seguro de retaguarda que aloja registos do sistema não indexados (11 letras)

5 vertical: ANONIMATO Manter os endereços IP públicos dos clientes ocultos dos servidores (9 letras)

6 vertical: INDEXADAS Conteúdo da web de superfície compilado e pesquisável no Google (9 letras)

7 vertical: DARKWEB Segmento de rede encriptado, acessível apenas através de navegadores especiais (7 letras)

Palavras baralhadas e soluções da cifra

Chave de correção da atividade de reordenação de letras do vocabulário e do Desafio do Código Secreto.

CHAVE DE SOLUÇÕES DAS PALAVRAS EMBARALHADAS

1. PEDWBEE — **DEEPWEB**
2. ONXSTEIANONOE — **EXTENSAOONION**
3. IAXNDSEAD — **INDEXADAS**
4. DOSESDDABAE — **BASEDEDADOS**
5. WBKRDEA — **DARKWEB**
6. INEMCNHTMENAOA — **ENCAMINHAMENTO**
7. MATOANNIO — **ANONIMATO**
8. ATANDNEODRE — **NODEENTRADA**

CHAVE DO DESAFIO DO CÓDIGO SECRETO

"ANONIMATO COM ENCAMINHAMENTO ONION SEGURO"

Soluções dos estudos de caso

A Estudo de caso 1: Identificação de fugas de dados

Solução para o professor

CRITÉRIO DE CLASSIFICAÇÃO

As respostas dos alunos devem abranger os seguintes pontos:

- Análise do cenário: Uma auditoria de segurança empresarial descobre que registos sensíveis de uma base de dados de clientes estão a ser comercializados num mercado onion. Os dados não estão indexados no Google.
- Estratégia e solução recomendadas: Segmentos envolvidos: A base de dados privada pertence à deep web (não indexada mas segura). O mercado que comercializa os dados roubados está na dark web (rede onion). Como aconteceu: Os hackers contornaram as defesas do servidor, roubaram a base de dados da deep web e listaram-na anonimamente na dark web para escapar ao rastreio das autoridades.

B Estudo de caso 2: Anonimato vs. riscos de malware

Solução para o professor

CRITÉRIO DE CLASSIFICAÇÃO

As respostas dos alunos devem abranger os seguintes pontos:

- Análise do cenário: Um analista quer consultar feeds de informações sobre ameaças num site Tor. Transfere o navegador Tor e acede ao site.
- Estratégia e solução recomendadas: Benefícios: o Tor encaminha o tráfego por três nós, mascarando o IP empresarial do analista. Riscos e mitigação: as ligações da dark web não têm qualquer verificação de reputação. Os analistas devem executar o Tor dentro de máquinas virtuais (VM) isoladas, desativar o JavaScript nas definições do Tor e evitar transferir quaisquer ficheiros para proteger a rede empresarial.