Nome: _____ Data: _____ Punteggio: _____

Dark web e deep web: sicurezza e Differenze

Indicizzazione dei motori di ricerca, database del deep web, onion routing di Tor, anonimato in rete e rischi

PANORAMICA DI APPRENDIMENTO: DARK WEB E DEEP WEB A CONFRONTO

PROTETTO
CRITTOGRAFIA DEI DATI
Standard AES a 256 bit

CONFORME
STANDARD GLOBALI
Framework GDPR e CCPA

ZERO-TRUST
POLITICA DI ACCESSO
Autenticazione a più fattori

Benvenuto! Questo pacchetto di attività ti guida attraverso le differenze tra il Deep Web e il Dark Web. Esplorerai i database non indicizzati, l'Onion Routing del browser Tor, i domini crittografici .onion e i rischi di sicurezza legati all'anonimato.

PUNTI DI CONTROLLO DELLA SCHEDA DI LAVORO

- [ ] **Parti 1-4: Padroneggia la sicurezza informatica e la prevenzione delle minacce.**
- [ ] **Parti 5-7: Risolvi cruciverba e parole nascoste.**
- [ ] **Parti 8-9: Risolvi casi di studio e la sfida del codice.**
- [ ] **Parte 10: Consulta le pagine delle domande frequenti di base e avanzate.**
- [ ] **Parte 11: Esplora 10 fatti interessanti dal mondo reale.**
- [ ] **Bonus: sfida Pensa veloce.**

Apri la guida alla sicurezza informatica di VPN.com

URL: https://www.vpn.com/it/sicurezza-informatica/dark-web-vs-deep-web/

Il tuo percorso di apprendimento sulla strategia per deep web e dark web

- Confronta il deep web (database non indicizzati) con il dark web (servizi onion).
- Comprendi come l'Onion Routing cifra e inoltra il traffico di rete.
- Valuta i rischi di sicurezza dell'accesso a siti non verificati della rete Tor.
- Distribuisci policy di gateway e sandboxing per il crawling di threat intelligence.
- Analizza il formato dell'indirizzo crittografico dei domini dei servizi onion.

ISTRUZIONI DELLA GUIDA AL DEEP E DARK WEB

Rispondi alle domande a scelta multipla e vero/falso, completa le frasi con gli spazi vuoti usando l'elenco di parole, abbina le definizioni e risolvi il cruciverba e la ricerca di parole. Applica le tue conoscenze alla privacy nel deep web e nel dark web. Concludi con l'attività bonus Pensa veloce.

DATABASE DEL DEEP WEB E ONION ROUTING DEL DARK WEB (INTRODUZIONE)

Il deep web è costituito da pagine non indicizzate protette da password e accessi, come email private o portali bancari aziendali. Il dark web è un sottoinsieme del deep web nascosto intenzionalmente, a cui si accede in modo anonimo solo con browser specializzati (come Tor) e reti onion.

LEGGI CON ATTENZIONE OGNI PUNTO DI CONTROLLO E SELEZIONA O SCRIVI LA RISPOSTA CORRETTA.

Punto di controllo 1: Sfida a scelta multipla

1. Che cosa distingue il deep web dal surface web?

- A. Le pagine del deep web non sono indicizzate dai motori di ricerca pubblici
- B. Il traffico del deep web è illegale e monitorato dalle forze dell'ordine
- C. I siti del deep web richiedono browser specializzati come Tor per essere raggiunti
- D. Le pagine del deep web si caricano sempre più velocemente delle pagine del web di superficie

2. Come si accede al dark web?

- A. Tramite browser specializzati che usano reti di onion routing
- B. Configurando impostazioni DNS personalizzate sui router standard
- C. Tramite console di ricerca del web di superficie private, solo su invito
- D. Installando una normale estensione del browser per bloccare gli annunci

3. Quale struttura costituisce la parte più grande del deep web?

- A. Database utente e account privati protetti da password
- B. Forum illegali del mercato nero che commerciano beni illeciti
- C. Protocolli di condivisione file peer-to-peer non cifrati
- D. Database della cache pubblica dei motori di ricerca

4. Che cosa fa l'Onion Routing al traffico di rete?

- A. Cifra i pacchetti e li instrada attraverso più relay
- B. Aumenta le velocità di download aggirando i nodi dell'ISP
- C. Associa i numeri di serie dell'hardware dei dispositivi ai record IP
- D. Elimina i cookie del browser web dopo ogni clic

5. Quale suffisso di dominio è usato esclusivamente sulle reti Tor?

- A. L'estensione di primo livello crittografica .onion
- B. La storica estensione commerciale .com
- C. L'estensione blockchain decentralizzata Web3 .eth
- D. L'estensione tecnologica .ai del codice Paese

Punto di controllo 2: Sfida Vero o Falso

6 Domanda V/F 6

6. Il deep web e il dark web indicano lo stesso segmento di rete.

- ◯ Vero
- ◯ Falso

7 Domanda V/F 7

7. I portali intranet aziendali fanno parte del deep web.

- ◯ Vero
- ◯ Falso

8 Domanda V/F 8

8. L'onion routing decifra completamente i pacchetti di dati a ogni nodo di transito.

- ◯ Vero
- ◯ Falso

9 Domanda V/F 9

9. Accedere al dark web espone i dispositivi a elevati rischi di malware.

- ◯ Vero
- ◯ Falso

10 Domanda V/F 10

10. I normali motori di ricerca web scansionano e indicizzano i siti onion.

- ◯ Vero
- ◯ Falso

Punto di controllo 3: Inserimento dei termini chiave

Leggi ogni frase qui sotto e completa lo spazio vuoto con il termine corretto dell'elenco di parole.

1. I portali bancari privati risiedono nel segmento non indicizzato del _____ .
2. Nodi Tor specializzati ospitano servizi nascosti del _____ .
3. I siti Tor usano l'estensione di primo livello crittografica _____ .
4. Il percorso del traffico cifrato a più livelli si chiama _____ .
5. I motori di ricerca di superficie scansionano le pagine pubblicamente _____ .
6. Le reti Onion cifrano gli IP dei client per mantenere l' _____ dell'utente.

BANCA DELLE PAROLE DEL VOCABOLARIO

ANONIMATO DARK WEB DATABASE DEEP WEB INDICIZZATE
NODO DI INGRESSO ONION ROUTING

Scrivi qui le tue risposte:

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

Punto di controllo 4: Abbinamento di concetti sulla sicurezza

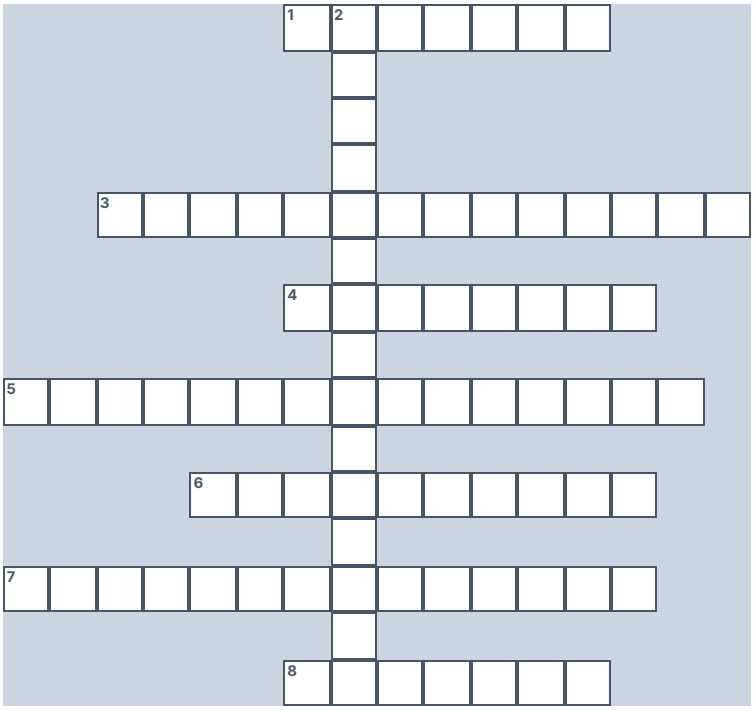
ABBINAMENTO DELLE DEFINIZIONI

Abbina ogni termine del vocabolario a sinistra alla sua definizione corretta a destra scrivendo la lettera corrispondente (A-H) nella casella compilabile.

☐	**1. Segmento del Deep Web**	**A**	Segmento di rete cifrato accessibile solo tramite browser speciali.
☐	**2. Portale del Dark Web**	**B**	Cifrare i dati a strati e inoltrarli attraverso tre nodi.
☐	**3. Estensione Onion**	**C**	Archiviazione backend sicura che ospita record di sistema non indicizzati.
☐	**4. Instradamento Tor**	**D**	Suffisso di dominio di primo livello crittografico usato sulle reti Tor.
☐	**5. Pagine indicizzate**	**E**	Il nodo del punto di ingresso usato per accedere alla rete Tor.
☐	**6. Anonimato dell'utente**	**F**	Contenuti del web di superficie raccolti e ricercabili su Google.
☐	**7. Database privato**	**G**	Mantenere nascosti ai server gli indirizzi IP pubblici dei client.
☐	**8. Gateway di ingresso**	**H**	Contenuti web non indicizzati come accessi privati, email e record di database.

Punto di controllo 5: Cruciverba

Risolvi il cruciverba digitando le lettere nelle caselle bianche attive. I numeri corrispondono alle definizioni qui sotto.



ORIZZONTALI

1. Segmento di rete cifrato accessibile solo tramite browser speciali (7)

3. Contenuti del web di superficie raccolti e ricercabili su Google (14)

4. Archiviazione backend sicura che ospita i record di sistema non indicizzati (8)

5. Suffisso di dominio di primo livello crittografico usato nelle reti Tor (15)

6. Cifratura dei dati a strati e inoltro attraverso tre nodi (10)

7. Il nodo d'ingresso usato per accedere alla rete Tor (14)

8. Contenuti web non indicizzati come accessi privati, email e record di database (7)

VERTICALI

2. Mantenere nascosti ai server gli indirizzi IP pubblici dei client (15)

Punto di controllo 5, alternativa: Indizi accessibili del cruciverba

Gli utenti di screen reader e di tastiera possono digitare le risposte del cruciverba direttamente nei campi di testo qui sotto.

ORIZZONTALI

1 orizzontale: Segmento di rete cifrato accessibile solo tramite browser speciali (7 lettere):

3 orizzontale: Contenuti del web di superficie raccolti e ricercabili su Google (14 lettere):

4 orizzontale: Archiviazione backend sicura che ospita i record di sistema non indicizzati (8 lettere):

5 orizzontale: Suffisso di dominio di primo livello crittografico usato nelle reti Tor (15 lettere):

6 orizzontale: Cifratura dei dati a strati e inoltro attraverso tre nodi (10 lettere):

7 orizzontale: Il nodo d'ingresso usato per accedere alla rete Tor (14 lettere):

8 orizzontale: Contenuti web non indicizzati come accessi privati, email e record di database (7 lettere):

VERTICALI

2 verticale: Mantenere nascosti ai server gli indirizzi IP pubblici dei client (15 lettere):

Punto di controllo 6: Cerca la parola nascosta

Trova gli 8 termini chiave del vocabolario nascosti nella griglia qui sotto. Le parole possono essere orizzontali, verticali o diagonali.

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

ELENCO DELLE PAROLE DEL VOCABOLARIO

DEEPWEB DARKWEB ESTENSIONEONION ROUTINGTOR INDICIZZAZIONE
ANONIMATOUTENTE DATABASE NODODIINGRESSO

Punto di controllo 6, alternativa: Abbinamento accessibile del vocabolario

Abbina ciascuno degli 8 termini del vocabolario della Ricerca di parole alla sua definizione corretta scrivendo la lettera (A-H) nello spazio vuoto.

TERMINI DEL VOCABOLARIO
A. DEEPWEB
B. DARKWEB
C. ESTENSIONEONION
D. ROUTINGTOR
E. INDICIZZAZIONE
F. ANONIMATOUTENTE
G. DATABASE
H. NODODIINGRESSO

DEFINIZIONI E CAMPI DI ABBINAMENTO

_____ 1. Mantenere nascosti ai server gli indirizzi IP pubblici dei client.

_____ 2. Archiviazione backend sicura che ospita i record di sistema non indicizzati.

_____ 3. Cifratura dei dati a strati e inoltro attraverso tre nodi.

_____ 4. Contenuti web non indicizzati come accessi privati, email e record di database.

_____ 5. Segmento di rete cifrato accessibile solo tramite browser speciali.

_____ 6. Suffisso di dominio di primo livello crittografico usato nelle reti Tor.

_____ 7. Il nodo d'ingresso usato per accedere alla rete Tor.

_____ 8. Contenuti del web di superficie raccolti e ricercabili su Google.

Punto di controllo 7: Sfida delle parole mescolate

Riordina le lettere qui sotto per scoprire concetti e termini chiave della sicurezza informatica. Scrivi le tue risposte nelle caselle fornite.

1. PEDWBEE
2. SSEITOIENOE ONNN
3. IANNZEZIDZC IOI
4. ASEABDAT
5. WBKRDEA
6. OITGTRONRU
7. UTAOAENOEM NTNTI
8. ONSIGROONI DSED

Attività bonus: Pensa veloce

3 RISPOSTE PER CATEGORIA. VINCE CHI COMPLETA PER PRIMO LA LISTA.

1	Motivi per stare alla larga dal dark web			
2	Cose che un motore di ricerca non riesce a trovare			
3	Dispositivi che possono essere hackerati			
4	Motivi legali per usare Tor			
5	Motivi per aggiornare il software			
6	Segnali di allarme in un'email			
7	Cose vendute illegalmente sul dark web			
8	Persone a cui puoi chiedere aiuto per l'IT			
9	Buone abitudini sicure che puoi iniziare oggi			
10	Cose da fare dopo una fuga di dati			
11	Cose che appartengono al deep web			
12	Siti che usi con un login			
13	Parole legate all'anonimato			
14	Informazioni che non dovresti mai condividere			
15	Cose che si trovano 'sotto la superficie'			

Punto di controllo 8: Casi di studio sulla sicurezza informatica

Applica i concetti che hai imparato per risolvere gli scenari reali qui sotto.

CASO DI STUDIO 1: INDIVIDUARE UNA FUGA DI DATI



Scenario: Un audit di sicurezza aziendale scopre che record sensibili di un database di clienti vengono scambiati su un marketplace onion. I dati non sono indicizzati su Google.

Domanda di discussione: Spiega quali segmenti del web sono coinvolti e come è avvenuta questa fuga di dati.

CASO DI STUDIO 2: ANONIMATO E RISCHI DEL MALWARE A CONFRONTO



Scenario: Un analista vuole controllare i feed di threat intelligence su un sito Tor. Scarica il browser Tor e accede al sito.

Domanda di discussione: Valuta i vantaggi in termini di anonimato e illustra i passaggi per mitigare il malware.

Punto di controllo 9: Decifrare il codice

Un professionista della sicurezza informatica protegge le risorse di rete dagli attori delle minacce online. Usa la chiave lettera-numero qui sotto per decifrare il messaggio scrivendo le lettere corrispondenti negli spazi vuoti.

CHIAVE DI CIFRATURA LETTERA-NUMERO

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

13	1	14	20	9	5	14	9		1	14	15	14	9	13	1	20	15
3	15	14		18	15	21	20	9	14	7		15	14	9	15	14
				19	9	3	21	18	15							

Messaggio decifrato:

SUGGERIMENTO: OGNI NUMERO RAPPRESENTA LA POSIZIONE DI QUELLA LETTERA NELL'ALFABETO (AD ES. 1 = A, 2 = B, 26 = Z).

Punto di controllo 10: Domande frequenti di base sulla sicurezza informatica (Parte A)

Rivedi domande e risposte comuni sulla mitigazione delle minacce online.

Q1: Che cos'è il deep web?

Il deep web è costituito da tutte le pagine web che i motori di ricerca non possono indicizzare, tra cui home banking, database di posta elettronica e riviste a pagamento.

Q2: Che cos'è il dark web?

Il dark web è un piccolo sottoinsieme del deep web, intenzionalmente nascosto e accessibile solo tramite browser specializzati che usano reti onion.

Q3: Come indicizzano le pagine i motori di ricerca?

I motori eseguono programmi automatici (spider) per seguire i link pubblici, indicizzando le pagine che non bloccano la scansione tramite direttive per i robot.

Q4: Perché l'online banking è considerato parte del deep web?

I portali bancari si trovano dietro schermate di accesso e password, che impediscono ai motori di ricerca pubblici di indicizzare le pagine degli estratti conto.

Q5: Cos'è l'Onion Routing del browser Tor?

L'onion routing è un metodo di trasmissione che cifra il traffico a livelli e lo fa passare attraverso più relay per mascherare gli indirizzi IP degli utenti.

Punto di controllo 10: Domande frequenti di base sulla sicurezza informatica (Parte B)

Rivedi domande e risposte comuni sulla mitigazione delle minacce online.

Q6: Accedere al dark web è illegale?

No. L'accesso al dark web è legale nella maggior parte dei paesi, anche se è vietato partecipare a mercati illegali o ad attività informatiche illecite.

Q7: Perché i siti del dark web si caricano lentamente?

Il traffico viene instradato e decifrato attraverso almeno tre relay globali (ingresso, intermedio, uscita), il che aumenta la latenza di trasmissione.

Q8: Cosa significa il suffisso di dominio .onion?

È un suffisso di dominio di primo livello specializzato usato sulle reti Tor, che punta a indirizzi generati crittograficamente anziché ai normali server DNS.

Q9: Quali rischi comportano i link del dark web?

I siti non hanno alcun controllo di sicurezza, esponendo gli utenti a elevati tassi di infezione da malware, script di phishing e truffe nelle transazioni.

Q10: Chi ha creato il protocollo di routing della rete Tor?

La tecnologia è stata sviluppata originariamente dal Naval Research Laboratory degli Stati Uniti negli anni '90 per proteggere le comunicazioni governative.

Punto di controllo 10: Domande frequenti avanzate sulla sicurezza (Parte C)

Esplora gli aspetti tecnici avanzati dei framework di sicurezza, dell'analisi del malware e della conformità dei dati.

Q1: Come proteggono i nodi intermedi l'anonimato su Tor?

Ogni nodo decifra un solo livello dei dati di instradamento, conoscendo soltanto il salto precedente e quello successivo, mai sia l'origine sia la destinazione.

Q2: Qual è il ruolo del nodo di uscita?

Il nodo di uscita decifra l'ultimo livello di crittografia e invia il traffico verso il server di destinazione pubblico o verso il server onion.

Q3: Cos'è un gateway di bridge Tor?

I bridge sono relay di ingresso Tor non elencati, usati per aggirare i blocchi dell'ISP e la censura nelle regioni che limitano l'accesso al browser Tor.

Q4: Come sfruttano le criptovalute gli attori del dark web?

Gli attori usano criptovalute anonime per eseguire transazioni finanziarie sui mercati del dark web, eludendo i normali controlli delle transazioni bancarie.

Q5: Perché i normali motori di ricerca non riescono a scansionare i database profondi?

I crawler non possono inserire credenziali di accesso, risolvere i CAPTCHA di sicurezza o eseguire gli script di query SQL di back-end necessari per accedere ai database del deep web.

Punto di controllo 10: Domande frequenti avanzate sulla sicurezza (Parte D)

Esplora gli aspetti tecnici avanzati dei framework di sicurezza, dell'analisi del malware e della conformità dei dati.

Q6: Cos'è un server di directory nelle reti Tor?

È un server attendibile che mantiene l'elenco dei relay di ingresso, intermedi e di uscita attivi, usato dai client per costruire i percorsi di instradamento.

Q7: Come eseguono lo sniffing sui nodi di uscita gli attori malevoli?

Gli operatori di nodi di uscita non autorizzati possono intercettare il traffico HTTP non crittografato quando lascia la rete Tor, rubando nomi utente e cookie.

Q8: Qual è la differenza tra Tor e I2P?

Tor usa una directory centralizzata di relay e nodi di uscita per l'accesso al web pubblico, mentre I2P usa una struttura peer-to-peer decentralizzata per l'hosting interno.

Q9: Come tracciano i mercati del dark web le forze dell'ordine?

Le agenzie usano l'analisi della blockchain, individuano le configurazioni fisiche di hosting dei server ed eseguono operazioni esca per identificare gli operatori.

Q10: In che modo la perdita DNS compromette l'anonimato del client?

Le fughe di DNS si verificano quando le richieste DNS del browser vengono inviate direttamente tramite l'ISP locale anziché essere instradate attraverso la rete Tor cifrata.

Parte 11: 10 fatti e spunti reali sulla sicurezza informatica

Rivedi fatti reali su violazioni della sicurezza, meccanismi di difesa e standard di conformità.

1. APPROFONDIMENTO SULLA SICUREZZA

Il deep web è molto più vasto del web di superficie consultabile, perché la maggior parte dei contenuti si trova dietro accessi e database.

2. APPROFONDIMENTO SULLA SICUREZZA

Il dark web è una piccola parte del deep web, intenzionalmente nascosta, raggiungibile con strumenti come Tor.

3. APPROFONDIMENTO SULLA SICUREZZA

L'instradamento di Tor cifra i pacchetti di dati tre volte, rimuovendo a ogni nodo di inoltro uno strato di crittografia come le foglie di una cipolla.

4. APPROFONDIMENTO SULLA SICUREZZA

Tor è nato dal progetto di onion routing del Naval Research Lab degli Stati Uniti e il suo codice è stato rilasciato come software libero. [1]

5. APPROFONDIMENTO SULLA SICUREZZA

Gli indirizzi onion sono stringhe alfanumeriche di 56 caratteri generate crittograficamente da coppie di chiavi pubbliche.

6. APPROFONDIMENTO SULLA SICUREZZA

I nodi di uscita possono leggere il traffico in chiaro, il che significa che su Tor servono comunque TLS/HTTPS per i dati di sessione sicuri.

7. APPROFONDIMENTO SULLA SICUREZZA

I siti intranet, i cloud drive e i database privati rappresentano i più grandi segmenti di archiviazione dei dati nel deep web.

8. APPROFONDIMENTO SULLA SICUREZZA

Motori di ricerca specializzati come DuckDuckGo gestiscono portali onion per consentire ricerche anonime sulle reti Tor.

9. APPROFONDIMENTO SULLA SICUREZZA

Oltre 2 milioni di utenti si connettono ogni giorno alla rete Tor per aggirare la censura e mantenere la privacy delle comunicazioni.

10. APPROFONDIMENTO SULLA SICUREZZA

Le operazioni globali delle forze dell'ordine (come l'Operation Bayonet) chiudono i principali mercati del dark web sequestrando l'hardware di hosting.

Riferimenti tecnici e fonti

La guida di studio e i puzzle interattivi sono compilati a partire dagli standard globali NIST, OWASP e di conformità alla privacy dei dati.

RIFERIMENTI ACCADEMICI E DI SETTORE

[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

Soluzioni: Punto di controllo 1 – Scelta multipla

1 **Indicizzazione dei motori di ricerca** DEEP WEB Risposta corretta: A

NOTA DIDATTICA

Le pagine del deep web si trovano dietro pagine di login e database, che impediscono ai crawler dei motori di ricerca di scansionarle. Citazione: IETF RFC 3986.

2 **Accesso a Tor** DARK WEB Risposta corretta: A

NOTA DIDATTICA

Il dark web è costituito da servizi onion nascosti, accessibili solo tramite browser come Tor. Citazione: IETF RFC 3986.

3 **Database profondi** DATABASE Risposta corretta: A

NOTA DIDATTICA

Gli account protetti da password e i registri aziendali costituiscono il segmento più grande del deep web. Fonte: NIST Digital Identity.

4 **Onion routing** RETE TOR Risposta corretta: A

NOTA DIDATTICA

L'onion routing cifra i pacchetti di dati a livelli, inoltrandoli attraverso più nodi per garantire l'anonimato. Fonte: IETF RFC 3986.

5 **Dominio Onion** SUFFISSO Risposta corretta: A

NOTA DIDATTICA

Il suffisso di dominio crittografico.onion instrada il traffico internamente su Tor senza DNS pubblico. Citazione: IETF RFC 3986.

Soluzioni: Punto di controllo 2 – Vero o falso

6 **Segmenti web** STRUTTURA — **Risposta corretta: Falso**

NOTA DIDATTICA

Il deep web comprende tutte le pagine non indicizzate, mentre il dark web è un piccolo sottosegmento onion cifrato. Citazione: IETF RFC 3986.

7 **Intranet aziendali** DEEP WEB — **Risposta corretta: Vero**

NOTA DIDATTICA

I siti intranet si trovano dietro portali protetti da password e non sono indicizzati, quindi appartengono al deep web. Citazione: NIST Digital Identity.

8 **Crittografia a livelli** RELAY — **Risposta corretta: Falso**

NOTA DIDATTICA

I relay onion decifrano un solo livello di instradamento per proteggere l'anonimato dell'utente, mai l'intero pacchetto. Fonte: IETF RFC 3986.

9 **Esposizione al malware** MINACCE — **Risposta corretta: Vero**

NOTA DIDATTICA

I marketplace del dark web non hanno alcun filtro di sicurezza e comportano rischi estremi di infezione da malware. Citazione: Center for Internet Security (CIS).

10 **Domanda 10** — **Risposta corretta: Falso**

NOTA DIDATTICA

I normali crawler dei motori di ricerca non usano Tor, quindi non possono raggiungere né indicizzare i siti .onion.

Chiavi del vocabolario e griglia di valutazione

Griglia di valutazione per l'insegnante: assegna 1 punto per ogni abbinamento corretto (8 punti in totale) e per ogni termine di contesto (6 punti in totale).

PUNTO DI CONTROLLO 4: SOLUZIONI ABBINAMENTO DI CONCETTI

H 1. Segmento del Deep Web	A 2. Portale del Dark Web	D 3. Estensione Onion	B 4. Instradamento Tor
F 5. Pagine indicizzate	G 6. Anonimato dell'utente	C 7. Database privato	E 8. Gateway di ingresso

PUNTO DI CONTROLLO 3: SOLUZIONI TERMINI CHIAVE

1 DEEP WEB	2 DARK WEB	3 ONION	4 ROUTING
5 INDICIZZATE	6 ANONIMATO		

PUNTO DI CONTROLLO 6, ALTERNATIVA: SOLUZIONI ABBINAMENTO DI PAROLE

1 F – ANONIMATOUTENTE	2 G – DATABASE	3 D – ROUTINGTOR	4 A – DEEPWEB
5 B – DARKWEB	6 C – ESTENSIONEONION	7 H – NODODIINGRESSO	8 E – INDICIZZAZIONE

NOTE DI DISCUSSIONE PER GLI INSEGNANTI

Termini chiave:
Verifica che gli studenti sappiano spiegare Segmento del Deep Web, Portale del Dark Web e Estensione Onion con parole proprie e fare un esempio per ciascuno.

Casi di studio:
Chiedi agli studenti di motivare le loro raccomandazioni con fatti tratti dalla scheda anziché con supposizioni.

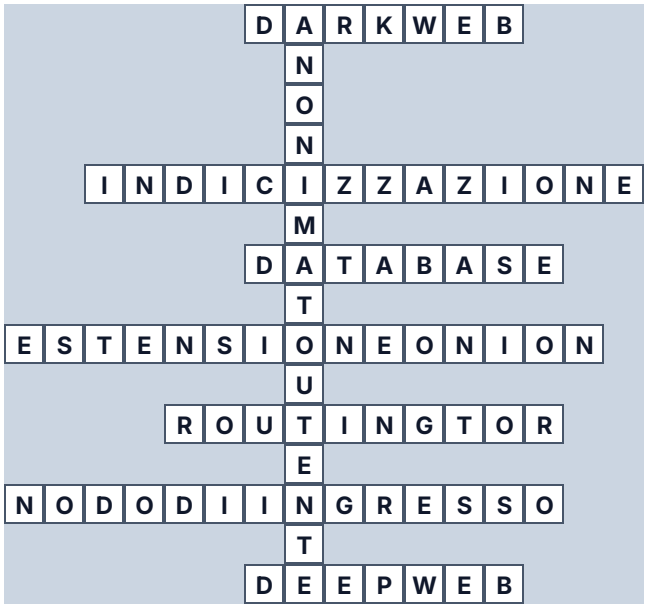
Valutazione delle fonti:
Fai verificare almeno un'affermazione con le fonti della scheda e discuti perché cifre, prezzi e regole possono cambiare nel tempo.

Soluzioni dei rompicapi e note per l'insegnante

SOLUZIONE DELLA RICERCA DELLE PAROLE

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

SOLUZIONE DEL CRUCIVERBA



GUIDA PER L'INSEGNANTE: SOLUZIONI DEL CRUCIVERBA

ORIZZONTALI

1 orizzontale: DARKWEB Segmento di rete cifrato accessibile solo tramite browser speciali (7 lettere)

3 orizzontale: INDICIZZAZIONE Contenuti del web di superficie raccolti e ricercabili su Google (14 lettere)

4 orizzontale: DATABASE Archiviazione backend sicura che ospita i record di sistema non indicizzati (8 lettere)

5 orizzontale: ESTENSIONEONION Suffisso di dominio di primo livello crittografico usato nelle reti Tor (15 lettere)

6 orizzontale: ROUTINGTOR Cifratura dei dati a strati e inoltro attraverso tre nodi (10 lettere)

7 orizzontale: NODODIINGRESSO Il nodo d'ingresso usato per accedere alla rete Tor (14 lettere)

8 orizzontale: DEEPWEB Contenuti web non indicizzati come accessi privati, email e record di database (7 lettere)

VERTICALI

2 verticale: ANONIMATOUTENTE Mantenere nascosti ai server gli indirizzi IP pubblici dei client (15 lettere)

Soluzioni delle parole mescolate e del codice cifrato

Chiave di valutazione per l'attività di riordino delle parole del vocabolario e per la sfida del codice segreto.

CHIAVE DELLE PAROLE DA RIORDINARE

1. PEDWBEE — **DEEPWEB**
2. SSEITOIENOEONNN — **ESTENSIONEONION**
3. IANNZEZIDZCIOI — **INDICIZZAZIONE**
4. ASEABDAT — **DATABASE**
5. WBKRDEA — **DARKWEB**
6. OITGTRONRU — **ROUTINGTOR**
7. UTAOAENOEMNTNTI — **ANONIMATOUTENTE**
8. ONSIGROONIDSED — **NODODIINGRESSO**

CHIAVE DELLA SFIDA DEL CODICE SEGRETO

"MANTIENI ANONIMATO CON ROUTING ONION SICURO"

Soluzioni dei casi di studio

A Caso di studio 1: individuare una fuga di dati

Soluzione per l'insegnante

LINEA GUIDA DI VALUTAZIONE

Le risposte degli studenti dovrebbero coprire i seguenti punti:

- Analisi dello scenario: un audit di sicurezza aziendale scopre che record sensibili di database di clienti vengono scambiati su un mercato onion. I dati non sono indicizzati su Google.
- Strategia e soluzione consigliate: Segmenti coinvolti: il database privato appartiene al deep web (non indicizzato ma sicuro). Il mercato che scambia i dati rubati si trova sul dark web (rete onion). Come è successo: gli hacker hanno aggirato le difese del server, hanno rubato il database dal deep web e lo hanno messo in vendita in modo anonimo sul dark web per sfuggire al tracciamento delle forze dell'ordine.

B Caso di studio 2: Anonimato e rischi del malware a confronto

Soluzione per l'insegnante

LINEA GUIDA DI VALUTAZIONE

Le risposte degli studenti dovrebbero coprire i seguenti punti:

- Analisi dello scenario: un analista vuole controllare i feed di threat intelligence su un sito Tor. Scarica il browser Tor e accede al sito.
- Strategia e soluzione consigliate: vantaggi: Tor instrada il traffico attraverso tre nodi, mascherando l'IP aziendale dell'analista. Rischi e mitigazione: i link del dark web non hanno alcuna verifica reputazionale. Gli analisti devono eseguire Tor all'interno di macchine virtuali (VM) isolate, disattivare JavaScript nelle impostazioni di Tor ed evitare di scaricare qualsiasi file per proteggere la rete aziendale.