Jméno: _____ Datum: _____ Body: _____

Úniky hesel a zabezpečení přihlašovacích údajů

Credential stuffing, úniky dat, hashovací algoritmy, vícefaktorová autentizace a zabezpečení hesel.

PŘEHLED VÝUKY: ÚNIKY HESEL

ZABEZPEČENO

ŠIFROVÁNÍ DAT

Standard 256bitového AES

VYHOVUJÍCÍ

GLOBÁLNÍ STANDARDY

Rámce GDPR a CCPA

ZERO-TRUST

ZÁSADY PŘÍSTUPU

Vícefaktorové ověřování

Vítejte! Tento balíček aktivit vás provede úniky hesel a zabezpečením přihlašovacích údajů. Prozkoumáte credential stuffing, úniky dat, hashovací algoritmy, vícefaktorové ověřování a správce hesel.

KONTROLNÍ BODY PRACOVNÍHO LISTU

- [ ] **Část 1-4: Zvládněte kyberbezpečnost a prevenci hrozeb.**
- [ ] **Část 5-7: Vyřešte křížovku a osmisměrku.**
- [ ] **Část 8-9: Vyřešte případové studie a šifrovací výzvu.**
- [ ] **Část 10: Projděte si stránky se základními i pokročilými FAQ.**
- [ ] **Část 11: Prozkoumejte 10 zajímavých faktů z praxe.**
- [ ] **Bonus: výzva Mysli rychle.**

Otevřete průvodce kyberbezpečností od VPN.com

URL: https://www.vpn.com/cs/kyberneticka-bezpecnost/unik-hesel/

Váš studijní plán: zabezpečení hesel

- Pochopte rizika odhalení přihlašovacích údajů na fórech dark webu.
- Zaveďte vícefaktorové ověřování (MFA) a monitorování kompromitovaných přihlašovacích údajů.
- Navrhněte firemní bezpečnostní obranu proti cíleným podvodům sociálního inženýrství.

POKYNY K PRŮVODCI ÚNIKY HESEL

Odpovězte na otázky s výběrem odpovědí a otázky pravda/nepravda, doplňte věty s vynechanými slovy pomocí banky slov, přiřaďte definice a vyřešte křížovku a osmisměrku. Uplatněte své znalosti na ochranu přihlašovacích údajů. Zakončete bonusovou aktivitou Mysli rychle.

ÚNIKY HESEL A ZABEZPEČENÍ PŘIHLAŠOVACÍCH ÚDAJŮ (ÚVOD)

Úniky hesel odhalují přihlašovací údaje uživatelů na veřejných webech a na dark webu. Jedinečná hesla ze správce hesel, kontrola hesel proti známým únikům a vícefaktorové ověřování (MFA) snižují riziko útoků typu credential stuffing, zatímco solené, pomalé hashování hesel omezuje škody, pokud je databáze hesel odcizena.

PŘEČTĚTE SI POZORNĚ KAŽDÝ KONTROLNÍ BOD A VYBERTE NEBO NAPIŠTE SPRÁVNOU ODPOVĚĎ.

Kontrolní bod 1: Výzva s výběrem odpovědí

1 **1. Co je credential stuffing?**

- A. Automatizované zkoušení uniklých kombinací jména a hesla na více webech
- B. Šifrování místních úložných souborů databáze
- C. Zahlcování webových serverů požadavky síťového provozu
- D. Tajné sledování stisků kláves

2 **2. Který algoritmus OWASP v současnosti uvádí jako svou první volbu pro ukládání hesel?**

- A. Argon2id
- B. MD5
- C. SHA-1
- D. ROT13

3 **3. Jak vícefaktorové ověřování (MFA) zmírňuje riziko úniků hesel?**

- A. Vyžaduje další ověřovací faktor, takže samotné ukradené heslo nestačí
- B. Automaticky mění heslo každou hodinu
- C. Šifruje uživatelské jméno při přenosu
- D. Upozorňuje úvěrový registr na podvodné žádosti

4 **4. Co je výpis dat z úniku (data breach dump)?**

- A. Sbírka uniklých přihlašovacích údajů uživatelů zveřejněná online nebo prodávaná na hackerských fórech
- B. Záložní kopie databázových souborů uložená mimo pracoviště
- C. Dočasná mezipaměť logů webového serveru
- D. Administrátorský nástroj pro resetování uživatelských hesel

5 **5. Jaká je role správce hesel?**

- A. Generování a ukládání jedinečných, silných hesel pro každý účet
- B. Sledování síťového provozu kvůli únikům hesel
- C. Blokování automatizovaných brute-force útoků na bráně
- D. Skenování databázových bloků úložiště kvůli nešifrovaným heslům

Kontrolní bod 2: Výzva Pravda/Nepravda

6 Otázka 6

6. Opakované používání hesel napříč účty zvyšuje riziko credential stuffingu.

○ Pravda ○ Nepravda

7 Otázka 7

7. SHA-1 je doporučená hashovací funkce pro moderní ukládání hesel.

○ Pravda ○ Nepravda

8 Otázka 8

8. Samotné vynucení složitosti hesel (bez MFA) zcela zastaví credential stuffing.

○ Pravda ○ Nepravda

9 Otázka 9

9. Nástroje pro monitoring temného webu prohledávají internet a hledají kompromitované firemní přihlašovací údaje.

○ Pravda ○ Nepravda

10 Otázka 10

10. Solené hashe přidávají k heslům před hashováním jedinečná náhodná data, čímž maří útoky pomocí rainbow tables.

○ Pravda ○ Nepravda

Kontrolní bod 3: Doplňování klíčových pojmů

Přečtěte si každou větu níže a doplňte do vynechaného místa správný termín ze slovní banky.

1. Zkoušení uniklých údajů napříč mnoha webovými aplikacemi je credential _____ .
2. Pomalý adaptivní algoritmus hašování hesel stále uznávaný OWASP je _____ .
3. Odhalení důvěrných databázových souborů na internetu je datový _____ .
4. Přidávání náhodných hodnot k heslům před hašováním se nazývá _____ .
5. Bezpečná lokální databáze přihlašovacích údajů je _____ hesel.
6. Přidání druhého ověřovacího kroku při přihlášení využívá _____ .

ZÁSOBNÍK SLOV

BCRYPT DUHOVÁ MFA PHISHING SOLENÍ SPRÁVCE STUFFING ÚNIK

Sem napište své odpovědi:

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

Kontrolní bod 4: Přiřazování bezpečnostních pojmů

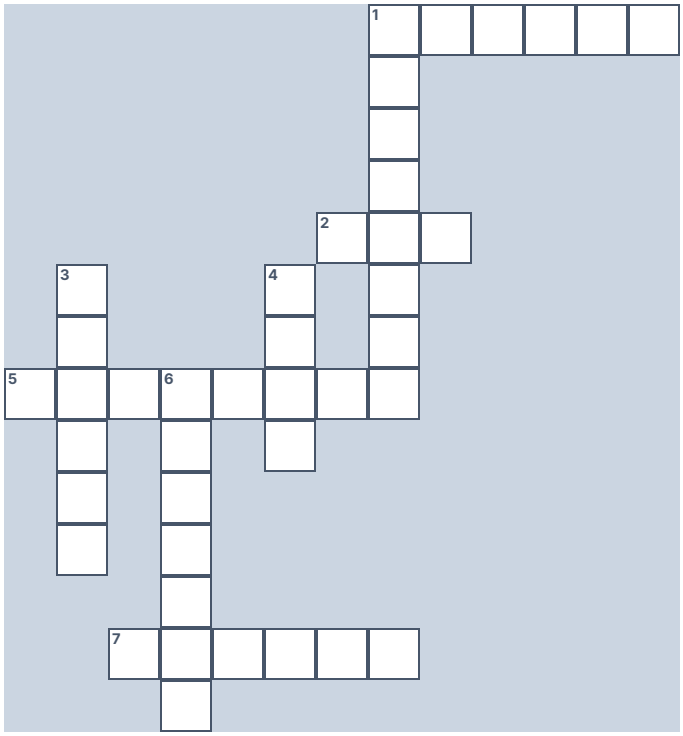
PŘIŘAZOVÁNÍ DEFINIC

Přiřaďte každý slovníčkový pojem vlevo k jeho správné definici vpravo zapsáním odpovídajícího písmene (A–H) do vyplnitelného pole.

☐	1. STUFFING	A	Předpočítaná tabulka hashů hesel.
☐	2. BCRYPT	B	Vícefaktorová kontrola přihlášení.
☐	3. NARUŠENÍ	C	Nástroj pro ukládání přihlašovacích údajů.
☐	4. SOLENÍ	D	Neoprávněné odhalení databáze.
☐	5. SPRÁVCE	E	Sociální inženýrství ke krádeži přihlašovacích údajů.
☐	6. MFA	F	Testování uniklých přihlašovacích údajů.
☐	7. DUHOVÉ	G	Přidání náhodné soli k haši hesla.
☐	8. PHISHING	H	Pomalý algoritmus hashování hesel.

Kontrolní bod 5: Křížovka

Vyřešte křížovku zapisováním písmen do aktivních bílých políček. Čísla odpovídají nápovědám níže.



VODOROVNÉ NÁPOVĚDY

1. Přidání náhodné soli do haše hesla. (6)

2. Vícefaktorová kontrola přihlášení. (3)

5. Sociální inženýrství ke krádeži přihlašovacích údajů. (8)

7. Pomalý algoritmus hašování hesel. (6)

SVISLÉ NÁPOVĚDY

1. Zkoušení uniklých přihlašovacích údajů. (8)

3. Předpočítaná tabulka hašů hesel. (6)

4. Neoprávněné odhalení databáze. (4)

6. Nástroj pro ukládání přihlašovacích údajů. (7)

Kontrolní bod 5, alternativa: Přístupná zadání křížovky

Uživatelé čteček obrazovky a klávesnice mohou odpovědi křížovky zapisovat přímo do textových polí níže.

VODOROVNÉ NÁPOVĚDY

1 vodorovně: Přidání náhodné soli do haše hesla. (6 písmen):

2 vodorovně: Vícefaktorová kontrola přihlášení. (3 písmen):

5 vodorovně: Sociální inženýrství ke krádeži přihlašovacích údajů. (8 písmen):

7 vodorovně: Pomalý algoritmus hašování hesel. (6 písmen):

SVISLÉ NÁPOVĚDY

1 svisle: Zkoušení uniklých přihlašovacích údajů. (8 písmen):

3 svisle: Předpočítaná tabulka hašů hesel. (6 písmen):

4 svisle: Neoprávněné odhalení databáze. (4 písmen):

6 svisle: Nástroj pro ukládání přihlašovacích údajů. (7 písmen):

Kontrolní bod 6: Hledání skrytých slov

Najděte 8 klíčových pojmů skrytých v mřížce níže. Slova mohou být vodorovně, svisle nebo úhlopříčně.

Ě	Q	Á	M	Č	Š	I	Ě	O	S	N	R	Y	R	Ó
Č	U	V	T	Ť	E	L	Í	B	B	A	B	C	P	Y
L	J	O	Y	L	Y	U	K	Ď	C	Ř	N	J	D	I
O	Ň	H	Í	N	E	L	O	S	K	R	R	Q	F	Ň
Ň	Ř	U	S	T	S	U	Ť	F	C	T	Y	R	Ó	H
E	Š	D	B	V	T	D	P	T	Z	Ů	C	P	Ž	V
C	Ě	K	G	Ž	U	D	Ň	H	Ď	Ř	X	Q	T	C
V	Ú	B	A	Ž	F	O	D	L	I	A	A	Ď	Ó	Ď
Á	É	G	I	D	F	S	Ř	N	E	S	I	F	Š	Ž
R	T	É	Ř	Ů	I	E	A	Á	Ř	P	H	O	M	Q
P	U	Y	R	J	N	S	U	Š	Č	K	Ň	I	Ý	B
S	Ě	Š	X	W	G	Í	A	S	I	Ž	Ý	Ý	N	L
F	I	N	S	J	N	M	Ť	N	P	G	R	Ř	G	G
Ž	Á	Ó	Ů	Ě	Ú	C	Ú	Ý	Š	Ý	B	G	M	Ž
F	J	Ó	Q	O	X	C	N	Ž	Z	Ě	Ý	P	W	Ú

SEZNAM SLOV

STUFFING, BCRYPT, ÚNIK, SOLENÍ, SPRÁVCE, MFA, DUHOVÁ, PHISHING

Kontrolní bod 6, alternativa: Přístupné přiřazování slovíček

Přiřaďte každý z 8 slovníčkových pojmů z osmisměrky k jeho správné definici zapsáním písmene (A–H) do prázdného pole.

POJMY SLOVNÍ ZÁSOBY

- **A. STUFFING**
- **B. BCRYPT**
- **C. ÚNIK**
- **D. SOLENÍ**
- **E. SPRÁVCE**
- **F. MFA**
- **G. DUHOVÁ**
- **H. PHISHING**

DEFINICE A POLE K PŘIŘAZENÍ

1. Sociální inženýrství ke krádeži přihlašovacích údajů.
2. Neoprávněné odhalení databáze.
3. Pomalý algoritmus hašování hesel.
4. Předpočítaná tabulka hašů hesel.
5. Zkoušení uniklých přihlašovacích údajů.
6. Přidání náhodné soli do haše hesla.
7. Nástroj pro ukládání přihlašovacích údajů.
8. Vícefaktorová kontrola přihlášení.

Kontrolní bod 7: Výzva s přeházenými slovy

Přeuspořádejte písmena níže a odhalte klíčové pojmy a termíny kybernetické bezpečnosti. Odpovědi pište do připravených polí.

1. **NFFSITGU**
2. **ÚIKN**
3. **ÁSVERCP**
4. **ÁOHVDU**
5. **YRTBPC**
6. **NESLÍO**
7. **AFM**
8. **SHHGPNII**

Bonusová aktivita: Mysli rychle

3 ODPOVĚDI V KAŽDÉ KATEGORII. VYHRÁVÁ, KDO PRVNÍ VYPLNÍ CELÝ SEZNAM.

1	Bezpečné návyky, se kterými můžete začít už dnes			
2	Pravidla pro silné heslo			
3	Správci hesel, které znáte			
4	Bezpečnostní nástroje, které znáte			
5	Varovné signály v e-mailu			
6	Zábavná slova pro dlouhou přístupovou frázi			
7	Způsoby, jak se přihlásit bez hesla			
8	Informace, které byste nikdy neměli sdílet			
9	Důvody, proč aktualizovat software			
10	Věci, které je třeba udělat, když heslo unikne			
11	Účty, které potřebují MFA			
12	Místa, kde by hesla nikdy neměla být uložena			
13	Známky toho, že je počítač nakažený			
14	Špatná hesla, která lidé používají			
15	Věci, které si zálohujete			

Kontrolní bod 8: Případové studie kyberbezpečnosti

Použijte naučené koncepty k vyřešení níže uvedených reálných scénářů.

PŘÍPADOVÁ STUDIE 1: NÁPRAVA ÚNIKU PODNIKOVÝCH PŘIHLAŠOVACÍCH ÚDAJŮ



Scénář: Služba monitoringu dark webu upozorní organizaci, že databázový výpis obsahující hesla firemních systémových administrátorů byl zveřejněn online.

Otázka k diskusi: Analyzujte rizika úniku přihlašovacích údajů a navrhněte strategii administrativního resetu.

PŘÍPADOVÁ STUDIE 2: ZAVEDENÍ STANDARDŮ HASHOVÁNÍ HESEL



Scénář: Podniková databáze v současnosti ukládá uživatelská hesla pomocí zastaralého hashe MD5 bez kryptografické soli, což je činí zranitelnými vůči rychlé extrakci.

Otázka k diskusi: Navrhněte migrační strategii pro upgrade hashovacího algoritmu databáze.

Kontrolní bod 9: Dešifrování šifry

Profesionál v kyberbezpečnosti chrání síťová aktiva před online útočníky. Pomocí níže uvedeného klíče písmeno–číslo dešifrujte zprávu zapsáním odpovídajících písmen do prázdných polí.

ŠIFROVACÍ KLÍČ PÍSMENO–ČÍSLO

A=1 Á=2 B=3 C=4 Č=5 D=6 Ď=7 E=8 É=9 Ě=10 F=11 G=12 H=13 I=14
Í=15 J=16 K=17 L=18 M=19 N=20 Ň=21 O=22 Ó=23 P=24 Q=25 R=26 Ř=27 S=28
Š=29 T=30 Ť=31 U=32 Ú=33 Ů=34 V=35 W=36 X=37 Y=38 Ý=39 Z=40 Ž=41

33	20	14	17	18	1		13	8	28	18	1
		40	1	3	8	40	24	8	5	30	8
35	15	4	8	11	1	17	30	22	26	22	35	39	19
			22	35	10	27	8	20	15	19			

Dešifrovaná zpráva:

TIP: KAŽDÉ ČÍSLO PŘEDSTAVUJE POZICI DANÉHO PÍSMENE V ABECEDĚ (NAPŘ. 1 = A, 2 = B, 41 = Ž).

Kontrolní bod 10: Základní časté otázky ke kyberbezpečnosti (část A)

Projděte si časté otázky a odpovědi ohledně zmírňování online hrozeb.

Q1: Co je únik hesel?

K úniku hesel dochází, když jsou přihlašovací údaje uživatelů odhaleny při únicích dat nebo chybných konfiguracích serverů.

Q2: Jak hackeři nacházejí uniklá hesla?

Hackeři prohledávají fóra na dark webu, veřejné výpisy databází a weby typu paste, kde se zveřejňují data z úniků [8].

Q3: Je opakované používání hesel nebezpečné?

Ano, protože pokud je jeden web kompromitován, hackeři mohou stejné přihlašovací údaje vyzkoušet na tisících dalších platforem [3].

Q4: Co je kryptografická sůl?

Sůl jsou náhodná data přidaná k heslu před hashováním, díky nimž jsou útoky pomocí předpočítaných vyhledávacích tabulek neúčinné [2].

Q5: Proč je MD5 zastaralé?

MD5 je rychlá, zastaralá hashovací funkce pro obecné účely, takže útočníci mohou odhady hesel testovat extrémně rychle, zejména když hashe nejsou solené [2].

Kontrolní bod 10: Základní časté otázky ke kyberbezpečnosti (část B)

Projděte si časté otázky a odpovědi ohledně zmírňování online hrozeb.

Q6: Jak správce hesel chrání uživatele?

Automaticky generuje složité, jedinečné přihlašovací údaje pro každý web, čímž omezuje lidské chyby paměti a opakované používání hesel.

Q7: Co je útok hrubou silou?

Útok, který systematicky zkouší všechny možné kombinace znaků, dokud nenajde správné heslo [4].

Q8: Jak pomáhá uzamčení účtu?

Zablokování účtu nebo omezení rychlosti zpomaluje opakované online hádání a spolu s monitorováním a MFA snižuje riziko útoku hrubou silou [4].

Q9: Jsou hlavní hesla bezpečná?

Jsou bezpečná, pokud jde o passphrase s vysokou entropií, které se nikdy nepoužívají opakovaně na jiných webových systémech.

Q10: Měla by se hesla pravidelně měnit?

NIST uvádí, že se nemají vynucovat pravidelné změny; hesla měňte při důkazech kompromitace a upřednostněte délku, blokovací seznamy a MFA [1].

Kontrolní bod 10: Pokročilé časté otázky k bezpečnosti (část C)

Prozkoumejte pokročilé technické aspekty bezpečnostních rámců, analýzy malwaru a datové compliance.

Q1: Jak si stojí Argon2 ve srovnání s bcrypt?

OWASP uvádí Argon2id jako svou první volbu; jeho paměťově náročná nastavení odolávají prolamování pomocí GPU a ASIC lépe než bcrypt [2].

Q2: Co je key stretching?

Technika, která spouští hashovací algoritmus v tisících opakováních, aby zpomalila ověřování hesla a prolamování se prodražilo [2].

Q3: Jak fungují duhové tabulky?

Jsou to předpočítané vyhledávací tabulky propojující hesla v otevřeném textu s jejich hashi, používané k rychlému zpětnému dohledání nesolených hashů [2].

Q4: Co je recyklace přihlašovacích údajů?

Opakované použití ukradených dvojic uživatelské jméno/heslo z jednoho úniku k pokusům o přístup do jiných služeb, zejména tam, kde lidé hesla používali opakovaně [3].

Q5: Lze hacknout správce hesel?

Ano. Mnohé používají šifrování s nulovou znalostí, takže při průniku na server jsou odhaleny jen zašifrované trezory, ale slabá hlavní hesla lze stále prolomit offline.

Kontrolní bod 10: Pokročilé časté otázky k bezpečnosti (část D)

Prozkoumejte pokročilé technické aspekty bezpečnostních rámců, analýzy malwaru a datové compliance.

Q6: Co je slovníkový útok?

Varianta útoku hrubou silou, která zkouší běžná slova, fráze a historicky uniklá hesla namísto náhodných písmen.

Q7: Proč se upřednostňují přístupové fráze?

Přístupové fráze používají několik náhodných slov, a vytvářejí tak vysokou entropii, kterou si lidé snadno zapamatují, ale jejíž prolomení je výpočetně nákladné [1].

Q8: Jak jednotné přihlášení (SSO) ovlivňuje úniky hesel?

SSO omezuje bujení hesel, ale poskytovatel identity se stává cenným cílem, který potřebuje silné, nejlépe vůči phishingu odolné MFA [6].

Q9: Co je únos relace?

Útočník získá nebo zneužije platný token relace, aby se vydával za přihlášeného uživatele, aniž by znovu potřeboval heslo [5].

Q10: Jak odhalíte password spraying?

Hledáním stejných několika hesel zkoušených na mnoha účtech, často pomalu, aby útok zůstal pod limity pro zablokování účtu [7].

Část 11: 10 faktů a poznatků o kyberbezpečnosti z praxe

Projděte si fakta z praxe o bezpečnostních incidentech, obranných mechanismech a standardech souladu.

1. BEZPEČNOSTNÍ POSTŘEH

NIST SP 800-63B vyžaduje, aby se nová hesla kontrolovala proti blokovacím seznamům běžných a kompromitovaných hesel [1].

2. BEZPEČNOSTNÍ POSTŘEH

Výpis 'Collection #1' z roku 2019 sloučil data z mnoha dřívějších úniků do jednoho obrovského souboru dvojic e-mail a heslo [8].

3. BEZPEČNOSTNÍ POSTŘEH

NIST nyní vyžaduje, aby hesla používaná jako jediný ověřovací faktor měla alespoň 15 znaků [1].

4. BEZPEČNOSTNÍ POSTŘEH

Hardware ASIC dokáže vypočítat miliardy hashů SHA-256 za sekundu, takže holé hashování SHA není pro uživatelská hesla bezpečné [2].

5. BEZPEČNOSTNÍ POSTŘEH

Jedinečné soli znamenají, že dva uživatelé s naprosto stejným heslem mají v databázi různé hashe [2].

6. BEZPEČNOSTNÍ POSTŘEH

Mnoho správců hesel šifruje data trezoru lokálně silnou kryptografií odvozenou z hlavního hesla uživatele.

7. POSTŘEH K BEZPEČNOSTI

Credential stuffing funguje, protože mnoho lidí používá stejné heslo pro účty v e-shopech, bankovnictví i e-mailu [3].

8. POSTŘEH K BEZPEČNOSTI

NIST SP 800-63B uvádí, že ověřovatelé nesmějí vyžadovat pravidelné změny hesel, pouze změny po prokázání kompromitace [1].

9. POSTŘEH K BEZPEČNOSTI

Přidání jednoho velkého písmene a symbolu ke krátkému heslu nezastaví moderní automatizované slovníkové útoky pomocí GPU [1].

10. BEZPEČNOSTNÍ POSTŘEH

MFA může zablokovat mnoho pokusů o credential stuffing i po úniku hesla; MFA odolné vůči phishingu je silnější než kódy v SMS [3].

Technické reference a zdroje

Studijní příručka a interaktivní hádanky jsou sestaveny z globálních standardů NIST, OWASP a předpisů o ochraně osobních údajů.

AKADEMICKÉ A OBOROVÉ REFERENCE

[1] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.

https://pages.nist.gov/800-63-4/sp800-63b.html

[2] OWASP. (n.d.). Password Storage Cheat Sheet.

https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html

[3] OWASP. (n.d.). Credential Stuffing Prevention Cheat Sheet.

https://cheatsheetseries.owasp.org/cheatsheets/Credential_Stuffing_Prevention_Cheat_Sheet.html

[4] OWASP. (n.d.). Authentication Cheat Sheet.

https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html

[5] OWASP. (n.d.). Session Management Cheat Sheet.

https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html

[6] CISA. (2022). Implementing Phishing-Resistant MFA (fact sheet).

https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf

[7] CISA. (2018). Brute Force Attacks Conducted by Cyber Actors (Alert TA18-086A).

https://www.cisa.gov/news-events/alerts/2018/03/27/brute-force-attacks-conducted-cyber-actors

[8] Hunt, T. (2019). The 773 Million Record "Collection #1" Data Breach. Troy Hunt.

https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/

Klíč odpovědí: Kontrolní bod 1 - Výběr z možností

1 **Otázka 1** **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Credential stuffing využívá automatizaci ke zkoušení uniklých dvojic uživatelské jméno/heslo na jiných webech [3].

2 **Otázka 2** **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

OWASP doporučuje především Argon2id; bcrypt je hlavně pro starší systémy, kde Argon2id ani scrypt nejsou k dispozici [2].

3 **Otázka 3** **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

MFA vyžaduje další faktor, takže samotné ukradené heslo účet neodemkne [3].

4 **Otázka 4** **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Výpisy z úniků jsou uniklé sbírky přihlašovacích údajů, například kompilace Collection #1 z roku 2019 [8].

5 **Otázka 5** **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Správce hesel generuje a ukládá jedinečné silné heslo pro každý účet, a brání tak opakovanému použití [3].

Klíč odpovědí: Kontrolní bod 2 - Pravda, nebo nepravda

6 **Otázka 6** **Správná odpověď: Pravda**

POZNÁMKA PRO VYUČUJÍCÍ

Pravda: opakovaně používaná hesla umožňují útočníkům znovu použít údaje uniklé z jednoho webu na jiných webech [3].

7 **Otázka 7** **Správná odpověď: Nepravda**

POZNÁMKA PRO VYUČUJÍCÍ

Nepravda: SHA-1 je rychlý hash; OWASP místo něj doporučuje Argon2id, scrypt, bcrypt nebo PBKDF2 [2].

8 **Otázka 8** **Správná odpověď: Nepravda**

POZNÁMKA PRO VYUČUJÍCÍ

Nepravda: samotná pravidla složitosti nezastaví stuffing pomocí opakovaně používaných uniklých hesel; je nutné MFA [3].

9 **Otázka 9** **Správná odpověď: Pravda**

POZNÁMKA PRO VYUČUJÍCÍ

Pravda: monitorovací služby prohledávají výpisy z úniků a zdroje na dark webu a hledají odhalené přihlašovací údaje [8].

10 **Otázka 10** **Správná odpověď: Pravda**

POZNÁMKA PRO VYUČUJÍCÍ

Pravda: jedinečná sůl pro každé heslo činí předpočítané duhové tabulky neúčinnými [2].

Klíče slovní zásoby a hodnoticí rubrika

Hodnoticí rubrika pro vyučující: Udělte 1 bod za každé správné přiřazení (celkem 8 bodů) a kontextový termín (celkem 6 bodů).

KONTROLNÍ BOD 4: KLÍČ K PŘIŘAZOVÁNÍ POJMŮ

F 1. STUFFING	H 2. BCRYPT	D 3. NARUŠENÍ	G 4. SOLENÍ
C 5. SPRÁVCE	B 6. MFA	A 7. DUHOVÉ	E 8. PHISHING

KONTROLNÍ BOD 3: KLÍČ KE KLÍČOVÝM POJMŮM

1 STUFFING	2 BCRYPT	3 ÚNIK	4 SOLENÍ
5 SPRÁVCE	6 MFA		

KONTROLNÍ BOD 6, ALTERNATIVA: KLÍČ K PŘIŘAZOVÁNÍ SLOV

1 H – PHISHING	2 C – ÚNIK	3 B – BCRYPT	4 G – DUHOVÁ
5 A – STUFFING	6 D – SOLENÍ	7 E – SPRÁVCE	8 F – MFA

POZNÁMKY K DISKUSI PRO VYUČUJÍCÍ

Klíčové pojmy:
Ověřte, že studenti umí vlastními slovy vysvětlit pojmy STUFFING, BCRYPT a NARUŠENÍ a ke každému uvést příklad.

Případové studie:
Požádejte studenty, aby svá doporučení zdůvodnili fakty z pracovního listu, nikoli domněnkami.

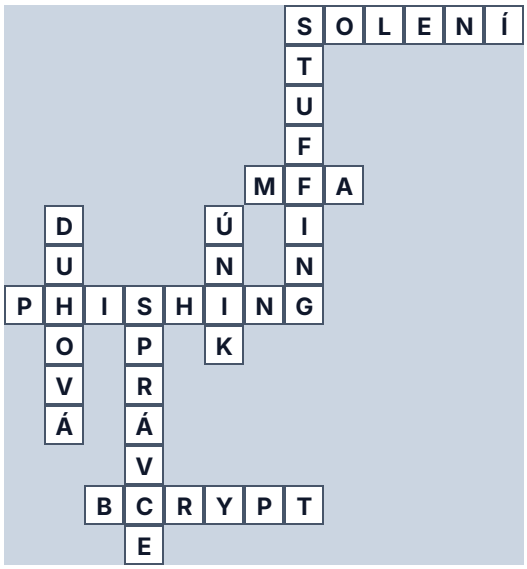
Práce se zdroji:
Nechte studenty ověřit alespoň jedno tvrzení proti referencím v pracovním listu a proberte, proč se čísla, ceny a pravidla mohou v čase měnit.

Klíče k úlohám a poznámky pro vyučující

ŘEŠENÍ OSMISMĚRKY

Ě	Q	Á	M	Č	Š	I	Ě	O	S	N	R	Y	R	Ó
Č	U	V	T	Ť	E	L	Í	B	B	A	B	C	P	Y
L	J	O	Y	L	Y	U	K	Ď	C	Ř	N	J	D	I
O	Ň	H	Í	N	E	L	O	S	K	R	R	Q	F	Ň
Ň	Ř	U	S	T	S	U	Ť	F	C	T	Y	R	Ó	H
E	Š	D	B	V	T	D	P	T	Z	Ů	C	P	Ž	V
C	Ě	K	G	Ž	U	D	Ň	H	Ď	Ř	X	Q	T	C
V	Ú	B	A	Ž	F	O	D	L	I	A	A	Ď	Ó	Ď
Á	É	G	I	D	F	S	Ř	N	E	S	I	F	Š	Ž
R	T	É	Ř	Ů	I	E	A	Á	Ř	P	H	O	M	Q
P	U	Y	R	J	N	S	U	Š	Č	K	Ň	I	Ý	B
S	Ě	Š	X	W	G	Í	A	S	I	Ž	Ý	Ý	N	L
F	I	N	S	J	N	M	Ť	N	P	G	R	Ř	G	G
Ž	Á	Ó	Ů	Ě	Ú	C	Ú	Ý	Š	Ý	B	G	M	Ž
F	J	Ó	Q	O	X	C	N	Ž	Z	Ě	Ý	P	W	Ú

ŘEŠENÍ KŘÍŽOVKY



PRŮVODCE PRO VYUČUJÍCÍ K ŘEŠENÍ KŘÍŽOVKY

VODOROVNÉ NÁPOVĚDY

1 vodorovně: SOLENÍ Přidání náhodné soli do haše hesla. (6 písmen)

2 vodorovně: MFA Vícefaktorová kontrola přihlášení. (3 písmen)

5 vodorovně: PHISHING Sociální inženýrství ke krádeži přihlašovacích údajů. (8 písmen)

7 vodorovně: BCRYPT Pomalý algoritmus hašování hesel. (6 písmen)

SVISLÉ NÁPOVĚDY

1 svisle: STUFFING Zkoušení uniklých přihlašovacích údajů. (8 písmen)

3 svisle: DUHOVÁ Předpočítaná tabulka hašů hesel. (6 písmen)

4 svisle: ÚNIK Neoprávněné odhalení databáze. (4 písmen)

6 svisle: SPRÁVCE Nástroj pro ukládání přihlašovacích údajů. (7 písmen)

Klíč řešení přesmyček a šifry

Klíč k hodnocení aktivity s přesmyčkami slovní zásoby a výzvy Tajná šifra.

KLÍČ K PŘESMYČKÁM

1. NFFSITGU — STUFFING
2. ÚIKN — ÚNIK
3. ÁSVERCP — SPRÁVCE
4. ÁOHVDU — DUHOVÁ
5. YRTBPC — BCRYPT
6. NESLÍO — SOLENÍ
7. AFM — MFA
8. SHHGPNII — PHISHING

KLÍČ TAJNÉ ŠIFROVACÍ VÝZVY

"ÚNIKLA HESLA ZABEZPEČTE VÍCEFAKTOROVÝM OVĚŘENÍM"

Klíč k případovým studiím

A Případová studie 1: Náprava úniku podnikových přihlašovacích údajů

Řešení pro vyučující

POKYNY K HODNOCENÍ

Odpovědi studentů by měly pokrýt následující body:

- Analýza scénáře: Služba monitoringu dark webu upozorní organizaci, že byl online zveřejněn výpis databáze s hesly firemních systémových administrátorů.
- Doporučená strategie a řešení: Zrušte všechny aktivní relace administrátorů a resetujte přihlašovací údaje pomocí generátoru s vysokou entropií. Vynucujte MFA odolné vůči phishingu na administrátorských portálech [6], vyměňte dotčené klíče API, zkontrolujte protokoly přihlášení, najděte místo prvotního úniku a prověřte další privilegované účty.

B Případová studie 2: Zavedení standardů hashování hesel

Řešení pro vyučující

POKYNY K HODNOCENÍ

Odpovědi studentů by měly pokrýt následující body:

- Analýza scénáře: Podniková databáze aktuálně ukládá uživatelská hesla v zastaralých MD5 hashích bez kryptografické soli, takže jsou zranitelná vůči rychlé extrakci.
- Doporučená strategie a řešení: Zaveďte Argon2id (nebo bcrypt u starších systémů) s jedinečnou solí pro každého uživatele [2]. Stávající hashe MD5 hned obalte novým algoritmem, při příštím přihlášení každého uživatele heslo přímo znovu zahashujte a u dlouho neaktivních účtů vynuťte reset.