SMLOUVA O POSKYTNUTÍ SLUŽBY PENETRAČNÍHO TESTOVÁNÍ

Město Český Krumlov, se sídlem náměstí Svornosti 1, Vnitřní Město, 381 01 Český Krumlov, IČO 00245836, zastoupená Tomášem Železným, vedoucí odboru informatiky

(„**Objednatel**")

a

Integra Czech Republic, s.r.o., se sídlem U Sluncové 666/12a, Karlín, 186 00 Praha 8, IČO 24216941, Zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl C, vložka 189573, zastoupená Jiřím Harcubou, jednatelem

(„**Poskytovatel**")

Poskytovatel a Objednatel společně jako „**Smluvní strany**", nebo jednotlivě jako „**Smluvní strana**", uzavírají tímto tuto smlouvu o poskytnutí služby penetračního testování (dále jen „**Smlouva**") dle § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník (dále jen „**Občanský zákoník**").

1 Úvodní ustanovení

1.1 Tato Smlouva stanoví podmínky poskytnutí služby penetračního testování interní a externí sítě provozované Objednatelem ze strany Poskytovatele, jejímž cílem je ověřit bezpečnost nově dodaných technologií v rámci projektu "Český Krumlov automatizované digitální služby města", reg. č. CZ.06.01.01/00/22_004/0000166.

1.2 Součástí této Smlouvy je jako její příloha č. 1 nabídka Poskytovatele blíže vymezující předmět plnění služby dle této Smlouvy (dále jen „**Nabídka**"). V případě rozporu mezi textem Smlouvy a Nabídkou má přednost text Smlouvy.

2 Předmět Smlouvy

2.1 Poskytovatel se zavazuje za podmínek sjednaných touto Smlouvou:

- Provést penetrační testování v souladu s mezinárodními metodikami OSSTMM, OWASP, PTES a LPT, tj. testování zranitelnosti infrastruktury a IT systémů;
- vyhotovení závěrečné zprávy o provedení penetračního testu v českém jazyce;
- bližší popis průběhu poskytování služby penetračního testování včetně struktury závěrečné zprávy je uveden v Nabídce.

2.2 Plnění dle této Smlouvy bude poskytováno v rámci realizace projektu "Český Krumlov automatizované digitální služby města", reg. č. CZ.06.01.01/00/22_004/0000166, spolufinancovaného Evropskou unií v rámci Integrovaného regionálního operačního programu.

2.3 Pracovníci Poskytovatele podílející se na plnění služeb podle této Smlouvy budou specialisté splňující příslušné kvalifikační předpoklady.

2.4 Objednatel se zavazuje zaplatit cenu ve výši a dle podmínek dohodnutých v této Smlouvě.

3 Termín a další podmínky plnění

3.1 Služba penetračního testování bude dokončeno do 30 dní od podepsání této smlouvy, pokud nebude zajištěna součinnost ze strany Objednatele, může se termín posunout.

4 Cena

4.1 Cena za služby penetračního testování včetně vypracování závěrečné zprávy se sjednává ve výši 60 750 Kč bez DPH, včetně DPH pak 73 507 Kč.

4.2 Poskytovatel je oprávněn vystavit fakturu za celou cenu služby po akceptaci projektu této Smlouvy, se splatností 20 dnů od jejího vystavení.

4.3 Faktura musí být označena registračním číslem projektu: CZ.06.01.01/00/22_004/0000166

4.4 Faktura musí být doručena na e-mailovou adresu uvedenou v čl. 6 této Smlouvy.

4.5 Platba faktury bude provedena bezhotovostním převodem na účet Poskytovatele uvedený ve faktuře. Za den platby se považuje den, ve kterém byla řádně fakturovaná částka odepsána z účtu Objednatele.

5 Součinnost Smluvních stran

5.1 Objednatel je povinen poskytnout potřebnou součinnost pro provedení služby penetračního testování.

6 Komunikace Smluvních stran

6.1 Smluvní strany budou komunikovat primárně elektronickou formou.

6.2 Kontaktními osobami Objednatele pro účely plnění této Smlouvy jsou:

Jméno	E-mail	Telefon
Tomáš Železný		

6.3 Kontaktními osobami Poskytovatele pro účely plnění této Smlouvy jsou:

Jméno	E-mail	Telefon
David Pícha		

7 Náhrada škody

7.1 Smluvní strany odpovídají za způsobenou škodu v rámci platných právních předpisů a Smlouvy. Smluvní strany budou předcházet riziku vzniku škod v souvislosti s plněním Smlouvy.

7.2 Žádná ze Smluvních stran neodpovídá za škodu způsobenou v důsledku chybných či nesprávných zadání nebo jakýchkoli jiných informací předaných druhou Smluvní stranou.

7.3 Na odpovědnost za škodu způsobenou při plnění Smlouvy se uplatní okolnosti vylučující odpovědnost dle Občanského zákoníku.

7.4 Poskytovatel odpovídá za škodu způsobenou při plnění této smlouvy podle příslušných ustanovení občanského zákoníku. Smluvní strany sjednávají, že případné smluvní omezení výše náhrady škody se neuplatní v případě škody způsobené úmyslně, z hrubé nedbalosti, porušením

povinností v oblasti kybernetické bezpečnosti, porušením povinností týkajících se důvěrnosti, nebo škody způsobené třetím osobám.

8 Důvěrné informace

8.1 Pro účely této Smlouvy výraz „**Důvěrné informace**" znamená veškeré informace, zejména náklady a ceny (potenciální nebo skutečné); zákazníci; dodavatelé; technologie; technické, finanční a obchodní strategie, marketingové a propagační strategie; IT informace, vlastní metodologie a postupy a obchodní tajemství (bez ohledu na to, zda je či není patentovatelné), týkající se příslušné Smluvní strany, ať už ústní nebo písemné, uložené nebo přenášené jakýmkoli médiem, které jsou zpřístupněny druhé Smluvní straně, přímo nebo nepřímo, stejně jako všechny údaje, záznamy, poznámky, analýzy, kompilace, studií nebo jiných dokumentů získaných z, nebo jinak použitých a zveřejněných jako Důvěrné informace s výjimkou informací, které:

8.1.1 byly veřejně k dispozici v době takového zveřejnění, nebo následně se stanou veřejně dostupnými jinak, než v důsledku porušení povinností tohoto závazku důvěrnosti ze strany příslušné Smluvní strany;

8.1.2 byly k dispozici příslušné Smluvní straně jako veřejné před uzavřením této Smlouvy;

8.1.3 byly nezávisle vyvinuty příslušnou Smluvní stranou bez přístupu k Důvěrným informacím;

8.1.4 druhá smluvní strana dala ke zveřejnění takové Důvěrné informace souhlas.

8.2 Smluvní strany se zavazují k níže uvedenému:

8.2.1 zacházet s Důvěrnými informacemi jako se soukromými a přísně důvěrnými, a v případě neexistence předchozího písemného souhlasu od druhé Smluvní strany nezpřístupnit Důvěrné informace žádné třetí osobě, ledaže takové sdělení bylo předem dohodnuto s druhou Smluvní stranou (ať už písemně nebo ústně), nebo to od příslušné Smluvní strany budou oprávněně žádat závazné právní předpisy, správní orgán nebo příslušný soud. Takové zpřístupnění nebude považováno za porušení této Smlouvy, nicméně i v tomto případě však musí být Objednatel informován před tímto zveřejněním;

8.2.2 používat Důvěrné informace výhradně za účelem plnění této Smlouvy;

8.2.3 nesmí kopírovat nebo reprodukovat jakoukoli část Důvěrné informace bez předchozího písemného souhlasu druhé Smluvní strany, pouze v míře přiměřeně a nezbytné k provedení služeb dle této Smlouvy;

8.2.4 informovat druhou Smluvní stranu o porušení jakékoliv výše uvedené povinnosti bez zbytečného prodlení,

8.2.5 zavázat své pracovníky, jakož i každou třetí osobu, které příslušná Smluvní strana zpřístupnila Důvěrné informace, k povinnosti ochrany Důvěrných informací alespoň v rozsahu odpovídajícím této Smlouvě.

8.3 Povinnosti Smluvních stran k ochraně Důvěrných informací trvá i po skončení této Smlouvy.

8.4 Poskytovatel uděluje Objednateli neodvolatelný souhlas zveřejnit plně nebo částečně závěrečnou zprávu a/nebo certifikát podle odst. 2.1 této Smlouvy.

9 Smluvní Pokuty

9.1 V případě prodlení Objednatele se zaplacením peněžité částky Poskytovateli je Objednatel povinen zaplatit smluvní pokutu ve výši 0,05% z dlužné částky za každý den prodlení.

9.2 V případě prodlení Poskytovatele s dodáním služby podle odst. 3.1 této Smlouvy je Poskytovatel povinen poskytnout Objednateli slevu z ceny služby (podle odst. 4.1 této Smlouvy) ve výši 0,05% za každý den prodlení.

9.3 Za každé porušení ustanovení o ochraně Důvěrných informacích dle čl. 8 této Smlouvy je porušující Smluvní strana povinna zaplatit druhé Smluvní straně smluvní pokutu ve výši 250.000,- Kč.

9.4 Ustanoveními o smluvní pokutě není dotčeno právo na náhradu škody, uhrazená smluvní pokuta se však započte do náhrady škody.

10 Ukončení Smlouvy

10.1 Tato Smlouva může být ukončena

10.1.1 písemnou dohodou obou Smluvních stran;

10.1.2 odstoupením od Smlouvy v případě podstatného porušení povinností vyplývajících z této Smlouvy druhou Smluvní stranou, přičemž takové odstoupení nabývá účinnosti ihned po dni doručení písemného oznámení druhé Smluvní straně.

10.1.3 Za podstatné porušení povinností dle této Smlouvy se považuje zejména:
a) prodlení Poskytovatele s dodáním služby přesahující 10 kalendářních dnů bez předchozí dohody s Objednatelem;

b) závažné porušení povinností v oblasti ochrany důvěrných informací dle čl. 8 této Smlouvy;

c) dodání vadné či neúplné výstupní zprávy, která není akceptovatelná z hlediska metodik uvedených ve Smlouvě;

d) odmítnutí součinnosti potřebné pro řádné poskytnutí služeb dle této Smlouvy;

e) jakékoli jednání, které by vedlo ke zneužití přístupových údajů nebo jinému zásahu do systémů Objednatele v rozporu s účelem smlouvy.

11 Rozhodné Právo, řešení sporů

11.1 Tato Smlouva a její výklad se řídí právním řádem České republiky.

11.2 Smluvní strany se zavazují řešit případné spory vyplývající z této Smlouvy nebo v souvislosti s ní především smírnou cestou a ve vzájemné shodě. Nebude-li spor vyřešen smírně do 30 dnů od doručení písemné výzvy k jednání, bude kterýkoli ze smluvních partnerů oprávněn obrátit se na věcně a místně příslušný soud v České republice.

12 Závěrečná ustanovení

12.1 Veškeré změny v této Smlouvě musí být v písemné formě a podepsány oběma Smluvními stranami.

12.2 Poskytovatel prohlašuje, že on sám ani žádný z jeho zaměstnanců, zástupců či osob podílejících se na plnění této Smlouvy:

12.2.1. není a v době plnění Smlouvy nebude v pracovním, smluvním ani jiném obdobném vztahu k žádnému subjektu, který je dodavatelem nebo správcem testovaných systémů nebo prvků infrastruktury Objednatele v oblasti kybernetické bezpečnosti;

12.2.2. nemá žádný majetkový, obchodní či personální podíl ve výše uvedených subjektech;

12.2.3. je si vědom skutečnosti, že výskyt střetu zájmů by mohl vést k neplatnosti výstupní zprávy.

12.3 V případě, že by jakýkoli potenciální střet zájmů vznikl, zavazuje se Poskytovatel bezodkladně o této skutečnosti písemně informovat Objednatele a učinit veškeré kroky k jeho odstranění.

12.4 Poskytovatel se zavazuje mít po celou dobu účinnosti této Smlouvy uzavřené profesní pojištění odpovědnosti za škodu v minimální výši 5 000 000 Kč a na vyžádání předloží Objednateli doklad o jeho existenci.

12.5 Poskytovatel je povinen uchovávat veškerou dokumentaci související s plněním dle této Smlouvy včetně účetních dokladů minimálně do 31. 12. 2035, pokud není ve Specifických pravidlech ve vztahu k projektu "Český Krumlov automatizované digitální služby města", reg. č. CZ.06.01.01/00/22_004/0000166 stanoveno jinak. Pokud je v českých právních předpisech stanovena lhůta delší, musí být pro úschovu použita lhůta delší.

12.6 Poskytovatel je povinen minimálně do 31. 12. 2035 poskytovat požadované informace a dokumentaci související s realizací projektu zaměstnancům nebo zmocněncům pověřených orgánů (Centra, MMR, MF, Evropské komise, Evropského účetního dvora (dále také „EÚD“), Nejvyššího kontrolního úřadu (dále také „NKÚ“), příslušného orgánu finanční správy a dalších oprávněných orgánů státní správy) a je povinen vytvořit výše uvedeným osobám podmínky k provedení kontroly vztahující se k realizaci projektu a poskytnout jim při provádění kontroly součinnost.

12.7 Poskytovatel poskytuje na dílo záruku za jakost v délce 24 měsíců od řádného předání a převzetí díla. Po tuto dobu odpovídá za to, že dílo bude bez vad, bude odpovídat smluveným požadavkům a bude způsobilé k dohodnutému účelu.

12.8 V případě zjištění vad během záruční doby je zhotovitel povinen je bezplatně odstranit do 14 dnů od oznámení. Neodstraní-li vadu ve lhůtě, je objednatel oprávněn zajistit nápravu na náklady zhotovitele.

12.9 Pokud některé z ustanovení této Smlouvy je nebo se stane neplatným nebo nevymahatelným, nebude to mít vliv na platnost a vymahatelnost ostatních ustanovení této Smlouvy a Smluvní strany se zavazují nahradit takové neplatné nebo nevymahatelné ustanovení novým, platným a vykonatelným ustanovením, které nejefektivnější pro obchodní záměr Smluvních stran.

12.10 Obě Smluvní strany souhlasí se zveřejněním této smlouvy v Registru smluv podle zákona č. 340/2015 Sb., o registru smluv, ve znění pozdějších předpisů. Prohlašují, že žádná její část neobsahuje obchodní tajemství ani jiné skutečnosti, jejichž zveřejnění by mohlo ohrozit kybernetickou bezpečnost nebo jiný chráněný zájem. Zveřejnění smlouvy v Registru smluv zajistí Objednatel.

12.11 Tato Smlouva je vyhotovena ve dvou stejnopisech, přičemž každá Smluvní strana si ponechá jeden exemplář. Smluvní strany se mohou dohodnout na elektronickém podpisu této Smlouvy.

Příloha: 1) Nabídka Poskytovatele č. NAB-25-085

Datum:	Datum:
Za Objednatele:	Za Poskytovatele:
Podpis: ……..	Podpis: ……..
Jméno: Tomáš Železný	Jméno: Jiří Harcuba
Funkce: vedoucí odboru informatiky	Funkce: jednatel

INTEGRA

Předkládá nabídku na

PENETRAČNÍ TESTY

pro:

ČESKÝ KRUMLOV

Zákazník:	**Město Český Krumlov**
Projekt:	KyBez projekt - Penetrační testy
Dodavatel:	**Integra Czech Republic, s.r.o.** U Sluncové 666/12a 186 00 Praha
Vypracoval:	David Pícha david.picha@integra.cz
Datum vytvoření:	15.5.2025
Platnost do:	30.6.2025

Obsah

1 Představení dodavatele

Společnost **Integra Czech Republic, s.r.o.** je jedním z předních poskytovatelů kybernetické bezpečnosti a IT služeb v České republice. Od roku 2012 pomáháme firmám chránit jejich digitální aktiva prostřednictvím profesionálních penetračních testů, auditů a bezpečnostních školení.

1.1 Identifikační údaje

Obchodní název	**Integra Czech Republic, s.r.o.**
Datum založení	9. 2. 2012
Sídlo společnosti	U Sluncové 666/12a, 186 00 Praha 8
Jednatel	Jiří Harcuba
Webové stránky	www.integra.cz
Kontaktní údaje	security@integra.cz, +420 214 214 602
IČ	24216941
DIČ	CZ24216941
Bankovní spojení	Komerční banka a.s.
Číslo účtu	107-7261940297/0100
Certifikace ISO	ISO 9001 & 27001
Obrat společnosti	Více než 540 mil Kč bez DPH

1.2 Hlavní portfolio služeb:

- **Penetrační testy** – identifikace a eliminace bezpečnostních zranitelností
- **Red teaming** – simulace sofistikovaných útoků s cílem otestovat reakce obrany
- **Audit konfigurace IT systémů** – ověření zabezpečení cloudových a on-premise řešení
- **Školení bezpečnosti** – vzdělávání zaměstnanců a IT týmů v oblasti kybernetických hrozeb
- **Zajištění IT specialistů** – dodávka expertů v oblasti bezpečnosti a IT infrastruktury

Jsme držiteli **certifikací ISO 9001 a ISO 27001**, které potvrzují náš závazek k nejvyšším standardům kvality a bezpečnosti.

- ISO 9001 zajišťuje neustálé zlepšování procesů a poskytování kvalitních služeb.
- ISO 27001 dokazuje naši odbornost v oblasti ochrany citlivých dat a informační bezpečnosti.

Integra byla opakovaně oceněna v žebříčku **"Českých TOP 100 ICT společností"** v letech **2020, 2021, 2022 a 2023**, což potvrzuje naši silnou pozici na trhu IT bezpečnosti

2 Úvod

Děkujeme za možnost připravit nabídku na provedení penetračních testů. Naši certifikovaní specialisté mají bohaté zkušenosti s odhalováním bezpečnostních hrozeb a jejich eliminací.

Díky kombinaci manuálních a automatizovaných testovacích technik dokážeme identifikovat nejen známé zranitelnosti, ale i chyby v business logice, bezpečnostní konfiguraci a architektuře aplikací. Naším cílem je pomoci organizacím minimalizovat kybernetická rizika, splnit bezpečnostní standardy a chránit citlivá data před neoprávněným přístupem.

Přístup a metodologie:

- Naše unikátní metodika spojuje osvědčené mezinárodní standardy jako OWASP a OSSTMM, s našimi vlastními postupy, zaručuje vysokou úroveň ochrany a přesné identifikování zranitelností.
- Manuální testování je pro nás klíčové, protože přesně napodobuje reálné útoky a techniky, které používají skuteční útočníci. Automatizované nástroje používáme tam, kde to výrazně zvýší efektivitu testování, aniž bychom snížili jeho kvalitu.
- Díky kombinaci manuálních a automatizovaných přístupů dokážeme efektivně odhalit i složitější bezpečnostní mezery, které by mohly být jinak přehlédnuty.

Naše přidaná hodnota:

- **Komplexní bezpečnostní report** – Zahrnuje nejen seznam zranitelností, ale i reálné scénáře zneužití, proof-of-concept exploitace a konkrétní kroky k nápravě, prioritizované dle CVSS hodnocení a doplněné manažerským shrnutím.
- **Konzultace s odborníky:** Po testování vám naši experti podrobně vysvětlí výsledky a poskytnou detailní přehled o průběhu testů.
- **Certifikát o provedení testu:** Po dokončení testování obdržíte certifikát, který potvrzuje, že vaše systémy byly důkladně prověřeny a splňují vysoké standardy kybernetické bezpečnosti.
- **Online test zranitelností:** Poskytujeme možnost provedení rychlého online skenu zranitelností zcela zdarma, což vám umožní získat základní přehled o bezpečnosti vašich veřejně dostupných služeb. Více informací naleznete na našem webu https://www.integra.cz/cs/online-sken-zranitelnosti/

Tým našich bezpečnostních expertů

- Jsme jedním z největších poskytovatelů penetračních testů v České republice
- Máme dlouholeté zkušenosti v oblasti IT bezpečnosti a detailní znalost široké škály platforem a systémů
- Naši odborníci pravidelně procházejí školeními v oblasti IT bezpečnosti a etického hackingu, abychom drželi krok s nejnovějšími hrozbami a technikami
- Náš tým se pyšní mezinárodními certifikacemi uznávanými po celém světě
    - OSCP (Offensive Security Certified Professional)
    - CEH (Certified Ethical Hacker)
    - CHFI (Computer Hacking Forensic Investigator)
    - ECSA (EC-Council Certified Security Analyst)
    - eJPT (eLearnSecurity Junior Penetration Tester)
    - eCPPT (eLearnSecurity Certified Professional Penetration Tester)
    - eWPT (eLearnSecurity Web Application Penetration Tester)
    - OSWP (Offensive Security Wireless Professional)
    - CMPen (Certified Master in Penetration Testing)
    - AWS CSC-C01 (AWS Certified Security – Specialty)
    - AWS CLF-02 (AWS Certified Cloud Practitioner)

3 Cenová nabídka

Integra Czech Republic, s.r.o., U Sluncové 666/12a
IČO: 24216941 / DIČ: CZ24216941
Bank: Komerční banka a.s., bank number: 107-7333280217/0100, IBAN: CZ20 0100 0001 0773 3328 0217, SWIFT: KOMBCZPPXXX

Datum vystavení: 15.5.2025
Datum platnosti: 30.6.2025

Odběratel:
Město Český Krumlov
náměstí Svornosti 1
Český Krumlov
Česká republika
CZ00245836

Vystavil:
David Pícha

Kontaktní osoba:
Tomáš Železný

KyBez projekt - Penetrační testy

Popis položky	Počet	Cena / jedn.	Celkem
Penetrační testy interní a externí sítě Cílem penetračních testů je ověřit bezpečnost nově dodaných technologií v rámci projektu IROP.	4,50 MD	13 500,00 Kč	60 750,00 Kč

Uvedené ceny položek jsou bez DPH

Celkem bez DPH:	60 750,00 Kč
Částka DPH:	12 757,50 Kč
Celkem vč. DPH:	73 507,50 Kč

4 Technický detail testů

Níže uvedené testovací scénáře představují typické postupy při penetračním testování. Konkrétní rozsah testu, používané metody a simulované hrozby se však mohou lišit v závislosti na požadavcích klienta, testovaném systému a aktuálních bezpečnostních rizicích. Testy jsou vždy přizpůsobeny konkrétním podmínkám s cílem efektivně identifikovat zranitelnosti a poskytnout relevantní doporučení.

4.1 Interní penetrační test

Interní penetrační testy simulují útok z perspektivy útočníka, který již získal přístup k vnitřní síti organizace. Tento typ testování umožňuje zjistit, jak efektivní jsou současná bezpečnostní opatření a jaké kroky mohou útočníci podniknout k dalšímu kompromitování systémů.

Hlavní testované oblasti:

1. **Mapování interní sítě a identifikace zranitelností**

   Analyzujeme síťovou architekturu, identifikujeme aktivní systémy, servery a služby. Testujeme jejich odolnost proti útokům, které zneužívají:

   - Softwarové zranitelnosti (CVE)
   - Špatné konfigurace systémů
   - Slabé autentizační mechanismy
   - Nedostatečnou segmentaci sítě

2. **Testování zabezpečení síťových prvků**

   Prověřujeme bezpečnost síťové infrastruktury, včetně firewallů, switchů, routerů, Wi-Fi sítí a VPN bran. Zaměřujeme se na:

   - Neautorizovaný přístup a možnost obejití bezpečnostních opatření
   - Chyby v konfiguraci síťových pravidel a ACL
   - Možnost ARP spoofingu, DNS hijackingu a dalších MITM útoků
   - Možnost neautorizovaného přístupu k síťovým management rozhraním

3. **Sběr informací a rozpoznání síťových služeb**
   - Port scanning: Identifikace otevřených portů (TCP/UDP) na interních systémech
   - Service enumeration: Detekce běžících služeb, protokolů a jejich verzí
   - Default credentials & Weak passwords: Testování standardních přihlašovacích údajů a provádění slovníkového útoku na slabá hesla
   - Vulnerability scanning: Automatizovaná detekce známých zranitelností v OS a aplikacích

4. **Simulace útoku na zaměstnance a eskalace oprávnění**

   Testujeme scénáře, kdy útočník získá přístup k firemní síti například prostřednictvím:

   - Kompromitovaného počítače zaměstnance
   - Phishingového útoku (sociální inženýrství)
   - Nechráněného ethernetového portu nebo Wi-Fi sítě

5. **Pokusy o prolomení domény a získání administrátorských práv**

   Cílem je zjistit, zda lze eskalovat oprávnění až na úroveň doménového administrátora:

   - Pass-the-Hash a Pass-the-Ticket útoků
   - Kerberoasting – zneužití slabých služebních účtů Active Directory
   - NTLM relay attacks – přeposílání autentizačních relací
   - Token Impersonation – přebírání přihlašovacích relací privilegovaných uživatelů

6. **Prověření ochrany citlivých dat**

   Ověřujeme, zda jsou správně nastavena přístupová práva k databázím, souborovým serverům a dalším kritickým systémům. Zjišťujeme, zda lze data:

   - Neoprávněně získat (přístup k důvěrným dokumentům, databázím, emailům)
   - Modifikovat (manipulace s firemními daty)
   - Exfiltrovat (data exfiltration testy)

7. **Exploitace nalezených zranitelností**

   Pokud je nalezena zranitelná služba nebo systém, provádíme kontrolovanou exploitaci, která zahrnuje:

   - Získání shell přístupu k systému
   - Využití zranitelností OS nebo aplikací (RCE, privilege escalation)
   - Analýzu možností post-exploitation útoků

8. **Lateral Movement a Post-exploitation**

   Po úspěšném kompromitování jednoho systému testujeme možnosti horizontálního pohybu v síti a přístupu k dalším systémům. Simulujeme scénáře, kdy útočník:

   - Používá odcizené přihlašovací údaje ke kompromitaci dalších účtů
   - Přeskakuje mezi servery a pracovními stanicemi
   - Pokouší se šířit malware nebo ransomware v interní síti

9. **Simulace útoku insidera (Malicious Insider Threat)**

   Testujeme scénáře, kdy útočník již disponuje interními přihlašovacími údaji nebo přístupem k firemním zařízením. Ověřujeme, zda lze:

   - Získat neautorizovaný přístup k interním systémům
   - Obejít monitorovací a detekční mechanismy
   - Manipulovat s citlivými informacemi nebo systémy

4.2 Externí penetrační test

Externí penetrační test simuluje útok na systémy organizace z veřejné sítě, tedy z pohledu externího útočníka. Cílem je identifikovat zranitelnosti a posoudit rizika neoprávněného přístupu.

Hlavní testované oblasti:

1. **Identifikace cíle a sběr informací**

   Prvním krokem je získání co největšího množství dostupných informací o infrastruktuře cíle. Využíváme jak pasivní, tak aktivní metody sběru dat:

   - DNS reconnaissance (subdomény, reverzní DNS, záznamy WHOIS)
   - Analýza veřejných databází (Shodan, Censys, certifikáty SSL/TLS, IP záznamy)
   - Ověření metadat dokumentů (emaily, uživatelská jména, verze SW z veřejných souborů)

2. **Zjištění aktivních služeb (Port scanning & Service enumeration)**

   Cílem je detekovat otevřené porty a zjistit běžící služby na testovaných IP adresách. V této fázi probíhá:

   - Skenování TCP/UDP portů (Nmap, Masscan)
   - Fingerprinting operačních systémů (identifikace typu OS a verzí)
   - Detekce dostupných služeb (HTTP(S), VPN, RDP, SSH, FTP, SMTP atd.)

3. **Hledání zranitelností (Vulnerability Scanning & Exploitation)**

   Identifikujeme známé i neznámé zranitelnosti na základě zjištěných služeb a konfigurací:

   - Automatizovaný scanning zranitelností (CVE databáze)
   - Kontrola slabých TLS/SSL konfigurací (SSL Labs, testy certifikátů)
   - Identifikace špatně nakonfigurovaných veřejných služeb (databáze, nechráněné API)
   - Manuální testování zranitelností (Zero-days, Log4Shell, ProxyShell aj.)

4. **Testování autentizace a hesel (Credential Attacks)**

   Zaměřujeme se na slabé přihlašovací mechanismy, které by mohly umožnit neoprávněný přístup k systémům:

   - Testování výchozích přihlašovacích údajů (admin/admin, root/root)
   - Slovníkové a brute-force útoky (hydra, medusa, patator)

5. **Získání přístupu k systémům (Initial Access)**

   Pokud jsou nalezeny zranitelnosti nebo slabé autentizační mechanismy, provádíme pokusy o získání přístupu k cílovým systémům:

   - Exploitace známých zranitelností (SQLi, RCE, SSRF, XXE, LFI/RFI)
   - Testování veřejných exploitů (Metasploit, Exploit-DB)
   - Kombinace OSINT informací s cílem prolomení přístupu

6. **Eskalace oprávnění a ovládnutí cíle (Privilege Escalation & Post-Exploitation)**

   Po úspěšném získání přístupu k systému testujeme možnosti další eskalace oprávnění a post-exploitation aktivity:

   - Privilege escalation (root/admin) – využití zranitelností OS
   - Lateral Movement – rozšíření kompromitace na další servery a aplikace
   - Pivoting – využití kompromitovaného systému pro útoky na interní síť
   - Data exfiltration – simulace úniku citlivých informací (přístup k databázím, souborovým serverům, e-mailovým schránkám)

5 Testování

V rámci testování kombinujeme **manuální i automatizované metody**, abychom dosáhli maximální přesnosti a efektivity. Bereme v úvahu specifika testovaných systémů a aplikací, a pokud testy probíhají v produkčním prostředí, minimalizujeme automatizované zásahy, abychom nezpůsobili výpadky nebo narušení provozu.

Před samotným testováním vypracujeme interní testovací plán, který reflektuje vaše požadavky a technologickou architekturu. Testování provádíme pomocí osvědčených bezpečnostních nástrojů, mezi které patří například **Nmap, Nikto, MetaSploit, Burp Suite, Nessus, OWASP ZAP, Hydra, Aircrack-ng, Gophish** a další. Tam, kde je to nutné, vytváříme vlastní exploitovací skripty, abychom co nejvěrněji simulovali reálné hrozby.

5.1 Výsledky a vyhodnocení

Po dokončení testování obdržíte komplexní report, který obsahuje podrobný popis provedených testů, zjištěných zranitelností a doporučených opatření. **Každá zranitelnost je hodnocena dle CVSS**, což umožňuje jasné stanovení její závažnosti a prioritizaci oprav.

Report se skládá ze dvou hlavních částí:

Manažerské shrnutí poskytuje přehled hlavních zjištění a doporučení v srozumitelné formě, určené především pro vedení společnosti. Tato část stručně popisuje klíčové bezpečnostní problémy a navrhovaná opatření.

Technická zpráva obsahuje detailní analýzu testování, včetně jeho cílů, rozsahu a použitých metod. Dále vysvětluje klasifikaci nalezených zranitelností, podrobně popisuje identifikované problémy a poskytuje konkrétní doporučení k jejich nápravě. Závěr zprávy shrnuje celkové hodnocení bezpečnostního stavu testovaného systému.

5.2 Potenciální rizika spojená s penetračními testy

Penetrační testy mohou vyžadovat interakci s testovanými systémy jiným způsobem než při běžném provozu. I přes maximální opatrnost může v ojedinělých případech dojít k výpadku systému, změně nebo smazání dat či ovlivnění služeb.

Možná rizika:

- Exploitace zranitelností může způsobit dočasnou nefunkčnost některých služeb, nebo změnu dat.
- Logovací systémy mohou zaznamenat testovací aktivitu jako bezpečnostní incident.

Opatření ke snížení rizika:

- Bezpečný testovací přístup – vyhýbáme se DoS útokům a destruktivním testům.
- Zálohy – doporučujeme zajistit aktuální zálohy klíčových dat před testováním.
- Koordinace s klientem – testy provádíme v domluvených časech.
- Souhlas poskytovatele cloudu – nutné při hostovaných službách.
- Testovací prostředí – doporučujeme testování mimo produkční systémy.

Akceptací nabídky klient potvrzuje:

- Jsme si vědomi možných dopadů testování na naše systémy a data.
- Zajistili jsme souhlas všech relevantních třetích stran.

6 Referenční klienti

Klient		Typ penetračních testů
Home Credit international	HOME CREDIT	API, Web aplikace, Mobilní aplikace, Interní infrastruktura, Externí infrastruktura, Baiting, Phishing
LOGEX	LOGEX HEALTHCARE ANALYTICS	API, Web aplikace, Mobilní aplikace, Interní infrastruktura, Externí infrastruktura
Partners Bank	Partners Banka	API, Web aplikace, Mobilní aplikace
Afriland First Bank	Afriland First Bank	Web aplikace, Externí infrastruktura
Wultra	wultra	API, Web aplikace, Mobilní aplikace
NumberFour AG	enfore	API, Web aplikace, Externí infrastruktura, AWS
Allianz	Allianz	API, Web aplikace, Mobilní aplikace, Interní infrastruktura, Externí infrastruktura
Česká Spořitelna	ČESKÁ spořitelna	API, Web aplikace, Mobilní aplikace, Interní infrastruktura
Schwarz Gruppe	SCHWARZ LIDL Kaufland	API, Web aplikace, Mobilní aplikace, Interní infrastruktura, Externí infrastruktura
ŠKODA ICT	ŠKODA	API, Web aplikace, Interní infrastruktura
UCED	UCED	Web aplikace, Interní infrastruktura, Externí infrastruktura, Phishing, Vishing
SIEMENS	SIEMENS	Interní infrastruktura, Externí infrastruktura

7 Realizační tým

Penetrační testeři	**Certifikace**	**Jazyk**
Josef Havel	CHFI, CEH, ECSA, eWPT	CZ / EN
Michal Frič	CEH Master	CZ / EN
Elena Selkina	CompTIA Security+	CZ / EN / RU
Timotei Adamec	eJPT, eCPPT, eWPT, CMPen, AWS CLF-C02	CZ / EN
Filip Phouc anh Tran Huu	PNTP	CZ / EN / VIET
František Kotačka	OSCP, SCS-C01 AWS	CZ / EN
Marek Murgaš	OSCP, KLCP, OSWP	SK / EN
Projektový tým	**Role**	**Jazyk**
David Pícha	Vedoucí oddělení	CZ / EN
Kateřina Csirková	Projektová manažerka	CZ / EN

8 Závěr a poděkování

Vážíme si příležitosti poskytnout Vám naše profesionální služby v oblasti penetračních testů. Kybernetická bezpečnost je dnes klíčovým tématem a s rostoucí složitostí IT systémů je nezbytné identifikovat a eliminovat potenciální zranitelnosti.

Penetrační testování je pro nás posláním – nejen službou, ale i cestou, jak pomoci organizacím chránit jejich data a systémy. Naši klienti oceňují detailní provedení testů a konkrétní ukázky exploitace, které jasně ukazují závažnost nalezených zranitelností.

Děkujeme za Vaši důvěru a těšíme se na úspěšnou spolupráci.