Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

Č.J. NEPŘIŘAZENO • BRNO • 7. BŘEZNA 2022

VERZE DOKUMENTU: 1.0

# PENETRAČNÍ TESTOVÁNÍ
# –
# ÚVOD DO PROBLEMATIKY

Podpůrný materiál

# Obsah

# 1 Úvod

Penetrační testování a testování zranitelností je jednou z povinností vyplývajících z vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat. Konkrétně lze tuto povinnost najít v § 11 odst. 3 a § 25 odst. 1 této vyhlášky.

Vzhledem k této povinnosti vznikl podpůrný materiál, jehož cílem je poskytnout všem jeho čtenářům obecný úvod do této problematiky. Tento dokument je také vhodnou pomůckou manažerům kybernetické bezpečnosti nebo jiným osobám odpovědným za zajištění penetračního testování v rámci konkrétní organizace, především však při zajištění penetračního testování prostřednictvím externí společnosti.

Podpůrný materiál obsahuje řadu informací, které slouží k usnadnění nákupu služeb penetračního testování a upřesnění představy toho, co od něj očekávat, jako např.:

- popis rozdílu mezi penetračním testováním a skenováním zranitelností,
- popis různých typů penetračního testování,
- informace o průběhu penetračního testování,
- běžné problémy spojené s penetračním testováním,
- informace o smluvním zajištění penetračního testování.

Kromě toho materiál obsahuje také kapitoly (např. kapitola 8 a kapitola 9), které mohou být přínosné pro interní IT specialisty, včetně četných odkazů na webové stránky, kde lze najít informace o zranitelnostech nebo rady k proaktivní ochraně organizace.

Kapitola 10 „Zákulisí penetračního testování“ je určená pro osoby, které uvažují o dráze testera, a přibližuje, co tato profese obnáší a jak začít.

## 1.1 Použité zdroje

SELECKÝ, Matúš. *Penetrační testy a exploitace*. Brno: Computer Press, 2012. ISBN 978-80-251-3752-9.

## 1.2 Kontakt

V případě dotazů se prosím obracejte na sekretariát Národního úřadu pro kybernetickou a informační bezpečnost (dále jen „Úřad“):

**Národní úřad pro kybernetickou a informační bezpečnost**

Mučednická 1125/31

616 00 Brno – Žabovřesky

Tel.: +420 541 110 632

E-mail: regulace@nukib.cz

Upozornění:

Tento dokument slouží jako podpůrné vodítko, nenahrazuje žádný ze zákonů ani prováděcích právních předpisů. Právo změny tohoto dokumentu vyhrazeno.

Informace obsažené v dokumentu se vztahují k právní úpravě účinné ke dni platnosti publikované verze dokumentu.

## 2 Používané zkratky

CEH Certified Ethical Hacker (certifikace)

CISA Certified Information Systems Auditor (certifikace)

CPT Cone Penetration Test (certifikace)

DNS Domain Name System

ECSA Certified Security Analyst (certifikace)

GIAC Global Information Assurance Certification (certifikace)

GPEN GIAC Penetration Tester (certifikace)

IDS Intrusion Detection System (systém detekce napadení)

IP Internet Protocol

IPS Intrusion Prevention System (systém prevence průniku)

IT Informační technologie

Úřad Národní úřad pro kybernetickou a informační bezpečnost

OSCP Offensive Security Certified Professional (certifikace)

OSWE Offensive Security Web Expert (certifikace)

OSWP Offensive Security Wireless Professional (certifikace)

PDF Portable Document Format (přenosný formát dokumentů)

SCADA Supervisory Control And Data Acquisition (dispečerské řízení a sběr dat)

# 3 Základní informace

Penetrační testování je jeden ze způsobů proaktivní ochrany snažící se odhalit slabá místa v obraně dříve, než je někdo zneužije. Jedná se tedy o reálnou simulaci útoku, kdy dochází k pokusu proniknout do testovaného systému.

Cílem penetračního testování je identifikovat zranitelnosti a navrhnout, jak tyto nedostatky odstranit.

Na základě výsledků penetračního testování by mělo dojít k nasazení dodatečných nebo úpravě stávajících bezpečnostních opatření, a tedy ke zvýšení celkové úrovně zabezpečení.

Na základě vyhodnocení výsledků penetračního testování, by měly být zjištěné nedostatky co nejrychleji odstraněny. Po prvním penetračním testování je zpravidla odhaleno velké množství reálně zneužitelných zranitelností zabezpečení. V případě, že dojde k důslednému odstraňování zjištěných nedostatků, každé další penetrační testování odhalí menší množství reálně zneužitelných zranitelností, o to větší je však efekt na praktické zabezpečení celého systému. Pokud by nedocházelo k reakci na výsledky penetračního testování, resp. k nápravě zjištěných nedostatků, pak samotné provedení penetračního testování nebude mít žádnou přidanou hodnotu pro správce systému.

Penetrační testování nabízí specifický přístup ověření odolnosti systému vůči kybernetickým útokům, může odhalit reálně zneužitelné zranitelnosti, které mohou například interní zaměstnanci organizace přehlédnout.

Jaké výhody může provádění penetračního testování mít:

- odhalení reálně zneužitelných zranitelností,
- odhalení méně závažných zranitelností,
- ověření skutečnosti, že systém je zabezpečen efektivně a účelně,
- odhalení špatné konfigurace,
- odhalení špatného návrhu systému,
- dokončení dokumentace,
- zvýšení schopností odpovědných zaměstnanců organizace a získání doporučení, jak nálezy odstranit,
- zajímavé zkušenosti,
- poučení,
- atd.

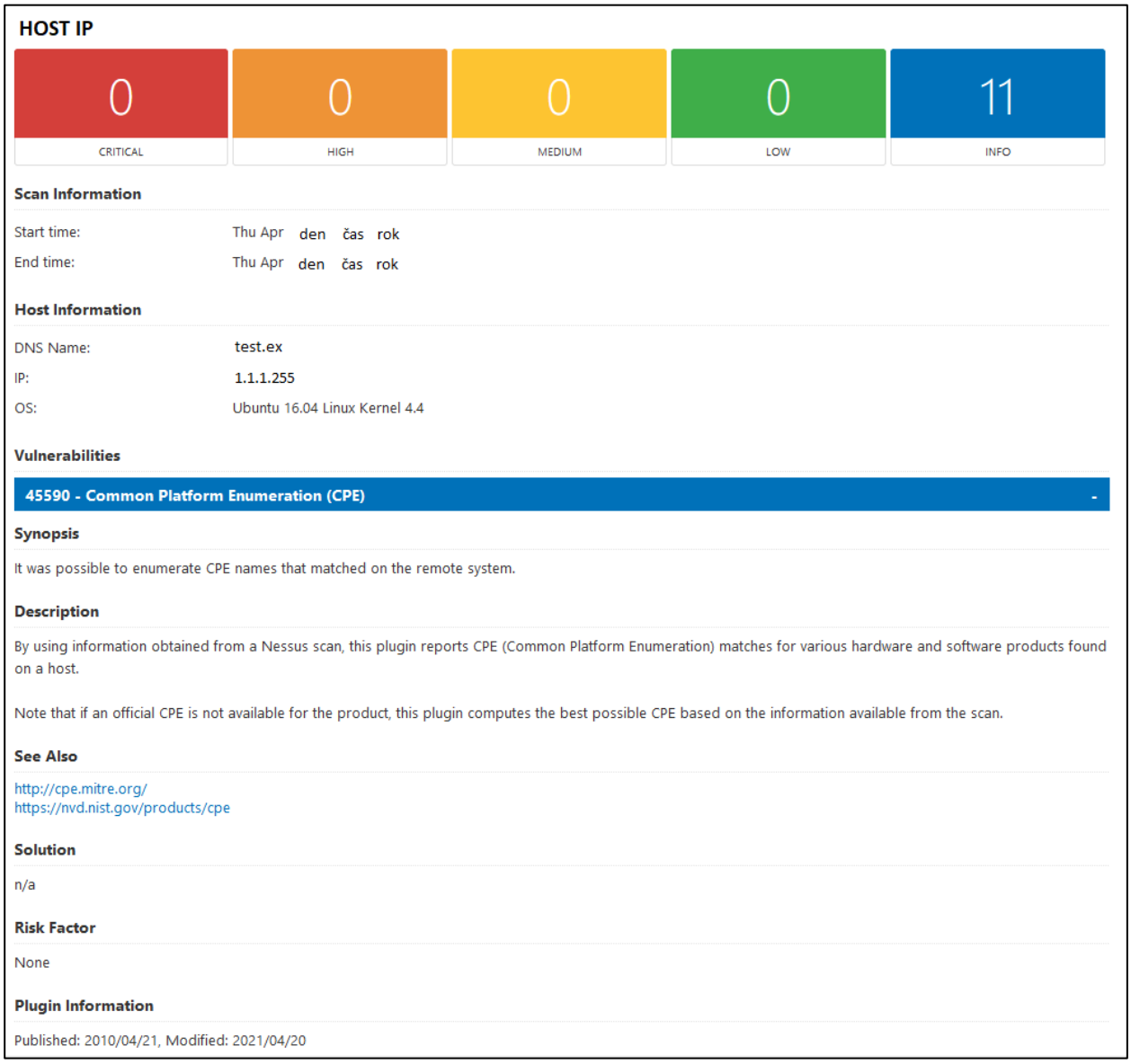
Je potřeba mít na paměti, že penetrační testování je proces směřující k získání porozumění či znalosti, který je omezen vybraným scénářem a časem, který má tester na realizaci.

## 3.1 Sken zranitelností vs. penetrační testování

Penetrační testování a sken zranitelností jsou dva rozdílné pojmy, které se mezi sebou často zaměňují, ve skutečnosti se však jedná o odlišné postupy s jinými cíli.

Zjednodušeně lze říct, že **skenování zranitelností** (Vulnerability Scan) slouží k identifikaci systémů, které mohou být potenciálně zranitelné. Pro skenování zranitelností se nejčastěji využívají automatizované skenery, jejichž výstupem je report potenciálních zranitelností. Potenciální zranitelnosti jsou to z toho důvodu, že tyto skenery určují zranitelnosti na základě předem definovaných parametrů, např. skener odešle dotaz na server a v jeho odpovědi hledá předem specifikované znaky, které by mohly naznačovat, že je server zranitelný.

Vzhledem k tomu, že se jedná o automatizovaný proces, jeho výstupem často mohou být tzv. falešně pozitivní nálezy (false positive). Jedná se o nálezy, které splňují předem definované chování pro označení dané zranitelnosti, ale ve skutečnosti se o zranitelnosti nejedná.



**HOST IP**

| 0 | 0 | 0 | 0 | 11 |
|---|---|---|---|---|
| CRITICAL | HIGH | MEDIUM | LOW | INFO |

**Scan Information**

Start time: Thu Apr den čas rok
End time: Thu Apr den čas rok

**Host Information**

DNS Name: test.ex
IP: 1.1.1.255
OS: Ubuntu 16.04 Linux Kernel 4.4

**Vulnerabilities**

**45590 - Common Platform Enumeration (CPE)** -

**Synopsis**

It was possible to enumerate CPE names that matched on the remote system.

**Description**

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

**See Also**

http://cpe.mitre.org/
https://nvd.nist.gov/products/cpe

**Solution**

n/a

**Risk Factor**

None

**Plugin Information**

Published: 2010/04/21, Modified: 2021/04/20

Obrázek č. 1: Ukázka z provedeného skenu zranitelností

**Penetrační testování** je proces identifikace zranitelností použitím různých útočných technik. Proces penetračního testování zahrnuje posuzování bezpečnosti zvolených systémů a jejich potenciálních slabin, které mohou vzniknout např. díky nedostatečné nebo nesprávné konfiguraci systému, známé nebo neznámé hardwarové či softwarové slabině atd.

Penetrační testování tedy slouží k identifikaci bezpečnostních rizik a určení jejich priorit.

Sken zranitelností je často součástí samotného penetračního testování, při kterém testeři otestují zjištěné nedostatky a určí, zda se skutečně jedná o zranitelnost. Samotný sken zranitelností není schopen odhalit všechny zranitelnosti, a proto je nutné jej doplnit manuálním testováním.

Na základě nedostatků zjištěných v průběhu penetračního testování je vytvořena závěrečná zpráva, která obsahuje nalezené zranitelnosti a doporučení, jak je odstranit.

## 3.2 Sociální inženýrství

Kromě zneužití technických zranitelností patří k útočným technikám také sociální inženýrství.

Pojem sociální inženýrství se používá pro pojmenování široké škály škodlivých aktivit sloužících k manipulaci lidí za účelem získání důvěrných informací.

Nejčastějšími záměry sociálního inženýrství bývají pokusy o získání přihlašovacích jmen a hesel, anebo instalace malwaru k získání těchto údajů.

Sociální inženýrství je technika, která se využívá čím dál víc. Kriminálníci ji používají proto, že tyto techniky umožňující zneužití lidského faktoru bývají jednodušší než se pokoušet proniknout do zabezpečené infrastruktury. **Zneužití lidského faktoru je v současnosti jedním z nejčastějších a nejúspěšnějších vektorů útoku.** Z toho důvodu je nezbytné ustavičně rozvíjet bezpečnostní povědomí uživatelů, vzdělávat je o základech kybernetické hygieny, důležitosti ochrany bezpečnosti informací a upozorňovat je na aktuální hrozby a způsoby obrany.

Phishing je typem sociálního inženýrství a má zpravidla podobu e-mailu, SMS, telefonátu nebo zprávy na sociální síti, ve které se útočník snaží přesvědčit oběť, aby mu poskytla citlivou informaci, otevřela odkaz vedoucí na škodlivou stránku, ze které stáhne malware, nebo otevřela přiložený soubor obsahující malware. Na rozdíl od spear-phishingu není personalizovaný a zpravidla je odesílán velkému množství lidí najednou. Příkladem nepříliš sofistikovaného phishingu byl v ČR v roce 2018 vyděračský e-mail, ve kterém útočníci sdělují oběti, že přes webovou kameru získali její choulostivé záběry a vyhrožují jejich zveřejněním. Aby tomu oběť zabránila, měla poslat částku v řádech stovek dolarů v bitcoinech.

Výše uvedený scénář je pouze jedním z možných.

Úřad na svých webových stránkách publikuje řadu doporučení a upozornění, která se této problematiky týkají, např.:

- Doporučení, jak se chránit před Spear-phisingem ze dne 3. dubna 2020: https://www.nukib.cz/cs/infoservis/doporuceni/1514-spear-phishing-a-jak-se-pred-nim-chranit/.

- Upozornění na některé typy hrozeb: https://www.nukib.cz/cs/infoservis/hrozby/.
- Upozornění ze dne 19. února 2020 na hrozbu typu sociálního inženýrství: https://www.nukib.cz/cs/infoservis/hrozby/1486-upozorneni-na-podvodne-emaily-zneuzivajici-epidemie-koronaviru/.
- Upozornění ze dne 27. dubna 2020 na vyděračské e-maily: https://www.nukib.cz/cs/infoservis/hrozby/1521-nova-vlna-vyderacskych-e-mailu/.
- Upozornění ze dne 4. ledna 2021 na podvodné vyděračské e-maily: https://www.nukib.cz/cs/infoservis/hrozby/1670-upozorneni-na-novou-vlnu-podvodnych-vyderacskych-emailu/.
- Upozornění ze dne 21. ledna 2021 na phisingové e-maily: https://www.nukib.cz/cs/infoservis/hrozby/1680-upozornujeme-na-novou-vlnu-phishingovych-mailu/.
- Upozornění ze dne 20. dubna 2021 na podvodné telefonáty: https://www.nukib.cz/cs/infoservis/hrozby/1705-upozorneni-na-vishing-zneuzivajici-identitu-bankovnich-instituci/.

# 4 Typy penetračních testů

Existuje několik typů penetračního testování. Penetrační testy lze rozlišovat např.:

- podle role testera,
- podle množství informací o testovaném systému,
- podle informovanosti zaměstnanců testované organizace,
- podle cíle testu.

## 4.1 Podle role testera

### 4.1.1 Externí

U externích testů se jedná o simulaci útočníka, který útočí z vnější sítě. Útočník nemá přehled o síťové infrastruktuře společnosti a disponuje jenom informacemi, které jsou volně dostupné. Externí testování je cíleno na služby, které jsou vystaveny do internetu. Může se jednat o webové stránky, webové aplikace, e-mail, DNS servery a různé jiné služby. Primárním cílem je odhalení co největšího počtu závažných zranitelností, které mohou vést k průniku a neoprávněnému přístupu do interní sítě a k získání cenných dat společnosti.

### 4.1.2 Interní

U interních testů se jedná o simulaci útočníka, který se nachází ve vnitřní síti společnosti. Může se jednat o nespokojeného zaměstnance nebo útočníka, který má fyzický nebo vzdálený přístup do síťové infrastruktury společnosti. Simulace tohoto útoku má potenciálně nejvyšší účinky dopadu, protože útočník má od počátku přístup do interní sítě.

Interní testy slouží k ohodnocení zabezpečení interní sítě a nalezení zranitelností v této síti, dále k prověření bezpečnostních mechanismů sloužících k ochraně zdrojů, služeb a dat před neoprávněným přístupem a případným zneužitím ze strany uživatelů ve vnitřní síti, jako jsou například partneři nebo vlastní dodavatelé.

## 4.2 Podle množství dostupných informací o testovaném systému[1]

### 4.2.1 Black-box

Black-box testy simulují vnější přístup útočníka, který zná jenom vstupy a potenciální výstupy aplikace, ale nikoliv vnitřní strukturu aplikace či sítě. Pro určení výstupů testovaného systému je v některých případech nezbytný poměrně rozsáhlý průzkum. Samotná funkcionalita systému je pro testera černou skříňkou (angl. black-box). Protikladem black-box testů jsou tzv. white-box testy.

Výhodou tohoto typu testů je, že v případě testování aplikací a systémů není potřebná znalost použitého programovacího jazyka a není vyžadováno ani zpřístupnění zdrojového kódu, který se často firmy snaží udržet v tajnosti. Další výhodou je vysoká míra variability, tj. možnost přizpůsobit testy na míru požadavkům zadavatele.

[1] SELECKÝ, Matúš. *Penetrační testy a exploitace.* s. 17

Mezi nevýhody lze zařadit potřebu širokých znalostí testera. Dále nemusí být objeveny chyby, které vyžadují sofistikovanější přístupy, a není ověřena efektivita (optimalizace) kódu.

#### 4.2.2 White-box

V porovnání s předchozím typem testů (black-box) jsou pro tyto testy typické plné vstupní znalosti. Jsou založeny na znalosti architektury a zdrojového kódu aplikace nebo, v případě počítačových sítí, na znalosti architektury, typu a počtu přítomných zařízení a na firemních politikách. Při testování probíhá analýza zdrojového kódu, v němž se hledají chyby. Takový druh testů vyžaduje znalost použitého programovacího jazyka a dobře napsaný a okomentovaný kód.

Hlavní výhodou je, že znalost kódu nebo struktury sítě umožňuje najít potenciální zranitelná místa v podstatně kratší době při současně podrobnější kompletní analýze. V případě aplikací je přidruženou výhodou také optimalizace kódu, kterou je možné provést na základě nalezených chyb a zranitelných míst.

V případě aplikací je nevýhodou nutná znalost použitého programovacího jazyka, což může v nepřímém důsledku zvýšit cenu testu, jelikož je od testera vyžadována vyšší kvalifikace. Další nevýhodou je časová náročnost a relativně úzké zaměření na kód a architekturu.

#### 4.2.3 Grey-box

Alternativou k předchozím dvěma typům testů jsou tzv. grey-box testy. Ty se snaží maximálně využít výhody a přínosy obou výše uvedených typů testů. Při testech se využívají znalosti vnitřní logiky aplikace, ale testy probíhají z hlediska uživatele nebo, v případě bezpečnostních testů, potenciálního útočníka.

Grey-box testy mohou také zahrnovat metody reverzního inženýrství pro určení limitních hodnot vstupních údajů nebo chybových hlášení.

### 4.3 Podle míry spolupráce

#### 4.3.1 Ohlášené (se spoluprací)

Během ohlášeného penetračního testování jsou informováni, kromě manažera kybernetické bezpečnosti (případně také jiné osoby, které objednávaly penetrační testování), také administrátoři jednotlivých systémů.

#### 4.3.2 Neohlášené

Během neohlášeného penetračního testování nejsou administrátoři jednotlivých systémů informováni a testuje se také jejich reakce a způsob detekce nežádoucích činností.

### 4.4 Podle cíle testu

Penetrační testování lze dělit také podle cíle testu:

- externí („standardní“) test – externí perimetr,
- interní test – interní síť organizace,
- webové aplikace – detailní zaměření pouze na aplikaci,

- mobilní aplikace, wifi sítě, autentizační mechanizmy, …,
- testy oddělených sítí (technická síť),
- specifické zařízení (IP telefonie, automaty, SCADA, …),
- testy nastavení IDS/IPS mechanizmů,
- atd.

## 4.5 Specifické

Tento typ testu závisí na požadavcích objednatele a na vzájemné domluvě mezi ním a poskytovatelem penetračního testu.

# 5 Fáze penetračního testování

Proces penetračního testování se skládá z několika fází, které na sebe navazují.

1. **Určení rozsahu penetračního testování**
2. **Výběr poskytovatele**
3. **Příprava (účty, prostupy, oznámení, …)**
4. **Testování**
5. **Závěrečná zpráva**
6. **Vyhodnocení testu**
7. **Závěrečná schůzka**
8. **Odstranění nálezů**

## 5.1 Určení rozsahu penetračního testování

V této primární fázi je důležité jednoznačně a nejlépe i písemně specifikovat, jaké systémy, IP adresy (odkazující například na aplikace, webové servery, databáze nebo operační systémy) a další případná aktiva organizace budou podrobena penetračnímu testování. Doporučuje se také specifikace toho, co není součástí testování, například z důvodů zajištění kontinuity služeb nabízených objednavatelem. Další nutností je určení typu plánovaného penetračního testu. V této fázi si tedy objednatel určuje obsah samotného testování a zároveň identifikuje významná aktiva (může se jednat o osobní, finanční údaje či jiná citlivá obchodní data), které jsou součástí testovaného IT systému.

Více k této fázi v kapitole 7 Smlouva.

## 5.2 Výběr poskytovatele

Při výběru poskytovatele je vhodné posuzovat jeho reputaci a reference. Reference by měly být ověřené.

Při stanovování ceny není vhodné spoléhat pouze na tzv. man-day. Někteří poskytovatelé poté dokážou položky kreativně účtovat a reálná cena penetračního testování se může značně lišit.

Při výběru testerů je vhodné posuzovat jejich praxi. V některých případech se do smlouvy uvádí i konkrétní jména testerů, kteří budou testování provádět. Lze se tak vyhnout situaci, kdy poskytovatel disponuje testery s příslušnou praxí a certifikacemi, ale reálné testování provádí méně zkušení testeři.

Na trhu je řada certifikací z oblasti penetračního testování, jako např.:

- CEH (certifikace potvrzující základní znalosti, většinou však zkouška vyžaduje jenom teoretické znalosti),
- CISA (spíše auditorská certifikace, pro penetrační testování méně vhodná),
- ECSA (certifikace potvrzující teoretické znalosti),
- GIAC (certifikace vyžadující vyšší nároky na znalosti testera),

- GPEN (certifikace potvrzující mírně pokročilé znalosti, zkouška vyžaduje i praktické znalosti),
- OSCP (certifikace potvrzující profesionální znalosti),
- OSWE (certifikace potvrzující teoretické i praktické znalosti na vysoké úrovni),
- OSWP (certifikace potvrzující teoretické i praktické znalosti na vysoké úrovni),
- atd.

Dále je možné od poskytovatele požadovat vzorové zprávy, anebo u větších rámcových smluv je možné požadovat praktické prokázání kompetence.

## 5.3 Příprava (účty, prostupy, oznámení, …)

Před samotným penetračním testováním je nutná příprava, liší se dle typu testu, patří sem např. vytvoření příslušných účtů, informování příslušných osob atd. V případě, že příprava nebude řádně provedena před samotným testováním, může dojít ke zdržení nebo jiným problémům.

## 5.4 Testování

Samotné testování lze rozdělit na několik dílčích fází:

- **Plánování a průzkum** – tato fáze se skládá z pasivního a aktivního získávání informací o objednateli. Výstupem jsou rozsahy IP adres a informace o zaměstnancích (např. telefonní čísla, e-mailové adresy).
- **Skenování** – jedná se o proces testování cílené stanice se záměrem získání užitečných informací, které by mohly být využity v pozdějších fázích testování.
- **Enumerace** – je proces extrahování informací z cíleného systému z důvodu získání bližšího určení specifikací systému. Výstupem této fáze mohou být uživatelé a skupiny, sdílené složky, jména strojů atd.
- **Zisk přístupu** – jedná se o komplexní fázi, která se dělí do více kroků jako lámání hesel ke kompromitaci účtu, eskalování privilegií z běžného uživatele na administrátora apod.

## 5.5 Závěrečná zpráva

Jedná se o dokument, který je poskytnut objednateli jako důkaz o tom, co bylo vykonáno.

Existují případy, kdy je snaha odevzdat sken zranitelností jako výstup penetrační testování. Jedná se však o odlišné procedury, které nelze vzájemně zaměňovat. **Výstup ze skenování zranitelností není závěrečnou zprávou penetračního testování.**

Závěrečná zpráva zpravidla obsahuje:

- manažerské shrnutí,
- harmonogram testu,
- přesné zadání testu,
- omezení testu,

- použitou metodologii,
- nalezené problémy,
- detailní popis zranitelností,
- doporučení k odstranění nálezů,
- přehledové tabulky (tabulka nálezů, tabulka systémů apod.).

Užitečným zdrojem pro tuto oblast může být podpůrný materiál zveřejněný na stránkách Úřadu týkající se požadavků na zprávy z penetračních testů v souvislosti s cloud computingem: https://www.nukib.cz/download/publikace/podpurne_materialy/_2021-11-02_Pozadavky_zprava_pentesty_1.0.pdf.

## 5.6 Vyhodnocení testu

Po provedení penetračního testování je potřeba prodiskutovat nálezy.

Dále je potřeba jednotlivé nálezy posoudit v kontextu samotné organizace, určit priority k nápravě a zadat jednotlivé úkoly.

## 5.7 Závěrečná schůzka

U větších nebo závažnějších testů je **doporučeno udělat závěrečnou schůzku,** kdy dojde k osobnímu setkání s testery a prodiskutování problémových nálezů.

V rámci diskuze dojde k vyjasnění nálezů a doporučení, jak se s těmito nálezy vypořádat. Testeři mohou poskytovat i neformální rady.

Cílem závěrečné schůzky je lepší vysvětlení nálezů, zlepšení vzájemného vztahu a poskytnutí zpětné vazby všem účastníkům.

## 5.8 Odstranění nálezů

Na základě výsledku testu je potřeba stanovit úkoly vedoucí k nápravě nevyhovujícího stavu včetně termínu jejich provedení.

Po jejich splnění je často realizován **retest nálezů.** Retest nálezů zkoumá, zda byly zjištěné nedostatky napraveny. **Nejedná se o opakování penetračního testu.**

Nelze předpokládat, že po odstranění nálezů je již systém bezpečný. Tyto nálezy mohly blokovat jiné chyby, které se mohou objevit např. v průběhu dalšího penetračního testování.

# 6 Běžné problémy u penetračního testování

- snaha vydávat sken zranitelností za penetrační testování,
- nekompetentní poskytovatel (nebo tester),
- nedokončená práce,
- špatný odhad rozsahu testu,
- nadhodnocování/podhodnocování nálezů,
- termíny (např. nedodržení termínu, špatně zvolený termín),
- není dodržena nezávislost testerů,
- zásahy administrátorů do průběhu testování,
- vyjmutí důležitých prvků z testování,
- nedostatečná komunikace v rámci organizace nebo s testery.

## 6.1 Rizika spojená s průběhem penetračního testování

Penetrační testování s sebou přináší rizika, mezi která patří např.:

- při provádění automatizovaných testů může dojít k odmítnutí služby (denial of service) nebo k omezení provozu,
- pád systému,
- zahlcení sítě,
- spuštění tiskáren,
- při testování autentizace může dojít k zablokování účtů,
- získání přístupu do systému a k získání citlivých dat,
- získání přístupu jako reálný uživatel nebo administrátor,
- nestandardní chování aplikace,
- nechtěná aktivita (např. e-maily zákazníkům),
- průnik do cizích systémů (dodavatelé, soukromé, VPN, …)
- aktivace bezpečnostních mechanizmů aplikace/firewallu (může dojít k zaslání oznámení administrátorovi),
- zaplnění logovacího systému,
- poškození/zahlcení prvku nacházejícím se mezi útočícím a testovaným systémem,
- ztráta nebo znehodnocení dat,
- tvorba fiktivních registrací,
- shromažďování osobních údajů a jejich zpracovávání pro potřeby řádného provedení penetračního testování,
- při nedostatečné komunikaci může v organizaci nastat panika.

# 7 Smlouva

Písemná smlouva je neodmyslitelnou součástí penetračních testů a poskytuje právní ochranu všem zainteresovaným stranám. Kvalitně zpracovaná smlouva o provedení penetračních testů jednoznačně vymezuje záměry stran, atributy testu a předchází sporům, či případně významně urychluje jejich řešení. Její zpracování by mělo být provedeno po technické a právní stránce odborně a pečlivě. V následujícím textu se zaměříme na její nejdůležitější obsahové náležitosti.

Obecná smlouva o provedení penetračních testů by měla obsahovat alespoň následující informace:

- **Identifikace smluvních stran**

V této části smlouvy jsou uvedeny základní údaje o objednateli a poskytovateli služeb penetračních testů.

- **Vymezení pojmů**

Vzhledem k tomu, že se bude často jednat o smlouvu, kterou mezi sebou sjednávají nejen IT profesionálové, je vhodné smluvně definovat jak pojmy typické pro oblast penetračního testování, tak i další pojmy, které mohou mít v kontextu smlouvy specifický význam. Tímto se předchází nejednoznačnému výkladu zavedených pojmů a případným sporům o jejich významu.

- **Předmět smlouvy**

Tato část by měla konkrétně popisovat sjednávaný penetrační test, jeho rozsah a atributy, včetně vymezení vzájemných práv a povinností mezi objednatelem a poskytovatelem. Předmětem plnění je závazek poskytovatele k provedení penetračních testů pro předem určený rozsah zvolených IP adres. Objednatel v této části smlouvy, nebo formou odkazu na přílohu smlouvy upravující specifikaci testování, sepíše seznam IP adres s určením, co se na nich zpravidla nachází (může se jednat například o aplikace, servery nebo operační systémy). Dále konkretizuje závazek poskytovatele k dodržení nezbytných požadavků, před, v průběhu a po ukončení penetračních testů, jakými jsou například:

  - určení typu penetračních testů;
  - určení časového harmonogramu penetračních testů, s ohledem na zajištění běžného chodu IT systémů;
  - podrobné vymezení rozsahu penetračních testů;
  - sjednání možnosti účasti objednatele na penetračním testování;
  - určení způsobu vyhodnocení zjištěných skutečností;
  - zakotvení pravidel vzájemné komunikace;
  - vytvoření seznamu používaných testovacích nástrojů a jejich konfigurace;

- vyjasnění podmínek prováděného penetračního testu ve vztahu k platné legislativě České republiky[2] (např. přístup do systému v rámci smluveného penetračního testování nebude vnímán jako kybernetický bezpečnostní incident dle § 8 zákona o kybernetické bezpečnosti nebo porušení zabezpečení osobních údajů dle čl. 33 GDPR);
- zakotvení povinnosti postupu poskytovatele v souladu s mezinárodně uznávanou metodikou a standardy pro provádění penetračních testů, jako je metodika OSSTMM a standardy NIST 800–115 a OWASP Top 10;[3]
- zajištění sběru dat ve smyslu vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti.

Důležitou součástí tohoto článku je závazek poskytovatele k vypracování závěrečné zprávy (viz podkapitola 5.5 Závěrečná zpráva) a určení maximální doby pro její zpracování od provedení penetračních testů. Pro obě strany je důležité smluvní vymezení konkrétních náležitostí, ve smyslu, co má a co nemá závěrečná zpráva o provedeném penetračním testování obsahovat. Jedná se zejména o rozsah penetračního testu, metodu testování, popis jednotlivých testovaných prvků, popis zjištěných zranitelností[4] a další sjednané náležitosti dle konkrétních požadavků objednatele.

- **Cena penetračního testu a platební podmínky**

V rámci transparentnosti a naplnění vzájemných očekávání smluvních stran je možné určit cenu penetračních testů stanovením pevné finanční částky zohledňující náročnost, rozsah a zvolenou metodiku testovaní. Pokud bude předem objektivně určena cena, nebude docházet k případným nejasnostem mezi objednatelem a poskytovatelem penetračního testování, plynoucím z určení ceny až po provedení penetračních testů.

V případě, že smlouva bude obsahovat závazek k provedení většího množství penetračních testů v delším časovém období, je vhodné smluvně zakotvit, že cena za jednotlivé penetrační testy bude hrazena na základě vystavení akceptačního protokolu, ten zpravidla obsahuje náležitosti vyúčtování a ustanovení o splatnosti sjednané ceny za jednotlivé penetrační testování. Kontrola plnění a proces jednotlivé akceptace většího počtu penetračních testů uskutečněných v delším

[2] Zákon o kybernetické bezpečnosti č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (**zákon o kybernetické bezpečnosti**), ve znění pozdějších předpisů, vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (**vyhláška o kybernetické bezpečnosti**), zákon č. 110/2019 Sb., o zpracování osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů a Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volném pohybu těchto údajů („**GDPR**“)

[3] The Open Source Security Testing Methodology Manual (OSSTMM): https://www.isecom.org/OSSTMM.3.pdf; https://www.isecom.org/research.html#content5-9d, Technical Guide to Information Security Testing and Assessment, NIST SP 800-115: https://csrc.nist.gov/publications/detail/sp/800-115/final, OWASP Top ten web application security risks: https://owasp.org/www-project-top-ten/.

[4] Například odkazem na mezinárodně uznávanou metodiku hodnocení závažnosti objevených zranitelností CVSS https://www.first.org/cvss/specification-document.

časovém období je prováděna smluvně určenými oprávněnými osobami. Akceptační protokol (který bývá zpravidla přílohou smlouvy) bude vycházet z jednotlivých zpráv o provedeném penetračním testování, které byly poskytovatelem předloženy k akceptaci. Poskytovatel vypracuje a odešle objednateli akceptační protokol o provedeném penetračním testování ke schválení. Objednatel je zpravidla povinen dle smlouvy akceptační protokol akceptovat, resp. podepsat, nebo definovat výhrady k provedenému penetračnímu testování. Smlouva o penetračním testování by měla také obsahovat závazek poskytovatele objednatelem uplatněné výhrady co nejdříve napravit, nedohodnou-li strany smlouvy jinak. Jakmile jsou objednatelem vznesené výhrady opraveny, doporučuje se vystavit nový akceptační protokol. Po jeho schválení poskytovatel penetračního testování vystaví fakturu. Samotná faktura by kromě ceny měla obsahovat specifikaci provedených penetračních testů, měla by odkazovat na sjednanou smlouvu o penetračním testování a obsahovat rozpis jednotlivých položek určující celkovou cenu za penetrační testování.

- **Místo plnění a doba trvání smlouvy**

Ve smlouvě se doporučuje mít uvedenou konkrétní adresu místa plnění, nebo zakotvit jiné ujednání, které zohledňuje konkrétní typ a lokalizaci testovaného prostředí objednatele. Penetrační testy je možné realizovat i vzdáleně, pokud to povaha plnění organizačně i technicky umožňuje. Smlouva je obvykle uzavírána na dobu určitou a běžně je ukončena dokončeným skenováním a předáním závěrečné zprávy.

- **Oprávněné osoby**

V tomto článku jsou typicky konkretizovány osoby oprávněné jednat jménem objednatele a poskytovatele při plnění smlouvy. Může být uveden celý realizační tým poskytovatele a objednatele penetračního testu, nebo pouze primární a sekundární kontaktní osoby. Pro rychlou identifikaci oprávněných osob se doporučuje uvádět jejich celé jméno, funkci, e-mail a telefonní kontakt. Z praktických důvodů je tento článek často samostatnou přílohou smlouvy.

- **Mlčenlivost a ochrana osobních údajů**

V tomto článku mezi sebou smluvní strany sjednají vzájemnou povinnost zachovávat mlčenlivost o všech informacích, o kterých se dozvěděly během uzavírání smlouvy a v průběhu jejího trvání. Jedná se o informace, které nejsou běžně dostupné a jedna ze smluvních stran projevila vůli, aby se na tyto informace povinnost mlčenlivosti vztahovala, nebo s ohledem na povahu těchto informací to lze oprávněně předpokládat. Trvání této povinnosti by mělo být písemně zakotveno i po skončení platnosti smlouvy o provedení penetračního testu. Ustanovení o mlčenlivosti se nebude vztahovat na případy, kdy jsou smluvní strany povinny poskytnout informace na základě zákona, nebo jedna ze smluvních stran se zpřístupněním konkrétní informace písemně souhlasila. V souvislosti s plněním smlouvy by primárně nemělo docházet ke zpracování osobních údajů. Bude-li to s ohledem na specifikaci testovaného prostředí nezbytné, je dobré v tomto článku, případně v samostatné zpracovatelské smlouvě, stanovit povinnost poskytovatele v pozici

zpracovatele osobních údajů přijmout adekvátní organizační a technická opatření k dostatečné ochraně osobních údajů a zajištění jejich znepřístupnění bez souhlasu objednatele.

- **Rizika skenování a náhrada újmy**

V průběhu penetračního testu dochází k využití různých útočných technik, které mohou vykazovat znaky reálného kybernetického útoku. Aktivity, které bude poskytovatel v souvislosti s penetračním testem provádět, mohou ohrozit či omezit provoz a fungování informačních systémů objednatele a infrastruktury s nimi spojené, a mohou přímo či nepřímo způsobit újmu objednateli nebo jiným osobám.

Doporučuje se mít smluvně ošetřeny veškeré nestandardní jevy, ke kterým v souvislosti s penetračním testem může docházet. Demonstrativní výčet rizik je možné smluvně zakotvit odkazem na přílohu smlouvy, ve které budou jednotlivá rizika uvedena (viz podkapitola 6.1). Díky jejich smluvnímu zakotvení, včetně vyloučení či omezení povinnosti k náhradě vzniklé újmy, je objednatel včas seznámen s riziky a byl před jejich možným vznikem varován. Poskytovatel pak není odpovědný za škody vzniklé v průběhu penetračního testování jako je nedostupnost, ale i poškození informačního systému. To neplatí, pokud tyto škody byly způsobeny úmyslným jednáním poskytovatele nebo z jeho hrubé nedbalosti.

Ujednání upravující náhradu újmy by mělo být koncipováno takovým způsobem, že není-li ve smlouvě stanoveno jinak, bude se řídit platnými právními předpisy. Objednatel je odpovědný za škody způsobené poskytovateli jakýmkoliv porušením smluvní povinnosti, poskytovatel zase za veškerou újmu vzniklou v důsledku vadného plnění nebo porušením jiné právní povinnosti.

Je na domluvě smluvních stran, jakým způsobem si upraví vzájemnou odpovědnost za případně způsobenou újmu, to platí také ve vztahu ke třetím stranám. Typicky bude docházet k omezení či úplnému vyloučení odpovědnosti poskytovatele za jakoukoli újmu vzniklou v souvislosti s plněním smlouvy, nebyla-li způsobena úmyslně nebo z hrubé nedbalosti. Objednal může případně požadovat, aby měl poskytovatel po dobu účinnosti smlouvy sjednané pojištění odpovědnosti za škodu způsobenou vlastní činností v souvislosti s poskytováním penetračních testů. Smluvně lze předem upravit i maximální možnou výši pojistného plnění.

- **Sankční ujednání**

Tento článek, pokud se strany na jeho sjednání mezi sebou dohodnou, plní preventivní funkci pro případ, že jedna ze stran poruší konkrétní smluvní povinnost. Jeho obsahem bude často ujednání k specifickému finančnímu plnění, resp. smluvní pokutě. Typické důvody pro sjednání smluvní pokuty jsou například prodlení poskytovatele s provedením penetračního testu nebo vypracováním závěrečné zprávy, nebo prodlení objednatele se splacením faktury za provedený penetrační test, případně porušení ustanovení o mlčenlivosti. Strany smlouvy mohou mezi sebou stanovit jednotlivé dílčí smluvní pokuty při porušení konkrétních smluvních povinností.

- **Odstoupení od smlouvy**

S ohledem na § 2002 zákona č. 89/2012 S b., občanský zákoník, ve znění pozdějších předpisů jsou smluvní strany oprávněny, za určitých okolností od sjednané smlouvy odstoupit. Doporučuje se smluvně zakotvit objektivní okolnosti, na základě kterých by k takovému odstoupení některé ze stran mělo dojít. Může se jednat například o déle trvající prodlení poskytovatele s plněním smluvně zakotvených lhůt nebo o jakékoliv jiné porušení povinnosti, které nebude ve sjednané době napraveno. Aby mohlo být odstoupení od smlouvy platné, je nutné zakotvení jeho písemného doručení straně, jíž se odstoupení týká.

- **Závěrečná ustanovení**

Tento poslední článek obvykle reflektuje a doplňuje specifická ujednání z předchozích článků, jako je upřesnění doručování vzájemné komunikace či způsob zaslání odstoupení od smlouvy (ideálně do datové schránky). Běžně rovněž upravuje okolnosti, za kterých může dojít k změnám a doplněním smlouvy, například formou dodatků, které však musí být smluvními stranami řádně datovány a podepsány. Standardní je také písemné prohlášení smluvních stran, že smlouva byla uzavřena na základě pravé, vážné a svobodné vůle, při respektování principu rovnosti.

# 8 Praktické rady a doporučení k zabezpečení organizace

Ochrana organizace vůči kybernetickým útokům se může zdát jako příběh bez konce. Po opravení jedné zranitelnosti se objeví další a tahle situace se neustále opakuje. Proto je potřeba dbát na proaktivní ochranu organizace.

Základním stavebním kamenem je používat aktuální software, ať už se jedná o operační systém nebo například software na čtení PDF dokumentů. Ne vždy je možné toto pravidlo dodržet, proto je dobré alespoň disponovat seznamem nainstalovaného softwaru a jeho verzí, kde se dá na základě známých zranitelností určit potenciální riziko.

Na klientských stanicích je dobré používat seznam povolených aplikací tzv. application whitelisting, který povoluje spouštění jenom předem definovaných aplikací. Toto opatření není u uživatelů úplně oblíbeno, ale slouží například k zabránění spuštění malwaru. Uživatelské účty by měly být rozděleny do skupin a měly by mít jenom ta oprávnění, která jsou zapotřebí k výkonu práce. To znamená, že uživatelé by ke stanici neměli mít administrátorský přístup. To stejné pravidlo platí pro administrátory. Nedoporučuje se používat jeden administrátorský účet napříč celou doménou, protože pokud dojde k jeho kompromitaci, útočník bude schopen získat všechna data. Z toho důvodu by se měl účet doménového administrátora používat výhradně při přihlašování k řadiči domény a nikam jinam.

Dalším důležitým bodem je tvorba hesel. Pro uživatele se může jednat o náročný proces, např. pokud jsou vyžadována dlouhá a komplexní hesla (obsahující malá i velká písmena, číslici, speciální znaky atd.) a navíc je v organizaci vyžadována pravidelná změna hesla v krátkém časovém období. Pro uživatele je náročné si tato hesla pamatovat, obzvlášť pokud v rámci výkonu běžné pracovní činnosti potřebují takových hesel několik. Většina uživatelů má tendenci používat krátká hesla (pokud nejsou zakázána), nebo „recyklovaná“ hesla, což znamená, že jsou využívána i v jiných aplikacích.

Příklad: mám psa, který se jmenuje Bobík, takže si heslo nastavím na „Bobik123“. Pokud si mě útočník vyprofiloval a na základě dohledaných informací ví, že můj pes se jmenuje Bobík, tak při tvorbě přizpůsobeného slovníku se tam tohle heslo bude nacházet. Doporučením pro tvorbu hesla může být například použití nějaké věty s aplikací velkých/malých písmen a čísel, takže pokud moje heslo bude např. „MujPesJeBobik1“, pravděpodobnost, že útočník tohle heslo uhádne, je zanedbatelná.

Doporučit lze v maximální možné míře využívat vícefaktorovou autentizaci s nejméně dvěma různými typy faktorů.

Dále doporučujeme:

- penetrační testy provádět pravidelně,
- střídat poskytovatele (alespoň 2 různé),
- využívat doporučení a zkušenosti odborníků zabývajících se danou problematikou,
- implementovat nápravná opatření,

- snažit se o pozitivní přijetí procesu penetračního testování u administrátorů systémů (vyzdvihovat zlepšení zabezpečení, cílem není kontrolovat administrátora),
- zajistit nezávislé provedení penetračního testování (testeři by neměli být potenciálně závislí na dodavateli nebo provozovateli systému).

Není vhodné:

- spoléhat na tvrzení dodavatelů, že provádí „vlastní testování“,
- vybírat podle nejnižší ceny,
- preferovat „univerzální konzultanty“,
- čekat na poslední chvíli (např. konec roku),
- snažit se změnit skutečnosti uvedené v závěrečné zprávě.

# 9 Informace o zranitelnostech

Tato kapitola obsahuje odkazy na webové stránky, na kterých lze nalézt informace o zranitelnostech.

Weby s popisem známých zranitelností:

https://vuldb.com/

https://cve.mitre.org/

https://nvd.nist.gov/

https://snyk.io/vuln

Weby s nejnovějšími informacemi o zranitelnostech:

https://portswigger.net/daily-swig/vulnerabilities

https://www.scmagazine.com/home/security-news/vulnerabilities/

https://www.trendmicro.com/vinfo/in/security/news/vulnerabilities-and-exploits

https://thehackernews.com/search/label/Vulnerability

https://nakedsecurity.sophos.com/

https://www.hackread.com/

# 10 Zákulisí penetračního testování

Tento podpůrný materiál v předchozích kapitolách přibližoval problematiku penetračního testování tak, aby se čtenář mohl seznámit se základními pojmy, získal povědomí o tom, jak penetrační testování probíhá, anebo co všechno obnáší, když chce organizace zajistit penetrační testování svých systémů.

Tato kapitola však přináší pohled z druhé strany, a to přímo od zdroje – odborníka na penetrační testování a zaměstnance Úřadu. Formou rozhovoru se nyní můžete seznámit s tím, jaké to je „hrát si na útočníka a zdolávat překážky při dobývání nepřátelského území“.

*Jak vypadá takový typický den odborníka na penetrační testování?*

Je náročné definovat typický den, protože každý den přináší něco nového. Někdy dojde k odhalení potenciální zranitelnosti, a potom u ní člověk klidně prosedí celý den a vůbec nevnímá čas. Někdy je tak zabraný do práce, že vůbec nevnímá okolí nebo základní potřeby jako hlad.

Jiné dny jde zase práce hezky od ruky, ale nezbývá čas na pečlivé zapisování poznámek, např. jaká zranitelnost byla využita, jakým způsobem byl kompromitován daný systém nebo eskalována oprávnění.

*Co je na práci odborníka na penetrační testování zajímavé?*

Jak jsem už zmínil v předchozí otázce, každý den přináší něco nového, což s sebou přináší motivaci k rozvíjení svých schopností a znalostí. Penetrační testování není jen o tom hledat zranitelnosti a pokoušet se o jejich zneužití, ale hlavně o samotném rozvoji testera.

*Existuje více typů odborníků na penetrační testování?*

Penetrační testování se dá rozdělit do různých podkategorií, např. testování webových aplikací, síťové infrastruktury, mobilních aplikací, kryptografie atd. Každý si najde to, co ho baví.

*Když by se někdo chtěl stát testerem, kde by měl začít?*

Existují spousty knih, které popisují proces penetračního testování a návody, jak využívat vhodné nástroje. Často bývají na online portálech akce na soubory takových knih v PDF verzi. Tyto knihy jsou dobrým zdrojem užitečných informací. Pro získání praktických zkušeností existují portály s virtuálními stroji a lze na nich zkoušet exploitace různých typů zranitelností. Mezi nejznámější portály patří HackTheBox, PentesterLab, TryHackMe nebo Hack.Me.

*Pokud by se někdo chtěl stát profesionálem, jak může dokázat úroveň svých schopnosti? Existuje nějaký typ certifikace?*

V rámci informační bezpečnosti existuje několik druhů certifikací, které dokazují, že daný člověk disponuje znalostmi potřebnými pro jejich získání. Některé typy certifikátů, např. od EC-Council CEH, ECSA atd. dokazují teoretickou znalost problematiky, ale ne tu praktickou. Tyto certifikace jsou vhodným vstupním bodem do problematiky penetračního testování.

Mezi certifikace s vyššími nároky na znalosti patří např. GIAC. Tato certifikace je v Evropě málo známá a je spojena s odbornými kurzy pořádanými organizací SANS.

Certifikace, které vyžadují jak teoretické, tak praktické znalosti na vysoké úrovni jsou ty od společnosti Offensive Security. Jedná se o certifikáty jako OSCP, OSWP, OSWE atd.

# 11 Podmínky využití informací

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol (dostupná na webových stránkách www.nukib.cz/cs/infoservis/doporuceni/1593-doporuceni-k-pouzivani-protokolu-tlp-ke-sdileni-chranenych-informaci/). Informace je označena příznakem, který stanoví podmínky použití informace. Jsou stanoveny následující příznaky s uvedením charakteru informace a podmínkami jejich použití:

| Barva | **Podmínky použití** |
|---|---|
| Červená<br>TLP: RED | Informace nemůže být poskytnuta jiné osobě než té, které byla informace určena, nebudou-li výslovně stanoveny další osoby, kterým lze takovou informaci poskytnout. V případě, že příjemce považuje za důležité informaci poskytnout dalším subjektům, lze tak učinit pouze se souhlasem původce informace. |
| Oranžová<br>TLP: AMBER | Informace může být sdílena v rámci organizace, které byla informace poskytnuta. Dále může být poskytnuta pouze těm partnerům, kteří splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci. Jiným osobám, než výše uvedeným, nesmí být informace poskytnuta. Původce informace může rozsah sdílení dále omezit. |
| Zelená<br>TLP: GREEN | Informace může být sdílená v rámci organizace příjemce a případně také s dalšími partnerskými subjekty příjemce, avšak nikoli skrze veřejně dostupné kanály; příjemce musí při předání zajistit důvěrnost komunikace. |
| Bílá<br>TLP: (WHITE) | Informace může být dále poskytována a šířena bez omezení. Případné omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran nejsou tímto ustanovením dotčena. |

| **Verze dokumentu** | | | |
|---|---|---|---|
| **datum** | **verze** | **změněno** | **popis změny** |
| 7. března 2022 | 0.1 | Odbor regulace, oddělení penetračního testování | Vytvoření dokumentu |