

Penetrační testování a Red Teaming

V oblasti kybernetické bezpečnosti jsou **penetrační testování** a **Red Teaming** dvěma hlavními metodami, jak aktivně prověřovat odolnost systémů. Ačkoliv se často zaměňují, jejich cíle, rozsah a metodika se výrazně liší.

1. Penetrační testování (Pen-testing)

Penetrační test je autorizovaný a simulovaný útok na počítačový systém, aplikaci nebo síť s cílem najít zranitelnosti.

- **Cíl:** Identifikovat co nejvíce zranitelností v daném časovém rámci.
- **Rozsah:** Obvykle omezen na konkrétní aplikaci, IP adresy nebo segment sítě.
- **Povaha:** Systematické hledání chyb (např. SQL injection, slabá hesla, neaktualizovaný software).
- **Výstup:** Podrobný seznam nálezů s doporučením k jejich opravě.

2. Red Teaming

Red Teaming je komplexní simulační cvičení, které testuje nejen technologie, ale i lidi a procesy. Simuluje reálného útočníka (APT - Advanced Persistent Threat), který má konkrétní cíl (např. zcizit databázi klientů).

- **Cíl:** Provéřit detekční a reakční schopnosti organizace (Blue Teamu).
- **Rozsah:** Široký. Zahrnuje technologický útok, sociální inženýrství i fyzické vniknutí do budovy.
- **Povaha:** Skrytá operace. O testu ví jen minimum lidí v organizaci, aby byla reakce IT týmu autentická.
- **Výstup:** Hodnocení toho, jak hluboko se útočník dostal a jak efektivně byl (nebo nebyl) odhalen.

Srovnání metod

Vlastnost	Penetrační testování	Red Teaming
Hlavní zaměření	Zranitelnosti a chyby (Assets)	Schopnost detekce a reakce (People/Process)
Délka trvání	1-4 týdny	Měsíce
Nápadnost	Často odhalitelný (skenování)	Velmi nízká (stealth)
Metodika	OWASP, PTES, NIST	TIBER-EU, MITRE ATT&CK
Výsledek	Seznam „děr“ k záplatování	Zlepšení celkové bezpečnostní strategie

Red Teaming v éře AI

S nástupem modelů jako ChatGPT nebo TensorFlow se objevuje nová disciplína: **AI Red Teaming**. Ten se zaměřuje na specifické útoky proti umělé inteligenci:

- **Prompt Injection:** Pokusy přimět model ignorovat své instrukce a vygenerovat škodlivý obsah.
- **Data Poisoning:** Manipulace s trénovacími daty za účelem vytvoření „zadních vrátek“ v modelu.
- **Exfiltrace modelu:** Snaha ukrást váhy modelu nebo citlivá data, na kterých byl model trénován.

Blue Team a Purple Teaming

Kromě útočného týmu (Red Team) existují i další role:

- **Blue Team:** Obránci. Monitorují síť, detekují útoky a reagují na incidenty.
- **Purple Teaming:** Model spolupráce, kde Red Team a Blue Team pracují společně v reálném čase. Red Team provede útok a okamžitě s Blue Teamem probírá, zda byl vidět v logách a jak zlepšit detekci.

Tip: Pro menší firmy je vhodnější začít pravidelným penetračním testováním. Red Teaming je určen pro zralé organizace, které už mají vybudované silné obranné mechanismy a chtějí je otestovat pod reálným tlakem.

— Související témata:

- [Bezpečnostní standardy \(AI Safety\)](#)
- [Psychologie sociálního inženýrství](#)
- [Nástroje pro SIEM a SOC](#)

From:

<https://www.serviceit.cz/> - IT ENCYKLOPEDIE

Permanent link:

<https://www.serviceit.cz/doku.php?id=cyber:pentesting>

Last update: **2026/01/20 18:04**

