Penetrační testování (Pentest)

Penetrační testování je proces aktivního prověřování bezpečnosti IT infrastruktury. Na rozdíl od pouhého „skenování zranitelností“ jde pentest o krok dál – tester se pokouší nalezené chyby skutečně zneužít, aby prokázal jejich reálný dopad a zjistil, jak hluboko do systému se může dostat.

Typy penetračních testů

Pentesty se dělí podle toho, kolik informací má tester o cíli předem k dispozici:

- **Black Box (Černá skříňka):** Tester nemá žádné informace o vnitřní struktuře systému. Simuluje útok zvenčí (např. od neznámého hackera z internetu).
- **White Box (Bílá skříňka):** Tester má k dispozici kompletní dokumentaci, síťová schémata i zdrojové kódy. Jde o nejdetailnější formu prověrky.
- **Grey Box (Šedá skříňka):** Tester má omezené informace, například uživatelský účet s nízkými právy. Simuluje útok zevnitř firmy (např. nespokojený zaměstnanec).

Metodika a fáze pentestu

Profesionální penetrační test (např. podle metodiky OWASP nebo OSSTMM) probíhá v několika krocích:

```
1. **Plánování a průzkum (Reconnaissance):** Sběr veřejně dostupných informací o cíli (OSINT), zjišťování IP adres, domén a používaných technologií.
2. **Skenování a analýza (Scanning):** Zjišťování otevřených portů, běžících služeb a hledání známých zranitelností.
3. **Získání přístupu (Exploitation):** Samotný pokus o průnik (např. pomocí [[sql_injection|SQL Injection]], [[command_injection|Command Injection]] nebo sociálního inženýrství).
4. **Udržení přístupu (Persistence):** Tester zjišťuje, zda by v systému dokázal zůstat delší dobu (např. instalací zadních vrátek – backdoors).
5. **Analýza a reportování:** Nejdůležitější fáze. Výsledkem je detailní zpráva obsahující seznam chyb, jejich riziko a doporučení k opravě.
```

Oblasti testování

- **Webové aplikace:** Testování zranitelností v kódu stránek (dle standardu OWASP Top 10).
- **Síťová infrastruktura:** Prověrka Wi-Fi sítí, firewallů, VPN a serverových služeb.

- **Mobilní aplikace:** Hledání chyb v aplikacích pro Android a iOS.
- **Sociální inženýrství:** Testování ostražitosti zaměstnanců (např. pomocí simulovaného phishingu).
- **Fyzický pentest:** Pokus o fyzické vniknutí do budovy nebo datového centra.

Pentest vs. Skenování zranitelností

Vlastnost	Skenování zranitelností	Penetrační test
Provedení	Automatizované (nástroje jako Nessus).	Kombinace automatizace a ruční práce experta.
Hloubka	Najde jen povrchní chyby.	Najde složité logické chyby a řetězové útoky.
Dopad	Identifikuje riziko.	Prokáže reálný dopad (např. ukradne data).
Četnost	Často (týdně/měsíčně).	Nárazově (1–2x ročně nebo po velké změně).

Etika a legálnost

Základním rozdílem mezi pentesterem a hackerem je **souhlas**. Každý pentest musí mít:

```
1. Písemnou smlouvu (Rules of Engagement): Jasně definované cíle, co se smí a nesmí testovat.
2. Právní krytí: Dokument, který chrání testera před trestním stíháním za průnik.
3. Cíl: Zlepšení bezpečnosti, nikoliv obohacení nebo poškození.
```

Související pojmy: OWASP, SQL Injection, WAF, Malware, Kybernetická bezpečnost, Phishing, Rootkit.