



# G - Pentest I

## Interné penetračné testovanie

Čo si predstavíte, keď počujete slovo „bezpečnosť“?  
Bezpečnostné dvere na svojom byte, airbag vo vašom aute,  
bankovú bezpečnostnú schránku?

Na ktorom mieste v poradí dôležitosti stojí  
bezpečnosť vášho informačného systému?

# G - Pentest I

## Interné penetračné testovanie bezpečnosti IS



Väčšina súčasných firiem používa celý komplex rôznych operačných systémov a aplikácií vrátane integrácie služieb internetu. Pritom sa však v štandardných komerčných a voľne šíriteľných softvérových produktoch **každý týždeň objaví niekoľko nových bezpečnostných chýb**. Zneužitie týchto chýb predstavuje vážne narušenie bezpečnosti, jeho dôsledkom je únik, strata či zmena údajov, strata dostupnosti služieb alebo kontroly nad nimi.

Štatistiky ukazujú prekvapujúci paradox: viac ako 50% bezpečnostných incidentov spôsobujú interní užívatelia systému. Riešenie tejto situácie má dve roviny. Prvou je neustále hodnotenie pracovníkov, druhou je periodické hodnotenie dostatočnosti, konzistentnosti a vhodnosti použitých bezpečnostných opatrení v informačnom systéme.

**Spoločnosť GORDIAS vám ponúka mechanizmus, ktorý prakticky overí dostatočnosť a účinnosť ochranných prvkov vášho informačného systému - Interné penetračné testovanie.**

Interné penetračné testovanie sa realizuje prostredníctvom zariadení pripojených do vybraných bodov počítačovej siete vo vašej organizácii a pozostáva z niekoľkých etáp:

### 1. Zber informácií

Úvodnou fázou je zber informácií o systéme a používaných aplikáciách, ktoré môžu byť zneužitú pri útokoch.

Najdôležitejšie sú údaje o:

- používaných komunikačných protokoloch,
- rozdelení adresného priestoru,
- DNS záznamoch a smerovaní elektronickej pošty,
- routovaní v sieti,
- používaných aplikáciách.

Súčasťou tejto fázy je vytvorenie základného obrazu o infraštruktúre, ktorý identifikuje používané počítače, adresy aktívnych prvkov a poskytované služby.

V testovaní sú simulované anonymné útoky, ale aj útoky oprávnených užívateľov. Ich cieľom býva zvýšenie svojich privilégií alebo získanie prístupu k údajom, ktoré nie sú pre nich určené. V tejto fáze sú identifikované scenáre pre jednotlivé skupiny užívateľov.

### 2. Analýza informácií a plánovanie

Na základe zhromaždených údajov sú identifikované ciele útokov. Sú to najmä dôležité zariadenia, počítače s dôvernými materiálmi a zdieľané zdroje v sieti. Opäť sú hodnotené alternatívy útokov na jednotlivé ciele z hľadiska nárokov na čas a úsilie.

### 3. Detekcia slabín

V tejto fáze testovanie odhaľuje slabiny („diery“) v operačných systémoch, aplikáciách, infraštruktúre (aktívne prvky siete a ich prepojenia) a zdieľaných zdrojoch v sieti. Používajú sa pritom aplikácie na automatizované vyhľadávanie slabín – tzv. security scannery, ale aj jednocelové aplikácie pre konkrétne systémy. Zároveň prebieha ručné vyhľadávanie slabín.

### 4. Penetrácia

Identifikované slabiny sú potenciálnou hrozbou narušenia bezpečnosti systému (detekcia môže byť aj falošná). Skutočnú zneužitelnosť overuje penetrácia. Pre každú slabinu je zvolený scenár zneužitia (exploit) prispôbený konkrétnym podmienkam. Vyberajú sa také exploity, ktoré nenarušia prevádzku a bezpečnosť systému (napr. odstavením bezpečnostných kontrol).

Potom nasleduje samotný útok. Základné typy útokov sú:

- odpočúvanie komunikácie (sniffing) prenášaných údajov a hesiel,
- falšovanie identity (spoofing) – vydávanie sa za oprávneného užívateľa a zariadenie,
- útoky hrubou silou (brutal force attacks) – obchádzanie autentifikačných mechanizmov, hádanie hesiel a tajných kľúčov,
- prerušenie prevádzky (Denial of Service attack) – tieto útoky sú testované len krátkodobo s cieľom zistiť ich realizovateľnosť.

**Experti spoločnosti GORDIAS uskutočňujú testy útokov vždy tak, aby nebola ohrozená funkčnosť a prevádzka systému. Cieľom testu nie je poškodiť, ale pomôcť!**

### 5. Eskalácia

Po každom útoku sú vyhodnotené získané údaje a privilégiá, posudzuje sa možnosť ich zneužitia (napr. použitie kompromitovaného počítača ako nástroja útoku). Rovnako sa vyhodnotia možnosti kombinovaných útokov, napr. viacerých útokov proti jednému cieľu alebo DOS útoku proti centrálnym zdrojom so súčasným použitím ich identity pri inom útoku.

### 6. Analýza a dokumentácia výsledkov

V tejto fáze sú sumarizované všetky získané informácie o systéme, jeho slabinách, zneužitelných „diarach“, vedených útokoch a ich následkoch. Slabiny sú ohodnotené podľa stupňa závažnosti, ktorý predstavujú. Zároveň sú formulované odporúčania o možnostiach ich odstránenia. Všetky informácie sú zhrnuté do záverečnej správy o penetračnom testovaní.

**Spoločnosť GORDIAS vám ponúka celý systém služieb, ktoré zvýšia bezpečnosť vášho informačného systému. Penetračný test najlepšie ukáže, nakoľko sú tieto služby pre vašu firmu potrebné.**

