

Penetračné testovanie

Tímový projekt – posudok na konkurenčný tím

Tím č. 3:

Bc. Rami Al Beyrouti
Bc. Martin Blesák
Bc. Peter Daniš
Bc. Martin Močol
Bc. Peter Štuller

0. Úvod

Predkladaný dokument obsahuje posudok vypracovaný na náš konkurenčný tím (tím č. 8). Posudok vychádza z dokumentácie, ktorú odovzdal konkurenčný tím, a ktorá by mala obsahovať analýzu, špecifikáciu a hrubý návrh riešenia.

Štruktúra tohto dokumentu kopíruje posudzovaný dokument. Ku každej jeho časti je napísané stručné vyjadrenie, zhodnotenie dobrých a zlých aspektov.

1. Analýza

Analýza problému obsahuje stručný úvod do penetračného testovania a ďalej ponúka:

- Všeobecný prehľad základov počítačovej bezpečnosti. Uvádzajú sa dôvody pre bezpečnostné opatrenia na príklade dopadov, ktoré môže mať prienik do systému.
- Kategorizácia útokov.
- Analyzujú sa možné typy a princípy obrany používané v počítačovej bezpečnosti.
- Bezpečnosť sa konkretizuje na najviac používané oblasti ako sú počítačové siete a hlavne Internet. Uvádzajú sa aspekty bezpečnosti najpoužívanejších protokolov a komunikačných služieb v Internete. Takisto sa stručne uvádzajú stratégie bezpečnostných opatrení.
- Ako základ sieťovej bezpečnosti sa uvádzajú firewally a proxy servery. Penetračné testovanie sa tu uvádza ako spôsob testovania firewallu.
- Ako zástupcovia penetračných testov sa v analýze uvádzajú systémy Nessus a Saint.

Analýza stručne a výstižne popisuje základné princípy počítačovej bezpečnosti, ale málo priestoru sa následne necháva samotnému penetračnému testovaniu. Obsahuje len definíciu penetračného testovania a stručný popis 2 nástrojov. Mala by sa rozšíriť hlavne o popis metód penetračných testov a následne poukázať ako sa uplatňujú v existujúcich riešeniach.

Takisto sa neuvádza analýza možností jednotlivých nástrojov penetračných testov zahrnúť svoje testy do spoločného integračného prostredia.

2. Návrh

Autori uvádzajú v špecifikácii požiadaviek na systém tieto:

- rozšíriteľnosť
- možnosť výberu časti testov
- automatické riadenie behu testov
- príjemné užívateľské prostredie a prezentácia výsledkov užívateľovi

Samotný návrh sa sústreďuje na nasledovné komponenty:

- testovacie skripty
- testovacie jadro
- medzirozhranie medzi jadrom a skriptami – podporná knižnica

- báza znalostí
- používateľské rozhranie

Celý návrh sa zameriava na vytvorenie penetračného testovacieho nástroja a písanie vlastných testovacích skriptov. Zadanie ale požaduje vytvorenie integračného prostredia, ktoré bude umožňovať spúšťať hotové testovacie skripty iných nástrojov penetračného testovania.

3. Zhodnotenie

Pripomienky k jednotlivým častiam sa nachádzajú na záver každej z nich. Dokumentácia je spracovaná prehľadne a je dobre štrukturovaná. Zopár gramatických chýb sa dá prehliadnuť s ohľadom na to, že sa jedná len o prvý výstup z projektu.

Na záver však musím uviesť hlavnú námietku voči práci. Žiadna časť dokumentácie sa nezaobráva www prezentáciou penetračného testovania, ktorá má byť jedným z výstupov projektu (v prípade nášho tímu má byť hotová už v zimnom semestri). Celý návrh sa venuje len testovaciemu nástroju.