

Penetračné testovanie a jeho úloha pri budovaní bezpečnej infraštruktúry

Pavel Jurečka
Vladimír Staňák

Beset, spol. s r. o.

Beset

*e***FOCUS**

Kto sme...

Beset, spol. s r. o.

- 1992: vstup na slovenský trh ako ICL Slovakia
- 2002 – 2004: pôsobenie pod názvom Fujitsu Services
- 2003: príliv domácich investícií
- 2004: rebranding na Beset

Kto sme...certifikáty

- ✓ **1994:** prvá IT spoločnosť držiteľom Certifikátu systému riadenia kvality
- ✓ **2004:** Potvrdenie o priemyselnej bezpečnosti na stupeň “Tajné”
- ✓ **2004:** Potvrdenie o priemyselnej bezpečnosti na stupeň “Tajné” pre EU
- ✓ **2005:** Certifikát systému environmentálneho managementu
- ✓ **2005:** Certifikát informačnej bezpečnosti podľa normy BS7799



Penetračné testovanie a ISMS

Základnou rodinou noriem pre riadenie životného cyklu informačnej bezpečnosti sú nasledujúce normy:

- ☐ ISO/IEC 27000
- ☐ ISO/IEC 27001
- ☐ ISO/IEC 27002
- ☐ ISO/IEC 27005



Penetračné testovanie

Penetračné testovanie

- ✓ jedna zo základných techník analýzy sieťovej bezpečnosti
- ✓ simulácia reálneho útoku na vyhodnocovaný systém alebo jeho časti
- ✓ zisťovanie zraniteľnosti infraštruktúry
- ✓ audit alebo kontrola spustených služieb

Čo všetko sa dá testovať?

- ✓ všetko, čo má pre firmu hodnotu
- ✓ informačná bezpečnosť, bezpečnosť procesov, komunikačná bezpečnosť, aplikačná bezpečnosť, fyzická bezpečnosť

Význam penetračných testov

- ✓ overenie úrovne bezpečnosti služieb, aktuálnosť služieb
- ✓ zistenie zraniteľností, preverenie logovacích techník
- ✓ pripravenosť administrátorov prípadne softvérov reagovať pri možných útokoch

Metodiky penetračných testov

Metodiky sú súbory pravidiel a zásad pre vykonávanie bezpečnostných auditov, penetračných testov, hodnotenia zraniteľnosti a ďalších metód hodnotenia bezpečnosti.

Použitie metodík zabezpečuje:

- ✓ úplnosť testovaných oblastí
- ✓ aktuálnosť
- ✓ vyhodnotiteľnosť
- ✓ opakovateľnosť



Metodiky penetračných testov

- ✓ OSSTMM (Open Source Security Testing Methodology Manual)
www.isecom.org
- ✓ OWASP (Open Web Application Security Project)
www.owasp.org



Typy penetračných testov

Testovanie bez znalosti infraštruktúry

- ✓ jednotlivé informácie sa zisťujú testovacími technikami
- ✓ tento typ testu zodpovedá reálnemu útoku



Testovanie so znalosťou infraštruktúry

- ✓ testovaného prostredia alebo systému
- ✓ testerom sú k dispozícii informácie o testovanej infraštruktúre; topológia siete, IP adresácia, operačné systémy, bežiacie služby

Penetračné testy

Základné rozdelenie testov:

Externé testy

- ✓ môžu byť bez znalosti infraštruktúry a so znalosťou infraštruktúry
- ✓ testuje sa štruktúra siete, doménové mená, IP adresy, otvorené porty, identifikácia operačných systémov, identifikácia bežiacich služieb, nájdenie zraniteľností prípadné ich použitie, routre, FW, DNS, Mail GW, bezdrôtové systémy, webové systémy, aplikačné systémy

Interné testy

- ✓ môžu byť rovnako bez znalosti infraštruktúry a so znalosťou infraštruktúry
- ✓ testujú sa serverové systémy, pracovné stanice, routre, switche, bezdrôtové systémy, webové systémy, aplikačné systémy

Fázy penetračného testovania

Prípravná fáza:

- ✓ plánovanie a príprava
- ✓ určenie kontaktných osôb, rozsahu testu, dohodnutie časových úsekov a postupu pri testovaní

Testovacia fáza:

- ✓ spustenie samotných testov, testy manuálne / automatické
- ✓ získavanie informácií, mapovanie siete, identifikácia zraniteľných miest, prienik, získavanie prístupu a zvyšovanie právomocí
- ✓ zbieranie ďalších údajov, kompromitovanie vzdialených používateľov, udržiavanie prístupu, zahladenie stôp

Záverečná fáza:

- ✓ hodnotiaca správa: zdokumentovanie priebehu testu
- ✓ odporúčania pre riešenie zistených zraniteľností
- ✓ údaje o použitých nástrojoch, čase konania jednotlivých testov, výstupy získané pri testovaní, zoznam všetkých zistených zraniteľností, návrh ich zabezpečenia

SW na penetračné testovanie

Programy, prípadne SW distribúcie na penetračné testovanie:

- ✓ Kali Linux predtým Backtrack
- ✓ Fedora Security Spin
- ✓ Nessus
- ✓ Metasploit Network
- ✓ Nmap
- ✓ OpenVAS
- ✓ W3AF
- ✓ Core Impact
- ✓ Microsoft Baseline Security Analyzer



Ďakujeme za pozornosť

Beset

*e***FOCUS**