Príloha č.1

Predmet zmluvy:

Simulácia internetového útočníka bude pozostávať z dvoch etáp: vulnerability assessment a samotného penetračného testovania.

Vulnerability assessment

Úlohou tejto časti bude poskytnúť čo najviac informácií pre nasledujúcu fázu testovania. Zákazníkom dodaný rozsah IP adries a služieb bude oskenovaný poprednými komerčným a voľne dostupnými nástrojmi, ktoré budu systematicky a komplexne skúmať poskytované služby s cieľom identifikovať všetky potenciálne zneužiteľné miesta.

Okrem iného budú podľa relevantnosti jednotlivé služby skúmané na:

Parameter Injection
Command Execution
SQL Injection
Cross-Site Scripting
Directory Traversal
Abnormal Input
Parameter Overflow
Buffer Overflow
Parameter Addition
Path Manipulation
Path Truncation
Character Encoding
MS-DOS 8.3 Short Filename
Character Stripping
Site Search
Application Mapping
Crawl
Automatic Form-Filling
SSL Support
Proxy Support
Client Certificate Support
State Management
Directory Enumeration
Web Server Assessment
HTTP Compliance
WebDAV Compliance
SSL Strength
Certificate Analysis
Content Investigation
Spam Gateway Detection
Client-Side Pricing
Sensitive Developer Comments
WebServer/Web Package Identification

Absolute Path Detection
Error Message Identification
Permissions Assessment
Brute Force Authentication attacks
Known Attacks

Výstupom tejto časti bude správa obsahujúca všetky zistené informácie. Táto správa bude odovzdaná zákazníkovi a zároveň bude slúžiť ako vstup pri samotných pokusoch o prienik a zneužitie služieb na systémoch zákazníka.

Penetračné testovanie

V tejto časti testov budú vykonané pokusy o zneužitie všetkých identifikovaných bezpečnostných slabín, na základe informácií, ktoré boli získané v predchádzajúcej časti. Súčasť tejto fázy je taktiež eliminácia prípadných identifikovaných false positives.

Priebeh tejto časti testovania môže zasiahnuť do normálneho fungovania zákazníckych serverov, preto bude presný postup pred jeho začatím dohodnutý so zákazníkom. Zákazník bude zároveň informovaný o výstupoch z vykonaných testov, aby prípadné závažné slabiny bolo možné čo najrýchlejšie odstrániť

Výstupy projektu

O priebehu celého testovania budú vytvorené dve záverečné správy. Jedná zo správ bude podrobná technická správa, ktorá bude obsahovať všetky auditné zistenia. Správa bude okrem iného obsahovať zoznamy služieb, zoznam zistených slabín týchto služieb a prípadne aj úspešné pokusy o ich zneužitie. V správe bude tak isto zoznam jednotlivých vykonaných testov a to aj vrátane testov ktoré dopadnú negatívne. Súčasťou správy budú odporúčania pre zákazníka, ako zvýšiť zabezpečenie testovaného prostredia. Jednotlivé zistenia budú v správe vo forme položiek zoznamu, pričom ku každému zisteniu bude uvedené:

- popis zistenia
- riziko vyplývajúce zo zistenia
- úroveň rizika (v trojstupňovom ohodnotení nízka, stredná, vysoká)
- odporúčanie na odstránenie rizika

Správa bude odovzdaná po odprezentovaní jej obsahu zákazníkovi na pripomienkovanie, ten po jej prečítaní bude mať priestor vyjadriť sa k jednotlivým auditným zisteniam. Ak sa pripomienky ukážu ako opodstatnené, budú akceptované a do správy zapracované. Následne bude odovzdaná výsledná technická auditná správa.
Druhou odovzdanou správou bude výsledná správa pre manažérov. Táto správa bude kratšia a bude napísaná v slovenskom a v anglickom jazyku. V správe budú prehľadné zhrnuté najzávažnejšie auditné zistenia pre jednotlivé aktíva (vo forme písaného textu, grafov a zoznamov). Manažérska správa bude vytvorená a odovzdaná spolu so záverečnou technickou správou.

Príloha č. 2

Poradie	Popis činností	Človekodni
1	Úvodné projektové stretnutie (kick-off meeting) , prezentácia, dohodnutie detailov testovania (*), projektový manažment , príprava na testovanie	1
2	1. etapa testov (vulnerability assessment), zisťovanie informácii potrebných pre samotný prienik	2
3	2. etapa testov – pokusy o prienik do systému z Internetu, pokusy o narušenie integrity systémov, pokusy o zníženie dostupnosti alebo úplne odstavenie služieb systémov, eliminácia false positives	3
5	Vypracovanie záverečných správ (detailná technická správa, manažérske správy)	2
6	Záverečné prezentovanie výsledkov, akceptácia, pripomienkovanie, prípadne zapracovanie zmien do dokumentov	1
7	Rezerva	0
	Spolu	9

Jednotková cena za manday je 20.000,- Sk bez DPH,
23.800,- Sk s DPH,
z toho 3.800,- Sk je DPH

Cena za dielo je 180.000,- Sk bez DPH,
214.200,- Sk s DPH,
z toho 34.200,- Sk je DPH