Příloha č. 2 ZD Specifikace předmětu veřejné zakázky

Obecné požadavky na penetrační testy

Cílem penetračního testování je prověřit zabezpečení aplikací a infrastrukturních prvků a identifikovat slabá místa interní infrastruktury, která by mohla být potenciálně zneužita útočníky k poškození zadavatele. Penetrační testy se zaměřují na odhalení zranitelností, které mohou být použity k prolomení bezpečnostních opatření a narušení dostupnosti, integrity nebo důvěrnosti systému či aplikace.
Výsledky testů musí být kvantifikovatelné, opakovatelné a založené na faktech zjištěných během testování. Reportované zranitelnosti musí obsahovat informace o potenciálním riziku, konkrétním postupu nápravy a pravděpodobnosti zneužití v praxi.
Testy musí být prováděny nedestruktivně a k ověření zranitelností by měly být preferovány méně invazivní techniky, aby se minimalizovalo riziko narušení chodu aplikací nebo systémů. Přístup do prostředí objednatele buď fyzicky nebo zabezpečeným vzdáleným přístupem na testovací zařízení. Otestována by měla být veškerá zařízení dostupná po síti v době testu. Poskytovatel musí mít potřebné licence pro použitý software a v případě zjištění omezené dostupnosti systémů musí ihned informovat kontaktní osobu na straně zadavatele. Povinností poskytovatele služby je zajistit nápravná opatření a zadavateli poskytnout veškerá data z penetračního testování, postupu prací, log činností, které pomohou co nejrychleji navrátit infrastrukturu do funkčního stavu. Dle závažnosti problému může dojít k pozastavení testování.

Data z interního testování nesmí opustit organizaci, to znamená, použije-li dodavatel vlastní zařízení pro penetrační test, použité úložiště (pevný disk) zůstává objednateli.
Poskytovatel musí při provádění penetračních testů dodržovat zavedené metodiky a standardy bezpečnostního testování. V případě objevení kritických zranitelností musí neprodleně informovat zadavatele a navrhnout opatření ke zmírnění rizika zneužití těchto zranitelností. Součástí je hledání informací z veřejných zdrojů tzv. OSINT.
Testy budou předem konzultovány se zadavatelem, který poskytne potřebnou součinnost. Testování se bude provádět pouze ve stanovených dnech a časech, a z IP adres schválených zadavatelem.
Poskytovatel je povinen zajistit bezpečnost dat a výstupů vzniklých během testování. Fyzické kopie výsledků musí být chráněny a přístupné pouze autorizovaným osobám. Při předávání výsledků musí být použity kryptografické metody šifrování.
Po skončení testu bude celé prostředí uvedeno do původní stavu, veškeré uložené skripty či modifikace infrastruktury budou navráceny do stavu před započetím penetračního testu.
Úroveň autentizace při testech závisí na konkrétním scénáři a požadavcích testování. Mohou být použity různé úrovně autentizace, aby testy věrně odrážely skutečné možnosti kompromitace systému.

Fáze testování

1. **Fáze 1**
   - Testování interní infrastruktury
   - Testování externí infrastruktury
   - Závěrečná zpráva z testování
   - Prezentace a vysvětlení výsledků

2. **Fáze 2 - re-test infrastruktury**
   - Testování interní infrastruktury
   - Testování externí infrastruktury
   - Závěrečná zpráva z testování opatřené informací o validaci oprav z prvního testování

- Prezentace a vysvětlení výsledků

Závěrečná zpráva z testování musí obsahovat:

- Název testovaného systému nebo aplikace,
- Manažerské shrnutí s přehledovou tabulkou nálezů (popis, dopad, závažnost, doporučení, odkaz na detailní popis),
- Technické podrobné shrnutí výsledku testování,
- Použitou metodiku testování a klasifikaci zranitelností (Black box, Gray box, White box),
- Úroveň autentizace při testech,
- Seznam nalezených zranitelností podle metodiky CVSS verze 3.0 nebo PTES pro Red Team testy,
- Popis nálezů, potenciálních vektorů útoku, rizik a dopadů,
- Návrh řešení k odstranění nebo zmírnění nálezu,
- Časovou osu vedeného útoku pro pozdější analýzu
- Vzorový příklad úspěšného útoku pro střední a vysoké riziko podle CVSS nebo PTES.

Výstup z re-testování:

- Zpráva z re-testu bude navíc oproti testování obsahovat validaci oprav nalezených kritických a závažných zranitelností.

Prezentace a vysvětlení výsledků

- Z manažerského pohledu, který bude vysvětlovat dopady na infrastrukturu či chod společnosti
- Z technického pohledu, který bude detailně popisovat jednotlivé problémy, zjištěné na infrastruktuře vedoucí k následujícím nápravným opatřením

<u>Testování interní infrastruktury</u>

Scénář testování:

Testování proběhne s cílem identifikovat slabiny v interní ochraně informačního prostředí. Testovací tým, hrající roli běžného uživatele, bude simulovat útoky s úkolem proniknout do systému a získat přístup k citlivým informacím či kritickým systémům. Testování se zaměří na zjištění slabin v konfiguraci systémů a nastavení domény, a ověření jejich zneužitelnosti.

V rámci testování zařízení je zahrnuto

- Odolnost vůči základním síťovým útokům (VLAN hopping, DHCP starvation, ARP/MAC spoofing, STP manipulation).
- Útoky na doménový řadič (Kerberoasting, Golden/Silver ticket, Pass-the-hash apod.).
- Ověření zranitelností všech zařízení a možnosti jejich zneužití běžným interním uživatelem.
- Testování je omezeno alokovaným časem a zahrnuje i re-test případných kritických a vysoce závažných zranitelností.

Nástroje a technologie:

- Nástroje pro skenování zranitelností, manuálně ověřené dalšími technikami.
- Nástroje pro testování konfigurace sítě
- Nástroje pro testování domény a autentizace

Metodiky testování:

Testovací tým bude používat osvědčené metodiky nebo vlastní metodiku v souladu s:

- Penetration Testing Execution Standard (PTES)
- Open Source Security Testing Methodology Manual (OSSTMM)

- Information Systems Security Assessment Framework (ISSAF)

Testování externí infrastruktury

V rámci testování externí infrastruktury je zahrnuto:
Testování vnějšího perimetru bude zahrnovat simulaci útoku neautentizovaného externího útočníka, který se pokouší získat neoprávněný přístup do sítě nebo systémů organizace. Testování bude probíhat metodou Black box (Zero-knowledge), kdy útočník nemá žádné předem získané informace.
Cílem bude identifikovat potenciální zranitelnosti v obraně perimetru, zahrnující firewally, systémy IPS, webové firewally, řešení pro vzdálený přístup (např. VPN nebo RDP), interní služby, servery a používané protokoly (SMTP, FTP, databáze atd.). Testovací tým se zaměří na možnosti zneužití známých zranitelností a chyb v nastavení služeb přístupných z internetu. Výsledkem bude mapování celého perimetru, identifikace potenciálně zranitelných cílů a pokus o zneužití zranitelností pro získání výhodnější pozice k dalšímu postupu.
Součástí testování bude také re-test kritických a vysoce závažných zranitelností.

Nástroje a technologie testování
Testování bude zahrnovat použití nástrojů typu skenerů zranitelností, jejichž nálezy budou manuálně ověřeny pomocí dodatečných technik. Dále budou využity nástroje jako nmap pro mapování perimetru a exploitační frameworky typu Metasploit pro zneužití nalezených zranitelností.

Metodiky testování
Testovací tým bude používat osvědčené metodiky nebo jejich kombinace, případně vlastní metodiku, která je v souladu s těmito standardy. Mezi hlavní používané metodiky patří:

- Penetration Testing Execution Standard (PTES)
- Open Source Security Testing Methodology Manual (OSSTMM)
- Information Systems Security Assessment Framework (ISSAF)

Výstup testování
Výstupem bude podrobná písemná zpráva obsahující zjištění, doporučení a kroky k nápravě, doplněná o manažerské shrnutí. Zpráva musí obsahovat seznam zjištěných zranitelností, jejich dopad a hodnocení potenciálního rizika. Testovací tým poskytne informace o použitých nástrojích a technikách spolu s případnými vytvořenými skripty nebo kódem. Zpráva také bude obsahovat hodnocení zranitelností pomocí skóre a vektoru CVSS nebo CWE. Pokud je zranitelnosti přidělen CVE identifikátor, musí být uveden ve zprávě. Zpráva stanoví priority a doporučení k nápravě na základě závažnosti zranitelností a potenciálního dopadu na organizaci.

Rozsah a parametry testování

Parametry testování interní infrastruktury:

- Typ testu: Gray-box
- Prostředí testu: Produkční
- Forma testu: Assumed breach z pozice běžného uživatele
- Počet zařízení: 160
    - 30 serverů
    - 30 aktivních prvků (switche, AP)
    - 100 uživatelských stanic v podobné konfiguraci, hloubkový test 5 stanic
- Operační systémy: Linux, Microsoft Windows Server, Microsoft Windows 10
- Průměrný počet otevřených portů / běžících služeb na serveru: 6
- Segmentace prostředí: cca 10 VLAN

Parametry testování interní infrastruktury:

- Typ testu: Gray-box
- Prostředí testu: Produkční
- Forma testu: z pozice administrátora infrastruktury
- Počet zařízení: 63
    - 3 administrátorských stanic
    - 30 aktivních prvků
    - 30 serverů
- Operační systémy: Linux, Microsoft Windows Server, Microsoft Windows 10,11
- Průměrný počet otevřených portů / běžících služeb na serveru: 6
- Segmentace prostředí: cca 10 VLAN

Externí služby

Počet externích IP adres: 10