Druhy testů zranitelností, perimetru a základní penetrační test

Metody OSINT

Metoda sběru informací z veřejně dostupných zdrojů.

Testy perimetru

- SCAN IP
- SCAN TCP portů
- SCAN UDP portů
- SCAN služeb
- Detekce OS

Výsledkem testu perimetru je odhalení zranitelností otevřených portů, operačních systémů a služeb na nich běžících.

Test SSL/TLS zabezpečení

Výsledkem testu je ověření zabezpečení SSL certifikátem. Ověření služeb TLS 1.0 - SSL 3.0

Testy dle standardu OWASP:

- **AppDOS** – Application Flooding - zpracování velkého objemu požadavků, transakcí a/nebo síťového provozu
- **Access Control** - Jedná se o problémy, které mohou umožnit uživatelům přístup k prostředkům nebo funkcím, ke kterým nemají oprávnění.
- **Authentication** - Používá se pro problémy související s určením identity jednotlivců nebo entit a ověřováním této identity.
- **Authentication User** - Slouží pro problémy související s identifikací a ověřováním lidí, kteří mají používat aplikaci. Příklady zahrnují problémy s uživatelskými jmény, hesly, tokeny, čipovými kartami, biometrikou a dalšími přihlašovacími údaji
- **Authenication Session Management** - Tato kategorie se věnuje problémům s vydáváním, používáním, ochranou, změnou a ukončováním identifikátorů relací všech druhů. Identifikátory relací nahrazují přihlašovací údaje, ale často nejsou tak pečlivě chráněny.
- **Configuration Management** - Tato kategorie se používá k popisu problémů s konfigurací aplikace nebo prostředí aplikace.
- **Configuration Management infrastructure** - Tato kategorie se zabývá problémy souvisejícími s konfigurací infrastruktury, tj. hardware, sítě a dalších základních prvků, které podporují provoz aplikace.
- **Configuration Management Application** - Slouží k popisu problémů s konfigurací aplikace, jako jsou špatně nakonfigurované bezpečnostní mechanismy, výchozí programy, nepoužitý kód a nepotřebné povolené funkce.

- **Error Handling** - Tato kategorie se používá pro problémy související s zpracováním chyb, včetně tisku sledu volání na obrazovku, zabezpečovacích mechanismů se selháváním do otevřeného stavu (tzv. fail open), umožňování chybám ovlivnit chod celé aplikace a odhalování příliš mnoho informací o selhání.
- **Data Protection** - Slouží k problémům souvisejícím s nevhodným odhalováním dat.
- **Data Protection Transport** - Používá se pro problémy související s bezpečným přenosem informací. Často se jedná o problémy s konfigurací SSL nebo TLS, ale může zahrnovat i jiné protokoly s bezpečnostními funkcemi.
- **Input Validation** - Tato kategorie se používá pro problémy související s nedostatečným ověřením neověřených vstupů před jejich použitím aplikací.
- **Input Validation SQL** - Chyby, které mohou umožnit útočníkovi vkládat speciální znaky a příkazy do databáze SQL a upravit zamýšlený dotaz. Útok se může pokusit změnit význam dotazu nebo připojit další příkazy.
- **Input Validation OS** - Chyby, které mohou umožnit útočníkovi vkládat speciální znaky a příkazy do příkazového shellu operačního systému a upravit zamýšlený příkaz. Útok se může pokusit změnit způsob spouštění programu nebo připojit další příkazy.
- **Input Validation LDAP** - Chyby, které mohou umožnit útočníkovi vkládat speciální znaky a vyhledávací termíny do serveru LDAP a upravit zamýšlený dotaz.
- **Input validation XSS** - Cross-Site Scripting injection, česky nazýváno Vkládání křížových skriptů, je typ bezpečnostního zranitelnosti webových aplikací. Při této útočné metodě dochází k vkládání kódů (skriptů) do webových stránek nebo aplikací, které jsou následně spouštěny uživateli, kteří tyto stránky navštíví.
- **Buffer Overflow** - Jedná se o chyby, které mohou umožnit útočníkovi využít formátovací řetězce k přepsání míst v paměti, což umožňuje změnit data, ovládat chování programu nebo způsobit pád programu.

Penetrační test

Dle zjištěných informací (zranitelností) ze SCANŮ je proveden pokus napadení daných služeb a aplikací.

- Ftp
- SSH
- Apache
- SQL
- …

Pokus o neautorizované přihlášení, eskalací privilegií, napojení na databázi,...