|  |  |
| --- | --- |
| **Odkaz EL** | Zákazník Penetračný test |
| **Dátum EL** | 27.2.2023 |
| **Zákazník (skrátený názov)** | Zákazník |
| **Zákazník** | Zákazník, s.r.o. |
|  |  |
| **Kópia** |  |
| **EL titul** | Externá infraštruktúra a aplikačné penetračné testovanie |

# Príloha č.2 – Autorizačný list

# Typ testovacej činnosti

Podpisom tohto splnomocnenia Zákazník, s.r.o. (ďalej len zákazník) oprávňuje POSKYTOVATEĽ, s.r.o. (ďalej len POSKYTOVATEĽ) vykonať (výber z) nasledujúcich testov:

|  |  |
| --- | --- |
| **Testovacie activity** | |
| **Pravidelné testy** | **Špeciálne testy** |
| Externý (internetový) penetračný test;  Interný test prieniku do siete;  Skenovanie zraniteľnosti;  Test webovej aplikácie;  Hackovanie hardvéru (napr. ukradnuté zariadenie);  War-drive test (hackovanie Wi-Fi). | Test sociálneho inžinierstva (SE);  Kontrola fyzickej bezpečnosti;  Red-teaming;  Priemyselné riadiace systémy;  Purple-teaming. |

# Kontaktné údaje všetkých zúčastnených strán

Táto sekcia obsahuje všetky relevantné kontaktné informácie súvisiace s aktivitami.

## Testovací tím - POSKYTOVATEĽ

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Meno** | **Funkcia** | **Telefónne číslo** | **Email** |
|  |  |  |  |  |
|  |  |  |  |  |

## Zákazník - priamo zainteresovaní zamestnanci

Počas realizácie zadania by mala byť k dispozícii kontaktná osoba, ktorá je schopná poskytnúť konkrétne informácie o infraštruktúre a na ktorú je možné sa obrátiť v prípade problémov a po začatí a ukončení prevádzkových činností.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **#** | **Meno** | **Funkcia** | **Telefónne číslo** | | **Email** |
|  |  |  |  |  | |
|  |  |  |  |  | |

# Rozsah a prevádzkové obmedzenia

Táto časť obsahuje všetky relevantné informácie týkajúce sa rozsahu a prevádzkových obmedzení súvisiacich s činnosťami.

## Objekty zahrnuté v rozsahu

Nasledujúce objekty sú v rozsahu testovania:

* servery;
* sieťové zariadenia (ako sú bezdrôtové prístupové body, smerovače, prepínače a brány firewall).

Zoznam cieľových IP adries, názvov hostiteľov a/alebo umiestnení pre tieto objekty je nasledujúci:

|  |  |  |  |
| --- | --- | --- | --- |
| **Rozsahy IP** | **Mená** | **Popis** | **Fyzické umiestnenie cieľových systémov** |
| IP1  IP2  IP3  IP4 |  |  | Zákazník |

Zástupcovia zákazníka a tretej strany vyhlasujú, že sú zákonným vlastníkom alebo držiteľom vyššie špecifikovaných cieľov, a preto majú oprávnenie povoliť POSKYTOVATEĽom vykonať vyššie špecifikovaný test na týchto objektoch. Zákazník je výlučne zodpovedný za informovanie tretích strán a získanie písomného súhlasu (oprávnenia) na vykonanie testovania bezpečnosti v rozsahu, ako je zdokumentované v tomto autorizačnom liste. Zákazník prevezme plnú zodpovednosť za tretie strany v súvislosti s touto zákazkou testovania bezpečnosti a bude chrániť POSKYTOVATEĽA (pozri časť „Požiadavky slovenského práva“ pre širší text) aj v mene tretích strán.

## Načasovanie našich aktivít

Testovanie je povolené v období od XXX do XXX. Platné časové úseky na testovanie počas tohto obdobia sú:

počas pracovnej doby (09:00 – 17:00)

mimo pracovnej doby a víkendov

## Pravidlá zákazky

Počas bezpečnostného testu možno použiť procedúry a mechanizmy, ktoré môžu (dočasne) znížiť celkovú bezpečnosť vášho systému. Nižšie uvedené kontrolované techniky sú počas nášho bezpečnostného testu POVOLENÉ :

Zachytenie prihlasovacích údajov používateľa (napr. ID používateľa a hesiel) a iných údajov.

Vytváranie snímok obrazovky.

Sniffing cieľovej siete po dosiahnutí prístupu.

Inštalácia zadných dvierok na cieľové systémy.

Odosielanie trójskych koní prostredníctvom e-mailu (alebo podobných služieb).

Používanie (hardvérového alebo softvérového) hesla a/alebo zapisovačov klávesnice na cieľoch.

Vykonanie rekonfigurácie systému na cieľoch (ktoré sú niekedy potrebné na vykonanie špeciálnych typov útokov).

Útoky typu Denial-of-Service.

Iné:.………………………………..…………………………………………..…………..………………….

Zákazník (a akákoľvek tretia strana) tiež berie na vedomie, že pri vykonávaní bezpečnostného testovania môže POSKYTOVATEĽ získať prístup k informáciám Zákazníka ( a akejkoľvek tretej strany) alebo iným systémom Zákazníka ( a akejkoľvek tretej strany), ako je uvedené vo vyššie uvedenom zozname cieľových IP adries a/alebo alebo názvy hostiteľov ako výsledok úspešného prieniku. Zákazník ( a akákoľvek tretia strana) súhlasí s tým, že je to prijateľné.

Zákazník (a akákoľvek tretia strana) ďalej vyhlasuje, že odškodní a ochráni POSKYTOVATEĽA a akúkoľvek spoločnosť vlastnenú alebo pridruženú k POSKYTOVATEĽOVI a ich príslušným predstaviteľom, zamestnancom a pridruženým spoločnostiam voči akejkoľvek škode, požiadavkám, záväzkom a nárokom na ujmy na zdraví a/alebo majetková škoda, ktorá môže byť spôsobená alebo vyplynúť z vykonania bezpečnostnej skúšky.

Chceli by sme zdôrazniť skutočnosť, že penetračný test nemôže preukázať alebo dokázať, že systém je bezpečný. Penetračný test môže ukázať len slabé stránky a zraniteľné miesta v momente testovania.

Zabezpečený spôsob komunikácie

Tím bezpečnostných testerov môže narábať s niektorými citlivými údajmi, ako sú podrobnosti o zraniteľnostiach a záverečná správa, ktorú možno budeme musieť doručiť zákazníkovi (kontaktnému bodu). Tieto informácie budú oznámené dohodnutým spôsobom výmeny dokumentov pomocou šifrovaných príloh e-mailu.

|  |  |
| --- | --- |
| V mene Zákazník, s.r.o. | |
| Podpis: | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |  |
| Názov: |  |  | |
| Funkcia: |  |  | |
| Dátum: |  |  | |