EXTERNÉ PENETRAČNÉ TESTOVANIE INFRAŠTRUKTÚRY

Štandardná infraštruktúra pozostáva z množstva zariadení a väčšina z nich, ak nie všetky, zohrávajú kritickú úlohu vo Vašej informačnej bezpečnosti.

Mnoho medializovaných bezpečnostných incidentov ukázalo ako jednoduché ponechanie jedného z týchto zariadení s nezabezpečenou konfiguráciou, chýbajúcou aktualizáciou alebo slabým heslom môže viesť k úplnej kompromitácií systémov.

Pravidelné testovanie celej infraštruktúry je strategickým krokom nielen pri ochrane Vašich dát ale aj pre celkové zlepšenie stavu bezpečnosti vo Vašej spoločnosti.

PREHĽAD SLUŽBY

Cieľom externého penetračného testu je identifikovať bezpečnostné zraniteľnosti vo Vašej externej infraštruktúre a predísť tak útokom reálnych hackerov.

Test je vykonaný z externého prostredia a sústreďuje sa na všetky systémy a aplikácie dostupné z internetu, pričom sa overuje či je možné zneužiť zraniteľností za účelom úniku dát, získania vyšších privilégií, či spustenia cudzieho/škodlivého kódu.

Manuálne preverujeme každú identifikovanú zraniteľnosť a snažíme sa ju využiť na kompromitáciu cieľových systémov, prípadne na exfiltráciu citlivých údajov.

Po ukončení testovania získate prehľadný priorizovaný report zraniteľností spolu s odhadom technického rizika, ktoré predstavujú. Report neobsahuje žiadne "false-positive" nálezy, ale len overené zraniteľnosti a odporúčania ako ich odstrániť. Na požiadanie sú výsledky odprezentované na spoločnom stretnutí.

Test môže byt vykonaný pomocou metódy BLACK BOX (žiadne informácie o testovanej infraštruktúre), GREY BOX (čiastočné informácie o testovanej infraštruktúre) alebo WHITE BOX (všetky potrebné informácie o testovanej infraštruktúre).

Cena penetračného testu záleží od hĺbky testov, veľkosti a komplexnosti testovanej infraštruktúry. Táto cena je určená po vzájomnej konzultácii vzhľadom aj na ďalšie požiadavky zákazníka (testovanie mimo prevádzky/pracovnej doby, atď.).

DETAILNÝ PREHĽAD SLUŽBY

Pri externom teste je zvyčajným cieľom prienik do vnútornej infraštruktúry pričom sa zameriava najmä na zariadenia bezpečnostného perimetra (routre, firewally, IDS, WAF). Ďalším častým cieľom je exfiltrácia citlivých údajov ako sú napríklad emaily, dáta z databáz a interných a externých portálov, atď.

Stručný prehľad preberaných tém:

- Určenie rozsahu testovania

- Prieskum a enumerácia serverov a iných zariadení (v prípade ak nie je dopredu zadaný rozsah)
- Mapovanie a identifikácia služieb
- Analýza zraniteľností
- Exploitácia
- Eskalácia privilégií
- Reportovanie

Každý test je prispôsobený konkrétnemu testovanému prostrediu. Využívame kontrolný zoznam, ktorý zabezpečuje, že sa nevynechajú žiadne dôležité kroky. Metodológiu testovania je možné prispôsobiť bezpečnostným štandardom ako je napríklad OSSTM.