INTERNÉ PENETRAČNÉ TESTOVANIE INFRAŠTRUKTÚRY

Zatiaľ čo väčšina sietí je pomerne dobre chránená z verejných sietí, opak býva pravdou v prípade interných sietí. Útoky v interných sieťach majú potenciál mať oveľa väčší bezpečnostný dopad, nakoľko útočníkom môže byť Váš zamestnanec, ktorý pozná dané prostredie.

Okrem Vášho zamestnanca, útočníkom môže byť ktokoľvek (hacker, externý dodávateľ, ...), kto získal prístup do Vašej internej siete.

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 interného penetračného testu je identifikovať bezpečnostné zraniteľnosti vo Vašej internej infraštruktúre a predísť tak útokom reálnych hackerov.

Test je vykonaný z interného prostredia a sústreďuje sa na všetky systémy a aplikácie dostupné v internej sieti, 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).

Testovanie je možné vykonať na diaľku pomocou PWNboxu, ktorý posielame svojim zákazníkom. Toto zariadenie je možné jednoducho pripojiť do existujúcej infraštruktúry. PWNbox vytvorí šifrované spojenie k našim bezpečnostným expertom, ktoré im umožní pracovať na diaľku čím sa redukuje cena daného testu.

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 u zákazníka, testovanie mimo prevádzky/pracovnej doby, atď.).

DETAILNÝ PREHĽAD SLUŽBY A METODOLÓGIA

Komplexnosť informačných systémov a sietí spôsobuje, že útočník môže nájsť zraniteľnosti v rôznych komponentoch Vašej infraštruktúry.

Počínajúc od problémov v sieťovej infraštruktúre, cez softvér bez aplikovaných bezpečnostných záplat, nedostatky v konfiguráciách systémov, až k zraniteľnostiam, ktoré sa skrývajú v aplikáciách na mieru.

Test môže byť vykonaný z pohľadu útočníka s prístupom do internej siete bez prihlasovacích údajov alebo z pohľadu zamestnanca s obmedzenými prístupovým kontom do domény.

Interný penetračný test odhaľuje zraniteľnosti, ktoré je niekedy možné kombinovať na dosiahnutie určitého cieľa ako je napríklad získanie priameho / privilegovaného prístupu k dátam alebo inej sieti, ktorá slúži na administráciu prostredia, prípadne ovládnutie účtu doménového administrátora.

Pri testovaní používame metodológiu, ktorá sa skladá nasledujúcich fáz:

- 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
- Pivoting
- 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.