IstroSec

Data Sheet

Ofenzívna bezpečnosť

V rámci komplexného zabezpečenia adekvátnej úrovne bezpečnosti je potrebné reflektovať na nové hrozby, overovať komplexitu a systematickosť implementovaných bezpečnostných opatrení ako aj detegovať úroveň odolnosti organizácie voči hrozbám a útokom, ktoré sú relevantné pre organizáciu.

Poskytujeme nasledovné ofenzívne služby:

- Vulnerability scan
- Vulnerability assessment
- Penetračný test
- Red teaming
- Purple teaming

Posúdenie zraniteľností

V rámci ohodnotenia zraniteľností experti zo spoločnosti IstroSec vykonajú sken zraniteľností prostredníctvom automatizovaných nástrojov (komerčne dostupných a aj vlastne vyvinutých pre tento účel). Zraniteľnosti, ktoré nie je možné detegovať automatizovaným spôsobom (najmä zraniteľnosti business logiky, zraniteľnosti, ktoré je potrebné identifikovať na základe komplexného posúdenia okolitého prostredia a ďalšie) sú identifikované manuálne.

Po identifikácií zraniteľností dochádza k prevereniu, či sa nejedná o false-positive a zraniteľnosti sú posudzované v jednotlivosti aj vo vzťahu s ostatnými zraniteľnosťami.

Pri posúdení zraniteľností nedochádza k exploitácií zraniteľností.

IstroSec ponúka tieto typy posudzovania zraniteľností:

- Externé posúdenie zraniteľností
- Interné posúdenie zraniteľností
- Posúdenie zraniteľností cloudu
- Posúdenie zraniteľnosti aplikácie alebo aplikačného endpointu

Posúdenie zraniteľností by sa malo vykonávať podľa typu organizácie:

- Kontinuálne (pre organizácie s najvyššími požiadavkami na bezpečnosť)
- 1x mesačne (pre organizácie so zvýšenými požiadavkami na bezpečnosť)
- 1x za 6 mesiacov (pre organizácie so štandardnými požiadavkami na bezpečnosť)
- 1x ročne pre ostatné organizácie

Program pre posúdenie zraniteľností

Pre niektoré organizácie vzhľadom na ich požiadavky na bezpečnosť a bezpečnostný profil je vhodné vybudovať vlastný program na ohodnocovanie zraniteľností. Program sa skladá z nasledujúcich komponentov:

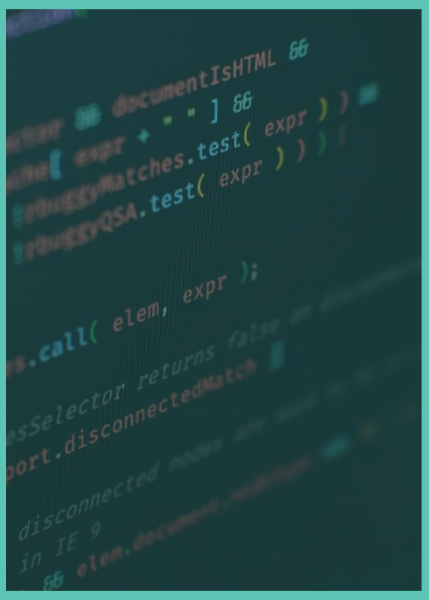
- Analýza infraštruktúry a návrh programu na ohodnotenie zraniteľností
- Implementácia technických prerekvizít na program ohodnotenia zraniteľností:
  - testovacie zariadenia (vulnerability scannery sieťové, aplikačné)
  - automatizácia vyhodnocovania
- Návrh a implementácia procesov ohodnocovania zraniteľností
- Vyškolenie špecialistov na vykonávanie ohodnocovania zraniteľností
- Návrh a Implementácia procesov na rozvoj programu

Prečo IstroSec?

- Kombinované skúsenosti expertov viac ako 70 rokov
- Prístup k odborníkom na všetky oblasti informačnej bezpečnosti, vrátane audítorov, penetračných testerov, forenzných analytikov, analytikov malvéru, školiteľov a ďalších
- Systematické zlepšenie informačnej bezpečnosti v zmysle štandardov a na základe skúseností s riešením pokročilých bezpečnostných incidentov
- Certifikovaní odborníci a zaistenie súladu s bezpečnostnými štandardmi a legislatívou - skúsenosti z verejnej správy (zákon o kybernetickej bezpečnosti, zákon o ITVS a iné) ako aj zo súkromného sektora (ISO 27001, NIST, HIPAA a iné)

IstroSec

Data Sheet



Prípadová štúdia

Typ organizácie: výrobný podnik
Poskytnutá služba: posúdenie zraniteľností
Riešenie:
Organizácia nás oslovila s cieľom zistiť, aké verejne dostupné služby a systémy má a následne vykonať vulnerability assessment na všetky identifikované IP adresy ktoré jej patria. V úvode sme vykonali Open-source intelligence (OSINT) fázu počas ktorej sme pomocou kombinácie rôznych techník získali rozsahy IP adries patriace klientskej spoločnosti, vykonali enumeráciu subdomén a identifikáciu domén. Medzi použité techniky patrí DNS brute-forcing, hľadanie v Certificate Transparency (CT), prehľadávanie rôznych webov ako napríklad github.com, pastebin.com, shodan.io, censys.io a iné. Zoznam identifikovaných IP adries a webov dostal zákazník prostredníctvom správy z prvej časti testovania tzv. enumerácie, pričom nám na základe údajov z tejto správy zadefinoval testovací rozsah. Na tomto rozsahu sme vykonali automatizované skenovanie portov, identifikovali otvorené porty, bežiace služby a ich verzie, SSL/TLS zraniteľnosti a iné. Následne sme každú identifikovanú zraniteľnosť manuálne overili pričom sme tieto zraniteľnosti neexploitovali ďalej. Výsledkom testovania bol zoznam identifikovaných zraniteľností a spôsob ako ich odstrániť. Zraniteľnosti boli manuálne overené aby sa zabránilo falošne pozitívnym zraniteľnostiam, čo umožnilo ušetriť klientovi čas pri ich mitigácii.

Penetračné testovanie

Penetračné testovanie (etický hacking) je autorizovaný prienik do sietí, aplikácií alebo infraštruktúr zákazníka na posúdenie úrovne zabezpečenia týchto komponentov z pohľadu útočníka. Na rozdiel od posúdenia zraniteľností dochádza aj k exploitácií nájdených zraniteľností, vykonávanie post exploitácie (posúdenie a otestovanie možností, ktoré útočníkovi dá exploitácia nájdenej zraniteľnosti na systéme v sieti alebo infraštruktúre), lateral movement v rámci povoleného rozsahu a vyhľadávanie ďalších zraniteľností a opätovná exploitácia.

IstroSec ponúka tieto typy penetračného testovania:

Externý penetračný test:
- Webové aplikácie a aplikačné endpointy
- Sieťový penetračný test
- Sociálne inžinierstvo (phishing, spearphishing, smishing, vishing)

Interný penetračný test:
- Penetračný test aplikácie
- Sieťový / infraštruktúrny penetračný test
- Penetračný test Active Directory

Platformovo špecifické testy:
- Penetračný test cloudu
- Penetračný test mobilnej aplikácie
- Penetračný test bezdrôtových sietí

Kompletné penetračné testovanie zahŕňa manuálne ale aj automatizované testovanie s cieľom získať citlivé dáta a preniknúť čo najďalej je to možné (samozrejme v rámci vopred dohodnutého rozsahu testovania).

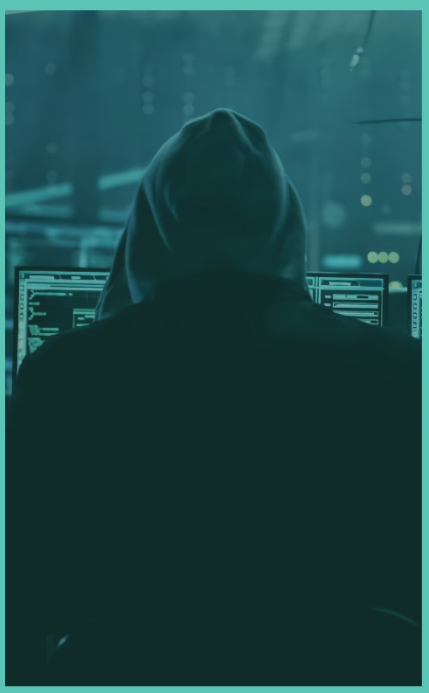
Poukázať z pohľadu útočníka na možné získanie rôznych prístupov, následnú eskaláciu privilégií na vyšší level a využitie nájdených zraniteľností na kompromitáciu systému. Testovanie prebieha v niekoľkých fázach s cieľom odhaliť a poukázať na slabé body či už z vnútra alebo z vonku testovaného systému.
Po ukončení poslednej fázy penetračného testovania, obdrží klient finálnu správu (report) ktorý obsahuje:
- manažérske zhrnutie
- výsledný stav testovaného systému
- podrobne opísané nájdené zraniteľnosti a ich risk level
- odporúčania založené na identifikovanom prostredí
- spôsob ako odstrániť identifikované zraniteľnosti

Pre koho je penetračné testovanie určené?

Najmä pre organizácie ktoré chcú preveriť aktuálny stav systému alebo siete z pohľadu bezpečnosti a nestačí im automatizované testovanie ktoré sa nachádza v službách ako sken zraniteľností či vulnerability assessment. Vyžadujú naozaj dôkladné testovanie s cieľom odhaliť čo najviac slabých miest a chcú vedieť kam by sa až mohol reálny útočník dostať, prípadne ako by tieto zraniteľnosti vedel využiť keďže pri penetračnom testovaní dochádza k aktívnej exploitácií už identifikovaných zraniteľností.

IstroSec

Data Sheet



Prípadová štúdia

Typ organizácie: firma zaoberajúca sa digitálnym marketingom
Poskytnutá služba: penetračné testovanie webovej aplikácie
Riešenie:
Klient nás požiadal o overenie bezpečnosti webovej aplikácie a jej komponentov. V tomto prípade bola využitá služba penetračného testovania webovej aplikácie, ktoré zahŕňa testovanie pomocou metodológie OWASP Testing Guide v4.2 spolu s našimi overenými a fungujúcimi postupmi. Penetračný test prebiehal formou black-box, čo znamená, že nám neboli neposkytnuté údaje o tom ako aplikácia funguje, a bolo na nás, aby sme z vonkajšieho prostredia odhalili celý povrch aplikácie, na ktorý je možné útočiť. Klient mal taktiež záujem o otestovanie REST API, kde bolo odhalených viacero kritických zraniteľností. Výsledkom testovania bolo odhalenie a vyriešenie viacerých chýb v testovacej verzii aplikácie, čo umožnilo jej nasadenie do produkcie až po zmiernení bezpečnostných rizík. Na konci testovania klient obdržal záverečnú správu, teda dokument v ktorom sa nachádza manažérske zhrnutie, detailný popis identifikovaných zraniteľností, postup ako ich odstrániť a záver v ktorom bol zhrnutý stav testovanej aplikácie z hľadiska bezpečnosti. V prípadoch keď ma záujem o overenie, či boli zraniteľnosti naozaj správne odstránené, je možné výsledky testovania doručovať aj priebežne počas testovania.

Red Teaming

Red team engagement využíva taktiky, techniky a procedúry (TTP) na simuláciu reálnych kybernetických hrozieb na základe bezpečnostného profilu organizácie. Cieľom red teamu je okrem overenia úrovne kybernetickej bezpečnosti organizácie pomôcť obrannému tímu organizácie detegovať kybernetický útok a reagovať naň.

Cieľom red teamu je zároveň simulovať realistický útok na organizáciu, ktorý je založený na relevantných hrozbách a TTP pre organizáciu. Pri tejto simulácií je cieľom taktiež preveriť bezpečnostné opatrenia, technológie, procesy, bezpečnostný tím organizácie a identifikovať možné nedostatky.

Red teaming sa obyčajne vykonáva bez znalosti bezpečnostného tímu organizácie s výnimkou vybraných zamestnancov.

Fázy red teamingu:

Vytvorenie profilu hrozieb pre cieľovú organizáciu a pasívne a aktívne získavanie informácií o organizácií:

- Pasívny reconnaissance (vrátane OSINT a DarkWeb Search)
- Aktívny reconnaissance

Naplánovanie útokov za účelom dosiahnutia vytýčených cieľov (napríklad prístup k špecifickým dátam, ovládnutie infraštruktúry, kompromitácia špecifického používateľa, spustenie kódu na zariadeniach organizácie a podobne) a definovaných obmedzení.

Vektory prvotného útoku obyčajne zahŕňajú:

- útoky na používateľa (sociálne inžinierstvo),
- útoky na používateľské zariadenia,
- útoky na perimeter organizácie,
- útoky na vzdialené aktíva organizácie (najmä cloudové služby),
- (optional) fyzickú bezpečnosť a
- (optional) útoky typu supply chain.

Vykonanie a dokumentácia útokov (úspešných aj neúspešných) a vykonanie krokov na dosiahnutie vytýčených cieľov. Súčasťou týchto krokov obyčajne býva:

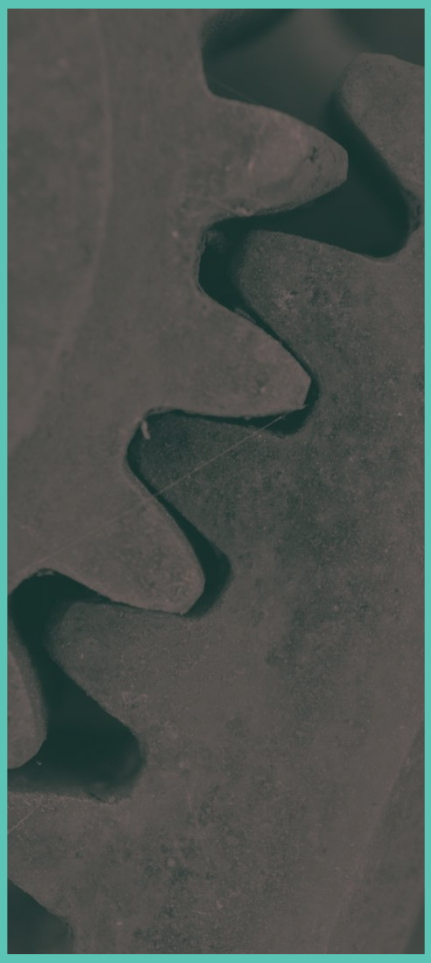
- eskalácia privilégií na zariadeniach a systémoch a ďalšie post exploitačné aktivity na zariadeniach alebo systémoch,
- distribúcia nástrojov, špeciálne upraveného škodlivého kódu v rozsahu špecifikovaných cieľov,
- laterálny pohyb medzi systémami a ďalšie potrebné kroky v závislosti od špecifikovaných cieľov organizácie.

Vytvorenie správy z red teamingu, ktorá obsahuje:

- úspešné vektory útoku,
- identifikované zraniteľnosti v cieľovej organizácií,
- návrh opatrení,
- časový harmonogram vykonávaných aktivít a
- posúdenie efektivity implementovaných bezpeč-nostných opatrení.

IstroSec

Data Sheet



Prípadová štúdia

Typ organizácie: finančná inštitúcia
Poskytnutá služba: red teaming
Riešenie:
Finančná inštitúcia sa na nás obrátila s požiadavkou o simuláciu útoku pomocou red teamingu, ktorá by overila odolnosť celej vonkajšej a vnútornej infraštruktúry voči kybernetickým hrozbám. Tento typ simulácie má niekoľko výhod oproti klasickému penetračnému testu. Nezameriava sa len na úzko definovaný testovací rozsah, ako napríklad pár webových aplikácií či prípadne časť siete, ale na všetko čo spadá pod testovanú organizáciu, a je vopred dohodnuté v rámci testovacieho rozsahu. Ďalšou nespornou výhodou je možnosť využitia sociálneho inžinierstva, a teda v prípade, že má organizácia malý počet systémov dostupných z internetu, nechýba im patch management, a nie je možné cez tieto systémy preniknúť do vnútornej siete organizácie, red team sa pokúsi o prienik inou cestou, napríklad cez spearphishing a úzko profilovanú kampaň. Simuláciu útokov ktoré využívajú útočníci vykonávajú skúsení etickí hackeri so školeniami a certifikáciami práve v tejto oblasti. Red teaming v tomto prípade pomohol organizácii nájsť miesta, ktoré ani pravidelné penetračné testy a vulnerability assessmenty neboli schopné objaviť. Poukázali sme na viaceré miesta cez ktoré mohol útočník preniknúť do siete. Využili sme pritom techniky, ktoré nám umožnili neupútať na seba pozornosť a vyhnúť sa detekcii blue teamom, ktorého úlohou nás bolo zastaviť. Definovaným cieľom na začiatku simulácie bolo získanie konta doménového administrátora, a prístup na zdieľané diskové úložisko, na ktorom sa nachádzali citlivé dáta. Podarilo sa nám kompromitovať doménu, pričom sme využili práve spear-phishing na získanie iniciálneho vstupu do siete. Na konci simulácie, obdržal zákazník finálnu správu s manažérskym záverom, zhrnutím silných a slabých miest, detailný popis ako sme postupovali pri kompromitácií domény, identifikované zraniteľnosti s popisom ako ich odstrániť a ďalšie užitočné informácie. V organizácii zákazníka vedel o simulácií prostredníctvom red teamingu minimálny počet zamestnancov. Aby nedošlo k vyzradeniu, blue team o tom nemohol mať žiadne informácie.

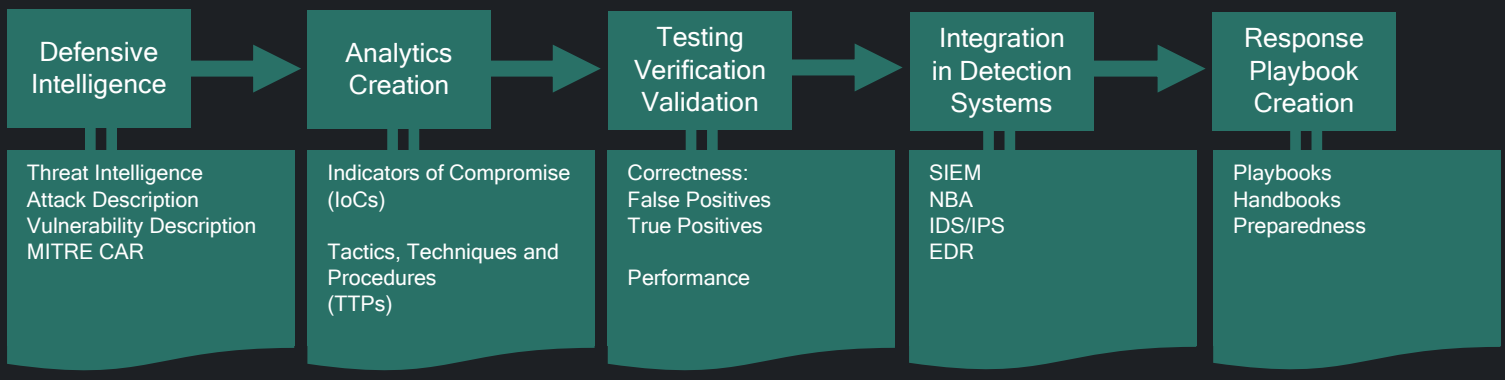
Purple Teaming

Pre organizácie so zvýšenými požiadavkami na bezpečnosť, ako aj pre organizácie, ktoré sú dlhodobo cieľom pokročilých útokov je potrebné kontinuálne implementovať bezpečnostné opatrenia a detekcie na aktuálne bezpečnostné hrozby.

Pri purple team engagemente sa **Istro**Sec sústredí na ľudí, procesy a technológie.

Na základe tohto prístupu **Istro**Sec:

- vytvorí potrebné procesy/smernice a postupy pre purple teaming,
- vyškolí interný bezpečnostný team,
- navrhne a implementuje potrebné technológie,
- identifikuje relevantné zdroje a implementuje analytiky na základe metodológie.



IstroSec | Černyševského 10 | 851 01 Bratislava | Slovensko | +421 917 699 002 | info@istrosec.com | www.istrosec.com