Penetračné testy

Vykonávame simulácie kybernetických útokov na systémy, aplikácie a celú infraštruktúru.
Z našej ponuky si môžete vybrať špecifické penetračné testy pre konkrétne aplikácie a systémy.

Penetračné testy aplikácií

- Webové
- Mobilné
- Desktopové
- API

Penetračné testovanie infraštruktúry

- Interné
- Externé
- Záťažové/DoS testy
- Siete Wi-Fi
- IoT

Konfiguračné testy

- Operačné systémy
- Cloud

Špecializované testy a služby

- ATM
- RFID
- Reverzné inžinierstvo
- Phishing
- Revízia zdrojového kódu
- Advanced White-Box
- Computer Forensics

Testy sociálnym inžinierstvom

Red Team Operations

Pomocou cvičení Red Teaming **overíte svoju schopnosť odhaliť útok a správne reagovať** prostredníctvom svojich procesov a bezpečnostných špecialistov. Ponúkame aj službu, ktorá simuluje phishingové útoky pomocou metód sociálneho inžinierstva.

Penetračné testy aplikácií

Webové
Pri testovaní aplikácií je naším cieľom odhaliť zraniteľnosti, ktoré môžu ohroziť ich dôvernosť, integritu alebo dostupnosť. V rámci bezpečnosti aplikácií sa zaoberáme nielen bežnými útokmi využívajúcimi typické zraniteľnosti, ale zameriavame sa aj na návrh alebo architektúru aplikácie.

Mobilné
Pri testovaní mobilných aplikácií hľadáme bezpečnostné chyby a nedostatky v ich implementácii, a to na strane aplikácie aj na strane servera. V prípade business aplikácií analyzujeme potenciálne riziká a hľadáme bezpečné riešenia pre používanie mobilných zariadení vo firemnom prostredí. V prípade mobilných telefónov vykonávame forenznú analýzu zariadení, ktoré sa stali terčom hackerských útokov. Testujeme aj aplikácie a IoT, aby sme overili ich bezpečnú prevádzku. Využívame všetky naše skúsenosti a pomáhame vytvárať bezpečnejší mobilný svet.

Desktopové
V prípade desktopových aplikácií používame dekompiláciu na úroveň zdrojového kódu vrátane úprav. Identifikujeme bezpečnostné riziká, citlivé údaje alebo iné chyby v autorizácii alebo prenose medzi klientskou aplikáciou a serverom.

API
Penetračné testy API skúmajú slabé miesta rozhrania na poskytovanie služieb. V prípade API testujeme rôzne typy rozhraní, najčastejšie REST a SOAP. Používame príslušné časti metodiky OWASP na testovanie webových aplikácií a tiež vlastnú metodiku, ktorá vychádza z našich skúseností s testovaním služieb API, smernice PSD2 a ďalších.

Penetračné testovanie infraštruktúry

Interné
Počas penetračných testov internej infraštruktúry mapujeme internú sieť spoločnosti, identifikujeme aktívne sieťové prvky a overujeme ich bezpečnosť. Pokúšame sa prelomiť vybrané systémy a kompromitovať doménu spoločnosti zvýšením oprávnení z bežného používateľa na správcu domény. Súčasťou sú aj testy z pracovnej stanice bežného používateľa.

Externé
Pri penetračných testoch externej infraštruktúry kladieme dôraz na odhalenie všetkých dostupných sieťových služieb, komponentov a ich podrobný výpočet. Zhromažďovanie verejných informácií o sieťovej infraštruktúre spoločnosti je pre útočníka kľúčové. Na tento účel používame automatizované aj vlastné nástroje a metodiky.

Záťažové
Útočníci často poškodzujú webové stránky spoločností pre kľúčové webové aplikácie tak, že ich jednoducho zneprístupnia. Čím dlhšie je webová aplikácia pre používateľov nedostupná, tým väčšie sú straty. V rámci odmietnutia služby testujeme vybrané služby, aby sme zabezpečili, že k takýmto situáciám nedôjde a že kritické webové aplikácie budú fungovať aj pri neočakávane vysokom zaťažení.

IoT
Pri testovaní internetu vecí (IoT) sa zameriavame najmä na to, aby sme zistili, ako ľahkým cieľom sú tieto zariadenia. Aké informácie z nich možno získať a ako odhaliť zraniteľnosti, ktoré možno zneužiť na získanie neoprávneného prístupu alebo krádež údajov.

Konfiguračné testy

Operačné systémy
V prípade operačných systémov kontrolujeme úroveň zabezpečenia jednotlivých konfiguračných prvkov. Ponúkame tiež implementáciu odporúčaní, ktoré vydávame na základe výsledkov našich testov, odstránenie zistených slabých miest a zvýšenie vašej obrany v prípade náhleho skutočného útoku.

Cloud
Firemná infraštruktúra, webové aplikácie a iné internetové služby sú v súčasnosti vo veľkej miere umiestnené v cloude. Konfigurácia týchto služieb, či už vlastných alebo tretích strán, zohráva kľúčovú úlohu v oblasti zabezpečenia. Chyby v konfigurácii môžu viesť k strate firemných údajov a dôvery zákazníkov, preto sme pripravení pomôcť vám bezpečne nakonfigurovať vaše cloudové prostredie. V súčasnosti sa špecializujeme na služby AWS, MS Azure a MS 365.

Testy sociálnym inžinierstvom
Sociálne inžinierstvo je činnosť, pri ktorej sa sociálny inžinier pokúša prinútiť svoj cieľ vykonať činnosť, ktorá nemusí byť v najlepšom záujme subjektu. Zamestnanci sú považovaní za najslabší článok bezpečnosti v spoločnosti. Útočník tak môže pomocou sociálneho inžinierstva prelomiť aj tie najbezpečnejšie perimetre. Sociálni inžinieri používajú útoky ako vishing, phishing alebo fyzickú infiltráciu prostredníctvom vydávania sa za niekoho iného. Naším cieľom je preskúmať bezpečnosť vašej spoločnosti pomocou týchto metód a následne navrhnúť najlepšie riešenie na odstránenie zistených rizík.

Red Team Operations
Štandardné metódy penetračného testovania zisťujú rôzne typy zraniteľností, ale netestujú schopnosť odhaliť kybernetický útok, reagovať naň a zotaviť sa z neho. Red Team Operations, známe aj ako Red Teaming, sú odvodené od pojmu Red Team, ktorý označuje tím skúsených etických hackerov, ktorí vykonávajú útok s použitím rovnako sofistikovaných prostriedkov ako skutoční útočníci. Red Teaming preto verne simuluje útočné hrozby s využitím najnovších technológií a taktík a zároveň poskytuje informácie o pripravenosti spoločnosti na odhalenie, elimináciu a nápravu týchto útokov.

Siete Wi-Fi
Penetračné testy technológií Wi-Fi simulujú útok na prístup do internej siete organizácie prostredníctvom bezdrôtového signálu Wi-Fi. Po získaní prístupu skontrolujeme kvalitu filtrovania prevádzky medzi segmentom siete klienta Wi-Fi a ostatnými internými sieťami. Naše testy zahŕňajú aj analýzu konfigurácie bezdrôtového sieťového pripojenia na strane klienta.

NFC / RFID
Ve firemním prostředí se technologie RFID či NFC využívají nejčastěji ve formě vstupních karet pro řízení fyzického přístupu v budově, ale existuje i mnoho jiných využití. Během analýzy prověříme bezpečnost implementovaného řešení a jeho schopnost zamezení přístupu neautorizovaných osob do budovy, zcizení dat uložených na kartě či modifikaci jejich obsahu. U RFID technologií replikujeme veřejně známé útoky na konkrétní typy karet a rovněž se pouštíme do vlastního průzkumu možných slabých míst a potenciálních vektorů útoku.

Naše hlavné služby

- Testy sociálnym inžinierstvom
- Penetračné testy aplikácií
- Revízia zdrojového kódu
- Penetračné testy cloudových služieb
- Penetračné testy infraštruktúry
- Konfiguračné testy
- Penetračné testy bezdrôtových sietí WiFi
- Penetračné testy mobilných zariadení
- Red Teaming

Špecializované testy a služby

ATM
Do týždňa skontrolujeme zraniteľnosti bankomatov. Naša komplexná analýza zahŕňa metódy fyzického prístupu, eskaláciu privilégií, testy operačného systému a aplikácií. Môžeme sa však zamerať len na penetračné testy infraštruktúry, integračných služieb a manažmentu, reverznú analýzu softvéru alebo bezpečnostnú analýzu zdrojového kódu.

Reverse Engineering
Pri reverznom inžinierstve spätne analyzujeme funkčnosť testovaných aplikácií bez prístupu k ich zdrojovému kódu alebo bez znalosti tohto kódu s cieľom overiť ich odolnosť voči potenciálnym reálnym útokom. Pri analýze kódu využívame naše skúsenosti z penetračných testov desktopových klientov.

Phishing
Testujeme odolnosť firiem voči útokom vydieračskými programami. Počas preverovania analyzujeme existujúce situácie vrátane testu odolnosti systému. Výstupom je report s odporúčaniami vhodných riešení.

Codebashing
Ak vyvíjate aplikácie, ponúkame vám riešenia na vzdelávanie a propagáciu bezpečnosti aplikácií prostredníctvom služby Codabashing. To umožňuje bezpečnostným a vývojovým tímom vytvárať a udržiavať kultúru bezpečného vývoja. Prostredníctvom komunikačných nástrojov, gamifikácie, vzájomných výziev a priebežného hodnotenia vám Codebashing pomôže odstrániť vznik softvérových zraniteľností vo vašom zdrojovom kóde.

Computer Forensics
Cieľom počítačovej forenznej analýzy je preskúmať digitálne médiá a údaje s cieľom identifikovať, zachovať, obnoviť, analyzovať a následne prezentovať fakty a zistenia. Zistenia možno následne použiť ako dôkaz v súdnych konaniach týkajúcich sa počítačovej kriminality, ale aj v občianskoprávnych konaniach.

Advanced white-box
Ide o kombináciu penetračného testovania a secure code review alebo iných hodnotiacich služieb. Cieľom advanced white-box je komplexne overiť bezpečnosť vyvíjaných aplikácií simuláciou hackerských útokov, automatizovanou analýzou kódu, manuálnymi revíziami kódu a auditmi.

hackingLab

Vytvorili sme komunitný projekt, v rámci ktorého si vymieňame know-how a budujeme atraktívnu platformu pre pravidelné stretnutia, ktoré posúvajú našich členov vpred.

Zámerne obchádzame logiku testovaných produktov a systémov. Nabúravame ich procesy, hľadáme zraniteľnosti, implementáciu a bezpečnostné chyby.

Zapojte sa do programu testovania zabezpečenia zariadení IoT
Zanalyzujeme vaše zariadenia a odhalené bezpečnostné chyby popíšeme v podrobnom reporte s návrhmi na nápravu.

Dajte nám vedieť, ak ste
- výrobcovia IoT a smart technológií
- predajcovia, ktorí chcú svojim zákazníkom ponúknuť kvalitné služby
- používatelia, ktorí si nie sú istí kvalitou zabezpečenia zakúpeného produktu

Viac informácií o HackingLab, komunite a možnostiach spolupráce nájdete na hackinglab.cz.