ARICOMA

Penetrační testy

Provádíme simulace kybernetických útoků na systémy, aplikace i celou infrastrukturu. Z naší nabídky si můžete vybrat specifické penetrační testy pro konkrétní aplikace a systémy.

Penetrační testy aplikací

- Webové
- Mobilní
- Desktopové
- API

Penetrační testy infrastruktury

- Interní
- Externí
- Zátěžové/DoS testy
- Wi-Fi sítě
- IoT

Konfigurační testy

- Operační systémy
- Cloud

Specializované testy a služby

- ATM
- RFID
- Reverse Engineering
- Phishing
- Revize zdrojového kódu
- Advanced White-Box
- Computer Forensics

Testy sociálním inženýrstvím

Red Team Operations

S Red Teaming cvičeními **ověříte schopnost detekce útoku a správné reakce** prostřednictvím vašich procesů a bezpečnostních specialistů. Nabízíme i službu simulující phishingové útoky s využitím metod sociálního inženýrství.

Penetrační testy aplikací

Webové
Při testování aplikací je naším cílem odhalení zranitelností, které mohou narušit jejich důvěrnost, integritu či dostupnost. V rámci aplikační bezpečnosti se zabýváme nejen běžnými útoky zneužívajícími typické zranitelnosti, ale věnujeme se také návrhu či architektuře dané aplikace.

Mobilní
Při testech mobilních aplikací hledáme bezpečnostní chyby a nedostatky v jejich implementaci, ať již na straně aplikace, tak na serverové části. U business aplikací analyzujeme možná rizika a hledáme bezpečná řešení pro užívání mobilních zařízení ve firemním prostředí. U mobilních telefonů provádíme forenzní analýzu přístrojů, které se staly terčem hackerských útoků. Rovněž IoT aplikace a systémy podrobujeme testům, abychom ověřili jejich bezpečný provoz. S využitím všech našich zkušeností pomáháme tvořit bezpečnější mobilní svět.

Desktopové
U desktopových aplikací postupujeme pomocí dekompilace až na úroveň zdrojového kódu, včetně jeho úprav. Identifikujeme z pohledu bezpečnosti riziková místa, citlivá data nebo jiné nedostatky v autorizaci či samotném přenosu mezi klientskou aplikací a serverem.

API
API penetračními testy prověřujeme slabiny rozhraní pro poskytování služeb. U API testujeme různé typy rozhraní, mezi které nejčastěji patří REST a SOAP. Při testování využíváme relevantní části metodiky OWASP pro testování webových aplikací a také naší vlastní metodiku, která vzešla s našich zkušeností testováním API služeb, PSD2 a jiných.

Penetrační testy infrastruktury

Interní
Při penetračních testech interní infrastruktury mapujeme vnitřní síť společnosti, identifikujeme aktivní síťové prvky a prověřujeme jejich bezpečnost. Pokoušíme se prolomit vybrané systémy a kompromitovat doménu společnosti eskalací privilegií z běžného uživatele na doménového administrátora. Součástí jsou také testy z pracovní stanice běžného uživatele.

Externí
Při penetračních testech externí infrastruktury klademe důraz na odhalení všech dostupných síťových služeb, komponent a jejich detailní enumeraci. Sběr veřejných informací o síťové infrastruktuře společnosti je pro útočníka klíčový. K tomuto účelu využíváme jak automatizované, tak vlastní proprietární nástroje a metodiky.

Zátěžové
Útočníci často u klíčových webových aplikací poškozují weby společností tím, že je jednoduše znepřístupní. Čím déle není uživatelům daná webová aplikace dostupná, tím větší jsou ztráty. V rámci Denial of Service testujeme vybrané služby, aby k těmto situacím nedocházelo a kritické webové aplikace tak fungovaly i při neočekávaně vysoké zátěži.

IoT
Našim hlavním zaměřením při testování internetu věcí (IoT) je zjištění, jak jednoduchým cílem daná zařízení jsou. Jaké informace z nich lze získat, a jak detekovat jejich zranitelnosti, které mohou být zneužity pro získání neautorizovaných přístupů či krádeží dat.

Konfigurační testy

Operační systémy
U operačních systémů prověřujeme míru zabezpečení jednotlivých konfiguračních prvků. Nabízíme i implementaci doporučení, které vám na základě výsledků z námi provedených testů vystavíme, eliminujeme tak nalezené slabiny a zvyšujeme obranyschopnost při nenadálém reálném útoku.

Cloud
Firemní infrastruktury, webové aplikace a další internetové služby jsou dnes z velké části hostovány v cloudovém prostředí. Klíčovou roli v oblasti bezpečnosti představuje konfigurace těchto služeb, ať už nativních, nebo služeb třetích stran. Konfigurační nedostatky mohou vést ke ztrátě firemních dat i důvěry zákazníků, proto jsme připraveni vám s otázkou bezpečné konfigurace vašeho cloudového prostředí pomoci. Aktuálně se specializujeme na služby AWS, MS Azure či MS 365.

Testy sociálním inženýrstvím
Sociální inženýrství je akt, ve kterém se sociální inženýr pokouší přimět svůj cíl k provedení akce, která nemusí být v nejlepším zájmu daného subjektu. Zaměstnanci jsou považováni za nejslabší článek bezpečnosti ve společnosti. Útočník tak může využít sociální inženýrství k prolomení i těch nejzabezpečenějších perimetrů. Sociální inženýři k tomu využívají útoky jako například vishing, phishing, nebo fyzickou infiltraci pomocí impersonace. Našim cílem je prověřit zabezpečení vaší společnosti za pomocí těchto metod a následně navrhnout nejlepší řešení, pro eliminaci nalezených rizik.

Red Team Operations
Standardní způsoby penetračních testů odhalí různé typy zranitelností, ale neprověří schopnost detekce, reakce a zotavení z kybernetického útoku. Red Team Operations, také nazývaný Red Teaming je odvozen od výrazu Red Team, jenž označuje tým zkušených etických hackerů, který útok realizuje a využívá při tom stejně sofistikované prostředky jako reální útočníci. Služba Red Teaming tedy věrně simuluje hrozby útoků s pomocí nejmodernějších technologií a taktik, a také poskytuje informace o připravenosti společnosti tyto útoky detekovat, eliminovat a provést nápravná opatření.

Wifi sítě
Penetračními testy Wi-Fi technologií simulujeme útok na přístup do vnitřní sítě organizace prostřednictvím bezdrátového signálu Wi-Fi sítí. Po získání přístupu prověříme kvalitu filtrování provozu mezi síťovým segmentem Wi-Fi klientů a zbytkem interních sítí. Do testů zahrnujeme i analýzy konfigurace připojení k bezdrátové síti na straně klientských zařízení.

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 hlavní služby

- Testy sociálním inženýrstvím
- Penetrační testy aplikací
- Revize zdrojového kódu
- Penetrační testy cloudových služeb
- Penetrační testy infrastruktury
- Konfigurační testy
- Penetrační testy bezdrátových sítí WiFi
- Penetrační testy mobilních zařízení
- Red Teaming

Specializované testy a služby

ATM
Prověříme zranitelnosti bankomatů během jednoho týdne. Naše komplexní analýza zahrnuje způsoby fyzického přístupu, eskalaci privilegií, testy operačního systému a aplikací. Můžeme se však soustředit pouze na penetrační testy infrastruktury, integračních služeb a managementu, reverzní analýzu softwaru, případně bezpečností analýzu zdrojového kódu.

Reverse Engineering
Při reverzním inženýrství zpětně analyzujeme funkčnosti testovaných aplikací, bez přístupu, či znalosti jejich zdrojových kódů a tím ověříme jejich odolnost vůči možným reálným útokům. Při analýze kódů využíváme zkušenosti z penetračních testů desktopových klientů.

Phishing
Testujeme odolnosti firem proti útokům vyděračskými programy. Při prověřování analyzujeme stávající situace včetně testu odolnosti systému. Výstupem je report s doporučeními příslušných řešení.

Codebashing
Pokud vyvíjíte aplikace, nabízíme vám prostřednictvím služby Codabashing řešení pro edukaci a evangelizaci v oblasti aplikační bezpečnosti. Ta umožňuje bezpečnostním a vývojovým týmům vytvářet a udržovat kulturu bezpečného vývoje. Prostřednictvím komunikačních nástrojů, gamifikace, vzájemných výzev a průběžných hodnocení vám Codebashing pomůže eliminovat vznik softwarových zranitelností ve zdrojovém kódu.

Computer Forensics
Cílem počítačové forenzní analýzy je prozkoumat digitální média a data s cílem identifikovat, zachovat, obnovit, analyzovat a následně prezentovat fakta a zjištění. Zjištění mohou následně být použita jako důkazní materiál u soudních řízení počítačové kriminality ale také pro občanskoprávní řízení.

Advanced white-box
Jedná se o kombinaci penetračních testů a secure code review, případně další assessment služeb. Cílem advanced white-box je komplexní prověření bezpečnosti vyvíjených aplikací za pomoci simulace hackerských útoků, automatizované analýzy kódu, manuálních revizí kódu a auditů.

hackingLab

Založili jsme komunitní projekt, kde sdílíme know-how a budujeme atraktivní platformu pro pravidelná setkávání, která své členy posouvají vpřed.

Záměrně obcházíme logiku testovaných výrobků a systémů. Nabouráváme jejich procesy, hledáme zranitelnosti, chyby v implementaci a zabezpečení.

Zapojte se do programu testování zabezpečení IoT zařízení
Vaše zařízení podrobíme analýze a nalezené bezpečnostní zranitelnosti popíšeme v detailním reportu s návrhy na jejich odstranění.

Ozvěte se nám, pokud jste
- výrobci IoT a smart technologií
- prodejci, kteří chtějí svým zákazníkům nabídnout kvalitní servis
- uživatelé, kteří si nejsou jistí kvalitou zabezpečení zakoupeného produktu

Pro více informací o HackingLabu, komunitě a možnostech spolupráce navštivte hackinglab.cz.