TESTY ZRANITELNOSTÍ

Otestujeme zranitelnosti systémů, zařízení a aplikací přístupných z Internetu. Používáme neinvazivní techniky, které neohrožují chod ani provoz systémů. Testování je možné vykonávat jednorázově nebo periodicky. Výsledkem testu je zpráva o stavu zranitelnosti, která obsahuje popis jednotlivých zjištění, ohodnocení závažnosti a návody na odstranění bezpečnostních chyb.

- prevence před bezpečnostními incidenty
- včasná identifikace slabých míst systému
- optimalizace nákladů na implementaci bezpečnostních opatření
- sledování vývoje stavu zabezpečení

Výsledkem je závěrečná zpráva s hodnocením závažností podle OWASP včetně popisu zranitelnosti a uvedené chyby.

www.viruslab.cz +420 222 220 051 info@viruslab.cz

RUČNÍ SKEN PERIMETRU

V tomto skenu provádíme to, čemu útočníci říkají REACON - tedy průzkum prostředí před útokem. Zmapujeme, co všechno jde o Vaší společnosti a infrastruktuře zjistit, pomocí technik OSINTu.

- Zmapujeme všechny služby vystavené „do internetu“ a jejich provázanost
- Odhalíme rizikové zranitelnosti v síťových službách
- Detekujeme zastaralé operační systémy a technologie
- Zjistíme zda se hesla Vašich zaměstnanců nenacházejí v uniklých databázích
- Ověříme zda na Vašem webu nejsou dohledatelné citlivé dokumenty

TEST WEBOVÝCH STRÁNEK

V tomto skenu prověříme bezpečnost webu Vaší společnosti, od aktuálnosti použitých knihoven, přes bezpečné nastavení cookies až po kontrolu toho, zda není možné vykrást databázi z webové aplikace.

- Správná konfigurace HTTPS
- Bezpečné nastavení cookies
- Náchylnost na cross-site-scripting (XSS) - vložení cizího kódu
- Náchylnost na SQL injection - zcizení databáze
- Zranitelnosti ve WordPress, Joomla a Drupal
- Aktuálnost použitých technologií (JavaScript, PHP...)
- Test zranitelností webserveru
- Veřejně dostupné dokumenty a citlivé údaje

www.viruslab.cz +420 222 220 051 info@viruslab.cz

AKTIVNÍ SKEN ON-LINE INFRASTRUKTURY

V tomto skenu aktivně prověříme bezpečnost Vaší infrastruktury vystavené do internetu. Oskenujeme je na známé zranitelnosti a miskonfiguraci, ověříme skutečný dopad nalezených CVE i jiné možnosti exploitace.

- Kontrola a detekce otevřených portů
- Analýza služeb běžících na serverech
- Scan operačních systémů a výskyt exploitů
- Testování proti známým zranitelnostem (CVE)
- Vyhledávání subdomén a návazností na další služby
- Testování výchozích přihlašovacích údajů
- Bezpečná exploitace nalezených zranitelností
- Zpracování výsledného reportu a doporučení

www.viruslab.cz +420 222 220 051 info@viruslab.cz