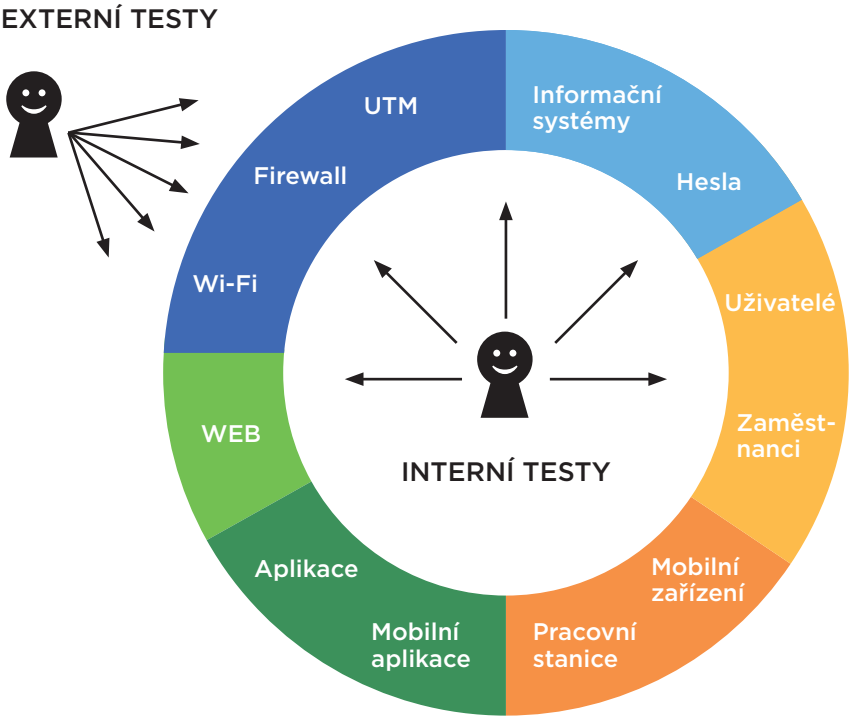
TRUSTED NETWORK SOLUTIONS

Penetrační testy

Na základě simulace reálného útoku dokážeme poskytnout přehled o slabých místech využitelných k průniku do vašich systémů a aplikací. Odhalíme bezpečnostní nedostatky, zhodnotíme stupeň jejich závažnosti a navrhneme nápravná opatření vedoucí k jejich odstranění.



Testy infrastruktury

Externí penetrační testy

Cílem je prověření bezpečnostních mechanismů sloužících k ochraně zdrojů, služeb a dat před neoprávněným přístupem či manipulací ze strany útočníků z vnější sítě. Důraz je kladen na odhalení co největšího počtu závažných zranitelností, které jsou zneužitelné k úspěšnému získání neoprávněného přístupu do interní sítě.

Interní penetrační testy

Cílem je prověření bezpečnostních mechanismů sloužících k ochraně zdrojů, služeb a dat před neoprávněným přístupem a případným zneužitím ze strany uživatelů ve vnitřní síti, jako jsou např. zaměstnanci, partneři nebo dodavatelé. Důraz je kladen na odhalení co největšího počtu závažných zranitelností a nalezení způsobu jejich zneužití.

Penetrační test Wi-Fi sítě

Cílem je prověření bezpečnostních mechanismů sloužících k ochraně zdrojů, služeb a dat před neoprávněným přístupem ze strany uživatelů připojených prostřednictvím Wi-Fi sítě.

Fáze testování

Identifikace cílů

Detekce aplikací a služeb

Identifikace zranitelností

Odhalení nedostatků

Analýza a návrh opatření

Závěrečná zpráva

Re-test

Režimy testování

Black-box

Testerovi je umožněn přístup k testovanému prostředí bez poskytnutí jakýchkoliv dalších informací o jeho architektuře, použitých technologiích či konfiguraci. Je tak simulován útok z pozice hosta nebo externího útočníka.

White-box

Tester má k dispozici velmi podrobné informace o testovaném prostředí, architektuře sítě, použitých technologiích i konfiguraci. Je tak simulován útok z pozice administrátora.

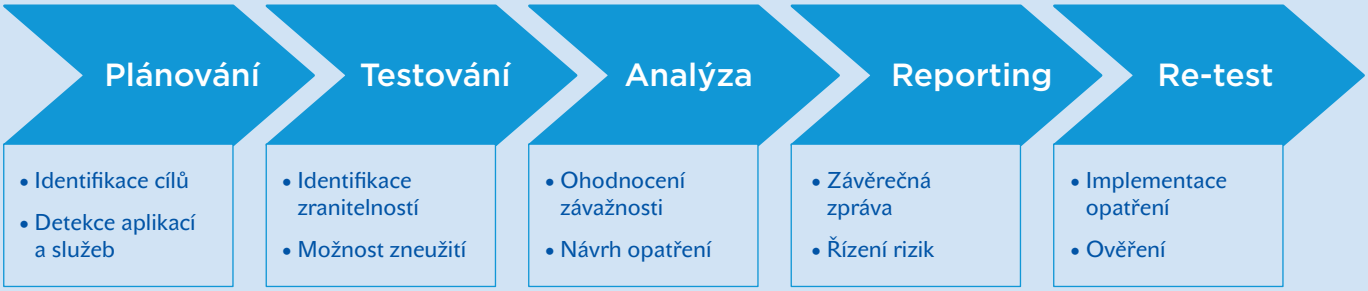
Grey-box

Jedná se o kombinaci obou předchozích režimů. Testerovi jsou poskytnuty předem dostupné informace, které má uživatel v dané roli k dispozici. Simulován tak může být útok např. ze strany bývalého zaměstnance, partnera nebo dodavatele.

Metodika testování

Penetrační testy probíhají dle vlastní metodiky. Vycházíme z obecně uznávaných a ověřených metodik OSSTMM, PTES a OWASP s ohledem na doporučení institutu NIST a asociace ISACA.

Nečekejte, až vás otestuje skutečný hacker! Odhalte včas slabá místa a chraňte své zdroje.



Testy webových aplikací

Základní penetrační test

- Test zaměřený na odhalení nejzávažnějších zranitelností webových aplikací
- Přehledový test s využitím automatických testovacích nástrojů
- Manuální testování nejzávažnějších nalezených zranitelností
- Test vhodný pro webové stránky a základní webové aplikace

Detailní penetrační test

- Test zaměřený na komplexní bezpečnostní audit webových aplikací
- Přehledový test s využitím automatických testovacích nástrojů
- Detailní manuální testování všech nalezených zranitelností
- Návrh a provedení kombinovaných útočných scénářů
- Test vhodný pro rozsáhlé webové aplikace vyžadující vysoké zabezpečení

Specializované testy

- **DoS útok:** útok s cílem zahlcení požadavky
- **Sociální inženýrství:** získání informací pod falešnou záminkou
- **Phishing:** podvodná technika používaná k získání přístupových údajů
- **Audit mobilních zařízení:** ověření zabezpečení vůči neoprávněnému použití
- **Audit pracovní stanice:** ověření zabezpečení proti případnému zneužití
- **Prolamování hesel:** útoky hrubou silou
- **Analýza metadat na webových serverech:** prevence úniku citlivých dat
- **Audit mobilních aplikací:** ověření úrovně zabezpečení aplikace
- **Audit zdrojového kódu:** vyhledání bezpečnostních mezer
- **Zátěžové testy:** testování výkonu síťové a aplikační infrastruktury
- **Testy na míru:** dle specifických požadavků a potřeb klienta

Závěrečná zpráva

- Výčet nalezených zranitelností a ohodnocení jejich závažnosti
- Doporučená opatření k jednotlivým zranitelnostem a snížení rizik
- Manažerské shrnutí pro strategické řízení bezpečnosti
- Výsledné zhodnocení detekované úrovně zabezpečení
- Závěrečná zpráva je výstupem každého penetračního testu

Re-test

- Opakování testu po implementaci nápravných opatření

REFERENCE

České dráhy
Testy zákaznického portálu

Plzeňský kraj
Externí a interní testy infrastruktury,
Testy zabezpečení Wi-Fi sítě

Raiffeisenbank
Testy webové aplikace investičního portálu

GUMOTEX
Externí a interní testy infrastruktury,
DoS útoky

KONTAKT

TRUSTED NETWORK SOLUTIONS

Jsou vaše data dostatečně zabezpečena?
Sestavíme vám na míru penetrační test, který prověří skutečnou úroveň ochrany vašich informačních systémů.

Telefon: +420 545 423 160
E-mail: info@tns.cz

www.tns.cz