Penetrační testy externí infrastruktury

AEC

Zabraňte neautorizovanému přístupu

V rámci penetračních testů externí infrastruktury je kladen důraz na odhalení všech dostupných síťových služeb a komponent a jejich detailní enumeraci. Sběr co nejvíce veřejných informací o síťové infrastruktuře společnosti je pro útočníka klíčový – tyto informace jsou využívány k odhalování zranitelností, provádění kybernetických útoku a získání přístupů do vnitřní sítě společnosti nebo odcizení klientských dat.

Jedná se tedy o typ testu simulující akce útočníka, který si vyhlédne společnost jako cíl svého zájmu a útočí anonymně a vzdáleně přes internet na externí perimetr společnosti.

www.aec.cz

Penetrační testy externí infrastruktury

Vnější penetrační test představuje simulaci napadení komponent informačního systému útočníkem z vnějšího prostředí. Cílem testů je zjistit, jak snadno identifikovatelný cíl ICT infrastruktura organizace představuje, jaké technické informace lze získat o veřejně dostupných službách, detekovat zranitelnosti, které mohou být zneužity k získání neautorizovaného přístupu k citlivým systémovým zdrojům, a navrhnout doporučení k jejich odstranění.

Komplexní hodnocení bezpečnosti testovaných externích komponent při penetračním testování zahrnuje následující kroky:

- identifikace cíle,
- zjištění aktivních služeb,
- nalezení zranitelností,
- exploitace zranitelností / získání přístupu,
- eskalace privilegií a ovládnutí cíle.

Penetrační testy externí infrastruktury

Při realizaci penetračních testů vycházíme především z aktuální metodiky OSSTMM, přičemž je kladen důraz na níže uvedené techniky:

Identifikace cíle

- Sběr co největšího množství dostupných informací (DNS jména, IP adresy, veřejně dostupné informace, evidenční databáze, trasování, odezva atd.).

Zjištění aktivních služeb

- Skenování otevřených portů a běžících služeb.
- Zjištění typu operačního systému a verzí jednotlivých SW.
- Ddůraz na využití systémových nástrojů i automatizovaných skenerů.

Nalezení zranitelností

- Zjišění výskytu zranitelností na základě výsledků předchozích fází a dalšího skenování.
- Snaha o zneužití zranitelnosti (exploitace) a kompromitace daných služeb a systémů.
- Využíváme výkonné komerční skenery zranitelností i vlastní proprietární nástroje.

Získání přístupu

- Snaha o průnik do systémů / služeb za pomoci nalezených zranitelností z předchozích fází.
- Snaha o neautorizované získání citlivých informací, přístupů do systémů, atd.

Eskalace privilegií a ovládnutí cíle

- Cílem je získat plnou kontrolu nad daným aktivem,
- Případné využití cíle pro „pivoting“ – útočení na další systémy prostřednictvím již kompromitovaných.

Naše přednosti

- Patříme mezi zavedené české security firmy, na trhu úspěšně působíme již déle než 30 let.
- Máme více než 20 let zkušeností na poli bezpečnosti externí infrastruktury.
- Disponujeme největším týmem etických hackerů v ČR, který je složen z více než 15ti vlastních pracovníků na hlavní pracovní poměr.
- Jsme držiteli certifikací CEH, eMAPT, CISSP, OSCP, OSCE a celé řady dalších.
- Náš tým tvoří specialisté se zkušenostmi ze stovek projektů.
- Naslouchámе klientům a přizpůsobujeme testy jejich potřebám a časovým možnostem.
- Sledujeme moderní trendy v oblasti bezpečnosti a technologií.
- Při testování klademe důraz na důslednou enumeraci zadaných cílů, která vede k odhalení většího množství zranitelností.

Praha – AEC a.s., Voctářova 20a, 180 00 Praha 8, tel: +420 226 229 133
Brno – AEC a.s., Veveří 102, 616 00 Brno, tel: +420 541 235 466
Bratislava – AEC s. r. o., Prievozská 6, 821 09 Bratislava, tel.: +421 254 410 283