Penetrační testy interní infrastruktury

AEC

Nenechte se připravit o celou doménu

V rámci penetračních testů interní infrastruktury je kladen důraz na odhalení všech dostupných síťových služeb a komponent a jejich detailní enumeraci. Sběr co nejvíce dostupných informací o síťové infrastruktuře společnosti je pro útočníka klíčový – tyto informace jsou využívány k odhalování zranitelností, provádění útoků a získání přístupů k citlivým systémům ve vnitřní síti společnosti.

Jedná se tedy standardně o typ testu simulující akce interního zaměstnance / útočníka, který získal přístup do vnitřní sítě organizace. Hlavní snahou, kromě získání přístupů do jednotlivých systémů, je získat oprávnění doménového administrátora a kompromitovat celou doménu organizace.

www.aec.cz

Penetrační testy interní infrastruktury

Vnitřní penetrační test představuje simulaci napadení komponent informačního systému útočníkem z vnitřního prostředí společnosti. Cílem testů je zjistit, jak snadno identifikovatelný cíl ICT infrastruktura organizace představuje, jak snadno lze detekovat zranitelnosti, které mohou být zneužity k získání neautorizovaného přístupu k citlivým systémovým zdrojům, a navrhnout doporučení k jejich odstranění.

V následujících bodech jsou uvedeny obecné činnosti, jejichž cílem je získat podklady pro komplexní hodnocení bezpečnosti testovaných systémů při interních penetračních testech:

- Identifikace cílů, prostředí a hledání zranitelností.
- Identifikace aktivních serverů, síťových prvků a prověření jejich zabezpečení.
- Pokus o prolomení vybraných identifikovaných systémů a služeb – eskalace privilegií.
- Pokus o kompromitaci domény společnosti.

Penetrační testy interní infrastruktury

Při realizaci interních penetračních testů vycházíme především z aktuální metodiky OSSTMM a zkušeností testerů s útoky na doménové stroje, přičemž je kladen důraz na níže uvedené postupy:

Identifikace cílů, prostředí a hledání zranitelností

Prvotní fáze zahrnuje rozpoznání a mapování jednotlivých systémů (typy serverů, operačních systémů atd.) a služeb dostupných v uživatelské síti organizace. Testujeme zde bezpečnostní slabiny související se softwarovými chybami, chybami v konfiguraci a chybami vycházejícími z nevhodného designu a nastavení služeb.

Identifikace aktivních síťových prvků a prověření jejich bezpečnosti

Fáze zahrnuje rozpoznání aktivních síťových prvků (firewall, switche, routery, monitorovací sondy) a prověření jejich úrovně bezpečnosti z pohledu celkové koncepce sítě organizace, i z pohledu samotných systémů.
Testy jsou realizovány automatizovanými metodami skenování, které rozpoznají strukturu sítě a vlastní zranitelnosti jednotlivých systémů dle získaných „otisků" služeb. Dopady na bezpečnost sítě jsou následně vyhodnoceny dle doporučení výrobců a uznávaných best practices.

Pokus o prolomení vybraných identifikovaných systémů a služeb – eskalace privilegií

Na základě výsledků předchozích fází jsou identifikovány a ověřeny možnosti povýšení daných práv a případného plného ovládnutí testovaných systémů.
Jednotlivé testy jsou realizovány různými metodami. Zejména však útoky hádání hesel, zneužití nalezených informací (nalezená hesla, skripty) a dále pak i využití exploitů pro konkrétní nalezené zranitelnosti.

Pokus o kompromitaci domény společnosti

V této fázi je uskutečněn pokus o eskalaci privilegií na úroveň doménového administrátora. Cílem je kompromitace interní domény společnosti. Během prováděných technik jsou použity klasické i nejmodernější techniky útočníků, jakými jsou například Pass the Hash, LSASS Dumping, Kerberoasting, Incognito Token Impersonation a další.

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 webových aplikací a platforem.
- 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 webových projektů.
- Naslouchámе klientům a přizpůsobujeme testy jejich potřebám a časovým možnostem.
- Sledujeme moderní trendy v oblasti webové bezpečnosti a technologií.
- Při testování klademe důraz na manuální přístup, který vede k odhalení většího množství chyb zejména v business logice aplikací.

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

www.aec.cz