

ИНФОРМАЦИОНЕН ЛИСТ ЗА УСЛУГАТА

Active Directory и вътрешна мрежа

Вътрешна оценка с фокус върху Active Directory и мрежата около него: членствата в групи, правата и сесиите, които превръщат една-единствена опорна точка в пълен контрол над домейна.

ПОДХОДЯЩО ЗА	Мрежи с преобладаващ Windows; тестване с предполагаем пробив; укрепване на защитата преди трансформация
ПОЛУЧАВАТЕ	Карта на пътищата за атака, приоритизирани тесни места в AD, план за укрепване на защитата
ОБХВАЩА	AD и вътрешна мрежа

Пътища за атака, а не просто констатации

Компрометирането на Active Directory рядко е един-единствен експлойт; то е верига от напълно легитимни права. Картографираме този граф така, както го правят нападателите, и след това показваме едно или две тесни места, чието отстраняване срива десетки пътища наведнъж. (Това е работата зад нашата публикация за BloodHound.)

Можем да започнем от предполагаем пробив или от акаунт с ниски права и да работим заедно с вашия екип или незабелязано — както предпочитате.

Какво разглеждаме

- Обекти, ACL-и и доверителни връзки в AD
- Прекомерни права на локални администратори и разрастване на привилегированите групи
- Излагане на идентификационни данни и хигиена на сесиите
- Слабости в Kerberos и делегирането
- Пътища за странично движение и ескалация
- Нива на администриране и административна хигиена

Как протича

- Опорна точка и събиране — От договорена начална точка картографираме домейна.
- Анализ на пътищата — Определяме най-късите маршрути до целите с висока стойност.
- Потвърдена експлоатация — Доказваме пътищата безопасно, от край до край.
- Доклад и повторен тест — Приоритизирани корекции на тесните места, след което проверени.

Какво получавате

- Резюме за ръководството — Бизнес рискът, представен ясно за ръководството и управителния съвет.
- Технически доклад — Всяка констатация със степен на критичност, доказателства и възпроизвеждане.
- Приоритизирани корекции — Конкретни стъпки за отстраняване, подредени по реален риск и готови за изпълнение от разработчиците.
- Писмо за повторен тест — Проверяваме вашите корекции и потвърждаваме писмено закриването им.

Методологии и стандарти, на които се опираме

MITRE ATT&CK; · Моделът Microsoft Enterprise Access (разделяне на нива) · NIST SP 800-115 · PTES · Принципите за тестване на OWASP · Базови правила за хигиена и укрепване на защитата на Active Directory · CIS бенчмаркове за Microsoft Windows и AD

Старши тестери. Доказателства за всяка констатация. Включен повторен тест. Минимум пет дни тестване. Обхват и примерни доклади — pxlsec.com/bg/services/active-directory-assessment.