УДК 004.891.3: 004.021
Торяник А. – ст. гр. СНм-51
Тернопільський національний технічний університет імені Івана Пулюя

ТЕХНОЛОГІЇ АНАЛІЗУ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ

Науковий керівник: асистент Маєвський О.В.

В організації, що використовує корпоративну інформаційну систему, потрібно регулярно перевіряти, наскільки реалізовані або використовувані механізми захисту інформації відповідають положенням прийнятої в організації політики безпеки. Таке завдання періодично виникає при зміні і оновленні компонентів інформаційної системи, зміні конфігурації операційної системи і тому подібне.

Використання засобів аналізу захищеності дозволяє визначити уразливості на вузлах корпоративної мережі і усунути їх до того, як ними скористаються зловмисники.

Засоби аналізу захищеності працюють на початковому етапі здійснення атаки. Виявляючи і своєчасно усуваючи уразливості, вони тим самим запобігають самій можливості реалізації атаки, що дозволяє понизити витрати (фінансові, ресурсні, людські і так далі) на експлуатацію засобів захисту. Технології аналізу захищеності є дієвим методом, що дозволяє проаналізувати і реалізувати політику мережевої безпеки перш, ніж здійсниться спроба її порушення зовні або зсередини організації.

Засоби аналізу захищеності можуть функціонувати на мережевому рівні, рівні операційної системи (ОС) і рівні застосування. Вони можуть проводити пошук уразливостей, поступово нарощуючи число перевірок і "поглиблюючись" в інформаційну систему, досліджуючи усі її рівні.

Найбільшого поширення набули засоби аналізу захищеності мережевих сервісів і протоколів. Обумовлено це в першу чергу універсальністю використовуваних протоколів. Вивченність і повсюдне використання таких протоколів, як IP, TCP, HTTP, FTP, SMTP і тому подібне, дозволяють з високою мірою ефективності перевіряти захищеність інформаційної системи, що працює в мережевому оточенні.

Другими за поширеністю є засоби аналізу захищеності операційних систем. Обумовлено це також універсальністю і поширеністю деяких операційних систем (наприклад, UNIX і Windows NT). Проте, через те, що кожен виробник вносить до операційної системи свої зміни (як приклад можна привести велику кількість різновидів ОС UNIX), засоби аналізу захищеності ОС аналізують в першу чергу параметри, характерні для всього сімейства однієї ОС. І лише для деяких систем аналізуються специфічні для неї параметри.

Засобів аналізу захищеності застосувань на сьогодні не так вже багато. Такі засоби доки існують тільки для широко поширених прикладних систем типу: Web-браузери (Netscape Navigator, Microsoft Internet Explorer), СУБД (Microsoft SQL Server, Oracle) і тому подібне.

Застосування засобів аналізу захищеності дозволяє швидко визначити усі вузли корпоративної мережі, доступні у момент проведення тестування, виявити всі використовувані в мережі сервіси і протоколи, їх налаштування і можливості для несанкціонованої дії (як зсередини корпоративної мережі, так і зовні). За результатами сканування ці засоби виробляють рекомендації і покрокові заходи, що дозволяють усунути виявлені недоліки.

Цей метод контролю порушень політики безпеки не може замінити фахівця з інформаційної безпеки. Засоби аналізу захищеності можуть лише автоматизувати пошук деяких відомих уразливостей.