П'ять кроків процесу тестування на проникнення

1. Планування
   Тестувальник на проникнення збирає якомога більше інформації про цільову систему або мережу, її потенційні вразливості та експлойти для використання проти неї. Це передбачає проведення пасивної або активної розвідки (отримання відбитка, footprinting) та дослідження вразливості.
2. Сканування
   Тестувальник на проникнення проводить активну розвідку, щоб дослідити цільову систему або мережу та виявляти потенційні слабкі місця, які, якщо їх використовувати, можуть дати зловмиснику доступ. Активна розвідка може містити:
   * сканування портів для виявлення потенційних точок доступу до цільової системи
   * сканування вразливостей для виявлення потенційних уразливостей конкретної цілі, які можна використовувати
   * встановлення активного з'єднання з ціллю (перерахування) для ідентифікації облікового запису користувача, облікового запису системи та облікового запису адміністратора.
3. Отримання доступу
   Тестувальник на проникнення намагатиметься отримати доступ до цільової системи та перевіряти мережний трафік, використовуючи різні методи для експлуатації системи, зокрема:
   * запуск експлойту з корисним навантаженням в систему
   * злам фізичних бар'єрів для активів
   * соціальна інженерія
   * використання вразливостей веб-сайту
   * використання вразливостей програмного та апаратного забезпечення або неправильних конфігурацій
   * злам безпеки засобів контролю доступу
   * злам слабко зашифрованого Wi-Fi.
4. Підтримка доступу
   Тестувальник на проникнення підтримуватиме доступ до цілі, щоб з’ясувати, які дані та системи є вразливими для експлуатації. Важливо, щоб дії залишалися непоміченими, зазвичай використовуючи бекдори, троянські коні, руткіти та інші приховані канали, щоб приховати свою присутність.
   Коли ця інфраструктура буде створена, тестувальник на проникнення приступить до збору даних, які вважаються цінними.
5. Аналіз та звітність
   Тестувальник на проникнення надасть зворотній зв’язок за допомогою звіту, який рекомендує оновлення продуктів, політик та навчання для підвищення безпеки організації.

Коротко

- Знайдіть шляхи проникнення в мережу
- Визначте потенційні уразливі місця, які можна використовувати
- Використовуйте будь-які вразливості, виявлені в мережі, імітуючи атаку
- Зберіть якомога більше інформації, щоб вас не виявили

- Повідомте про свої висновки команді