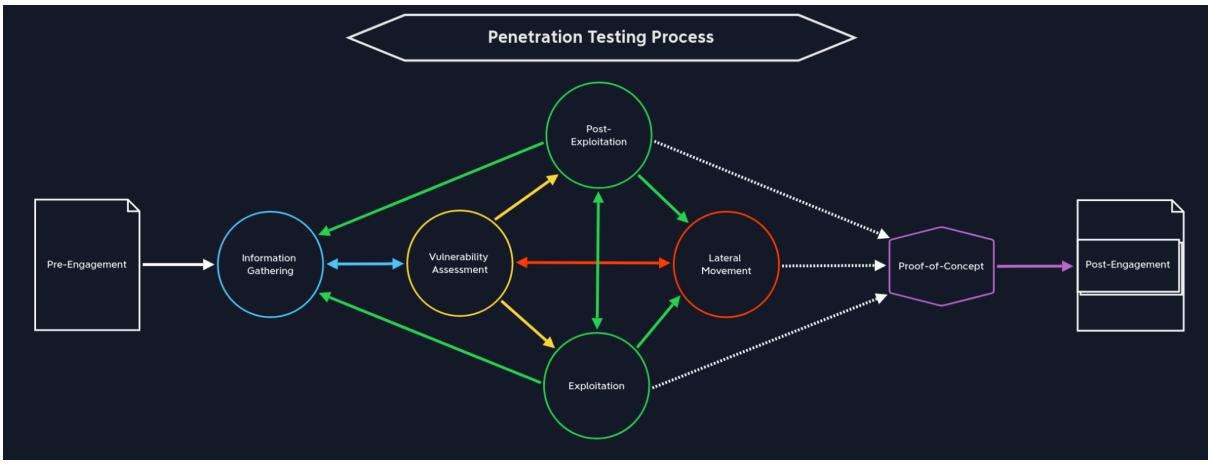
Этапы тестирования на проникновение

Представить и определить этапы тестирования на проникновение наиболее эффективным образом можно посредством взаимозависимых этапов. В наших исследованиях мы часто обнаруживаем, что эти процессы представлены в виде циклического процесса. Если мы рассмотрим это более внимательно и представим, что хотя бы один компонент этого циклического процесса не применяется, то весь процесс будет нарушен. Строго говоря, весь процесс терпит неудачу. Если предположить, что мы начинаем этот процесс с начала, но уже с новоприобретенной информацией, то это уже подход к новому процессу, который не отменяет предыдущий.

Проблема в том, что при таких представлениях и подходах зачастую не на что опереться для расширения нашего процесса тестирования на проникновение. Как мы уже обсуждали, нет пошагового руководства, которому можно следовать, но есть этапы, которые позволяют гибко варьировать и адаптировать отдельные шаги и подходы к результатам и информации, которые мы получаем. Мы можем разработать собственный план действий для различных вещей, которые мы пробуем на разных этапах тестирования на проникновение, но каждая среда отличается, и поэтому нам нужно постоянно адаптироваться.



Мы подробно рассмотрим каждый из этих этапов и изучим их особенности в следующих разделах, а также рассмотрим опциональный учебный план о том, как продвигаться в изучении множества тактик, техник и процедур (TTP), используя структуру, демонстрирующую, как каждый этап строится на основе предыдущего и может быть итеративным по своей сути. Сначала давайте рассмотрим основные компоненты процесса тестирования на проникновение и обсудим отдельные модули и их важность.

Этот опциональный учебный план основан на наборах модулей для каждого этапа, которые мы рекомендуем проработать перед переходом к следующему этапу. Мы проработаем различные фазы почти во всех модулях, систематически выполняя такие шаги, как сбор разведывательной информации, горизонтальное продвижение по сети и снятие информации из систем. Разделение модулей предназначено для фокусировки на теме, которая требует специфических знаний, которые нельзя пропускать. Пробелы в любых из этих знаний, даже если мы думаем, что знакомы с ними, могут привести к недопониманию или трудностям в ходе обучения. Соответственно, процесс тестирования на проникновение с его этапами выглядит следующим образом:

Предварительное взаимодействие

Предварительное взаимодействие - это информирование клиента и корректировка контракта. Все необходимые тесты и их компоненты строго определяются и прописываются в контракте. На личной встрече или во время общего созвона заключается множество договоренностей, таких как:

- Соглашение о неразглашении;
- Цели и задачи;
- Область применения;
- Оценка времени;
- Правила взаимодействия.