Моделирование атаки - тестрирование на проникновение. – Telegraph

telegra.ph/Modelirovanie-ataki---testrirovanie-na-proniknovenie-06-20

Life-Hack - Linux/Хакинг/Хакер/ИБ/Osint June 20, 2024

Один из наиболее эффективных способов обнаружения уязвимостей в системе безопасности до того, как возникнет возможность для хакеров, – это нанять профессионального пентестера для моделирования атаки на инфраструктуру компании.

Пентестер должен предпринять все доступные действия, чтобы имитировать настоящего злоумышленника, в некоторых случаях действуя в обстановке полной секретности, незаметно для ИТ-отдела и службы внутренней безопасности организации, пока не придет время опубликовать свой окончательный отчет. Данный вид проверки безопасности называется тестированием на проникновение. Конкретные методы и объем тестирования могут различаться в зависимости от потребностей клиента и возможностей компании заказчика. Воздействие пентестера может быть сосредоточено на веб-приложениях и мобильных приложениях, сетевой инфраструктуре, беспроводных устройствах, физических офисах и всем остальном, что вы можете придумать для атаки. В зависимости от условий они могут стремиться быть незамеченными или наоборот, получить максимум информации об уязвимостях за короткое время. Пентестеры могут использовать человеческий фактор (социальная инженерия), специально разработанный код эксплойта или даже копаться в мусорных баках клиента в поисках паролей для доступа. Все зависит от масштаба планируемого вторжения. Однако наиболее распространенный тип вторжения – тест на проникновение во внутреннюю сеть (internal network penetration test, INPT). Этот вид атаки моделирует угрозу, которую представляет для

организации злоумышленник с доступом к внутренней сети. В данном курсе мы постараемся раскрыть тему тестирования внутреннего периметра компании или, как ее еще называют, «внутрянка».

Планируя INPT, вы предполагаете, что злоумышленник смог успешно получить физический доступ в корпоративный офис или, возможно, получил удаленный доступ к рабочей станции сотрудника с помощью фишинга. Также возможно, что злоумышленник – действующий сотрудник компании, который прошел со своим пропуском через парадную дверь. Возможно, злоумышленник посетил офис в нерабочее время, представившись охранником, или в течение дня, представившись торговцем либо доставщиком цветов.

Существует бесчисленное множество способов получить физический доступ в офис, которые не вызовут особых затруднений. Во многих случаях злоумышленнику просто нужно пройти через главный вход и бродить по коридорам, вежливо улыбаясь любому, кто проходит мимо, и делая вид, что он разговаривает по мобильному телефону, пока он не обнаружит укромный уголок, где можно подключиться к розетке локальной сети. Профессиональные компании, предлагающие услуги высококлассного тестирования на проникновение, обычно дорого стоят, в результате для клиента, заказавшего пентест, зачастую дешевле пропустить эту творческую часть вторжения и с самого начала предоставить злоумышленнику физический доступ к внутренней сети компании.

Так или иначе, злоумышленнику удается проникнуть в корпоративную сеть. Каковы его дальнейшие действия и что он видит? Чаще всего у злоумышленника нет данных о внутренней сети, специального доступа или учетных данных. Все, что у него есть, – это доступ к сети, и обычно этого ему достаточно. Однако тесты на проникновение подразделяются на три категории:

- Тестирование по стратегии черного ящика. Как и большинство злоумышленников, белые хакеры не владеют полезной информацией о цели.
- Тестирование по стратегии серого ящика. Белые хакеры знают о системах и мерах безопасности цели. При этом типе теста на проникновение хакеры пытаются найти любые внутренние уязвимости, которые можно использовать.
- Тестирование по стратегии белого ящика. Белые хакеры обладают обширными знаниями обо всех системах, технологиях и инфраструктуре компании заказчика. Этот тип тестирования на проникновение занимает больше всего времени, поскольку с его помощью хакеры пытаются найти мельчайшие недостатки.

Пентест является незаменимым способом оценки и улучшения безопасности информационных систем. Регулярное тестирование помогает повысить уровень защиты и предотвратить возможные атаки злоумышленников.