HOW 2 HACK

TOP10 OF CYBERSECURITY ATTACKS

1. Malware
2. Phishing
3. Man-in-the-Middle (MitM) Attacks
4. Denial-of-Service (DOS) Attack
5. SQL Injections
6. Zero-day Exploit
7. Password Attack
8. Cross-site Scripting
9. Rootkits
10. Internet of Things (IoT) Attacks

https://www.cisco.com/c/en/us/products/security/security-reports.html

Анатомия хака

1. Сбор первоначальных разведывательных данных
2. Анализ полученной информации о цели
3. Выбор перспективных векторов для проникновения
4. Первоначальный взлом
5. Закрепление на взломанном объекте инфраструктуры
6. Сбор информации (файлы, сетевой трафик, данные ОС)
7. Продвижение по инфраструктуре
8. Закрепление на взломанных объектах инфраструктуры
9. Сбор доступной информации на регулярной основе

Сбор и анализ информации о цели

- Сбор и анализ данных из открытых источников (OSINT)
- Сбор разведывательных данных (RECON)
- Сбор и анализ приватной информации (форумы, чаты, Jabber)

Обработка открытых источников (OSINT)

Сбор информации о работниках (email, linkeind, VK, phone)

Поиск паролей в существующих утечках

Сбор информации о ПО используемом (госзакупки, метаинформация из файлов)

Сбор информации о сопредельных объектах (поставщики, службы доставки, соц связи)

Поиск исходного кода (github, GITLAB)

Сбор разведывательных данных (recon)

Поиск объектов инфраструктуры (локальные сетевые ресурсы, внешние сетевые ресурсы)

Построение топологии инфраструктуры (поддомены, сервисы)

Аудит безопасности объектов инфраструктуры в пассивном режиме (Сетевые порты, версии используемого ПО, информация об ошибках ПО)

ПРОНИКНОВЕНИЕ

Вирус

- Создание вирусной нагрузки
- Доставка и запуск вирусной нагрузки
- Получение доступа

Варианты доставки

- Отправка на почту, мессенджер, в службу поддержки (апдейты)
- Эмуляция HID устройства (Teensy)
- Подброс флешек, модемов
- Поддельная беспроводная сеть (Fake AP)
- Заражение устройств во время ремонта
- Заражение сопредельных объектов инфраструктуры (ноут секреташи)

Фишинг

- Клонирование объекта инфраструктуры или используемых сервисов (похожее доменное имя + внешнее сходство)
- Подготовка информационного поля для вброса
- Отправка ссылки в составе вброса
- Сбор логинов и паролей на ресурсе клоне
- Получение доступа

Человек по середине

- Организация врезки в проводную или беспроводную сеть
- Сбор и анализ сетевого трафика
- Получение логинов, паролей или сессий, ключей доступа
- Получение доступа

Отказ в обслуживании

- Определение критических мест в инфраструктуре обслуживаемых третье стороной
- Аренда серверных мощностей с учетом топологии инфраструктуры
- Организация максимальной нагрузки на объект инфраструктуры
- Отказ в обслуживании -> вызов третьей стороны
- Получение доступа от лица третьей стороны

SQL инъекции

Активное сканирование сервисов доступных из вне

Обнаружение сообщений об ошибке или зависаний системы

Выявление уязвимого параметра из запроса

Инъекция SQL запроса в уязвимый параметр

Получение доступа к БД

Уязвимость нулевого дня

Активное сканирование сервисов доступных из вне

Фаззинг данных передаваемых системе

Обнаружение сообщений об ошибке или зависаний системы

Создание эксплойта

Получение доступа с помощью эксплойта

Атака по паролю

- Проверка стандартных паролей к сервисам доступным из вне
- Использование паролей из утечек и полученных развед данных
- Перебор паролей к сервисам доступным из вне

КРОСС САЙТ СКРИПТИНГ

- Активное сканирование для выявления уязвимых параметров
- Подготовка XSS вектора
- Подготовка информационного поля для вброса
- Отправка XSS вектора и в составе вброса
- Сбор сессий из браузера пользователя
- Получение доступа

Руткиты

- Внедрение закладки в программное и аппаратное обеспечение
- Доставка внутрь периметра (поставщики, ремонт, разброс флешек)
- Получение доступа

Интернет вещей

- Поиск применения интернета вещей
- Определение связанных с ним сервисов
- Атаки на сервисы обработки данных от IoT (см. SQL, XSS)
- Получение доступа