????? ??????????

Определения

Фреймворк эксплуатации — платформа для создания и отладки эксплойтов. Кроме того, включает в себя базу опкодов, архив шеллкодов и информацию по исследованиям информационной безопасности.

Уязвимость нулевого дня — термин, обозначающий неустранённые уязвимости.

Шелл-код — двоичный исполняемый код, передающий управление консоли (/bin/sh, cmd.exe). Шелл-код может быть использован как полезная нагрузка эксплойта, обеспечивающая доступ к консоли.

Опкод — код, представляющий операцию или команду, выполняемую процессором компьютера. Он является непосредственной инструкцией для выполнения определенного действия, такого как сложение, умножение, сравнение и т.д.

Типовые проблемы сетевых сервисов:

- Проблемы конфигурации
- Слабые пароли
- Неиспользование шифрования
- Известные уязвимости

Этапы анализа сервисов:

- Поиск существующих сервисов
- Получение версий сервисов
- Поиск уязвимостей и эксплойтов для них
- Попытки использования эксплойтов

Поиск эксплойта

Популярные фреймворки эксплуатации:

- Metasploit Framework (Free): https://www.metasploit.com/
- CobaltStrike ($$$): https://www.cobaltstrike.com/
- Exploit Pack ($$$): http://exploitpack.com/
- Core Impact Pro ($$$): https://www.coresecurity.com/products/core-impact

Если есть эксплоит, то:

- разобраться в принципах его работы,
- изучить код эксплойта, прежде чем запускать его,
- донастроить\дописать эксплоит под свою задачу
- отладить его на своем локальном стенде
- применить эксплоит

Попытка использования эксплоита

Обязательно должна быть уверенность в:

- что будет делать эксплоит, как и почему это сработает;
- эксплоит не нарушит работоспособности системы и не изменит ее состояние существенно;
- эксплоит не содержит закладок и “логических бомб”, которые могут быть спрятаны туда злоумышленником;
- после выполнения эксплойта вам не придется применять его второй раз (подготовьтесь к закреплению доступа,
- убедитесь что вы решаете задачу за наименьшее число шагов)

Доп. информация

Практика:

- https://www.revshells.com/
- Платформа для самостоятельного решения задач и практик (раздел, посвященный метасплоит)
- Знакомство с метасплоит и документация
- Краткий курс об особенностях и деталях метасплоит от разработчиков
- Практика сборки и исследования уязвимых стендов
- Задачи на эксплуатацию уязвимостей разного рода, в т.ч. с применение готовых эксплойтов

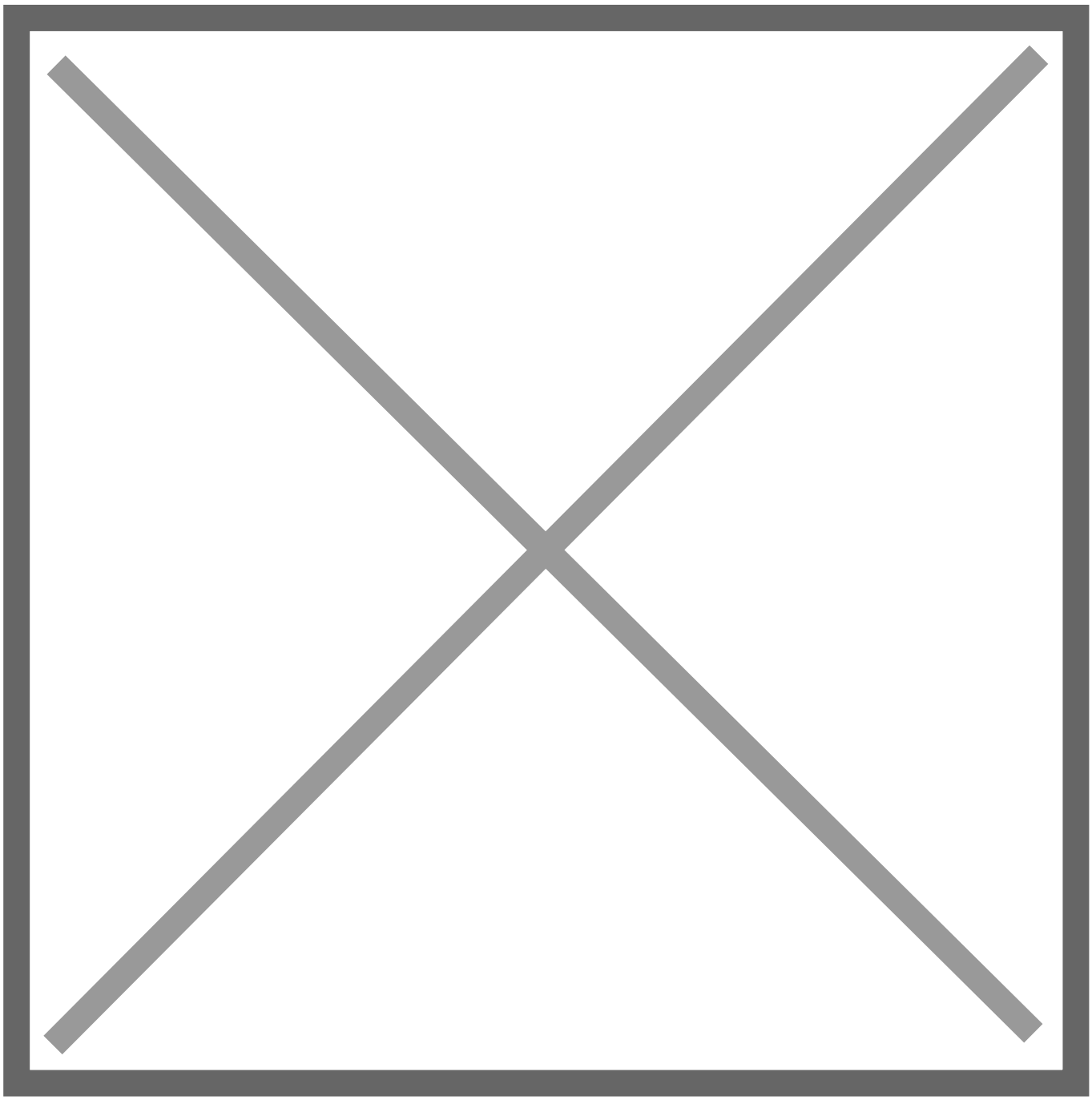
Теория:

- Nmap гайд

CheatSheets:

- Nmap все команды и флаги на 2023 г.

Хакерские инструменты:



Revision #5
Created 29 September 2025 14:48:18 by Admin
Updated 2 October 2025 07:11:35 by Admin