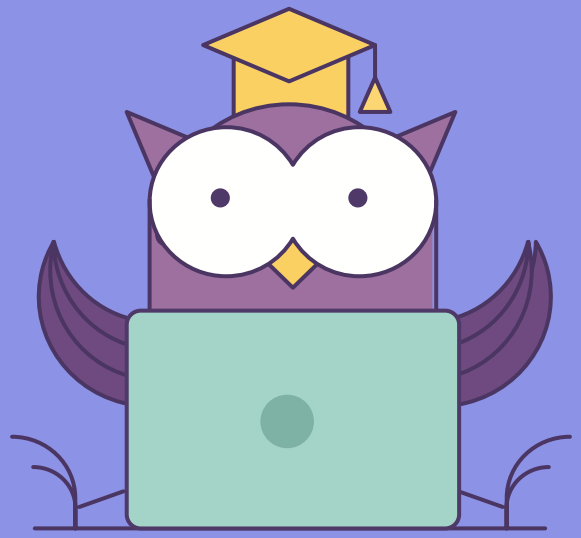
ОНЛАЙН-ОБРАЗОВАНИЕ

OTUS

«Инструментарий для проведения Pentest»

Колесников Александр Александрович

Меня хорошо слышно && видно?



Напишите в чат, если есть проблемы!

Ставьте + если все хорошо

Содержание

- Metasploit
  - Основные модули и структура
- Burp Suite
  - Функционал и настройка
  - Плагины и модули

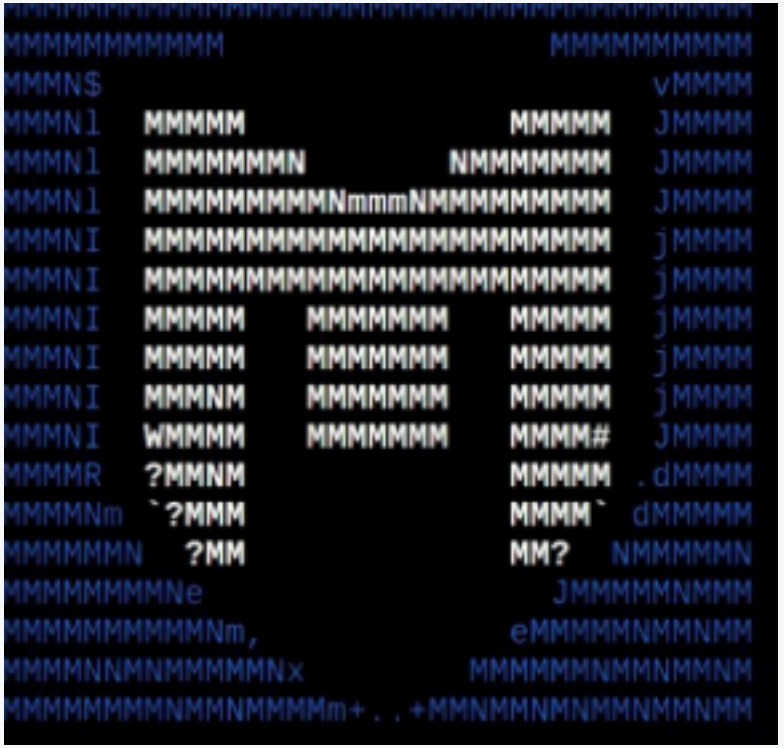
01

Metasploit

Metasploit

FrameWork и набор инструментов и скриптов для:

- Локальной эксплуатации
- Удаленная эксплуатации
- Подбора паролей
- Фаззинга
- IDS/IPS/Anti-AV обхода
- Атаки на веб приложения
- Сканирования и поиска уязвимостей
- Разработка эксплойтов



Metasploit компоненты

MSFCONSOLE

OTUS

- Консоль управления фреймворком

ПОЛЕЗНЫЕ КОМАНДЫ:

- **use** - выборка модуля для концигурации и использования
- **back** - завершить работу с модулем
- **set** - установить параметр модуля или фреймворка
- **search** - поиск модуля по заданному фильтру
- **check** - проверка работоспособности модуля
- **run** - запуск модуля alias для exploit
- **exploit** - запуск модуля эксплуатации
- **connect** - соединение с сервером (аналог netcat)
- **sessions** - контроль работы с активной сессией
- **show options advanced** - получение полного списка опций для модуля
- **show options** - показать основные опции для модуля

MSFVENOM

- **ИСПОЛНЯЕМЫЕ ФОРМАТЫ**

- Asp, aspx, aspx-exe, axis2, dll, elf, elf-so, exe, exe-only, exe-service, exe-small, hta-psh, jar, jsp, loop-vbs, macho, msi, msi-nouac, osx-app, psh, psh-cmd, psh-net, psh-reflection, vba, vba-exe, vba-psh, vbs, war.

- **ФОРМАТЫ**

- Bash, c, csharp, dw, dword, hex, java, js, js_be, js_le, num, perl, pl, powershell, ps1, py, python, raw, rb, ruby, sh, vbapplication, vbscript

MSFVENOM

- **Фильтр символов:**
  - -b ‘\x00\x0a’
- **Кодирование полезной нагрузки:**
  - -e xor
- **Количество циклов кодирования:**
  - -i 100500
- **Выбор шаблона для создания нагрузки:**
  - -x

METERPRETER

- Приложение, которое используется в качестве полезной нагрузки для эксплойтов.
- Имеет механизм расширения функционала за счет dll модулей
- Реализует свою работу посредством stager модулей
- Основной функционал и конфигурации подгружаются последовательно
- Работает по TLS протоколу
- Работает только в оперативной памяти
- Способен мигрировать из пространства скомпрометированного процесса

METERPRETER полезные команды

- **help** - информация о команде
- **clearev** - очистить журналы операционной системы
- **download** - загрузить файл из целевой системы
- **edit** - правка файла
- **execute** - выполнить команду на удаленном хосте
- **hashdump** - сдампить хэши паролей из оперативной памяти
- **migrate** - мигрировать в другой процесс
- **upload** - загрузка файла в удаленную систему
- **search** - поиск информации по файловой системе удаленного хоста

MSFCONSOLE DB, WORKSPACE

- **Workspace** - рабочее пространство, может содержать информацию о тестируемой системе
- **db_init** - инициализация базы данных для хранения информации
- **db_status** - проверка состояния соединения с базой данных
- **sessions** - взаимодействие с активными сессиями

02

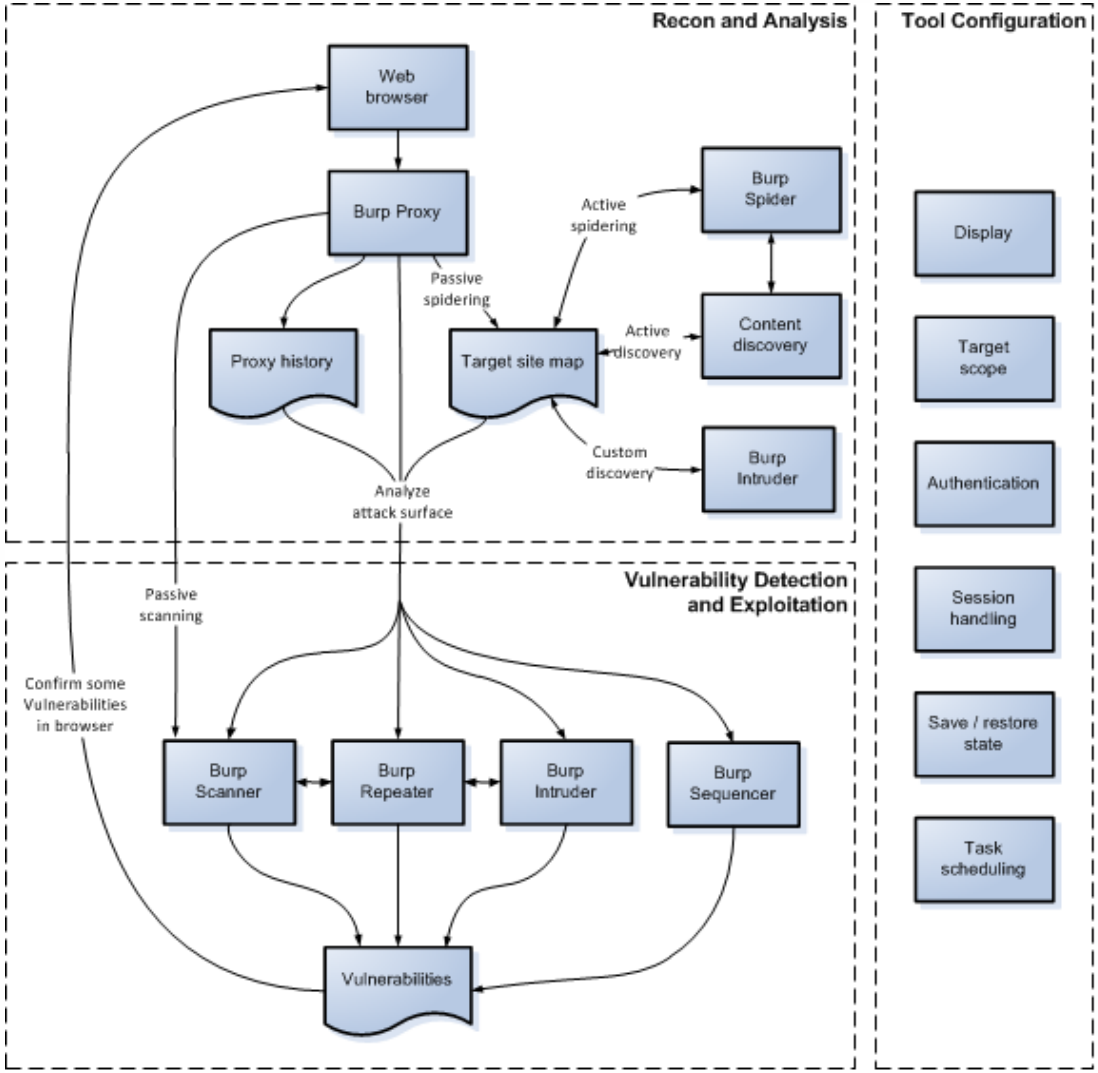
Burp Suite

Burp Suite

Приложение для тестирования web-приложений на уязвимости.

- **Модули:**
  - Scanner
  - Intruder
  - Repeater
  - Collaborator Client
  - Clickbandit
  - Sequencer
  - Decoder
  - Comparer
- **Общие типы уязвимостей, которые можно обнаружить:**
  - Уязвимости вводимых данных
  - Проблемы в логике, заложенной в алгоритм
  - Ошибки доступа

Использование



01

Practice

Колесников Александр

Спасибо
за внимание!