Payloads

Проверять на https://virustotal.com

Нагрузка (payload) — часть эксплойта, выполняющаяся после успешной эксплуатации уязвимости. Типы нагрузок:

- одиночные (Singles)
- комплексные (Stagers)
- поэтапные (Stages)

Например, windows/shell_bind_tcp представляет собой единую полезную нагрузку без этапа, тогда как windows/shell/bind_tcp состоит из этапа (bind_tcp) и этапа (shell).

Генерация полезной нагрузки

Переходим в payload. Генерация командой generate. Опции:

-E	Ускоренное кодирование
-b	Список символов для исключения '\x00\xff'. Например `msf  payload(shell_bind_tcp) > generate -b '\x00'` При большом наборе исключаемых символов возможна ошибка "Payload generation failed: No encoders encoded the buffer successfully.". Это означает, что не найден энкодер для данного набора.
-e	Энкодер По умолчанию происходит автоматический поиск наиболее подходящего энкодера. Выбор зависит от списка символов для исключения.
-i	Количество итераций энкодера.
-o	Разделенные запятыми параметры в виде парам=знач
-p	Платформа
-s	Количество добавляемых NOP
-f	Имя файла. По умолчанию вывод в консоль.
-t	Формат выходного файла: raw,ruby,rb,perl,pl,c,js_be,js_le,java,dll,exe,exe-small,elf,macho,vba,vbs,loop-vbs,asp,war
-x	Шаблон используемого исполняемого файла

-k	Сохранять функциональность используемого шаблона

Revision #4
Created 2 October 2025 02:08:29 by Admin
Updated 7 October 2025 06:37:07 by Admin