?????????????? MSF

Ресурсные скрипты

Аналог bash скриптов для msf. Текстовые файлы с расширением rc, выполняются консолью msf построчно. Можно создать скрипт из введенных команд

Запуск

Из существующего где-то файла:

```
msfconsole -r /path/to/script/attack.rc param1 param2
```

Их скрипты размещаются в /usr/share/metasploit-framework/scripts/resource

```
msf > resource /path/to/script param1 param 2
```

Можно сохранить последние введенные команды. ! ~ не работает, нужен полный путь !

```
msf > makerc /home/kali/lessons_ruby/myscript.rc
```

makerc запоминает, какие команды уже были сохранены. Поэтому если сразу же повторить предыдущую команду, то будет сообщение [-] No commands to save!

Добавление Ruby

В данные скрипты можно добавлять скрипты на Ruby:

```
workspace -a http_title
db_nmap -Pn -T4 -n -v -p 80 --open 192.168.33.0/24
use auxiliary/scanner/http/title
<ruby>
run_single("set RHOSTS #{framework.db.hosts.map(&:address).join(' ')}")
</ruby>
run
```

Скрипты расположены в /usr/share/metasploit-framework/scripts/resource

Вариант для python:

```
pip install pymetasploit3
```

Пример скрипта:

```
from pymetasploit3.msfrpc import MsfRpcClient

client = MsfRpcClient('your_password', port=55553)

# Запуск сканирования
scan = client.modules.use('auxiliary', 'scanner/portscan/tcp')
scan['RHOSTS'] = '192.168.1.1-100'
scan['PORTS'] = '1-1000'
scan['THREADS'] = '20'

result = scan.execute()
print(result)

# Получение результатов из БД
for host in client.db.hosts():
    print(f"Host: {host['address']}")
    for service in client.db.services(host['address']):
        print(f"  Port: {service['port']}/{service['proto']} - {service['state']}")
```

Revision #2
Created 2 October 2025 05:18:45 by Admin
Updated 1 November 2025 07:21:19 by Admin