ПРЕЗЕНТАЦИЯ НА ТЕМУ: **ШЕЛЛКОДИНГ**

Студента: Беляева И.Р
1 курс
Факультет:
Информационная безопасность

ПОНЯТИЯ ФИГУРИРУЮЩИЕ В ТЕМЕ

Shell-программирование

Exploit(эксплоит)

Интерпретатор

Интерпретация

Back door(бэкдор)

DATA ENCODING, ИЛИ ШИФРОВАНИЕ КАК ИСКУССТВО

- Для скрытия присутствия вируса в системе применяются различные техники и методы, к примеру использование rootkits или bootkits.
- **Rootkits-** Набор ПО скрывающих присутствие запущенного malware-кода в целевой системе.
- **Bootkits-** Уникальный метод реализации руткитов — модификацию загрузочной записи MBR и загрузку руткита до старта ядра операционной системы.
- Задача- усложнить вирусному аналитику анализ образца малваря, когда он уже попал в антивирусную лабораторию. Это позволяет оттянуть время до того, как сигнатуру малваря добавят в антивирусные базы.
- Один из вариантов — шифрование собственного кода малвари, называемое обфускацией

АЛГОРИТМЫ ШИФРОВАНИЯ

- Кодирование для отдельных байтов блока с помощью функций ADD и SUB.
- ROR- и ROL-инструкции позволяют перевернуть несколько битов в байте справа или слева. Они должны использоваться вместе, поскольку они необратимы, то есть выполняются только в одну сторону.
- ROT — это оригинальный шифр Цезаря. Обычно используется латинский алфавит (A–Z и a–z), начиная с любой буквы, или 94 печатных символа в стандартной кодировке символов **ASCII**.
- Многобайтовые преобразования заключаются в том, что заменяется не один байт, данный алгоритм позволяет использовать больше ключевых значений (к примеру, часто берутся цепочки 4 или 8 байт длиной).

Внедрение Shell-code.Теория

- Шелл-код- часть кода, встроенного в малварь и позволяющего после инфицирования системы жертвы получить доступ к командной оболочке.
- Зачем все это нужно? мало просто инфицировать систему, проэксплуатировать уязвимость или положить какую-нибудь системную службу. Все эти действия черных и серых шляп(хакеров) во многих случаях нацелены на получение админского доступа к зараженной машине. Так что малварь — это всего лишь способ попасть на машину и получить shell, то есть управление. А это уже прямой путь к сливу конфиденциальной информации, созданию ботнет-сетей, превращающих целевую систему в зомби, или просто выполнению иных деструктивных функций на взломанной машине.
- Шелл-код внедряется в память программы, после чего на него передается управление при помощи использования программных ошибок, таких как переполнение стека или переполнение буфера в куче, или использования атак форматной строки. Управление шелл-коду передается перезаписью адреса возврата в стеке адресом внедренного шелл-кода, перезаписью адресов вызываемых функций или изменением обработчиков прерываний. Результатом всего этого и будет выполнение шелл-кода, который открывает командную строку для использования взломщиком.

- При эксплуатации удаленной уязвимости (exploit) шелл-код может открывать на уязвимом компьютере заранее заданный порт TCP для дальнейшего удаленного доступа к командной оболочке. Такой код называется ***привязывающим к порту***. Если же шелл-код подключается к порту компьютера атакующего (с целью обхода брандмауэра или просачивания через NAT), то такой код называется ***обратной оболочкой***.(NAT-это механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса транзитных пакетов)

- **Существуют два способа запуска шелл-кода в память на исполнение:**
- Метод position-independent code (PIC) — это код, который использует жесткую привязку бинарного кода к определенному адресу или данным. Шелл-код — это по сути PIC. Почему привязка так важна? Шелл не может знать, в каком именно месте оперативной памяти будет располагаться, поскольку во время выполнения различных версий скомпрометированной программы или малвари они могут загрузить шелл-код в разные ячейки памяти.
- Метод Identifying Execution Location заключается в том, что шелл-код должен разыменовать базовый указатель при доступе к данным в позиционно независимой структуре памяти.

ОБНАРУЖЕНИЕ ШЕЛЛ-КОДА НА ВЗЛОМАННОЙ МАШИНЕ

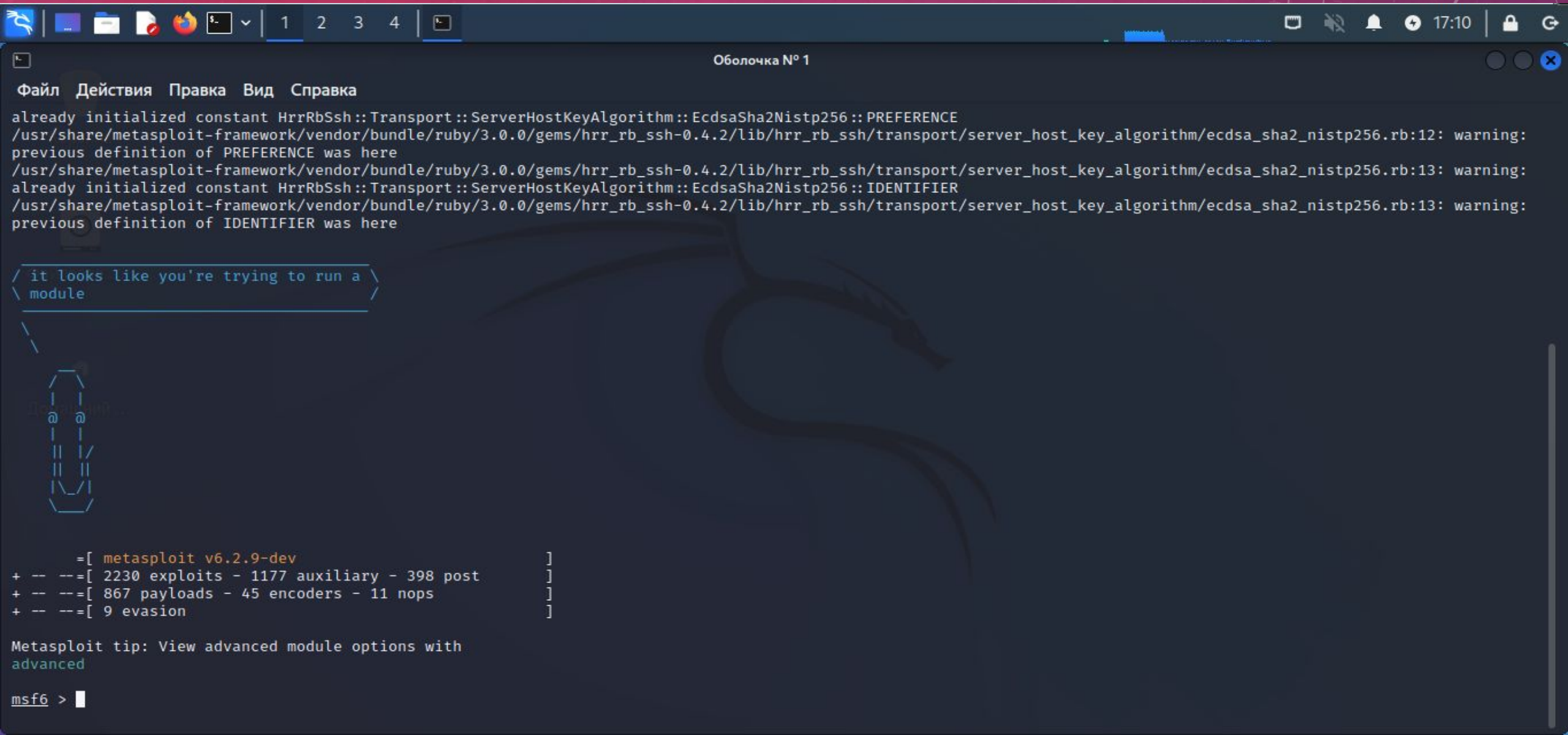
- Хакеры, дорожащие своей свободой и репутацией, пишут шелл-коды, используя техники, скрывающие их атаку. Так, типичная система обнаружения вторжений (англ. IDS) обычно просматривает весь входящий сетевой трафик в поисках структуры, специфичной для шелл-кода. Если IDS находит такую структуру, то пакет, содержащий эту сигнатуру, уничтожается до того, как он еще достигнет своей цели. Однако слабая позиция IDS состоит в данном случае в том, что если трафик закодирован, то распознать его не удастся.

Практика:

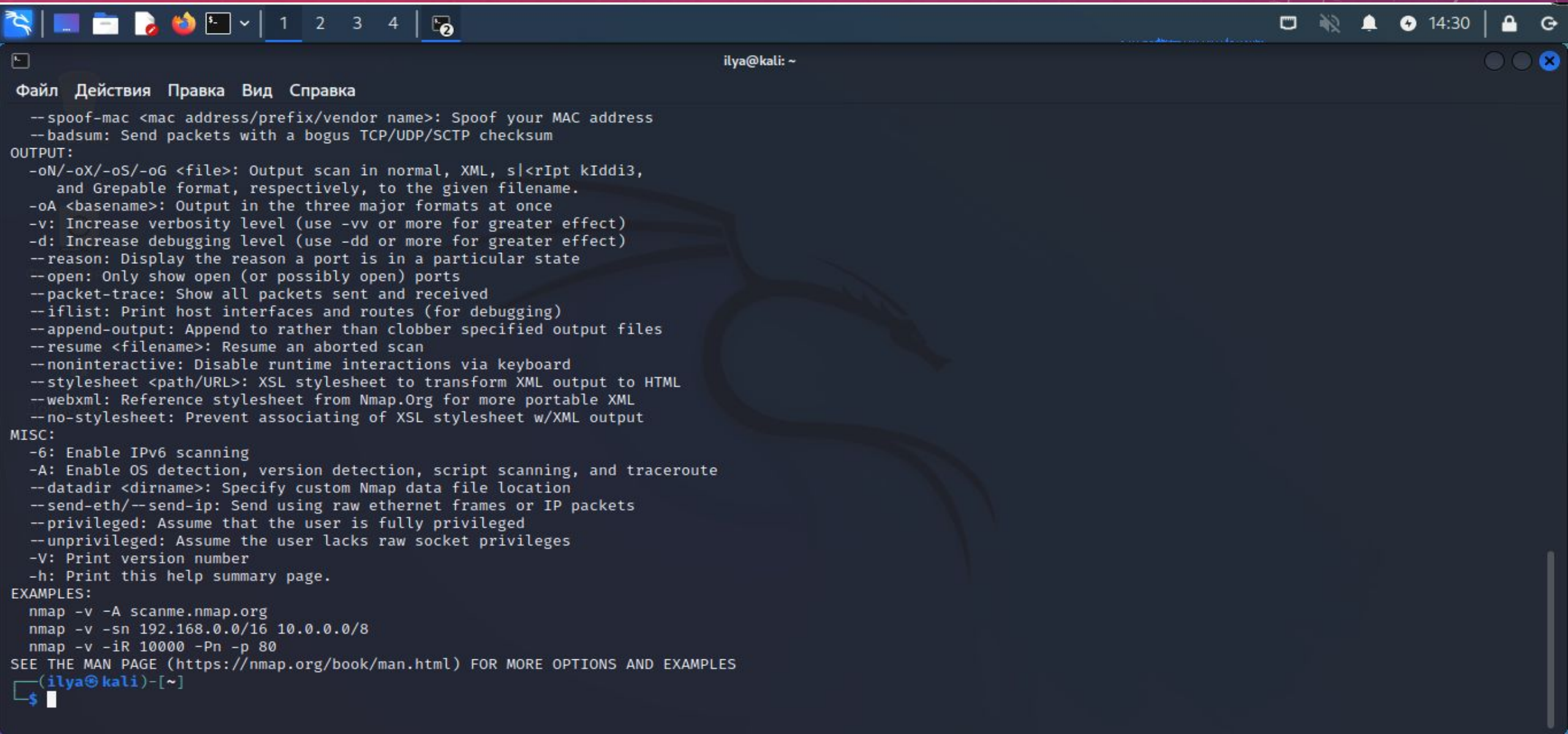
Для шелл-кодинга мы будем использовать:

1. **MetaSploit Framework**
2. **Nmap scanner**
3. **OS: Linux(в нашем случае Kali Linux)**

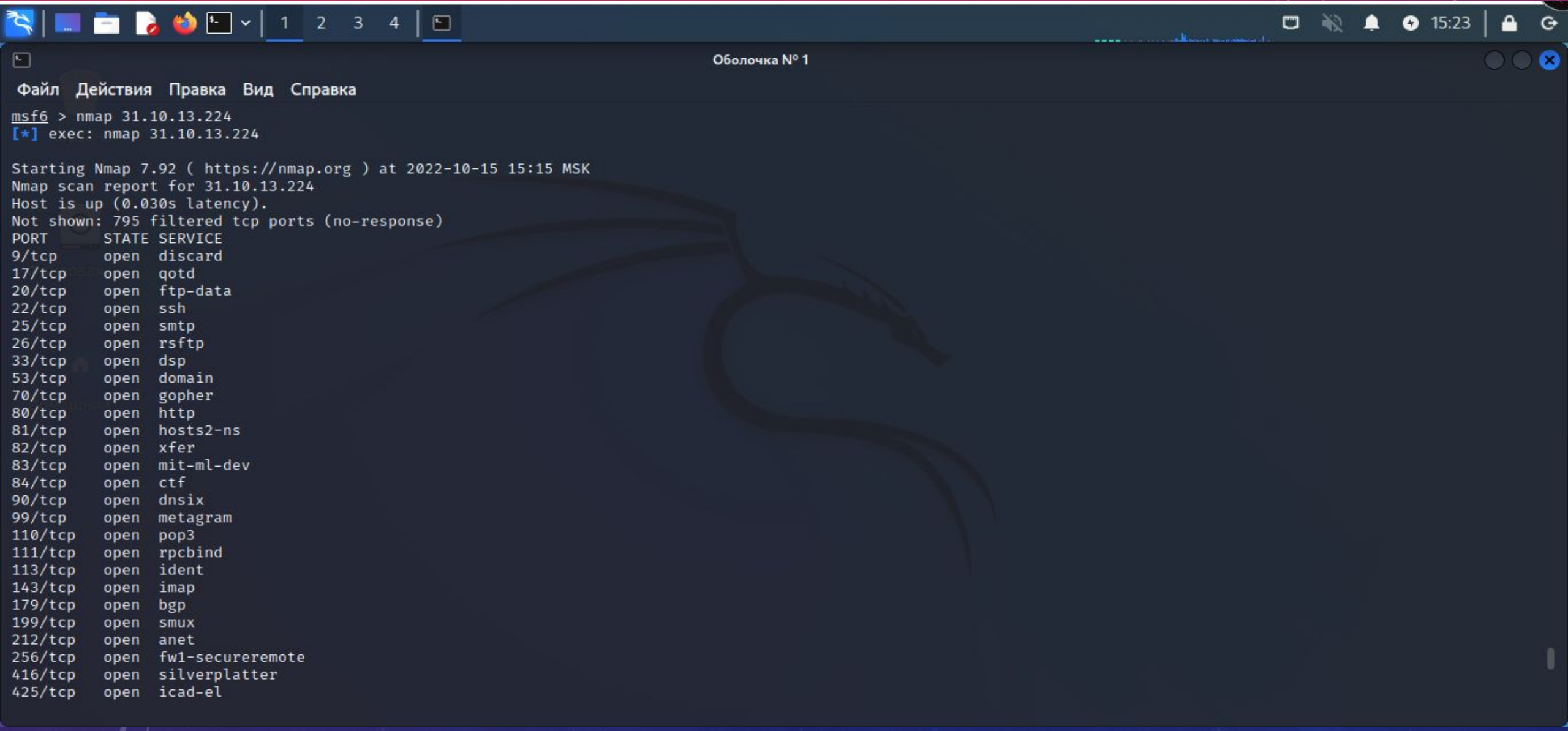
Как выглядит MetaSploit Framework:



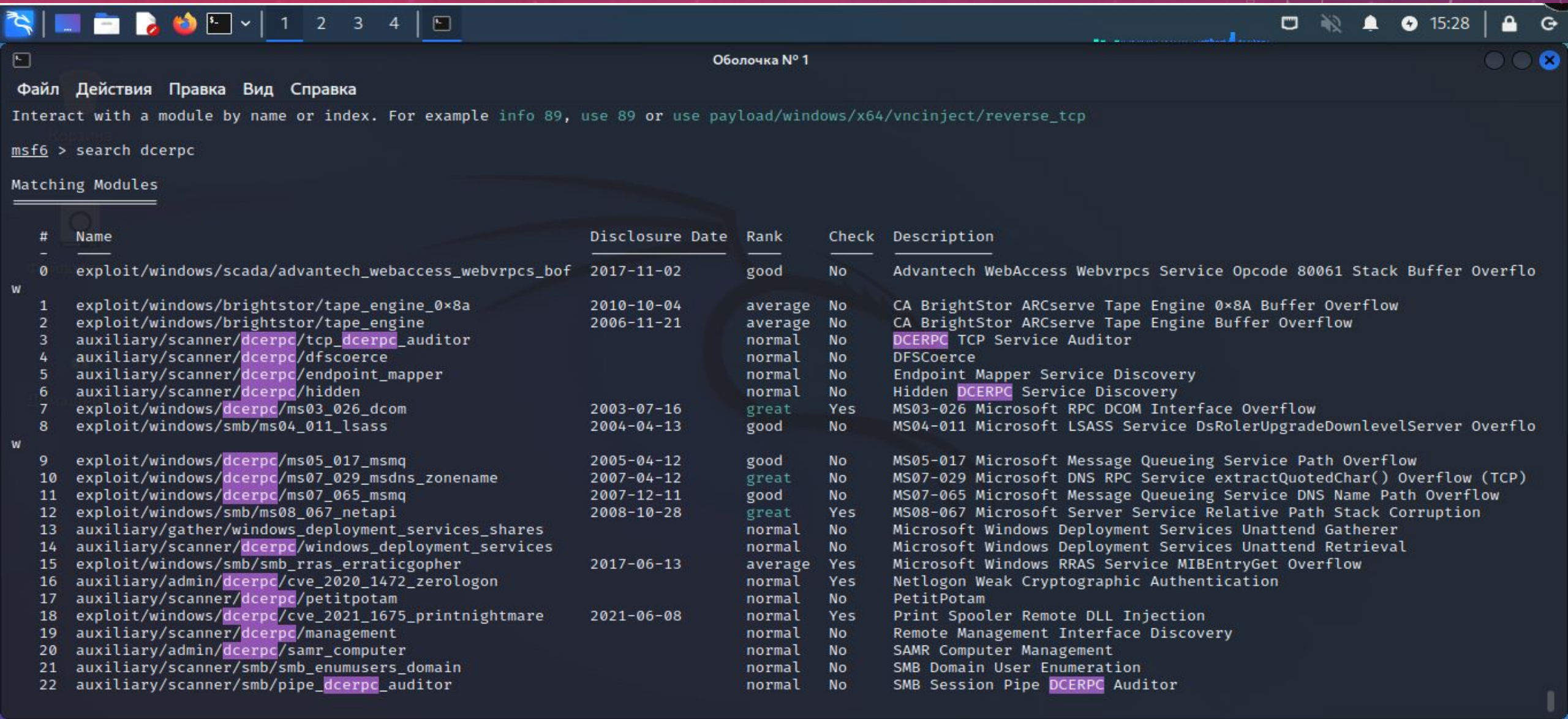
Как выглядит NMAP scaner:



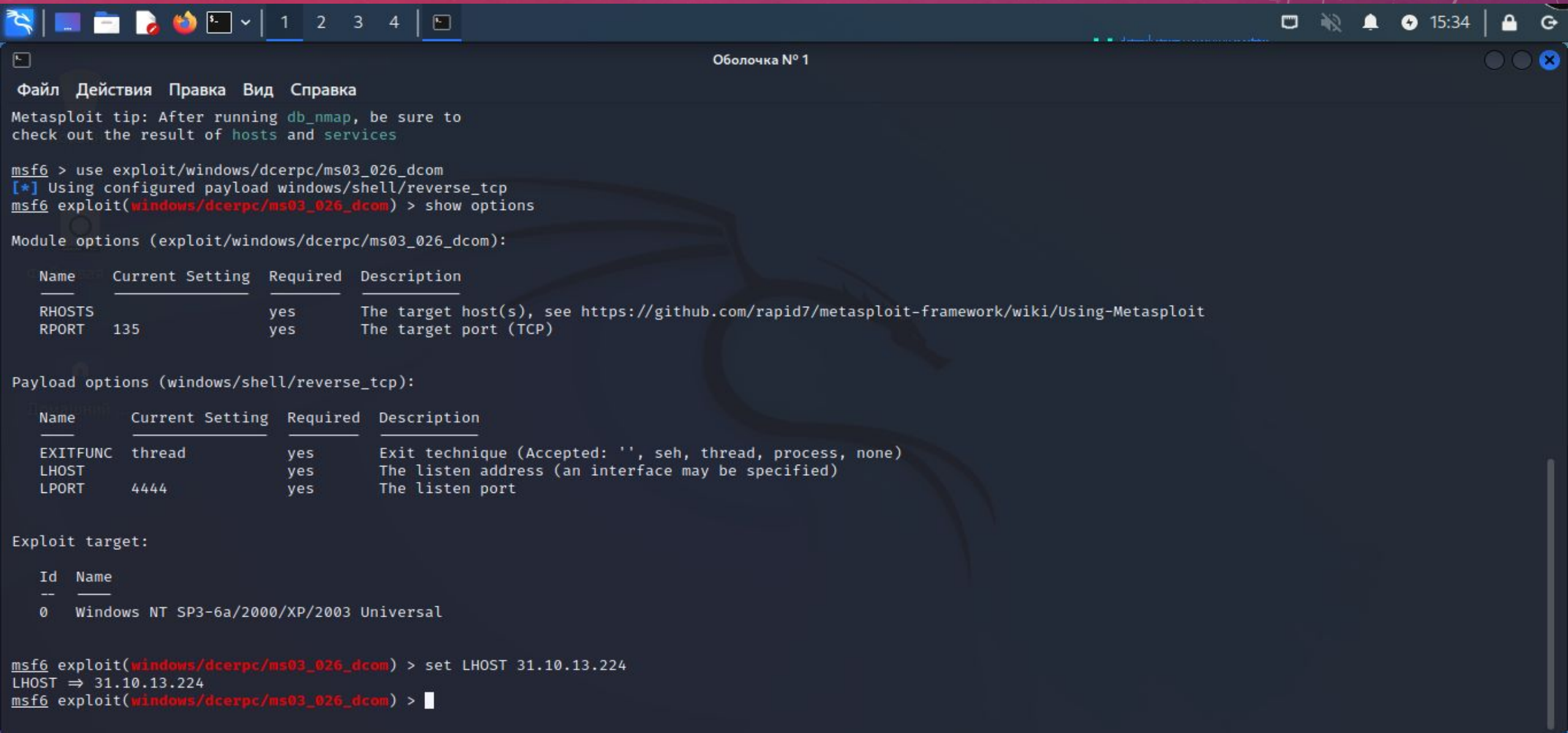
ПРАКТИКА: 1.Сканируем порты с помощью NMAP



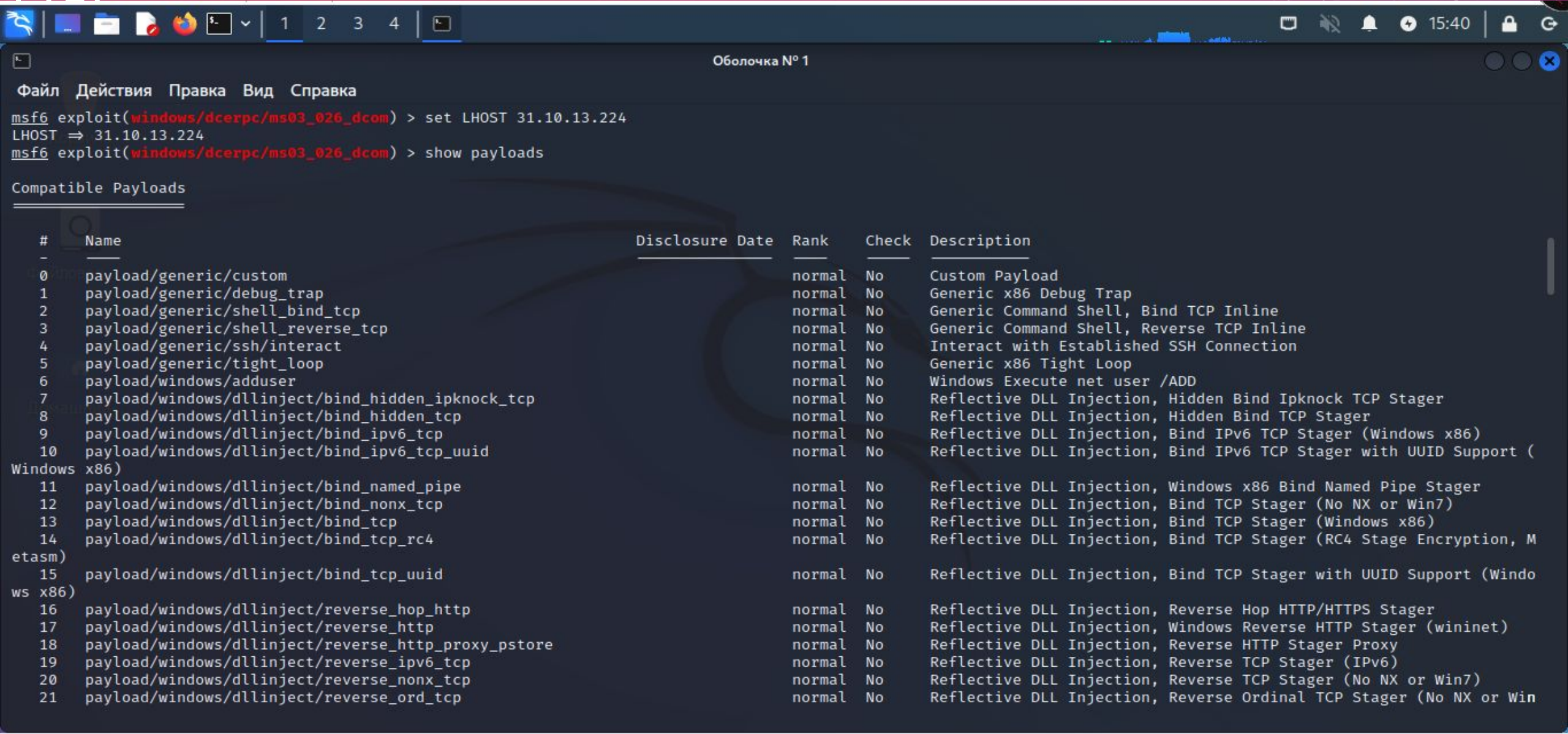
2.Ищем открытые порты в базе MetaSploit (ранг эксплоита важен)+важно изучить требования эксплоита, описание, цели)



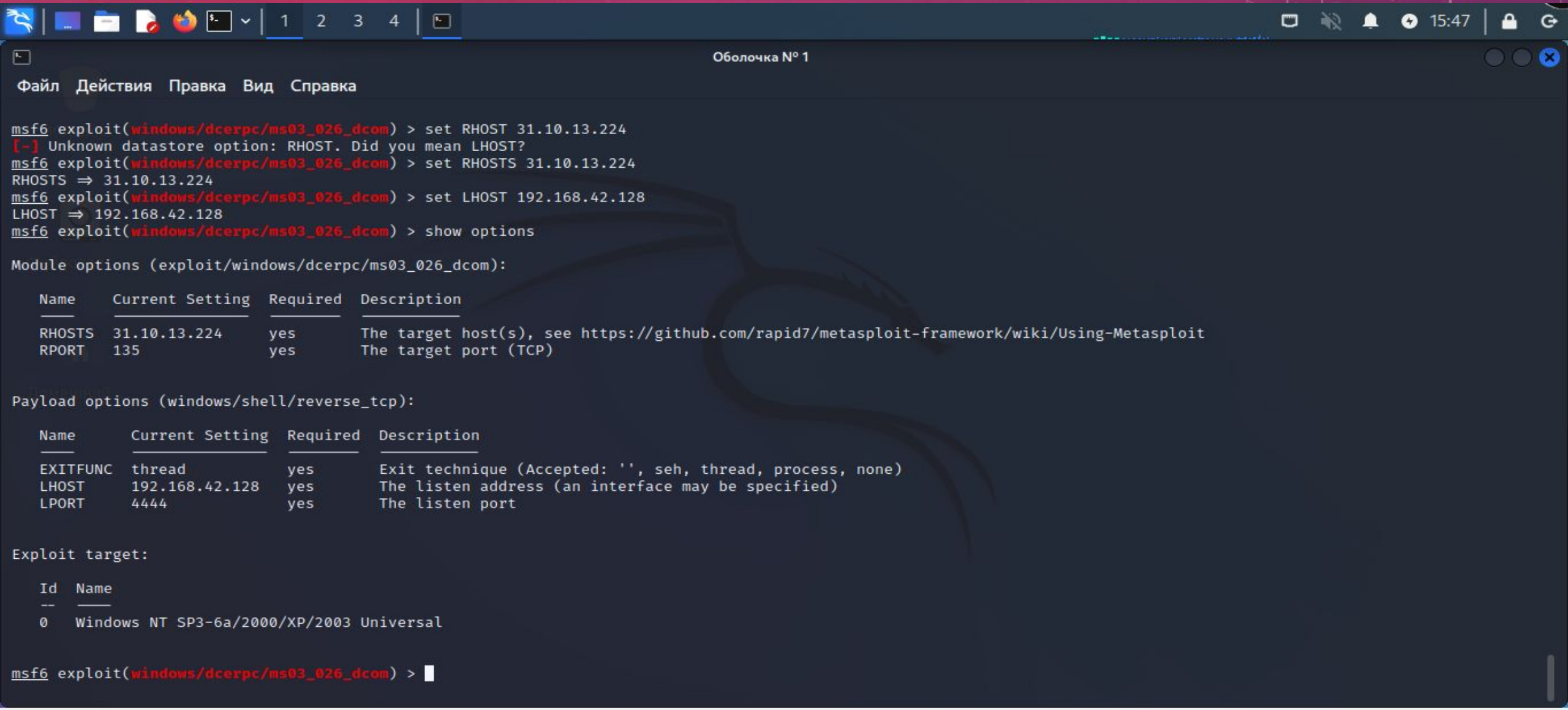
3.Применяем эксплоит, меняем конфигурацию, ip атакуемой машины



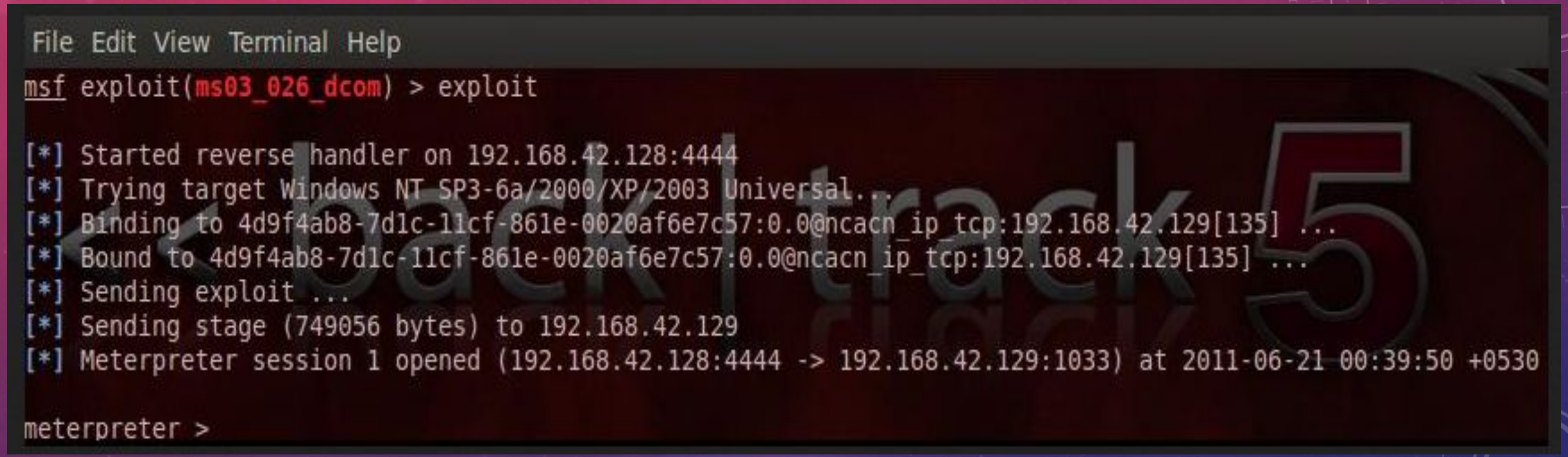
4.Ищем совместимый PayLoads(жесткая привязка-метод PIC)



5.Применяем PayLoad (в нашем случае-meterpreter)+меняем в конфиге локальный ip



6.Запускаем эксплоит



Таким образом, мы успешно использовали **Metasploit** фреймворк для получения доступа к удаленному серверу с запущенным на нем Windows 2003 Server. Мы предоставили себе возможность выполнять команды в командной оболочке, что дает нам право полностью контролировать удаленную машину и запускать любые задачи на ней.

СПАСИБО ЗА ВНИМАНИЕ!