Сбор информации: 2 Часть. – Telegraph

telegra.ph/Sbor-informacii-2-CHast-06-23

Life-Hack - Linux/Хакинг/Хакер/ИБ/Osint June 23, 2024

В данной статье мы сосредоточимся на рассмотрении популярных скриптов Nmap, которые сильно упрощают процесс тестирования на проникновение. Один из наиболее эффективных и широко используемых скриптов - smb-os-discovery.nse. Это NSE-скрипт (Nmap Scripting Engine), используемый для определения операционной системы на удаленных хостах, работающих через протокол SMB (Server Message Block). Это сетевой протокол, обеспечивающий возможность общего доступа к файлам, принтерам и другим ресурсам в сети.

Этот скрипт может быть полезен для администраторов и инженеров безопасности, когда требуется определить ОС хоста для более точной настройки безопасности или планирования изменений в инфраструктуре.

Для запуска скрипта необходимо воспользоваться параметром "--script smb-os-discovery.nse" в командной строке Nmap. Пример команды:

```
nmap -p 139,445 --script smb-os-discovery <target>
```

Результатом работы smb-os-discovery.nse будет информация об операционной системе, имя компьютера, домен, рабочая группа (имя рабочей группы является взаимоисключающим с именем домена) и текущее системное время. Это делается путем запуска сеанса с анонимной учетной записью (или с правильной учетной записью пользователя, если таковая предоставлена). В ответ на начало сессии сервер отправит обратно всю эту информацию.

```
nmap -p 445 --script smb-os-discovery 192.168.1.0/24

Starting Nmap 6.46 ( http://nmap.org ) at 2014-09-24 23:32 EST

Nmap scan report for test1 (192.168.1.115)
Host is up (0.0035s latency).
PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.6.3)
|   Computer name: ubuntu003
|   NetBIOS computer name:
|   Domain name:
|   FQDN: ubuntu003
|_  System time: 2014-09-24T23:34:41+10:00

Nmap scan report for 192.168.1.101
Host is up (0.018s latency).
PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: test-xp3
|   NetBIOS computer name: TEST-XP3
|   Workgroup: WORKGROUP
|_  System time: 2014-09-24T23:33:01+01:00
```

Например, при сканировании с использованием этого скрипта, вы можете узнать, что удаленный хост работает под управлением Windows 7 или Windows Server 2016. Эта информация может послужить отправной точкой для оценки уязвимостей, планирования обновлений программного обеспечения или улучшения общей безопасности сети.

Следующий полезный скрипт - smb-vuln-ms17-010.nse. С его помощью можно определить, уязвим ли сервер Microsoft SMBv1 к уязвимости удаленного выполнения кода (CVE-2017-0143, также известной как EternalBlue). Уязвимость активно эксплуатируется программами-вымогателями WannaCry и Petya, а также другими вредоносными программами.

```
nmap -p445 --script smb-vuln-ms17-010 <target>
```

Сценарий подключается к $IPC, выполняет транзакцию в FID 0 и проверяет, возвращается ли ошибка "STATUS_INSUFF_SERVER_RESOURCES", чтобы определить, уязвим ли данный сервер. Кроме того, он проверяет наличие известных кодов ошибок, возвращаемых исправленными системами. Протестировано на Windows XP, 2003, 7, 8, 8.1, 10, 2008, 2012 и 2016.

pop3-ntlm-info - сценарий перечисляет информацию из удаленных служб POP3 с включенной проверкой подлинности NTLM. Отправка запроса на проверку подлинности POP3 NTLM с нулевыми учетными данными приведет к тому, что удаленная служба ответит сообщением NTLMSSP, раскрывающим информацию: NetBIOS, DNS и версию сборки ОС.

```
nmap -p 110,995 --script pop3-ntlm-info <target>
```

```
110/tcp   open     pop3
| pop3-ntlm-info:
|   Target_Name: ACTIVEPOP3
|   NetBIOS_Domain_Name: ACTIVEPOP3
|   NetBIOS_Computer_Name: POP3-TEST2
|   DNS_Domain_Name: somedomain.com
|   DNS_Computer_Name: pop3-test2.somedomain.com
|   DNS_Tree_Name: somedomain.com
|_  Product_Version: 6.1.7601
```

nbstat.nse - пытается получить NetBIOS-имена и MAC-адрес целевого объекта. По умолчанию скрипт отображает имя компьютера и вошедшего в систему пользователя; Если уровень детализации повышен, отображаются все имена, которые, по мнению системы, ей принадлежат.

```
sudo nmap -sU --script nbstat.nse -p137 <host>
```

```
Host script results:
|_ nbstat: NetBIOS name: WINDOWS2003, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:c6:da:f5

Host script results:
|  nbstat: NetBIOS name: WINDOWS2003, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:c6:da:f5
|  Names:
|    WINDOWS2003<00>      Flags: <unique><active>
|    WINDOWS2003<20>      Flags: <unique><active>
|    SKULLSECURITY<00>    Flags: <group><active>
|    SKULLSECURITY<1e>    Flags: <group><active>
|    SKULLSECURITY<1d>    Flags: <unique><active>
|    \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
```

Использование скриптов поможет сэкономить время и автоматизировать вашу работу. Более подробно познакомиться с изобилием скриптов можно по ссылке: https://nmap.org/nsedoc/scripts/