1.通过本地PC中渗透测试平台Kali对靶机场景Server1进行系统服务及版本扫描渗透测试，以xml格式向指定文件输出信息（使用工具Nmap），将以xml格式向指定文件输出信息必须要使用的参数作为Flag值提交；

nmap -n -Pn -sS -A -oX target 172.16.1.0/24 扫描局域网中存活的靶机，并导出为xml格式，由于扫描的速度很慢，我们这里这针对靶机一个ip进行扫描

```
┌──(root💀kali2021)-[/var/www/html]
└─# nmap -n -Pn -sS -A -oX target 192.168.1.26
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2022-06-30 10:44 CST
Nmap scan report for 192.168.1.26
Host is up (0.00042s latency).
Not shown: 991 closed ports
PORT     STATE SERVICE      VERSION
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds Windows 7 Ultimate 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROU
P)
1025/tcp open  msrpc        Microsoft Windows RPC
1026/tcp open  msrpc        Microsoft Windows RPC
1027/tcp open  msrpc        Microsoft Windows RPC
1028/tcp open  msrpc        Microsoft Windows RPC
1036/tcp open  msrpc        Microsoft Windows RPC
1086/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:E6:65:F5
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_serve
r_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:wind
ows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows
8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: WIN-N4MI1AI4PS1; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Flag: oX

2.在本地PC的渗透测试平台Kali中，使用命令初始化MSF数据库并将此命令作为Flag值提交；

使用命令msfdb init 初始化msf数据库

```
root@kali:~# msfdb init
A database appears to be already configured, skipping initialization
root@kali:~#
```

Flag:msfdb init

3. 在本地 PC 的渗透测试平台 Kali 中，打开 MSF，使用 db_import 将扫描结果导入到数据库中，并查看导入的数据，将查看该数据要使用的命令作为 Flag 值提交；

首先使用命令 msfconsole 打开渗透测试平台

```
root@Kali:~# msfconsole

# cowsay++
 ______________
< metasploit >
 --------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||--|| *


       =[ metasploit v4.16.48-dev                         ]
+ -- --=[ 1749 exploits - 1002 auxiliary - 302 post       ]
+ -- --=[ 536 payloads - 40 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```

然后使用命令 db_import /root/target，导入之前扫描后导入到 xml 文件的的结果

```
msf > db_import /root/target
[*] Importing 'Nmap XML' data
[*] Import: Parsing with 'Nokogiri v1.8.1'
[*] Importing host 172.16.1.6
[*] Successfully imported /root/target
msf >
```

再使用命令 services 查看所导入的数据

```
172.16.1.6       21     tcp    ftp            open    Microsoft ftpd
172.16.1.6       23     tcp    telnet         open    Microsoft Windows XP telnetd
172.16.1.6       80     tcp    http           open    Microsoft IIS httpd 6.0
172.16.1.6       135    tcp    msrpc          open    Microsoft Windows RPC
172.16.1.6       139    tcp    netbios-ssn    open    Microsoft Windows netbios-ssn
172.16.1.6       1026   tcp    msrpc          open    Microsoft Windows RPC
172.16.1.6       1027   tcp    msrpc          open    Microsoft Windows RPC
172.16.1.6       1433   tcp    ms-sql-s       open    Microsoft SQL Server 2005 9.00.1399.00; RTM
172.16.1.6       2383   tcp    ms-olap4       open
172.16.1.6       3389   tcp    ms-wbt-server  open    Microsoft Terminal Service
```

最后使用命令 hosts 查看主机的数据

```
msf > hosts

Hosts
=====

address          mac                name     os_name          os_flavor  os_sp  purpose  info  comments
-------          ---                ----     -------          ---------  -----  -------  ----  --------
172.16.1.1       00:0c:29:70:e3:20           Windows 2003                       server
172.16.1.4       00:0c:29:13:25:ff           ESXi                        5.X    device
172.16.1.6       52:54:00:45:ab:4b           Windows XP                         client
172.16.1.8       00:0c:29:c4:80:0e           Linux                       2.6.X  server
```

Flag: hosts

4. 在 MSF 工具中用 search 命令搜索 CVE-2019-0708 漏洞利用模块，将回显结果中的漏洞公开时间作为 Flag 值（如：2017-10-16）提交；

```
msf6 > search cve-2019-0708

Matching Modules
================

   #  Name                                          Disclosure Date  Rank    Check  Description
   -  ----                                          ---------------  ----    -----  -----------
   0  auxiliary/scanner/rdp/cve_2019_0708_bluekeep  2019-05-14       normal  Yes    CVE-2019-0708 BlueKeep Microsoft Remote Desktop RCE Check
   1  exploit/windows/rdp/cve_2019_0708_bluekeep_rce  2019-05-14     manual  Yes    CVE-2019-0708 BlueKeep RDP Remote Windows Kernel Use After Free
```

Flag:2019-05-14

5. 在 MSF 工具中调用 CVE-2019-0708 漏洞攻击模块，并检测靶机是否存在漏洞，将回显结果中最后一个单词作为 Flag 值提交。

```
msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > check

[+] 172.16.1.200:3389     - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
[+] 172.16.1.200:3389 - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) >
```

Flag:channel