目录

伍济鹏 10.22 号备赛总结

总结前言

我会用写博客的方式写总结，我认为

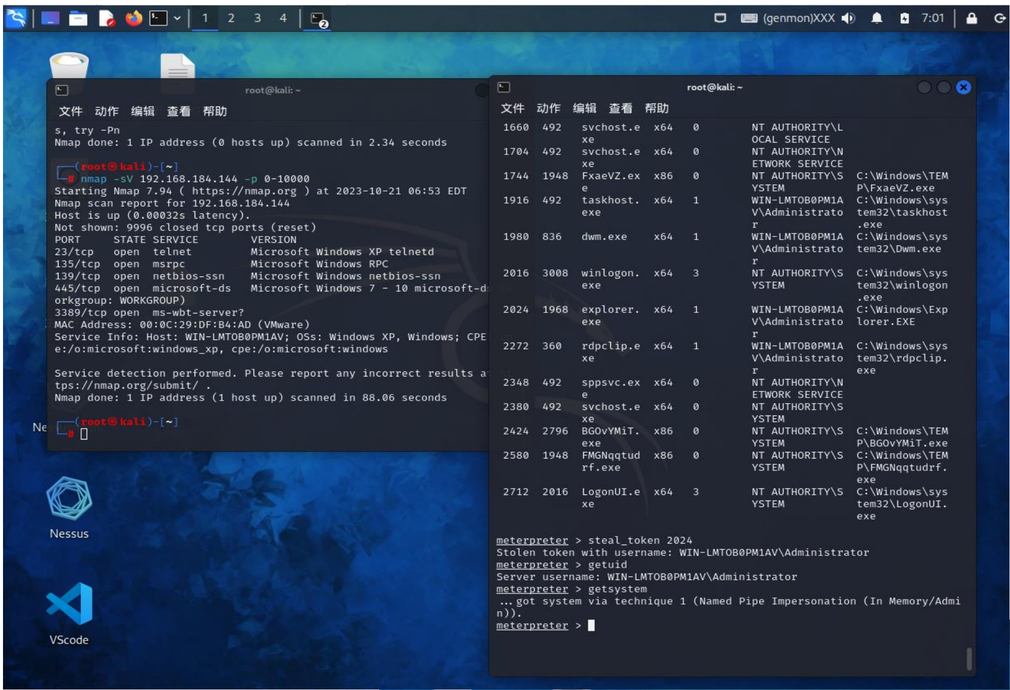
“教别人学习是最好的学习方法”

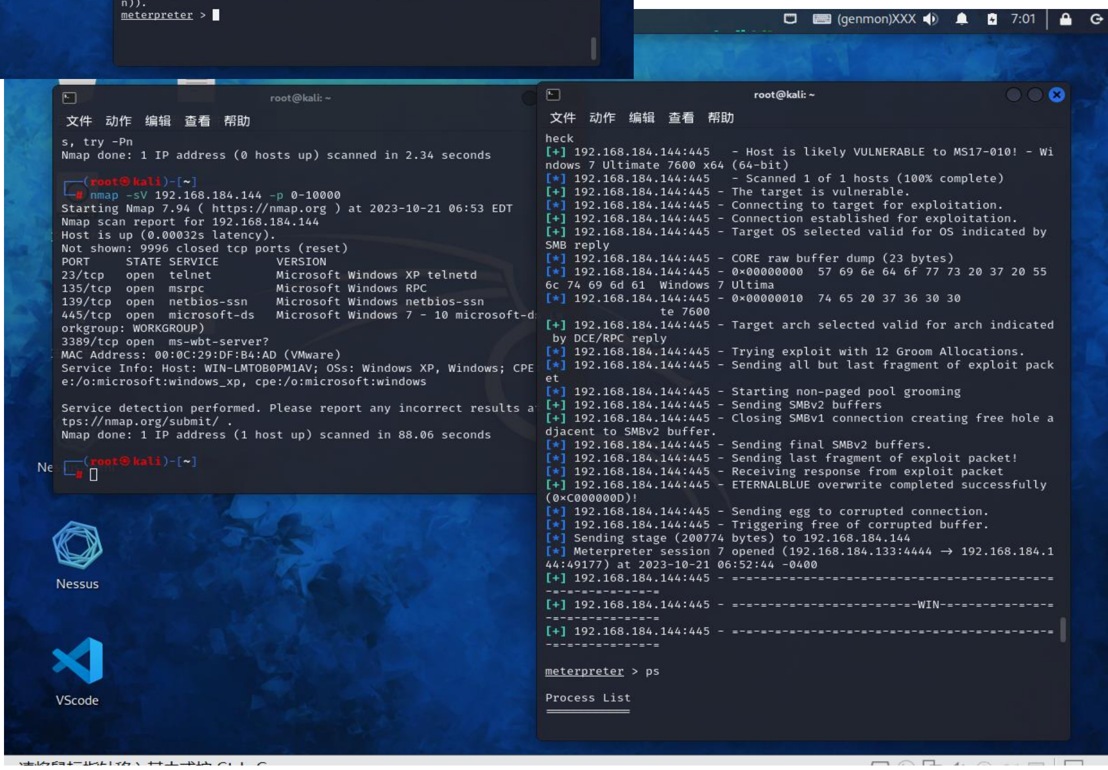
--费曼学习法

所以我会用写博客的方法写总结

一：win7 远程权限

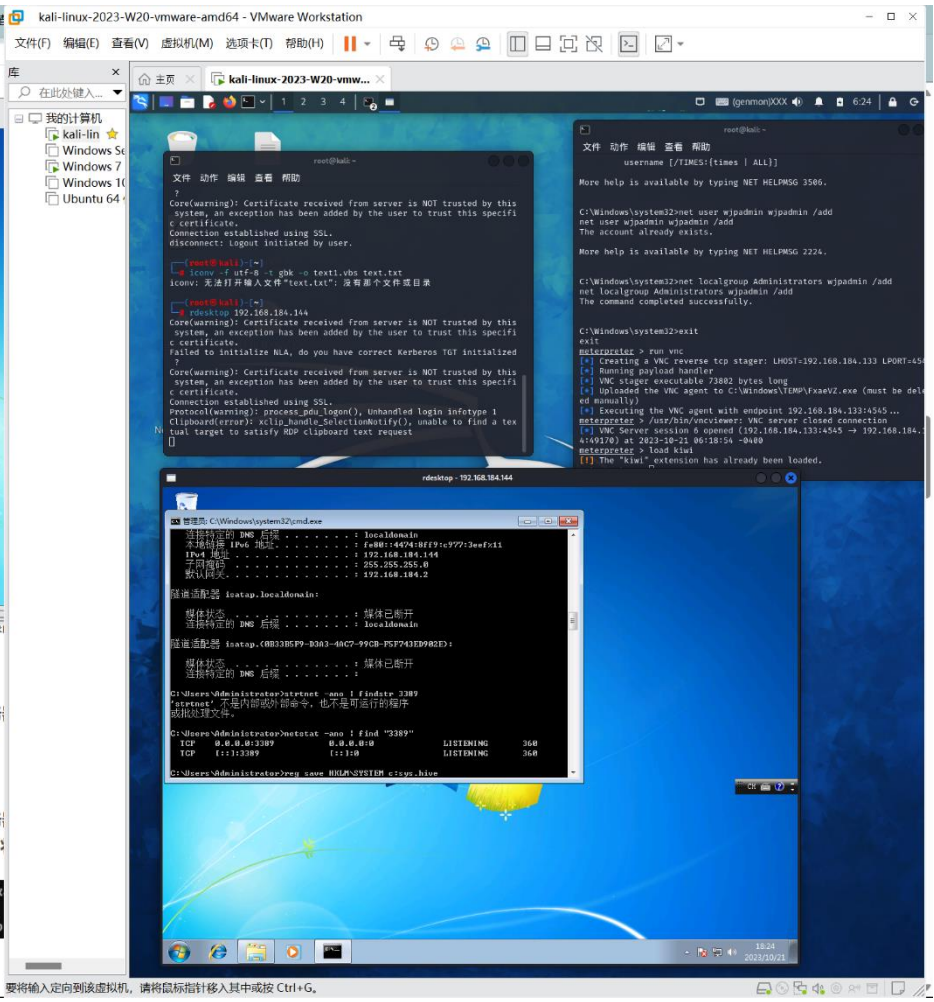
首先，使用 **msf** *中的* **ms17_010** *模块进行权限获取，这个由于时间问题，我直接跳过了，可以看到我刚刚进去后是普通用户的权限，这里使用* **ps,steal_token,getuid** *和* **getsystem** *命令获得了管理员权限，使用* **nmap** *发现对方没有开启* **3389** *端口，这说明没有办法开启远程桌面，下面开始远程桌面教程。*





二：Win7 远程桌面开启

使用 shell 创建一个名为”wjpadmin”和密码为”wjpadmin”的一个 windows 用户（必须是管理员权限）并且加入管理员（Administrators）组（记得加 s 否则是管理员不是管理员组），使用 vnc 命令开启虚拟机的 3389 端口（命令 run vnc）再使用 rdesktop 命令开启虚拟机的远程桌面，输入刚刚创建的账号密码

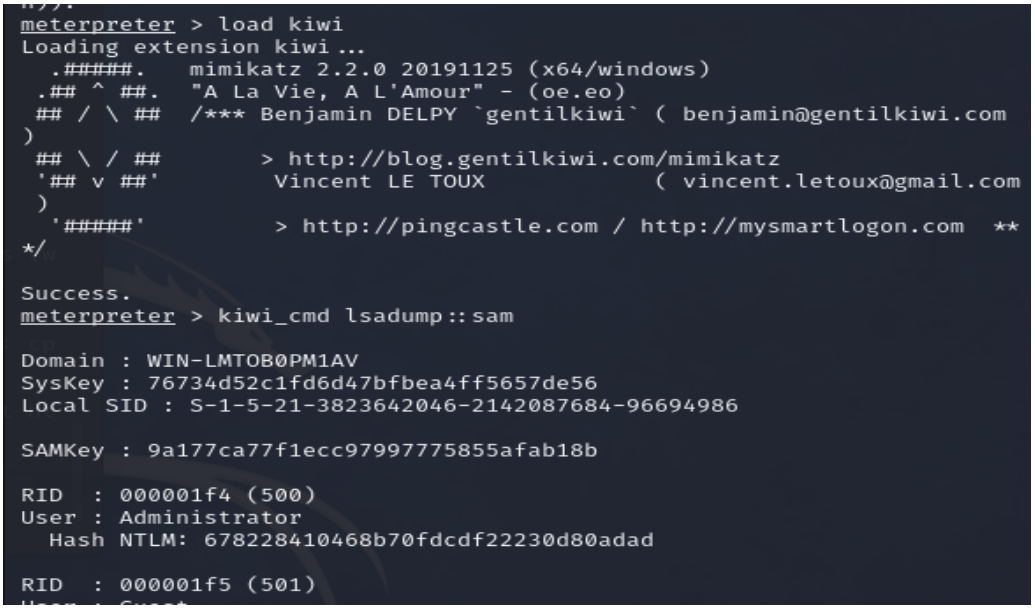


三：reg 命令获得 sam 和 system 文件

此时我们已经获得了管理员权限和远程桌面，然后就是渗透测试的下一步，获得目标的 sam 文件和 system 文件，给不明白的说一下，因为有人问我了（），其中 sam 文件是用户的账号密码，system 文件是系统文件，这两个都是非常重要的文件，非常容易被坏人利用

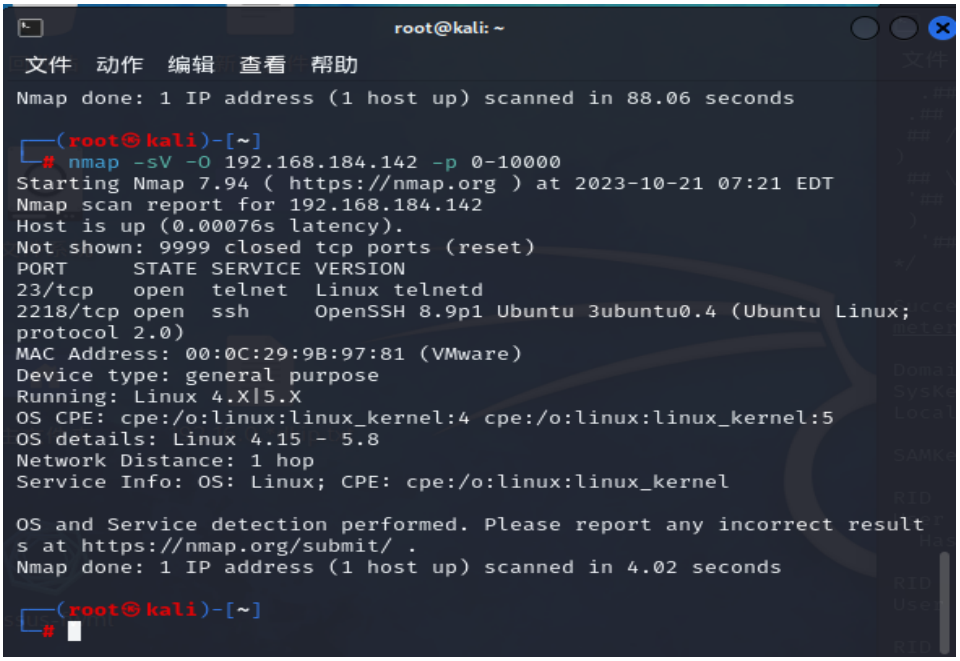
在 win7 远程桌面 shell 输入 reg save HKLM\SYSTEM 和 reg save HKLM\SAM 命令，把文件保存

或者。在 meterpreter 对话中输入 kiwi_cmd lsadump::sam 也可以看到 sam，但是是哈希表要在破解网站解码一下



四：hyard 破解 ssh 协议

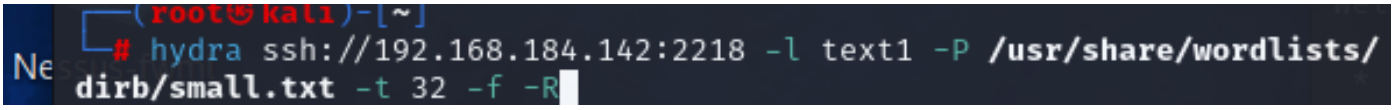
先使用 nmap *获得对方的协议和对应端口号* nmap -sV IP



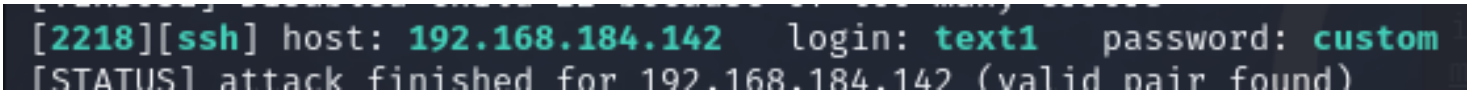
可以看到，这是一台 linux4-5 *的主机，它开启了* ssh *和* telnet *服务，端口号分别为* 22 *和* 2218

然后使用 hydra *工具破解 ssh 协议账号密码*

具体命令为 hyard ssh://IP:"端口号" -l 账号 -P 密码字典



结果为



可以看到，账号为 text1*，密码为* custom

这里我已经知道了账号，要破解密码，这是比赛会告诉你的，因为可以用账号字典破解出来，比赛节约时间

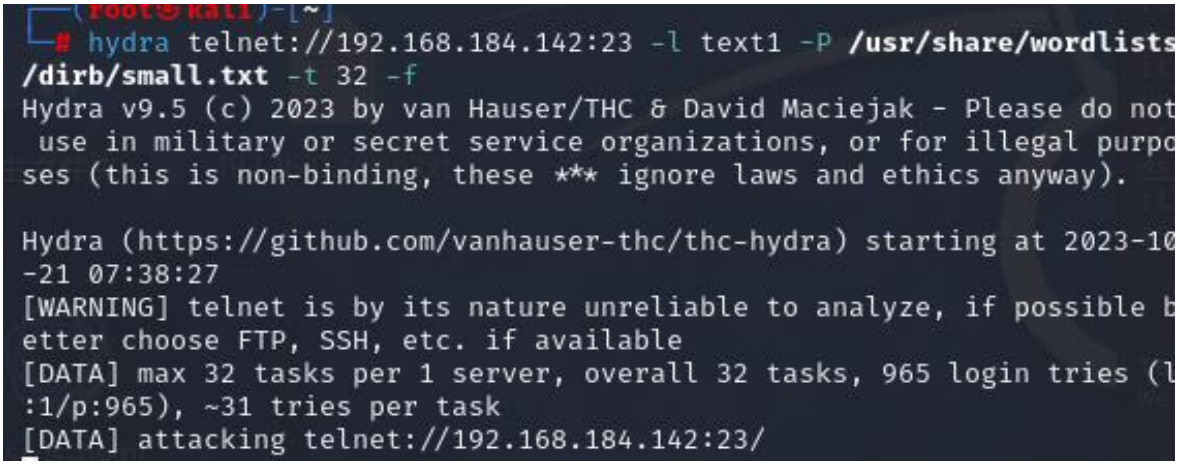
五：hyard 破解 ssh 协议

老样子，nmap 扫描

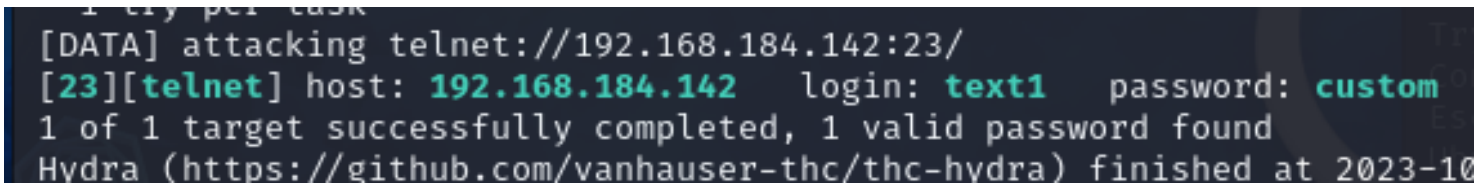
这里看到，open(打开)了 23 端口，协议为 telnet

直接上命令 hyard telnet://IP:"端口号" -l 账号 -P 密码字典

和 ssh 一样的



结果为



结果账号 text1，密码 custom

总结

把之前的复习了一下，又学了一些新的东西，还有很多很

很杂，知识点很简单的东西就不说了