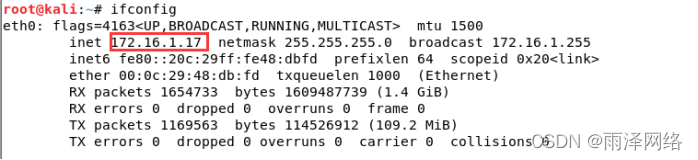
**CVE-2017-7494漏洞**

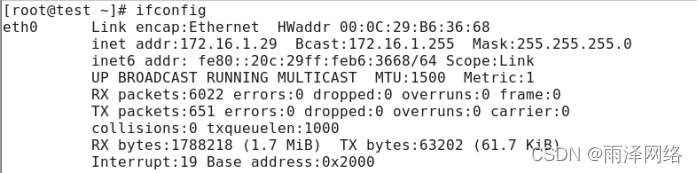
第一步，打开网络拓扑，点击启动选项，启动实验虚拟机

第二步，使用ifconfig和ipconfig命令分别获取渗透机和靶机的IP地址，使用ping命令进行网络连通性测试，确保网络可达

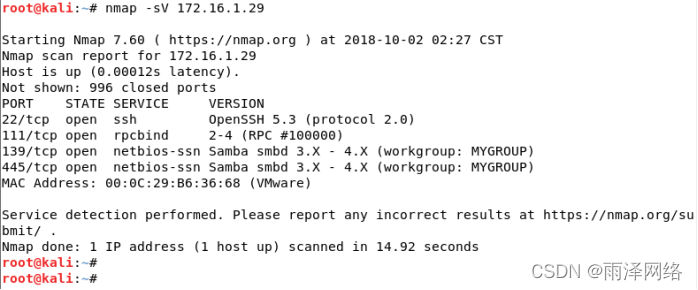
渗透机ip地址172.16.1.17



靶机ip地址172.16.1.29

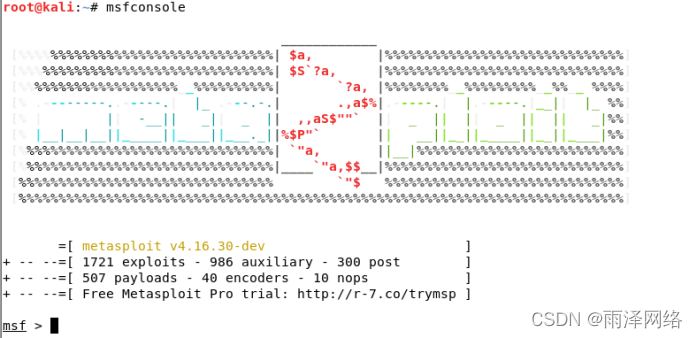


第三步，使用命令nmap -sV 172.16.1.29扫描目标服务器版本信息



发现靶机上存在samba服务，并且版本号为3.X-4.X，初步分析可能包含漏洞尝试使用exploit\_CVE-2017-7494(msf-ruby)，对靶机进行溢出操作

第四步，使用命令msfconsole打开metasploit渗透测试平台

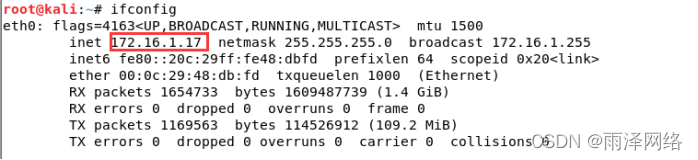


第五步，使用命令search is\_known\_pipename搜索smb漏洞利用模块

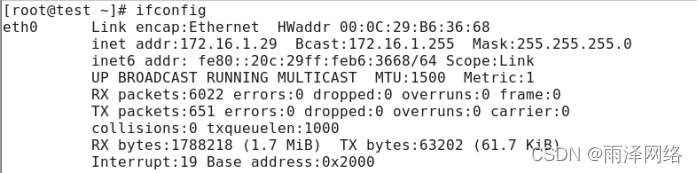
第一步，打开网络拓扑，点击启动选项，启动实验虚拟机

第二步，使用ifconfig和ipconfig命令分别获取渗透机和靶机的IP地址，使用ping命令进行网络连通性测试，确保网络可达

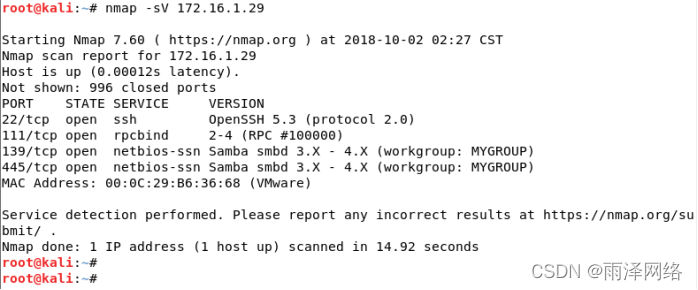
渗透机ip地址172.16.1.17



靶机ip地址172.16.1.29

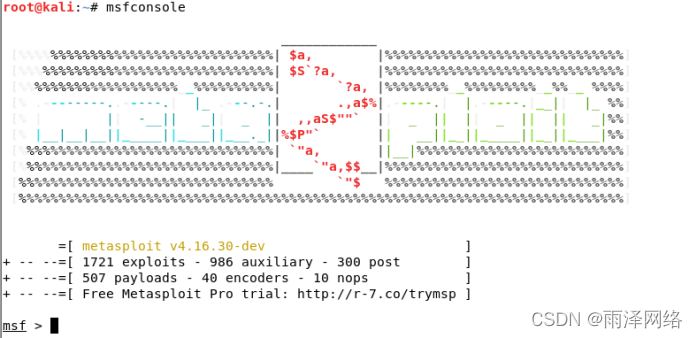


第三步，使用命令nmap -sV 172.16.1.29扫描目标服务器版本信息



发现靶机上存在samba服务，并且版本号为3.X-4.X，初步分析可能包含漏洞尝试使用exploit\_CVE-2017-7494(msf-ruby)，对靶机进行溢出操作

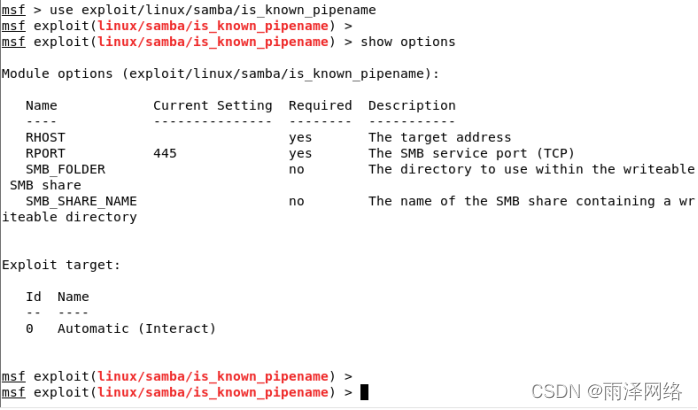
第四步，使用命令msfconsole打开metasploit渗透测试平台



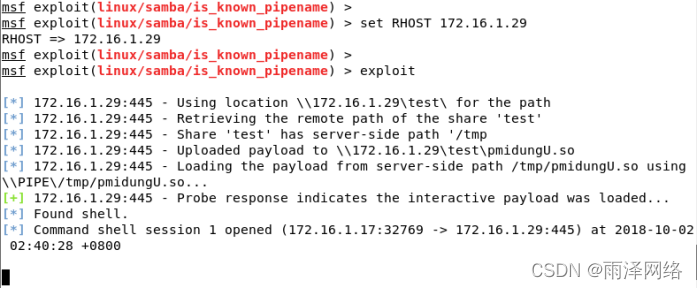
第五步，使用命令search is\_known\_pipename搜索smb漏洞利用模块



第六步，使用命令use exploit/linux/samba/is\_known\_pipename调用溢出模块，然后使用命令show options 查看所有需要配置的参数

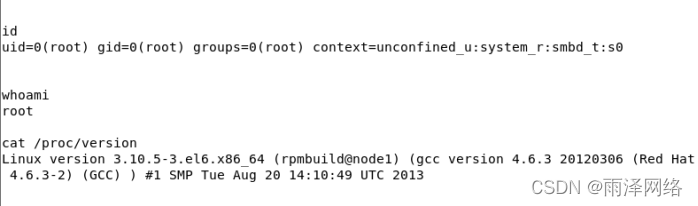


第七步，使用命令set RHOST 172.16.1.29，然后执行exploit命令



发现命令被成功执行，成功上线了一个shell

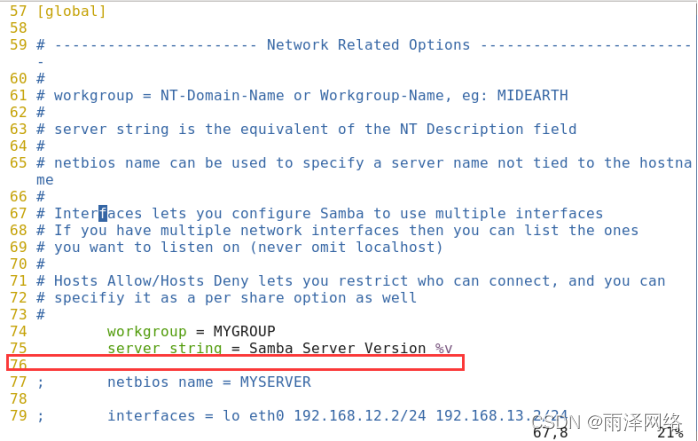
第八步，使用命令id;whoami;cat /proc/version进行查看靶机基本信息



第九步，使用命令vim /etc/samba/smb.conf在smb.conf文件中的[global]节点下增加　nt pipe support = no 选项，然后重新启动samba服务临时关闭pipe支持以防止此漏洞。



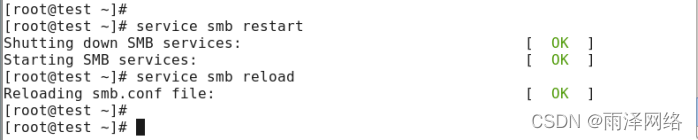
在76行的位置，添加nt pipe support = no



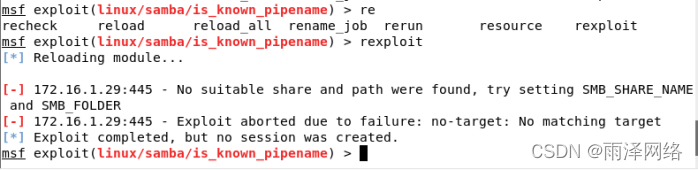
添加成功后，使用进入vim命令行界面使用输入wq保存并退出



第十步，使用命令service smb restart，然后使用命令service smb reload 重新加载smb配置文件，并重启服务



第十一步，回到渗透机上，重新使用溢出模块对靶机的smb服务进行溢出操作，使用命令rexploit



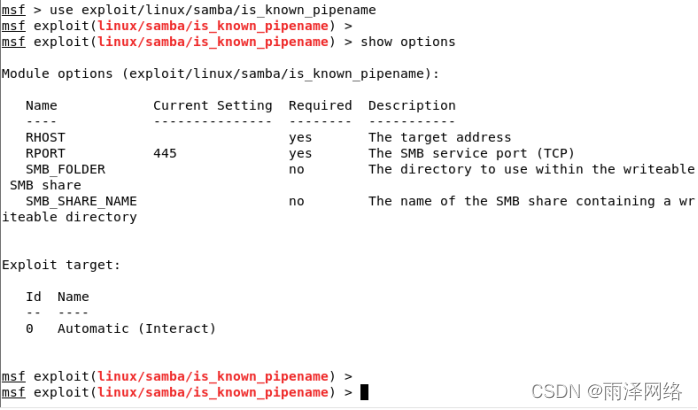
此时发现利用脚本给出的操作提示：

[-] 172.16.1.29:445 - No suitable share and path were found, try setting SMB\_SHARE\_NAME and SMB\_FOLDER

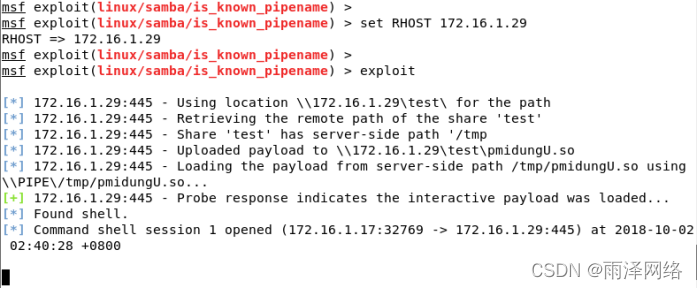
//没有找到合适的共享和路径，尝试设置Smb\_Share\_Name和SMB\_FOLDER

由于我们关闭了pipe support会禁用 Windows 客户端的共享列表。所以此处漏洞无法成功进行利用

第六步，使用命令use exploit/linux/samba/is\_known\_pipename调用溢出模块，然后使用命令show options 查看所有需要配置的参数

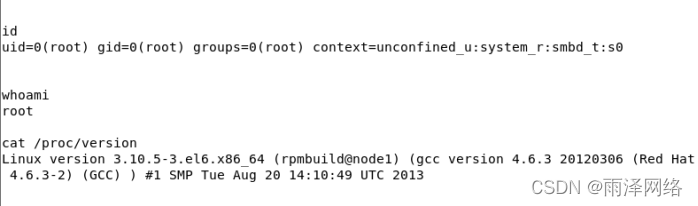


第七步，使用命令set RHOST 172.16.1.29，然后执行exploit命令



发现命令被成功执行，成功上线了一个shell

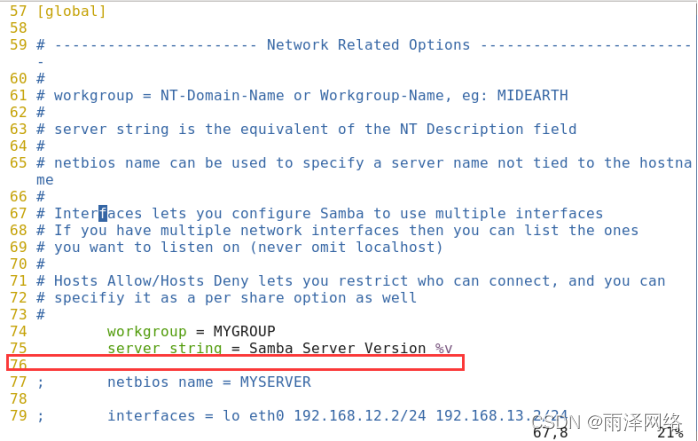
第八步，使用命令id;whoami;cat /proc/version进行查看靶机基本信息



第九步，使用命令vim /etc/samba/smb.conf在smb.conf文件中的[global]节点下增加　nt pipe support = no 选项，然后重新启动samba服务临时关闭pipe支持以防止此漏洞。



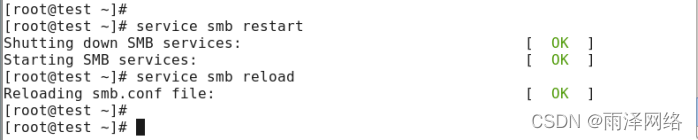
在76行的位置，添加nt pipe support = no



添加成功后，使用进入vim命令行界面使用输入wq保存并退出



第十步，使用命令service smb restart，然后使用命令service smb reload 重新加载smb配置文件，并重启服务



第十一步，回到渗透机上，重新使用溢出模块对靶机的smb服务进行溢出操作，使用命令rexploit

