Unix User Enumeration

pentestlab.blog/category/information-gathering/page/9

April 10, 2012

One of the first activities while conducting a penetration test in Unix environments is to perform a user enumeration in order to discover valid usernames.In this article we will examine how we can manually discover usernames based on the services that are running.

Lets say that we have perform a port scan with Nmap on our host and we have discover that the finder daemon is running on port 79.

```
root@bt:~# nmap -sV 192.168.1.80
Starting Nmap 5.61TEST4 ( http://nmap.org ) at 2012-04-10 00:29 BST
Nmap scan report for 192.168.1.80
Host is up (0.00090s latency).
Not shown: 989 closed ports
PORT    STATE SERVICE             VERSION
7/tcp   open  echo
13/tcp  open  daytime
19/tcp  open  chargen             Linux chargen
21/tcp  open  ftp                 vsftpd 2.0.4
22/tcp  open  ssh                 OpenSSH 4.3 (protocol 1.99)
25/tcp  open  smtp                Sendmail 8.13.5/8.13.5
37/tcp  open  time                (32 bits)
79/tcp  open  finger              Debian fingerd
111/tcp open  rpcbind (rpcbind V2) 2 (rpc #100000)
139/tcp open  netbios-ssn         Samba smbd 3.X (workgroup: YORK)
445/tcp open  netbios-ssn         Samba smbd 3.X (workgroup: YORK)
MAC Address: 00:50:56:BB:00:79 (VMware)
Service Info: Host: localhost.localdomain; OSs: Linux, Unix; CPE: cpe:/o:linux:kernel
```

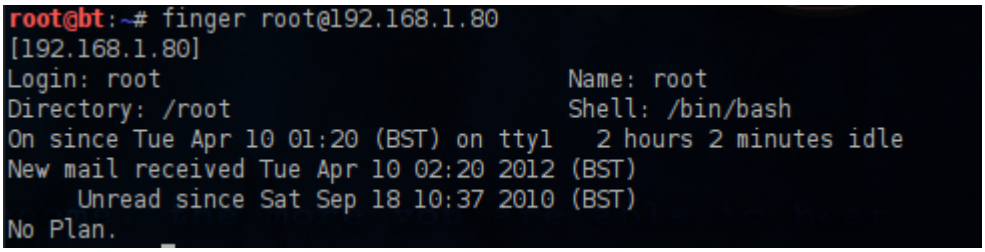
Discovery of the Finger Service

We can use the finger command in order to enumerate the users on this remote machine.For example if we execute the command **finger @host** we will get the following output.

```
root@bt:~# finger @192.168.1.80
[192.168.1.80]
Login     Name       Tty      Idle  Login Time   Office     Office Phone
root      root       tty1     1:42  Apr 10 01:20
```

List the logged users on the remote host

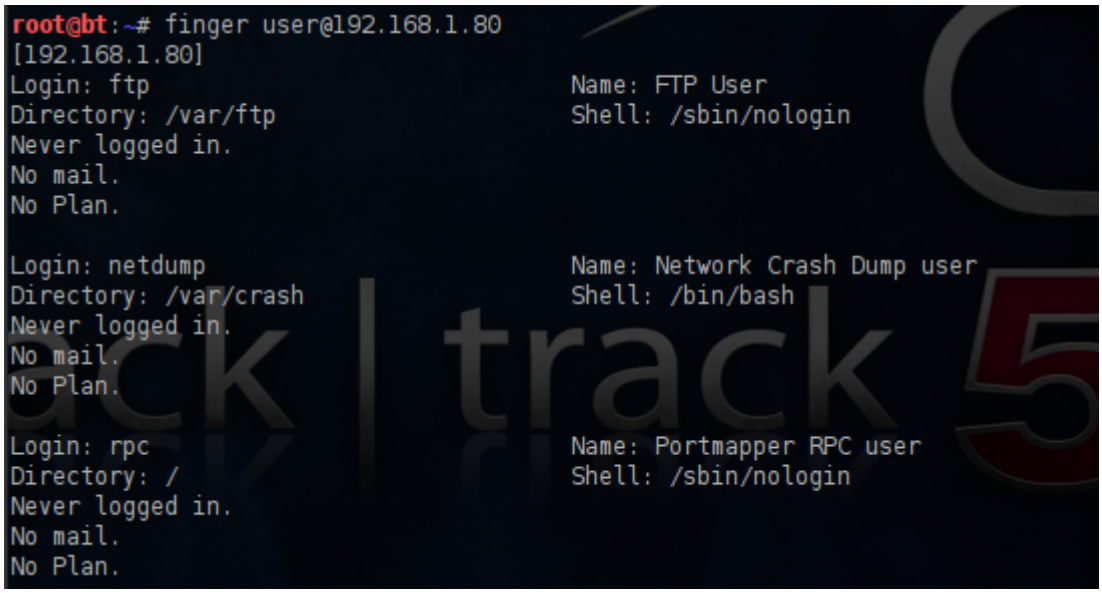
As you can see the root user is the only account which is logged on the remote host.Now that we have a specific username we can use it in order to obtain more information about this user with the command **finger root@host**.



Finger a specific user

As the image indicates the finger command obtained information about the name,the home directory,login name and shell.Also we can see that the root user doesn't have a **.plan** file.

Another effective use of the finger command is when you use it with the following syntax: **finger user@host**

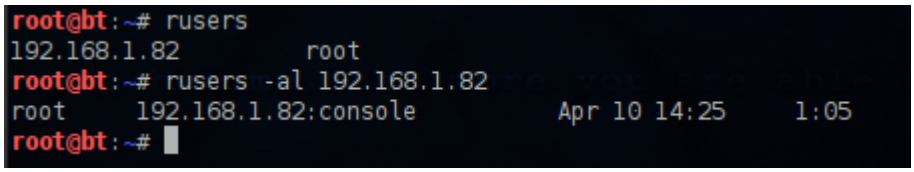


Enumerate all users with the string user

This specific command will enumerate all user accounts that have the string ***user***.Alternatively you can use other words instead of user like **admin**,**account** and **project**.

Older versions of Solaris that run the finger daemon are affected by an enumeration bugs.For example you can run the command **finger 0@host** and it will enumerate all users with an empty GCOS field in the password file.Additionally you can run **finger 'a b c d e f g h'@host** and it will enumerate all users on the remote target.

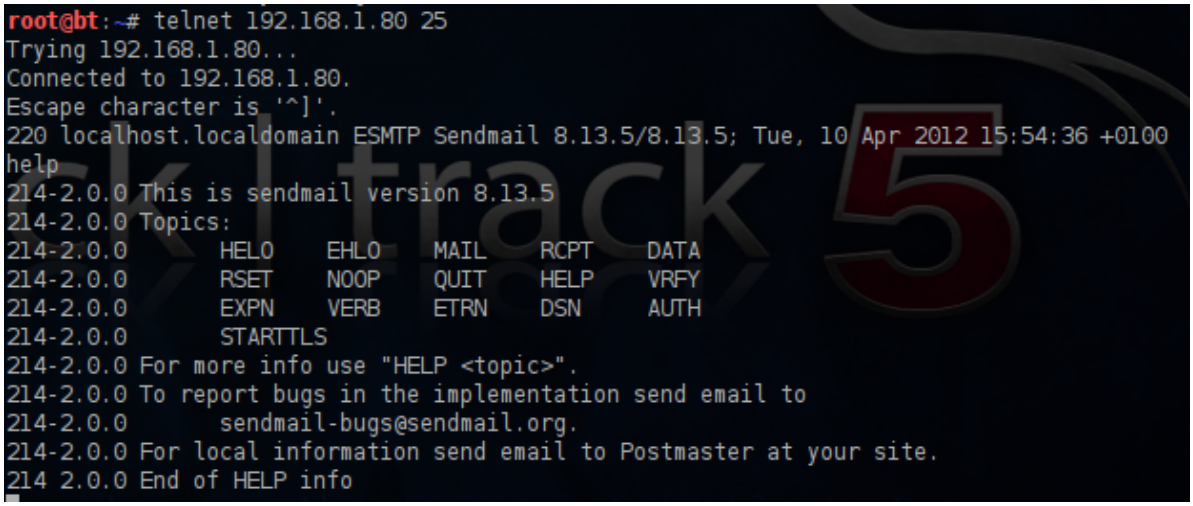
In SunOS there are RPC services that allow also user enumeration.For example the command **rusers** will return a list with the users that are logged into machines on the local network.Alternatively if you are looking for the list of a specific host you can combine it with **rusers -al host**.



rusers output

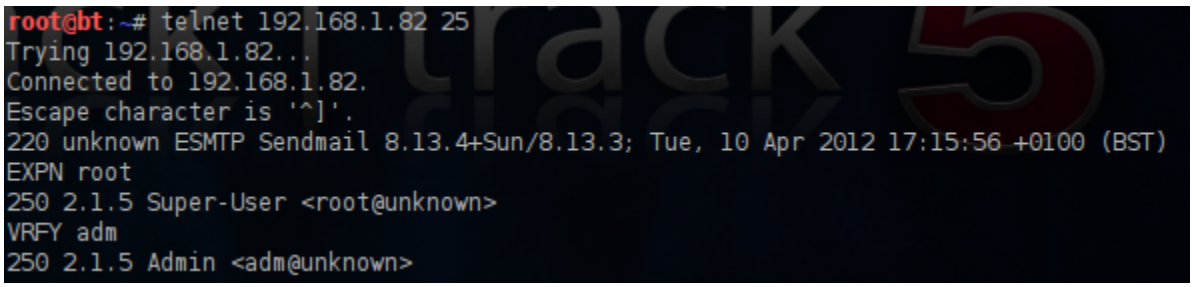
Another option is the **rwho** command which can be used also to enumerate network users.All the systems that are running the **rwhod** daemon will respond and an output will produced of the users that are currently logged in to these systems.This service runs at 513 (UDP) port.

If you discover a host which is running an SMTP service (port 25) you can also use it for username enumeration.We can connect through telnet to the mail server and then we can execute the command help in order to see the available commands.



SMTP - Commands

As you can see from the image above there are plenty of commands but the commands that we will need for the discovery of valid usernames are the **VRFY** and **EXPN**.



Discover valid usernames through SMTP

The image above indicates that we have successfully verify the existence of two users root and admin.

Conclusion

In production systems it is almost impossible to find any of these services running due to this information leakage.However many Linux distributions include these daemons as part of their default installation.

In nowadays this process can be done automatically through the nmap script engine but it is good to know also how you can manually discover usernames in Unix systems.Also many commercial certifications are still requiring from you to know how to enumerate users with these commands.