Network Penetration Testing Methodology-Internal

6 Hr 40 Min Remaining

Instructions Resources Help  100%

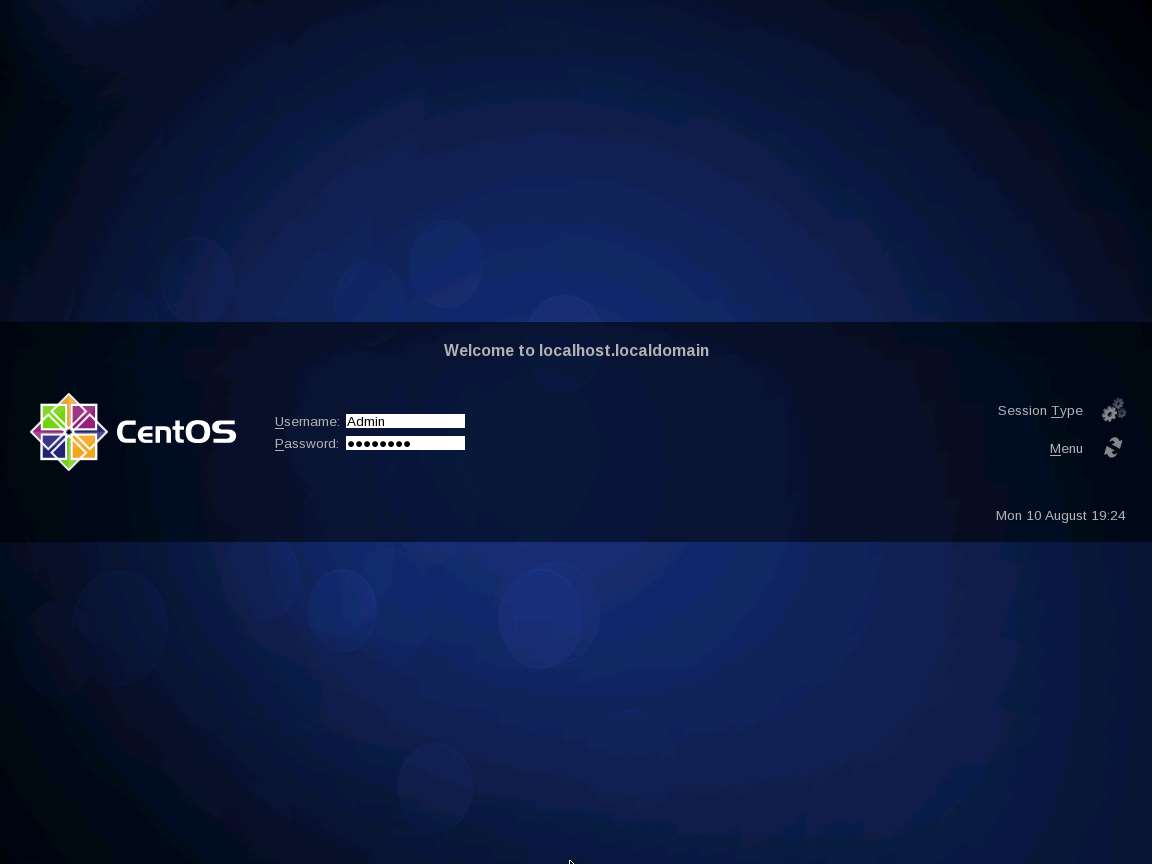
Exercise 12: Enumerating Logged on Users Using Finger Protocol

Scenario

The Finger service displays information such as currently logged-on users (if any), email address, full name etc.  
During a penetration test, the initial task of a pentester is to enumerate user information such as usernames, email addresses, etc.  
In this lab, you are going to learn how to enumerate user information using finger client.

**Lab Duration**: **15** Minutes

1. Click @lab.VirtualMachine(RedHatEnterpriseLinux-SubnetC(ECSAv10)).SelectLink. Type **Admin** in the **Username** field, **password** in the **Password** field and press **Enter**.



1. On successful login, Red Hat Enterprise Linux CentOS desktop appears as shown in the screenshot. We are logging into the machine since **Finger** enumerates only the logged on users.



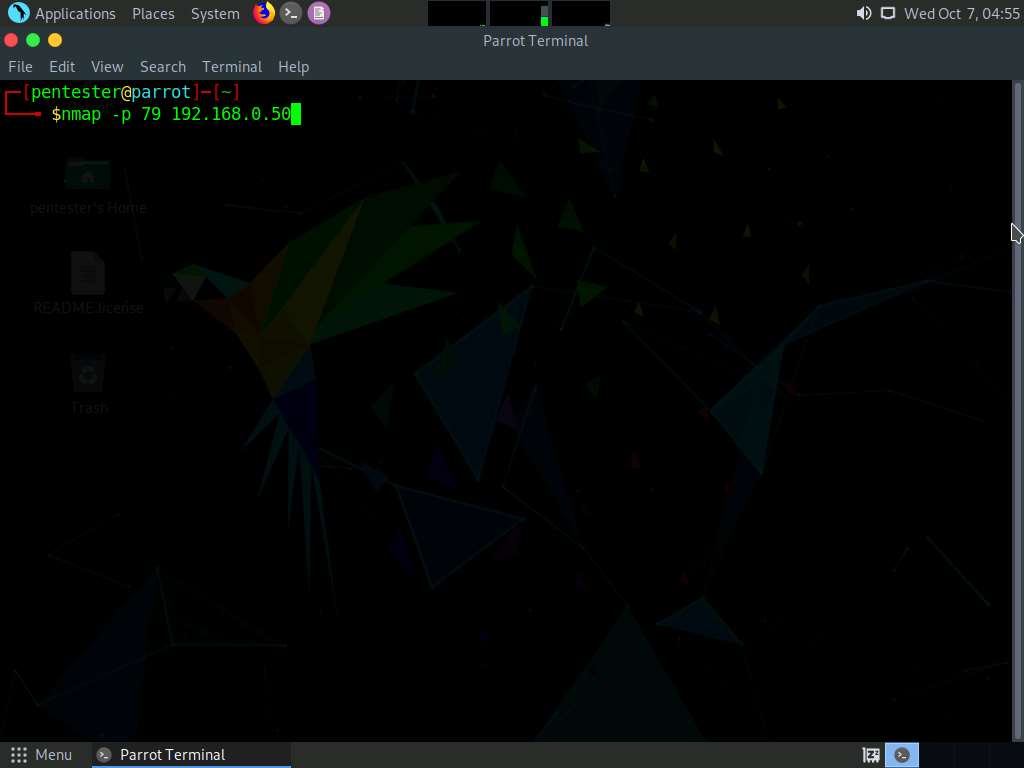
1. Click [Parrot](https://labclient.labondemand.com/Instructions/52f4d542-434e-4a10-8f51-0c2b8ca1d32b?rc=10). Parrot lock screen appears.



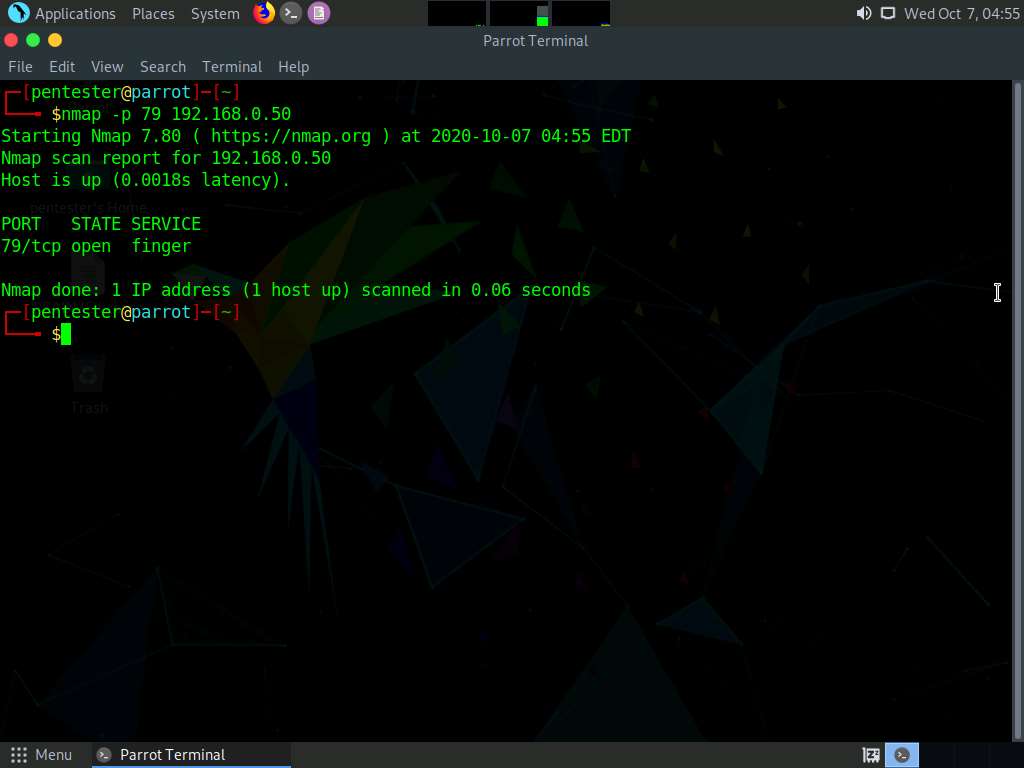
1. By default **pentester** is selected as the **user**. Type **toor** in the Password field and press **Enter**.



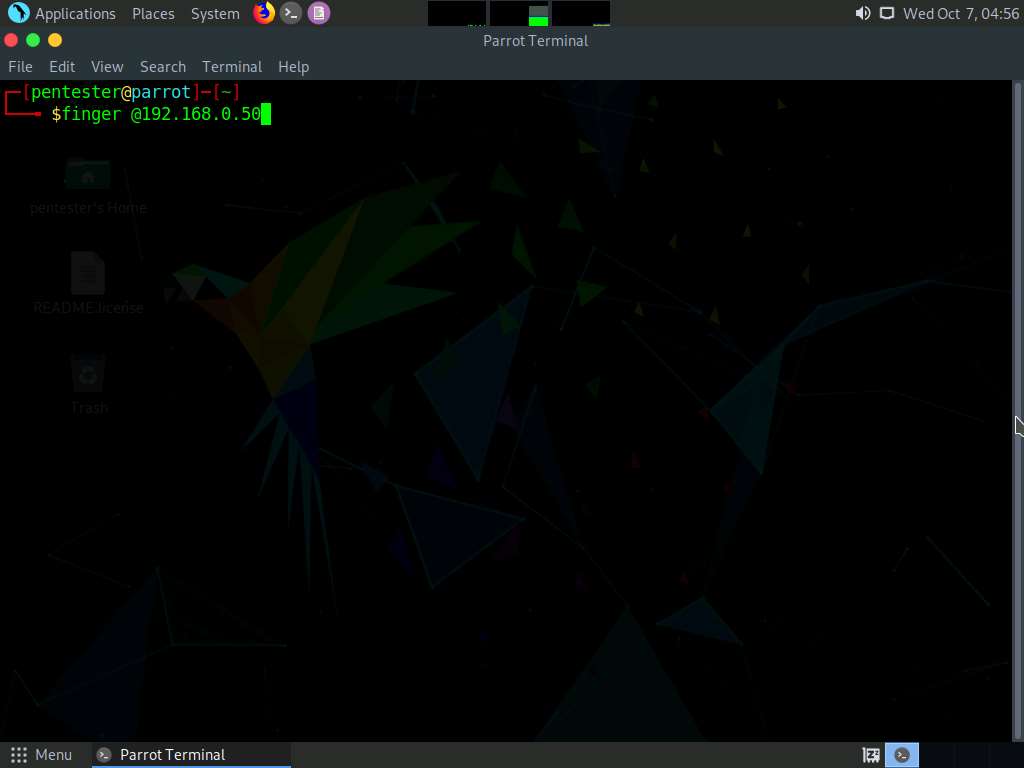
1. In this lab, we are going to target the IP address **192.168.0.50** (Red Hat Enterprise Linux machine) that was discovered during the ping sweep scan in the earlier lab exercises. Finger protocol uses port 79, so, choosing CentOS as our target machine, let us perform an Nmap scan on **port 79**. Launch a command line terminal, type **nmap -p 79 192.168.0.50** and press **Enter.**



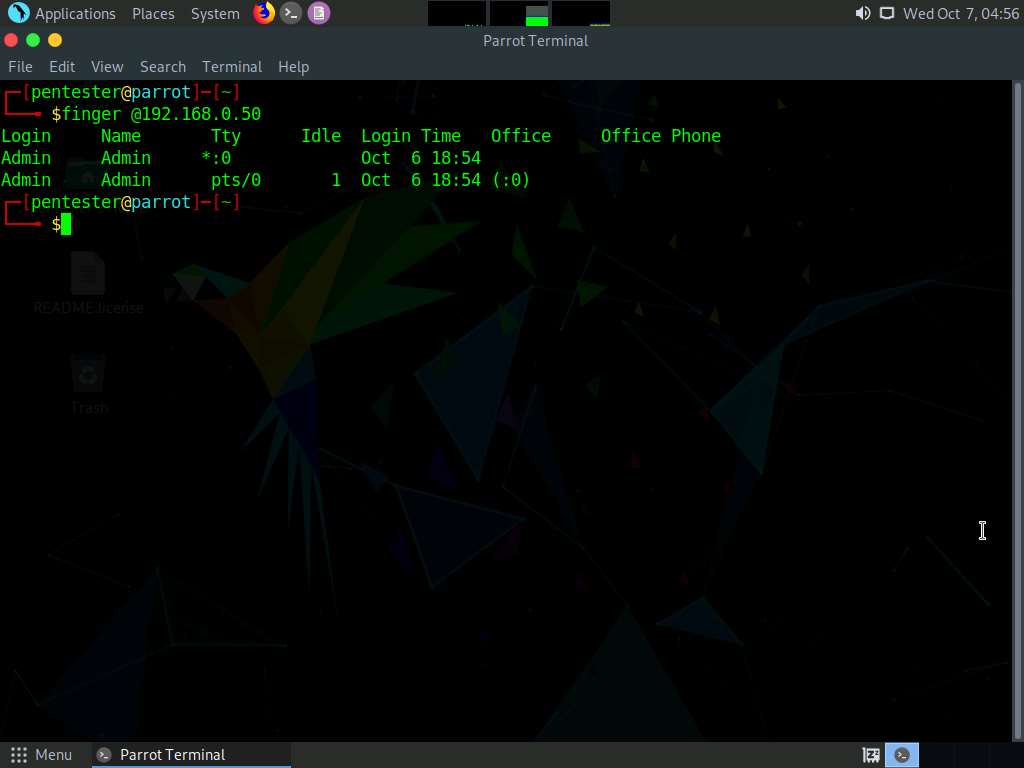
1. You will observe that the **port 79** is open in the Nmap result, meaning finger service is running on the target machine.



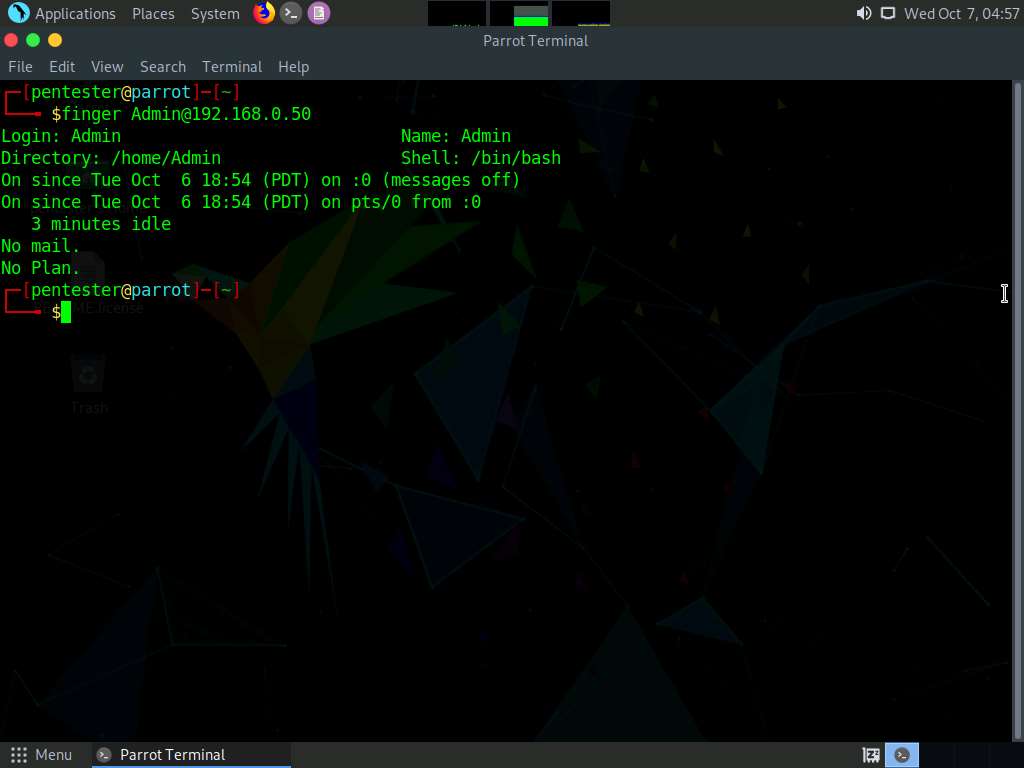
1. Now, we shall enumerate the logged on users on the remote machine using Finger client. Assuming we don't know the logged on username, type **finger @192.168.0.50**, and press **Enter**.



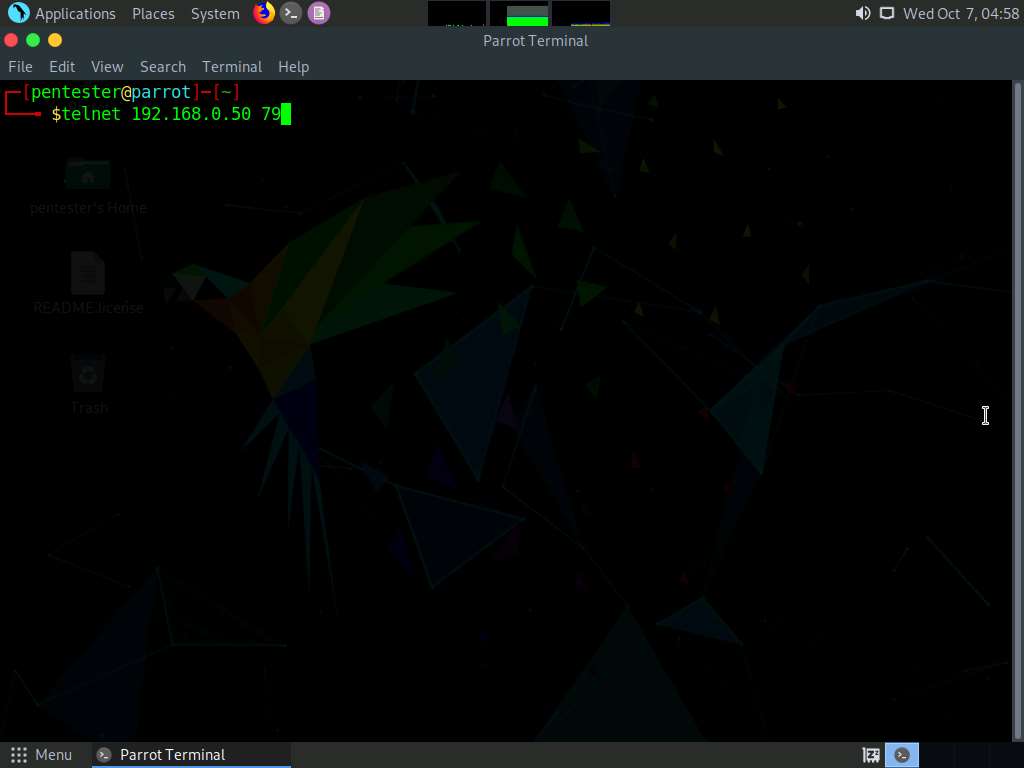
1. Finger client returns the logged in user information such as the login name, name of the user and login time as shown in the screenshot below.



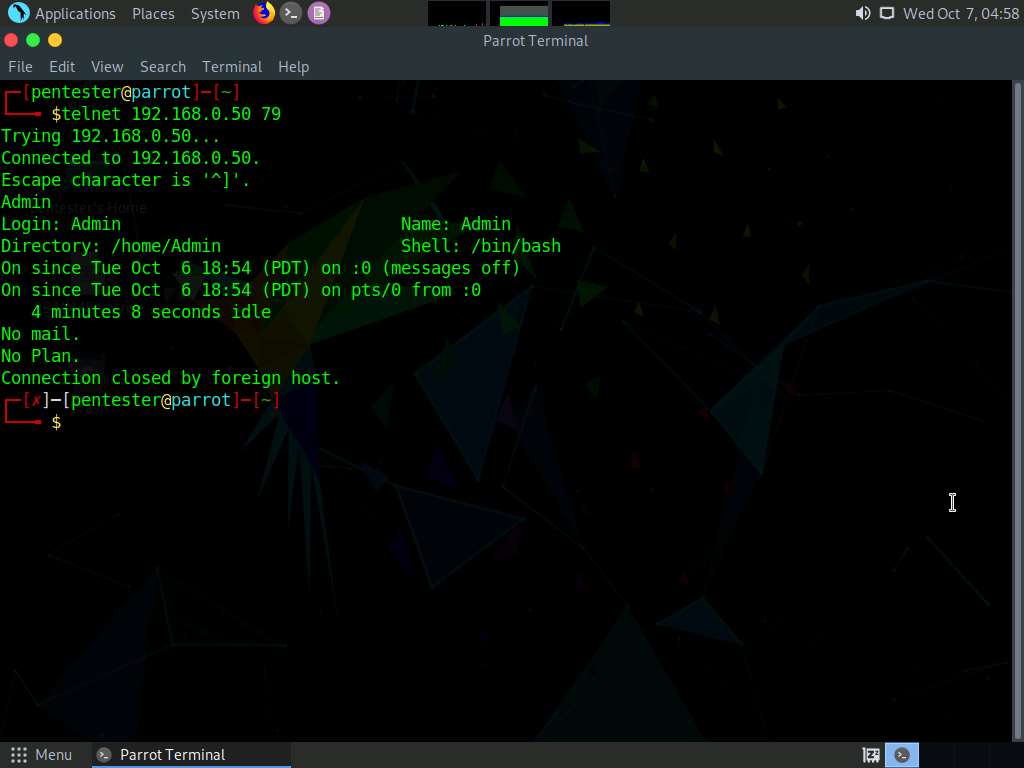
1. Since we found the username, we shall use this to extract additional information such as the name of the user, home directory, login name, and shell. Type **finger Admin@192.168.0.50** and press **Enter**.



1. Alternatively, we can enumerate usernames using Telnet service by issuing the following command in the command line terminal: **telnet 192.168.0.50 79**



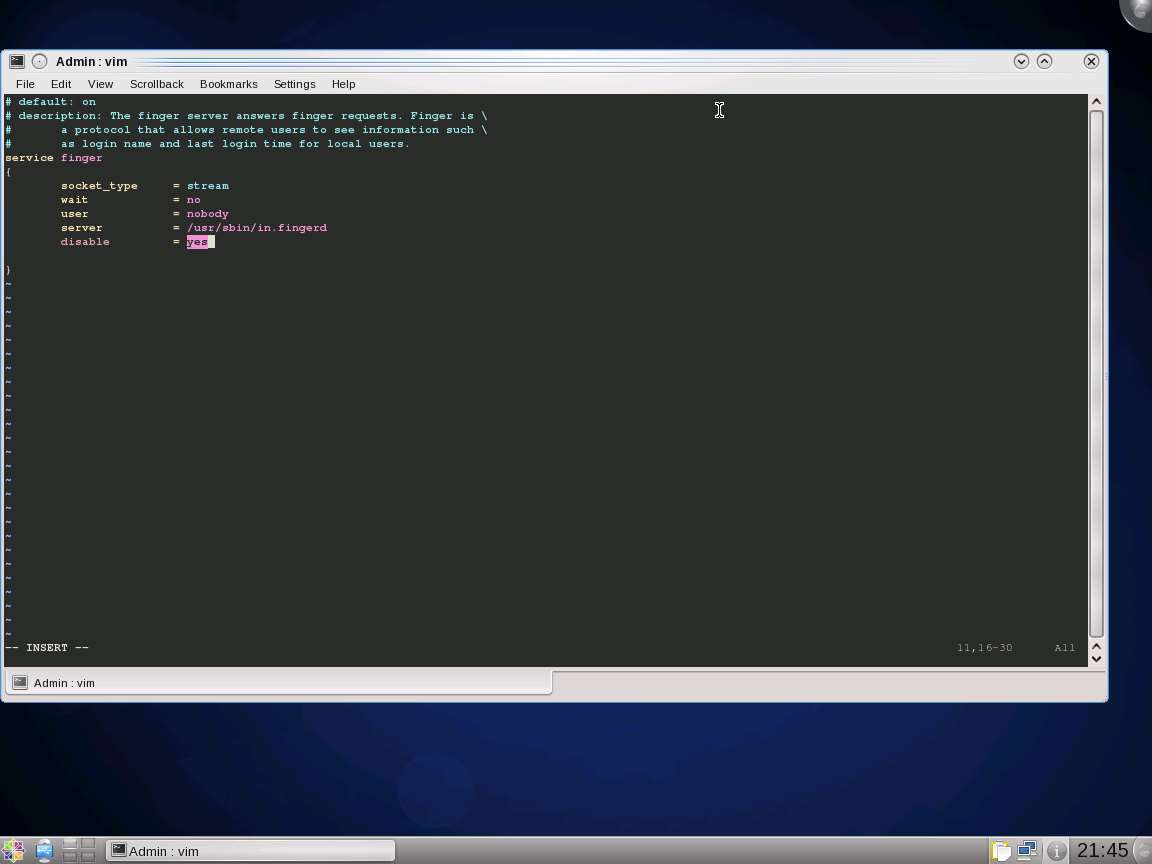
1. Type **Admin** and press **Enter**. This displays the enumerated user information as shown in the screenshot below.



1. To safeguard your machine from returning the logged in user information, it is recommended to disable finger service on the machine by editing the **finger** text file located in the **/etc/xinetd.d**.

This is just a proof of concept to show the reason for the vulnerability and you are not required to log in to the machine to view the above-mentioned file.

The finger text file is located in **/etc/xinetd.d**.



In this lab, you have learned how to enumerate user information using finger client.