

CS581 (Computer & Network Security)

Lab-06

Group No.: 05

Group Members:

01. Rajnish Kumar (CIN: 304470392)
02. Jay Purohit (CIN: 304455065)
03. Rupal Jaiswal (CIN: 304442169)
04. Gaurav Prajapati (CIN: 304470132)

AAA

Configure your Cisco router to use AAA for user authentication via a TACACS+ or RADIUS server (such as Clear box) that you installed on your computer. Submit the configuration files used on the Cisco router. Submit screenshots of decoded packet capture of TACACS+ or RADIUS packets as evidence that AAA authentication works whenever you telnet to your router.

We, Group No. 5, performed this lab in below steps:

Step 1: Configuration of **Server** Computer

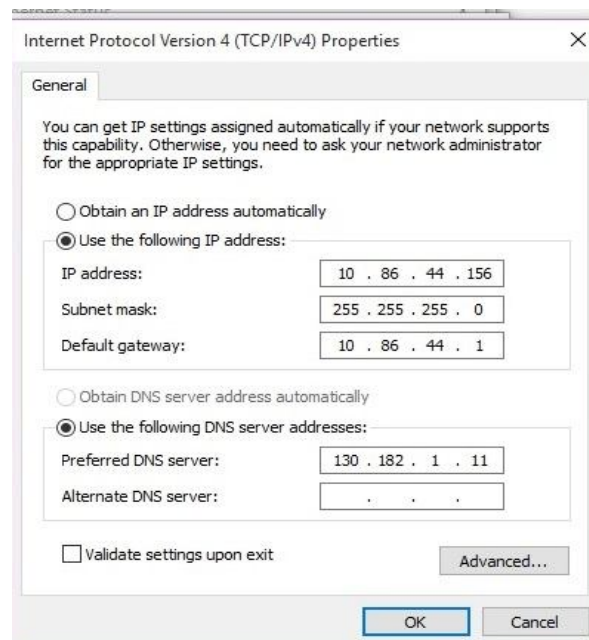
Step 2: Installation of **WinRadius** on Server Computer

Step 3: Configuration of **Cisco** Router

Step 4: Screenshots of Cisco Router's Configuration File

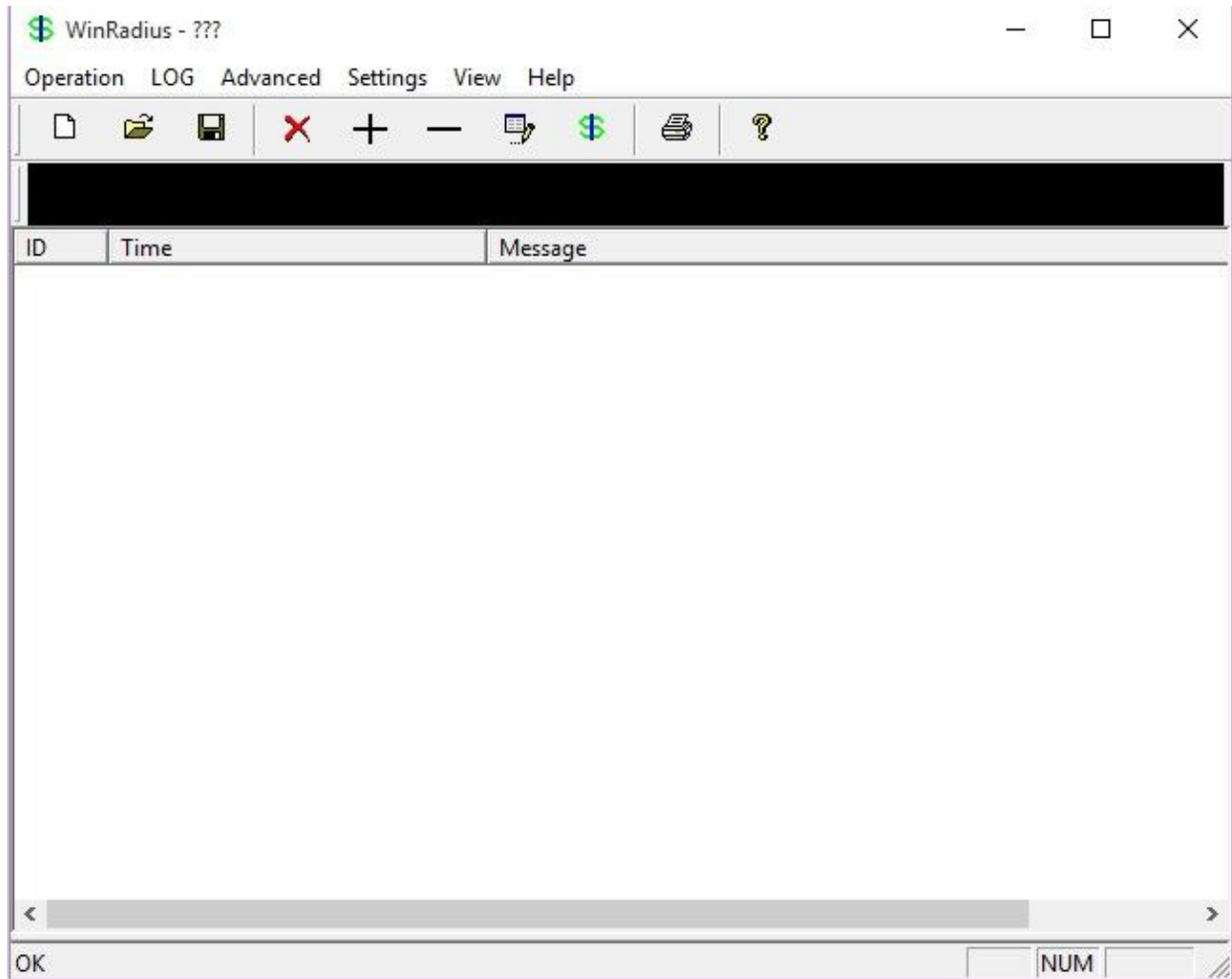
Step 5: Screenshot of WinRadius when We telnet to our Router

Step 1: Configuration of **Server** Computer



Step 2: Installation of **WinRadius** on Server Computer

I installed WinRadius and here is the window when we open WinRadius after installation:



ODBC settings

Please use 'Control panel/ODBC' to set your RADIUS database. Default database is 'WinRadius.mdb'. You can also add this database to your ODBC system by clicking the following button.

ODBC name:

Note: Please input "yourOdbcName;Uid=yourUsername;Pwd=yourPassword" if username/password is needed.

User table name:

Billing table name:

VoIP table name:

Refresh user information every minutes

This database supports

Add user

User name:

Password:

Group:

Calling address:

Please fill MAC address or Calling number, thus this user will be binded to this address. Empty means no limitation, 0 means using first address of first login.

Cash prepaid: Cents

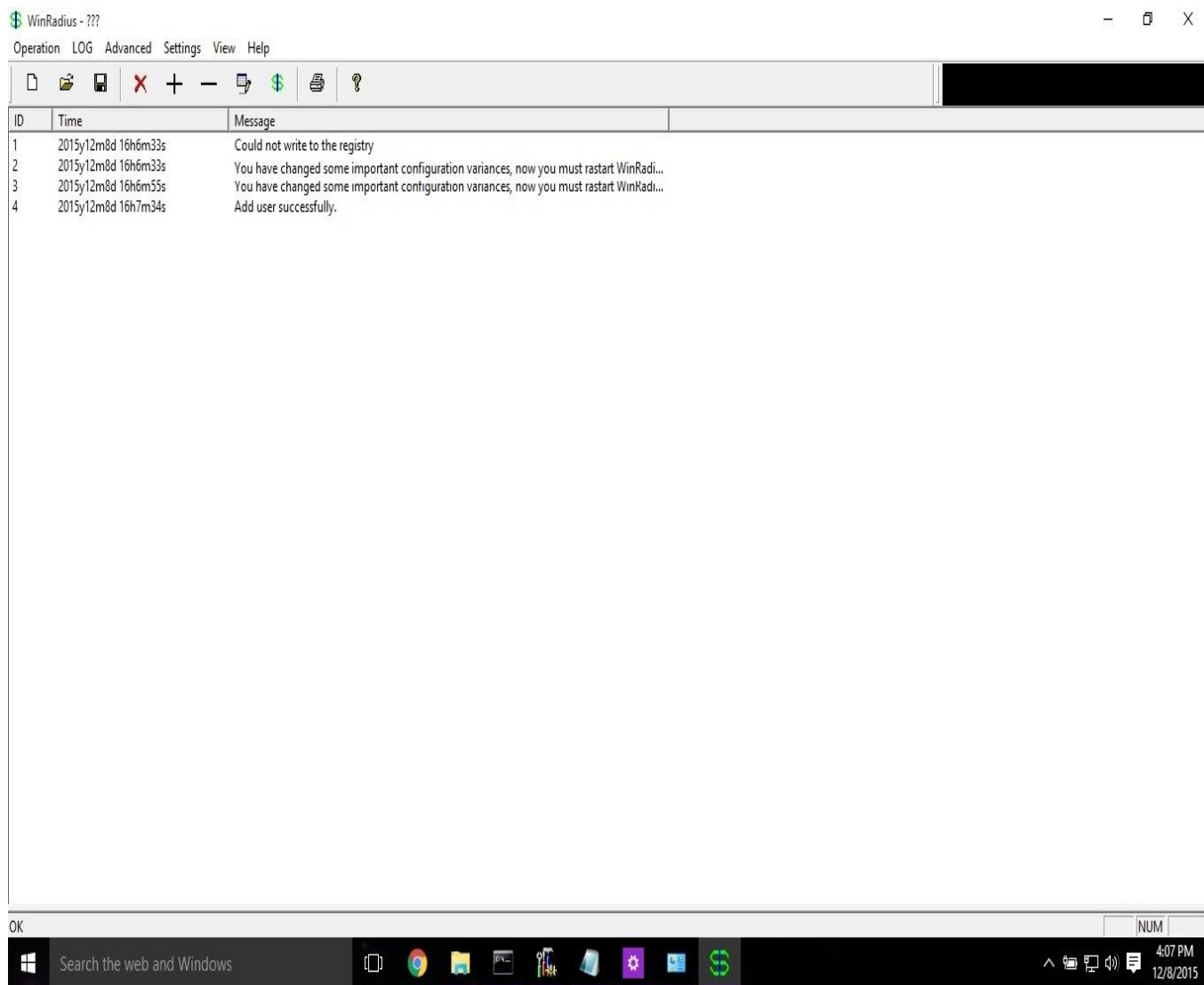
Expiry date:

Note: yyyy/mm/dd means expiry date; digit means valid days since first login; empty means never expired.

Others:

☐ Prepaid user ☒ Postpaid user

Accounting method:



Step 3: Configuration of Cisco Router

We configured following command to our cisco router:

```
R1#
```

```
R1# conf t
```

```
R1 (config)# username testuser password testpass
```

```
R1 (config)# aaa new-model
```

```
R1 (config)# aaa authentication login VTY_LINES group radius local
```

```
R1 (config)# radius-server host 10.86.44.156 auth-port 1812 acct-port 1813 key TestRadius
```

```
R1 (config)# line vty 0 4
```

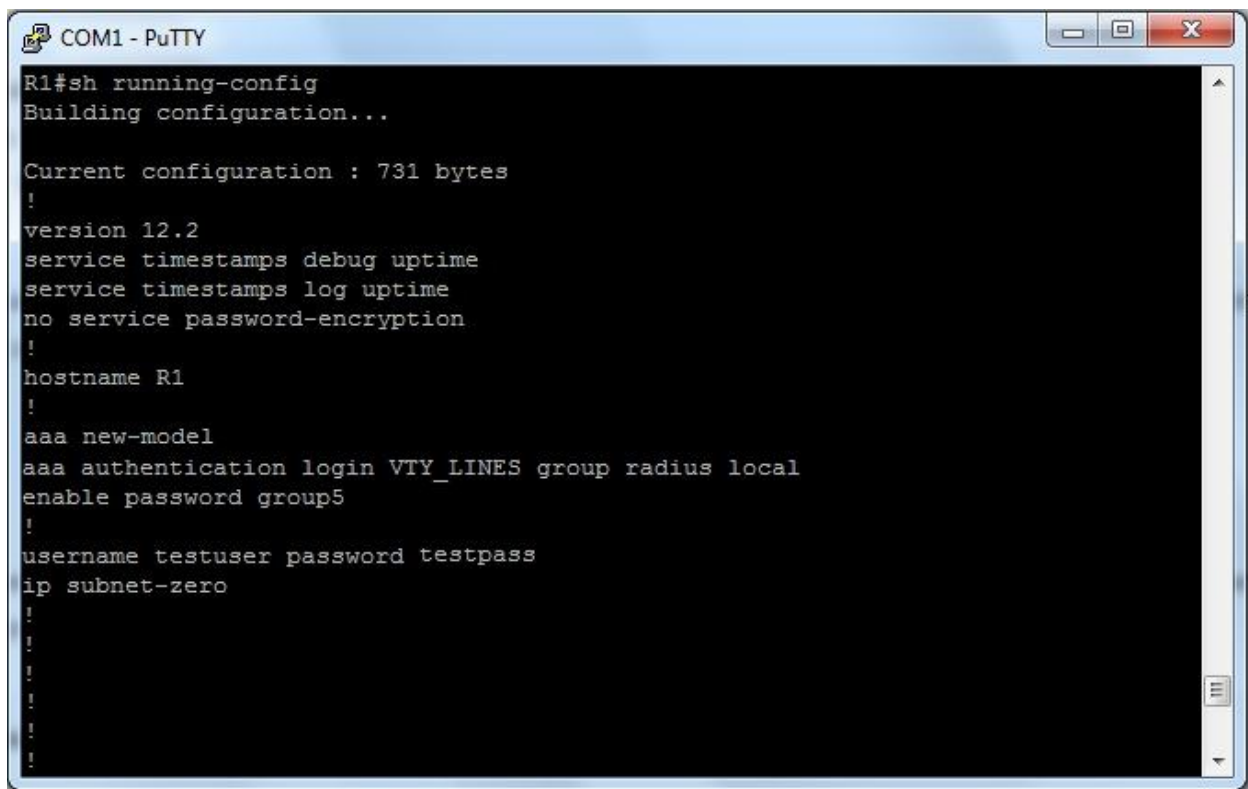
```
R1 (config-line)# login authentication VTY_LINES
```

```
R1 (config-line)# exit
```

```
R1 (config)# exit
```

```
Router#
```

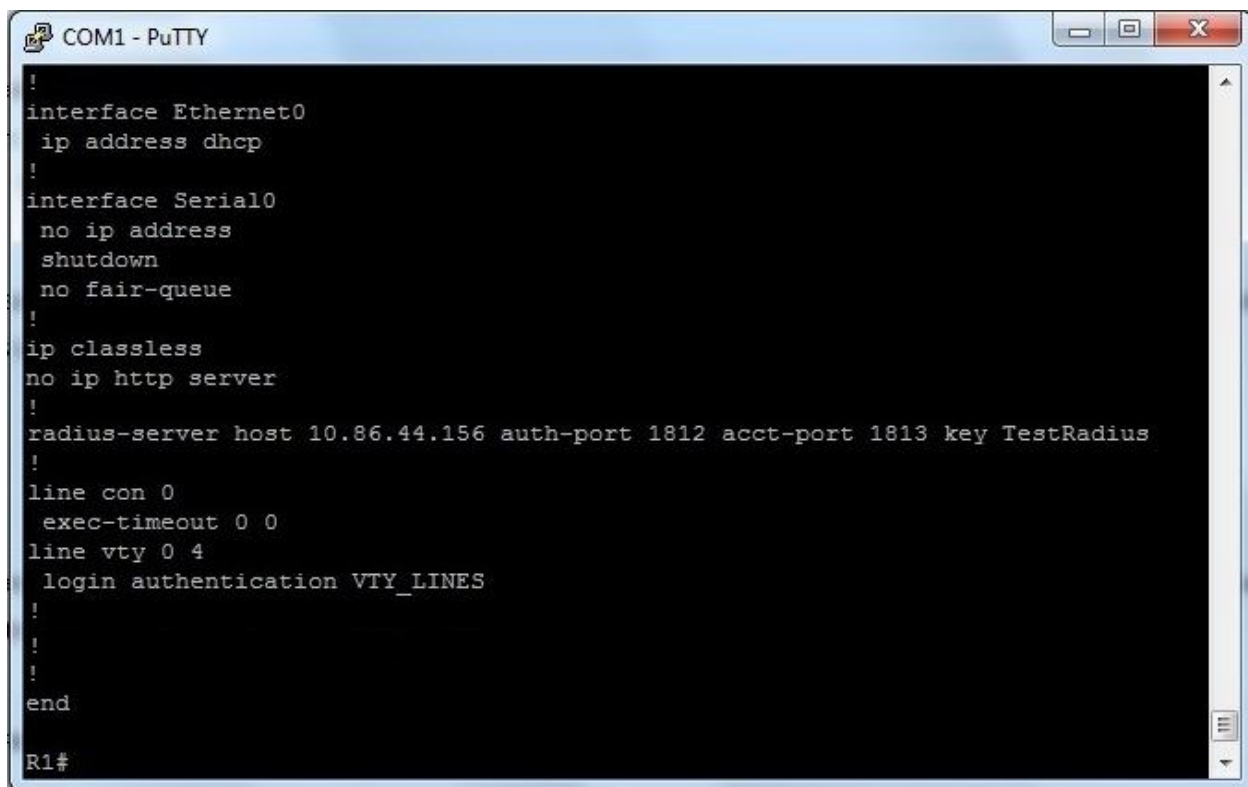
Step 4: Screenshots of Cisco Router's Configuration File



A screenshot of a PuTTY window titled "COM1 - PuTTY". The terminal shows the command "R1#sh running-config" and the output "Building configuration...". It then displays the current configuration, which is 731 bytes long. The configuration includes version 12.2, service timestamps for debug and log uptime, no service password-encryption, hostname R1, aaa new-model, aaa authentication login for VTY_LINES using a radius local group, enable password group5, a username testuser with password testpass, and ip subnet-zero. The output is preceded and followed by exclamation marks (!).

```
R1#sh running-config
Building configuration...

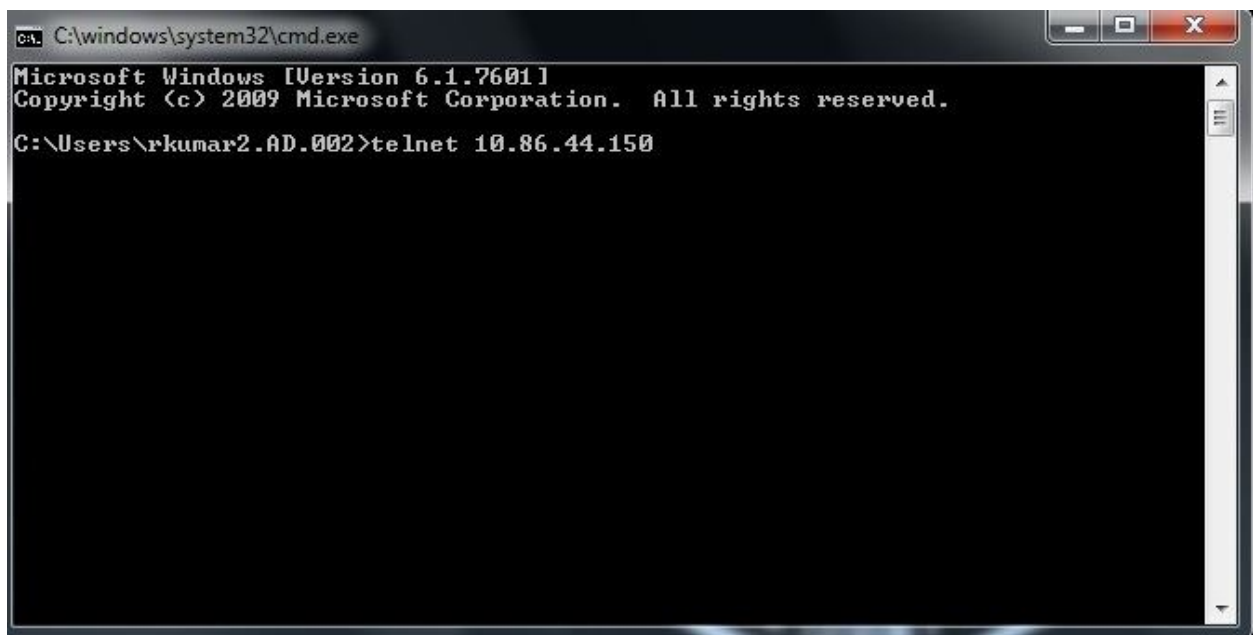
Current configuration : 731 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname R1
!
aaa new-model
aaa authentication login VTY_LINES group radius local
enable password group5
!
username testuser password testpass
ip subnet-zero
!
!
!
!
!
!
```



A screenshot of a PuTTY window titled "COM1 - PuTTY". The terminal shows the configuration of a Cisco router R1. The configuration includes interface Ethernet0 with ip address dhcp, interface Serial0 with no ip address, shutdown, and no fair-queue, ip classless, no ip http server, radius-server host 10.86.44.156 with auth-port 1812, acct-port 1813, and key TestRadius, line con 0 with exec-timeout 0 0, line vty 0 4 with login authentication VTY_LINES, and the end command. The prompt R1# is shown at the bottom.

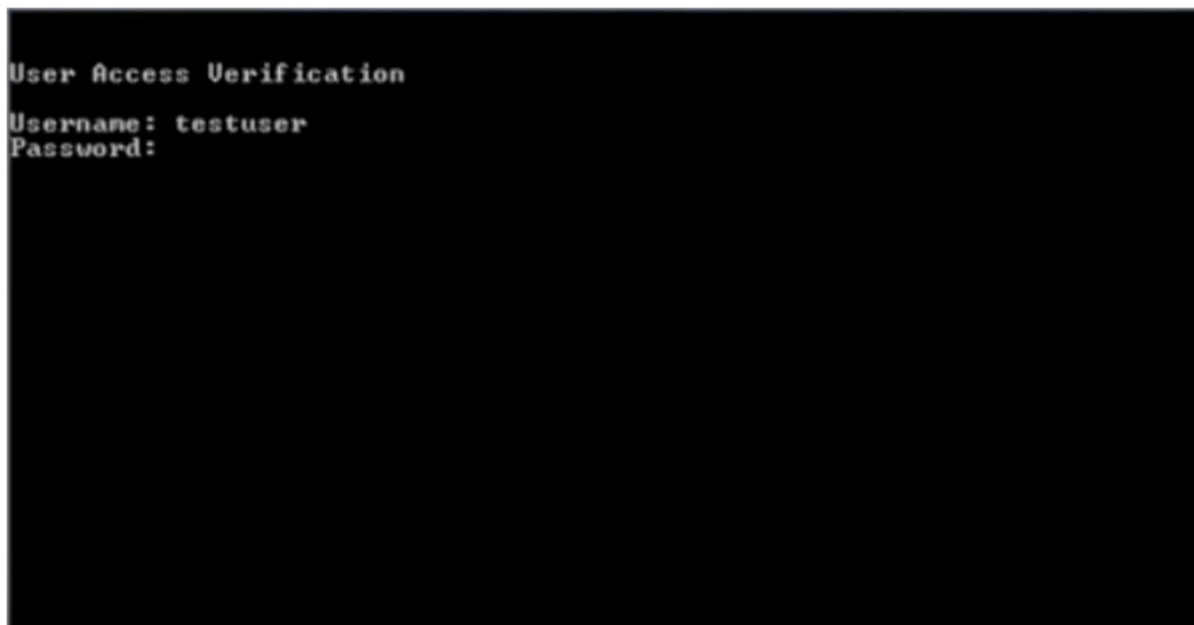
```
!
interface Ethernet0
 ip address dhcp
!
interface Serial0
 no ip address
 shutdown
 no fair-queue
!
ip classless
no ip http server
!
radius-server host 10.86.44.156 auth-port 1812 acct-port 1813 key TestRadius
!
line con 0
 exec-timeout 0 0
line vty 0 4
 login authentication VTY_LINES
!
!
!
end
R1#
```

Step 5: Screenshot of WinRadius when We telnet to our Router



A screenshot of a Windows command prompt window. The title bar shows the path "C:\windows\system32\cmd.exe". The window contains the following text: "Microsoft Windows [Version 6.1.7601] Copyright (c) 2009 Microsoft Corporation. All rights reserved. C:\Users\rkumar2.AD.002>telnet 10.86.44.150". The rest of the window is black, indicating the telnet connection is in progress or has failed.

```
C:\windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\rkumar2.AD.002>telnet 10.86.44.150
```



A screenshot of a telnet session. The text displayed is: "User Access Verification Username: testuser Password:". The rest of the screen is black, suggesting the session is waiting for input or has been terminated.

```
User Access Verification
Username: testuser
Password:
```

User Access Verification

Username: testuser

Password:

R1>

WinRadius - ???

Operation LOG Advanced Settings View Help

ID	Time	Message
.	2015y12m8d 17h21m5s	0 users were loaded
!	2015y12m8d 17h22m5s	WinRadius is running OK, (Auth port=1812, Acct port=1813, Secret=TestRadius)
i	2015y12m8d 17h25m5s	WinRadius is waiting for NAS request packets. If no request packet reached, pleas
f	2015y12m8d 17h30m5s	Selected collating sequence not supported by the operating system, : INSERT INTO
i	2015y12m8d 17h34m5s	Add user successfully.
i	2015y12m8d 17h46m5s	User (testuser) authenticate OK.
'	2015y12m8d 17h47m5s	User (testuser) authenticate OK.