Rocket®

MultiValue University 2015

D3 Security - Authentication

Lab Guide

Developed by
D3 MVU Team

Lab Overview

Abstract

The purpose of this lab is to demonstrate the two modes of authentication available in D3 (classic and host). The administrator will be guided through how to configure and use the system in each mode. The emphasis will be on host authentication and the benefits it provides, specifically the use of the same credentials used to access the domain.

About the Lab Environment

The lab environment uses the following:

- D3 10.1 Linux, vi, pick0 configuration file
- D3 9.2 Windows, D3 Device Manager
- Telnet client

This lab used a controlled environment at MV University. The following exercises can be done in your own environment but you must use caution. Know what the command does before you execute it.

Lab Overview

- Time estimate: 45 minutes
- There are six sections to this lab:
  - Section 1: Enabling Classic Authentication on Linux
  - Section 2: Enabling Classic Authentication on Windows
  - Section 3: Using Classic Authentication (Linux and Windows)
  - Section 4: Enabling Host Authentication on Linux
  - Section 5: Enabling Host Authentication on Windows
  - Section 6: Using Host Authentication (Linux and Windows)

Either or both the Linux and Windows tracks may be followed.

© 2015 Rocket Software, Inc. All Rights Reserved.
Lab materials may not be reproduced in whole or in part without prior written permission of Rocket Software.

Exercise 1: Enabling Classic Authentication on Linux

Purpose of the Exercise

This exercise will show you how to enable Classic Authentication on Linux.

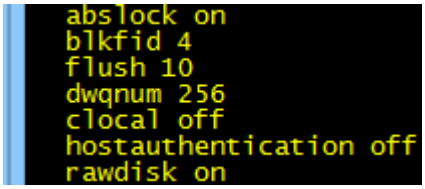
After this exercise you will be able to:

Enable Classic Authentication on Linux

Exercise Instructions

Perform the following steps:

__ 1. Enable Classic Authentication.



a. Run the following command:

```
vi /usr/lib/pick/pick0
```

b. If there is no entry for **hostauthentication**, insert one.

c. Set the **hostauthentication** value to **off**.

d. Save the file and exit vi.

©2015 Rocket Software, Inc. All Rights Reserved.
Lab materials may not be reproduced in whole or in part without prior written permission of Rocket Software.

__ 2. If D3 is running, reboot it – otherwise, only "Boot D3".

a. From the Linux shell, enter **d3** and respond to the promps as shown below:

```
user id: dm
master dictionary: dm
```

b. At the TCL prompt, enter:

```
shutdown
```

c. When prompted to continue, press **y**.

d. Boot D3:

```
d3 0
```

e. When prompted, press **x**.

Exercise 1 summary: Classic Authentication has been enabled on Linux.

End of Exercise 1

©2015 Rocket Software, Inc. All Rights Reserved.
Lab materials may not be reproduced in whole or in part without prior written permission of Rocket Software.

Exercise 2: Enabling Classic Authentication on Windows

Purpose of the Exercise

This exercise will show you how to enable Classic Authentication on Windows.

After this exercise you will be able to:

- Enable Classic Authentication on Windows

Exercise Instructions

Perform the following steps:

__ 1. Enable Classic Authentication

a. Select **Start** → **Programs** → **Rocket D3** → **Device Manager**.

b. On the D3 Settings tab in the Logon Security panel, make sure the **Users File** option is selected.

c. If necessary, click the **Update** button and then Exit.

©2015 Rocket Software, Inc. All Rights Reserved.
Lab materials may not be reproduced in whole or in part without prior written permission of Rocket Software.

__ 2. If D3 is running, reboot it – otherwise, only "Boot D3".

a. Telnet to localhost and respond to the promps as shown below:

```
user id: dm
master dictionary: dm
```

b. At the TCL prompt, enter:

```
shutdown
```

c. When prompted to continue press **y**.

d. Boot D3 from Windows Services.

Exercise 2 summary: Classic Authentication has been enabled on Windows.

End of Exercise 2

©2015 Rocket Software, Inc. All Rights Reserved.
Lab materials may not be reproduced in whole or in part without prior written permission of Rocket Software.

Exercise 3: Using Classic Authentication (Linux and Windows)

Purpose of the Exercise

This exercise will demonstrate how to display the D3 users file, the **who** command, how to detect the current authentication configuration and changing passwords. Much of this behavior may already be familiar as this is the way it has always been done.

After this exercise you will be able to:

- Detect whether D3 is using Classic or Host Authentication
- Change passwords for existing users

Exercise Instructions

Perform the following steps:

__ 1. Log in to D3.

a. Do one of the following”

- On Linux, from the shell, enter **d3**.
- On Windows, Telnet to localhost.

b. Respond to the promps as shown below:

```
user id: dm
master dictionary: dm
```

__ 2. Display the users file.

a. Enter the following command:

```
sort users
```

All of the available users are shown in the report. For this exercise there is a predefined user, **testuser1**. Note that **testuser1** does not have a value in the password column

©2015 Rocket Software, Inc. All Rights Reserved.
Lab materials may not be reproduced in whole or in part without prior written permission of Rocket Software.

__ 3. Switch to one of the test users and try the **who** command.

a. Enter the following command and then respond the prompts:

off

user id: **testuser1**

master dictionary: **dm**

b. Enter the following command:

who

```
:who
1 testuser1 dm
```

The current line number, user-id, and account name are displayed.

__ 4. Detect the current configuration.

a. From the command line, enter:

getlogonmode

```
:getlogonmode
D3 DM,USERS, mode
```

This shows that D3 is configured to use the D3 users file (aka Classic Authentication).

__ 5. Change the password.

a. From the command line, enter:

password

b. When prompted to change a user or account password, enter **u**.

c. Enter your user-id:

testuser1

d. Finally, enter and re-enter the new password.

e. Display the users file. Note that now **testuser1** has a value in the password column (not shown in clear text).

__ 6. Test the password.

a. Log off and back on as **testuser1**.

This time there is a password challenge.

b. Enter the password to proceed with the logon.

Exercise 3 summary: Detecting whether D3 is running in Classic or Host Authentication mode.

End of Exercise 3

©2015 Rocket Software, Inc. All Rights Reserved.
Lab materials may not be reproduced in whole or in part without prior written permission of Rocket Software.

Exercise 4: Enabling Host Authentication on Linux

Purpose of the Exercise

This exercise will show you how to enable Host Authentication on Linux.

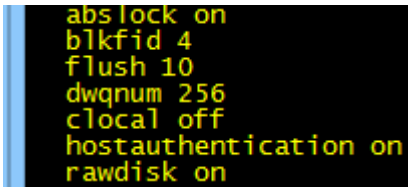
After this exercise you will be able to:

- Enable Host Authentication on Linux

Exercise Instructions

Perform the following steps:

__ 1. Enable Host Authentication.



a. Run the following command:

```
vi /usr/lib/pick/pick0
```

b. If there is no entry for **hostauthentication**, insert one.

c. Set the **hostauthentication** value to **on**.

d. Save the file and exit vi.

©2015 Rocket Software, Inc. All Rights Reserved.
Lab materials may not be reproduced in whole or in part without prior written permission of Rocket Software.

__ 2. If D3 is running, reboot it, otherwise only "Boot D3"

a. From the Linux shell enter **d3** and respond to the promps as shown below:

```
user id: dm
master dictionary: dm
```

b. At the TCL prompt, enter:

```
shutdown
```

c. When prompted to continue, press **y**.

d. Boot D3:

```
d3 0
```

e. When prompted, press **x**.

Exercise 4 summary: Host Authentication has been enabled on Linux.

End of Exercise 4

©2015 Rocket Software, Inc. All Rights Reserved.
Lab materials may not be reproduced in whole or in part without prior written permission of Rocket Software.

Exercise 5: Enabling Host Authentication on Windows

Purpose of the Exercise

This exercise will show you how to enable Host Authentication on Windows.

After this exercise you will be able to:

Enable Host Authentication on Windows

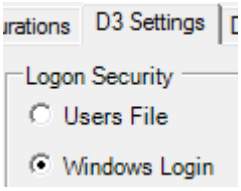
Exercise Instructions

Perform the following steps:

__ 1. Enable Host Authentication.

a. Select **Start** → **Programs** → **Rocket D3** → **Device Manager**.

b. On the D3 Settings tab in the Logon Security panel, make sure the **Windows Login** option is selected.



c. If necessary, click the **Update** button and then Exit.

©2015 Rocket Software, Inc. All Rights Reserved.
Lab materials may not be reproduced in whole or in part without prior written permission of Rocket Software.

__ 2. If D3 is running, reboot it – otherwise, only "Boot D3".

a. Telnet to localhost and respond to the promps as shown below:

```
user id: dm
master dictionary: dm
```

b. At the TCL prompt, enter:

```
shutdown
```

c. When prompted to continue, press **y**.

d. Boot D3 from Windows Services.

Exercise 5 summary: Host Authentication has been enabled on Windows.

End of Exercise 5

©2015 Rocket Software, Inc. All Rights Reserved.
Lab materials may not be reproduced in whole or in part without prior written permission of Rocket Software.

Exercise 6: Using Host Authentication (Linux and Windows)

Purpose of the Exercise

This exercise will demonstrate the behavior of D3 with Host Authentication enabled. The behavior of logging off and on will be explored as well as the haforcecheck option, users item, and changing passwords.

After this exercise you will be able to:

- Detect whether D3 is using Classic or Host Authentication
- Use the haforcecheck option to configure the challenge for credentials
- Use the u71 user exit to programmatically configure the haforcecheck option
- Create a users item to customize the logon experience after authenticating
- See the behavior of changing the users password at the operating system level

Exercise Instructions

Perform the following steps:

__ 1. Log in to D3.

a. Do one of the following:

- On Linux, from the shell, enter **d3**.
- On Windows, Telnet to localhost.

b. Respond to the promp as shown below:

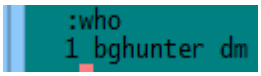
```
master dictionary: dm
```

Notice that there was no challenge for a user-id and password. The premise behind Host Authentication is that the user has already authenticated with the host operating system. Therefore, there is no need to challenge the user again.

__ 2. Issue the **who** command.

a. Enter the following command

who



Notice that on both Linux and Windows the user-id matches the one used to start the D3 process.

©2015 Rocket Software, Inc. All Rights Reserved.
Lab materials may not be reproduced in whole or in part without prior written permission of Rocket Software.

- On Linux, D3 is multi-process, single threaded. Therefore, the user-id will match the one used to logon to the host operating system. In other words, each client shows as the user that started the client.
- On Windows, D3 is single process, multi-threaded. Therefore, the user-id will match the one used to start the D3 process. In other words, each client shows as the same user-id. This is probably not ideal. Typically, the Telnet Forced Host Authentication setting should be enabled. This is shown in one the following steps.

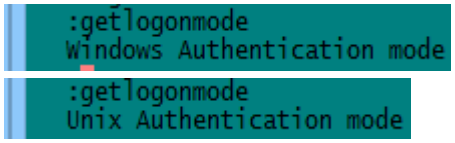
__ 3. Display the users file.

a. Enter the following command:

sort users

Notice that there is no entry for the user-id shown by the **who** command. This is because the D3 users file is not being used.

__ 4. Detect the current configuration.



a. From the command line, enter:

getlogonmode

This shows that D3 is configured to use the host operating system for authentication (aka Host Authentication)

__ 5. Log off.

b. From the command line, enter:

off

Notice that even though an **off** (not an **exit**) was issued, you have returned to the shell (Linux) or disconnected (Windows) instead of returning to a logon prompt. This is because there was no logon prompt when logging in. So, there is no logon prompt to which to return.

__ 6. Set the haforcecheck option programmatically using u71.

The haforcecheck option instructs Host Authentication to force the checking of credentials. If this option is set, the user will be challenged for a user-id and password instead of dropping straight to the master dictionary prompt. This also creates a method by which a user may choose to log in to D3 using different credentials than those supplied when logging into the network. It may be set programmatically using the BASIC user exit u71.

©2015 Rocket Software, Inc. All Rights Reserved.
Lab materials may not be reproduced in whole or in part without prior written permission of Rocket Software.

a. Create, compile, and run the following program, which enables the haforcecheck option:

```
code = oconv( "1", "u71" )
```

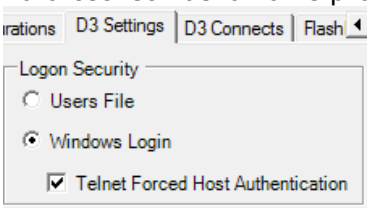
b. Log off by entering **off**.

Notice that this time a challenge for credentials is displayed.

c. On Linux there is also a **haforcecheck** option that may be added to the command line to force challenging the user for credentials:

```
d3 haforcecheck
```

On Windows, since users directly connect to D3 without going through a shell, the ability to set the default haforcecheck behavior is provided through the D3 Device Manager.



__ 7. Log on as a different user.

a. The following user and password have already been created. Use these credentials to log on.

user id: **hatestuser**

password: **MVUgetready**

master dictionary: **dm**

__ 8. Change your password.

1. Change the password for the **hatestuser**.
   - From the Linux shell, use the **passwd** command.
   - From Windows use the VMware menu: Click on VM => Send Ctrl + Alt + Delete → Change a password.
2. Log off from D3 and then back on. The new password will be required.

__ 9. The D3 users file revisited.

As demonstrated, the D3 users file is not being used for authentication. However, the other features available in a users file item are still available.

a. Create a users item with an item-id matching your operating system user-id. That is, the user-id shown by the **who** command.

©2015 Rocket Software, Inc. All Rights Reserved.
Lab materials may not be reproduced in whole or in part without prior written permission of Rocket Software.

b. Set the privilege attribute to **sys2** and the macro to **to dm**. If the line editor or some other editor is being used, privilege is attribute 8 and macro is attribute 12.

```
:u users bghunter

users  'bghunter' NEW ITEM
name       Big Game Hunter
address
zip
phone
keys
password
privilege  sys2
options
macro      to dm
users  'bghunter' NEW ITEM size = 54 filed.
```

c. Log off and then back on. Notice that this time there is no **master dictionary:** prompt.

d. Create, compile, and run the following program, which disables the haforcecheck option:

```
code = oconv( "0", "u71" )
```

e. Log off and the back on. Notice that the user goes straight to the TCL command prompt without being challenged for credentials or a master dictionary.

Exercise 6 summary: Detecting whether D3 is running in Classic or Host Authentication mode, haforcecheck option, u71 user exit, users item and the effect of password changes.

End of Exercise 6

©2015 Rocket Software, Inc. All Rights Reserved.
Lab materials may not be reproduced in whole or in part without prior written permission of Rocket Software.