

Milestone Two

MILESTONE REQUIREMENTS

User Login
Pages Display
Assign User Permissions
View Neflow

CHECKS

User Login	Yes
I am able to login as deepika@gmail.com	
I am able to login as admin@netflow.com	
* There are two login screens. The first, index.php, does not work with admin. The other, index.php/login works with admin. There should be only one login screen!	
Pages Display	Yes
Assign User Permissions	
- Assign Single folder	No. We are only able to assign users all sources. The sources are found under the "live" folder.
- Assign Multiple folders	
Add Users	Yes
Delete Users	Yes
View Netflow (Charts)	
- Selected January 1 st , 2018 (00:00) through current date of April 24 th , 2018 (04:45)	Fails. See 1 st error below.
- Selected February 2 nd , 2018 (00:00) through February 2 nd , 2018 (04:45)	Yes.
- Edit Chart	I changed Test from aggregate by SourceID to aggregate by protocol and from top 1 to top 20. It did not effect the chart. However, changing the chart from bar to line took effect. Charts should be limited to the user that created to them. Is this true?
- Add Chart	I add a new chart, Test2. As deepika@gmail.com, I should



not have access to all available data. The chart was aggregated by protocol and shows the top 20. I got the same chart as Test. Both seem, despite the configuration, to be using port numbers. They also seem to be showing all instead of the top X.

- Delete Chart
- Use standard nfdump filter with chart
- Schedule Chart

Failed. See 2nd error below.
Adding a filter had no effect.

View Netflow (Tables)

- I don't see an option for that.

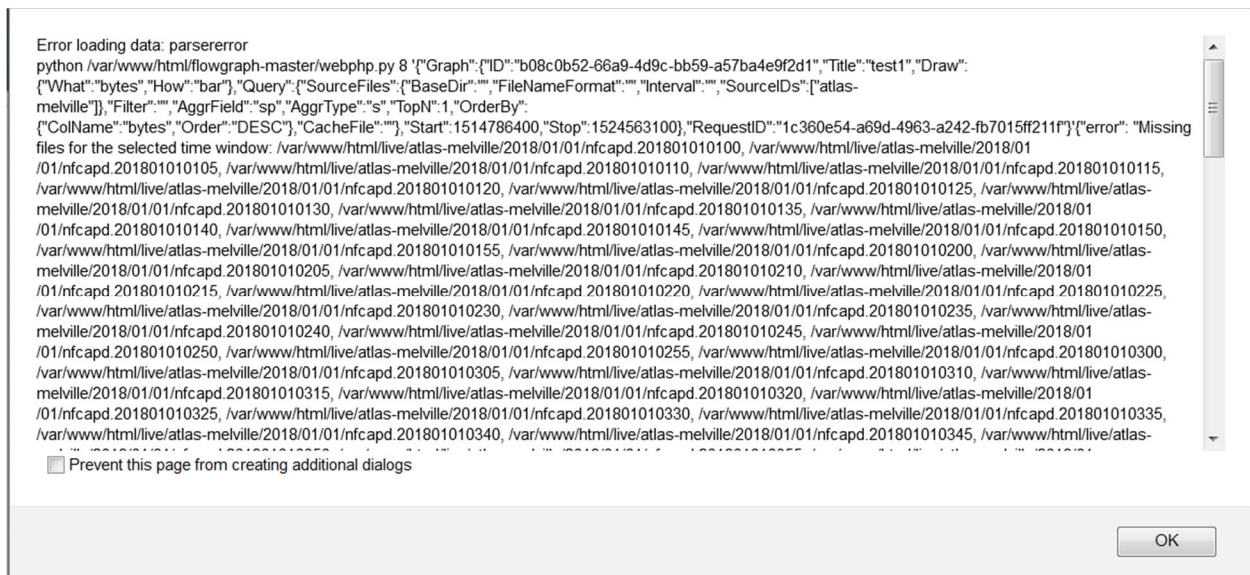
View Profile

- Select folder
- Change password

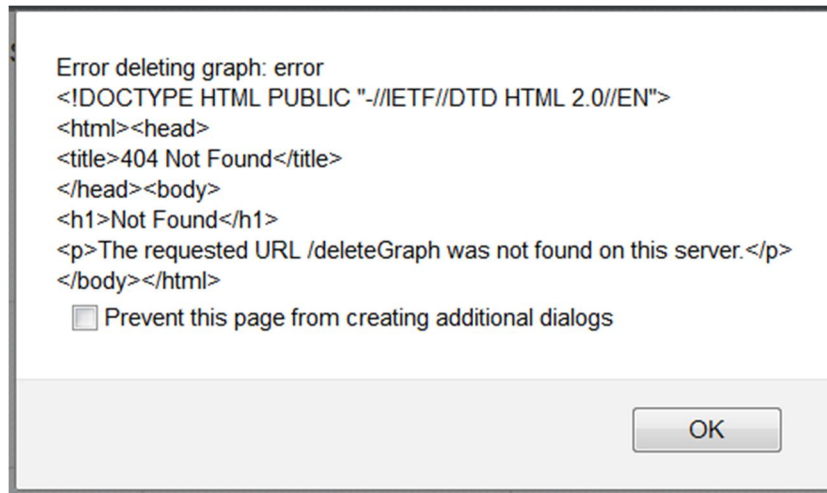
As a user, I should not be able to select folders!

Yes

ERRORS



The error should not reveal internal paths. Is it possible to build chart with what is there?



Shouldn't this be there?

Milestone Three

MILESTONE REQUIREMENTS

User Login
Pages Display
Assign User Permissions
View Neflow

CHECKS

User Login Yes

I am able to login as khalid@gmail.com

I am able to login as admin@netflow.com

Pages Display Yes

Assign User Permissions

- Assign Single folder Yes

After creating info@hellfiresecurity.com and assigning a single folder, I logged into the user to see if only that folder was available. It is, however, despite this being a new user. I already have a profile image and several charts. I shouldn't have either. I have created this user before. I suspect the charts were orphaned before and accessible once another user with the same name was created. See "Other" below.

- Assign Multiple folders Yes

Add Users Yes

Delete Users Yes

View Netflow (Charts)

- Selected January 1st, 2018 (00:00) through current date of April 24th, 2018 (04:45) Yes

- Selected February 2nd, 2018 (00:00) through February 2nd, 2018 (04:45) Yes

The legend is not in order.

- Edit Chart Yes

- Add Chart Yes

- Delete Chart Yes

- Use standard nfdump filter with chart Yes

- Schedule Chart

View Netflow (Tables)

- The results do not match what you would expect. As an example, please see "Other" below.

- Initially, the rows are not in order. If I have selected in descending order by bytes, the rows are not in descending order by bytes. You have to put them in that order by yourself. They should start in that order.

View Profile

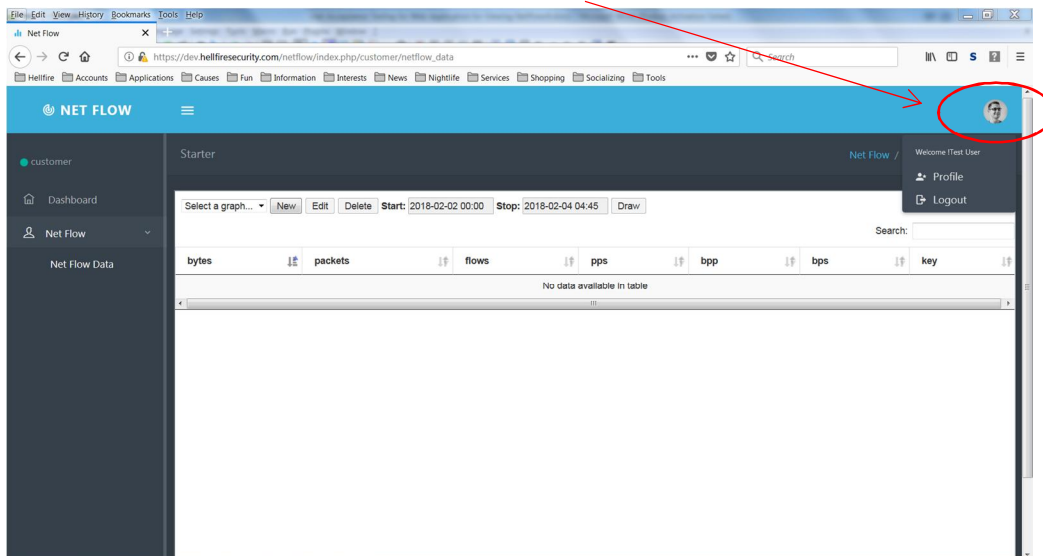
- Select folder
- Change password

Just remove this. See "Other" below.

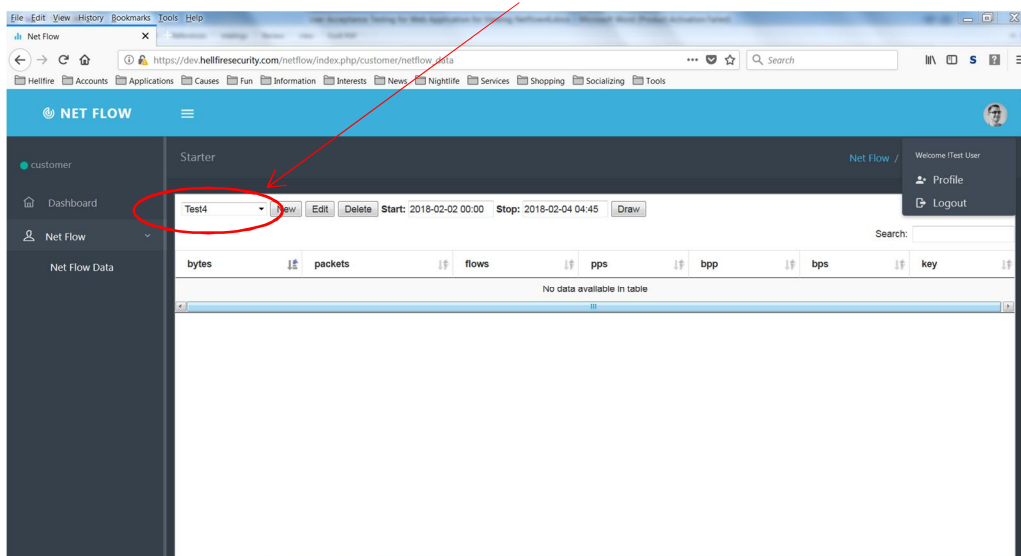
Yes

OTHER

This is a new user. It shouldn't have a profile picture.

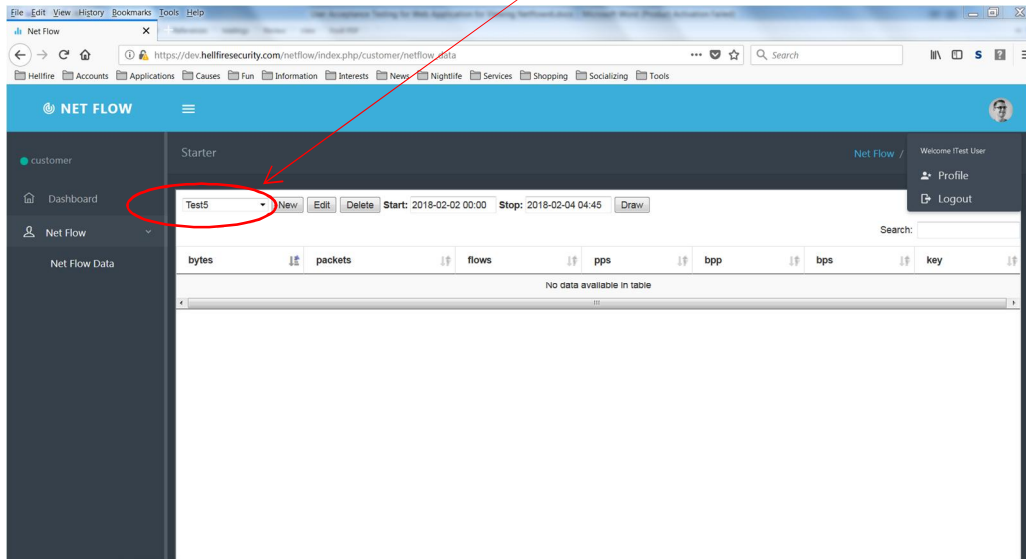


This is a new user. It shouldn't have any charts.

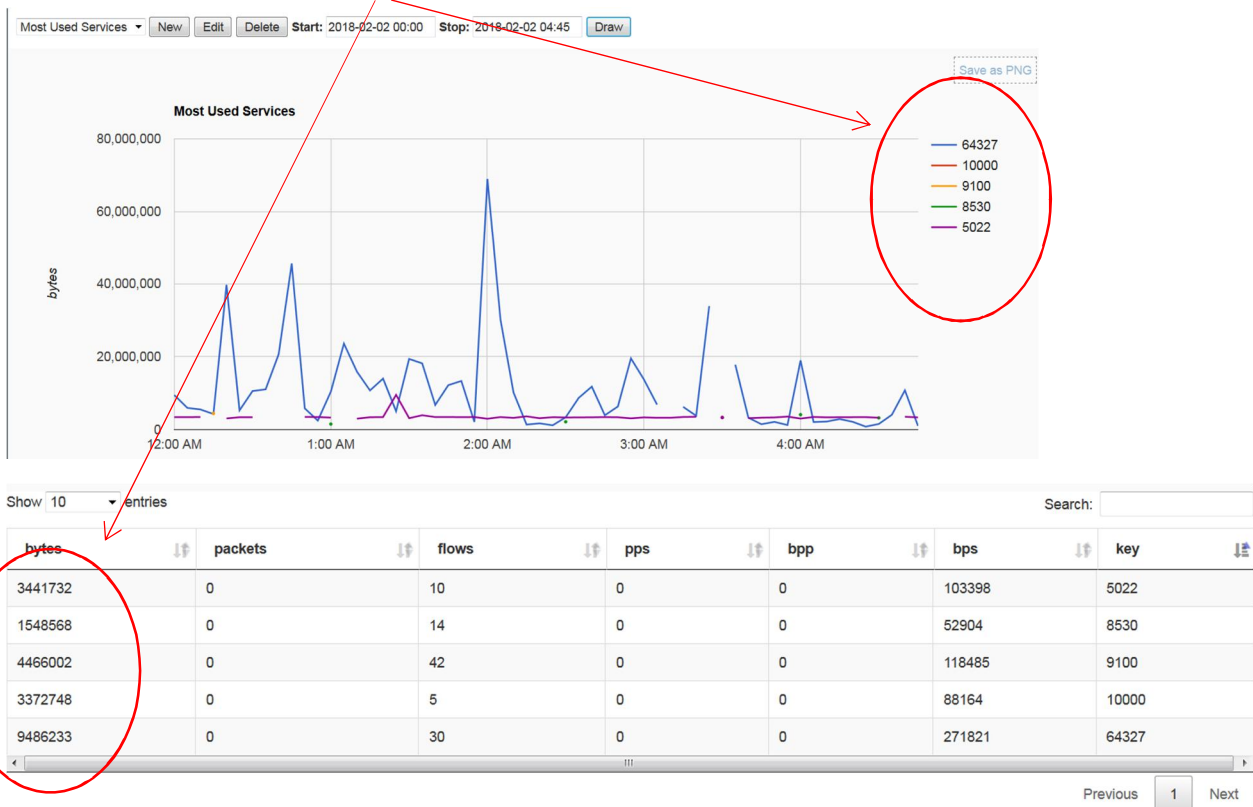


OTHER (CONTINUED)

This is a new user. It shouldn't have any charts.



This is not what you would expect to get.






You would expect this instead.

```
[ec2-user@ip-172-30-0-27 ~]$ nfdump -M /home/netflow/cloud-alerts/data/live/atlas-melville:atlas-stlouis -T -R 2018/02/02/nfcpad.201802020000:2018/02/02/nfcpad.201802020445 -n 5 -s dstport/bytes
Top 5 Dst Port ordered by bytes:
Date first seen      Duration Proto      Dst Port  Flows(%)  Packets(%)  Bytes(%)  pps      bps      bpp
2018-02-01 17:01:23.785 21750.020 any      64327     1716( 0.3) 0( 0.0)    792.3 M(19.2) 0 291418  0
2018-01-31 12:09:27.568 125716.647 any      444       67958(13.5) 0( 0.0)    691.7 M(16.7) 0 44015  0
2018-02-01 18:14:55.055 17400.990 any      2525     3732( 0.7) 0( 0.0)    501.3 M(12.1) 0 230473  0
1969-12-31 19:00:00.005 1517544296.140 any  443      179400(35.6) 0( 0.0)    470.5 M(11.4) 0  0      2  0
2018-02-01 18:14:58.145 17398.680 any      475      1173( 0.2) 0( 0.0)    441.4 M(10.7) 0 202944  0

Summary: total flows: 503343, total bytes: 4133295457, total packets: 0, avg bps: 21, avg pps: 0, avg bpp: 0
Time window: Time Window unknown
Total flows processed: 503343, Blocks skipped: 0, Bytes read: 30252548
Sys: 0.069s flows/second: 7227578.2 Wall: 0.072s flows/second: 6959460.8
[ec2-user@ip-172-30-0-27 ~]$
```

 **Customer Update Profile**

First Name :

khalid

Last Name :

hashmi

Email :

khalid@gmail.com

Phone Number :

8743265328

Select Folder :

atlas-melville

atlas-stlouis

Remove

UPDATE

ADDITIONAL

- This needs to be given a penetration test
- What is the password policy?
- What is the procedure for password reset by the user? Is the password reset by the user? Is it reset by the administrator?

Improvements

- We need a valid certificate
- Switch to a graph like nfsen (rrd). Until then, remove bar, line charts, scheduling, and advanced. The protocols could be changed from numbers to names.
- Switch from MySQL to sqlite
- Messaging is a little off. The "Delete User" confirmation has inconsistent capitalization. The response is a pop-up. The "Add User" response appears at the top of the user list. Not all pop-ups are the same color or using the same button styles.