

OB360 USER MANUAL

Vulnerability Test Flow

We will need the following information to do the Vulnerability Test.

1. VPN Details

- VPN Username and VPN Password
- VPN configuration files
- IP address range

2. Linux Network Details

- Network administrator username and password
- IP address list or range

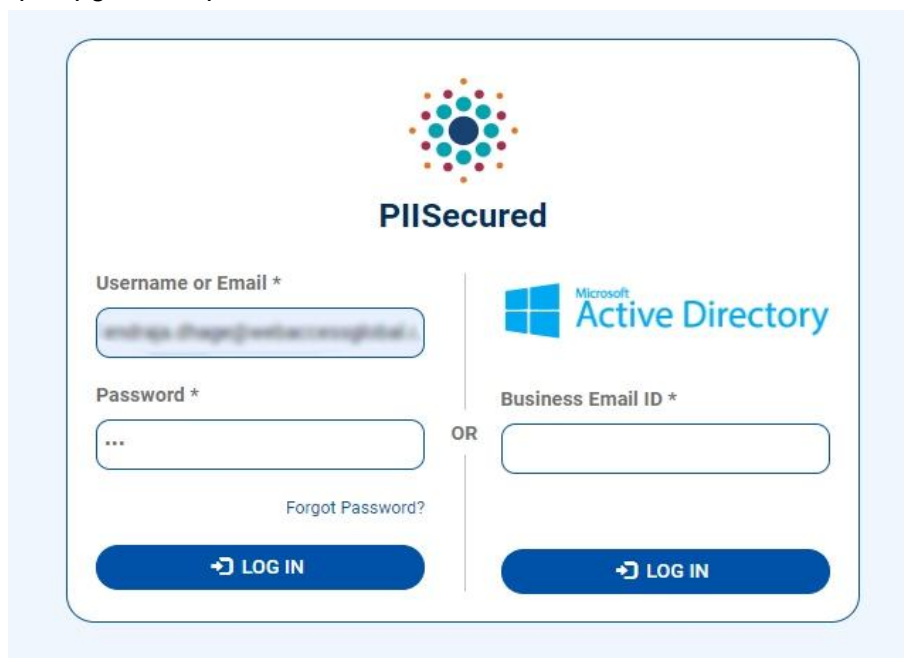
3. Windows Network Details

- Network administrator username and password
- Network Domain name
- IP address list or range
- Remote access should be enabled for accessing windows systems.

The steps for creating a vulnerability test in the OB360 application :

Step 1: Go to the PII Secured portal and use your partner user credentials to log in.

URL : <https://pg-ob360.piisecured.com/>



The login screen for PII Secured features a central logo at the top. Below it, there are two main login paths. The left path is for 'Username or Email' and 'Password', with a 'Forgot Password?' link. The right path is for 'Business Email ID' and includes a 'Microsoft Active Directory' logo. Both paths have a 'LOG IN' button. An 'OR' separator is placed between the two paths.

Figure : Login Screen

Step 2 : After login, go to the side menu bar section. Click on the 'OB360 Login' button.

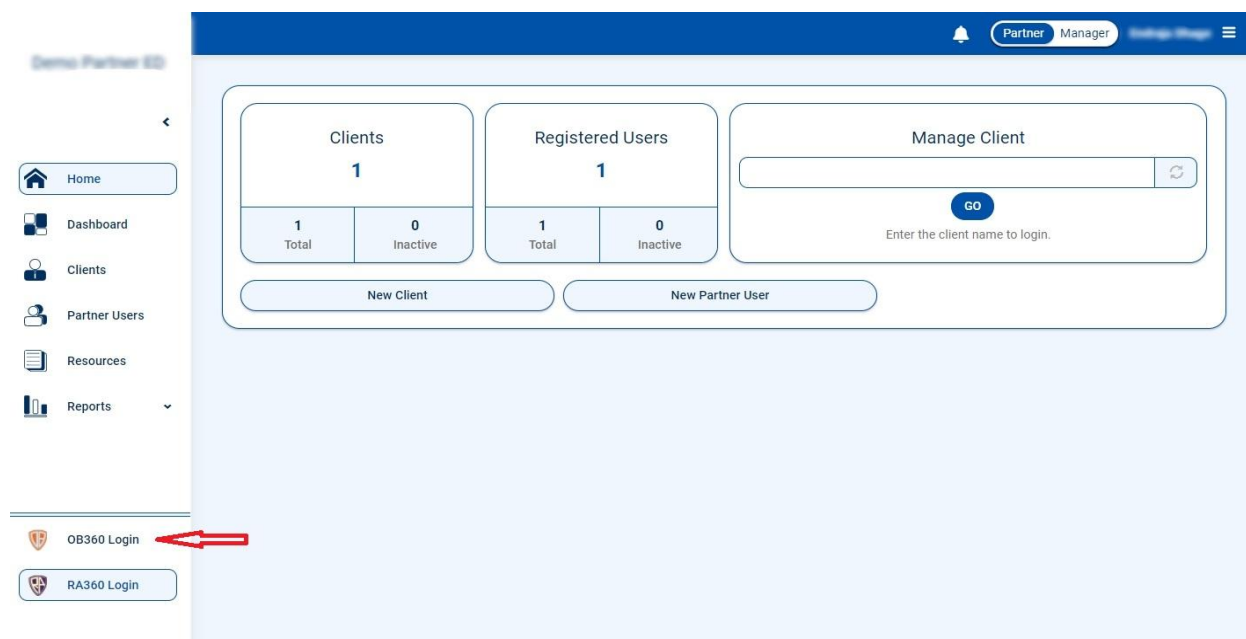
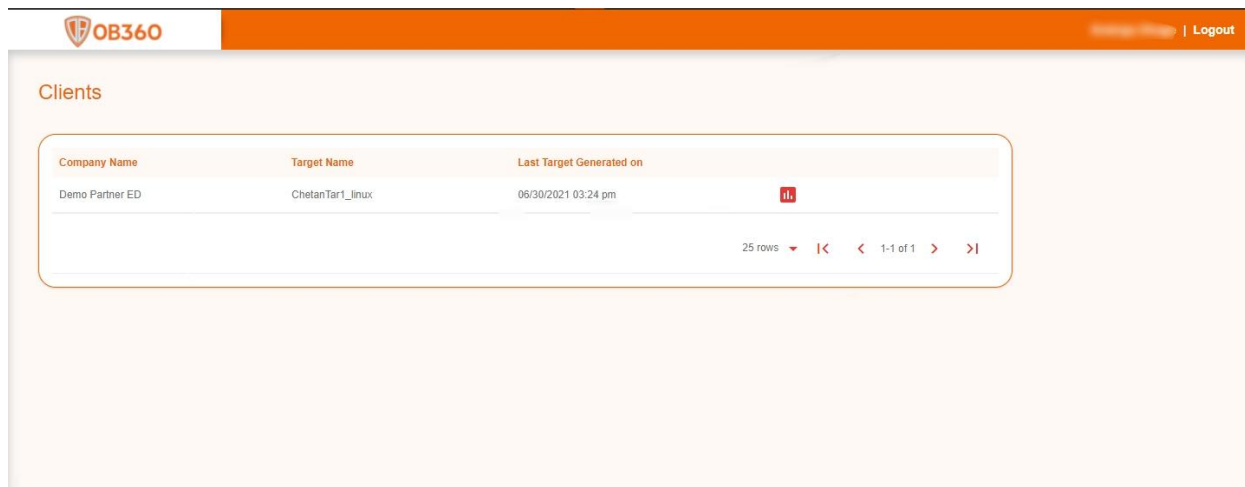



Figure : Home Screen

Step 3: You will now be redirected to the ob360 application in a new tab.



The screenshot shows the OB360 application interface. At the top, there is an orange header bar with the OB360 logo on the left and "Welcome User | Logout" on the right. Below the header, the page title "Clients" is displayed. A table is shown with the following data:

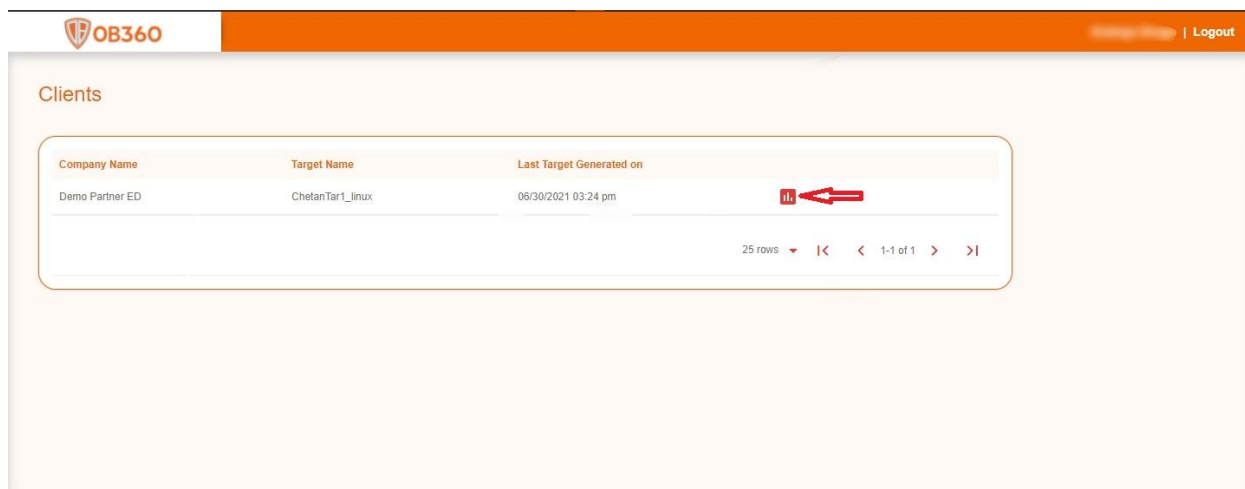
Company Name	Target Name	Last Target Generated on	
Demo Partner ED	ChetanTar1_linux	06/30/2021 03:24 pm	

At the bottom right of the table, there is a pagination control showing "25 rows", navigation arrows, and "1-1 of 1".


Figure : Clients Screen 1

Here you will see a client list with its latest created target.

Step 4: Click on the "Vulnerability Test" icon for creating a new vulnerability test.



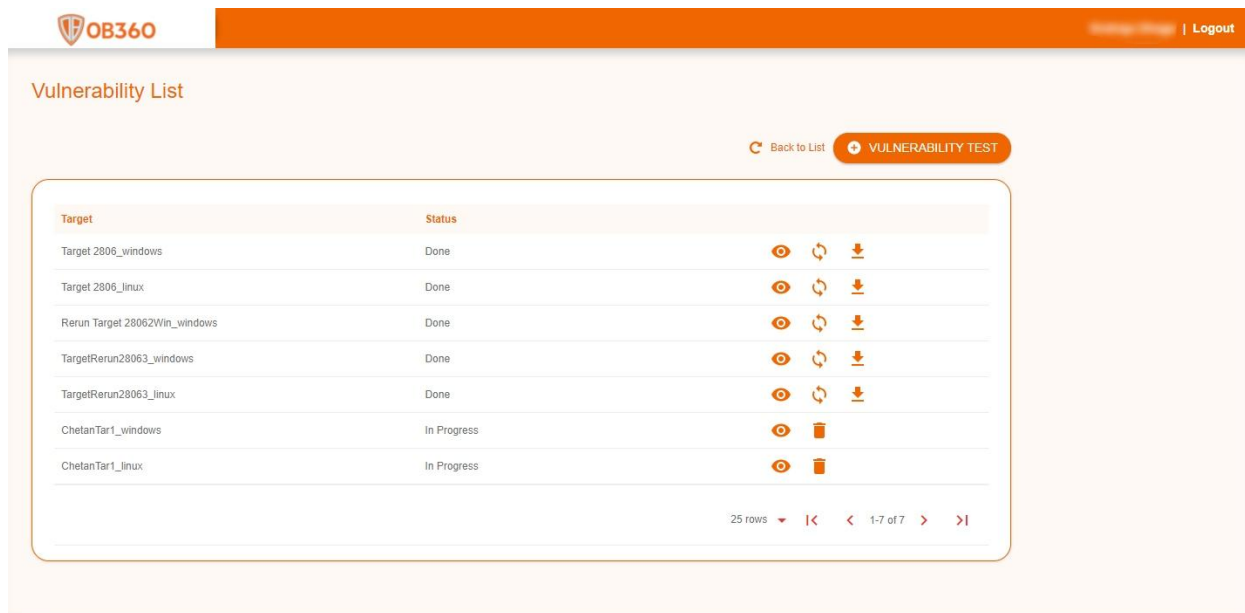
This screenshot is identical to the previous one, but with a red arrow pointing to the "Vulnerability Test" icon in the table row.

Company Name	Target Name	Last Target Generated on	
Demo Partner ED	ChetanTar1_linux	06/30/2021 03:24 pm	

The red arrow points to the icon in the fourth column of the first data row.

Figure : Clients Screen 2

Here you will see a list of all Vulnerabilities along with their current status.



Vulnerability List

Back to List VULNERABILITY TEST

Target	Status	Icons
Target 2806_windows	Done	🔍 ↻ ⬇️
Target 2806_linux	Done	🔍 ↻ ⬇️
Rerun Target 28062Win_windows	Done	🔍 ↻ ⬇️
TargetRerun28063_windows	Done	🔍 ↻ ⬇️
TargetRerun28063_linux	Done	🔍 ↻ ⬇️
ChetanTar1_windows	In Progress	🔍 🗑️
ChetanTar1_linux	In Progress	🔍 🗑️

25 rows |< < 1-7 of 7 > >|

Figure : Vulnerability List Screen 1

Through this page you will be able to do the following activities :

1. Creating a new vulnerability test.
2. View status of created task.
3. Make a copy of the target.
4. Download the report.

Step 5: To create a new vulnerability test click on 'VULNERABILITY TEST' button.

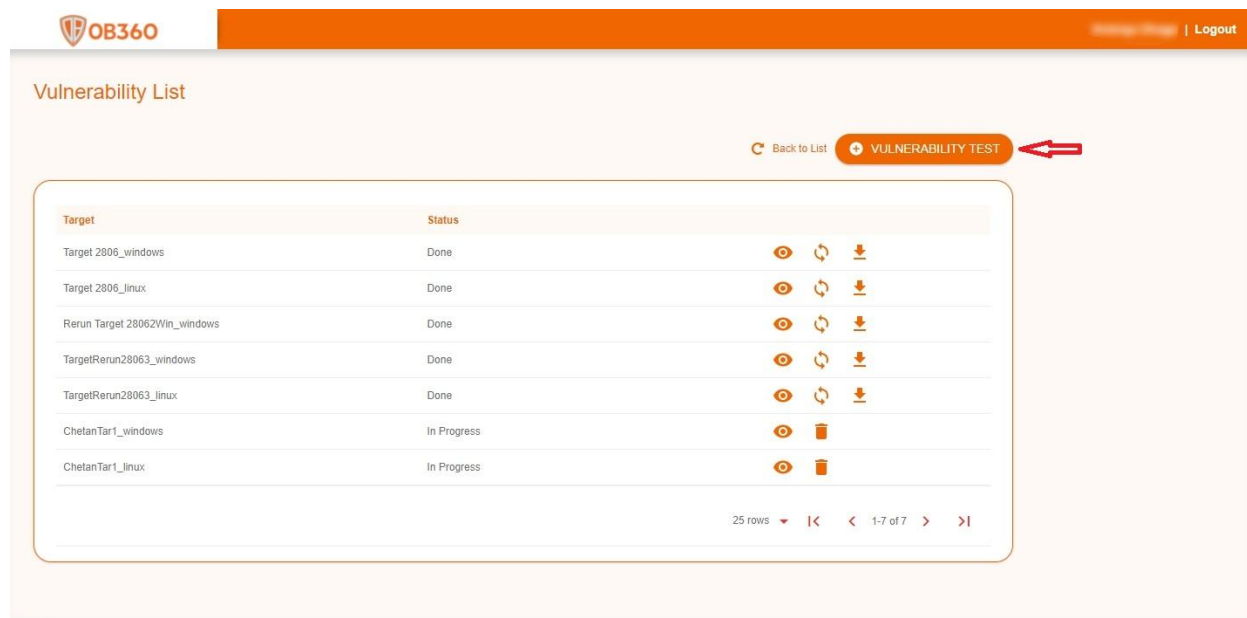


Figure : Vulnerability List Screen 2

Step 6: Now you will redirect to the target page. Do the following steps to create a target.

- Enter the Target Name, IP Range, VPN Username and VPN Password.
- Upload VPN configuration file given by your network administrator.
- Click on the 'Test Connection' button.

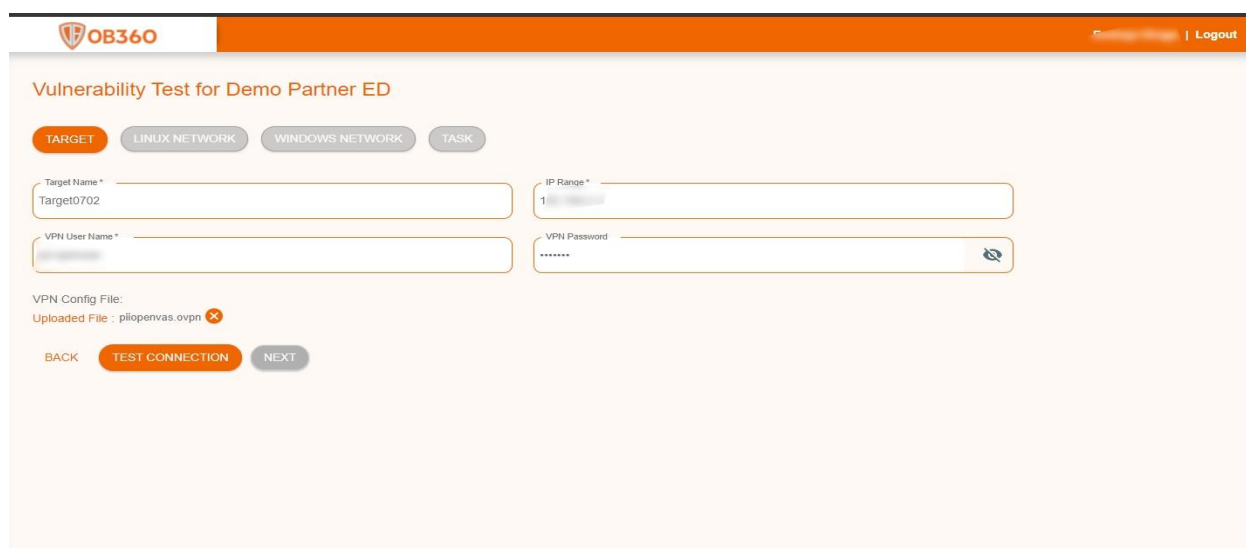
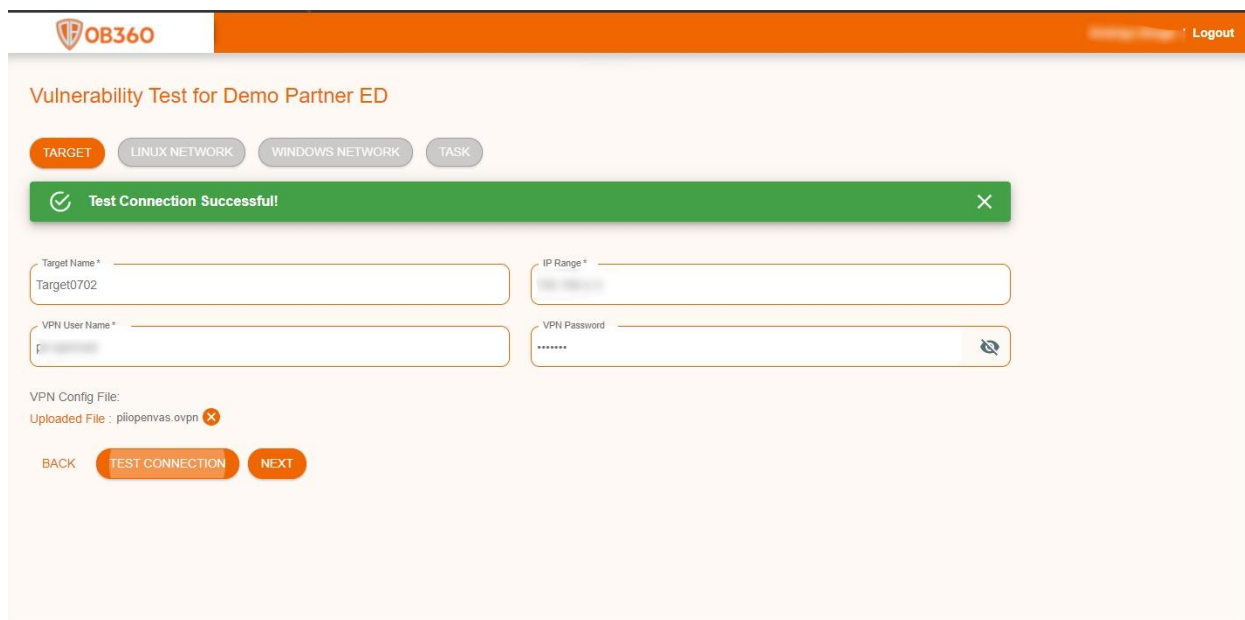


Figure : Target Screen

After Successful test connection you will get the 'Test Connection Successful' message and the 'Next' button will be enabled.

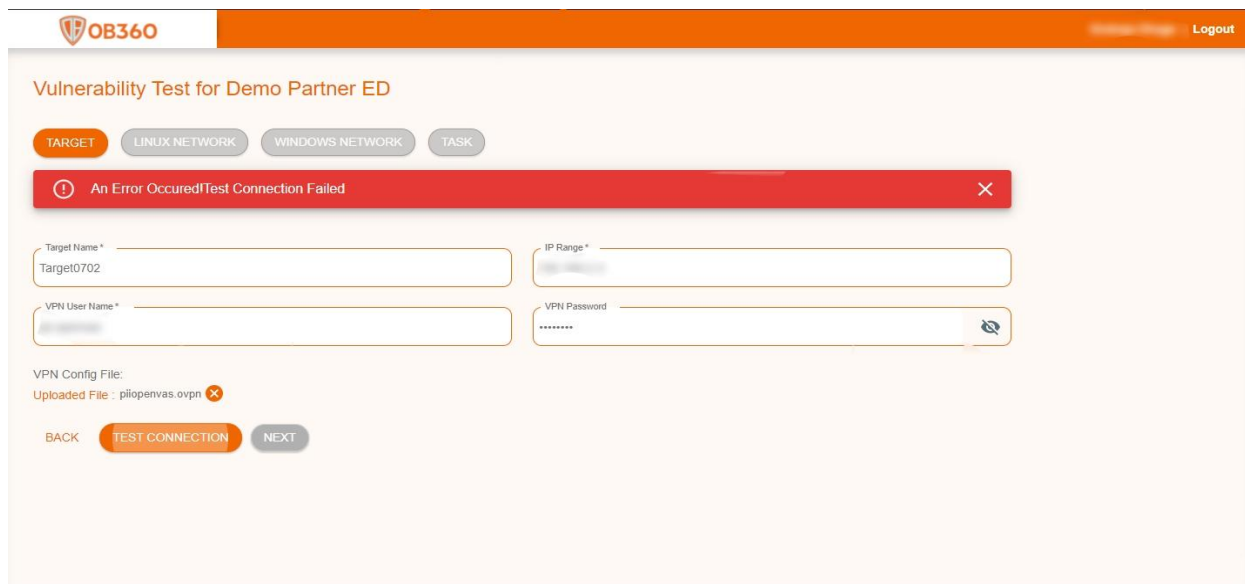


The screenshot shows the OB360 web interface for a vulnerability test. At the top, there's a navigation bar with the OB360 logo and a 'Logout' link. Below the navigation bar, the title 'Vulnerability Test for Demo Partner ED' is displayed. There are four tabs: 'TARGET' (selected), 'LINUX NETWORK', 'WINDOWS NETWORK', and 'TASK'. A green success message banner reads 'Test Connection Successful!'. Below this, there are four input fields: 'Target Name *' (containing 'Target0702'), 'IP Range *' (containing '10.10.10.10'), 'VPN User Name *' (containing 'f'), and 'VPN Password' (containing '*****'). Below the input fields, it says 'VPN Config File: Uploaded File : pilopenvas.ovpn' with a red 'x' icon. At the bottom, there are three buttons: 'BACK', 'TEST CONNECTION' (highlighted in orange), and 'NEXT'.

OB360 | © Copyright 2020

Figure : Target Success Screen

If you get an error message 'Test Connection Failed' then enter correct credentials for target and try again till you get the success message.



The screenshot shows the same OB360 web interface as the previous one, but with a red error message banner that reads 'An Error Occured!Test Connection Failed'. The input fields and buttons are the same as in the previous screenshot.

Figure : Target Failure Screen

Step 7: After the Next button is enabled click on it.

On clicking the next button a popup window will appear showing 'Do You have Linux Domain?'

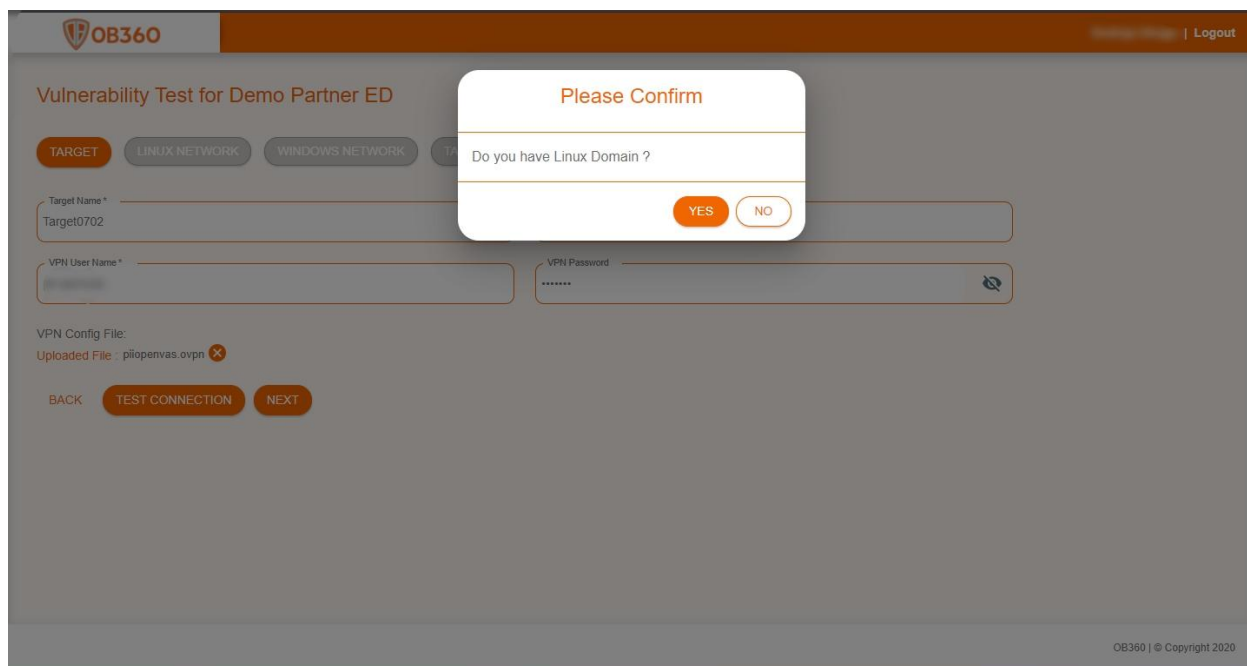


Figure : Linux Confirmation Screen

Click on 'Yes' if you have linux network else click on 'No'

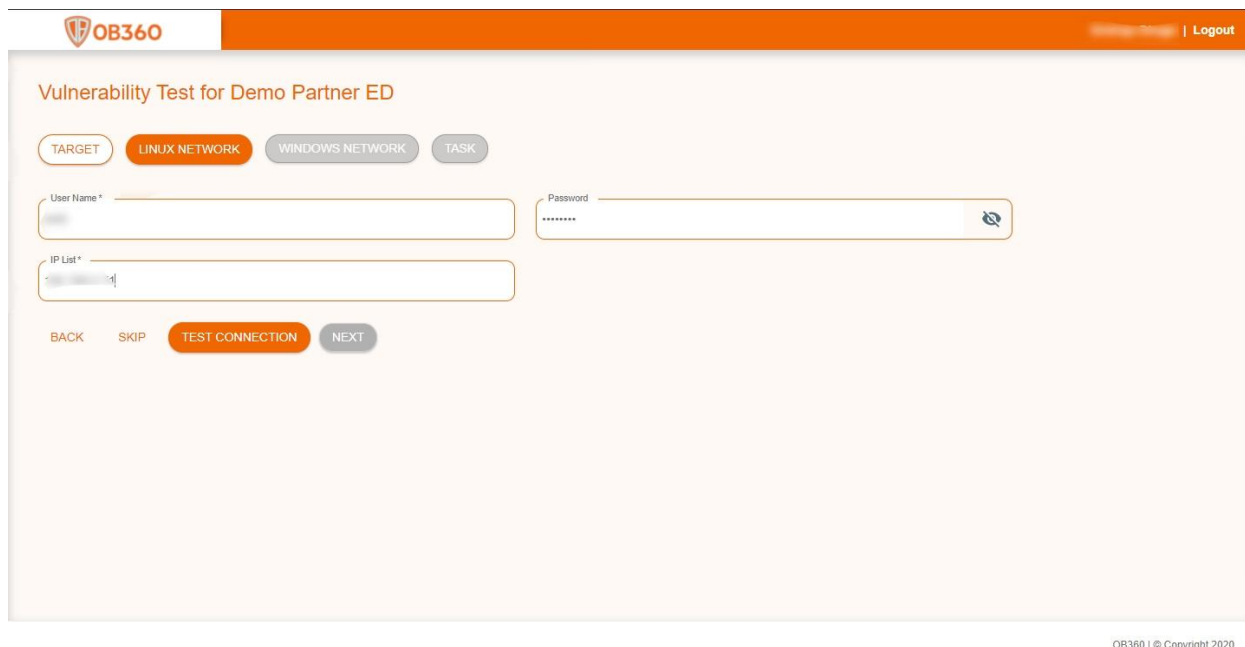
On click of 'Yes' you will redirect to step 8.

On click of 'No' you will redirect to step 10.

Step 8: Now you will redirect to the linux network page.

Do the following steps to create a target for the linux network.

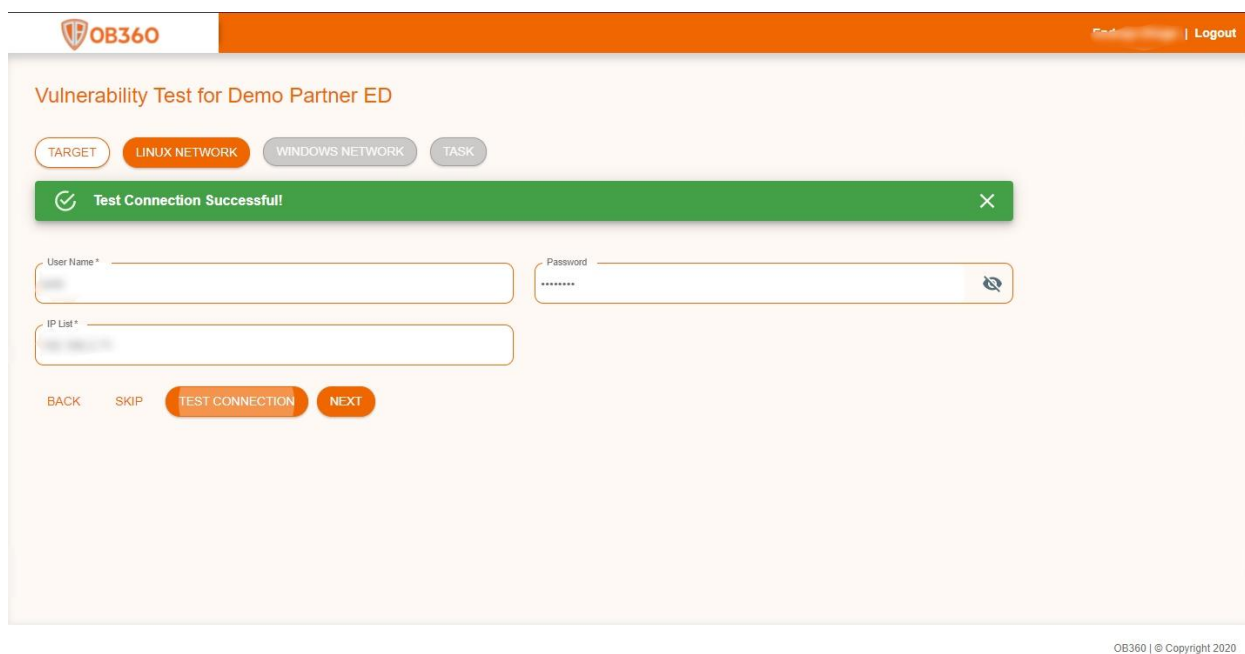
- Enter network administrator Username and Password
- Enter IP address list or IP range
- Click on the 'Test Connection' button.



The screenshot shows the 'Vulnerability Test for Demo Partner ED' interface. At the top, there's a header with the OB360 logo and a 'Logout' link. Below the header, the title 'Vulnerability Test for Demo Partner ED' is displayed. The interface features four tabs: 'TARGET', 'LINUX NETWORK' (which is selected and highlighted in orange), 'WINDOWS NETWORK', and 'TASK'. Below the tabs, there are three input fields: 'User Name *', 'Password' (with a toggle for visibility), and 'IP List *'. At the bottom, there are four buttons: 'BACK', 'SKIP', 'TEST CONNECTION' (highlighted in orange), and 'NEXT'.

Figure : Linux Network Screen

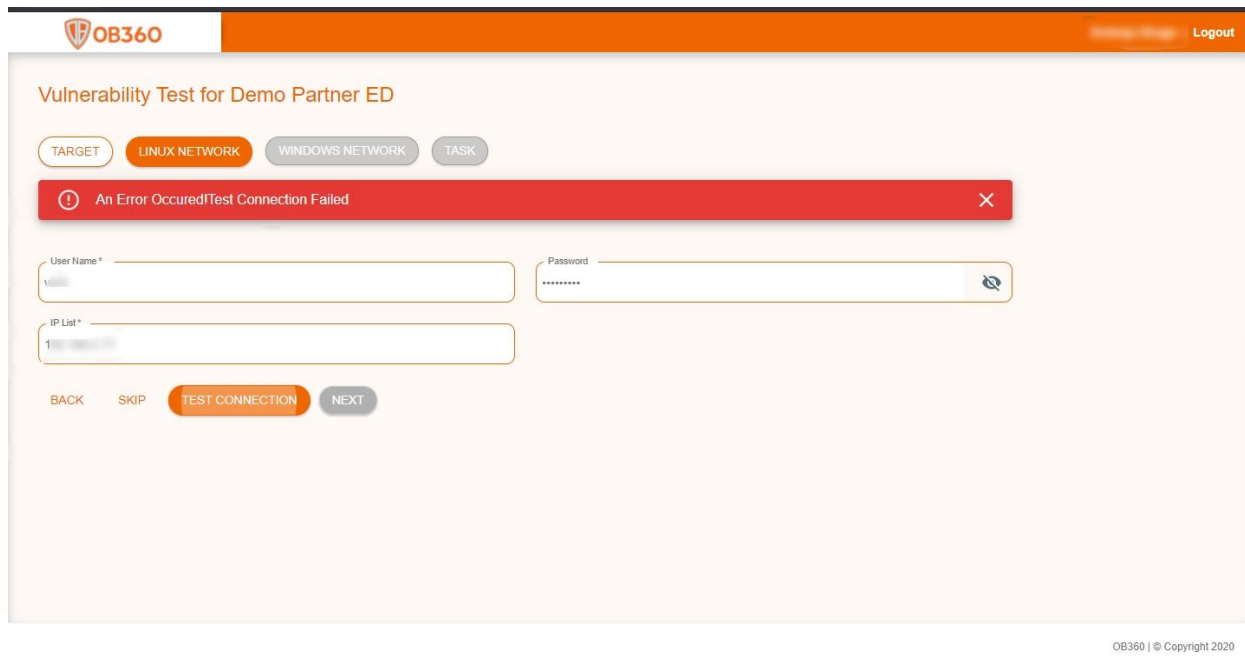
After Successful test connection you will get the 'Test Connection Successful' message and the 'Next' button will be enabled.



This screenshot shows the same interface as the previous one, but with a green success message banner at the top that reads 'Test Connection Successful!'. The 'TEST CONNECTION' button remains highlighted in orange, and the 'NEXT' button is now enabled and highlighted in orange. The other elements, including the tabs and input fields, remain the same.

Figure : Linux Success Screen

If you get an error message 'An Error Occurred' then enter correct credentials for linux network and try again till you get the success message.

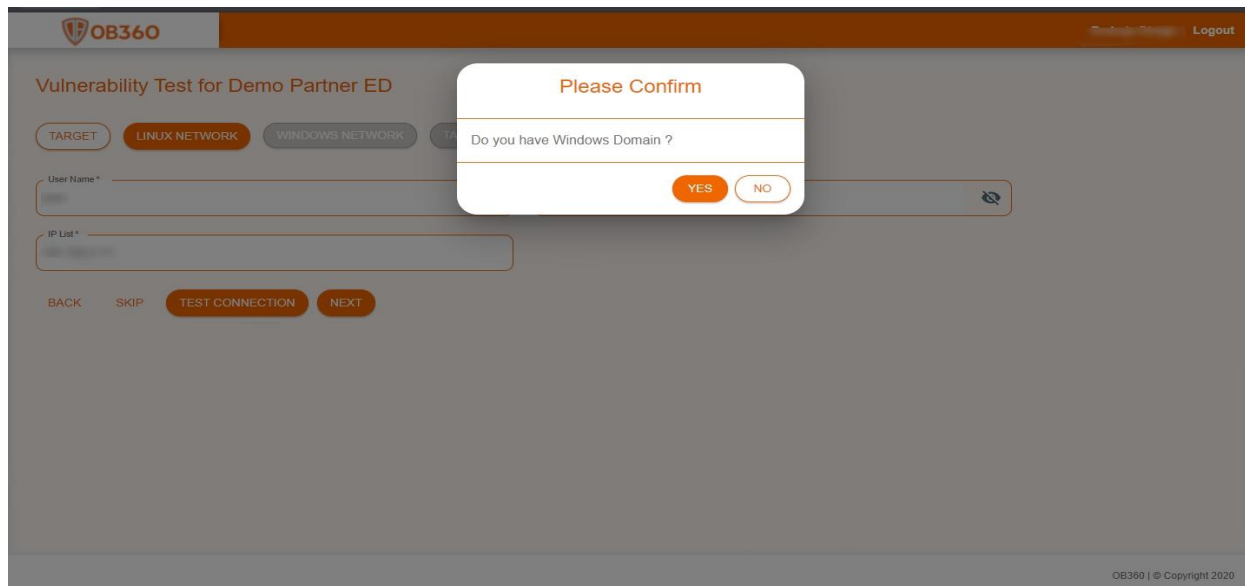


The screenshot shows the 'Vulnerability Test for Demo Partner ED' interface. At the top, there's a navigation bar with the OB360 logo and a 'Logout' link. Below the navigation bar, there are four tabs: 'TARGET', 'LINUX NETWORK' (which is selected), 'WINDOWS NETWORK', and 'TASK'. A red error message banner at the top of the main content area reads 'An Error Occurred! Test Connection Failed'. Below this, there are three input fields: 'User Name *' (containing 'root'), 'Password' (containing '*****'), and 'IP List *' (containing '10.10.10.10'). At the bottom of the form, there are four buttons: 'BACK', 'SKIP', 'TEST CONNECTION' (which is highlighted in orange), and 'NEXT'. The footer of the page contains the text 'OB360 | © Copyright 2020'.

Figure : Linux Failure Screen

Step 9: After the Next button is enabled click on it.

On clicking the next button a popup window will appear showing 'Do You have Windows Domain?'



The screenshot shows the same 'Vulnerability Test for Demo Partner ED' interface as before, but with a confirmation dialog box overlaid. The dialog box has a title 'Please Confirm' and a question 'Do you have Windows Domain?'. It has two buttons: 'YES' (highlighted in orange) and 'NO'. The background of the interface is dimmed. The footer of the page contains the text 'OB360 | © Copyright 2020'.

Figure : Windows Confirmation Screen

Click on 'YES' if you have windows network else click on 'NO'

On click of 'Yes' you will redirect to step 10.

On click of 'No' you will redirect to step 11.

Step 10: Now you will redirect to the windows network page.

Do the following steps to create a target for windows network..

- Enter network administrator Username and Password
- Enter IP address list or IP range
- Click on the 'Test Connection' button.

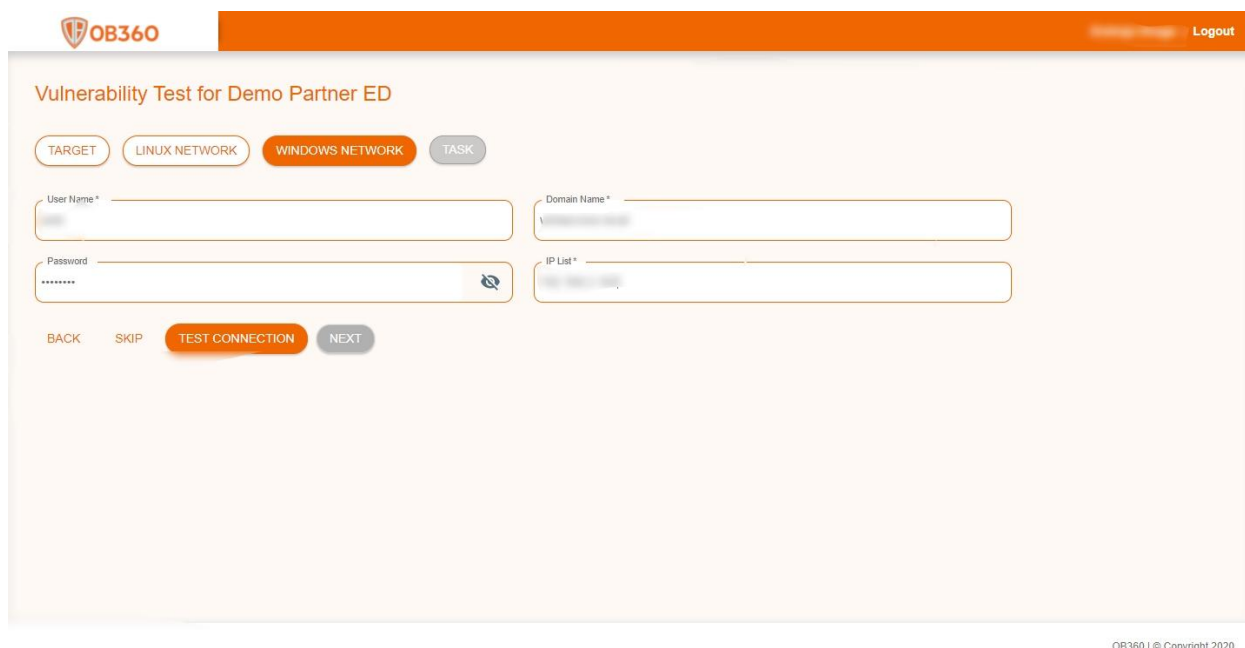
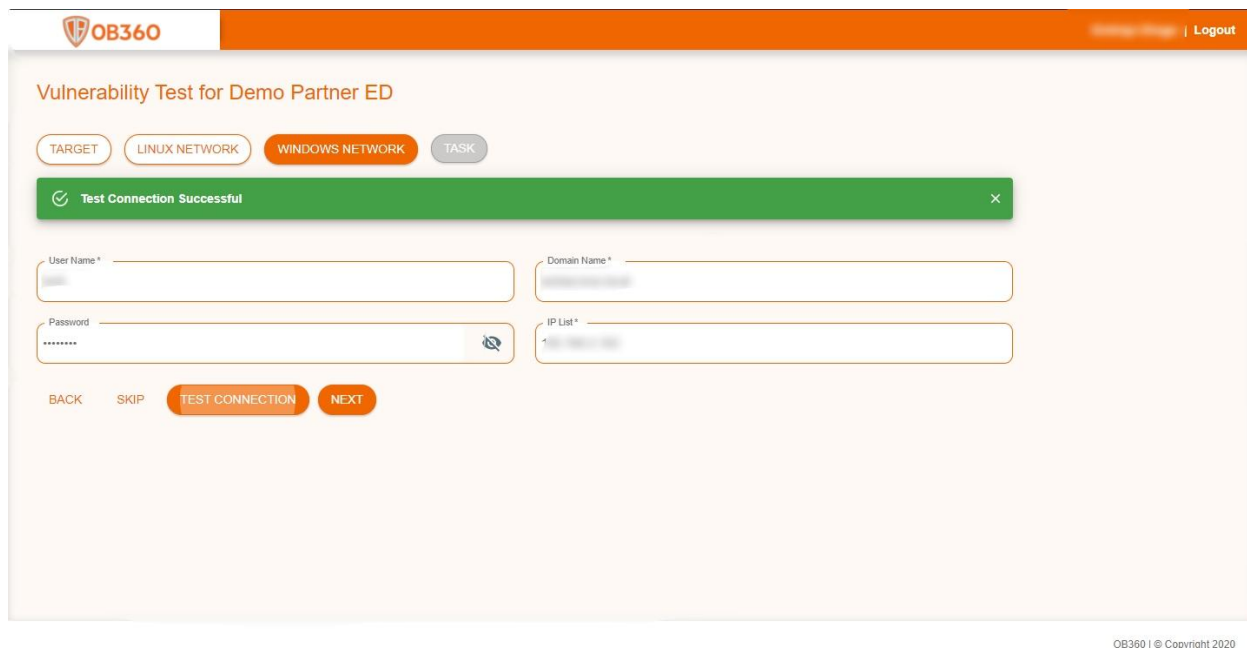


Figure : Windows Network Screen

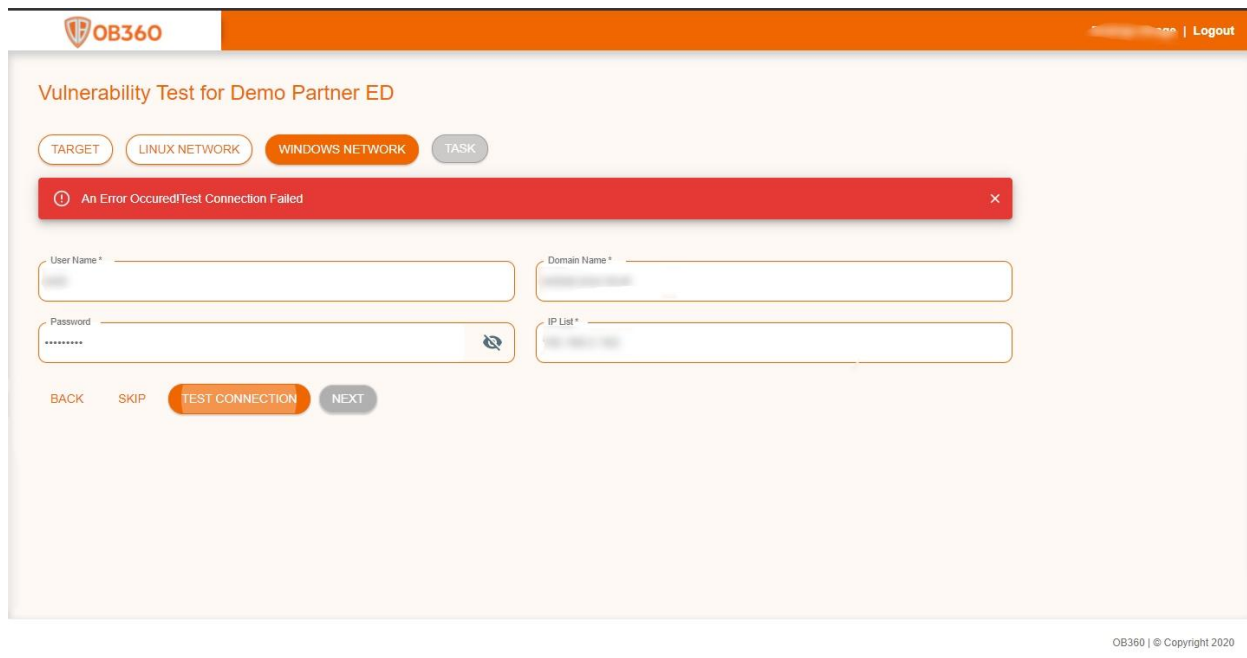
After Successful test connection you will get the 'Test Connection Successful' message and the 'Next' button will be enabled.



The screenshot shows the 'Vulnerability Test for Demo Partner ED' interface. At the top, there's a navigation bar with the OB360 logo and a 'Logout' link. Below the navigation bar, there are four tabs: 'TARGET', 'LINUX NETWORK', 'WINDOWS NETWORK' (which is selected), and 'TASK'. A green success message banner at the top reads 'Test Connection Successful'. Below this, there are four input fields: 'User Name *', 'Domain Name *', 'Password' (with a toggle for visibility), and 'IP List *'. At the bottom, there are four buttons: 'BACK', 'SKIP', 'TEST CONNECTION' (which is highlighted in orange), and 'NEXT' (which is also highlighted in orange). The footer of the page reads 'OB360 | © Copyright 2020'.

Figure : Windows Success Screen

If you get an error message 'An Error Occurred' then enter correct credentials for windows network and try again till you get the success message.



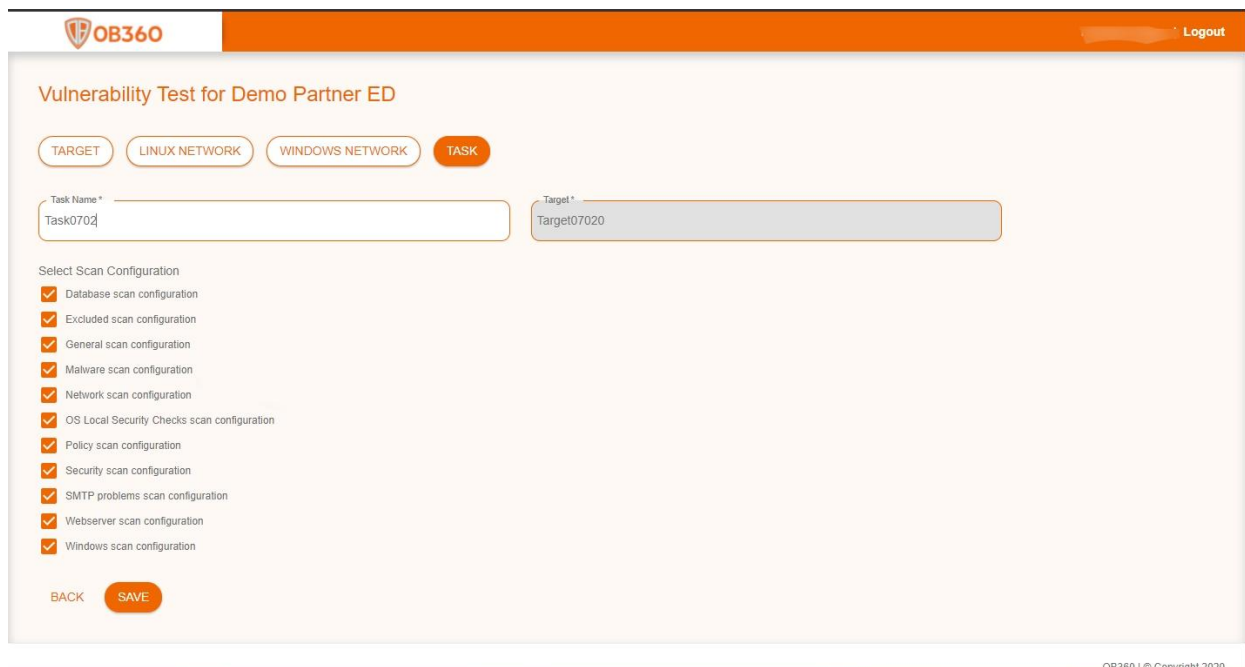
The screenshot shows the same 'Vulnerability Test for Demo Partner ED' interface as the previous one, but with a red error message banner at the top that reads 'An Error Occurred! Test Connection Failed'. The 'TEST CONNECTION' button is still highlighted in orange, but the 'NEXT' button is now disabled (greyed out). The footer of the page reads 'OB360 | © Copyright 2020'.

Figure : Windows Failure Screen

Step 10: After the Next button is enabled click on it.

Now you will redirect to the task creation page.

Enter the task name and click on the save button after selecting at least one scan configuration from the list.



Vulnerability Test for Demo Partner ED

TARGET LINUX NETWORK WINDOWS NETWORK **TASK**

Task Name * Target *

Task0702 Target0702

Select Scan Configuration

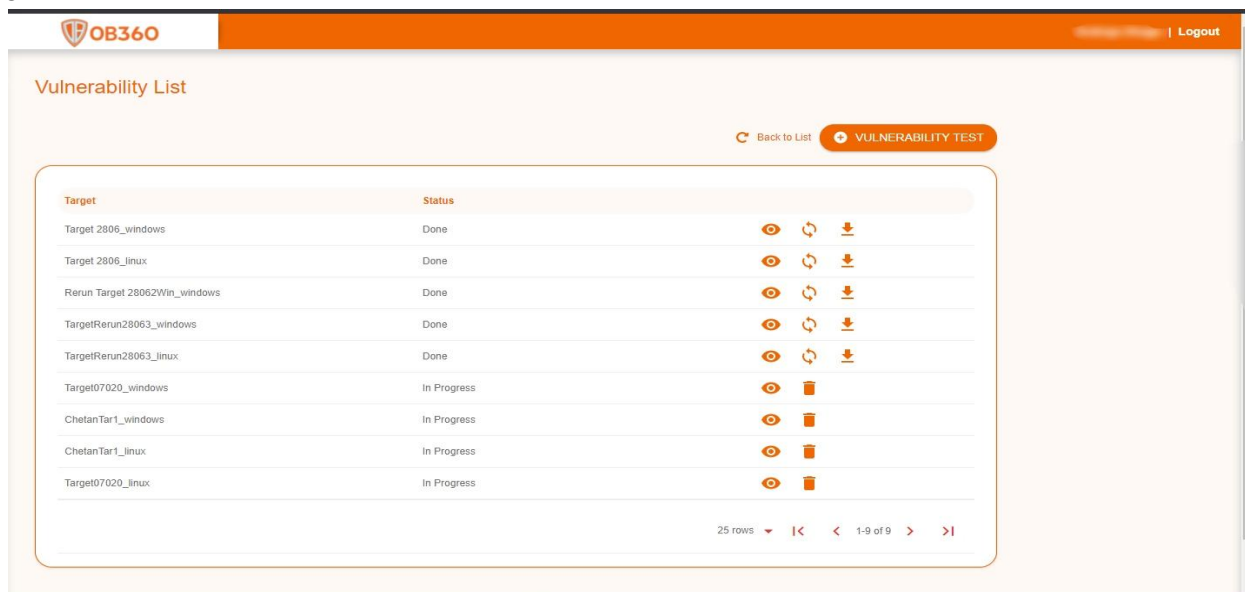
- ☒ Database scan configuration
- ☒ Excluded scan configuration
- ☒ General scan configuration
- ☒ Malware scan configuration
- ☒ Network scan configuration
- ☒ OS Local Security Checks scan configuration
- ☒ Policy scan configuration
- ☒ Security scan configuration
- ☒ SMTP problems scan configuration
- ☒ Webservice scan configuration
- ☒ Windows scan configuration

BACK SAVE

Figure : Task Screen

Step 11: After clicking the save button.

The page will redirect to the Report List page, where you will see the most recently generated vulnerabilities.



Vulnerability List

Back to List VULNERABILITY TEST

Target	Status	Details	Refresh	Delete
Target 2806_windows	Done			
Target 2806_linux	Done			
Rerun Target 28062Win_windows	Done			
TargetRerun28063_windows	Done			
TargetRerun28063_linux	Done			
Target07020_windows	In Progress			
ChetanTar1_windows	In Progress			
ChetanTar1_linux	In Progress			
Target07020_linux	In Progress			

25 rows 1-9 of 9

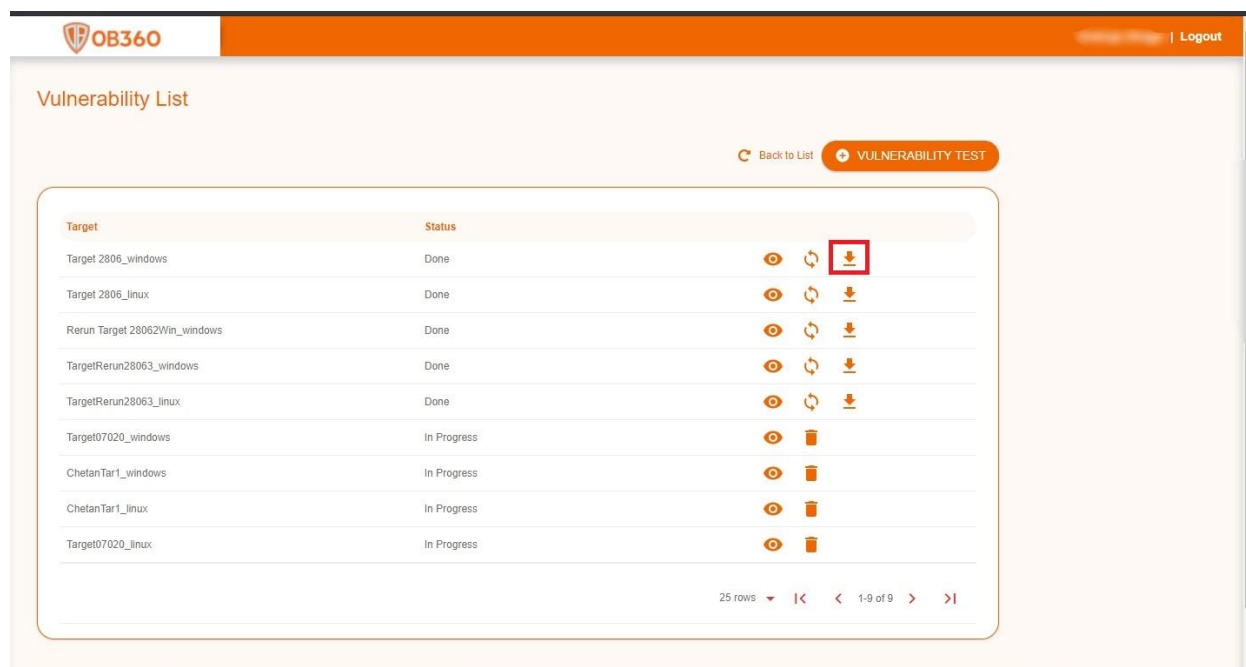
Figure : Latest Vulnerability List Screen

Status of the current Vulnerability test is 'In Progress'.

The selected task will be scanned. A report will be generated after all of the tasks have been scanned.

By clicking the view button, you can see the status of the created target.

When all the tasks have been completed, the status will be changed to "Done".



Target	Status	View	Refresh	Download
Target 2806_windows	Done			
Target 2806_linux	Done			
Rerun Target 28062Win_windows	Done			
TargetRerun28063_windows	Done			
TargetRerun28063_linux	Done			
Target07020_windows	In Progress			
ChetanTar1_windows	In Progress			
ChetanTar1_linux	In Progress			
Target07020_linux	In Progress			

Figure : Vulnerability List Screen

Now you can download the report by clicking the 'Download' button . You will get the report in zip format.

Extract the zip and you will get all the reports generated for your task.

This completes the OB360 flow.