Module 02: Penetration Testing Scoping and Engagement Methodology

Objective

The objective of this lab is to understand the pre-penetration testing steps and pre-execution administration issues.

Scenario

There is much more to an engagement than “throwing packets at the network” and, like most things in life, an engagement begins and ends with paperwork.

As an Engagement Team Leader (ETL) or Engagement Team Member (ETM), you perform several non-billable, administrative tasks in order to ensure a successful and profitable engagement. Although these tasks do not generate income in and of themselves, when executed properly, they help to ensure the greatest margin of profitability for engagements.

In the rush to begin billable time on an engagement, it is easy to succumb to the temptation of “cutting corners”, especially for non-billable activities and administration. Do not yield to this temptation. Profit is counted not only by the number of dollars in the bank but also by the customer loyalty, references and referrals resulting from a well planned and executed engagement.

The information technology security business is a business like no other. First, you are not selling a tangible item. You can't hold security in your hands. You can't smell it, taste it or feel it. It is an intangible “peace of mind” like the feeling you have when purchasing life or health insurance. Indeed, it is a form of insurance; insurance against an attack that could ruin your client's business or reputation. However, like insurance, there are no guarantees. You cannot “guarantee” to your client that they will never be attacked or that an attack will not be successful as a result of the work you perform on an engagement. You work in concert with the management at your clients to identify ways in which the security of their business information could be compromised and recommend appropriate mitigation strategies for discovered problems. However, you can help to ensure that the report presented to your clients is as accurate and comprehensive as possible, thereby diminishing the possibility of a successful attack. In addition, you must take every possible precaution to ensure that your clients' data is not compromised while it is in your possession.

Some of the administrative tasks may seem excessive or unnecessary to you. These tasks help ensure the security of client data and demonstrate to your clients that you and your company take security very seriously. Don't cut corners!

You start with reviewing the Engagement Letter (EL) to understand what you and your team members will be required to do during the engagement, set up the engagement folders you will need to store the engagement data, and perform due diligence for conflicts of interest. You prepare the initial draft copies of engagement control and other documents, establish contact with the client and, in coordination with the Target Organization (TORG), ensure that all documentation is correct and in compliance with the TORG's expectations as defined in the EL.

In addition to these administrative control activities, you also coordinate personnel and logistical issues.

You first prepare and then update, as required, a plan of how you will conduct the project, scheduling when various portions of the work specified in the EL will occur and which of your team members will participate in the engagement. Individual vulnerability discovery, analysis and penetration testers are assigned to the engagement, forming the penetration test team. Secure communication channels are established with the client to transmit communications containing sensitive information.

Transportation and lodging requirements are determined. At the conclusion of this phase, the Engagement Team Leader issues a mission briefing to the penetration test team to allow them the maximum amount of time to prepare for the next phase, the execution of the engagement.

Exercise 1: Penetration Testing Project Planning and Scheduling Using GanttProject

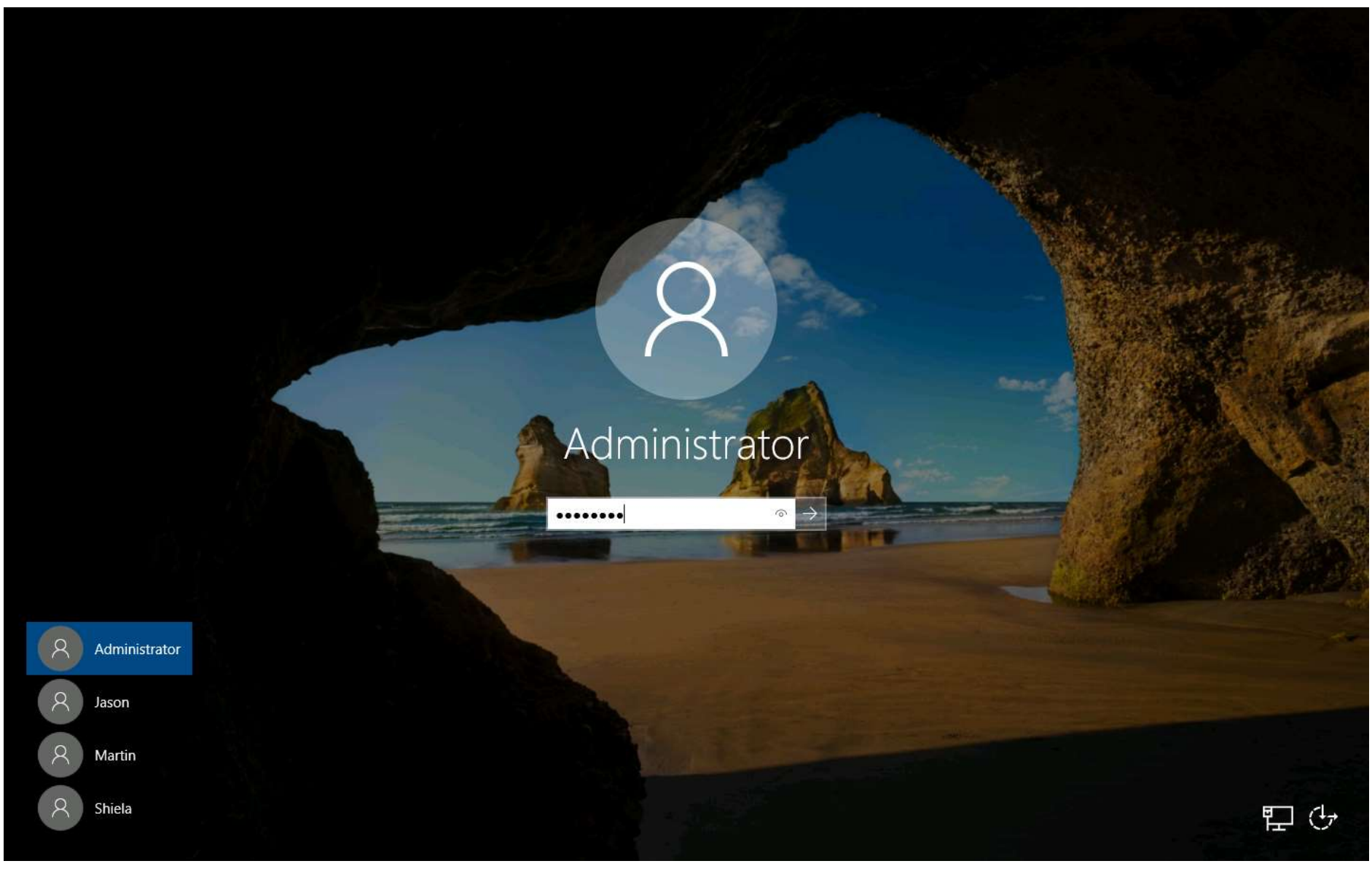
Scenario

Project planning is part of project management, which relates to the use of schedules such as Gantt charts to plan and subsequently report progress within the project environment. GanttProject helps you to plan your penetration testing projects in an effective and tim manner. Project planning and scheduling projects will help you to in maximizing use of resources effectively and meeting deadlines. As expert penetration tester, you must understand how to plan and schedule activities in penetration testing projects using GanttProject to

Lab Duration: **5** Minutes

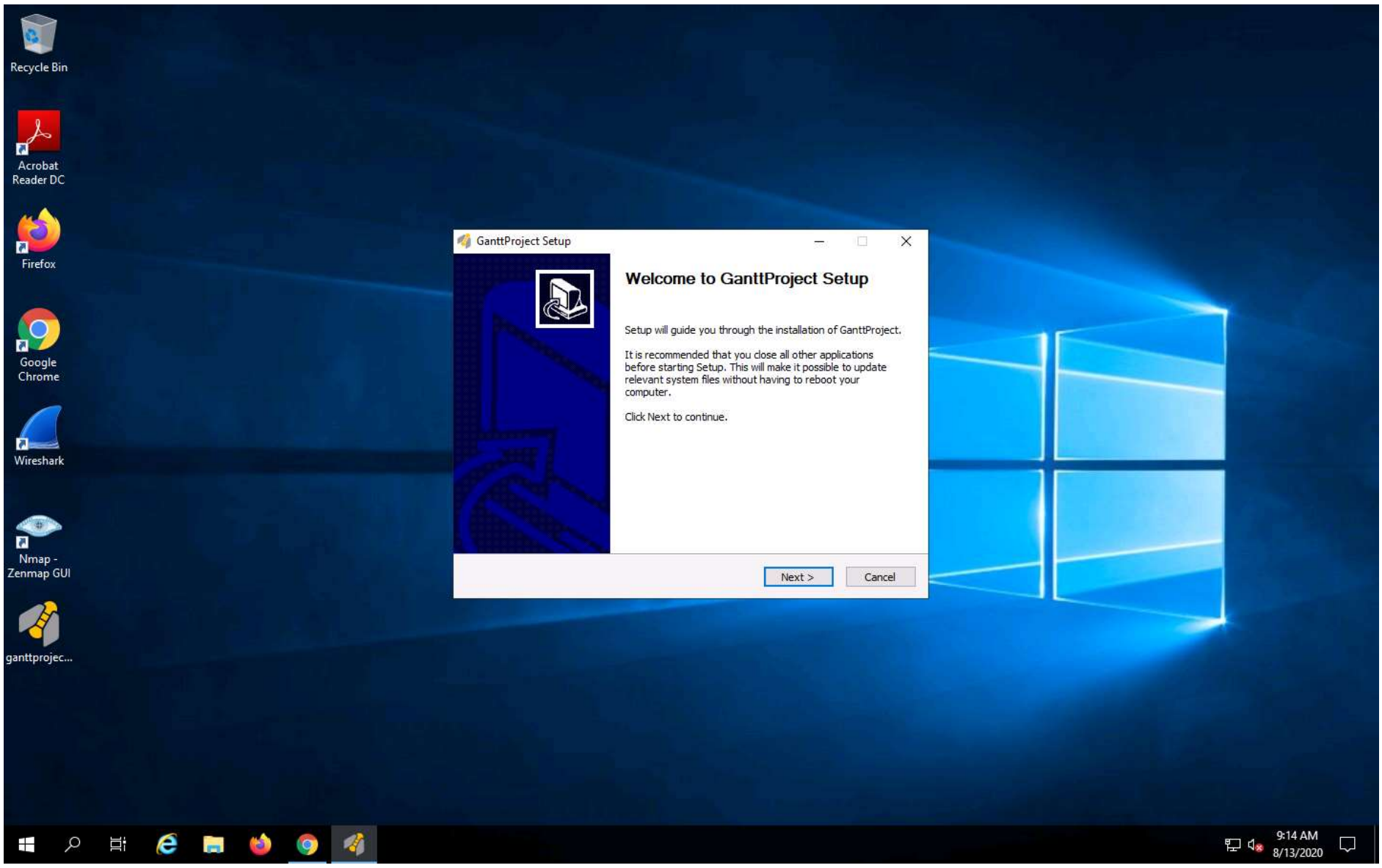
1. By default, **CPENT-M2 Windows Server 2019** machine appears, click **Ctrl+Alt+Del**.

2. In the password field type **Pa$$w0rd** and press **Enter**

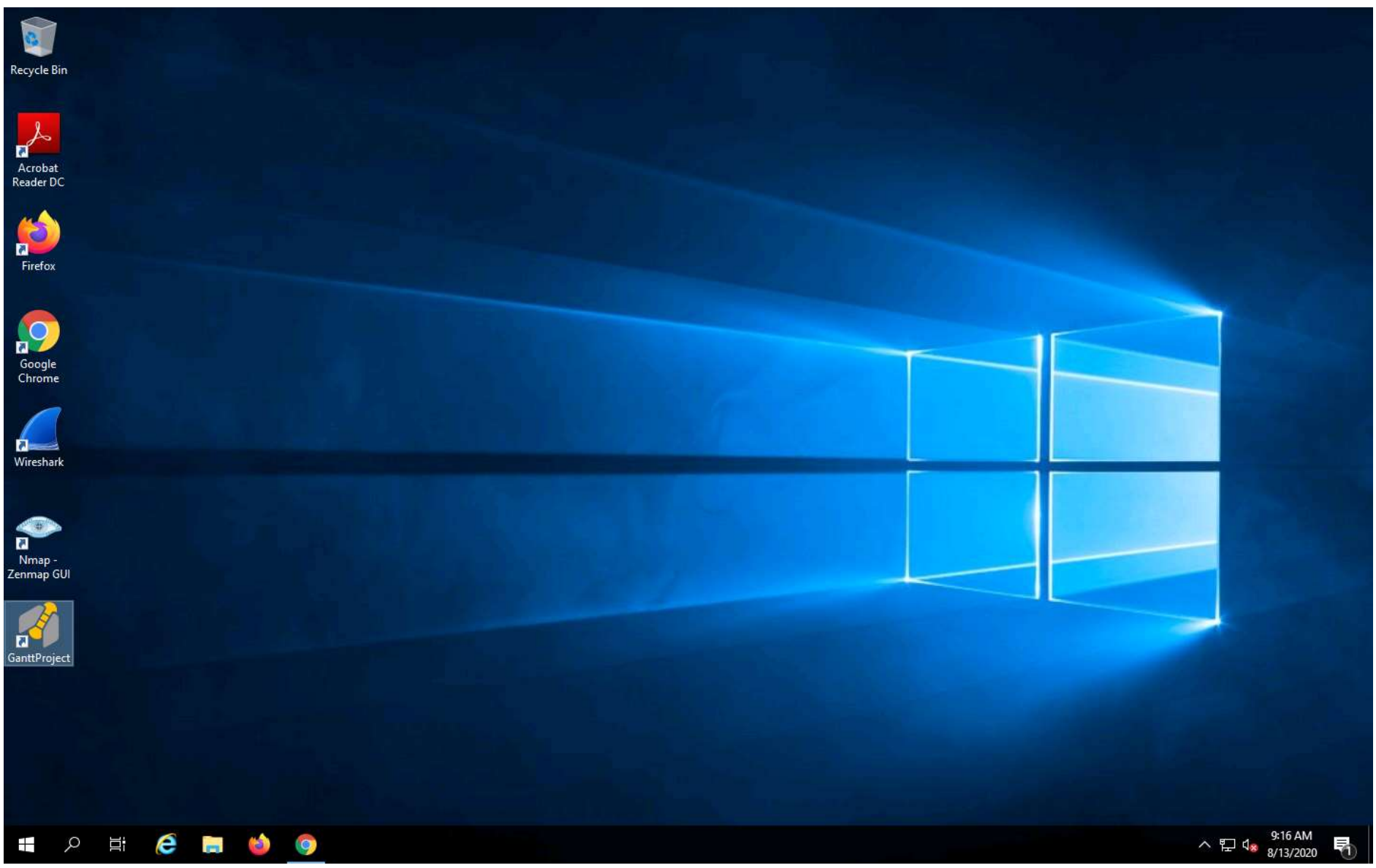


3. To install **GanttProject**, navigate to **E:\CPENT Module 02 Penetration Testing Scoping and Engagement Methodology\GanttProject**, double-click **ganttproject-2.8.11-r2396.exe** and follow the steps to install **GanttProject**.

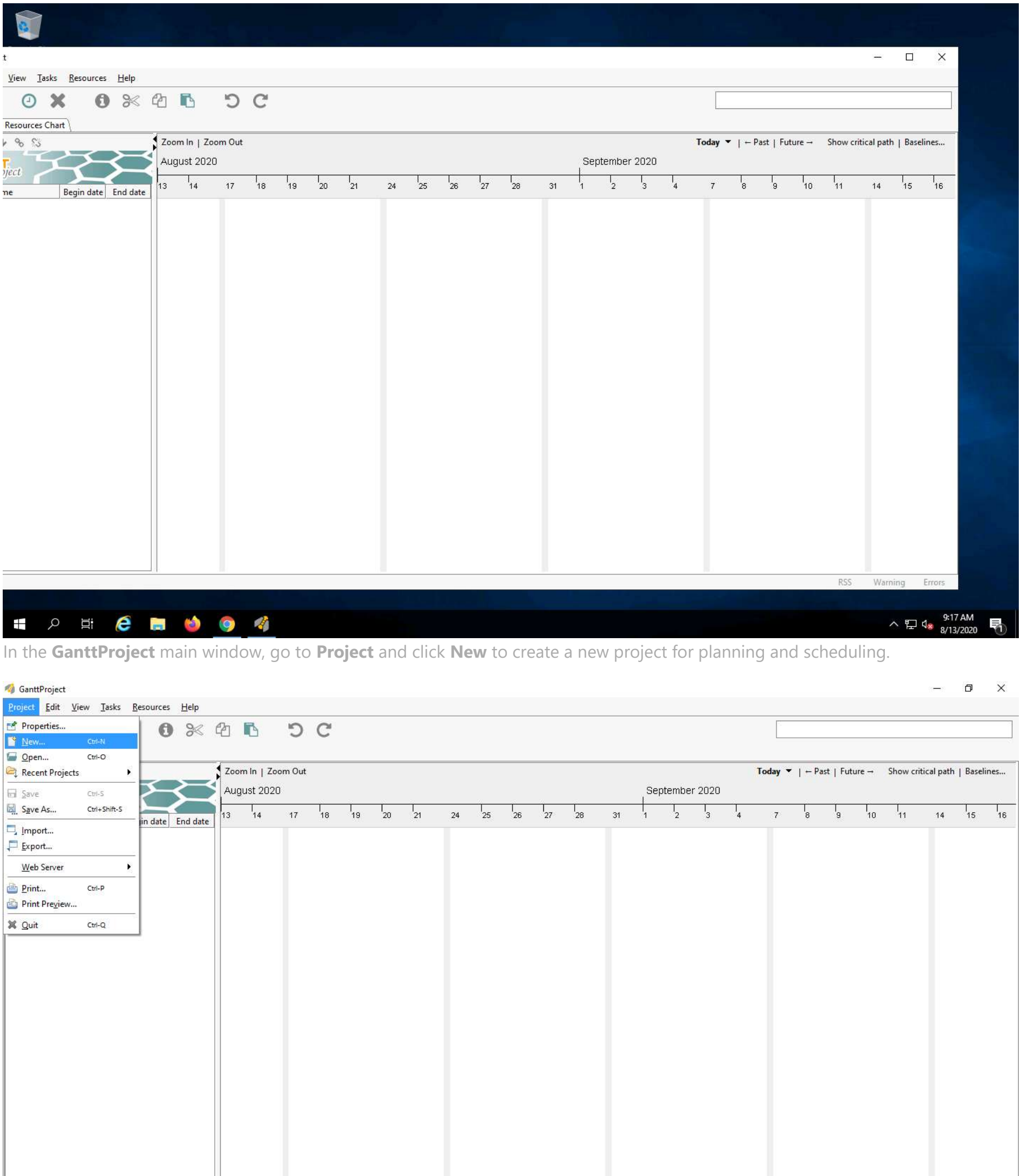
Note: If an Open File - Security Warning window appears click **Run**.



4. To launch, GanttProject double-click the **GanttProject** icon on the **Desktop**.

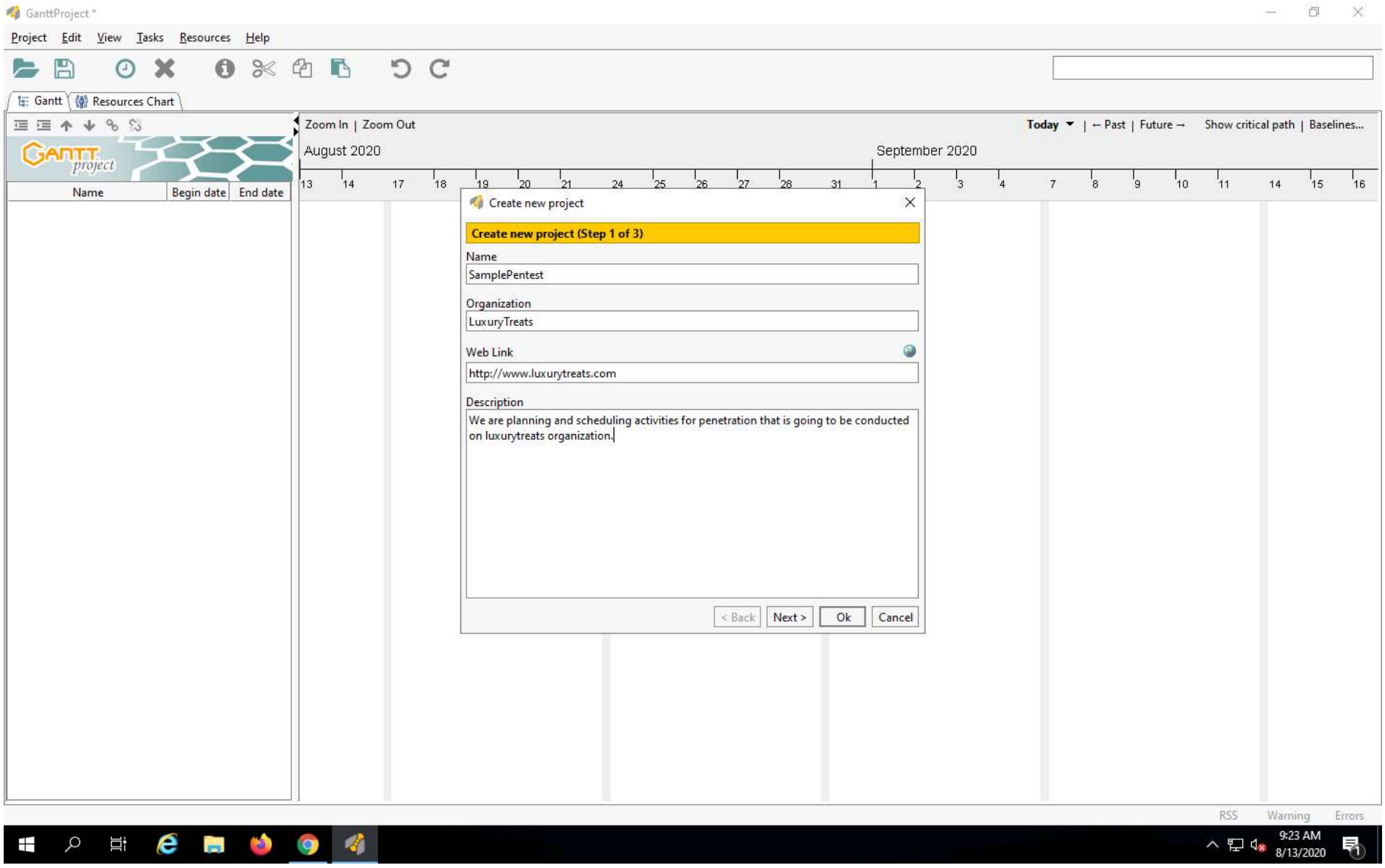


5. The main window of **GanttProject** appears as shown in the screenshot.

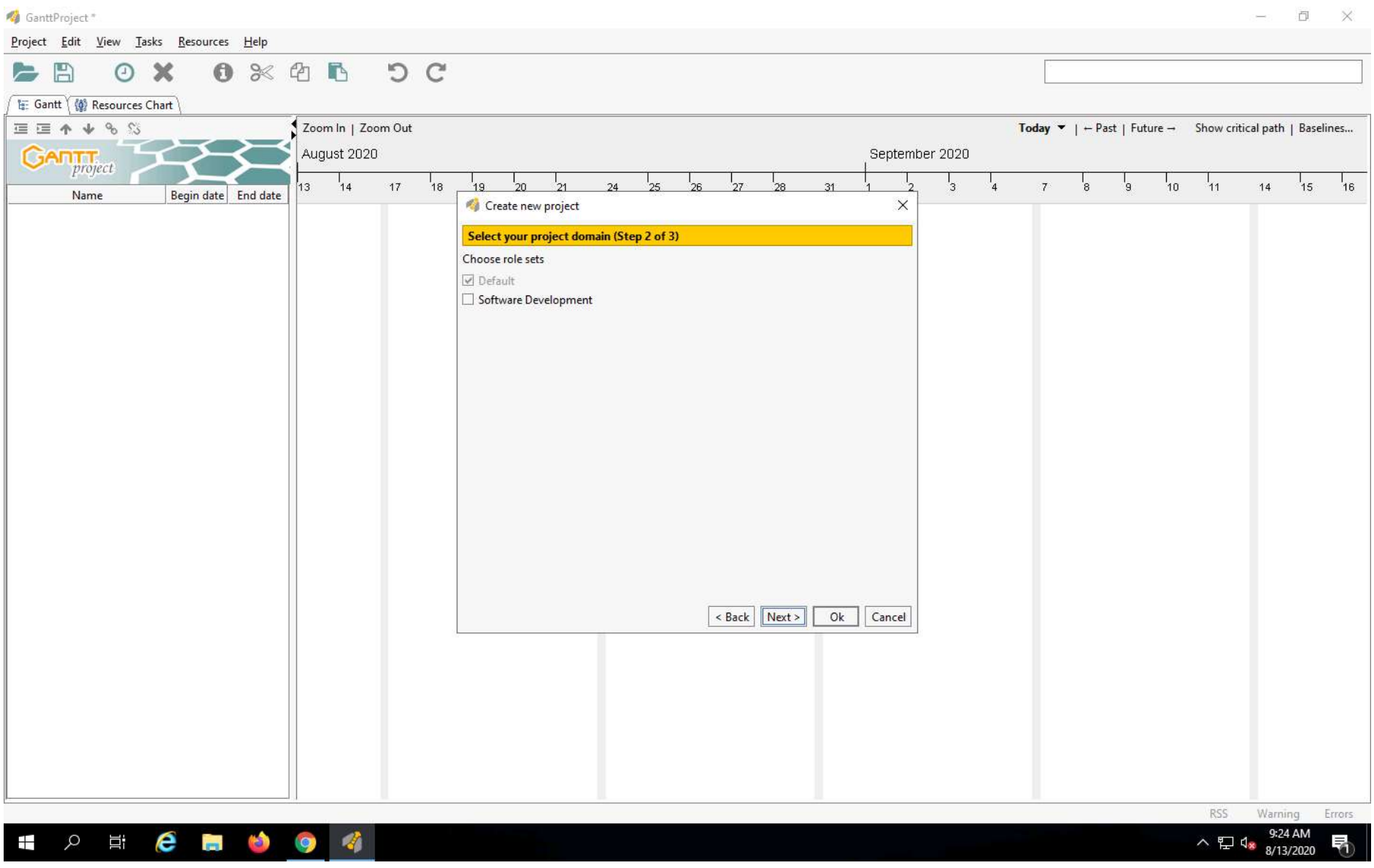


6. In the **GanttProject** main window, go to **Project** and click **New** to create a new project for planning and scheduling.

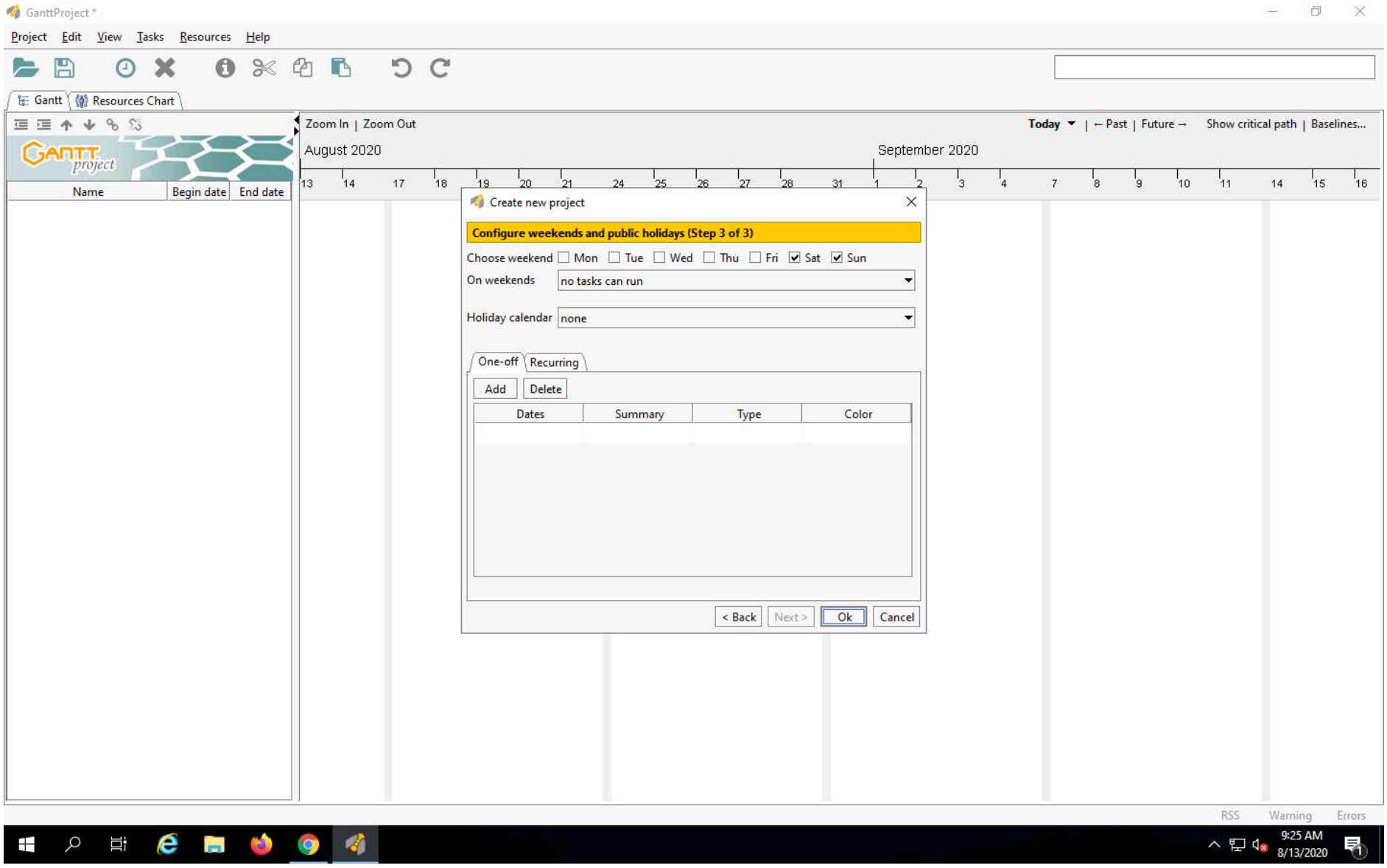
7. The **Create new project** window appears, on the screen. In **Step 1** enter the name of your project, the name of the target organization, its website and the Description of the project. Here we use **SamplePentest** as the name of the project, target **organization** as **LuxuryTreats**, Its URL as **http://www.luxurytreats.com**. Write something about the project in the **Description** text area. Click **Next**.



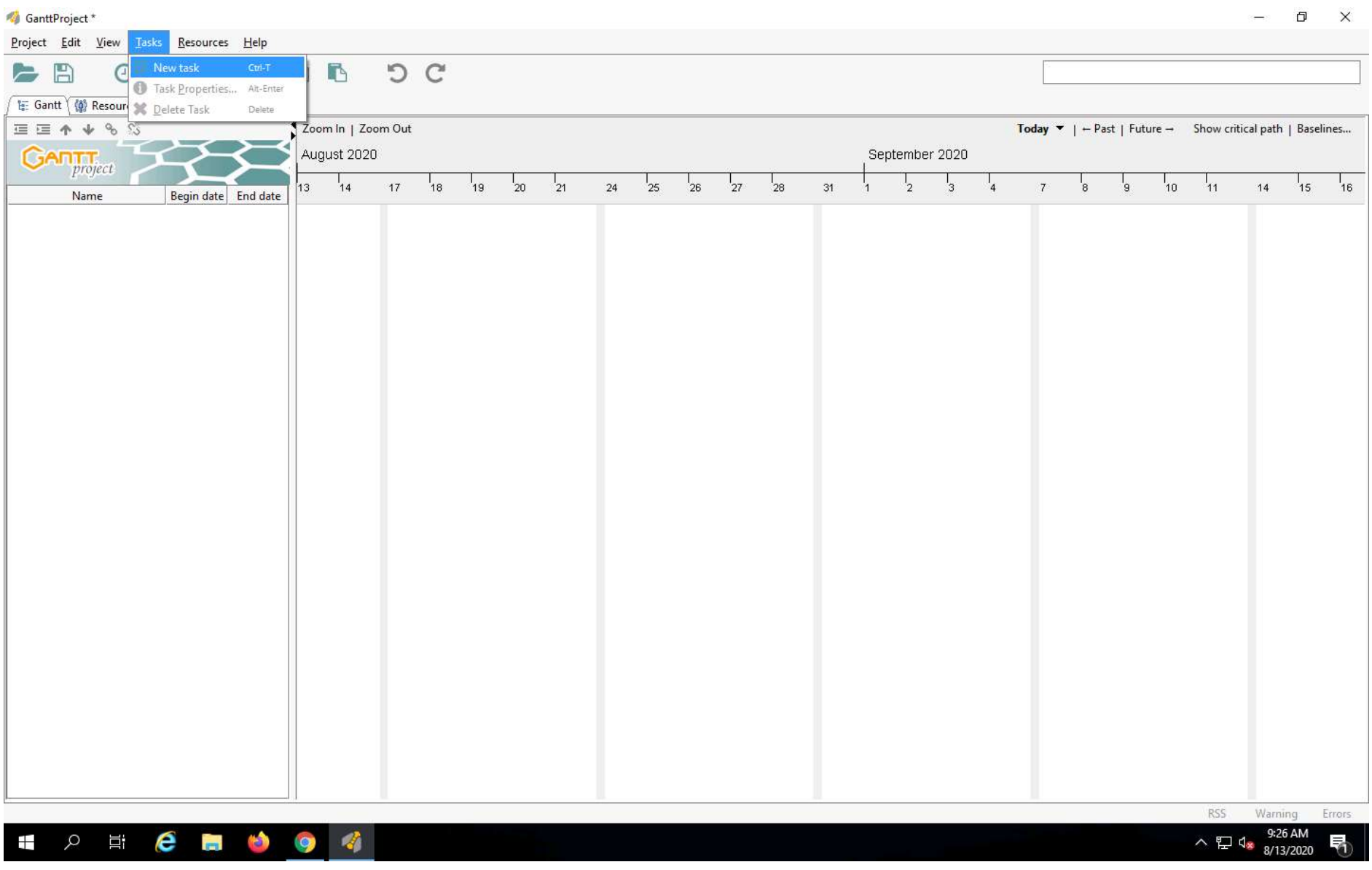
8. Leave the **default** value as it is in **Step 2** and click **Next**.



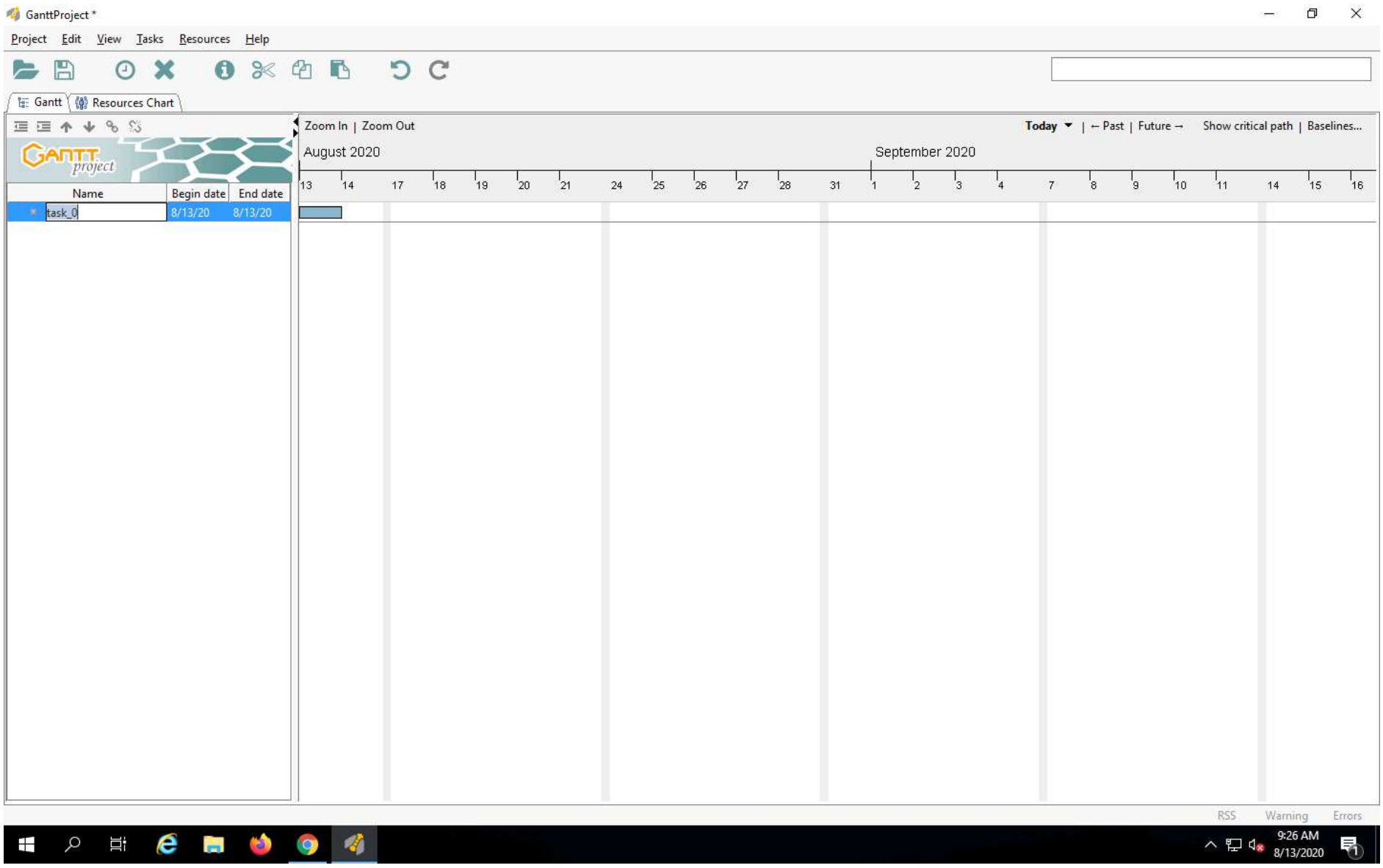
9. Again, leave the default values as it is for **Step 3** and click **Ok**.



10. Go to **Tasks** menu and click **New task**.

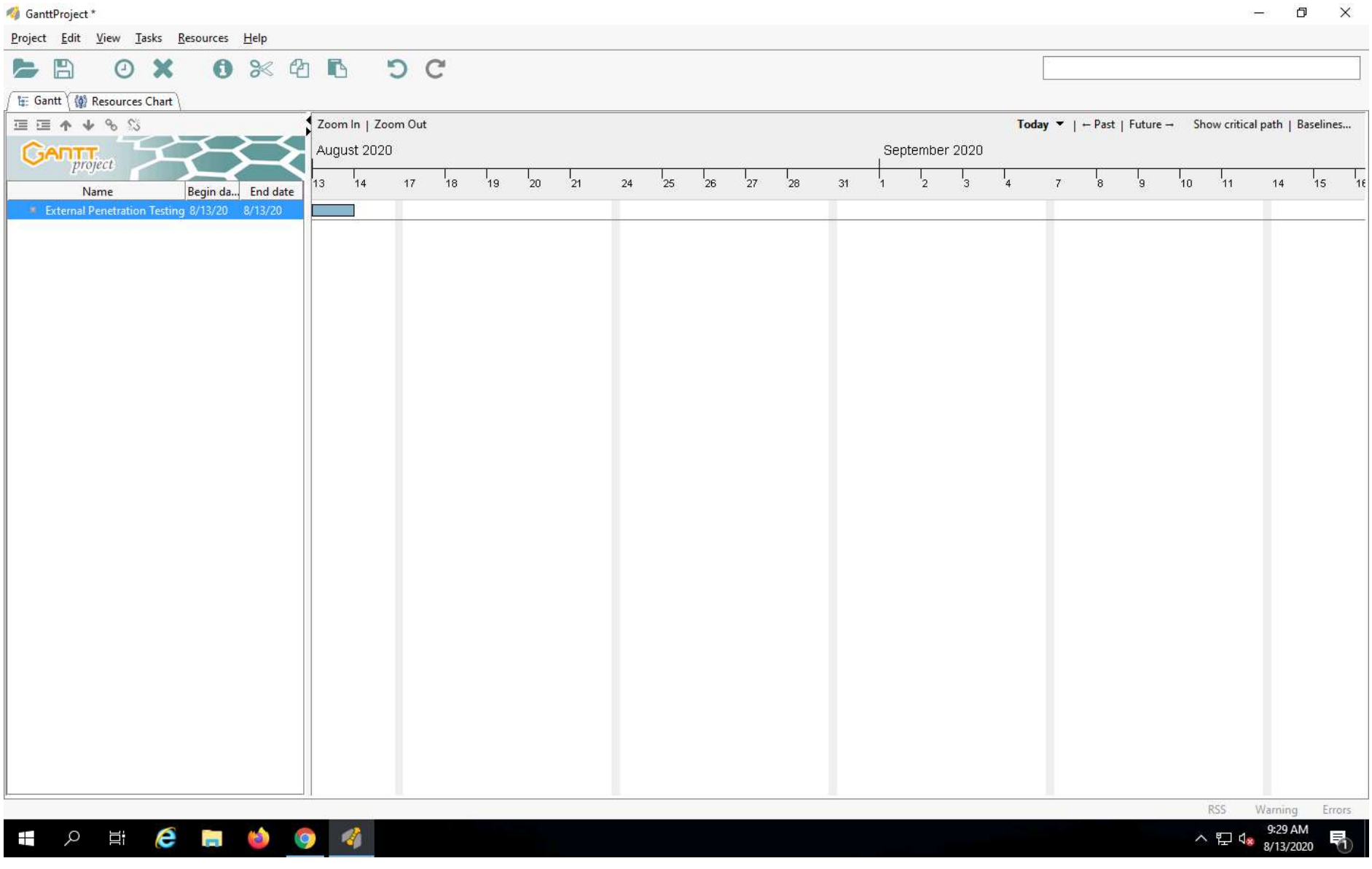


11. The **New Task** will be added under **Gantt** tab with its default name as shown in the screenshot.

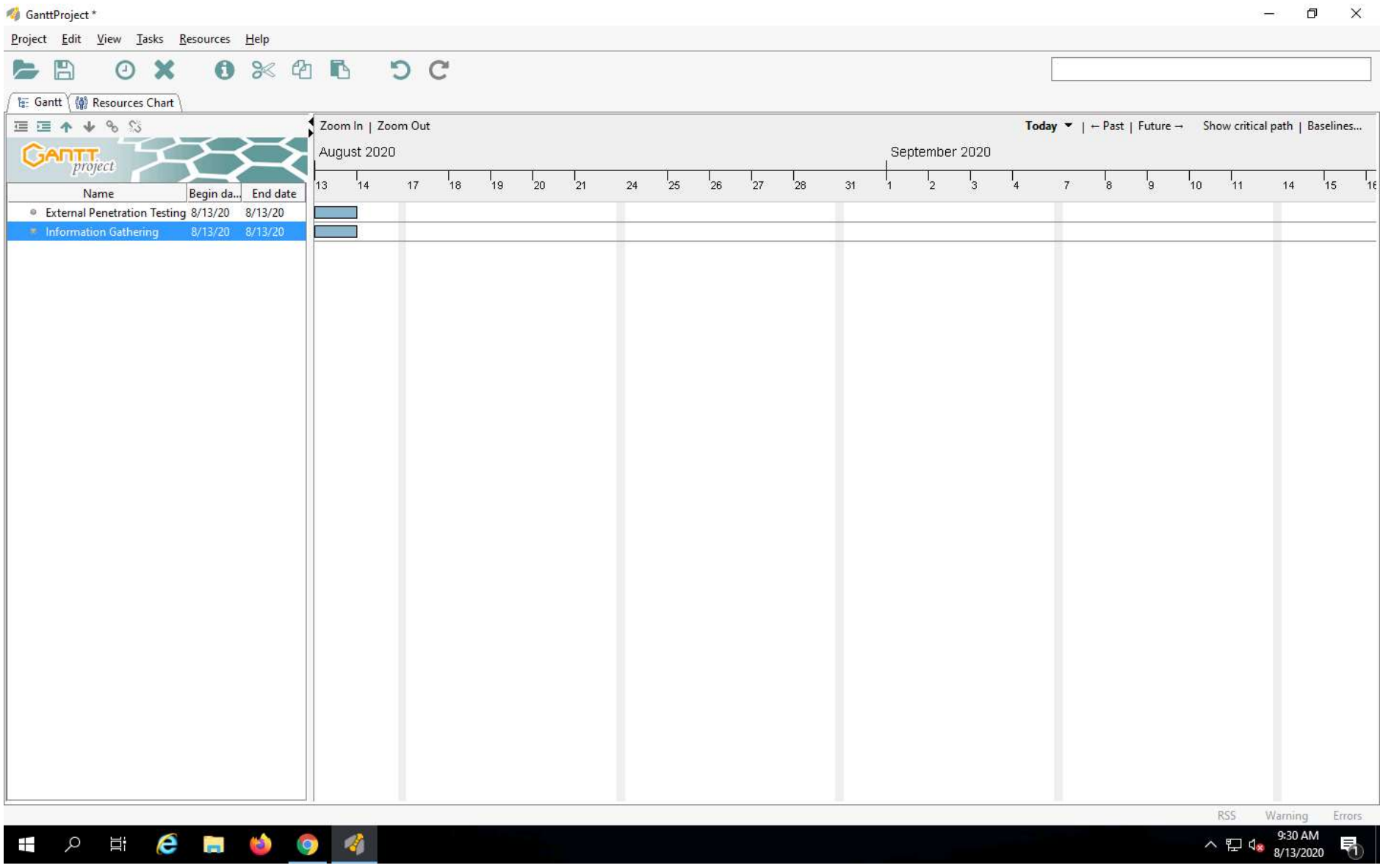


12. **Rename** the default name with your penetration task as **External Penetration Testing**. Schedule this task by specifying the **Begin date** and **End date** for task completion.

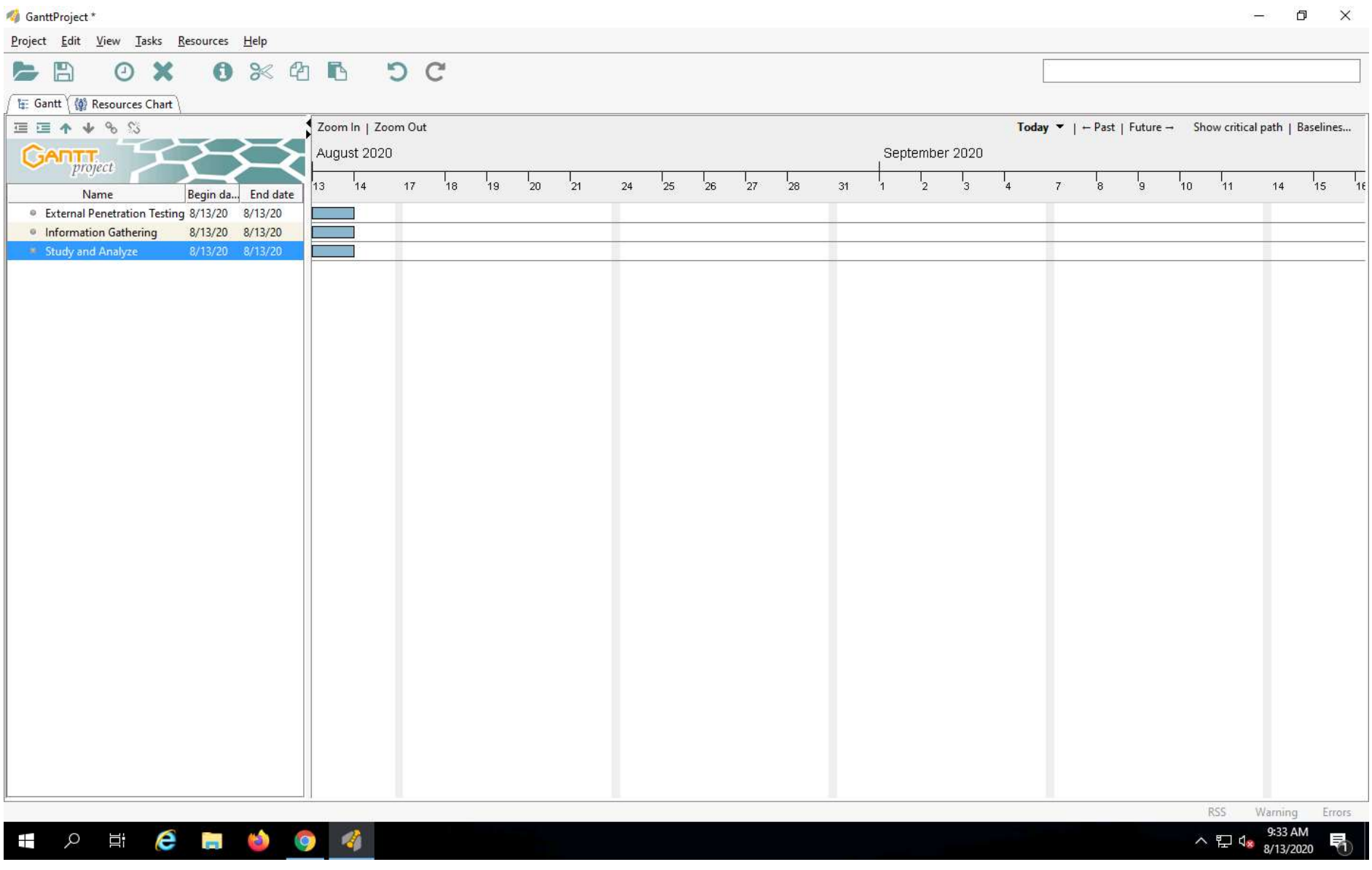
Note: If your task is not displayed as a gantt chart in the right pane of the window, click Zoom Out in the upper left corner of the right tab until you view the task defined.



13. Similarly, repeat **steps 10 to 12** to create and define the next task in your penetration testing project. Create another task and call it **Information Gathering**.

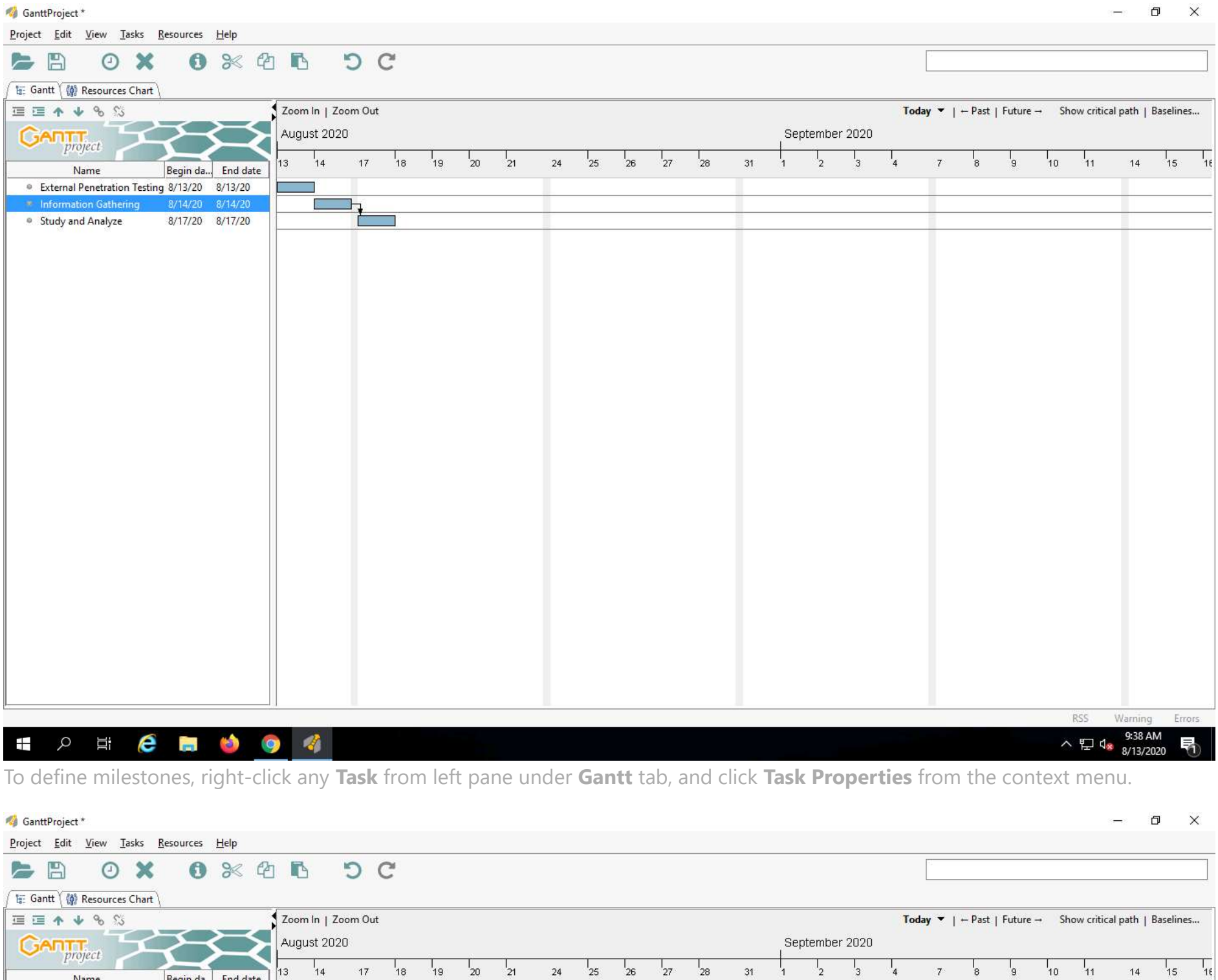


14. Repeat **steps 10 to 12** to plan and schedule the next task in your penetration testing project. Create another task and call it **Study and Analyze**. If there is a relation between the two tasks defined, you can specify this relationship with directed arrows as follows.

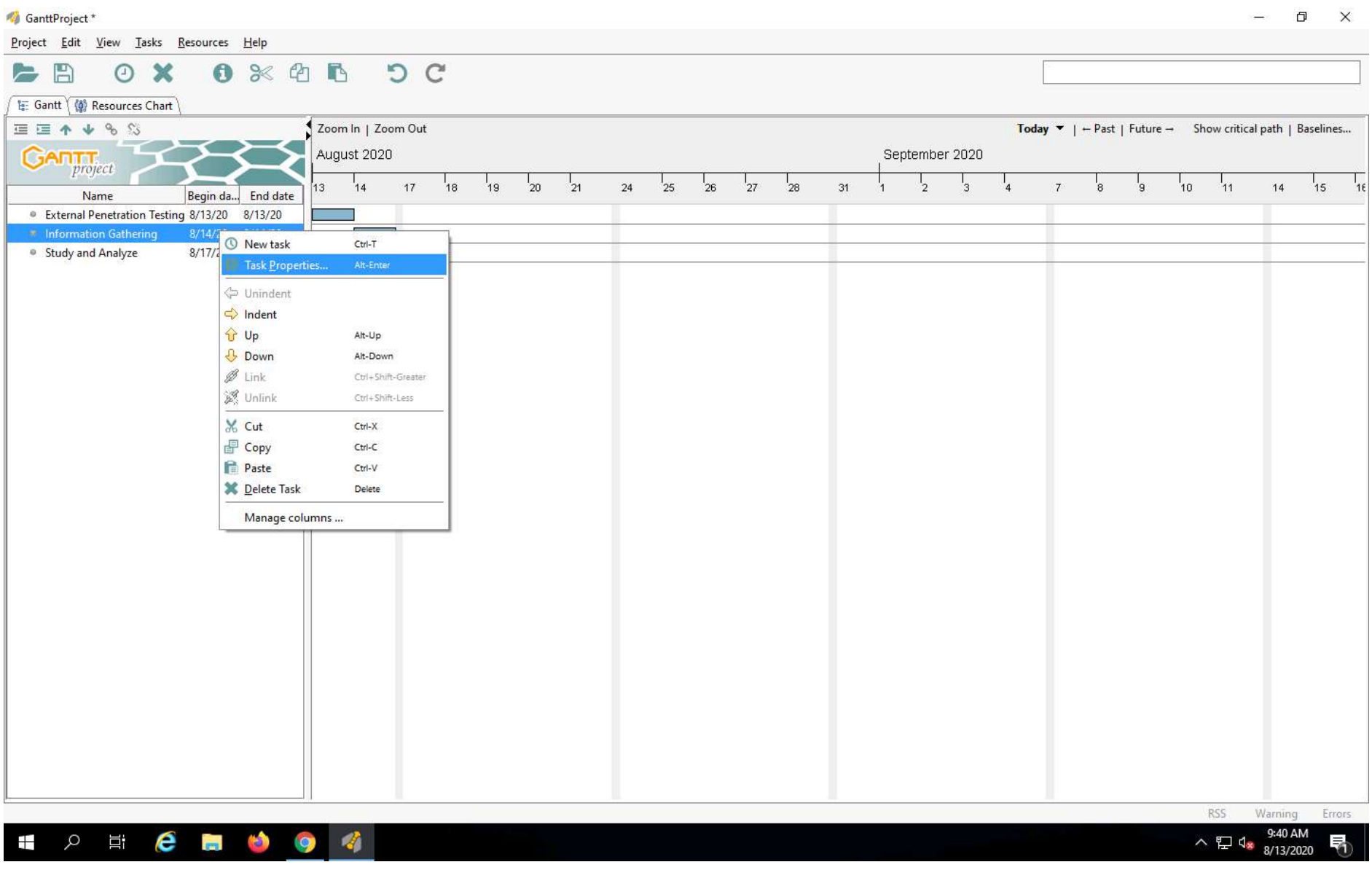


15. In the right pane, click on the **source task** and drag it to next task in the relationship. The arrow will be established between these two tasks as shown in the screenshot.

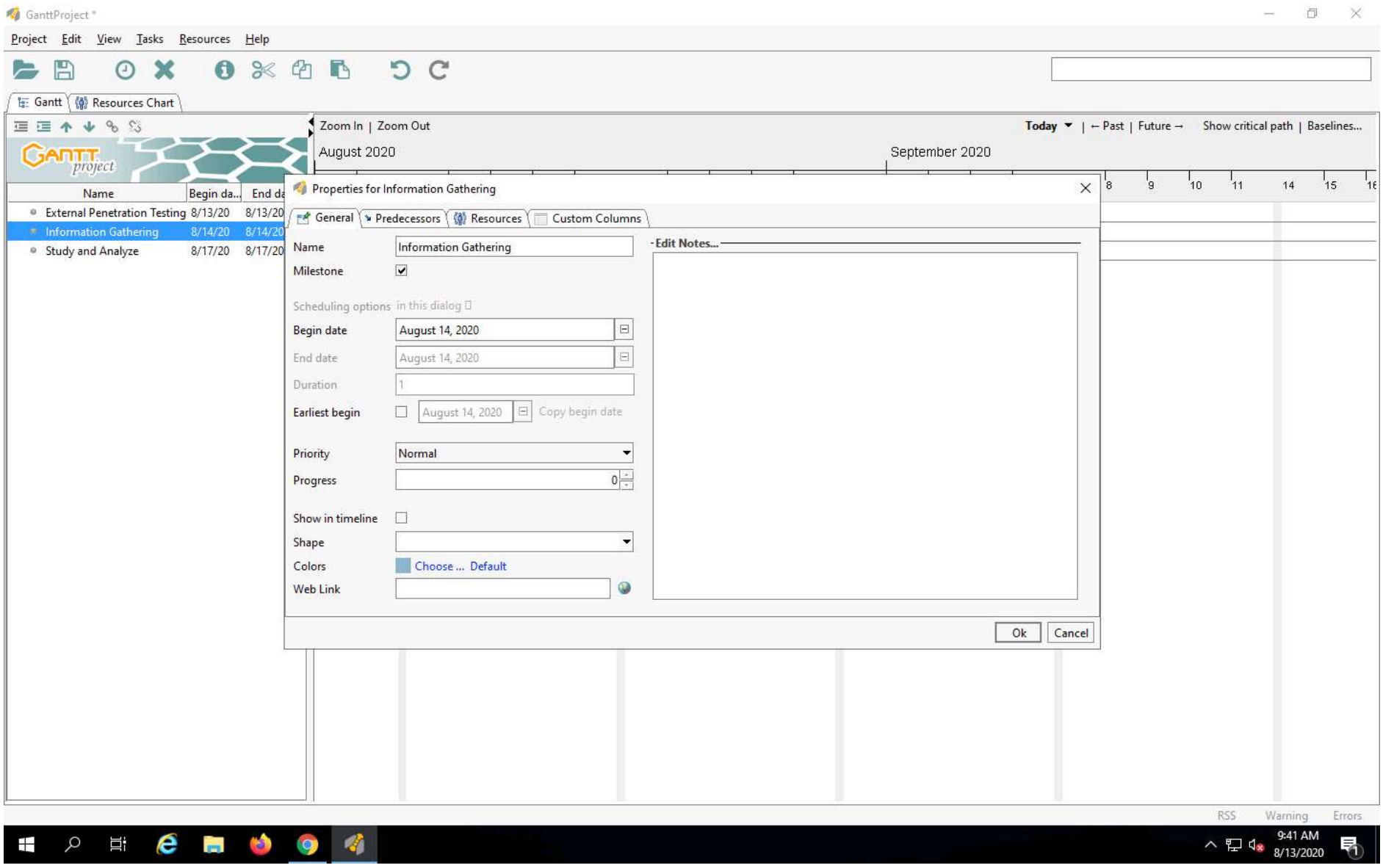
> Note: Similarly, define all the tasks and their relations in the Gantt chart. To show the relationship between the two tasks, drag towards the beginning of the associated project to connect. Click on the middle of the task icon and then drag the cursor to next task in the relation to display the relation between two tasks.



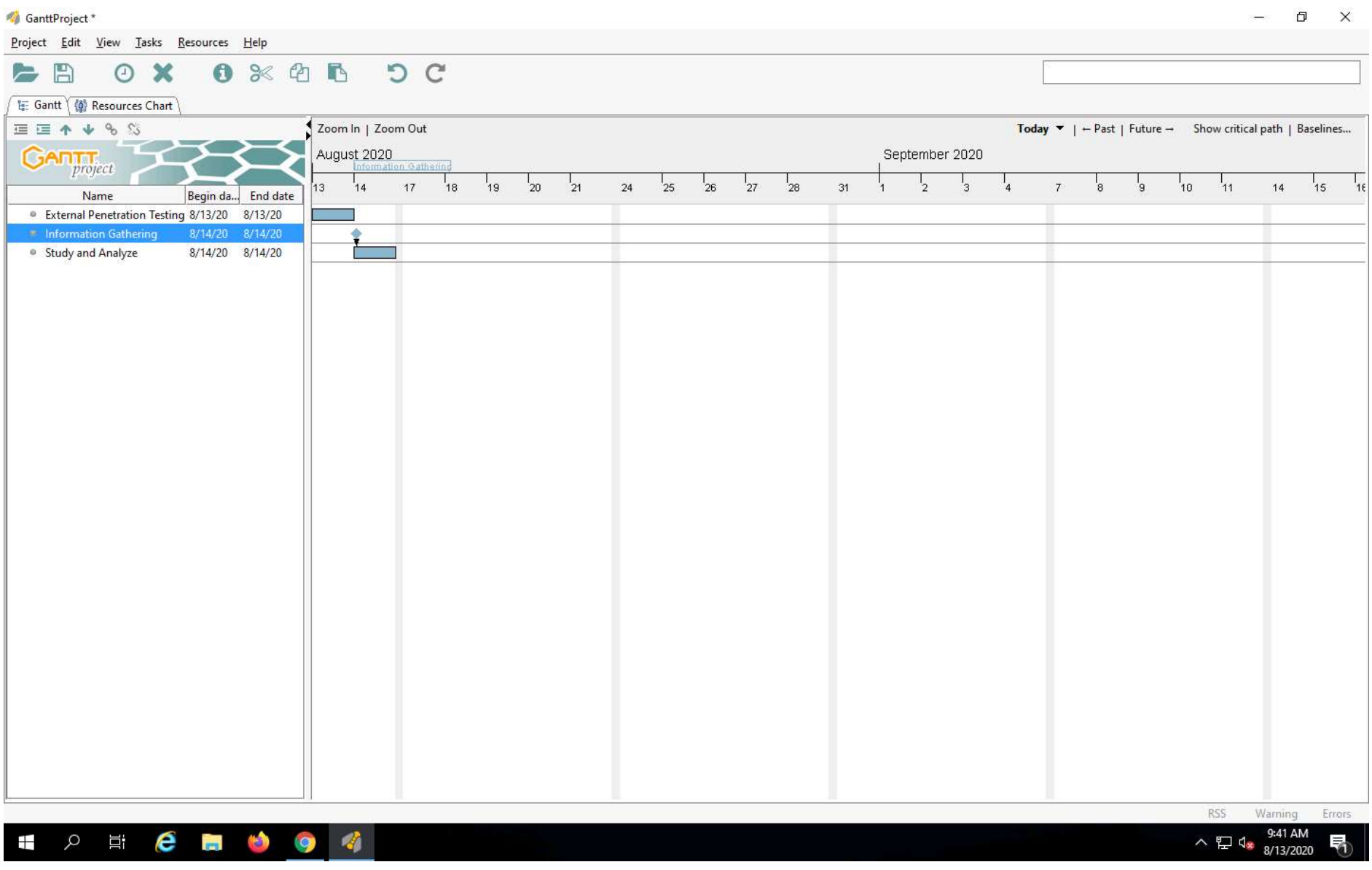
16. To define milestones, right-click any **Task** from left pane under **Gantt** tab, and click **Task Properties** from the context menu.



17. Properties for the Task window appears (here, Information Gathering), check **Milestone** and click **Ok**.

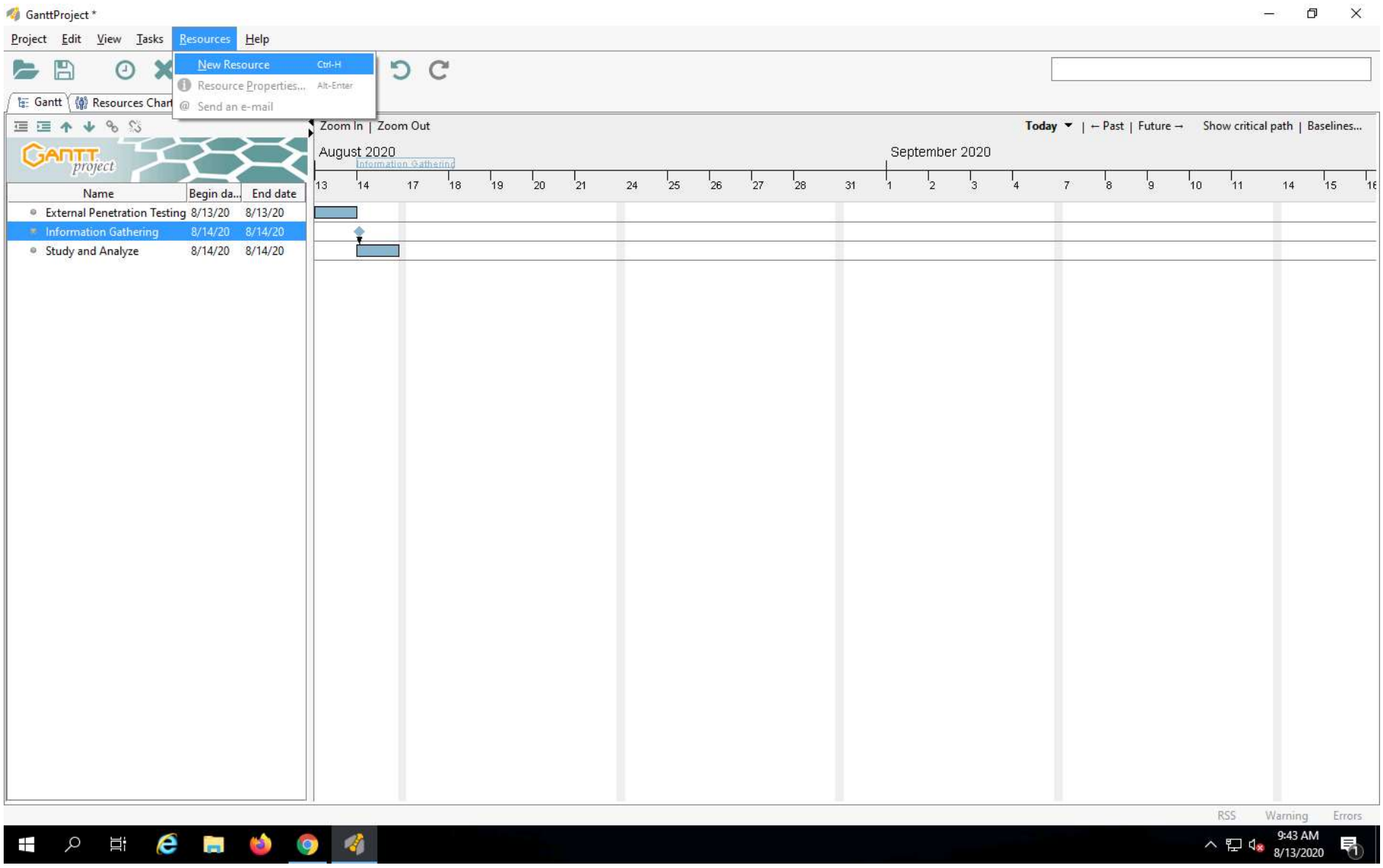


18. The Milestones are displayed as **Diamond** symbols in the Gantt chart as shown in the screenshot.

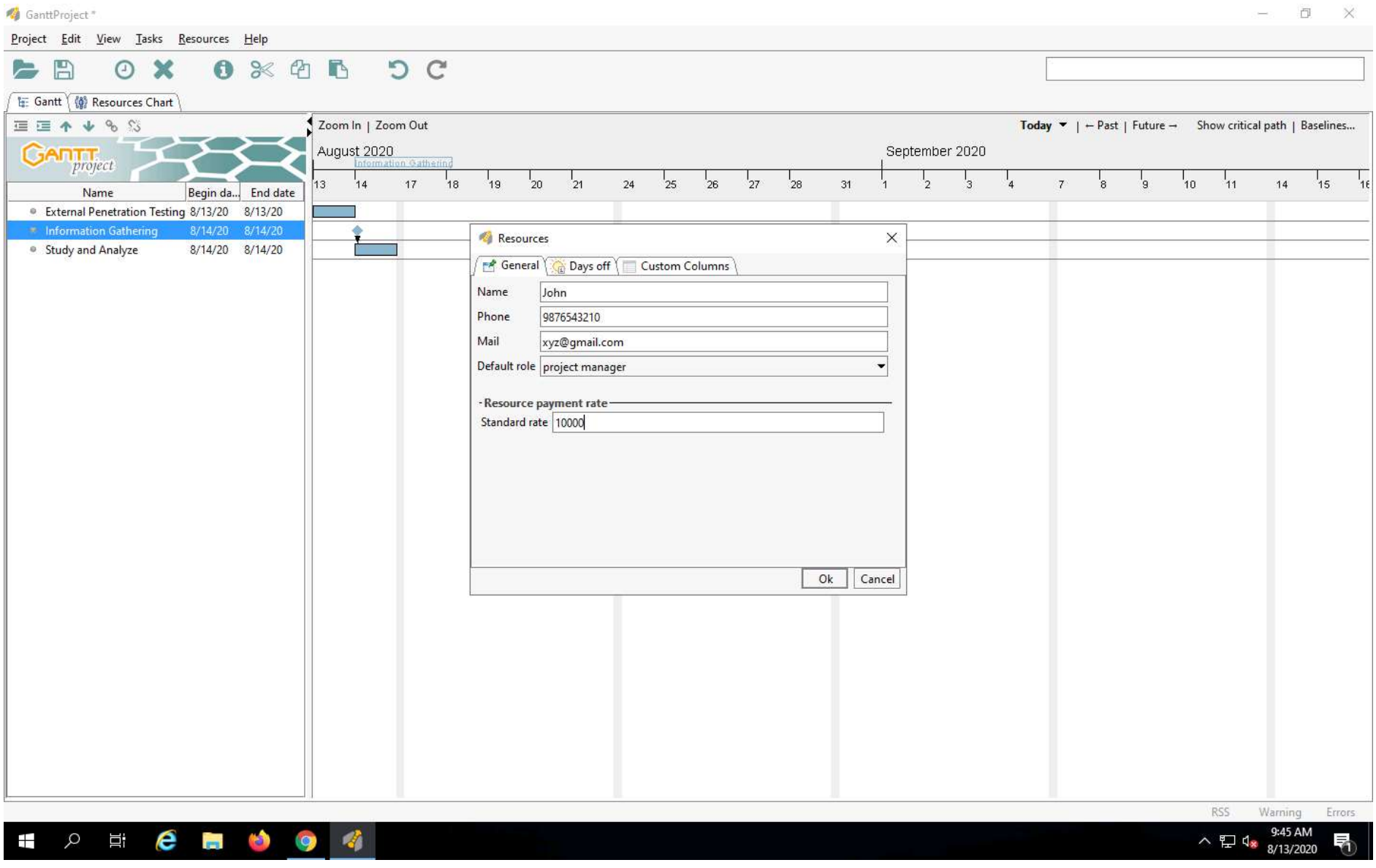


19. Click **Resources Chart** from the left pane and go to **Resources** and then click **New Resource** to assign the resources for your penetration testing project.

> Note: Resources can be people, materials, equipment, budget amounts, or anything else. Typically, you might enter the names of people who will work on the tasks as resources.

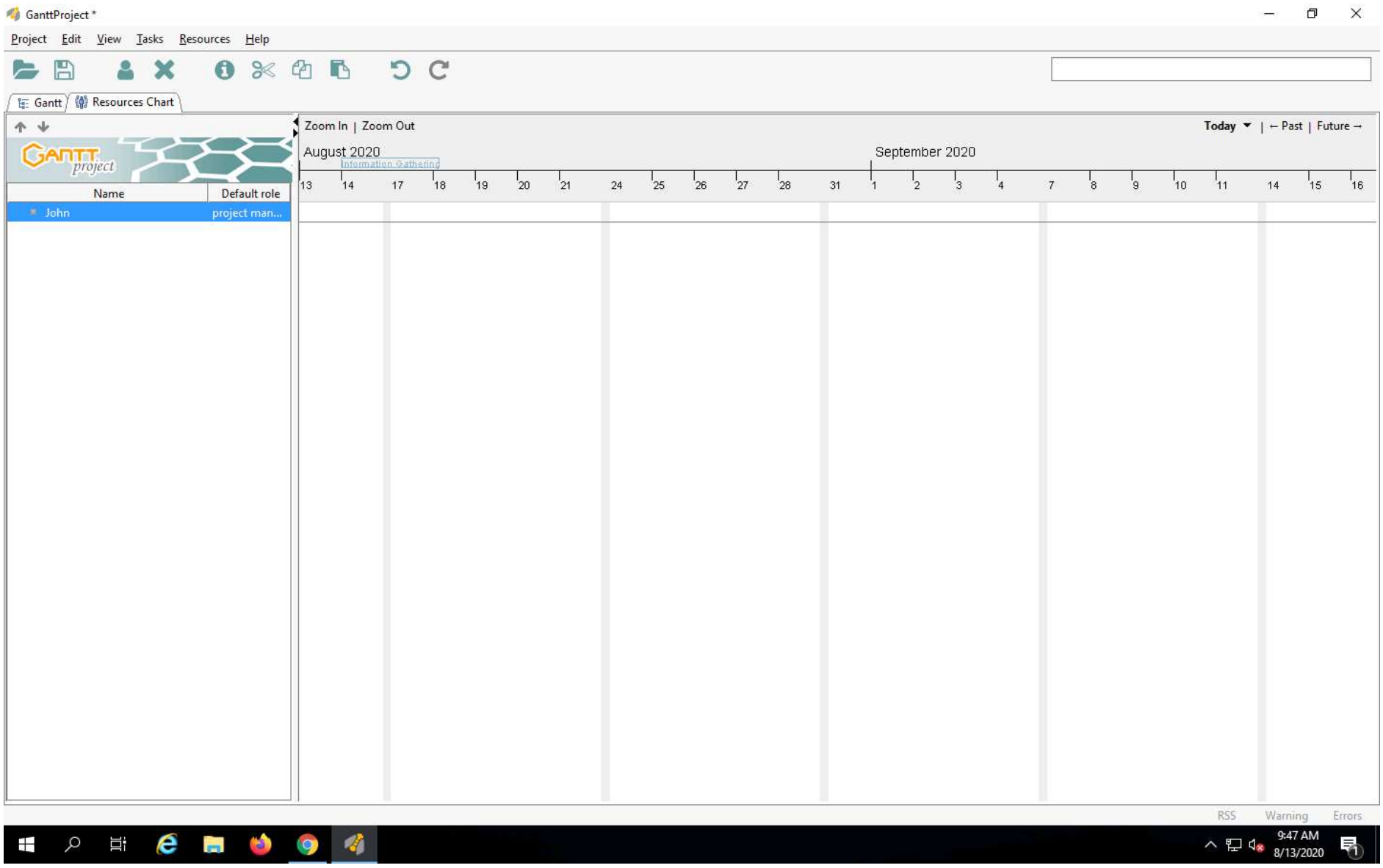


20. The **Resources** window will appear. Specify the **name, phone, email, role,** etc. of the resource as shown in the screenshot, and click **Ok**.

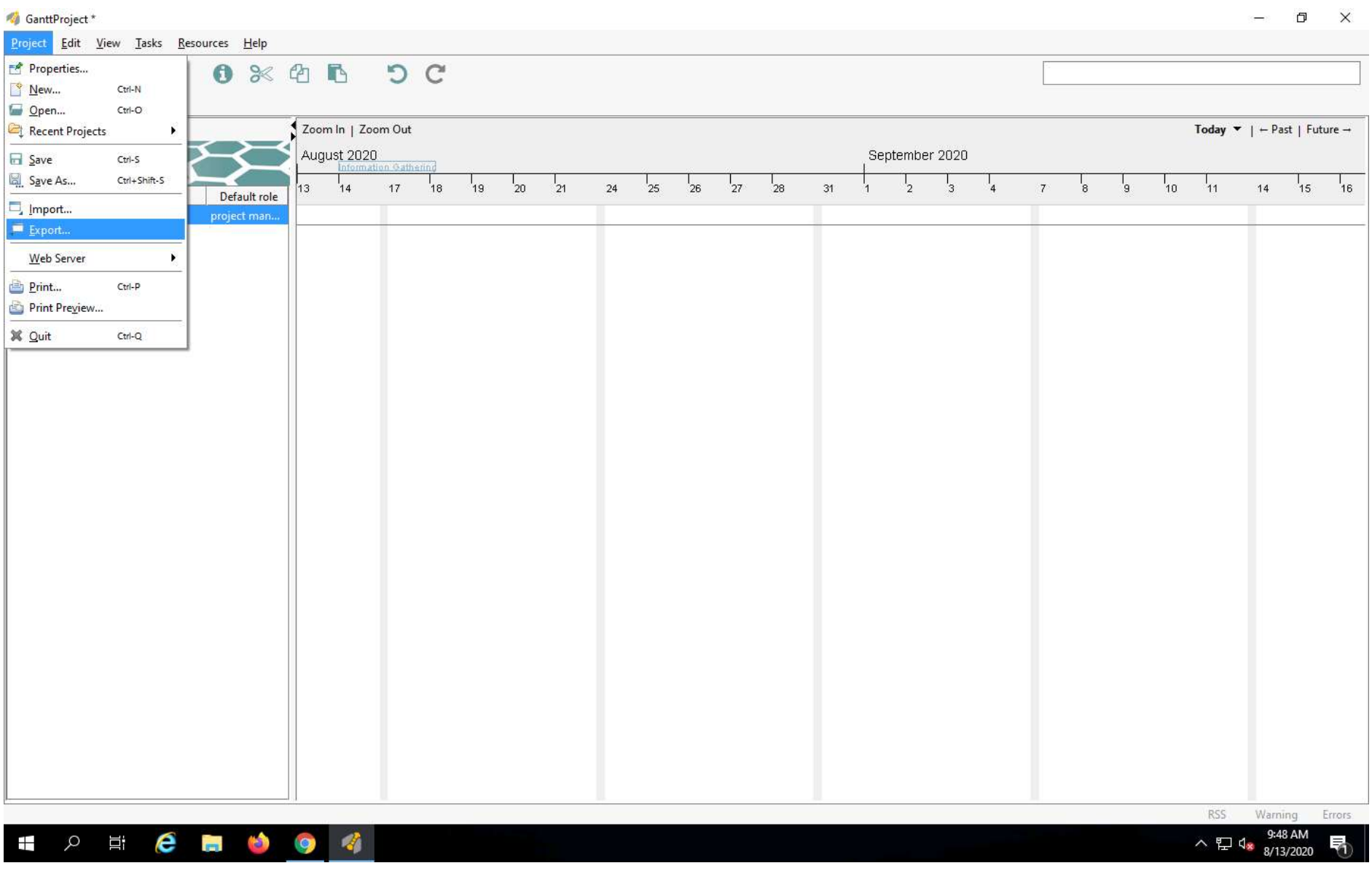


21. The specified **Resource** will be added in the **Resources Chart** tab of the GanttProject.

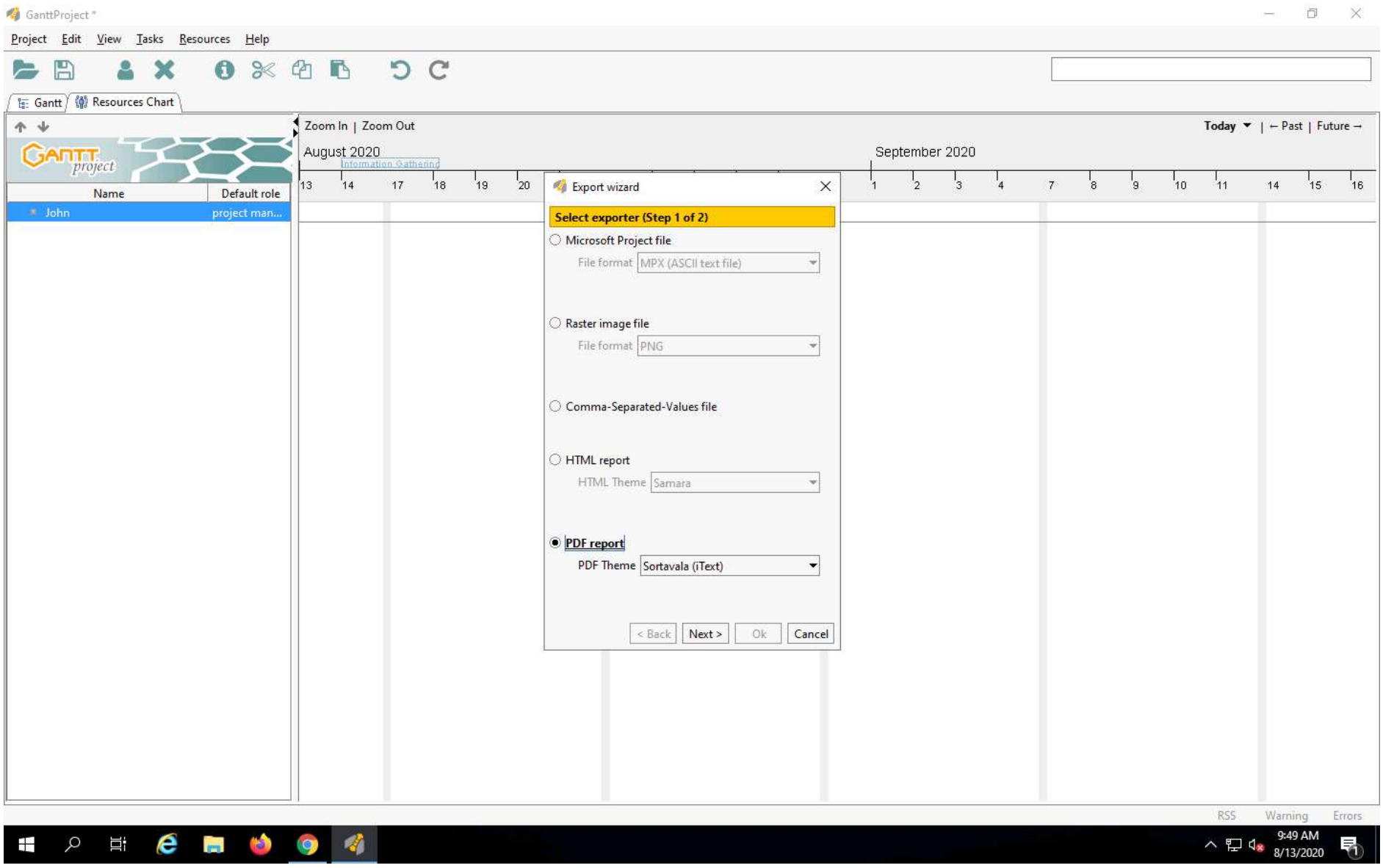
Note: Similarly, you can add any number of resources and their roles working on your penetration project



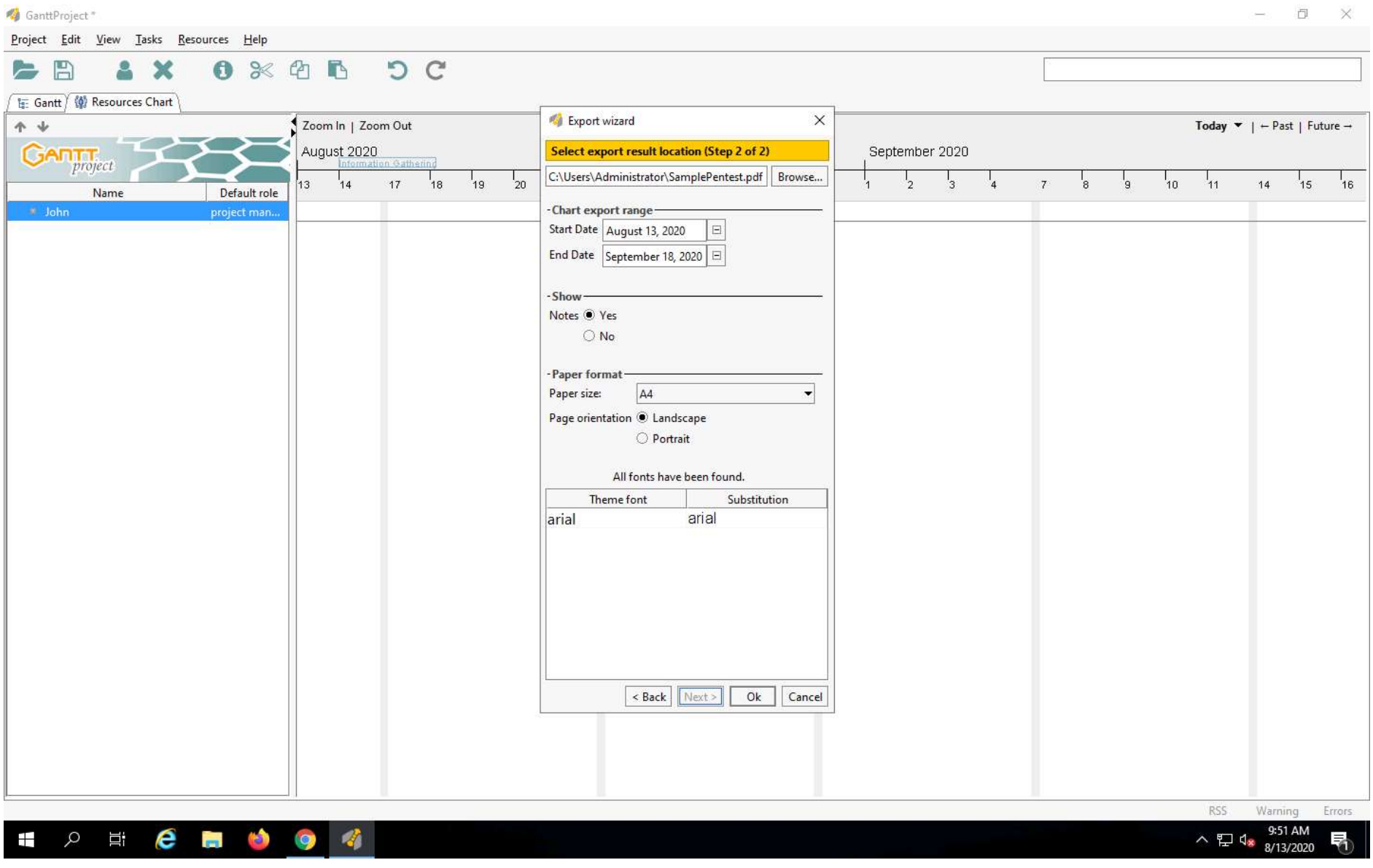
22. Go to **Project** menu and click **Export** to export the planning and scheduling report.



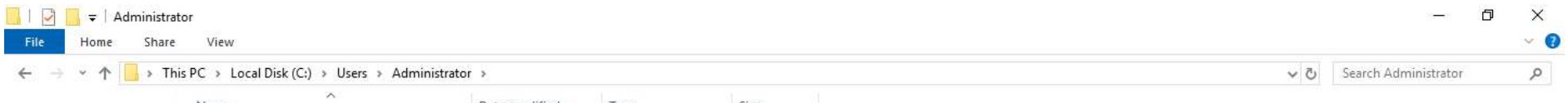
23. **Export Wizard** appears, with Select exporter (Step 1 of 2) wizard as shown in the screenshot. It can publish the report in various formats such as **Microsoft Project file, Raster image file, HTML report, Comma-Separated-Values file and PDF report**. Choose **PDF report format** and click **Next**.



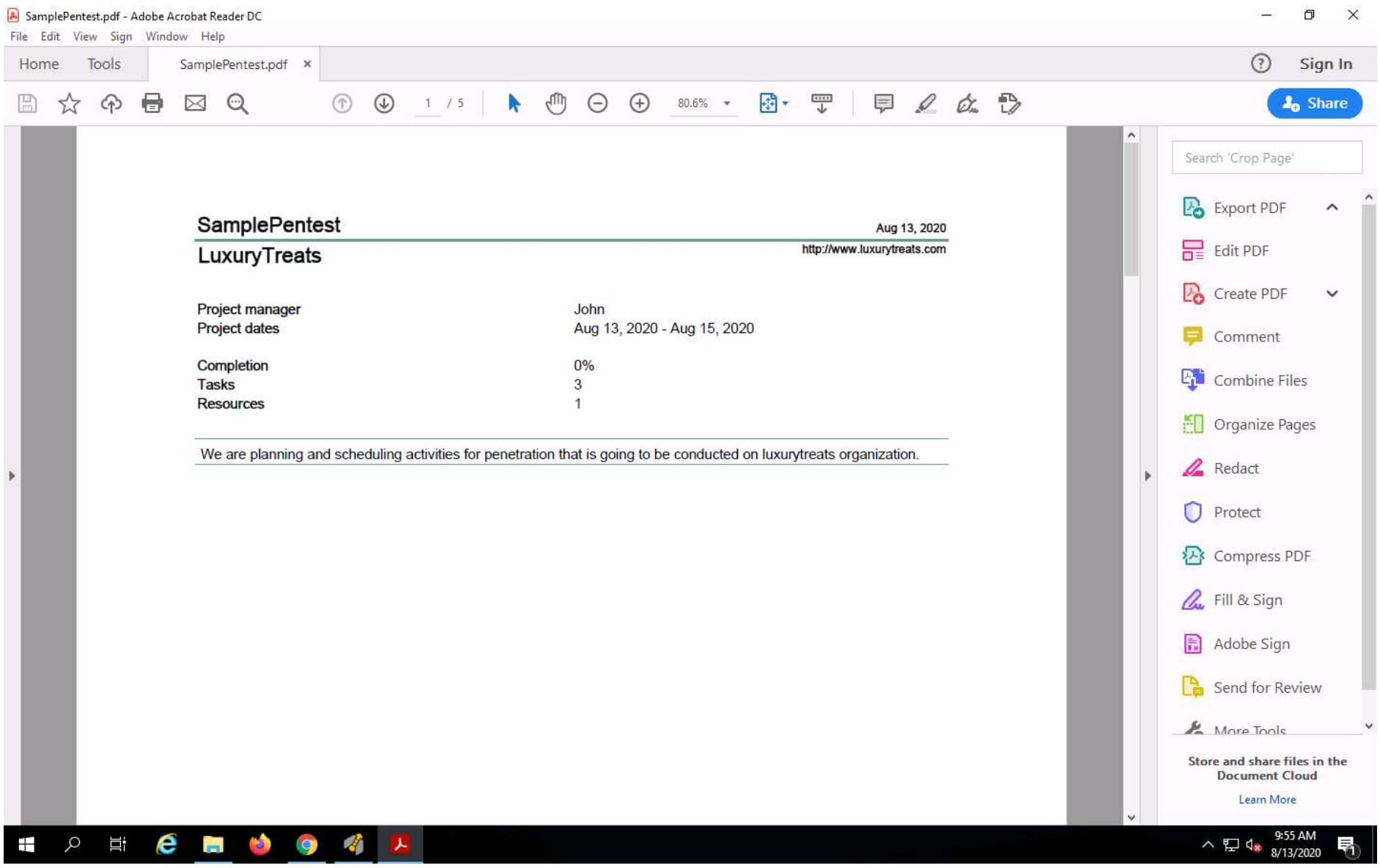
24. In **Step 2** of Export wizard choose the location where you want to save the report (Here,**C:\Users\Administrator**) and click **Ok** to generate a planning and scheduling report in your chosen format.



25. In this task we are generating a pdf format report with the name **SamplePentest.pdf** and the report is saved in the default location **C:\Users\Administrator**.



26. The Penetration Planning and Scheduling report will be saved and displayed in .pdf format in the specified location. Double click **SamplePentest.pdf**



27. Close all the opened windows. You have successfully planned and scheduled the activities in the penetration testing project.

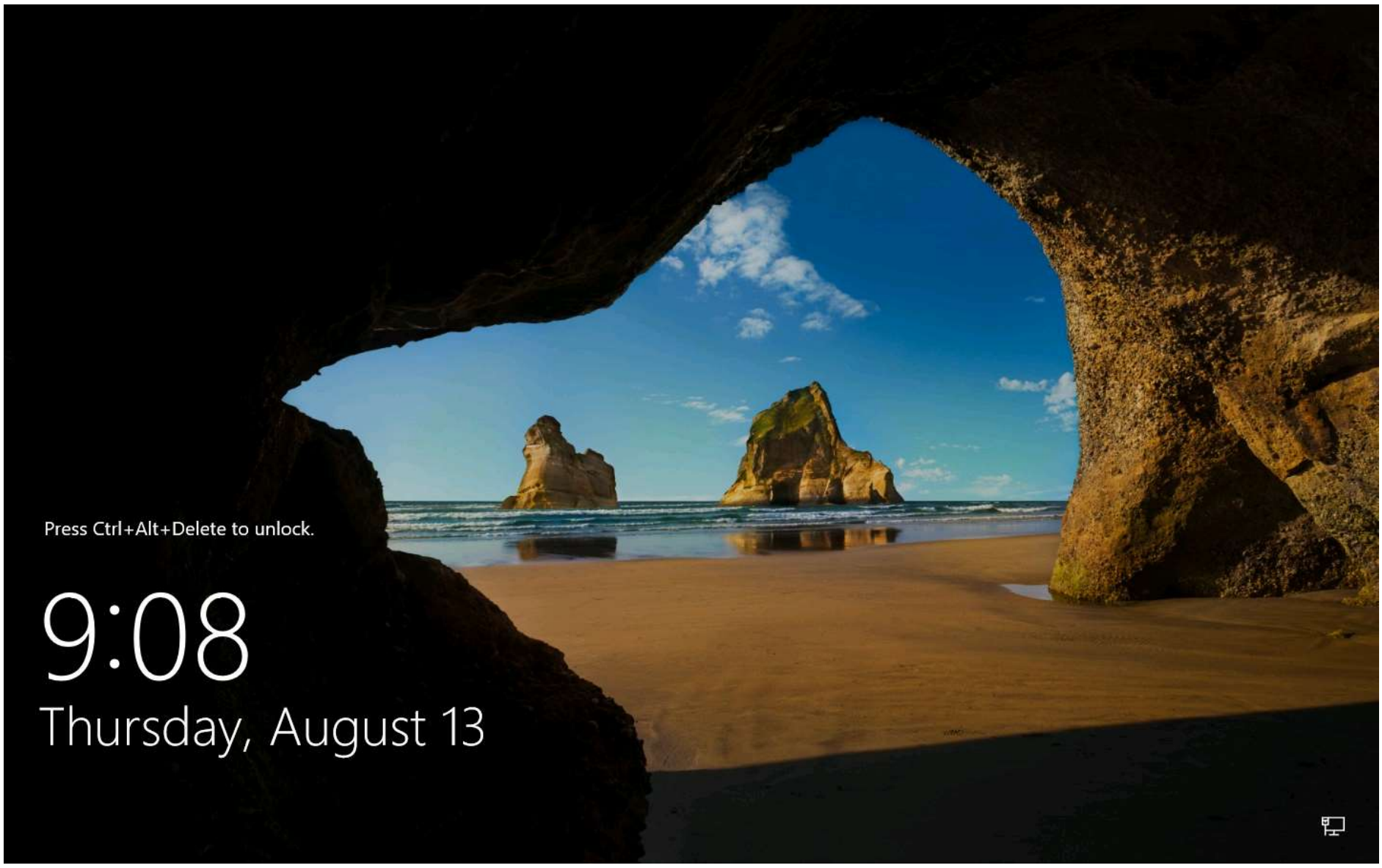
Exercise 2: Penetration Testing Project Planning and Scheduling Using OpenProj

Scenario

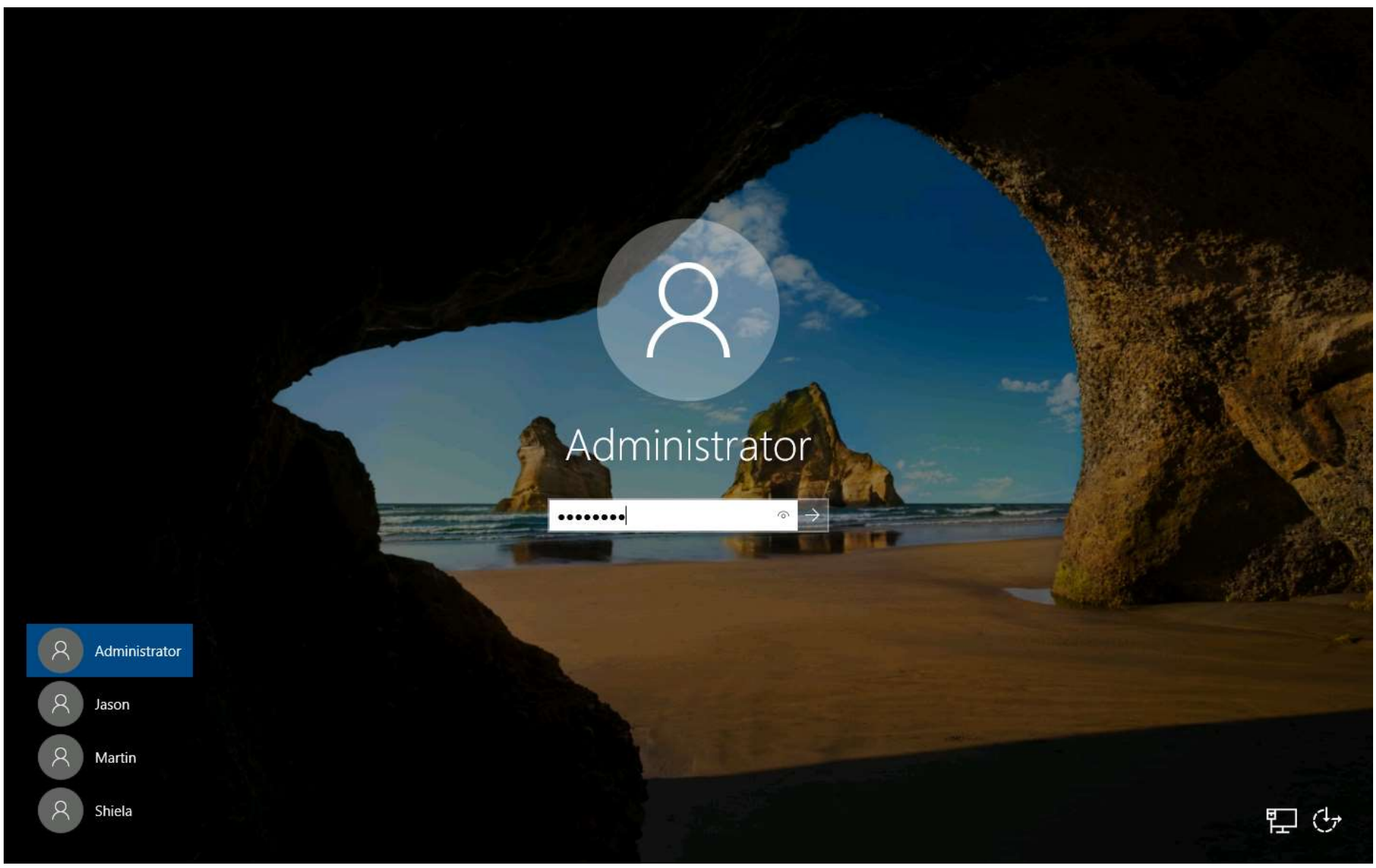
OpenProj software can help you in planning and scheduling the penetration testing assignment in well-structured and efficient manner. This software is used for controlling, tracking and managing the various projects in the organizations.

1. By default **CPENT-M2 Windows Server 2019** machine appears, click **Ctrl+Alt+Del**.

Note: If you are already logged in skip to **step 3**.

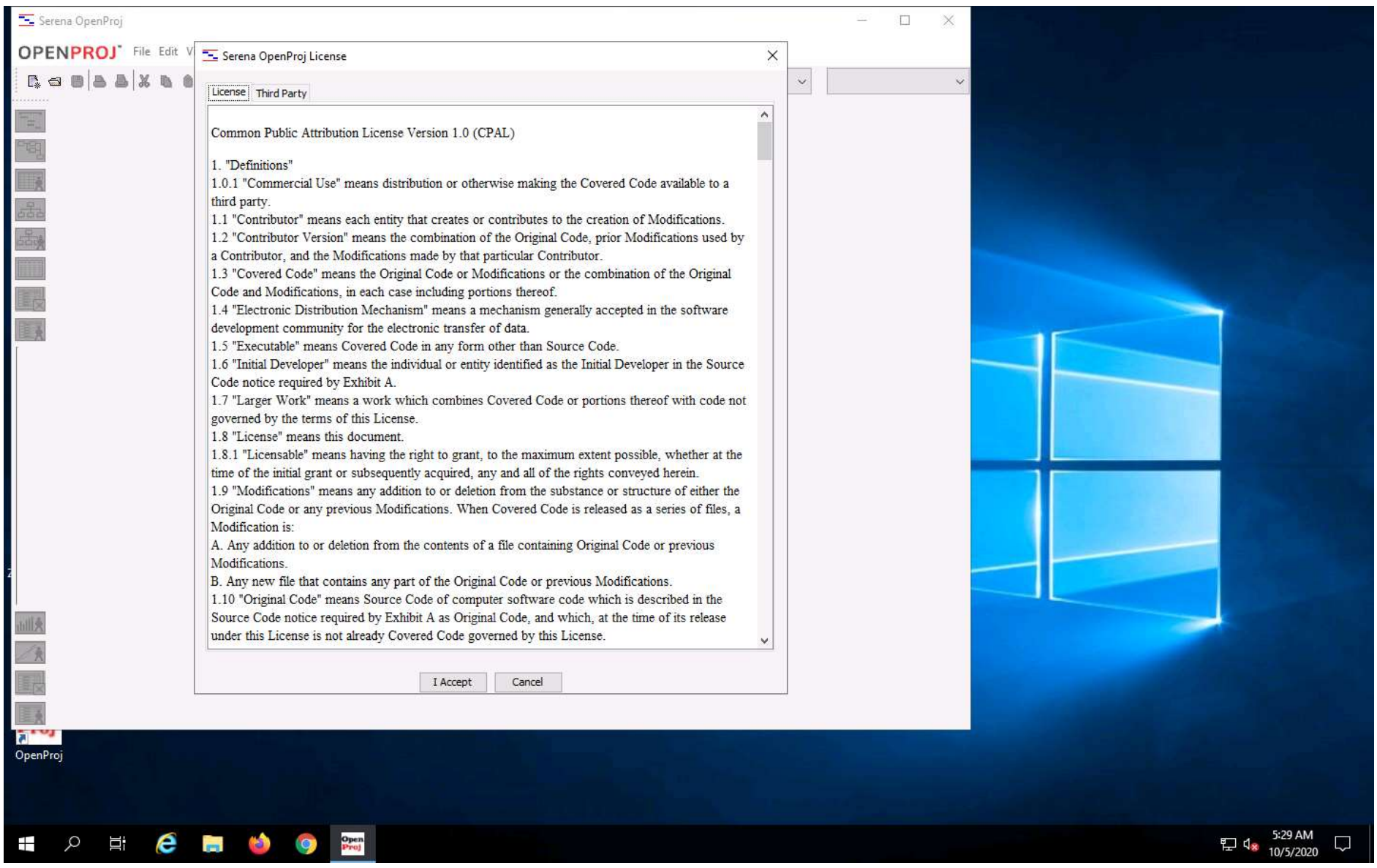


2. In the password field type **Pa$$w0rd** and press **Enter**



3. To launch **OpenProj**, double-click **OpenProj** shortcut icon on the Desktop.

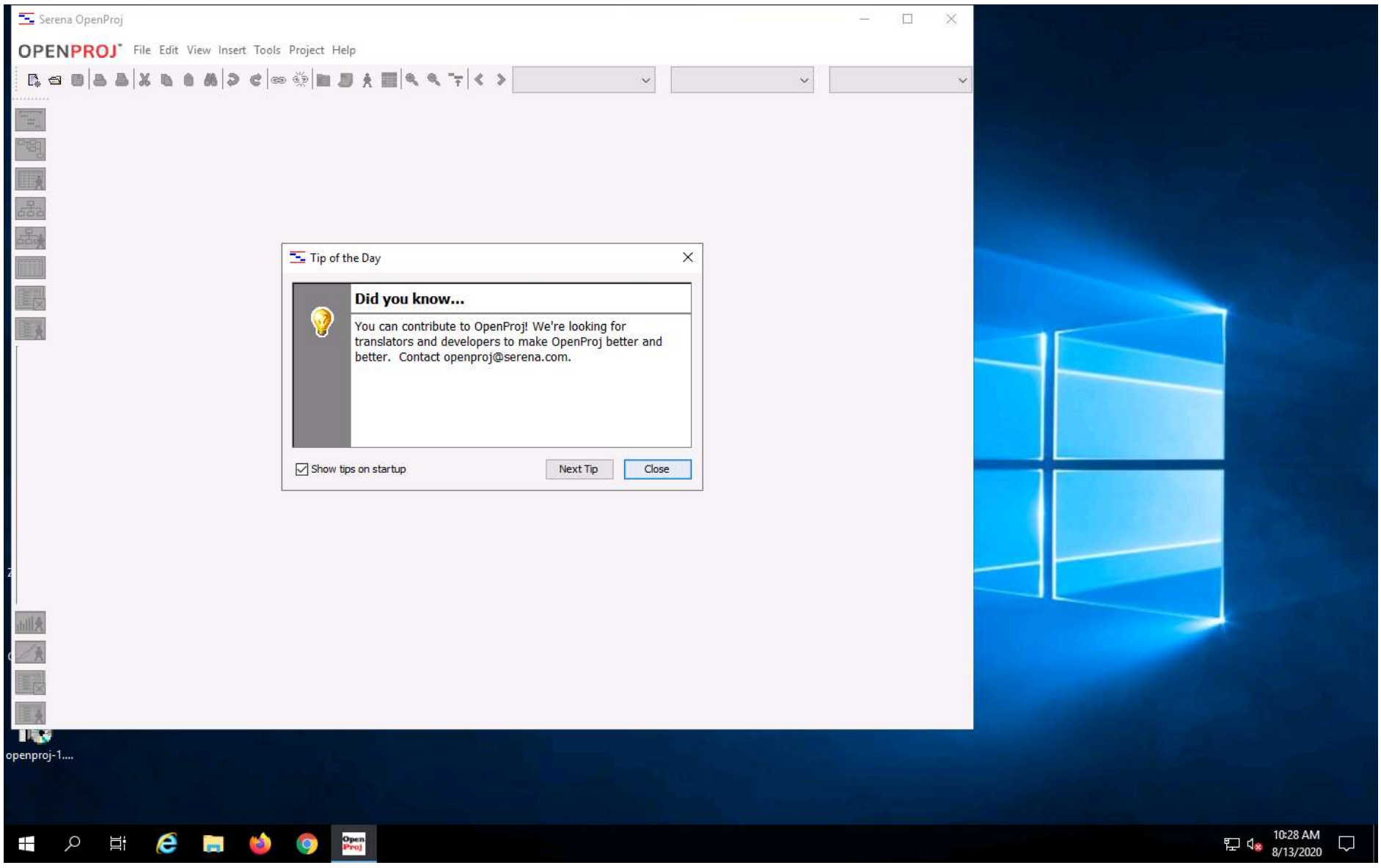
4. Serena OpenProj License window appears, click **I Accept**.



5. The **OpenProj** main window appears.

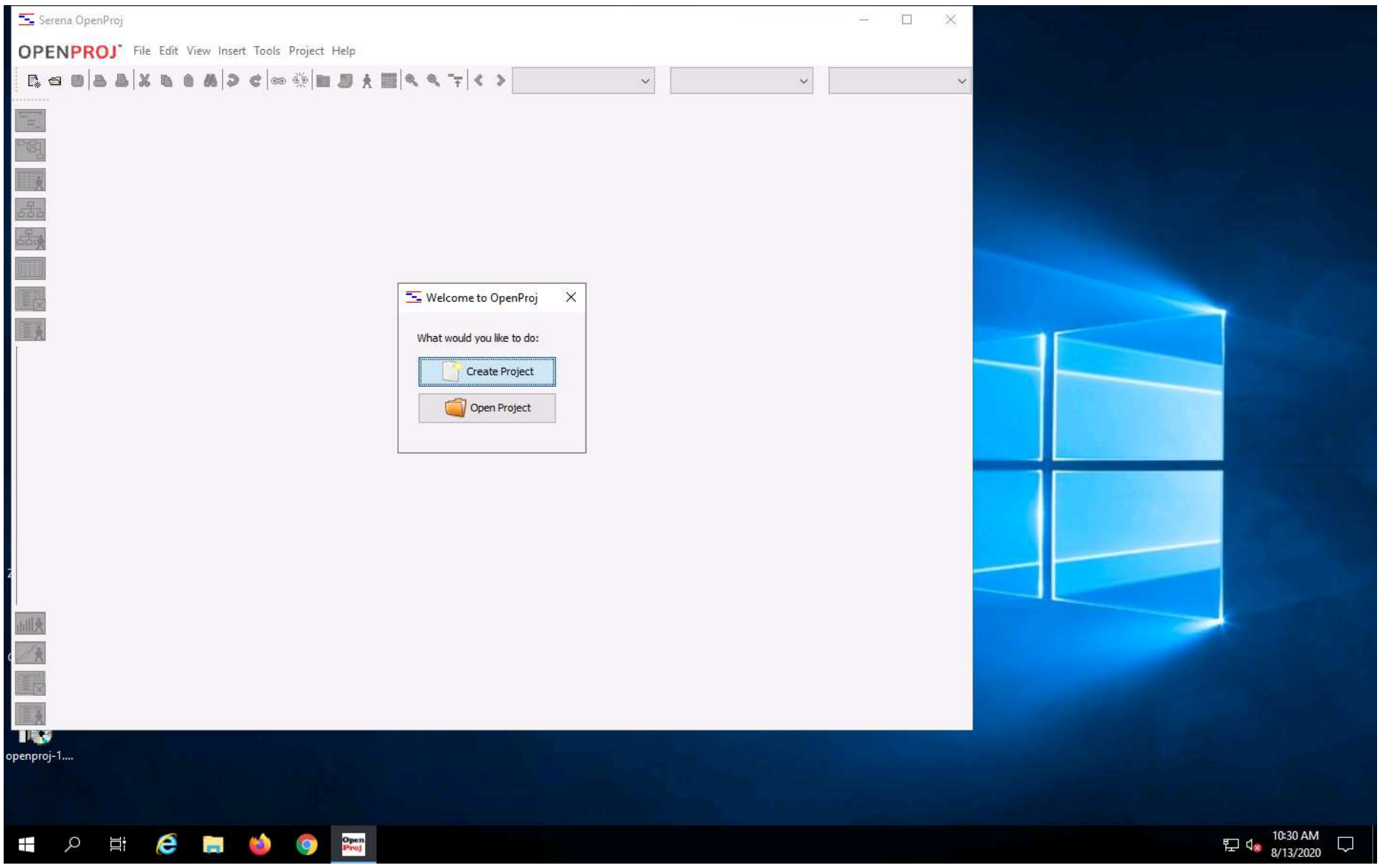
> Note: The Serena OpenProj Customer Information pop-up appears, register with OpenProj using your email address and click **Cancel**.

6. The OpenProj main window appears, along with the Tip of the Day pop-up. Click **Close**.



7. Click **Create Project** on **Welcome to OpenProj** window in order to plan and schedule your penetration testing project.

Note: You can also create a new project from File menu i.e., from File -> New Project menu



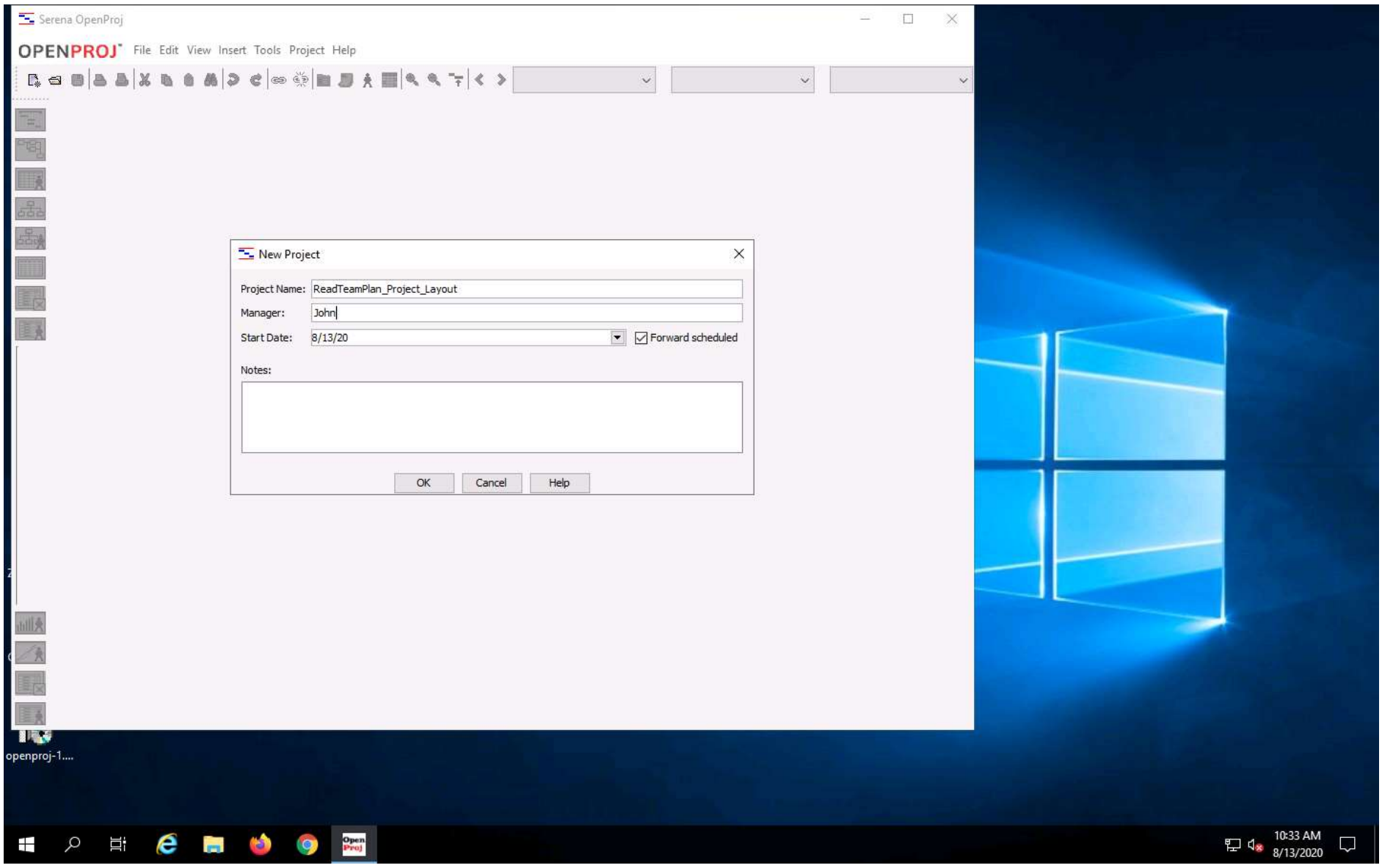
8. The **New Project** window appears; **enter the name of your project, Start date of project, Name of the Manager,** and click **OK**. Here,

   Project Name: RedTeamPlan_Project_Layout

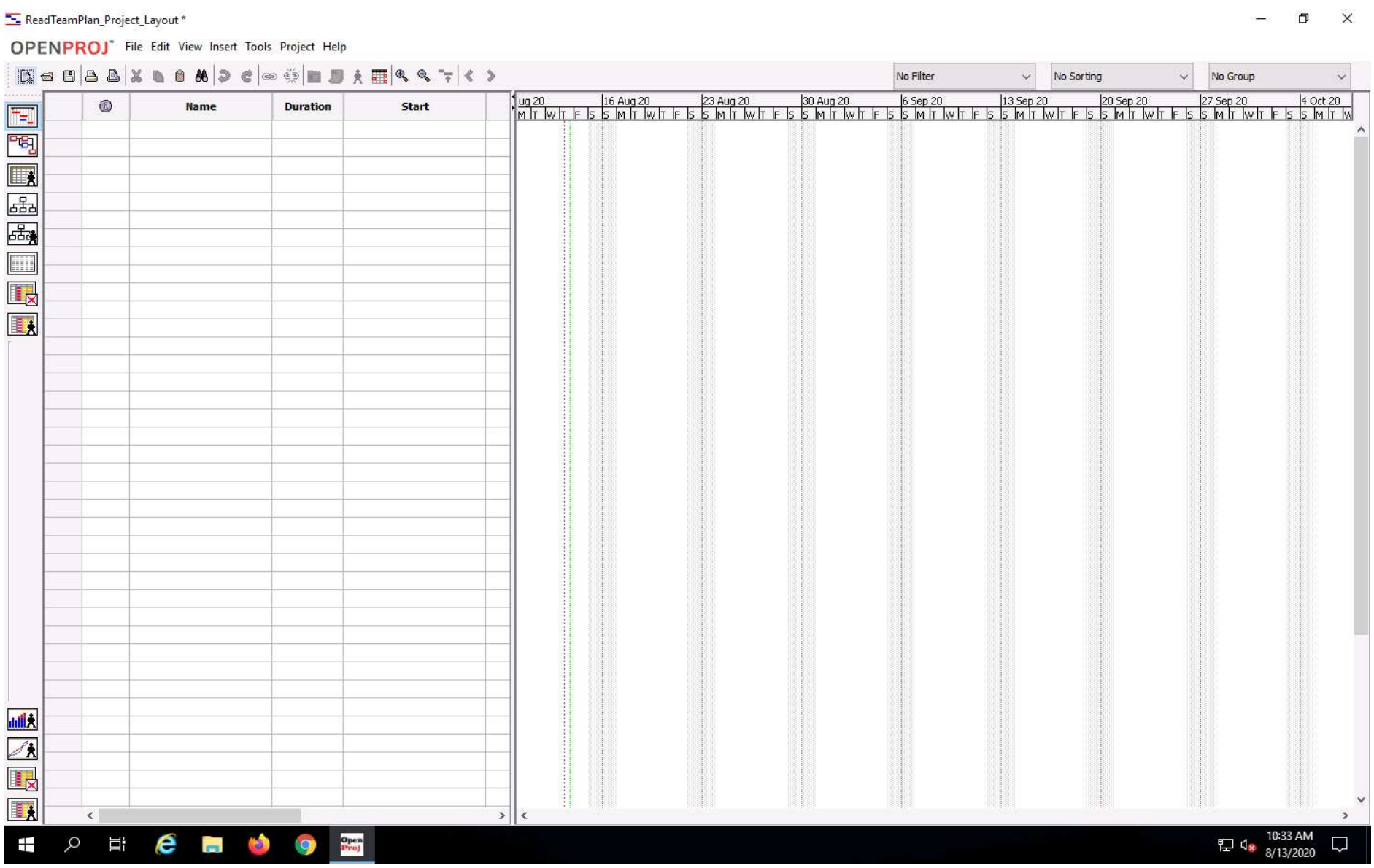
   Start date: Mention the date

   Manager: John

   Notes: Optional.



9. The empty new project is created as shown in the screenshot.

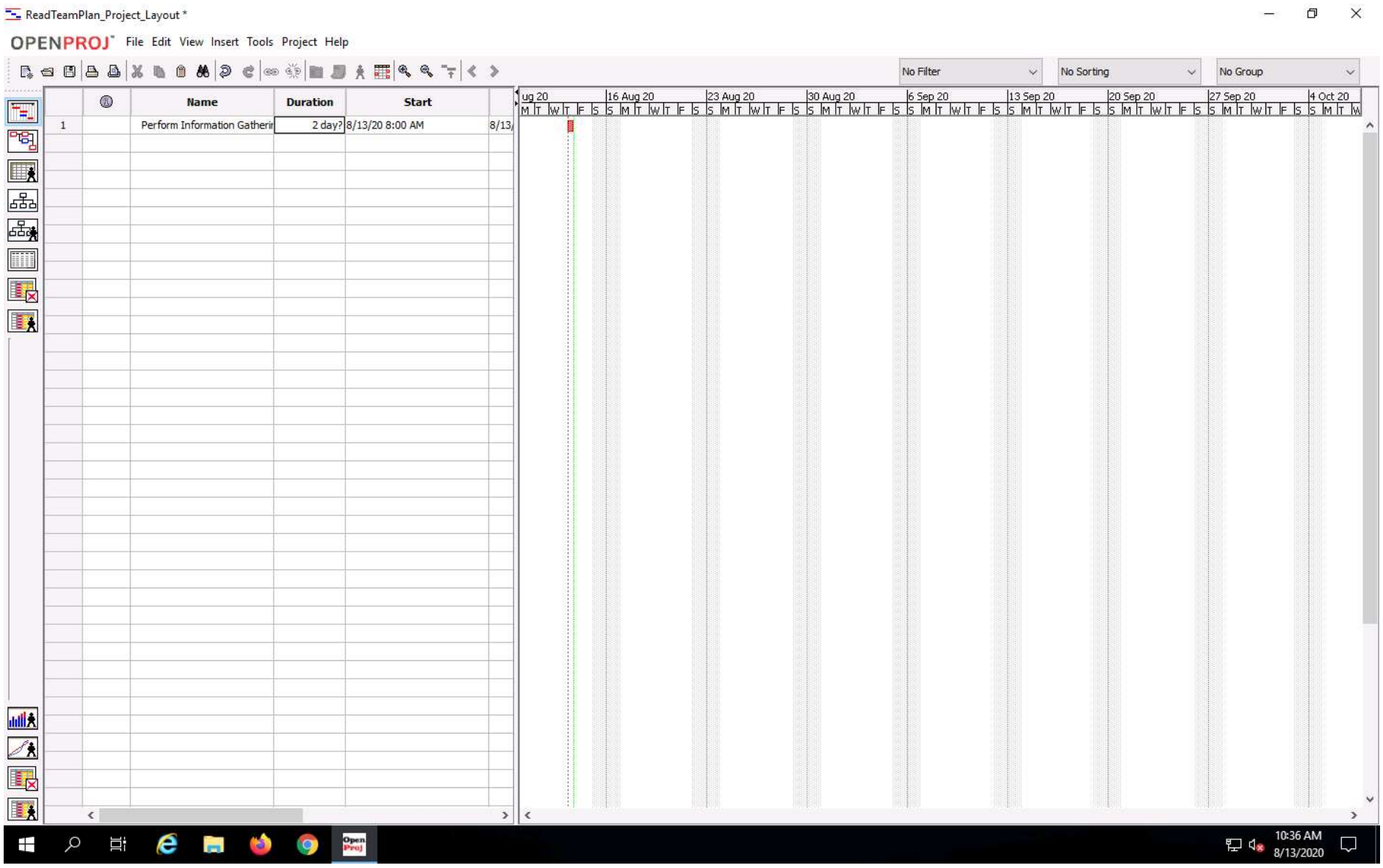


10. Enter the name of the task directly under the **Name** column and schedule the task by adding start date / time and finish date/time for the task under **Start** and **Finish** columns respectively.

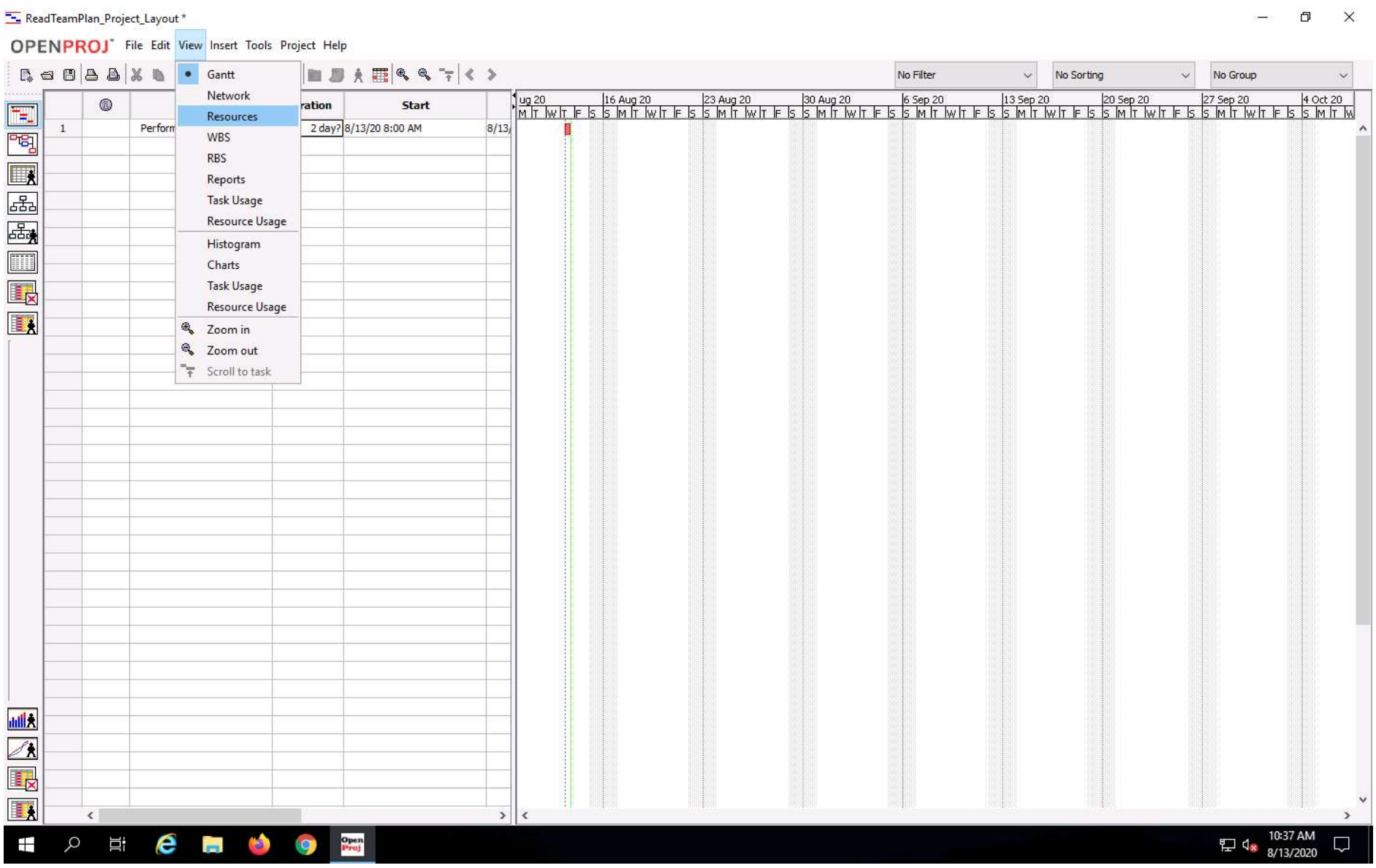
> Note: The Start date/time and Finish date/time may vary as you perform the tasks. You can also provide preferred Start and Finish date/time accordingly.

Drag the left pane to the right until all the column names are visible.

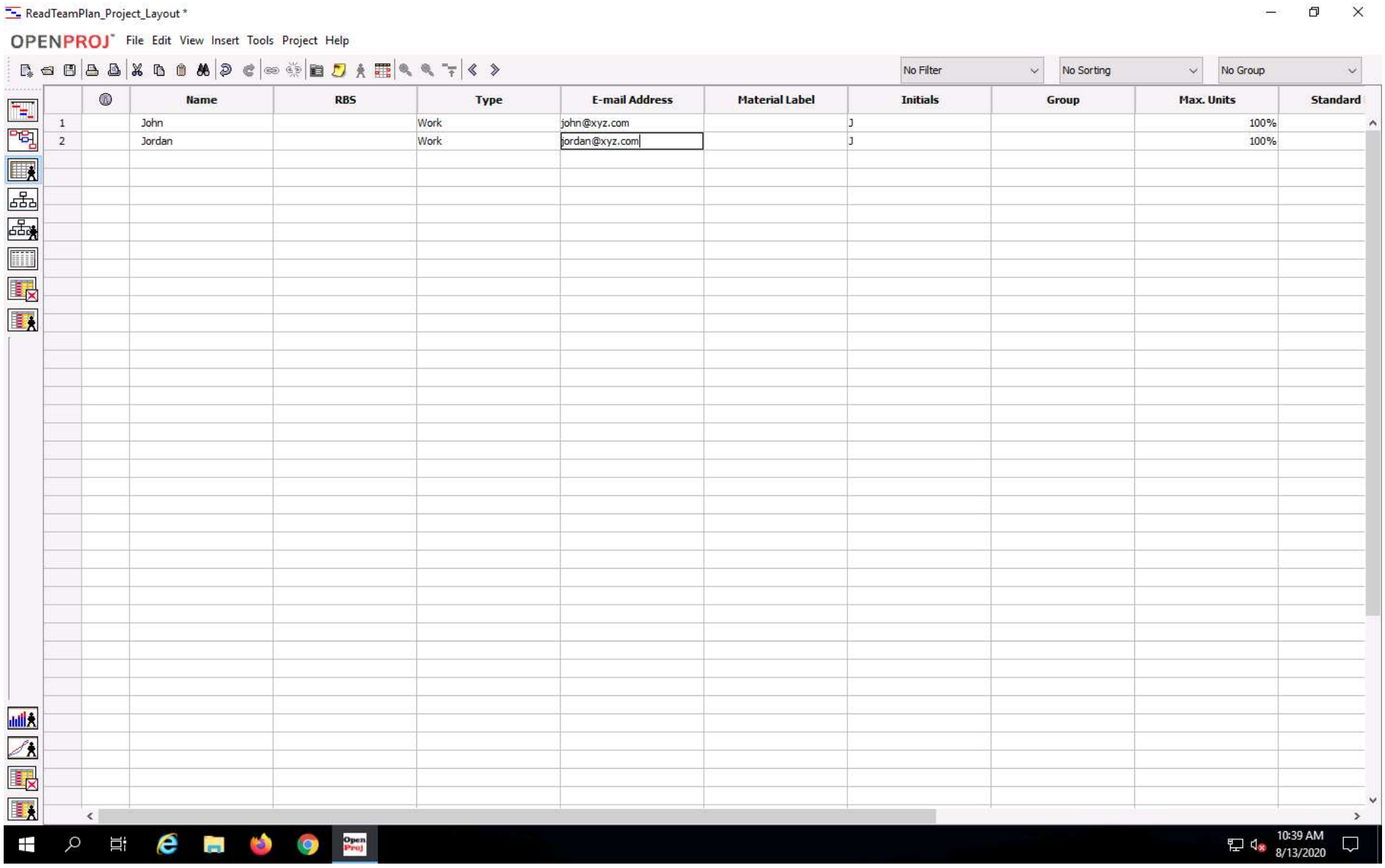
You can also double-click on column field to fill the task details with Task Information wizard. If the task completes within 8 hours, you can also change the number of hours the task will take with the help of Task Information wizard



11. Go to **View** -> **Resources** from the menu to add the resources that will be involved in the project.

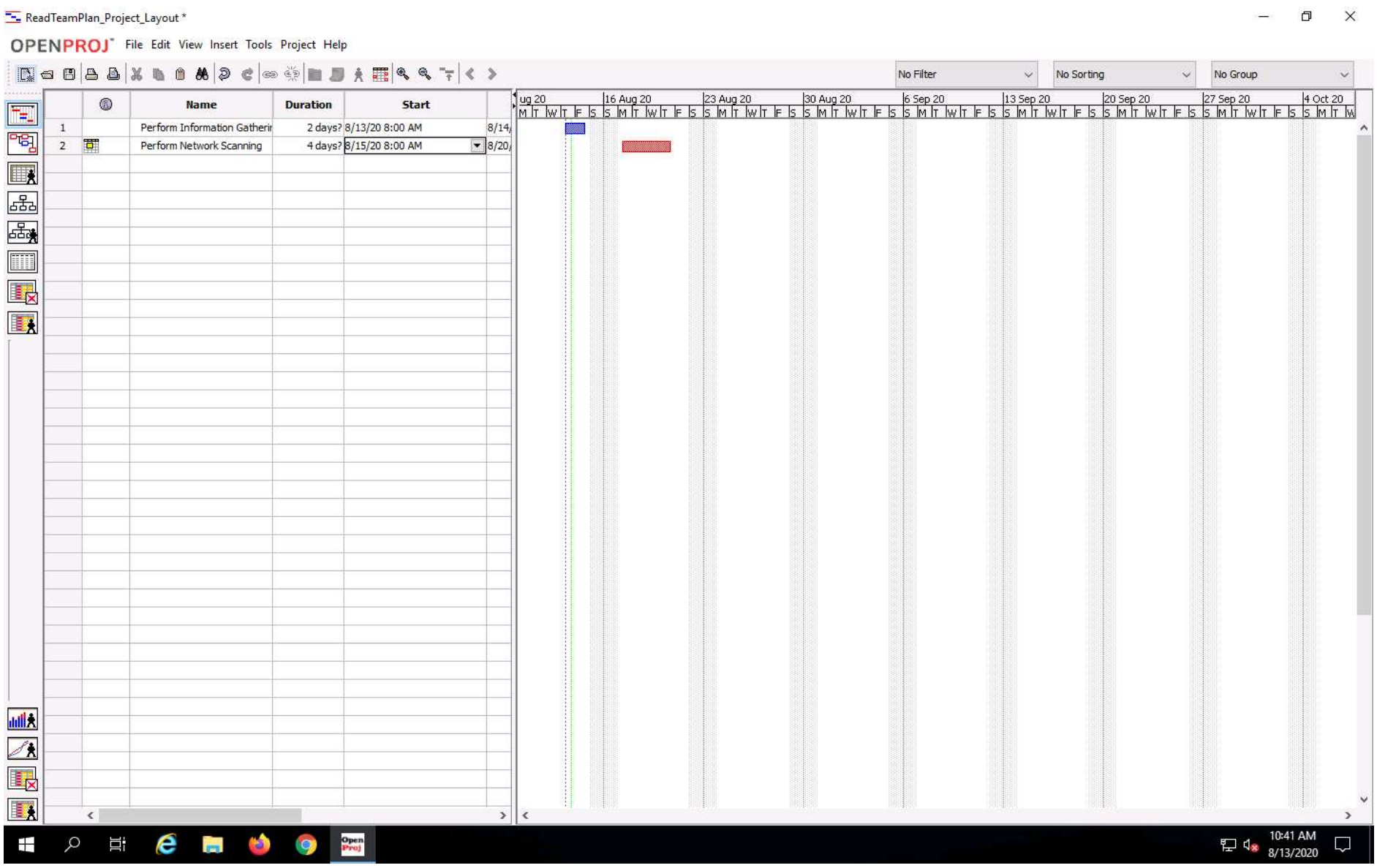


12. Enter all the **resources** details that will be engaged in the activities of project.

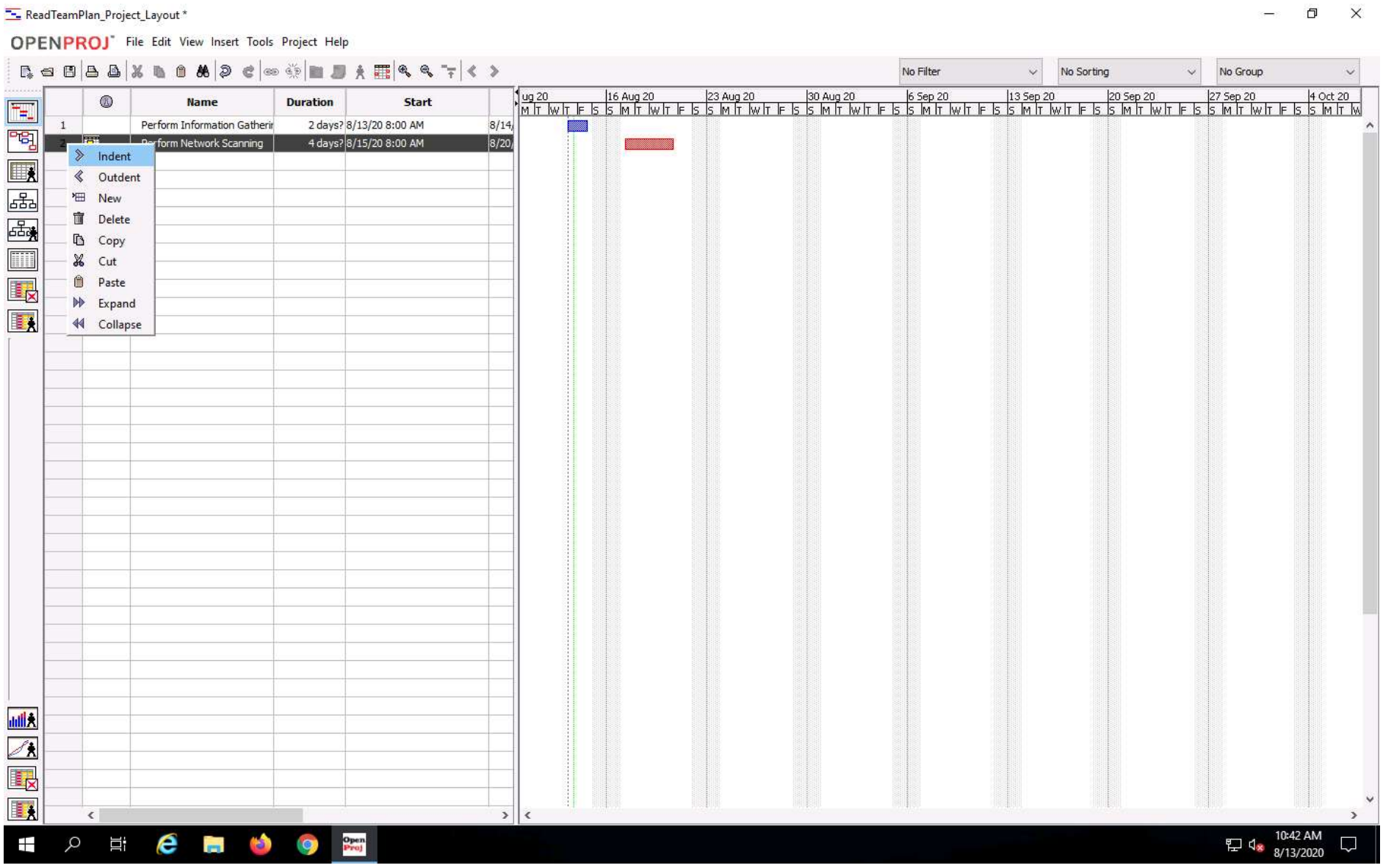


13. Now click **Gantt** tab from the left-hand side (1st tab) and enter the name of the task directly under Name column and schedule the task by adding start date / time and finish date/time for the task under **Start** and **Finish** columns respectively.

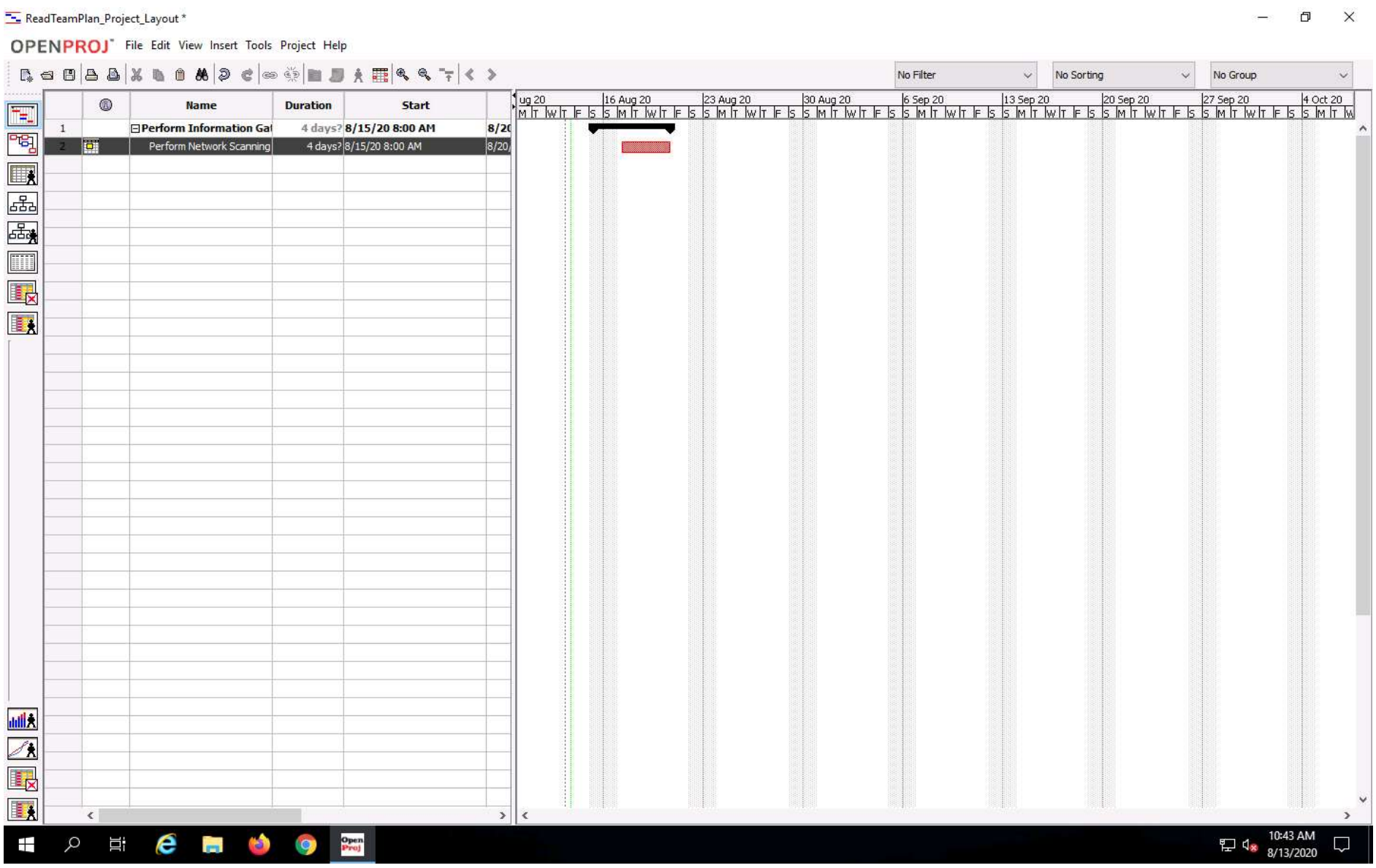
Note: You can also directly enter the number of days that task will take with the help of Task Information



14. **Right Click** on the task that you want to have as a subtask, and then click **Indent (>)** from the context menu to create a new subtask as shown in the screenshot.

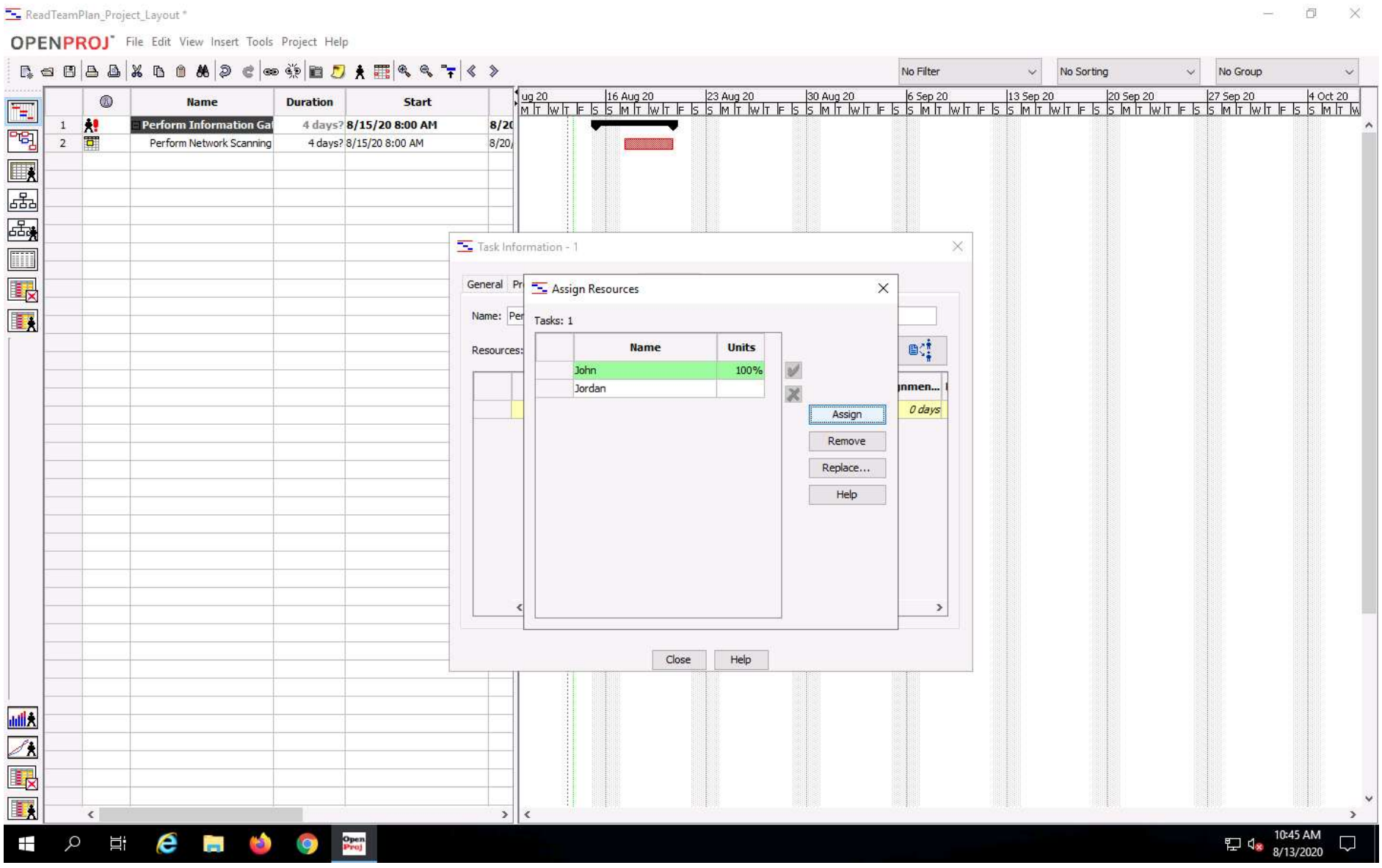


15. A new subtask is created as shown in the screenshot. The prior task will get a **node** option, with which you can expand the tasks.

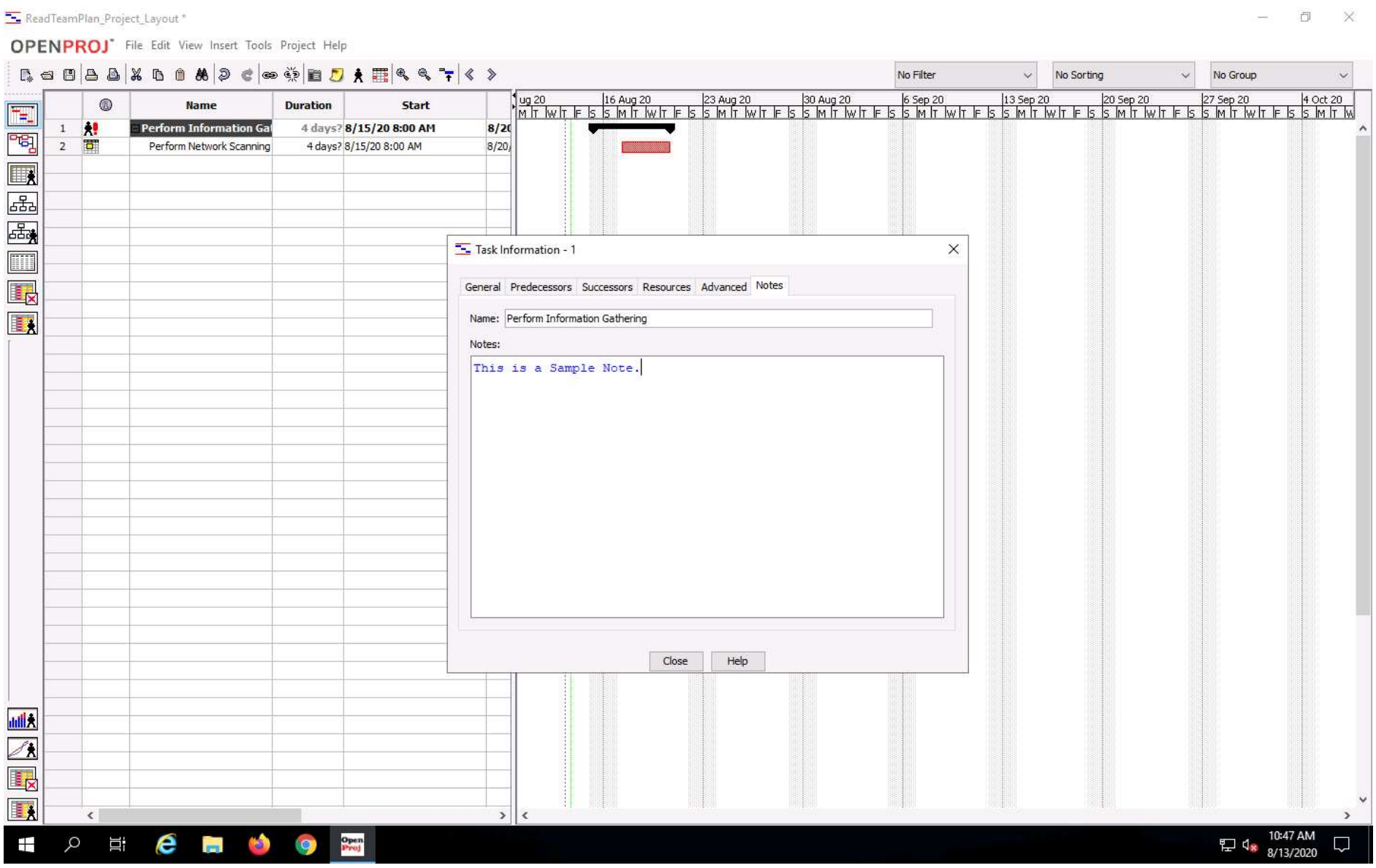


16. **Double-click** on the task to which resources must be assigned. **Task Information - 1** wizard will pop up. Go to **Resources** tab and click **Assign Resources** button ( ). The Assign Resources window will appear; click **Assign** button to assign resources from available resources.

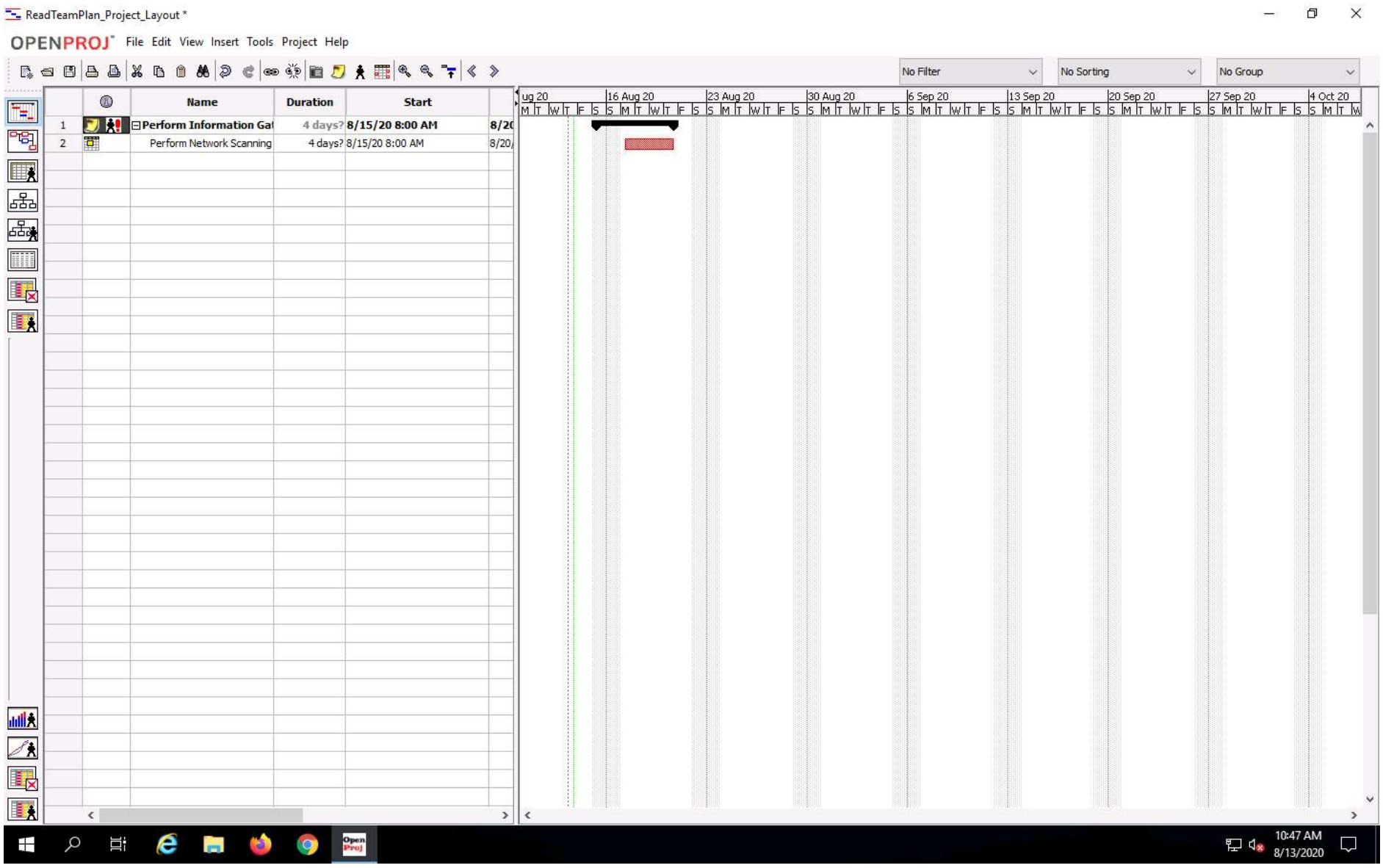
Note: Once you have assigned the resources, close the Assign Resources.



17. **Double-click** the task for which you want place notes. Under Task **Information - 1** wizard, go to **Notes** tab and write your note about the task. Click **Close**.



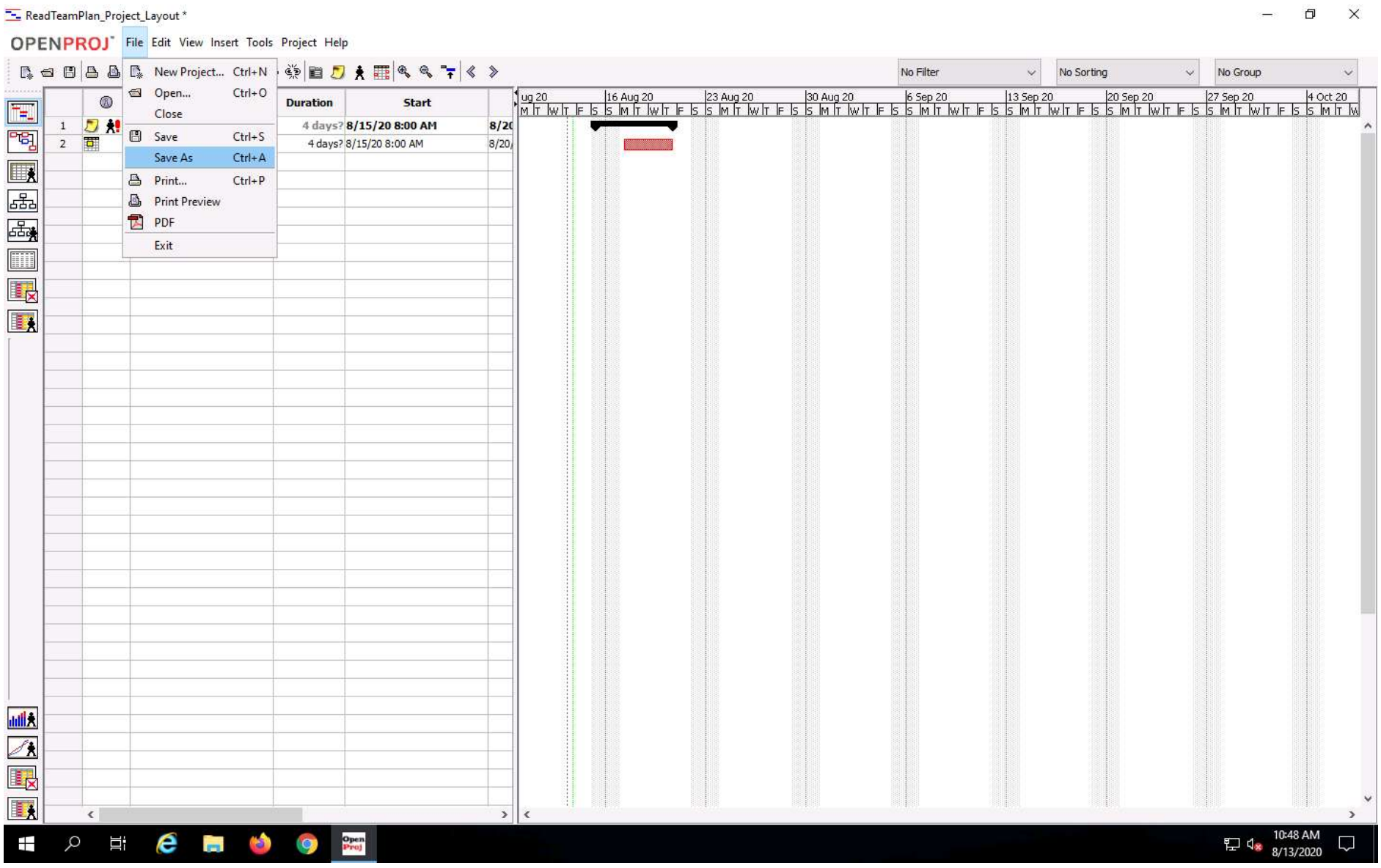
18. The Note and Assignee will be added in the Task as shown in the screenshot.

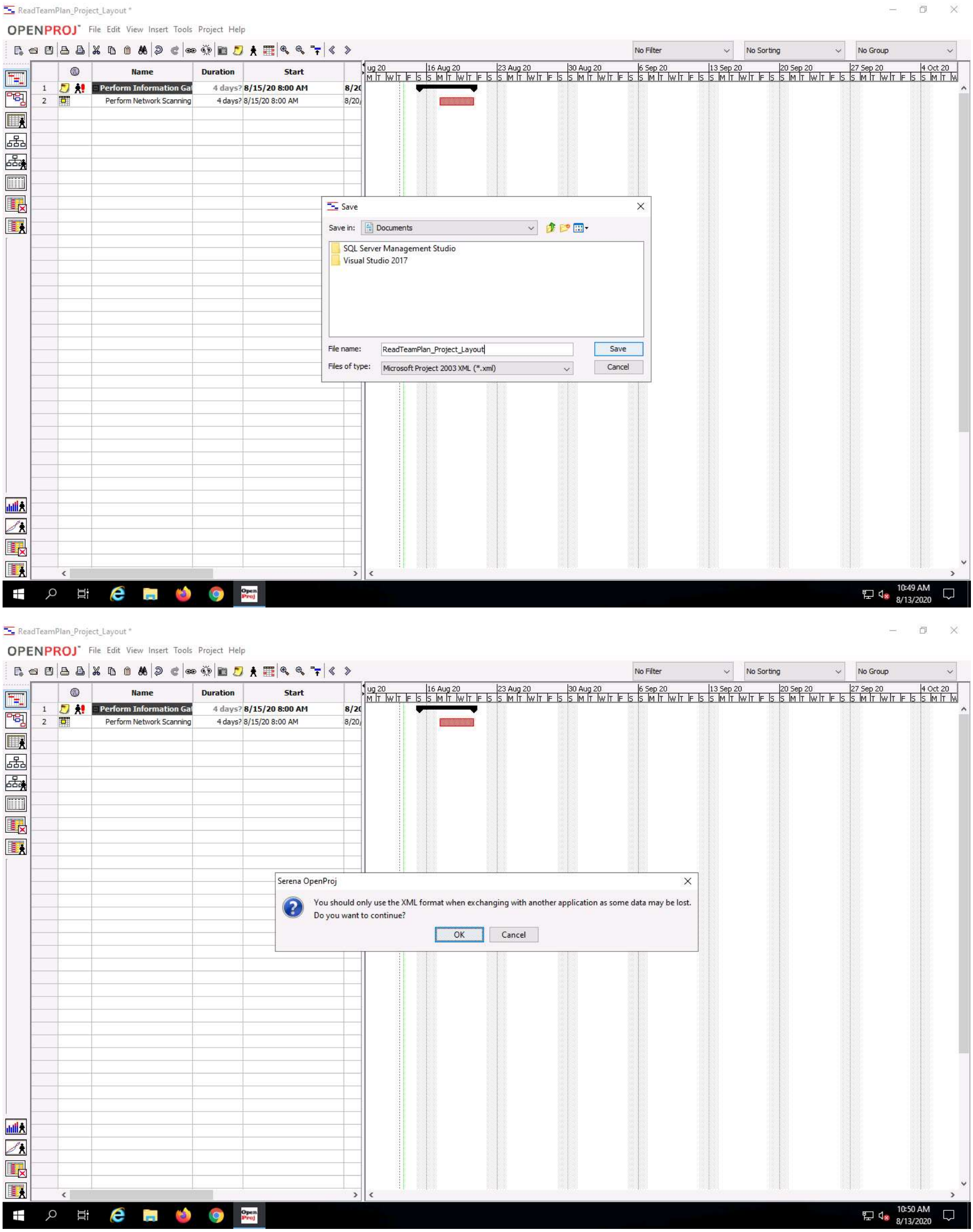


19. Go to the **File** menu and click the **Save As** option to save the report in **.xml format**. Choose the file type as .xml from drop-down list and click **Save**

Note: As this is a free version you cannot save or import the pentest report.

A pop-up appears saying You should only use xml format when exchanging with another application as some data may be lost. Do you want to continue? Click **Ok**





20. Close all the opened windows. After completion of this lab, you will be aware of how to plan and schedule your penetration testing project with OpenProj.with OpenProj.