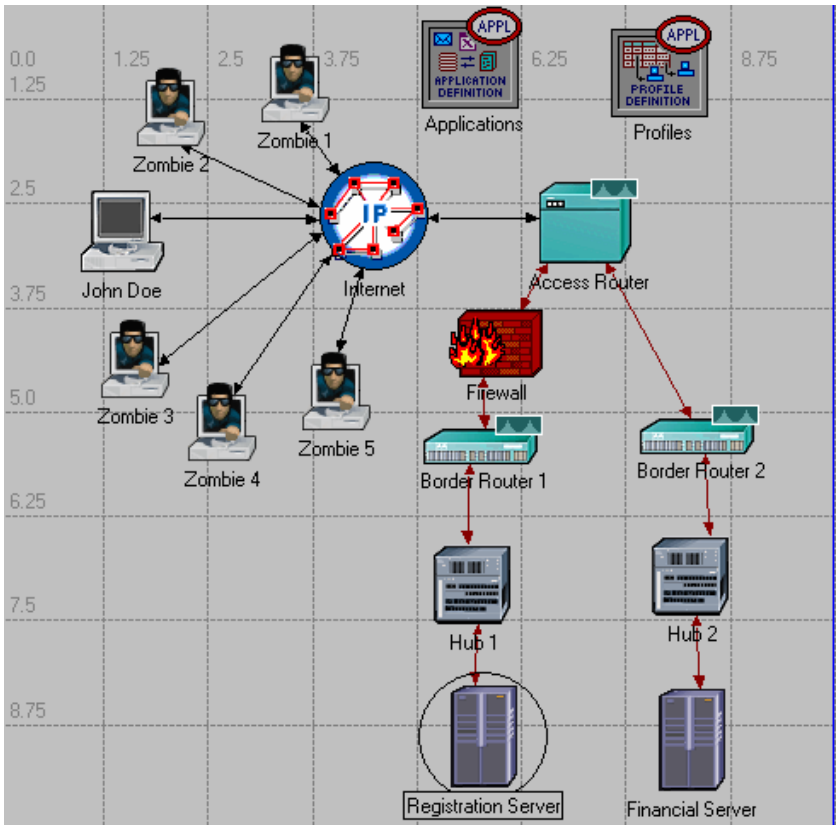
CSE 4482: Security Lab 2

Distributed Web Attack

This lab has been partially based on the material appearing at:
http://polaris.umuc.edu/de/csi/undergrad_opnet1_web/directory.html.



Objective

The goal of this lab is to help the student understand the principle mechanisms behind a distributed denial of service (DDoS) attack, as well as to examine the end effects and possible defences against a DDoS attack.

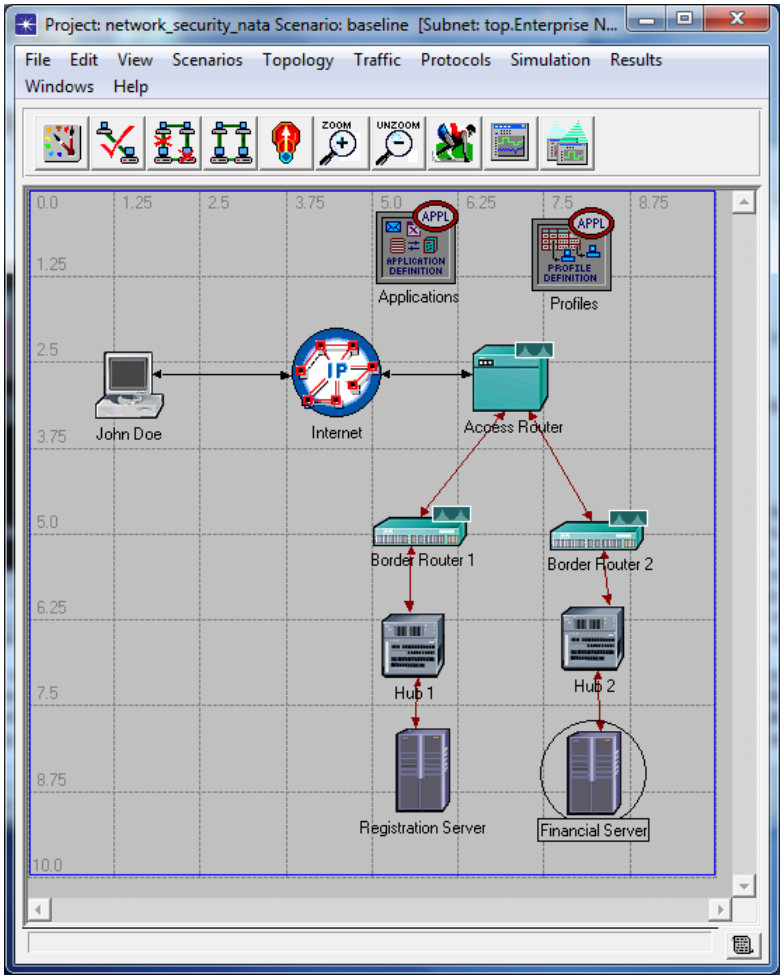
Overview

A virus has infected six machines connected to the Internet. The virus causes the machines to behave as zombie machines, following pre-programmed instructions created by a hacker. In this laboratory, we will see an example of a coordinated denial of service attack performed by such a group of zombies.

The laboratory is composed of three parts: In Part 1, we will build the 'baseline scenario' – basic network infrastructure (without infected zombie machines) that will be used as the main building block for the remaining two exercises – Part 2 and Part 3. In Part 2, the baseline scenario will be expanded to include the infected machines. In Part 3, a firewall will be added to the network, to aid the defense against the infected machines.

Part 1: Build the Baseline Scenario

The goal of the first part of this laboratory is to model an internet commerce company called “Enterprise”, and one user of their service. Enterprise's network consists of: 1) an access router that connects Enterprise to the Internet, and 2) the network infrastructure of two departments of the Enterprise - Registration and Finance (see picture below). Each department has a border router, hub, and a server.



At the top right of the above picture are two square icons labeled “Applications” and “Profiles”. These objects are not network objects - they do not represent real-world devices. Instead, they tell the IT Guru software how to model applications and which applications are active. For example, in this exercise you will use a Web application. In general, a Web application can have many flavors: it can use either HTTP 1.1 protocol or HTTP 1.0 protocol, it can assume the use of Microsoft Internet Explorer browser or Netscape browser. IT Guru must know which particular version of the Web application you wish to model. In order to determine that, IT Guru reads attributes of the “Applications” object, once you have properly set them up. Default settings are available at each step of the modeling process, so one can make as few or as many choices as they wish.

The workstation icon represents a user named “John Doe”, who is connected to the Internet over a dial-up connection. His goal is to access Enterprises’ application/server called “Registration”. We will build a model of this activity in IT Guru, and observe different aspects of network performance. We will analyze the obtained results, determine whether the performance is satisfactory, and take action if needed.

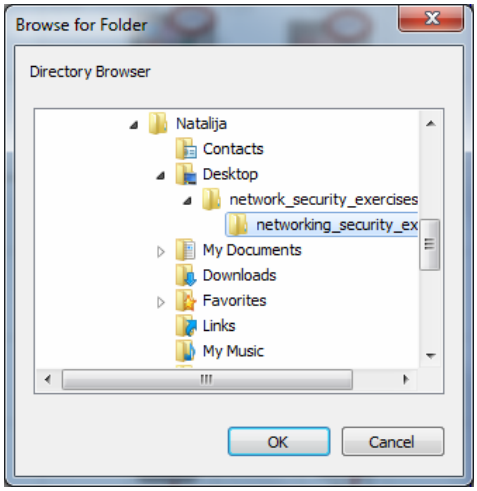
Part 1.1 Network Setup

1. Click here to download lab files: **http://www.cse.yorku.ca/course/4482/network_security_exercises.zip**. Save the file on your desktop.

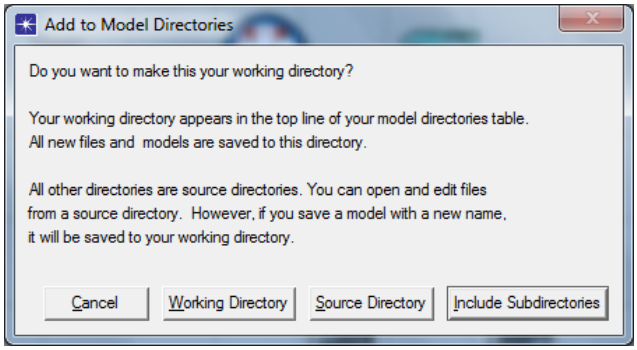
2. Go to your desktop, right click on the **network_security_exercises.zip** and choose **Extract to Folder**.

3. Start IT Guru.

4. From the IT Guru menu, select **File** → **Model Files** → **Add Model Directory**. Navigate to the furthest **network_security_exercises** folder and click **OK**.



5. Click on **Working Directory** to make this the directory where IT Guru stores network security scenarios that you will build.



6. Next, select **File** → **New …** choose **Project** and click **OK**.

7. Set the **Project Name** to **network_security_xx** (where **xx** are your initials). Set the **Scenario Name** to **baseline**. Click **OK**.

8. In the **Initial Topology** window, select **Create Empty Scenario** and click on **Next**.

9. In the **Choose Network Scale** window, select **Enterprise** and click on **Next**.

10. Check **Specify Size** radio button and click on **Next**.

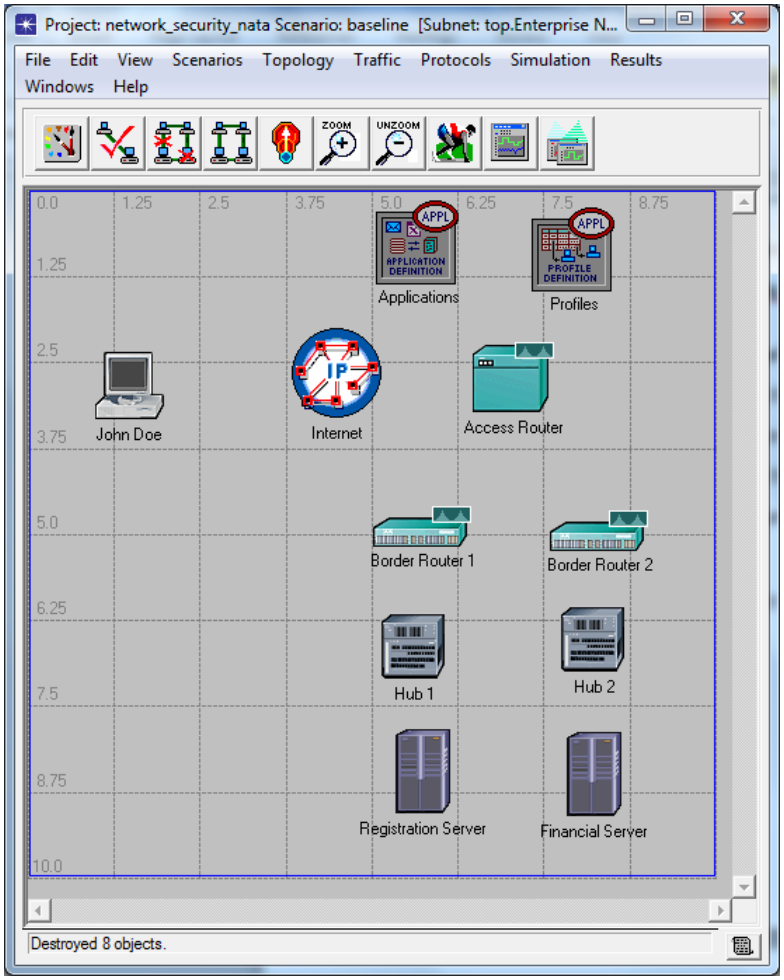
11. Set the size of the enterprise network to 10x10 km and click on **Next**.

12. Select the **network_security_labs** model family and click on **Next**.

13. In the **Review** window, click **OK**.

14. Drag the following objects from the Object Palette  into the Project workspace, and place them as shown on the picture below.

- Application Config
- Profile Config
- John Doe
- Internet
- Access Router
- two “Cisco 4000”-s
- two “ethernet16_switch”-es
- Registration Server
- Financial Server



15. Set the name of the inserted objects/nodes to match the above picture. The name of an object can be set by right-clicking on the object, and selecting the **Set Name** item from the menu.

16. Connect the nodes with links:

a) Click on the **100BaseT** link type in the object palette, then draw a link from the source node to the destination node as follows:

- Registration Server to Hub 1
- Hub 1 to Border Router 1

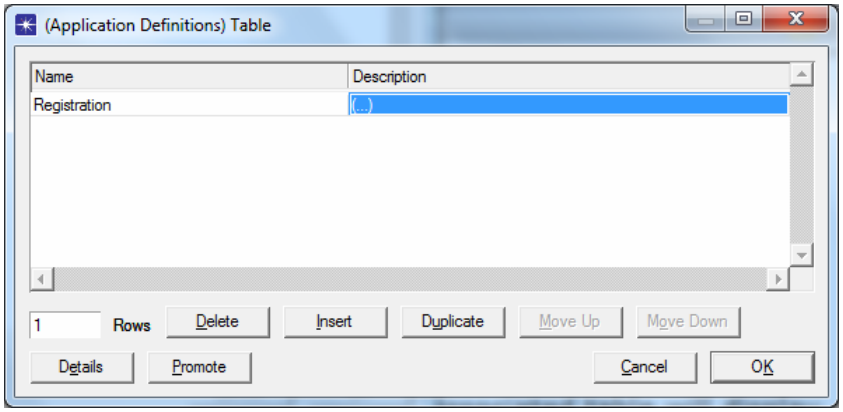
- Border Router 1 to Access Router
- Financial Server to Hub 2
- Hub 2 to Border Router 2
- Border Router 2 to Access Router

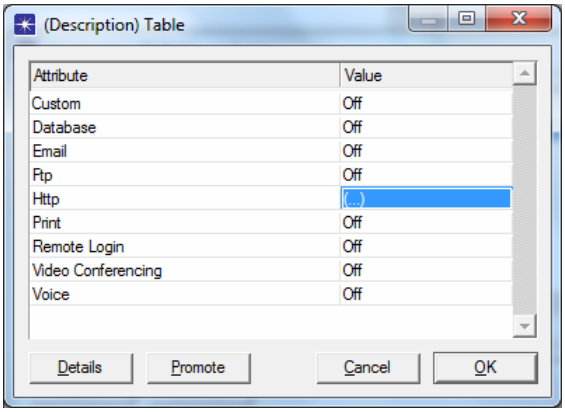
b) Use a **T1** link to connect the following:
- Access Router to Internet

c) Use a **PPP 56K** link to connect the following:
- John Doe to Internet

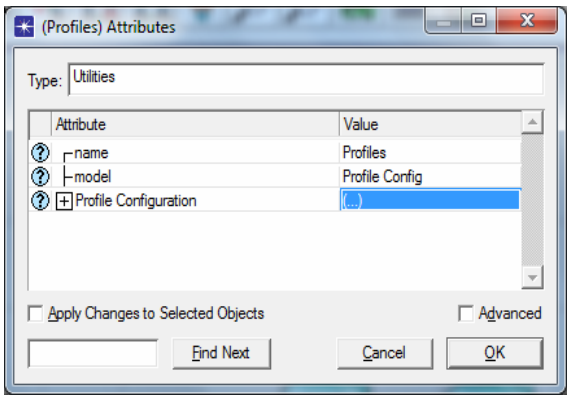
17. Check the consistency of network links by clicking on the respective button  . If some links are inconsistent, delete all links that you created in the previous step, and recreate those links.

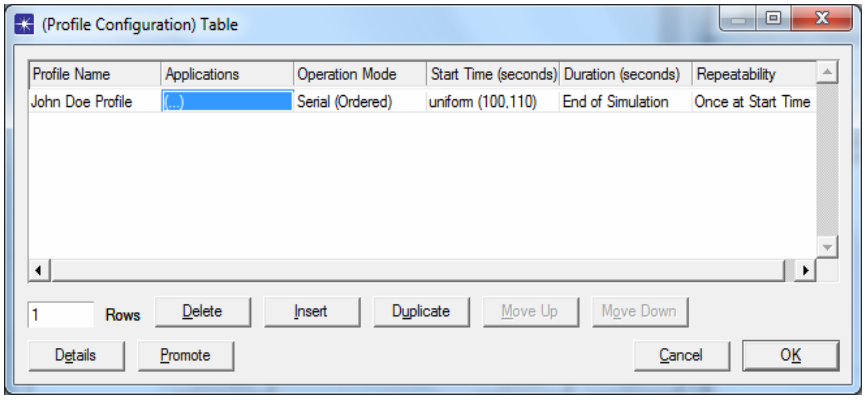
18. Configure the **Registration** application:
a) Right-click on the **Applications** object, and select **Edit Attributes**.
b) Double-click the **Application Definitions** attribute value – Attribute Definitions table will appear.
c) Add a single row to the **Application Definitions** table.
d) In the **Name** field, type **Registration**.
e) Double-click the **Description** field, and set the value of the **HTTP** application to **Image Browsing**.
f) Click OK to close the open dialog boxes. Configuration of the **Registration** application is complete.

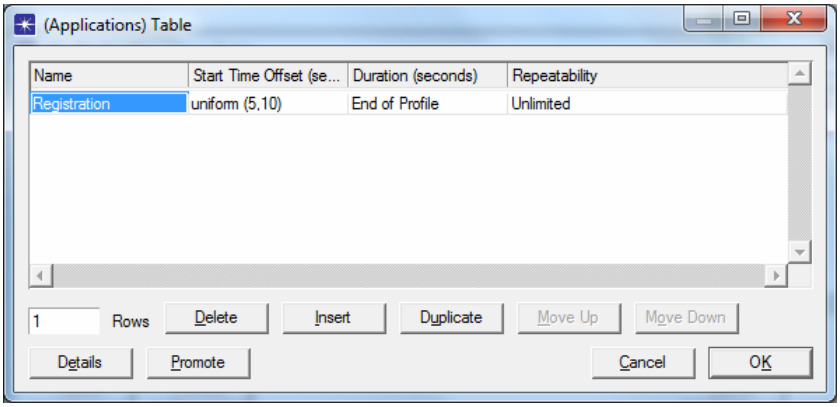




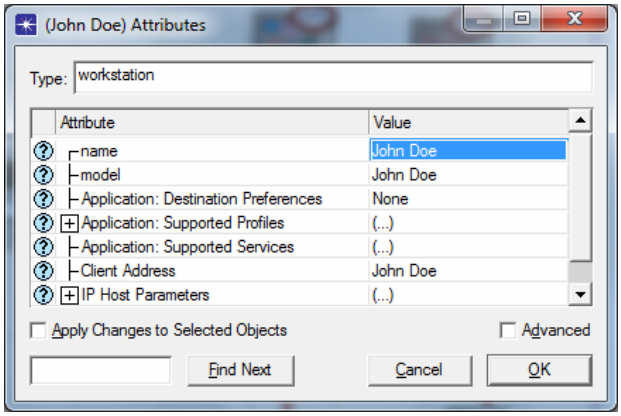
19. Build the **John Doe Profile**:
a) Right-click on the **Profiles** object, and select **Edit Attributes**.
b) Double-click the value of the **Profile Configuration** attribute (currently set to **None**).
c) Add a row to the **Profile Configuration** table by setting the number of rows to 1.
d) Name the profile **John Doe Profile**.
e) Double-click the **Applications** value (currently set to **None**).
f) Add an application to the **Applications** table by setting the number of rows to 1.
g) Click in the **Name** column in the Applications Table and select **Registration** from the list. (This is the Application that you defined in step 12.)
h) Click OK to close all open dialog boxes. Configuration of the John Doe profile is complete.

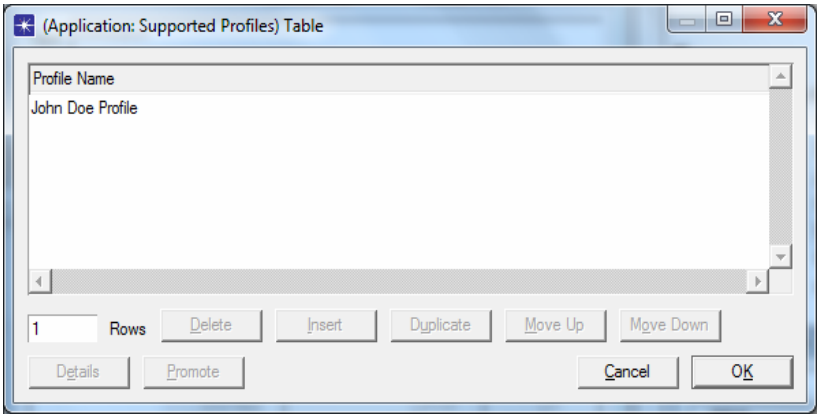




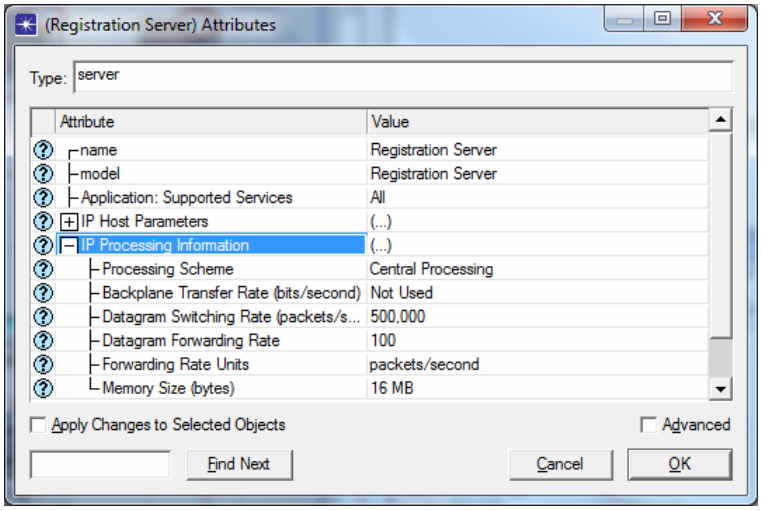


20. Configure traffic on workstation **John Doe**:
    a) Right-click on the workstation named **John Doe**, and select **Edit Attributes**.
    b) Double-click on the **Application: Supported Profiles** attribute value (currently set to **None**).
    c) Add a row to the **Application: Supported Profiles** table.
    d) Click in the blank space under the **Profile Name** column header and choose **John Doe Profile** from the list.
    e) Click OK to close all open dialog boxes. Configuration of traffic on workstation **John Doe** is complete.





21. Configure the IP Datagram Forwarding rate on the Registration server. Set the value of this attribute to **100**. Note that the normal value of this attribute is 100,000 packets/second. We are purposely slowing down the Registration Server so that we can easily observe when the server gets overloaded.

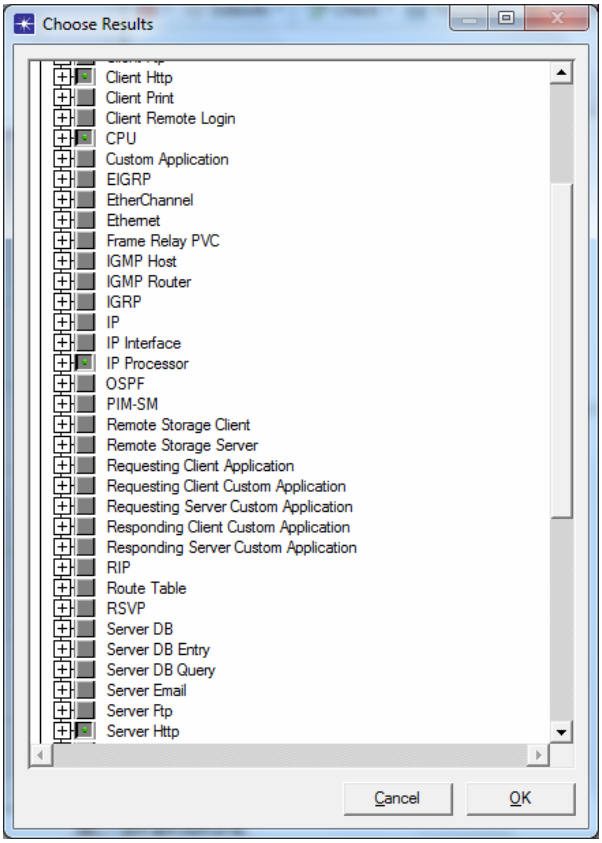


Configuration of the network is complete. You are now ready to run the simulation and study its performance.

Part 1.2 Simulation Setup

1. Right click on an empty section of the IT Guru workspace, and select **Choose Individual Statistics** from the menu.

2. In the Choose Results dialog box, expand the **Node Statistics** tab and select:
   a) **Client Http** group of statistics.
   b) **CPU** group of statistics
   c) **IP Processor** group of statistics.
   d) **Server Http** group of statistics.



3. Click OK after you have selected the statistics to be collected during the simulation.

Part 1.3 Simulation Execution

1. Click the **Run Simulation** icon on the IT Guru toolbar  .

2. Click the **Run** button on the Configure Simulation dialog box.

3. Wait for notification that the simulation is complete.

4. Click **Close** to close the dialog box after the simulation has finished.

Part 1.4 View Results

1. Right click on the workstation **John Doe** and select **View Results**.
   a) Expand **Client Http** in the View Results dialog box.
   b) Select the **Page Response Time (seconds)** and **Object Response Time (seconds)**.
   c) Set the chart display mode to **Overlaid Statistics**.
   d) Click the **Show** button in the View Results dialog box.

QUESTION 1
Your task is to take a screenshot of the graph obtained by performing Step 1.4.1, and include it in the final report. You are also required to comment on the obtained results, i.e. explain the difference between the values in the two plots?

2. Right click on the **Registration server** and choose **View Results**.
   a) Click on the **IP Processor**.
   b) Click on the **IP Processor Forwarding Memory Queue Size (packets)**, and click on **IP Processor Forwarding Memory Queuing Delay**.
   c) Set the chart display mode to **Stacked Statistics**.
   d) Click the **Show** button in the **View Results** dialog box.

QUESTION 2
Take a screenshot of the graph obtained by performing Step 1.4.2, and include it in the final report. You are also required to comment on the obtained results, i.e. explain whether there is any (co)relation between the two plots?

3. e) Unclick **Forwarding Memory Queue Size** and **Queuing Delay**.
   f) Click on **CPU** and then on **CPU Utilization**.
   h) Click the **Show** button in the **View Results** dialog box.

QUESTION 3
Take a screenshot of the graph obtained by performing Step 1.4.3, and include it in the final report.

Congratulations! You have built the baseline network. You are now ready to start building the second exercise, involving 6 infected zombie machines.

Part 2: Build the Distributed Web Attack Scenario

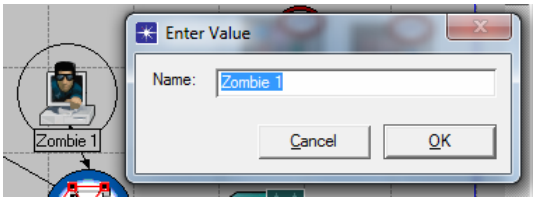
Part 2.1 Network Setup

1. Choose **Scenarios** => **Duplicate Scenario**, name the new scenario **web_attack**, and click OK.

2. Open the IT Guru palette  . Select **Zombie** icon from the palette and place it in the scenario.

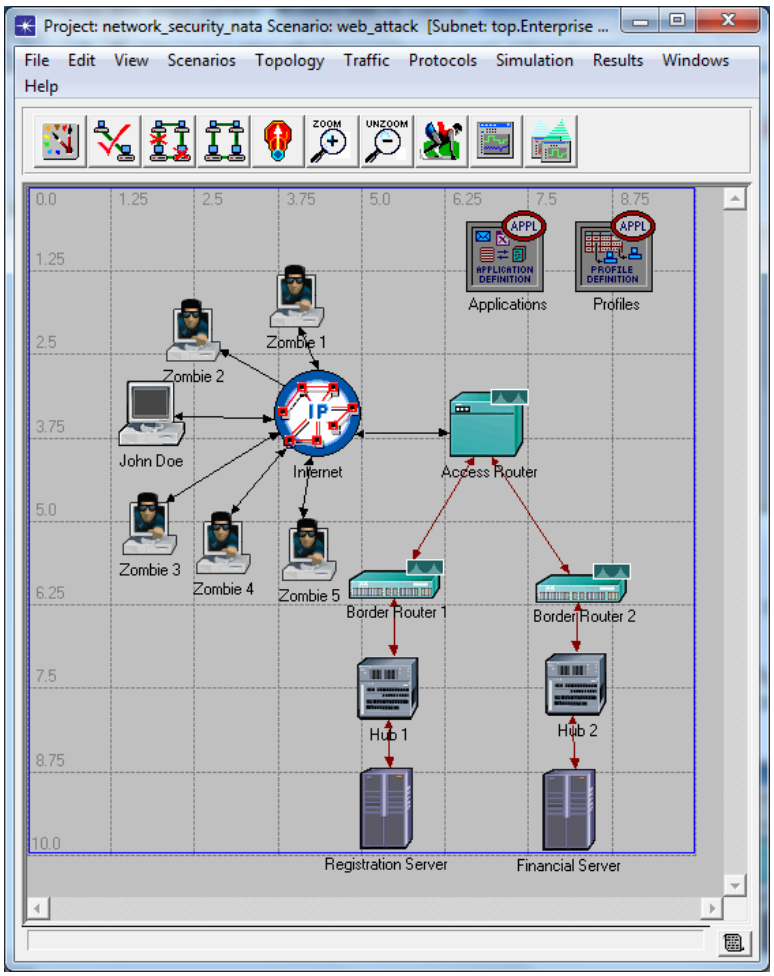
3. Right-click on the newly placed zombie node in the IT Guru project workspace.

4. Select the "Set Name" menu option. Type in the new name (**Zombie 1**) and click OK.



5. Select the **Zombie 1** node. Copy the node into the clipboard by pressing **CTRL-c** on the keyboard. Paste 5 copies of the node into the IT Guru project workspace by pressing **CTRL-v**.

6. Use **PPP_56K** links to connect the zombies to the Internet. After all the zombie machines are connected to the Internet, the network should look as follows:

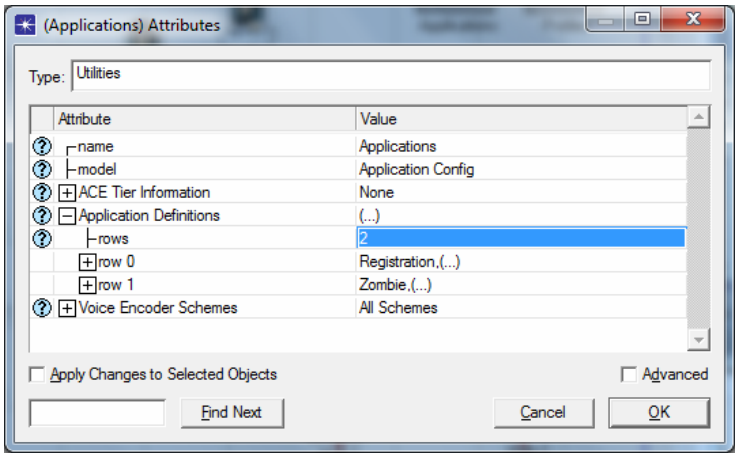


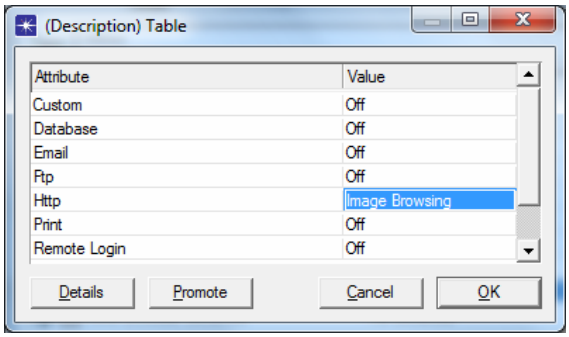
7. Check the consistency of network links by clicking on the respective button  . If some links are inconsistent, delete all links that you created in the previous step, and recreate those links.

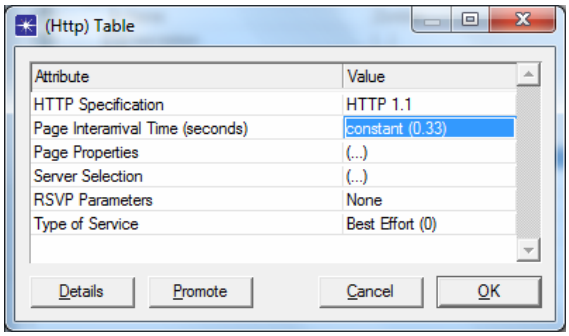
8. Set up a **Zombie Application**:

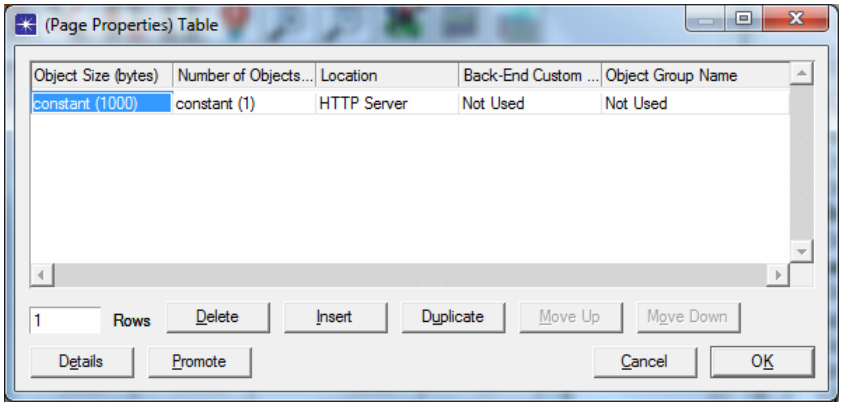
a) Right-click on the **Applications** object, and select **Edit Attributes**.
b) Double-click on the **Application Definitions** attribute value.
c) Set number of rows in the **Application Definitions** table to **2**.
d) Enter the name of the new application (**row 1** -> **Name**) as **Zombie**.
e) Double-click the description of the new application. Set value of the **HTTP** attribute to **Image Browsing** in the **Description** table.
f) Double-click on the **Image Browsing** value. Set the **Page Interarrival Time** to **constant(0.314) seconds**. (This implies that each zombie machine, while active, generates/sends 1 web-request to Registration server every 0.314 seconds.)
g) Double-click on the **Page Properties**. Set the number of rows to **1**. (You will see **2** rows in this table when it first pops up.)
h) Set the **Object Size** to a **constant value** of **1000 bytes**, and the **Number of Objects** to **1**, as shown in the picture.
i) Click OK buttons until all the **Application Definition** dialog boxes are closed.

Definition of the "zombie" application is complete. Now IT Guru will know exactly how frequently a zombie application will download a Web page, and the exact number of bytes in the Web page.





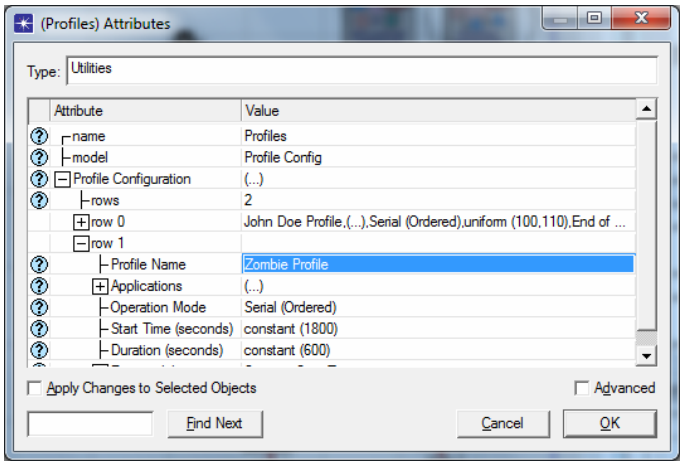


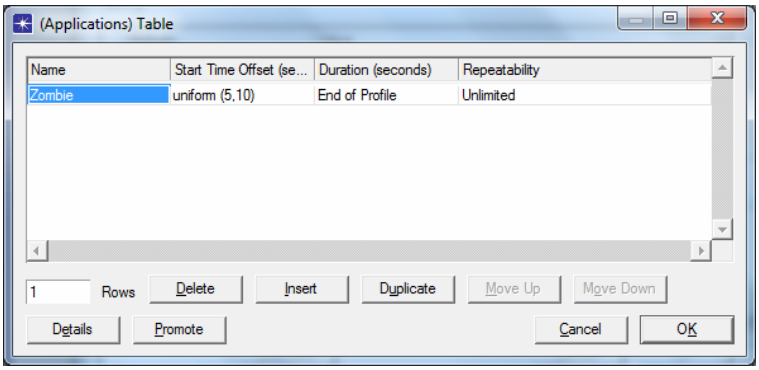


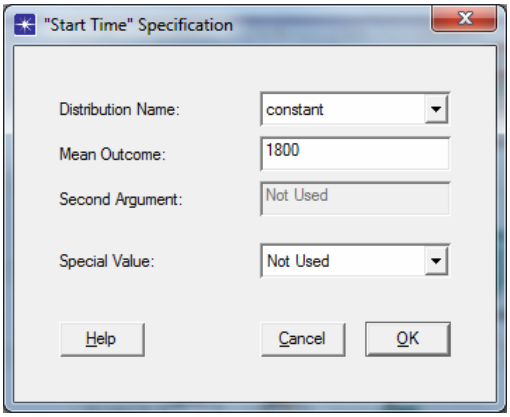
9. Build a **Zombie Profile** that activates the **Zombie Application** at **1800 seconds** for a duration **of 600 seconds**:

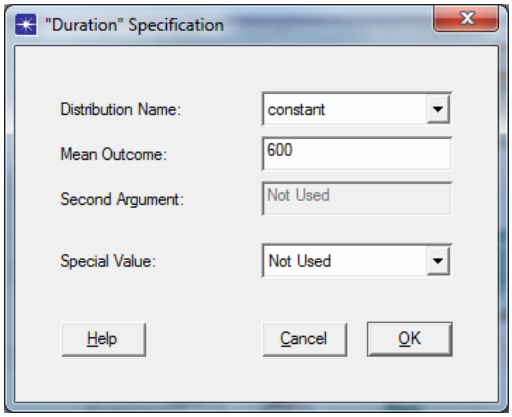
a) Right-click on the **Profiles** object, and select **Edit Attributes**.
b) Double-click on the value of the **Profile Configuration** attribute (currently set to **1**).

c) Add a row to the **Profile Configuration** table by setting the number of rows to **2**.
d) Name the profile **Zombie Profile**.
e) Double-click on the **Applications** value (currently set to **None**).
f) Add an application to the **Applications** table by setting the number of rows to **1**.
g) Click on the **Name** column in the **Applications** table and select the **Zombie** application (this is the Application that was defined in step 8).
h) Click OK to close the **Applications** table dialog box.
i) Set the **Zombie Profile** to start at **1800 seconds**. Double-click on the **Start Time (seconds)** column on the **Profile Configuration** table. Set the start time **Distribution Name** to **constant**, **Mean Outcome** to **1800** as shown in the picture, then click OK to close the dialog box.
j) Set the **Zombie Profile Duration** to **600 seconds**. Double-click on the **Duration** field on the **Profile Configuration** table. First set the **Special Value** to **Not Used**, **Distribution Name** to **constant**, and the **Mean Outcome** to **600** as shown below.
k) Click OK buttons until all the **Profile** dialog boxes are closed.

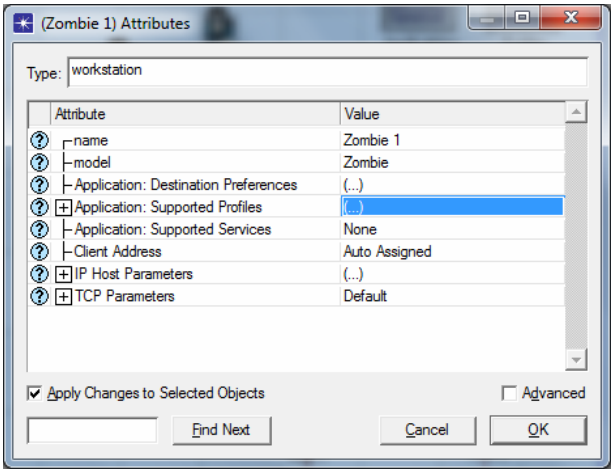


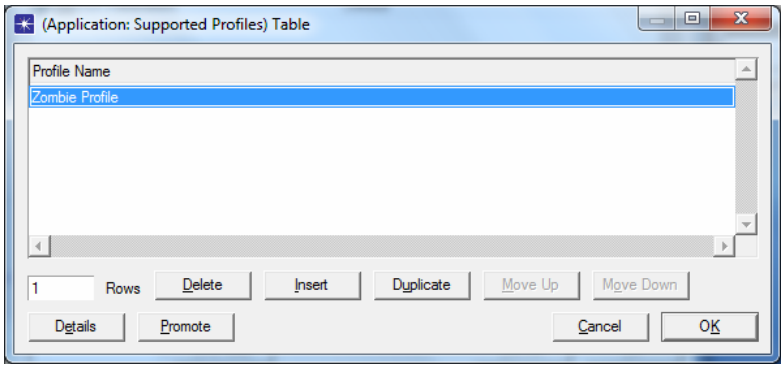




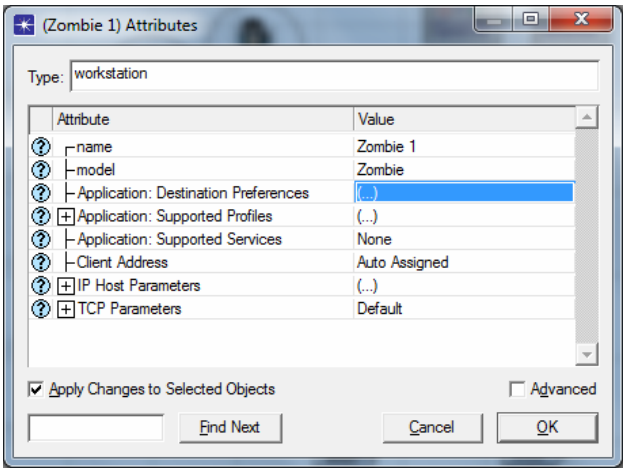


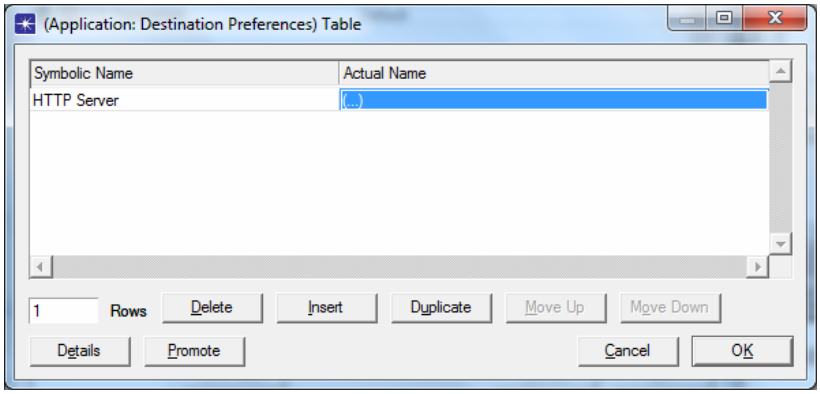
10. Activate the **Zombie Profile** on all zombie nodes:
a) Right-click on a **Zombie** node, and select the **Select Similar Nodes** menu item. A circle will be drawn around each zombie machine.
b) Right-click on one of the zombie nodes and select **Edit Attributes**. Check **Apply Changes to Selected Objects**.
c) Double-click on the **Application: Supported Profiles** attribute value (currently **None**). Set the number of rows on the **Supported Profiles** table to **1**.
d) Click in the blank space under the **Profile Name** column header and choose **Zombie Profile** from the list.
e) Click OK to close the dialog box.

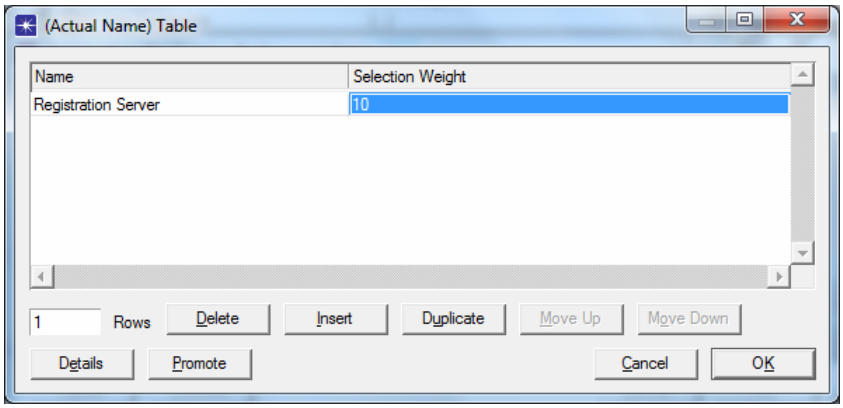




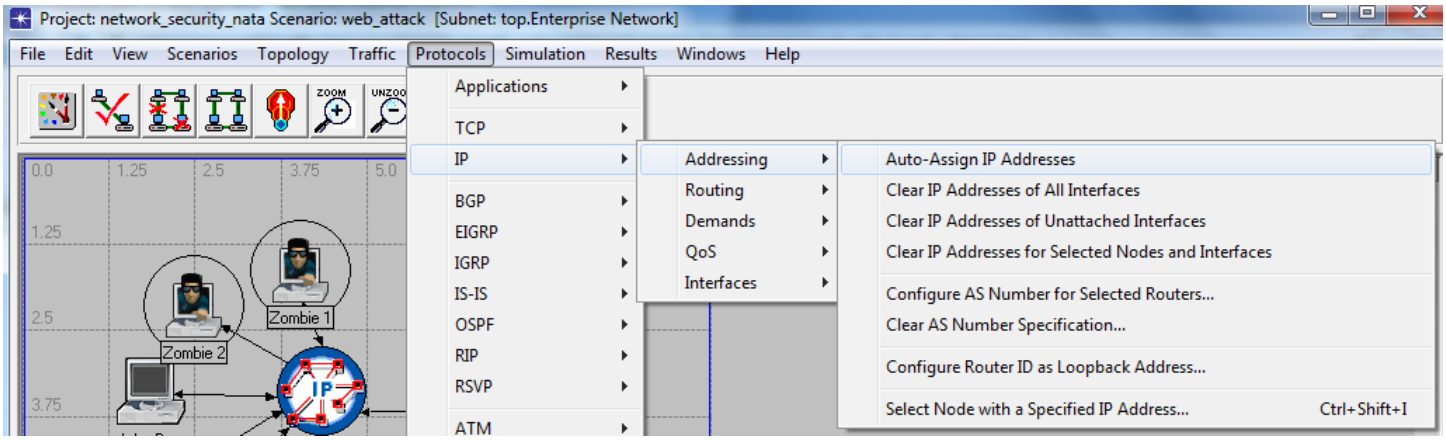
11. Set the **HTTP destination preference** of all zombie machines to the Registration server:
    a) Select all the **Zombie** nodes. Select **Edit Attributes** and make sure that Apply to all Selected Objects is checked. Double click the **Application: Destination Preferences** attribute value (currently set to **None**).
    b) You should see an empty **Application: Destination Preference** table. Add a row to the table and set the **Symbolic Server** name to **HTTP Server**.
    c) Double-click on the **Actual Name** field. Add a row to the **Actual Name** table. Set the **Name** field to **Registration Server**. See the picture for the result.
    d) Click OK to close the dialog box.







12. Assign IP addresses using **Protocols -> IP -> Addressing -> Auto Assign IP Addresses** menu selections.



You have completed building the network model for the distributed Web attack.

Part 2.2 Simulation Execution

1. Click the **Run Simulation** icon on the IT Guru toolbar  .

2. Click the **Run** button on the Configure Simulation dialog box.

3. Wait for notification that the simulation is complete.

4. Click **Close** to close the dialog box after the simulation has finished.

Part 2.3 View Results

1. Right click on the workstation **John Doe** and select **View Results**.
   a) Expand **Client Http** in the View Results dialog box.
   b) Select the **Page Response Time (seconds)** and **Object Response Time (seconds)**.
   c) Set the chart display mode to **Overlaid Statistics**.
   d) Click the **Show** button in the View Results dialog box.

QUESTION 4

Your task is to take a screenshot of the graph obtained by performing Step 2.3.1, and include it in the final report. You are also required to comment on the obtained results, i.e. explain the difference between the values in the two plots? In addition, explain why and how these plots differ from those obtained in Question 1? Be as detailed as possible.

2. Right click on the **Registration server** and choose **View Results**.
   a) Click on the **IP Processor**.
   b) Click on the **IP Processor Forwarding Memory Queue Size (packets)**, and click on **IP Processor Forwarding Memory Queuing Delay**.
   c) Set the chart display mode to **Stacked Statistics**.
   d) Click the **Show** button in the **View Results** dialog box.

QUESTION 5
Take a screenshot of the graph obtained by performing Step 2.3.2, and include it in the final report. You are also required to comment on the obtained results, i.e. explain whether there is any (co)relation between the two plots? In addition, explain why and how these plots differ from those obtained in Question 2?

3. e) Unclick **Forwarding Memory Queue Size** and **Queuing Delay**.
   f) Click on **CPU** and then on **CPU Utilization**.
   h) Click the **Show** button in the **View Results** dialog box.

QUESTION 6
Take a screenshot of the graph obtained by performing Step 2.3.3, and include it in the final report. In addition, explain why and how the given plot differs from the one obtained in Question 3?

QUESTION 7
In step 2.1.8.f), we have set the zombies' inter-arrival request time to constant(0.314) seconds. Change this value to constant(0.317) seconds, take the screenshot of respective **Registration server's CPU Utilization**, and include the resultant graph in the final report. Explain why and how this graph differs from the one obtained in Question 6 and 3?

QUESTION 8
Now, reduce the zombies' inter-arrival request time to constant(0.329) seconds. Take the screenshot of respective **Registration server's CPU Utilization**, and include the resultant graph in the final report?
It should be obvious from the obtained graph that with the inter-arrival request time of constant(0.329) seconds, the zombies' do NOT manage to successfully stall **Registration server**. Hence, in this case, the only way of executing a successful attack is by increasing the number of zombies. How many more zombies should be deployed in the system in order to successfully stall **Registration server**?

Note: In order to add new elements (i.e. more zombies) to a network, IP addresses need to be properly reconfigured. The details of IP address reconfiguration are explained in step 3.7.1.

Part 3: Build the Distributed Web Attack Scenario with Firewall

In the previous exercise, you saw how a "zombie herd" or team of zombie machines could coordinate attacks and cause the Registration server to stop functioning.

Users of the Registration application would call the Registration department of our Enterprise to complain about the interruption in service. The network administrator of the department could use network monitoring tools to discover the IP addresses of the attacking zombie machines. Using this information, the network administrator could configure a firewall to stop traffic originating from these machines.

In the third part of the lab, you will see how to configure a firewall node using IT Guru Academic Edition to stop traffic from the zombie machines.

Part 3.1 Network Setup

1. Open the **network_security_<your_initials>** project, and switch to the **web_attack** scenario.

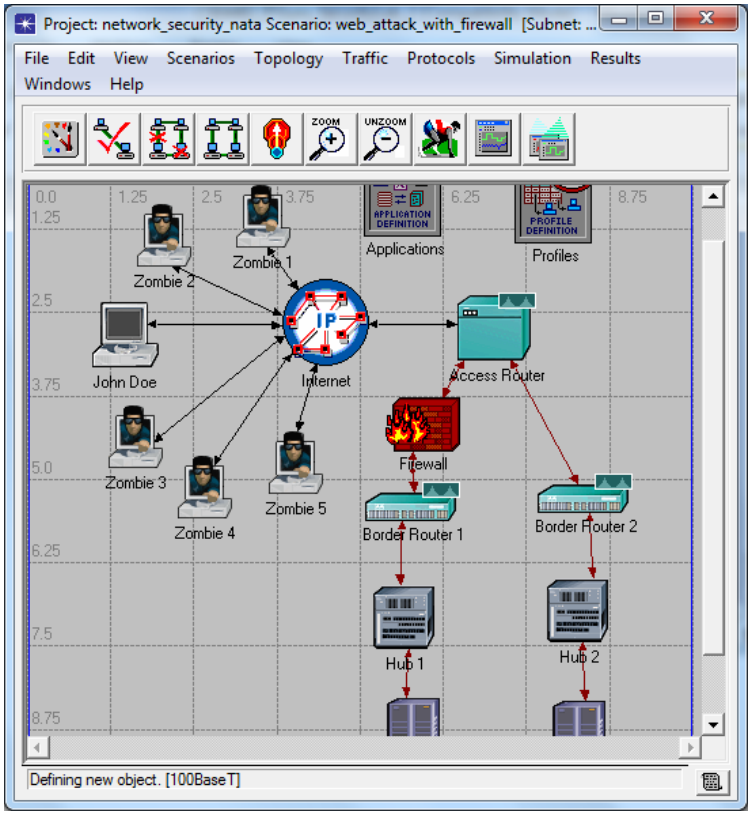
2. Choose **Scenarios** => **Duplicate Scenario**, name the new scenario **web_attack_with_firewall**, and click OK.

3. Click on the link between **Border Router 1** and **Access Router**. Delete this link using the **Delete** button on the keyboard.

4. Open the **IT Guru object palette** and place a **Firewall** node in the scenario, as shown below. Set the name of this node to **Firewall**.

5. Use **100BaseT** links from the object palette to connect the following:
   a) **Border Router 1** to the **Firewall**.
   b) **Firewall** to the **Access Router**.

6. Verify link consistency by clicking on **Verify Links** button.



7. Now that the network has been modified, we need to reconfigure IP addresses to match the modification:

a) Select **Border Router 1**, **Firewall**, and **Access Router** nodes by control-clicking on each of them. IT Guru will draw circles around them indicating that they are selected.

b) Select **Protocol -> IP -> Addressing -> Clear IP Addresses for Selected Nodes and Interfaces**. This will clear IP addresses so that you can reassign them.

c) Next, tell IT Guru to reassign IP addresses by selecting **Protocol -> IP -> Addressing -> Auto Assign IP Addresses.**

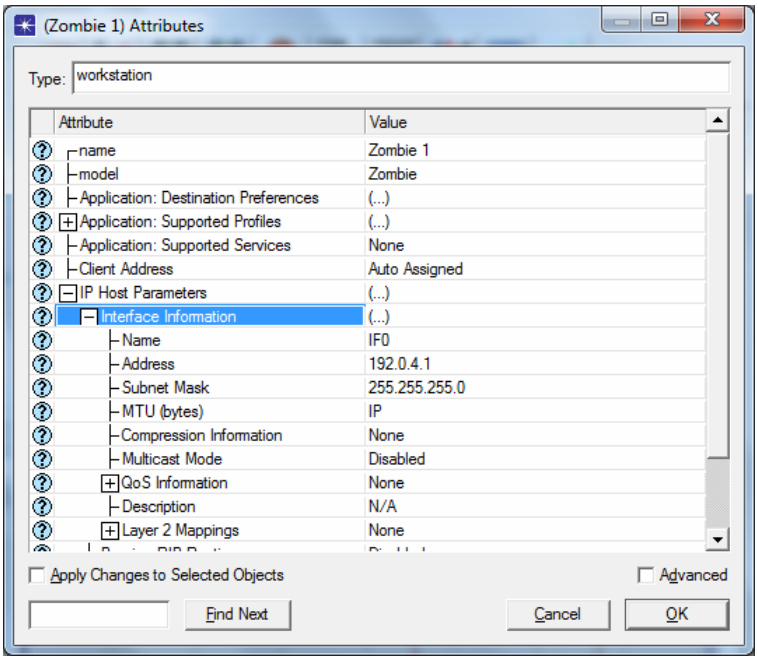
8. Read the IP addresses of the zombie machines and note them down on a piece of paper, or in a text editor on your computer:

a) Right-click on a zombie machine and select **Edit Attributes**. Open the **IP Host Parameters** tab, and then the **Interface Information** tab.

b) You should now be able to see/read the IP address, as shown below.

c) Click **Cancel** on the dialog box after you note the IP address.

d) Repeat the process for each of the 5 zombies. At the end, you should have 5 IP addresses.



9. Configure the firewall to block these IP addresses:

a) Right-click on the **Firewall** node and select **Edit Attributes**. Expand **IP Routing Parameters**. Double-click **on Extended ACL Parameters**.

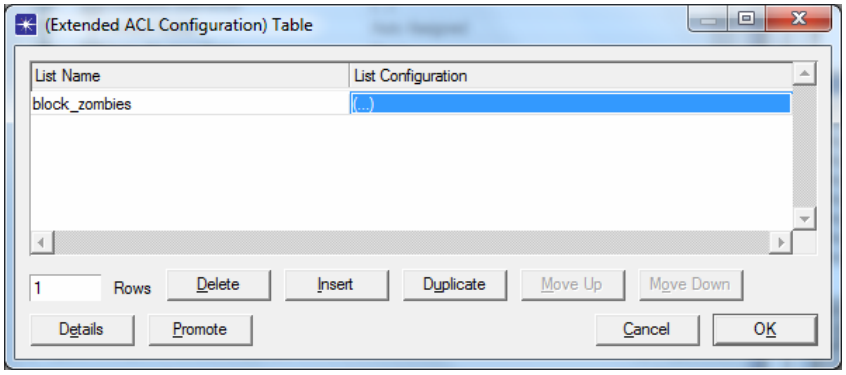
b) Add a row to the **Extended ACL Configuration** table and set the **List Name** to **block_zombies**.

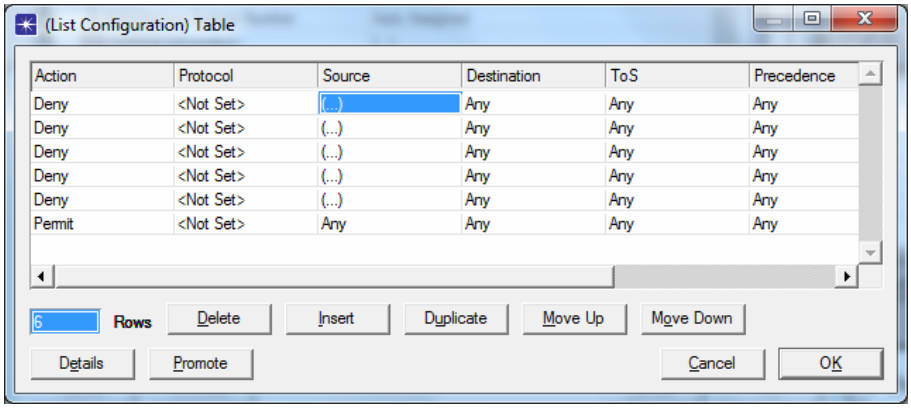
c) Double-click on the **List Configuration** value. Add 6 rows to the table.

d) Double-click on the **Source** filed of the first row, and enter the first zombie IP address. Set the **Wildcard** field to **host** as shown below.

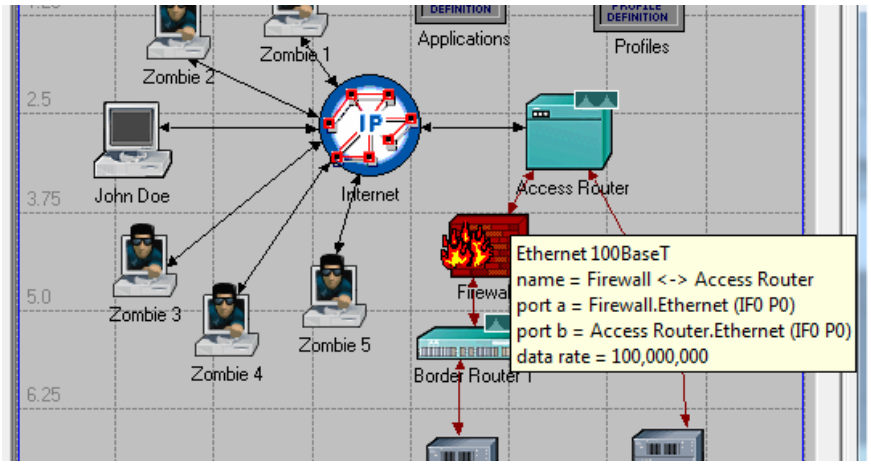
e) Enter the IP addresses of remaining 4 zombie machines into the **Source** filed of the next 4 rows.

f) Set **Action** on the last row to **Permit**. (Note that the last entry in the ACL must be set to "Permit". This is because the firewall will attempt to match packets to entries in the ACL, and will drop packets that do not match any of the entries. So the last entry must be set to match all packets aside from those being received from the zombie nodes.)

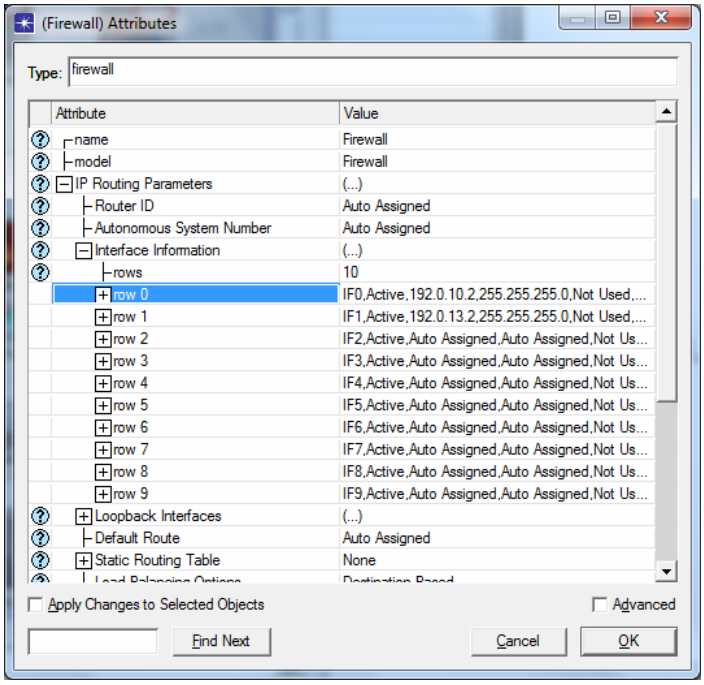


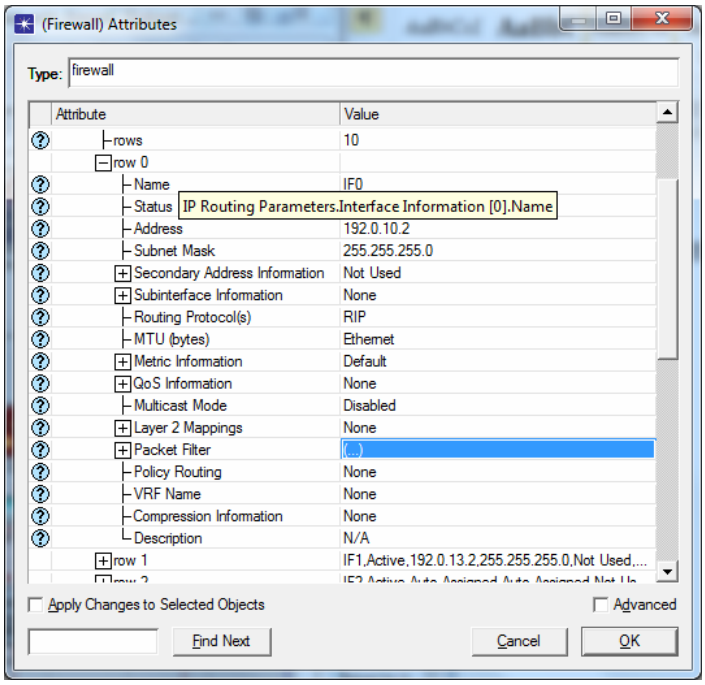


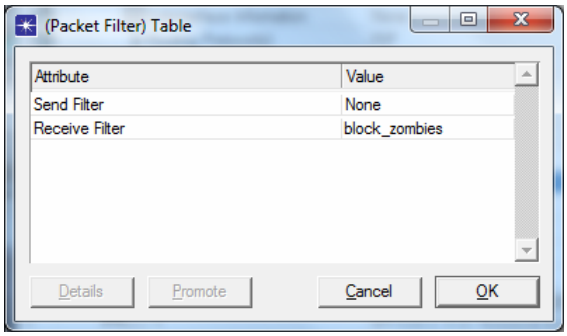
10. Activate the ACL on the firewall interface that connects to the access router:
    a) Move your mouse cursor to the link/interface that connects the **Firewall** to the **Access Router**. Hold the cursor stationary for a couple of seconds until the tooltip is displayed. The tooltip will show the port number that connects the **Firewall** to the **Access Router**. Here the tooltip shows that Firewall interface IF0 connects to the Access Router.



    b) Right-click on the **Firewall** and select **Edit Attributes**. Expand **IP Routing Parameters** tab and **Interface Information**.
    c) Open the row for the **Firewall interface** connecting to the **Access Router**. Here it is **IF0**, so we will open **row 0**.
    d) Double-click on the **Packet Filter** attribute value. Set **Receive Filter** to **block_zombies**.
    e) Click OK to close all of the dialog boxes.







Now, run the simulation as in the previous exercises.

Part 3.2 View Results

1. Right click on the workstation **John Doe** and select **View Results**.
   a) Expand **Client Http** in the View Results dialog box.
   b) Select the **Page Response Time (seconds)** and **Object Response Time (seconds)**.
   c) Set the chart display mode to **Overlaid Statistics**.
   d) Click the **Show** button in the View Results dialog box.

QUESTION 9
Take a screenshot of the graph obtained by performing Step 3.2.1, and include it in the final report. Comment on the obtained results, i.e. explain why and how these plots differ from those obtained in Question 1 and 4?

2. Right click on the **Registration server** and choose **View Results**.
   a) Click on the **IP Processor**, and then on **IP Processor Forwarding Memory Queue Size (packets)** and **IP Processor Forwarding Memory Queuing Delay**.
   c) Set the chart display mode to **Stacked Statistics**.
   d) Click the **Show** button in the **View Results** dialog box.

QUESTION 10
Take a screenshot of the graph obtained by performing Step 3.2.2, and include it in the final report. Comment on the obtained results, i.e. explain why and how these plots differ from those obtained in Question 2 and 5?

3. e) Unclick **Forwarding Memory Queue Size** and **Queuing Delay**.
   f) Click on **CPU** and then on **CPU Utilization**.
   h) Click the **Show** button in the **View Results** dialog box.

QUESTION 11
Take a screenshot of the graph obtained by performing Step 3.2.3, and include it in the final report. In addition, explain why and how the given plot differs from the one obtained in Question 3 and 6?

4. Right click on the **Access Router** and select **View Results**.
   a) Click on **CPU** and then on **CPU Utilization**.
   b) Click the **Show** button in the **View Results** dialog box.

QUESTION 12
Take a screenshot of the graph obtained by performing Step 3.2.4, and include it in the final report. In addition, explain why and how **Access Router's CPU Utilization** differs from **Registration Server's utilization** obtained in Questions 11?