CompTIA Network+® Lab Series
Network Concepts

Lab 6: Network Management

Objective 4.2: Identify types of configuration management documentation: Baselines
Objective 4.4: Conduct network monitoring to identify performance and connectivity issues
Objective 6.6: Identify common security threats and mitigation techniques: Patches and Updates

Document Version: 2015-09-18

Development was funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48; The National Information Security, Geospatial Technologies Consortium (NISGTC) is an entity of Collin College of Texas, Bellevue College of Washington, Bunker Hill Community College of Massachusetts, Del Mar College of Texas, Moraine Valley Community College of Illinois, Rio Salado College of Arizona, and Salt Lake Community College of Utah.

This workforce solution was funded by a grant awarded by the U.S. Department of Labor's Employment and Training Administration. The solution was created by the grantee and does not necessarily reflect the official position of the U.S. Department of Labor. The Department of Labor makes no guarantees, warranties or assurances of any kind, express or implied, with respect to such information, including any information on linked sites, and including, but not limited to accuracy of the information or its completeness, timeliness, usefulness, adequacy, continued availability or ownership.

Contents

Contents 2
Introduction 3
Objective: Understand and Perform Network Management Tasks 3
Lab Topology 5
Lab Settings 6
1 Analyze CPU and Network Utilization with Performance Monitor 8
1.1 Monitoring CPU Utilization 9
1.2 Monitoring Network Utilization by Adding a Counter 11
1.3 Using the Resource Monitor 16
1.4 Conclusion 18
1.5 Review Questions 18
2 Use the Event Viewer to View Logs 19
2.1 Open Event Viewer and Trigger a Failed Audit Event 19
2.2 Viewing Windows Logs 23
2.3 Conclusion 25
2.4 Review Questions 25
3 Manage Patches and Updates 26
3.1 Navigating to the Windows Update Utility 26
3.2 Changing Windows Update Settings 28
3.3 Selectively Installing Windows Updates 30
3.4 Conclusion 31
3.5 Review Questions 31

Introduction

This lab is part of a series of lab exercises designed to supplement coursework and provide students with a hands-on training experience based on real world applications. This series of lab exercises is intended to support courseware for CompTIA Network+® certification.

This lab explores concepts in Network Management including **baselines**, performance monitoring, logs and implementation of patches and upgrades as a mitigation technique to security threats. By the end of this lab, students will be able to use the **Performance Monitor** to analyze network and CPU utilization, the **Event Viewer** to view various logs, and **Windows Update** to manage operating system patches and updates.

This lab includes the following tasks:

1. Analyze CPU and Network Utilization with Performance Monitor
2. Use the Event Viewer to View Logs
3. Manage Patches and Updates

Objective: Understand and Perform Network Management Tasks

Network Management is an important responsibility of the CompTIA Network+® technician that is very broad in scope. Network Management is a major Domain (4.0) of the CompTIA Network+® examination, and represents 20% of the exam. Network Management topics include, but are not limited to the OSI model, network documentation, establishing baselines, monitoring, optimization, and troubleshooting. This lab will explore Network Management concepts and by the end of the lab, students should be able to understand and perform common network management tasks.

Key terms for this lab;

Baseline – a documented reference of resource utilization from which we can compare

Counter – an object in the Performance Monitor that represents a system resource, such as CPU, Memory or Network and can be added to the graph area to view resource utilization

Critical Updates – this type of update patches known vulnerabilities to the operating system and should be implemented immediately to mitigate security threats

Event Viewer – allows users to view event logs in Windows operating systems, which include application, system and security logs, among others

Idle/Idling – the state of the computer (CPU) when not in use by a program or user. System resource utilization should be little to none. Documenting what resource utilization looks like when idling can be important when establishing baselines.

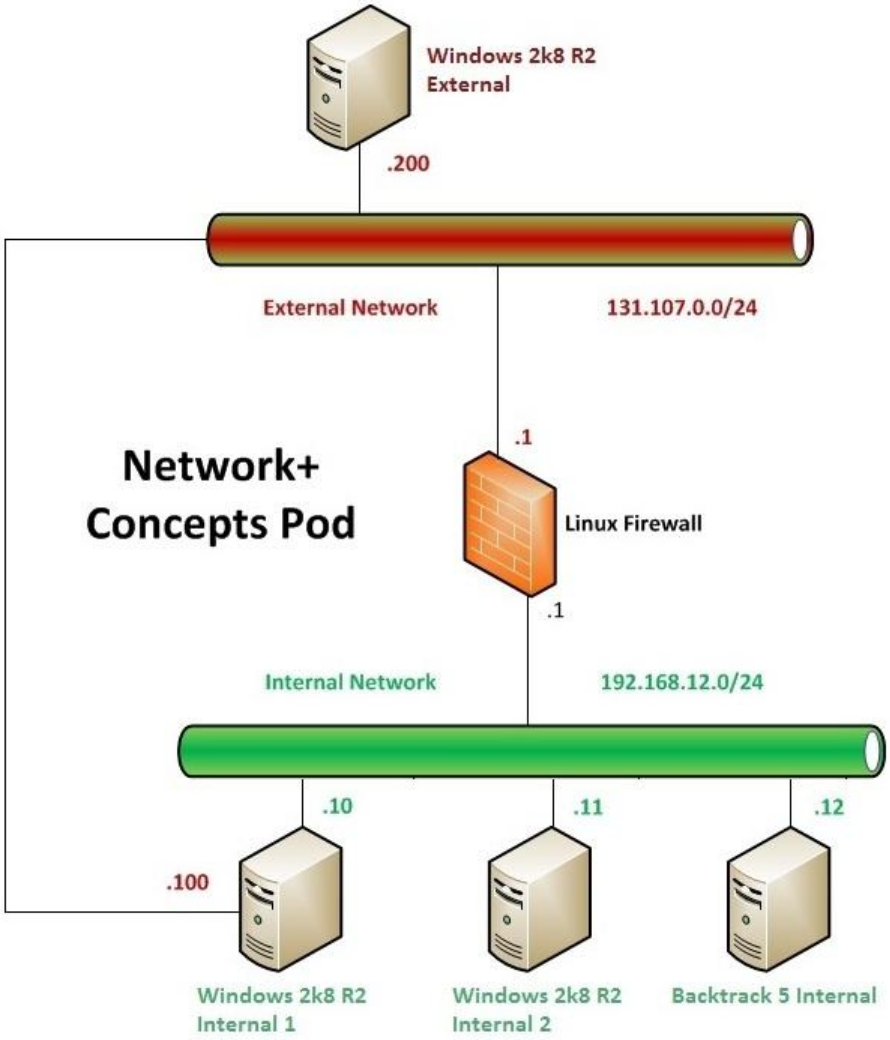
Performance Monitor/Resource Monitor – used to monitor system resource utilization in Windows operating systems. Both provide a graphical reference to resource utilization. The Performance Monitor is more advanced and customizable, whereas the Resource Monitor provides a more user-friendly interface.

Recommended Updates – in Windows operating systems, recommended updates are classified as updates to hardware, such as device drivers and other hardware information

Service Pack – a "bundle" of patches and updates for the operating system, downloadable as a single installable package, service packs may provide hundreds of updates and patches in one convenient download

Windows Update Utility – used to find, and apply patches and updates to the Windows operating system. The Windows Update Utility is accessible through the Control Panel.

Lab Topology



Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

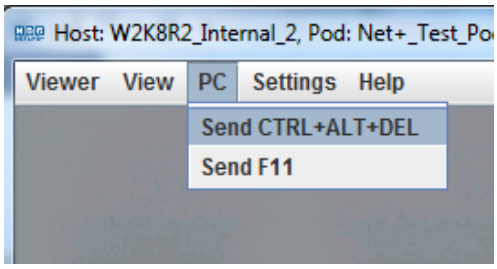
Required Virtual Machines and Applications

Log in to the following virtual machines before starting the tasks in this lab:

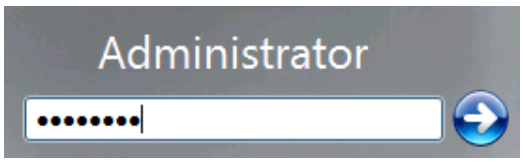
Windows 2k8 R2 Internal 1	192.168.12.10
Windows 2k8 R2 Internal 1 password	P@ssw0rd
Backtrack 5 Internal	192.168.12.12
Backtrack 5 Internal username/password	root/toor

Windows 2k8 R2 Login (applies to all Windows machines)

1. Click on the Windows 2k8 R2 icon on the topology that corresponds to the machine you wish to log in to.
2. Use the PC menu in the NETLAB+ Remote PC Viewer to send a **Ctrl-Alt-Del** (version 2 viewer), or click the **Send Ctrl-Alt-Del** link in the bottom right corner of the viewer window (version 1 viewer).



3. In the password text box, type **P@ssw0rd** and press enter to log in.



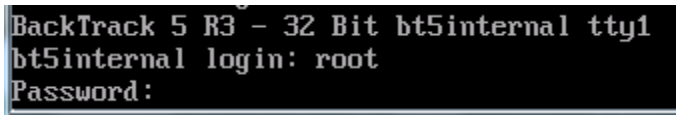
4. If the **Initial Configuration Tasks** and/or **Server Manager** windows appear, close them by clicking on the "**X**" in the top-right corner of the window.

Backtrack 5 Internal Login

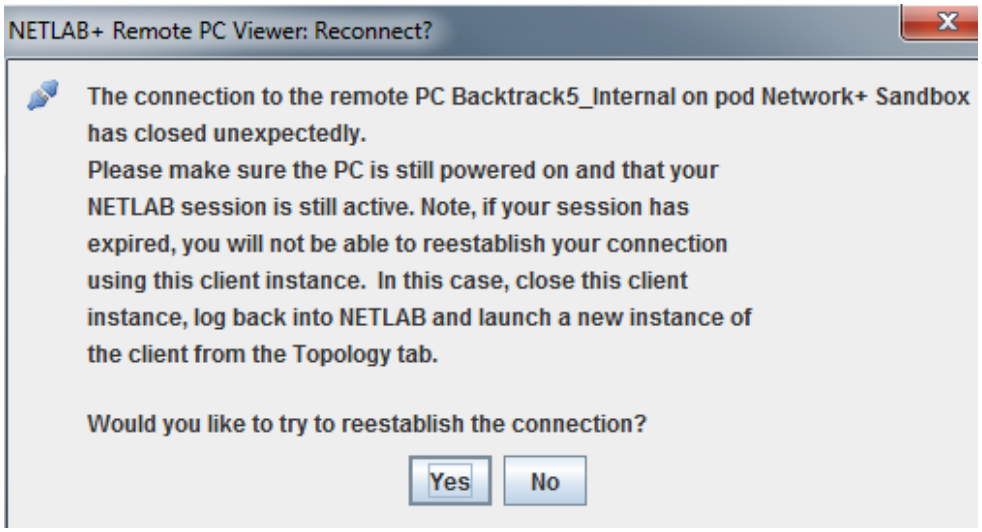
1. Click on the Backtrack 5 Internal icon on the topology.
2. At the **bt5internal login**: prompt, type the username **root** and press **Enter**.

3. At the **Password:** prompt, type the password **toor** and press **Enter.**

The password will not be displayed as you type into the prompt.



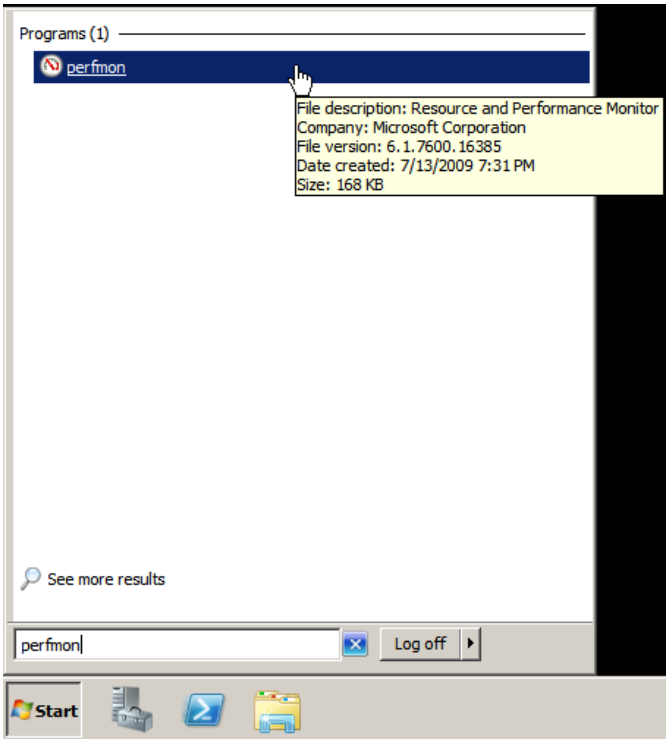
4. Once you have successfully logged in, type **startx** at the **root@bt5internal:~#** prompt and press **Enter**. This will start the GUI (Note: if you are disconnected after typing startx, click yes on the popup message to reconnect).



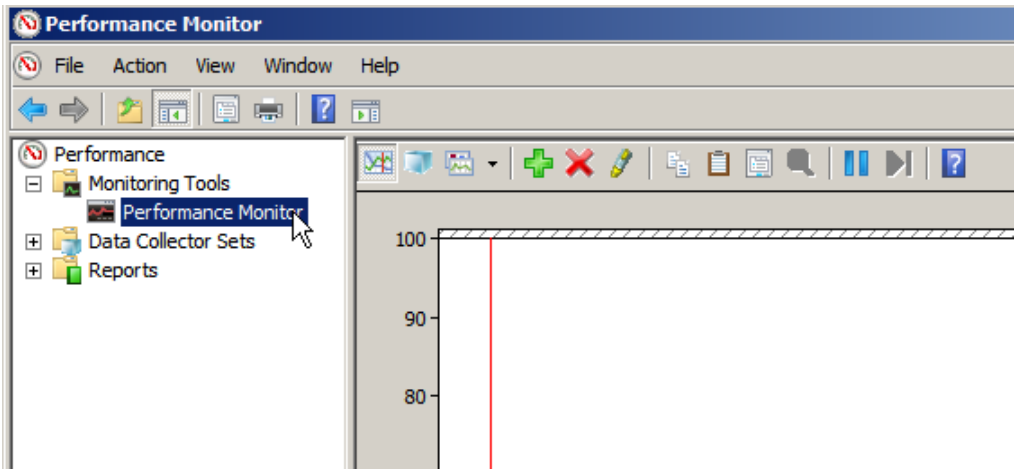
1 Analyze CPU and Network Utilization with Performance Monitor

Performance Monitor is a resource monitoring tool included in Windows-based operating systems. It provides utilization information on an expansive list of resources including, but not limited to processor, memory and network interfaces. Performance Monitor is also capable of monitoring granular aspects of resources that are beyond the scope of this lab, such as IPv4 and IPv6 traffic, hard disk activity, IPSec and more! In this task, we will open the Performance Monitor and use it to monitor CPU (processor) and network utilization.

1. Use the instructions in the Lab Settings section to log into the Windows 2k8 R2 Internal 1 machine, if you are not logged in already.
2. Click the **Start** button in the bottom-left corner and type **perfmon** in the Search Bar. Click perfmon to open the Performance Monitor.

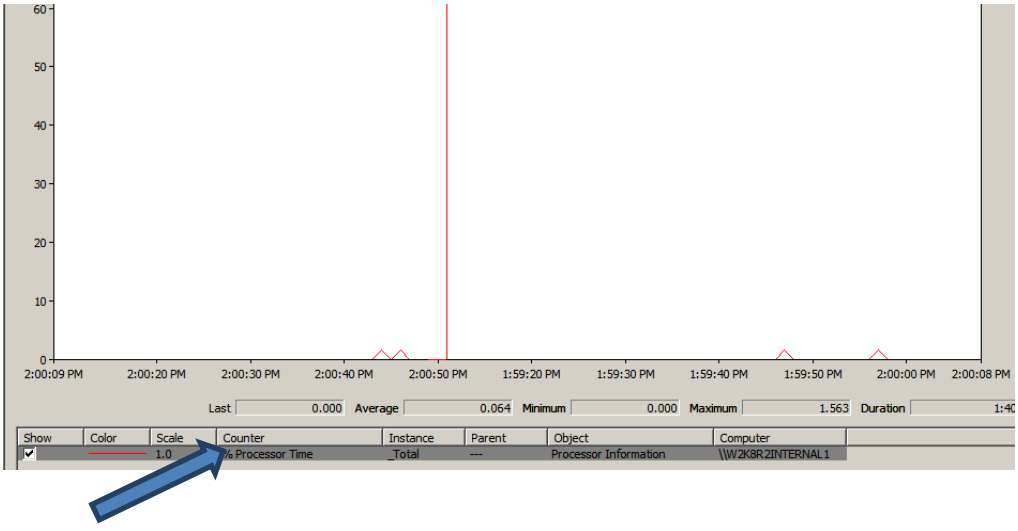


3. The Performance Monitor window will open. Under Monitoring Tools on the left, click on Performance Monitor.

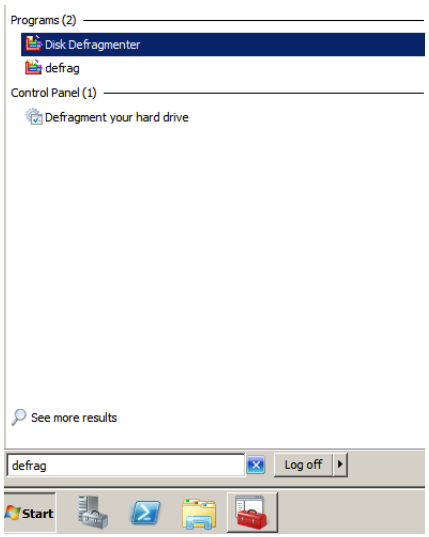


1.1 Monitoring CPU Utilization

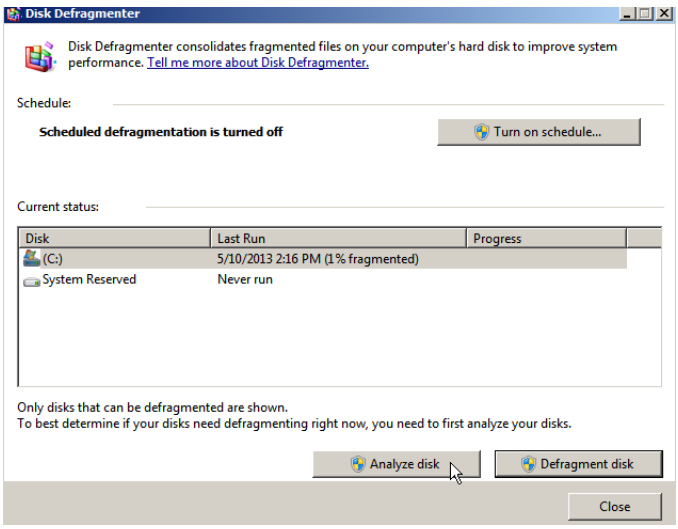
Currently, the only **counter** that is being monitored is the **%Processor Time** counter, which shows processor utilization. The X-axis, across the bottom, indicates the time, and the Y-axis, shown vertically on the left, represents % of usage from 0 – 100%. You may notice little to no activity in the graph while the machine is sitting **idle**. When **idling**, we can use information about resource utilization to establish a **baseline**.



1. In order to see activity on our graph, we will need to generate a work-load for the processor, give it something to do! We will use the Disk Defragmenter to generate this work-load. Click the Start button and type Defrag. Click Disk Defragmenter to open the program.

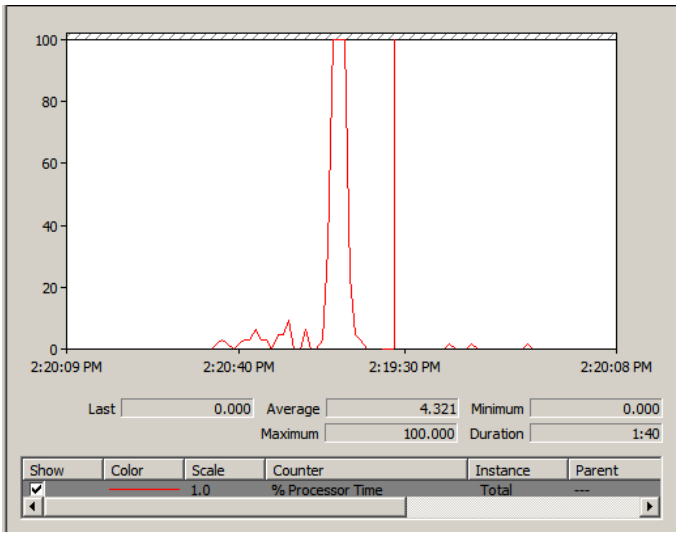


2. Disk Defragmenter will open. Click Analyze Disk, then immediately return to the Performance Monitor to see the effect on CPU utilization.



The graph shows the effect that analyzing the hard drive with Disk Defragmenter had on CPU **utilization**. Although the spike in utilization was relatively short-lived, the user may have noticed that other processes or programs on the system would have been affected by this spike in CPU activity. A user may notice slower Internet browsing, jerky video playback and slower system responsiveness in general when the CPU utilization is at 100%.

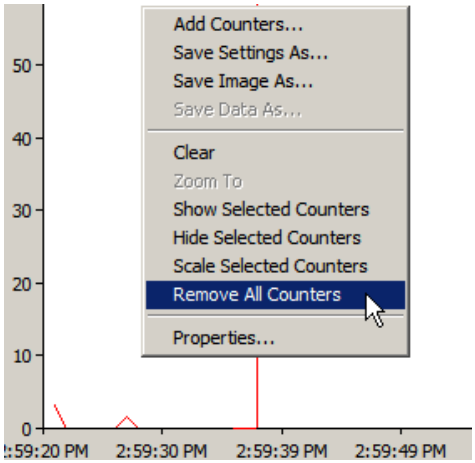
When compared, the graphs should show significant differences. Having the baseline graph of what a machine processor usage looks like when the system is idle allows the user to compare results while the system is in use and determine normal or abnormal system behavior.



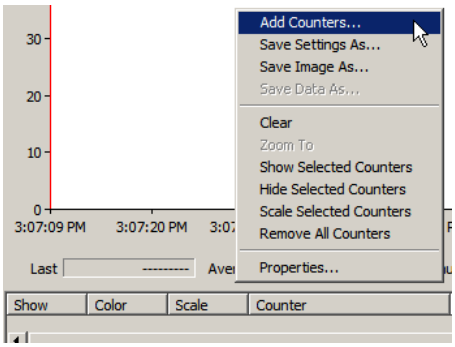
1.2 Monitoring Network Utilization by Adding a Counter

The Performance Monitor can be used to monitor network activity as well. In this section, we will add a counter for Bytes Received in the Performance Monitor utility then generate traffic and use the graph to observe the resource usage of the system for bytes received.

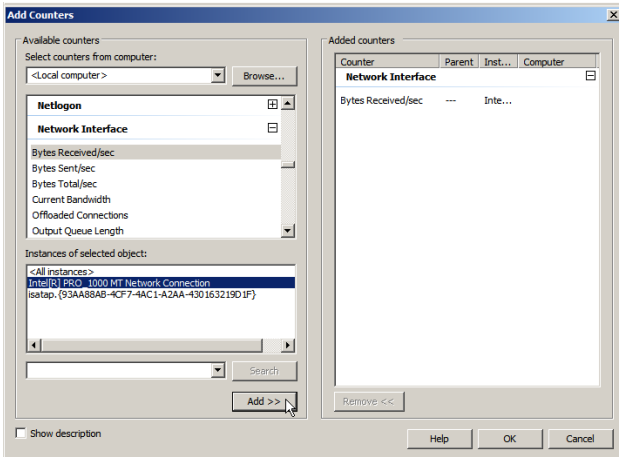
1. Right-click anywhere inside or close to the graph in Performance Monitor and select Remove All Counters. This will remove the %Processor Time counter from the Performance Monitor. When asked if you are sure you want to remove all added counters, click OK.



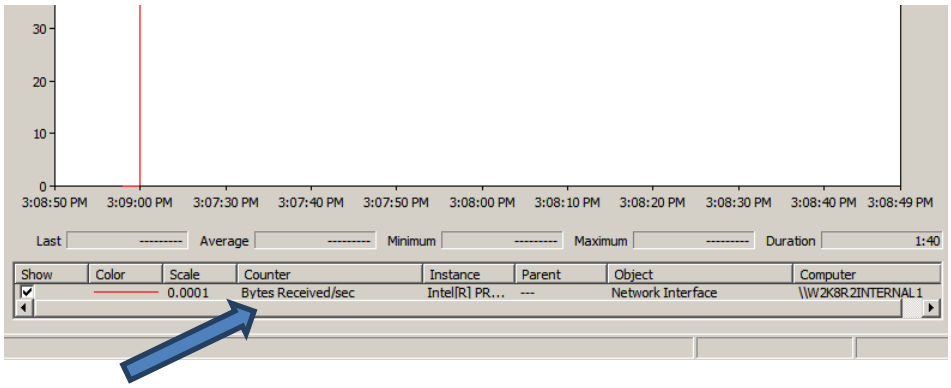
2. Right-click in the same area again and select **Add Counters…** to open the Add Counters dialog window.



3. The **Add Counters** window will open. From the list of available counters, locate **Network Interface** and expand the category by clicking the **+** sign next to it. From the sub-list, select Bytes **Received/sec**, then from the list below, titled "Instances of Selected Object", select **Intel[R]** PRO**_1000 MT Network Connection** and click the **Add>>** button. The new counter should appear on the right. Click **OK**.

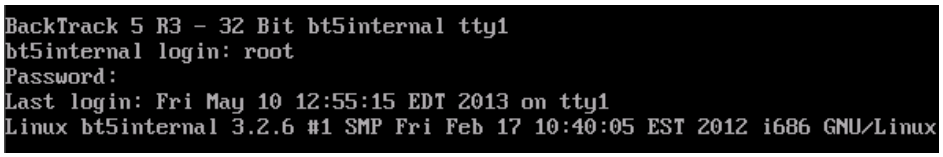


The new counter for Bytes Received/sec should appear in the counter table underneath the graph. The graph will show little to no activity until we generate some network activity.



To generate data on the network, we will execute a flood ping from another system.

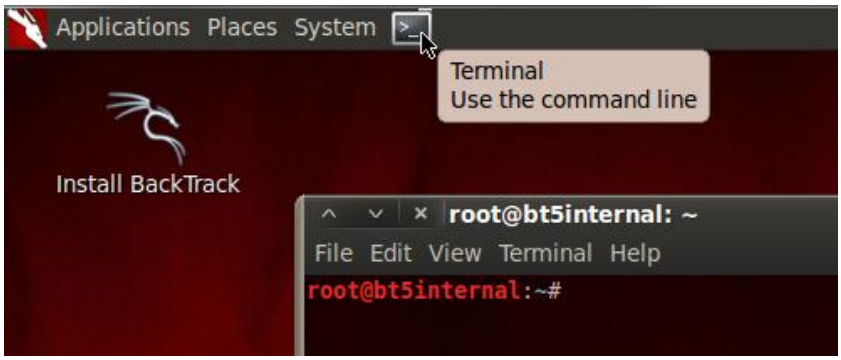
4. Click on the Backtrack 5 Internal icon on the topology.
5. At the bt5internal login: prompt, type the username root and press Enter.
6. At the **Password:** prompt, type the password **toor** and press **Enter**. NOTE: The password will not be displayed as you type into the prompt.



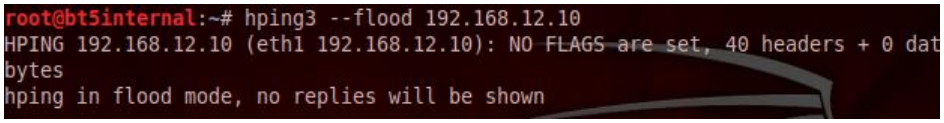
Keep in mind that **Linux commands are case sensitive**. The Linux commands below must be entered exactly as shown.

7. Once you have successfully logged in, type **startx** at the **root@bt5internal:~#** prompt and press **Enter**. This will start the GUI.

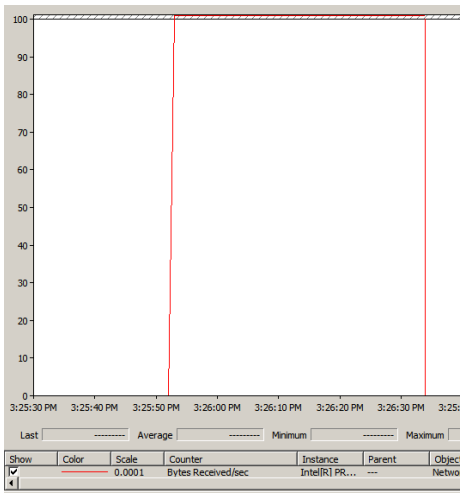
8. Click the icon to the right of the System menu to launch a Terminal window.



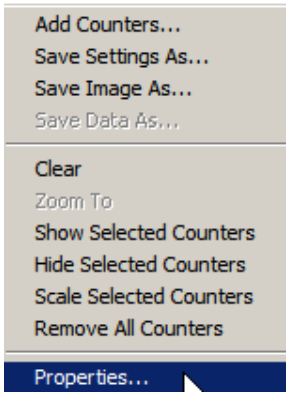
9. Execute a ping flood by entering the following command:
hping3 --flood 192.168.12.10



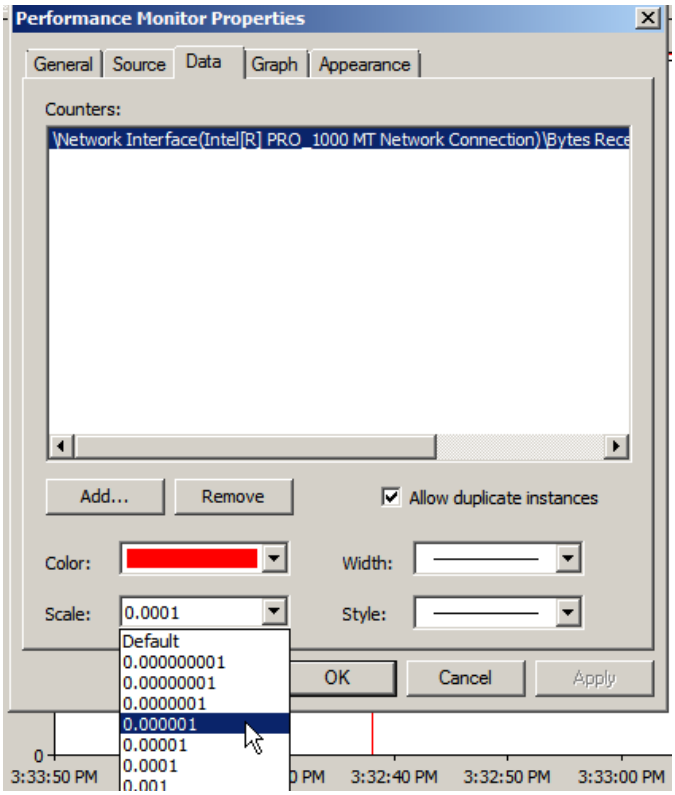
10. Return to the **Windows 2k8 R2 Internal 1** machine. Notice that the reading on the graph quickly disappears to the top of the screen.



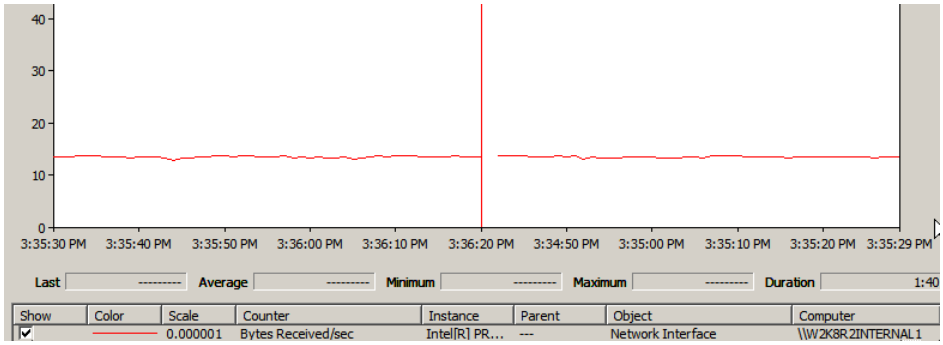
11. The graph disappears to the top because the y-axis only registers up to 100. We will either need to increase the y-axis, or change the scale of the counter to be able to see it on the chart. **Right-click** anywhere on the graph and select **Properties** from the menu.



12. From the Properties window, click the dropdown box next to **Scale:** and select **0.000001** from the list. Click **OK**.



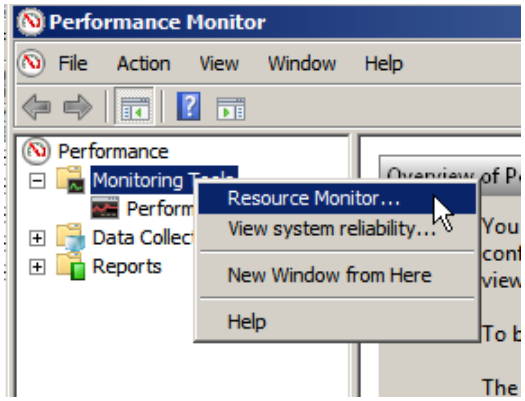
Immediately, you should see the Bytes Received register within the graph range, as shown below:



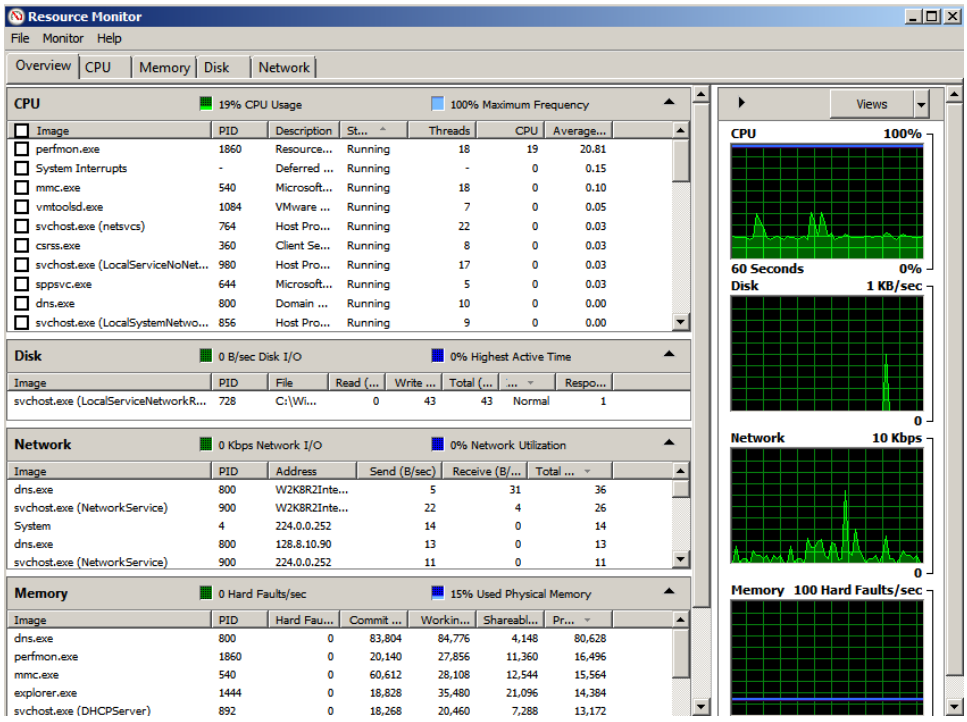
1.3 Using the Resource Monitor

The Resource Monitor, found within the Performance Monitor can provide a quick and detailed overview of system resources, including CPU, memory, disk and network. Some may find the Resource Monitor to be a more user friendly interface and display when monitoring system resources. This task will cover how to access the Resource Monitor and view network utilization.

1. From the Performance Monitor, right-click **Monitoring Tools** in the menu on the left-hand side of the screen and select Resource **Monitor**.

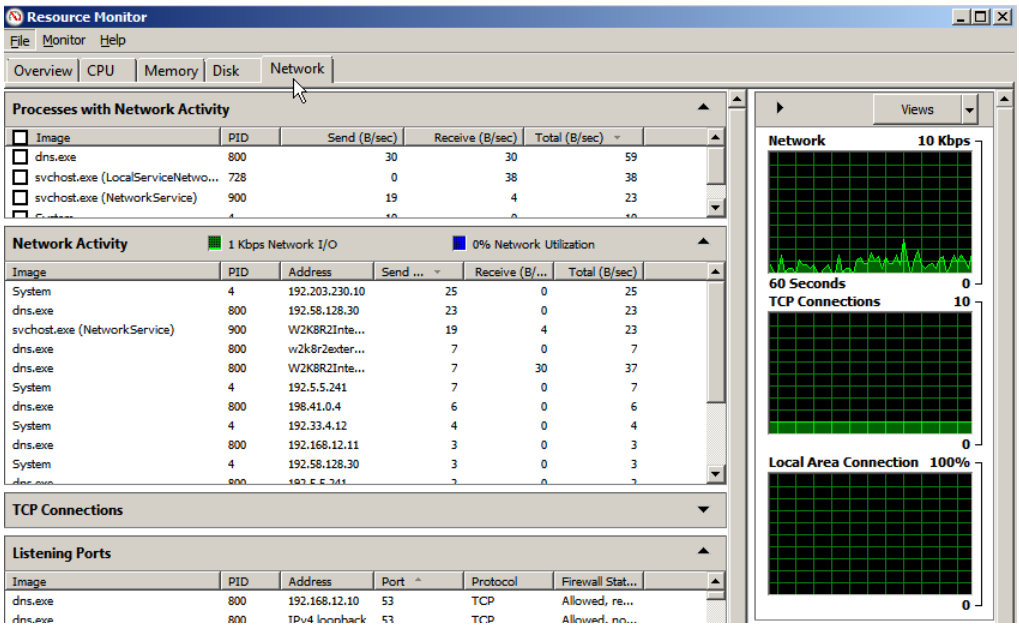


2. The Resource Monitor window will appear. The **Overview** tab should be the default tab displayed on your screen when Resource Monitor opens. If not, select the **Overview** tab.



The Overview tab in the Resource Monitor provides a summary on four major system resources: CPU, Disk, Network and Memory. Each resource can be expanded to show which processes are responsible for resource utilization. A graph for each of the resources appears on the right.

3. Click the **Network** tab.



The Network tab provides detailed information on network utilization. Details on processes that are using network resources such as Process ID (PID), remote IP addresses (IPv4 and IPv6), bytes sent, bytes received, protocols in use, ports listening for a connection, and the firewall status of those ports (allowed or blocked) are provided.

Explore the various tabs in Resource Monitor. Notice in each tab the list of processes that are being monitored. Placing a check in the box next to a process allows the monitor to filter based on one or more of the running processes selected. For troubleshooting this makes it easier to focus on tracking processes that could be causing issues and help with the problem solving.

4. Close all open Windows and stay logged in to continue with the next section of the lab.

1.4 Conclusion

The Performance Monitor provides a wealth of information on system resources and can be used as a troubleshooting tool by network technicians. Technicians can create a custom graph to monitor select system resources by adding counters for those resources. The Resource Monitor provides similar information, but is already setup to show resource utilization for four major system resources (CPU, Memory, Disk and Network) and requires no customization. The Resource Monitor provides a quick overview of those four major system resources and details on which processes are responsible for resource utilization.

1.5 Review Questions

1. *What program provides an overview of four major system resources?*

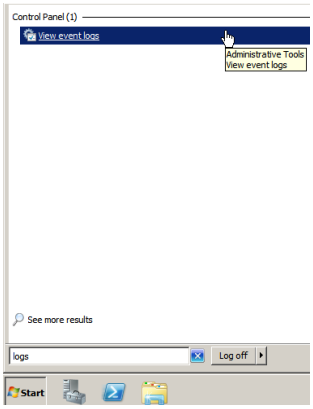
2. *In the Performance Monitor, what can you change if the reading on the graph is too high to display within the graph window?*

2 Use the Event Viewer to View Logs

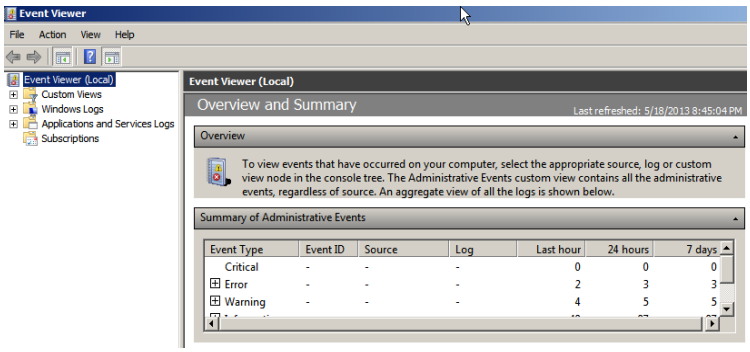
Sometimes, when troubleshooting, technicians must view system logs for clues to solve problems. The **Event Viewer** is a utility that can be used to view logs about program, security, and system events on Windows-based machines. These logs can be a good starting point for technicians to get a detailed view of what the system has been doing and allowing one to gain insight in to the correct behavior of a system and track the source of problems as well. In this task, we will learn how to access the event viewer to view various Event Viewer logs.

2.1 Open Event Viewer and Trigger a Failed Audit Event

1. To launch Event Viewer on the **Windows 2k8 R2 Internal 1** machine, click the **Start** button and type **logs** in the search bar. Click **View event logs** in the search results to open the Event Viewer. You could have also typed **event** and that would have also been enough to locate the Event Viewer. The Event Viewer is also located in Administrative Tools, located in the Control Panel.



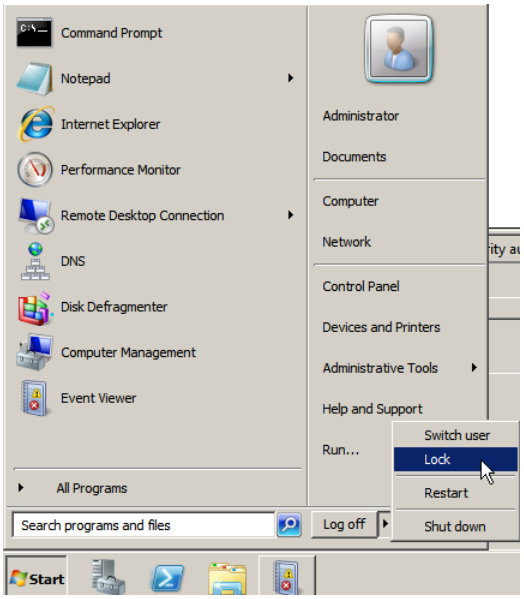
2. The Event Viewer will open and by default you should see **Overview and Summary** in the middle pane of the window. This is a brief look at the events that have occurred on the machine. Investigate the Overview and Summary pane and notice the types of Administrative Events logged and the names of the logs enabled in the Log Summary.



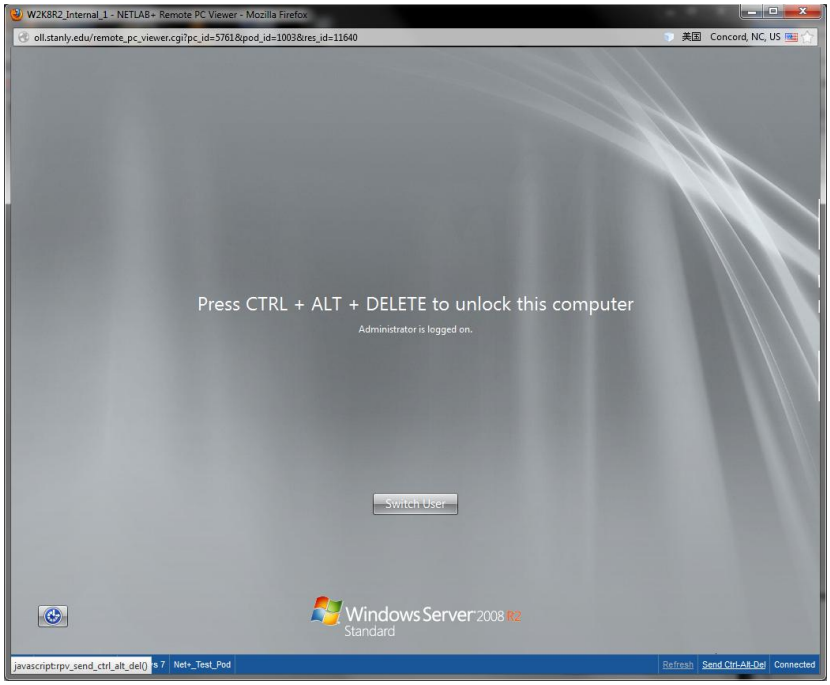
Under the **Summary of Administrative Events** section, you should see a summary of events that have been logged in the last hour, 24 hours, or 7 days. You may see events in this section that are classified into the following categories. Although there are other categories not listed here, these are most common:

- **Critical:** These are events caused by applications or hardware from which the system was not able to recover.
- **Error:** These are system errors that occur with services on the machine, such as services and software embedded in the operating system.
- **Warning:** These events are not critical in nature, but should be examined. This type of event may occur when an application fails perform a certain task.
- **Information:** This type of event is not an indication of a problem. This event may merely indicate that a service was successfully started or stopped.
- **Audit Success:** Logs successful login attempts
- **Audit Failure:** Logs failed login attempts

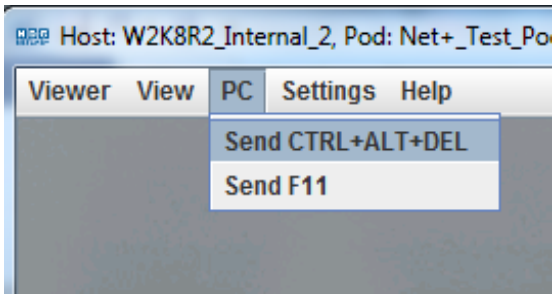
3. We will now generate a failed login attempt and see if an event is recorded in the log. Click the **Start** button, then click the **arrow** next to **Log off** and then click **Lock.**



The computer will be locked and you will be returned to the log in screen.

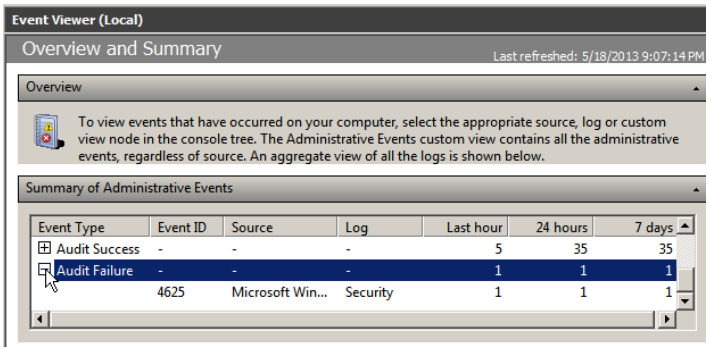


4. Use the PC menu in the NETLAB+ Remote PC Viewer to send a **Ctrl-Alt-Del** (version 2 viewer), or click the **Send Ctrl-Alt-Del** link in the bottom right corner of the viewer window (version 1 viewer).

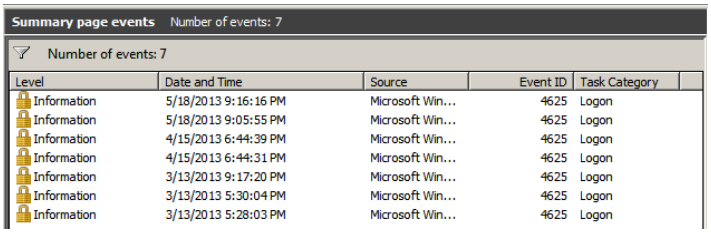


5. When prompted for a password, enter an incorrect password such as **password**, and attempt to login. You'll get the following message, indicating you entered an incorrect password.

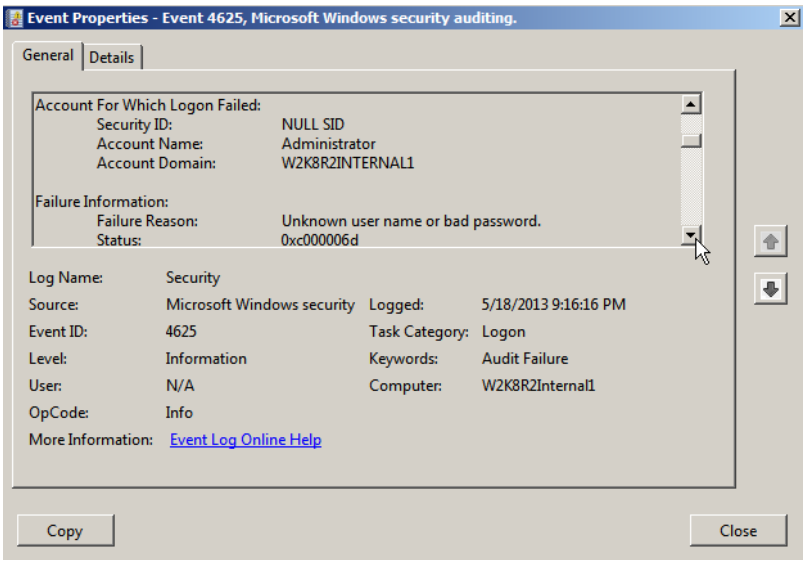
6. Now, click **OK,** login with the correct password**, P@ssw0rd**,and return to the **Event Viewer.** Once there, you will need to refresh the Overview and Summary screen. Click **Action** in the menu at the top of the screen and select **Refresh.** Now, scroll to the bottom of the **Summary of Administrative Events** and expand the **Audit Failure** event type.



7. Double-click on the event ID **4625**. A Summary page will be displayed showing all previous logged events for failed login attempts.

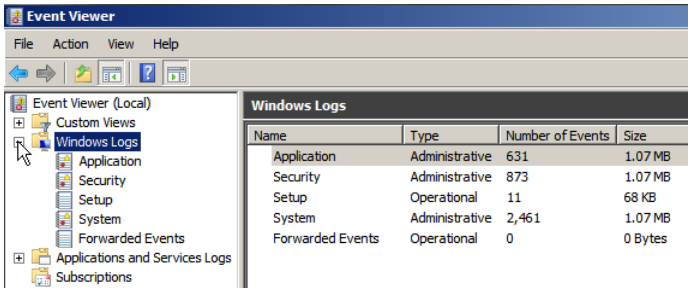


8. You should see the most recent failed attempt at the top. If not, you can click the Date and Time Column to toggle between ascending and descending order. Double-click on the most recent event. An **Event Properties** window will be displayed. Use the scroll buttons and scroll down until you see **Account For Which Logon Failed.** This shows which account had the failed login attempt.

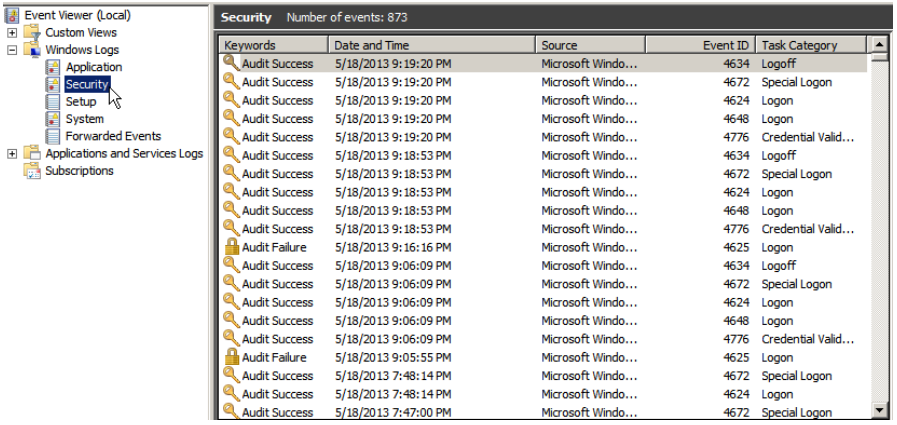


2.2 Viewing Windows Logs

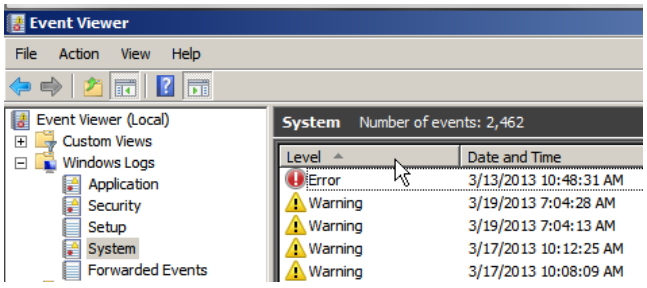
1. In the left panel of the **Event Viewer** window click on **Windows Logs.** A list of some of the default logs will appear in the middle pane, showing information such as the number of events in each log, as well as the size of the logs being stored. 1.07MB may not seem like a lot of space, but note that it represents a significant number of events.



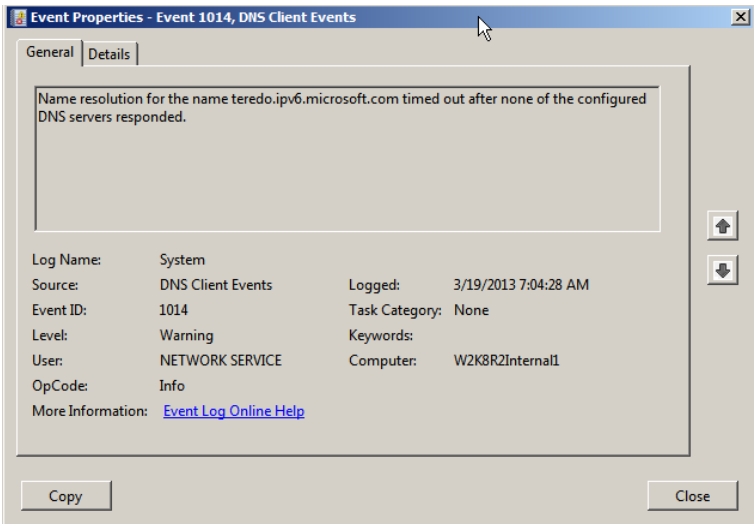
2. Double-click **Security** in the list of logs in the middle panel. This will open the Security log, which shows events such as successful and failed logon attempts. Our failed login attempt from earlier should appear in this list.



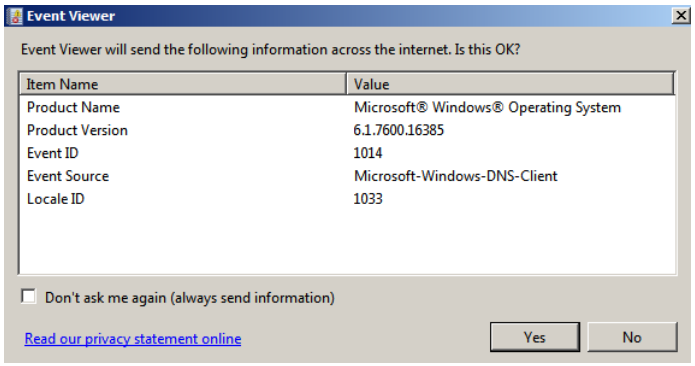
3. Click on the + next to **Windows Logs i**n the left pane then click **System** underneath **Windows Logs.** This log shows events related to Windows operating system services. Click the **Level** column to put levels in ascending order, this puts the most significant issue at the top of the list. If necessary, scroll to the top of the screen to see Errors and Warnings.



4. Double-click on any **Warning** event. An **Event Properties** window will appear showing details about the selected event.



5. Click the **Event Log Online Help** link at the bottom of the Event Properties page. A window opens, indicating you can transmit information about the event over the Internet and asks if this is OK. If you want to continue with sending you would need to click the **Yes** button. This machine has no Internet access, so we will not be able to proceed. However, this is a way technicians can find out more information about events and possible solutions.



6. Close all windows and stay logged in to continue with the next task section.

2.3 Conclusion

The Event Viewer in Windows keeps logs on the system to aid in monitoring systems and is a powerful troubleshooting tool for discovering and researching system errors. These logs are recorded as separate "events" and categorized for easy access and viewing. From the Event Viewer, a technician may find information about an error message displayed by an application, a failed login attempt, or simply an event showing where a service was stopped or started. Examining the Event Viewer can be a great first step for a technician troubleshooting an error message.

2.4 Review Questions

1. *What type of event is caused by applications or hardware from which the system is not able to recover?*

2. *What does an Audit Failure event usually indicate?*

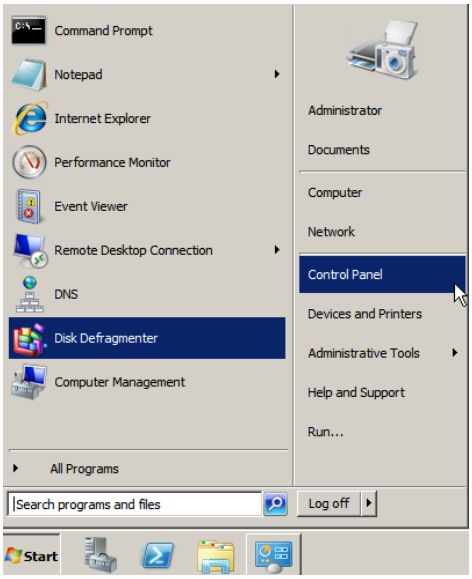
3. *What type of event indicates a successful login attempt?*

3 Manage Patches and Updates

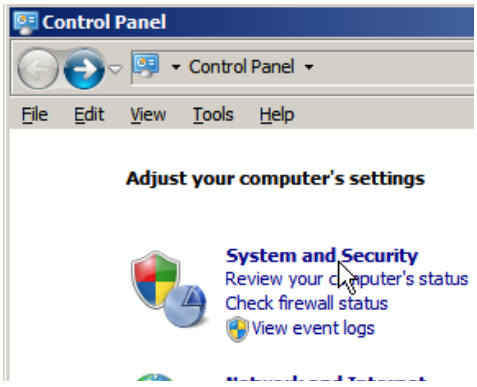
Patches and updates are an important part of network administration. Operating system and application updates play a vital role in mitigating security threats. Updates come in various types and sizes; with the most important updates being classified as "critical". **Critical Updates** patch known vulnerabilities to the operating system and should be implemented immediately to mitigate threats. This task will explore the **Windows Update utility** and its settings and features.

3.1 Navigating to the Windows Update Utility

1. On the Windows **2k8 R2 Internal 1** machine, click the **Start** button and then click **Control Panel.**



2. The Control Panel window will appear. Select the **System and Security** category.



3. Click **Windows Update**.

The Windows Update applet is a program used to configure the parameters of how to receive and view the status of updates on the system. As this machine is not connected to the Internet and is not able to be updated during this exercise, you will explore various features of the Windows Update utility and operations that can be performed by using it. **It is very important the updates are downloaded and installed after verifying that they are compatible with the system. Updates are available to improve system performance as well as fix or prevent problems from occurring.**

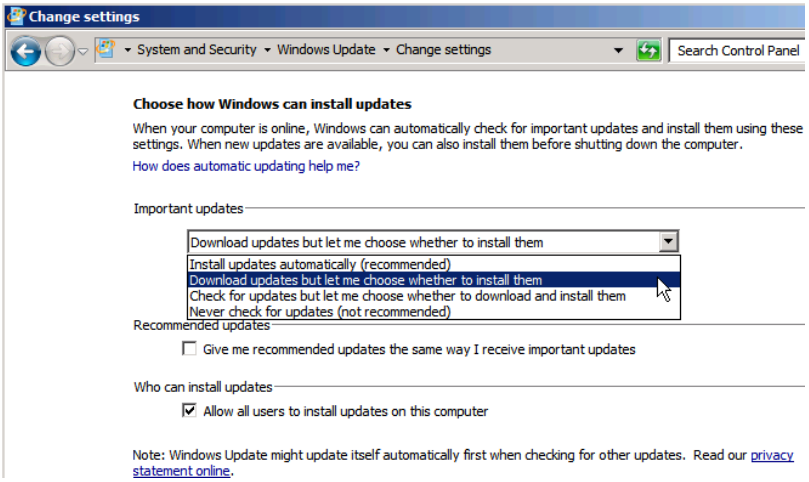
4. In the left area of the Windows Update utility window there are links to the different actions that they program can run. Click on **Updates: frequently asked questions**.

    1. *Does Microsoft charge users for updates?*

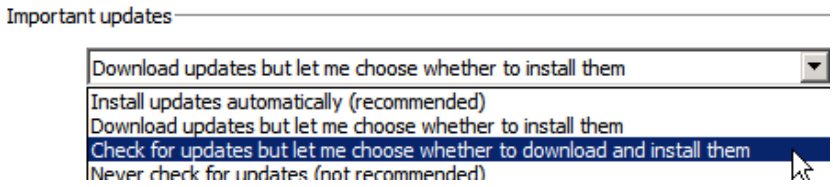
    2. *Once installed, can an update be removed?*

3.2 Changing Windows Update Settings

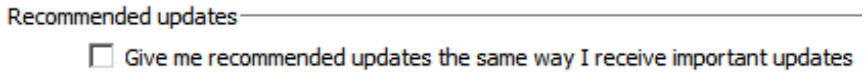
1. Click on **Change Settings** in the left area of the Windows Update utility. The **Change settings** window should appear. On this screen, a user can choose how Windows checks for and installs updates. Windows classifies updates as either "important" or "recommended". Important updates include **service packs** and other critical updates, whereas recommended updates provide updates to your hardware, such as device drivers and other hardware information. Windows allows you to customize which updates you receive, how often your machine checks for updates, how and when they are installed, and who has rights to install them.
2. First, you choose how to install important updates. Click the dropdown box under **Important updates** and look at the available options.



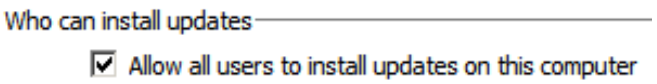
3. Click on the drop-down arrow under the Important Updates heading. "Install updates automatically" is the recommended setting. Other choices are "Download updates automatically, but let me choose whether to install them" or "Check for updates, but let me choose whether to download and install them." Select **Download updates but let me choose whether to install them.**



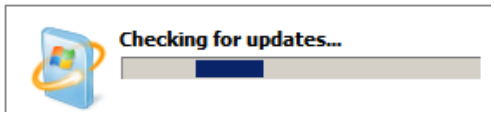
4. Next, choose how to receive recommended updates. Recall that recommended updates are sometimes updates to hardware, such as device drivers. You should exercise caution when updating device drivers, as they may have a negative impact on the system. It is a better practice to manually download device drivers from the manufacturer's website and implement those updates on a schedule of your choosing; for example, once every six months, or once a year. It is possible for some Windows updates to affect device driver functionality. For now, leave the box for recommended updates unchecked.



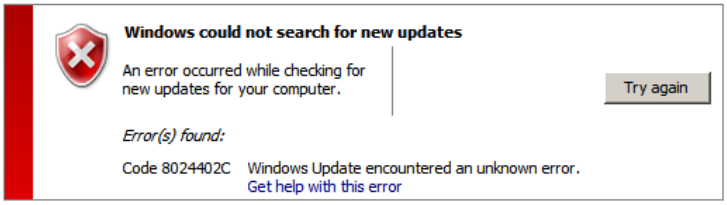
5. The last checkbox determines who can install updates. To be sure standard users can install updates, leave this box checked. If only administrators should be able to install updates, uncheck this box. Leave the box checked for now. Click **OK** when done.



Windows Update immediately begins checking for updates:



After a few minutes, Windows Update will fail because there is no connection to the Internet. If there were a connection to the Internet, this would have been successful.



6. In your local computer, open a command prompt. On the command line, type echo "your first and last names". Then press the Enter key. Take a screenshot that contains your full name and the running outputs obtained at Step 5 above.

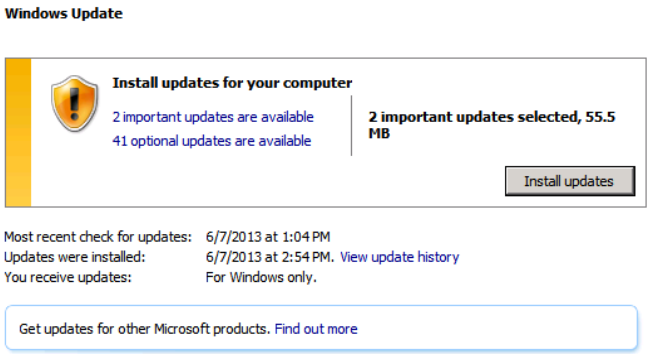
3.3 Selectively Installing Windows Updates

Another option available for configuration is to be able to selectively install Windows updates that have already been downloaded to the computer. Periodically, Microsoft will release an update that may cause issues on some computers, depending on hardware, or other software installed. Perhaps the systems administrator at a company is aware of a bug caused by a new Microsoft update that will affect the company's proprietary software. In this instance, the administrator may choose to selectively install Windows updates, avoiding the installation of the update that may cause issues.

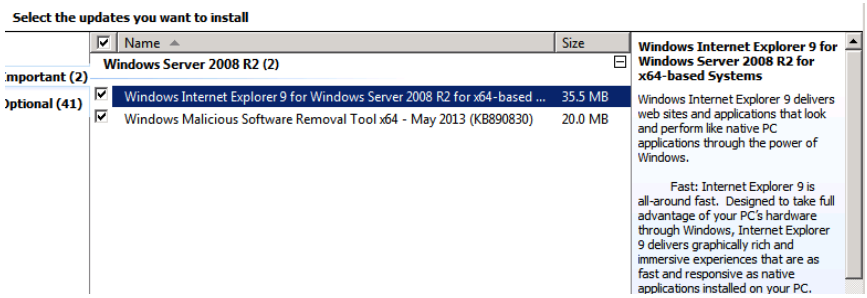
To do so, an administrator would follow the process in the previous exercise and select **Download updates but let me choose whether to install them** and be sure that the **Allow users to install updates on this computer** check box is unchecked. Then, when Windows downloads updates and you open the Windows Update utility, the opening page will list the downloaded updates as links allowing an administrator to review what has been downloaded and make a decision on how to proceed, install or skip the update.

DO NOT attempt to perform the steps below, since the lab environment does not have access to the Internet to download Windows Updates. The steps are included only as informational.

1. There is an **Install Updates** button available on the same page as the update links.



2. Two updates are listed: an update to Internet Explorer 9 and a Malicious Software Removal Tool update. Clicking to highlight an update shows a description and details of the update.



3. **Uncheck** the box next to any update that is not to be installed and leave the box checked next to those necessary. Then the **Install Now** button would be used to initiate the process.

3.4 Conclusion

The Windows Update utility can check for and install new, important and recommended updates. Critical updates patch known security vulnerabilities; therefore, installing updates regularly is an important component to threat mitigation. Updates are sometimes very large and can take long periods of time to download and install; therefore, updates should be installed on a schedule, at a time that imposes as little impact to end-users as possible.

3.5 Review Questions

1. *Updates to device drivers are classified as what type of update?*
2. *A Service Pack is classified as what type of update?*
3. *What category in the Control Panel is Windows Update located?*