Security
Hands-on Exercise
Background Story

You have been hired as the lead IT Administrator at the Florida International University (FIU) to manage the computers at the School of Computing and Information Sciences (SCIS), the Machine Room (MR), the Green Library (GL), and the College of Engineering and Computing (CEC). As shown in Fig. 11.16, SCIS, MR, GL, and CEC are physically located in four buildings. SCIS maintains about 200 desktop workstations in its instructional lab, MR maintains about 5 servers, GL maintains about 50 open access guest desktops, and CEC maintains about 500 PCs and laptops. The exact number and configurations of computers are not well documented. Typically, the servers run Windows 2003 and the desktop workstations, PCs, and laptops all run Windows XP. Active Directory is implemented in one of the servers, named dc, and is assigned to all computers in SCIS and GL, but not to those in CEC. As the lead IT Administrator of the organization you are responsible for ensuring that all systems run efficiently with minimal disruption of computing services to the users.

![Fig. 11.16: A logical diagram of FIU's network.](image)

You have decided to employ a Kaseya server to help you manage all computers at SCIS, MR, GL, and CEC. Your Kaseya server is now installed and is fully operational. In addition, you have successfully deployed agents on some of the machines under your management.

Internet security is becoming an important aspect to IT specialist. Malicious software is a major problem to networks that are unprotected and exposed to the Internet. Without a stable Internet security solution in place, computers exposed to the Internet will be infected with malicious software and most likely make the environment unusable or worse, expose sensitive information to hackers.

Kaseya’s Security module enables you to install and configure anti-virus software. By using alarms, this module allows the monitoring of Internet security.
Technical Information

Your dedicated virtual environment includes the computers and network devices depicted in Fig. 11.16 and further described below:

- NAT Router: 192.168.0.1 & 192.168.1.1 & 192.168.2.1 & 192.168.3.1
- SCIS: ws1.scis.fiu.edu - 192.168.0.100
- MR: dc.scis.fiu.edu - 192.168.0.10 & 192.168.1.10 & 192.168.3.10
- GL: guest1.gl.fiu.edu - 192.168.1.100
- CEC: pc1.cec.fiu.edu - 192.168.2.100 & laptop1: laptop1.cec.fiu.edu - 192.168.2.200

Note: This virtual environment includes only a limited number of representative servers and workstations physically housed in the four buildings.

Exercise

Before installing the security software (i.e., the Kaseya Endpoint Security (KES) client), a security profile must be defined first. Create the profile to limit the size of the virus vault to only 5% of the local disk and configure it to scan for all potential threats. Once the profile is created, install the security client on all computers in the scis, gl, and cec buildings and associate the profile with the installation. After installation, update the virus definitions on all machines and turn on automatic updates. Since guest1 is used more than the other computers, schedule an immediate scan on guest1, then schedule a scan once a week on Saturdays on all KES clients. Creating an alarm set will help when the KES client fails to remove a threat or when the KES client is removed. Create an alarm set and apply it to all machines.

Part 1

Create the security profile. The profile will limit the size of the virus fault to 5% to preserve hard drive space. Make sure all threats will be scanned for and resolved. Since you don’t want to waste computing resources, the scan will run on low priority. After the profile is created, install the KES client on all computers within the scis, gl, and cec buildings and assign the profile to the installation.

Create a security profile. The security profile should limit the size of the virus vault to 5%. Also make sure when a full scan is initiated, it scans for all threats. Finally, configure the scan to run on low priority.

1. Open the Security module. Go to Configure > Define Profile.
2. Type “5” in the Maximum Size of the Vault textbox.
3. Click on **Full Scan**.
4. Verify all checkboxes are checked.
5. Select **Low Priority** in the Select System Priority for Scan dropdown.

6. Click on **Resident Shield**.
7. Select the **Scan for Tracking Cookies** checkbox.
8. Click on **Save As**.
9. Type in "<USERNAME> Security Profile" in the textbox.

10. Click on OK. Install the KES client on guest1, laptop1, pc1, and ws1. Include the newly created security profile within the installation.


12. Select <USERNAME> Security Profile in the Select Profile dropdown.

13. Select the guest1, laptop1, pc1, and ws1 checkboxes.

14. Select the Immediate checkbox.

15. Select the Install from KServer (override file source) checkbox.

16. Verify Force install without warning user is selected.

17. Click on Install.
Chapter 11 – Security Hands-On Exercises

Note: This process will take some time. Please wait 20-30 minutes before continuing.

Part 2

Updating the KES client is an important task since different malicious software is found every week. Updating can be done automatically, if set to do so; otherwise, manually scheduling an update can be done. Schedule an immediate update on all KES clients and turn on automatic updates for future virus definitions. After updating the KES client, schedule a scan on guest1 then schedule all computers to run a scan at 9:00am on Saturdays only.

- Manually update the KES client. After the update, enable automatic updates.


19. Select all available computer checkboxes.
20. Click on the *Immediate* checkbox.
21. Click on the *Update from KServer* checkbox.
22. Click on *Update*.
23. Click on *Enable Automatic Update*.

-Schedule an immediate scan on guest1. After, schedule a scan every Saturday at 9:00am.
24. Open the Security module. Go to *Protection > Schedule Scan*.
25. Select the guest1 checkbox.
26. Click on the *Immediate* checkbox.
27. Click on *Scan*.

28. Select the laptop1, pc1, and ws1 checkboxes.
29. Uncheck the *Immediate* checkbox.

30. Open the *Calendar* popup.

31. Select the next Saturday date.

32. Select the *Every* checkbox and change the frequency to once a week.

33. Click on *Scan*.

Defining an alarm set will help to notify you when certain actions take place in any of the KES clients. If a threat is detected and not healed, then using an alarm will notify you and allow you to take the necessary steps. Also, if the protection is disabled or the KES client is removed, you can be notified as well. Create a security alarm set that will notify you when a threat is detected and not healed, protection is disabled, or AVG is removed by the user. Once created, apply the alarm sets to all KES clients.
35. Select the Threat Detected and Not Healed checkbox.
36. Select the Protection Disabled checkbox.
37. Select the AVG Removed By User checkbox.
38. Click on Save As.
39. Type in “<USERNAME> Alarm Set” in the textbox.
40. Click on Ok.
41. Go to Security Alarms > Assign Alarm Sets.
42. Select <USERNAME> Alarm Set in the Select an Alarm Set dropdown.
43. Select the Create Alarm checkbox.
44. Select the Email Recipients checkbox and type in your personal email into the textbox.
45. Select all available machine checkboxes.

46. Click on Apply.

Fig. 11.28

It would be best to check if the Security module is configured successfully. To do so, you will rely on Info Center to produce a report on your security settings.

47. Open the Info Center module. Go to Reporting > Reports.

48. Click on your Private folder, “myReports-<USERNAME>”, choose New Report and a new window will open up.

Fig. 11.29


51. Click Next.

52. Click on Save.
53. Select the newly created report under your folder then choose Run Report.

54. Choose “fiu-<USERNAME>” next to Organization in the new window.

55. Click on Submit.

56. Once the scheduled report is done, a green icon will appear on top of a clipboard in the Schedule window. Click on the icon to view your report.
Note: Use the report to check and see if the tickets are configured successfully. The report can be printed out for record keeping; however, this is not necessary for this exercise.