

**SSN College of Engineering,  
Department of Computer Science and Engineering  
CS6711 Security Laboratory**

**Exercise 10:**

To setup a honey pot and monitor the honeypot on network

**Hints:**

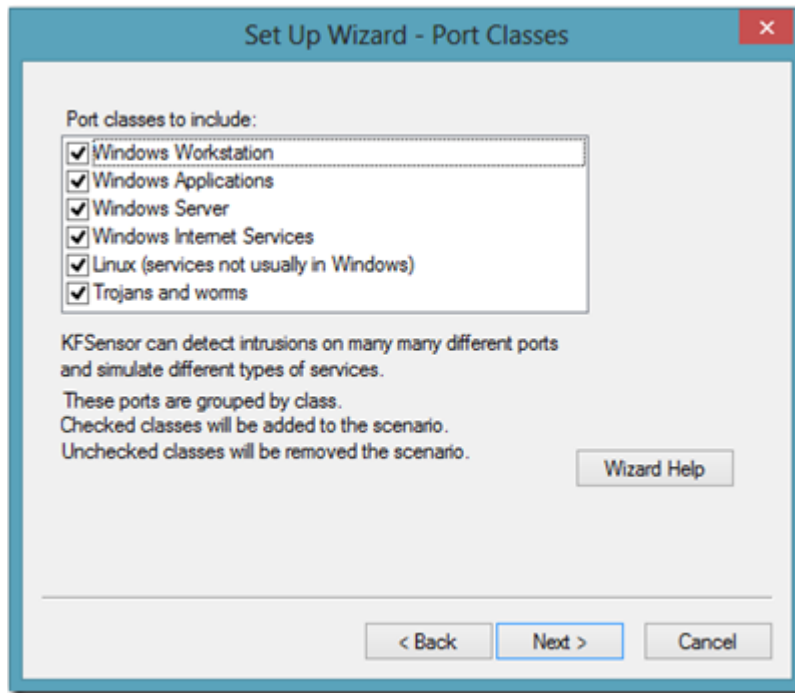
- Honey Pot is a device placed on Computer Network specifically designed to capture malicious network traffic.
- KF Sensor is the tool to setup as honeypot when KF Sensor is running it places a siren icon in the windows system tray in the bottom right of the screen.
- It performs by opening ports on the machine it is installed on and waiting for connections to be made to those ports.
- By doing this it sets up a target, or a honeypot server, that will record the actions of a hacker.
- KFSensor\_Server- Performs core functionality by listening to both TCP and UDP ports on the server machine and interacts with visitors and generates events. It runs as a daemon at the background.
- **KFSensor Monitor :**
  - Interprets all the data and alerts captured by server in graphical form.
  - Using it you can configure the KFSensor Server and monitor the events generated by the KFSensor Server.
- **Sim server** is short for simulated server.
- It is a definition of how KFSensor should emulate real server software.
- A visitor is an entity that connects to KFSensor.
- Visitors could be hackers, worms, viruses or even legitimate users that have stumbled onto KFSensor by mistake.
- Visitors can also be referred to as the clients of the services provided by KFSensor.
- An event is a record of an incident detected by the KFSensor Service.
- For example if a visitor attempts to connect to the simulated web server then an event detailing the connection is generated.
- Events are recorded in the log file and displayed in the KFSensor monitor.
- KFSensor is rules based. All of the data that was produced was the result of KFSensor detecting certain types of activity and then using a rule to determine what type of action should be taken.
- We can easily modify the existing rules or add your own

**Setting Up a KF Sensor HoneyPot:**

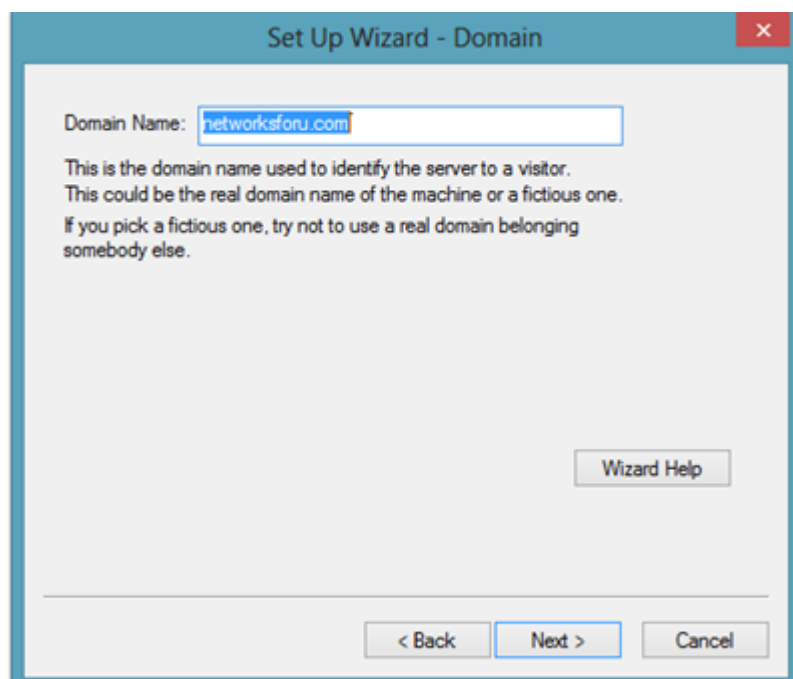
1. Download and install winpcap
2. Download KF Sensor Evaluation Set File from KF Sensor Website.
3. Install with License Agreement and appropriate directory path.
4. Reboot the Computer now.
5. The KF Sensor automatically starts during windows boot Click Next to setup wizard.
6. Select all port classes to include and Click Next.
7. Send the email and Send from email enter the ID and Click Next.
8. Select the options such as Denial of Service[DOS], Port Activity, Proxy Emulsion, Network Port Analyzer, Click Next.
9. Select Install as System service and Click Next.
10. Click finish.

### **Monitor the honeypot on network**

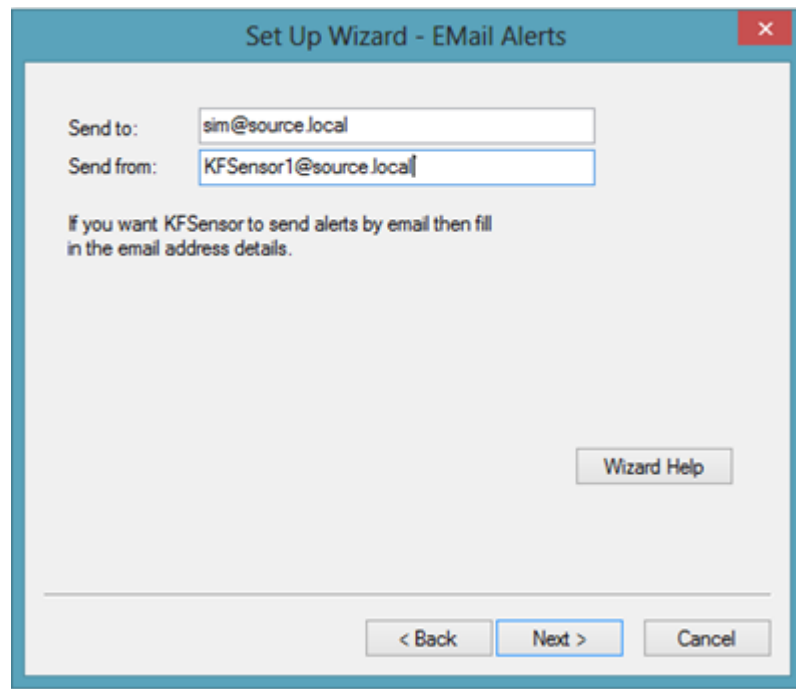
1. Select Settings > Set Up Wizard. The Set Up Wizard guides you through the configurations of:
  - Port Classes
  - Domain Name Selection
  - Email Alerts
  - Systems Service
2. Click the Next button to begin configuring KF Sensor. By default all the port classes will be selected.



3. Now you need to give your system a name. Use a fictitious name that may be attractive to someone who is doing discovery for “juicy” targets. For example, using the following words somewhere in your domain name may get you more hits: - credit - bank- financial- investment- accounting- private- internal. Enter your domain name (don’t forget to include the .com, .org, .net or whatever extension you are going to use). Click Next.



4. If you would like to receive email alerts of events, enter your target email address and the source email address in this window.



The image shows a Windows-style dialog box titled "Set Up Wizard - EMail Alerts". It has a blue title bar with a red close button. The main area is light gray. There are two text input fields: "Send to:" with the value "sim@source.local" and "Send from:" with the value "KFSensor1@source.local". Below these fields is a small text instruction: "If you want KFSensor to send alerts by email then fill in the email address details." At the bottom right is a button labeled "Wizard Help". At the bottom center are three buttons: "< Back", "Next >", and "Cancel".

5. Now you can configure the system services. Click the Wizard Help button for more details on each option.
  - Denial of Service
    - Normal/Cautious
  - Port Activity
    - 1-12 Hours
  - Proxy Emulation
    - Allow banner grabs and loop backs
    - No external connections
  - Network Protocol Analyzer
    - Disable packet dump files
    - Enable packet dump files
6. Use the following settings and Click Next.

**Denial Of Service Options**

Normal

Controls how many events are recorded before the server locks up

**Port Activity**

1 Hour

How long a port should indicate activity after after an event

**Proxy Emulation**

Allow banner grabs and loop backs

Controls if KFSensor is allowed to make limited external connections

**Network Protocol Analyzer**

Enable packet dump files

Dump files are useful for detailed analysis but take up a lot of disk space

7. Now you are on the system service set up window. A system service allows KFSensor to run like a daemon on your system regardless of who is logged into it. You can change between users without affecting the system service. You must be logged in as the administrator to install the system service.  
 "Install as a system service" should be selected.

**Set Up Wizard - Systems Service**

☒ Install as systems service

A systems service is a special type of application that Windows runs in the background and is similar in concept to a UNIX daemon.

The KFSensor Server becomes independent of the logged on user, so you can log off and another person can log on without affecting the server.

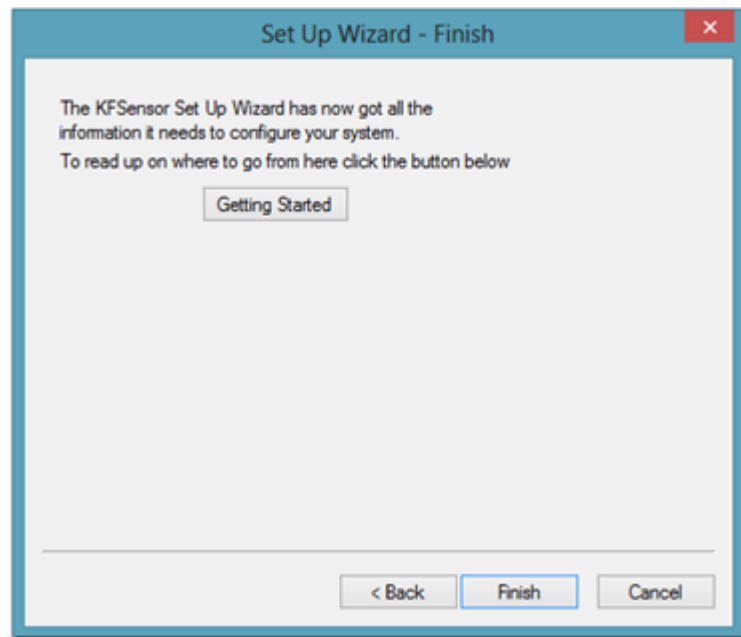
The KFSensor Server can be configured to start automatically when the systems starts, even before you log on.

You must be logged in a the Administrator to install a systems service.

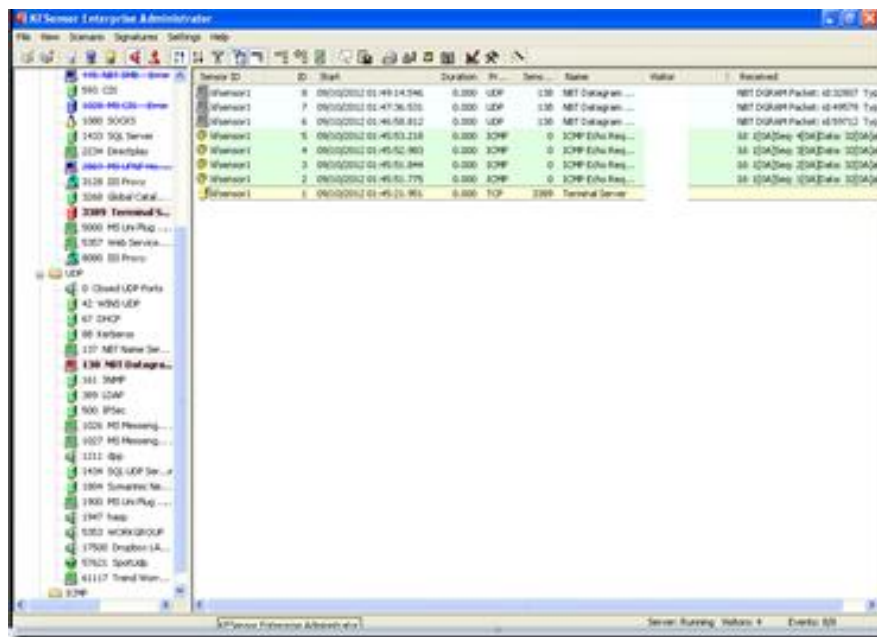
Wizard Help

< Back   Next >   Cancel

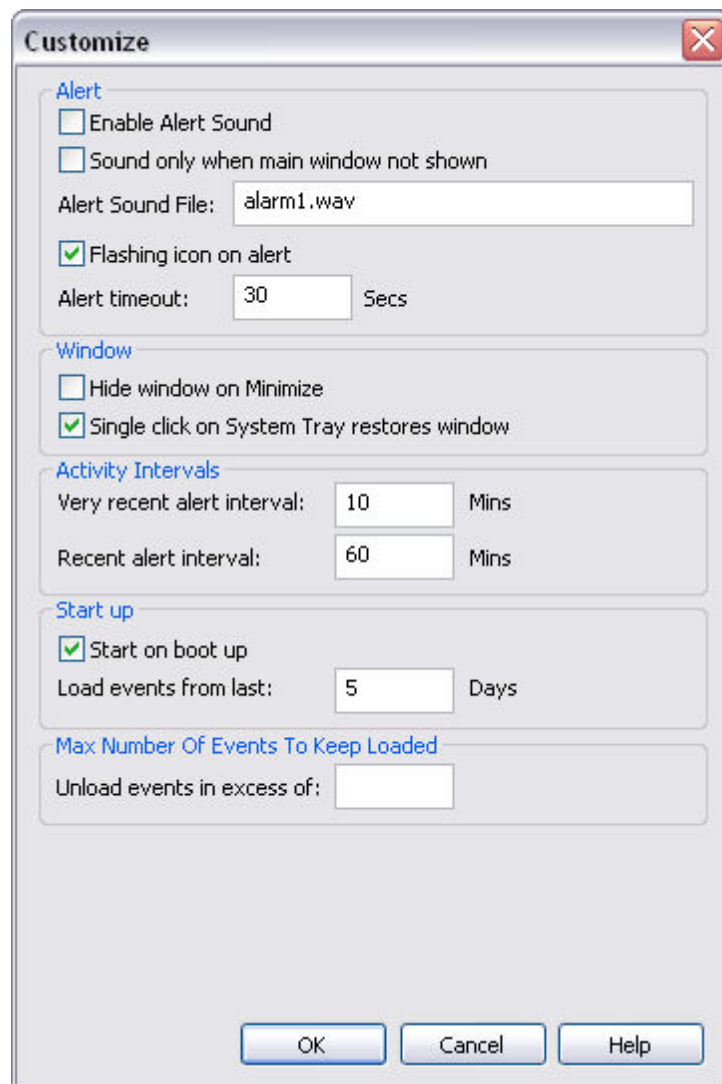
8. KFSensor should now be ready to configure your system. Click Finish.



After completing the setup wizard, you can see the KFSensor output by using the interactive GUI. Note: The “Visitor” filed contain the source IP/Host Name.



- Now we are going to customize KF Sensor. Select *Settings > Customize*. In this area you define the alert behavior, KFSensor window behavior, recent activity intervals, startup behavior and the maximum number of events to keep loaded. We definitely want to disable the audible alarm and we want to increase the number of events that are displayed when KFSensor starts up. Configure your KFSensor as shown next.



Click OK when you have set these configurations.

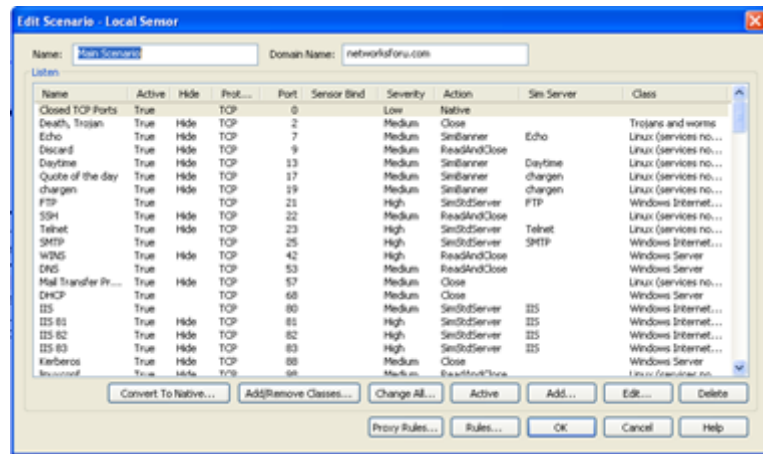
**10. Edit Active Scenario:** To create or modify rules, Scenario menu ->select the Edit Active Scenario command ->you will see a dialog box which contains a summary of all of the existing rules. Either select a rule and click the Edit button to edit a rule, or you can click the Add button to create a new rule.

#### **11. Adding a rule :**

- Click the Add button and you will see the Add Listen dialog box.
- The first thing that this dialog box asks for is a name. This is just a name for the rule.
- Pick something descriptive though, because the name that you enter is what will show up in the logs whenever the rule is triggered.

## 12. Convert to Native service:

- Convert the stroked off services as native services. \*Select Scenario ->Edit Active Scenario.
- Choose the respective service listed in the dialog box opened and press convert to native button and ok.



## 13. Setting up Server :

- To start the server, Settings-> Set Up Wizard, Go through the wizard, give fictitious mail ids when they are asked and start the server running by pressing the finish button.
- Kfsensor now start showing the captured information in its window.

## 14. FTP Emulation:

- Open command prompt and type
  - Ftp ipaddress
  - Enter user name anonymous
  - Enter any password
  - Get any file name with path
- Monitor this ftp access in KFSensor monitor
- Right click KFSensor entry, select Event details, see the details captured by the server
- Create visitor rule by right clicking the FTP entry and check either ignore / close under actions in the dialog box that opened.



- Now redo the above said operations at the command prompt and see how the emulation behaves.
- You can see/ modify the created rules in Scenario->edit active visitor rules.

#### 15. SMTP Emulation:

- open command prompt and type
  - telnet ipaddress 25
  - Helo
  - Mail from:<mail-id>
  - Rcpt to:<mail-id>
  - Data
  - type contents of mail end that with . in new line
- Check the kfsensor for the captured information.

#### 16. IIS emulation:

- Enable Telnet client, server, Internet Information server in Control Panel-> Programs-> Turn windows features on/off
  - Check Telnet client, Telnet server, IIS-> FTP (both options),
- Create an index.html, store it in c:\keyfocus\kfsensor\files\iis7\wwwroot
- Select scenario->edit simserver
  - Choose IIS and edit
  - Make sure index.html is in first place in the listed htm files in the dialog box
- Check the kfsensor for the captured information.

#### 17. DOS attack:

- Settings-> DOS attack settings modify (reduce) values in general tab, ICMP and other tabs. Press ok.
- Open command prompt and type
- Ping ipaddress -t or
- Ping -l 65000 ipaddress -t
- Check the kfsensor for the DOS attack alerts, open event details in right click menu for further details.