# Experiment Number: 5th

|  |  |
| --- | --- |
| **Student Name: Gautam Sharma** | **UID: 20BCS3548** |
| **Branch: CSE (Information Security)** | **Section & Group: 20BIS-1/A** |
| **Semester: 5** th | **Date: 10/11/** 2022 |
| **Course Name: Network Defence Essential Lab** | **Course Code: 20CSB-331** |

1. **Aim/Overview of the Practical:**

Detect Malicious Network Traffic using Honey BOT.

# Task to be Done:

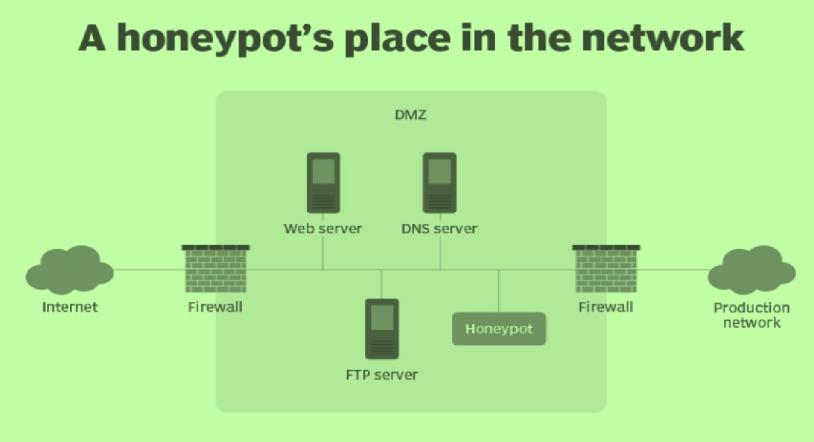
Configuring a Honeypot for your network using KF Sensor.

# Procedure:

Honeypot disguises itself as an actual server to give the false idea to the attackers and divert their attacks. Therefore, a honeypot should be set up just like the real server so that data can appear authentic by showing fake files, ports, directories, etc. As the honeypot creates the illusion of being legitimate; the attacker tends to believe that they have gained access

to the real deal.

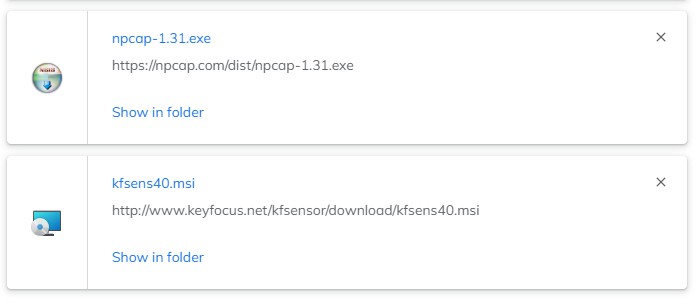
KFSensor is a honeypot for a windows system. it also acts as an IDS. Its job is to attract and detect all the attackers in the network, hence the name ‘Honeypot’. It does so by imitating a vulnerable environment and disguising itself as a server and this way, it succeeds to not only catching the attacker but also helping to know their motive.



# What KFSensor does?

* 1. Monitors all traffic
  2. Interacts with an attacker
  3. Alerts
  4. Statistical Analysis

We can download KFSensor from <http://www.keyfocus.net/kfsensor/>. The KFSensor download consists of a 1.7 MB self-extracting executable file.

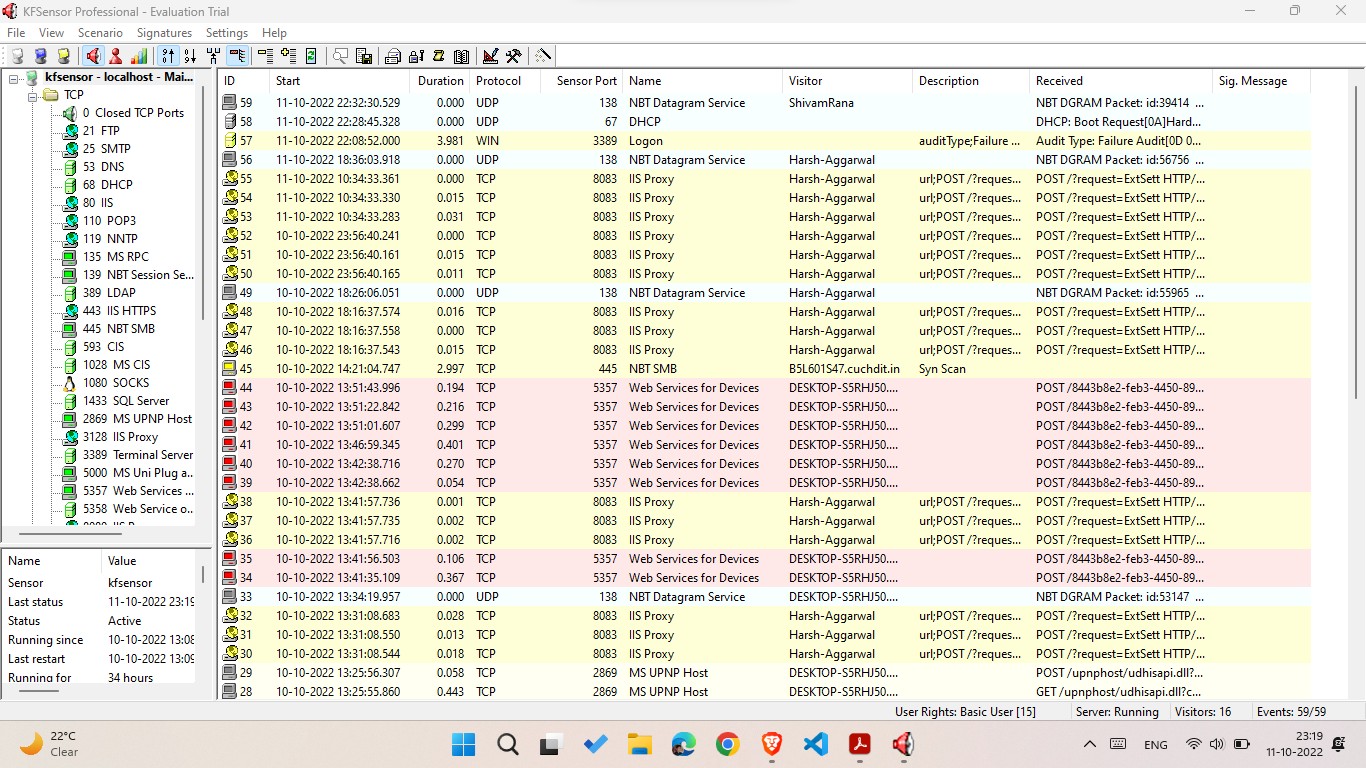


# Working of KFSensor

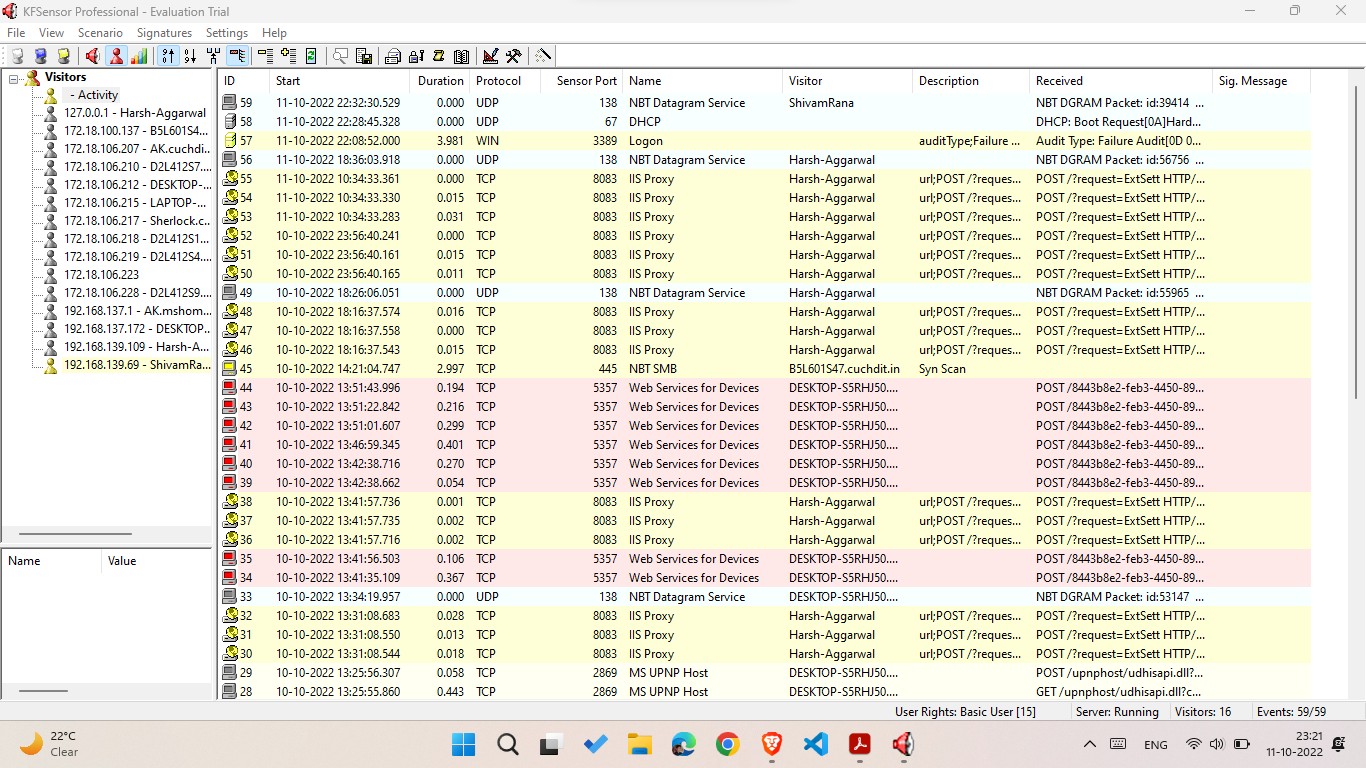
KFSensor’s role is to be a decoy server for the attackers in order to protect the real thing. It does its job perfectly by opening fake ports on the system where it’s installed and gathering the information when a connection is made.

When the Setup wizard closes, you will see the main KFSensor screen shown in Figure. As you can see, the column on the left contains a list of port numbers and what the port is typically used for. If the icon to the left of a port listing is green, it means that KFSensor actively monitors that port for attacks. If the icon is blue, it means that there has been an error and KFSensor is not watching for exploits aimed at that particular port.

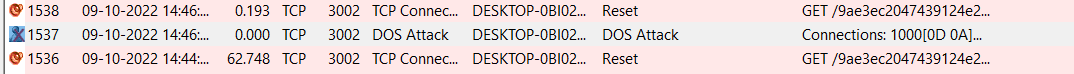
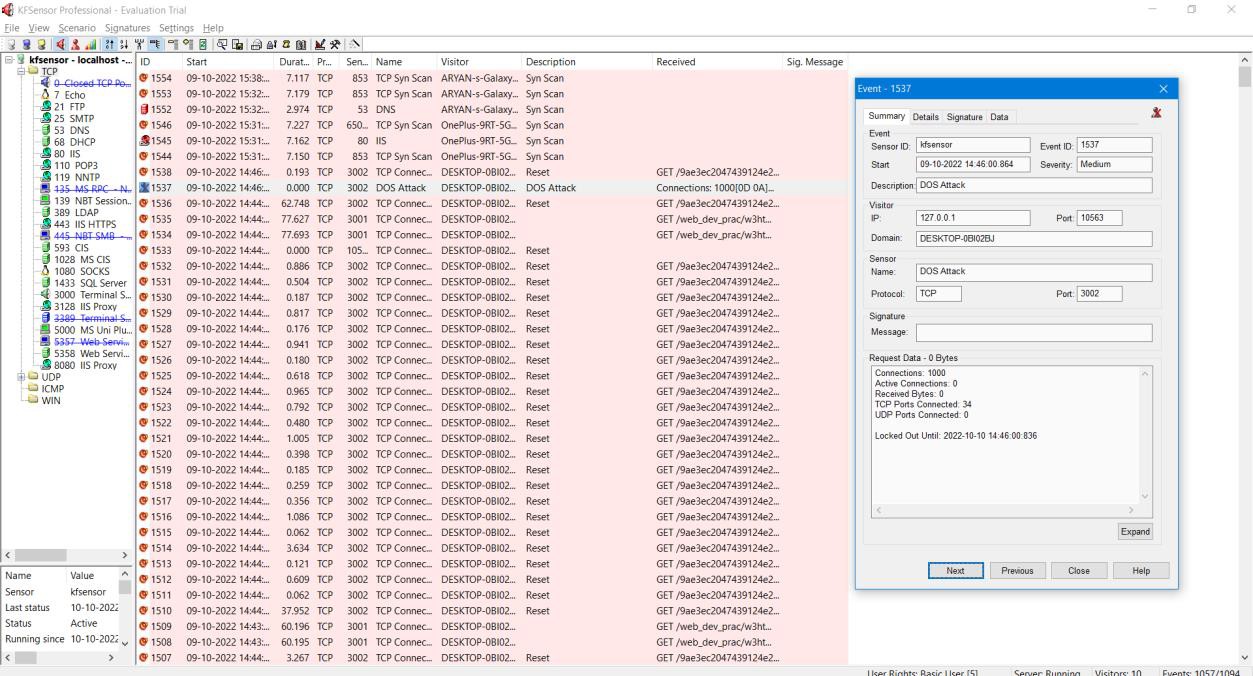
And in KFSensor it will show the details of the scan along with its IP. It will also generate an alarm to alert you.



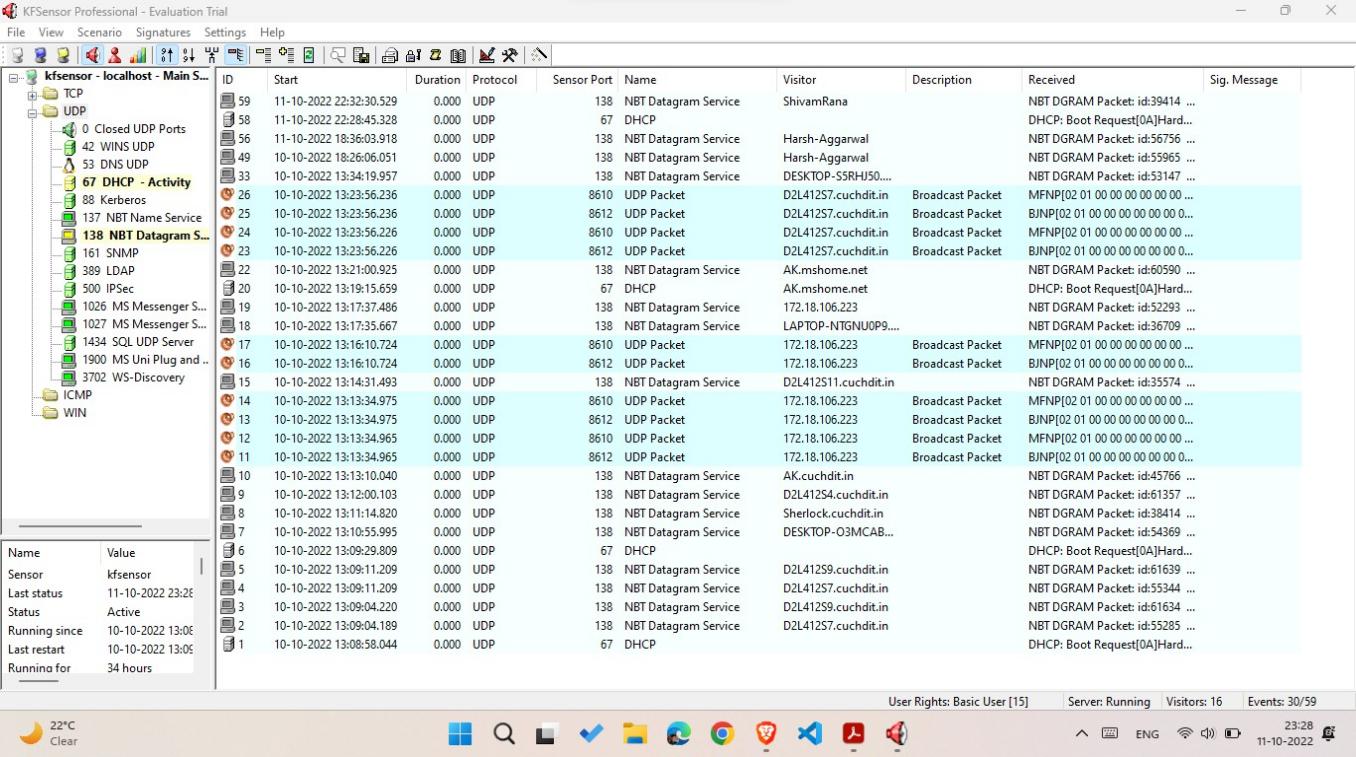
We can click on the visitor to check for visitors to the network



Under the TCP ports section we can check for any type of attack Like in this case a DOS attack is detected:

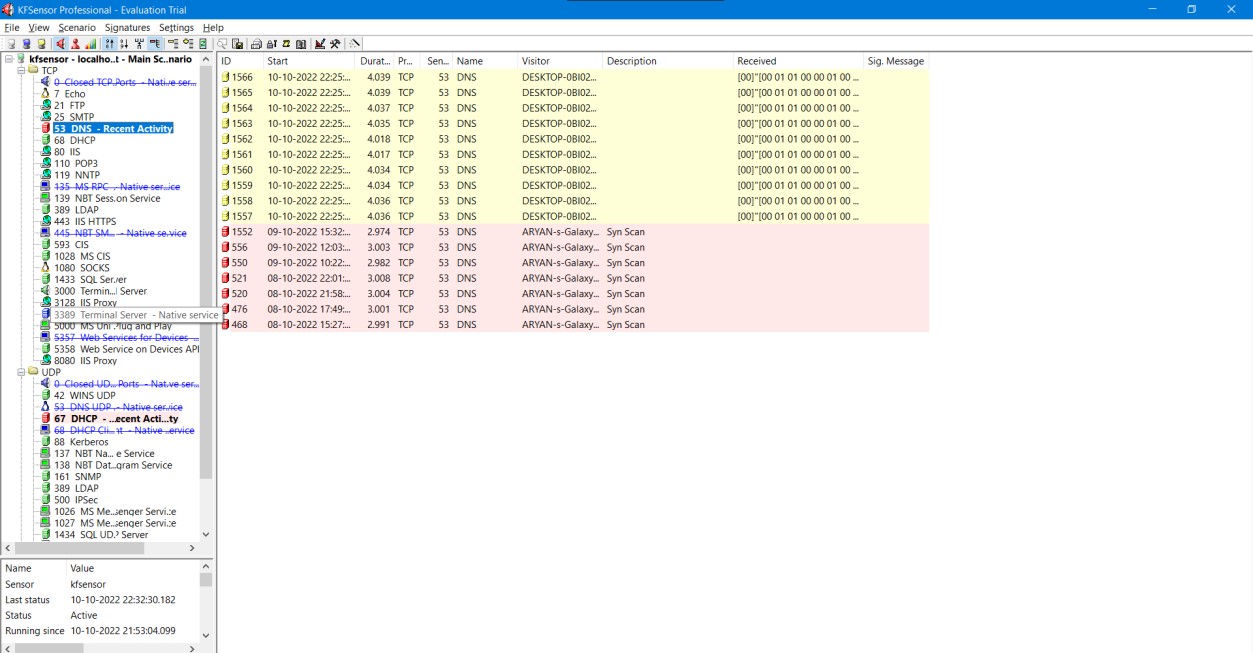


Under UDP Port we can check for any attack on UDP



The TCP/IP protocol suite is vulnerable to a variety of attacks ranging from password sniffing to denial of service. Software to carry out most of these attacks is freely available on the Internet. These vulnerabilities-unless carefully controlled-can place the use of the Internet or intranet at considerable risk. This article classifies a range of known attack methods focusing in particular on SYN flooding, IP spoofing, TCP sequence number attack, TCP session hijacking, RST and FIN attacks, and the Ping O' Death. The article concludes with an examination of the vulnerabilities of the common protocols carried by TCP/IP (including SMTP, Telnet, NTP, Finger, NFS, FTP, WWW, and X windows) and proposes configuration methods to limit their vulnerability.

We can even check for DNS RECENT ACTIVITY, FTP, TRANSFER OF ANY MAIL



# Learning Outcomes (What I have learnt):

1. Learned about Honeypots and Firewalls.
2. Learned about protocols and TCP, UDP, and FTP.
3. Practical Implementation of HONEYPOT.

**Evaluation Grid (Created as per the Assessment Model):**

|  |  |  |  |
| --- | --- | --- | --- |
| Sr. No. | Parameters | Marks Obtained | Maximum Marks |
| 1. | Worksheet completion |  | 8 |
| 2. | Conduct of Experiment |  | 12 |
| 3. | Quiz/Viva Voce |  | 10 |
|  | Total |  | 30 |