LAB ASSIGNMENT - 3

Name: Ashwin Balaji
Roll Number: 2020PMD4221
Course: M.Tech (Mobile Computing and Data Analytics)

Title: To study and work with KF SENSOR Intrusion Detection Tool. Setup a honeypot and monitor the honeypot on the network.

Software Requirements: Key Focus Sensor, WinPCap 5.1.31, NpCap 1.31

Theory:

An intrusion detection system (IDS) is a device or software application that monitors a network for malicious activity or policy violations. Any malicious activity or violation is typically reported or collected centrally using a security information and event management system. Some IDS's are capable of responding to detected intrusion upon discovery. These are classified as intrusion prevention systems (IPS).

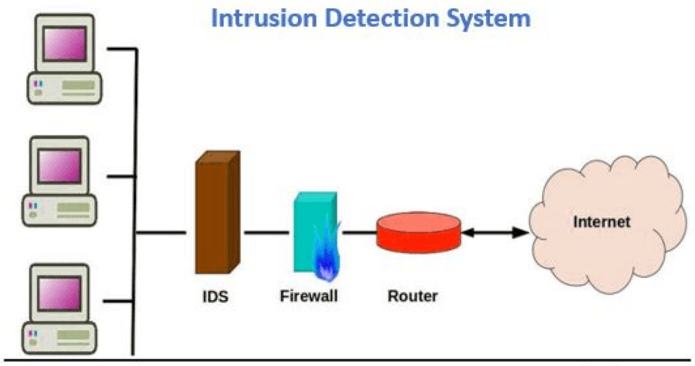
There is a wide array of IDS, ranging from antivirus software to tiered monitoring systems that follow the traffic of an entire network. The most common classifications are:

1. **Network intrusion detection systems (NIDS):** A system that analyzes incoming network traffic.
2. **Host-based intrusion detection systems (HIDS):** A system that monitors important operating system files.

There is also subset of IDS types. The most common variants are based on signature detection and anomaly detection.

3. **Signature-based:** Signature-based IDS detects possible threats by looking for specific patterns, such as byte sequences in network traffic, or known malicious instruction sequences used by malware. This terminology originates from antivirus software, which refers to these detected patterns as signatures. Although signature-based IDS can easily detect known attacks, it is impossible to detect new attacks, for which no pattern is available.
4. **Anomaly-based:** a newer technology designed to detect and adapt to unknown attacks, primarily due to the explosion of malware. This detection method uses machine learning to create a defined model of trustworthy activity, and then compare new behavior against this trust model. While this approach enables the detection of previously unknown attacks, it can suffer from false positives: previously unknown legitimate activity can accidentally be classified as malicious.

Modern networked business environments require a high level of security to ensure safe and trusted communication of information between various organizations. An intrusion detection system acts as an adaptable safeguard technology for system security after traditional technologies fail. Cyber-attacks will only become more sophisticated, so it is important that protection technologies adapt along with their threats.



Honeypots in network security are a way to trick attackers into investing time and effort exploiting deliberate vulnerabilities while alerting your internal security team of their compromise attempts. The information you receive from observing a live attack through security honeypots is much more detailed than what you get from some intrusion detection systems. And it also helps to keep cybercriminals from attacking your legitimate targets.

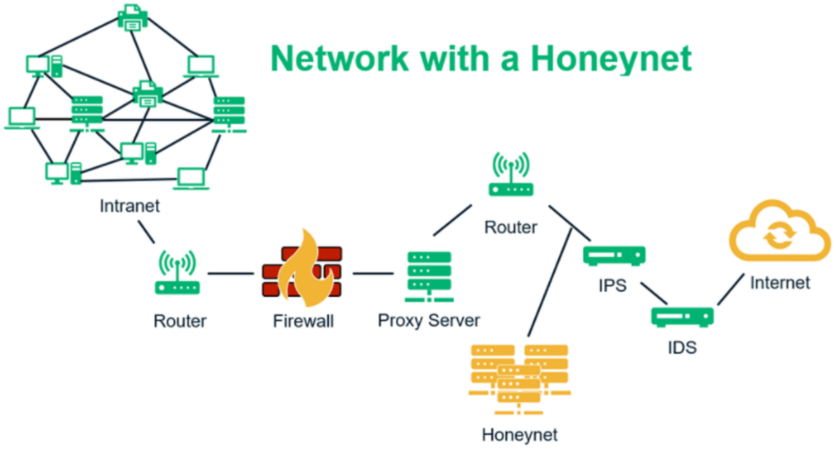
Moreover, a honeypot is a computer system that helps IT security pros observe and learn from cybercriminals' attacks by observing them in real time. Basically, it helps organizations detect unauthorized use or access to systems. It also helps them gain crucial information about attackers and how they operate. Of course, all of this occurs with the intruder being none the wiser about what's really happening. It may comprise of several components such as:

- Network devices
- Key-loggers
- Monitoring tools
- Packet analyzers
- Alerting tools

Honeypots help organizations:

- Assess the latest trends in attacks
- Understand where cyber-attacks arise
- Better frame security policies to mitigate future risks

This deceptive technology can be hardware-based (like an appliance) or software-based virtual honeypots that can scale and be set up to emulate a legitimate network.



A network of honeypots (honeynet) can be placed in different positions, for example — outside the external firewall, in the DMZ, or within the internal network. A honeynet has servers, networking devices, and systems that are similar to a legitimate network with fake data. Since the purpose is to lure attackers into exploiting intentionally vulnerable systems to monitor and study their activities, placing a honeynet on the internal network is risky business unless the attack can be trapped within it.

However, since more than 75% of security incidents occur due to insider threats, installing a honeypot with proper configurations to monitor user behavior on the internal network is often worth the risk. A honeypot on the internal network can detect misconfigured firewall settings and be useful in detecting zero-day exploits. All in all, installing honeypots can strengthen your organization's network security posture significantly.

Types of honeypots:

a) Research Honeypots

These honeypots are deployed and used by researchers to gain a better understanding of attack techniques, motivations, information about malware strains in the wild, and security vulnerabilities. This is done to specifically use the knowledge gained to make informed decisions about:

- Defense strategies,
- Patching prioritizations,
- Future security investments, and
- Identifying and developing new security solutions.

b) Production Honeypots

Production honeypots are placed within your organization's internal network with other production servers. Though the intention is similar in terms of gaining insights about active attacks, it is typically less complex than research honeypots with lesser data. It is primarily deployed to identify active attacks on the internal network and distract or misdirect hackers from attacking your legitimate servers.

Advantages of Honeypots:

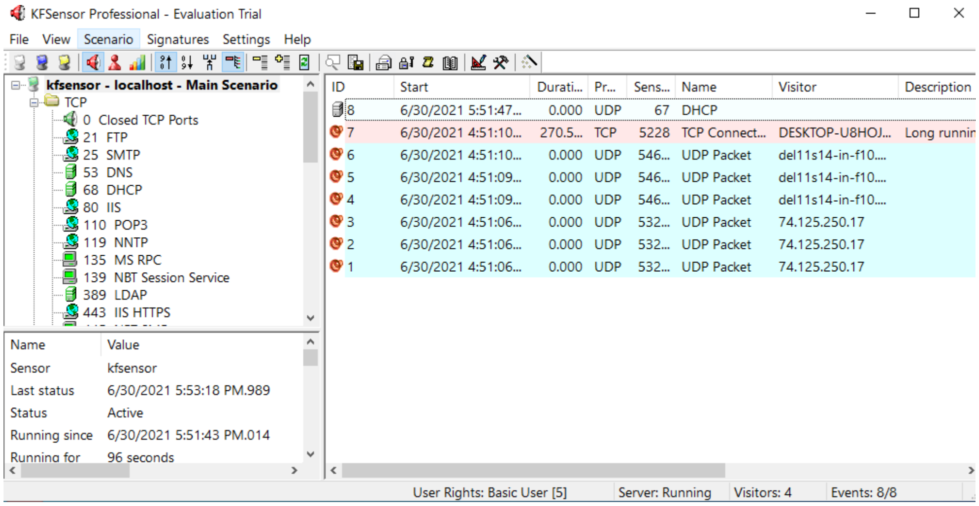
- Distracts cybercriminals from targeting legitimate systems. The more time and effort they spend on the honeypot, the less they have to invest in attacking your organization's real network and systems.
- Gives you greater visibility of attacks as they're happening. Logs an attacker's keystrokes during a session and share instant alerts whenever there is an attempted access to the system.
- Monitors an attacker's behaviors and detect zero-day vulnerabilities. An IDS/IPS, on the other hand, relies on already published signatures to identify an attack.
- Puts your organization's incident response capabilities to the test. Does your team know how to take appropriate countermeasures to block the attacker's access to legitimate servers?
- Helps to improve your organization's overall security. A honeypot shines a light on the types of adversaries and attacks in the wild so that you can formulate appropriate prevention strategies.

Disadvantages of Honeypots:

- Perhaps one of the primary downsides with using honeypots is that it may introduce additional risks into your environment. A compromised honeypot that's not isolated effectively may be used launch an attack on the real network.
- Another major drawback of using honeypots is that it can only detect an intrusion when it is attacked directly. However, if an attacker identifies the honeypot for what it is, they can evade the system and infiltrate the network.
- Additionally, attackers may be able to fingerprint a honeypot (i.e. identify honeypots) based on certain specific characteristics such as misspelt error messages and so on. They can launch false attacks to distract administrators and while the organization chases these alerts, the attacker can focus on orchestrating a real attack.

Procedure:

1. Download and install KF Sensor, WinPcap and NpCap.
2. Restart the machine, KF Sensor starts automatically.


KFSensor Professional - Evaluation Trial
File View Scenario Signatures Settings Help

```
kfsensor - localhost - Main Scenario
  TCP
    0  Closed TCP Ports
    21  FTP
    25  SMTP
    53  DNS
    68  DHCP
    80  IIS
    110  POP3
    119  NNTP
    135  MS RPC
    139  NBT Session Service
    389  LDAP
    443  IIS HTTPS
```

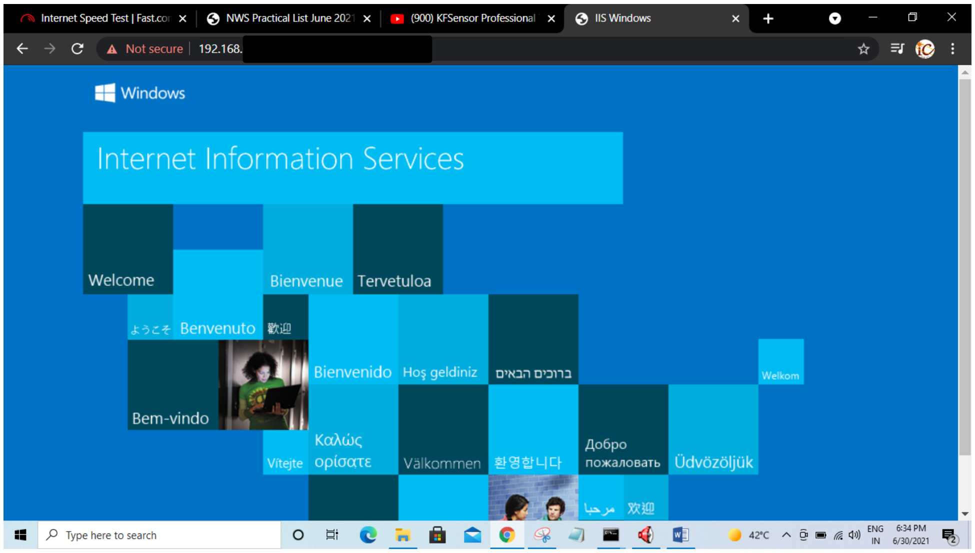
Name	Value
Sensor	kfsensor
Last status	6/30/2021 5:53:18 PM.989
Status	Active
Running since	6/30/2021 5:51:43 PM.014
Running for	96 seconds

ID	Start	Durati...	Pr...	Sens...	Name	Visitor	Description
8	6/30/2021 5:51:47...	0.000	UDP	67	DHCP		
7	6/30/2021 4:51:10...	270.5...	TCP	5228	TCP Connect...	DESKTOP-U8HOJ...	Long runnin
6	6/30/2021 4:51:10...	0.000	UDP	546...	UDP Packet	del11s14-in-f10....	
5	6/30/2021 4:51:09...	0.000	UDP	546...	UDP Packet	del11s14-in-f10....	
4	6/30/2021 4:51:09...	0.000	UDP	546...	UDP Packet	del11s14-in-f10....	
3	6/30/2021 4:51:06...	0.000	UDP	532...	UDP Packet	74.125.250.17	
2	6/30/2021 4:51:06...	0.000	UDP	532...	UDP Packet	74.125.250.17	
1	6/30/2021 4:51:06...	0.000	UDP	532...	UDP Packet	74.125.250.17	

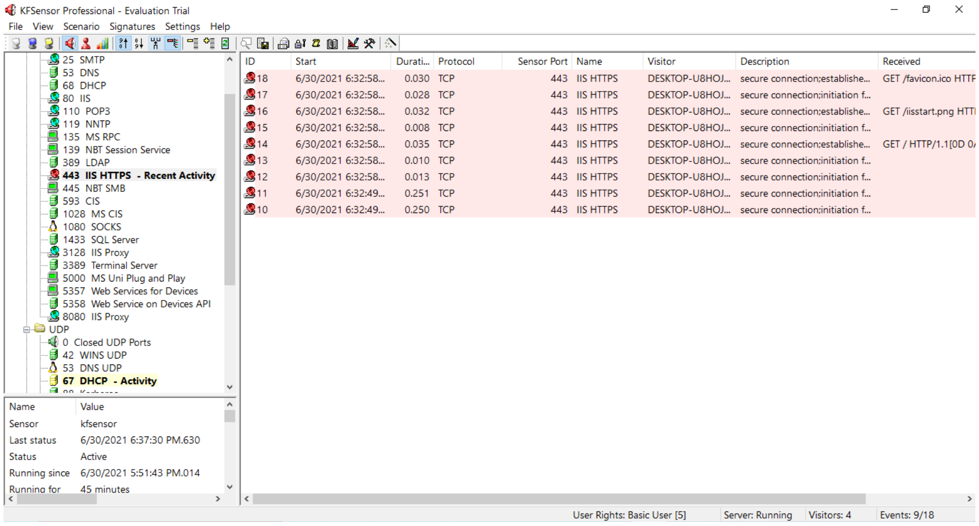
User Rights: Basic User [5] Server: Running Visitors: 4 Events: 8/8

3. Ping the machine to check packet flow:
   a) To identify machine ip-address **C:\Users\win-10>ipconfig**
   b) **C:\Users\win-10>ping <ip-address>**

4) Enter **https://<ip-address>** in browser to generate packet request.



5) Immediately you will see red color symbols in **HTTPS RECENT ACTIVITY at port number** which is mentioned.


KFSensor Professional - Evaluation Trial
File View Scenario Signatures Settings Help

25 SMTP
53 DNS
68 DHCP
80 IIS
110 POP3
119 NNTP
135 MS RPC
139 NBT Session Service
389 LDAP
443 IIS HTTPS - Recent Activity
445 NBT SMB
593 CIS
1028 MS CIS
1080 SOCKS
1433 SQL Server
3128 IIS Proxy
3389 Terminal Server
5000 MS Uni Plug and Play
5357 Web Services for Devices
5358 Web Service on Devices API
8080 IIS Proxy
UDP
0 Closed UDP Ports
42 WINS UDP
53 DNS UDP
67 DHCP - Activity

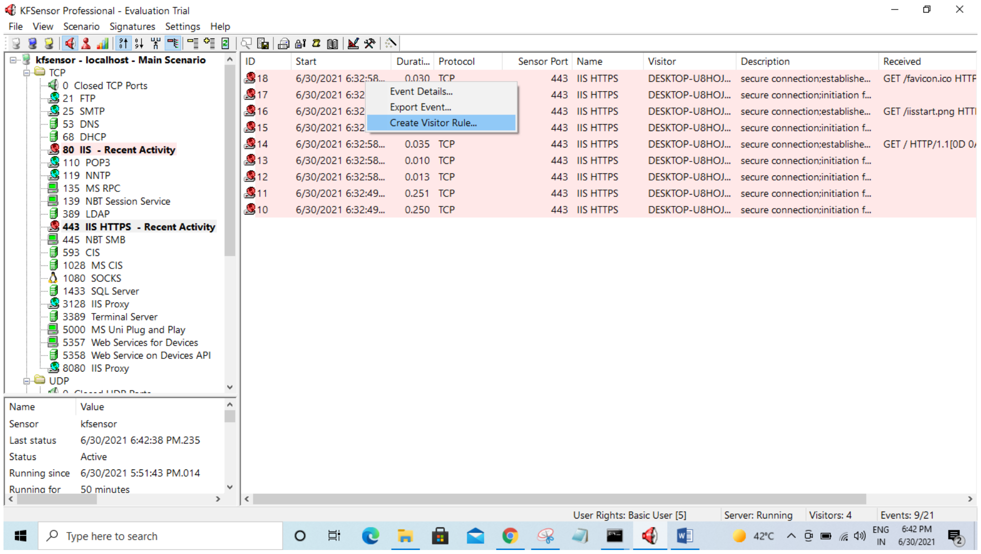
Name	Value
Sensor	kfsensor
Last status	6/30/2021 6:37:30 PM.630
Status	Active
Running since	6/30/2021 5:51:43 PM.014
Running for	45 minutes

ID	Start	Durati...	Protocol	Sensor Port	Name	Visitor	Description	Received
18	6/30/2021 6:32:58...	0.030	TCP	443	IIS HTTPS	DESKTOP-U8HOJ...	secure connection;establishe...	GET /favicon.ico HTTP
17	6/30/2021 6:32:58...	0.028	TCP	443	IIS HTTPS	DESKTOP-U8HOJ...	secure connection;initiation f...	
16	6/30/2021 6:32:58...	0.032	TCP	443	IIS HTTPS	DESKTOP-U8HOJ...	secure connection;establishe...	GET /iisstart.png HTTI
15	6/30/2021 6:32:58...	0.008	TCP	443	IIS HTTPS	DESKTOP-U8HOJ...	secure connection;initiation f...	
14	6/30/2021 6:32:58...	0.035	TCP	443	IIS HTTPS	DESKTOP-U8HOJ...	secure connection;establishe...	GET / HTTP/1.1[0D 0/
13	6/30/2021 6:32:58...	0.010	TCP	443	IIS HTTPS	DESKTOP-U8HOJ...	secure connection;initiation f...	
12	6/30/2021 6:32:58...	0.013	TCP	443	IIS HTTPS	DESKTOP-U8HOJ...	secure connection;initiation f...	
11	6/30/2021 6:32:49...	0.251	TCP	443	IIS HTTPS	DESKTOP-U8HOJ...	secure connection;initiation f...	
10	6/30/2021 6:32:49...	0.250	TCP	443	IIS HTTPS	DESKTOP-U8HOJ...	secure connection;initiation f...	

User Rights: Basic User [5] Server: Running Visitors: 4 Events: 9/18

6) We can **add visitor rules** to restrict the traffic as per the desire.

7) **Right Click on the event -> Create Visitor Rule**.



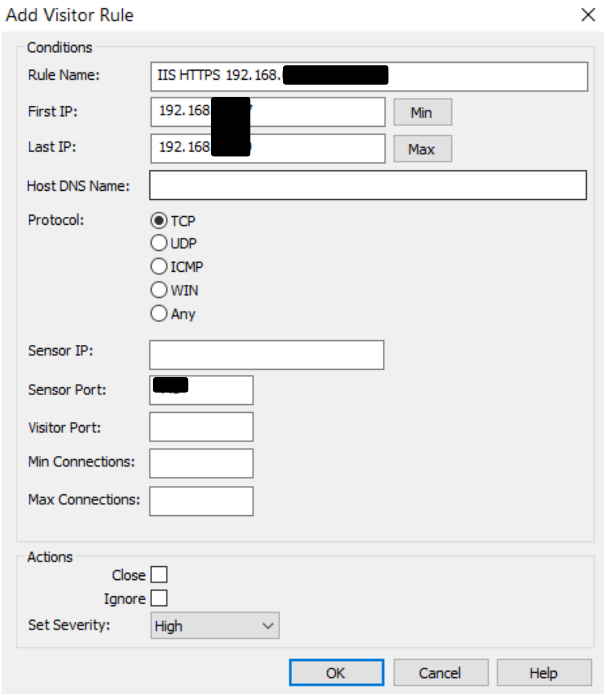
kfsensor - localhost - Main Scenario
TCP
0 Closed TCP Ports
21 FTP
25 SMTP
53 DNS
68 DHCP
80 IIS - Recent Activity
110 POP3
119 NNTP
135 MS RPC
139 NBT Session Service
389 LDAP
443 IIS HTTPS - Recent Activity
445 NBT SMB
593 CIS
1028 MS CIS
1080 SOCKS
1433 SQL Server
3128 IIS Proxy
3389 Terminal Server
5000 MS Uni Plug and Play
5357 Web Services for Devices
5358 Web Service on Devices API
8080 IIS Proxy
UDP

Name	Value
Sensor	kfsensor
Last status	6/30/2021 6:42:38 PM.235
Status	Active
Running since	6/30/2021 5:51:43 PM.014
Running for	50 minutes

ID	Start	Durati...	Protocol	Sensor Port	Name	Visitor	Description	Received
18	6/30/2021 6:32:58...	0.030	TCP	443	IIS HTTPS	DESKTOP-U8HOJ...	secure connection;establishe...	GET /favicon.ico HTTP
17	6/30/2021 6:32			443	IIS HTTPS	DESKTOP-U8HOJ...	secure connection;initiation f...	
16	6/30/2021 6:32			443	IIS HTTPS	DESKTOP-U8HOJ...	secure connection;establishe...	GET /iisstart.png HTTI
15	6/30/2021 6:32			443	IIS HTTPS	DESKTOP-U8HOJ...	secure connection;initiation f...	
14	6/30/2021 6:32:58...	0.035	TCP	443	IIS HTTPS	DESKTOP-U8HOJ...	secure connection;establishe...	GET / HTTP/1.1[0D 0/
13	6/30/2021 6:32:58...	0.010	TCP	443	IIS HTTPS	DESKTOP-U8HOJ...	secure connection;initiation f...	
12	6/30/2021 6:32:58...	0.013	TCP	443	IIS HTTPS	DESKTOP-U8HOJ...	secure connection;initiation f...	
11	6/30/2021 6:32:49...	0.251	TCP	443	IIS HTTPS	DESKTOP-U8HOJ...	secure connection;initiation f...	
10	6/30/2021 6:32:49...	0.250	TCP	443	IIS HTTPS	DESKTOP-U8HOJ...	secure connection;initiation f...	

User Rights: Basic User [5] Server: Running Visitors: 4 Events: 9/21

8) **Ports, Ip address or severity level, incoming packet type to be signalled etc. can be added to implement IDS rules**. Moreover we can also **identify the source of packet** and the **time at which the packet detected by honeypot**.



Add Visitor Rule

Conditions

Rule Name: IIS HTTPS 192.168.[redacted]

First IP: 192.168[redacted]

Last IP: 192.168[redacted]

Host DNS Name:

Protocol:
● TCP
○ UDP
○ ICMP
○ WIN
○ Any

Sensor IP:

Sensor Port: [redacted]

Visitor Port:

Min Connections:

Max Connections:

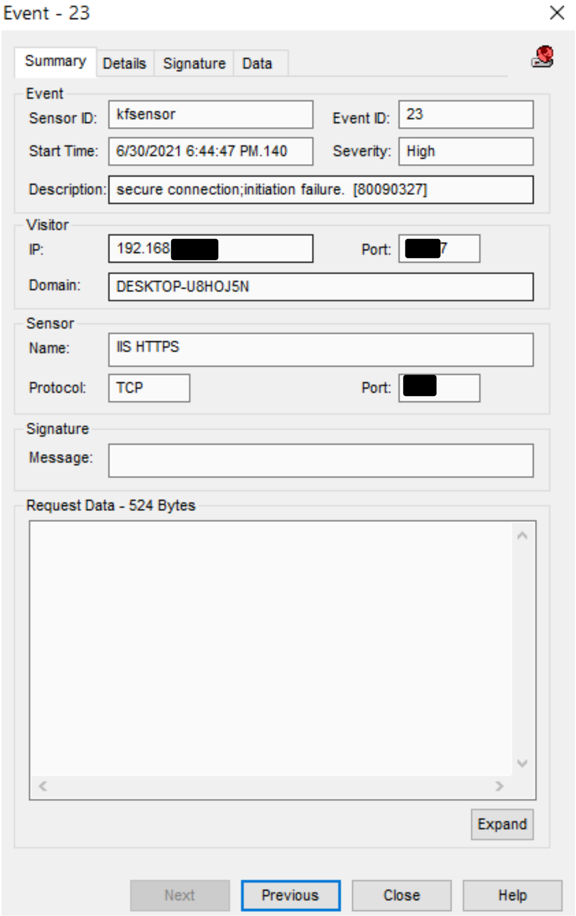
Actions

Close □

Ignore □

Set Severity: High

9) We can see that the **dummy request for the ip-address has been acknowldged and marked as severe** based on the rules we have set.



Event

Sensor ID: kfsensor Event ID: 23

Start Time: 6/30/2021 6:44:47 PM.140 Severity: High

Description: secure connection;initiation failure. [80090327]

Visitor

IP: 192.168[redacted] Port: [redacted]7

Domain: DESKTOP-U8HOJ5N

Sensor

Name: IIS HTTPS

Protocol: TCP Port: [redacted]

Signature

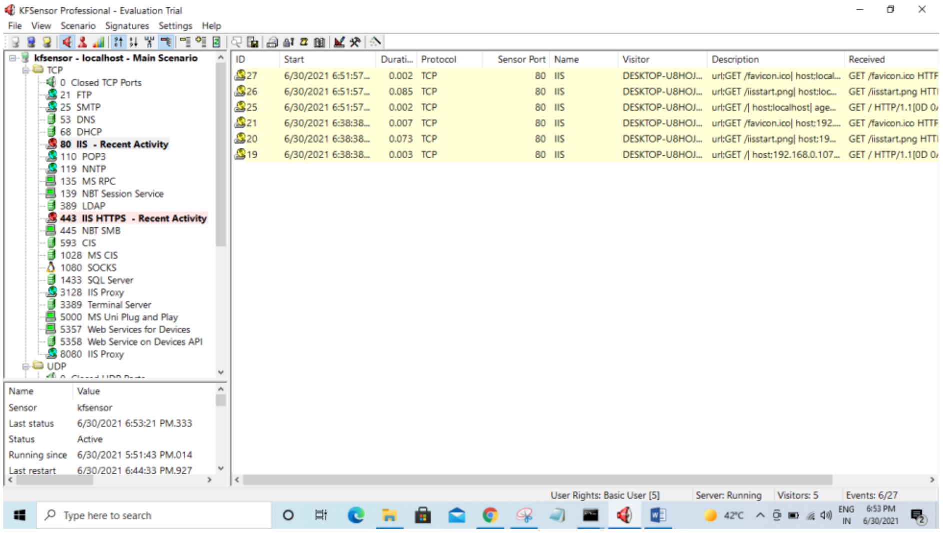
Message:

Request Data - 524 Bytes

10) Similarly it can be tried for various connections like **FTP, HTTP, localhost 127.0.0.1** etc.

11) Checked for http://localhost, for example, **ID: 27** been marked as yellow at port 80 having a TCP request.

12) To **change the severity of request or change the type of traffic to be analysed** at next iteration, we may need to edit visitor rules.



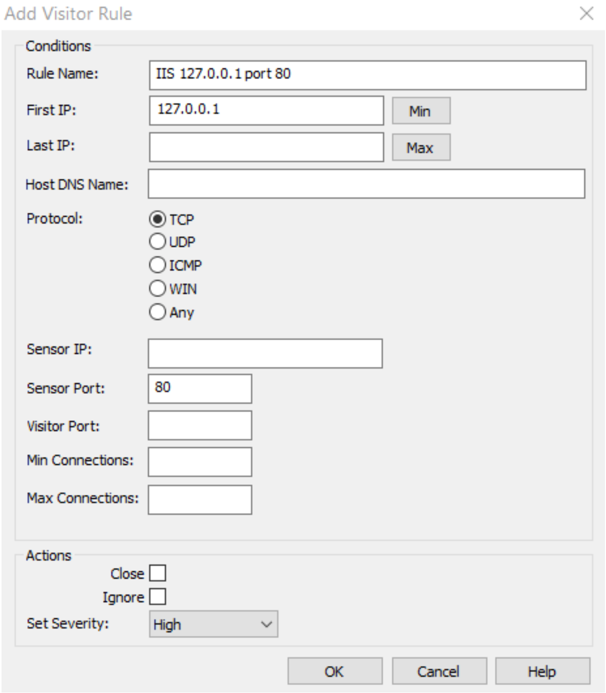
kfsensor - localhost - Main Scenario
- TCP
  - 0 Closed TCP Ports
  - 21 FTP
  - 25 SMTP
  - 53 DNS
  - 68 DHCP
  - **80 IIS - Recent Activity**
  - 110 POP3
  - 119 NNTP
  - 135 MS RPC
  - 139 NBT Session Service
  - 389 LDAP
  - **443 IIS HTTPS - Recent Activity**
  - 445 NBT SMB
  - 593 CIS
  - 1028 MS CIS
  - 1080 SOCKS
  - 1433 SQL Server
  - 3128 IIS Proxy
  - 3389 Terminal Server
  - 5000 MS Uni Plug and Play
  - 5357 Web Services for Devices
  - 5358 Web Service on Devices API
  - 8080 IIS Proxy
- UDP

Name	Value
Sensor	kfsensor
Last status	6/30/2021 6:53:21 PM.333
Status	Active
Running since	6/30/2021 5:51:43 PM.014
Last restart	6/30/2021 6:44:33 PM.927

ID	Start	Durati...	Protocol	Sensor Port	Name	Visitor	Description	Received
27	6/30/2021 6:51:57...	0.002	TCP	80	IIS	DESKTOP-U8HOJ...	url;GET /favicon.ico| host;local...	GET /favicon.ico HTTF
26	6/30/2021 6:51:57...	0.085	TCP	80	IIS	DESKTOP-U8HOJ...	url;GET /iisstart.png| host;loc...	GET /iisstart.png HTTI
25	6/30/2021 6:51:57...	0.002	TCP	80	IIS	DESKTOP-U8HOJ...	url;GET /| host;localhost| age...	GET / HTTP/1.1[0D 0/
21	6/30/2021 6:38:38...	0.007	TCP	80	IIS	DESKTOP-U8HOJ...	url;GET /favicon.ico| host;192....	GET /favicon.ico HTTF
20	6/30/2021 6:38:38...	0.073	TCP	80	IIS	DESKTOP-U8HOJ...	url;GET /iisstart.png| host;19...	GET /iisstart.png HTTI
19	6/30/2021 6:38:38...	0.003	TCP	80	IIS	DESKTOP-U8HOJ...	url;GET /| host;192.168.0.107...	GET / HTTP/1.1[0D 0/

User Rights: Basic User [5] Server: Running Visitors: 5 Events: 6/27

13) **Right click on ID 27 -> Create Visitor rule.**



Add Visitor Rule

Conditions

Rule Name: IIS 127.0.0.1 port 80

First IP: 127.0.0.1

Last IP:

Host DNS Name:

Protocol: ● TCP ○ UDP ○ ICMP ○ WIN ○ Any

Sensor IP:

Sensor Port: 80

Visitor Port:

Min Connections:

Max Connections:

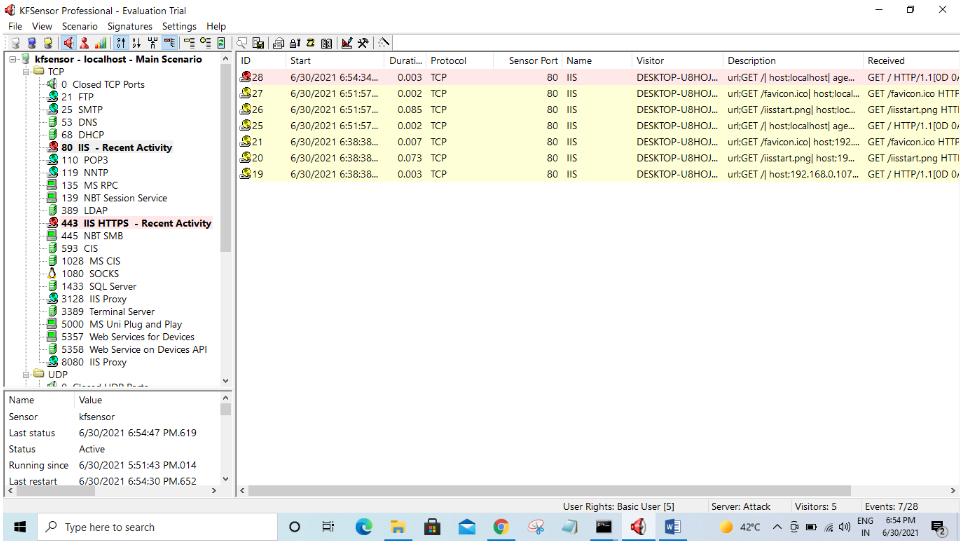
Actions

Close □

Ignore □

Set Severity: High

14) Since we kept the **severity as high** (from the default value), the **symbol changes from yellow to red to signify high severity packet request**, when pinged for localhost again.



KFSensor Professional - Evaluation Trial

kfsensor - localhost - Main Scenario

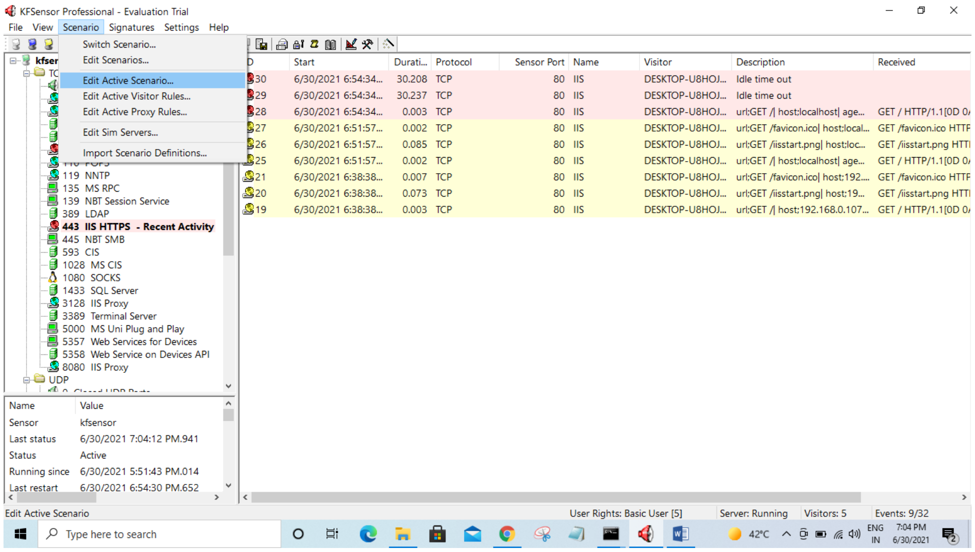
TCP
0 Closed TCP Ports
21 FTP
25 SMTP
53 DNS
68 DHCP
80 IIS - Recent Activity
110 POP3
119 NNTP
135 MS RPC
139 NBT Session Service
389 LDAP
443 IIS HTTPS - Recent Activity
445 NBT SMB
593 CIS
1028 MS CIS
1080 SOCKS
1433 SQL Server
3128 IIS Proxy
3389 Terminal Server
5000 MS Uni Plug and Play
5357 Web Services for Devices
5358 Web Service on Devices API
8080 IIS Proxy
UDP

Name	Value
Sensor	kfsensor
Last status	6/30/2021 6:54:47 PM.619
Status	Active
Running since	6/30/2021 5:51:43 PM.014
Last restart	6/30/2021 6:54:30 PM.652

ID	Start	Durati...	Protocol	Sensor Port	Name	Visitor	Description	Received
28	6/30/2021 6:54:34...	0.003	TCP	80	IIS	DESKTOP-U8HOJ...	url;GET /| host;localhost| age...	GET / HTTP/1.1[0D 0/
27	6/30/2021 6:51:57...	0.002	TCP	80	IIS	DESKTOP-U8HOJ...	url;GET /favicon.ico| host;local...	GET /favicon.ico HTTF
26	6/30/2021 6:51:57...	0.085	TCP	80	IIS	DESKTOP-U8HOJ...	url;GET /iisstart.png| host;loc...	GET /iisstart.png HTTI
25	6/30/2021 6:51:57...	0.002	TCP	80	IIS	DESKTOP-U8HOJ...	url;GET /| host;localhost| age...	GET / HTTP/1.1[0D 0/
21	6/30/2021 6:38:38...	0.007	TCP	80	IIS	DESKTOP-U8HOJ...	url;GET /favicon.ico| host;192....	GET /favicon.ico HTTF
20	6/30/2021 6:38:38...	0.073	TCP	80	IIS	DESKTOP-U8HOJ...	url;GET /iisstart.png| host;19...	GET /iisstart.png HTTI
19	6/30/2021 6:38:38...	0.003	TCP	80	IIS	DESKTOP-U8HOJ...	url;GET /| host;192.168.0.107...	GET / HTTP/1.1[0D 0/

User Rights: Basic User [5]   Server: Attack   Visitors: 5   Events: 7/28

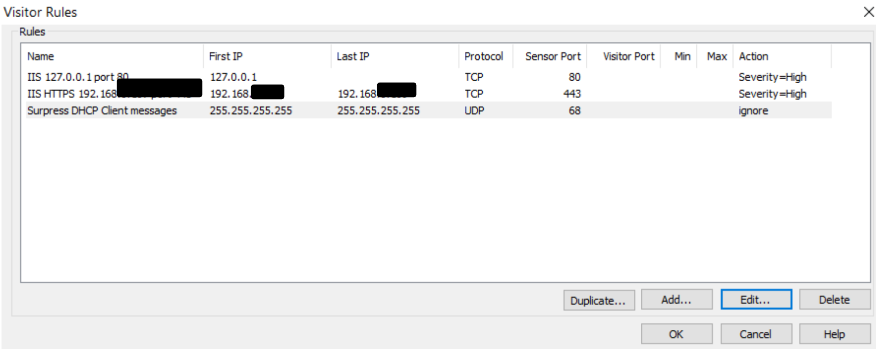
15) Click **Scenario -> Edit Active Scenario**, we can see the various rules we have added to protect the network.



D	Start	Durati...	Protocol	Sensor Port	Name	Visitor	Description	Received
30	6/30/2021 6:54:34...	30.208	TCP	80	IIS	DESKTOP-U8HOJ...	Idle time out	
29	6/30/2021 6:54:34...	30.237	TCP	80	IIS	DESKTOP-U8HOJ...	Idle time out	
28	6/30/2021 6:54:34...	0.003	TCP	80	IIS	DESKTOP-U8HOJ...	url;GET /| host;localhost| age...	GET / HTTP/1.1[0D 0/
27	6/30/2021 6:51:57...	0.002	TCP	80	IIS	DESKTOP-U8HOJ...	url;GET /favicon.ico| host;local...	GET /favicon.ico HTTP
26	6/30/2021 6:51:57...	0.085	TCP	80	IIS	DESKTOP-U8HOJ...	url;GET /iisstart.png| host;loc...	GET /iisstart.png HTTI
25	6/30/2021 6:51:57...	0.002	TCP	80	IIS	DESKTOP-U8HOJ...	url;GET /| host;localhost| age...	GET / HTTP/1.1[0D 0/
21	6/30/2021 6:38:38...	0.007	TCP	80	IIS	DESKTOP-U8HOJ...	url;GET /favicon.ico| host;192....	GET /favicon.ico HTTP
20	6/30/2021 6:38:38...	0.073	TCP	80	IIS	DESKTOP-U8HOJ...	url;GET /iisstart.png| host;19...	GET /iisstart.png HTTI
19	6/30/2021 6:38:38...	0.003	TCP	80	IIS	DESKTOP-U8HOJ...	url;GET /| host;192.168.0.107...	GET / HTTP/1.1[0D 0/

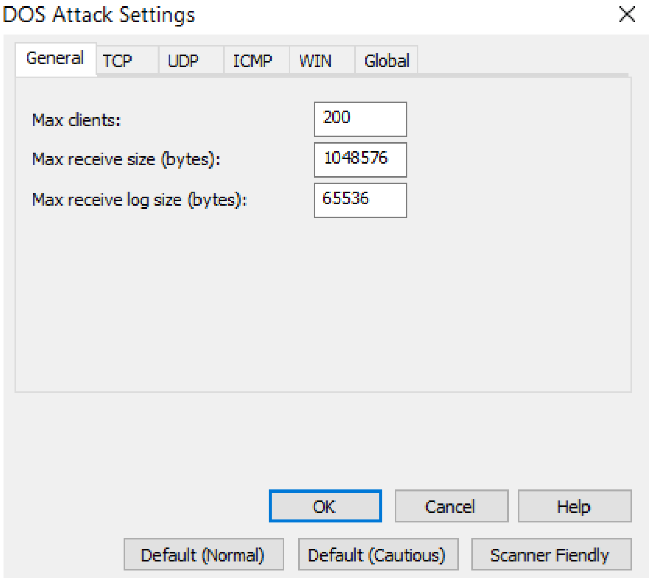
Name	Value
Sensor	kfsensor
Last status	6/30/2021 7:04:12 PM.941
Status	Active
Running since	6/30/2021 5:51:43 PM.014
Last restart	6/30/2021 6:54:30 PM.652

Edit Active Scenario   User Rights: Basic User [5]   Server: Running   Visitors: 5   Events: 9/32



Name	First IP	Last IP	Protocol	Sensor Port	Visitor Port	Min	Max	Action
IIS 127.0.0.1 port 80 [redacted]	127.0.0.1		TCP	80				Severity=High
IIS HTTPS 192.168[redacted]	192.168.[redacted]	192.168[redacted]	TCP	443				Severity=High
Surpress DHCP Client messages	255.255.255.255	255.255.255.255	UDP	68				ignore

16) We can also **edit the rules to prevent DOS attacks.**



Max clients: 200

Max receive size (bytes): 1048576

Max receive log size (bytes): 65536

***** In this way various types of packets can be analyzed using honeypots IDS *****