**Module 12**

**Evading IDS, Firewalls, and Honeypots**

**IDS, IPS, Firewall and Honeypots**

As an Ethical Hacker we should know how these Network device work like design of firewall, IDS, IPS and function of these device how it is protecting the Organization.

**IDS (Intrusion Detection System )**

Intrusion Detection system is a security software and hardware device which is used by organization to monitor, and protect his system and network from malicious activity. It detect the suspicious activity like security breach or malicious activity. It also match the activity with intrusion pattern, as pattern match it automatically raise the alarm . IDS are extremely powerful and usefull for organization as it has the feature of monitoring the network and system.

**Main function of IDS**

IDS also work as a packet sniffer, which also intercepts the packet.

IDS analyzes the packet after capture it.

IDS analyze the network and system, identify possible security breach and intrusion.

IDS analyzes the traffic of TCP/IP and suspects the intrusion and raises the alarm after detecting intrusion.

**IPS (Intrusion Prevention System)**

Intrusion Prevention System is also known as active of IDS(intrusion detection System). IPS has capability of detecting intrusion as well as it also prevents system and network. It continuously monitoring the system from behind the Firewall. As IDS is passive in network but IPS is an active in network because it is kept inline in the network between the client and server so it can actively analyze the network and make automatic decision by detecting intrusion or detecting any malicious activity in traffic.

**Main Function of IPS**

IPS generate alert alarm as soon as it find any abnormal traffic in the network or on the system.

It records the network activity in real-time logs.

IT automatically blocks and filter malicious traffic.

It also detects and eliminates threat quickly by itself.

**Advantage of IPS**

IPS is active in network and it can block the illegal packet and also drop it from the network..

IPS also used to monitor the traffic in real time.

IPS can prevent the direct attack in the network by controlling and monitoring the network traffic.

**Fire Wall**

Firewall is a software and hardware based system. It is placed at the network gateway and between of two network to protect the organization from unauthorize access from user. It examine all message of network whatever getting in or getting out on the intranet and it also block those message if it will not meet the requirement of security.

A firewall always placed at the network level and it work close with the route so it can analyze all network packet, determine the packet from where it is coming and whether to forward the packet to its destination. Always placed the Firewall away from the other network so no malicious request access the private network directly .

**We can configure window firewall like we can set inbond & outbond rules**.

**Step :** Go to the control panel> select window defender> select advance setting >

Know here we can set rules according to us in outbond we can block the outgoing service like Microsoft edge, chrome, opera etc.

In inbond we can allow any service which may not configured or restricted to use.

**Advantage of FireWall**

A firewall can detect the intrusion that is specially designed for organization.

Firewall can be modified according to the organization policy.

A firewall can be configured to block the incoming traffic of POP and SMTP

In Firewall consist of all logs of logging information that notify the administrator about all various services which was attempt by user to access

Firewall can verifies the traffic of incoming and outgoing and act as a router to move data between network.

Firewall can denies the request if it was found malicious.

**Types of FireWall**

**Hardware FireWall**

Hardware Firewall is a device it is placed on the network gateway. A hardware firewall protect the network and system and work very affectively, it also do packet filtering and read the header of packet to find the source and destination address. It has predefined rule whether to forward the packet or drop the packet, if packet doesn’t meet the security requirement it drop the packet.



Both are cisco firewall .

**Advantage of Hardware Firewall**

**Security:** A hardware Firewall reduce the risk of operating system and increase the level of security.

**Speed:** Hardware firewall regulate faster responses and enable the more traffic .

**Minimal Interface:** Hardware firewall is stand-alone network device for this reason it gives better management. It can be shut down, move from one place to another or can be reconfigured.

**Disadvantage of Hardware Firewall**

It is costly

Difficult to implement and configure.

Consumes more spaces and involves cabling.

**Software firewall**

Software hardware is filtering the network . It is placed between the regular used application and network component of operating system (OS). It is very help full for separate user and mobile user who need digital security when working out side of corporate. It is easy to install on individual PC. It protect the system from trojan and email worm everyday. It also analyze the data of OS.

**Advantages of Software Hardware**

Less expensive than hardware firewalls.

Easy for personal and home use.

Easy for configure and reconfigure.

**Disadvantages of Software Hardware**

Consume system resources

Difficult to unistall

Not appropriate for faster responses

**HONEYPOT**

Honeypot is a computer system mechanism which trap the cybercriminal. Basically it create fake proxy over the network, when attacker try to exploit that proxy it send alert to VICTIM. At Honeypot there has no authorize activity, does not have any production value and any traffic. If any attacker come and try to access the network, every key stroke of attacker and attack report was send to the victim. As other network device honeypot is different, it not solve any specific problem but it is very useful tool for preventing the attack, detecting attack, and information gathering .

**Type of Honeypot**

**Low-interaction Honey pot**

Low-interaction Honey pot analyze very limited number of services and application of a target system or network

Low-interaction honeypot is use to observe attacks against TCP and UDP services.

**Medium-interaction Honey pot**

Medium-interaction honey pot analyze the real operating system and network as well as application and services.

Medium-interaction honey pot is capable to analyze the log and more complex attack.

**High-interaction Honey pot**

As we seen above two type of honey pot, this honey pot doesn’t analyze any packet.

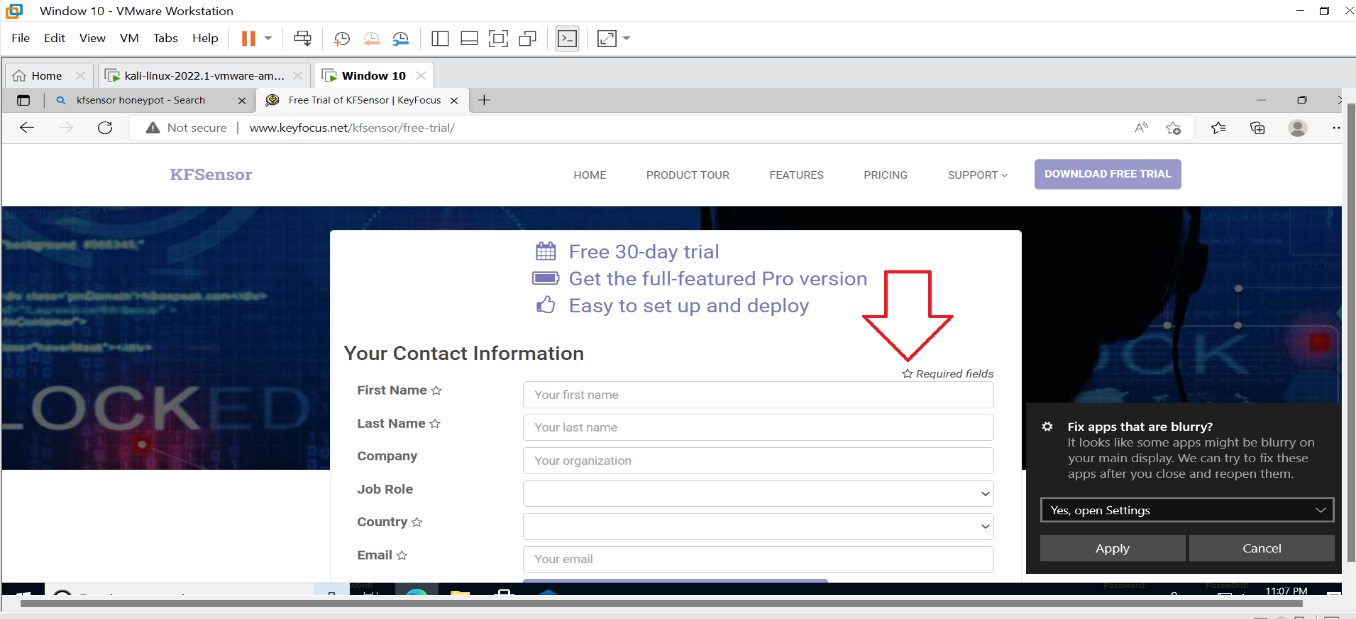
High-interaction honey pot run actual vulnerable server which can be completely compromised by attacker to gain full access.

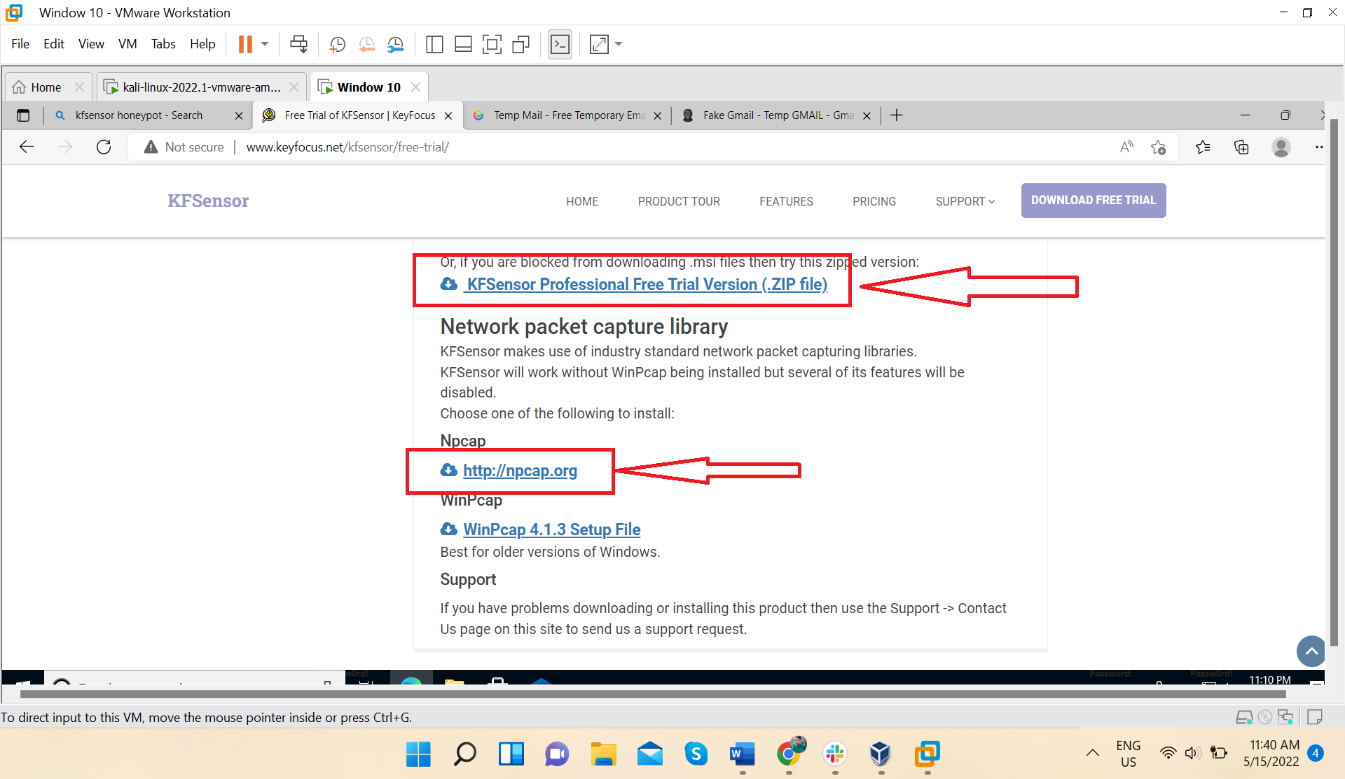
Lets install Honey Pot name is KFSenor

Source :- <http://www.keyfocus.net/kfsensor/free-trial/>

Fill the detail and download it professional zip file and also download ncap file

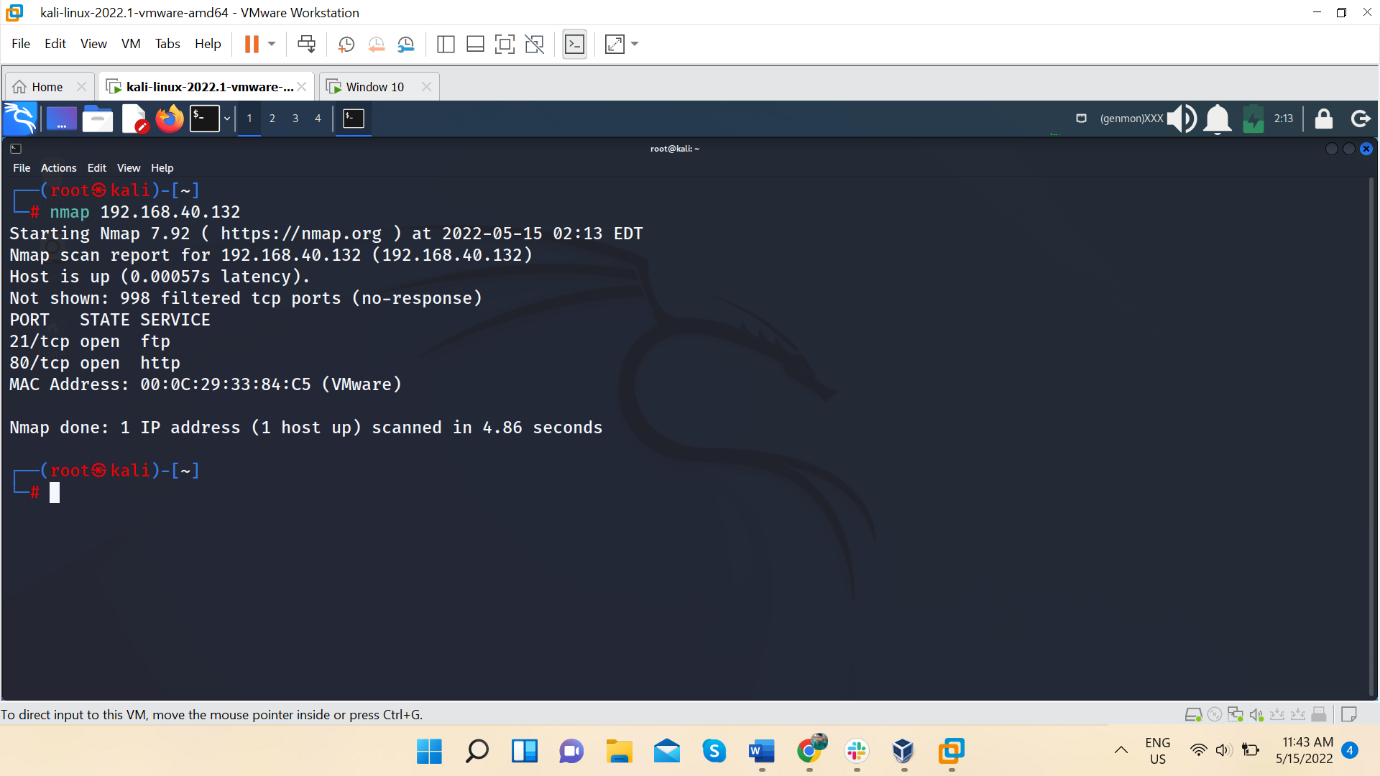
At the time filling of detail no need to fill it correctly, you can fill it wrong detail and use temp gmail.



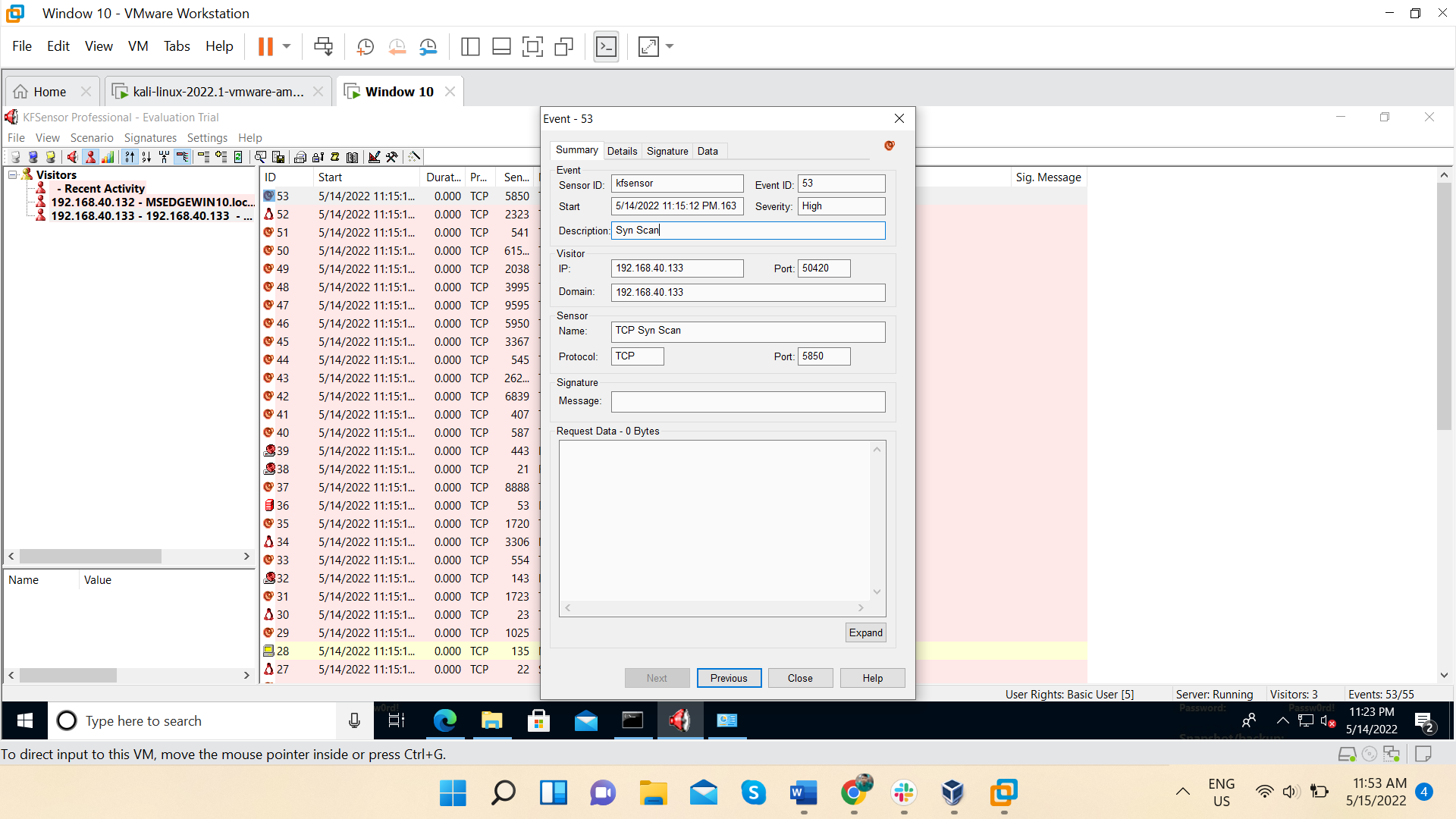


Download this two file & install it.

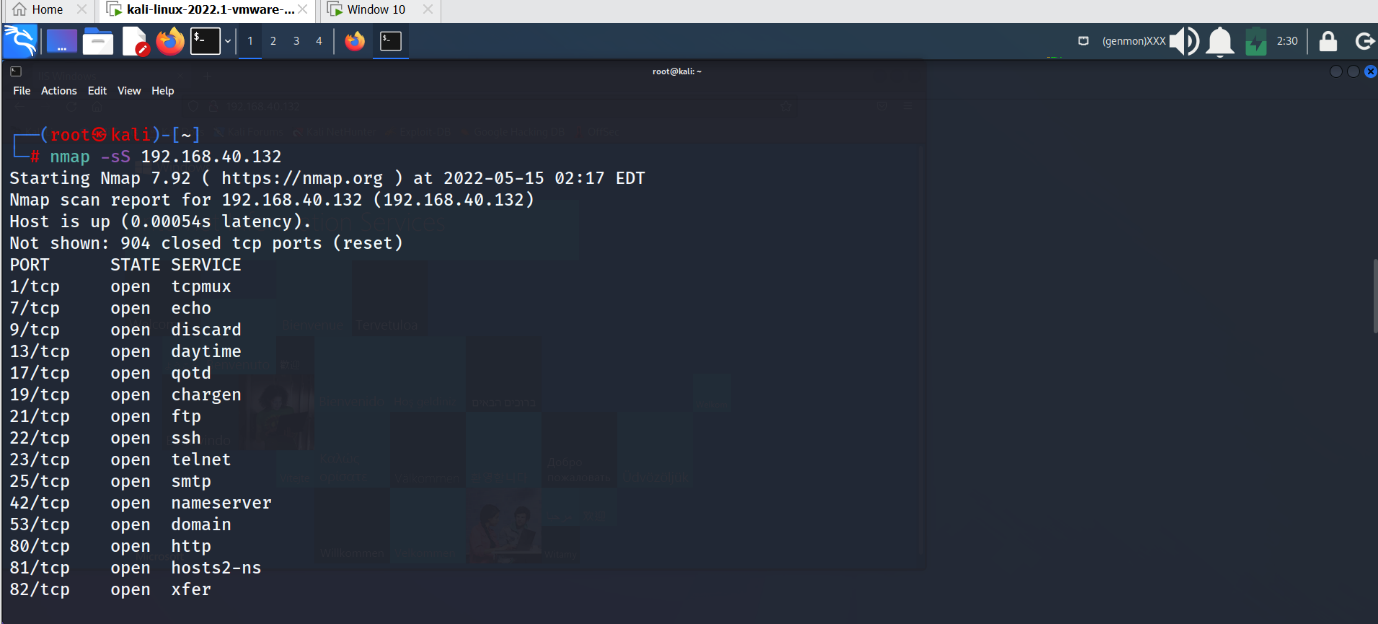
Before installing KFSensor lets run nmap against this system and see the result.



Now lets install and run KFSensor

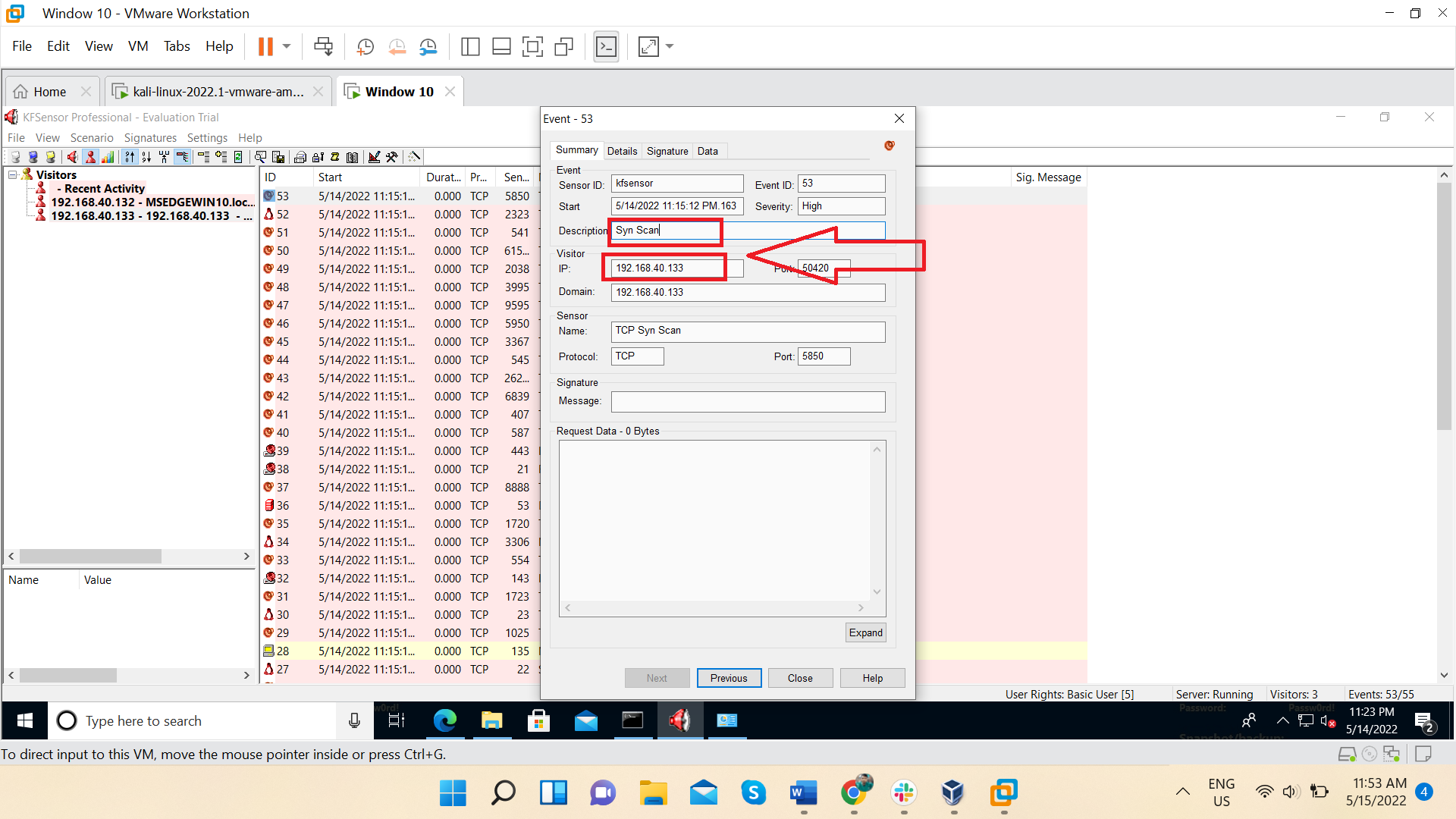


Now again lets run nmap against this system



This is a small list many more open ports are there.

All activity is recorded by KFSensor what ever we had done against window system



It is clearly recorded that which type of scan we run against this system.

This is the power of HONEYPOT