ICT 320 Computer Systems Project
Box Hill Institute

‘INTRUSION MONITORING AND THREAT PREVENTION’

Lecturer: Mr. Umesh Patel

Guide: Mr. David Brooks

Group Project by:

1. Ching Nung Teresa Chan S10049017
2. Anish Niure S10086062
3. Kavindu Perera S10094765
4. Jeetendra Subedar S10092964

Date: 21st November 2022

Table of Contents

Executive Summary:

Corporates and large entities today are striving hard to cope with the security loopholes and focusing mainly on safeguarding the data and information from attackers and hackers. These businesses have to upgrade their technology as it is not a one-time process. The hackers will keep trying to intrude their systems and data with new ways and methods. The recent examples we can consider are Medibank and Optus. Though they follow a strong security protocol, the attackers still managed to hack their database which resulted in millions of customers data being compromised. This is the main reason as to why the business have to continuously monitor their systems, data, and network from being hacked. The network administrators can use SIEM tools to monitor any unusual traffic and any attempt from the attackers to gain access to the network. This project focuses on some of the SIEM tools and monitoring techniques.

What is SIEM?

SIEM stands for Security Information and Event Management. Put simply, SIEM is a security solution that helps organizations recognize potential security threats and vulnerabilities before they have a chance to disrupt business operations. It surfaces user behavior anomalies and uses artificial intelligence to automate many of the manual processes associated with threat detection and incident response and has become a staple in modern-day security operation centers (SOCs) for security and compliance management use cases [1].

The Team and Stakeholders:

1. Jeetendra Subedar –Project Manager, ELK Analyst
2. Anish Niure – Network Admin
3. Teresa Chan – ELK Analyst
4. Kavindu Perera – Splunk Analyst

Team Goals:

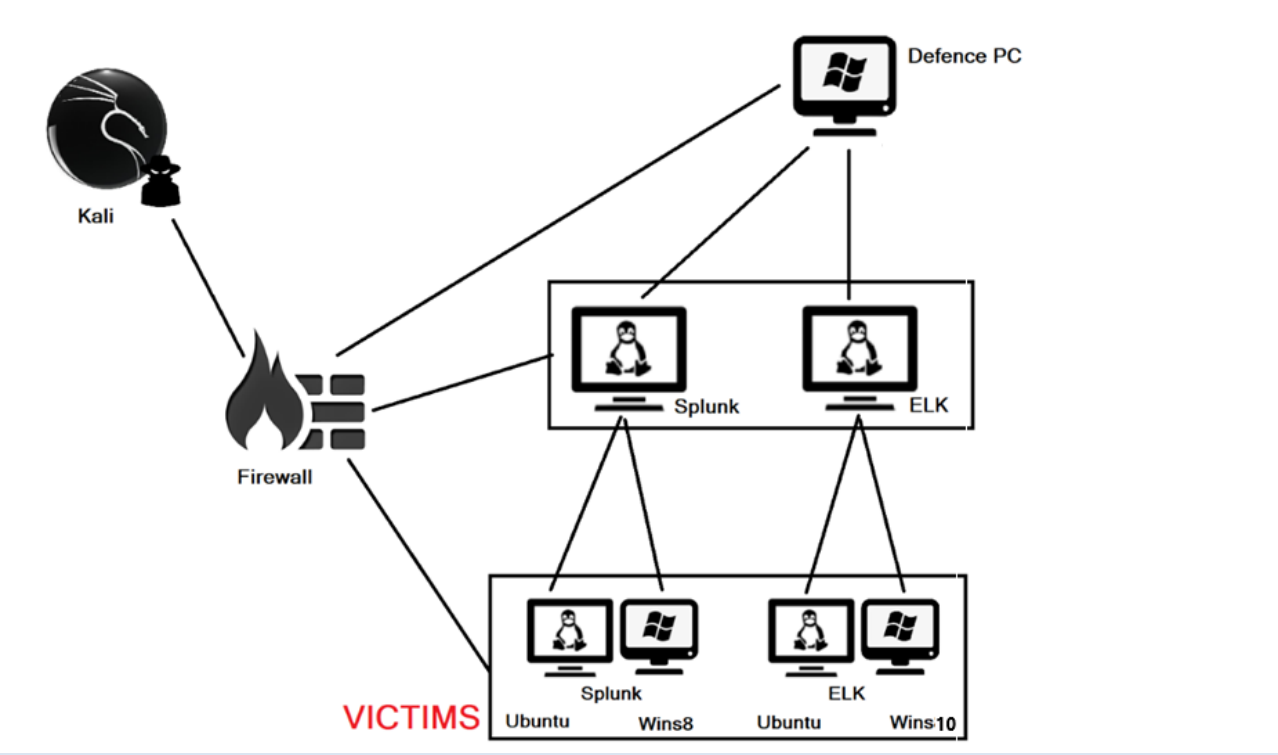
1. To identify the project and project requirements.
2. Budget and gather the resources.
3. To identify the required skill, skill gaps and learn the required skills.
4. To acquire the knowledge and understanding of the technology involved.
5. To design, implement and demonstrate the intrusion monitoring system.
6. To keep track of project improvement and deadlines.
7. To create and submit weekly meeting reports.
8. To overcome the challenges and obstacles
9. To design affordable turn-key solutions to enterprises and entities.

Product Scope:

The project was originally designed in a virtual environment to demonstrate the working of the SIEMs. The main components include:

1. VMware Workstation 16 Pro
2. OS – Linux, PFsense, Ubuntu, Win8 and Win10
3. SIEM – Splunk and ELK

The topology:



Addressing Table:

The virtual environment was established with the systems and IP addresses configured as per the following addressing scheme

Device Name	IP Address
Kali	172.10.10.10
Firewall	192.168.10.11 172.10.10.20
Defence PC	192.168.10.1
Splunk	192.168.10.2
Elastic Stack	192.168.10.3
Victim_Splunk_Ubuntu	192.168.10.5
Victim_Splunk_Wins8	192.168.10.6
Victim_ELK_Ubuntu	192.168.10.7
Victim_ELK_Wins10	192.168.10.8

Networking:

Resources used - Virtual Machines – Kali Linux, Windows 10, PFsense

VMware Workstation or any hypervisor.

The overall goal of this part is to make the connection between the external network and internal LAN network.

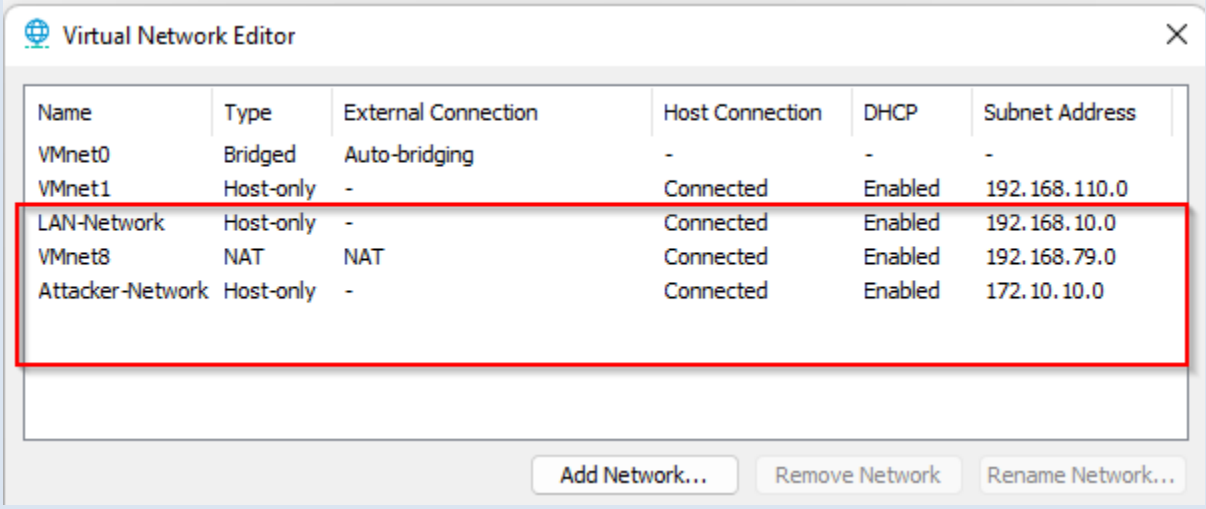
In this part we will need the three interfaces in our PFsense, The minimum number of interfaces that a PFsense has are two. WAN and LAN interfaces are the primary interfaces and PFsense is the intermediary device in between [2]. PFsense provides a lot of features other than firewall, one of the most features are Routing, with this flexibility, I will create two Internal Networks, and one WAN network. One internal LAN, I will name as Attacker-Network another internal Network named as LAN- Network. Attacker-Network will be acting as the external network for LAN-Network. I will connect my WAN interface to NAT mode from my hypervisior and configure my WAN interface to connect to Internet via my Host PC which is connected to my Home Router. I will test connectivity to internet from my LAN-Network and Attacker-Network. Finally, I will set up firewall rule for the Attacker-Network and LAN-Network.

If we see our overall lab we have different systems in our LAN-Network. User Computers, SIEM server, Defense Machine. In this part, I will take Defense Machine and configure networking. I will then configure DHCP server in my PFsense to distribute the IP address to Victim Machines.

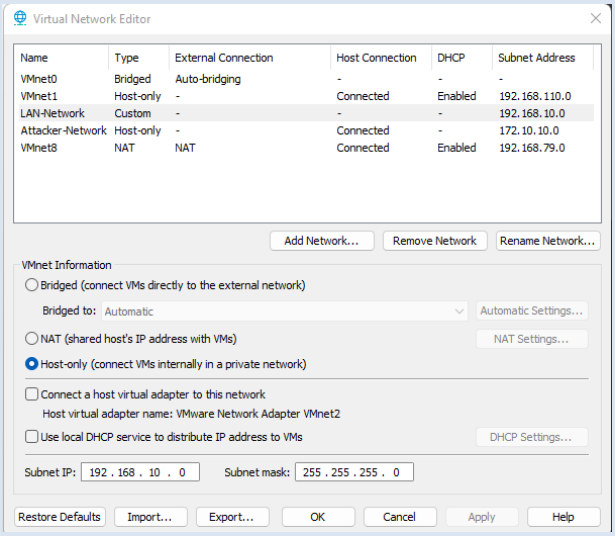
Setting up VMware Networks:

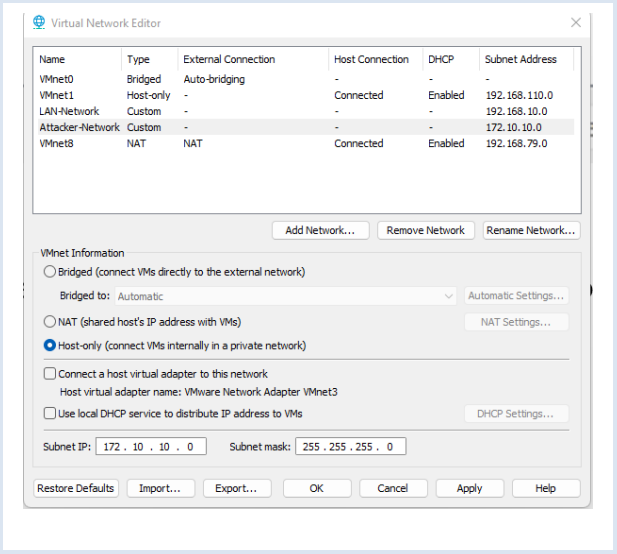
In VMware workstation we will create two custom Host only network (vmnet2 and vmnet3), which will be used as the LAN-network and Attacker Network respectively. I will use NAT Mode for internet connection to the outside world, from the default NAT network adapter in my vmware workstation.

Edit the virtual machine Network. I have added two adapters (vmnet2 and vmnet3 and named them as LAN-Network and Attacker Network.

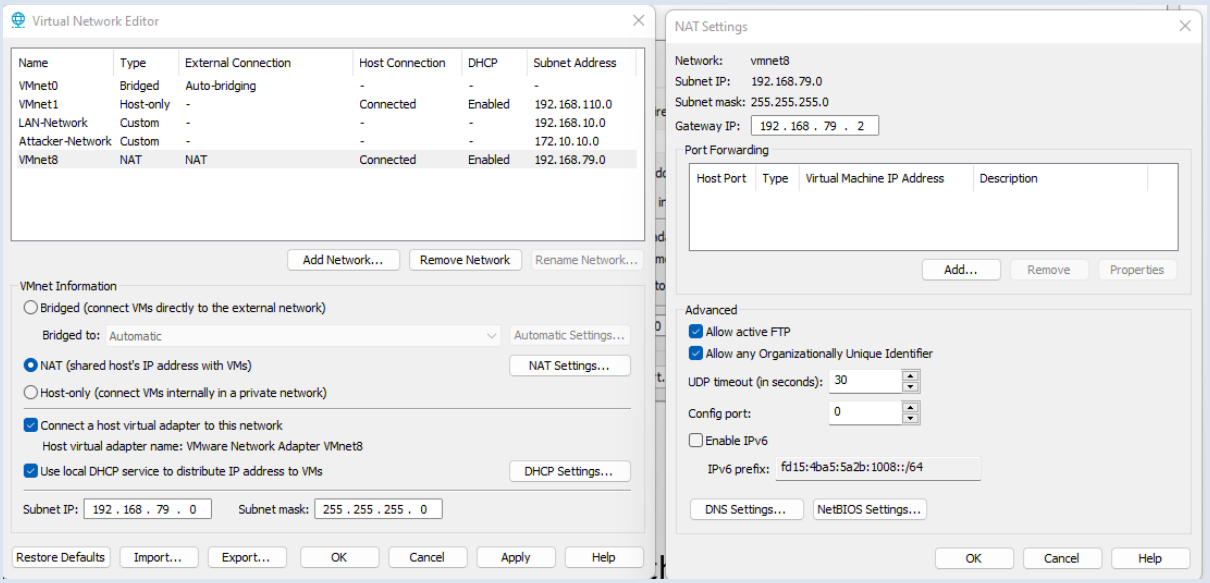


I have provided network address and subnet mask for both LAN-Network and Attacker Network which is 192.168.10.0 and 172.10.10.0 respectively. I will disable DHCP and DNS servers from both of the internal networks.





I am using vmnet8 as a WAN interface for my lab. I will enable DHCP for this network, so that my WAN interface will automatically get the IP address. We can see Gateway IP form my NAT network, which will forward traffic to internet from this virtual lab.



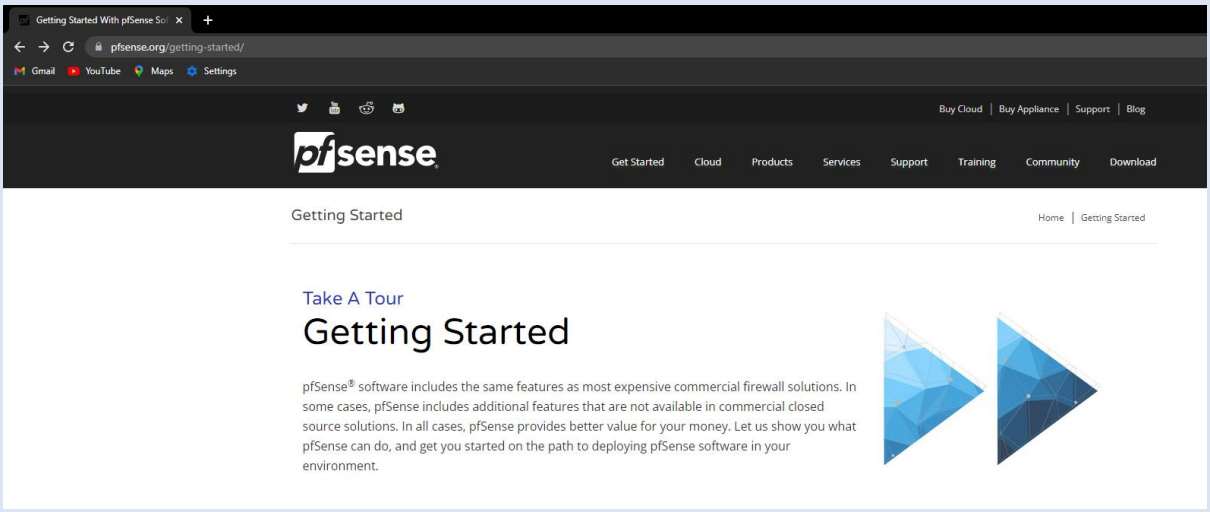
LAN network will be configured to my LAN interface of my PFsense as the default gateway of my Internal network.

WAN network will be the network my ISP will provide and assign the IP address using DHCP server in my home router [3]. In real scenario, it looks something like the following diagram.

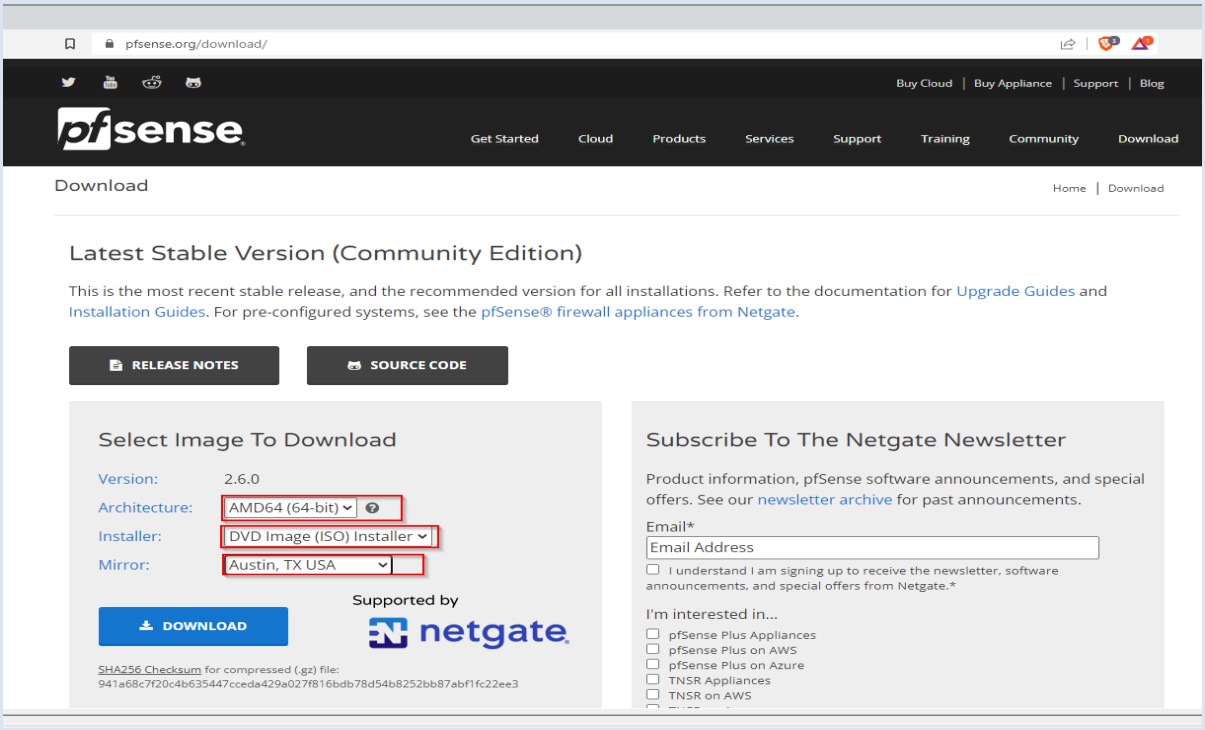
Installing PFSense:

PFsense is an Open-source firewall. Despite of being open source, pfsense provides many different features compared to the proprietary firewalls which are vendor controlled and highly expensive. In this lab, we will Install PFsense and run as the firewall and gateway between our Attacker-Network and LAN network and connect both networks to outside internet.

Installation of PFsense is not hard and documentation for the installation and configuration of PFsense can be easily available from PFsense documentations and guides [4]. Also, many answers can be found from community discussions. Navigating to pfsense.org/getting started will lead you to various installation and configuration guides.

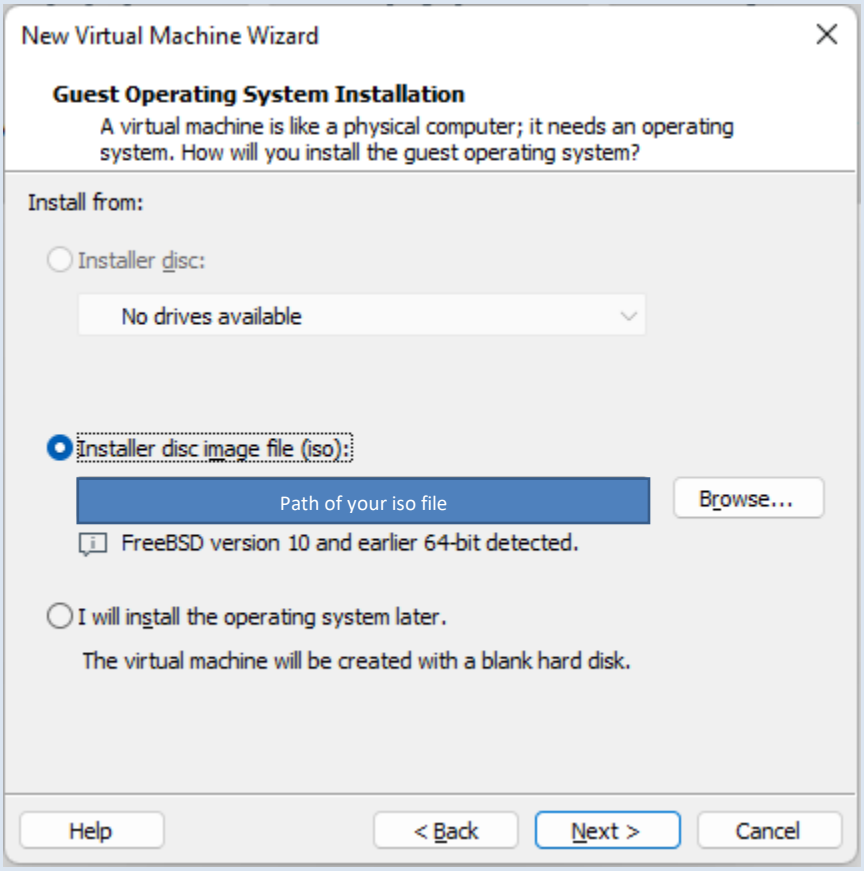


We are using Pfsense as a virtual machine so, I will download the .iso file of my PFsense from the official PFsense website.



Create Virtual Machine:

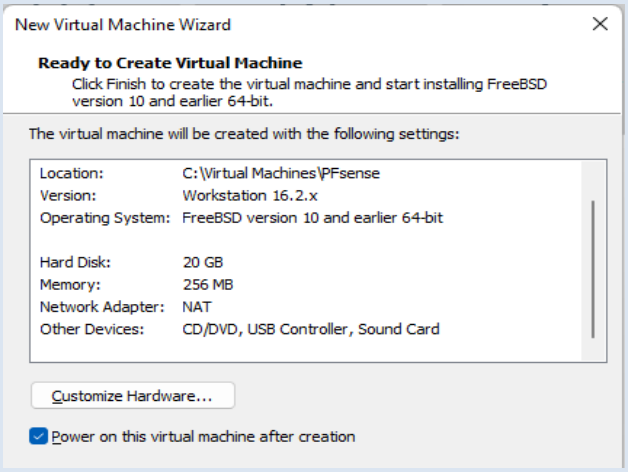
To install our .iso file we need one virtual machine. In my vmware workstation I will create a virtual machine using typical(recommended) steps. I will provide my .iso path as the installer dic_image file. I will then provide the path to store my virtual machine in my host computer. I have used the accessible location for me to use.

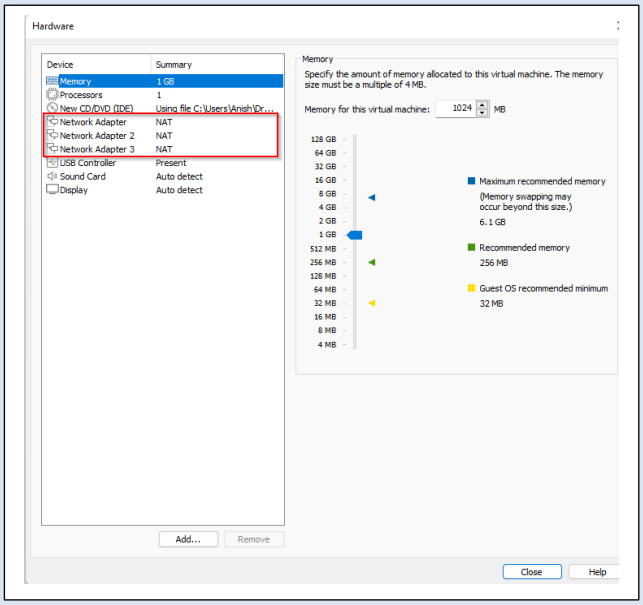


Pfsense is used for storing the firewall log files, based on the matched and unmatched rules in the Pfsense generates log report. Based on the usage, resources storage should be determined. I am allocating 20 GB for now and store into same file. In the review section, we can customize

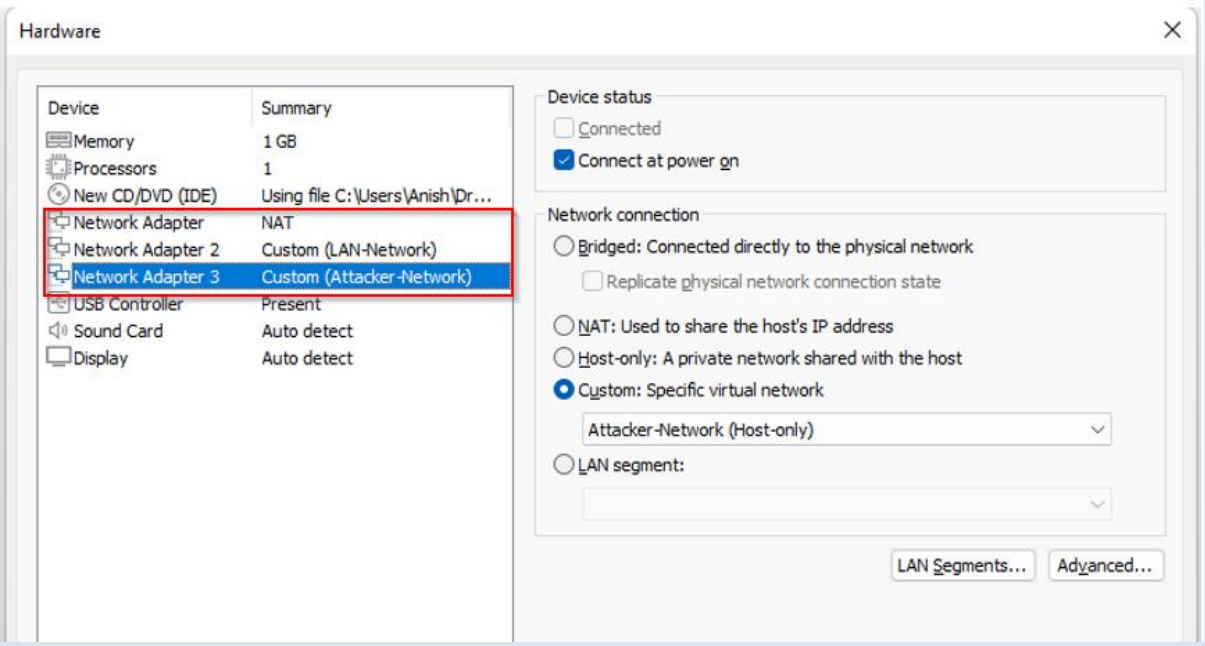
our hardware, I want to change my RAM size and add three virtual network adapters.

After changing to RAM size to 1GB, I will add two more network adapter clicking network adapter and Add Network Adapter. By default my hypervisior has put all the adapters in NAT network.





In this lab, I will leave ‘Network Adapter’ to default NAT and change ‘Network Adapter 2’ and ‘Network Adapter 3’ to LAN-Network and Attacker Network respectively, which we had created before.



Saving configuration PFsense will auto boot, PFsense is exclusively licensed to netgate and have some proprietary trademarks, I will accept the 'Copyright and Distribution Notice' and continue the Installation.

I will choose the default keyboard layout in keymap selection which is English US.

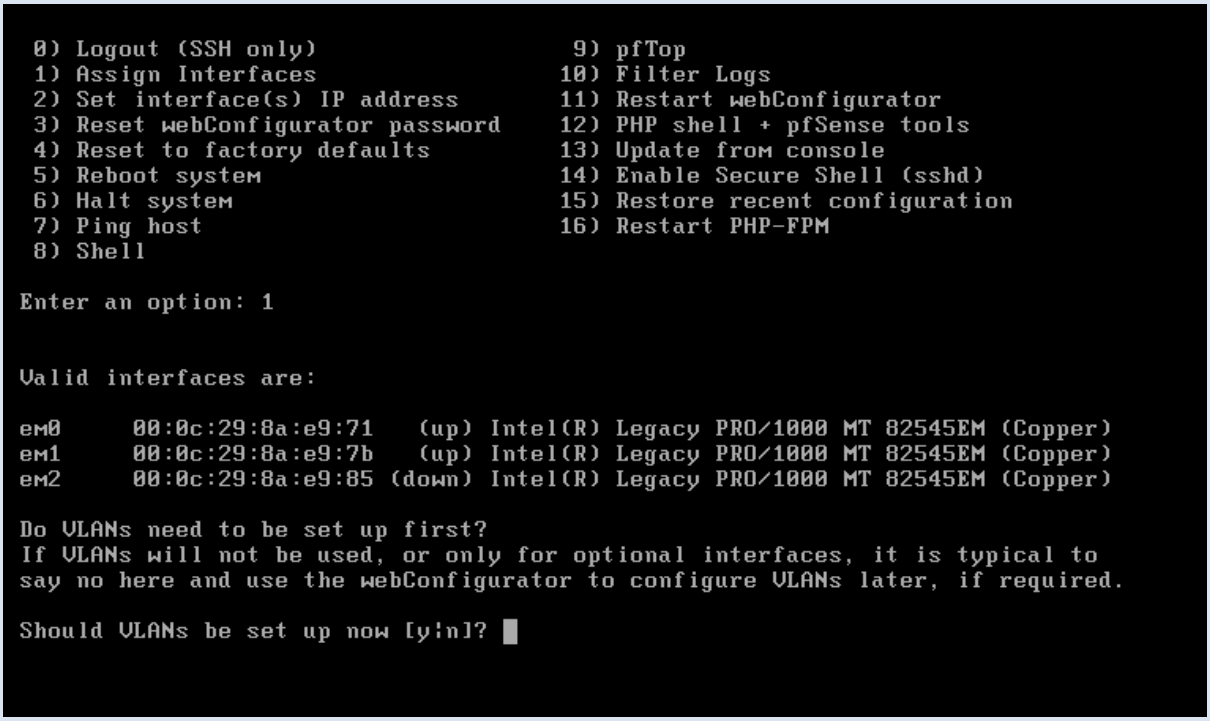
In Partitioning wizard, I will select Auto (ZFS) file system, which is Zettabyte File System. You can choose any file system. Unix File System with BIOS and UEFI both are also available. As the redundancy I will choose Stripe -No Redundancy, and select the default disk provided da0 to store the stripe files [5]. Use Spacebar from the keyboard to select the disk.

After finishing the installation Pfsense will ask weather to open shell in any other system to make change, I will say no and reboot my pfsense.

Configure PFsense:

After installing PFsense and rebooting it, now we can configure our pfsense. The default Username and password for our PFsense is admin and pfsense respectively. We can configure different settings from this interface as shown below. However, now I will only configure my interfaces and network. PFsense can be access in web interface using the browser once interfaces and network are configured.

To configure interfaces, select option 1 and Enter. It has already identified three available interfaces, I am not creating vLans so I will type ‘n’ to the question to set up vlan and enter to the next step.



Configure Interfaces:

First, I want to configure my WAN interface so I will choose number 1. I want to statically enter the ip address which should be in 192.168.79.128 with subnet 255.255.255.0 and default gateway of 192.168.79.2. Network address and default gateway can be reviewed in virtual network editor from vmware workstation. We are not using IPV6 and enter n for the http as the web configurator protocol.

```
Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)
3 - OPT1 (em2)

Enter the number of the interface you wish to configure: 1

Configure IPv4 address WAN interface via DHCP? (y/n) n

Enter the new WAN IPv4 address.  Press <ENTER> for none:
> 192.168.79.128

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new WAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 192.168.79.2
```

Similarly, configure the remaining interface providing the IP address statically as planned for the LAN interface and attacker Interface (OPT1) in my case. I will set IP address from LAN-Network to em1 and Attacker-Network to em2 interface.

Following are the IP addresses for each interface.

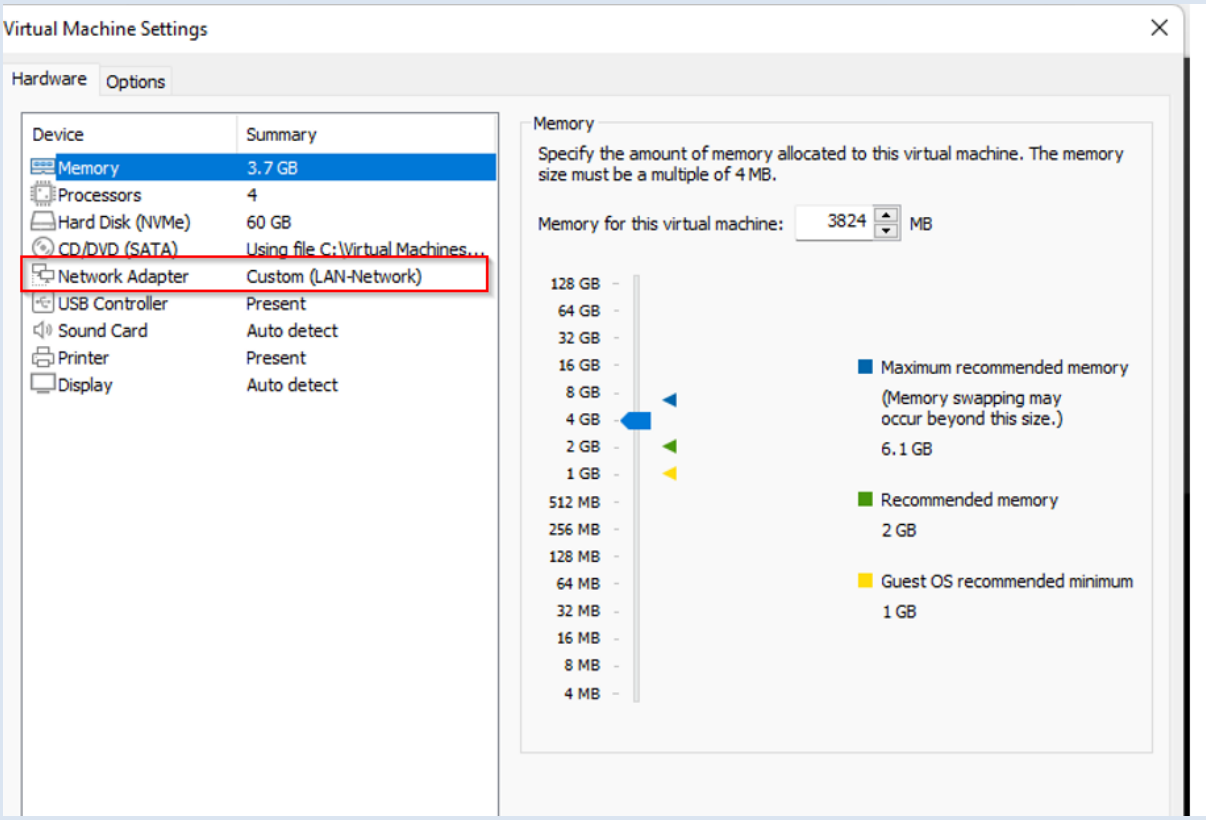
```
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4: 192.168.79.128/24
 LAN (lan)       -> em1        -> v4: 192.168.10.11/24
 OPT1 (opt1)     -> em2        -> v4: 172.10.10.20/24
```

After configuring the network and interfaces, now we can access our pfsense from the devices in LAN network, which was also notified after configuring LAN network.

Configuring Network in Defense PC:

In our internal network we have a defense PC which will be our windows 10 Operating system. I have already installed windows 10. I will edit my

windows 10 and connect the network adapter in LAN-Network in my vmware workstation.



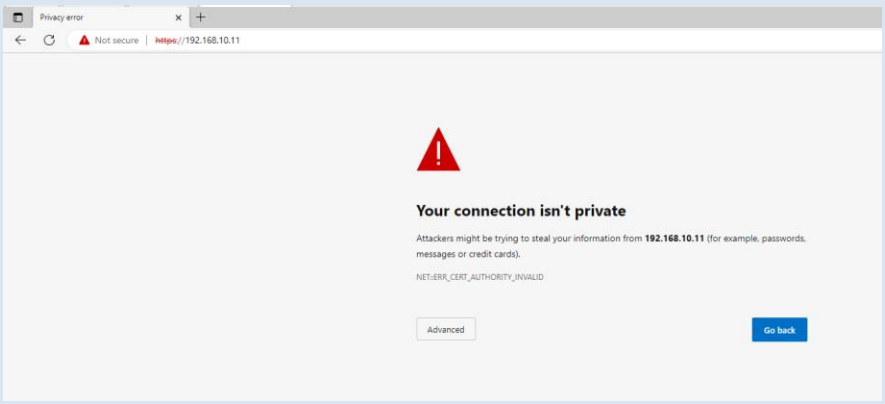
After starting my windows 10 (Defense Machine), statically configure IPV4 address from the IP address table which is 192.168.10.1 with the default gateway 192.168.10.11, which is the address of LAN interface in our pfsense machine. Verify the changed address using Ipconfig command from command terminal.

```
C:\Users\Anish>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.10.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.10.11

C:\Users\Anish>ping 192.168.10.11

Pinging 192.168.10.11 with 32 bytes of data:
Reply from 192.168.10.11: bytes=32 time=1ms TTL=64
Reply from 192.168.10.11: bytes=32 time=1ms TTL=64
Reply from 192.168.10.11: bytes=32 time<1ms TTL=64
Reply from 192.168.10.11: bytes=32 time=2ms TTL=64

Ping statistics for 192.168.10.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 1ms
```

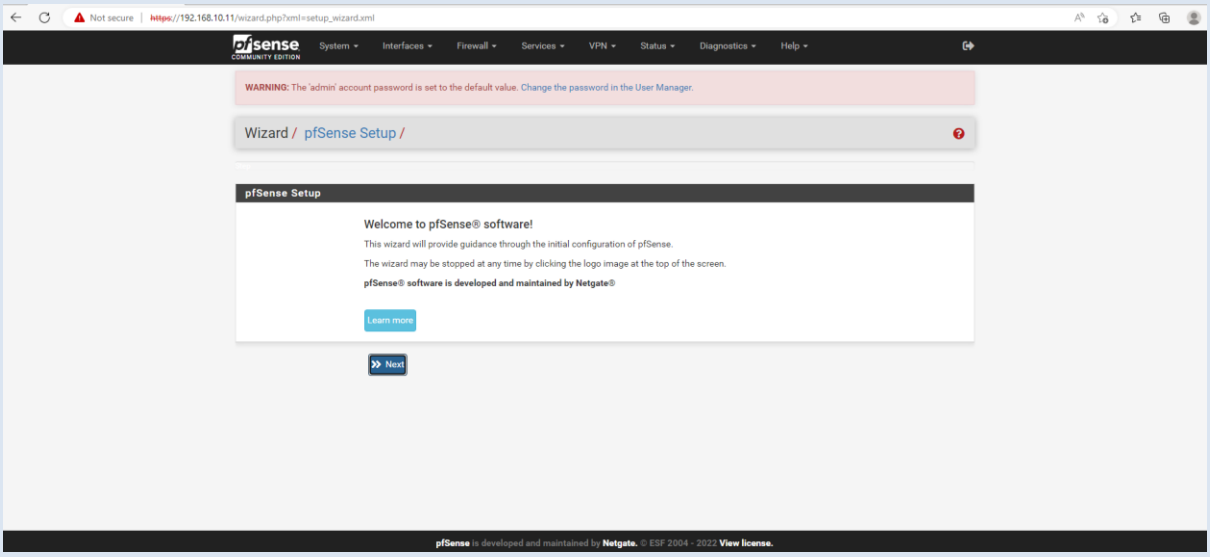
Access PFsense Web Interface from Defense PC:

We can verify the connection between Defense machine and pfsense by pinging default gateway address from our defense machine. In my case it is so, I will open my pfsense web interface using my favourite browser ‘Microsoft Edge’. Enter http://192.168.10.11 as the url for the pfsense. I will proceed the connection clicking advance and proceed anyway option.

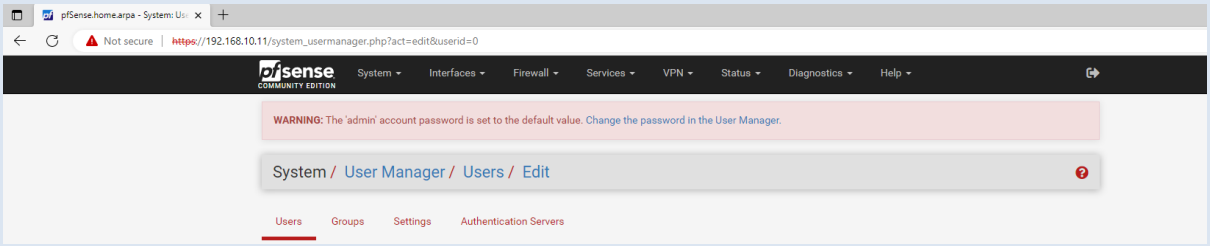
We have not created any passwords so use default credentials i.e. admin and pfsense to log in.



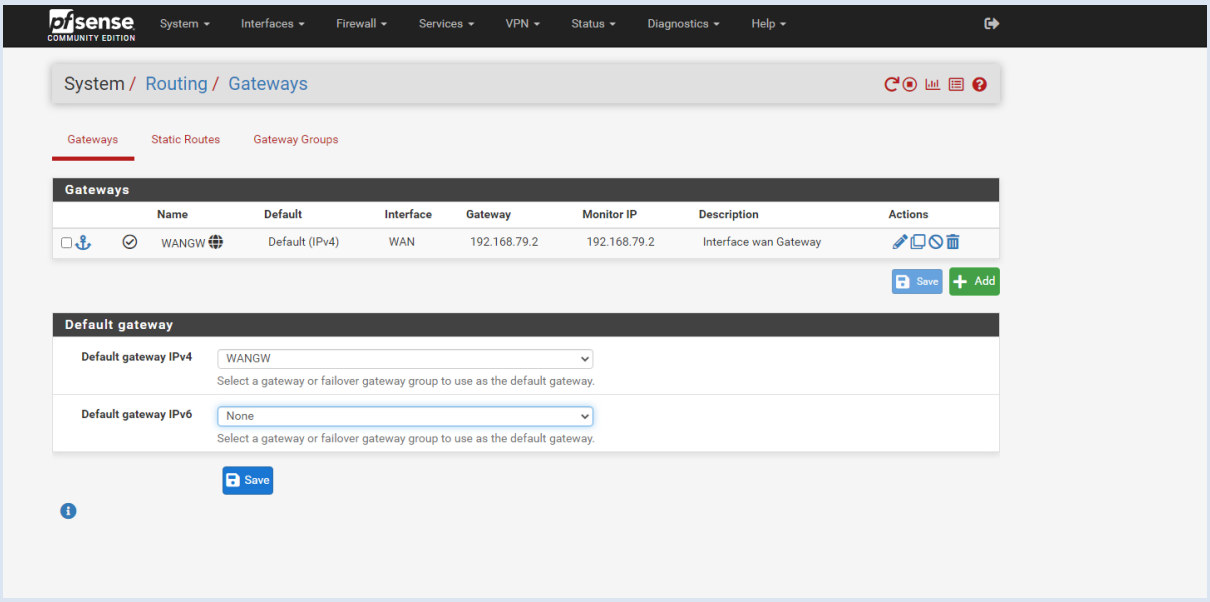
This is the Web interface of our pfsense interface. We can see the warning message to change the password for the admin user.

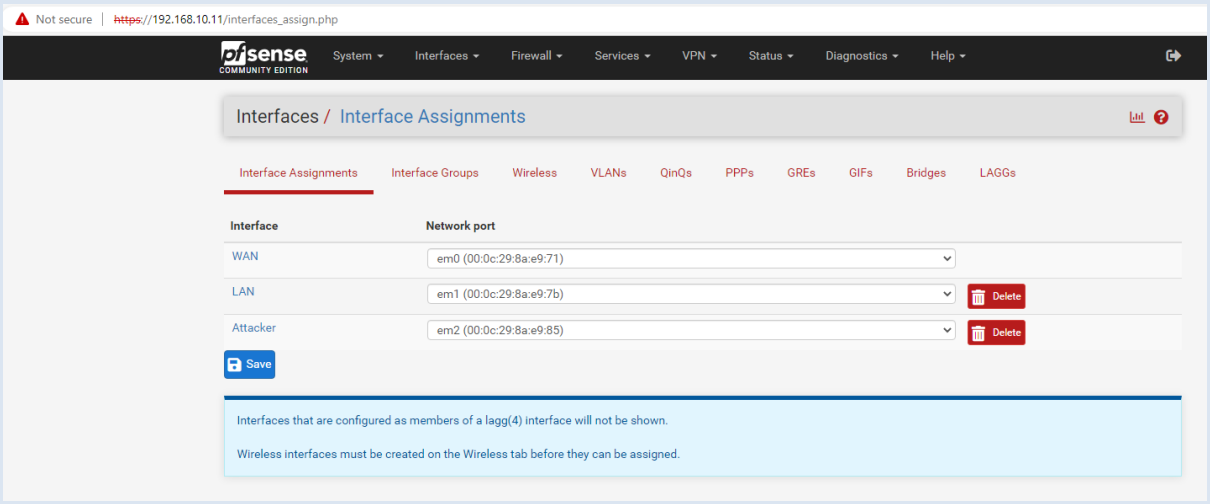


Going System/ User Manager / Users we can add users, edit passwords, and assign different policy regarding the access to the pfsense firewall. Setting up good password policy and implementing it is crucial step to maintain security.

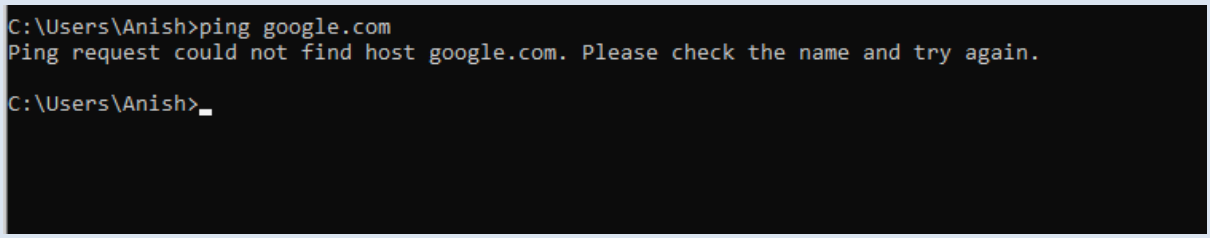


Navigate to System/Routing/Gateways to configure gateway addresses, in my case my WAN interface is talking to the gateway of NAT network of my vmware workstation, and also from interface/interface Assignments we can see the interface that are available in PFSense. We can edit our interfaces from here.

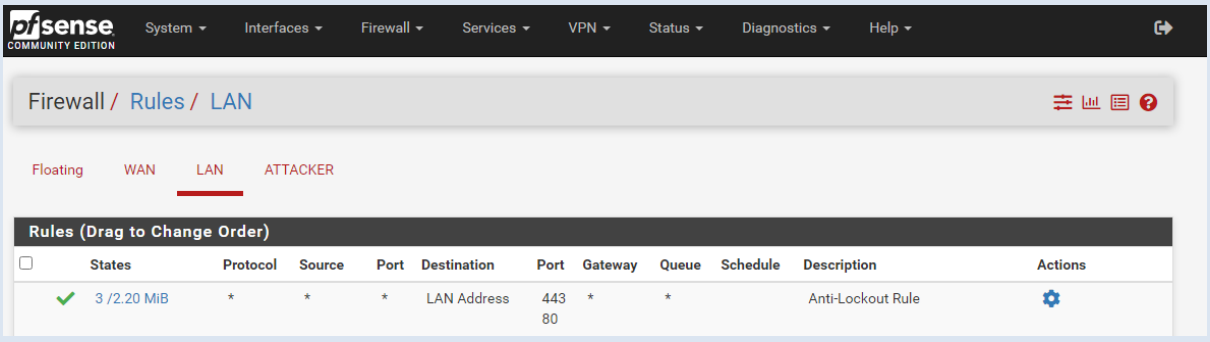




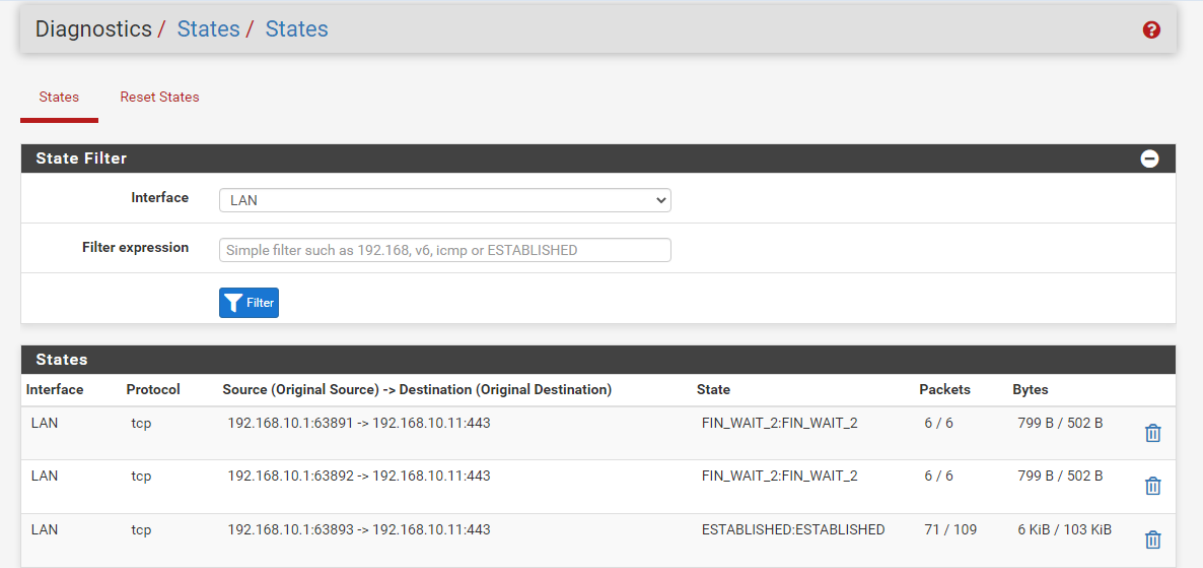
Let's ping external domains such as google.com to verify the connection with internet from our LAN network. Our request failed, it is because we have not created any firewall rules in our pfsense to connect LAN network to other network.



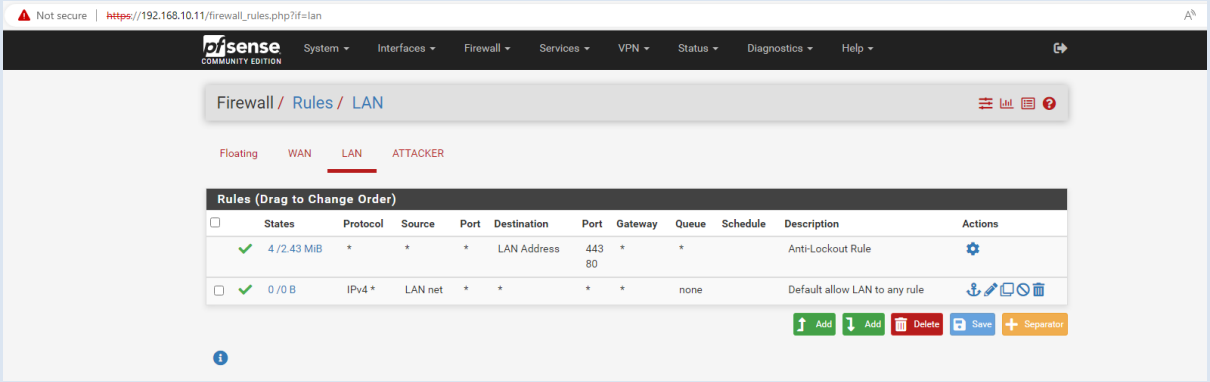
Review Firewall rules, to search the firewall rules we can simply navigate, firewall/Rules. We can see the default rule created by pfsense to allow http and https connection in LAN address. Because og this rule we are able to connect to our pfsense from our browser.



Viewing the state of the rule we can see many logs generated while accessing the web interface form defense machine to pfsense are generated. We can reset or view the logs from this screen, we can even filter our output using filter expression.



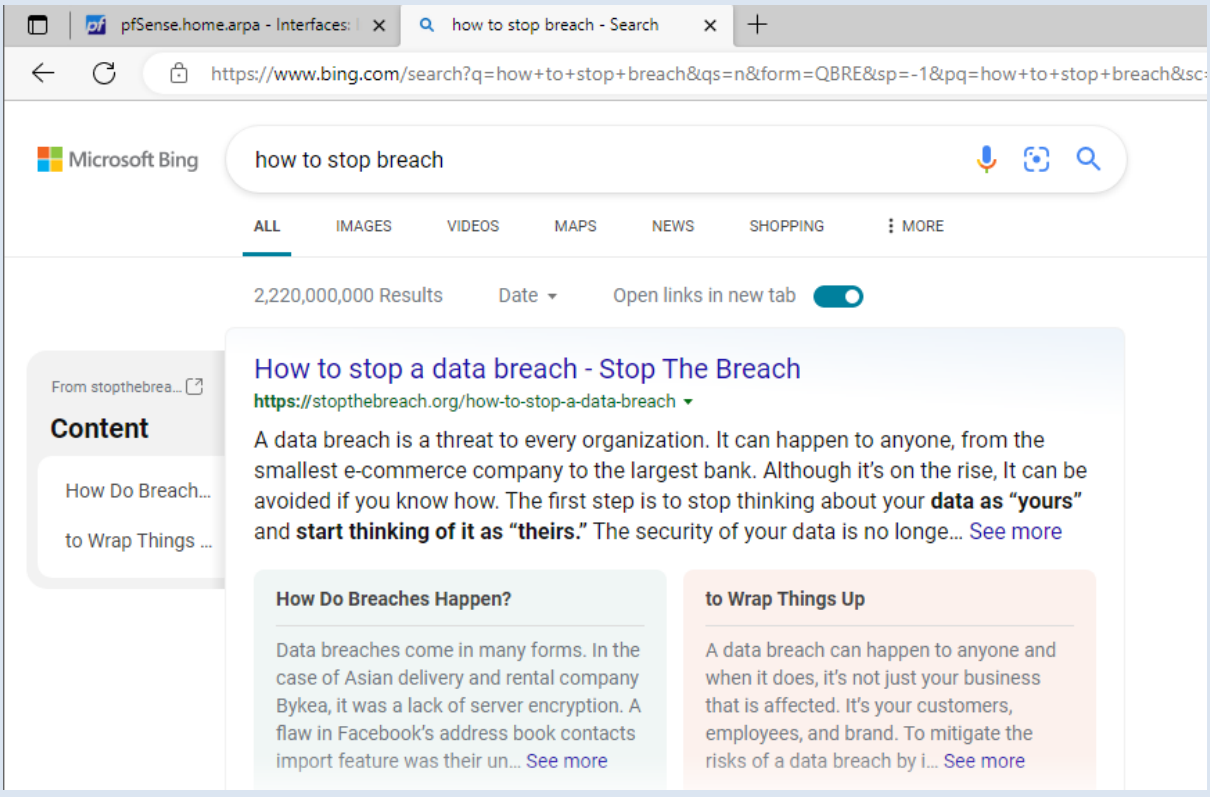
For now, let's create one firewall rule that will allow our internet net to go anywhere in the internet. Navigating Firewalls/Rules/LAN.



We can verify that our LAN network can access network using ping command or visiting websites from our windows machine. Ping the attacker interface in pfsense as well. We see after creating the firewall

rule, we can surf the internet from inside network and can also connect to attacker network. Allowing every machine inside the organization to go to internet is risky so, creating firewall like this for the internal network is not appropriate. Let's leave the rule as it is right now.

```
Microsoft Windows [Version 10.0.19044.2130]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Anish>PING GOOGLE.COM

Pinging GOOGLE.COM [142.250.70.142] with 32 bytes of data:
Reply from 142.250.70.142: bytes=32 time=15ms TTL=127
Reply from 142.250.70.142: bytes=32 time=13ms TTL=127
Reply from 142.250.70.142: bytes=32 time=33ms TTL=127
Reply from 142.250.70.142: bytes=32 time=15ms TTL=127

Ping statistics for 142.250.70.142:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 13ms, Maximum = 33ms, Average = 19ms
```

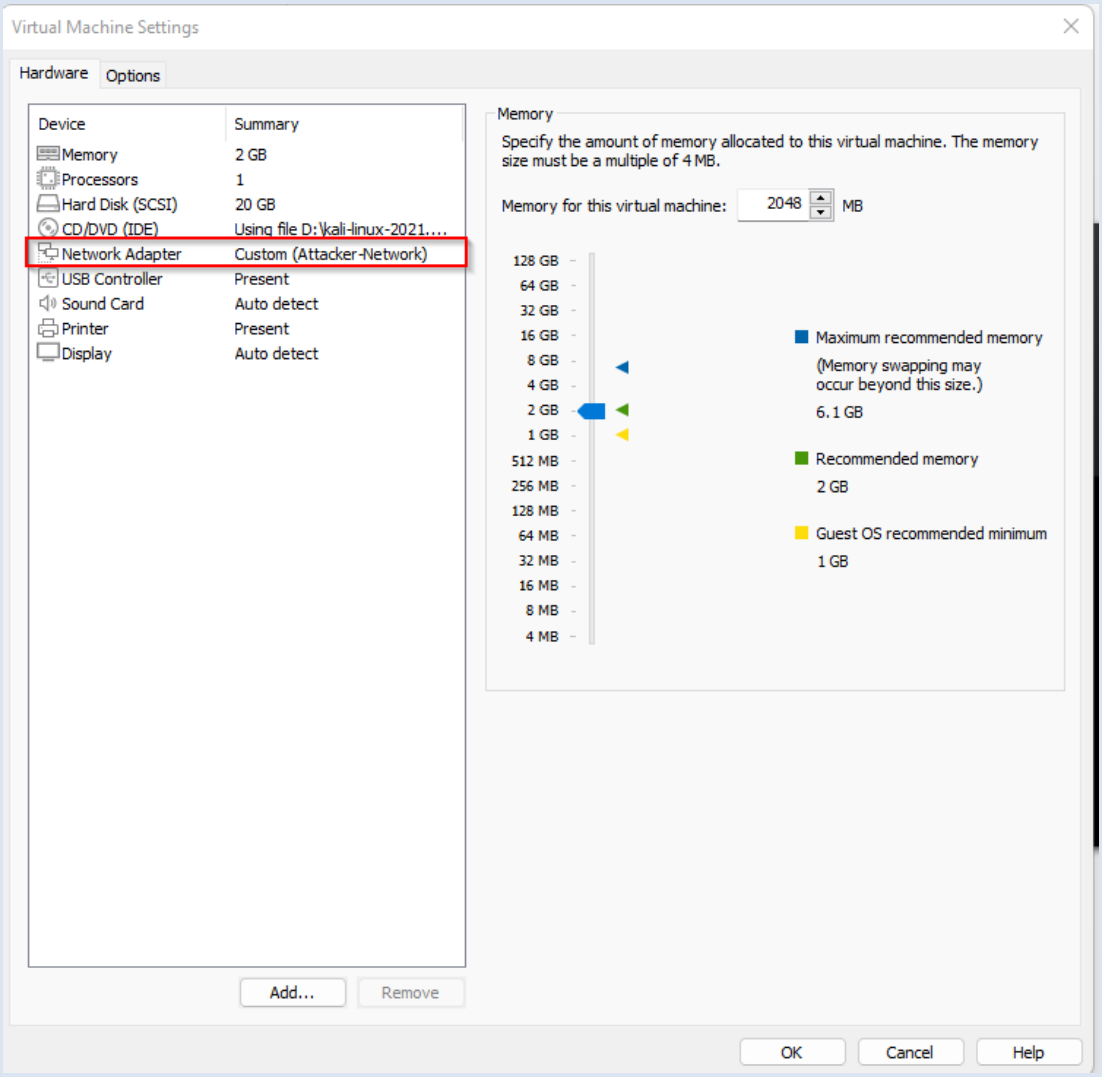


Configuring Kali Linux network:

We have kali linux in our Attacker Network and use pfsense as a gateway to surf the internet from our Kali Linux. Also, to reach our internal network we will set up firewall rules.

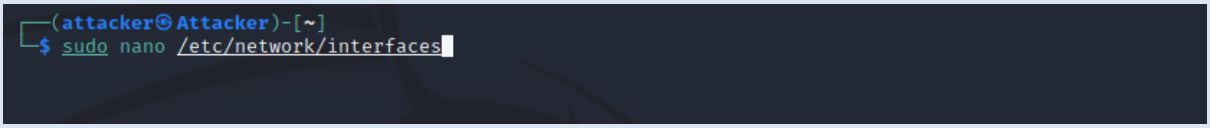
I assume kali linux is already installed in the virtual box, it is as simple as installing other operating systems.

I have the following hardware compatibility, also most importantly, change the Network Adapter to Custom (Attacker-Network)

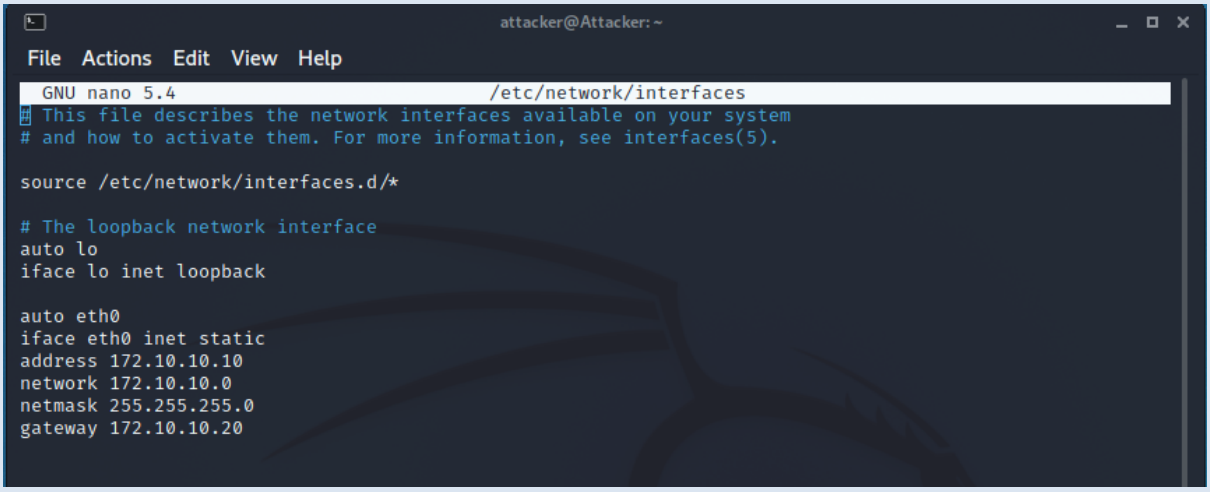


We have disabled the DHCP configuration in our Attacker-Network that means we will manually configure our network in Kali Linux. We will assign 172.10.10.10 as ipv4 and 255.255.255.0 as the subnet mask. Also, as a default gateway, I will assign the ip address of em2 in PFSesne that is 172.168.10.20.

We can assign static ip address using GUI or just by editing /etc/network/Interfaces file in kali. We can edit our file using nano and we will need sudo privilege to make any changes.



In the interfaces file add the following lines, save the changes made.



Let's turn the interface down and turn it again using 'ifdown eth0' and 'ifup eth0' command. Verify the changes using 'ip addr' command.

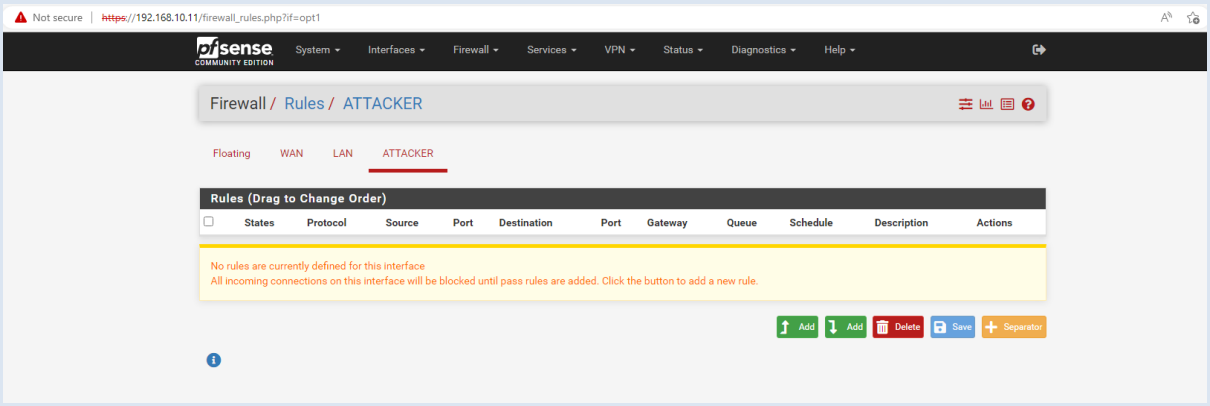
```
┌──(attacker㉿Attacker)-[~]
└─$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:24:81:d2 brd ff:ff:ff:ff:ff:ff
    inet 172.10.10.10/24 brd 172.10.10.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe24:81d2/64 scope link
       valid_lft forever preferred_lft forever
```

Connection between Kali and PFsense:

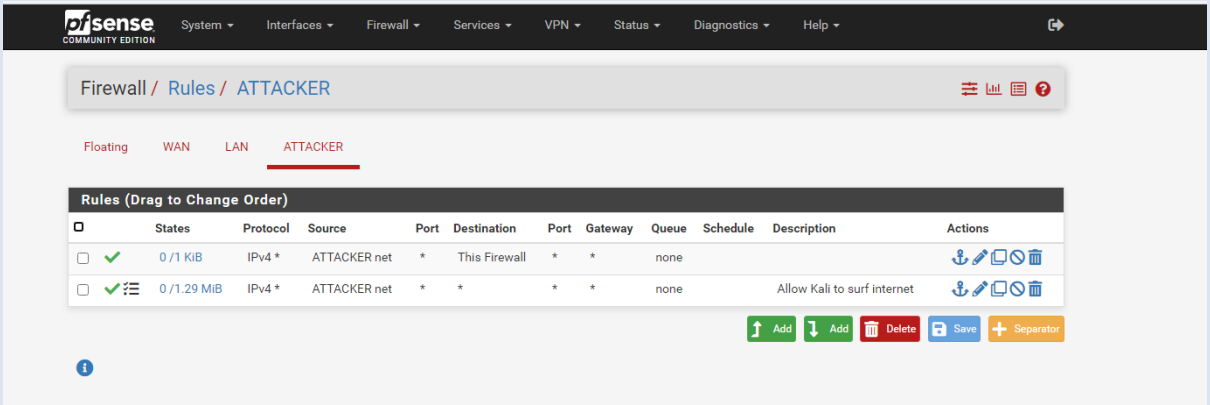
Now, let's try to ping default gateway in PFsense, use command 'ping 172.10.10.20', and also try to ping our internal network, however we cannot ping to any networks, because we have not created any firewall rules in our pfsense that will allow attacker address to go anywhere.

```
┌──(attacker㉿Attacker)-[~]
└─$ ping 172.10.10.20
PING 172.10.10.20 (172.10.10.20) 56(84) bytes of data.
^C
--- 172.10.10.20 ping statistics ---
6 packets transmitted, 0 received, 100% packet loss, time 5111ms


┌──(attacker㉿Attacker)-[~]
└─$
```

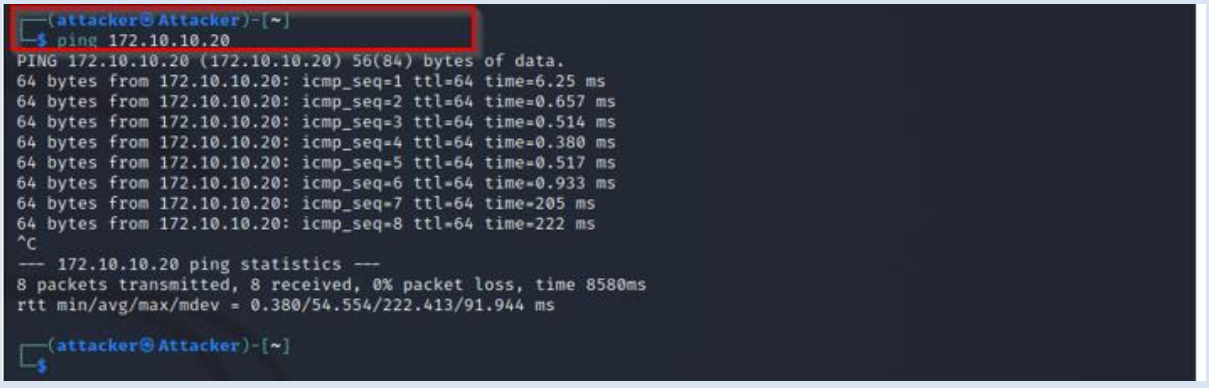
Let's open pfsense from our Defense machine which is in LAN-Network and review our firewall rules for attacker network.

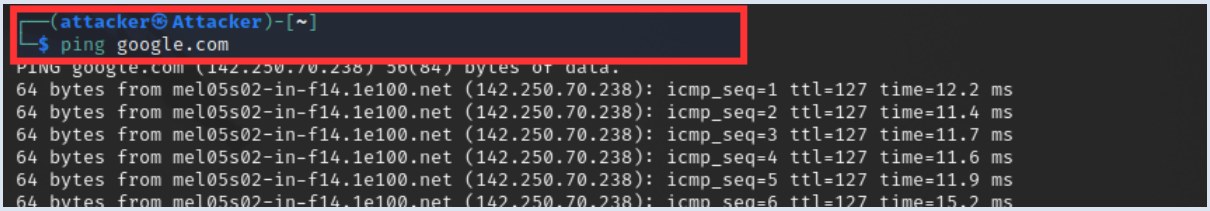


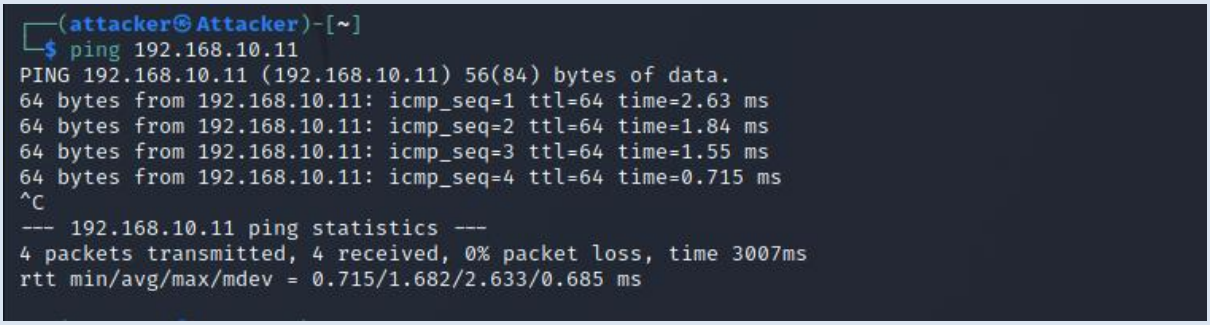
We do not have any rules that will allow our kali linux to go outside the network. Let's create some rules so that we can ping kali linux with external world. Navigate to pfsense firewall /rules/ attacker. Click Add button. We will create rule that will allow attacker addresses to access the firewall so that we can ping pfsense from our Kali machine [6]. And also allow attacker network to go anywhere, so that we can access internet in our kali linux.



Now, let's try to verify connection from our attacker machine to our firewall. We will also test the connection between internet and our Attacker network. We can ping our pfsense, we can ping LAN-Interface in pfsense and also google.com.

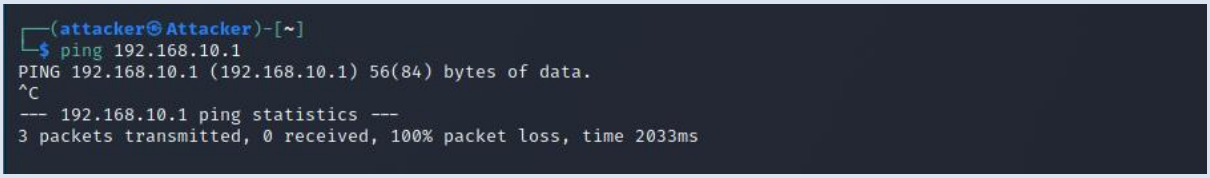






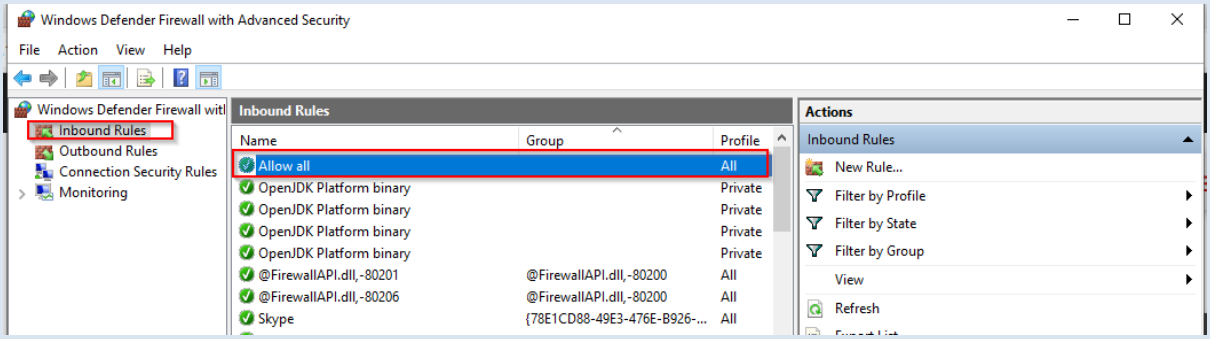
Connection Between Kali Linux In Attacker Network and Defense PC in LAN-Network:

We can ping to our LAN gateway but we cannot ping to windows 10, which is our defense machine in Lan-Network. It is nothing to do with the pfsense firewalls but the default firewall in windows 10, that will block every bogan network tries to connect to windows 10.

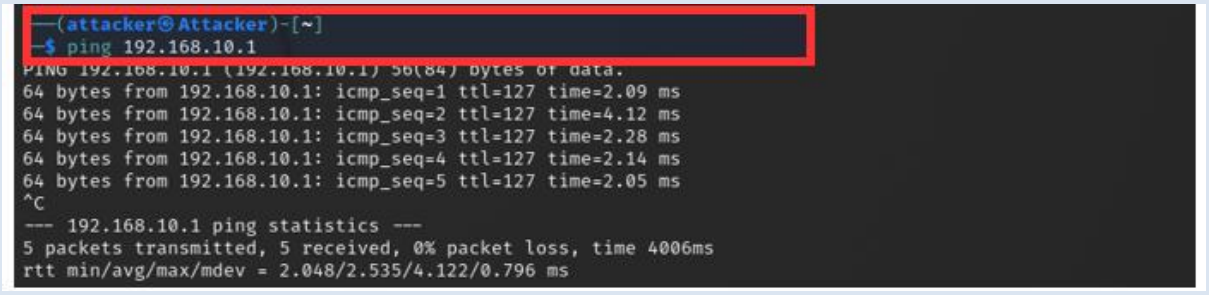


From our windows 10, defense machine, Navigate to Windows Defender Firewall with Advance Security and add rule that will allow everything to

connect our Defense machine. DOING SO IS RISKFUL, HOWEVER FOR AN EXAMPLE WE WILL ALLOW THAT.



It is very important that an organization should block every external network to reach out to their internal network. However, organizations can run services such as DNS server or web server or RDP connections from external IP address and only those services should be allowed to enter the internal network. Now we can see we can sucessfully connect to our internal network.



At this point, we have successfully created our network topologies, as requirements we have installed and configured our kali machine in attacker network, our defense machine in internal network. We have created different firewall rules, reviewed the rules from web interface of pfsense connected in our internal machine. We have troubleshoot

different problems that have denied the access of external(Attacker Network) to our internal (LAN network).

After this we will install different machines in our LAN environemnt, SIEM server. We will create many other firewall rules as requirements that will pass form our pfsense Machine.

SPLUNK:

The project has been allocated to identify the most effective tool between SPLUNK and ELK. Both tools provide great services for industrial data.

Splunk was selected due to its high demand in the industry and the potential future it holds.

Imagine the security admin try to find the system threat through access logs that are populated by thousands of lines. How would the admin determine where the threat entered and through what. This procedure takes hours of work.

Machine data is complex to understand, it is in an unstructured format and not suitable for making analysis [7].

Some of the Splunk customers within Australia are Vodafone, Domino's, and ING bank.

Vodafone – Uses to manage big data and mapping key indicators

Domino's – To gain insight on consumer behaviour

ING bank – Faster troubleshooting of key apps and insight into customer behaviour.

What is Splunk?

It is a tool used to analyse machine data. Splunk is an extensible data platform that can process data from cloud or any data centre. The tool allows any third-party tool to work at a massive scale.

The need was created by data growth that keeps on increasing over time.

Data such as Machine data, Sensory Data and Business data used by IoT devices.

The reason to analyse this data is to pinpoint and grab the information required from heaps of information.

Analysing better data will help us identify Security Issues and system failure.

As computer systems students we enter organizations that generate data from multiple sources. Such as sensors, Network devices, Cloud Service, IoT and Mobile Services.

This data needs to be identified specifically to flag them according to their risk level.

Not only for its security factor, but also Splunk provides the service to share error information and work together to solve problems. From using industrial data storage to the level of protecting patient privacy, this tool expands its uses.

How does it work?

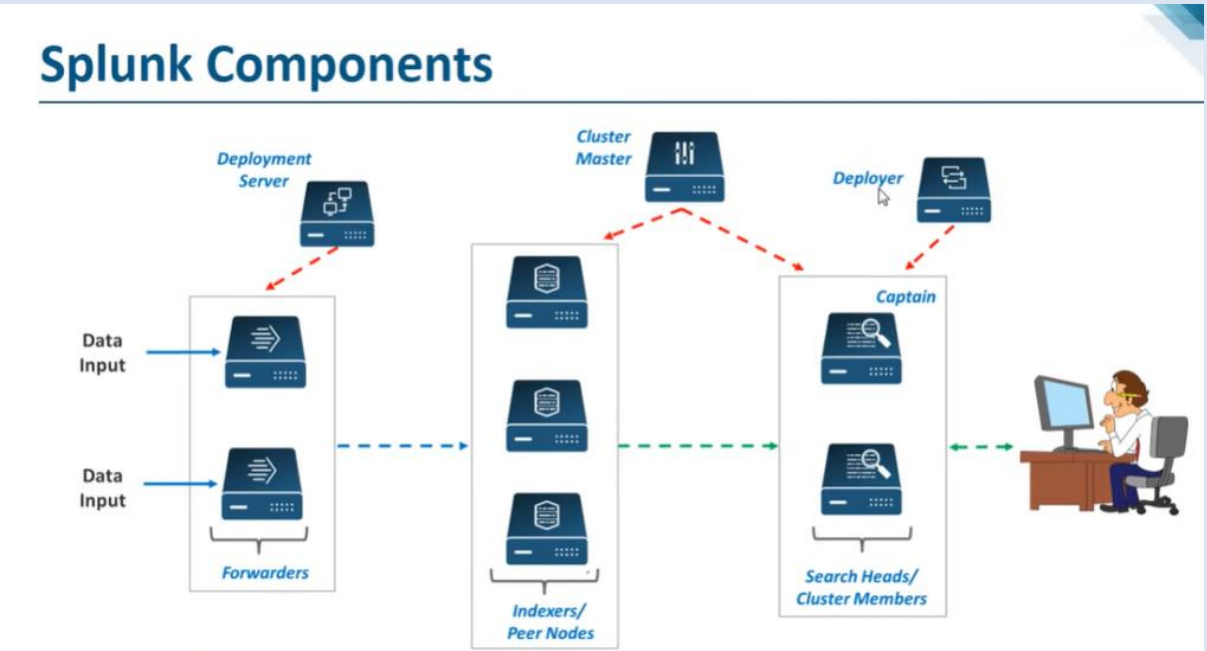


Image 1: Splunk component topology

Splunk accepts the user data and indexes them (Assign them numbers according to order) and divides into categories. Google uses natural language interpret to their search engine while Splunk uses SPL [2].

S – Search

P- Processing

L- Language

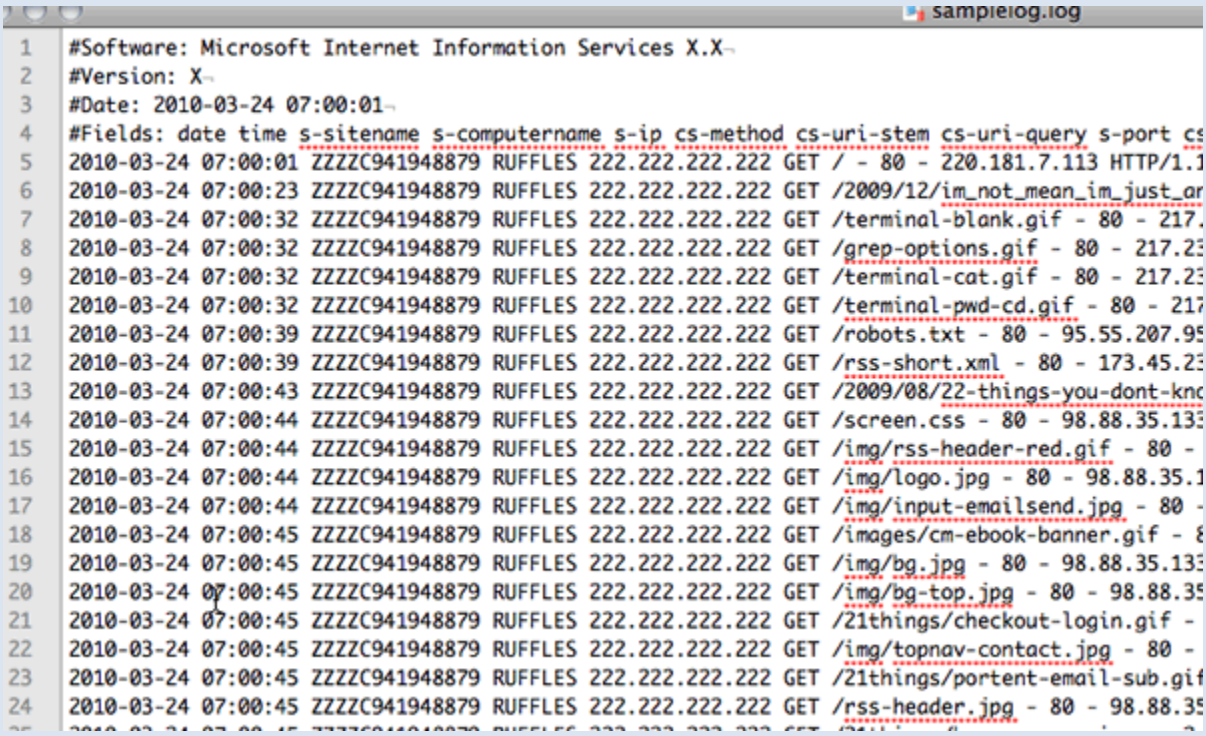
SQL processes structured query language but SPL deals with unstructured data.

The Splunk enterprise version allows the user to analyse and create reports, dashboards with the data.

Implementing machine learning is time consuming. However, this tool allows it to be more user friendly for someone with basic tech knowledge.

Explore Logs

Logs are generated on computing devices. They are system logs and server logs. The servers and systems will keep populating the logs. The logs are data about transactions. The data included in these logs are security threats, the network vulnerability, and the network traffic are some information registered in them. This is a big pile of data waiting to be discovered.



When there is a security breach, you cannot read line by line through the logs to find the threat.

This is when Splunk comes in handy.

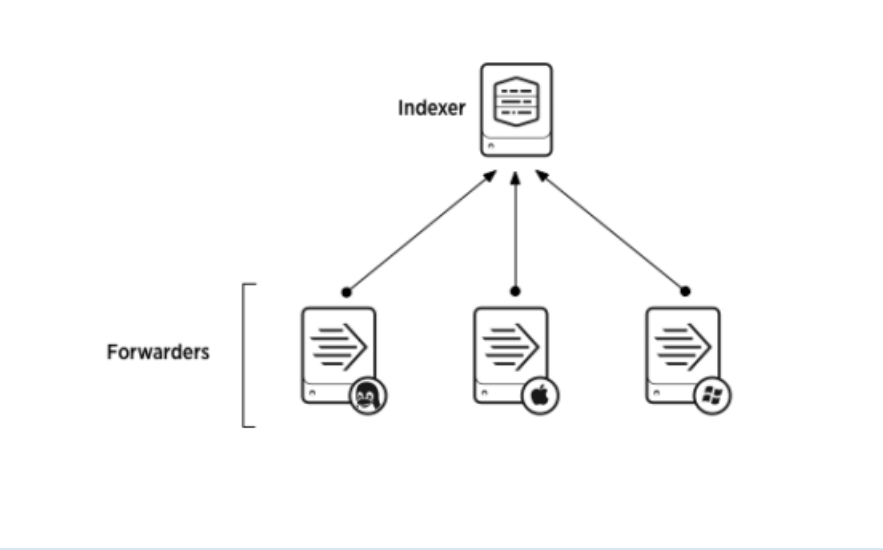
Advantages of SPLUNK

Real time log forwarding

Real time syslog analysis – allows the end user to see the analysis and get an idea of the threat they are dealing with.

Historical data – By comparing past attacks, the logs are matched to identify the attack by comparison.

Universal forwarder



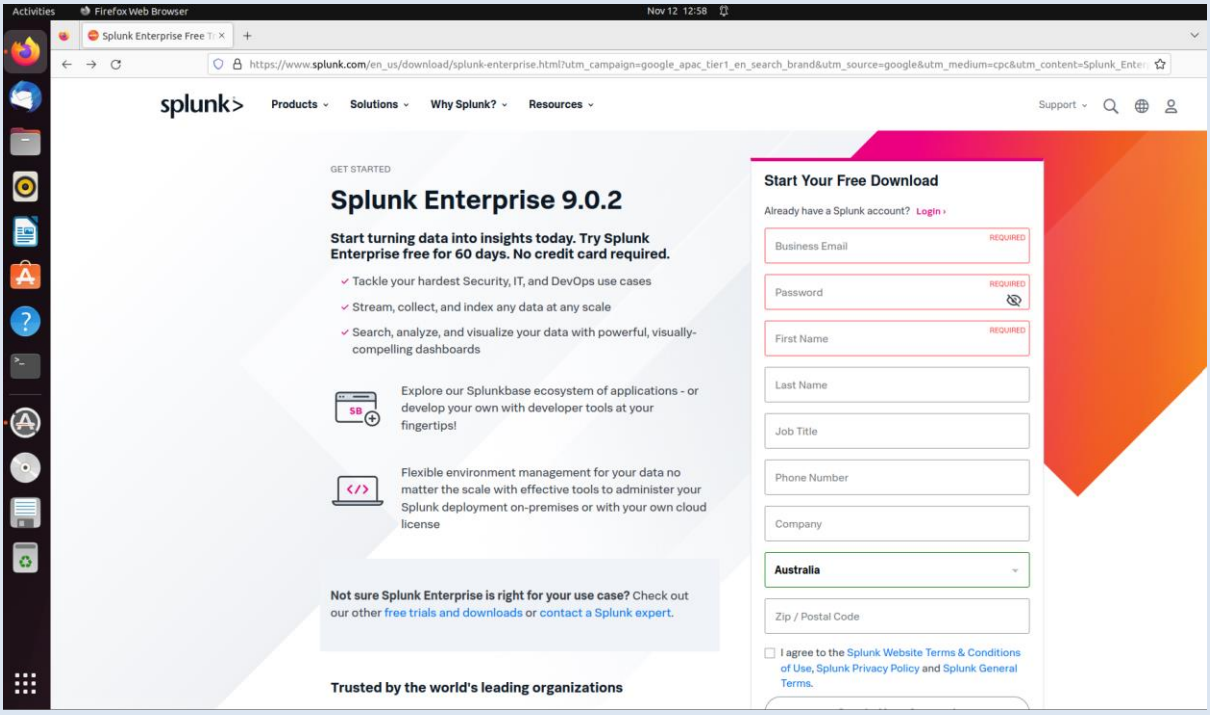
Splunk Enterprise Instance that sends data to another instance or a third-party system.

It contains only essential components needed to send the data from the deployment server to the receiving server.

Universal forwarders are highly scalable. They use significantly less hardware resources. We can install massive number of forwarders without impacting the network performance. The Universal forwarders do not have a user interface which helps minimize the resources used.

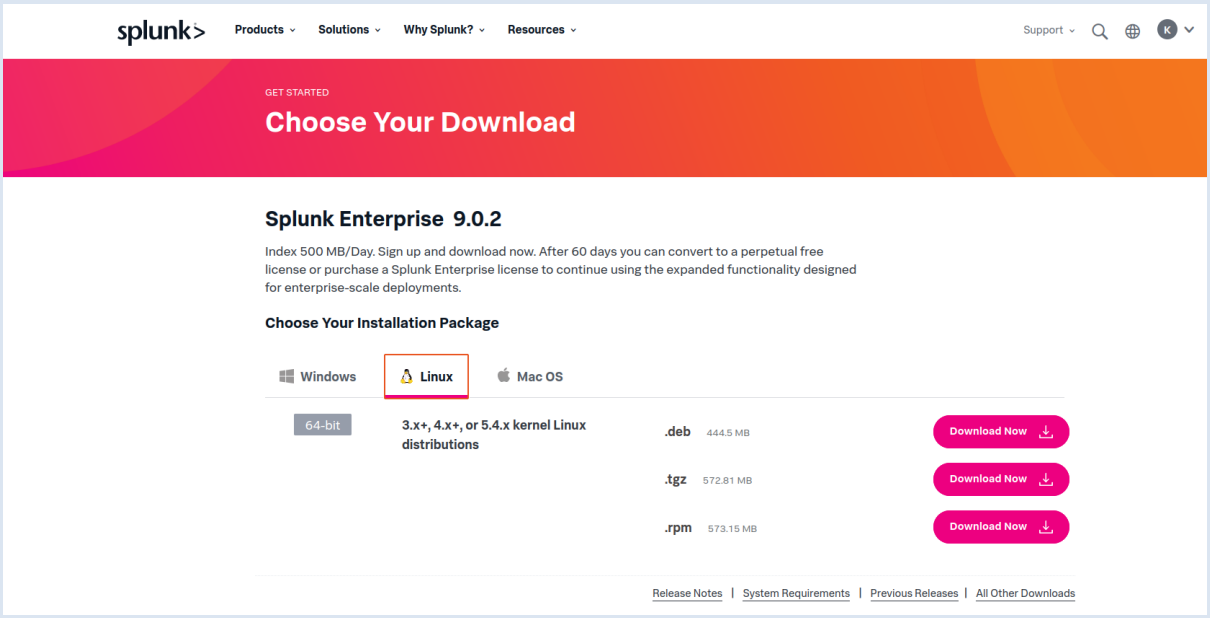
When installed the forwarder needs either deployment or receiving ip address along a hostname.

The Splunk website allows to free download after creating an account.



This account is for the downloading purpose and access to all splunk's products and services. For the project we created a dummy account to avoid using personal information to testing virtual machines.

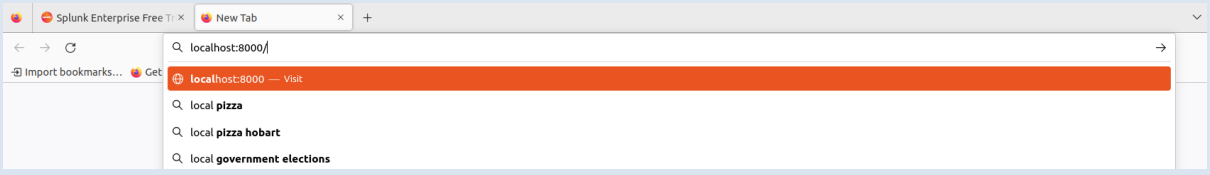
Splunk on Ubuntu



After installing the universal forwarder, the Client will access through localhost:8000

This is because Splunk avoids using an interface to install (This saves data and operating speed)

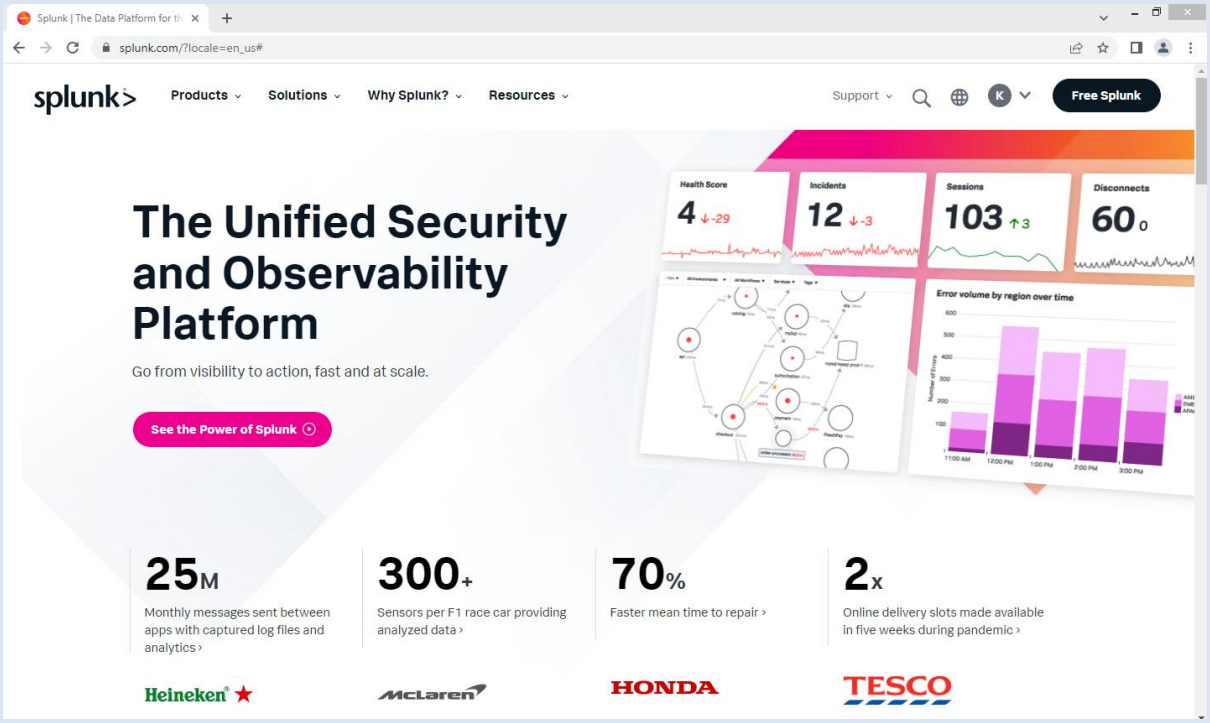
It's a win for both parties as this can be installed easily and prevent the employee meddling or accidently deleting the software [8].

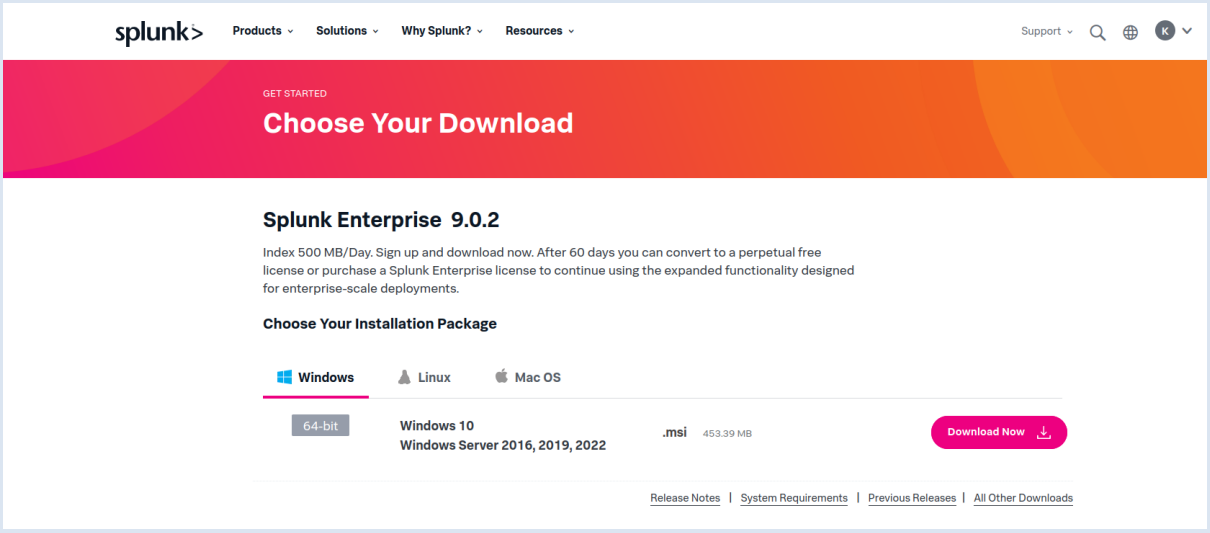


If you can't access the port 8000

Most probably the port is blocked for inbound traffic by the Firewall.

Windows 8 Victim





After downloaded the Splunk forwarder, initiate the installation procedure.

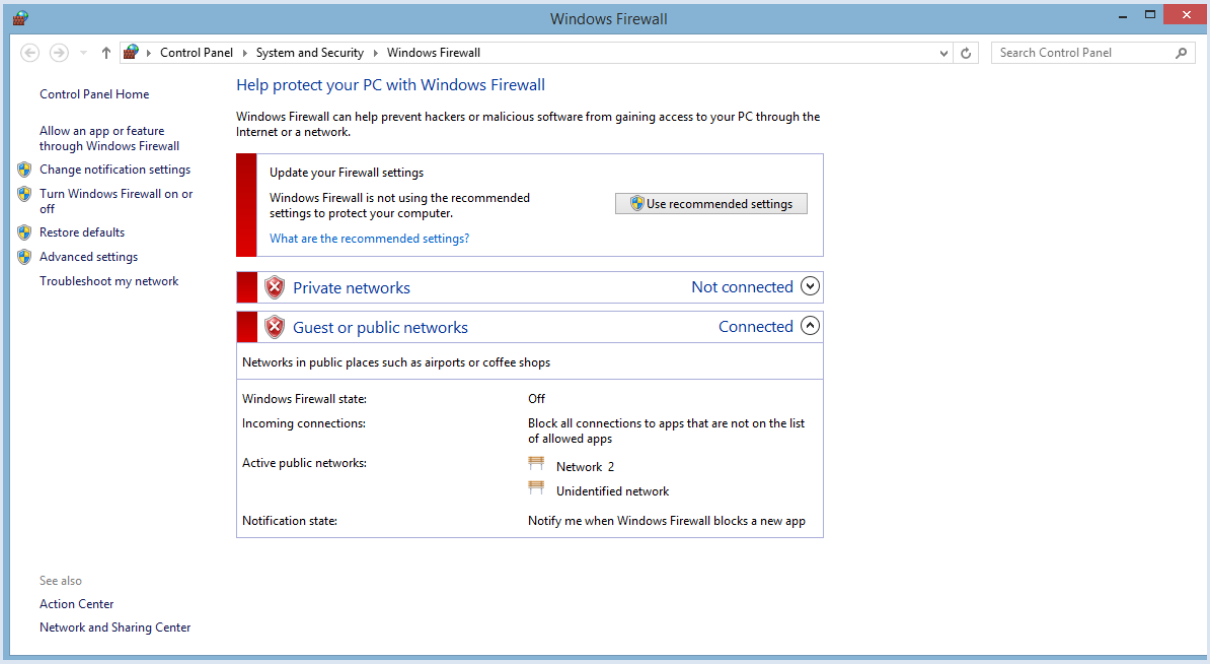
Allow connection

Step 1: Disable Firewall and allow connection

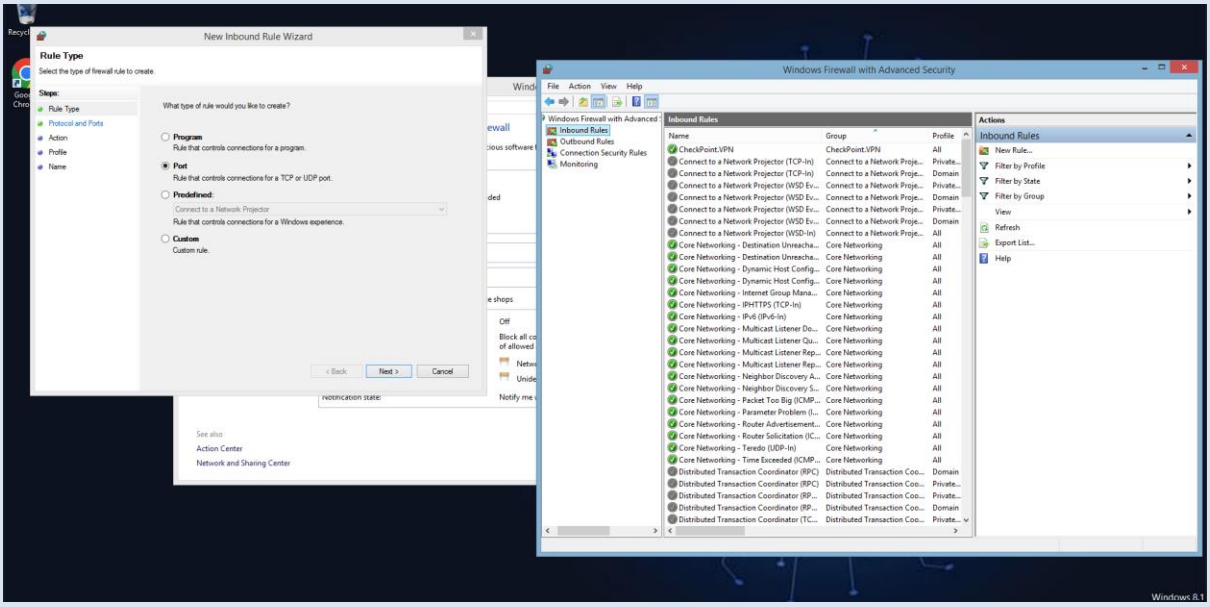
Windows Firewall need to be configured. The firewall by default will block third-party connections. We had to disable the firewall and create inbound and outbound rules to allow the universal forwarder to send the connection through.

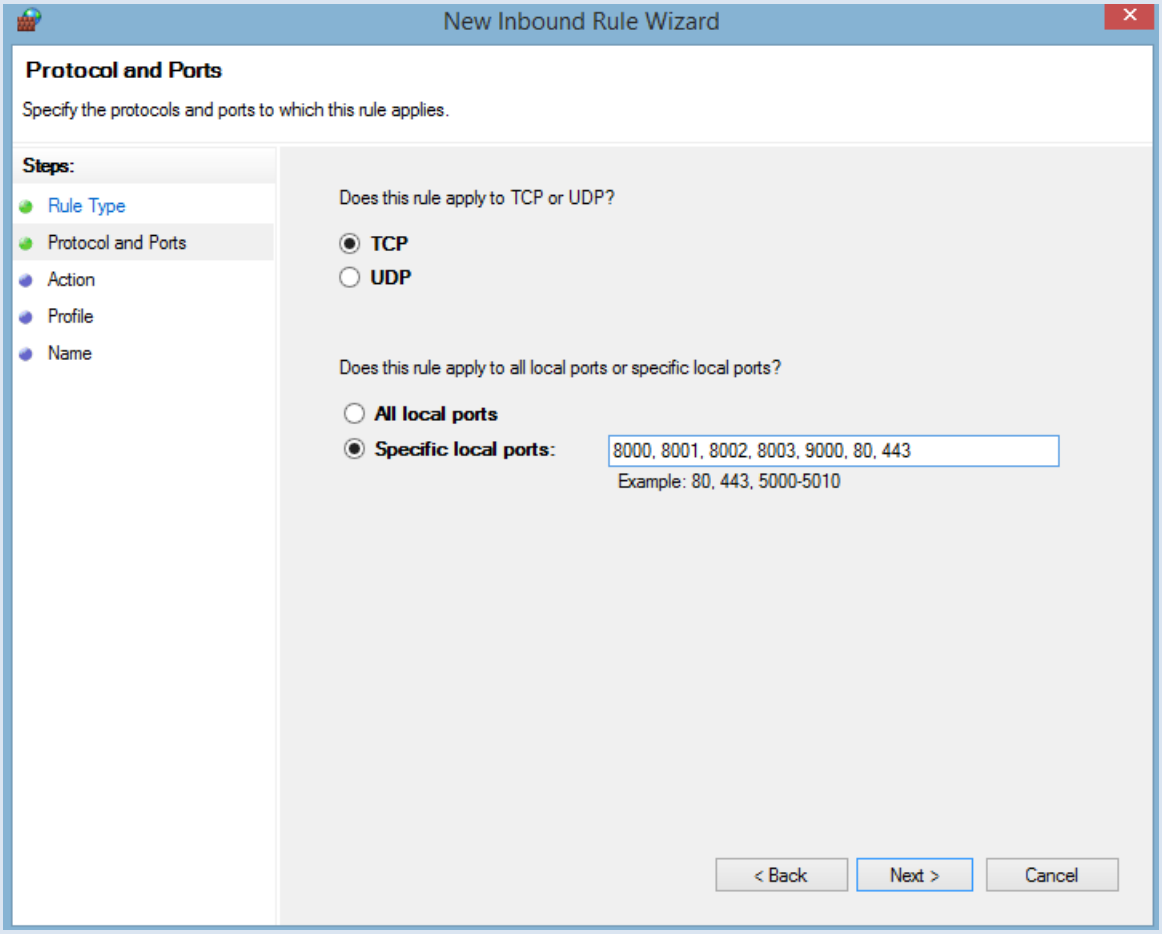
In this case, port 8000 was the localhost we needed the forwarder to access.

It was a port recommended by Splunk for better ease.



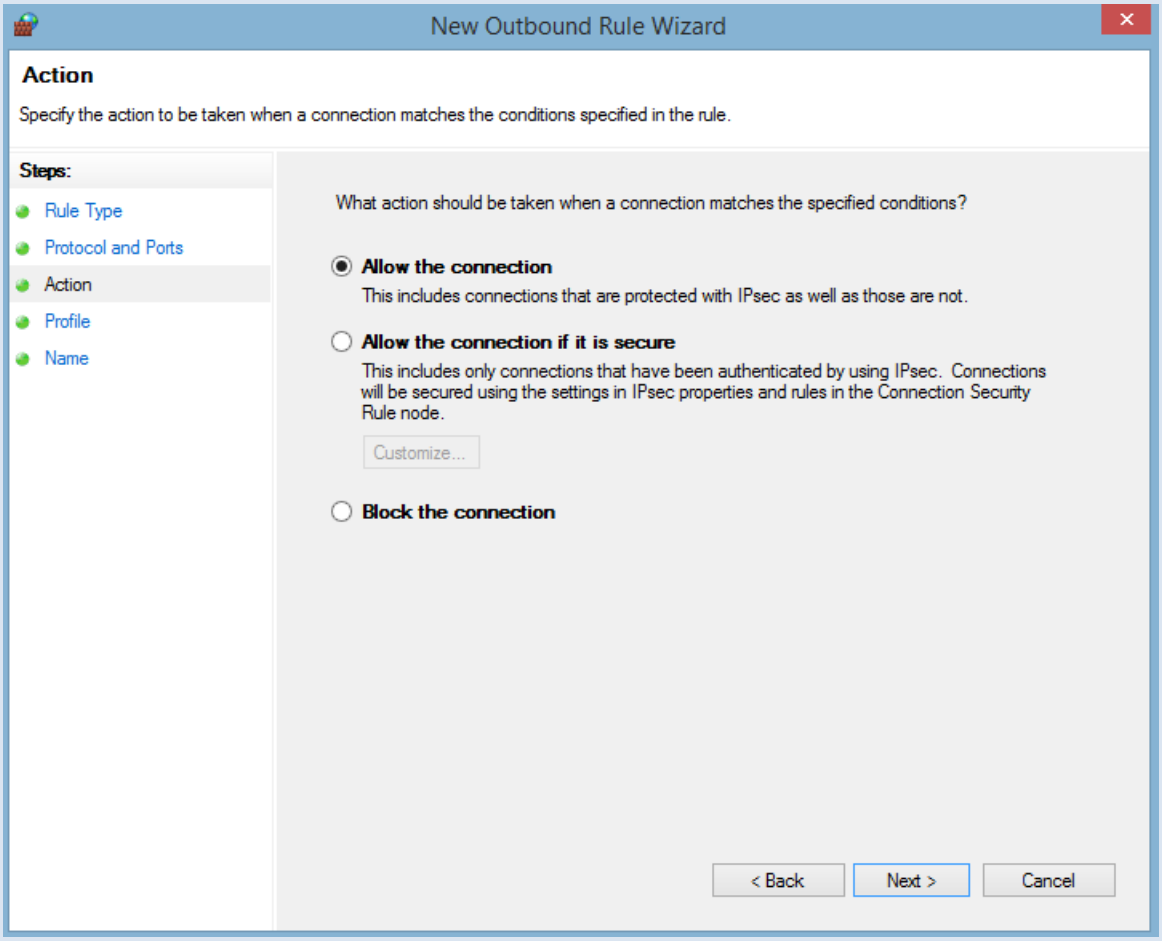
STEP 2: Create inbound and Outbound rules





After Configuring the Inbound we will follow the same steps to do the Outbound.

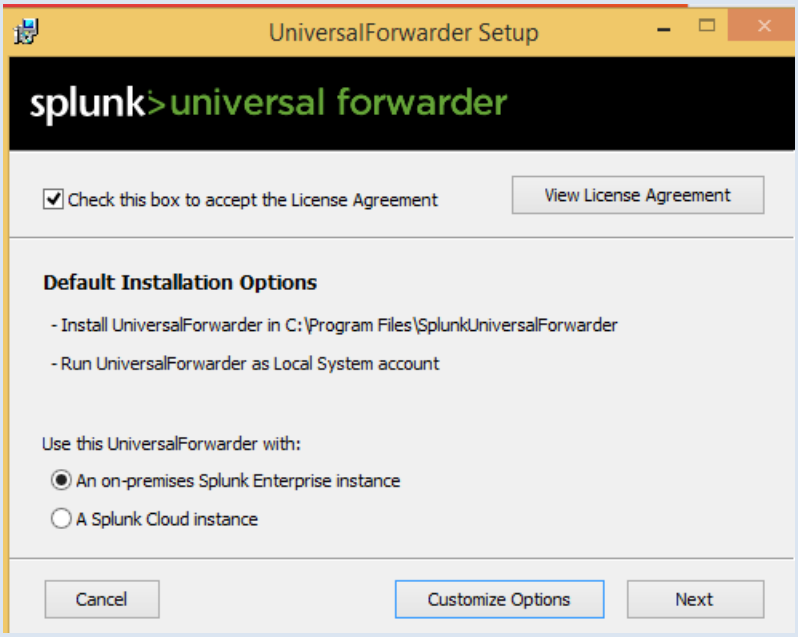
Make sure to select * Allow the connection



Installation Steps

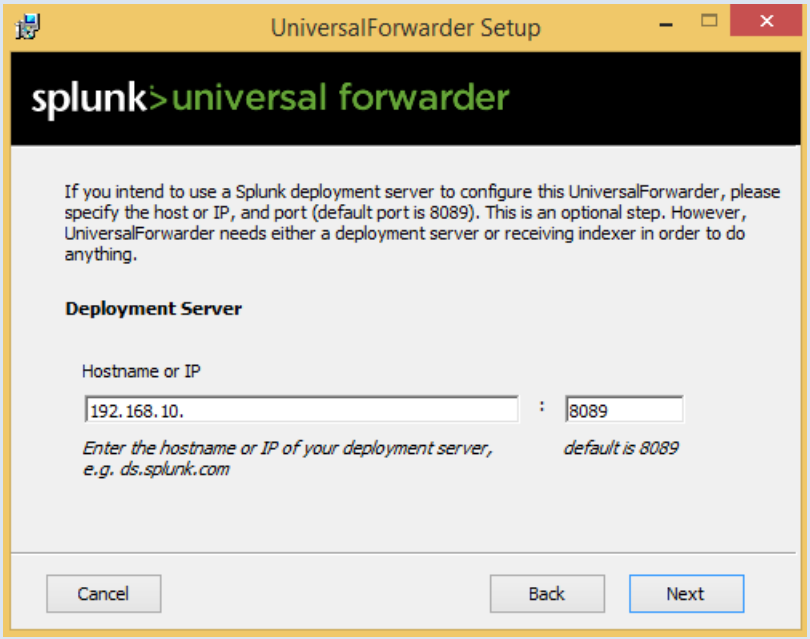
Step 1: Select an on premise splunk

Industry level workplaces deal with splunk cloud instances, however for our lab environment we will be adding data manually.



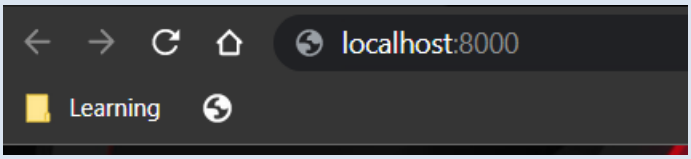
Step 2: Setting up a Deployment Server

Enter the PC ip address along with the port number recommended



Step 3: When completed open internet browser

Step 4: Access splunk through localhost:8000

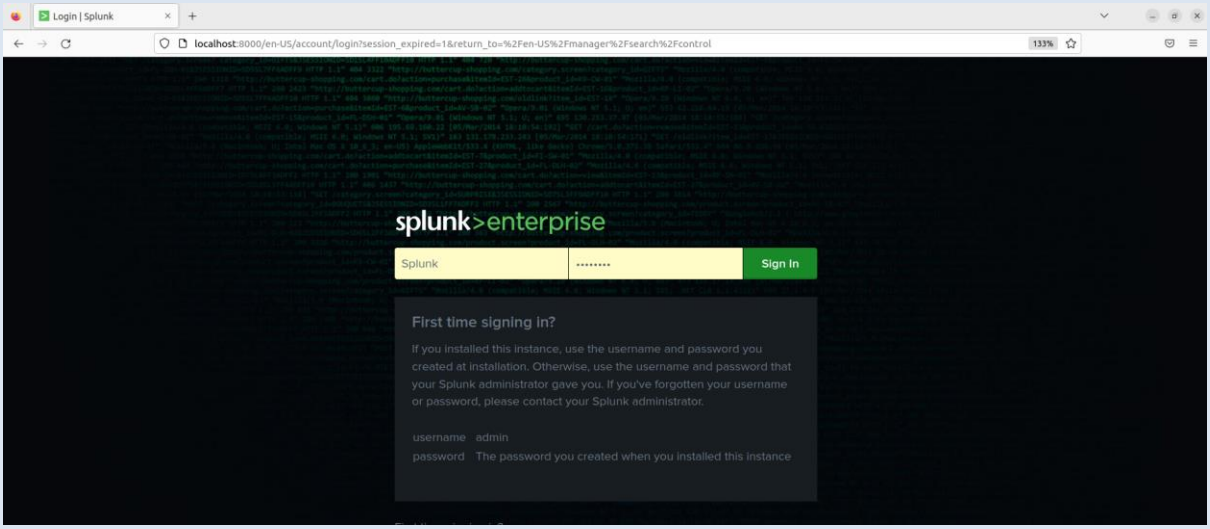


It is that simple for the universal forwarder to run.

The employee would use splunk through localhost, making it much easier to deal with and prevents accidental deletion on the users end.

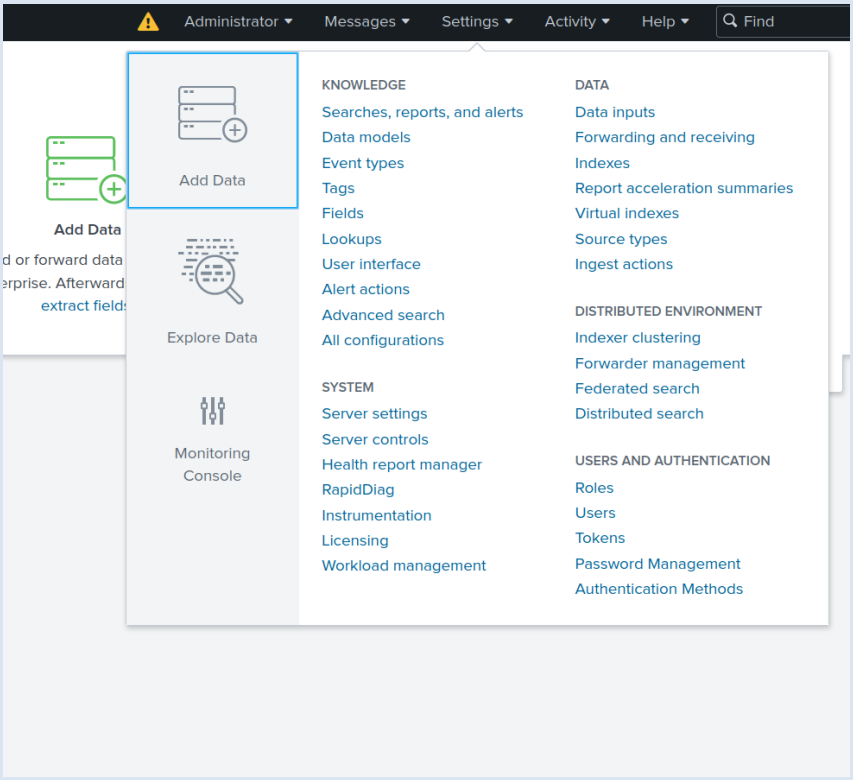
Add data to forwarder

Step 1: Access through the localhost

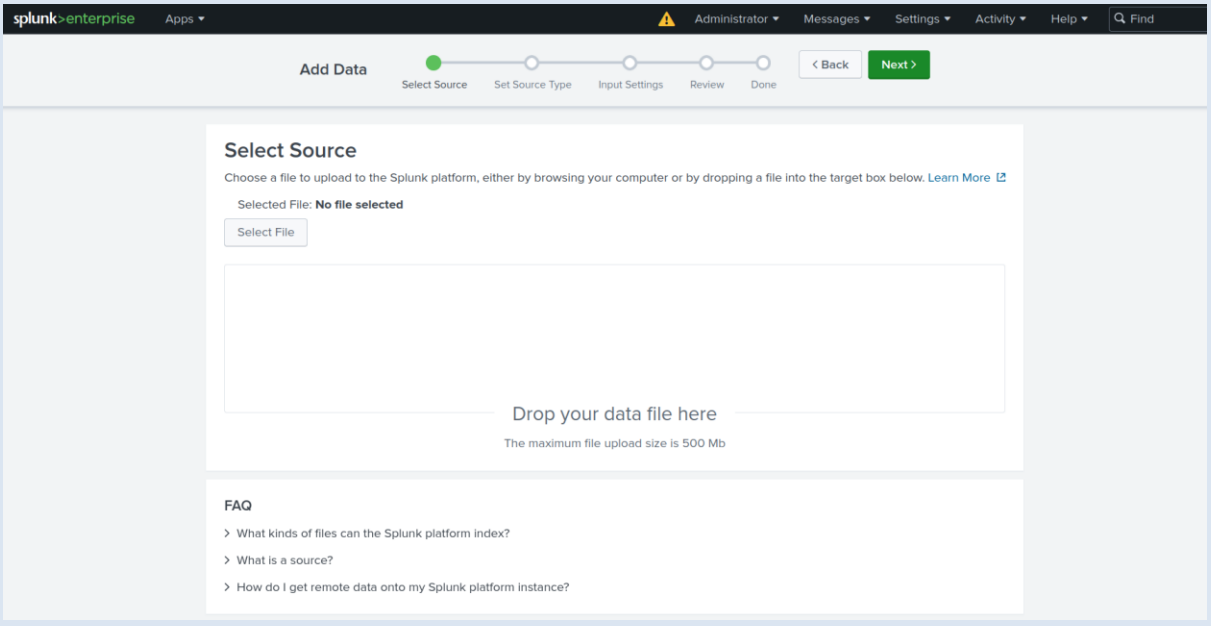


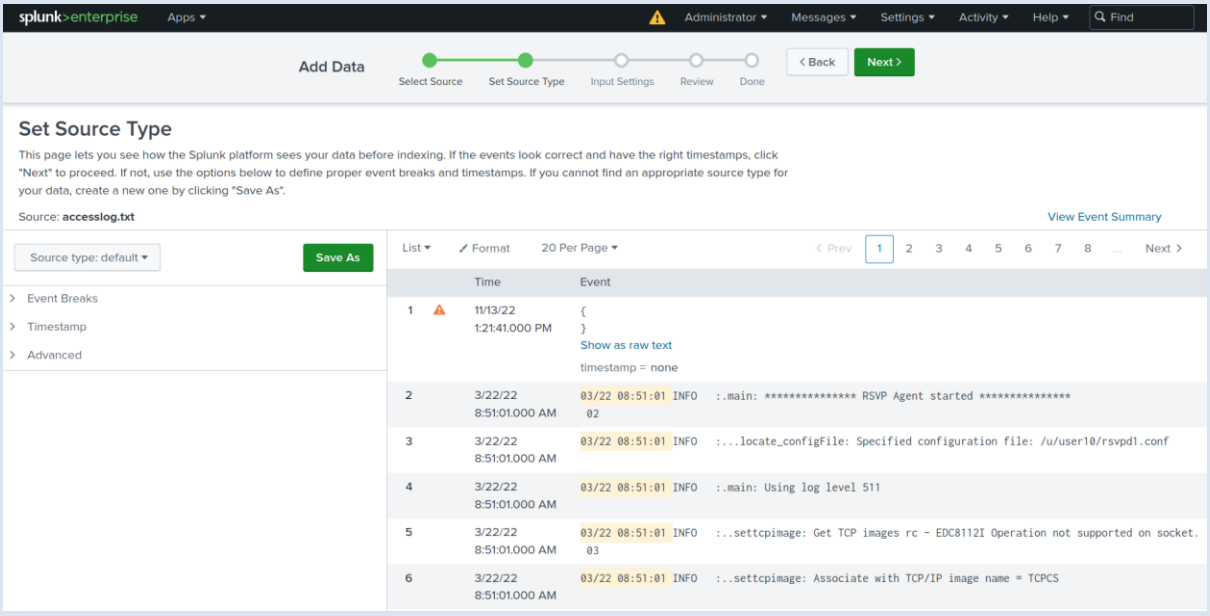
Step 2: Enter Account admin information

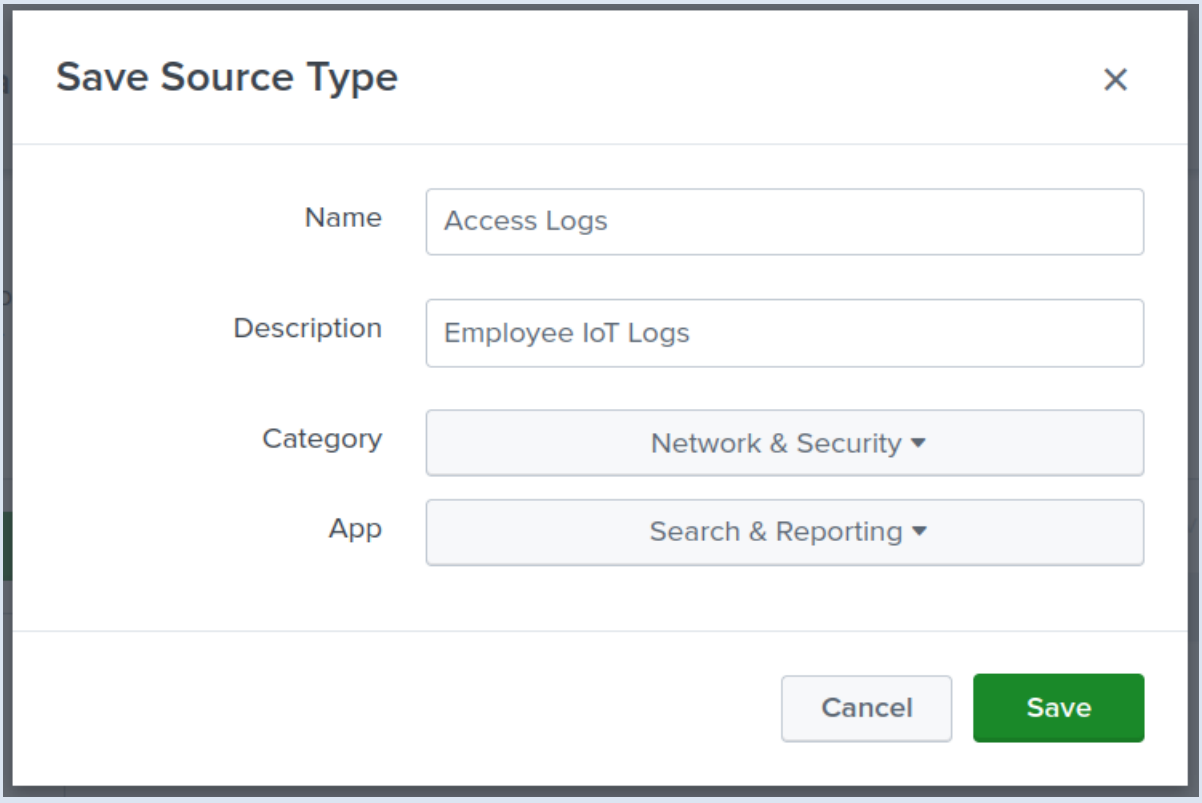
Step 3: Settings > Forwarding and Receiving

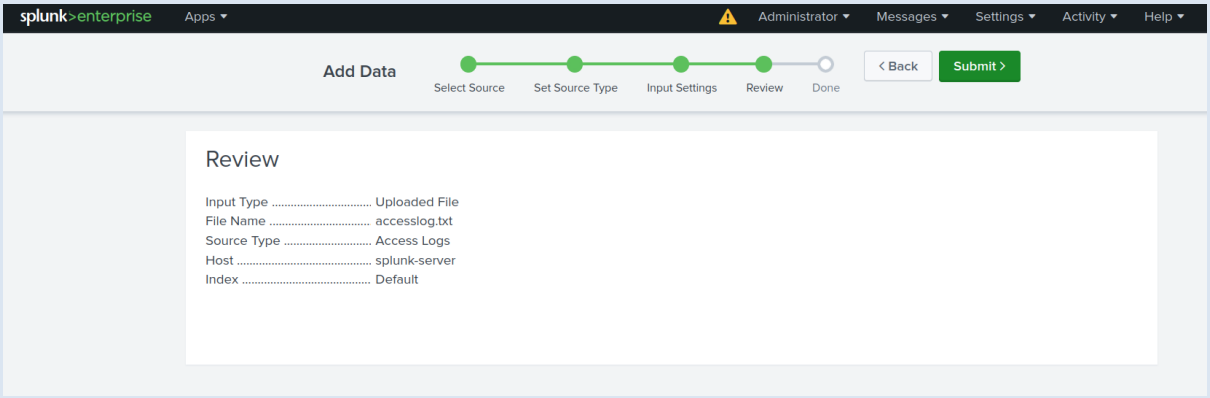


Step 4: Select access file log to add source







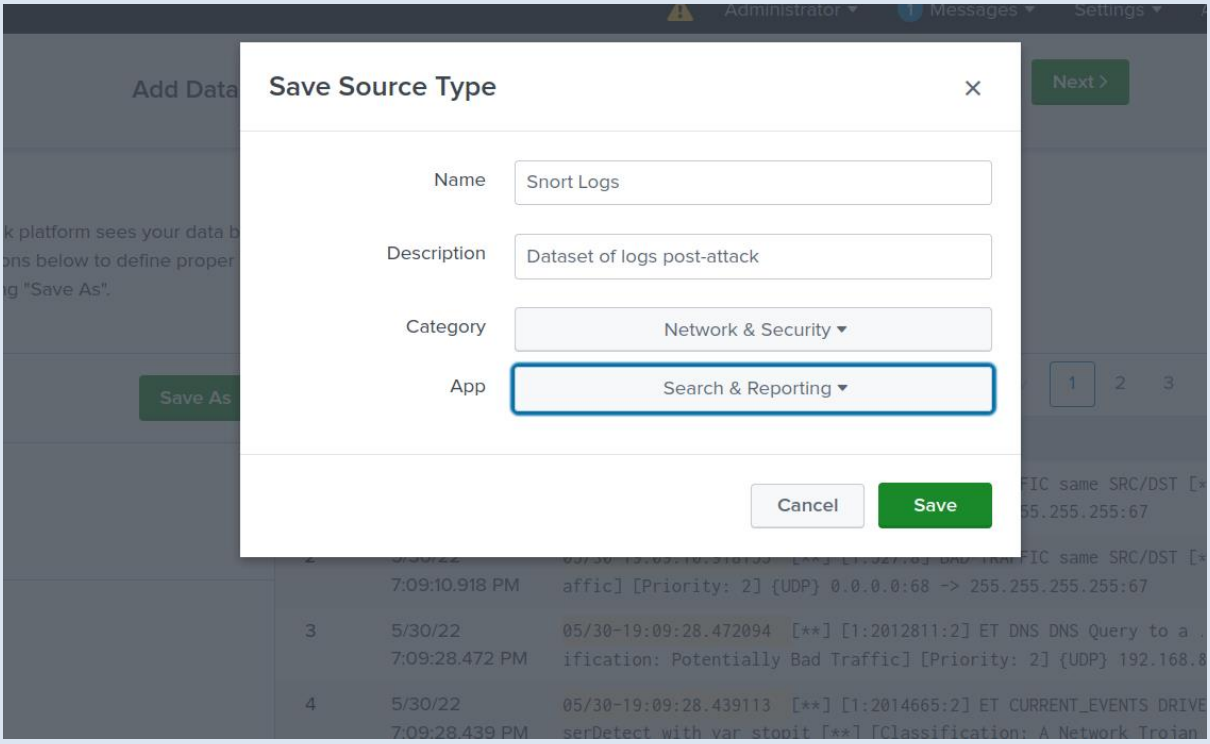


To test attack methods, we added an access log from a device exposed to attacks

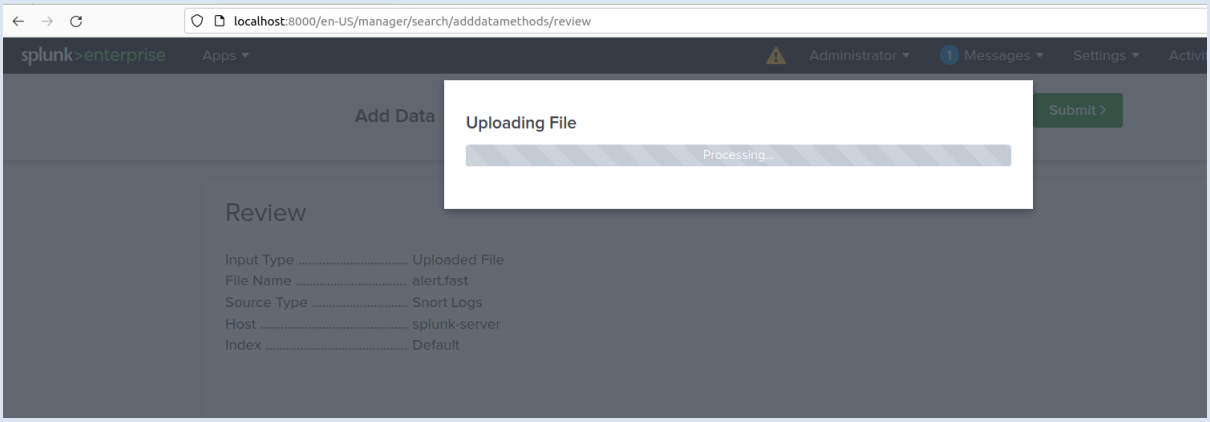
Live monitoring uses the cloud resources to alert threats.

For the purpose of this demonstration, we will be adding access logs.

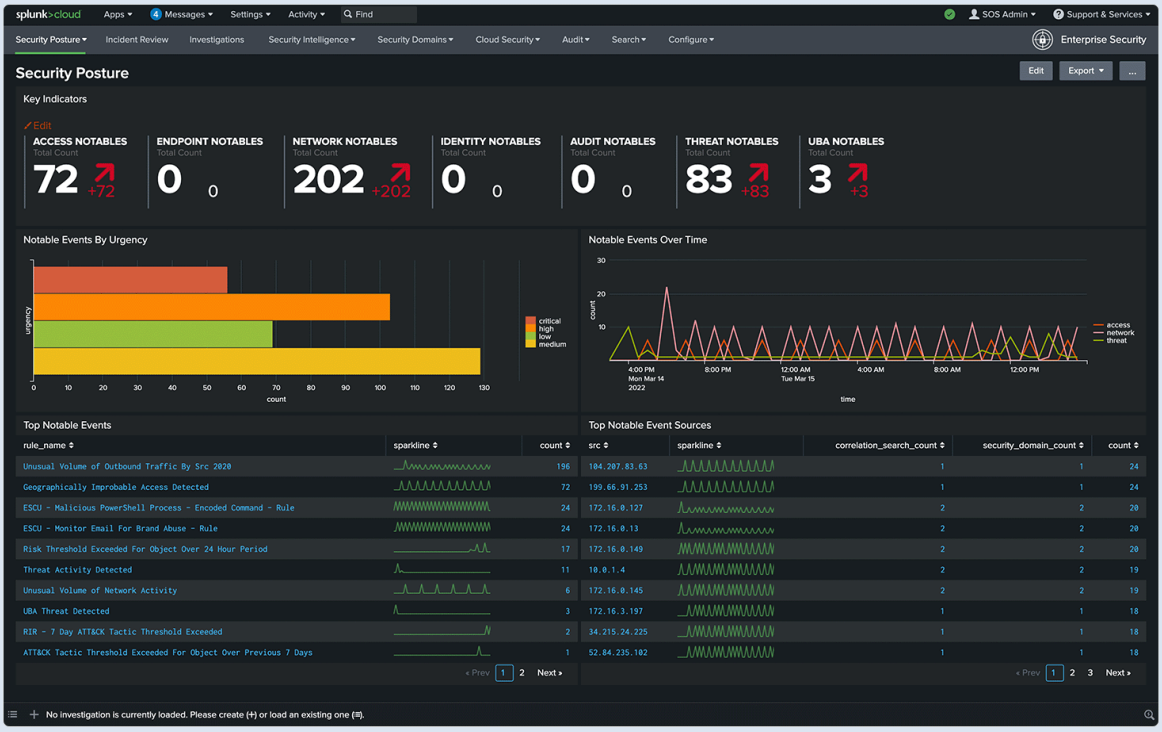
The file was saved as alert.file



Upload time will differ according to the size of the dataset.



Security Posture

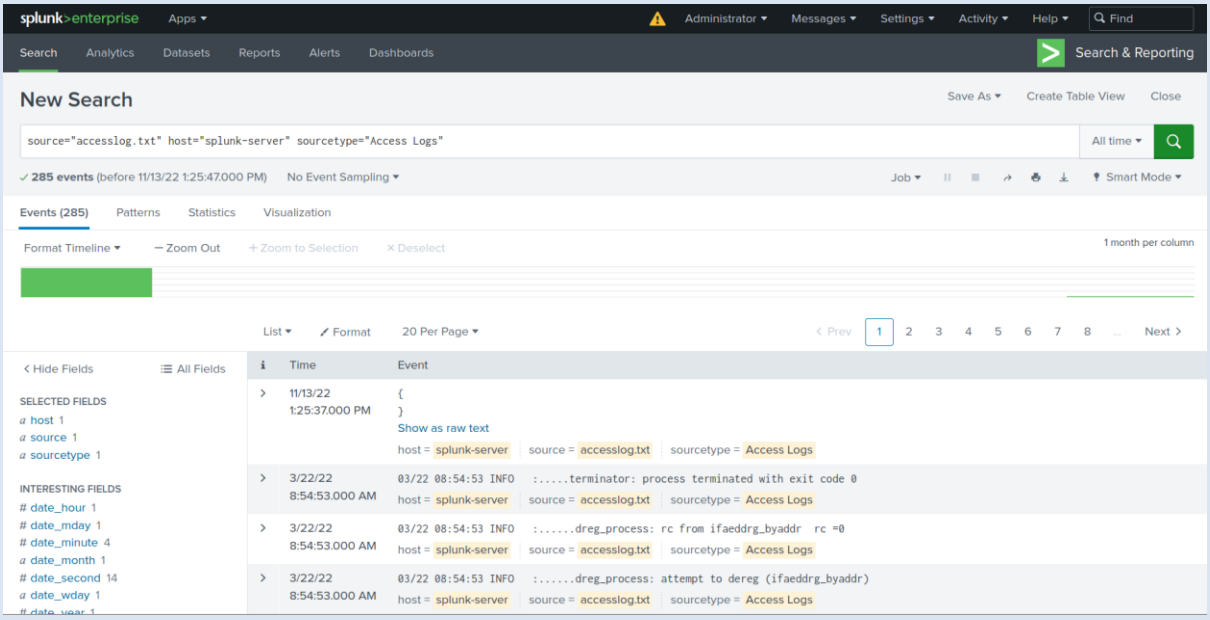


The above image was the dashboard of the data received by the windows 10 defender pc.

There are overwhelming numbers of security attacks affecting the industry. Splunk security helps observe and attack through the security services. With the machine learning components, the security will be counter for the network attacks. This level of enhanced detection allows the user to find the areas to fixate rather than finding an entry point through endless data [9].

Cloud features as well as hybrid environment are compatible to use this feature and install in all supported devices. What we have done with the project is a very simple step to demonstrate the outcome of an environment using this feature. The access log files entered provided outcomes and alerts as they were snort attacks added to test them.

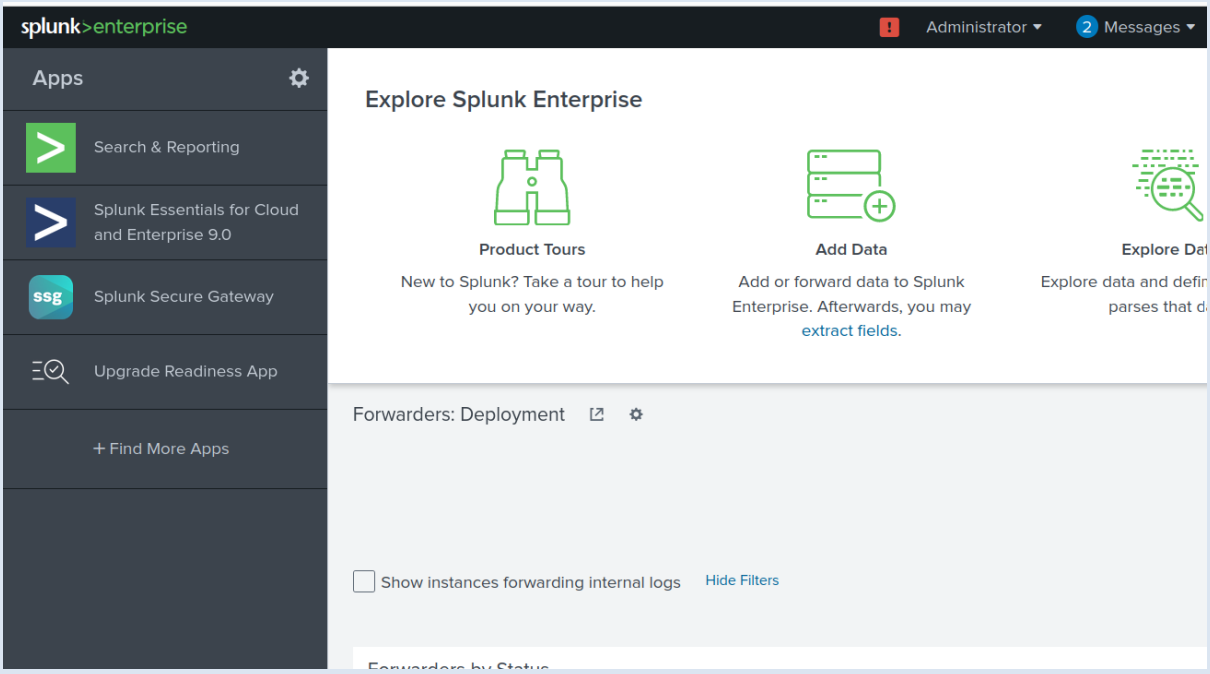
Splunk had successfully alerted them and highlighted the index value associated with it.



With the attack keyword the date, and server related to the attack has been flagged.

When selecting view attacks, the brief information will be presented to the user.

Errors Occurred



Splunk displays any level of errors occurred

This made it easier for us to determine where to troubleshoot. Some errors were because we failed to provide a sound log file. We managed to get an access file that was populated by snort requests.

These errors developed troubleshooting skills within the team.

1. Installing Forwarder on new VMs

Splunk required other machines to stay active as well. To have deployment server and a receiving end to make the data parse. The meeting time was 4 hours one day a week, which made turning on virtual machines, copying them and moving from device to device harder to work with.

2. Failure to save data

The Splunk instance would have lost all the configurations unless they were saved. This is a lesson learned with experience due to failure of simply saving the instance configurations when the installation is complete. When the forwarder was re installed the new indexer was performing slowly.

3. Not loading the past added data

Adding new data sources cost the instance to overload its allocated data resources. In order to protect the storage capacity Splunk has allocated limitations to the storage it takes. When trying to add new data every time we test our lab, the insufficient storage error kept interrupting.

These types of technical errors lead us to delaying the due date.

Skills Learned

After meeting with members and identifying the delay, we had managed to narrow our work priority to getting the systems working to provide a successful report.

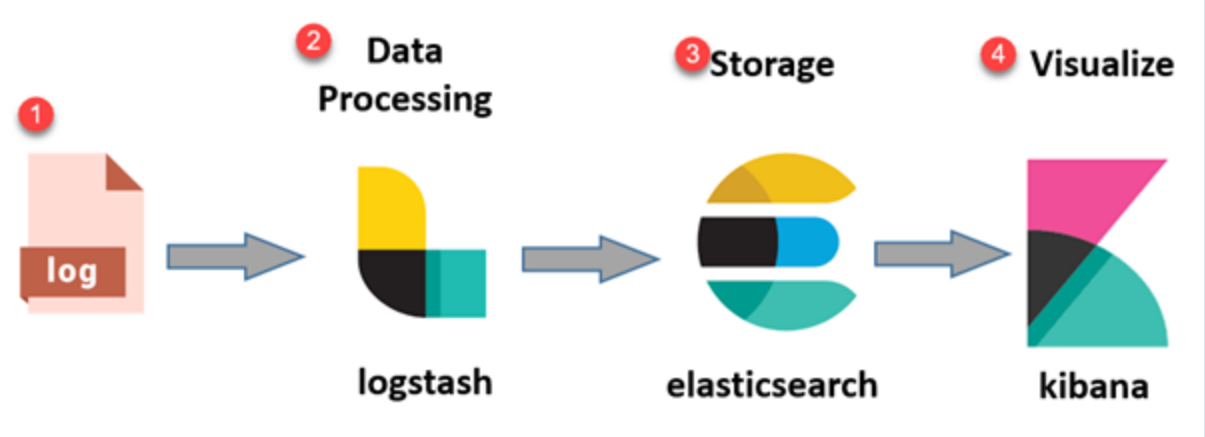
Some of the skills achieved through Splunk enterprise management,

1. Splunk Enterprise product and Service Identification
2. Installing universal forwarders
3. Troubleshooting Networking Errors
4. Priority Tasking

Each member focused on different parts of the topology mainly, however all members taught each other's their work part.

ELK on Ubuntu and Windows:

What is ELK



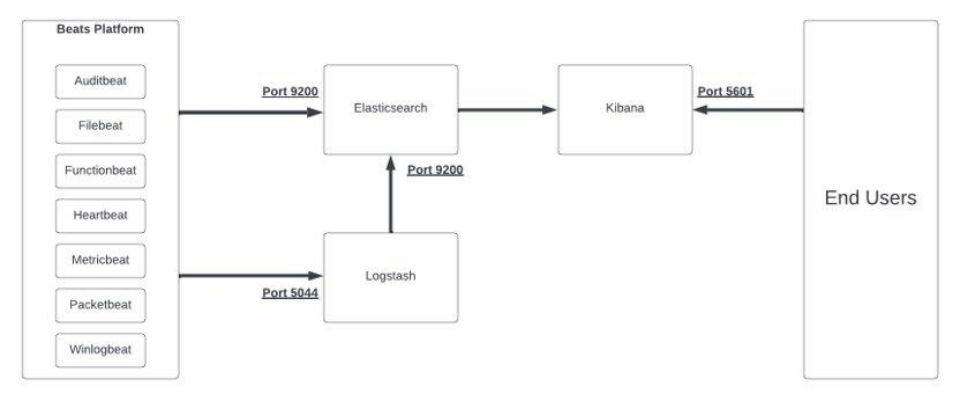
ELK is an open-source log analysis solution, which combined Elasticsearch, Logstash, and Kibana [10]. Whether it is a developer or operation and maintenance personnel, analysing logs is a very good way to troubleshoot errors in our daily work, but if the platform to be analysed is relatively large, there will be relatively more days generated, and a centralized life management platform will make our work more convenient and easier. In addition, through this centralized management day, we can also observe other useful information.

Elasticsearch is a search server based on a full-text search framework. It adopts the Restful API standard to provide high-scalability and high-availability services. It also has real-time search capabilities and real-time analysis capabilities. It allows people to set up many nodes easily by adding them into the same cluster. Since it is a distributed engine, each of the node have a backup, when some nodes are down, it can still work fine.

Logstash is a tool that runs on the Java emulator to collect, analyse and forward data. It is like a data pipeline through which logs generated from various systems can be processed. It can centrally process various types of data, standardize data in different modes and formats, and quickly expand and customize two consistent formats and very convenient Add plugins to customize data sources.

Kibana is an open-source analysis and visualization platform. It can be connected to elasticsearch, it has very flexible interface design, easy to analyse and share the results, it can generate a variety of data charts, such as histograms, pie charts, scatter diagrams, and even maps.

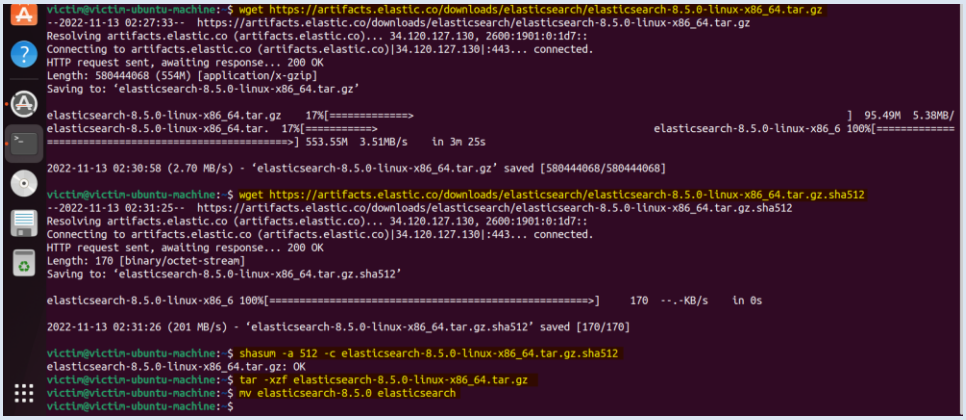
How ELK works?



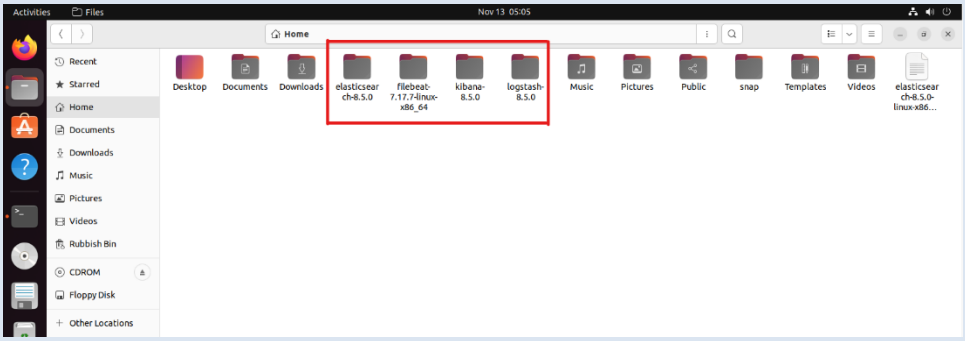
The whole process begins with filebeat collecting data, and then sending it to port 5044, and logstash listens to the information of port 5044 and starts filtering, parsing the collected data, converting it into json format data, and then sending it to elasticsearch on port 9200, and finally it can be displayed graphically through kibana. In fact, some steps in this process can be changed. For example, we can skip logstash and send the collected data directly from filebeat to elasticsearch, but this method also skips the process of parsing and processing data .

Although we can directly download and install various software on the official website of elastic stack, we choose to use the terminal and command line to perform it because it is easier to demonstrate.

The commands in the figure download elasticsearch, then verify that it is the correct file and decompressing it. We have used the same method to download, verify, decompress and install kibana, logstash and filebeat.



The figure below shows that all four of the ELK software are located under the HOME directory, this will make us easier to manage and configure different settings.

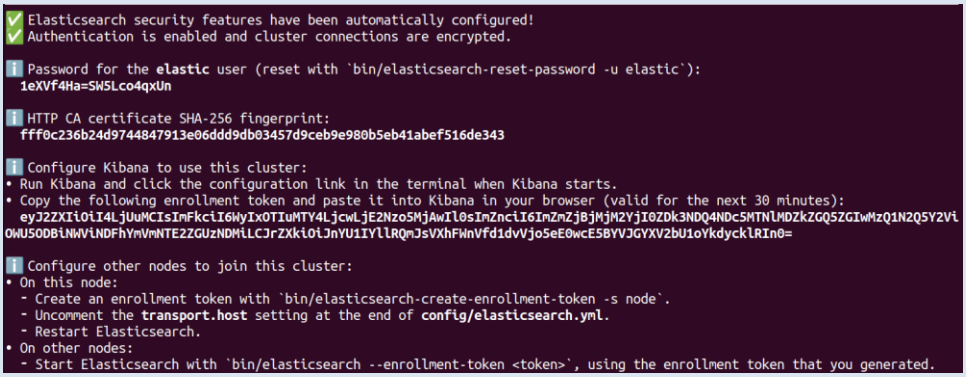


After the installation is complete, follow the correct order to start each software. Because Filebeat needs to set port 5044 of logstash, and logstash and kibana also need to specify port 9200 of elasticsearch, so elasticsearch will be started first. The command below starts elasticsearch.

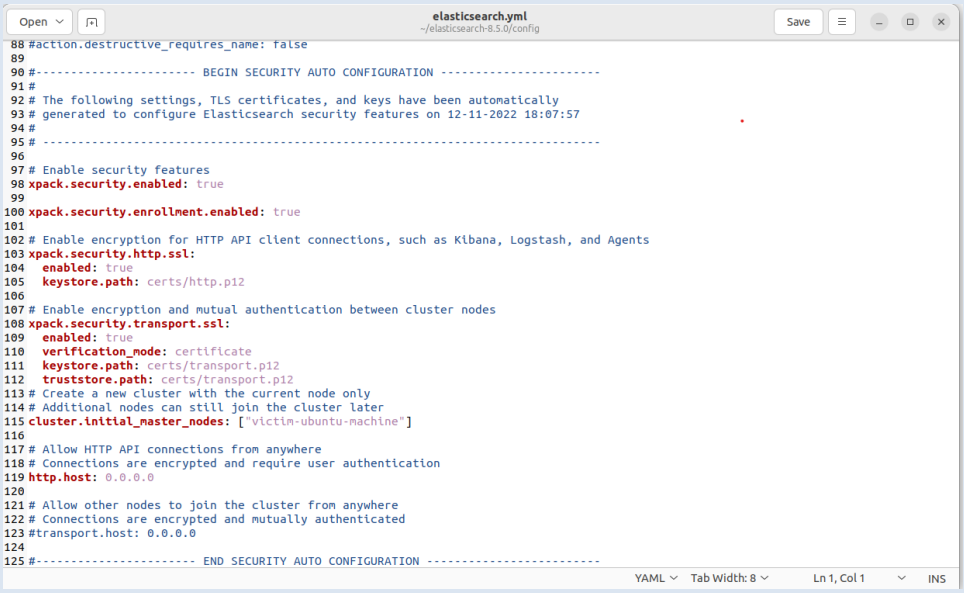
```
victim@victim-ubuntu-machine:~$ ./elasticsearch-8.5.0/bin/elasticsearch
```

When we start elasticsearch for the first time, the information in the figure will be displayed in the terminal, including the login password, HTTP CA certificate and the token used to connect to kibana. Since we

have installed ELK so many times, we find that the best practice is to save the whole paragraph to a note after we get this information. This information can always recall by running the related commands under the bin directory.



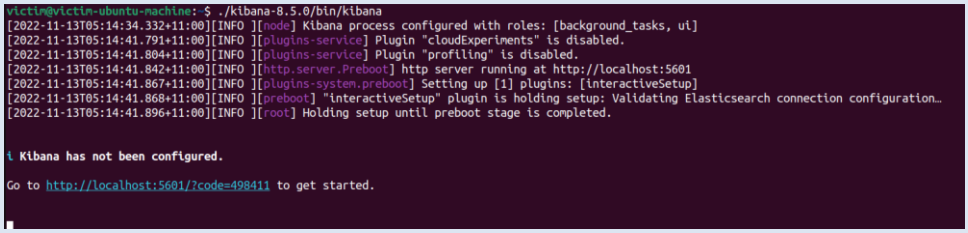
There are different ways to configure elasticsearch setting, because we are not used to json and to avoid mistake, we decided to do all the setting in the .yml files. All the settings in the elasticsearch.yml was commented, some of them will uncomment automatically when we start elasticsearch in the first time. Whenever we change a setting inside the yml file, we must restart elasticsearch to update the settings.



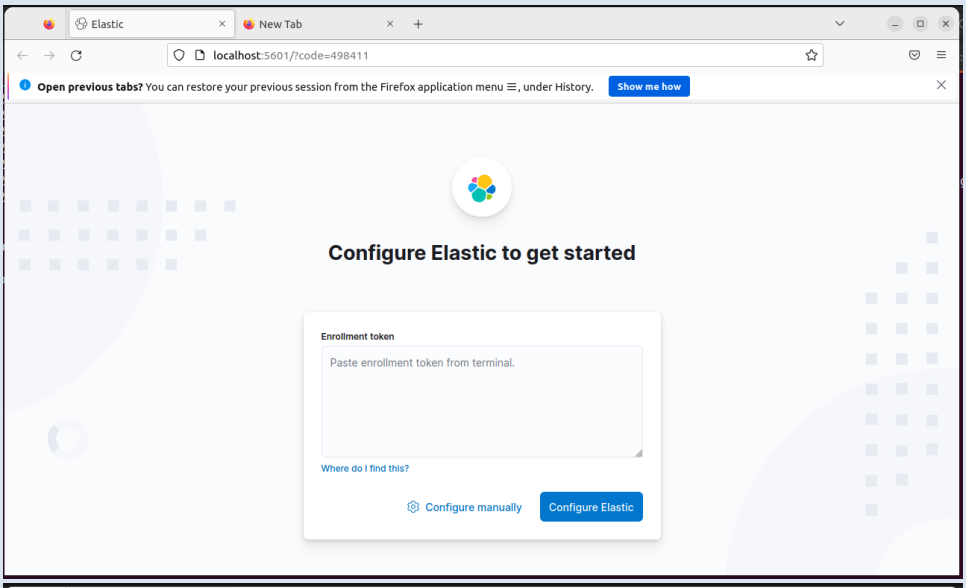
Any misconfiguration will bring us an error, to verify elasticsearch is running, enter the command below with the elastic password (the one

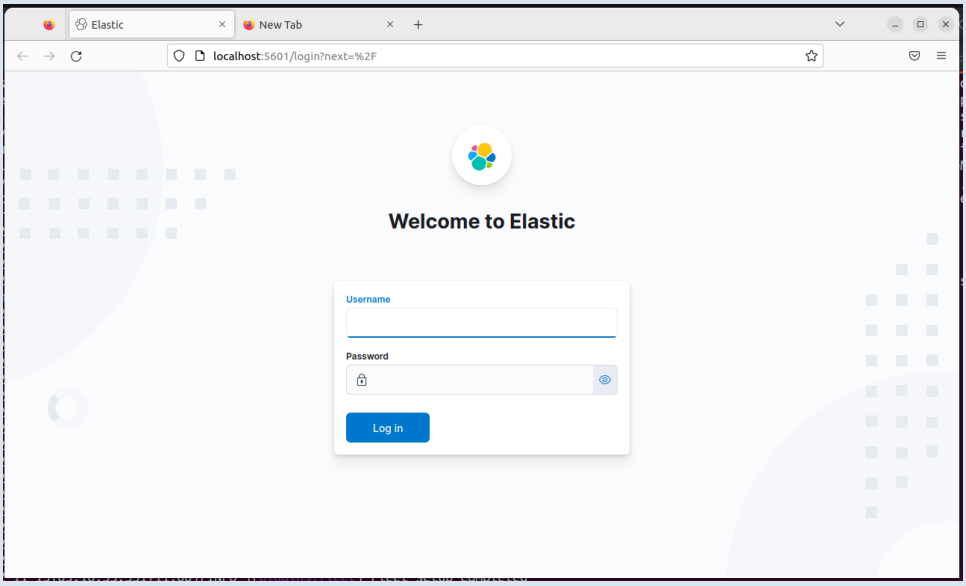
we save in the note) and if you get the message below means elasticsearch is working fine.

Then we start Kibana using the command below.

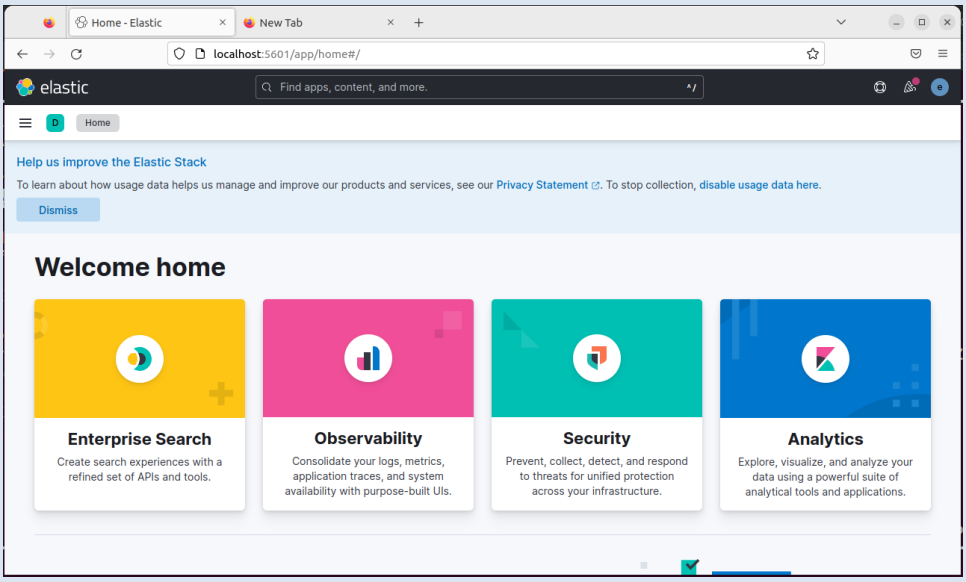


Click on the blue link, it will bring us to the web browser, to connect Kibana with our elasticsearch, we input the token that was general when the elasticsearch start on the first time. That token only works within 30 minutes, if it passed the used by time, we can use command ‘bin/elasticsearch-create-enrollment-token -s kibana’ to general a new token. After connecting Kibana with elasticsearch, it requires us to log in to our elastic account.

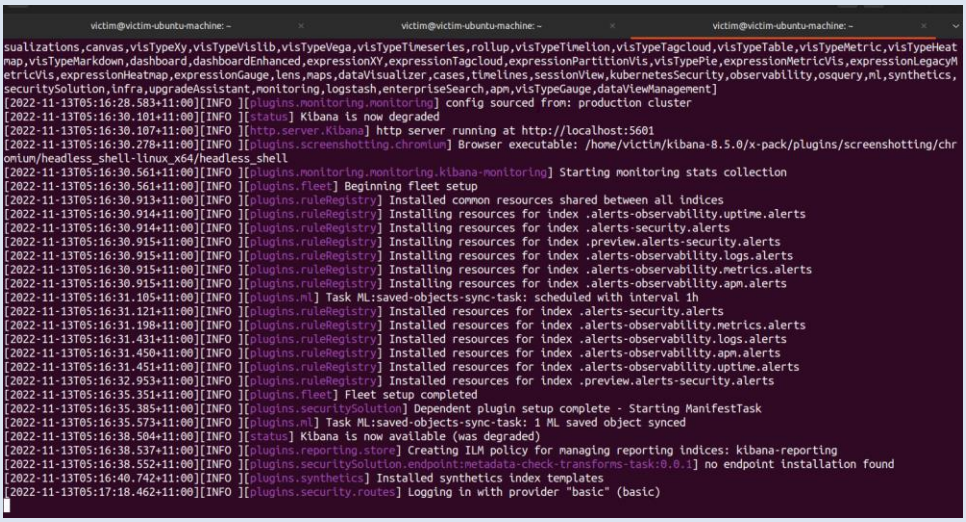




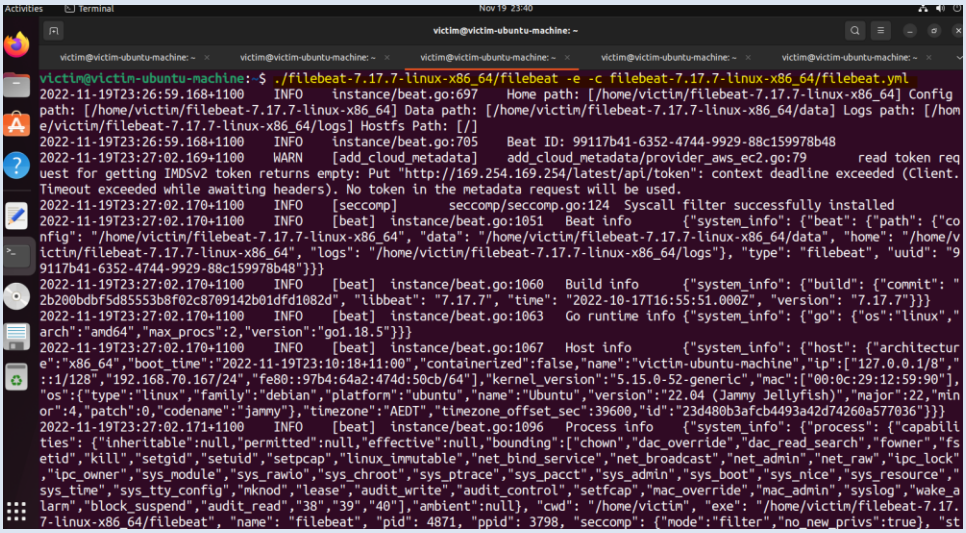
Once everything is set, the following screen can verify that we have connect Kibana and Elasticsearch successfully.



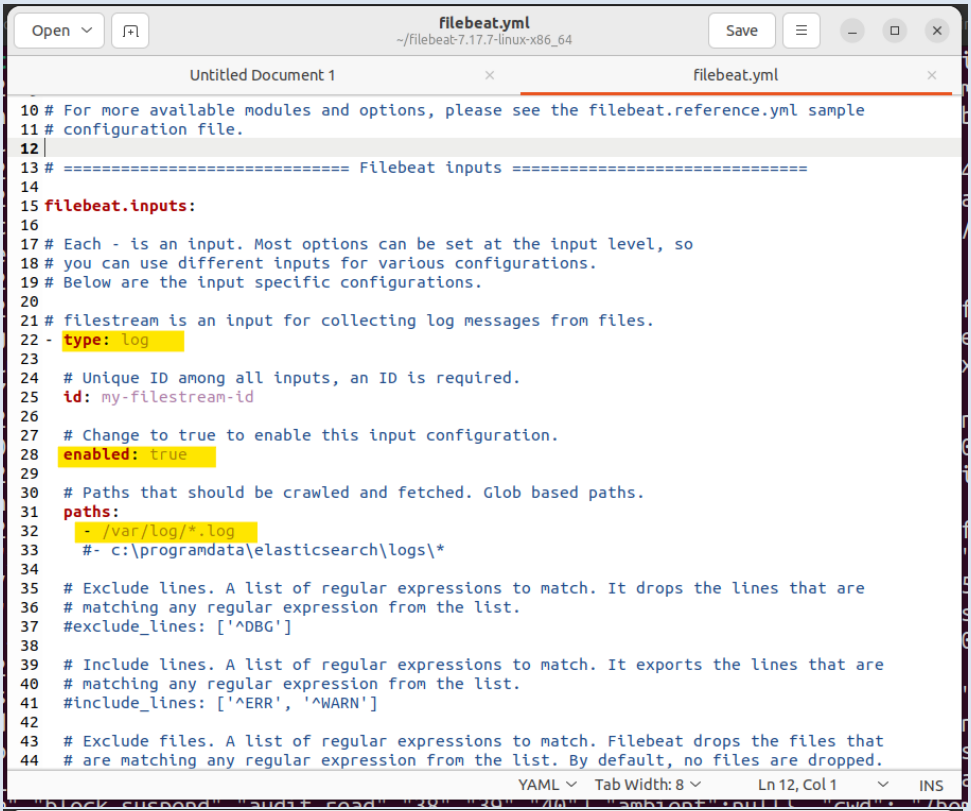
Every single event that we have done will be display in the terminal that is running Elasticsearch and Kibana.

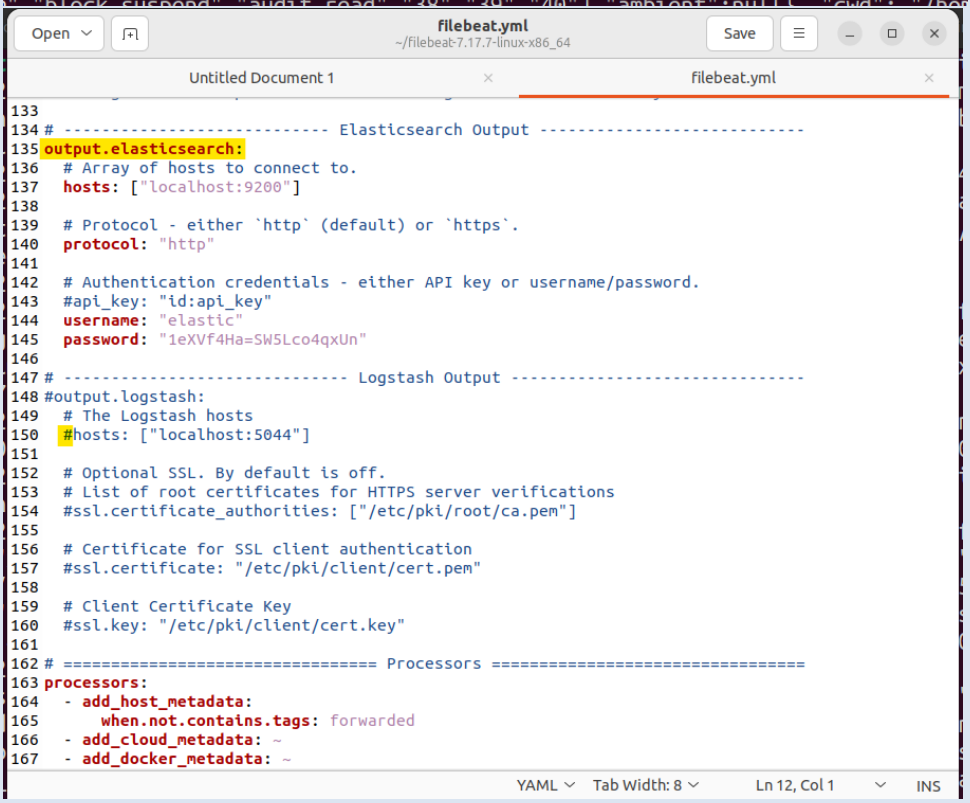


Then we run Logstash or filebeat to forward data to Elasticsearch.



Configurate the filebeat.yml file, enable the function and depending on the need, set the output to Elasticsearch or logstash by commenting or uncommenting the setting.





Problems and solutions whilst setting up elastic stack

1. Logstash configuration contains a syntax error

Not only happened in Logstash, also in other yml settings file. Whenever we configurate the setting in the yml file, everything has to be right, one mistake will return an error.

The solution is:

After we change a setting, run the command '/opt/logstash/bin/logstash --configtest -f /etc/logstash/conf.d/30-lumberjack-output.conf' to validate the setting.

2. SSL certificate is missing or invalid

SSL is needed to establish communication between logstash and filebeat, if the SSL is missing, the service will not be able to start.

The solution is:

Copy the certificate from logstash to the logstash forwarder.

3. Error when starting elasticsearch using root account

For security reasons, elasticsearch is not allowed to run as root.

The solution is:

Create another user and assign permissions to that account, then switch to that user and use that user to run elasticsearch.

What have we learned?

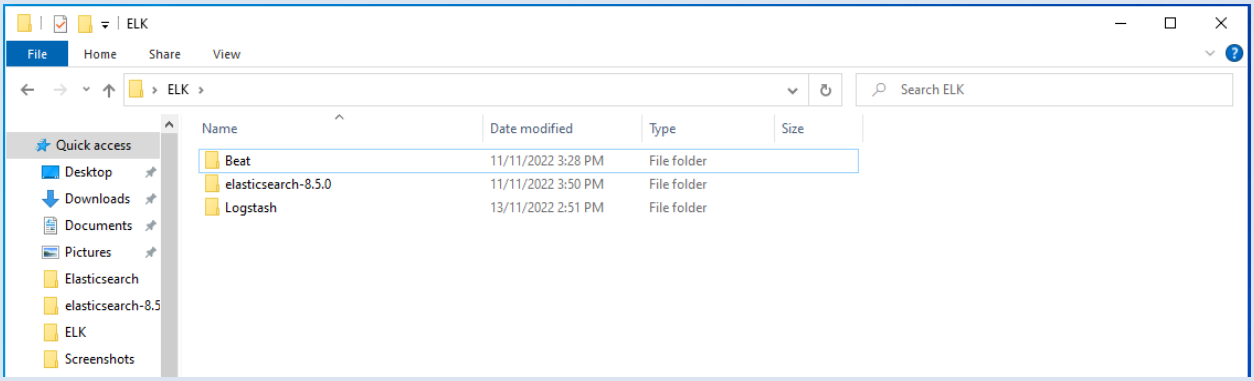
When we started this project, we didn't know anything about elastic stack, and faced many different problems from installation to configuration. We kept changing, trying and used many different methods to install before we successfully started elasticsearch. After start-up, we need to try to set different settings. Whenever one of the settings is incorrect, it will cause elasticsearch to fail to work.

After reading many related documents, we finally managed to make all the software work and communicate. Since we have read a lot of documentation to learn about elastic stack, we discovered how powerful this tool is, and what it can be used to help us to make our cyber security career easier.

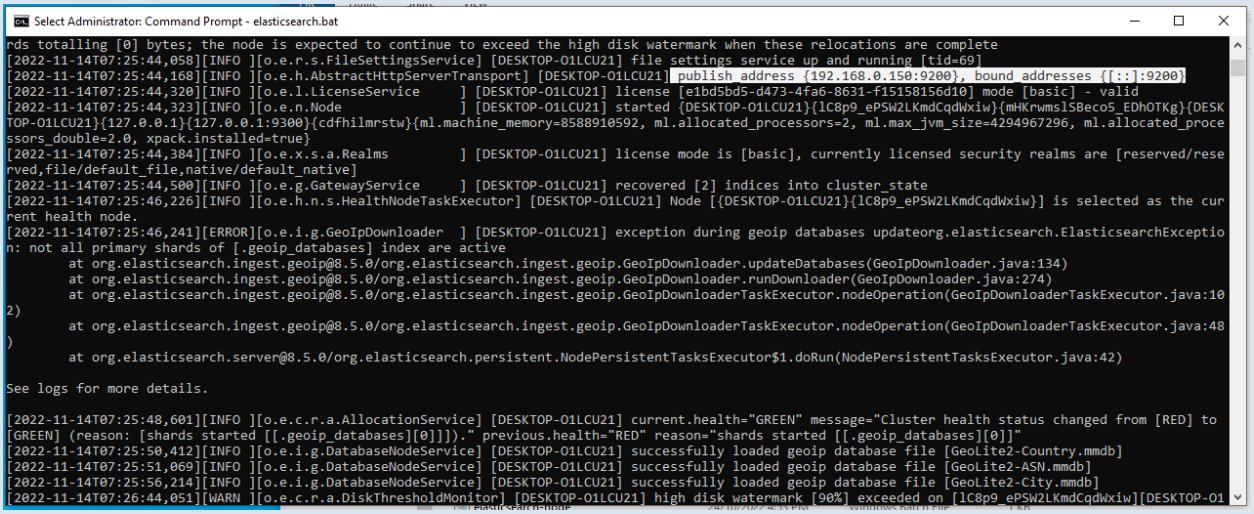
In addition to learning the operation of the elastic stack, we also have a deeper understanding of the Linux operating system and are more capable of handling Linux-related operations than at the beginning. This is a very useful unexpected gain for us.

Elk on Windows

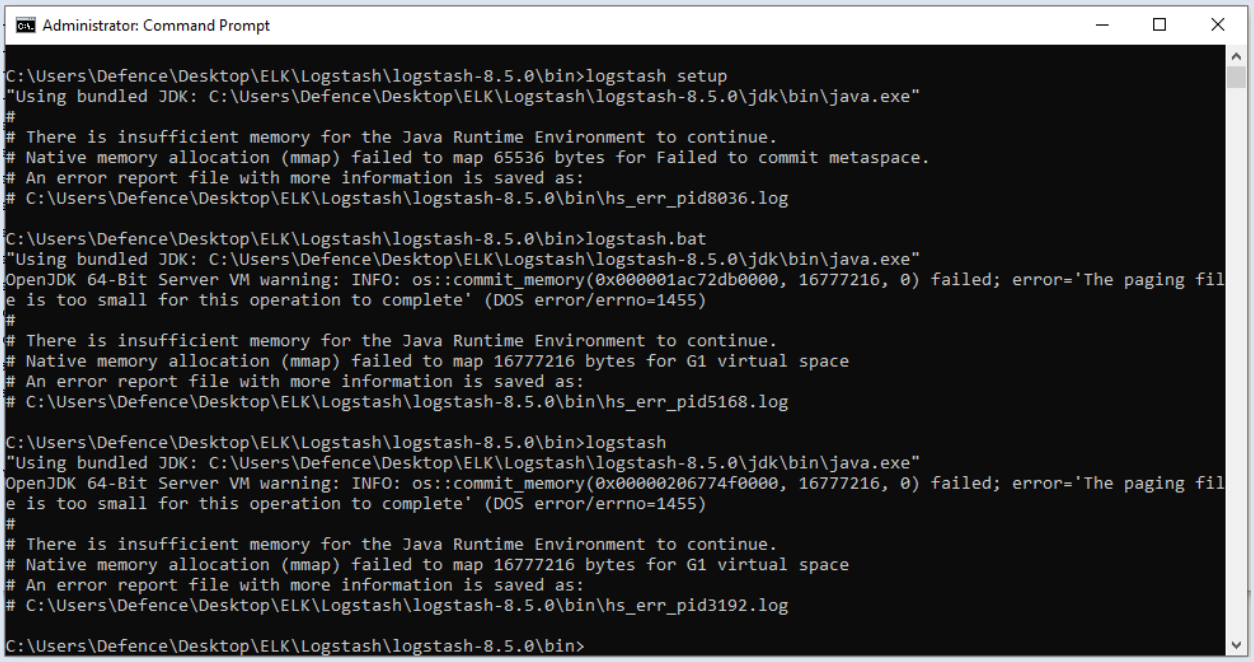
Similar to Ubuntu, download and extract the zip files from the ELK website on the victim machine (Win10). The image below shows we have downloaded Beat, Elasticsearch and Logstash.



After installing elasticsearch, you will see the server running on localhost 9200



After installing Logstash, the server showed some issues with the space



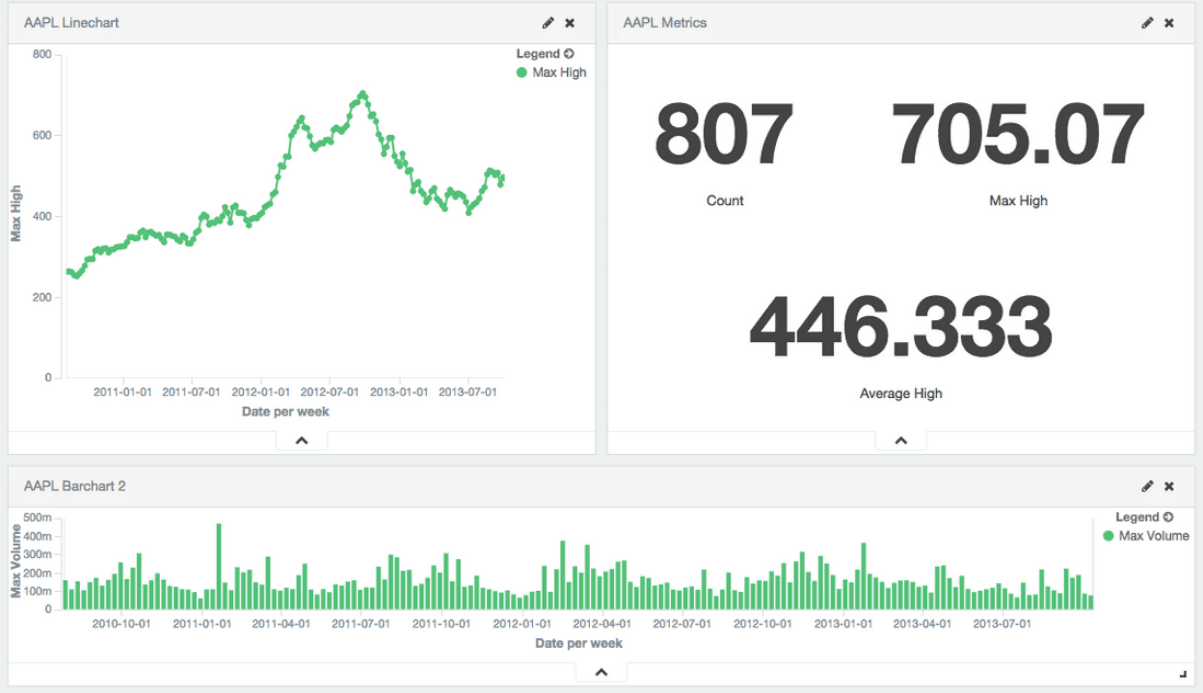
The desired output:

Though we encountered certain connectivity issues with ELK on Win10, we were expecting the following desired output.

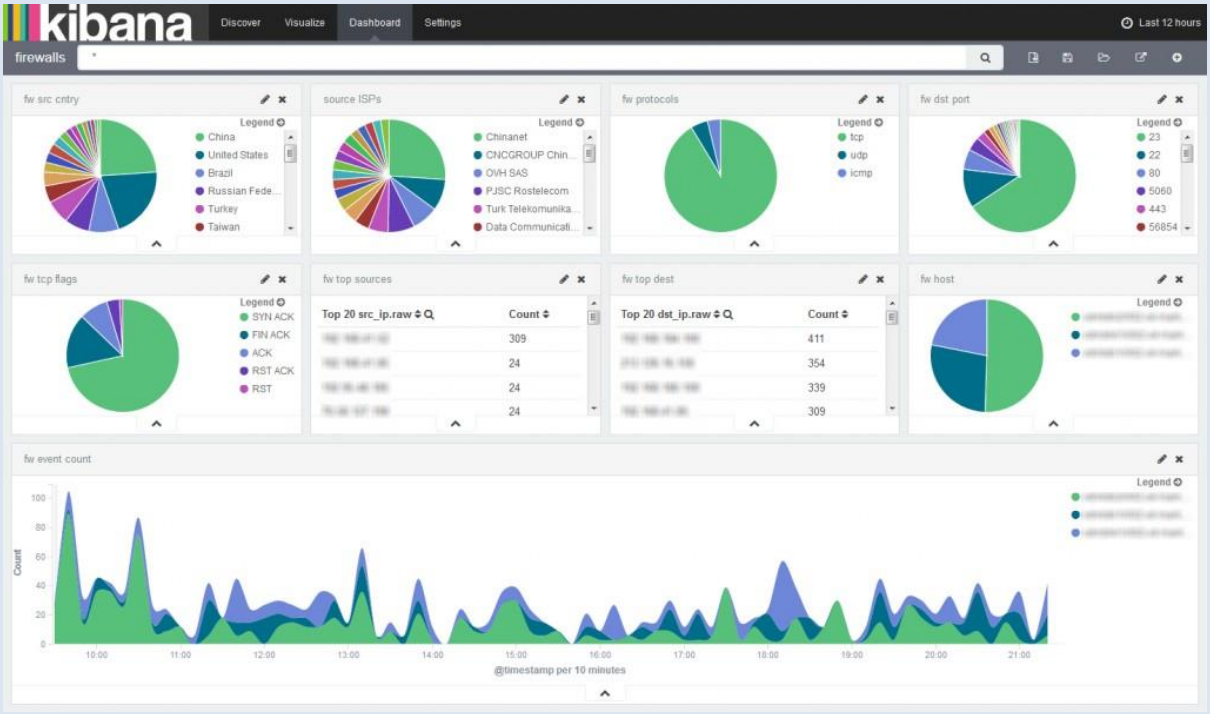
Real Time interactive visualisation

Monitoring Feature in Log stash deployment

Visualizing Data -Including numeric displays



Cisco ASA alerts



Conclusion:

Working with virtual machines is always a challenge. As this project focuses on round the clock monitoring it requires high speed processors, minimum 16GB RAM. Not to forget the space as monitoring network traffic requires a lot of space. It is not recommended to conduct this project on virtual machines because combining all the VMs in one system takes a long time that in return may encounter connectivity and compatible issues. Overall, it was a great experience and learning whilst working on this project.

References

[1] M. Buckbee, "Varonis," 15 06 2020. [Online]. Available: https://www.varonis.com/blog/what-is-siem. [Accessed 20 11 2022].

[2] A. Heddings, "How-To-Geek," 23 06 2020. [Online]. Available: https://www.howtogeek.com/devops/which-type-of-networking-should-you-use-for-your-virtual-machine/. [Accessed 20 11 2022].

[3] C. BasuMallick, "Spiceworks," 10 02 2020. [Online]. Available: https://www.spiceworks.com/tech/networking/articles/what-is-wide-area-network/. [Accessed 15 10 2022].

[4] I. Khan, "4sysops," 22 09 2022. [Online]. Available: https://4sysops.com/archives/how-to-install-the-pfsense-firewall-on-a-virtual-machine/. [Accessed 12 10 2022].

[5] C. Lloyd, "How-To-Geek," 30 03 2018. [Online]. Available: https://www.howtogeek.com/346907/backups-vs.-redundancy-what%E2%80%99s-the-difference/#:~:text=Redundancy%20is%20a%20data%20protection,files%20across%20several%20hard%20drives.. [Accessed 23 09 2022].

[6] V. Kumar, "CyberPratibha," 29 06 2021. [Online]. Available: https://www.cyberpratibha.com/blog/using-the-command-line-to-configure-network-interface-in-kali-linux/. [Accessed 10 10 2022].

[7] Vardhan, "edureka," 07 11 2022. [Online]. Available: https://www.edureka.co/blog/what-is-splunk/. [Accessed 16 11 2022].

[8] Sagar, "AdamTheAutomator," 30 06 2022. [Online]. Available: https://adamtheautomator.com/splunk-forwarder/. [Accessed 12 11 2022].

[9] L. Rosencrance, "TechTarget," [Online]. Available: https://www.techtarget.com/searchsecurity/definition/security-posture. [Accessed 09 11 2022].

[10] D. Taylor, "Guru99," 05 11 2022. [Online]. Available: https://www.guru99.com/elk-stack-tutorial.html. [Accessed 19 11 2022].